Дискретная математика, модуль 2 из 4

Danił Szubin

12 февраля 2019 г.

Содержание

Аксиоматическая теория натуральных чисел

Конспект главы 1 книги Э.Ландау «Основы анализа» с комментариями Д.Грохольского и В. Таллера

1 Аксиомы

Аксиома 1. $\mathbb{N} \ni 1$

Замечание 1. Т.е. наше множество не пусто; оно содержит вещь, именуемую 1 (читается: единица). Другими словами 1 есть натуральное число.

Аксиома 2. $\forall x \in \mathbb{N}\ \exists!\ x' \in \mathbb{N}$

Замечание 2. Символ x' означает «число. следующее за x».

При записи последующих для чисел x, заданных не в виде одной буквы, мы будем, во избежание путаницы, заключать такие числа в скобки. Аналогично мы будем поступать во всей книге при записи выражений $x + y, xy, x - y, -x, x^y$ и т.п.

Замечание 3. $(x = y) \Longrightarrow (x' = y')$

Аксиома 3. $x' \neq 1 \quad \forall x \in \mathbb{N}$

Замечание 4. Аксиома 3 говорит, что 1 не следует ни за каким натуральным числом. То есть 1 — первое натуралное число.

Аксиома 4. $(x' = y') \Longrightarrow (x = y)$

Аксиома 5. Пусть $M \subset \mathbb{N}$, и M обладает следующими свойствами:

I) $1 \in M$.

II) Если $x \in M$, то и $x' \in M$.

Тогда (утверждает аксиома 5) верно, что $M = \mathbb{N}$.

Замечание 5. На аксиоме 5 основан так называемый «принцип математической ндукции».

2 Сложение

Теорема 1.

$$(x \neq y) \Rightarrow (x' \neq y')$$

Доказательство. В противном случае мы имели бы $x' = y'$ и, следовательно, по аксиоме 4, $x = y$. □

Теорема 2.

$$x' \neq x$$

Доказательство. Пусть M множество тех x, для которых это утверждение справедливо. Проверим, что для множества M выполнены условия I) и II) асиомы 5.

I) По аксиоме 1 и аксиоме 3,

$$1' \neq 1.$$

следовательно, 1 принадлежит множеству M.

II) Если x принадлежит M, то $x' \neq x$, следовательно, по теореме 1, $(x')' \neq x'$, значит, x' также принадлежит M.

В силу аксиомы 5, Mсодержит тогда все натуральные числа, т.е. для каждого x имеем

$$x' \neq x.$$

$\square$

Теорема 3. Если

$$x \neq 1,$$

то существует (и притом по аксиоме 4, только одно) $u \in \mathbb{N}$ такое, что

$$x = u'.$$

Доказательство. Пусть M – множество, состоящее из 1 и тех x, для которых существует u, обладающее указанным свойством (по аксиоме 3, каждое такое $x \neq 1$.). То есть

$$M = \{1\} \sqcup \{x \colon \exists u \in \mathbb{N} \big| x = u'\}.$$

Обоснуем комментарий в скобках, т.е. утверждение $1 \notin \{x \colon \exists u \in \mathbb{N} \big| x = u'\}$. В самом деле, если $x \in \{x \colon \exists u \in \mathbb{N} \big| x = u'\}$, то x является последующим для некоторого $u \in \mathbb{N}$, а 1 не является последующим ни для какого натурального числа согласно аксиоме 3. Поэтому $1 \notin \{x \colon \exists u \in \mathbb{N} \big| x = u'\}$. Если нам удастся доказать, что $M \supset \mathbb{N}$, то тем самым утверждение теоремы 3 будет доказано. Для доказательства включения $M \supset \mathbb{N}$ мы будем использовать аксиому 5. Проверим выполнение условий I) и II) аксиомы 5.

I) $1 \in M$ по определению множества M.

II) Из того, что $x \in M$, выведем $x' \in M$. Включение $x \in M$ означает, что либо $x = 1$, либо x является последующим за каким-то натуральным числом. Однако, x' является последующим за x, поэтому x' тоже удовлетворяет тому свойству, по которому натуральные числа отбираются в множество M, поэтому $x' \in M$.

