Множества и алгебра

В этом курсе мы вспомним сначала наивную теорию множеств вместе с элементарной логикой. Затем изучим самые начала алгебры: отношения эквивалентности и порядка, решетки, группы, кольца и модули. В конце курса мы познакомимся немного с линейной алгеброй, которую вероятно правильнее называть "линейная геометрия".

Заведомо скучные упражнения 1.1.1, 1.1.2, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.4.1 и 1.5.2.

1. Множества и логические символы

Увидел Бяку — обозначь!
— В. А. Уфнаровский, *Математический аквариум*

Математическая логика и теория множеств — это довольно серьезные науки. После преодоления "кризиса противоречий" в начале прошлого столетия они составили надежное основание современной математики[1] и служат языком для выражения понятий, идей и доказательств.

Здесь же мы излагаем упомянутые науки в упрощенной (примитивной и наивной) форме, которая тем не менее достаточна для изучения математики (отличной от серьезных логики и теории множеств) при соблюдении определенных правил безопасности. Итак, для начала, "вспомним" материал, который, наверное, правильнее называть *патологика и наивная теория множеств.*

1.1. Смысл элементарных логических символов. *Предложение* P (= высказывание, имеющее смысл) может быть *ложным* (= *неверным*), что обозначаем как $P = 0$, или *справедливым* (= *верным*), что обозначаем как $P = 1$. Из данных предложений P, P_1, P_2 можно построить новые предложения:

• $\neg P$, то есть *отрицание* P; верно в точности, когда P неверно;
• $P_1 \vee P_2$, то есть P_1 *или* P_2; верно в точности, когда по крайней мере одно из P_1 и P_2 верно;
• $P_1 \wedge P_2$, то есть P_1 *и* P_2; верно в точности, когда оба P_1 и P_2 верны;
• $P_1 \Rightarrow P_2$, то есть P_1 *влечет* P_2; верно в точности, когда P_1 неверно (ложное утверждение влечет все, что угодно) или P_2 верно (справедливое утверждение следует из любого);
• $P_1 \Leftrightarrow P_2$, то есть P_1 *эквивалентно* P_2; верно в точности, когда справедливость P_1 совпадает со справедливостью P_2.

1.1.1. Упражнение ("таблицы умножения")**.** В терминах верно/неверно имеем

$$\neg 0 = 1, \quad \neg 1 = 0, \quad 0 \vee 0 = 0, \quad 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1; \quad 0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0,$$

$$1 \wedge 1 = 1, \quad (1 \Rightarrow 0) = 0, \quad (0 \Rightarrow 0) = (0 \Rightarrow 1) = (1 \Rightarrow 1) = 1,$$

$$(0 \Leftrightarrow 1) = (1 \Leftrightarrow 0) = 0, \quad (0 \Leftrightarrow 0) = (1 \Leftrightarrow 1) = 1.$$

[1] В наши дни, теория множеств все больше и больше замещается теорией категорий, более современным, эффективным и адекватным языком математики.

1.1.2. Упражнение. Используя “таблицы умножения” приведенные выше, или лучше здравый смысл, проверьте следующие *законы Моргана*:

$$\neg\neg P \leftrightarrow P, \quad P \vee \neg P \leftrightarrow 1, \quad P \wedge \neg P \leftrightarrow 0, \quad P \vee P \leftrightarrow P, \quad P \wedge P \leftrightarrow P, \quad P_1 \vee P_2 \leftrightarrow P_2 \vee P_1,$$
$$P_1 \wedge P_2 \leftrightarrow P_2 \wedge P_1, \quad (P_1 \vee P_2) \vee P_3 \leftrightarrow P_1 \vee (P_2 \vee P_3), \quad (P_1 \wedge P_2) \wedge P_3 \leftrightarrow P_1 \wedge (P_2 \wedge P_3),$$
$$P_1 \wedge (P_2 \vee P_3) \leftrightarrow (P_1 \wedge P_2) \vee (P_1 \wedge P_3), \quad P_1 \vee (P_2 \wedge P_3) \leftrightarrow (P_1 \vee P_2) \wedge (P_1 \vee P_3),$$
$$\neg(P_1 \vee P_2) \leftrightarrow \neg P_1 \wedge \neg P_2, \quad \neg(P_1 \wedge P_2) \leftrightarrow \neg P_1 \vee \neg P_2, \quad \neg P_1 \vee P_2 \leftrightarrow P_1 \Rightarrow P_2,$$
$$P_1 \Leftrightarrow P_2 \leftrightarrow (P_1 \Rightarrow P_2) \wedge (P_1 \Leftarrow P_2), \quad P_1 \Rightarrow P_2 \leftrightarrow \neg P_1 \Leftarrow \neg P_2,$$

где P, P_1, P_2, P_3 — предложения, а символ $\leftrightarrow$ говорит, что вовлеченные предложения справедливы/несправедливы одновременно.

Кроме того, мы будем использовать символ $:=$ в смысле “равно по определению”.

1.2. Множества. Вместо определения мы примем наивную, но небессмысленную точку зрения: будем воображать множество как пакет с *элементами.* Продолжая метафору, полезно представлять такой пакет как бы сделанным из мыльной пленки (позволяя, таким образом, одному пакету частично совпадать с другим). Символически мы изображаем пакет, используя фигурные скобки $\{\ \}$. Например, $\{0, 1\}$ (или $\{0, 0, 1\}$) — это множество состоящее из двух элементов, 0 и 1. Когда e — элемент (или *член*) множества E (e находится в пакете E), мы пишем $e \in E$ или $E \ni e$.

Для того, чтобы описать какое-нибудь множество, мы можем использовать предложение $P(x)$, зависящее от параметра x. Такое предложение — это всего-навсего функция $\mathcal{E} \xrightarrow{P} \{0, 1\}$ (см. пункт 1.5), где $\mathcal{E}$ обозначает класс всех множеств, или же, если мы желаем ограничить область изменения параметра, функция $E \xrightarrow{P} \{0, 1\}$, где E — заданное множество. Таким образом, используя $P(x)$ вместо $P(x) = 1$, приходим к обозначению $C := \big\{e \mid P(e)\big\}$ или $C := \big\{e \in E \mid P(e)\big\}$, где $P(x)$ трактуется как некоторое свойство элементов. Читается это так: множество C состоит из всех тех элементов e (или из всех тех членов e множества E), которые удовлетворяют свойству $P(e)$.

1.2.1. Стандартные обозначения.

$\mathbb{C} := \{c \mid c$ является комплексным числом$\}$ — множество всех комплексных чисел;
$\mathbb{R} :=]{-\infty}, \infty[:= \{r \mid r$ является действительным числом$\}$ — множество всех действительных чисел;
$\mathbb{Q} := \{q \in \mathbb{R} \mid q$ является рациональным числом$\}$ — множество всех рациональных чисел;
$\mathbb{Z} := \{z \in \mathbb{Q} \mid z$ является целым числом$\}$ — множество всех целых чисел;
$\mathbb{N} := \{n \in \mathbb{Z} \mid n \geqslant 0\}$ — множество всех натуральных чисел;
$\mathbb{R}^{\geqslant 0} := [0, \infty[:= \{r \in \mathbb{R} \mid r \geqslant 0\}$ — множество всех неотрицательных действительных чисел;
$\mathbb{R}^{>0} :=]0, \infty[:= \{r \in \mathbb{R} \mid r > 0\}$ — множество всех положительных действительных чисел;
$[a, b] := \{r \in \mathbb{R} \mid a \leqslant r \leqslant b\}$, $]a, b[:= \{r \in \mathbb{R} \mid a < r < b\}$, $[a, b[:= \{r \in \mathbb{R} \mid a \leqslant r < b\}$, $]a, b] := \{r \in \mathbb{R} \mid a < r \leqslant b\}$ — замкнутый, открытый и полуоткрытые интервалы с концами $a, b \in \mathbb{R}$;
$]{-\infty}, b] := \{r \in \mathbb{R} \mid r \leqslant b\}$, $]{-\infty}, b[:= \{r \in \mathbb{R} \mid r < b\}$, $[a, \infty[:= \{r \in \mathbb{R} \mid a \leqslant r\}$, $]a, \infty[:= \{r \in \mathbb{R} \mid a < r\}$ — полубесконечные интервалы;
$\varnothing := \{e \mid e \neq e\}$ — пустое множество (пустой пакет).

Заметьте, что $[a, b] = \varnothing$, если $a > b$.

1.2.2. Парадоксы. Наивная точка зрения на теорию множеств сопряжена с некоторыми опасностями. Рассмотрите следующие парадоксы.

Парадокс брадобрея. Брадобрей — *это такой человек, который бреет тех, и только тех, кто не бреет себя сам. Кто бреет брадобрея?*
Парадокс Рассела. *Определим* $C := \{x \mid x \notin x\}$. *Если* $C \in C$, *то* $C \notin C$. *Если* $C \notin C$, *то* $C \in C$.
Парадокс Ришара. *Наименьшее натуральное число, которое нельзя корректно определить при помощи русской фразы, содержащей не более* 130 *символов.*

Отметьте, что размер важен: если ограничить мощность (см. пункт 1.6) множеств x в парадоксе Рассела, то никакого противоречия нет.

Рецепт — как бороться с такими опасностями — довольно прост. Достаточно избегать самореференций и не рассматривать слишком больших "множеств" (таких как, например, "множество всех множеств"). Это все еще позволяет иметь дело с огромными совокупностями называемыми *классами* и образованными, например, всеми множествами.

Рассматривая парадокс Ришара, вообразим, что рядом с каждой фразой корректно описывающей какое-нибудь конкретное натуральное число, мы напишем это самое число. После чего проанализируем, что произойдет, когда очередь дойдет до фразы, участвующей в парадоксе.

Следуя этому рецепту, мы запрещаем соотношения[2] вида $x_1 \in x_2 \in \dots \in x_n \in x_1$.

1.2.3. Операции над множествами и отношения между множествами. Пусть C_1 и C_2 — множества. Будем говорить, что C_1 *содержится* в C_2, или что C_2 *содержит* C_1, или что C_1 — *подмножество* в C_2, если $\forall x\ x \in C_1 \Rightarrow x \in C_2$, записывая этот факт как $C_1 \subset C_2$ или $C_2 \supset C_1$. Другими словами, чтобы проверить, что $C_1 \subset C_2$, нужно доказать импликацию $x \in C_1 \Rightarrow x \in C_2$.

