УВОД У МАТЕМАТИЧКУ ЛОГИКУ

Небојша Икодиновић

– Белешке, 2021/22 –

Испитна питања:

1. Исказне формуле [исказна алгебра; индуктивна дефиниција формула; дрво формуле и потформуле; валуације; задовољиве формуле]
2. Таутологије [важне таутологије; еквивалентне формуле; теорема о замени еквивалената и примене]
3. Принцип математичке индукције [индуктивне дефиниције сабирања и множења; основне особине сабирања и множења]
4. Формалне граматике и формалне теорије [појмови: алфабет, реч, правила за трансформацију; језик одређен формалном граматиком; формалне теорије и извођење у формалној теорији]
5. Исказни рачун Ł [теорема сагласности; извођење из хипотеза и став дедукције]
6. Потпуност исказног рачуна Ł [примене става дедукције; теорема потпуности]
7. Природна дедукција у исказној логици [основна и изведена правила природне дедукције]
8. Предикатске формуле [Универзум и предикати (пример коначног универзума са бар једним унарним и бар једним бинарним предикатом); исказне функције; квантификатори; атомске и предикатске формуле]
9. Правила природне дедукције за квантификаторе [теореме предикатске логике]
10. Аксиоме: екстензионалности, празног скупа, пара, уније и партитивног скупа; схема издвајања [Да ли постоји скуп свих скупова?]
11. Булове операције и Декартов производ [унија, пресек, разлика и везе са инклузијом; Де Морганови закони; уређен пар, тројка, четворка, ...; Декартов производ]
12. Релације и функције [композиција релација; композиција функција; инверзна релација; 1-1 функције, на-функције, бијекције]
13. Примери релација и функција: рестрикције; једнакост и идентичко пресликавање; релације еквиваленције; количнички скуп
14. Примери релација и функција: бинарне операције; карактеристичне функције; празна функција; директне и индиректне слике
15. Аксиоме: замене, регуларности, бесконачности; Скуп природних бројева
16. Уређење и аритметичке операције скупа $\mathbb{N}$ [принцип потпуне индукције; добро уређење; теорема рекурзије и основне аритметичке операције]
17. Коначни скупови; Основни комбинаторни принципи [Дирихлеов принцип и последице; принцип збира и производа]
18. Бесконачни скупови; Кантор-Бернштајнова теорема; теорема $|A| < |\mathcal{P}(A)|$
19. Пребројиви и непребројиви скупови
20. Бројевне структуре [конструкције структура целих и рационалних бројева]
21. Структуре и њихов вокабулар [језик првог реда; изрази; атомске формуле; формуле; вредност израза; истинитост формула/реченица]
22. Различите интерпретације вокабулара. Теорије [Групе; Булове алгебре; Линеарна уређења]
23. Семантичка и синтаксна последица [правила природне дедукције за једнакост и последице]
24. Аксиома избора [принцип доброг уређења; Цорнова лема]

1. Исказна алгебра

1.1 **Исказне формуле (одн. логички изрази)**

1

Пример 1. Очигледно је да реченице:

1. *Земља се окреће око Сунца или се Земља не окреће око Сунца.*
2. *Број* $1,4142$ *јесте решење једначине* $x^2 = 2$ *или* $1,4142$ *није решење једначине* $x^2 = 2$.

Током људске историје, исказ

Земља се окреће око Сунца

некада је сматран нетачним, а некада тачним. Без обзира на то, увек се знало да је тачан исказ:

Земља се окреће око Сунца или Земља се не окреће око Сунца.

имају исту структуру '$\cdots$ ***или*** ***не*** $\cdots$', и да их управо због тога сматрамо тачним без обзира на то да ли је исказ који се налази на месту тачкица тачан или нетачан. Одавде се јасно види значај везника *или* и *не* у структури наведених реченица. Још много аналогних примера можемо саставити. Анализирајмо даље и следећа два закључивања.

