Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Основы комбинаторики и теории чисел, осень 2021
Лекция 1: множества и операции над ними

Краткое содержание

Понятие множества. Задание множества перечислением и определяющим свойством. Отношение подмножества и его свойства: рефлексивность, антисимметричность, транзитивность. Равенство множеств. Пустое множество и его единственность. Парадокс Рассела. Аксиома регулярности и следствия из неё. Операции над множествами: объединение, пересечение, разность, симметрическая разность, дополнение. Диаграммы Эйлера. Тождества: коммутативность, ассоциативность, дистрибутивность, законы де Моргана. Доказательства при помощи диаграмм Эйлера и непосредственные. Упорядоченные пары и кортежи. Декартово произведение и декартова степень. Их свойства, следующие из базовой ассоциативности.

Теория множеств является фундаментом всей математики. На её основе можно построить арифметику, геометрию, анализ, комбинаторику, теорию вычислимости и другие разделы математики. Эти построения действуют в парадигме «всё есть множество». Так, элементами множеств являются другие множества, упорядоченная пара это множество, конечная последовательность (кортеж) это тоже множество, функция или отношение это множество пар, натуральные числа это множества определённого вида, граф это пара из множества вершин и множества рёбер, вычислительная машина это набор из множеств и функций, описывающих программу, и т.д. Впрочем, рассмотрение каких угодно множеств может привести к парадоксам: например, не может быть множества всех множеств. На этой лекции мы познакомимся с базовыми понятиями «наивной» теории множеств, в которой вопросы о том, какими могут быть множества, игнорируются.

1 Понятие множества. Способы задания множеств

Определение 1. *Множеством* называется произвольный набор (совокупность, класс, семейство) каких-либо объектов. Объекты, входящие во множество, называются его *элементами*. Если объект x является элементом множества A, то говорят, что *x принадлежит A*, и пишут $x \in A$.

На самом деле это не определение, а пояснение: оно лишь ссылается на синонимы. Полностью выйти из этой ситуации нельзя, ведь цепочку определений надо с чего-то начинать. Обычно базовыми считаются три понятия: множество, элемент и принадлежность. Множество — это то, чему принадлежат элементы. Элементы — это то, что принадлежит множеству. А принадлежность — это то, как относится элемент к множеству.

В наивной теории множеств никаких ограничений на состав элементов нет. Из-за этого возникают парадоксы, о которых мы поговорим чуть позже.

Есть два стандартных способа записи множеств. Первый — простое перечисление элементов, например $A = \{6, 28, 496\}$ или $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$[1]. При этом каждый элемент должен встречаться в перечислении ровно один раз: запись $\{1, 1, 2, 3\}$ нужно признать либо не имеющей смысла, либо эквивалентной $\{1, 2, 3\}$. Иногда рассматривают *мультимножества*, в которые каждый элемент может входить несколько раз, но в нашем курсе такого не будет. При записи множеств не важен порядок, в котором идут элементы: например, записи $\{1, 2, 3\}$, $\{2, 3, 1\}$ и $\{3, 1, 2\}$ задают одно и то же множество. При записи бесконечных множеств используют многоточие $(\dots)$, когда считают, что принцип построения множества понятен из первых нескольких элементов[2].

Второй способ задания множеств — формулировка определяющего свойства (по-английски этот способ называется “set builder notation”). В этом случае рассматриваются все элементы, удовлетворяющие некоторому свойству. Например, $\{x \mid x > 0\}$ — множество всех положительных x. Часто явно указывают, какому объемлющему множеству должны принадлежать все элементы. Например, $\{x \in \mathbb{R} \mid x > 0\}$ — множество всех положительных действительных чисел. Иногда вместо черты $(|)$ используют двоеточие $(:)$, особенно когда черта уже встречается в формуле. Например, запись $\{x \in \mathbb{R} \colon |x| < 1\}$ выглядит лучше, чем $\{x \in \mathbb{R} \mid |x| < 1\}$. Слева от черты могут стоять более сложные выражения. Например, $\{(a, b, c) \mid a^2 + b^2 = c^2, a, b, c \in \mathbb{N}, a, b, c > 0\}$ обозначает множество всех пифагоровых троек, а $\{a^2 \mid a \in \mathbb{N}\}$ обозначает множество всех полных квадратов.