Множества C_1 и C_2 считаются равными, если они имеют одни и те же элементы. Таким образом, $C_1 = C_2$ эквивалентно $C_1 \subset C_2 \wedge C_1 \supset C_2$.

Мы говорим, что множество C_1 — это *собственное подмножество* множества C_2, символически $C_1 \subsetneq C_2$, если $C_1 \subset C_2 \wedge C_1 \neq C_2$.

Обозначим через $C_1 \cap C_2$ *пересечение* множеств C_1 и C_2, то есть $C_1 \cap C_2 := \{x \mid x \in C_1 \wedge x \in C_2\}$.

Обозначим через $C_1 \cup C_2 := \{x \mid x \in C_1 \vee x \in C_2\}$ *объединение* множеств C_1 и C_2. Если $C_1 \cap C_2 = \varnothing$, мы имеем *дизъюнктное объединение* $C_1 \sqcup C_2 := C_1 \cup C_2$, то есть обычное объединение, но с подчеркнутой *дизъюнктностью* $C_1 \cap C_2 = \varnothing$.

Обозначим через $C_1 \times C_2 := \big\{(c_1, c_2) \mid c_1 \in C_1 \wedge c_2 \in C_2\big\}$ *декартово произведение* множеств C_1 и C_2. Это произведение состоит из всех *упорядоченных пар* (c_1, c_2) таких, что $c_1 \in C_1$ и $c_2 \in C_2$. Нет необходимости определять, что такое упорядоченная пара. Достаточно знать характеристические свойства этого объекта:

$$(c_1, c_2) = (c_1', c_2') \Leftrightarrow (c_1 = c_1' \wedge c_2 = c_2').$$

(Очевидный пример: декартово произведение $[0,1] \times [0,1]$ можно визуализировать как единичный квадрат.) Аналогично, *декартово произведение* $C_1 \times C_2 \times \dots \times C_n$ множеств $C_1, C_2, \dots, C_n$ состоит из всех *упорядоченных* n*-ок* $(c_1, c_2, \dots, c_n)$ таких, что $c_i \in C_i$ для

[2] В действительности, стандартная аксиома регулярности в аксиоматике Цермело-Френкеля еще сильнее: для любого непустого множества $C \neq \varnothing$ существует элемент $c \in C$ такой, что $c \cap C = \varnothing$.

всех $1 \leqslant i \leqslant n$,

$$C_1 \times C_2 \times \cdots \times C_n := \big\{(c_1, c_2, \ldots, c_n) \mid c_1 \in C_1 \wedge c_2 \in C_2 \wedge \cdots \wedge c_n \in C_n\big\}.$$

Обозначим через $C_1 \setminus C_2 := \{x \in C_1 \mid x \notin C_2\}$ *дополнение* множества C_2 в множестве C_1.

Чтобы не засорять обозначения, мы будем писать p вместо $\{p\}$, если нет опасности что-либо перепутать. Например, $\mathbb{R} \setminus 0$ — это множество всех ненулевых действительных чисел, $\mathbb{R} \setminus 0 := \mathbb{R} \setminus \{0\}$. Круглые скобки тоже будут использоваться экономно. Лишь изредка мы будем отдавать дань традиции при использовании скобок.

1.2.4. Упражнение. Пусть C, C_1, C_2, C_3 — множества и $C \supset S, S_1, S_2$ — подмножества. Используйте законы Моргана, чтобы проверить следующие соотношения.

$$C \setminus (C \setminus S) = S, \quad S \sqcup (C \setminus S) = C, \quad C \cup C = C, \quad C \cap C = C, \quad C_1 \cup C_2 = C_2 \cup C_1,$$
$$C_1 \cap C_2 = C_2 \cap C_1, \quad (C_1 \cup C_2) \cup C_3 = C_1 \cup (C_2 \cup C_3), \quad (C_1 \cap C_2) \cap C_3 = C_1 \cap (C_2 \cap C_3),$$
$$C_1 \cap (C_2 \cup C_3) = (C_1 \cap C_2) \cup (C_1 \cap C_3), \quad C_1 \cup (C_2 \cap C_3) = (C_1 \cup C_2) \cap (C_1 \cup C_3),$$
$$C \setminus (S_1 \cup S_2) = (C \setminus S_1) \cap (C \setminus S_2), \quad C \setminus (S_1 \cap S_2) = (C \setminus S_1) \cup (C \setminus S_2),$$
$$(C \setminus S_1) \cup S_2 = C \Leftrightarrow S_1 \subset S_2, \quad C_1 = C_2 \Leftrightarrow (C_1 \subset C_2) \wedge (C_1 \supset C_2),$$
$$S_1 \subset S_2 \Leftrightarrow (C \setminus S_1) \supset (C \setminus S_2).$$

Соотношения из упражнения 1.2.4 могут быть получены, используя так называемое “*доказательство по определению*”. Поскольку любое определение — это по сути своей лишь аббревиатура, то метод состоит в простой “расшифровке аббревиатур”.

В качестве примера докажем тождество $C_1 \cup (C_2 \cap C_3) = (C_1 \cup C_2) \cap (C_1 \cup C_3)$. По определению объединения, включение $x \in C_1 \cup (C_2 \cap C_3)$ эквивалентно предложению $x \in C_1 \vee x \in C_2 \cap C_3$. По определению пересечения, это можно переписать как $x \in C_1 \vee (x \in C_2 \wedge x \in C_3)$. В силу аналогичных доводов, $x \in (C_1 \cup C_2) \cap (C_1 \cup C_3)$ эквивалентно $(x \in C_1 \vee x \in C_2) \wedge (x \in C_1 \vee x \in C_3)$. Остается применить подходящий закон Моргана, взяв $x \in C_i$ в качестве P_i для $i = 1, 2, 3$.

1.2.5. Упражнение. Докажите соотношения

$$\varnothing \in \{\varnothing\}, \quad \{\varnothing\} \neq \varnothing, \quad \varnothing \subset \{\varnothing\}, \quad \{\varnothing \mid \varnothing \neq \varnothing\} = \varnothing, \quad \varnothing \subset C, \quad \varnothing \cup C = C, \quad \varnothing \cap C = \varnothing,$$
$$C \setminus C = \varnothing, \quad (C_1 \subset C_2 \wedge C_2 \subset C_3) \Rightarrow C_1 \subset C_3, \quad C_1 \subset C_1 \cup C_2, \quad C_1 \supset C_1 \cap C_2,$$
$$(C_1 \subset C \wedge C_2 \subset C) \Rightarrow C_1 \cup C_2 \subset C, \quad (C \subset C_1 \wedge C \subset C_2) \Rightarrow C \subset C_1 \cap C_2,$$
$$C_1 \cup C_2 = C_2 \Leftrightarrow C_1 \subset C_2 \Leftrightarrow C_1 \cap C_2 = C_1, \quad \varnothing \times C = \varnothing,$$
$$(C_1 \times C_2) \cap (C_1' \times C_2') = (C_1 \cap C_1') \times (C_2 \cap C_2'), \quad (C_1 \cup C_1') \times C = (C_1 \times C) \cup (C_1' \times C),$$
$$C \times (C_2 \cup C_2') = (C \times C_2) \cup (C \times C_2'), \quad (C_1 \setminus C_1') \times C = (C_1 \times C) \setminus (C_1' \times C),$$
$$(C_1 \times C_2) \setminus (C_1' \times C_2') = \big((C_1 \setminus C_1') \times C_2\big) \sqcup \big((C_1 \cap C_1') \times (C_2 \setminus C_2')\big),$$
$$C_1 \times C_2 = C_2 \times C_1 \neq \varnothing \Rightarrow C_1 = C_2$$

для любых множеств $C, C_1, C_1', C_2, C_2', C_3$.

1.3. Кванторы. Пусть $P(x)$ — предложение, зависящее от параметра x. Мы можем сконструировать новые предложения, которые уже не зависят от параметра x :

- $\exists x\ P(x)$, то есть *существует x такой, что $P(x)$ справедливо*;
- $\forall x\ P(x)$, то есть *для любого x выполнено $P(x)$*.

Неэлементарные логические символы $\exists$ и $\forall$ называются *кванторами.*

Область, где варьируется параметр x, обычно ясна из контекста или указывается явно. К примеру, предложение “любое целое число четно” записывается в виде $\forall x \in \mathbb{Z}\ P(x)$, где $P(x)$ утверждает, что “x четно”. Фактически же, предложения $\exists x \in C\ P(x)$ и $\forall x \in C\ P(x)$ означают $\exists x\ x \in C \wedge P(x)$ и $\forall x\ x \in C \Rightarrow P(x)$, соответственно.

Прочтение логических символов на данной идиоме как правило допускает многочисленные синонимы. Так предложения $P_1 \Rightarrow P_2$ и $\forall x\ P(x)$ могут быть прочитаны как “P_2 выполняется всякий раз, когда P_1 выполняется” и “каков бы не был x, справедливо $P(x)$”. С формальной точки зрения, выбор синонима не меняет математического смысла. Тем не менее, почти всегда полезно переформулировать утверждение, используя синонимы, или же, вообще, придать ему другую форму, поскольку это проливает дополнительный свет на обсуждаемый вопрос, то есть позволяет видеть математические объекты с другой стороны.

Для конечного множества $C = \{c_1, c_2, \dots, c_n\}$, предложения $\exists x \in C\ P(x)$ и $\forall x \in C\ P(x)$ эквивалентны предложениям $P(c_1) \vee P(c_2) \vee \dots \vee P(c_n)$ и $P(c_1) \wedge P(c_2) \wedge \dots \wedge P(c_n)$, соответственно. Так получается следующая (изредка полезная) интерпретация кванторов: $\exists$ и $\forall$ можно трактовать соответственно как разновидности операций $\vee$ и $\wedge$, вовлекающих бесконечно много аргументов.