Ако некоме кажемо	*Ако си ти у праву, онда сам ја луд.*
и додамо	*Ја нисам луд.*
саговорник ће знати да смо рекли	*Ти ниси у праву.*

Знамо да важи	*Ако је четвороугао $ABCD$ квадрат, онда је $ABCD$ правоугаоник.*
и ако уочимо да	*Четвороугао $ABCD$ није правоугаоник.*
закључујемо да	*Четвороугао $ABCD$ није квадрат.*

Ова два закључивања, иако се односе на потпуно различите ситуације, суштински се не разликују.

Претпоставке:	*Ако* $\cdots$, *онда* $***$.
	Не $***$.
Закључак:	*Не* $\cdots$.

И овога пута, исправност наведених закључивања оправдавамо везницима '*Ако* $\cdots$, *онда* $***$' и '*Не* $***$' не обазирући се много на смисао реченица које стоје уместо $\cdots$ и $***$.

Шаблоне закључивања, попут оних из претходног примера, описаћемо посебном врстом алгебарских израза, тзв. логичким изразима.

У исказној логици централно место заузимају тзв. *логички везници*: *и*, *или*, *не*, *ако . . .* , *онда . . .* , *ако и само ако*. Помоћу њих градимо сложене исказе полазећи од неких једноставних. Истинитост сложенијих исказа одређујемо само на основу тзв. истинитосних таблица придружених везницима. Ово начело, које је у основи дефиниције исказних везника, познато је као **принцип истинитосне функционалности**. За сваки везник, истинитосном таблицом је одређена одговарајућа (рачунска) операција са *истином*, коју означавамо 1, и *лажи*, означеном 0.

	$\neg$
0	1
1	0

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Наведене операције називамо и **логичким операцијама**:

негација $\neg$ – *не* (унарни везник),

конјункција[3] $\wedge$ – *и* (бинарни везник),

дисјункција $\vee$ – *или* (бинарни везник),

импликација $\Rightarrow$ – *ако . . . , онда . . .* (бинарни везник),

еквиваленција $\Leftrightarrow$ – *ако и само ако*[4] (бинарни везник).

Скуп истинитосних вредности $\{0, 1\}$, заједно са логичким операцијама

$$(\{0, 1\}, \vee, \wedge, \neg, \Rightarrow, \Leftrightarrow, 0, 1)$$

представља тзв. **исказну алгебру**. Попут бројевних израза које користимо бавећи се неком бројевном алгебром (коју чини скуп бројева са одговарајућим операцијама), градимо и алгебраске изразе прилагођене исказној алгебри. Ове алгебарске изразе називамо *исказним формулама*. Променљиве су најједноставније исказне формуле; сложеније исказне формуле добијамо применом логичких операција на изграђене формуле.

Пример 2. Исказне формуле, тј. изразе исказне алгебре, можемо замишљати као алгебарски опис структуре исказа – реченице чији нам смисао није важан већ само то да ли су тачне или нетачне. Ако променљиве p, q, r означавају неке једноставне исказе, онда формула:

- $(p \wedge q) \Rightarrow r$ представља сложени исказ *'ако p и q, онда r'*;
- $p \vee \neg p$ представља сложени исказ *'p или не p'*; итд.

Исказне формуле дефинишемо као и било коју другу врсту израза тзв. *индуктивним дефиницијама*[5].

Најпре прецизирамо које симболе користимо при грађењу исказних формула. Исказне формуле градимо од:

- исказних слова (или исказних променљивих) $a, b, c, \ldots, p, q, r, \ldots, p_1, q_1, \ldots$, при чему претпостављамо да их има неограничено много,
- логичких константи $\top$ и $\bot$,
- логичких везника $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$,

употребом заграда на уобичајени начин.

Логичку константу $\top$ замишљамо као ознаку неког исказа који је тачан, а $\bot$ као ознаку исказа који је нетачан.

