Московский государственный технический университет
имени Н.Э. Баумана

А.Н. Щетинин

# Применение теории групп в комбинаторике

*Рекомендовано Научно-методическим советом МГТУ им. Н.Э. Баумана в качестве учебного пособия*

Москва
Издательство МГТУ им. Н.Э. Баумана
2013

УДК 519.8(075.8)
ББК 22.141
Щ70

Рецензенты: *Ю.В. Селиванов*, *В.И. Алехнович*

**Щетинин А. Н.**

Щ70 Применение теории групп в комбинаторике : учеб. пособие / А. Н. Щетинин. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2013. — 23, [5] с. : ил.

ISBN 978-5-7038-3657-6

В пособии доказана лемма Бернсайда и приведена без доказательства теорема Пойа о производящей функции запаса классов эквивалентности раскрашиваний. Изложение не предполагает никаких предварительных сведений и доступно студентам первого курса. Введены основные алгебраические понятия, начиная с множеств, отображений и бинарных отношений и заканчивая действием группы на множестве. Пособие содержит многочисленные примеры, а также варианты домашнего задания по вычислению количества способов раскрашивания вершин, ребер и граней многогранников.

Для студентов младших курсов МГТУ им. Н. Э. Баумана, изучающих алгебру и дискретную математику.

УДК 519.8(075.8)
ББК 22.141

*Учебное издание*

**Щетинин** Александр Николаевич

**Применение теории групп в комбинаторике**

Редактор *С.А. Серебрякова*
Корректор *М.А. Василевская*
Компьютерная верстка *А.Н. Щетинин*

Подписано в печать 26.04.2013. Формат 60×84/16.
Усл. печ. л. 1,63. Тираж 500 экз. Изд. № 20.
Заказ

Издательство МГТУ им. Н. Э. Баумана.
Типография МГТУ им. Н. Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.

ISBN-978-5-7038-3657-6 

# ПРЕДИСЛОВИЕ

Не вызывает сомнения, что знакомство с основами алгебры, в частности с теорией групп, необходимо каждому квалифицированному специалисту в области прикладной математики. Теория групп — наука очень абстрактная, и уследить за всеми тонкостями неискушенному человеку сложно. Нашей целью было продемонстрировать пользу этой науки, приведя ее конкретные применения к задачам комбинаторики, имеющим практическое значение. Сформулированная в пособии теорема Пойа (G. Polya) отличается как математической красотой, так и полезными приложениями.

# 1. МНОЖЕСТВА И ОТОБРАЖЕНИЯ

**Множества.** Под *множеством* понимают любую совокупность объектов, называемых *элементами* множества. Запись $x \in X$ означает, что элемент $x$ принадлежит множеству $X$. Множества с конечным числом различных элементов могут быть описаны путем перечисления их элементов. Например, $J_5 = \{1, 2, 3, 4, 5\}$ — множество первых пяти натуральных чисел. Мы будем также использовать запись

$$M = \{x \mid P(x)\}.$$

Это означает, что множество $M$ состоит из всех элементов $x$, обладающих свойством $P$.

Используем стандартное обозначение $\mathbb{Z}$ для множества всех целых чисел.

Напомним, что $X$ есть подмножество множества $Y$, $X \subseteq Y$, если любой элемент $X$ принадлежит $Y$. Пустое множество $\emptyset$

считается подмножеством любого множества. Множества $X$ и $Y$ называют *равными*, если $X \subseteq Y$ и $Y \subseteq X$. *Пересечением* двух множеств $X$ и $Y$ называют множество

$$X \cap Y = \{x \mid x \in X \ \text{ и } \ x \in Y\},$$

а их *объединением* — множество

$$X \cup Y = \{x \mid x \in X \ \text{ или } \ x \in Y\}.$$

Аналогично определяются пересечение и объединение произвольных совокупностей множеств.

Скажем, что система $Y_\alpha (\alpha \in A)$ подмножеств множества $X$ образует его *разбиение*, если

$$X = \bigcup_{\alpha \in A} Y_\alpha, \quad Y_\alpha \cap Y_\beta = \emptyset \ \text{ при } \ \alpha \neq \beta.$$

Пусть $X$ и $Y$ — множества. Множество

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

упорядоченных пар элементов множеств $X$ и $Y$ называется *прямым* (или *декартовым*) *произведением* этих множеств.

**Отображения.** *Отображением* $f\colon X \to Y$ множества $X$ в множество $Y$ называют правило, сопоставляющее каждому элементу $x \in X$ элемент $f(x) \in Y$. Множество

$$f(X) = \{f(x) \mid x \in X\} \subseteq Y$$

называют *образом* отображения $f$. Отображение $f\colon X \to Y$ *сюръективно*, если $f(X) = Y$, и *инъективно*, если из $x \neq x'$ следует $f(x) \neq f(x')$. Наконец, $f\colon X \to Y$ *биективно*, когда оно одновременно сюръективно и инъективно.

**Пример 1.1.** Пусть $X = \{1, 2, 3\}, Y = \{1, 2, 3, 4\}$. Отображение $f$, заданное формулой $f(i) = i + 1, i = 1, 2, 3$ инъективно, но не сюръективно. Отображение $g\colon Y \to X$, для которого $f(i) = i$, $i = 1, 2, 3$ и $f(4) = 3$, сюръективно, но не инъективно. Отображение $h\colon X \to X$, где $h(1) = 2, h(2) = 3, h(3) = 1$, биективно. $\square$

Отображения $f : X \to X$ называют *преобразованиями* множества $X$. Преобразование, заданное формулой $\mathrm{id}_X(x) = x$ для всех $x \in X$, называют *тождественным.*

*Произведением* (или *композицией*) отображений $f\colon X \to Y$ и $g : Y \to Z$ называют отображение $g \circ f\colon X \to Z$, заданное формулой

$$(g \circ f)(x) = g(f(x)), \quad x \in X.$$

Ясно, что для любого $f : X \to Y$ имеем

$$f \circ \mathrm{id}_X = f, \quad \mathrm{id}_Y \circ f = f.$$

**Теорема 1.1.** *Пусть* $f\colon X \to Y, g\colon Y \to Z, h : Z \to V$ *— отображения. Тогда*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

**Доказательство.** Имеем

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = \\ = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x). \ \square$$

Пусть $f\colon X \to Y$ и $g\colon Y \to X$ — отображения. Определены их композиции $f \circ g$ и $g \circ f$. Если

$$f \circ g = \mathrm{id}_Y, \quad g \circ f = \mathrm{id}_X, \tag{1.1}$$

то отображения $f$ и $g$ называют *взаимно обратными.*

Не каждое отображение имеет обратное. Но если обратное отображение существует, то оно единственно. В самом деле, пусть $h$ — еще одно отображение, обратное $f$. Тогда

$$f \circ h = \mathrm{id}_Y, \quad h \circ f = \mathrm{id}_X. \tag{1.2}$$

Из равенств (1.1) и (1.2) с помощью теоремы 1.1 получаем

$$h = \mathrm{id}_X \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \mathrm{id}_Y = g.$$

Отображение, обратное $f$, обозначают через $f^{-1}$.

