Змістовий модуль 5. Формальні теорії (числення)

Тема 12. Загальний опис формальної теорії. Числення висловлень

План лекції.

- Загальний опис формальної теорії
  - Означення формальної теорії, або числення
  - Означення доведення
  - Повнота теорії. Несуперечливість теорії. Розв’язність теорії
- Числення висловлень
  - Мова і правила виведення числення висловлень
  - Приклади доведення в численні висловлень. Теорема дедукції
  - Повнота і несуперечність числення висловлень
  - Розв’язність числення висловлень

5.1. Загальний опис формальної теорії

Криза основ математики на межі XIX–XX століття, зумовлена відкриттям парадоксів теорії множин, спонукала вчених шукати шляхи виходу з такого стану. Один із шляхів запропонував Д. Гільберт, який висунув програму порятунку класичної математики.

Гільберт виходив з того, що математика має справу переважно з ідеальними об’єктами. Такі об’єкти використовують актуальну (завершену) нескінченність, вони далеко виходять за межі безпосереднього осмислення та обґрунтування на інтуїтивній основі. За Гільбертом, ідеальні об’єкти та твердження потрібні лише як проміжні ланки для отримання реальних результатів і в цьому розумінні *не є необхідними*. Проте математика не може існувати без ідеальних об’єктів, вони необхідні для ефективності міркувань, без них *не можна отримати реальні результати*. Тому потрібно обґрунтувати *принципову можливість* видалення ідеальних об’єктів і тверджень із виведень реальних тверджень. Доведення можливості такої перебудови виведень необхідно виконувати максимально надійними, інтуїтивно переконливими засобами, що не викликають сумнівів. Такі засоби Гільберт назвав *фінітними*, тому що вони мають уникати використання актуальної нескінченності. Для фінітного доведення теорем про перебудову виведень потрібно дати математичне уточнення мови й логічного виведення. Це означає побудову формальної теорії для відповідного розділу математики. Після формалізації необхідно довести суто фінітними методами несуперечливість і повноту отриманої формальної теорії (точне означення цих понять буде дано нижче).

Формальна теорія – це спосіб опису логіки без приписування пропозиційним змінним, предикатам і формулам якогось значення. За ідеєю фундаторів формальних теорій (Гільберт і інші) таким способом можна уникнути багатьох незручностей, які виникають при застосуванні в логіці природної мови, яка допускає двозначність, недомовленість, переінакшування початково закладеного значення й смислу.

Формальна теорія – це гра зі знаками, гра зі словами та реченнями, складеними з цих знаків. При цьому мається на увазі, що правила утворення слів із знаків і правила гри зі словами та реченнями заздалегідь узгоджені, точно й строго прописані. В основі формальної теорії – *мова*, на якій «розмовляє теорія». На перше місце виходить *синтаксис* цієї мови, тобто спосіб побудови формул, у противагу *семантиці* (смисловій стороні одиниць мови).

5.1.1. Означення формальної теорії, або числення

Формальна теорія $\mathcal{T}$ складається з таких компонент.

1. Множина знаків, які утворюють *алфавіт* мови теорії.
2. Множина слів, складених із знаків алфавіту, ці слова називають *формулами*.
3. Підмножина формул усієї множини формул. Формули цієї підмножини називають *аксіомами*.
4. Множина *правил виведення*, за допомогою яких із формул отримують формули.

У мову теорії $\mathcal{T}$ входить алфавіт і формули. Кількість аксіом може бути скінченною або нескінченною. В останньому випадку для наочного подання їх задають за допомогою *схем аксіом*. За схемами можна легко виписати самі аксіоми. Під *логічними аксіомами*, як правило, розуміють *аксіоми базової логіки*, над якою надбудовуються конкретні теорії за рахунок додавання нових аксіом, які відображають специфіку конкретної теорії. Такі аксіоми називають *нелогічними*.

5.1.2. Означення доведення

Нехай Γ – множина формул. Формула A *вивідна* в теорії $\mathcal{T}$ із множини *гіпотез* Γ, якщо існує скінченна послідовність

$$A_1, A_2, \ldots, A_n,$$

у якій кожна формула A_i є або аксіомою, або гіпотезою, або отримана з попередніх формул послідовності за допомогою правил виведення, і A_n – це формула A.