Различные кванторы, вообще говоря, не коммутируют. Пусть $\mathcal{E} \times \mathcal{E} \xrightarrow{P} \{0,1\}$ — предложение, зависещее от параметров x и y. Тогда предложения $\exists x \forall y\ P(x,y)$ и $\forall y \exists x\ P(x,y)$ могут оказаться неэквивалентными. Чтобы разобраться с этим, фиксируем в первом предложении некий x_0 так, чтобы предложение $P(x_0, y)$ выполнялось для всех y. Во втором предложении, полезно представлять переменную x как зависящую от переменной y : для каждого y существует некий $x(y)$ такой, что выполнено $P\big(x(y), y\big)$. Мы видим, что, в случае первого предложения, x_0 не зависит от y. Теперь легко построить контрпример взяв, скажем, $x = y$ в качестве $P(x,y)$.

1.3.1. Упражнение. Пусть P — предложение, не зависящее от x (это означает, что справедливость $P(x)$ всегда одна и та же, независимо от выбора x), и пусть $Q(x)$ и $R(x,y)$ — предложения, зависящие соответственно от x и от x, y. Убедитесь, что

$$\exists x\ Q(x) \leftrightarrow \exists y\ Q(y), \quad \forall x\ Q(x) \leftrightarrow \forall y\ Q(y), \quad \exists x \exists y\ R(x,y) \leftrightarrow \exists y \exists x\ R(x,y),$$
$$\forall x \forall y\ R(x,y) \leftrightarrow \forall y \forall x\ R(x,y), \quad \neg\forall x\ Q(x) \leftrightarrow \exists x\ \neg Q(x), \quad \neg\exists x\ Q(x) \leftrightarrow \forall x\ \neg Q(x),$$
$$P \vee \exists x\ Q(x) \leftrightarrow \exists x\ P \vee Q(x), \quad P \vee \forall x\ Q(x) \leftrightarrow \forall x\ P \vee Q(x), \quad P \wedge \exists x\ Q(x) \leftrightarrow \exists x\ P \wedge Q(x),$$
$$P \wedge \forall x\ Q(x) \leftrightarrow \forall x\ P \wedge Q(x), \quad P \Rightarrow \exists x\ Q(x) \leftrightarrow \exists x\ P \Rightarrow Q(x),$$
$$P \Rightarrow \forall x\ Q(x) \leftrightarrow \forall x\ P \Rightarrow Q(x), \quad \big(\exists x \forall y\ R(x,y)\big) \Rightarrow \forall y \exists x\ R(x,y),$$

где символ $\leftrightarrow$ говорит, что вовлеченные предложения справедливы/несправедливы одновременно.

1.3.2. Упражнение. Пусть P — предложение, не зависящее от x, пусть C — множество и пусть $Q(x)$ и $R(x,y)$ — предложения, зависящие соответственно от x и от x, y. Какие из импликаций

$$\big(\exists x \in C\ Q(x)\big) \Rightarrow \forall x \in C\ Q(x), \quad \big(\forall x \in C\ Q(x)\big) \Rightarrow \exists x \in C\ Q(x),$$
$$\big(\forall y \exists x\ R(x,y)\big) \Rightarrow \exists x \forall y\ R(x,y), \quad \Big(\big(\exists x \in C\ Q(x)\big) \Rightarrow P\Big) \Rightarrow \big(\exists x \in C\ Q(x) \Rightarrow P\big),$$
$$\big(\exists x \in C\ Q(x) \Rightarrow P\big) \Rightarrow \Big(\big(\exists x \in C\ Q(x)\big) \Rightarrow P\Big),$$

$$\Big(\big(\forall x \in C\ Q(x)\big) \Rightarrow P\Big) \Rightarrow \big(\forall x \in C\ Q(x) \Rightarrow P\big),$$

$$\big(\forall x \in C\ Q(x) \Rightarrow P\big) \Rightarrow \Big(\big(\forall x \in C\ Q(x)\big) \Rightarrow P\Big)$$

всегда справедливы и почему?

1.3.3. Упражнение. Пусть $P(x)$ — предложение, зависящее от x. Используя логические символы описанные выше, выразите предложение $\exists!\, x\ P(x)$, означающее, что “существует единственный x такой, что выполнено $P(x)$”.

В дальнейшем мы используем упражнения 1.1.2 и 1.3.1 в качестве средства манипулирования предложениями, не ссылаясь явно на сами упражнения. Это особенно полезно, когда кажется невозможным (или очень трудным) понимание смысла рассматриваемых утверждений.

Заметьте, что достаточно было бы использовать логические символы $\neg$, $\vee$, $\exists$, поскольку остальные выражаются в терминах $\neg$, $\vee$, $\exists$ в силу упражнений 1.1.2 и 1.3.1.

1.4. Семейства множеств. Пусть I — множество (*индексов*). Если для каждого $i \in I$ задано множество C_i, мы говорим о *семействе* множеств C_i, $i \in I$. Семейство называется *дизъюнктным,* если $C_i \cap C_{i'} = \varnothing$ для любых различных $i, i' \in I$, $i \neq i'$.

Объединение семейства — это множество, образованное всеми теми элементами, что принадлежат по крайней мере одному члену семейства, $\bigcup\limits_{i\in I} C_i := \{x \mid \exists i \in I\ x \in C_i\}$. В случае, когда семейство дизъюнктно, мы получаем *дизъюнктное объединение* $\bigsqcup\limits_{i\in I} C_i := \bigcup\limits_{i\in I} C_i$, то есть обычное объединение семейства с подчеркнутой дизъюнкностью семейства.

Пересечение семейства — это множество, образованное всеми теми элементами, что принадлежат всем членам семейства, $\bigcap\limits_{i\in I} C_i := \{x \in U \mid \forall i \in I\ x \in C_i\}$. (Здесь U — “универсальное” множество такое, что $C_i \subset U$ для всех $i \in I$. Если $I = \varnothing$, ограничение $x \in U$ необходимо, поскольку без него мы столкнемся с парадоксом.)

Пусть $C_i \subset X$, $i \in I$, — некоторое семейство множеств. Произвольное подмножество $I' \subset I$ задает новое семейство C_i, $i \in I'$, *подсемейство* исходного семейства. Можно также рассматривать какое-нибудь семейство подсемейств данного семейства. Формально: пусть $I_j \subset I$, $j \in J$, — семейство подмножеств I; тогда имеем семейство, чей j-тый член — это семейство C_i, $i \in I_j$, причем j пробегает J.

1.4.1. Упражнение. Пусть C_i, $i \in I$, и $C'_{i'}$, $i' \in I'$, — семейства множеств, пусть $I_j \subset I$, $j \in J$, — семейство подмножеств в I, и пусть C — множество. Докажите следующие формулы:

$$C \setminus \bigcup_{i\in I} C_i = \bigcap_{i\in I}(C \setminus C_i), \qquad C \setminus \bigcap_{i\in I} C_i = \bigcup_{i\in I}(C \setminus C_i), \qquad C \cap \bigcup_{i\in I} C_i = \bigcup_{i\in I}(C \cap C_i),$$

$$C \cup \bigcap_{i\in I} C_i = \bigcap_{i\in I}(C \cup C_i), \qquad \Big(\bigcup_{i\in I} C_i\Big) \cap \Big(\bigcup_{i'\in I'} C'_{i'}\Big) = \bigcup_{i\in I, i'\in I'} (C_i \cap C'_{i'}),$$

$$\Big(\bigcap_{i\in I} C_i\Big) \cup \Big(\bigcap_{i'\in I'} C'_{i'}\Big) = \bigcap_{i\in I, i'\in I'} (C_i \cup C'_{i'}),$$

$$\bigcup_{j\in J}\Big(\bigcup_{i\in I_j} C_i\Big) = \bigcup_{i\in \bigcup\limits_{j\in J} I_j} C_i, \qquad \bigcap_{j\in J}\Big(\bigcap_{i\in I_j} C_i\Big) = \bigcap_{i\in \bigcup\limits_{j\in J} I_j} C_i.$$

Имеется весьма полезный частный случай семейств, когда множество индексов — это само семейство. Такое семейство $\mathcal{F}$ — это просто множество (множеств). В терминах индексов, оно описывается как C, $C \in \mathcal{F}$. Для такого типа семейств будем обозначать объединение и пересечение как $\cup\mathcal{F} := \bigcup\limits_{C\in\mathcal{F}} C$ и $\cap\mathcal{F} := \bigcap\limits_{C\in\mathcal{F}} C$, соответственно.

1.5. Функции. *Функция* или *отображение* $f : D \to C$ из D в C — это некое правило (или закон, или формула), ассоциирующее с каждым элементом $d \in D$ единственный элемент $c \in C$, обозначаемый через $c = f(d)$ и называемый *образом* элемента d при отображении f. Используется также обозначение $D \xrightarrow{f} C$. Мы называем множество D *областью* и множество C — *кообластью* функции f. Заметьте, что функции $f : D \to C$ и $f' : D' \to C'$ считаются по определению различными, если их области или кообласти различны, то есть если $D \neq D'$ или $C \neq C'$, даже если правила выглядят одинаково. Например, мы имеем две разные функции $f : \mathbb{R} \to \mathbb{R}$, $f : r \mapsto r^2$, и $f' : \mathbb{R} \to \mathbb{R}^{\geqslant 0}$, $f' : r \mapsto r^2$, хотя они и заданны при помощи одинакового правила $r \mapsto r^2$. (Написав $f : d \mapsto c$, мы подчеркиваем, как именно функция f "действует" на уровне элементов; формула $f : d \mapsto c$ эквивалентна равенству $f(d) = c$.)

Множество $\Gamma_f := \Big\{\big(d, f(d)\big) \in D \times C \mid d \in D\Big\}$ называется *графиком* функции $D \xrightarrow{f} C$. Иногда бывает удобно интерпретировать функцию как ее график.

Пусть $f : D \to C$ — функция, и пусть $D \supset D'$ и $C \supset C'$ — подмножества. Тогда множество $fD' := \big\{f(d) \mid d \in D'\big\}$ называется *образом* D' при отображении f и множество $f^{-1}C' := \big\{d \in D \mid f(d) \in C'\big\}$ называется *обратным образом* (или *прообразом*) C' при отображении f.