**Теорема 1.2.** *Отображение* $f : X \to Y$ *тогда и только тогда имеет обратное, когда оно биективно.*

**Доказательство.** Для любого $y \in Y$ определен элемент $f^{-1}(y) = x \in X$. Значит, $f(x) = y$, т. е. $f$ сюръективно. Если $f(x) = f(x')$, то $x = f^{-1}(f(x)) = f^{-1}(f(x')) = x'$ и $f$ инъективно.

Докажем обратное утверждение. Пусть $f$ биективно. В силу сюръективности $f$ для любого $y \in Y$ найдется такой $x \in X$, что

$f(x)=y$; в силу инъективности такой элемент ровно один. Положим $g(y)=x$. Мы получили отображение $g\colon Y\to X$. Так как $f(g(y))=f(x)=y$, то $f\circ g=\mathrm{id}_Y$. Так как $g(f(x))=g(y)=x$, имеем $g\circ f=\mathrm{id}_X$. Значит, отображения $f$ и $g$ взаимно-обратны. $\square$

**Следствие.** *Из биективности отображения $f: X\to Y$ вытекает биективность $f^{-1}$, причем*

$$(f^{-1})^{-1}=f.$$

*Пусть, далее, $f\colon X\to Y, h\colon Y\to Z$ — биективные отображения. Тогда биективна и их композиция $h\circ f$, причем*

$$(h\circ f)^{-1}=f^{-1}\circ h^{-1}. \tag{1.3}$$

**Доказательство.** По теореме 1.2 биективность $f$ влечет существование $f^{-1}$. По той же теореме преобразование $f^{-1}$ имеет обратное. Равенства (1.1) показывают, что $(f^{-1})^{-1}=f$. Из равенств

$$(h\circ f)\circ(f^{-1}\circ h^{-1})=((h\circ f)\circ f^{-1})\circ h^{-1}= \\ =h\circ(f\circ f^{-1})\circ h^{-1}=h\circ h^{-1}=\mathrm{id}_Z;$$

$$(f^{-1}\circ h^{-1})\circ(h\circ f)=f^{-1}\circ(h^{-1}\circ h)\circ f^{-1}= \\ =f^{-1}\circ\mathrm{id}_Y\circ f=f^{-1}\circ f=\mathrm{id}_X$$

следует, что $f^{-1}\circ h^{-1}$ — преобразование, обратное $h\circ f$. $\square$

**Конечные множества.** Множество называют *конечным*, если существует его биективное отображение на одно из множеств $J_n=\{1,2,...,n\}$. Число элементов конечного множества $M$ обозначают через $|M|$.

Пусть $M$ и $N$ — конечные множества, $|M|=m, |N|=n$. Тогда ясно, что

$$|M\times N|=mn, \quad |M\cup N|=m+n-|M\cap N|.$$

Пусть $R$ и $M$ — конечные множества. Рассмотрим множество $R^M$ всех отображений $f: M\to R$.

**Теорема 1.3.** *Имеет место формула*

$$\left|R^M\right|=|R|^{|M|}.$$

**Доказательство.** Можно считать, что $M = J_m$, $R = J_q$. Отображение $f : R \to M$ ставит в соответствие элементу $i \in M$ элемент $f(i) \in R$. Таким образом, множество $R^M$ находится в биективном соответствии с множеством целочисленных наборов $(y_1, y_2, ..., y_m)$, где $y_i = f(i)$ и $y_i$ принимает одно из значений $1, 2, ..., q$. Таких наборов, как легко видеть, $q^m$. $\square$

**Подстановки.** Рассмотрим множество $\boldsymbol{S}_n$ всех биективных преобразований множества $J_n$ $(n = 1, 2, ...)$. Его элементы $\sigma \in \boldsymbol{S}_n$ называют *подстановками* (на $n$ элементах). Их удобно записывать в виде

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}. \tag{1.4}$$

Так как подстановки являются преобразованиями одного множества, их можно перемножать. Как показывает следствие из теоремы 1.2, для $\sigma, \tau \in \boldsymbol{S}_n$ их композиция $\sigma \circ \tau$ также является подстановкой. Результатом применения этой подстановки к элементу $i$ служит элемент $(\sigma \circ \tau)(i) = \sigma(\tau(i))$.

**Пример 1.2.** Пусть

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

Тогда

$$\sigma(\tau(1)) = \sigma(3) = 2, \quad \sigma(\tau(2)) = \sigma(2) = 1, \quad \sigma(\tau(3)) = \sigma(1) = 3.$$

Аналогично,

$$\tau(\sigma(1)) = \tau(3) = 1, \quad \tau(\sigma(2)) = \tau(1) = 3, \quad \tau(\sigma(3)) = \tau(2) = 2.$$

Значит,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

В частности, мы видим, что $\sigma \circ \tau \neq \tau \circ \sigma$. $\square$

Далее мы вместо $\sigma \circ \tau$ будем писать просто $\sigma\tau$.

Пусть $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_{l-1}) = i_l$, $\sigma(i_l) = i_1$ и $\sigma(j) = j$, если $j \neq i_1, ..., i_l$. Такая подстановка называется *циклом* (длины $l$) и обозначается $(i_1\, i_2 \ldots i_l)$.

**Пример 1.3.** Для данной подстановки $\sigma \in S_9$ имеем

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 4 & 3 \end{pmatrix} = (193)(26)(48)(5)(7).$$

Эта подстановка разложена в произведение независимых (т. е. не содержащих одинаковых элементов) циклов. Циклы длины 1 обычно опускают, т. е. пишут $\sigma = (193)(26)(48)$. $\square$

Ясно, что то же самое можно сделать с любой подстановкой. В итоге мы приходим к следующему результату.

**Теорема 1.4.** *Каждая подстановка $\sigma \neq e$ в $S_n$ является произведением независимых циклов длины $\geqslant 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.* $\square$

Цикл длины 2 называют *транспозицией*. Любая транспозиция имеет, таким образом, вид $\tau = (ij)$.

