Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Основы комбинаторики и теории чисел, осень 2021
Лекция 2: отображения и соответствия

Краткое содержание

Понятие соответствия. Понятие отображения. Обозначения. Инъективные и сюръективные соответствия. Инъекции и сюръекции. Биекции. Взаимно однозначные отображения. Понятия образа и прообраза множества при соответствии. Критерий равенства образа пересечения и пересечения образов. Область определения и область значений соответствия. Сужение и продолжение соответствия. Частично определённые функции. Композиция соответствий, её ассоциативность и некоммутативность. Тождественное отображение. Обратное соответствие. Возведение соответствия в степень. Возведение множества в степень другого множества. Булеан. Свойства возведения множества в степень. Пустое множество в роли основания и показателя возведения в степень.

Эта лекция целиком будет состоять из определений и простых утверждений, из них вытекающих. Мы поговорим о соответствиях, отображениях и связанных понятиях. Они немного по-разному определяются в разных источниках, поэтому нужно договориться о терминологии.

1 Основные виды соответствий и отображений

Определение 1. *Соответствием* между множествами A и B называют произвольное подмножество декартова произведения $F \subset A \times B$.

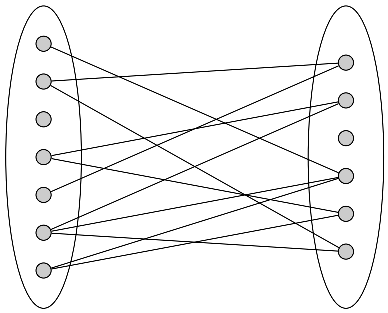
При этом множества A и B понимаются несимметрично: вместо того, чтобы говорить, что элементы $a \in A$ и $b \in B$ соответствуют друг другу, говорят, что элементу a соответствует элемент b (или несколько разных элементов, или ни одного). Эту асимметрию подчёркивают обозначениями: вместо $F \subset A \times B$ пишут $F\colon A \to B$, а вместо $(a, b) \in F$ пишут $b \in F(a)$. В последнем случае $F(a)$ выступает как множество всех элементов B, соответствующих данному a.

Определение 2. *Отображением* из множества A в множество B называется однозначное соответствие между A и B, т.е. такое соответствие, что для любого $a \in A$ найдётся ровно одно $b \in B$, соответствующее a.

Для отображения тоже используют запись $F\colon A \to B$, а про отдельные элементы пишут $b = F(a)$ или $F\colon a \mapsto b$. Отображения также называют *функциями*.

Некоторые авторы произвольное подмножество $A \times B$ называют (бинарным) отношением и пишут aFb. В нашем курсе слово «отношение» будет использоваться только для подмножеств $A \times A$. Также иногда на соответствия накладывают требование непустозначности, при которой каждому a должно соответствовать хотя бы одно b, т.е. $F(a)$ должно быть непустым. Мы этого делать не будем. Соответствия также называют *многозначными функциями* и используют обозначение $F\colon A \rightrightarrows B$, чтобы подчеркнуть многозначность.

Наглядно соответствия можно представлять различными способами:

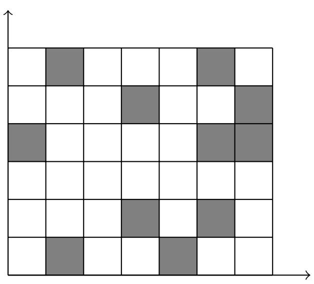


(а) Соответствие произвольного вида

(б) Непустозначное соответствие

(в) Отображение

Рис. 1: Представление соответствий в виде двудольного графа.