2 Подмножество. Пустое множество

Определение 2. Множество A является *подмножеством* множества B, если любой элемент множества A также принадлежит множеству B. Обозначение: $A \subset B$. Множества A и B равны, если одновременно $A \subset B$ и $B \subset A$. Обозначение: $A = B$. Если $A \subset B$, но $A \neq B$, то A называют *собственным* или *строгим* подмножеством. Обозначение $A \subsetneq B$.[3]

Из этого определения можно вывести независимость множества от порядка записи элементов и многократного повторения элементов, ведь по этому определению множества $\{1, 2, 3\}$, $\{1, 1, 1, 2, 2, 3\}$ и $\{2, 1, 3\}$ равны.

Утверждение 3. *Имеют место следующие свойства:*

a) Рефлексивность $\subset$: для любого множества A выполнено $A \subset A$;

[1] Мы будем считать, что натуральные числа начинаются с нуля, т.е. отвечают на вопрос «сколько?» Часто предполагается, что натуральные числа начинаются с единицы, т.е. отвечают на вопрос «какой по счёту?» Выбор того или иного подхода является делом вкуса и традиций, объективной истины тут нет.

[2] Однако, тут надо быть осторожным: вообще говоря, любую последовательность можно продолжить как угодно. Например, известна шутка Дугласа Хофштадтера: продолжите последовательность $(0, 1, 2, \dots)$. Ответом будет 720! (факториал семисот двадцати). Закономерность попробуйте угадать самостоятельно.

[3] В некоторых источниках используют смещённые обозначения: любое подмножество обозначают $A \subseteq B$, а строгое — $A \subset B$, по аналогии со строгим и нестрогим неравенством.

б) Антисимметричность $\subset$: если $A \subset B$ и $B \subset A$, то $A = B$;

в) Транзитивность $\subset$: если $A \subset B$ и $B \subset C$, то $A \subset C$;

г) Рефлексивность $=$: для любого множества A выполнено $A = A$;

д) Симметричность $=$: если $A = B$, то $B = A$;

е) Транзитивность $=$: если $A = B$ и $B = C$, то $A = C$;

ж) Антирефлексивность $\subsetneq$: неверно, что $A \subsetneq A$;

з) Антисимметричность $\subsetneq$: невозможно одновременно $A \subsetneq B$ и $B \subsetneq A$;

и) Транзитивность $\subsetneq$: если $A \subsetneq B$ и $B \subsetneq C$, то $A \subsetneq C$.

Доказательство остаётся читателю в качестве упражнения.

Определение 4. *Пустым множеством* $\varnothing$ называется множество, не содержащее ни одного элемента.

На первый взгляд множества, не содержащие ни одного элемента, могут быть различными. Например, множество шестиногих млекопитающих и множество простых чисел, делящихся на 4, кажутся разными. Однако, эти множества равны по нашему определению. Действительно, невозможно предъявить шестиногое млекопитающее, не являющееся простым числом, делящимся на 4. Значит, любое шестиногое млекопитающее таким числом является. Аналогично, верно и обратное. Значит, эти множества равны. Такие рассуждения могут быть непривычны, но с их справедливостью приходится соглашаться. Ещё одной иллюстрацией служит небольшая песенка С. Я. Маршака:

> Спросил меня голос в пустыне дикой:
> — Много ли в море растёт земляники?
>
> — Столько же, сколько селёдок солёных
> Растёт на берёзах и ёлках зелёных

Часто говорят, что *элементы пустого множества обладают любыми свойствами.* Это можно сформулировать следующим образом:

Утверждение 5. *Для любого множества A выполнено $\varnothing \subset A$.*

Зачастую знаки $\in$ (принадлежность) и $\subset$ (подмножество) путают. Это грубая ошибка: первый знак относится к объекту и множеству, второй — к двум множествам. Особенно внимательным нужно быть, если объекты сами являются множествами. Например, множество $A = \{1, 2, \{3\}\}$ состоит из числа 1, числа 2 и одноэлементного множества $\{3\}$. Для него будет выполнено $\{3\} \in A$, но $\{3\} \not\subset A$. И наоборот, $\{1\} \subset A$, но $\{1\} \notin A$. А для множества $B = \{1, 2, 3, \{3\}\}$ выполнено как $\{3\} \in B$, так и $\{3\} \subset B$.

3 Парадокс Рассела

С отношением принадлежности связан открытый в 1901 году парадокс Рассела. Назовём множество *правильным*, если оно не является собственным элементом. Например, множество натуральных чисел правильное: оно само не является натуральным числом.

Множество точек на плоскости тоже не является точкой. А вот множество всех множеств является множеством, а множество всех бесконечных множеств бесконечно. Эти множества неправильны.

Теперь рассмотрим множество всех правильных множеств, иными словами, пусть $M = \{X \mid X \notin X\}$. Является ли M правильным? Пусть не является. Тогда $M \notin M$. Но тогда $X \notin X$ выполнено при $X = M$. То есть $X \in M$ для $X = M$. То есть $M \in M$, что противоречит предположению. Но и случай $M \in M$ противоречив. Действительно, тогда $X \notin X$ не выполнено при $X = M$. А тогда $X \notin M$ для $X = M$, то есть $M \notin M$. Значит, любой ответ на поставленный вопрос приводит к противоречию, т.е. ответить на вопрос нельзя. Рассуждения над этим и другими парадоксами привели к построению аксиоматической теории множеств (в противовес наивной теории), в которой множества можно строить не как угодно, а лишь по определённым правилам. В частности, соотношение $X \in X$ не может быть выполнено никогда, а множества всех множеств не существует. Изучение этой теории выходит за рамки нашего курса, но упомянем одну нужную здесь аксиому.

Аксиома 6 (Аксиома регулярности)**.** *В любом непустом множестве A найдётся элемент $X \in A$, такой что $X \cap A = \varnothing$.*

Из этой аксиомы можно вывести такие утверждения:

Утверждение 7. *Ни для какого множества B невозможно $B \in B$.*

Доказательство. Пусть $A = \{B\}$. По аксиоме регулярности $B \cap \{B\} = \varnothing$. Но это и значит, что $B \notin B$. □

Про это утверждение говорят, что отношение $\in$ *антирефлексивно* или *иррефлексивно*.

Утверждение 8. *Ни для каких множеств B и C невозможно одновременно $B \in C$ и $C \in B$.*

Доказательство. Пусть $A = \{B, C\}$. Тогда либо $B \cap \{B, C\} = \varnothing$, либо $C \cap \{B, C\} = \varnothing$. В первом случае получаем $C \notin B$, во втором — $B \notin C$. □

Отсюда следует, что отношение $\in$ антисимметрично: поскольку одновременно $B \in C$ и $C \in B$ не выполнены никогда, то во всех случаях, когда они всё же выполнены, верно и $B = C$.[4] Что касается транзитивности, то она может как присутствовать, так и не присутствовать. Рассматривают *транзитивные множества*, т.е. такие A, что из $x \in A$ и $y \in x$ следует $y \in A$. Они играют важную роль в теории ординалов. Примерами транзитивных множеств являются $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$ или $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

[4]Тут мы снова встречаемся с принципом пустой импликации: из ложного утверждения следует что угодно.

4 Операции над множествами

Если несколько множеств уже заданы, то с ними можно производить различные операции. Будем считать, что определено некоторое множество U (*универсум*), которому заведомо принадлежат все элементы всех множеств.

