§1. Справочник по множествам и отображениям

1.1. Множества. Мы не будем заниматься основаниями теории множеств, полагаясь на школьное интуитивное представление о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множества мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

Множество X задано, как только про любой объект можно сказать, является он точкой множества X или нет. Принадлежность точки x множеству X записывается как $x \in X$. Два множества *равны*, если они состоят из одних и тех же элементов. Существует единственное множество, не содержащее ни одного элемента. Оно называется *пустым* и обозначается $\varnothing$. Если множество X конечно, то мы обозначаем через $|X|$ количество элементов в нём.

Множество X называется *подмножеством* множества Y, если каждый элемент $x \in X$ лежит также и в Y. В этом случае пишут $X \subset Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Непустые подмножества, отличные от всего множества, называются *собственными подмножествами*.

Упражнение 1.1. Сколько всего подмножеств (включая несобственные) имеется у множества, состоящего из n элементов?

Для любых двух множеств X и Y множество $X \cup Y$, состоящее из всех элементов, принадлежащих хотя бы одному из них, называется их *объединением*; множество $X \cap Y$, состоящее из всех элементов, принадлежащих одновременно каждому из них, называется их *пересечением*; множество $X \setminus Y$, состоящее из всех элементов множества X, которые не содержатся в Y, называется их *разностью*.

Упражнение 1.2. Проверьте, что операция пересечения выражается через разность по формуле $X \cap Y = X \setminus (X \setminus Y)$. Можно ли выразить разность через пересечение и объединение?

Если множество X является объединением непересекающихся подмножеств Y и Z, то говорят, что X является *дизъюнктным объединением* Y и Z и пишут $X = Y \sqcup Z$.

Множество $X \times Y$, элементами которого являются, по определению, всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

1.2. Отображения. Отображение $f : X \to Y$ из множества X в множество Y — это правило, которое сопоставляет каждой точке $x \in X$ некоторую однозначно определяемую по x точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f.

Множество всех точек $x \in X$, образ которых равен данной точке $y \in Y$, называется *полным прообразом* точки y (или *слоем* отображения f над y) и обозначается

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}.$$

Полные прообразы различных точек не пересекаются и могут быть как пустыми, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, называется *образом отображения* $f : X \to Y$ и обозначается

$$\operatorname{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \varnothing\} = \{y \in Y \mid \exists\, x \in X : f(x) = y\}.$$

Два отображения $f : X \to Y$ и $g : X \to Y$ *равны*, если их значения в каждой точке одинаковы: $\forall x \in X \;\; f(x) = g(x)$. Множество всех отображений из множества X в множество Y обозначается $\mathrm{Hom}(X, Y)$.

Отображение $f : X \to Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\mathrm{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюръективные отображения стрелками $X \twoheadrightarrow Y$.

Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$, т. е. когда прообраз каждой точки $y \in Y$ содержит не более одного элемента. Инъективные отображения мы обозначает стрелками $X \hookrightarrow Y$.

Упражнение 1.3. Перечислите все отображения $\{0, 1, 2\} \to \{0, 1\}$ и все отображения $\{0, 1\} \to \{0, 1, 2\}$. Сколько среди них вложений и сколько наложений?

Отображение $f : X \to Y$, которое является одновременно и вложением и наложением, называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*). Иными словами, биективность отображения f означает, что для каждого $y \in Y$ существует единственный $x \in X$, такой что $f(x) = y$. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$.

Упражнение 1.4. Какие из отображений: $\mathbb{N} \xrightarrow{x \mapsto x^2} \mathbb{N}$, $\mathbb{Z} \xrightarrow{x \mapsto x^2} \mathbb{Z}$, $\mathbb{Z} \xrightarrow{x \mapsto 7x} \mathbb{Z}$, $\mathbb{Q} \xrightarrow{x \mapsto 7x} \mathbb{Q}$ являются а) биекциями б) инъекциями в) сюръекциями?

Отображения $X \to X$ из множества X в себя обычно называют *эндоморфизмами* множества X. Множество всех эндоморфизмов обозначается $\mathrm{End}(X) \stackrel{\text{def}}{=} \mathrm{Hom}(X, X)$.

Упражнение 1.5 (принцип Дирихле). Покажите, что следующие три условия на множество X попарно равносильны друг другу:

а) X бесконечно

б) $\exists$ вложение $X \hookrightarrow X$, не являющееся наложением

в) $\exists$ наложение $X \twoheadrightarrow X$, не являющееся вложением.