(а) Соответствие произвольного вида

(б) Непустозначное соответствие

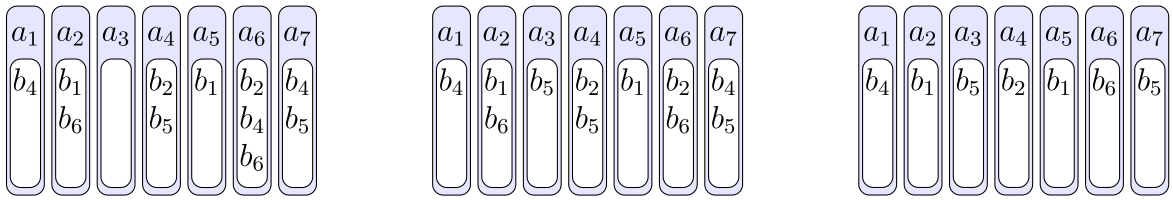
(в) Отображение

Рис. 2: Представление соответствий в виде графиков

- **Представление в виде двудольного графа (см. рис. 1)**. Можно себе представить два облака точек, левое индексировано элементами A, а правое — элементами B. Между некоторыми точками проведены рёбра, но лишь между точками из разных облаков. Ребро между точками a и b будем понимать как признак того, что $b \in F(a)$. Такое представление удобно использовать, когда A и B содержат немного точек. Соответствие будет являться отображением, если из каждого узла слева выходит ровно одно ребро. Соответствие будет непустозначным, если из каждого узла слева выходит хотя бы одно ребро.

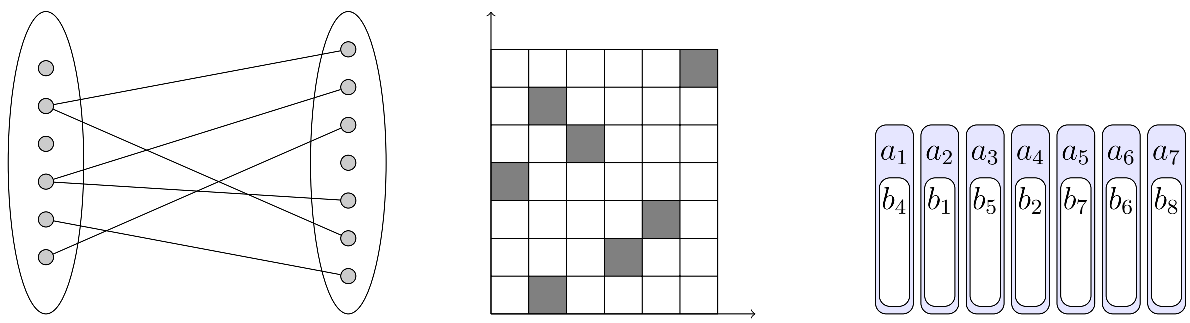
- **Представление в виде графика (см. рис. 2).** Как обычно, по оси абсцисс откладываются элементы множества A, по оси ординат — элементы множества B, закрашиваются пары, соответствующие друг другу. Такое представление удобно использовать, когда A и B либо содержат немного точек (тогда график будет клетчатой таблицей), либо являются подмножествами $\mathbb{R}$. Соответствие будет отображением, когда на каждой вертикали закрашена ровно одна точка/клетка, непустозначным соответствием — когда хотя бы одна.

- **Представление в виде набора контейнеров (см. рис. 3).** Это удобная метафора, которая позволяет наглядно объяснять некоторые утверждения. Нужно представить, что имеется набор контейнеров, индексированных элементами множества A, и в каждом контейнере содержатся какие-то элементы B, возможно,



(а) Соответствие произвольного вида (б) Непустозначное соответствие (в) Отображение

Рис. 3: Представление соответствий в виде набора контейнеров



(а) Инъективное соответствие произвольного вида (б) Инъективное непустозначное соответствие (в) Инъекция

Рис. 4: Примеры инъективных соответствий

повторяющиеся в разных контейнерах. При отображении в каждом контейнере лежит ровно 1 элемент, при непустозначном соответствии — хотя бы один.