Наведена послідовність – це *виведення* формули A із множини гіпотез Γ. Для виведення використовують позначення:

$$\Gamma \vdash A.$$

Коли $\Gamma = \varnothing$, то виведення називають *доведенням* формули A, а саму формулу A називають *теоремою* теорії $\mathcal{T}$ (тобто теорема – це формула, вивідна тільки з аксіом, без гіпотез). Для теорем використовують символічний запис $\vdash A$.

Якщо $\Gamma \vdash A$, то очевидно, що $\Gamma, \Delta \vdash A$, де Γ і Δ – будь-які множини формул (тобто при додаванні зайвих гіпотез виводимість зберігається).

5.1.3. Повнота теорії. Несуперечливість теорії. Розв'язність теорії

Формальну теорію називають *повною*, якщо для всякого висловлення A маємо:

$$\vdash A \text{ або } \vdash \neg A.$$

Зауваження. Висловлення в логіці першого порядку – це закрита формула, тобто формула, усі змінні якої зв'язані кванторами.

За ідеєю засновника числення предикатів Фреге, будь-яка правильно побудована формула, точне висловлення, має бути теоремою, тобто має бути твердженням, яке можна довести. Це означає, що числення висловлень і числення предикатів повинні бути *повними теоріями*. Очікування Фреге справдилися (див. далі теореми 5.3 і 5.7). Але, як виявилося, більш сильні теорії, які включають арифметику, неповні. Це доведено Ґеделем (див. далі теореми 5.11 і 5.12).

Формальну теорію називають *несуперечливою*, якщо в ній не є доказовою формула $A \wedge \neg A$, де A – довільне висловлення теорії.

Смисл умови несуперечливості в тому, що її можна довести в межах самої формальної теорії. Нажаль, як виявилося, таким способом неможливо довести навіть несуперечливість формальної арифметики.

Під час вивчення формальних теорій ми маємо справу з двома типами висловлень: по-перше, з висловленнями самої теорії (теоремами), котрі розглядають як чисто формальні об'єкти, визначені раніше, а по-друге, з *висловленнями про теорію* (про властивості її теорем, доведень тощо). Ці висловлення про теорію формулюють на мові, зовнішній по відношенню до теорії, – на метамові, і називають *метатеоремами*. Наприклад, якщо вдалося побудувати виведення B із $A_1, \ldots, A_k$, то висловлення

$$«A_1, \ldots, A_k \vdash B»$$

є метатеоремою; її можна розглядати як додаткове правило виведення, яке можна приєднати до множини правил теорії та використовувати в подальшому.

Ще одна характеристика формальної теорії – це її розв'язність. Формальну теорію $\mathcal{T}$ називають *розв'язною*, якщо існує алгоритм, який для будь-якої формули мови визначає, чи є вона теоремою в $\mathcal{T}$, чи ні.

5.2. Числення висловлень

5.2.1. Мова і правила виведення числення висловлень

Числення висловлень – це така формальна теорія.

1. Алфавіт.

- Знаки змінних висловлень (пропозиційних букв): p, q, r, …
- Знаки логічних зв'язок $\vee$, $\wedge$, $\neg$, $\rightarrow$.
- Допоміжні знаки (,).

2. Формули.

- Змінне висловлення є формулою.
- Якщо A і B – формули, то $(A\vee B)$, $(A\wedge B)$, $(A\rightarrow B)$ і $\neg A$ – формули.
- Інших формул немає.

Зовнішні дужки у формулах як правило домовляються випускати: наприклад, замість $(A\vee B)$ пишуть $A\vee B$. Замість синтаксично зручнішого знака $\neg$ можна використовувати риску над формулою.

3. Аксіоми. Наведемо тут дві системи аксіом. Перша з них безпосередньо використовує всі логічні операції.

Система аксіом I (система Кліні).

