Л.Я. Куликов

Алгебра и теория чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Л11

Л.Я. Куликов
Л11 Алгебра и теория чисел / Л.Я. Куликов – М.: Книга по Требованию, 2023. – 560 с.

ISBN 978-5-458-27102-8

В книге систематически изложены элементы логики, множества и отношения, алгебры и алгебраические системы, основные числовые системы, основы линейной алгебры, включающие системы линейных неравенств, группы, теоретико-числовые темы, кольца и кольца полиномов, полиномы над основными числовыми полями и элементы теории полей.

ISBN 978-5-458-27102-8

Глава первая
ЭЛЕМЕНТЫ ЛОГИКИ

§ 1. ЛОГИКА ВЫСКАЗЫВАНИЙ

Высказывания. Понятие «высказывание» первично. Под высказыванием в логике понимают повествовательное предложение, о котором можно говорить, что оно истинно или ложно. Любое высказывание либо истинно, либо ложно, и никакое высказывание не является одновременно истинным и ложным.

Примеры высказываний: «$0 < 1$», «$2 \cdot 3 = 6$», «5 есть четное число», «1 есть простое число». Истинностное значение первых двух высказываний — «истина», истинностное значение последних двух — «ложь».

Вопросительные и восклицательные предложения не являются высказываниями. Определения не являются высказываниями. Например, определение «целое число называется четным, если оно делится на 2» не является высказыванием. Однако повествовательное предложение «если целое число делится на 2, то оно четное» есть высказывание, и притом истинное. В логике высказываний отвлекаются от смыслового содержания высказывания, ограничиваясь рассмотрением его с той позиции, что оно либо истинно, либо ложно.

В дальнейшем будем понимать под значением высказывания его истинностное значение («истина» или «ложь»). Высказывания будем обозначать прописными латинскими буквами, а их значения, т. е. «истина» или «ложь» — соответственно буквами И и Л.

Логика высказываний изучает связи, которые полностью определяются тем, каким образом одни высказывания строятся из других, называемых *элементарными*. Элементарные высказывания при этом рассматриваются как целые, не разложимые на части, внутренняя структура которых нас не будет интересовать.

Логические операции над высказываниями. Из элементарных высказываний с помощью логических опера-

ций можно получать новые, более сложные высказывания. Истинностное значение сложного высказывания зависит от истинностных значений высказываний, составляющих сложное высказывание. Эта зависимость устанавливается в данных ниже определениях и отражается в истинностных таблицах. В левых столбцах этих таблиц размещаются всевозможные распределения истинностных значений для высказываний, непосредственно составляющих рассматриваемое сложное высказывание. В правом столбце пишут истинностные значения сложного высказывания соответственно распределениям в каждой строке.

Пусть A и B — произвольные высказывания, относительно которых мы не предполагаем, что известны их истинностные значения. *Отрицанием высказывания* A называется новое высказывание, истинное тогда и только тогда, когда A ложно. Отрицание A обозначается через $\neg A$ и читается «не A» или «неверно, что A». Операция отрицания полностью определяется истинностной таблицей

A	$\neg A$
И	Л
Л	И

Пример. Высказывание «неверно, что 5 — четное число», имеющее значение И, есть отрицание ложного высказывания «5 — четное число».

С помощью операции *конъюнкции* из двух высказываний получается одно сложное высказывание, обозначаемое $A \wedge B$. По определению, высказывание $A \wedge B$ истинно тогда и только тогда, когда оба высказывания истинны. Высказывания A и B называются соответственно *первым* и *вторым членами конъюнкции* $A \wedge B$. Запись «$A \wedge B$» читается как «A и B». Истинностная таблица для конъюнкции имеет вид

A	B	$A \wedge B$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

Пример. Высказывание «7 — простое число и 6 — нечетное число» ложно, как конъюнкция двух высказываний, одно из которых ложно.

