Не нужно
(в экзаменационную программу ничего не входит)

Множества

Теория множеств — это теория первого порядка, а это означает, что её язык — это язык логики первого порядка, в котором используются

- символы переменных (обычно $x, y, z, x_1, \ldots$)
- логические операции $\neg$, $\wedge$, $\vee$ $\rightarrow$
- кванторы $\forall$ и $\exists$ (в отличие от логики второго порядка, они применяются только к переменным)
- служебные символы (),
- [множество функциональных символов — их нет] и множество предикатных символов — их два: $\in$ и $=$.

Это алфавит. Формулы определяются по индукции:

- атом имеет вид $x \in y$ или $x = y$, где x и y — символы переменных;
- формула — либо атом, либо одна из конструкций $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$, $\forall x \varphi$, $\exists x \psi$, где φ и ψ — формулы, x — переменная.

Переменная x связана в формуле φ, если φ имеет вид $\forall x \psi$ или $\exists x \psi$ или представима в виде $\neg\psi$, $\psi \vee \pi$, $\psi \wedge \pi$, $\psi \rightarrow \pi$, причем x связана в ψ и π. Если x не связана в φ, то говорят, что x свободна в φ. Формула без свободных переменных — предложение. Теория первого порядка — это любое множество предложений.

Аксиомы логики первого порядка

Система логических аксиом логики первого порядка состоит из аксиом исчисления высказываний (см. ниже) и двух новых аксиом:

- $\forall x \; A \rightarrow A[t/x]$
- $A[t/x] \rightarrow \exists x A$.

($A[t/x]$ — формула, которая получается в результате подстановки символа переменной t вместо каждой свободной переменной в формуле A)

Используются два правила вывода:

- Modus ponens

$$\frac{A, A \rightarrow B}{B}$$

(это правило используется также в логике высказываний)

- Правило обобщения:

$$\frac{A}{\forall x A}$$

(если можно вывести $A(x)$, то можно вывести и $\forall x A(x)$).

Не нужно

Следует иметь в виду, что многое из того, что не входит в экзаменационные вопросы и помечено как ненужное, полезно для решения задач

(Однако задач по теории множеств на экзамене не будет)

Один из возможных вариантов (гильбертовой) аксиоматизации логики высказываний:

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $A \land B \to A$
4. $A \land B \to B$
5. $A \to (B \to (A \land B))$
6. $A \to (A \lor B)$
7. $B \to (A \lor B)$
8. $(A \to C) \to ((B \to C) \to ((A \lor B) \to C))$
9. $\neg A \to (A \to B)$
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$
11. $A \lor \neg A$

Аксиомы теории множеств

Современная теория множеств строится на системе аксиом, из которых выводятся все утверждения теории множеств. Система ZFC (Цермело-Френкеля и выбора) является стандартной. Существуют и другие системы, например, NBG (фон Нейман – Бернайс – Гёдель), которая наряду с множествами рассматривает классы. ZFC:

1. Аксиома объемности: два множества равны тогда и только тогда, когда они имеют одни и те же элементы.
2. Аксиома пары: для любых множеств x и y существует множество z такое, что x и y – его единственные элементы.
3. Аксиома объединения: для любого множества x существует множество $y = \cup x$, состоящее из элементов элементов x.
4. Схема выделения: любому множеству x и свойству φ отвечает множество y, элементами которого являются те элементы x, которые обладают свойством φ. (Каждая формула порождает аксиому.) [$\Rightarrow \exists\, \varnothing$]
5. Схема подстановки: пусть $\varphi(x, y)$ – такая формула, что при любом x_0 из множества x существует единственное y_0, для которого $\varphi(x_0, y_0)$ истинно. Тогда объекты u, для которых $\exists v \in x$ такое, что $\varphi(v, u)$ истинна, образуют множество.
6. Аксиома бесконечности: существует множество, которое содержит $\varnothing$ и вместе с каждым своим элементом x содержит $x \cup \{x\}$.
7. Аксиома множества подмножеств: для любого множества x существует множество y, состоящее из всех подмножеств x.
8. Аксиома регулярности: каждое непустое множество x содержит элемент y такой, что $x \cap y = \varnothing$.
9. Аксиома выбора: для каждого множества x, состоящего из непустых непересекающихся множеств, существует множество y, имеющее ровно один общий элемент с каждым $z \in x$.

Альтернативная формулировка: на любом множестве x существует функция (выбора) $f: x \to \cup x$ такая, что $f(y) \in y$ для каждого $y \in x$.

