§1. Множества и отображения.

1.1. Символические сокращения. Если это не наносит большого вреда восприятию текста, мы в этих записках иногда вульгарно заменяем некоторые стандартные словесные обороты их общепринятыми сокращёнными обозначениями:

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ — множества *натуральных*, *целых*, *рациональных*, *действительных* и *комплексных* чисел соответственно.

$\Rightarrow$ и $\Longleftrightarrow$ — «влечёт» и «равносильно»; например, $k \in \mathbb{Z} \Rightarrow k(k+1)/2 \in \mathbb{Z}$; или: x — чётно $\Longleftrightarrow$ $x = 2k$, где $k \in \mathbb{Z}$.

$\forall$ — «для любого»; например: $\forall\, k \in \mathbb{Z}\;\; k(k+1)/2 \in \mathbb{Z}$.

$\exists$ — «существует»; например: $x \in \mathbb{Z}$ чётно, если $\exists\, k \in \mathbb{Z}$, такой что $x = 2k$.

$:$ — «такой что»; например: $x \in \mathbb{Z}$ чётно, если $\exists\, k \in \mathbb{Z} \, : \, x = 2k$.

$\{\, x \in X \mid \dots \,\}$ — множество всех $x \in X$, для которых выполняется свойство « … »; например, формула $\{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 2k = x\}$ задаёт множество чётных чисел.

$\{\, \dots \,\}$ — множество чего-то, что описывается текстом « … »; например: {чётные числа}.

1.2. Множества. Мы не будем заниматься основаниями теории множеств[1], оставаясь при интуитивных представлениях о множестве как абстрактной «совокупности произвольных объектов[2]». Эти представления таковы. Каждое множество состоит из *элементов*, которые мы часто будем также называть его *точками*. Множество задано, как только про любой объект можно сказать, является он точкой данного множества или нет. Принадлежность точки x множеству X записывается как $x \in X$. Все точки в любом множестве, по определению, *различны*. Два множества *равны*, если они состоят из одних и тех же элементов. Единственное множество, не содержащее ни одного элемента, называется *пустым* и обозначается $\varnothing$. Множество X называется *подмножеством* множества Y (обозначение: $X \subset Y$), если каждый элемент $x \in X$ лежит также и в Y. В частности, пустое множество является подмножеством любого множества.

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 $X \smallsetminus Y$, состоящее из всех элементов множества X, которые не содержатся в Y, называется их *разностью*.

Упражнение 1.1. Сколько различных подмножеств (включая пустое и всё множество) имеется у множества, состоящего из n элементов?

Упражнение 1.2. Можно ли выразить:
а) пересечение через разность? б) разность через пересечение и объединение?

Если множество X является объединением множеств Y и Z, таких что $Y \cap Z = \varnothing$, то это записывается как $X = Y \sqcup Z$ и называется *дизъюнктным объединением*. 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] чуть позже вы познакомитесь с ними в курсе математической логики

[2] на самом деле в теории множеств, как и в программировании, надо зафиксировать некоторый набор выразительных средств («язык») и ограничиться только такими «совокупностями» и «объектами», которые можно описать посредством этого языка; однако прежде, чем придумывать новый язык программирования, разумно спросить себя, чего мы от него хотим; минимальный набор требований к *языку теории множеств*, который вы будете изучать в курсе логики, как раз и состоит в том, чтобы на нём можно было непротиворечиво выразить всё, чему вас обучат в курсах алгебры, геометрии и анализа

1.3. Отображения. Отображение $X \xrightarrow{f} Y$ из множества X в множество Y — это правило, сопоставляющее каждой точке $x \in X$ некоторую точку $f(x) \in Y$, однозначно определяемую по x. Эта точка называется *образом* точки x при отображении f. Множество всех точек x, образ которых равен данной точке $y \in Y$ обозначается

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

и называется *полным прообразом*[1] точки y. Полный прообраз может быть как пустым, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, обозначается

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

и называется *образом отображения* $X \xrightarrow{f} Y$.