Ограничение или *сужение* $f|_{D'} : D' \to C$ отображения $f : D \to C$ на подмножество $D' \subset D$ задано очевидным правилом $f|_{D'} : d' \mapsto f(d')$. Функция *включения* $i : D' \hookrightarrow D$ задана правилом $i : d' \mapsto d'$ для всех $d' \in D'$.

Пусть $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3$ — пара функций указанного формата. Мы определим *композицию* или *суперпозицию* $f_2 \circ f_1 : C_1 \to C_3$ этих функций по формуле $(f_2 \circ f_1)(x) := f_2\big(f_1(x)\big)$ для всех $x \in C_1$. Эта операция ассоциативна: легко проверить, что $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$ для функций $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3 \xrightarrow{f_3} C_4$. Легко также заметить, что ограничение $f|_{D'}$ функции $f : D \to C$ на подмножество $D' \subset D$ — это композиция $f \circ i$, то есть, $f|_{D'} = f \circ i$, где $i : D' \hookrightarrow D$ — функция включения. Для произвольного множества C, мы имеем *тождественную* функцию $1_C : C \to C$ заданную правилом $1_C : c \mapsto c$. Эта функция удовлетворяет тождествам $f_1 \circ 1_C = f_1$ и $1_C \circ f_2 = f_2$ для произвольных функций $f_1 : C \to C_1$ и $f_2 : C_2 \to C$.

Функция $f : D \to C$ называется *инъективной, инъекцией* или *вложением,* если

$$\forall d_1, d_2 \in D \ f(d_1) = f(d_2) \Rightarrow d_1 = d_2.$$

Мы используем обозначение $f : D \hookrightarrow C$, подчеркивая, что функция $f : D \to C$ инъективна. Упомянутая выше функция включения является примером инъекции.

Функция $f : D \to C$ называется *сюръективной, сюръекцией* или *наложением,* если каждый элемент кообласти C является f-образом некоторого элемента области D, то есть если $\forall\ c \in C\ \exists\ d \in D\ f(d) = c$. Эквивалентно, функция f сюръективна тогда, и только тогда, когда $fD = C$.

Одновременно инъективная и сюръективная функция $f : D \to C$ называется *биективной* или *биекцией.*

1.5.1. Упражнение. Даны функции $f : D \to C$ и $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3$. Докажите, что

• функция f сюръективна тогда, и только тогда, когда она обладает правой обратной $g : D \leftarrow C$, то есть $f \circ g = 1_C$ (такую функцию g называют *сечением* сюръекции f);

• в предположении $D \neq \varnothing$, функция f инъективна тогда, и только тогда, когда она обладает левой обратной $g : D \leftarrow C$, то есть $g \circ f = 1_D$;

• функция f биективна тогда, и только тогда, когда она обладает двусторонней обратной $g : D \leftarrow C$, то есть $f \circ g = 1_C$ и $g \circ f = 1_D$; такая *обратная* функция единственна, если существует, и обозначается символом f^{-1};

• если функции f_1 и f_2 — биекции, то композиция $f_2 \circ f_1$ — биекция и $(f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1}$.

Мы пришли к другому, правильному[3] определению: биекция — это функция обладающяя двусторонней обратной.

1.5.2. Упражнение. Пусть $f : D \to C$ и $f' : C \to B$ — функции, пусть $D \supset D_i$, $i \in I$, и $C \supset C_j$, $j \in J$, — семейства подмножеств и пусть $D \supset D'$, $C \supset C'$ и $B \supset B'$ — подмножества. Докажите следующие формулы.

$$f \bigcup_{i \in I} D_i = \bigcup_{i \in I} fD_i, \quad f \bigcap_{i \in I} D_i \subset \bigcap_{i \in I} fD_i, \quad (f' \circ f)D' = f'(fD'), \quad (f' \circ f)^{-1}B' = f^{-1}(f'^{-1}B'),$$

$$f^{-1} \bigcup_{j \in J} C_j = \bigcup_{j \in J} f^{-1}C_j, \qquad f^{-1} \bigcap_{j \in J} C_j = \bigcap_{j \in J} f^{-1}C_j, \qquad f^{-1}(C \setminus C') = D \setminus f^{-1}C'.$$

Мы планируем опускать в дальнейшем доказательства по определению. В качестве последнего примера продемонстрируем, как доказать формулу $(f' \circ f)^{-1}B' = f^{-1}(f'^{-1}B')$. По определению прообраза, утверждение $x \in f^{-1}(f'^{-1}B')$ означает $x \in D \wedge f(x) \in f'^{-1}B'$ и, по той же причине, оно означает $x \in D \wedge \Big(f(x) \in C \wedge f'\big(f(x)\big) \in B'\Big)$. Поскольку $f(x) \in C$ для любого $x \in D$, мы можем убрать фрагмент $f(x) \in C$ из формулы и получить $x \in D \wedge (f' \circ f)(x) \in B'$ по определению композиции. По определению прообраза, это означает $x \in (f' \circ f)^{-1}B'$.

Декартово произведение $C_1 \times C_2$ снабжено *проекциями* $\pi_i : C_1 \times C_2 \to C_i$, $i = 1, 2$. Эти проекции очевидно[4] сюръективны. И, более общо, пусть C_i, $i \in I$, — семейство множеств. Определим *декартово произведение* этого семейства формулой

$$\prod_{i \in I} C_i := \Big\{ I \xrightarrow{f} \bigcup_{i \in I} C_i \mid \forall i \in I\ f(i) \in C_i \Big\}.$$

Элементы декартова произведения $\prod\limits_{i \in I} C_i$ типично обозначаются как $(c_i)_{i \in I}$ вместо $I \xrightarrow{f} \bigcup\limits_{i \in I} C_i$, где $c_i := f(i)$ для всех $i \in I$. Для каждого $i \in I$, имеем *проекцию* $\pi_i : \prod\limits_{i \in I} C_i \to C_i$ (очевидно сюръективную).

[3]Определение — вовсе не аббревиатура. Мы поймем в процессе изучения, что ситуация с определениями гораздо более тонкая и сформулируем максиму: Если определения правильные — доказательства тривиальны.

[4]Слово “очевидный” не всегда уместно в математике.

$$\begin{tikzcd} & C \arrow[dl, "f_i"'] \arrow[d, "f"] \\ C_i & \prod\limits_{i\in I} C_i \arrow[l, "\pi_i"] \end{tikzcd}$$

1.5.3. Упражнение. Пусть $f_i : C \to C_i$, $i \in I$, — семейство функций. Покажите, что существует единственная функция $f : C \to \prod\limits_{i\in I} C_i$ такая, что $\pi_i \circ f = f_i$ для всех $i \in I$.

$$\begin{tikzcd} & C \\ C_i \arrow[ur, "f_i"] \arrow[r, "\iota_i"'] & \coprod\limits_{i\in I} C_i \arrow[u, "f"'] \end{tikzcd}$$

1.5.4. Упражнение. Пусть C_i, $i \in I$, — дизъюнктное семейство множеств, и пусть $f_i : C_i \to C$, $i \in I$, — семейство функций. Покажите, что существует единственная функция $f : \coprod\limits_{i\in I} C_i \to C$ такая, что $f \circ \iota_i = f_i$ для всех $i \in I$, где $\iota_i : C_i \hookrightarrow \coprod\limits_{i\in I} C_i$, $i \in I$, — это функции включения.

$$\begin{tikzcd} X \arrow[drr, bend left, "j"] \arrow[dr, "h"] \arrow[ddr, bend right, "g"'] & & \\ & f^{-1}C' \arrow[r, "\iota'"] \arrow[d, "f'"] & D \arrow[d, "f"] \\ & C' \arrow[r, "\iota"] & C \end{tikzcd}$$

1.5.5. Упражнение. Пусть $f : D \to C$ — функция, и пусть $\iota : C' \hookrightarrow C$ и $\iota' : f^{-1}C' \hookrightarrow D$ — функции включения. Заметьте, что существует единственная функция $f' : f^{-1}C' \to C'$ такая, что $f \circ \iota' = \iota \circ f'$. Пусть $C' \xleftarrow{g} X \xrightarrow{j} D$ — функции такие, что $f \circ j = \iota \circ g$. Покажите, что существует единственная функция $h : X \to f^{-1}C'$ такая, что $f' \circ h = g$ и $\iota' \circ h = j$.

1.5.6. Упражнение. Покажите, что любая функция $D \xrightarrow{f} C$ является композицией функций $D \xrightarrow{b} \Gamma_f \overset{i}{\hookrightarrow} D \times C \xrightarrow{\pi} C$, то есть $f = \pi \circ i \circ b$. Здесь b — биекция, $\Gamma_f := \Big\{\big(d, f(d)\big) \in D \times C \mid d \in D\Big\}$ — график функции f, i — включение графика в произведение и π — проекция.

1.5.7. Определение. Каждую функцию $f : D \to C$ можно интерпретировать как дизъюнктное семейство $f^{-1}c$, $c \in C$, *слоев функции* f. При этом область D функции f в точности составлена из всех таких слоев, $D = \coprod\limits_{c\in C} f^{-1}c$.

Пусть $D_1 \xrightarrow{f_1} C \xleftarrow{f_2} D_2$ — функции. *Расслоенное произведение* множеств D_1 и D_2 над множеством C — это множество $D_1 \times_C D_2 := \big\{(d_1, d_2) \in D_1 \times D_2 \mid f_1(d_1) = f_2(d_2)\big\}$. Имеются композиции $p_i := \pi_i \circ \iota : D_1 \times_C D_2 \to D_i$ проекций $\pi_i : D_1 \times D_2 \to D_i$, $i = 1, 2$, с функцией включения $\iota : D_1 \times_C D_2 \hookrightarrow D_1 \times D_2$, удовлетворяющие соотношению $f := f_1 \circ p_1 = f_2 \circ p_2$. Обозначение $D_1 \times_C D_2$ подразумевает неявное присутствие функций f_i, p_i.