I.1. $A \to (B \to A)$

I.2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

I.3. $(A \wedge B) \to A$

I.4. $(A \wedge B) \to B$

I.5. $A \to (B \to (A \wedge B))$

I.6. $A \to (A \vee B)$

I.7. $B \to (A \vee B)$

I.8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$

I.9. $(A \to B) \to ((A \to \neg B) \to \neg A)$

I.10. $\neg\neg A \to A$

Інша система аксіом використовує лише дві логічні зв'язки $\neg$ і $\to$; при цьому скорочується алфавіт числення (вилучаються знаки $\vee$ і $\wedge$) і відповідно означення формули. Операції $\vee$ і $\wedge$ розглядаються не як зв'язки числення висловлень, а як скорочення для деяких формул: $A\vee B$ заміняє $\neg A\to B$, $A\wedge B$ заміняє $\neg(A\to\neg B)$. Використовувати ці скорочення зручно, але не обов'язково. Як результат система аксіом стає набагато компактнішою.

Система аксіом II.

II.1. $A\to(B\to A)$

II.2. $(A\to(B\to C))\to((A\to B)\to(A\to C))$

II.3. $(\neg A\to\neg B)\to((\neg A\to B)\to A)$

Наведені дві системи аксіом рівносильні в тому сенсі, що породжують одну й ту саму множину формул. Зрозуміло, що таке твердження вимагає доведення, яке полягає в тому, що доводиться виводимість усіх аксіом системи II із аксіом системи I і, навпаки, системи I із системи II (з урахуванням зауважень щодо $\vee$ і $\wedge$).

Можливі й інші системи аксіом, рівносильні наведеним двом системам.

Котра з наведених систем аксіом краща? Це залежить від погляду. Система II компактніша й осяжніша, відповідно компактніші й доведення різних її властивостей. З іншої сторони, у багатшій системі I коротші виведення різних формул.

4. Правила виведення.

Правило виведення одне – *modus ponens*:

$$\frac{A,\ A \to B}{B}.$$

Зауваження. У цьому описі числення висловлень формули, які описують аксіоми, і формули, які використані у правилі виведення – це *схеми формул*. Схема формули, наприклад, $A \to B$, позначає множину всіх тих формул числення, котрі можна отримати, коли замість букв схеми формули (їх називають «метазмінними») підставити формули числення. Наприклад, якщо A замінити на p, а B – на $p \wedge q$, то зі схеми формул $A \to B$ одержимо формулу $p \to (p \wedge q)$.

5.2.2. Приклади доведення в численні висловлень. Теорема дедукції

Приклад 5.1. Доведемо, що формула $A \to A$ є вивідною в системі аксіом II:

$$\vdash A \to A.$$

1. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$. Підстановка в аксіому II.2 $A \to A$ замість B і A замість C.
2. $A \to ((A \to A) \to A)$. Підстановка в аксіому II.1 $A \to A$ замість B.
3. $(A \to (A \to A)) \to (A \to A)$. Із кроків 2 і 1 за правилом modus ponens.
4. $A \to (A \to A)$. Підстановка в аксіому II.1 A замість B.
5. $A \to A$. Із кроків 4 і 3 за правилом modus ponens.

Отже, $A \to A$ є теоремою числення висловлень.

Приклад 5.2. Доведемо, що із A виводиться $B{\to}A$ в системі аксіом II:

$$A \vdash B{\to}A.$$

Нехай формула A є вивідною. Тоді з A і аксіоми II.1 за правилом modus ponens одержимо

$$\frac{A,\, A \to (B \to A)}{B \to A},$$

що доводить потрібну виводимість.

Як уже було зазначено, всяку доведену в численні виводимість виду $\Gamma \vdash A$, де Γ – список формул, A – формула, можна розглядати як правило виведення $\frac{\Gamma}{A}$, яке можна приєднати до наявних правил. Отриману нами виводимість $A \vdash B{\to}A$ можна розглядати як правило $\frac{A}{B \to A}$: «якщо формула A є вивідною, то вивідна і формула $B{\to}A$, де B – будь-яка формула». Скористаємося цим правилом у наступному прикладі.

Приклад 5.3. $A{\to}B,\, B{\to}C \vdash A{\to}C$.

1. $A{\to}(B{\to}C)$. Із гіпотези $B{\to}C$ за новим правилом $\frac{A}{B \to A}$. Тут використано підстановки $B{\to}C$ замість A і A замість B, тобто маємо $\frac{B \to C}{A \to (B \to C)}$.
2. $(A{\to}B){\to}(A{\to}C)$. Із кроку 1 і аксіоми II.2 за правилом modus ponens.
3. $A{\to}C$. Із гіпотези $A{\to}B$ і кроку 2 за правилом modus ponens.