Два отображения $X \xrightarrow{f} Y$ и $X \xrightarrow{g} Y$ *равны*, если их значения в каждой точке одинаковы: $f(x) = g(x) \quad \forall\, x \in X$. Множество всех отображений из множества X в множество Y обозначается $\operatorname{Hom}(X, Y)$. При $X = Y$ отображения $X \longrightarrow X$ обычно называют *эндоморфизмами* множества X и пишут $\operatorname{End}(X)$ вместо $\operatorname{Hom}(X, X)$. У всякого множества X имеется *тождественный эндоморфизм* $X \xrightarrow{\mathrm{Id}_X} X$, который переводит каждый элемент в самого себя: $\forall\, x \in X \ \ \mathrm{Id}_X(x) = x$.

Отображение $X \xrightarrow{f} Y$ называется *наложением*[2], если $\operatorname{im}(f) = Y$, т. е. прообраз каждой точки $y \in Y$ не пуст. Отображение f называется *вложением*[3], если $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, т. е. прообраз каждой точки $y \in Y$ содержит не более одной точки. При желании подчеркнуть, что отображение инъективно (соотв. сюрьективно), мы будем изображать его стрелкой $X \hookrightarrow Y$ (соотв. $X \twoheadrightarrow Y$).

Отображение $X \xrightarrow{f} Y$ называется *взаимно однозначным*[4], если для каждого $y \in Y$ существует единственный $x \in X$, такой что $f(x) = y$. Иными словами, биективность отображения означает, что оно одновременно является вложением и наложением. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$. Изоморфизмы $X \xrightarrow{\sim} X$ чаще называют *автоморфизмами* или *симметриями*. В «житейском» понимании, автоморфизмы — это *перестановки элементов*. Множество всех автоморфизмов множества X обозначается через $\operatorname{Aut}(X)$.

Упражнение 1.3. Нарисуйте все отображения а) $\{0, 1, 2\} \longrightarrow \{0, 1\}$; б) $\{0, 1\} \longrightarrow \{0, 1, 2\}$. Сколько среди них сюрьективных и сколько инъективных?

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

1.3.1. Пример: отображения и слова. Пусть $X = \{x_1, x_2, \dots, x_n\}$, $Y = \{y_1, y_2, \dots, y_m\}$. Сопоставим каждому отображению $X \xrightarrow{f} Y$ выписанный в ряд слева направо набор его значений:

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

и будем воспринимать его как n-буквенное слово, написанное при помощи m-буквенного алфавита

$$y_1\, y_2\, \cdots\, y_m\, .$$

Например, отображениям $\{1, 2\} \xrightarrow{f} \{1, 2, 3\}$ и $\{1, 2, 3\} \xrightarrow{g} \{1, 2, 3\}$

$$f:\ \begin{tikzcd}[row sep=tiny] & 1 \\ 1 \arrow[ddr] & \\ & 2 \\ 2 \arrow[ur] & \\ & 3 \end{tikzcd} \qquad g:\ \begin{tikzcd} 1 \arrow[r] & 1 \\ 2 \arrow[r] & 2 \\ 3 \arrow[ur] & 3 \end{tikzcd}$$

[1] а также *слоем* отображения f над точкой y

[2] а также *сюрьектцией* или *эпиморфизмом*

[3] а также *инъекцией*, или *мономорфизмом*

[4] а также *биекцией* или *изоморфизмом*

отвечают слова $w(f) = (3,2)$ и $w(g) = (1,2,2)$, составленные из букв трёхбуквенного алфавита $\{1, 2, 3\}$. Очевидно, что построенное нами отображение

$$w : \mathrm{Hom}(X,Y) \xrightarrow{\sim} \{n\text{-буквенные слова в алфавите } y_1\, y_2\, \dots\, y_m\} \tag{1-2}$$

является биекцией.