Нетрудно видеть, что $f^{-1}c = f_1^{-1}c \times f_2^{-1}c$ для любого $c \in C$. Иными словами, в терминах слоев, функция f — это послойное произведение фунций f_1 и f_2.

$$\begin{tikzcd} X \arrow[drr, bend left, "g_2"] \arrow[dr, "h"] \arrow[ddr, bend right, "g_1"'] & & \\ & D_1 \times_C D_2 \arrow[r, "p_2"'] \arrow[d, "p_1"] & D_2 \arrow[d, "f_2"'] \\ & D_1 \arrow[r, "f_1"] & C \end{tikzcd}$$

1.5.8. Упражнение. В ситуации расслоенного произведения (см. определение 1.5.7), пусть $D_1 \xleftarrow{g_1} X \xrightarrow{g_2} D_2$ — функции такие, что $f_1 \circ g_1 = f_2 \circ g_2$. Покажите, что существует единственная функция $h : X \to D_1 \times_C D_2$ такая, что $p_1 \circ h = g_1$ и $p_2 \circ h = g_2$.

1.6. Мощность. Грубо говоря, мощность множества измеряет насколько велико это множество, то есть "сколько" в нем элементов.

Любую биекцию $C_1 \xrightarrow{b} C_2$ мы будем также называть *взаимно однозначным соответствием* между множествами C_1 и C_2. Будем представлять, что b производит из множества C_1 некую копию C_2, то есть b как бы изготавливает множество C_1 из другого материала, и в результате получается множество C_2.

Мы говорим, что множества C_1 и C_2 имеют одинаковую *мощность,* если существует биекция между C_1 и C_2. (Неважно, $C_1 \to C_2$ или $C_1 \leftarrow C_2$, поскольку функция обратная к биекции является биекцией; символы $C_1 \simeq C_2$ выражают тот факт, что между множествами C_1 и C_2 существует биекция.) Мы обозначаем через $|C|$ (или через $\#C$) мощность множества C.

Мы будем писать $|C_1| \leqslant |C_2|$, если существует инъекция $C_1 \hookrightarrow C_2$. Можно показать (и это нетривиально), что для любых мощностей c_1, c_2 справедливо $c_1 \leqslant c_2$ или $c_1 \geqslant c_2$. Таким образом, натуральные числа — это в точности мощности конечных множеств. По определению, множество $\mathbb{N}$ счетно. Соответствующая мощность является наименьшей бесконечной мощностью. С мощностями можно совершать различные операции: сложение, умножение, возведение в степень и т.д.: $|C_1| + |C_2| := |C_1 \sqcup C_2|$, $|C_1| \cdot |C_2| := |C_1 \times C_2|$, $|C_2|^{|C_1|} := |C_2^{C_1}|$, где $C_2^{C_1} := \{C_1 \to C_2\}$ — это множество всех функций из C_1 в C_2. В действительности, $|C_1| + |C_2| = |C_1| \cdot |C_2| = \max\big(|C_1|, |C_2|\big)$, если $C_1 \neq \varnothing$ и C_2 бесконечно.

Обозначим через $2^C := \{X \mid X \subset C\}$ множество всех подмножеств множества C или *булеан* множества C. С каждым подмножеством $S \subset C$ связана *характеристическая функция* этого подмножества. Эта функция $\chi_S : C \to \{0, 1\}$ задана правилом

$$\chi_S(c) := \begin{cases} 0 & \text{если} \quad c \notin S \\ 1 & \text{если} \quad c \in S \end{cases}.$$

Формула $f \mapsto f^{-1}1$ устанавливает биекцию $\{0, 1\}^C \simeq 2^C$.

Часто соотношение между (натуральными) числами имеет естественную и глубинную природу на уровне множеств. Следующее упражнение иллюстрирует эту максиму.

1.6.1. Упражнение. Пусть C, C_1, C_2 — множества. Заметьте, что $2^{C_1 \cap C_2} = 2^{C_1} \cap 2^{C_2}$ и $C_1 \subset C_2 \Rightarrow 2^{C_1} \subset 2^{C_2}$. Установите следующие биекции.

$$2^C \simeq \{0, 1\}^C, \qquad 2^{C_1 \sqcup C_2} \simeq 2^{C_1} \times 2^{C_2}, \qquad C^{C_1 \sqcup C_2} \simeq C^{C_1} \times C^{C_2},$$

$$(2^{C_1})^{C_2} \simeq 2^{C_1 \times C_2}, \qquad (C^{C_1})^{C_2} \simeq C^{C_1 \times C_2}.$$

1.6.2. Упражнение.* Покажите, что $|C| \neq |2^C|$ для произвольного множества C.

1.6.3. Теорема (Кантор-Шредер-Бернштейн)**.** *Пусть A и B множества такие, что $|A| \leqslant |B|$ и $|A| \geqslant |B|$. Тогда $|A| = |B|$.*

Доказательство. Имеем биекции $f : A \to B'$ и $g : A' \leftarrow B$, где $A' \subset A$ и $B' \subset B$. Определим индуктивно $C_0 := A \setminus A'$ и $C_{n+1} := gfC_n$. Положим $C := \bigcup\limits_{n \in \mathbb{N}} C_n$ и $C' := \bigcup\limits_{n \in \mathbb{N}} C_{n+1}$. Из $A \setminus C = A' \setminus C'$ следует, что

$$g^{-1}(A \setminus C) = g^{-1}\Big(A' \setminus \bigcup_{n \in \mathbb{N}} C_{n+1}\Big) = B \setminus \bigcup_{n \in \mathbb{N}} g^{-1} C_{n+1} =$$

$$= B \setminus \bigcup_{n \in \mathbb{N}} g^{-1} g f C_n = B \setminus \bigcup_{n \in \mathbb{N}} f C_n = B \setminus f\Big(\bigcup_{n \in \mathbb{N}} C_n\Big) = B \setminus fC.$$

Другими словами, g устанавливает биекцию между $B \setminus fC$ и $A \setminus C$. При этом f устанавливает биекцию между C и fC ■

1.7. Счетные множества. Мы называем множество C *счетным,* если оно конечно[5] или имеет мощность $|\mathbb{N}|$.

1.7.1. Лемма. $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$.

Доказательство. Определим функцию $\iota : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $\iota : (m,n)\mapsto(2m+1)2^n$. Предположим, что $(2m+1)2^n = (2m'+1)2^{n'}$ и $n\leqslant n'$. Тогда $2m+1=(2m'+1)2^{n'-n}$. Отсюда заключаем, что $n=n'$, поскольку $2m+1$ было бы четным в противном случае. Значит, $2m+1=2m'+1$, что влечет $m=m'$. Другими словами, функция ι инъективна. Остается применить теорему 1.6.3 ■

Следующие упражнения используют теорему 1.6.3 и лемму 1.7.1.

1.7.2. Упражнение. Почему объединение $\bigcup\limits_{n\in\mathbb{N}} C_n$ счетно, если каждое C_n счетно?

1.7.3. Упражнение. Покажите, что множества $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{Q}[x]$ счетны. Здесь $\mathbb{Q}[x]$ обозначает множество всех *многочленов от одной переменной* x с коэффициентами из $\mathbb{Q}$, то есть множество всех формальных выражений вида $q_0+q_1x+\dots+q_nx^n$, где $q_0,q_1,\dots,q_n\in\mathbb{Q}$ и $n\in\mathbb{N}$ варьируются.

1.7.4. Упражнение.* Докажите, что $|\mathbb{R}| = |2^{\mathbb{N}}|$.

1.8. Аксиома выбора. Эта аксиома (АВ) утверждает, что всякая сюръективная функция $f : D\to C$ обладает правой обратной $g : D\leftarrow C$, то есть $f\circ g = 1_C$ (см. упражнение 1.5.1). Другими словами, функция g реализует выбор $g(c)$ элемента в непустом для каждого $c\in C$ прообразе $f^{-1}c$. АВ кажется очевидной, однако имеет некоторые удивительные последствия. Например, АВ влечет, что шар радиуса 1 в $\mathbb{R}^3$ можно разрезать на 5 дизъюнктных подмножеств и передвинуть их как твердые тела в $\mathbb{R}^3$ так, чтобы в результате получились два дизъюнктных шара радиуса 1 (парадокс Банаха–Тарского). С другой стороны, если принять АВ, то ничего плохого не произойдет: если вдруг получится противоречие, то его можно было получить и без АВ. Тем не менее, многие математики избегают пользоваться АВ, поскольку доказательства, использующие АВ, в высокой степени неконструктивны, то есть апеллируют к неявно сконструированным объектам и, кроме того, вовлекают произвольный выбор.[6]

В дальнейшем мы принимаем АВ.

2. Отношения

Человек воспитанный никогда не напишет
эпиграф под таким заголовком
— Ч. Воспитанный

2.1. Соответствия. Пусть $C_1,\dots,C_n$ — множества. Подмножество $R\subset C_1\times\dots\times C_n$ называется *n-арным соответствием.* Вместо $(c_1,\dots,c_n)\in R$ иногда пишут $R(c_1,\dots,c_n)$ и говорят, таким образом, что $R(c_1,\dots,c_n)$ *выполнено.* В случае $C := C_1=\dots=C_n$, получаем *n-арное отношение* на множестве C. Для бинарного соответствия $R\subset C_1\times C_2$

[5] Вопреки стандартной терминологии, предполагающей бесконечность счетных множеств, часто удобнее считать счетными и конечные множества.

[6] В какой-то момент мы поймем, что надо по мере возможностей избегать случайного выбора в математике.

часто используют обозначение c_1Rc_2 вместо $R(c_1,c_2)$. Когда мы сопоставляем функции $f : D \to C$ ее график $\Gamma_f \subset D\times C$, мы фактически интерпретируем функцию как бинарное соответствие. В этом смысле, бинарное отношение равенства $=$ на множестве C, называемое также *диагональю* $\Delta_C \subset C \times C$, соответствует тождественной функции $1_C : C \to C$.

С каждым бинарным соответствием $R \subset C_1 \times C_2$ связано *обратное* соответствие $R^{-1} \subset C_2\times C_1$, являющееся образом соответствия R относительно очевидной биекции $C_1\times C_2 \xrightarrow{\sigma} C_2 \times C_1$, $(c_1,c_2) \overset{\sigma}{\longmapsto} (c_2,c_1)$, то есть $R^{-1} := \sigma R$.