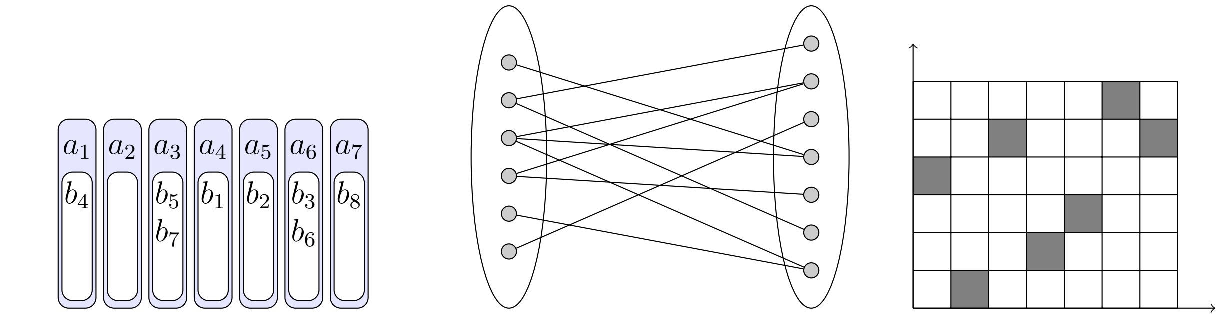
- **Представление в виде «чёрного ящика».** Можно также представлять себе соответствие как «чёрный ящик», который на вход получает x, а на выход выдаёт все элементы $F(x)$. Непустозначность соответствия означает, что на выходе всегда что-то будет, при отображении на выходе будет ровно один элемент.

Определение 3. Соответствие F называется *инъективным*, если для любых $a_1 \neq a_2$ множества $F(a_1)$ и $F(a_2)$ не пересекаются. Инъективное отображение называется *инъекцией*.

Требование инъективности соответствия можно переформулировать так: каждый элемент B соответствует не более, чем одному элементу A. А для отображения достаточно потребовать, чтобы при $a_1 \neq a_2$ было выполнено $F(a_1) \neq F(a_2)$. Иногда для инъекции используют обозначение $F\colon A \hookrightarrow B$. Примеры инъективных соответствий показаны на рис. 4.

Определение 4. Соответствие F называется *сюръективным*, если любой элемент B соответствует хотя бы одному элементу A, т.е. любой $b \in B$ лежит в $F(a)$ для некоторого $a \in A$. Сюръективное отображение называется *сюръекцией*.

Для определения сюръекции можно сказать, что любой элемент b равняется $F(a)$ для некоторого a. Иногда для сюръекции используют обозначение $F\colon A \twoheadrightarrow B$. Примеры сюръективных соответствий показаны на рис. 5.



(а) Сюръективное соответствие произвольного вида (для B из 8 элементов)

(б) Непустозначное сюръективное соответствие

(в) Сюръекция

Рис. 5: Примеры сюръективных соответствий

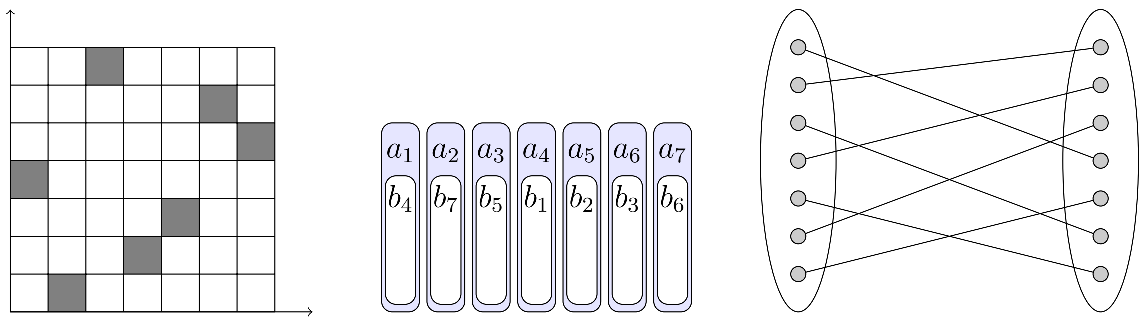


Рис. 6: Примеры биекций

Определение 5. *Биекцией* называется отображение, являющееся одновременно инъекцией и сюръекцией (см. рис. 6).