Индуктивна дефиниција исказних формула:

[3] Савремени правопис тражи, у нескладу са вуковским начелима, да се *конјункција* не пише са њ него са нј, као и *конјунктив*, *конјунктивитис* и *инјекција*.

[4] Уместо *ако и само ако*, често се краће пише *акко*. Слично је и у другим језицима; нпр. на Енглеском језику, скраћеница за if and only if је iff.

[5] Индуктивним дефиницијама се одређују математички објекти саграђени постепено почевши од најједноставнијих, основних, базних објеката, а сложенији објекти се граде неким утврђеним правилима применљивим на већ саграђене, једноставније објекте.

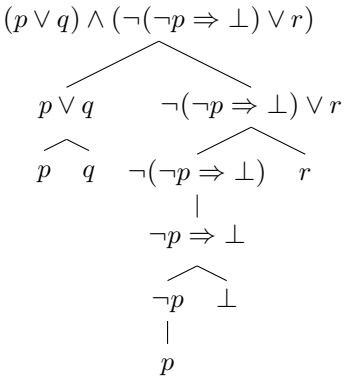
- Исказна слова и логичке константе су исказне формуле. Називамо их и *атомским исказним формулама*.
- ако је α исказна формула, онда је и $\neg\alpha$ исказна формула;
- ако су α и β исказне формуле, онда су и $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ исказне формуле.

Наведеном (индуктивном) дефиницијом најпре су уведене најједноставније исказне формуле: свако исказно слово и свака логичка константа представља једну исказну формулу. Затим је прецизирано како се формирају сложеније исказне формуле: полазећи од најједноставнијих исказних формула, помоћу наведених правила градимо нове формуле, које даље користимо за изградњу још сложенијих формула. Подразумева се да се исказне формуле могу градити само на овај начин.

Претпостављамо да су познате уобичајене конвенције о брисању заграда, па их овде нећемо све наводити. Истичемо само договор о приоритету логичких везника: $\neg$ је везник највећег приоритета, за њим следе $\vee$ и $\wedge$ који су подједнаког приоритета, а за њима $\Rightarrow$ и $\Leftrightarrow$, такође једнаког приоритета.

Постепена изградња сваке исказне формуле сликовито се приказује тзв. **дрветом формуле**.

Пример 3. Нацртајмо дрво формуле $(p \vee q) \wedge (\neg(\neg p \Rightarrow \bot) \vee r)$:



Дрво јасно показује кораке изградње формуле. Наравно, да бисмо поједноставили запис, изостављамо заграде када год то не доводи до забуне.

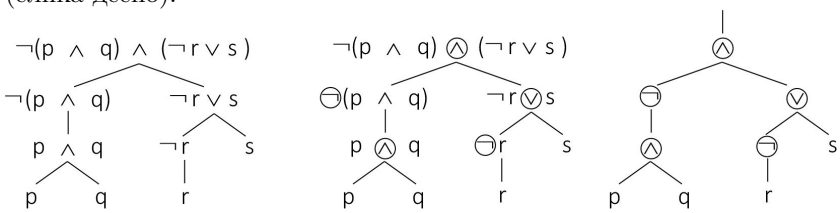
Потформуле неке формуле су њени делови који су и сами формуле, при чему се сматра да је и свака формула потформула саме себе. Потформуле неке исказне формуле јесу формуле које се појављују индуктивном изградњом посматране исказне формуле. Потформуле неке исказне формуле су природно уређене у структуру која подсећа на дрво – рачва се само на једну страну. Места дрвета где стоје потформуле зову се *чворови*. Сваки чвор има нула или једног непосредног претходника, а непосредних наследника може да има нула, један, или два. Када чвор нема претходника зове

се *корен*, а када нема наследника зове се *лист*. Дрво има само један корен. Чвор дрвета који није лист назива се *унутрашњи чвор*. Сваки унутрашњи чвор дрвета формуле одређен је заправо једним логичким везником. Приказ дрвета формуле се често поједоставља тако што се сваки унутрашњи чвор означава само одговарајућим везником. *Главни везник* формуле јесте логички везник који је последњи уведен приликом њеног грађења, одн. везник који одговара корену поједностављеног приказа дрвета.[7].