Взаимно однозначные эндоморфизмы $X \xrightarrow{\sim} X$ называются *автоморфизмами* X и множество всех автоморфизмов обозначается через $\mathrm{Aut}(X)$. Автоморфизмы можно воспринимать как *перестановки* элементов множества X. У всякого множества X имеется *тождественный эндоморфизм* $\mathrm{Id}_X : X \to X$, который переводит каждый элемент в самого себя: $\forall x \in X \; \mathrm{Id}_X(x) = x$.

Упражнение 1.6. Счётно ли множество $\mathrm{Aut}(\mathbb{N})$?

Пример 1.1 (запись отображений словами)
Рассмотрим множества $X = \{1, 2, \ldots, n\}$ и $Y = \{1, 2, \ldots, m\}$, сопоставим каждому отображению $f : X \to Y$ последовательность его значений:

$$w(f) \stackrel{\text{def}}{=} \big(f(x_1), f(x_2), \ldots, f(x_n)\big) \tag{1-1}$$

и будем воспринимать её как n-буквенное слово, написанное при помощи m-буквенного алфавита Y. Так, отображениям $f : \{1, 2\} \to \{1, 2, 3\}$ и $g : \{1, 2, 3\} \to \{1, 2, 3\}$, действующим по правилам $f(1) = 3$, $f(2) = 2$ и $g(1) = 1$, $g(2) = 2$, $g(3) = 2$, сопоставятся слова $w(f) = (3, 2)$ и $w(g) = (1, 2, 2)$, составленные из букв алфавита $\{1, 2, 3\}$.

Запись отображения словом задаёт биекцию

$$w : \mathrm{Hom}(X, Y) \xrightarrow{\sim} \{\text{слова из } |X| \text{ букв в алфавите } Y\}, \quad f \mapsto w(f). \tag{1-2}$$

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюръективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых задействованы все буквы алфавита Y, причём каждая — ровно по одному разу.

1.3. Разбиения. Задать отображение $f : X \to Y$ это то же самое, что представить X в виде дизъюнктного объединения непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \operatorname{im}(f)$:

$$X = \bigsqcup_{y \in \operatorname{im}(f)} f^{-1}(y)\,. \tag{1-3}$$

Такой взгляд на отображения часто оказывается полезным при подсчёте числа элементов в том или ином множестве.

Скажем, когда все непустые слои отображения $f : X \to Y$ состоят из одного и того же числа точек $m = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X формулой

$$|X| = m \cdot |\operatorname{im} f|\,, \tag{1-4}$$

которая при всей своей банальности имеет множество применений.

Предложение 1.1
Если $|X| = n$ и $|Y| = m$, то $|\operatorname{Hom}(X, Y)| = m^n$.

Доказательство. Зафиксируем какую-нибудь точку $x \in X$ и рассмотрим *отображение вычисления*[1], сопоставляющее отображению $f : X \to Y$ его значение в точке x:

$$\operatorname{ev}_x : \operatorname{Hom}(X, Y) \to Y\,, \quad f \mapsto f(x)\,. \tag{1-5}$$

Прообраз $\operatorname{ev}_x^{-1}(y)$ любой точки $y \in Y$ находится в очевидной биекции с множеством всех отображений из $(n-1)$-элементного множества $X \smallsetminus \{x\}$ в Y:

$$\operatorname{ev}_x^{-1}(y) = \{f : X \to Y \mid f(x) = y\} \simeq \operatorname{Hom}(X \smallsetminus \{x\}\,,\, Y)\,.$$

Так как $\operatorname{im} \operatorname{ev}_x = Y$, по формуле (1-4) получаем $|\operatorname{Hom}(X, Y)| = |\operatorname{Hom}(X \smallsetminus \{x\}\,,\, Y)| \cdot |Y|$, т. е. при добавлению к множеству X одной точки, количество отображений из X в Y увеличивается в $|Y|$ раз. Отсюда $\operatorname{Hom}(X, Y) = |Y|^{|X|}$. □

Замечание 1.1. Множество отображений $\operatorname{Hom}(X, Y)$ часто обозначают через Y^X, и предыдущее рассуждение объясняет это обозначение.

Замечание 1.2. В предл. 1.1 мы молчаливо предполагали, что $m, n > 0$, т. е. что оба множества X, Y непусты. Если $X = \varnothing$, то удобно считать, что $\operatorname{Hom}(\varnothing, Y)$ для любого множества Y состоит ровно из одного элемента, «вкладывающего» $\varnothing$ в качестве подмножества в Y, ибо формально $\varnothing \subset Y$. И хотя отображения вычисления (1-5) в этом случае не определены, утверждение предл. 1.1 формально верно: $1 = m^0$. Если $Y = \varnothing$, то $\operatorname{Hom}(X, \varnothing) = \varnothing$ для любого $X \neq \varnothing$, а $\operatorname{Hom}(\varnothing, \varnothing)$ — это одноэлементное множество $\{\mathrm{Id}_\varnothing\}$. Первое также формально согласуется с предл. 1.1: $0^n = 0$. Последнее указывает на то, что 0^0 имеет смысл считать равным 1.

