Теория конечных множеств

Понятие множества в математике является единственным понятием, которое невозможно определить «строго». Надо к этому понятию просто привыкнуть, как дети привыкают пользоваться словами языка, на котором говорят взрослые. *Множество* состоит из *элементов.*

Задать множество, это значит, задать все его элементы, а также задать идентификацию его элементов. Более строго: мы говорим, что нам задано множество, если:

1. Для любого объекта нам задано, принадлежит этот объект данному множеству или нет
2. Для любых двух элементов множества мы можем определить, совпадают они или нет.

Для профессиональных математиков теоретико-множественная терминология является основой их языка, поэтому для изучения математики в любом направлении и в любом объеме овладение терминологией теории множеств необходимо. Проще всего осваивать терминологию теории множеств на примере самых простых конечных множеств.

Пусть A и B – два множества.

Через A U B обозначается объединение этих множеств: a ∈ A∪ B тогда и только тогда когда a ∈ A или a ∈ B.

Через A∩B обозначается пересечение этих множеств: a ∈ A∩ B тогда и только тогда, когда a ∈ A и a ∈ B.

Множество B называется подмножеством множества A, если каждый элемент множества B является элементом множества A, применяется такое обозначение: B ⊂ A. Все подмножества множества A сами образуют множество. Множество всех подмножеств множества A обозначается через 2^A.

Через A x B обозначается прямое произведение множеств A и B, это множество всех пар (a, b), где a ∈ A и b ∈ B.

Имеется уникальное *пустое множество*, которое обозначается через Ø. Это множество, в котором вообще нет ни одного элемента.

Пусть задано множество A. Вопрос: можно ли считать, что Ø является подмножеством множества A?

Отображением f:A → B называется правило, которое с каждым элементом a ∈ A сопоставляет элемент f(a) ∈ B.

Отображение f:A → B называется *вложением* или *инъективным отображением,* если из f(a)=f(b) следует, что a=b.

Отображение f:A → B называется сюръективным отображением если для каждого b ∈ B существует a ∈ A, для которого f(a) = b.

Отображение, которое одновременно является инъективным и сюръективным называется *взаимно-однозначным соответствием* или *биекцией*.

Множество всех отображений A → B обозначается через Map(A, B) или B^A.

Пусть f:A → B отображение. Рассмотрим в множестве A x B подмножество элементов (x, f(x)) при всех x ∈ A. Это подмножество называется графиком отображения f.

Примеры множеств: множество всех целых чисел Z, множество всех вещественных чисел R, множество точек на прямой R, множество N(n) всех натуральных чисел от 1 до n.

Вопрос: образуют ли множество все теоремы математики?

Множество A называется конечным, если для некоторого натурального n существует взаимно-однозначное соответствие A -> N(n), в этом случае говорят, что n является *мощностью* множества A, обозначается n = IAI.

Конечные множества являются материальной первоосновой натуральных чисел. Арифметические операции с натуральными числами, такие как сложение, умножение и возведение в степень происходят из соответствующих операций над конечными множествами: объединение, прямое произведение и множество всех отображений.

Рассмотрим простые и общеизвестные факты:

$|A \cup B| = |A| + |B|$, если $A \cap B = \emptyset$,

$|A \times B| = |A| * |B|$,

$|A^B| = |A|^{|B|}$.

Подмножества множества A находятся в естественном взаимно-однозначном соответствии с отображениями A -> {0, 1}, поэтому всего подмножеств в множестве A имеется $2^{|A|}$. Например, в пустом множестве имеется ровно одно подмножество: пустое. В множестве, состоящем из одного элемента имеется два подмножества: пустое и само множество.

Для любого множества A рассмотрим в множестве A x A подмножество пар (a, a), где a ∈ A. Можно сказать иначе: рассмотрим множество пар (a, b), для которых a = b. Это подмножество называется *диагональю*. Требование 2 идентифицируемости элементов множества равносильно существованию диагонали в прямом квадрате A x A.

Пусть A и B конечные множества.

Сколько имеется отображений A -> B ?

Ответ: $|B|^{|A|}$.

Пусть A, B, C – произвольные множества.

Тогда имеется естественное взаимно-однозначное соответствие между $A^{B \times C}$ и $(A^B)^C$. Иначе говоря:

$$Map(B \times C, A) = Map(B, Map(C, A)),$$

Постройте это естественное взаимно-однозначное соответствие.

здесь знак равенства означает биекцию. А можно ли сказать, что два множества равны? Нет. Множества неидентифицируемы: про два множества можно лишь сказать, что между ними существует биекция, а в некоторых случаях можно сказать, что между ними существует «естественная биекция». Неидентифицируемость множеств является источником знаменитых антиномий теории множеств.

Сколько имеется вложений A -> B ?

Ответ: пусть n = IBI, k = IAI; если k > n, то 0, в противном случае

n(n-1)(n-2) … (n-k+1) = n!/(n-k)!. В частности, если k = n, то n!.

Рассмотрим этот случай подробнее. Итак, сколько имеется вложений A -> A ? Иными словами, сколько имеется взаимно-однозначных соответствий A -> A ? Ответ мы уже видели: n! Этот случай особенно интересен, т.к. биекции A -> A образуют группу, обозначаемую обычно через S(n) и называемую *симметрической группой*. Это очень важные конечные группы, они используются во многих приложениях, например, при доказательстве неразрешимости в радикалах алгебраических уравнений степени > 4. Эта область математики называется *теория Галуа.*

Пусть A – конечное множество мощности n и пусть k ≤ n. Вопрос: сколько имеется подмножеств мощности k ?

Ответ: n!/(k!(n-k)!). Число

n!/(k!(n-k)!) обычно обозначается через C_n^k или еще через $\binom{n}{k}$. Имеет место равенство:

$C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$

Бином Ньютона:

$(a + b)^n = a^n + C_n^1 a^{n-1} b + \ldots + C_n^k a^{n-k} b^k + \ldots + b^n$

Отношение эквивалентности

Отношение это операция, принимающая два значения 0 или 1 (или И и Л).

Отношение называется отношением эквивалентности если

1. a ~ a
2. если a ~ b, то b ~ a
3. если a ~ b и b ~ c, то a ~ c

Если на множестве A задано отношение эквивалентности, то это множество разбивается на непересекающиеся подмножества.

Множество этих непересекающихся подмножеств называется *фактор-множеством* множества A и обозначается через A/~. Если в множестве A

имеется какая-то структура (например, группы), то как правило фактор-множество наследует эту структуру.

Типичный пример: поле Z/pZ.

Теорема Кантора. Не существует биекции между множеством и множеством всех его подмножеств.

Доказательство. Будем рассуждать от противного: пусть существует биекция f между A и 2^A. Обозначим через M с A подмножество всех таких элементов a, для которых a не входит в подмножество f(a), и рассмотрим соответствующий этому подмножеству элемент $b = f^{-1}(M)$. Зададимся вопросом, входит ли элемент b в соответствующее ему подмножество M ? Если входит, то должен не входить, а если не входит, то должен входить. Это противоречие.

Знаменитые антиномии теории множеств.

Широко известен такой парадокс теории множеств. Рассмотрим множество ВСЕХ МНОЖЕСТВ. По теореме Кантора не существует биекции между ним и множеством всех его подмножеств. Но этого не может быть, так как множество всех подмножеств множества всех множеств это снова множество всех множеств.

Разгадка этого парадокса в том, ВСЕ МНОЖЕСТВА не образуют множества, т.к. среди всех множеств нет возможности идентификации.

Трудная задача: доказать, что в Z/pZ каждый ненулевой элемент имеет обратный.