

О множествах и отображениях

В этом разделе собраны некоторые факты о множествах и отображениях, которые будут использоваться в нашем курсе. Я надеюсь, что многие из них знакомы читателю из школы, ну а те, что не знакомы, будут в самое ближайшее время изучены в параллельном нашему курсу теории множеств и топологии. Нет нужды «учить» данный раздел *перед* тем, как браться за курс алгебры. Но к нему стоит выборочно обращаться всякий раз, когда Вы почувствуете себя неуверенно в тех или иных рассуждениях, использующих множества, отображения, отношения или незнакомую Вам комбинаторику.

0.1. Множества. В наши цели не входит построение логически строгой теории множеств. Для понимания этого курса достаточно школьного интуитивного представления о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множеств 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 элементом 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 \emptyset . Если множество X конечно, то мы обозначаем через $|X|$ количество точек в нём.

Множество X называется *подмножеством* множества Y , если каждый его 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. Подмножества, отличные от всего множества, называются *собственными*. В частности, пустое подмножество непустого множества *собственное*. Если надо указать, что X является собственным подмножеством в Y , используется обозначение $X \subsetneq Y$.

Упражнение 0.1. Сколько всего подмножеств (включая пустое и несобственное) имеется у множества, состоящего из n элементов?

Для заданных множеств X, Y их *объединение* $X \cup Y$ состоит из всех элементов, принадлежащих хотя бы одному из множеств X, Y ; *пересечение* $X \cap Y$ состоит из всех элементов, принадлежащих одновременно каждому из множеств X, Y ; *разность* $X \setminus Y$ состоит из всех элементов множества X , которые не содержатся в Y .

Упражнение 0.2. 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 по определению являются всевозможные пары (x, y) с $x \in X, y \in Y$, называется *декартовым (или прямым) произведением* множеств X и Y .

0.2. Отображения. Отображение $f : X \rightarrow Y$ из множества X в множество Y есть правило, однозначно сопоставляющее каждой точке $x \in X$ некоторую точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f . Множество всех таких точек $x \in X$, образ которых равен заданной 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* $f : X \rightarrow Y$ и обозначается

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

Два отображения $f : X \rightarrow Y$ и $g : X \rightarrow Y$ равны, если $f(x) = g(x)$ для всех $x \in X$. Множество всех отображений из множества X в множество Y обозначается $\text{Hom}(X, Y)$.

Отображение $f : X \rightarrow Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\text{im}(f) = Y$, 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 *моморфизмом*), 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 изображаются стрелками $X \hookrightarrow Y$.

УПРАЖНЕНИЕ 0.3. Перечислите все отображения $\{0, 1, 2\} \rightarrow \{0, 1\}$ и $\{0, 1\} \rightarrow \{0, 1, 2\}$. Сколько среди них вложений и сколько наложений?

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

УПРАЖНЕНИЕ 0.4. Из отображений: а) $\mathbb{N} \rightarrow \mathbb{N} : x \mapsto x^2$ б) $\mathbb{Z} \rightarrow \mathbb{Z} : x \mapsto x^2$ в) $\mathbb{Z} \rightarrow \mathbb{Z} : x \mapsto 7x$ г) $\mathbb{Q} \rightarrow \mathbb{Q} : x \mapsto 7x$ выделите все инъекции, все сюръекции и все биекции.

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

УПРАЖНЕНИЕ 0.5 (принцип Дирихле). Покажите, что следующие три условия на множество X равносильны: а) X бесконечно б) существует вложение $X \hookrightarrow X$, не являющееся наложением в) существует наложение $X \twoheadrightarrow X$, не являющееся вложением.

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

УПРАЖНЕНИЕ 0.6. Счётно¹ ли множество $\text{Aut}(\mathbb{N})$?

¹Множество M называется *счётным* если существует биекция $\mathbb{N} \xrightarrow{\sim} M$.

ПРИМЕР 0.1 (ЗАПИСЬ ОТОБРАЖЕНИЙ СЛОВАМИ)

Рассмотрим множества $X = \{1, 2, \dots, n\}$ и $Y = \{1, 2, \dots, m\}$, сопоставим каждому отображению $f : X \rightarrow Y$ последовательность его значений:

$$w(f) \stackrel{\text{def}}{=} (f(x_1), f(x_2), \dots, f(x_n)) \quad (0-1)$$

и будем воспринимать её как n -буквенное слово, написанное при помощи m -буквенного алфавита Y . Так, отображениям $f : \{1, 2\} \rightarrow \{1, 2, 3\}$ и $g : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$, 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

$$w : \text{Hom}(X, Y) \simeq \{\text{слова из } |X| \text{ букв в алфавите } Y\}, \quad f \mapsto w(f). \quad (0-2)$$

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 каждая буква алфавита Y встречается ровно один раз.

ПРЕДЛОЖЕНИЕ 0.1

Если множества X и Y конечны, то $|\text{Hom}(X, Y)| = |Y|^{|X|}$.

Доказательство. Пусть X состоит из n элементов, а Y — из m , как в [прим. 0.1](#) выше. Нас интересует количество всех n -буквенных слов, которые можно написать при помощи алфавита из m букв. Обозначим его через $W_m(n)$ и выпишем все эти слова на m страницах, поместив на i -ю страницу все слова, начинающиеся на i -ю букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Поэтому $W_m(n) = m \cdot W_m(n-1) = m^2 \cdot W_m(n-2) = \dots = m^{n-1} \cdot W_m(1) = m^n$. \square

ЗАМЕЧАНИЕ 0.1. В виду [предл. 0.1](#) множество $\text{Hom}(X, Y)$ всех отображений $X \rightarrow Y$ часто обозначают Y^X . В доказательстве [предл. 0.1](#) мы молчаливо предполагали, что оба множества непусты. Если $X = \emptyset$, то для любого множества Y множество $\text{Hom}(\emptyset, Y)$ по определению состоит из единственного элемента — вложения \emptyset в Y в качестве пустого подмножества или, что то же самое, пустого слова в алфавите Y . В этом случае [предл. 0.1](#) остаётся в силе: $|\text{Hom}(\emptyset, Y)| = 1 = |Y|^0$. В частности, $\text{Hom}(\emptyset, \emptyset)$ тоже состоит из одного элемента¹ — тождественного автоморфизма Id_\emptyset . Если $Y = \emptyset$, а $X \neq \emptyset$, то $\text{Hom}(X, \emptyset) = \emptyset$, что тоже согласуется с [предл. 0.1](#), ибо $0^{|X|} = 0$ при $|X| > 0$.