1.3.2. ПРЕДЛОЖЕНИЕ. *Если множество X состоит из n элементов, а множество Y — из m, то множество $\mathrm{Hom}(X,Y)$ состоит из m^n элементов.*

Доказательство. Обозначим через $W_m(n)$ количество всех n-буквенных слов, которые написать при помощи алфавита из m букв. Выпишем все эти слова на m страницах, поместив на i-тую страницу все слова, начинающиеся на i-тую букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Стало быть $W_m(n) = m \cdot W_m(n-1) = m \cdot m \cdot W(n-2) = \dots = m^{n-1} \cdot W(1) = m^n$. □

1.3.3. ПРЕДЛОЖЕНИЕ. *У n-элементного множества имеется ровно $n!$ автоморфизмов.*

Доказательство. Пусть $X = \{x_1, x_2, \dots, x_n\}$. Построенный в n° 1.3.1 изоморфизм (1-2) между отображениями и словами устанавливает взаимно однозначное соответствие между биекциями $X \xrightarrow{f} X$ и n-буквенными словами (в алфавите $x_1, x_2, \dots, x_n$), содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. На каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \dots = n \cdot (n-1) \cdot (n-2) \cdot \,\cdots\, \cdot 2 \cdot 1$. □

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.

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

1.4. Отображения и разбиения. Со всяким отображением $X \xrightarrow{f} Y$ связано разбиение множества X в объединение непересекающихся подмножеств — полных прообразов различных точек $y \in Y$. Поэтому задать отображение $X \xrightarrow{f} Y$ — это то же самое, что представить X в виде объединения непустых непересекающихся подмножеств и занумеровать эти подмножества точками $y \in \mathrm{im}\,(f)$:

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

Такой взгляд на отображения часто бывает очень полезен.

1.4.1. Пример: другое доказательство предложений (n° 1.3.2)–(n° 1.3.3). Обозначим через $\mathrm{Map}_{\,m,n}$ множество всех отображений из n-элементного множества X_n в m-элементное множество Y_m, зафиксируем какой-нибудь элемент $x \in X_n$ и рассмотрим *отображение вычисления*

$$\mathrm{ev}_x : \mathrm{Map}_{\,m,n} \xrightarrow{f \mapsto f(x)} Y_m \ , \tag{1-4}$$

которое сопоставляет каждому отображению $X_n \xrightarrow{f} Y_m$ его значение в точке x. Отображение вычисления, очевидно, сюрьективно. Прообраз каждой точки $y \in Y$ находится во взаимно однозначном соответствии с множеством всех отображений из $(n-1)$-элементного множества $X_{n-1} = X_n \smallsetminus \{x\}$ (получающегося выкидыванием из X точки x) в Y_m:

$$\mathrm{ev}_x^{-1}(y) = \{X_n \xrightarrow{f} Y_m \mid f(x) = y\} \simeq \mathrm{Hom}(X_{n-1}, Y_m) \ ,$$

Разложение (1-3) означает в этом случае, что множество $\mathrm{Map}_{\,m,n}$ распадается в дизъюнктное объединение m подмножеств, каждое из которых изоморфно $\mathrm{Map}_{\,m,(n-1)}$. Поэтому[1]

$$|\mathrm{Map}_{\,m,n}| = m \cdot |\mathrm{Map}_{\,m,(n-1)}| = m \cdot m \cdot |\mathrm{Map}_{\,m,(n-2)}| = \ \cdots \ = m^{n-1} \cdot |\mathrm{Map}_{\,m,1}| = m^n \ .$$

Аналогичным образом, обозначим через $\mathfrak{S}_n$ множество автоморфизмов n-элементного множества X_n, зафиксируем $x \in X_n$ и рассмотрим *отображение вычисления*

$$\mathrm{ev}_x : \mathfrak{S}_n \xrightarrow{f \mapsto f(x)} X_n \ .$$

[1]здесь и далее мы обозначаем через $|M|$ число элементов в конечном множестве M

Повторяя предыдущее рассуждение, мы видим, что $\mathfrak{S}_n$ распадается в объединение непересекающихся слоёв отображения ev_x, причём слой $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X_n$, состоящий из всех биекций $X_n \xrightarrow{\sim} X_n$, переводящих x в x', изоморфен множеству всех биекций между $(n-1)$-элементным множеством $X_{n-1} = X \smallsetminus \{x\}$ и $(n-1)$-элементным множеством $X'_{n-1} = X \smallsetminus \{x'\}$. Поэтому число элементов во всех слоях одинаково и равно $|\mathfrak{S}_{n-1}|$. Стало быть,

$$|\mathfrak{S}_n| = |X_n| \cdot |\mathfrak{S}_{n-1}| = n \cdot |\mathfrak{S}_{n-1}| = n \cdot (n-1) \cdot |\mathfrak{S}_{n-2}| = \cdots = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!\,.$$