В силу аксиомы 5, M содержит тогда все натуральные числа; таким образом,

$$\forall x \neq 1$$

существует u такое, что

$$x = u'.$$

$\square$

Замечание 6. Порочный круг (circulus vitious) Это «доказательство» проведённое по схеме:

Теорема. Верно A и B.

Доказательство. Пусть верно A. Рассуждения. Верно B.
Пусть верно B. Другие рассуждения. Верно A. $\square$

Вопрос: Почему плохо?

Ответ : Вместо $A \wedge B$ доказали $A \iff B$

Теорема 4.

$$\exists\, f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

что

$$f(x,1) = x'$$

$$f(x,y') = (f(x,y))'$$

Более того, эта система уравнений имеет единственное решение.

Замечание 7. Иными словами, теорема утверждает, что каждой паре натуральных чисел x, y можно, и притом лишь единственным образом, отнести натуральное число, обозначаемое $x+y$, так, чтобы:

$$x + 1 = x', \forall x \tag{1}$$

$$x + y' = (x+y)', \forall x, y \tag{2}$$

Определение 1. Функция f, определённая выше, называется **операцией сложения**.

Замечание 8. Положим по определению, что $x + y = f(x, y)$

Доказательство. А) Покажем сначала, что если при фиксированном x можно определить $x + y \quad \forall y$:

$$x + 1 = x' \tag{3}$$

$$x + y' = (x+y)', \forall y \tag{4}$$

то этими условиями $x+y$ определяется однозначно. Пусть a_y и b_y определены $\forall y$ и таковы, что

$$a_1 = x' \tag{5}$$

$$b_1 = x' \tag{6}$$

$$a_{y'} = (a_y)' \tag{7}$$

$$b_{y'} = (b_y)' \tag{8}$$

Пусть M – множество тех y, для которых $a_y = b_y$. Проверим, что для множества M верны условия I) и II) аксиомы 5; тогда по аксиоме 5 будет $M \supset \mathbb{N}$, и тем самым А будет доказано.

Проверим условие I). В самом деле:

$$a_1 \overset{(5)}{=} x' \overset{(6)}{=} b_1$$

следовательно $1 \in M$.

Проверим условие II). Если $y \in M$, то

$$a_y = b_y,$$

следовательно по аксиоме 2,

$$(a_y)' = (b_y)' \tag{9}$$

значит

$$a_{y'} \overset{(7)}{=} (a_y)' \overset{(9)}{=} (b_y)' \overset{(8)}{=} b_{y'}$$

и таким образом $y' \in M$.

Поэтому по аксиоме 5 $M \supset \mathbb{N}$. Но из определения множества M следует, что $M \subset \mathbb{N}$. Таким образом, $M = \mathbb{N}$, то есть

$$a_y = b_y, \forall y \in \mathbb{N}.$$

В) Покажем теперь, что $\forall$ фиксированного x действительно возможно определить $x+y$ так, что

$$x + 1 = x' \tag{10}$$

$$x + y' = (x+y)' \quad \forall y \tag{11}$$

Пусть M – множество тех x, для которых такая возможность (притом, в силу А только одна) имеется. Используя аксиому 5, докажем, что $M = \mathbb{N}$, т.е. что возможность эта имеется для всех натуральных x. Проверим условия I) и II) аксиомы 5.

I) Проверим, что $1 \in M$. В самом деле, при $x = 1$ выражение $x + y$ имеет вид $1 + y$. То есть, надо определить $1 + y$ так, что равенства (10) и (11) будут верны при $x = 1$ и всех натуральных y. Итак, определим $1 + y$ при всех натуральных y равенством

$$1 + y \overset{\text{опр}}{=} y' \tag{12}$$

и докажем следующие два равенства (получающиеся из (10) и (11) заменой x на 1):

$$1 + 1 = 1' \tag{10'}$$

$$1 + y' = (1 + y)' \quad \forall y \tag{11'}$$

В самом деле, равенство (10') получится, если в (12) положить $y = 1$.

