ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

проф. В. А. Успенский

1/2 года, 1 курс, 2 семестр.

1. Предварительные понятия.

Имена и их денотаты. Смысл знака равенства. Десятичная (двоичная, римская и т. п.) запись числа как имя числа; число как денотат своей записи. Как образуются имена русских слов, имена множеств и имена функций; лямбда-обозначения.

Переменные и их области изменения (они же области значений). Сорта переменных. Именные формы (т.е. имена, зависящие от параметра). Свободные и связанные вхождения переменных. Явные и фиктивные переменные. Параметры именной формы.

Множества, их элементы и подмножества. Знаки принадлежности "$\in$" и включения "$\subset$". Бинарные (они же двуместные) операции над множествами: объединение, пересечение, разность. Объединение и пересечение произвольного множества множеств. Выпуклость пересечения произвольного множества выпуклых фигур. Будет ли пересечение двух связных фигур связным? Мощность множества. Характеристическая и полухарактеристическая функция множества относительно его надмножества.

Покрытия и разбиения.

Функции из одного множества в другое, многоместные функции из одного множества в другое, их области определения, области значений и графики. Тотальные функции. Понятие одноместной, двуместной и т.д. операции на данном множестве. Композиция функций.

Неупорядоченные пары, упорядоченные пары (или просто *пары*). Кортежи. Прямое (или декартово) произведение двух или нескольких множеств; проекция на данные оси.

Свойства, их области осмысленности и области истинности (иначе — объёмы).

Отношения, их области осмысленности и области истинности (они же объёмы, они же графики).

Виды отношений: рефлексивные, симметричные, транзитивные; эквивалентности. Инверсия, или обращение, отношения.

Теорема о разбиении множества на классы эквивалентности (они же смежные классы).

Отношения частичного порядка (называемые также просто отношениями порядка), строгие и нестрогие. Отношения линейного порядка, строгие и нестрогие.

Частично упорядоченные множества (называемые также упорядоченными множествами). Линейно упорядоченные множества. Наибольший, или первый, и наименьший, или последний, элементы. Максимальные и минимальные элементы. Плотные множества. Вполне упорядоченные множества.

Сечения упорядоченных множеств и их виды: скачки, щели, дедекиндовы сечения. Аксиома Дедекинда для действительных чисел.

Предпорядок и индуцированная эквивалентность. Фактор-множество и его упорядочение.

Изоморфизм одного упорядоченного множества на другое. Понятие изоморфии упорядоченных множеств. Примеры изоморфных и неизоморфных множеств.

Алфавит, слово в данном алфавите, его длина. Пустое слово. Графическое равенство слов. Чем графическое равенство отличается от обычного равенства? Конечные и бесконечные алфавиты. Кортеж слов как слово в расширенном алфавите; текст как слово. Вхождение слова (в частности, буквы) в другое слово.

Словарное пространство как множество всех слов в конечном алфавите, его лексикографическое и иные упорядочения. Биекции между словарными пространствами. Словарные множества и словарные функции. Погружение прямого произведения двух словарных пространств в новое словарное пространство.

Высказывания и их истинностные значения. Употребление знака "$\models$" для обозначения истинности высказывания. Равносильные высказывания и знак равносильности "$\equiv$".

Операции над высказываниями: отрицание, конъюнкция, дизъюнкция, импликация.

Высказывательные формы. Свободные и связанные вхождения переменных. Явные и фиктивные переменные. Параметры высказывательной формы. Равносильность высказывательных форм.

Знак "!" осмысленности выражения и знак "$\simeq$" условного равенства.

2. Язык логики высказываний.

Алфавит языка логики высказываний: скобки, высказывательные переменные и логические связки: отрицание, конъюнкция, дизъюнкция, импликация. Правильно построенные выражения (они же формулы языка логики высказываний). Правила сокращённой записи (т. е. правила опускания и восстановления скобок).

Истинностное значение высказывания. Истинностные таблицы логических связок. Истинностное значение формулы. Равносильность формул.

Тавтологии. Законы логики высказываний в форме тавтологий. Знак "$\models$" для обозначения тавтологий.

Существование алгоритма для распознавания тавтологий.

Законы логики в форме равносильностей: закон снятия двойного отрицания; законы ассоциативности, коммутативности и дистрибутивности; законы де Моргана.

Выражение одних логических операций через другие. Невыразимость отрицания через конъюнкцию, дизъюнкцию и импликацию.