Внимательно сопоставляя нынешние рассуждения с доказательствами из (n° 1.3.2–n° 1.3.3), нетрудно составить «словарик», позволяющий переговаривать одни в другие. Так фраза «зафиксируем какой-нибудь элемент $x \in X$» из нынешнего доказательства на языке (n° 1.3.2–n° 1.3.3) звучала бы как «зафиксируем в слове $w(f)$ какою-нибудь позицию, например, будем смотреть на *самую левую* букву слова». При этом «самую левую» означает, что в качестве $x \in X_n$ фиксируется $x = x_1$, а «смотреть, чему равна самая левая буква в слове $f(w)$» означает «применить к f отображение вычисления ev_{x_1}». Читателю настоятельно рекомендуется во всех деталях проследить это соответствие до конца.

1.4.2. Пример: мультиномиальные коэффициенты. При раскрытии скобок и приведении подобных слагаемых в выражении $(a_1 + a_2 + \cdots + a_k)^n$ мы будем получать (взятые с некоторыми коэффициентами) одночлены $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$, показатели степеней которых принимают любые целые значения $0 \leqslant m_i \leqslant n$ суммарной степени $m_1 + m_2 + \cdots + m_k = n$, т. е.

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{m_1 + m_2 + \cdots + m_k = n} \binom{n}{m_1 \dots m_k} \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}\,, \tag{1-5}$$

где через $\binom{n}{m_1 \dots m_k}$ обозначен коэффициент, возникающий при соответствующем одночлене[1]. Перемножение n скобок $(a_1 + a_2 + \cdots + a_k)$ заключается в выборе внутри каждой из скобок по букве, перемножении этих букв и суммировании всех получившихся произведений (отвечающих всем возможным выборам букв внутри скобок). Выбирая в каждой скобке какую-нибудь букву и записывая выбранные буквы слева направо друг за другом, мы получаем n-буквенное слово. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$ при этом биективно соответствуют словам из m_1 букв a_1, m_2 букв a_2, … , m_k букв a_k. Чтобы подсчитать количество таких слов, сделаем m_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с m_2 буквами a_2, m_3 буквами a_3 и т. д. В результате получится набор из $n = m_1 + m_2 + \cdots + m_k$ попарно различных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \dots, a_1^{(m_1)}}_{m_1 \text{ меченых букв } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \dots, a_2^{(m_2)}}_{m_2 \text{ меченых букв } a_2}, \dots \dots \dots, \underbrace{a_k^{(1)}, a_k^{(2)}, \dots, a_k^{(m_k)}}_{m_k \text{ меченых букв } a_k}\,. \tag{1-6}$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, всего таких слов будет $n!$. Теперь обозначим через Y интересующее нас множество слов из m_1 одинаковых букв a_1, m_2 одинаковых букв a_2, … , m_k одинаковых букв a_k, и рассмотрим отображение $X \xrightarrow{f} Y$, которое стирает верхние индексы у помеченных букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $m_1! \cdot m_2! \cdot \cdots \cdot m_k!$ слов, получающихся всевозможными перестановками m_1 верхних индексов у букв $a_1^{(j)}$, m_2 верхних индексов у букв $a_2^{(j)}$, … , m_k верхних индексов у букв $a_k^{(j)}$ в каком-нибудь одном слове $x \in X$, переходящем в y. Из разложения (1-3) вытекает равенство

$$\binom{n}{m_1 \dots m_k} = \frac{n!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!}\,, \tag{1-7}$$

и формула (1-5) приобретает вид

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{m_1 + m_2 + \cdots + m_k = n} \frac{n! \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!}\,. \tag{1-8}$$

При $k = 2$ она превращается в известную формулу раскрытия бинома с натуральным показателем[2]:

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

[1] он называется *мультиномиальным коэффициентом*

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

Упражнение 1.7. Из скольких слагаемых состоит сумма в правой части формулы (1-8)?