Для отримання виведень у численні висловлень дуже корисною є наступна метатеорема.

Теорема 5.1 (теорема дедукції). Якщо $\Gamma, A \vdash B$, то $\Gamma \vdash (A \to B)$.

Доведення. Скористаємося системою аксіом II.

Нехай $\Gamma, A \vdash B$. Тоді існує виведення $B_1, \ldots, B_n$ з Γ, A, таке, що $B_n = B$. Доведемо за індукцією, що для довільного $k \le n$ виконується $\Gamma \vdash (A \to B_k)$. Розглянемо спочатку B_1. Як перша формула виведення, B_1 повинна бути або аксіомою, або міститися в Γ, або співпадати з A. Із схеми аксіом II.1 випливає, що $B_1 \to (A \to B_1)$ є аксіомою. Якщо B_1 – аксіома або B_1 міститься в Γ, то за правилом modus ponens $A \to B_1$ вивідна з Γ. Якщо ж $B_1 = A$, то з прикладу 5.1 маємо $A \to A$, тобто $A \to B_1$. У кожному разі $\Gamma \vdash (A \to B_1)$.

Припустимо тепер, що $\Gamma \vdash (A \to B_i)$ для будь-якого $i < k$, і розглянемо B_k. Можливими є чотири випадки: а) B_k – аксіома; б) $B_k \in \Gamma$; в) $B_k = A$; г) B_k виводиться з якихось попередніх формул B_j, B_l за правилом modus ponens, але тоді B_l матиме вигляд $B_j \to B_k$. У випадках «а» – «в» доведення таке саме, як і для B_1 (випадки «а», «б» – за допомогою аксіоми II.1, випадок «в» – за допомогою прикладу 5.1). У випадку «г» за індуктивним припущенням маємо

$$\Gamma \vdash (A \to B_j) \qquad (1)$$

і $\Gamma \vdash (A \to B_l)$, тобто

$$\Gamma \vdash (A \to (B_j \to B_k)). \qquad (2)$$

Підставимо в схему аксіом II.2 B_j замість B і B_k замість C. Отримаємо:

$$(A\to(B_j\to B_k)\to((A\to B_j)\to(A\to B_k)). \tag{3}$$

Застосуємо правило modus ponens до (2) і (3), отримаємо

$$\Gamma\vdash((A\to B_j)\to(A\to B_k)). \tag{4}$$

Якщо тепер застосувати modus ponens до (1) і (4), отримаємо $\Gamma\vdash(A\to B_k)$. Залишається взяти $k = n$. Теорему дедукції доведено.

Зазначимо, що при побудові виведень використовувалися тільки аксіоми II.1 і II.2, котрі є і в системі аксіом I. Тому наведене доведення теореми дедукції годиться і для числення висловлень, яке ґрунтується на системі аксіом I.

Приклад 5.4. Як перше застосування теореми дедукції, доведемо, що $A \vdash B$ тоді і тільки тоді, коли $\vdash A \to B$.

Для доведення покладемо $\Gamma = \varnothing$.

Приклад 5.5. Доведемо, що $A\to(B\to C)$, $B\vdash A\to C$.

1. $A\to(B\to C)$. Гіпотеза.
2. A. Гіпотеза.
3. $B\to C$. Modus ponens до 2 і 1.
4. B. Гіпотеза.
5. C. Modus ponens до 4 і 3.
6. $A\to(B\to C)$, B, $A\vdash C$. Кроки 1–5.
7. $A\to(B\to C)$, $B\vdash A\to C$. За теоремою дедукції.

Приклад 5.6. Як ще одне застосування теореми дедукції, доведемо, що аксіома ІІ.3 вивідна із системи аксіом І.