**Следствие 1.** *Каждая подстановка $\sigma \in S_n$ является произведением транспозиций.*

**Доказательство.** В силу теоремы 1.4 подстановка $\sigma \neq e$ разлагается в произведение циклов. Поэтому достаточно разложить цикл в произведение транспозиций. Это делается так:

$$(1\,2\,\ldots\,l-1\,l) = (1\,l)(1\,l-1)\ \ldots\ (13)(12).$$

Наконец, $e = (12)(12)$. $\square$

**Следствие 2.** *Каждая подстановка разлагается в произведение транспозиций вида $(i, i+1)$.*

**Доказательство.** Имеем

$$(13) = (23)(12)(23), \quad (14) = (34)(13)(34) \text{ и т. д. } \square$$

Рассмотрим подстановку (1.4). Пусть $i < j$. Скажем, что элементы $\sigma(i)$ и $\sigma(j)$ образуют *инверсию*, если $\sigma(i) > \sigma(j)$. Число инверсий в подстановке $\sigma$ обозначим через $l(\sigma)$ и положим $\varepsilon(\sigma) = (-1)^{l(\sigma)}$. Если $\varepsilon(\sigma) = +1$, подстановка называется *четной*, если $\varepsilon(\sigma) = -1$ — *нечетной.*

**Пример 1.4.** В множестве $S_3$ подстановки $e, (123), (132)$ — четные, подстановки $(12), (13), (23)$ — нечетные. $\square$

**Теорема 1.5.** *Четность подстановки меняется при умножении на транспозицию*:

$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma),$$

*где* $\sigma, \tau \in \boldsymbol{S}_n$, $\tau$ *— транспозиция.*

**Доказательство.** Пусть $\sigma$ имеет вид (1.4), а $\tau = (i,\ i+1)$. Тогда

$$\sigma\tau = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}.$$

Как легко понять, число инверсий в подстановках $\sigma$ и $\sigma\tau$ отличается на единицу. Значит, эти подстановки имеют разную четность. Доказательство следствия 2 из теоремы 1.4 показывает, что любая транспозиция разлагается в произведение нечетного числа транспозиций вида $(i, i+1)$. Значит, при умножении на произвольную транспозицию знак подстановки меняется нечетное число раз, т. е. изменяется на обратный. $\square$

**Следствие.** *Для любых* $\sigma, \tau \in \boldsymbol{S}_n$ *имеем*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau), \quad \varepsilon(\sigma^{-1}) = \varepsilon(\sigma).$$

**Доказательство.** Представим подстановки $\sigma$ и $\tau$ в виде произведения транспозиций: $\sigma = \sigma_1 \dots \sigma_k$, $\tau = \tau_1 \dots \tau_m$. Тогда

$$\sigma\tau = \sigma_1 \dots \sigma_k\tau_1 \dots \tau_m, \quad \sigma^{-1} = \sigma_k \dots \sigma_1.$$

На основании теоремы 1.5 имеем $\varepsilon(\sigma) = (-1)^k$, $\varepsilon(\tau) = (-1)^m$, $\varepsilon(\sigma\tau) = (-1)^{k+m}$, $\varepsilon(\sigma^{-1}) = (-1)^k$, откуда и получается требуемое утверждение. $\square$

**Отношение эквивалентности.** *Бинарным отношением* на множестве $X$ называют подмножество $B \subseteq X \times X$. То, что $(x, y) \in B$, обозначают через $xBy$. При этом обычно используют традиционную запись вида $x \leqslant y$, $x \approx y$ и т. п.

Бинарное отношение называют *рефлексивным*, если $xBx$ для всех $x$; *симметричным*, если $xBy$ тогда и только тогда, когда $yBx$. Его называют *транзитивным*, если из $xBy$ и $yBz$ следует, что $xBz$.

**Пример 1.5.** Пусть $X = J_9$, а $xBy$ означает, что $x - y$ делится на 3. Это отношение, очевидно, рефлексивно, симметрично и транзитивно. $\square$

Бинарное отношение называют *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно. Отношение эквивалентности обычно обозначают через $\sim$.

**Пример 1.6.** Отношение из примера 1.5 есть отношение эквивалентности. $\square$

Пусть на множестве $X$ задано отношение эквивалентности. Подмножество

$$[x] = \{y \in X \mid y \sim x\}$$

называют *классом эквивалентности*, содержащим $x$. Любой элемент $y \in [x]$ называют *представителем* этого класса.

**Теорема 1.6.** *Множество классов эквивалентности по отношению эквивалентности на множестве $X$ есть разбиение этого множества. И наоборот, если задано разбиение множества $X$, то существует ровно одно отношение эквивалентности, для которого множества разбиения служат классами эквивалентности.*

**Доказательство.** Так как $x \in [x]$, то $X$ есть объединение классов $[x]$. Покажем, что любые два класса либо не пересекаются, либо совпадают. Пусть $[x] \cap [y] \neq \emptyset$. Тогда существует такой элемент $z$, что $z \in [x]$ и $z \in [y]$. Значит, $z \sim x$, $z \sim y$. Ввиду транзитивности отношения эквивалентности имеем $x \sim y$. Если $y'$ — любой элемент из $[y]$, то $y' \sim y$. Но тогда $y' \sim x$, т. е. $y' \in [x]$. Значит, $[y] \subseteq [x]$. Аналогично и $[x] \subseteq [y]$, т. е. $[x] = [y]$.

Теперь пусть подмножества $Y_\alpha$ $(\alpha \in A)$ образуют разбиение множества $X$. Положим $x \sim y$ тогда и только тогда, когда $x$ и $y$ лежат в одном $Y_\alpha$. Как легко заметить, это отношение рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности. Ясно также, что множества $Y_\alpha$ совпадают с классами эквивалентности по этому отношению. $\square$

**Пример 1.7.** Рассмотрим отношение из примера 1.5. Имеем $[1] = \{1, 4, 7\}$, $[2] = \{2, 5, 8\}$, $[3] = \{3, 6, 9\}$. $\square$

## 2. ПОНЯТИЕ ГРУППЫ

**Бинарные алгебраические операции.** Пусть $M$ — множество. *Бинарной операцией* на этом множестве называют отображение $f\colon M \times M \to M$. Элемент $f(a, b)$ называют результатом применения операции к паре $(a, b)$. Вместо $f(a, b)$ пишут обычно $a * b$, $a \circ b$ или используют какой-то другой знак. Множество вместе с операцией обозначают $(M, *)$, $(M, \circ)$ и т. п.

Если не оговорено противное, операцию будем записывать мультипликативно, т. е. вместо $f(a, b)$ писать просто $ab$.

Пусть $(M, *)$ — множество с операцией. Операцию называют *ассоциативной*, если для любых $a, b, c \in M$ имеем

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

Ее называют *коммутативной*, если для любых $a, b \in M$ верно равенство

$$a * b = b * a.$$

Элемент $e$ называют *нейтральным*, если для всех $a \in M$ справедливы равенства

$$a * e = e * a = a.$$

Если нейтральный элемент существует, то он единственный. Действительно, пусть $e'$ — другой нейтральный элемент. Тогда $e = e * e' = e'$.