1.5. Разбиения и отношения. Альтернативный способ задавать разбиение данного множества X в объединение непересекающихся подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество разбиения «эквивалентными». Формальное описание этой процедуры таково. Назовём *бинарным отношением* на множестве X произвольное подмножество $R \subset X \times X$ в множестве всех упорядоченных пар

$$X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}\,.$$

Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$. Например, на множестве целых чисел $X = \mathbb{Z}$ часто рассматривают бинарные отношения

$$\underset{R}{\sim} \;:=\; «\leqslant» \qquad (x_1 \leqslant x_2 \text{ означает, что } x_1 \text{ не превосходит } x_2) \tag{1-10}$$

$$\underset{R}{\sim} \;:=\; «\,\vdots\,» \qquad (x_1 \,\vdots\, x_2 \text{ означает, что } x_1 \text{ делится на } x_2) \tag{1-11}$$

$$\underset{R}{\sim} \;:=\; «=» \qquad (x_1 = x_2 \text{ означает, что } x_1 \text{ равен } x_2) \tag{1-12}$$

$$\underset{R}{\sim} \;:=\; «\equiv \pmod n» \qquad (x_1 \equiv x_2 \pmod n \text{ означает}^1\text{, что } (x_1 - x_2) \,\vdots\, n) \tag{1-13}$$

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

$$x \underset{R}{\sim} x \quad \forall\, x \in X\;; \qquad (\textit{рефлексивность}) \tag{1-14}$$

$\forall\, x_1, x_2, x_3 \in X$ одновременное выполнение условий

$$x_1 \underset{R}{\sim} x_2 \quad \text{и} \quad x_2 \underset{R}{\sim} x_3 \qquad (\textit{транзитивность}) \tag{1-15}$$

возможно только при $x_1 \underset{R}{\sim} x_3$;

$$\forall\, x_1, x_2 \in X \quad x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1\,. \qquad (\textit{симметричность}) \tag{1-16}$$

Так, отношения (1-12) и (1-13) являются эквивалентностями, а (1-10) и (1-11) — нет (они несимметричны). Если 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, если на множестве X задано какое-нибудь отношение эквивалентности R, назовём *классом эквивалентности* элемента $x \in X$ множество

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

состоящее из всех элементов, эквивалентных x (в силу симметричности отношения R не важно с какой стороны от знака $\underset{R}{\sim}$ писать x). Если пересечение каких-нибудь двух классов $[x]_R$ и $[y]_R$ не пусто и содержит некоторую точку, R-эквивалентную как x, так и y, то x и y, в силу транзитивности и симметричности отношения R, будут R-эквивалентны между собой, и, по тем же причинам, классы $[x]_R$ и $[y]_R$ будут совпадать. Таким образом, любые два класса эквивалентности или не пересекаются или совпадают, а значит, X разбиваются в дизъюнктное объединение различных классов эквивалентности.

Итак, задание на X какого-нибудь отношения эквивалентности равносильно разбиению X в объединение непересекающихся подмножеств.

1.5.1. Отступление: частично упорядоченные множества. Бинарное отношение $\underset{R}{\sim}$ называется *частичным порядком*, если оно рефлексивно и транзитивно, но (в отличие от эквивалентности) не симметрично, а *антисимметрично*. Последнее свойство определяется так:

$\forall\, x_1, x_2 \in X$ одновременное выполнение условий

$$x_1 \underset{R}{\sim} x_2 \quad \text{и} \quad x_2 \underset{R}{\sim} x_1 \qquad (\textit{антисимметричность}) \tag{1-17}$$

возможно только при $x_1 = x_2$.

[1] обозначение $x_1 \equiv x_2 \pmod n$ читается «x_1 сранимо с x_2 по модулю n»

Из бинарных отношений (1-10)–(1-11) на множестве целых чисел $\mathbb{Z}$ частичными порядками являются первые три, а четвёртое — нет[1]. Множество с заданным на нём отношением частичного порядка называется *частично упорядоченным множеством* (сокр. чум ом).