Безымпликативные формулы. Нормальные формулы. Дизъюнктивные и конъюнктивные нормальные формулы. Приведение произвольной формулы к нормальному виду, к дизъюнктивному (конъюнктивному) нормальному виду.

Элементарные конъюнкции и совершенные дизъюнктивные нормальные формы. Теорема: если две с. д. н. ф. над данным списком переменных равносильны, то они графически равны. Совершенные конъюнктивные нормальные формы.

Операция на множестве {и, л}, выражаемая данной формулой (при данном списке переменных). Существование для любой n-местной операции (кроме одной) выражающей её с. д. н. ф. и выражающей её с. к. н. ф.

Язык теоретико-множественных равенств и включений; построение алгоритма, отличающего верные равенства и включения от неверных.

3. Язык упорядоченных множеств.

Алфавит языка упорядоченных множеств. Правильно построенные выражения (они же формулы языка упорядоченных множеств). Атомные формулы.

Запись на языке упорядоченных множеств аксиом порядка (строгого и нестрогого), аксиом линейного порядка, аксиом плотного порядка.

Свободные и связанные вхождения переменных в формулу. Подстановка имён вместо свободных вхождений переменных.

Расширение алфавита языка за счёт введения имён элементов. Смысл кванторов при задании области изменения подкванторной переменной.

Интерпретация формулы на данном упорядоченном множестве в виде высказывания или высказывательной формы. Формулы, тождественно истинные на данном упорядоченном множестве.

Равносильность формул на данном упорядоченном множестве.

Бескванторные формулы, нормальные бескванторные формулы, дизъюнктивные и конъюнктивные нормальные бескванторные формулы. Приведение бескванторной формулы к нормальному, дизъюнктивному нормальному, конъюнктивному нормальному виду.

Переименование связанных переменных и ограничения на такое переименование. Выражение квантора существования через квантор общности и обратное выражение.

Возможности выноса квантора наружу за знаки отрицания, конъюнкции, дизъюнкции.

Предварённые формулы и приведение формулы к предварённому виду.

Ограничения на подстановку одной переменной вместо другой. Разрешённые, или свободные, подстановки.

Теорема о свободной подстановке: $B(q/x)(q/y)$ графически равно $B(y/x)(q/y)$ (здесь B - формула, q - имя или переменная, x и y - переменные, а подстановка y вместо x - свободная).

Следствие теоремы о свободной подстановке: $\exists x\ (x = y \,\&\, B) \equiv B(y/x)$.

Теорема об устранении кванторов для формул, рассматриваемых на плотных линейно упорядоченных множествах без первого и последнего элементов.

Понятие элементарной эквивалентности упорядоченных множеств. Элементарная эквивалентность всех плотных линейно упорядоченных множеств без первого и последнего элементов.

Понятие разрешимой теории. Разрешимость теории плотных линейно упорядоченных множеств без первого и последнего элементов.

Понятия 1) интерпретации языка упорядоченных множеств, 2) системы аксиом в этом языке, 3) модели системы аксиом.

4. Языки логики предикатов.

Понятие s-местного предиката на данном множестве. Соответствие между предикатами и подмножествами. Предикатные константы, или имена, и их валентность. Предикатные переменные и их валентность.

Понятие s-местной операции на данном множестве. Функциональные константы, или имена, и их валентности. Функциональные переменные и их валентности.

Алфавит языка логики предикатов: запятая, скобки, логические связки, кванторы, индивидные константы (они же индивидные имена), предикатные константы (они же предикатные имена), функциональные константы (они же функциональные имена), индивидные, функциональные и предикатные переменные.

Термы, атомные формулы, формулы. Элементарные формулы. Замыкание всеобщности.

Равносильные формулы. Понимание того, что основные равносильности и графические равенства, установленные для языка упорядоченных множеств, справедливы и для любого языка логики предикатов.

Запись на языке логики предикатов аксиом порядка (строгого и нестрогого), аксиом линейного порядка, аксиом плотного порядка.

Запись утверждения о бесконечности множества изменения переменных с помощью функциональной переменной.

Запись аксиомы Дедекинда и запись определения вполне упорядоченности множества.

Запись определения натурального ряда (точнее — упорядоченного множества, изоморфного натуральному ряду).

Запись аксиом упорядоченного множества, группы, кольца, поля, упорядоченного кольца, упорядоченного поля.

Запись аксиом евклидовой геометрии.

5. Структуры и сигнатуры, интерпретации и модели.