У корену дрвета исказне формуле налази се сама формула, док су листови атомске формуле које учествују у грађењу корена.

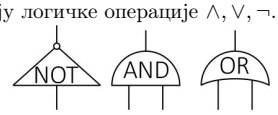
[7] Главни везник неке формуле могли бисмо звати и главна операција (логичког) израза. Главна операција израза истиче се приликом именовања израза. Нпр. израз $(a+b)\cdot(a-b)$ називамо *производом*, јер је $\cdot$ 'главна' операција. Слично, формулу $p \vee q \Rightarrow p \wedge q$ називамо '*импликацијом*', јер је $\Rightarrow$ главни везник. Приметимо да је формула $p \vee (q \Rightarrow p \wedge q)$ 'дисјункција', а да је $(p \vee q \Rightarrow p) \wedge q$ 'конјункција'.

Пример 4. На сликама испод, приказано је дрво исказне формуле $\neg(p \wedge q) \wedge (\neg r \vee s)$ (слика лево) и његова поједностављена варијанта (слика десно).



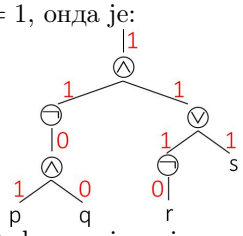
Поједностављену верзију дрвета формуле можемо посматрамо и као тзв. **логичко коло**. Листове дрвета посматрамо као *улазе*, а корен као *излаз* логичког кола. Остали чворови дрвета представљају *пролазе* у којима се реализују логичке операције. Улази и излази се могу налазити у два стања, означена са 0 и 1. За дате вредности улаза логичко коло даје излаз који је у складу са логичком функцијом коју представља.

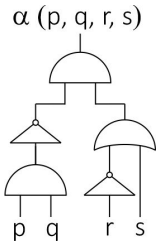
Логичка кола играју основну улогу у конструкцији дигиталних рачунара. Углавном се посматрају три врсте основних пролаза у којима се реализују логичке операције $\wedge, \vee, \neg$.



Исказна слова p, q, r, s одређују улазе, док излаз одређује полазна формула коју можемо означити $\alpha(p,q,r,s)$ да бисмо истакли да њена истинитосна вредност зависи од истинитосних вредности слова p, q, r, s. Нпр. ако је $p=1$, $q=0$, $r=0$, $s=1$, онда је:

$$\alpha(1,0,0,1) = \neg(1\wedge 0)\wedge(\neg 0\wedge 1) = \cdots = 1$$





Свака исказна формула одређује (логичку) функцију која истинитосним вредностима исказних слова (улаза, аргумената) додељује тачно једну истинитосну вредност посматране формуле.

Формулу α означавамо $\alpha(p_1,p_2,\ldots,p_n)$ када желимо да истакнемо чињеницу да у грађењу формуле α учествују слова p_1, p_2, $\ldots$, p_n. Додељујући словима $p_1,\ldots,p_n$ редом истинитосне вредности $v_1,\ldots,v_n$ из $\{0,1\}$, добијамо јединствену *истинитосну* вредност $\alpha(v_1,\ldots,v_n)$. Додељивање истинитосних вредности (0 или 1) исказним словима назива се *валуација* исказних слова. Подразумева се да је истинитосна вредност формуле $\bot$ једнака 0, а истинитосна вредност формуле $\top$ једнака 1.

Уопште, ако је алгебарски израз састављен од променљивих, константи и операција које се појављују у некој конкретној алгебарској структури, онда се вредност тог израза може израчунати када се променљивама доделе конкретне вредности из домена те структуре. Све ово важи и за исказне формуле, тј. алгебарске изразе који одговарају исказној алгебри.