Пусть существует нейтральный элемент $e$ и $a$ — элемент из множества $M$. Элемент $b \in M$ называют *обратным* к $a$, если

$$a * b = b * a = e.$$

**Пример 2.1.** Рассмотрим два множества с операциями $(\mathbb{Z}, +)$ и $(\mathbb{Z}, \cdot)$. Операции ассоциативны и коммутативны, есть нейтральные элементы — 0 и 1 соответственно. Обратным к элементу $a \in \mathbb{Z}$ относительно операции сложения служит элемент $-a$; по отношению к умножению обратимы только элементы 1 и $-1$. $\square$

**Определение группы.** *Группой* называют множество $G$, в котором введена бинарная операция, причем выполнены следующие аксиомы:

1) $(ab)c = a(bc)$ для всех $a, b, c \in G$;

2) существует единица, т. е. такой элемент $e \in G$, что $ae = ea = a$ для всех $a \in G$;

3) для любого элемента $a \in G$ существует обратный элемент $a^{-1}$, т. е. такой, что $aa^{-1} = a^{-1}a = e$.

Отметим, что обратный элемент всегда единственный. Это доказывается точно так же, как доказывалась единственность обратного преобразования в разд. 1. А именно, если $b$ и $c$ — элементы, обратные к $a$, то

$$b = (ba)b = b(ab) = be = b(ac) = (ba)c = ec = c.$$

Если для всех $a, b \in G$ справедливо равенство $ab = ba$, то группу называют *коммутативной*, или *абелевой.*

**Пример 2.2.** Множество целых чисел $\mathbb{Z}$ с операцией сложения образует абелеву группу. $\square$

**Пример 2.3.** Пусть $M$ — непустое множество, $G = \boldsymbol{S}(M)$ — множество биективных преобразований множества $M$. Тогда $G$ — группа относительно операции композиции. Единичным элементом $G$ является тождественное преобразование $\mathrm{id}_M$. Элементы группы называют *подстановками* множества $M$. В частности, если $M = J_n$, то группу $G$ называют *симметрической группой* и обозначают через $\boldsymbol{S}_n$. $\square$

Для конечной группы $G$ число $|G|$ называют ее *порядком.*

**Подгруппы. Гомоморфизмы групп.** Пусть $G$ — группа. Подмножество $H \subseteq G$ называют ее *подгруппой*, если:

1) $x \in H \Rightarrow x^{-1} \in H$;

2) $x, y \in H \Rightarrow xy \in H$.

Ясно, что подгруппа сама является группой.

Отметим, что если $N$ — подгруппа в $H$, а $H$ — подгруппа в $G$, то $N$ — подгруппа в $G$.

**Пример 2.4.** Как показывает следствие из теоремы 1.5, множество $\boldsymbol{A}_n$ всех четных подстановок на $n$ элементах образует подгруппу группы $\boldsymbol{S}_n$. Ее называют *знакопеременной группой.* $\square$

Пусть $G$ и $G'$ — группы. Отображение $f\colon G \to G'$ называют *гомоморфизмом* групп, если

$$f(xy) = f(x)f(y)$$

для всех $x, y \in G$. Биективный гомоморфизм называют *изоморфизмом.* Если существует изоморфизм группы $G$ на группу $G'$, то эти группы называют *изоморфными* и обозначают как $G \cong G'$. Как легко проверить, отношение изоморфности есть отношение эквивалентности. С точки зрения теории групп изоморфные группы неразличимы.

Назовем *порядком* $o(x)$ элемента $x$ группы наименьшее натуральное $n$ со свойством $x^n = e$.

**Пример 2.5.** В группе $\boldsymbol{S}_3$ имеем $o(\sigma) = 2$, где $\sigma$ — одна из транспозиций $(12), (13)$ или $(23)$, $o(\tau) = 3$, где $\tau$ — один из тройных циклов $(123)$ или $(132)$. $\square$.

Назовем элементы $x$ и $y$ группы $G$ *сопряженными*, если $y = gxg^{-1}$ для некоторого $g \in G$. Нетрудно доказать, что отношение сопряженности есть отношение эквивалентности.

Отметим, что порядки сопряженных элементов равны. Действительно, если $y = gxg^{-1}$ и $x^n = e$, то

$$y^n = (gxg^{-1})(gxg^{-1}) \ldots (gxg^{-1}) = \\ = gx(g^{-1}g)x \ldots (g^{-1}g)xg^{-1} = gx^n g^{-1} = e.$$

Значит, $o(y) \leqslant o(x)$. В силу симметрии и $o(x) \leqslant o(y)$, откуда $o(x) = o(y)$.

**Пример 2.6.** В группе $\boldsymbol{S}_3$ элементы $\sigma = (12)$ и $(13)$ сопряжены: $(23)(12)(23) = (13)$. Элементы $(12)$ и $(123)$ не сопряжены, так как их порядки различны. $\square$

Введем еще одно понятие, которое понадобится нам в дальнейшем. Назовем подгруппы $H, H' \subseteq G$ *сопряженными*, если существует такой $g \in G$, что

$$H' = gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Ясно, что сопряженные подгруппы изоморфны.

**Порождающие множества.** Как легко проверить, пересечение любого множества подгрупп — подгруппа. Пусть $G$ — группа и $M \subseteq G$ — подмножество. Пересечение $\langle M \rangle$ всех подгрупп группы $G$, содержащих $M$, называют *подгруппой, порожденной множеством* $M$, а само $M$ — *порождающим множеством* подгруппы $\langle M \rangle$.

**Пример 2.7.** Как мы видели (следствие 1 из теоремы 1.4), симметрическая группа $\boldsymbol{S}_n$ порождается всевозможными транспозициями $(ij)$. $\square$

**Пример 2.8.** Знакопеременная группа $\boldsymbol{A}_n$ порождается всевозможными тройными циклами $(ijk)$, так как четная подстановка есть произведение четного числа транспозиций и

$$(ij)(ik) = (ikj), \quad (ij)(kl) = (jkl)(ilj). \ \square$$

Подгруппу $\langle a \rangle$, порожденную одним элементом $a$, называют *циклической.* Элемент $a$ называют *образующей* этой группы.

**Пример 2.9.** Группа $\mathbb{Z}$ — циклическая. $\square$

Пусть $G = \langle a \rangle$ и $o(a) = n$. Тогда все элементы

$$e = a^0, \quad a, \quad a^2, \quad \ldots, \quad a^{n-1} \tag{2.1}$$

различны, а $a^n = e$. Пусть $l$ — целое число. Деля с остатком, получаем $l = qn + r$, где $0 \leqslant r < n$. Тогда $a^l = a^{qn+r} = a^r$. Значит, $a^l$ совпадает с одним из элементов (2.1), т. е. группа $G$ состоит в точности из элементов (2.1). Будем обозначать эту группу через $\boldsymbol{C}_n$. Ясно, что все циклические группы порядка $n$ ей изоморфны.

## 3. ТЕОРЕМА ЛАГРАНЖА

Пусть $G$ — группа и $H$ — ее подгруппа. Положим

$$gH = \{gh \mid h \in H\}.$$

Множества $gH$ называют *левыми смежными классами* группы $G$ по подгруппе $H$. Каждый элемент класса $gH$ называют представителем этого класса.