Нужно определение порядка, линейного порядка, полного порядка

Полезно знать формулы

Аксиома пары позволяет определить декартово произведение $X \times Y$ любых двух множеств, а аксиома выбора — декартово произведение произвольного семейства множеств. Подмножества декартова произведения $X \times Y$ называются (бинарными) <u>отношениями</u> между X и Y. Бинарное отношение на множестве X — это любое подмножество множества $X \times X$.*) <u>Отображение</u> $f: X \to Y$ — это бинарное отношение между X и Y со свойствами:

- $\forall x \in X\ \exists y \in Y\ ((x,y) \in f)$
- $((x,y) \in f) \wedge ((x,z) \in f) \to (y = z)$.

Без первого свойства получается частичное отображение. Отображения в $\mathbb{R}$ мы называем <u>функциями</u>.

<u>Операции над множествами</u>

- Бинарные: $\cap, \cup, \setminus, \Delta, \times$
- Унарные: дополнение (предполагает наличие фиксированного универсума — объемлющего множества), булеан $2^X = \mathcal{P}(X)$

<u>Свойства:</u>

- ассоциативность $\cap, \cup, \Delta$ и (с оговорками) $\times$
- коммутативность $\cap, \cup$ и Δ
- дистрибутивность $\cup$ и $\cap$: $A \cap \bigcup_{X \in B} X = \bigcup_{X \in B} (A \cap X)$
  $A \cup \bigcap_{X \in B} X = \bigcap_{X \in B} (A \cup X)$
- дистрибутивность $\cap$ относительно Δ: $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$

(однако формула $(A \Delta B) \cup C = (A \cup C) \Delta (B \cup C)$ неверна!)

- $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$
- Если $\mho$ — фиксированный универсум, то $A^c \cap A = \varnothing$, $A^c \cup A = \mho$, $\varnothing^c = \mho$, $\mho^c = \varnothing$, $A^c \Delta A = \mho$, $(A^c)^c = A$

Таким образом, множество $2^{\mho}$ образует алгебру с единицей (над $\mathbb{F}_2$) относительно операций Δ (сложение) и $\cap$ (умножение). Вообще, любое семейство $\mathcal{F} \subset 2^{\mho}$, замкнутое относительно $\cup$ и $\setminus$ (а тогда и Δ и $\cap$, потому что $A \cap B = A \setminus (A \setminus B)$) образует такую алгебру. Относительно $\cap$ и $\cup$ такие семейства образуют алгебраическую структуру, называемую <u>булевой алгеброй</u>.

- Законы де Моргана: $A \setminus \bigcup_{X \in B} X = \bigcap_{X \in B} (A \setminus X)$, $A \setminus \bigcap_{X \in B} X = \bigcup_{X \in B} (A \setminus X)$.

Приоритет при расстановке скобок: дополнение, $\cap$, затем $\cup$ и $\setminus$. одинаковый приоритет

*) Важный частный случай — отношение порядка. <u>Порядок</u> $\leq$ на множестве X — это любое рефлексивное ($x \leq x\ \forall x \in X$) антисимметричное ($(x \leq y) \wedge (y \leq x) \to (x = y)$) и транзитивное ($(x \leq y) \wedge (y \leq z) \to (x \leq z)$) отношение на X. Простейший пример — диагональ $\Delta_X = \{(x,x) \in X \times X : x \in X\}$. Порядок $\leq$ называется <u>линейным</u>, если $\forall x, y \in X$ имеем $x \leq y$ или $y \leq x$ (т.е. любые два элемента сравнимы). Пример — обычный порядок на $\mathbb{R}$. Порядок $\leq$ называется <u>полным</u>, если для любого непустого $A \subset X$ существует $x \in A$ (наименьший элемент) т.ч. $x \leq y\ \forall y \in A$; полный порядок автоматически линеен. При этом пара $(X, \leq)$ называется частично (линейно, вполне) упорядоченным множеством. Под просто "порядком" обычно имеется в виду частичный порядок.

Всё понятно
Ничего не нужно

Свойства отображений

Пусть $f: X \to Y$ — отображение, $A_1 \subset A_2 \subset X$, $B_1 \subset B_2 \subset Y$.

- $f(A_1) \subset f(A_2)$, $f^{-1}(B_1) \subset f^{-1}(B_2)$
- $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
- $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

Операции над отображениями

- Сужение: если $f: X \to Y$ и $M \subset X$, то $g = f \cap M \times Y : M \to Y$ называется *сужением* f на M (а f — продолжение g)
- Композиция: для $f: X \to Y$ и $g: Y \to Z$ композиция f и g — это $g \circ f: X \to Z$, определенное правилом $x \mapsto g(f(x))$.
- Декартово произведение: если $f_1: X_1 \to Y_1$ и $f_2: X_2 \to Y_2$, то $f_1 \times f_2 : X_1 \times X_2 \to Y_1 \times Y_2$
  $(x_1, x_2) \mapsto (f(x_1), f(x_2))$.
- Диагональное произведение: если $f: X \to Y$ и $g: X \to Z$, то $f \Delta g : X \to Y \times Z$
  $x \mapsto (f(x), g(x))$.