Понятия элементарной математической математической структуры (в дальнейшем, для краткости, просто *структуры*) и её носителя. Упорядоченные множества, группы, кольца, поля, упорядоченные кольца, упорядоченные поля, геометрия, натуральный ряд $\mathbb{N}$, множество действительных чисел $\mathbb{R}$ как структуры.

Сигнатура данной структуры как множество имён (они же константы), снабженных валентностями. Сигнатуры структур предыдущего абзаца.

Понятия изоморфизма и изоморфии структур одинаковой сигнатуры.

Язык данной сигнатуры, его алфавит, его термы и его формулы. Элементарные и неэлементарные языки.

Интерпретация сигнатуры (она же интерпретация языка). Какой смысл приобретают формулы при той или иной интерпретации? Выражение $I \models F$ для обозначения того, что формула F истинна (если она закрытая) или тождественно истинна (если она открытая) в интерпретации I. Равносильность формул при данной интерпретации.

Общезначимые формулы. Знак "$\models$" для обозначения общезначимости.

Два способа выражения законов предикатной логики: 1) посредством общезначимых формул; 2) посредством равносильностей, справедливых при любой интерпретации. Формула Лейбница. Теорема: $F_1 \models F_2$ тогда и только тогда, когда общезначима формула $(F_1 \Rightarrow F_2)\&(F_2 \Rightarrow F_1)$.

Система аксиом как произвольное множество закрытых формул рассматриваемой сигнатуры. Модели данной системы аксиом. Построение для каждого натурального n формулы, для которой произвольное множество тогда и только тогда является носителем какой-нибудь её модели, когда оно, это множество, имеет мощность (далее — варианты): 1) не менее n; 2) не более n; 3) n; 4) конечную; 5) бесконечную.

Понятие следствия системы аксиом. Запись $S \models F$ того факта, что формула F есть следствие системы аксиом S. Теорема: $\{A_1, \ldots, A_n\} \models F$ тогда и только тогда, когда $\models (A_1 \& \ldots \& A_n) \Rightarrow F$.

Совместные и локально совместные системы аксиом. Теорема компактности (без доказательства) для элементарных языков и её опровержение для языков неэлементарных.

Существование нестандартных моделей системы аксиом арифметики.

Элементарная эквивалентность структур. Полные системы аксиом.

Понятие независимой аксиомы. Независимые системы аксиом.

6. Язык арифметики.

Сигнатура языка, термы и формулы. Главная, или стандартная, интерпретация. Арифметические истины.

Запись аксиомы математической индукции. Аксиомы Пеано и единственность их модели с точностью до изоморфии.

Простые формулы и определение линейного арифметического множества, или арифметического множества размерности 1. Арифметичность множества всех чётных чисел, множества всех простых чисел.

Определение арифметического множества произвольной размерности. Арифметичность трёхмерного множества $\{(a, b, m) | \ a \equiv b \,(\mathrm{mod}\, m)\}$.

Существование неарифметических множеств.

Арифметичность объединения, пересечения, разности, прямого произведения, проекции арифметических множеств.

Арифметические функции. Арифметичность композиции арифметических функций. Арифметичность образа и полного прообраза арифметических множеств при арифметическом отображении.

Понятие плоского множества, универсального для данного класса линейных множеств. Теорема Кантора–Тарского о невозможности плоского арифметического множества, универсального для класса всех линейных арифметических множеств.

7. Алгоритмы, машины Тьюринга и вычислимые функции.

Общее понятие алгоритма; вход и выход алгоритма. Неформальное понятие конструктивного объекта и возможность представления конструктивных объектов словами в подходящем алфавите. Область возможных входов, или возможных исходных данных, область возможных выходов, или возможных результатов, область результативности. Три варианта протекания алгоритмического процесса. Как избавиться от безрезультатной остановки.

Функция, вычисляемая данным алгоритмом. Понятие вычислимой функции одного или нескольких аргументов.

Представление о шаге алгоритма. Сигнализирующее множество алгоритма.

Машина Тьюринга (она задаётся ленточным алфавитом, алфавитом внутренних состояний и программой). Кодирование программ посредством слов восьмибуквенного алфавита (*алфавита программ*).

Слабое (или *в слабом смысле*) и сильное (или *в сильном смысле*) вычисление функций из X^m в X на машине Тьюринга. Понимание того, что для фиксированных X и m, каждая машина вычисляет в слабом смысле какую-то функцию из X^m в X. Теорема: всякое слабое вычисление может быть заменено сильным (но на другой машине).