Аналогично определяют правые смежные классы.

Если группа $G$ конечна, то и число левых смежных классов конечно. Нетрудно доказать, что оно равно числу правых смежных классов. Это число называют *индексом* подгруппы $H$ в $G$ и обозначают через $(G : H)$.

**Пример 3.1.** Очевидно, $(\boldsymbol{S}_n : \boldsymbol{A}_n) = 2$. $\square$

Множество левых смежных классов группы $G$ по подгруппе $H$ обозначают через $G/H$.

**Теорема 3.1** (Лагранжа). *Если $H$ — подгруппа конечной группы $G$, то*

$$|G| = |H| \cdot (G : H).$$

**Доказательство.** Каждый левый смежный класс по подгруппе $H$ содержит $|H|$ элементов, а число смежных классов равно $|G/H|$. $\square$

**Следствие.** *Порядок подгруппы делит порядок группы. Порядок любого элемента делит порядок группы. Группа простого порядка всегда циклическая и с точностью до изоморфизма — единственная.*

**Доказательство.** Пусть $a \in G$ и $o(a) = k$. Тогда подгруппа $H = \langle a \rangle$ имеет порядок $k$. По теореме Лагранжа $k$ делит порядок $|G|$ группы $G$. Если $|G| = p$ — простое число и $a$ — элемент группы $G$, отличный от единицы, то $o(a) = p$. Значит, группа $G$ совпадает с подгруппой $\langle a \rangle$, т. е. является циклической. $\square$

## 4. ГРУППЫ ДВИЖЕНИЙ

Группы естественным образом возникают как группы движений симметричных фигур. Чем симметричнее фигура, тем больше группа ее движений.

Назовем *движением* преобразование пространства (плоскости), сохраняющее расстояния. Такое преобразование всегда биективно. Будем считать, что движение сохраняет ориентацию. Это и есть движение в обычном понимании. Пусть $\mathbf{\Omega}$ — фигура (например, многогранник) в пространстве. Движения, переводящие фигуру $\mathbf{\Omega}$ в себя, образуют подгруппу всей группы движений. Ее называют *группой движений* фигуры $\mathbf{\Omega}$.

**Пример 4.1.** Найдем группу движений плоскости, переводящих в себя равносторонний треугольник. Обозначим его вершины через $1, 2, 3$. Искомая группа $G$ может быть отождествлена с подгруппой в $\boldsymbol{S}_3$ перестановок элементов 1, 2. 3. При этом четные подстановки отвечают движениям, сохраняющим ориентацию, нечетные — не сохраняющим. Значит, $G$ можно отождествить с подгруппой $\boldsymbol{A}_3 \subset \boldsymbol{S}_3$. Итак, $G \cong \boldsymbol{A}_3 \cong \boldsymbol{C}_3$. $\square$

**Пример 4.2.** Найдем группу движений пространства, переводящих в себя равносторонний треугольник. Здесь кроме движений из примера 4.1 есть еще три вращения вокруг высот треугольника. Им отвечают подстановки (12), (13) и (23). Таким образом, группа движений совпадает с $\boldsymbol{S}_3$. $\square$

**Пример 4.3.** Найдем группу $G$ движений правильной четырехугольной пирамиды. Обозначим ее вершину числом 1, а вершины основания — последовательно 2, 3, 4 и 5. Ясно, что любое движение переводит вершину 1 в себя. Вращения вокруг высоты пирамиды на углы, кратные $\pi/2$ (включая тождественное), составляют еще четыре элемента группы. Как легко понять, этими движениями группа и исчерпывается. Ее можно отождествить с подгруппой в $\boldsymbol{S}_5$, состоящей из подстановок $e$, $\sigma = (1)(2345)$, $\sigma^2 = (1)(24)(35)$ и $\sigma^3 = \sigma^{-1} = (1)(2543)$. Группа $G$ изоморфна группе $\boldsymbol{C}_4$. $\square$

**Пример 4.4.** Назовем $n$-угольным *диэдром* многогранник, составленный из двух одинаковых правильных $n$-угольных пирамид с общими основаниями. Найдем группу $G$ движений четырехугольного диэдра, отличного от правильного октаэдра. Обозначим вершины составляющих его пирамид числами 1 и 6, а вершины основания — последовательно 2, 3, 4 и 5. Таким образом, группу $G$ можно рассматривать как подгруппу в $\boldsymbol{S}_6$. При любом движении вершина 2 переходит в одну из четырех вершин основания, а вершина 3 — в одну из двух соседних вершин. Положение остальных вершин тем самым будет полностью определено. Значит, группа $G$ не может содержать больше восьми элементов. Вращениям вокруг оси, соединяющей вершины 1 и 6, на углы, кратные $\pi/2$, отвечают подстановки $e$, $\sigma = (1)(2345)(6)$, $\sigma^2 = (1)(24)(35)(6)$, $\sigma^3 = (1)(2543)(6)$. Кроме того, есть еще повороты на угол $\pi$ вокруг осей симметрии квадрата, лежащего в основании пирамид. Этим поворотам соответствуют подстановки $\tau = (16)(24)(3)(5)$, $\tau' = (16)(35)(2)(4)$ и $\rho = (16)(23)(45)$, $\rho' = (16)(25)(34)$ соответственно. Группу $G$ называют *диэдральной группой* и обозначают через $\boldsymbol{D}_4$. $\square$

Аналогично строят группы $\boldsymbol{D}_n$ при других $n \geqslant 3$. Отметим, что при $n = 3$ группа $\boldsymbol{D}_3$ изоморфна $\boldsymbol{S}_3$.

**Пример 4.5.** Найдем группу $G$ движений правильного тетраэдра. Обозначив вершины тетраэдра числами 1, 2, 3 и 4, увидим, что искомая группа есть подгруппа группы $\boldsymbol{S}_4$. Так как мы рассматриваем только движения, сохраняющие ориентацию, то порядок $G$ не превосходит 12. Кроме того, группа $G$ содержит вращения $(123), (132)$ вокруг высоты тетраэдра, проходящей через вершину 4. Аналогично, $G$ содержит и остальные тройные циклы. Тройные циклы порождают подгруппу $\boldsymbol{A}_4 \subset \boldsymbol{S}_4$ (см. пример 2.8). Так как ее порядок равен 12, имеем $G \cong \boldsymbol{A}_4$. $\square$

## 5. ДЕЙСТВИЕ ГРУППЫ НА МНОЖЕСТВЕ

Пусть $G$ — группа и $M$ — множество. Скажем, что $G$ *действует* (слева) на $M$, если задано отображение

$$G \times M \to M, \ \ (g, x) \to gx,$$

удовлетворяющее условиям:

1) $ex = x, \ \ x \in M$;

2) $(gh)x = g(hx), \ \ g, h \in G, \ \ x \in M$.

