Лекция 2

§ 2. Исчисление логики высказываний

Аристотель родился в 322 г. до н.э., а в 330 г. до н.э. родился Евклид.

Опрос: 1. Кто из них старше?

2. Чем прославился Евклид?

Он предложил другой подход к тому, как получать истинные утверждения. Аристотель и мы вслед за ним говорим, что истинность конкретных утверждений – это забота конкретных наук, а мы только манипулируем с этими утверждениями посредством логических связок. Т.е. он, конечно, говорил не так, но смысл таков.

Евклид, будучи математиком, понимал эту проблему глубже, чем какой-то философ Аристотель. Во-первых, он говорил, что нам нужны некоторые утверждения, истинность которых мы принимает безоговорочно. Во-вторых, нам нужны правила, по которым мы из этих утверждений будем получать новые истинные утверждения.

Формализуем подход Евклида.

Есть формальный язык (его слова которого мы договорились называть формулами).

Фиксируем некоторое множество формул. Их мы будем называть **аксиомами**.

Фиксируем некоторое множество функций, определённых на множестве формул, со значениями снова в множестве формул. Они не обязаны быть всюду определёнными. Мы будем называть их **правилами вывода**.

Этот набор формул, аксиом и правил вывода будем называть **аксиоматической системой**.

Определение. Если φ – некоторое правило вывода, а формула $q = \varphi(p_1, p_2, \ldots, p_n)$, то формулу q называют **непосредственным следствием** формул $p_1, p_2, \ldots, p_n$, полученным с помощью правила φ.

Обычно правил бывает немного. Поэтому для них не используют обозначения, а записывают следующим образом: $\frac{p_1,\ p_2,\ \ldots,\ p_n}{q}$

Определение. Следующие формулы называются выводимыми в данной аксиоматической системе:

1) аксиома;
2) непосредственное следствие выводимых формул;
3) других выводимых формул нет.

Определение. Выводимые формулы, не являющиеся аксиомами, называются **формальными теоремами** в данной аксиоматической системе.

Эпитет «формальная» мы будем применять для того, чтобы отличать их от теорем нашего курса.

А чего мы хотим? Строя аксиоматическую систему, мы всегда будем хотеть три вещи.

1) Приняв аксиомы за истинные утверждения, мы должны быть уверены, что среди выводимых утверждений не будет ложных. Это называют **непротиворечивостью** системы.

2) Хорошо бы, чтобы любое истинное утверждение было теоремой. Это называется **полнотой** системы.

3) Хорошо бы иметь алгоритм, позволяющий для любой формулы определять, теорема она или нет. Это называется алгоритмической **разрешимостью**.

Мечтать не вредно.

Давайте строить аксиоматическую систему для логики высказываний.

Язык мы определили в предыдущем параграфе.

Система аксиом может быть выбрана по-разному. Её состав определяется двумя факторами.

Во-первых, количеством связок в языке. Из теоремы Поста следует, что при построении языка высказываний можно было бы обойтись только связками $\neg$ и $\to$. Тогда было бы достаточно трёх аксиом, чтобы построить непротиворечивую, полную и разрешимую теорию логики высказываний. Нам же ещё требуются аксиомы, которые описывают логическую зависимость между другими связками.

Во-вторых, мы не боремся за независимость аксиом, т.е. вполне возможно, что какие-то аксиомы на самом деле являются теоремами. Но на доказательство этих теорем требуется время, а у нас его не так много.

Итак, список аксиом. Он разбит на группы.

I. $x_1 \to (x_2 \to x_1)$

$(x_1 \to (x_2 \to x_3)) \to ((x_1 \to x_2) \to (x_1 \to x_3))$

II. $x_1 \wedge x_2 \to x_1$

$x_1 \wedge x_2 \to x_2$

$(x_1 \to x_2) \to ((x_1 \to x_3) \to (x_1 \to x_2 \wedge x_3))$

III. $x_1 \to x_1 \vee x_2$

$x_2 \to x_1 \vee x_2$

$(x_1 \to x_3) \to ((x_2 \to x_3) \to (x_1 \vee x_2 \to x_3))$

IV. $(x_1 \leftrightarrow x_2) \to (x_1 \to x_2)$

$(x_1 \leftrightarrow x_2) \to (x_2 \to x_1)$

$(x_1 \to x_2) \to ((x_2 \to x_1) \to (x_1 \leftrightarrow x_2))$

V. $x_1 \to \neg (\neg x_1)$

$\neg (\neg x_1) \to x_1$

$(x_1 \to x_2) \to (\neg x_2 \to \neg x_1)$

Правила вывода.