[1] обозначение «ev» является сокращением слова *evaluation*

Предложение 1.2
Если $|X| = n$, то $|\mathrm{Aut}\,(X)| = n!$.

Доказательство. Положим $Y = X$ в доказательстве предл. 1.1 и ограничим отображение вычисления (1-5) на подмножество биекций $\mathrm{Aut}\,(X) \subset \mathrm{Hom}(X, X)$. Получим отображение

$$\mathrm{ev}_x : \mathrm{Aut}\,(X) \to X\,, \quad f \mapsto f(x)\,.$$

Его слой $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X$ состоит из всех биекций $X \xrightarrow{\sim} X$, переводящих x в x'. Беря композицию такой биекции с автоморфизмом $X \xrightarrow{\sim} X$, который переставляет между собой x и x', оставляя все остальные точки на месте, мы получаем взаимно однозначное отображение из $\mathrm{ev}_x^{-1}(x')$ в множество автоморфизмов $(n-1)$-элементного множества $X \smallsetminus \{x\}$. Поэтому все слои $\mathrm{ev}_x^{-1}(x')$ непусты и состоят из одного и того же числа элементов. По формуле (1-4) $\quad |\mathrm{Aut}\,(X)| = |\mathrm{Aut}\,(X \smallsetminus \{x\})| \cdot |X|\,,$ $\quad$ т. е. при добавлении n-той точки к $(n-1)$-элементному множеству количество его автоморфизмов увеличивается в n раз. Поэтому $|\mathrm{Aut}\,(X)| = n \cdot (n-1) \cdot (n-2) \cdot \,\cdots\, \cdot 1 = n!$. □

Замечание 1.3. Так как $|\mathrm{Aut}\,(\varnothing)| = |\{Id_\varnothing\}| = 1$, мы по определению полагаем $0! \stackrel{\text{def}}{=} 1$.

Пример 1.2 (мультиномиальные коэффициенты)
При раскрытии скобок в выражении $(a_1 + a_2 + \,\cdots\, + a_m)^n$ получится сумма одночленов вида $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$, где каждый показатель k_i заключен в пределах $0 \leqslant k_i \leqslant n$, а общая степень $k_1 + k_2 + \,\cdots\, + k_m = n$. Коэффициент, возникающий при таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{k_1 \ldots k_m}$. Таким образом,

$$(a_1 + a_2 + \,\cdots\, + a_m)^n = \sum_{\substack{k_1 + k_2 + \,\cdots\, + k_m = n \\ \forall i\ 0 \leqslant k_i \leqslant n}} \binom{n}{k_1 \,\ldots\, k_m} \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}\,, \tag{1-6}$$

Чтобы явно выразить $\binom{n}{k_1 \ldots k_m}$ через $k_1, k_2, \ldots, k_m$, заметим, что раскрытие n скобок

$$(a_1 + a_2 + \,\cdots\, + a_m)(a_1 + a_2 + \,\cdots\, + a_m) \,\cdots\, (a_1 + a_2 + \,\cdots\, + a_m)$$

заключается в последовательном выборе внутри каждой из скобок какой-нибудь одной буквы и выписывании их слева направо друг за другом в одно n-буквенное слово. Это надо сделать всеми возможными способами и сложить все полученные слова. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$ суть слова, состоящие ровно из k_1 букв a_1, k_2 букв a_2, … , k_m букв a_m. Количество таких слов легко подсчитать по формуле (1-4).

А именно, сделаем на время k_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с k_2 буквами a_2, k_3 буквами a_3 и т. д. В результате получится набор из $n = k_1 + k_2 + \,\cdots\, + k_m$ попарно различных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(k_1)}}_{k_1 \text{ меченых букв } a_1},\ \underbrace{a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(k_2)}}_{k_2 \text{ меченых букв } a_2},\ \ldots\ \ldots\ \ldots,\ \underbrace{a_m^{(1)}, a_m^{(2)}, \ldots, a_m^{(k_m)}}_{k_m \text{ меченых букв } a_m}\,.$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n различными буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, $|X| = n!$. В качестве Y возьмём интересующее нас множество слов из k_1 одинаковых букв a_1, k_2 одинаковых букв a_2, и т. д. и рассмотрим отображение $f : X \to Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1!\cdot k_2!\cdot \ \cdots \ \cdot k_m!$ слов, которые получаются из y всевозможными расстановками k_1 верхних индексов у букв a_1, k_2 верхних индексов у букв a_2, и т. д. По формуле (1-4)

$$\binom{n}{k_1 \,\dots\, k_m} = \frac{n!}{k_1!\cdot k_2!\cdot \ \cdots \ \cdot k_m!}\,. \tag{1-7}$$