Дизъюнкцией двух высказываний A и B называется высказывание, обозначаемое $A \vee B$, истинное в том и только в том случае, когда хотя бы одно из высказываний

A и B истинно. Соответственно этому высказывание $A \vee B$ ложно в том и только том случае, когда и A и B оба ложны. Высказывания A и B называются соответственно *первым и вторым членами дизъюнкции* $A \vee B$. Читается запись $A \vee B$ как «A или B». Союз «или» в данном случае носит неразделительный смысл, поскольку высказывание $A \vee B$ истинно и при истинности обоих членов. Дизъюнкция имеет следующую истинностную таблицу:

A	B	$A \vee B$
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

Пример. Высказывание «$3 < 8$ или $5 < 2$», являющееся дизъюнкцией двух высказываний, одно из которых истинно, имеет значение И.

Высказывание, обозначаемое $A \to B$, ложное в том и только в том случае, когда A истинно, а B ложно, называется *импликацией* с посылкой A и заключением B. Высказывание $A \to B$ читается как «если A, то B», или «A влечет B», или «из A следует B». Истинностная таблица для импликации такова:

A	B	$A \to B$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

Отметим, что между посылкой и заключением могут отсутствовать причинно-следственные связи, но это не может повлиять на истинность или ложность импликации. Например, высказывание «если 5 — простое число, то биссектриса равностороннего треугольника является медианой» будет истинным, хотя в обычном понимании второе не следует из первого. Истинным также будет высказывание «если $2+2=5$, то $6+3=9$», поскольку истинно его заключение. При данном определении, если заключение истинно, импликация будет истинной независимо от истинностного значения посылки. В том случае, когда ложна посылка, импликация будет истинна независимо от истинностного значения заключения. Эти обстоятельства кратко формулируют так: «истина следует из чего угодно», «из ложного следует все, что угодно».

Высказывание, обозначаемое через $A \leftrightarrow B$, истинное в том и только в том случае, когда A и B имеют одно и то же истинностное значение, называется *эквиваленцией*. Высказывание $A \leftrightarrow B$ читается как «A тогда и только тогда, когда B», или «A эквивалентно B», или «A необходимо и достаточно для B». Истинностная таблица для эквиваленции имеет вид

A	B	$A \leftrightarrow B$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	И

Пример. Высказывание «$2 > 5$ тогда и только тогда, когда $3 + 0 = 4$» истинно, как эквиваленция двух ложных высказываний.

Формулы логики высказываний. Основной задачей логики высказываний является изучение логических форм сложных высказываний с помощью логических операций. Понятие логической формы сложного высказывания уточняется с помощью вводимого ниже понятия формулы логики высказываний.

Для обозначения высказываний будем использовать малые буквы конца латинского алфавита (возможно, с индексами). При этом, какое высказывание (истинное или ложное) будет обозначать та или иная буква, предполагаем неизвестным. Фактически буквы

(1) $p,\ q,\ r,\ \ldots,\ p_1,\ q_1,\ r_1,\ \ldots$

будут играть роль переменных, принимающих в качестве значений истинностные значения «истина» и «ложь». Обычно эти переменные называются *пропозициональными переменными*; будем также называть их *элементарными формулами* или *атомами*.

Для построения формул логики высказываний кроме символов (1) используются знаки логических операций

$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow,$$

а также символы, обеспечивающие возможность однозначного прочтения формул, — левая и правая скобки: (,).

Понятие *формулы логики высказываний* определим следующим образом:

1) элементарные формулы (атомы) суть формулы логики высказываний;

2) если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$ тоже являются формулами логики высказываний;

3) только те выражения являются формулами логики высказываний, для которых это следует из 1) и 2).

Определение формулы содержит перечисление правил образования формул. Согласно определению, всякая формула логики высказываний либо есть атом, либо образуется из атомов в результате последовательного применения правила 2). Например, выражения

$$p, (\neg q), ((r \vee s) \to t), ((p \vee (\neg p)) \leftrightarrow (p \to q))$$

являются формулами логики высказываний.

Обозначать произвольные формулы логики высказываний будем большими буквами латинского алфавита (возможно, с индексами):

$$A, B, C, \ldots, A_1 B_1, C_1, \ldots$$

При этом не исключено, что одна и та же формула может быть обозначена различными буквами.

Заметим, что никакой атом не имеет вида $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$. Такой вид имеют сложные формулы.