Мы будем также рассматривать операцию взятия подотображения, которая обобщает сужение; термин "подотображение" встречается в литературе редко, хотя само понятие весьма полезно и часто используется.

- Подотображение: если $f: X \to Y$, $A \subset X$, $B \subset Y$ и $f(A) \subset B$, то $g = f \cap A \times B : A \to B$ называется *подотображением* f. Иными словами, подображение отображения $f \subset X \times Y$ (как мы помним, f — отношение между X и Y) — это подмножество $g \subset f$, рассматриваемое как отношение на подмножестве $A \times B$ множества $X \times Y$; для сужения всегда $B = Y$ (хотя в дальнейшем мы допуская вольность, иной раз не делаем различия между сужением $f|A$ и подотображением $A \to f(A)$, если это допустимо).

Отображения бывают *инъективными* (когда $f(x) \neq f(y)$ для $x \neq y$), сюръективными (когда $f(X) = Y$) и биективными (сюръектив. + инъектив.)
Для биективных отображений есть ещё одна операция:

- Обратное отображение: если $f: X \to Y$ — биекция, то существует $g: Y \to X$, для которого $g \circ f = id_X$ *) и $f \circ g = id_Y$; оно называется *обратным* отображением f и обозначается f^{-1}.

---

*) Тождественное отображение $id_X : X \to X$ множества X на себя определено правилом $id_X(x) = x$ $\forall x \in X$.

Мощность

Как правило, в разных теориях рассматриваются свои специфические отображения, и имеются особые отображения, наличие которых между двумя объектами теории позволяет утверждать, что свойства этих объектов совершенно одинаковы (с точки зрения данной теории). Например, в теории групп рассматриваются гомоморфизмы, а особые отображения, наличие которых между двумя группами позволяет утверждать, что группы обладают одними и теми же свойствами — изоморфизмы. В теории векторных пространств это линейные отображение и линейные изоморфизм, а в теории евклидовых пространств — линейные отображения и линейные изоморфизмы, сохраняющие скалярные произведения, т.е. изометрии.

В теории множеств рассматриваются всевозможные отображения, и свойств, которыми могут обладать разные множества, не так много — множество может быть пустым или непустым, конечным или бесконечным; единственная отличительная черта множества — это его мощность. Роль изоморфизмов в теории множеств играют биекции. Мощность, единственная характеристика множества, обобщает понятие числа элементов. Мощности двух множеств одинаковы, если между ними существует биекция.

В "наивной" (канторовской) теории множеств мощность множества X (обозначается $|X|$) определялась как класс всех множеств, равномощных X. В современной теории множеств имеется аксиома бесконечности, которая позволяет определить порядковые числа (ординалы*) как множества, содержащие $\varnothing$, вполне упорядоченные отношением $\in$, в которых каждый элемент есть множество всех предыдущих (относительно этого порядка) элементов. В ZFC мощность множества X определяется как наименьший ординал α, равномощный множеству X. Такие ординалы (наименьшие ординалы данной мощности) называются кардиналами. По традиции мощности обозначаются буквой $\aleph$ с индексами, а соответствующие ординалы — буквой ω с индексами, хотя ω часто используется вместо $\aleph$.

*) В "наивной" теории множеств ординалы понимаются как порядковые типы, т.е. классы эквивалентности вполне упоряд-х мн-в, связанных порядковыми изоморфизмами. Теорема о том, что любой класс эквивалентности содержит ординал в определённом выше смысле позволила вместо классов эквивалентности рассматривать их конкретные представители — введенные здесь ординалы. Несложно убедиться в том, что разные ординалы имеют разные порядковые типы, т.к. не связаны порядковым изом-м.

Нужно только для понимания дальнейшего

Первый бесконечный ординал — не что иное, как множество натуральных чисел (с нулём), это ω_0. Соответствующий кардинал — $\aleph_0$. Множества X, равномощные множеству натуральных чисел, называются <u>счётными</u> (их элементы можно "пересчитывать" посредством биекции $X \rightleftarrows \mathbb{N}$. Таким образом, X счётно, если $|X| = \aleph_0$. Это самые маленькие бесконечные множества в некотором естественном смысле. Дело в том, что мощности можно упорядочить не только с помощью ординалов, но и другим способом, использовавшимся ещё во времена Кантора: скажем, что $|X| \leq |Y|$, если существует вложение X в Y, т.е. X равномощно подмножеству Y.

<u>Теорема Кантора-Бернштейна</u> $|X| \leq |Y|, |Y| \leq |X| \Rightarrow |X| = |Y|$.

Аксиома выбора равносильна утверждению, что любые два множества сравнимы по мощности.