Определение 9. Пусть заданы множества A и B, лежащие в некотором универсуме U. Тогда:

- *Объединением* A и B называется множество $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.
- *Пересечением* A и B называется множество $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.
- *Разностью* множеств A и B называется множество $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.
- *Симметрической разностью* множеств A и B называется множество $A \triangle B = \{x \mid x \in A \text{ и } x \notin B, \text{ или } x \in B \text{ и } x \notin A\}$.
- *Дополнением* множества A называется множество $\overline{A} = \{x \mid x \notin A\} = U \setminus A$.

Операции над множествами иллюстрируют на диаграммах, которые принято называть *кругами Эйлера* или *диаграммами Венна*. Каждому множеству соответствует круг (или другая плоская фигура), такая что все точки, лежащие внутри фигуры, принадлежат множеству, а остальные не принадлежат.[5] На рисунке 1 показана диаграмма Эйлера для множеств букв латинского, греческого и русского алфавитов. Когда речь идёт об операциях над множествами, нужные множества показываются штриховкой. На рисунке 2 мы приводим диаграммы Эйлера для всех основных операций над множествами.

Утверждение 10. *Для операций над множествами выполнены следующие тождества:*

а) *Коммутативность:* $A \cup B = B \cup A$, $A \cap B = B \cap A$, $A \triangle B = B \triangle A$;

б) *Ассоциативность:* $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;

в) *Дистрибутивность:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

г) *Идемпотентность:* $A \cup A = A$, $A \cap A = A$;

д) *Аннигиляция:* $A \setminus A = A \triangle A = \varnothing$;

е) *Законы де Моргана:* $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$, $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.

Доказательство. Каждое из тождеств можно доказывать при помощи кругов Эйлера или непосредственно. Мы продемонстрируем оба метода для тождества $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, оставив остальные в качестве упражнения.

[5] Обычно считается, что на диаграмме Эйлера должны присутствовать части для всех возможных вариантов принадлежности к множествам, а на диаграмме Венна можно не рисовать части, в которых нет элементов.

Рис. 1: Пример диаграммы Эйлера, показывающей прописные буквы латинского, греческого и русского алфавитов.

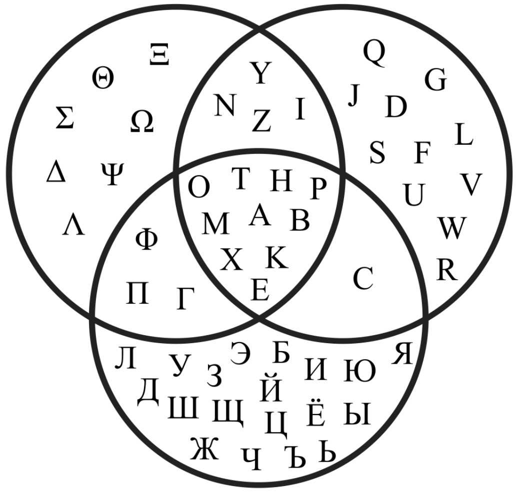
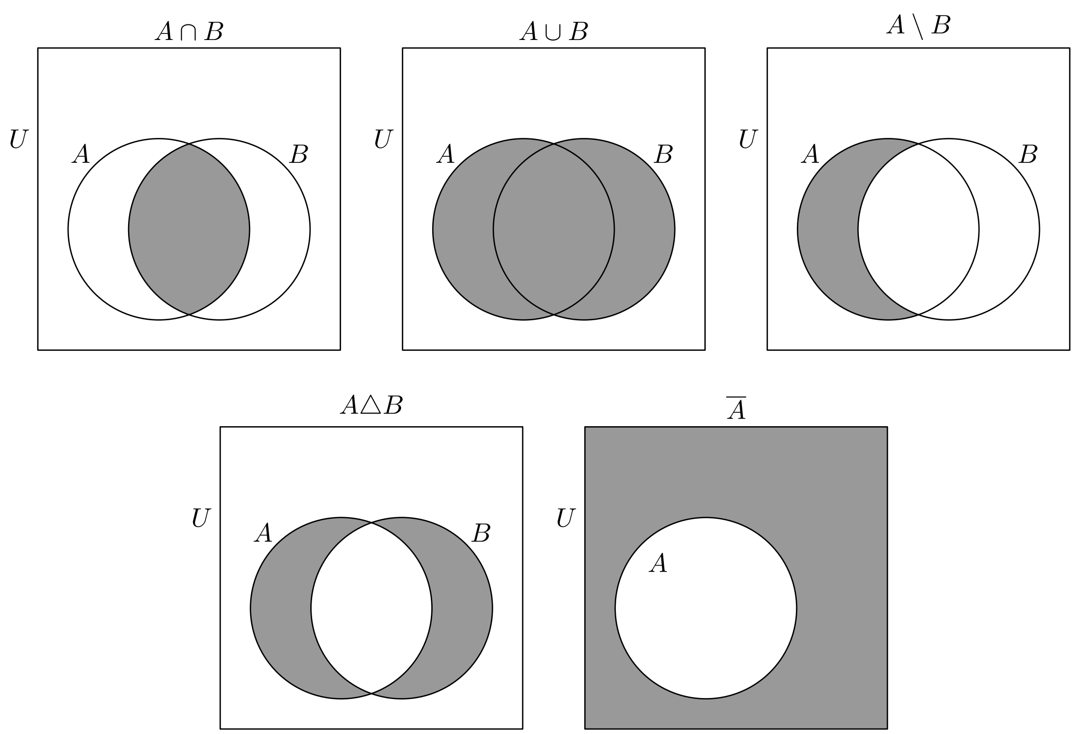
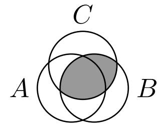
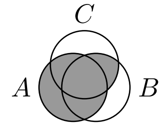
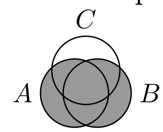