Если $G$ действует на $M$, то для $g \in G$ определено преобразование

$$\mathbf{\Phi}_g(x) = gx, \quad x \in M.$$

Из условия 2) следует, что $\mathbf{\Phi}_{gh} = \mathbf{\Phi}_g \circ \mathbf{\Phi}_h$. Далее, имеем

$$\mathbf{\Phi}_g \circ \mathbf{\Phi}_{g^{-1}} = \mathbf{\Phi}_e = \mathrm{id}_M.$$

Последнее равенство верно в силу условия 1). Значит, все преобразования $\mathbf{\Phi}_g$ обратимы, т. е. принадлежат $\boldsymbol{S}(M)$. Итак, $\mathbf{\Phi} : g \to \mathbf{\Phi}_g$ — гомоморфизм группы $G$ в группу $\boldsymbol{S}(M)$.

Точки $x, x' \in M$ называют *эквивалентными* относительно действия группы $G$, если $x' = gx$ для некоторого $g \in G$. Классы эквивалентности называют *$G$-орбитами*. Орбиту, содержащую элемент $x_0$, обозначают через $G(x_0)$. Таким образом,

$$G(x_0) = \{gx_0 \mid g \in G\}.$$

**Пример 5.1.** Пусть $G \cong \boldsymbol{C}_4$ — группа движений правильной четырехугольной пирамиды, $M$ — множество ее вершин, пронумерованных, как в примере 4.3. Элементы $G$ действуют как вращения вокруг высоты пирамиды. Орбитой точек $2, 3, 4, 5$ служит множество $\{2, 3, 4, 5\}$, а орбитой точки 1 — множество, состоящее из одной этой точки. $\square$

Пусть $x_0$ — фиксированная точка из $M$. Рассмотрим множество

$$\mathrm{St}(x_0) = \{g \in G \mid gx_0 = x_0\} \subseteq G.$$

Как легко проверить, $\mathrm{St}(x_0)$ — подгруппа в $G$. Ее называют *стационарной подгруппой* в $G$ точки $x_0 \in M$.

**Пример 5.2.** Пусть $G$ и $M$ такие же, как в примере 5.1. Тогда $\mathrm{St}(1) = G$ и $\mathrm{St}(i) = \{e\}$, если $i = 2, 3, 4$ или 5. $\square$

В общем случае имеем

$$gx_0 = g'x_0 \iff g^{-1}g' \in \mathrm{St}(x_0) \iff g' \in g\mathrm{St}(x_0).$$

Следовательно, левые смежные классы группы $G$ по подгруппе $\mathrm{St}(x_0)$ находятся в биективном соответствии с точками орбиты $G(x_0)$. В частности,

$$|G(x_0)| = |G/\mathrm{St}(x_0)| = (G : \mathrm{St}(x_0)). \tag{5.1}$$

Пусть $x_0' = gx_0$. Положим $H = \mathrm{St}(x_0)$, $H' = \mathrm{St}(x_0')$. Если $h \in H$, то

$$x_0' = gx_0 = (ghg^{-1})gx_0 = (ghg^{-1})x_0' = x_0'.$$

Значит, $ghg^{-1} \in H'$, т. е. $gHg^{-1} \subseteq H'$. Аналогично, если $h' \in H'$, то

$$x_0 = g^{-1}x_0' = g^{-1}h'gx_0,$$

откуда $h' \in gHg^{-1}$, т. е. $H' \subseteq gHg^{-1}$. Итак, $H' = gHg^{-1}$; подгруппы $H$ и $H'$ сопряжены:

$$g\mathrm{St}(x_0)g^{-1} = \mathrm{St}(x_0').$$

Мы видим, что доказано следующее утверждение.

**Теорема 5.1** *Пусть группа $G$ действует на множестве $M$. Если две точки $x_0, x_0' \in M$ лежат в одной орбите, то их стационарные подгруппы сопряжены*:

$$x_0' = gx_0 \Rightarrow \mathrm{St}(x_0') = g\mathrm{St}(x_0)g^{-1}.$$

*Если $G$ — конечная группа и*

$$M = M_1 \cup M_2 \cup ... \cup M_r$$

*— разбиение множества $M$ на конечное число орбит с представителями $x_1, x_2, ..., x_r$, то*

$$|M| = \sum_{i=1}^{r} (G : \mathrm{St}(x_i)). \ \square$$

**Пример 5.3.** Пусть группа $G$ действует на множестве $M$ и пусть $R$ — еще одно множество. Тогда определено действие $G$ на $R^M$. Обозначим через $gx$ результат действия $g \in G$ на элемент $x \in M$, а через $\mathbf{\Phi}_g f$ — результат применения $g$ к отображению $f\colon M \to R$. Положим

$$(\mathbf{\Phi}_g f)(x) = f(g^{-1}x). \tag{5.2}$$

Тогда

1) $(\mathbf{\Phi}_e f)(x) = f(ex) = f(x)$, т. е. $\mathbf{\Phi}_e f = f$;

2) $(\mathbf{\Phi}_h f)(x) = f(h^{-1}x) = (f \circ h^{-1})(x)$, откуда

$$((\mathbf{\Phi}_g \circ \mathbf{\Phi}_h)f)(x) = (\mathbf{\Phi}_g(f \circ h^{-1}))(x) = (f \circ h^{-1})(g^{-1}x) = \\ = f((h^{-1}g^{-1})(x)) = f((gh)^{-1}(x)) = \mathbf{\Phi}_{gh} f(x),$$

т. е. $\mathbf{\Phi}_{gh} = \mathbf{\Phi}_g \circ \mathbf{\Phi}_h$ и это в самом деле действие. □

## 6. ЛЕММА БЕРНСАЙДА

Пусть конечная группа $G$ действует на конечном множестве $M$. Для $g \in G$ положим

$$N(g) = |\{x \in M \mid gx = x\}|.$$

**Теорема 6.1** (лемма Бернсайда). *Пусть $N$ — число $G$-орбит. Тогда*

$$N = \frac{1}{|G|} \sum_{g \in G} N(g). \tag{6.1}$$

**Доказательство.** Обозначим через $M_G$ множество $G$-орбит. Пусть

$$\alpha(g, x) = \begin{cases} 1, & \text{если } gx = x, \\ 0, & \text{если } gx \neq x. \end{cases}$$

Используя теорему 5.1 и формулу (5.1), получаем:

$$\sum_{g \in G} N(g) = \sum_{g \in G} \sum_{x \in M} \alpha(g, x) = \sum_{G(x_0) \in M_G} \sum_{x \in G(x_0)} \sum_{g \in G} \alpha(g, x) = \\ = \sum_{G(x_0) \in M_G} \sum_{x \in G(x_0)} |\mathrm{St}(x)| = \sum_{G(x_0) \in M_G} \sum_{x \in G(x_0)} |\mathrm{St}(x_0)| = \\ = \sum_{G(x_0) \in M_G} |G(x_0)|\,|\mathrm{St}(x_0)| = |G|\,|M_G| = |G| N,$$

откуда и следует требуемая формула. $\square$

**Пример 6.1.** Поместим в вершины правильной четырехугольной пирамиды одинаковые шарики, каждый из которых можно окрасить в один из трех цветов. Найдем число $N$ различных раскрашиваний.