Тут нужно быть аккуратным: соответствие, являющееся одновременно инъективным и сюръективным, вовсе не обязательно будет биекцией. Ведь оно не обязательно будет отображением. В качестве синонима слова «биекция» используют выражение «взаимно однозначное соответствие». Это объясняется следующим утверждением:

Утверждение 6. *Соответствие является биекцией тогда и только тогда, когда каждому элементу A соответствует ровно один элемент B, а также каждый элемент B соответствует ровно одному элементу A.*

Доказательство. Пусть F является биекцией. Тогда, поскольку оно является отображением, каждому элементу A соответствует ровно один элемент B. Поскольку оно является сюръекцией, каждый элемент B соответствует хотя бы одному элементу A, а поскольку оно является инъекцией, то не более чем одному. Значит, каждый элемент B соответствует ровно одному элементу A, т.е. соответствие является взаимно однозначным.

Обратно, взаимно однозначное соответствие является однозначным, т.е. отображением. А поскольку каждый элемент B соответствует ровно одному элементу A, то оно является одновременно инъективным и сюръективным. А значит, это биекция. □

2 Образ и прообраз. Сужение и продолжение

Определение 7. Пусть $F\colon A \to B$ — соответствие, а $S \subset A$. Тогда *образом* множества S называется множество всех элементов B, соответствующих какому-то элементу S. Формально можно записать так: $F(S) = \bigcup_{s \in S} F(s) \subset B$.

Заметим, что для одноэлементных множеств $F(\{a\}) = F(a)$.

Определение 8. Пусть $F\colon A \to B$ — соответствие, а $T \subset B$. Тогда *прообразом* множества T называется множество элементов A, которым соответствует хотя бы один элемент T. Формально $F^{-1}(T) = \{a\colon F(a) \cap T \neq \varnothing\} \subset A$.

Для отображений определения образа и прообраза можно упростить. Образ можно определить как $F(S) = \{F(s)\colon s \in S\}$, а прообраз — как $F^{-1}(T) = \{a\colon F(a) \in T\}$. В терминах образов и прообразов можно определить инъективность и сюръективность: соответствие инъективно, если образы разных элементов не пересекаются, или, эквивалентно, если прообраз каждого элемента не более чем одноэлементен. Соответствие сюръективно, если образ A равен B, или если прообраз любого элемента непуст.

Замечание 9. Можно было бы определить прообраз T как множество элементов A, образ которых целиком лежит в T. (Можно одновременно потребовать непустоты этого образа). Для отображений все эти варианты определения эквивалентны. Однако указанные варианты обладают неприятным свойством: прообраз непустого множества T может быть пуст, даже если какие-то элементы A соответствуют каким-то элементам T. Кроме того, наше определение позволяет сказать, что прообраз — это то же самое, что образ для обратного отображения (см. ниже).

Про связь понятий образа и прообраза с теоретико-множественными операциями можно доказать много различных утверждений. Приведём для примера одно.

Утверждение 10. *Образ пересечения любых двух множеств равняется пересечению образов тех же множеств тогда и только тогда, когда соответствие инъективно.*

Доказательство. Пусть соответствие не инъективно. Тогда найдутся такие a_1 и a_2, что $F(a_1)$ и $F(a_2)$ пересекаются. Тогда $F(\{a_1\} \cap \{a_2\}) = F(\varnothing) = \varnothing$, но $F(\{a_1\}) \cap F(\{a_2\}) = F(a_1) \cap F(a_2)$ непусто по предположению. Значит, образ пересечения множеств $\{a_1\}$ и $\{a_2\}$ не равен пересечению образов.