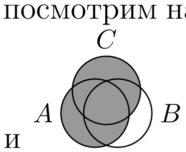
Рис. 2: Диаграммы Эйлера для основных операций над множествами.

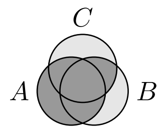


Доказательство при помощи кругов Эйлера. Посмотрим вначале на левую часть равенства. Множество $B \cap C$ изображается следующим образом: 

. После объединения с A получается следующая картина: 

. Теперь посмотрим на правую часть. Множества $A \cup B$ и $A \cup C$ изображаются как 

и 

соответственно. В пересечении получается диаграмма 

, идентичная полученной для левой части. Идентичность диаграмм и доказывает тождество. Фактически для каждой из 8 частей плоскости мы проверили, что они либо входит в оба множества, либо не входит ни в одно из них.

Непосредственное доказательство. Чтобы доказать равенство двух множеств, нужно доказать, что любой элемент каждого из них является элементом другого. Пусть $x \in A \cup (B \cap C)$. По определению объединения, это значит, что $x \in A$ или $x \in B \cap C$. В первом случае $x \in A \cup B$ и $x \in A \cup C$, откуда $x \in (A \cup B) \cap (A \cup C)$. Во втором случае по определению пересечения $x \in B$ и $x \in C$. Значит, $x \in A \cup B$ и $x \in A \cup C$, а значит $x \in (A \cup B) \cap (A \cup C)$. Получили, что в любом случае $x \in (A \cup B) \cap (A \cup C)$.

Обратно, пусть $x \in (A \cup B) \cap (A \cup C)$. Тогда $x \in A \cup B$ и $x \in A \cup C$. Если $x \in A$, то $x \in A \cup (B \cap C)$. Если же $x \notin A$, то поскольку $x \in A \cup B$, верно $x \in B$. Аналогично $x \in C$. Значит, $x \in B \cap C$, откуда $x \in A \cup (B \cap C)$. В любом случае $x \in A \cup (B \cap C)$.