Обозначим вершины пирамиды, как указано ниже. Каждому шарику поставим в соответствие один из трех цветов: красный ($r$), зеленый ($g$), голубой ($b$). Например,

$$\begin{pmatrix} 2 & & 3 \\ & 1 & \\ 5 & & 4 \end{pmatrix} \quad \to \quad \begin{pmatrix} g & & r \\ & r & \\ g & & b \end{pmatrix}.$$

У нас $M = \{1,2,3,4,5\}$, $R = \{r,g,b\}$, группа $G \cong \boldsymbol{C}_4$ действует на множестве $M$, как описано в примере 4.3, а тогда и на $R^M$ (см. пример 5.3). Число различных раскрашиваний (а различными считаются те, которые не переводятся одно в другое элементом группы $G$) задается формулой (6.1):

$$N = \frac{1}{|G|}(N(e) + N(\boldsymbol{\sigma}) + N(\boldsymbol{\sigma}^2) + N(\boldsymbol{\sigma}^3)).$$

Тождественное преобразование $e$ оставляет на месте любое раскрашивание, поэтому $N(e) = |R^M| = 3^5 = 243$. Элемент $\boldsymbol{\sigma}$ оставляет на месте такое раскрашивание, у которого в один цвет окрашены вершины 2, 3, 4 и 5. Поэтому $N(\boldsymbol{\sigma}) = 3^2 = 9$. Элемент $\boldsymbol{\sigma}^2$ оставляет на месте такое раскрашивание, у которого в один цвет окрашены вершины 2 и 4, а также 3 и 5. Значит, $N(\boldsymbol{\sigma}^2) = 3^3 = 27$. Аналогично, $N(\boldsymbol{\sigma}^3) = N(\boldsymbol{\sigma}) = 9$ и, следовательно,

$$N = \frac{1}{4}(243 + 9 + 27 + 9) = 72. \ \square$$

Формализуем ситуацию предыдущего примера. Пусть $M = \{1, 2, ..., n\}$ — множество номеров элементов некоторой фигуры $\boldsymbol{\Omega}$; $R$ — конечное множество цветов, в которые могут быть окрашены элементы этой фигуры. Пусть $\boldsymbol{\sigma} \in \boldsymbol{S}_n$ — некоторая подстановка. Определим действие подстановки $\boldsymbol{\sigma}$ на произвольное раскрашивание по формуле (5.2):

$$(\boldsymbol{\sigma} f)(i) = f(\boldsymbol{\sigma}^{-1}(i)).$$

Выведем формулу для числа $N(\sigma)$ раскрашиваний, остающихся на месте при действии $\sigma$. Разложим подстановку $\sigma$ в произведение независимых циклов: $\sigma = \sigma_1 \ \dots \ \sigma_k$, причем учитываются и циклы длины 1. Каждому циклу $(i_1, ..., i_l)$ соответствует $\langle\sigma\rangle$-орбита $\{i_1, ..., i_l\}$, и при этом совокупность всех $\langle\sigma\rangle$-орбит является разбиением множества $M$. Пусть $f$ — некоторое раскрашивание фигуры $\Omega$, которое сохраняется при действии на него подстановки $\sigma$. Как легко понять, для любого цикла $\sigma_j = (i_1, ..., i_l)$ имеем $f(i_1) = f(i_2) = ... = f(i_l)$. Поскольку $\langle\sigma\rangle$-орбиты не пересекаются, они могут быть окрашены независимо друг от друга, а тогда $N(\sigma) = |R|^k$. $\square$

**Пример 6.2.** Вычислим, сколькими способами можно раскрасить вершины правильного тетраэдра в $q$ различных цветов. Группа $G$ движений правильного тетраэдра найдена в примере 4.5. Эта группа действует на множестве $\{1, 2, 3, 4\}$ вершин тетраэдра и состоит в точности из четных подстановок. Она содержит элемент $e = (1)(2)(3)(4)$, восемь элементов вида $\sigma = (1)(234)$ и три элемента вида $\tau = (12)(34)$. Согласно доказанному выше имеем $N(e) = q^4, N(\sigma) = q^2, N(\tau) = q^2$. Теперь можно применить лемму Бернсайда, и мы получаем формулу для числа $N$ раскрашиваний:

$$N = \frac{1}{12}(q^4 + 8q^2 + 3q^2) = \frac{q^2}{12}(q^2 + 11). \tag{6.2}$$

Решенную задачу можно трактовать таким образом: имеются атомы $q$ различных элементов. Молекула вещества состоит из четырех атомов, расположенных в вершинах правильного тетраэдра. Сколько может существовать различных типов молекул, составленных из атомов данных элементов? Ответ дает формула (6.2). $\square$

## 7. ТЕОРЕМА ПОЙА

**Цикловой индекс группы.** Пусть $M$ — конечное множество, $|M| = n$ и $G$ — конечная группа, действующая на $M$. Эту группу можно отождествить с некоторой подгруппой в $\boldsymbol{S}_n$.

Для любого элемента $g \in G$ обозначим через $j_k(g)$ число циклов длины $k$ в разложении подстановки $g$ в произведение независимых циклов. Каждому элементу $g \in \boldsymbol{S}_n$ поставим в соответствие вес

$$w_G(g) = t_1^{j_1(g)} \dots t_n^{j_n(g)}.$$

Это многочлен от переменных $t_1, \dots, t_n$ с целыми коэффициентами. *Цикловым индексом* группы $G$, действующей на $M$, называют многочлен $P(G, M, t_1, \dots, t_n)$, определяемый формулой

$$P(M, G, t_1, \dots, t_n) = \frac{1}{|G|} \sum_{g \in G} w_G(g) = \frac{1}{|G|} \sum_{g \in G} t_1^{j_1(g)} \ \dots \ t_n^{j_n(g)}.$$

**Пример 7.1.** Пусть $G$ — группа движений правильной четырехугольной пирамиды (см. пример 4.3). Как мы знаем, $G \cong \boldsymbol{C}_4$ — циклическая группа порядка 4, порожденная поворотом $\sigma$ на угол $\pi/2$. При отождествлении $G$ с подгруппой в $\boldsymbol{S}_5$ имеем $\sigma = (1)(2345)$, $\sigma^2 = (1)(24)(35)$, $\sigma^3 = (1)(2543)$. Цикловой индекс группы, действующей на множестве $M = \{1, 2, 3, 4, 5\}$ вершин пирамиды, равен

$$P(M, G, t_1, t_2, t_3, t_4, t_5) = \frac{1}{|G|} \sum_{g \in G} w_G(g) =$$
$$= \frac{1}{4}(w_G(e) + w_G(\sigma) + w_G(\sigma^2) + w_G(\sigma^3)) =$$
$$= \frac{1}{4}(t_1^5 + t_1 t_4 + t_1 t_2^2 + t_1 t_4) = \frac{1}{4}(t_1^5 + t_1 t_2^2 + 2 t_1 t_4). \ \square$$