Тем самым, разложение (1-6) имеет вид

$$(a_1 + a_2 + \ \cdots \ + a_m)^n = \sum_{\substack{k_1+\ \cdots\ +k_m=n \\ \forall i\ 0\leqslant k_i\leqslant n}} \frac{n!\cdot a_1^{k_1} a_2^{k_2}\cdots a_m^{k_m}}{k_1!\cdot k_2!\cdot \ \cdots \ \cdot k_m!}\,. \tag{1-8}$$

Упражнение 1.7. Сколько всего слагаемых в правой части формулы (1-8)?

В частности, при $m = 2$ мы получаем известную формулу для раскрытия бинома с натуральным показателем[1]:

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!\cdot a^k b^{n-k}}{k!\,(n-k)!}\,. \tag{1-9}$$

При $m = 2$ мультиномиальный коэффициент

$$\binom{n}{k, n-k} = \frac{n\cdot(n-1)\cdot \ \cdots \ \cdot(n-k+1)}{k\cdot(k-1)\cdot \ \cdots \ \cdot 1}$$

(и в числителе и в знаменателе стоят по k последовательно убывающих сомножителей) обозначается через $\binom{n}{k}$ или C_n^k и называется k-тым *биномиальным коэффициентом* степени n или *числом сочетаний* из n по k.

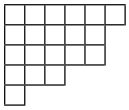
Пример 1.3 (диаграммы Юнга)
Разбиение конечного множества $X = \{1, 2, \dots, n\}$ в объединение непересекающихся подмножеств

$$X = X_1 \sqcup X_1 \sqcup X_2 \sqcup \ \dots \ \sqcup X_k\,. \tag{1-10}$$

часто бывает удобно кодировать следующим образом. Занумеруем подмножества в порядке нестрогого убывания их размера и обозначим количество элементов в i-том подмножестве через $\lambda_i = |X_i|$. Получим невозрастающую последовательность чисел

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)\,, \quad \lambda_1 \geqslant \lambda_2 \geqslant \ \cdots \ \geqslant \lambda_k\,,$$

которая называется *формой* разбиения (1-10). Форму разбиения удобно представлять себе в виде *диаграммы Юнга* — картинки вида

 , (1-11)

[1] это частный случай *формулы Ньютона*, которую в полной общности мы обсудим в n° 4.5, когда будем заниматься степенными рядами

составленной из выровненных по левому краю горизонтальных клетчатых полос, в i-той полосе λ_i клеток. Общее число клеток в диаграмме λ называется *весом* диаграммы и обозначается $|\lambda|$, а число строк называется *длиной* и обозначается $\ell(\lambda)$.

Так, диаграмма Юнга (1-11) отвечает разбиению формы $\lambda = (6,5,5,3,1)$ и имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 1.8. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток (включая пустую диаграмму и сам прямоугольник).

Будем называть *заполнением* диаграммы λ множеством X из $|X| = |\lambda|$ элементов произвольную расстановку этих элементов в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всего имеется $n!$ различных заполнений диаграммы λ множеством X.

Объединяя элементы, стоящие в i-той строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств $X_1, X_2, \dots, X_k$. Ясно, что любое разбиение (1-10) можно получить таким образом, так что мы получаем сюръективное отображение из множества заполнений диаграммы λ в множество разбиений множества X формы λ. Покажем, что все слои этого отображения состоят из одного и того же числа элементов.

Два заполнения приводят к одинаковым разбиениям тогда и только тогда, когда они получаются друг из друга перестановками элементов внутри строк и перестановками строк одинаковой длины между собою как единого целого. Если обозначить через m_i число строк длины[1] i в диаграмме λ, то перестановок первого типа будет $\prod \lambda_i! = \prod\limits_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod\limits_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod\limits_{i=1}^{n} (i!)^{m_i} m_i!$ элементов. Из формулы (1-4) вытекает

Предложение 1.3
Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, …, m_n n-элементных подмножеств равно

$$\frac{n!}{\prod\limits_{i=1}^{n} m_i! \cdot (i!)^{m_i}}. \tag{1-12}$$

□

1.4. Классы эквивалентности. Альтернативный способ разбить заданное множество X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так. Назовём *бинарным отношением* на множестве X произвольное подмножество $R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}$. Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$.