ПРЕДЛОЖЕНИЕ 0.2

Если $|X| = n$, то $|\text{Aut}(X)| \stackrel{\text{def}}{=} n \cdot (n-1) \cdot \dots \cdot 1$.

Доказательство. Пусть $X = \{x_1, \dots, x_n\}$. Биекции $X \simeq X$ записываются n -буквенными словами в n -буквенном алфавите x_1, \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

¹Т. е. 0^0 в этом контексте оказывается равным 1.

страницах, поместив на i -тую страницу все слова, начинающиеся на x_i . Тогда на каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \dots = n \cdot (n-1) \cdot \dots \cdot 2 \cdot V(1) = n!$. \square

ЗАМЕЧАНИЕ 0.2. Число $n! = n \cdot (n-1) \cdot \dots \cdot 1$ называется n -факториал. Так как множество $\text{Aut}(\emptyset)$ состоит из одного элемента Id_{\emptyset} , мы полагаем $0! \stackrel{\text{def}}{=} 1$.

0.3. Слои отображений. Задание отображения $f : X \rightarrow Y$ равносильно указанию подмножества $\text{im}(f) \subset Y$ и разбиению множества X в дизъюнктное объединение непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \text{im}(f)$:

$$X = \bigsqcup_{y \in \text{im}(f)} f^{-1}(y). \quad (0-3)$$

Такой взгляд на отображения часто оказывается полезным при подсчёте количества элементов в том или ином множестве. Например, когда все непустые слои отображения $f : X \rightarrow Y$ 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 соотношением

$$|X| = m \cdot |\text{im } f|, \quad (0-4)$$

которое при всей своей простоте имеет много разнообразных применений.

ПРИМЕР 0.2 (МУЛЬТИНОМИАЛЬНЫЕ КОЭФФИЦИЕНТЫ)

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

$$(a_1 + \dots + a_m)^n = \sum_{\substack{k_1 + \dots + k_m = n \\ \forall i \ 0 \leq k_i \leq n}} \binom{n}{k_1 \dots k_m} \cdot a_1^{k_1} \dots a_m^{k_m}, \quad (0-5)$$

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

$$(a_1 + \dots + a_m)(a_1 + \dots + a_m) \dots (a_1 + \dots + a_m)$$

заключается в 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 $a_1^{k_1} a_2^{k_2} \dots a_m^{k_m}$, суть слова, состоящие ровно из k_1 букв a_1 , k_2 букв a_2 , \dots , k_m букв a_m . Количество таких слов легко подсчитать по формуле (0-4). 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 получим $n = k_1 + \dots + k_m$ попарно разных букв:

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

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 $f: X \rightarrow Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1! \cdot k_2! \cdot \dots \cdot k_m!$ 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 (0-4)

$$\binom{n}{k_1 \dots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}. \quad (0-6)$$

Тем самым, разложение (0-5) имеет вид

$$(a_1 + \dots + a_m)^n = \sum_{\substack{k_1 + \dots + k_m = n \\ \forall i \ 0 \leq k_i \leq n}} \frac{n! \cdot a_1^{k_1} \dots a_m^{k_m}}{k_1! \cdot \dots \cdot k_m!}. \quad (0-7)$$

УПРАЖНЕНИЕ 0.7. Сколько всего слагаемых в правой части формулы (0-7)?

В частности, при $m = 2$ мы получаем известную формулу для раскрытия бинома с натуральным показателем¹:

$$(a + b)^n = \sum_{k=0}^n \frac{n!}{k!(n-k)!} a^k b^{n-k}. \quad (0-8)$$

При $m = 2$ мультиномиальный коэффициент $\binom{n}{k, n-k}$ принято обозначать $\binom{n}{k}$ или C_n^k и называть k -тым биномиальным коэффициентом степени n или числом сочетаний из n по k . Он равен

$$\binom{n}{k} = C_n^k = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k \cdot (k-1) \cdot \dots \cdot 1}$$

(сверху и снизу стоит по k последовательно убывающих сомножителей).

ПРИМЕР 0.3 (диаграммы Юнга)

Разбиение конечного множества $X = \{1, 2, \dots, n\}$ в объединение непересекающихся подмножеств

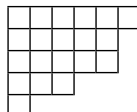
$$X = X_1 \sqcup X_2 \sqcup \dots \sqcup X_k \quad (0-9)$$

¹Это частный случай формулы Ньютона, которую мы обсудим в полной общности, когда будем заниматься степенными рядами.

можно 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

$$\lambda = (\lambda_1, \dots, \lambda_k), \quad \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k,$$

которая называется *формой разбиения (0-9)*. Форму разбиения удобно изображать *диаграммой Юнга* — картинкой вида


(0-10)

составленной из выровненных по левому краю горизонтальных клетчатых полосок, занумерованных сверху вниз, так что в i -й сверху полоске λ_i клеток. Общее число клеток в диаграмме λ называется её *весом* и обозначается $|\lambda|$, а количество строк называется *длиной* и обозначается $\ell(\lambda)$. Так, диаграмма Юнга (0-10) отвечает разбиению формы $\lambda = (6, 5, 5, 3, 1)$, имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 0.8. Подсчитайте количество всех диаграмм Юнга, уместяющихся 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, всякая диаграмма λ веса n имеет $n!$ различных заполнений заданным n -элементным множеством X .