Теперь пусть соответствие инъективно. Рассмотрим произвольные подмножества S и Q множества A. Докажем, что $F(S \cap Q) = F(S) \cap F(Q)$. Для этого докажем включение в обе стороны. Вначале пусть $y \in F(S \cap Q)$. Это значит, что $y \in F(x)$ для некоторого $x \in S \cap Q$. Но тогда $x \in S$ и $x \in Q$. А раз $y \in F(x)$, то $y \in F(S)$ и $y \in F(Q)$. Значит, $y \in F(S) \cap F(Q)$. (Заметим, что это включение верно для любых соответствий, не только для инъективных).

Теперь пусть $y \in F(S) \cap F(Q)$. Это значит, что $y \in F(S)$ и $y \in F(Q)$. Значит, $y \in F(x_1)$ для некоторого $x_1 \in S$ и $y \in F(x_2)$ для некоторого $x_2 \in Q$. Но при $x_1 \neq x_2$ в силу инъективности множества $F(x_1)$ и $F(x_2)$ не пересекаются. Но их пересечение содержит по крайней мере y. Значит, $x_1 = x_2 = x$, и $x \in S \cap Q$. А так как $y \in F(x)$, получаем, что $y \in F(S \cap Q)$. $\square$

Определение 11. *Областью определения* соответствия $F\colon A \to B$ называется множество $\operatorname{Dom} F = F^{-1}(B)$. Иными словами, область определения — множество тех элементов A, которым соответствует хотя бы один элемент B.

Определение 12. *Областью значений* соответствия $F\colon A \to B$ называется множество $\operatorname{Ran} F = F(A)$. Иными словами, область определения — множество тех элементов B, которые соответствуют хотя бы одному элементу A.

Заметим, что соответствие сюръективно, если его область значений совпадает с B.

Определение 13. Пусть $F\colon A \to B$ — соответствие, а $S \subset A$. Тогда *сужением* соответствия F на S называется соответствие $F\big|_S\colon S \to B$, принимающее те же значения, что и F, т.е. $b \in F\big|_S(a) \Leftrightarrow b \in F(a)$ для $a \in S$. Само соответствие F по отношению к $F\big|_S$ называют *продолжением*.

Определение 14. Соответствие $F\colon A \to B$ называют *частично определённой функцией*, если $F\big|_{\operatorname{Dom} F}$ — отображение.

Иными словами, при частично определённой функции каждому элементу A либо вообще не соответствует элементов B, либо соответствует ровно один. В теории алгоритмов под функцией мы будем понимать именно частично определённую функцию.

Для частично определённых функций сужение и продолжение могут определять иначе: отображение $F\colon A \to B$ называют сужением отображения $G\colon A \to B$, если $\operatorname{Dom} F \subset \operatorname{Dom} G$ и $F(x) = G(x)$ при $x \in \operatorname{Dom} F$. Соответственно, G в этом случае называется продолжением F. Мы будем использовать такое определение в теории вычислимых функций.

3 Композиция соответствий

Определение 15. Пусть $F\colon A \to B$ и $G\colon B \to C$ — соответствия. Тогда их композицией $G \circ F$ называется соответствие $H\colon A \to C$, определённое правилом: $c \in H(a)$ тогда и только тогда, когда найдётся b, такое что одновременно $c \in G(b)$ и $b \in F(a)$.

Иначе говоря, $(G \circ F)(a) = \bigcup_{b \in F(a)} G(b)$. Для отображений можно написать проще: $(G \circ F)(a) = G(F(a))$. Именно этой формулой объясняется порядок функций в записи: в композиции $G \circ F$ сначала применяется F, а потом G.

Для понимания, что такое композиция, полезна метафора «чёрного ящика»: сначала в чёрный ящик F кладётся a, на выходе получаются элементы $F(a)$. Затем все они по очереди подаются в чёрный ящик G и берётся множество из всех элементов, полученных на выходе.