[1] отметим, что многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \cdots + nm_n$

Например, на множестве целых чисел $X = \mathbb{Z}$ имеются бинарные отношения

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{1-13}$$

$$\text{неравенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{1-14}$$

$$\text{делимость} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 | x_2 \tag{1-15}$$

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \,(\mathrm{mod}\ n) \tag{1-16}$$

(последнее условие $x_1 \equiv x_2 \,(\mathrm{mod}\ n)$ читается как «x_1 сравнимо с x_2 по модулю n» и по определению означает, что x_1 и x_2 имеют одинаковые остатки от деления на n).

Определение 1.1
Бинарное отношение $\underset{R}{\sim}$ называется *эквивалентностью*, если оно обладает следующими тремя свойствами:

$$\begin{aligned} &\textit{рефлексивность}: && \forall\, x \in X \; x \underset{R}{\sim} x \\ &\textit{транзитивность}: && \forall\, x_1, x_2, x_3 \in X \text{ из } x_1 \underset{R}{\sim} x_2 \text{ и } x_2 \underset{R}{\sim} x_3 \text{ вытекает } x_1 \underset{R}{\sim} x_3 \\ &\textit{симметричность}: && \forall\, x_1, x_2 \in X \; x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1. \end{aligned}$$

Среди перечисленных выше бинарных отношений на множестве $\mathbb{Z}$ отношения (1-13) и (1-16) являются эквивалентностями, а (1-14) и (1-15) не являются (они несимметричны).

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $x_1 \sim x_2$, означающее, что x_1 и x_2 лежат в одном и том же подмножестве этого разбиения, очевидно, является эквивалентностью.

Наоборот, пусть на множестве X задано какое-нибудь отношение эквивалентности R. Рассмотрим для каждого $x \in X$ подмножество в X, состоящее из всех элементов, эквивалентных x. Оно называется *классом эквивалентности* элемента x и обозначается

$$[x]_R = \{z \in X \mid x \underset{R}{\sim} z\} = \{z \in X \mid z \underset{R}{\sim} x\}$$

(второе равенство выполняется благодаря симметричности отношения R). Два класса $[x]_R$ и $[y]_R$ либо вообще не пересекаются, либо полностью совпадают. В самом деле, если существует элемент z, эквивалентный и x и y, то в силу симметричности и транзитивности отношения $\underset{R}{\sim}$ элементы x и y будут эквивалентны между собой, а значит, любой элемент, эквивалентный x, будет эквивалентен также и y, и наоборот. Таким образом, множество X распадается в дизъюнктное объединение различных классов эквивалентности.

Множество классов эквивалентности по отношению $R \subset X \times X$ обозначается X/R и называется *фактором* множества X по отношению R. Сюръективное отображение

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]\,, \tag{1-17}$$

сопоставляющее каждому элементу $x \in X$ его класс эквивалентности $[x] \in X/R$, называется *отображением факторизации*. Слои этого отображения суть классы эквивалентных элементов. Наоборот, любое сюръективное отображение $f : X \twoheadrightarrow Y$ является отображением факторизации по отношению эквивалентности $x_1 \sim x_2 \iff f(x_1) = f(x_2)$.

Пример 1.4 (классы вычетов)
Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (1-16) обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и опускать индекс n, когда понятно чему он равен. Класс эквивалентности

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z-x) \vdots n\} \tag{1-18}$$

называется *классом вычетов по модулю n*. Отображение факторизации

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n), \quad z \mapsto [z]_n$$

называется *приведением по модулю n*. Множество $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n,\ [1]_n,\ \dots,\ [n-1]_n.$$

При желании их можно воспринимать как остатки от деления на n, но в практических вычислениях удобнее работать с ними именно как с *подмножествами* в $\mathbb{Z}$, поскольку возможность по-разному записывать один и тот же класс часто упрощает вычисления. Например, остаток от деления 12^{100} на 13 можно искать как

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}. \tag{1-19}$$

Упражнение 1.9. Докажите правомочность этого вычисления: проверьте, что классы вычетов $[x+y]_n$ и $[xy]_n$ не зависят от выбора чисел $x \in [x]_n$ и $y \in [y]_n$, т. е. правила

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{1-20}$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \tag{1-21}$$

корректно определяют на множестве $\mathbb{Z}/(n)$ операции сложения и умножения[1].

1.4.1. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap\limits_\nu R_\nu \subset X \times X$ также является отношением эквивалентности. В самом деле, если каждое из множеств $R_\nu \subset X \times X$ содержит диагональ

$$\Delta = \{(x,x) \mid x \in X\} \subset X \times X,$$

переходит в себя при симметрии $(x,y) \leftrightarrows (y,x)$ и вместе с каждой парой точек вида (x,y), (y,z) содержит также и точку (x,z), то этими свойствами обладает и пересечение $\bigcap\limits_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества $R \subset X \times X$ существует *наименьшее по включению* отношение эквивалентности $\overline{R}$, содержащее R — пересечение всех содержащих R отношений эквивалентности. Отношение $\overline{R}$ называется эквивалентностью, *порождённой* отношением R. К сожалению, по данному множеству R не всегда легко судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу[2], часто бывает не просто.