1) Правило подстановки. Пусть p и q – некоторые формулы. Если в записи p имеется предметный символ x_n, то все вхождения этого символа в формулу p заменяем на формулу q. Результат такой замены будем обозначать $S_q^{x_n}(p)$. Правило подстановки согласно нашим договорённостям запишется как $\frac{p,\ q,\ x_n}{S_q^{x_n}(p)}$.

2) Правило заключения. Его мы сразу запишем в договорном виде: $\frac{x_1,\ x_1 \to x_2}{x_2}$. По латыни это правило называют modus ponens. Мы будем его называть так же и для краткости обозначать MP.

Пример 1. Формула $x_1 \to x_1$ является формальной теоремой.

$(x_1 \to (x_2 \to x_3)) \to ((x_1 \to x_2) \to (x_1 \to x_3))$ – аксиома

$(x_1 \to (x_2 \to x_1)) \to ((x_1 \to x_2) \to (x_1 \to x_1))$ – подстановка x_1 на место x_3.

$((x_1 \to x_2) \to (x_1 \to x_1))$ – MP к аксиоме $x_1 \to (x_2 \to x_1)$ и предыдущей формуле.

$(x_1 \to (x_2 \to x_1)) \to (x_1 \to x_1)$ – подстановка $(x_2 \to x_1)$ на место x_2.

$(x_1 \to x_1)$ – MP к аксиоме $x_1 \to (x_2 \to x_1)$ и предыдущей формуле.

Пример 2. Формула $x_1 \wedge x_2 \to x_2 \wedge x_1$ является формальной теоремой.

$(x_1 \to x_2) \to ((x_1 \to x_3) \to (x_1 \to x_2 \wedge x_3))$ – аксиома

$(x_1 \wedge x_2 \to x_2) \to ((x_1 \wedge x_2 \to x_3) \to (x_1 \wedge x_2 \to x_2 \wedge x_3))$ – подстановка $x_1 \wedge x_2$ на место x_1.

$((x_1 \wedge x_2 \to x_3) \to (x_1 \wedge x_2 \to x_2 \wedge x_3))$ – MP к аксиоме $x_1 \wedge x_2 \to x_2$ и предыдущей формуле.

$(x_1 \wedge x_2 \to x_1) \to (x_1 \wedge x_2 \to x_2 \wedge x_1)$ – подстановка x_1 на место x_3.

$(x_1 \wedge x_2 \to x_2 \wedge x_1)$ – МР к аксиоме $x_1 \wedge x_2 \to x_1$ и предыдущей формуле.

Мы сейчас введём ещё одну операцию над формулами, обобщающую правило подстановки.

Пусть p – некоторая формула, содержащая в своей записи предметные символы $x_1, x_2, \dots, x_n$. Пусть $q_1, q_2, \dots, q_n$ – произвольные формулы. Через $S^{x_1 x_2 .. x_n}_{q_1 q_2 \dots q_n}(p)$ обозначим формулу, полученную из p одновременной заменой x_1 на q_1, x_2 на q_2, …, x_n на q_n.

Вопрос. Всегда ли $S^{x_1 x_2 .. x_n}_{q_1 q_2 \dots q_n}(p)$ совпадает с $(S^{x_n}_{q_n} \dots (S^{x_2}_{q_2}(S^{x_1}_{q_1}(p))\dots))$?

Выберем в качестве p аксиому $x_1 \to (x_2 \to x_1)$, в качестве q_1 формулу $(x_1 \wedge x_2)$, в качестве формулу $(\neg x_2)$. Тогда

$S^{x_1 x_2}_{q_1 q_2}(p) = (x_1 \wedge x_2) \to ((\neg x_2) \to (x_1 \wedge x_2))$,

а

$S^{x_2}_{q_2}(S^{x_1}_{q_1}(t)) = S^{x_2}_{q_2}((x_1 \wedge x_2) \to (x_2 \to (x_1 \wedge x_2))) = (x_1 \wedge (\neg x_2)) \to ((\neg x_2) \to (x_1 \wedge (\neg x_2)))$.

Не сошлось. Вторая формула – это формальная теорема. А первая?

Теорема 4. Пусть t – некоторая формула, являющаяся аксиомой или формальной теоремой, $x_1, x_2, \dots, x_n$ – предметные символы, имеющиеся в записи t. Пусть $q_1, q_2, \dots, q_n$ – произвольные формулы. Тогда $S^{x_1 x_2 .. x_n}_{q_1 q_2 \dots q_n}(t)$ также является теоремой.