Объединяя элементы, стоящие в i -й строке диаграммы в одно подмножество X_i , мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств X_1, \dots, X_k . Поскольку любое разбиение (0-9) заданной формы λ можно получить таким образом, возникает 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 $m_i = m_i(\lambda)$ число строк длины¹ i в диаграмме λ , то перестановок первого типа будет $\prod \lambda_i! = \prod_{i=1}^n (i!)^{m_i}$ штук, а второго типа — $\prod_{i=1}^n m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod_{i=1}^n (i!)^{m_i} m_i!$ элементов. Из формулы (0-4) вытекает

Предложение 0.3

Число разбиений n -элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, \dots , m_n n -элементных подмножеств равно

$$\frac{n!}{\prod_{i=1}^n m_i! \cdot (i!)^{m_i}}. \quad (0-11)$$

¹ Отметим, что многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \dots + nm_n$.

0.4. Классы эквивалентности. Альтернативный способ разбить заданное множество X в дизъюнктивное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так. Назовём *бинарным отношением* на множестве X любое 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 $x_1 \underset{R}{\sim} x_2$.

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

$$\text{равенство} \quad x_1 \underset{R}{\sim} x_2 \stackrel{\text{def}}{\iff} x_1 = x_2 \quad (0-12)$$

$$\text{неравенство} \quad x_1 \underset{R}{\sim} x_2 \stackrel{\text{def}}{\iff} x_1 \leq x_2 \quad (0-13)$$

$$\text{делимость} \quad x_1 \underset{R}{\sim} x_2 \stackrel{\text{def}}{\iff} x_1 \mid x_2 \quad (0-14)$$

$$\text{сравнимость по модулю } n \quad x_1 \underset{R}{\sim} x_2 \stackrel{\text{def}}{\iff} x_1 \equiv x_2 \pmod{n} \quad (0-15)$$

(последнее условие $x_1 \equiv x_2 \pmod{n}$ читается как « x_1 сравнимо с x_2 по модулю n » и по определению означает, что $x_1 - x_2$ делится на n).

ОПРЕДЕЛЕНИЕ 0.1

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

$$\text{рефлексивность} : \forall x \in X \quad x \underset{R}{\sim} x$$

$$\text{транзитивность} : \forall x_1, x_2, x_3 \in X \text{ из } x_1 \underset{R}{\sim} x_2 \text{ и } x_2 \underset{R}{\sim} x_3 \text{ вытекает } x_1 \underset{R}{\sim} x_3$$

$$\text{симметричность} : \forall x_1, x_2 \in X \quad x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1.$$

Среди бинарных отношений (0-12) – (0-15) первое и последнее являются эквивалентностями, а (0-13) и (0-14) не являются (они не симметричны).

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $x_1 \underset{R}{\sim} x_2$, 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 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). Любые 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 \sim_R 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 эквивалентности R . Сюръекция

$$f: X \rightarrow X/R, \quad x \mapsto [x]_R, \quad (0-16)$$

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

ПРИМЕР 0.4 (КЛАССЫ ВЫЧЕТОВ)

Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел \mathbb{Z} по отношению сравнимости по модулю n из (0-15) 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

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z - x) : n\} \quad (0-17)$$

называется *классом вычетов по модулю n* . Отображение факторизации

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

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

$$[12^{100}]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = [(-1)^{100}]_{13} = [1]_{13}. \quad (0-18)$$

УПРАЖНЕНИЕ 0.9. 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

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \quad (0-19)$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \quad (0-20)$$

корректно определяют на множестве $\mathbb{Z}/(n)$ операции сложения и умножения¹.

¹Именно такое умножение $[12]^{100} = \underbrace{[12] \cdot [12] \cdot \dots \cdot [12]}_{100} = [12^{100}]$ было использовано в (0-18).

0.4.1. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap_\nu R_\nu \subset X \times X$ 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 $(x, y) \Leftrightarrow (y, x)$ и вместе с каждой парой точек вида $(x, y), (y, z)$ содержит также и точку (x, z) , то этими свойствами обладает и пересечение $\bigcap_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества $R \subset X \times X$ существует *наименьшее по включению* отношение эквивалентности \bar{R} , содержащее R , а именно, пересечение всех содержащих R отношений эквивалентности. Отношение \bar{R} называется эквивалентностью, *порождённой* отношением R .

УПРАЖНЕНИЕ 0.10. Проверьте, что $(x, y) \in \bar{R}$ если и только если в X существует такая конечная последовательность точек $x = z_0, z_1, z_2, \dots, z_n = y$, что $(x_{i-1}, x_i) \in R$ или $(x_i, x_{i-1}) \in R$ при каждом $i = 1, 2, \dots, n$.

К сожалению, по данному подмножеству $R \subset X \times X$ не всегда легко судить о том, как устроена порождённая им эквивалентность \bar{R} . Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу может быть не просто.

ПРИМЕР 0.5 (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) , где $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus 0$, по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \quad \text{с произвольными } c \in \mathbb{Z} \setminus \{0\}. \quad (0-21)$$

Отношения (0-21) 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 $(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$ самый левый и самый правый элементы могут не отождествляться напрямую по правилу (0-21), как, например, $3/6$ и $5/10$. Поэтому эквивалентность, порождённая отождествлениями (0-21), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при } a_1 b_2 = a_2 b_1. \quad (0-22)$$

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

УПРАЖНЕНИЕ 0.11. Проверьте, что набор отношений (0-22) рефлексивен, симметричен и транзитивен.

Тем самым, он является минимальным отношением эквивалентности, содержащим все отождествления (0-21). Отметим, что если в отношениях (0-21) разрешить нулевые c , то все пары (a, b) окажутся эквивалентны паре $(0, 0)$.

0.5. Композиции отображений. Отображение $X \rightarrow Z$, получающееся в результате последовательного выполнения двух отображений $f: X \rightarrow Y$ и $g: Y \rightarrow Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf . Таким образом, композиция gf определена если и только если образ f содержится в множестве, на котором определено отображение g , и $gf: X \rightarrow Z$, $x \mapsto g(f(x))$.