В первой главе вместо «формула логики высказываний» часто будем говорить просто «формула» там, где это не может вызвать недоразумений.

Число скобок в формулах можно уменьшить, введя соглашения: 1) в сложной формуле будем опускать внешнюю пару скобок. 2) упорядочим знаки логических операций по «старшинству»: $\leftrightarrow$, $\to$, $\vee$, $\wedge$, $\neg$. В этом списке знак $\leftrightarrow$ имеет самую большую область действия, а знак $\neg$ — самую маленькую. Под областью действия знака операции понимаются те части формулы, к которым «применяется» (на которые «действует») рассматриваемое вхождение этого знака. Договоримся опускать во всякой формуле те пары скобок, которые можно восстановить, учитывая «порядок старшинства». При восстановлении скобок сначала расставляются все скобки, относящиеся ко всем вхождениям знака $\neg$ (при этом мы продвигаемся слева направо), затем ко всем вхождениям знака $\wedge$ и т. д.

Пример. В формуле $B \leftrightarrow \neg C \vee D \wedge A$ скобки восстанавливаются следующими шагами:

$$B \leftrightarrow (\neg C) \vee D \wedge A, \qquad B \leftrightarrow ((\neg C) \vee (D \wedge A)),$$
$$B \leftrightarrow (\neg C) \vee (D \wedge A), \qquad (B \leftrightarrow ((\neg C) \vee (D \wedge A))).$$

Не всякая формула может быть записана без скобок. Например, в формулах $A \to (B \to C)$, $\neg(A \to B)$ дальнейшее исключение скобок невозможно.

Законы логики. Существуют формулы, которые принимают значение И независимо от того, какие значения принимают входящие в них атомы. Например,

$$A \vee \neg A,\ A \to A,\ (A \to B) \vee (B \to A),\ A \to (B \to A).$$

Такие формулы играют особую роль в логике.

ОПРЕДЕЛЕНИЕ. Формула логики высказываний, которая принимает значение «истина» при любом распределении значений входящих в эту формулу атомов, называется *тождественно истинной формулой*, *тавтологией* или *законом логики*.

Существуют формулы, которые принимают значение «ложь» независимо от того, какие значения принимают входящие в них атомы. Например,

$$A \wedge \neg A,\ (A \vee \neg A) \to (A \wedge \neg A).$$

ОПРЕДЕЛЕНИЕ. Формула логики высказываний, принимающая значение «ложь» при любом распределении значений входящих в эту формулу атомов, называется *тождественно ложной формулой* или *противоречием*.

Легко убедиться, что если A — противоречие, то $\neg A$ будет тавтологией, и наоборот. Например, формула $p \wedge \neg p$ тождественно ложна, а $\neg(p \wedge \neg p)$ — тавтология.

Существуют формулы, которые принимают как значение И, так и значение Л в зависимости от того, какие значения принимают входящие в них атомы. Например,

$$A \vee A,\ A \to B,\ A \wedge B \to B \wedge C.$$

Запись $\models A$ означает, что формула A есть тавтология; например, $\models A \vee \neg A$. Этот закон носит название *закона исключенного третьего*.

ТЕОРЕМА 1.1. *Если A и $(A \to B)$ — тавтологии, то B — тавтология.*

Доказательство. Пусть A и $(A \to B)$ — тавтологии. Допустим, что для какого-либо распределения истинностных значений атомов, входящих в A и B, формула B принимает значение «ложь». Так как A — тавтология, то при том же распределении истинностных значений атомов формула A принимает значение И. Следовательно, формула $(A \to B)$ получит значение Л, что противоречит предположению о том, что $(A \to B)$ есть тавтология. Значит, фор-

мула B принимает значение И при любом распределении истинностных значений ее атомов. □*)

ТЕОРЕМА 1.2. *Пусть A — формула, содержащая атомы $p_1, \ldots, p_n$, а B — формула, получающаяся из A одновременной подстановкой формул $A_1, \ldots, A_n$ вместо $p_1, \ldots, p_n$ соответственно. Если A — тавтология, то и B — тавтология.*