[1] именно такое умножение $[12]^{100} = \underbrace{[12]\cdot[12]\cdot\dots\cdot[12]}_{100} = \left[12^{100}\right]$ и использовано в (1-19)

[2] т. е. существует ли хоть одна собственная (отличная от всего произведения $X \times X$) эквивалентность, содержащая R

Пример 1.5 (дроби)
Множество рациональных чисел $\mathbb{Q}$ обычно определяют как множество дробей a/b с $a, b \in \mathbb{Z}$ и $b \neq 0$. При этом под *дробью* понимается класс эквивалентности упорядоченных пар $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus 0)$ по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \qquad \forall\, c \neq 0\,. \tag{1-22}$$

Отношения (1-22) выражают собою равенства дробей $a\,/\,b = ac\,/\,bc$, но сами по себе не образуют эквивалентности. Например, при $a_1 b_2 = a_2 b_1$ в двухшаговой цепочке отождествлений (1-22)

$$(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$$

самый левый и самый правый элементы может оказаться нельзя отождествить напрямую по правилу (1-22). Но эквивалентность, порождённая отождествлениями (1-22), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{1-23}$$

Оказывается, что к этим отождествлениям уже больше ничего добавлять не надо.

Упражнение 1.10. Проверьте, что набор отношений (1-23) рефлексивен, симметричен и транзитивен (и, тем самым, полностью описывает минимальное отношение эквивалентности, содержащее все отождествления (1-22)).

1.5. Композиции отображений. Отображение $X \to Z$, получающееся в результате последовательного выполнения двух отображений $X \xrightarrow{f} Y \xrightarrow{g} Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf. Таким образом,

$$\forall\, x \in X \;\; gf(x) \stackrel{\text{def}}{=} g(f(x))\,.$$

Композиция gf определена только тогда, когда образ f содержится в множестве, на котором определено отображение g.

Композицию трёх отображений $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ можно вычислять двумя способами: как $(hg)f$ или как $h(gf)$. В обоих случаях получится отображение, переводящее точку $x \in X$ в точку $h(g(f(x))) \in T$. Это означает, что композиция отображений *ассоциативна*[1]: $(hg)f = h(gf)$ всякий раз, когда написанные композиции определены.

Предостережение 1.1. Хотя мы и обозначаем композицию отображений точно так же, как произведение, обращаться с формулами, включающими в себя композиции, надо с осторожностью: некоторые привычные по опыту работы с числами преобразования недопустимы при работе с композициями отображений. Так, умножение чисел *коммутативно*[2]: $fg = gf$, а композиция отображений, как правило, нет[3].

[1] т. е. подчиняется *сочетательному закону* — не зависит от расстановки скобок

[2] т. е. удовлетворяет *переместительному закону* — перестановка сомножителей в произведении не влияет на результат

[3] хотя бы потому, что одна из частей этого равенства может быть определена, а другая — нет

Упражнение 1.11. Рассмотрим на плоскости пару различных прямых ℓ_1, ℓ_2, пересекающихся в точке O, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. При каком условии на прямые выполняется равенство $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Чтобы почувствовать отличие алгебраических свойств композиции от свойств умножения чисел, поучительно взглянуть на «таблицу умножения» отображений из двухэлементного множества $X = \{1, 2\}$ в себя.

Есть ровно четыре таких отображения, причём все композиции между ними определены. Если обозначать отображение $f \in \mathrm{End}(X)$ двухбуквенным словом $(f(1),\ f(2))$, как в прим. 1.1, то эти четыре эндоморфизма запишутся словами

$$(1,1),\ (1,2) = \mathrm{Id}_X,\ (2,1),\ (2,2).$$

Значения композиций gf представлены в таблице:

$g \diagdown f$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$(1,2)$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(2,1)$	$(2,2)$	$(2,1)$	$(1,2)$	$(1,1)$
$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$

(1-24)

Обратите внимание на то, что $(2,2) \circ (1,1) \neq (1,1) \circ (2,2)$, а также на то, что в верхней и нижней строках все произведения одинаковы, но «сократить общий множитель» при этом нельзя, т. е. из равенства $fg_1 = fg_2$, вообще говоря, не следует равенство $g_1 = g_2$, как не следует оно и из равенства $g_1 f = g_2 f$.