Хотя композицию и принято записывать точно так же, как умножение чисел, единственным общим свойством этих операций является их *ассоциативность* или *сочетательный закон*: композиция трёх последовательных отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T,$$

как и произведение трёх чисел, не зависит от того, в каком порядке перемножаются последовательные пары элементов, т. е. $(hg)f = h(gf)$, если хотя бы одна из двух частей этого равенства определена. Действительно, в этом случае вторая часть тоже определена, и обе части действуют на каждую точку $x \in X$ по правилу $x \mapsto h(g(f(x)))$.

В остальном алгебраические свойства композиции весьма далеки от привычных свойств умножения чисел. Если композиция fg определена, то противоположная композиция gf часто бывает не определена. Даже если $f, g: X \rightarrow X$ являются эндоморфизмами одного и того же множества X , так что обе композиции fg и gf определены, равенство $fg = gf$ может не выполняться.

Упражнение 0.12. 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 $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Общие множители тоже бывает нельзя сокращать, т. е. ни равенство $fg = fh$, ни равенство $gf = hf$, вообще говоря, не влекут равенства $g = h$.

Пример 0.6 (эндоморфизмы двухэлементного множества)

Двухэлементное множество $X = \{1, 2\}$ имеет ровно четыре эндоморфизма. Если кодировать отображение $f: X \rightarrow X$ двубуквенным словом $(f(1), f(2))$, как в [прим. 0.1](#) на стр. 5, то эти четыре эндоморфизма запишутся словами $(1, 1)$, $(1, 2) = \text{Id}_X$, $(2, 1)$ и $(2, 2)$. Все композиции между ними определены, и таблица композиций gf имеет вид:

$g \setminus f$	$(1, 1)$	$(1, 2)$	$(2, 1)$	$(2, 2)$	
$(1, 1)$	$(1, 1)$	$(1, 1)$	$(1, 1)$	$(1, 1)$	(0-23)
$(1, 2)$	$(1, 1)$	$(1, 2)$	$(2, 1)$	$(2, 2)$	
$(2, 1)$	$(2, 2)$	$(2, 1)$	$(1, 2)$	$(1, 1)$	
$(2, 2)$	$(2, 2)$	$(2, 2)$	$(2, 2)$	$(2, 2)$	

Обратите внимание на то, что $(2, 2) \circ (1, 1) \neq (1, 1) \circ (2, 2)$ и что $(1, 1) \circ (1, 2) = (1, 1) \circ (2, 1)$, хотя $(1, 2) \neq (2, 1)$, и $(1, 1) \circ (2, 2) = (2, 1) \circ (2, 2)$, хотя $(1, 1) \neq (2, 1)$.

Лемма 0.1 (левые обратные отображения)

Если $X \neq \emptyset$, то следующие условия на отображение $f: X \rightarrow Y$ эквивалентны:

- 1) f инъективно
- 2) существует такое отображение $g : Y \rightarrow X$, что $gf = \text{Id}_X$
- 3) для любых отображений $g_1, g_2 : Z \rightarrow X$ из равенства $fg_1 = fg_2$ вытекает равенство $g_1 = g_2$.

Доказательство. Импликация (1) \Rightarrow (2): для точек $y = f(x) \in \text{im } f$ положим $g(y) = x$, а в точках $y \notin \text{im } f$ зададим g как угодно¹. Импликация (2) \Rightarrow (3): если $fg_1 = fg_2$, то умножая обе части слева на любое такое отображение $g : Y \rightarrow X$, что $gf = \text{Id}_X$, получаем $g_1 = g_2$. Импликация (3) \Rightarrow (1) доказывается от противного. Пусть $x_1 \neq x_2$, но $f(x_1) = f(x_2)$. Положим $g_1 = \text{Id}_X$, и пусть $g_2 : X \rightarrow X$ переставляет между собою точки x_1, x_2 , а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$. \square

ОПРЕДЕЛЕНИЕ 0.2

Отображение $f : X \rightarrow Y$, удовлетворяющее лем. 0.1, называется *обратимым слева*, и всякое такое отображение $g : Y \rightarrow X$, что $gf = \text{Id}_X$, называется *левым обратным к f* или *ретракцией Y на $f(X)$* .

УПРАЖНЕНИЕ 0.13. В условиях лем. 0.1 убедитесь, что вложение f тогда и только тогда имеет несколько различных левых обратных, когда оно не сюръективно.

0.5.1. Правое обратное отображение и аксиома выбора. Стремление к гармонии вызывает желание иметь «правую» версию лем. 0.1 — хочется, чтобы следующие три свойства отображения $f : X \rightarrow Y$ тоже были эквивалентны:

- 1) f сюръективно
- 2) существует такое отображение $g : Y \rightarrow X$, что $fg = \text{Id}_Y$
- 3) для любых отображений $g_1, g_2 : Y \rightarrow X$ из равенства $g_1f = g_2f$ вытекает равенство $g_1 = g_2$.

Отображение f , удовлетворяющее свойству (2), называется *обратимым справа*, а такое отображение $g : Y \rightarrow X$, что $fg = \text{Id}_Y$, называется *правым обратным к f* или *сечением эпиморфизма f* . Второе название связано с тем, что отображение g , удовлетворяющее свойству (2), переводит каждую точку $y \in Y$ в точку $g(y) \in f^{-1}(y)$, лежащую в слое отображения f над точкой y .

В строгой теории множеств, углубления в которую мы пытаемся избежать, импликация (1) \Rightarrow (2) постулируется в качестве одной из аксиом. Эта аксиома называется *аксиомой выбора* и утверждает, что в каждом слое любого сюръективного отображения можно выбрать по элементу².

¹Например, отобразим их все в одну и ту же произвольно выбранную точку $x \in X$.