Доказательство. Пусть задано произвольное распределение истинностных значений атомов, входящих в B. Для этого распределения значений атомов формулы $A_1, \ldots, A_n$ примут соответственно истинностные значения $a_1, \ldots, a_n$. Если атомам $p_1, \ldots, p_n$ придать соответственно значения $a_1, \ldots, a_n$, то в результате истинностное значение формулы A совпадет со значением формулы B при заданном распределении значений атомов, входящих в B. Так как, по условию, A — тавтология, то B при заданном распределении значений атомов принимает значение «истина», т. е. B тоже тавтология. □

Эта теорема показывает, что любая подстановка в тавтологию приводит к тавтологии.

Ниже (в теореме 1.3) приведены часто встречающиеся законы логики.

ТЕОРЕМА 1.3. *Следующие формулы являются тавтологиями:*

Тавтологические импликации:

$p \wedge (p \to q) \to q$	— *закон заключения;*
$p \wedge q \to p$ $p \wedge q \to q$	— *законы удаления конъюнкции;*
$p \to p \vee q$ $q \to p \vee q$	— *законы введения дизъюнкции;*
$(p \vee q) \wedge \neg q \to p$	— *закон удаления дизъюнкции;*
$p \to \neg\neg p$	— *закон введения двойного отрицания*
$\neg\neg p \to p$	— *закон удаления двойного отрицания;*
$(p \to q) \wedge (q \to p) \to (p \leftrightarrow q)$	— *закон введения эквиваленции;*

*) □ — знак, означающий, что доказательство теоремы или предложения закончено.

$(p \leftrightarrow q) \rightarrow (p \rightarrow q)$
$(p \leftrightarrow q) \rightarrow (q \rightarrow p)$ — *законы удаления эквиваленции;*

$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$ — *закон контрапозиции;*

$(\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \rightarrow p$ — *закон доказательства от противного;*

$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ — *закон силлогизма;*

$(p \rightarrow r) \wedge (q \rightarrow r) \rightarrow (p \vee q \rightarrow r)$ — *закон сложения посылок;*

$(p \rightarrow q) \wedge (p \rightarrow r) \rightarrow (p \rightarrow q \wedge r)$ — *закон умножения заключений;*

$(p \leftrightarrow q) \wedge (q \leftrightarrow r) \rightarrow (p \leftrightarrow r)$ — *закон транзитивности эквиваленции.*

Тавтологические эквиваленции:

$p \leftrightarrow p$ — *закон тождества;*

$p \wedge p \leftrightarrow p$ — *закон идемпотентности конъюнкции;*

$p \vee p \leftrightarrow p$ — *закон идемпотентности дизъюнкции;*

$p \wedge q \leftrightarrow q \wedge p$ — *закон коммутативности конъюнкции;*

$p \vee q \leftrightarrow q \vee p$ — *закон коммутативности дизъюнкции;*

$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$ — *закон ассоциативности конъюнкции;*

$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$ — *закон ассоциативности дизъюнкции;*

$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ — *закон дистрибутивности конъюнкции относительно дизъюнкции;*

$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$ — *закон дистрибутивности дизъюнкции относительно конъюнкции;*

$\neg \neg p \leftrightarrow p$ — *закон двойного отрицания;*

$(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$ — *закон коммутативности эквиваленции;*

$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ — *закон контрапозиции;*

$\neg (p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ — *закон отрицания дизъюнкции;*

$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$ — *закон отрицания конъюнкции;*

$(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$ — *закон противоположности;*

$p \rightarrow (q \rightarrow r) \leftrightarrow q \rightarrow (p \rightarrow r)$ — *закон перестановки посылок.*

Тавтологии, выражающие одни операции через другие:

$p \rightarrow q \leftrightarrow \neg p \vee q;$
$p \rightarrow q \leftrightarrow \neg(p \wedge \neg q);$
$p \vee q \leftrightarrow \neg p \rightarrow q;$
$p \vee q \leftrightarrow \neg(\neg p \wedge \neg q);$
$p \wedge q \leftrightarrow \neg(p \rightarrow \neg q);$
$p \wedge q \leftrightarrow \neg(\neg p \vee \neg q);$
$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$

Чтобы доказать, что каждая из приведенных формул является тавтологией, надо применить метод истинностных таблиц, т. е. составить для каждой формулы истинностную таблицу и убедиться, что в каждой строке крайнего правого столбца стоит буква И.