Пусть $C_1\times C_2 \supset R_1$ и $C_2\times C_3 \supset R_2$ — бинарные соответствия. *Композиция* или *суперпозиция* $R_2\circ R_1$ соответствий R_1 и R_2 — это бинарное соответствие определенное формулой $R_2 \circ R_1 := \big\{(c_1,c_3) \in C_1 \times C_3 \mid \exists c_2 \in C_2\ c_1R_1c_2 \wedge c_2R_2c_3\big\}$. Нетрудно видеть, что график композиции функций — это композиция графиков, то есть $\Gamma_{f_2}\circ\Gamma_{f_1} = \Gamma_{f_2\circ f_1}$ для функций $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3$. Кроме того, $\Gamma_b^{-1} = \Gamma_{b^{-1}}$ для любой биекции b.

2.2. Отношения эквивалентности. Довольно часто, когда мы утверждаем, что математические объекты равны, мы не имеем в виду, что они абсолютно равны. Вполне возможно, что мы думаем о “равенстве в некотором смысле”, считая несущественными некоторые аспекты изучаемых объектов. Бинарное отношение эквивалентности, определяемое ниже, формализует эту точку зрения.

2.2.1. Определение. Пусть $\sim$ — бинарное отношение на множестве C. Мы говорим, что $\sim$ — *отношение эквивалентности* (или просто *эквивалентность*) на C, если оно *рефлексивно, симметрично* и *транзитивно.* Это означает, что

- $\forall c \in C\ c \sim c$ (*рефлексивность*);
- $\forall c_1,c_2 \in C\ c_1 \sim c_2 \Rightarrow c_2 \sim c_1$ (*симметричность*);
- $\forall c_1,c_2,c_3 \in C\ (c_1 \sim c_2 \wedge c_2 \sim c_3) \Rightarrow c_1 \sim c_3$ (*транзитивность*).

В терминах пункта 2.1, перечисленные свойства переписываются так: $\Delta_C \subset\sim$, $\sim^{-1}\subset\sim$ и $\sim\circ\sim\subset\sim$.

Если $\sim$ — эквивалентность на множестве C и $C \supset S$ — подмножество, то на множестве S имеется *индуцированная эквивалентность* $\sim|_S$. Обычно эта эквивалентность обозначается тем же символом $\sim$.

2.2.2. Определение. *Разбиение* множества C — это разложение C в дизъюнктное объединение непустых подмножеств $C = \bigsqcup\limits_{i\in I} C_i$ такое, что $C_i \ne C_{i'}$ для любых различных $i, i' \in I$, $i \ne i'$. Эквивалентно: произвольное разбиение множества C можно интерпретировать как сюръекцию $f : C \to I$; при этом $C_i := f^{-1}i$ для любого $i \in I$.

2.2.3. Определение. Пусть $\sim$ — эквивалентность на множестве C, и пусть $c \in C$. Тогда множество $[c] := \{x \in C \mid c \sim x\}$ называется *классом эквивалентности* по отношению к $\sim$, и произвольный элемент $x \in [c]$ является *представителем* этого класса.

2.2.4. Лемма. *Пусть $\sim$ — эквивалентность на множестве C, и пусть $C \supset K,K'$ — классы эквивалентности по отношению к $\sim$. Тогда*

1. $K \ne \varnothing$,
2. $K = [c']$ *для любого* $c' \in K$,
3. $K = K'$ *или* $K \cap K' = \varnothing$.

Другими словами, классы эквивалентности образуют разбиение множества C.

Доказательство. 1. Поскольку $K = [c]$ для некоторого $c \in C$, имеем $c \in K$ ввиду рефлексивности отношения $\sim$.

2. Если $K = [c]$ и $c' \in K$, то $c \sim c'$. Это влечет $[c] \supset [c']$. Действительно, если $x \in [c']$, то $c' \sim x$ и, благодаря транзитивности отношения $\sim$, получаем $c \sim x$, то есть $x \in [c]$. Поскольку $\sim$ симметрично, имеем $[c] \subset [c']$. Следовательно, $[c] = [c']$.

3. Если $K \cap K' \neq \varnothing$, то существует элемент $c' \in K \cap K'$. Пункт 2 влечет $K = [c'] = K'$ ■

2.2.5. Определение. Пусть $\sim$ — эквивалентность на множестве C. Сюръективная функция $\pi : C \to C/{\sim}$, $\pi : c \mapsto [c]$, связанная с разбиением множества C на классы эквивалентности по отношению к $\sim$, называется *канонической проекцией* множества C на *фактор-множество* $C/{\sim}$ множества C по отношению к эквивалентности $\sim$; здесь *фактор* $C/{\sim}$ образован всеми классами эквивалентности, как элементами, $C/{\sim} := \big\{[c] \mid c \in C\big\}$.

2.2.6. Заключение. В действительности, нет никакой разницы между эквивалентностью на данном множестве C, разбиением множества C и сюръекцией из C на какое-то множество. Это один и тот же объект, рассматриваемый с разных сторон.

2.2.7. Упражнение. Дана функция $D \xrightarrow{f} C$. Докажите, что существуют единственные эквивалентность $\sim$ на D и инъекция $(D/{\sim}) \xhookrightarrow{\bar f} C$ такие, что $f = \bar f \circ \pi$, где $\pi : D \to D/{\sim}$ — каноническая проекция.

$$\begin{tikzcd} & C \\ D \arrow[ur, "f"] \arrow[r, "\pi"'] & D/{\sim} \arrow[u, "\bar f"'] \end{tikzcd}$$

2.2.8. Эквивалентность, порожденная бинарным отношением. Пусть $E_i \subset C \times C$, $i \in I$, — семейство эквивалентностей на множестве C. Легко видеть, что $\bigcap\limits_{i\in I} E_i$ — эквивалентность.

Рассмотрим произвольное бинарное отношение $R \subset C \times C$ на множестве C. Тогда $\hat R := \bigcap\limits_{\substack{\text{эквива-}\\ \text{лентность}\\ E \supset R}} E$ — это наименьшая эквивалентность содержащая R. Такая эквивалентность $\hat R$ называется *эквивалентностью порожденной* отношением R.

Эквивалентность $\hat R$ можно описать явно. Бинарное отношение $\bar R := \Delta_C \cup R \cup R^{-1}$ уже является рефлексивным и симметричным. Остается декларировать, что $c\hat R c'$ выполнено тогда, и только тогда, когда существуют $n \in \mathbb{N}$ и $c_1, \dots, c_n \in C$ такие, что $c = c_1$ и $c_n = c'$, причем $c_i \bar R c_{i+1}$ справедливо для всех $i = 1, \dots, n-1$. Таким образом, эквивалентность порожденная бинарным отношением R — это просто замыкание отношения R в соответствии с рефлексивностью, симметричностью и транзитивностью.

2.3. Отношения порядка. Отношения (частичного) порядка встречаются довольно часто. Типичный примером является отношение порядка на подмножествах данного множества, заданное включением подмножеств.

2.3.1. Определение. Бинарное отношение $\leqslant$ на множестве C называется *отношением частичного порядка* (или просто *порядком*) на C, а само множество C называется (*частично*) *упорядоченным,* если это отношение является *рефлексивным, антисимметричным* и *транзитивным.* Это означает, что

- $\forall c \in C\ c \leqslant c$ (*рефлексивность*);
- $\forall c_1, c_2 \in C\ (c_1 \leqslant c_2 \wedge c_2 \leqslant c_1) \Rightarrow c_1 = c_2$ (*антисимметричность*);
- $\forall c_1, c_2, c_3 \in C\ (c_1 \leqslant c_2 \wedge c_2 \leqslant c_3) \Rightarrow c_1 \leqslant c_3$ (*транзитивность*).

Эквивалентно: $\leqslant$ — порядок тогда, и только тогда, когда $\leqslant \cap \leqslant^{-1} = \Delta_C$ и $\leqslant \circ \leqslant \subset \leqslant$.

Ясно, что отношение $\leqslant^{-1}$ противоположное порядку $\leqslant$ тоже является порядком. Это позволяет дуализировать все понятия, рассмотрения, утверждения etc., касающиеся отношения порядка, то есть делать то же самое, но для противоположного порядка.

Имеется пара стандартных соглашений касающихся отношений порядка. Иногда мы пишем $c_2 \geqslant c_1$ вместо $c_1 \leqslant c_2$. Наряду с отношением порядка $c_1 \leqslant c_2$, мы используем отношение *строгого порядка* $c_1 < c_2$, которое означает $c_1 \leqslant c_2 \wedge c_1 \neq c_2$.

Если $\leqslant$ — порядок на множестве C и $C \supset S$ — подмножество, то на множестве S имеется *индуцированный порядок* $\leqslant |_S$. Обычно этот порядок обозначается тем же символом $\leqslant$.

2.3.2. Упражнение. Опишите строгий порядок аксиоматически.

2.3.3. Определение. Если $S \subset C$ и $c \in C$, то пишем $S \leqslant c$ и говорим, что c — *верхняя грань* подмножества S, если $\forall s \in S\ s \leqslant c$. *Нижняя грань* — это понятие двойственное понятию верхней грани. Мы пишем $S < c$, если $\forall s \in S\ s < c$ (аналогично для $c < S$).

2.3.4. Определение. Элемент $m \in C$ упорядоченного множества C называется *максимальным,* если $\forall c \in C\ m \leqslant c \Rightarrow m = c$ и *наибольшим,* если $C \leqslant m$. Аналогично определяются *минимальный* и *наименьший* элементы. В ряде случаев, когда $C \ni c$ — очевидный наибольший (наименьший) элемент, слова “максимальный (минимальный) элемент множества C” означают “максимальный (минимальный) элемент множества $C \setminus c$”.

2.3.5. Определение. Мы говорим, что порядок $\leqslant$ на множестве C является *линейным* или что C *линейно упорядоченно,* если $\forall c_1, c_2 \in C\ c_1 \leqslant c_2 \vee c_1 \geqslant c_2$. Подмножество $S \subset C$ является *цепью,* если S линейно упорядоченно относительно индуцированного порядка.

2.3.6. Определение. Мы говорим, что порядок $\leqslant$ на множестве C удовлетворяет *условию обрыва убывающих цепей* или *условию минимальности* или *условию индуктивности,* если любое непустое подмножество S множества C, $\varnothing \neq S \subset C$, обладает минимальным в S элементом. В этом случае, упорядоченное множество иногда называют *фундированным множеством.* Аналогично формулируется дуальное *условие обрыва возрастающих цепей* или *условие максимальности.* Такие условия позволяют действовать (доказывать, определять, строить etc.) по индукции. Например, обычный порядок на $\mathbb{N}$ удовлетворяет условию минимальности, и на этом основывается знаменитый метод математической индукции.