²Иными словами, если имеется множество попарно непересекающихся множеств, то в каждом из них можно выбрать по элементу.

Доказательство импликации (2) \Rightarrow (3) полностью симметрично доказательству аналогичной импликации из лем. 0.1: применяя отображения, стоящие в обеих частях равенства $g_1 f = g_2 f$, вслед за таким отображением $g : Y \rightarrow X$, что $f g = \text{Id}_Y$, получаем равенство $g_1 = g_2$.

Импликация (3) \Rightarrow (1), как и в лем. 0.1, доказывается от противного: если $y \notin \text{im } f$, то свойство (3) не выполняется для отображения $g_1 = \text{Id}_Y$ и любого отображения $g_2 : Y \rightarrow Y$, переводящего точку y в какую-нибудь точку из $\text{im } f$ и оставляющего на месте все остальные точки.

Таким образом, перечисленные выше свойства (1) – (3) действительно эквивалентны друг другу, если включить аксиому выбора в список свойств, определяющих множества.

0.5.2. Обратимые отображения. Если отображение $g : X \rightarrow Y$ 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 $g^{-1} : Y \rightarrow X$, которое является одновременно и левым, и правым обратным к g в смысле опр. 0.2 и н° 0.5.1, т. е.

$$g \circ g^{-1} = \text{Id}_Y \quad \text{и} \quad g^{-1} \circ g = \text{Id}_X \quad (0-24)$$

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

Предложение 0.4

Следующие условия на отображение $g : X \rightarrow Y$ эквивалентны друг другу:

- 1) g взаимно однозначно
- 2) существует такое отображение $g' : Y \rightarrow X$, что¹ $g \circ g' = \text{Id}_Y$ и $g' \circ g = \text{Id}_X$
- 3) g обладает левым и правым обратными отображениями².

При выполнении этих условий все левые и правые обратные к g отображения равны друг другу и отображению g^{-1} , описанному перед формулировкой предложения.

Доказательство. Импликация (1) \Rightarrow (2) уже была установлена. Очевидно, что (2) \Rightarrow (3). Докажем, что (3) \Rightarrow (2). Если у отображения $g : X \rightarrow Y$ есть левое обратное $f : Y \rightarrow X$ и правое обратное $h : Y \rightarrow X$, то $f = f \circ \text{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \text{Id}_X \circ h = h$ и условие (2) выполнено для $g' = f = h$. Остаётся показать, что (2) \Rightarrow (1), и $g' = g^{-1}$. Так как $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, поскольку для всех $x \in g^{-1}(y)$ выполнено равенство $x = \text{Id}_X(x) = g'(g(x)) = g'(y)$, прообраз $g^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, и $g' = g^{-1}$. \square

¹Т. е. g' двусторонне обратен к g .

²Обратите внимание, что совпадения левого обратного отображения с правым обратным отображением не требуется.

0.6. 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 каждым 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 $\text{Id}_X = g^{-1}g$ 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 называется *подгруппой* группы G .

ПРИМЕР 0.7 (ГРУППЫ ПЕРЕСТАНОВОК)

Множество $\text{Aut}(X)$ всех взаимно однозначных отображений $X \rightarrow X$ 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 $\{1, 2, \dots, n\}$ обозначается S_n и называется n -й *симметрической группой*. Согласно предл. 0.2 на стр. 5 порядок $|S_n| = n!$. Перестановки

$$\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

принято записывать строчками $\sigma = (\sigma_1, \dots, \sigma_n)$ их значений $\sigma_i \stackrel{\text{def}}{=} \sigma(i)$, как в прим. 0.1 на стр. 5. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ представляют собою отображения

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

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

УПРАЖНЕНИЕ 0.14. Составьте таблицу умножения шести элементов группы S_3 , аналогичную таблице (0-23) на стр. 12.

ПРИМЕР 0.8 (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 $n \geq 2$ повороты на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка n* .

0.7. Частично упорядоченные множества. Бинарное отношение¹ $x \leq y$ на множестве Z называется *частичным порядком*, если оно рефлексивно и транзитивно², но в отличие от эквивалентности не симметрично, а *кососимметрично*, т. е. из $x \leq y$ и $y \leq x$ вытекает равенство $x = y$. Если на множестве задан частичный порядок, мы пишем

¹См. п. 0.4 на стр. 9.

²Ср. с опр. 0.1 на стр. 9.

$x < y$, когда $x \leq y$ и $x \neq y$. Частичный порядок на множестве Z называется *линейным* (или просто *порядком*), если любые два элемента сравнимы, т. е. для всех $x, y \in Z$ выполняется одно из трёх альтернативных условий: или $x < y$, или $x = y$, или $y < x$. Например, обычное неравенство между числами является линейным порядком на множестве натуральных чисел \mathbb{N} , тогда как отношение делимости $n \mid m$, означающее, что n делит m , задаёт на \mathbb{N} частичный порядок, который не является линейным. Другим важным примером частичного, но не линейного порядка является отношение включения $X \subseteq Y$ на множестве $\mathcal{S}(M)$ всех подмножеств заданного множества M .

Упражнение 0.15 (предпорядок). *Предпорядком* на множестве Z называется любое рефлексивное транзитивное бинарное отношение $x < y$. Убедитесь, что для каждого предпорядка бинарное отношение $x \sim y$, означающее, что одновременно $x < y$ и $y < x$, является отношением эквивалентности, и на факторе Z/\sim корректно определено¹ бинарное отношение $[x] \leq [y]$, означающее, что $x \lesssim y$, которое является частичным порядком. Продумайте, как всё это работает для отношения делимости $n \mid m$ на множестве целых чисел \mathbb{Z} .