Докажем теперь, что равенство (11') выполняется $\forall y \in \mathbb{N}$. Сперва заметим, что (12) верно $\forall y \in \mathbb{N}$, поэтому $\forall z \in \mathbb{N}$ верно

$$1 + z = z' \tag{12'}$$

Так как y — натуральное число, то и

$$z = 1 + y \tag{13}$$

тоже является натуральным числом. Таким образом, приходим к выкладке

$$1 + y' \overset{(12)}{=} 1 + (1 + y) \overset{(13)}{=} 1 + z \overset{(12')}{=} z' \overset{(13),\,\text{Акс2}}{=} (1 + y)'$$

Левая часть этой цепочки равенств — это левая часть (11'), а правая часть этой цепочки – это правая часть (11'). Таким образом, равенсво (11') доказано. Итак, часть I) аксиомы 5 проверена.

II) Пусть $x \in M$, т.е. $x + y$ определено $\forall y$ так, что верны равенства

$$x + 1 = x' \tag{10}$$

$$x + y' = (x + y)' \quad \forall y \tag{11}$$

Нам нужно определить $x' + y$ так, чтобы были верны равенства

$$x' + 1 = (x')' \tag{10''}$$

$$x' + y' = (x' + y)' \quad \forall y \tag{11''}$$

которые получаются из (10) и (11) заменой x на x' и означают, что $x' \in M$.

Положим по определению

$$x' + y \overset{\text{опр}}{=} (x + y)' \tag{14}$$

и докажем $(10'')$ и $(11'')$.

Действительно, цепочка равенств

$$x' + 1 \overset{(14)}{=} (x + 1)' \overset{(10),\,\text{Акс2}}{=} (x')'$$

доказывает равенство $(10'')$, а цепочка равенств

$$x' + y' \overset{(14)}{=} (x + y')' \overset{(11),\,\text{Акс2}}{=} ((x + y)')' \overset{(14)}{=} (x' + y)'$$

доказывает равенство $(11'')$. Следовательно и $x' \in M$ поэтому по аксиоме 5 $M = \mathbb{N}$ и пункт B) теоремы 4, а вместе с ним и вся теорема 4, доказаны. □

Теорема 5. (Закон ассоциативности сложения)

$$(x+y)+z = x+(y+z)$$

Доказательство. Пусть x, y фиксированы, и M – множество тех z, для которых верно утверждение теоремы.

I) Проверим для 1, $(x+y)+1 \overset{(1)}{=} (x+y)' \overset{(2)}{=} x+y' \overset{(1)}{=} x+(y+1)$, следовательно, $1 \in M$.

II) Проверим $\forall z$. Пусть $z \in M$. Тогда

$$(x+y)+z = x+(y+z), \tag{15}$$

следовательно

$$(x+y)+z' \overset{(2)}{=} ((x+y)+z)' \overset{(15),\text{ Акс } 2}{=} (x+(y+z))' \overset{(2)}{=} x+(y+z)' \overset{(2)}{=} x+(y+z')$$

так что и $z' \in M$. Тем самым утверждение теоремы справедливо $\forall z$. □

Теорема 6. (Закон коммутативности сложения)

$$x+y = y+x$$

Доказательство. Пусть $y \in \mathbb{N}$ фиксированное. Возьмём множество $M = \{x|\ x+y = y+x,\ x \in \mathbb{N}$. Докажем, что $M = \mathbb{N}$, для чего воспользуемся аксиомой индукции. I) $y+1 = y'$ по (1)
Но по построению из доказательства теоремы 5 имеем: $1+y = y'$ по (12)

$$y+1 = 1+y \Longrightarrow 1 \in M$$

II)Пусть $x \in M$, тогда для него верно

$$x+y = y+x$$

$$(x+y)' \overset{\text{Акс } 2}{=} (y+x)' \overset{(2)}{=} y+x'$$

$$x'+y \overset{(14)}{=} (x+y)' \Longrightarrow x'+y = y+x' \Longrightarrow x' \in M$$

Итак (по аксиоме 5) M $\mathbb{N}$ □

Теорема 7. (9) Если $x \in \mathbb{N}, \quad y \in \mathbb{N}$, то верно ровно одно из условий:

1. $x = y$
2. $\exists! u \in \mathbb{N}| \quad x = y+u$

   Определение 2. В этом случае говорят, что $x > y$

3. $\exists! v \in \mathbb{N}| \quad y = x+v$

   Определение 3. В этом случае говорят, что $x < y$

Доказательство. Без доказательства! □

Замечание 9. $<, >$ — отношения строгого порядка на $\mathbb{N}$. $(<)^{-1} =>$

Положим $x \leqslant y \overset{def}{\Longleftrightarrow} (x = y) \vee (x < y)$. Тогда $\leqslant$ — отношение порядка на $\mathbb{N}$. Положим $\geqslant = (\leqslant)^{-1}$

Определение 4. Порядок $\leqslant$ называется **естественным порядком в** $\mathbb{N}$

Теорема 8. (27) Если $A \subset \mathbb{N},\ A \neq \varnothing$, то $\exists a_* \in A$, такое что $\forall a \in A$ верно $a_* \leqslant a$. То есть в каждом непустом множестве натуральных чисел есть наименьший элемент. То есть множество $\mathbb{N}$ — вполне упорядоченно.

Доказательство. Положим $M = \{x \in \mathbb{N}|\ \forall a \in A$ верно $x \leqslant a\}$. Ранее Ландау доказал, что $\forall x \in \mathbb{N} : 1 \leqslant x$, поэтому $1 \in M$. Кроме того $M \neq \mathbb{N}$. В самом деле: $A \neq \varnothing \Longrightarrow \exists a \in A \overset{\text{Ландау доказал}}{\Longrightarrow} a < a + 1 \overset{def M}{\Longrightarrow} (a+1) \notin M$.

Если бы для $\forall m \in \mathbb{N}$ из $m \in M$ следовало ба $(m+1) \in M$, то (уже доказали, что $1 \in M$ по аксиоме 5) было бы $M = \mathbb{N}$. Но это неверно, так как доказали, что $M \neq \mathbb{N}$.

Поэтому существует такой $m \in M$, что $(m+1) \notin M$. Тогда:
1) $\forall a \in A$ верно $m \leqslant a$ (по определению M и тому, что $m \in M$;
2) $m \in A$.

Докажем 2) от противного. Если $m \notin A$, то $a \in A$, что $m = a$, то есть $m \neq a\ \forall a \in A$. Имеем: $\begin{cases} m \leqslant a \\ m \neq a \end{cases} \overset{def \leqslant, <}{\Longrightarrow} m < a\ \forall a \in A$ Ландау доказал, что из $m < a$ следует $m + 1 \leqslant a$. Но $m + 1 \leqslant a\ \forall a \in A$ означает, что $m \in M$, что неверно. 2) доказано. m — наименьший элемент в A, положим $a_- = m$ $\square$

Замечание 10. Заметим, что из того, что в множестве $\mathbb{N}$ существует наименьший элемент не следует, что $\mathbb{N}$ вполне упорядоченно.

Домашнее задание:

1. *разобрать самостоятельно умножение по Ландау;*
2. *Доказать (со ссылками на Ландау):*
   - $1 \cdot (1 + 1) = 1 + 1$
   - $(1 + 1) \cdot (1 + 1) = 1 + 1 + 1 + 1$
   - $(x + y) \cdot z = xz + yz$

Осталось обсудить целые, рациональные, действительные, p–адические числа. Сделаем это позднее.

3 Булевые функции

$B = \{0,\ 1\}$ — множество возможных значений булевой функции. $\forall n \in \mathbb{N}$ определим $B^n = \underbrace{B \times B \times \cdots \times B}_{n}$ — n–мерный булев куб–область определения булевой функции от n переменных.

Малыми латинскими буквами $a,\ b,\ c, \ldots p,\ q, \ldots$ будем обозначать булевы переменные.

Булевые константы $0 =$ ложь, $\ 1 =$ истина можно вычислить как булевы функции от 0 переменных.

Вопрос: Сколько существует булевых функций от 1 переменных?

	$f_1(p)$	$f_2(p)$	$f_3(p)$	$f_4(p)$
p	0	$\overline{p}$	p	1
0	0	1	0	1
1	0	0	1	1

Имеем 4 функции:
$f_1(p) = 0$ — константа 0;

$f_2(p) = \overline{p}$ — отрицание;
$f_3(p) = p$ — тождественная функция;
$f_4(p) = 1$ — константа 1.