Упражнение 1.8. Будут ли частичными порядками следующие отношения на множестве минутных делений циферблата механических часов:

а) $x \preccurlyeq y$, если исчисляемый против часовой стрелки угол от x к y меньше $30°$?

б) $x \preccurlyeq y$, если после полудня минутная стрелка укажет на x раньше, чем на y ?

(Ответ можно подглядеть в сноске ([2]).)

Упражнение 1.9. Убедитесь, что единственное бинарное отношение, которое является одновременно эквивалентностью и частичным порядком, — это равенство.

1.5.2. Пример: возрастающие и неубывающие отображения. Пусть $X_m = \{1, 2, \dots, m\}$. Мы будем рассматривать его как упорядоченное множество со стандартным отношением порядка «$\leqslant$». Напомним, что отображение $X_m \xrightarrow{\varphi} X_n$ называется *возрастающим*[3], если $\forall\, x_1, x_2 \in X_m$ из строгого неравенства $x_1 < x_2$ в X_m следует строгое неравенство $\varphi(x_1) < \varphi(x_2)$ в X_n; отображение φ называется *неубывающим*[4], если из нестрогого неравенства $x_1 \leqslant x_2$ следует нестрогое неравенство $\varphi(x_1) \leqslant \varphi(x_2)$. Отметим, что имеется биекция между неубывающими отображениями $X_m \xrightarrow{\varphi} X_n$ и возрастающими отображениями $X_m \xrightarrow{\psi} X_{n+m-1}$. Эта биекция переводит неубывающее отображение $X_m \xrightarrow{\varphi} X_n$ в строго возрастающее отображение $X_m \xrightarrow{\psi} X_{n+m-1}$, заданное формулой $\psi(k) = \varphi(k) + k - 1$ где $k = 1, 2, \dots, m \in X_m$.

1.6. Композиция отображений. Последовательное выполнение двух отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

называется *композицией*. Получающееся в результате отображение $X \longrightarrow Z$, переводящее каждую точку $x \in X$ в точку $g(f(x)) \in Z$, обозначается $g \circ f$ или просто gf.

Упражнение 1.10. Убедитесь, что отображение $X \xrightarrow{g} Y$

а) инъективно $\iff \exists$ отображение $Y \xrightarrow{f} X$, такое что $fg = \mathrm{Id}_X$ (всякое такое f называется *левым обратным* к g);

б) сюрьективно $\iff \exists$ отображение $Y \xrightarrow{h} X$, такое что $gh = \mathrm{Id}_Y$ (всякое такое f называется *правым обратным* к g).

Как и умножение чисел, композиция отображений *ассоциативна*[5]:

$$(fg)h = f(gh) \quad \forall \text{ трёх отображений } X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} T\,. \tag{1-18}$$

Упражнение 1.11. Убедитесь, что обе части равенства (1-18) переводят каждый $x \in X$ в $f(g(h(x))) \in T$.

Однако поверхностная аналогия между числами и отображениями на этом кончается. Например, для отображений может не выполняться равенство $fg = gf$ (*коммутативность*, или *переместительный закон*).

Упражнение 1.12. Рассмотрим на плоскости пару прямых ℓ_1 и ℓ_2, пересекающихся в точке O под острым углом α, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. Равны ли они?

Более того, композиция не всегда определена (нельзя «перемножить» $X \xrightarrow{h} Y$ и $Z \xrightarrow{f} T$, если Y никак не связано с Z), и случается, что gf определено, а fg — нет.

Упражнение 1.13. Придумайте соответствующие контрпримеры.

Отметим, что проблем с неопределённостью не возникает, если $f, g \in \mathrm{End}(X)$ являются эндоморфизмами одного и того же множества X.