Множество P с зафиксированным на нём частичным порядком называется *частично упорядоченным множеством*, сокращённо — *чумом*. Если порядок линейный, чум P называется *линейно упорядоченным*. Всякое подмножество X любого чума P также является чумом по отношению к частичному порядку, имеющемуся на P . Если этот индуцированный с P порядок на X оказывается линейным, подмножество $X \subset P$ называют *цепью* в чуме P . Элементы x, y чума P называются *сравнимыми*, если $x \leq y$ или $y \leq x$. Если же ни одно из этих условий не выполняется, то x и y называются *несравнимыми*. Несравнимые элементы автоматически различны. Частичный порядок линейен тогда и только тогда, когда любые два элемента сравнимы.

Отображение $f: M \rightarrow N$ между чумами M, N называется *сохраняющим порядок*² или *морфизмом чумов*, если $f(x) \leq f(y)$ для всех $x \leq y$. Два чума M, N называются *изоморфными*, если имеется сохраняющая порядок биекция $M \simeq N$. В таком случае мы пишем $M \simeq N$. Отображение f называется *строго возрастающим*, если $f(x) < f(y)$ для всех $x < y$. Всякое сохраняющее порядок вложение является строго возрастающим. Обратное справедливо для возрастающих отображений из линейного упорядоченного множества, однако неверно в общем случае.

Элемент y чума P называется *верхней гранью* подмножества $X \subset P$, если $x \leq y$ для всех $x \in X$. Если при этом $y \notin X$, то верхняя грань y называется *внешней*. В таком случае для всех $x \in X$ выполнено строгое неравенство $x < y$.

Элемент $m^* \in X$ называется *максимальным* в подмножестве $X \subset P$, если для $x \in X$ неравенство $m^* \leq x$ выполняется только при $x = m^*$. Заметьте, что максимальный элемент не обязан быть сравним со всеми элементами $x \in X$ и, тем самым, может не являться верхней гранью для X . Частично упорядоченное множество может иметь несколько различных максимальных элементов или не иметь их вовсе, как, например, чум \mathbb{N} по отношению к делимости или к обычному неравенству между числами. Линей-

¹Т. е. выполнение или невыполнение условия $x \lesssim y$ не зависит от выбора представителей x и y в классах $[x]$ и $[y]$.

²А также *неубывающим* или *нестрого возрастающим*.

но упорядоченный чум имеет не более одного максимального элемента, и если такой элемент существует, то он является верхней гранью.

Симметричным образом, элемент $m_* \in X$ называется *минимальным* в X , если для $x \in X$ неравенство $m_* \geq x$ выполняется только при $x = m_*$. Аналогично определяются и нижние грани, и всё сказанное выше о максимальных элементах и верхних гранях в равной степени относится и к минимальным элементам и нижним граням.

0.8. Вполне упорядоченные множества. Линейно упорядоченное множество W называется *вполне упорядоченным*, если каждое непустое подмножество $S \subset W$ содержит такой элемент $s_* \in S$, что $s_* \leq s$ для всех $s \in S$. Этот элемент автоматически единствен и называется *начальным элементом* подмножества S . Например, множество натуральных чисел \mathbb{N} со стандартным отношением неравенства между числами вполне упорядочено, как и любое дизъюнктивное объединение вида $\mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \dots$, в котором все элементы каждой копии множества \mathbb{N} полагаются строго большими всех элементов всех предыдущих копий. Пустое множество тоже вполне упорядочено. Напротив, множество \mathbb{Q} со стандартным отношением неравенства между числами не является вполне упорядоченным.

Вполне упорядоченные множества замечательны тем, что их элементы можно рекурсивно перебрать точно также, как и элементы множества \mathbb{N} . А именно, пусть некоторое утверждение $\Phi(w)$ зависит от элемента w вполне упорядоченного множества W . Если $\Phi(w)$ истинно для начального элемента w_* множества W , и для каждого $w \in W$ истинность утверждения $\Phi(x)$ при всех $x < w$ влечёт за собою истинность утверждения $\Phi(w)$, то $\Phi(w)$ истинно для всех $w \in W$.

УПРАЖНЕНИЕ 0.16. Убедитесь в этом.

Такой способ доказательства утверждения $\Phi(w)$ для всех $w \in W$ называется *трансфинитной индукцией*. Используемые для индуктивного перехода подмножества, состоящие из всех элементов, предшествующих данному элементу w , называются *начальными интервалами* частично упорядоченного множества W и обозначаются

$$[w) \stackrel{\text{def}}{=} \{x \in W \mid x < w\}.$$

Элемент $w \in W$ называется *точной верхней гранью* начального интервала $[w) \subset W$ и однозначно восстанавливается по интервалу $[w)$ как начальный элемент множества $W \setminus [w)$. Отметим, что начальный элемент $w_* \in W$ является точной верхней гранью пустого начального интервала $[w_*) = \emptyset$.

УПРАЖНЕНИЕ 0.17. Покажите, что собственное подмножество $I \subsetneq W$ тогда и только тогда является начальным интервалом вполне упорядоченного множества W , когда $[x) \subset I$ для каждого $x \in I$, и в этом случае точная верхняя грань интервала I однозначно восстанавливается по I как начальный элемент дополнения $W \setminus I$.

Между вполне упорядоченными множествами имеется отношение порядка $U \leq W$, означающее, что U можно биективно и с сохранением порядка отобразить на W или на какой-нибудь начальный интервал $[w) \subset W$. Если при этом U и W не изоморфны, мы пишем $U < W$. Хорошим упражнением на трансфинитную индукцию является

УПРАЖНЕНИЕ 0.18. Убедитесь, что для любой пары вполне упорядоченных множеств U, W выполнено ровно одно из соотношений: или $U < W$, или $U \simeq W$, или $W < U$.

Классы изоморфных вполне упорядоченных множеств называют *ординалами*. Множество \mathbb{N} со стандартным порядком можно воспринимать как множество всех конечных ординалов. Все остальные ординалы, включая \mathbb{N} , называются *трансфинитными*.

0.9. Лемма Цорна. Рассмотрим произвольное частично упорядоченное множество P и обозначим через $\mathcal{W}(P)$ множество всех подмножеств $W \subset P$, которые вполне упорядочены имеющимся на P отношением $x \leq y$. Множество $\mathcal{W}(P)$ непусто и содержит пустое подмножество $\emptyset \subset P$, а также все конечные цепи¹ $C \subset P$, в частности, все элементы множества P .