Линейный порядок удовлетворяющий условию минимальности называется *полным,* а соответствующее упорядоченное множество — *вполне упорядоченным.*

Для линейно упорядоченного множества C, обозначим через

$$[c_1, c_2]_C := \{x \in C \mid c_1 \leqslant x \leqslant c_2\}, \qquad]c_1, c_2[_C := \{x \in C \mid c_1 < x < c_2\},$$

$$[c_1, c_2[_C := \{x \in C \mid c_1 \leqslant x < c_2\}, \qquad]c_1, c_2]_C := \{x \in C \mid c_1 < x \leqslant c_2\}$$

замкнутый, открытый и *полуоткрытые сегменты* множества C ограниченные элементами $c_1, c_2 \in C$.

2.3.7. Лемма. *Частичный порядок $\leqslant$ на множестве C удовлетворяет условию максимальности тогда, и только тогда, когда любая возрастающая последовательность элементов C стабилизируется. Это означает, что, для любого семейства $c_i \in C$, $i \in \mathbb{N}$, такого, что $c_i \leqslant c_{i+1}$ для всех $i \in \mathbb{N}$, существует $n \in \mathbb{N}$ такой, что $c_j = c_n$ для всех $j \geqslant n$.*

Доказательство. Предположим, что порядок $\leqslant$ удовлетворяет условию максимальности. Пусть $c_i \in C$, $i \in \mathbb{N}$, семейство такое, что $c_i \leqslant c_{i+1}$ для всех $i \in \mathbb{N}$. Тогда подмножество

$S := \{c_i \mid i \in \mathbb{N}\}$ обладает максимальным элементом $c_n \in S$. Очевидно, $c_j = c_n$ для всех $j \geqslant n$.

Теперь предположим, что любая возрастающая последовательность в C стабилизируется, и пусть $\varnothing \neq S \subset C$ — непустое подмножество не обладающее максимальным элементом. Поскольку $S \neq \varnothing$, существует $c_0 \in S$. Будучи c_0 не максимальным в S, существует $c_1 \in S$ такой, что $c_0 < c_1$, и так далее. Таким образом, мы построим возрастающую последовательность $c_0 < c_1 < \dots < c_i < c_{i+1} < \dots$, которая не стабилизируется ■

Пусть $(D, \leqslant)$ и $(C, \leqslant)$ — упорядоченные множества. Функция $D \xrightarrow{f} C$ называется *монотонной* или *морфизмом,* если

$$\forall d_1, d_2 \in D\ d_1 \leqslant d_2 \Rightarrow f(d_1) \leqslant f(d_2).$$

Изоморфизм между упорядоченными множествами — это такая биекция f, что обе функции f и f^{-1} являются монотонными. Мы можем представлять, что изоморфизм $D \xrightarrow{f} C$ производит из упорядоченного множества D некоторую его копию C, то есть f как бы изготавливает упорядоченное множество D из другого материала, и в результате получается упорядоченное множество C.

До конца пункта 2.3 под словами “начальный сегмент вполне упорядоченного множества” $(C, \leqslant)$ мы для краткости будем понимать либо полуоткрытый сегмент $[m, c[_C$, где $C \ni m$ минимальный в C и $c \in C$, либо все C. Любой замкнутый начальный сегмент $[m, c]_C$ в этой ситуации является (полуоткрытым) начальным сегментом.

2.3.8. Лемма. *Пусть C_1 и C_2 — вполне упорядоченные множества. Тогда одно из C_1 и C_2 изоморфно начальному сегменту другого. Такой изоморфизм единственен* (*с точностью до взятия обратного, если C_1 и C_2 изоморфны*).

Доказательство. Обозначим через $m_i \in C_i$ наименьший элемент в C_i.
Рассмотрим множество изоморфизмов

$$F := \{S_1 \xrightarrow{f} S_2 \mid f \text{ — изоморфизм, } C_i \supset S_i \text{ — начальный сегмент, } i = 1, 2\}$$

между начальными сегментами в C_1 и в C_2.

Докажем, что изоморфизм $f \in F$ однозначно определяется своим сегментом S_1; в частности, если $f, f' \in F$, то один из f и f' является продолжением другого. В самом деле, пусть $S_1 \xrightarrow{f} S_2$ и $S_1 \xrightarrow{f'} S'_2$ — различные изоморфизмы, и пусть $S_1 \ni s_1$ — минимальный такой, что $f(s_1) \neq f'(s_1)$. Тогда f и f' совпадают на $[m_1, s_1[_{C_1}$. Изоморфизмы f и f' отображают s_1, наименьший элемент не принадлежащий $[m_1, s_1[_{C_1}$, в наименьший элемент, не принадлежащий $f[m_1, s_1[_{C_1} = f'[m_1, s_1[_{C_1}$. Противоречие.

Все $f \in F$ согласованы, поэтому существует $f \in F$ с наибольшими S_1 и S_2. При $S_1 = C_1$ или $S_2 = C_2$, искомый изоморфизм — это f (или его обратный). В противном случае, изоморфизм f имеет вид $[m_1, c_1[_{C_1} \xrightarrow{f} [m_2, c_2[_{C_2}$ с $c_i \in C_i$ и, следовательно, индуцирует изоморфизм $[m_1, c_1]_{C_1} \to [m_2, c_2]_{C_2}$, что противоречит максимальности S_i ■

2.3.9. Теорема (лемма Цорна)**.** *Пусть* $(C, \leqslant)$ *— частично упорядоченное множество такое, что любая вполне*[7] *упорядоченная цепь в* C *обладает в* C *верхней гранью. Тогда для любого* $c_0 \in C$ *существует элемент* $m \in C$*, максимальный в* C*, такой, что* $c_0 \leqslant m$*.*

Доказательство. Рассматривая множество $\{x \in C \mid c_0 \leqslant x\}$ вместо C, можно предполагать, что $c_0 \leqslant C$, и доказывать, что C обладает максимальным элементом. Предположим, что такой элемент отсутствует в C.

Обозначим через $\mathcal{T} \subset 2^C$ множество $\mathcal{T} := \{T \mid C \supset T$ — вполне упорядоченная цепь$\}$ всех вполне упорядоченных цепей в C. По условию теоремы, для каждого $T \in \mathcal{T}$, существует $c' \in C$ такой, что $T \leqslant c'$. Но c' не максимален в C. Значит существует $c \in C$ такой, что $c' < c$. Поэтому, $T < c$.

Мы только что заметили, что ограничение $\mathcal{T} \xleftarrow{f} \mathcal{S}$ проекции $\mathcal{T} \leftarrow \mathcal{T} \times C$ на подмножество $\mathcal{S} \subset \mathcal{T} \times C$, заданное равенством $\mathcal{S} := \big\{(T, c) \in \mathcal{T} \times C \mid T < c\big\}$, — сюръективно. В силу АВ, существует правая обратная к функции f функция $g : \mathcal{T} \to \mathcal{S}$, $f \circ g = 1_{\mathcal{T}}$. Компонируя функцию g с проекцией $\mathcal{T} \times C \to C$, получаем функцию $c : \mathcal{T} \to C$, удовлетворяющую $T < c(T)$ для любого $T \in \mathcal{T}$. Можно предполагать, что $c(\varnothing) = c_0$.

Пусть $\mathcal{T}_0 := \big\{T \in \mathcal{T} \mid c_0 \in T \wedge \forall t \in T\ c[c_0, t[_T = t\big\}$. Тогда $\{c_0\} \in \mathcal{T}_0$, поскольку $c(\varnothing) = c_0$. Если $T, T' \in \mathcal{T}_0$, то для произвольных $t \in T$ и $t' \in T'$ равенство $[c_0, t[_T = [c_0, t'[_{T'}$ влечет равенство $t = t'$ по определению множества $\mathcal{T}_0$.

Покажем, что один из произвольных $T, T' \in \mathcal{T}_0$ является начальным сегментом другого. (В частности, $\mathcal{T}_0$ будет цепью относительно включения.)

Действительно, в случае когда, например, $T \subsetneq T'$, существует минимальный элемент $t' \in T' \backslash T$ в силу условия минимальности для T'. Ясно, что $[c_0, t'[_{T'} \subset T$. Если $[c_0, t'[_{T'} \neq T$, то существует минимальный элемент $t \in T \setminus [c_0, t'[_{T'}$ в силу условия минимальности для T. Тогда $[c_0, t'[_{T'} = [c_0, t[_T$, в силу выбора t и поскольку $t > [c_0, t'[_{T'} \subset T$ справедливо благодаря включению $T \subset T'$; это влечет $t = t'$, противоречие. Значит, $T = [c_0, t'[_{T'}$.

В случае, когда $T \not\subset T'$ и $T' \not\subset T$, существуют минимальные элементы $t \in T \setminus T'$ и $t' \in T' \setminus T$ в силу условия минимальности для T и для T'. Ясно, что $[c_0, t[_T \subset T'$ и $[c_0, t'[_{T'} \subset T$. Если $[c_0, t[_T = [c_0, t'[_{T'}$, то $t = c[c_0, t[_T = c[c_0, t'[_{T'} = t' \in T \cap T'$ по определению множества $\mathcal{T}_0$; противоречие. Поэтому и ввиду симметрии между T и T', мы можем предполагать, что существует минимальный элемент $t_0 \in [c_0, t[_T \setminus [c_0, t'[_{T'}$, используя условие минимальности для T. Мы видим, что $[c_0, t_0[_T \setminus [c_0, t'[_{T'} = \varnothing$, то есть, $[c_0, t'[_{T'} \supset [c_0, t_0[_T$. Из $t_0 \notin [c_0, t'[_{T'}$, $t_0 \in [c_0, t[_T \subset T'$ и $t' \in T' \in \mathcal{T}$ следует $t' \leqslant t_0$. Поэтому из $[c_0, t'[_{T'} \subset T$ заключаем, что $[c_0, t'[_{T'} \subset [c_0, t_0[_T$. Как и выше, $[c_0, t'[_{T'} = [c_0, t_0[_T$ влечет $t' = t_0 \in T$. Противоречие.