Доказательство. Поскольку предметных символов у нас бесконечно много, то мы сначала все предметные символы формулы q_1, которые имеются также в формуле t, заменим на предметные символы с номерами, бóльшими, чем номера символов встречающимися в записях t и q_1. Новую формулу обозначим q_1'. Через t_1 обозначим формулу $S^{x_1}_{q_1'}(t)$. По определению t_1 – формальная теорема. Аналогично получим t_2 из t_1 и q_2. И т.д., формула t_n получается из t_{n-1} и q_n. Все t_i – формальные теоремы. А теперь в t_n каждый новенький предметный символ заменим на тот, которого он подменял («мавр сделал своё дело, мавр должен уйти»). Получающаяся формула снова будет формальной теоремой, и она совпадает с $S^{x_1 x_2 .. x_n}_{q_1 q_2 \dots q_n}(t)$.

Следствие. Пусть p, q и r – произвольные формулы. Тогда следующие формулы являются формальными теоремами.

I. $p \to (q \to p)$
   $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$

II. $p \wedge q \to p$
   $p \wedge q \to q$
   $(p \to q) \to ((p \to r) \to (p \to q \wedge r))$

III. $p \to p \vee q$
   $q \to p \vee q$
   $(p \to r) \to ((q \to r) \to (p \vee q \to r))$

IV. $(p \leftrightarrow q) \to (p \to q)$
   $(p \leftrightarrow q) \to (q \to p)$
   $(p \to q) \to ((q \to p) \to (p \leftrightarrow q))$

V. $p \to \neg(\neg p)$
   $\neg(\neg p) \to p$
   $(p \to q) \to (\neg q \to \neg p)$

Примечание. В большинстве учебников по математической логике формулы, перечисленные в этом следствии, называют *схемами аксиом*, а аксиомами называют те конкретные формулы, которые получаются после записи вместо p, q и r конкретных формул. Тем самым получается бесконечное (правда, всё-таки счётное) множество аксиом.

Мы, конечно, тоже, говоря, например, что формула $p \to (q \to p)$ является формальной теоремой, имеем в виду, что формальной теоремой является та формула, которая получается, когда мы выписали вместо p, q и r их выражения через предметные символы. Конечно, мы тоже получаем бесконечное множество теорем, но разве это удивительно?

Процесс формального доказательства теорем весьма трудоёмкий. Даже такая простая теорема как $x_1 \to x_1$ потребовала пяти шагов. А воспринимается она как очевидная, Аристотель считал, что её надо брать за аксиому, т.е. то, что не нуждается в доказательстве. Мы сейчас будем изготовлять инструмент, который существенно облегчает доказательство формальных теорем. Для этого нам будет удобно расширять список аксиом, добавляя к ним какие-либо формулы. То множество формул, которые будут добавлены к аксиомам, мы будем обозначать большими греческими буквами. Чтобы легко отличать их от латинских, начнём с Γ. Тот факт, что формула q выводима из объединения Γ с множеством аксиом будем записывать $\Gamma \vdash q$. Ясно, что такие утверждения мы уже теоремами называть не будем. Более того, нам придется сузить само понятие вывода.

Определение. Выводом формулы q из Γ называют конечную последовательность формул $p_1, p_2, \ldots, p_n$ такую, что $p_n = q$, и каждая из формул p_i при $1 \le i \le n$ является либо формальной теоремой, либо формулой из Γ, либо получается применением правила MP к каким-либо формулам с меньшими номерами.

Заметьте, в этом определении запрещено пользоваться подстановками!

В обыденной жизни математика такой вывод называют доказательством.

Ясно, что отношение выводимости обладает следующими свойствами:

1. Если $\Gamma \subset \Delta$ и $\Gamma \vdash q$, то $\Delta \vdash q$.
2. Если $\Gamma \cup \{p\} \vdash q$ и $\Gamma \vdash p$, то $\Gamma \vdash q$.
3. Если $\Gamma \vdash q$, то существует конечное подмножество Λ формул из Γ такое, что $\Lambda \vdash q$.

Отметим, что ни вывод формулы q, ни множество Λ в пункте 3 не определены однозначно.

Давайте посмотрим на доказательство какой-нибудь теоремы из школьной геометрии. Например, «Диагонали прямоугольника равны». Конечно, для начала надо вспомнить определение прямоугольника: «Прямоугольником называется четырёхугольник, у которого все углы прямы». Значит, на самом деле школьная теорема звучит так: «Если у четырёхугольника все углы прямые (высказывание p), то отрезки, соединяющие его противоположные вершины, равны (высказывание q). Тем самым, речь идет о выводимости из аксиом $p \to q$. И это мы называем теоремой.