ЛЕММА 0.2

Не существует такого отображения $\varrho : \mathcal{W}(P) \rightarrow P$, что $\varrho(W) > w$ для всех $W \in \mathcal{W}(P)$ и $w \in W$.

Доказательство. Пусть такое отображение ϱ существует. Назовём вполне упорядоченное подмножество $W \subset P$ рекурсивным, если $\varrho(\{w\}) = w$ для всех $w \in W$. Например, подмножество

$$\left\{ \varrho(\emptyset), \varrho(\{\varrho(\emptyset)\}), \varrho(\{\varrho(\emptyset), \varrho(\{\varrho(\emptyset)\})\}), \dots \right\}$$

рекурсивно и его можно расширять дальше вправо, пока P не исчерпается, что противоречит наложенному на ϱ условию. Уточним сказанное. Если два рекурсивных вполне упорядоченных подмножества имеют общий начальный элемент, то либо они совпадают, либо одно из них является начальным интервалом другого.

УПРАЖНЕНИЕ 0.19. Докажите это.

Обозначим через $U \subset P$ объединение всех рекурсивных вполне упорядоченных подмножеств в P с начальным элементом $\varrho(\emptyset)$.

УПРАЖНЕНИЕ 0.20. Убедитесь, что подмножество $U \subset P$ вполне упорядочено и рекурсивно.

Поскольку элемент $\varrho(U)$ строго больше всех элементов из U , он не лежит в U . С другой стороны, множество $W = U \cup \{\varrho(U)\}$ вполне упорядочено, рекурсивно, и его начальным элементом является $\varrho(\emptyset)$. Следовательно, $W \subset U$, откуда $\varrho(U) \in U$. Противоречие. \square

ПРЕДЛОЖЕНИЕ 0.5

Если каждое вполне упорядоченное подмножество чума P имеет верхнюю грань², то в P есть максимальный элемент³ (возможно не единственный).

Доказательство. Если максимального элемента нет, то для любого $p \in P$ имеется такой элемент $p' \in P$, что $p < p'$. Тогда для каждого вполне упорядоченного подмножества $W \subset P$ найдётся такой элемент $w^* \in P$, что $w < w^*$ для всех $w \in W$. Сопоставляя каждому $W \in \mathcal{W}$ один⁴ из таких элементов w^* , мы получаем отображение $\varrho : \mathcal{W} \rightarrow P$,

¹Т. е. конечные линейно упорядоченные подмножества.

²Т. е. для любого вполне упорядоченного $W \subset P$ найдётся такой $p \in P$, что $w \leq p$ для всех $w \in W$.

³Т. е. такой $p^* \in P$, что неравенство $p^* \leq x$ выполняется в P только для $x = p^*$, см. последние два абзаца перед н° 0.8 на стр. 17.

⁴Для этого придётся воспользоваться аксиомой выбора из н° 0.5.1 на стр. 13.

которого не может быть по лем. 0.2. □

ОПРЕДЕЛЕНИЕ 0.3 (полные чумы)

Частично упорядоченное множество называется *полным*, если каждая его цепь имеет верхнюю грань.

СЛЕДСТВИЕ 0.1 (ЛЕММА ЦОРНА)

В каждом полном чуме есть максимальный элемент (возможно не единственный). □

УПРАЖНЕНИЕ 0.21 (ЛЕММА БУРБАКИ – ВИТТА О НЕПОДВИЖНОЙ ТОЧКЕ). Пусть отображение из полного чума в себя $f : P \rightarrow P$ таково, что $f(x) \geq x$ для всех $x \in P$. Покажите, что существует такое $p \in P$, что $f(p) = p$.

УПРАЖНЕНИЕ 0.22 (ТЕОРЕМА ЦЕРМЕЛЛО). Докажите, что каждое множество можно вполне упорядочить.

УПРАЖНЕНИЕ 0.23 (ТЕОРЕМА ХАУСДОРФА О МАКСИМАЛЬНОЙ ЦЕПИ). Докажите, что в любом чуме каждая цепь содержится в некоторой максимальной по включению цепи.

Ответы и указания к некоторым упражнениям

Упр. о.1. Ответ: 2^n .

Упр. о.2. Ответ на второй вопрос — нет. Пусть $X = \{1, 2\}$, $Y = \{2\}$. Все их парные пересечения и объединения суть $X \cap Y = Y \cap Y = Y \cup Y = Y$ и $X \cup Y = X \cup X = X \cap X = X$, и любая формула, составленная из X, Y, \cap, \cup , даст на выходе или $X = \{1, 2\}$, или $Y = \{2\}$, тогда как $X \setminus Y = \{1\}$.

Упр. о.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. о.5. Если X конечно, то инъективное или сюръективное отображение $X \rightarrow X$ автоматически биективно. Если X бесконечно, то в X есть подмножество, изоморфное \mathbb{N} . Инъекция $\mathbb{N} \hookrightarrow \mathbb{N}$, $n \mapsto (n + 1)$, и сюръекция $\mathbb{N} \twoheadrightarrow \mathbb{N}$, $n \mapsto \max(1, (n - 1))$, обе не биективны и продолжаются до точно таких же отображений $X \rightarrow X$ тождественным действием на $X \setminus \mathbb{N}$.

Упр. о.6. Ответ: нет. Воспользуйтесь «диагональным трюком» Кантора: пусть все биекции $\mathbb{N} \rightarrow \mathbb{N}$ занумерованы натуральными числами; глядя на этот список, постройте биекцию, которая при каждом $k = 1, 2, 3, \dots$ отображает некоторое число $n_k \in \mathbb{N}$ не туда, куда его отображает k -тая биекция из списка.