В итоге любой элемент левой части является элементом правой, и наоборот. Значит, два множества равны, что и требовалось. $\square$

5 Пары и кортежи. Декартово произведение

Как мы уже говорили, для множества не важен порядок следования элементов. Конечные структуры, для которых порядок важен, называются *кортежами*. Неформально говоря, кортеж это конечная последовательность элементов. Формально базовым понятием является упорядоченная пара, которую можно вводить разными способами. В любом случае нужно как-то указать, какой элемент пары первый, а какой второй. Также должно выполняться свойство, что из равенства пар следует равенство компонент: если $(a, b) = (c, d)$, то $a = c$ и $b = d$.

Вот несколько возможных подходов:

- Определение Винера: $(a, b) = \{\{\{a\}, \varnothing\}, \{\{b\}\}\}$;

- Определение Хаусдорфа: $(a, b) = \{\{a, 1\}, \{b, 2\}\}$, где 1 и 2 суть объекты, отличные от a, b и друг от друга;

- Определение Куратовского: $(a,b) = \{\{a\},\{a,b\}\}$;

- Упрощённое определение Куратовского: $(a,b) = \{a,\{a,b\}\}$.

Последнее определение наиболее естественно: для задания упорядоченной пары нужно задать неупорядоченную и первый элемент в ней. При этом если $a = b$, то определение схлопнется до $\{a,\{a\}\}$. Аксиома регулярности позволяет однозначно расшифровать такую запись: по утверждению 8 не может быть, что $a = \{\{a\}\}$. Если $a \neq b$, то определение тоже однозначно, т.к. по той же аксиоме регулярности $\{a,b\}$ не может быть одним из элементов a.

Определение пары можно «нарастить» до определения кортежа. Неформально говоря, кортеж — это пара из «головы» (первого элемента) и «хвоста» (всего остального). Далее, «хвост» раскручивается по индукции. По соображениям, которые станут яснее ниже, индукцию стоит проводить не до кортежа длины 2 (т.е. уже определённой пары) или длины 1 (т.е. последнего элемента), а до самого конца — пустого кортежа. Получается такое определение:

Определение 11. *Кортежем* длины 0 называется пустое множество. Если уже задан $T = (a_1,\ldots,a_n)$ — кортеж длины n, то $(a,a_1,\ldots,a_n) = \{a,\{a,T\}\}$ есть кортеж длины $n+1$.

Так можно получить ещё одно определение упорядоченной пары: (a,b) — это множество $\{a,\{a,\{b,\{b,\varnothing\}\}\}\}$. На базе любого такого определения возникает новая операция:

Определение 12. *Декартовым произведением* множеств A и B называется множество упорядоченных пар $A\times B = \{(a,b) \mid a \in A, b \in B\}$. *Декартовой степенью* A^n множества A называется множество кортежей длины n из элементов A.

Понятие декартова произведения обобщает идею декартовых координат: декартова плоскость является произведением двух осей. А, например, прямоугольник является произведением двух отрезков.

Как правило, возведение в степень и умножение согласованы: A^n должно равняться $\underbrace{A \times A \times \cdots \times A}_{n\text{ раз}}$. По нашим определениям это верно, если скобки расставить так: $A \times (A \times (A \times \cdots \times A)\ldots))$. Если скобки расставить иначе, то равенство не сойдётся: пары $(a,(b,c))$ и $((a,b),c)$ различны, т.к. $a \neq (a,b)$. Однако ассоциативность обычно требуется для умножения. Также хотелось бы равенства $A^1 = A$, однако по определению кортеж длины 1 имеет вид $\{a,\{a,\varnothing\}\}$ и не совпадает с отдельным элементом a. Чтобы получить эти и другие соотношения, мы разрешим проводить указанные преобразования. Формально определение будет таким:

Определение 13. Множества T и S задают один и тот же кортеж, если можно построить цепочку $T_0 = T, T_1, T_2, \ldots, T_k = S$, такую что для каждого $i = 0,1,\ldots,k-1$ верно одно из трёх условий:

а) $T_{i+1} = \{T_i,\{T_i,\varnothing\}\}$, или наоборот.