1. Підставимо в І.9 $\neg A$ замість A. Отримаємо:

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

2. Застосуємо два рази правило modus ponens до кроку 1, тоді матимемо:

$$\neg A \to B,\ \neg A \to \neg B \vdash \neg\neg A.$$

3. Оскільки з аксіоми І.10 випливає за правилом modus ponens що $\neg\neg A \vdash A$, то за транзитивністю виводимості із 2 отримаємо

$$\neg A \to B,\ \neg A \to \neg B \vdash A.$$

4. Переставимо гіпотези в 3, оскільки порядок гіпотез неважливий:

$$\neg A \to \neg B,\ \neg A \to B \vdash A.$$

5. До кроку 4 два рази застосуємо теорему дедукції, як результат отримаємо аксіому ІІ.3:

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

Приклад 5.7. Дуже поширеним методом математичних доведень є метод *доведення від протилежного*: Допускаємо, що A істинне і показуємо, що по-перше, із A виводиться B, а, по-друге, із A виводиться $\neg B$, що неможливо, і, отже, A фальшиве, тобто $\neg A$ істинне. Цей метод можна сформулювати як правило: «якщо $\Gamma, A \vdash B$ і $\Gamma, A \vdash \neg B$, то $\Gamma \vdash \neg A$». Доведемо, що в численні висловлень це правило виконується. Справді, за теоремою дедукції, якщо $\Gamma, A \vdash B$ і $\Gamma, A \vdash \neg B$, то $\Gamma \vdash A \to B$ та $\Gamma \vdash A \to \neg B$. Із цих двох імплікацій і аксіоми І.9 подвійним застосуванням правила modus ponens отримаємо $\Gamma \vdash \neg A$. Доведене правило називають *правилом уведення заперечення*.

Приклад 5.8. Доведемо тепер закон виключеного третього: $\vdash A\vee\neg A$.

1. $\neg(A\vee\neg A), A \vdash A\vee\neg A$. Аксіома I.6, підстановка $\neg A$ замість B, правило modus ponens.
2. $\neg(A\vee\neg A), A \vdash \neg(A\vee\neg A)$. Очевидно.
3. Застосуємо до кроків 1 і 2 доведене в прикладі 5.6 правило введення заперечення, отримаємо: $\neg(A\vee\neg A) \vdash \neg A$.
4. Аналогічно доводимо, що $\neg(A\vee\neg A) \vdash \neg\neg A$.
5. Застосуємо до кроків 3 і 4 правило введення заперечення, отримаємо $\vdash \neg\neg(A\vee\neg A)$.
6. За допомогою аксіоми I.10 і правила modus ponens знімаємо подвійне заперечення в кроці 5, отримуємо $\vdash (A\vee\neg A)$.

5.2.3. Повнота і несуперечливість числення висловлень

Теореми числення висловлень в термінах істинності (пропозиційна логіка) характеризуються так.

Теорема 5.2. Формула є загальнозначущою (тавтологією) в пропозиційній логіці тоді і тільки тоді, коли вона є теоремою в численні висловлень.

Іншими словами, для числення висловлень вірним є твердження:

$$\models A \text{ *тоді і тільки тоді, коли* } \vdash A.$$

Без доведення.

Теорема 5.3. Числення висловлень – повна теорія.

Доведення випливає із твердження «із $\models A$ випливає $\vdash A$» теореми 5.2.

Теорема 5.4. Числення висловлень – несуперечлива теорія.

Доведення випливає із твердження «із $\vdash A$ випливає $\models A$» теореми 5.2. Справді, якби в численні висловлень була доказовою формула $A=B\wedge\neg B$, то було би істинним твердження $B\wedge\neg B$. Але остання формула фальшива.

Насамкінець зазначимо таке. Еквівалентні формули булевої алгебри (тобто такі, що *одночасно* є T чи F) з'єднують знаком $\equiv$. У пропозиційній логіці еквівалентність виражається знаком $\leftrightarrow$ (див. 1.1). Якщо $A\equiv B$, то формула $A\leftrightarrow B$ є загальнозначущим висловленням. У численні висловлень формула $A\leftrightarrow B$ є скороченням формули $(A\rightarrow B)\wedge(B\rightarrow A)$. У силу теореми 5.2 всяка така еквівалентність, наприклад, $\neg(A\vee B)\leftrightarrow(\neg A\wedge\neg B)$ є теоремою числення висловлень.

5.2.4. Розв'язність числення висловлень

Теорема 5.5. Числення висловлень – розв'язна теорія.

Доведення. Розв'язувальний алгоритм для формули A числення висловлень полягає в обчисленні значень A при всіх інтерпретаціях. Застосування теореми 5.2 завершує доведення.