Понятие функции, вычислимой по Тьюрингу. Существование функций из X^m в X, не вычислимых по Тьюрингу.

Теорема: если две функции вычислимы по Тьюрингу, то их композиция вычислима по Тьюрингу.

Тьюрингова универсальная функция, дающая по слову p в алфавите программ $И$ и по элементу x словарного пространства X, значение функции, вычисляемой в слабом смысле программой p, применённой к x (если p не есть программа, то никакого результата, естественно, не возникает). Теорема: если T — тьюрингова универсальная функция, то для любой вычислимой по Тьюрингу функции $g\colon X^2 \to X$ найдётся такая тотальная вычислимая функция $h\colon X \to И^*$, что $\forall k \in X \quad \lambda x g(x,k) = \lambda x F(h(k), x)$.

Тезис Чёрча в версии Тьюринга.

Алгоритмическая проблема самоприменимости и её нерешимость. Нерешимость общей проблемы применимости. Две частные проблемы применимости: 1) когда фиксируется вход; 2) когда фиксируется выход; вопрос об их решимости.

8. Разрешимые и перечислимые множества.

Разрешимые и полуразрешимые множества в словарных пространствах. Характеризация разрешимости и полуразрешимости множества в терминах вычислимости характеристической и полухарактеристической функций. Примеры разрешимых числовых множеств. Разрешимость множества программ в словарном пространстве алфавита программ. Разрешимость сигнализирующего множества. Разрешимость объединения, пересечения, разности, прямого произведения разрешимых множеств.

Вычислимые последовательности и перечисляемые ими множества. Перечислимые множества. Перечислимость любого конечного множества, любого словарного пространства. Теорема: всякое бесконечное перечислимое множество допускает перечисление без повторений. Существования вычислимой биекции между бесконечными перечислимыми множествами.

Перечислимость объединения, пересечения, прямого произведения, проекции перечислимых множеств.

Теорема Чёрча–Поста: словарное множество разрешимо тогда и только тогда, когда перечислимо и оно само, и его дополнение. Теорема: бесконечное множество натуральных чисел разрешимо тогда и только тогда, когда оно есть область значений монотонно возрастающей вычислимой функции.

Теоремы: 1) область определения всякой вычислимой функции полуразрешима; 2) всякое полуразрешимое множество есть проекция разрешимого множества; 3) проекция всякого разрешимого множества перечислима; 4) всякое перечислимое множество есть область определения некоторой вычислимой функции.

Перечислимость области значений всякой вычислимой функции. Характеризация вычислимости функции в терминах перечислимости её графика.

Общее определение универсальной функции с данным индексным множеством. Существование универсальных функций с произвольным словарном пространством в качестве индексного множества.

Построение, для данной универсальной функции, точки, в которой она не определена. Существование вычислимой функции, не продолжаемой до тотальной вычислимой функции.

Главные универсальные функции. Главность универсальной функции Тьюринга.

9. Нерешимые алгоритмические проблемы.

Существование неразрешимого перечислимого множества (в произвольном словарном пространстве).

Неотделимые множества. Построение пары неотделимых перечислимых множеств.

Теорема о нераспознавании свойств вычислимых функций по их индексам в произвольной главной универсальной функции. Нераспознаваемость свойств вычислимых функций по их программам. Несуществование алгоритма, который по программе любой вычислимой тотальной функции распознаёт, совпадает ли эта функция с заранее заданной вычислимой тотальной функции f.

Примеры неразрешимых алгоритмических проблем из теории чисел и алгебры (без доказательства): из теории чисел — десятая проблема Гильберта; из алгебры — проблема представимости матриц.

10. Ограниченность выразительной и доказательной возможностей арифметики.

Арифметичность вычислимых функций с натуральными аргументами и значениями. Арифметичность перечислимых множеств натуральных чисел. Арифметичность произвольного арифметического множества в $\mathbb{N}^S$.

Нумерации словарных пространств. Определение арифметического множества в словарном пространстве; независимость этого определения от нумерации.

Арифметичность перечислимых множеств в словарных пространствах (без доказательства).

Построение плоского множества, универсального для класса линейных арифметических множеств, в виде полного прообраза множества арифметических истин при вычислимом отображении.

Теорема Тарского о неарифметичности множества арифметических истин.

Уточнение неформального понятия "система доказательств" в терминах алфавита доказательств, множества доказательств и функции выделения доказанного. Понятие дедуктики.

Теорема Гёделя о неполноте.

Неразрешимость формальной арифметики.