Упражнение 1.12 (левые обратные отображения). Покажите, что следующие три условия на отображение $f : X \to Y$ эквивалентны:

а) f инъективно

б) $\exists\ g : Y \to X$ такое что $gf = \mathrm{Id}_X$ (такое g называется *левым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \to X$ из $fg_1 = fg_2$ вытекает $g_1 = g_2$

и выясните, сколько левых обратных отображений имеется у заданного вложения n-элементного множества в m-элементное.

Упражнение 1.13 (правые обратные отображения). Покажите, что следующие три условия на отображение $f : X \to Y$ эквивалентны:

а) f сюръективно

б) $\exists\ g : Y \to X$ такое что $fg = \mathrm{Id}_Y$ (такое g называется *правым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \to X$ из $g_1 f = g_2 f$ вытекает $g_1 = g_2$

и выясните, сколько правых обратных отображений имеется у заданного наложения m-элементного множества на n-элементное.

1.5.1. Обратимые отображения. Если отображение $g : X \xrightarrow{\sim} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки. В этом случае правило $y \mapsto g^{-1}(y)$ определяет отображение $g^{-1} : Y \to X$, которое одновременно является и левым и правым обратным к g в смысле упр. 1.12 и упр. 1.13:

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X,$$

Отображение g^{-1} называется *двусторонним обратным* к g.

Предложение 1.4
Следующие условия на отображение $g : X \to Y$ попарно эквивалентны:

(1) g взаимно однозначно

(2) существует такое отображение $g' : Y \to X$, что $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

(3) g обладает левым и правым обратными отображениями[1].

При выполнении этих условий любое отображение g' из (2) и любые левые и правые обратные к g отображения из (3) совпадают друг с другом и с отображением g^{-1} описанным выше.

Доказательство. Импликация (1) ⇒ (2) уже была установлена. Импликация (2) ⇒ (3) очевидна. Докажем, что (3) ⇒ (2). Если у отображения $g : X \to Y$ есть левое обратное $f : Y \to X$ и правое обратное $h : Y \to X$, то $f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h$ и условие (2) выполняется для $g' = f = h$.

Остаётся показать, что (2) ⇒ (1) и доказать равенство $g' = g^{-1}$. Поскольку $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, для любого $x \in g^{-1}(y)$ выполнено равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$. Поэтому $f^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, и $g' = g^{-1}$. □

1.6. Группы преобразований. Непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$.

Если группа преобразований G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G.

Если подмножество $H \subset G$ тоже является группой, то H называются *подгруппой* группы G.

Пример 1.6 (группы перестановок)
Множество $\mathrm{Aut}(X)$ всех взаимно однозначных отображений $X \to X$ является группой. Эта группа называется *симметрической группой* (или *группой перестановок*) множества X. Все прочие группы преобразований множества X являются подгруппами этой группы.

Группа перестановок n-элементного множества $\{1, 2, \ldots, n\}$ обозначается S_n и называется n-той *симметрической группой*. Согласно предл. 1.2 $|S_n| = n!$.

Перестановку $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ мы будем записывать строчкой

$$(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

её значений $\sigma_i = \sigma(i)$, как в прим. 1.1. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ это отображения

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \end{array} \quad \text{и} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

[1] обратите внимание, что совпадения левого обратного отображения с правым обратным отображением не требуется

а их композиции записываются как $\sigma\tau = (4,2,1,3)$ и $\tau\sigma = (4,1,3,2)$.

Упражнение 1.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (1-24) на стр. 12.

1.6.1. Абелевы группы. Группа G, в которой любые два элемента $f, g \in G$ перестановочны, т. е. удовлетворяют соотношению $fg = gf$, называется *коммутативной* или *абелевой*. Примерами абелевых групп являются группы параллельных переносов плоскости или пространства, а также группа SO_2 поворотов плоскости вокруг фиксированной точки. Для каждого натурального $n \geqslant 2$ повороты на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка* n.

Ответы и указания к некоторым упражнениям

Упр. 1.1. Ответ: 2^n.

Упр. 1.2. Ответ на второй вопрос: нет. Решение: пусть $X = \{1, 2\}$, $Y = \{2\}$; тогда все возможные значения пересечений и объединений между ними суть

$$X \cap Y = Y \cap Y = Y \cup Y = Y$$
$$X \cup Y = X \cup X = X \cap X = X$$

и любая формула, составленная из X, Y, $\cap$ и $\cup$, даст на выходе либо $X = \{1, 2\}$, либо $Y = \{2\}$, тогда как $X \setminus Y = \{1\}$.