**Запас. Производящая функция запаса.** Множество исследуемых объектов в комбинаторике часто называют *запасом*. Пусть $Z$ — запас. Поставим в соответствие каждому $z \in Z$ многочлен $w(z)$ от нескольких переменных с целыми коэффициентами. Будем называть многочлен $w(z)$ *весом* элемента $a$. Сумму весов всех элементов запаса называют *производящей функцией* запаса $Z$ и обозначают через $W(Z)$, т. е.

$$W(Z) = \sum_{z \in Z} w(z).$$

Пусть $R$ — еще одно конечное множество. На множестве $R^M$ функций $f : M \to R$ действует группа $G$, как объяснялось в примере 5.3. Рассматривая $M$ как множество элементов некоторой фигуры, а $R$ — как множество красок, будем называть такие функции *раскрашиваниями.* Два раскрашивания назовем эквивалентными, если они эквивалентны относительно действия $G$, т. е. лежат в одной орбите этой группы, действующей на $R^M$. Обозначим через $[R^M]$ множество классов эквивалентности раскрашиваний.

Пусть каждому элементу $y \in R$ придан некоторый вес $w_R(y)$ — многочлен с целыми коэффициентами от фиксированного числа переменных. Тогда вес функции $f \in R^M$ есть, по определению,

$$w(f) = \prod_{x \in M} w_R(f(x)).$$

Если $f_1 \sim f_2$, то, очевидно, $w(f_1) = w(f_2)$, поэтому можно определить вес класса эквивалентности $w(F)$, где $F \in [R^M]$ как вес любого элемента $f \in F$.

**Пример 7.2.** Пусть $M = \{1, 2, 3, 4, 5\}$ — множество вершин правильной четырехугольной пирамиды:

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

$R = \{r, g\}$ — множество цветов. На множестве $M$ действует группа $G \cong \boldsymbol{C}_4$ (см. пример 5.1). Раскрашивания 1) и 2) $G$-эквивалентны, раскрашивание 3) им не эквивалентно:

$$1)\begin{pmatrix} r & & r \\ & r & \\ g & & g \end{pmatrix}; \qquad 2)\begin{pmatrix} g & & r \\ & r & \\ g & & r \end{pmatrix}; \qquad 3)\begin{pmatrix} r & & g \\ & r & \\ g & & r \end{pmatrix}.$$

Положим $w_R(r) = a$, $w_R(g) = b$. Тогда для веса $w(f)$ любого из раскрашиваний $1), 2), 3)$ и для веса $w(F)$ любого из сответствующих классов эквивалентности будем иметь

$$w(F) = w(f) = a^3 b^2. \ \square$$

**Формулировка теоремы Пойа. Пример.** Теперь мы можем сформулировать основной результат.

**Теорема 7.1** (Пойа). *Прозводящая функция запаса классов* *эквивалентности раскрашиваний удовлетворяет равенству*

$$\sum_F w(F) = P\left(G, M, \sum_{y\in R} w_R(y), \sum_{y\in R} \left(w_R(y)\right)^2, ..., \sum_{y\in R} \left(w_R(y)\right)^n\right),$$

*где* $P(G, M, t_1, ..., t_n)$ *— цикловой индекс группы* $G$, *действующей на* $M$. □

Доказывать эту теорему не будем, рассмотрим только пример ее применения.

**Пример 7.3.** Обратимся к примерам 7.1 и 7.2. Определим производящую функцию запаса классов эквивалентности раскрашиваний в два цвета. На основании теоремы имеем

$$\sum_F w(F) = P(M, G, a+b, a^2+b^2, a^3+b^3, a^4+b^4, a^5+b^5) =$$
$$= \frac{1}{4}\left((a+b)^5 + (a+b)(a^2+b^2)^2 + 2(a+b)(a^4+b^4)\right) =$$
$$= a^5 + 2a^4b + 3a^3b^2 + 3a^2b^3 + 2ab^4 + b^5.$$

Таким образом, число раскрашиваний, при которых, например, три элемента окрашены в красный цвет и два — в зеленый, равно коэффициенту при $a^3b^2$, т. е. 3. Общее число раскрашиваний равно сумме всех коэффициентов, т. е. 12. □

## ДОМАШНЕЕ ЗАДАНИЕ

Дан многогранник $\mathbf{\Omega}$, представляющий собой либо правильную $n$-угольную призму, либо правильную $n$-угольную пирамиду, либо правильную $n$-угольную усеченную пирамиду, либо $n$-угольный диэдр (фигуру, состоящую из двух одинаковых правильных $n$-угольных пирамид с общим основанием), либо такой же усеченный диэдр (фигуру, состоящую из двух одинаковых правильных усеченных пирамид с общим большим основанием). Требуется найти:

1) группу $G$ движений многогранника $\mathbf{\Omega}$;

2) цикловой индекс группы $G$, действующей на множестве $M$ вершин (варианты 1–10), граней (варианты 11–20), ребер (варианты 21–30) многогранника $\mathbf{\Omega}$;

3) число способов раскрашивания элементов множества $M$ в три цвета;

4) производящую функцию запаса классов эквивалентности раскрашиваний, если используются два цвета.

Данные для каждого варианта указаны в таблице.

| Номер варианта | $\mathbf{\Omega}$ | $n$ | Номер варианта | $\mathbf{\Omega}$ | $n$ |
|---|---|---|---|---|---|
| 1, 11, 21 | Призма | 3 | 6, 16, 26 | Диэдр | 5 |
| 2, 12, 22 | Усеченный диэдр | 3 | 7, 17, 27 | Призма (отличная от куба) | 4 |
| 3, 13, 23 | Диэдр | 3 | 8, 18, 28 | Призма | 5 |
| 4, 14, 24 | Усеченная пирамида | 4 | 9, 19, 29 | Усеченная пирамида | 5 |
| 5, 15, 25 | Пирамида | 6 | 10, 20, 30 | Диэдр (отличный от правильного октаэдра) | 4 |

## ЛИТЕРАТУРА

1. *Кострикин А.И.* Основы алгебры. М.: Изд-во МЦНМО, 2009.

2. *Курош А.Г.* Курс высшей алгебры. СПб.: Лань, 2007.

3. *Нефедов В.Н., Осипова В.А.* Курс дискретной математики. М.: Изд-во МАИ, 1992.

## ОГЛАВЛЕНИЕ