Композиция соответствий ассоциативна, т.е. для любых трёх соответствий $F\colon A \to B$, $G\colon B \to C$ и $H\colon C \to D$ выполнено $(H \circ G) \circ F = H \circ (G \circ F)$. (Равенство на соответствиях определяется как равенство подмножеств декартова произведения). Проверка этого проста, но занудна, и потому остаётся в качестве упражнения.

Композиция соответствий не обязательно коммутативна. Так, если $C \neq A$, то композиция $F \circ G$ попросту не определена. Если $C = A \neq B$, то композиция $F \circ G$ отображает

B в B, а $G \circ F$ — A в A, т.е. они действуют на разных множествах. И даже если $A = B = C$, то композиции в двух порядках всё равно могут не совпадать: например, если $F(x) = 2x$, а $G(x) = x^2$, то $(G \circ F)(x) = 4x^2$, а $(F \circ G)(x) = 2x^2$.

Определение 16. *Тождественным отображением* на множестве A называется отображение $\mathrm{id}_A \colon A \to A$, заданное формулой $\mathrm{id}_A(x) = x$.

Композиция ведёт себя похоже на умножение, а тождественное отображение исполняет роль единицы: для любого соответствия F выполнены равенства $F \circ \mathrm{id}_A = F$ и $\mathrm{id}_B \circ F = F$. Эти равенства также несложно проверить. Что касается операции, обратной к умножению, то тут всё несколько сложнее.

Определение 17. Пусть $F \colon A \to B$ — соответствие. *Обратным соответствием* называется соответствие $F^{-1} \colon B \to A$, определяемое правилом $a \in F^{-1}(b) \Leftrightarrow b \in F(a)$.

Хотя обратное соответствие можно определить для любого соответствия, условие $F^{-1} \circ F = \mathrm{id}_A$ выполнено только для инъективного и непустозначного соответствия. А условия $F^{-1} \circ F = \mathrm{id}_A$ и $F \circ F^{-1} = \mathrm{id}_B$ одновременно выполнены только для биекций. Зато для любых соответствий выполнено равенство $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.

Наконец, соответствия можно возводить в степень.

Определение 18. Пусть $F \colon A \to A$ — соответствие. Тогда возведение в степень определяется рекурсивно: $F^0 = \mathrm{id}_A$, а далее $F^{n+1} = F \circ F^n$.

Возведение соответствий в степень удовлетворяет равенствам: $F^n \circ F^k = F^{n+k}$ и $(F^n)^k = F^{nk}$. Однако из-за некоммутативности равенство $(F \circ G)^n = F^n \circ G^n$ в общем случае неверно.

4 Возведение множества в степень

Если множество A состоит из n элементов, а множество B — из k элементов, то существует всего k^n различных отображений из A в B: действительно, есть по k вариантов значения для каждого из n элементов A. Это мотивирует следующее определение:

Определение 19. Пусть A и B — два множества. Тогда множеством B^A называется множество всех отображений из A в B.

Если B состоит всего из двух элементов (обозначим их b_1 и b_2), то отображение из A в B задаёт разбиение A на два множества: прообраз b_1 и прообраз b_2. Ясно, что для определения отображения достаточно задать прообраз b_1, ведь тогда прообраз b_2 определится автоматически. Таким образом, отображения из A в двухэлементное множество и подмножества A находятся в естественном взаимно однозначном соответствии между собой. Это мотивирует обозначение в следующем определении:

Определение 20. *Булеаном* множества A называется множество всех подмножеств множества A. Обозначение: $\mathcal{P}(A)$ или 2^A.

При помощи булеана можно сформулировать ещё одну естественную эквивалентность: каждому соответствию A и B соответствует отображение из A в 2^B. Действительно, каждому элементу можно однозначно сопоставить его образ при соответствии.