Упр. 1.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. 1.5. Если множество X конечно, всякое отображение $X \to X$, которое инъективно или сюръективно, автоматически биективно. Если множество X бесконечно, то оно содержит подмножество, изоморфное $\mathbb{N}$, а у $\mathbb{N}$ есть инъективные небиективные эндоморфизмы (например, $n \mapsto (n+1)$) и сюръективные небиективные эндоморфизмы (например, $1 \mapsto 1$ и $n \mapsto (n-1)$ при $n \geqslant 2$), и их можно продолжить до эндоморфизмов $X \to X$ тождественным действием на $X \setminus \mathbb{N}$.

Упр. 1.6. Ответ: нет. Воспользуйтесь рассуждением Кантора: предположите, что все биекции $\mathbb{N} \to \mathbb{N}$ можно занумеровать натуральными числами, и, пользуясь этим списком, постройте биекцию, которая при каждом $k = 1, 2, 3, \ldots$ отображает число $k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 1.7. Ответ: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(k_1, k_2, \ldots, k_m)$ с суммой $\sum k_i = n$. Такой набор можно закодировать словом, составленным из $(m-1)$ букв 0 и n букв 1 : сначала пишем k_1 единиц, потом нуль, потом k_2 единиц, потом нуль, и т. д. (слово кончится k_m единицами, стоящими следом за последним, $(m-1)$-м нулём).

Упр. 1.8. Ответ: $\binom{n+k}{k}$. Каждая такая диаграмма представляет собою ломаную, ведущую из левого нижнего угла прямоугольника в правый верхний. В такой ломаной ровно n горизонтальных звеньев и ровно k вертикальных.

Упр. 1.9. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \ell \in \mathbb{Z}$. Тогда $x' + y' = x + y + n(k + \ell)$ и $x'y' = xy + n(\ell x + ky + k\ell n)$ сравнимы по модулю n с $x + y$ и xy соответственно, т. е. $[x' + y']_n = [x + y]_n$ и $[x'y']_n = [xy]_n$.

Упр. 1.10. Рефлексивность и симметричность очевидны. Транзитивность: если $(p, q) \sim (r, s)$ и $(r, s) \sim (u, w)$, т. е. $ps - rq = 0 = us - rw$, то $psw - rqw = 0 = usq - rwq$, откуда $s(pw - uq) = 0$, и $pw = uq$, т. е. $(p, q) \sim (u, w)$.

Упр. 1.11. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi/2$, то отражение относительно ℓ_1, а потом отражение относительно ℓ_2 — это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно ℓ_1 и ℓ_2 коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. 1.12. а) $\Rightarrow$ б). Левое обратное к вложению $f : X \hookrightarrow Y$ должно переводить $y = f(x) \in \operatorname{im} f$ в x, а на элементах $Y \setminus \operatorname{im} f$ может действовать как угодно. В частности, ответ на последний вопрос задачи — $(m-n)^n$.

б) ⇒ в). Равенство $g_1 = g_2$ получается из равенства $fg_1 = fg_2$ умножением обеих частей слева на любое левое обратное к f отображение.
в) ⇒ а). Если $f(x_1) = f(x_2)$ для каких-то $x_1 \neq x_2$, положим $g_1 = \mathrm{Id}_X$, а в качестве g_2 возьмём автоморфизм $X \to X$, который меняет между собой точки x_1 и x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$.

Упр. 1.13. Аналогично предыдущему упр. 1.12.

Упр. 1.14. Таблица композиций gf в симметрической группе S_3:

$g \diagdown f$	(1, 2, 3)	(1, 3, 2)	(3, 2, 1)	(2, 1, 3)	(2, 3, 1)	(3, 1, 2)
(1, 2, 3)	(1, 2, 3)	(1, 3, 2)	(3, 2, 1)	(2, 1, 3)	(2, 3, 1)	(3, 1, 2)
(1, 3, 2)	(1, 3, 2)	(1, 2, 3)	(3, 1, 2)	(2, 3, 1)	(2, 1, 3)	(3, 2, 1)
(3, 2, 1)	(3, 2, 1)	(2, 3, 1)	(1, 2, 3)	(3, 1, 2)	(1, 3, 2)	(2, 1, 3)
(2, 1, 3)	(2, 1, 3)	(3, 1, 2)	(2, 3, 1)	(1, 2, 3)	(3, 2, 1)	(1, 3, 2)
(2, 3, 1)	(2, 3, 1)	(3, 2, 1)	(2, 1, 3)	(1, 3, 2)	(3, 1, 2)	(1, 2, 3)
(3, 1, 2)	(3, 1, 2)	(2, 1, 3)	(1, 3, 2)	(3, 2, 1)	(1, 2, 3)	(2, 3, 1)