[1] скажем, целые числа -12 и 6 не равны, но $-12 \equiv 6 \pmod 9$ и $6 \equiv -12 \pmod 9$

[2] ответ: (б) является, а (а) — нет

[3] или *строго сохраняющим порядок*

[4] или *нестрого сохраняющим порядок*

[5] в начальной школе ассоциативность обычно называют *сочетательным законом*

Ещё одно важное предупреждение: 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 1.14. Придумайте соответствующие контрпримеры и покажите, что импликации

$$fg_1 = fg_2 \Rightarrow g_1 = g_2 \quad \text{и} \quad g_1 f = g_2 f \quad \Rightarrow \quad g_1 = g_2$$

имеют место, когда f обладает, соответственно, *левым* или *правым обратным* отображением (что равносильно инъективности или, соответственно, сюрьективности f, см. упр. 1.10)

1.6.1. Пример: таблица умножения эндоморфизмов двуэлементного множества. Составим таблицу умножения эндоморфизмов множества $\{1, 2\}$. Будем обозначать эндоморфизмы $\{1, 2\} \xrightarrow{f} \{1, 2\}$ словами $w(f) = ((f(1), f(2))$ (как в n° 1.3.1). В этих обозначениях множество $\mathrm{End}(\{1, 2\})$ состоит из четырёх эндоморфизмов $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$ которые перемножаются по правилам:

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

(1-19)

Таблица умножения $\mathrm{End}(\{1, 2\}) \times \mathrm{End}(\{1, 2\}) \xrightarrow{(g,f)\mapsto gf} \mathrm{End}(\{1, 2\})$.

(обратите внимание, 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).

Упражнение 1.15. Для $X = \{1, 2\}$ и $Y = \{1, 2, 3\}$ составьте аналогичные (1-19) таблицы умножения

$$\mathrm{Hom}(X,Y) \times \mathrm{Hom}(Y,X) \xrightarrow{(g,f)\mapsto gf} \mathrm{End}(X)$$
$$\mathrm{Hom}(Y,X) \times \mathrm{Hom}(X,Y) \xrightarrow{(f,g)\mapsto fg} \mathrm{End}(Y)\ .$$

1.7. Обратимость. Если отображение $X \xrightarrow{g} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки, и правило $y \mapsto g^{-1}(y)$ определяет отображение $X \xleftarrow{g^{-1}} Y$, которое называется *обратным* к g. По построению, мы имеем равенства

$$g\circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1}\circ g = \mathrm{Id}_X\ . \tag{1-20}$$

Таким образом, отображение g^{-1} является одновременно и левым и правым обратным к g в смысле упр. 1.10.

1.7.1. ПРЕДЛОЖЕНИЕ. *Следующие условия на отображение $X \xrightarrow{g} Y$ попарно эквивалентны:*
(1) *g взаимно однозначно;*
(2) *существует отображение $X \xleftarrow{g'} Y$, такое что $g\circ g' = \mathrm{Id}_Y$ и $g'\circ g = \mathrm{Id}_X$.*
(3) *g обладает как левым, так и правым обратными отображениями;*
При выполнении этих условий отображение g' из (2) и любые левые и правые обратные к g отображения из (2) совпадают друг с другом и с построенное выше отображением g^{-1}.

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была установлена в формуле (1-20). Импликация (2) $\Rightarrow$ (3) очевидна. Докажем, что из (3) вытекают условия (2) и (1). Пусть $X \xrightarrow{g} Y$ обладает левым обратным $X \xleftarrow{f} Y$ (таким что $f\circ g = \mathrm{Id}_X$) и правым обратным $X \xleftarrow{h} Y$ (таким что $g\circ h = \mathrm{Id}_Y$). Тогда они равны друг другу:

$$f = f\circ \mathrm{Id}_Y = f\circ(g\circ h) = (f\circ g)\circ h = \mathrm{Id}_X\circ h = h\ , \tag{1-21}$$

и условие (2) выполняется для $g' = f = h$. Поскольку $g(g'(y)) = y$ для любого $y \in Y$, прообраз $f^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, для любой точки $x \in g^{-1}(y)$ выполняется равенство $g(x) = y$, а значит, и равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$. Поэтому $f^{-1}(y)$ состоит из единственной точки $g'(y)$. Стало быть, g взаимно однозначно, и g' совпадает с g^{-1}. $\square$