Упр. о.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, \dots, 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. о.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. о.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. о.10. Положим $x \sim y$, если существует конечная последовательность точек

$$x = z_0, z_1, z_2, \dots, z_n = y$$

как в условии задачи. Проверьте, что это отношение эквивалентности и что оно содержится в любой эквивалентности $S \subset X \times X$, содержащей R .

Упр. о.11. 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. о.12. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leq \pi/2$, то отражение относительно ℓ_1 , за которым следует отражение относительно ℓ_2 , это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно пересекающихся прямых коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. о.14. Таблица композиций gf в симметрической группе S_3 :

$g \setminus f$	(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)

Упр. о.15. Отношение $n \mid m$ на множестве \mathbb{Z} не кососимметрично: $n \mid m$ и $m \mid n$ если и только если $m = \pm n$. Фактор множества \mathbb{Z} по этому отношению эквивалентности можно отождествить с множеством $\mathbb{Z}_{\geq 0}$ неотрицательных целых чисел, на котором отношение $n \mid m$ является частичным порядком (обратите внимание, что нуль является нижней гранью этого множества, т. е. делит все элементы.)

Упр. о.16. Пусть множество $S \subset W$ состоит из всех таких элементов $z \in W$, что утверждение $\Phi(z)$ ложно. Если $S \neq \emptyset$, то в нём есть начальный элемент $s_* \in S$. Поскольку утверждение $\Phi(w)$ истинно для всех $w < s_*$, утверждение $\Psi(s_*)$ тоже истинно, т. е. $s_* \notin S$. Противоречие.

Упр. о.17. Обозначим через x_I начальный элемент дополнения $W \setminus I$. Начальный интервал $[x_I) \subset W$ является объединением начальных интервалов $[y) \subset W$ по всем $y < x_I$. Так как I содержит все интервалы $[y)$ с $y < x_I$, мы заключаем, что $I \supseteq [x_I)$, откуда $I = [x_I)$.

Упр. о.18. Пусть соотношение $U \geq W$ не выполняется. Покажем, что любой начальный отрезок $[u) \subset U$ изоморфен некоторому начальному отрезку $[w) \subset W$, где $w = w(u)$ однозначно восстанавливается по u . Это верно для пустого начального отрезка $\emptyset = [u_*)$, где $u_* \in U$ — минимальный элемент. Пусть это верно для всех начальных отрезков $[y) \subset U$ с $y < u$. Тогда $[u) = \bigcup_{y < u} [y)$ изоморфен объединению вложенных отрезков $\bigcup_{y < u} [w(y)) \subset W$. Если это объединение исчерпывает всё множество W , то $W \simeq [y)$, т. е. $W \leq U$ вопреки предположению. Положим $w(u) \in W$ равным минимальному элементу, не содержащемуся в $\bigcup_{y < u} [w(y))$. Проверьте, что $\bigcup_{y < u} [w(y)) = [w(u))$ и что отображение $u \mapsto w(u)$ устанавливает изоморфизм множества U либо со всем множеством W , либо с некоторым его начальным отрезком.

Упр. о.19. Пусть рекурсивные подмножества $W_1, W_2 \subset P$ имеют общий начальный элемент. Рассмотрим подмножество $Z \subseteq W_1$, состоящее из всех таких $z \in W_1$, что начальный интервал $[z)_1$ в множестве W_1 совпадает с начальным интервалом $[z)_2$ в множестве W_2 . Множество Z не пусто, поскольку содержит общий начальный элемент множеств W_1 и W_2 . В силу рекурсивности W_1 и W_2 множество Z содержится в $W_1 \cap W_2$, являясь, по упр. 0.17 на стр. 17, начальным интервалом как в W_1 , так и в W_2 . Если $Z \neq W_1$ и $Z \neq W_2$, то точные верхние грани Z в W_1 и W_2 , с одной стороны, не лежат в Z и поэтому различны, а с другой стороны обе равны $\rho(Z)$ в силу рекурсивности W_1 и W_2 . Тем самым, $Z = W_1$ или $Z = W_2$.

Упр. о.20. Каждое подмножество $S \subset U$ имеет непустое пересечение с каким-нибудь рекурсивным вполне упорядоченным подмножеством $W \subset P$ с начальным элементом $\rho(\emptyset)$. По упр. 0.19 подмножество W является начальным интервалом всех содержащих W рекурсивных вполне упорядоченных подмножеств с начальным элементом $\rho(\emptyset)$. Поэтому начальный элемент пересечения $S \cap W$ не зависит от выбора такого W , что $W \cap S \neq \emptyset$, и является начальным элементом подмножества S . Каждый начальный интервал $[u) \subset U$ является начальным интервалом любого содержащего u множества W из цепи. В силу рекурсивности W элемент $\rho[u) = u$.

- Упр. о.21. Пользуясь аксиомой выбора, зафиксируем для каждого $W \in \mathcal{W}(P)$ какую-нибудь верхнюю грань $b(W) \in P$. Если $f(x) > x$ для всех $x \in P$, то отображение $\beta : \mathcal{W}(P) \rightarrow P, W \mapsto f(b(W))$ противоречит лем. 0.2 на стр. 18.
- Упр. о.22. Обозначим через $\mathcal{S}(X)$ множество всех непустых подмножеств данного множества X , включая само X . При помощи аксиомы выбора постройте такое отображение $\mu : \mathcal{S}(X) \rightarrow X$, что $\mu(Z) \in Z$ для всех $Z \in \mathcal{S}(X)$. Обозначим через $\mathcal{W}(X)$ множество всех $W \in \mathcal{S}(X)$, которые можно вполне упорядочить так, что $\mu(X \setminus [w]) = w$ для всех $w \in W$. Вдохновляясь лем. 0.2 на стр. 18 покажите, что $\mathcal{W}(X) \neq \emptyset$, и убедитесь, что $X \in \mathcal{W}(X)$.
- Упр. о.23. Убедитесь, что множество всех цепей, содержащих данную цепь, является полным чумом относительно отношения включения, и примените лемму Цорна.