А что мы делаем на самом деле?

«Пусть $ABCD$ – прямоугольник» – присоединяем к аксиомам высказывание p, т.е. $\Gamma = \{p\}$

«Тогда прямые AB и DC параллельны как два перпендикуляра к одной прямой AD» – высказывание q_1, выведенное из p когда-то ранее.

«Прямые AD и BC параллельны как два перпендикуляра к одной прямой AB» – высказывание q_2, выведенное из p когда-то ранее.

«Четырёхугольник $ABCD$ – параллелограмм» – это не высказывание, а определение.

«Тогда отрезки AD и BC равны как противоположные стороны параллелограмма» – высказывание q_3, выведенное ранее из теоремы о равенстве внутренних накрест лежащих углов при двух параллельных и секущей, в которой опять-таки фигурирует p.

«Треугольники ABC и ABD равны как прямоугольные (опять p!) по двум катетам» – высказывание q_3.

«Значит, $AC = BD$.» – высказывание q.

Последовательность q_1, q_2, q_3 – это вывод q из p, хотя неполный, поскольку для каждого из q_i надо было бы расписать, как оно-то получается. Но и так видно, что на каждом шаге вывода возникало p. Т.е. мы, конечно, получили $p \vdash q$. А хотели $\vdash p \to q$. Тем не менее, смело заявляем, что доказали, что хотели.

Ясно, что такие «доказательства», мы наблюдаем со времён Евклида. А где доказательство что это «доказательство»?

Так вот, доказательство этому способу доказательств в 1930 году дал Жак Эрбан. Это утверждение называют Теоремой дедукции.

Теорема 5. Если $\Gamma \cup \{ p \} \vdash q$, то $\Gamma \vdash p \to q$.

Доказательство. Пусть $\Gamma \cup \{ p \} \vdash q$ и $q_1, q_2, \ldots, q_n$ – вывод формулы q. Доказательство проведём индукцией по n. Если $n = 1$, то q либо формальная теорема, либо формула из Γ, либо $q = p$, поскольку MP применять ещё не к чему.

1) q – формальная теорема или формула из Γ. Вывод строится так:

$$\underset{}{q},\ \underset{\text{фор.т.}}{q \to (p \to q)},\ \underset{\text{MP}}{p \to q}$$

2) $q = p$. Вывод строится так:

$$\underset{\text{фор.т.}}{q \to q = p \to q}$$

Пусть для $k < n$ уже доказано. Рассмотрим $k = n$.

Теперь у нас 4 случая: q либо формальная теорема, либо формула из Γ, либо $q = p$, либо q_n получена по правилу MP из каких-то формул q_m и q_j для $m < n$ и $j < n$. Первые три случая не отличаются от варианта $n = 1$. В четвёртом случае q_j должна иметь вид $(q_m \to q_n)$ (чтобы применить MP!). Поскольку формул q_m и q_j расположены в выводе формулы q_n, то всё, написано перед каждой из них, – это её вывод из $\Gamma \cup \{ p \}$. По предположению индукции для формул $p \to q_j = p \to (q_m \to q_n)$ и $p \to q_m$ имеется вывод из Γ. Пишем теперь вывод формулы $p \to q_n$.

$$\underbrace{\ldots, \ldots, \ldots, \ldots,}_{\text{вывод } p \to q_j} \underbrace{p \to (q_m \to q_n)}_{\text{сама } p \to q_j}, \underbrace{(p \to (q_m \to q_n)) \to ((p \to q_m) \to (p \to q_n))}_{\text{фор.т.}}, \underbrace{((p \to q_m) \to (p \to q_n))}_{\text{MP}},$$

$$\underbrace{\ldots, \ldots, \ldots, \ldots,}_{\text{вывод } p \to q_m} \underbrace{(p \to q_m)}_{\text{сама } p \to q_m}, \underbrace{(p \to q_n)}_{\text{MP}}$$

Упражнение 1. Верно ли утверждение, обратное Теореме дедукции?

Упражнение 2. Вопрос на засыпку. В доказательстве Теоремы дедукции мы пользуемся тем же приёмом: вместо доказательства импликации предполагаем выполнение условия $\Gamma \cup \{ p \} \vdash q$ и приходим (да ещё с индукцией (!), т.е. многократно используя посылку) $\Gamma \vdash p \to q$. Разве это не порочный круг?