Возведение множества в степень обладает несколькими стандартными свойствами:

Утверждение 21. *При всех A, B и C выполнены следующие свойства:*

а) $(A \times B)^C \sim A^C \times B^C$;

б) $A^{B \cup C} \sim A^B \times A^C$ (если B и C не пересекаются);

в) $(A^B)^C \sim A^{B \times C}$,

где знак $\sim$ понимается как «элементы двух множеств могут быть естественным образом отождествлены».

Доказательство. Слова «естественным образом» определены нечётко. Формально нужно построить взаимно однозначное соответствие, которое будет в некотором смысле «естественным». Например, можно сказать, что у него есть очень простое описание.

Первая эквивалентность неформально означает, что пара функций это то же самое, что одна функция, принимающая значение среди пар. Это легко объяснить при помощи метафоры с контейнерами. Пара функций — это два набора контейнеров, индексированных элементами C. В каждом контейнере из первого набора лежит элемент A, а в каждом контейнере из второго набора — элемент B. Если переложить все элементы из контейнеров второго набора в соответствующие контейнеры из первого набора, то получится набор контейнеров с парами элементов A и B, что и требовалось.

Формально пусть $F \in (A \times B)^C$. Это значит, что $F\colon C \to A \times B$. То есть каждому элементу $c \in C$ сопоставлена некоторая пара $(a, b) \in A \times B$. Вместо этого ему можно сопоставить отдельно элементы $a \in A$ и $b \in B$. Получится два отображения, первое отображает c в a, а второе — c в b, то есть пара отображений $(F_1, F_2) \in A^C \times B^C$. Можно сказать, что $F_i = \mathrm{pr}_i \circ F$, где pr_i — проектор на i-ю координату: $\mathrm{pr}_i(a_1, a_2) = a_i$. Легко понять, что разные F переводятся в разные пары (F_1, F_2), и каждая пара получается из некоторой функции. Таким образом, первая эквивалентность установлена.

Вторая эквивалентность означает, что определить функцию на несвязном объединении двух множеств это то же самое, что определить её на каждом из этих множеств по отдельности. Метафорически элемент $A^{B \cup C}$ есть набор контейнеров, помеченных элементами B или C. А $A^B \times A^C$ — это два набора контейнеров, в первом они помечены элементами B, а во втором — элементами C. Таким образом, достаточно один набор разбить на два.

Третья эквивалентность означает, что функция двух аргументов есть то же самое, что отображение первого аргумента в функцию, зависящую от второго аргумента. Метафорически есть набор контейнеров, помеченных элементами C, в каждом из которых лежат контейнеры, помеченные элементами B, а уже в каждом из маленьких контейнеров лежит элемент A. Если убрать внешние контейнеры, но при этом перенести с них метки на внутренние, то получится набор контейнеров, помеченных элементами $B \times C$, что и требовалось.

Формальное доказательство последних двух эквивалентностей остаётся в качестве упражнения. $\square$

Закончим лекцию анализом крайнего случая:

Утверждение 22. *Для любого A верно $A^{\varnothing} = \{\varnothing\}$, а при непустом A также верно $\varnothing^{A} = \varnothing$.*

Доказательство. Прежде всего заметим, что $A \times \varnothing = \varnothing$: нет ни одной пары (a, b), такой что $b \in \varnothing$. Аналогично $\varnothing \times A = \varnothing$. Поскольку подмножество у $\varnothing$ ровно одно, а именно $\varnothing$, то есть ровно одно соответствие между $\varnothing$ и A, а также между A и $\varnothing$ — пустое. Нужно лишь понять, будет ли оно отображением.

Если в левой части нет элементов, то пустое множество будет отображением: любому элементу левой части соответствует ровно один элемент правой части. Если же слева хотя бы один элемент есть, то пустое множество отображением уже не будет. Отсюда и получаются оба заявленных утверждения. $\square$

Таким образом, неопределённость 0^0 раскрывается как 1. По крайней мере, если речь идёт о числе элементов множества.