Покажем теперь, что $T' := \bigcup\limits_{T \in \mathcal{T}_0} T \in \mathcal{T}_0$. Будучи $\mathcal{T}_0$ цепью относительно включения, порядок на T' линеен. Для того, чтобы проверить условие минимальности для T', используем утверждение дуальное лемме 2.3.7. Дано семейство $t_i \in T'$, $i \in \mathbb{N}$, такое, что $t_i \geqslant t_{i+1}$ для любого $i \in \mathbb{N}$. Для некоторых $T_i \in \mathcal{T}_0$, имеем $t_i \in T_i$. Поскольку один из T_0, T_i является начальным сегментом другого, то $t_i \in T_0$ (если T_0 — начальный сегмент в T_i, это следует

[7]Стандартная версия леммы Цорна требует существования верхней грани в множестве C для произвольной, необязательно вполне упорядоченной, цепи содержащейся в C. Представленная версия вместе с ее доказательством принадлежат Мише Вербицкому.

из $t_i \leqslant t_0$). Обсуждаемая последовательность стабилизируется благодаря условию минимальности для T_0. Наконец, пусть $t' \in T'$. Тогда $t' \in T$ для некоторого $T \in \mathcal{T}_0$. Только что использованные аргументы влекут $[c_0, t'[_{T'} = [c_0, t'[_T$. Отсюда $c[c_0, t'[_{T'} = c[c_0, t'[_T = t'$.

Остается заметить, что $T' \subsetneq T' \sqcup \big\{c(T')\big\} \in \mathcal{T}_0$. Противоречие ■

2.3.10. Упражнение (теорема Цермело)**.*** Докажите, что любое множество может быть вполне упорядочено.

2.3.11. Упражнение. Докажите, что для любых мощностей c_1 и c_2 справедливо $c_1 \leqslant c_2$ или $c_1 \geqslant c_2$.

2.3.12. Кардиналы, ординалы и трансфинитная индукция. *Кардинал* — это синоним мощности, то есть это множество рассматриваемое с точностью до биекции. Аналогично, *ординал* — это вполне упорядоченное множество рассматриваемое с точностью до изоморфизма.

В силу леммы 2.3.8, имеется линейный порядок[8] между ординалами: если вполне упорядоченное множество A изоморфно начальному сегменту другого вполне упорядоченного множества B, то соответствующие ординалы подвержены порядку $\alpha \leqslant \beta$. Каждое натуральное число можно считать конечным ординалом. Множество $\mathbb{N}$ со своим обычным порядком представляет собой наименьший бесконечный ординал, обычно обозначаемый символом ω. Легко понять, что порядок на ординалах удовлетворяет условию обрыва убывающих цепей.

В терминах порядка на ординалах, вполне упорядоченное множество $[0, \alpha[$ представляет ординал α. В самом деле, предполагая α минимальным с тем свойством, что $[0, \alpha[$ не представляет ординал α, обозначим через β ординал множества $[0, \alpha[$, и пусть A — вполне упорядоченное множество, представляющее ординал α. Если $\beta < \alpha$, то $[0, \beta[$ представляет ординал β в силу минимальности α. Из того, что $[0, \alpha[$ представляет ординал β, получаем изоморфизм между $[0, \beta[$ и $[0, \alpha[$, что противоречит лемме 2.3.8. Если $\alpha < \beta$, то A изоморфно собственному начальному сегменту множества $[0, \alpha[$, скажем, сегменту $[0, \gamma[$, где $\gamma < \alpha$. В силу выбора α, сегмент $[0, \gamma[$ представляет ординал γ. С другой стороны, он изоморфен A и поэтому представляет ординал α. Противоречие.

Допуская некоторую вольность в обозначениях, мы можем записать только что доказанный факт в виде тождества $[0, \alpha[= \alpha$.

С ординалами можно совершать различные операции. Пусть A и B — вполне упорядоченные дизъюнктные множества соответствующие ординалам α и β. Декларируя, что $A < B$, получаем полный порядок на множестве $A \sqcup B$, то есть ординал $\alpha + \beta$. На множестве $A \times B$ определим *лексикографический*[9] порядок, полагая $(a_1, b_1) \leqslant (a_2, b_2)$, когда $b_1 < b_2$ или $b_1 = b_2$ вместе с $a_1 \leqslant a_2$. Легко проверить, что лексикографический порядок является полным. Таким образом получается ординал $\alpha \cdot \beta$. Только что определенные операции довольно экзотичны: сложение и умножение некоммутативны (но ассоциативны). Можно было бы определить также и ординал α^β, но нам это не понадобится.

Ординал $\alpha + 1$ называется *следующим* за ординалом α и ординал α называется *предшествующим* ординалу $\alpha + 1$. Ординал не обладающий предшествующим ординалом называется *предельным.* (Следовательно, ординал 0 является предельным.)

---

[8] Принимая во внимание, что все ординалы образуют не множество, а класс.

[9] Дословно такое же определение задает *лексикографический* порядок на произведении произвольных упорядоченных множеств.

Трансфинитная индукция фактически опирается на теорему Цермело. Например, если мы собираемся доказать свойство $P(c)$ элементов множества C, то сначала "занумеровываем" множество C при помощи начального сегмента ординалов, $C = \{c_\alpha \mid \alpha < \beta\}$ для некоторого ординала β. Затем мы доказываем импликацию $\big(\forall\gamma < \alpha\ P(c_\gamma)\big) \Rightarrow P(c_\alpha)$ для каждого ординала $\alpha < \beta$. Эта импликация при $\alpha = 0$ сводится к справедливости *основания* индукции $P(c_0)$.

Сопоставляя каждому кардиналу наименьший ординал соответствующей мощности, заключаем, что кардиналы вполне упорядочены.

2.3.13. Лемма.[10] *Если C — бесконечное множество, то $|C \times \mathbb{N}| = |C|$. Следовательно, $|C_1| + |C_2| = \max\big(|C_1|, |C_2|\big)$, если одно из множеств C_1 и C_2 бесконечно.*

Доказательство. По теореме Цермело, можно предполагать, что C вполне упорядочено. Как выше, обозначим $c + 1 := \min\{x \in C \mid c < x\}$ если $C \ni c$ не максимальный в C, называя элемент c предшествующим элементу $c + 1$. Обозначим по индукции $c + 0 := c$, $c + (n + 1) := (c + n) + 1$ для $c \in C$ и $n \in \mathbb{N}$, если $c + n$ не максимален в C. Обозначим через $L \subset C$ множество всех предельных элементов множества C, то есть элементов, не обладающих предшествующим. Легко видеть, что каждый элемент $c \in C$ однозначно записывается в виде $c = l + n$, где $l \in L$ и $n \in \mathbb{N}$. И, наоборот, если $L \ni l$ не максимальный в L, то для любого $n \in \mathbb{N}$ существует элемент $l + n \in C$. Исключая из множества L его максимальный элемент, если он существует, обозначим оставшееся множество через $L_0 \subset L$. Итак, мы имеем биекцию $b : (L_0 \times \mathbb{N}) \sqcup F \to C$ такую, что $b : (l, n) \mapsto l + n$ для любых $l \in L_0$ и $n \in \mathbb{N}$, где F — подходящее конечное множество (непустое в точности, когда L обладает максимальным элементом). Остается заметить, что $|C \times \mathbb{N}| = |L_0 \times \mathbb{N} \times \mathbb{N}| + |F \times \mathbb{N}| = |L_0 \times \mathbb{N}| + |F \times \mathbb{N}| = |C|$ по лемме 1.7.1, поскольку C бесконечно, $|\varnothing \times \mathbb{N}| = 0$ и $|F \times \mathbb{N}| = |\mathbb{N}|$ если $F \neq \varnothing$ ∎

2.3.14. Упражнение.* Покажите, что $|C| = |C \times C|$, если множество C бесконечно. Заметьте, что $|C_1| \cdot |C_2| = \max\big(|C_1|, |C_2|\big)$, если $C_1 \neq \varnothing$ и C_2 бесконечно.

2.4. Предпорядок. Опуская второе требование в определении порядка 2.3.1, приходим к понятию *предпорядка.* Фактически, это понятие является гибридом понятий эквивалентности и порядка. В самом деле, пусть $\leqslant$ — предпорядок на C. Мы можем легко проверить, что бинарное отношение $c_1 \leqslant c_2 \wedge c_2 \leqslant c_1$ (это бинарное отношение $\leqslant \cap \leqslant^{-1}$), обозначаемое символом $\sim$, является эквивалентностью.

На фактор-множестве $C/{\sim}$ имеется естественный порядок: $[c_1] \preccurlyeq [c_2]$ выполнено в точности, когда $c_1 \leqslant c_2$. Это определение корректно: если $c_1' \sim c_1$, $c_1 \leqslant c_2$ и $c_2 \sim c_2'$, то $c_1' \leqslant c_1$ и $c_2 \leqslant c_2'$ влекут $c_1' \leqslant c_2'$. Рефлексивность и транзитивность отношения $\preccurlyeq$ легко проверяются на уровне представителей. Если $[c_1] \preccurlyeq [c_2]$ и $[c_2] \preccurlyeq [c_1]$, то $c_1 \leqslant c_2$ и $c_2 \leqslant c_1$. Другими словами, $c_1 \sim c_2$, то есть $[c_1] = [c_2]$.

Обратно, если $f : D \to C$ — сюръекция на частично упорядоченное множество $(C, \preccurlyeq)$, то бинарное отношение $d_1 \leqslant d_2$, выполненное по определению тогда, и только тогда, когда $f(d_1) \preccurlyeq f(d_2)$, является предпорядком на множестве D и соответствующая этому предпорядку эквивалентность задается сюръекцией f.

[10] Теорема 32, заимствованная вместе с доказательством из книги Н.К. Верещагина и А. Шеня "Лекции по математической логике и теории алгоритмов 1. Начала теории множеств", МЦНМО, 2012, стр. 80.

2.4.1. Заключение. В действительности, нет никакой разницы между предпорядком на данном множестве D и сюръекцией из D на какое-то упорядоченное множество. Это один и тот же объект, рассматриваемый с разных сторон.