Рассмотрим, к примеру, закон силлогизма:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$p \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$
И	И	И	И	И	И	И
И	И	Л	И	Л	Л	И
И	Л	И	Л	И	И	И
И	Л	Л	Л	И	Л	И
Л	И	И	И	И	И	И
Л	И	Л	И	Л	И	И
Л	Л	И	И	И	И	И
Л	Л	Л	И	И	И	И

Заметим, что на основании законов ассоциативности можно опускать скобки, посредством которых осуществляется группировка членов многочленных конъюнкций и дизъюнкций. Из закона двойного отрицания следует, что при желании всегда можно избежать двух подряд стоящих знаков «$\neg$» и более.

Упражнения

1. Составьте таблицу истинности для каждой из формул

(a) $p \to q \leftrightarrow \neg p \vee q$; (c) $r \to (r \to q)$;

(b) $p \to \neg (q \wedge r)$; (d) $(p \wedge q) \to (s \wedge \neg s \to p \vee s)$.

2. Что можно сказать об истинностном значении высказывания $\neg A \wedge B \leftrightarrow A \vee B$, если значение высказывания $A \to B$ есть Л?

3. Докажите, что формулы теоремы 1.3 являются тавтологиями.

4. Пусть C — формула, в которой выделено некоторое вхождение формулы A, а C' — формула, полученная из C заменой этого вхождения формулы A на формулу B. Докажите, что если $A \leftrightarrow B$ — тавтология, то $C \leftrightarrow C'$ — тоже тавтология.

5. Сколько строк имеет истинностная таблица для формулы логики высказываний, имеющей n различных атомов?

6. Пусть формула A построена из атомов $p_1, \ldots, p_n$ только с помощью знаков $\neg$, $\wedge$, $\vee$, а формула A^* получена из A заменой каждого вхождения символа $\wedge$ символом $\vee$ и наоборот и заменой каждого вхождения p_i вхождением $\neg p_i$ и наоборот. Докажите, что формула $\neg A \leftrightarrow A^*$ — тавтология.

7. Докажите, что следующие формулы являются тавтологиями:

(a) $(A \wedge B) \to C \leftrightarrow A \to (B \to C)$;
(b) $(A \wedge B) \to C \leftrightarrow (A \wedge \neg C) \to \neg B$;
(c) $\neg (A \to B) \leftrightarrow A \wedge \neg B$;
(d) $(A \to B) \wedge \neg B \to \neg A$;
(e) $A \to (\neg A \to B)$;
(f) $A \to (B \to A)$;
(g) $(\neg A \to A) \to A$;
(h) $(A \to B) \to (A \wedge C \to B \wedge C)$;
(i) $(A \to B) \wedge (C \to \mathrm{D}) \to (A \wedge C \to B \wedge \mathrm{D})$;
(k) $(A \to B) \wedge (C \to \mathrm{D}) \to (A \vee C \to B \vee \mathrm{D})$;
(l) $\neg (A \leftrightarrow B) \leftrightarrow (\neg (A \to B) \vee \neg (B \to A))$.

8. Докажите, что никакая формула логики высказываний, при построении которой используются только знаки логических операций $\wedge$, $\vee$, не является ни тавтологией, ни противоречием.

§ 2. ЛОГИЧЕСКОЕ СЛЕДСТВИЕ

Основные определения. Пусть $A_1, \ldots, A_m, B$ — формулы логики высказываний.

ОПРЕДЕЛЕНИЕ. Формула B называется *логическим следствием формул* $A_1, \ldots, A_m$, если при любом выборе истинностных значений атомов, входящих в формулы $A_1, \ldots, A_m, B$, формула B получает значение «истина» всякий раз, когда каждая из формул $A_1, \ldots, A_m$ получает значение «истина».

Запись

$$A_1, \ldots, A_m \models B$$