Определение 5. Переменная x_j называется для булевой функции f **фиктивной**, если $\forall i = 1,\ 2, \dots j-1,\ j+1, \dots n$, где $x_i \in \{0,\ 1\}$ верно

$$f(x_1,\ x_2, \dots, x_{j-1},\ 0,\ x_{j+1}, \dots x_n) = f(x_1,\ x_2, \dots, x_{j-1},\ 1,\ x_{j+1}, \dots x_n)$$

f — функция от n булевых переменных, но переменная x_j — фиктивная для f, то есть f от x_j по существу не зависит.

Пример 1. $f(x,\ y) = x + y - y$, y — фиктивная переменная.

3.1 Выбрасывание фиктивной переменной

$f_1(0) = f_1(1)$ — по таблице значений для f_1, поэтому переменная p в $f_1(p)$ фиктивная и f_1 не зависит ни от одной переменной.

Определение 6. Уменьшение числа аргументов функции за счёт отбрасывания фиктивных переменных называется **редукцией булевой функции**.

Если отбрасывание произведено столько раз, что фиктивных переменных не осталось, то говорят, что функция была подвергнута **полной редукции**.

Пример 2. Добавление функции переменной.

Пусть дана булевая функция от 1 переменного p:

p	$f(p)$
0	a
1	b

Добавим фиктивную переменную q, получим функцию двух переменных:

p	q	$f(p,q)$
0	0	a
0	1	a
1	0	b
1	1	b

Определение 7. Переменная, не являющаяся для функции фиктивной называется **существенной** для этой функции.

Замечание 11. Получим, что если у функции k существенных переменных, то можно представить её ($\forall n > k$) как функцию от n переменных. При полной редукции любой из этих получим исходную функцию от k переменных.

Сколько существует булевых функций от двух переменных?

Ответ : Перечислим их все и дадим им названия.

x	y	$f_1(x,y)$	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	1	0	1	0	1	0
0	1	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	1
1	1	0	0	0	0	0	0	0
		const 0	$\overline{x \vee y} = x \downarrow y$	$\overline{x} \wedge y$	$\overline{x}$	$\overline{x \to y}$	$\overline{y}$	$x \oplus y$
			стрелка Пирса	$x < y$		$x > y$		слож. по мод 2

x	y	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	1	0	1	0	1	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1
1	0	1	0	0	0	0	1	1	1	1
1	1	0	1	1	1	1	1	1	1	1
		$\overline{x \wedge y} = x \vert y$ штрих Шеффера	$x \wedge y$	$x \leftrightarrow y$	y	$x \to y$	x	$y \to x$	$x \vee y$	const 1

3.2 Классы булевых функций (классы Поста)

T_0 Сохраняющие 0. $f \in T_0 \iff f(0, \dots 0) = 0$;

T_1 Сохраняющие 1. $f \in T_1 \iff f(1, \dots 1) = 1$;

S Самодейственные. $f \in S \iff \forall x_1, \dots x_n \quad f(x_1, \dots x_n) = \overline{f(\overline{x_1}, \dots \overline{x_n})}$;

M Монотонные. $f \in M \iff (x_1, \dots x_n) > (y_1, \dots y_n) \Longrightarrow f(x_1, \dots x_n) > f(y_1, \dots y_n)$;

Функция также может не принадлежать ни одному классу.

Порядок в B задан так: $0 < 1$.

Порядок в B^n задан так: $(x_1, \dots x_n) > (y_1, \dots y_n) \iff \begin{cases} \forall j = 1 \\ x_j \geqslant y_j \end{cases}$

L Линейные. $f \in L \iff$ полином Жегалкина ф-ииf линеен

Определение 8. Полином Жегалкина — это сумма по модулю 2 мономов Жегалкина.

Определение 9. Моном Жегалкина от трёх переменных $x,\ y,\ z$
степени 0: $0,\ 1$;
степени 1: $x,\ y,\ z$;
степени 2: $xy,\ xz,\ yz$; степени 3: xyz; степени $\geqslant 4$: не существует; сложение: $\oplus$; умножение: $\wedge$

Почему только эти? Казалось бы, многочлен $x^2 = x \wedge x$ тоже имеет степень 2! Но на самом деле он имеет степень 1, так как $x \wedge x = x$.