б) Для некоторых a, b и c множество T_i является парой $(a,(b,c))$, а множество T_{i+1} — парой $((a,b),c)$, или наоборот.

в) Множества T_i и T_{i+1} являются упорядоченными парами, при этом один из элементов у них одинаковый, а для второго выполнено одно из этих трёх условий (в том числе само третье рекурсивно).

Теперь эквивалентность можно распространить на множества кортежей:

Определение 14. Множества A и B эквивалентны, если для каждого элемента A есть элемент B, задающий тот же кортеж, и наоборот.

Введя такое определение можно доказать такой набор хороших свойств.

Утверждение 15. *При всех A, B, C, n, m выполнены эквивалентности:*

а) $A \times (B \times C) \sim (A \times B) \times C$*;*
б) $A^n \sim A \times A \times \cdots \times A$ *(n раз);*
в) $A \times \{\varnothing\} \sim A$*;*
г) $A^n \times A^m \sim A^{n+m}$*;*
д) $(A^n)^m \sim A^{nm}$*.*

Доказательство. Первая эквивалентность следует напрямую из второго правила: если $(a, (b, c)) \in A \times (B \times C)$, то $((a, b), c) \in (A \times B) \times C$. Вторую мы уже обсудили: если скобки ставить слева направо, то получается равенство из определения кортежа, а любой другой порядок даст тот же результат по предыдущему. Третья следует из того, что мы отождествили объекты $(a, \varnothing)$ и a по первому правилу.

Для четвёртой докажем такую лемму.

Лемма 16. *Пара $((a_1, \dots, a_k), (a_{k+1}, \dots, a_n))$ задаёт тот же кортеж, что и $(a_1, \dots, a_n)$.*

Неформально можно сказать, что кортеж можно разбивать на голову и хвост в любом месте, а не только после первого элемента. Доказательство проводится при помощи нескольких индуктивных рассуждений.

Доказательство. По определению $(a_{k+1}, \dots, a_n) = (a_{k+1}, (a_{k+2}, \dots, a_n))$. Значит,

$$\begin{aligned}((a_1, \dots, a_k), (a_{k+1}, \dots, a_n)) &= ((a_1, \dots, a_k), (a_{k+1}, (a_{k+2}, \dots, a_n))) \\ &= (((a_1, \dots, a_k), a_{k+1}), (a_{k+2}, \dots, a_n))).\end{aligned}$$

Если теперь мы докажем, что $((a_1, \dots, a_k), a_{k+1}) = (a_1, \dots, a_{k+1})$, то дальше можно по индукции «перекинуть» все элементы в первый кортеж, второй останется пустым и «сократится». Ну а нужное равенство получается так:

$$((a_1, \dots, a_k), a_{k+1}) = ((a_1, (a_2, \dots, a_k)), a_{k+1}) = (a_1, ((a_2, \dots, a_k), a_{k+1}),$$

и далее снова по индукции. □

Теперь докажем четвёртую эквивалентность. Пусть $x \in A^n \times A^m$. Тогда $x = (y, z)$ для некоторых $y \in A^n$ и $z \in A^m$. Тогда $y = (a_1, \dots, a_n)$ и $z = (b_1, \dots, b_m)$, где все a_i и b_j лежат в A. Согласно лемме получаем $x = (y, z) = (a_1, \dots, a_n, b_1, \dots, b_m)$, то есть x есть кортеж $n + m$ элементов из A. Значит, $x \in A^{n+m}$.

Обратно, пусть $x \in A^{n+m}$. Тогда $x = (c_1, c_2, \ldots, c_{n+m})$, где все $c_i \in A$. Согласно лемме получаем $x = ((c_1, \ldots, c_n), (c_{n+1}, \ldots, c_{n+m}))$, а поскольку $(c_1, \ldots, c_n) \in A^n$ и $(c_{n+1}, \ldots, c_{n+m}) \in A^m$, получаем, что $x \in A^n \times A^m$.

Значит, каждое множество включено в другое, и потому они равны. Пятая эквивалентность доказывается аналогично. $\square$