Примеры счётных множеств привести легко — это само множество $\mathbb{N}$, а также $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N} \times \mathbb{N}$ и т.д. А вот множество $\mathbb{R}$ уже несчётно. Действительно, оно содержит подмножество, равномощное множеству всех последовательностей из нулей и единиц (с точностью до счетного множества последовательностей, постоянных с некоторого момента) — это числа в двоичной записи. Запишем эти последовательности друг под другом:

$\alpha_0 = a_{00}\ a_{01}\ a_{02} \ldots$

$\alpha_1 = a_{10}\ a_{11}\ a_{12} \ldots$

$\alpha_2 = a_{20}\ a_{21}\ a_{22} \ldots$

Рассмотрим последовательность $a_{00}\ a_{11}\ a_{22} \ldots$. Заменив все члены на противоположные, получим последовательность, отличающуюся от $\alpha_0, \alpha_1, \ldots$.

Отсюда следует, что $\mathbb{R}$ несчётно и поэтому существуют трансцендентные числа (т.к. множество алгебраических чисел счётно). Поскольку каждая двоичная последовательность — характеристическая функция подмножества $\mathbb{N}$, отсюда следует также, что множество подмножеств $\mathbb{N}$ несчётно (хотя само $\mathbb{N}$ счётно). На этот счёт имеется общая теорема Кантора.

Нужно знать для дальнейшего
Доказательство не нужно

Теорема Кантора. Никакое множество X не равномощно множеству всех своих подмножеств.

$\sqcap$ Пусть $\varphi: X \to \mathcal{P}(X)$ — биекция. Положим
$$Z = \{x \in X : x \notin \varphi(x)\}.$$
Поскольку φ — биекция, имеем $Z = \varphi(z)$ для некоторого $z \in X$. Для z имеем
$$z \in Z \Leftrightarrow z \notin \varphi(z) \Leftrightarrow z \notin Z. \blacksquare$$

С другой стороны, имеется естественная биекция между $x \in X$ и $\{x\} \in \mathcal{P}(X)$, поэтому всегда $|X| < |\mathcal{P}(X)|$.

Лемма Цорна нужна для дальнейшего
Остальное не нужно

Теорема Цермело, лемма Цорна и лемма о Δ-системе

Следующие две классические теоремы равносильны аксиоме выбора в том смысле, что каждая из них выводится из ZFC т.е. из ZF+(аксиома выбора) (ZF — это система первых восьми аксиом), а аксиома выбора выводится и из ZF+(теорема Цермело), и из ZF+(лемма Цорна).

Т. Теорема Цермело

Всякое множество можно вполне упорядочить.

Т. Лемма Цорна

Пусть $(X, \leq)$ — частично упорядоченное множество и для каждого линейно упорядоченного $C \subset X$ существует верхняя грань в X, т.е. $\exists x \in X$ т., что $y \leq x$ $\forall y \in C$. Тогда в X имеется максимальный элемент, т.е. $\exists x^* \in X$ т., что если $y \in X$, $x^* \leq y$, то $y = x^*$.

Сам Цорн формулировал эту лемму для отношения $\subset$: Пусть семейство множеств $\mathcal{M}$ таково, что если $\mathcal{M}' \subset \mathcal{M}$ — любое подсемейство $\mathcal{M}$ с тем свойством, что $X, Y \in \mathcal{M}' \Rightarrow X \subset Y$ или $Y \subset X$, то $\bigcup \mathcal{M}' \in \mathcal{M}$. Тогда $\mathcal{M}$ содержит максимальное множество, т.е. множество которое не содержится ни в каком отличном от него элементе $\mathcal{M}$.

Именно в этой формулировке лемма Цорна чаще всего используется в математике (при доказательстве сущ-я базиса в любом векторном пространстве, существования алгебраического замыкания произвольного поля, максимального идеала в кольце с 1 и пр.)

Следующее утверждение просто доказывается, но исключительно полезно.

Т. Лемма о Δ-системе (или о Δ-корне)

Для любого несчётного семейства $\mathcal{F}$ конечных множеств найдутся несчётное подсемейство $\mathcal{F}' \subset \mathcal{F}$ и (конечное) множество F такие, что $X \cap Y = F$ для любых $X, Y \in \mathcal{F}'$! (Ясно, что $F = \bigcap \mathcal{F}'$.)

Семейства множеств $\mathcal{G}$ с тем свойством, что $X \cap Y = \bigcap \mathcal{G}$ $\forall X, Y \in \mathcal{G}$, называются Δ-системами, а $\bigcap \mathcal{G}$ — Δ-корнем.

Для доказательства леммы о Δ-системе надо заметить, что существуют $n \geq 0$ и несчётное $\mathcal{F}'' \subset \mathcal{F}$ такие, что $|X| = n$ $\forall X \in \mathcal{F}''$ и применить индукцию по n. Δ-корень может быть пустым!