Пример 3. Многочлены Жегалкина.

$0,\ 1,\ x,\ y,\ z,\ x \oplus 1,\ y \oplus 1,\ z \oplus 1,\ xy,\ xy \oplus 1,\ xz,\ xz \oplus 1,\ yz,\ yz \oplus 1,\ xy \oplus x, xy \oplus x \oplus 1,\ xy \oplus y,\ xy \oplus y \oplus 1,\ xy \oplus z, xy \oplus z \oplus 1, \dots$

Выпишем все многочлены Жегалкина от двух переменных $x,\ y$:

$0,\ 1,\ x,\ y,\ x\oplus1,\ y\oplus1,\ xy,\ xy\oplus1,\ xy\oplus x,\ xy\oplus y,\ xy\oplus x\oplus1,\ xy\oplus y\oplus1,\ xy\oplus x\oplus y, xy\oplus x\oplus y\oplus1, x\oplus y, x\oplus y\oplus1$

16 Штук

Теорема 9. Любая булевая функция однозначно представляется в виде многочлена Жегалкина, то есть если $f\colon B^n \longrightarrow B$, то $\exists a_0,\ a_1, \dots a_n,\ a_{12},\ a_{13}, \dots a_{1n}, \dots a_{21}, \dots a_{2n}, \dots a_{123}, a_{124}, \dots a_{12n}, .$ что $\forall x_1,\ x_2 \dots x_n \in B$ верно $f(x_1, \dots x_n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n \oplus a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus \dots \oplus a_{1n}x_1x_n \oplus a_{23}x_2x_3 \oplus a_{24}x_2x_4 \oplus \dots \oplus a_{1234\dots n}x_1x_2x_3x_4 \dots x_n$

Коэффициенты a можно находить методом неопределённых коэффициентов.

Многочлены, отличающиеся лишь порядком переменных считаем одинаковыми. $(x_1x_2 = x_2x_1)$

Полиномы, отличающиеся лишь мономов считаем одинаковыми.

$f \in L \iff$ многочлен Жегалкина для функции f линеен $\iff$ многочлен Жегалкина для f имеет степень не выше 1, то есть 0 или 1.

Определение 10. Говорят, что функция f получена путём подстановки функции g в функцию h, если $\forall x_j \in B \quad f(x_1, \dots x_n) = h(x_1, \dots g(x_1, x_2, \dots x_k), \dots x_n)$ при этом подставить g можно на место любой переменной x_j. Каждая из $f,\ g,\ h$ может быть от любого количества переменных.

Определение 11. Говорят, что f получена из g путём отождествления переменных $x_1,\ x_2,\ x_3$ функции g если $f(x,\ y,\ z) = g(x,\ x,\ x,\ y,\ z)$

Отождествлять можно $\forall$ кол–во переменных на любых местах (то есть вместо $\forall$ переменных функции g подставены переменные от которых зависит f)

Пример 4. А
$f(x, y) = x \wedge y$;
$g(x, y, z) = x \vee y \vee z$;
Тогда $f(a, b, c) = a \wedge (a \vee b \vee c) = h(a, g(a, b, c))$ подставили g в h, получили f.

Пример 5. В $g(x_1, x_2, x_3, x_4) = (x_1 \wedge x_2) \longrightarrow (x_3 \vee x_4)$ отождествим в g переменные $x_2,\ x_3,\ x_4$. Получим $A(a, b) = g(a, b, b, b) = (a \wedge b) \longrightarrow (b \vee b)$.

Основной вопрос теории полноты систем булевых функций: Найти свойства набора булевых функций (конечного или бесконечного набора) F, что любую булевую функцию от любого числа переменных можно выразить через функции из набора F, используя слудующие операции:
— подстановка; — отождествление переменных;

Приложение этой теории:
Из какого набора элементов можно собрать любую логическую схему (сумматор, и тому подобное) $0 + 0 = 0 \quad 1 + 0 = 0 + 1 = 1 \quad 1 + 1 = 10$