Пример 5. Истинитосну вредност формуле $(p \Rightarrow q) \wedge (q \Rightarrow p)$, за

$p = 1$, $q = 0$, рачунамо користећи следећи сажети запис:

$$\begin{array}{ccccccc} (p & \Rightarrow & q) & \wedge & (q & \Rightarrow & p) \\ 1 & & 0 & & 0 & & 1 \\ & 0 & & & & 1 & \\ & & & 0 & & & \end{array}$$

или једноставније

$$\begin{array}{ccccccc} (p & \Rightarrow & q) & \wedge & (q & \Rightarrow & p) \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}$$

Испод исказних слова записујемо истинитосне вредности одређене валуацијом, а испод логичких везника вредности одређене одговарајућом таблицом.

За n исказних слова, постоји укупно 2^n различитих валуација. Одређивање истинитосних вредности неке формуле за све могуће валуације њених исказних слова приказујемо у облику таблице познате под називом *истинитосна таблица*.

Пример 6. Истинитосну таблицу исказне формуле можемо формирати и у следећем једноставнијем облику.

$$\begin{array}{ccccccccc} (p & \Rightarrow & q) & \wedge & (\neg & q & \vee & \neg & p) \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}$$

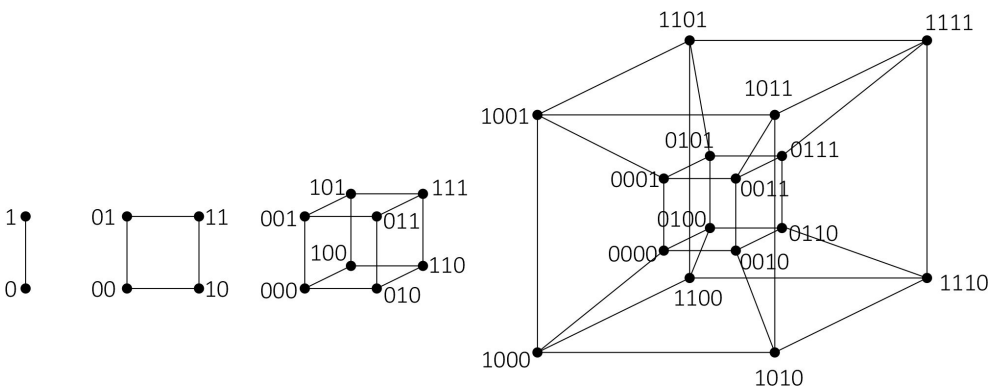
Из практичних разлога, све валуације за n исказних слова набрајамо на следећи систематичан начин: Испод свод сваког појављивања првог слова наводимо 2^{n-1} пута вредност 0, па 2^{n-1} пута вредност 1; затим испод сваког појављивања другог слова прво наводимо 2^{n-2} пута 0, па затим 2^{n-2} пута 1, па 2^{n-2} пута поново 0, и најзад у још 2^{n-2} пута 1, и тако даље, до n-тог слова испод кога наизменично уписујемо 0 и 1.

p	q
0	0
0	1
1	0
1	1

p	q	r
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

p	q	r	s
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

Скуп свих валуација n исказних слова назива се и n-димензионални Булов простор и представља се n-димензионалном коцком.



Дефиниција 1. *Исказна формула α је* ***задовољива*** *ако постоји валуација исказних слова за коју је вредност формуле α једнака* 1.

Пример 7. Формула $p \wedge \neg(q \Rightarrow r)$ је задовољива.

p	$\wedge$	$\neg$	$(q$	$\Rightarrow$	$r)$
0	**0**	0	0	1	0
0	**0**	0	0	1	1
0	**0**	1	1	0	0
0	**0**	0	1	1	1
1	**0**	0	0	1	0
1	**0**	0	0	1	1
1	**1**	1	1	0	0
1	**0**	0	1	1	1

Из таблице видимо да је дата формула тачна за валуацију $p = 1$, $q = 1$, $r = 0$.

Проблем испитивања задовољивости исказних формула краће се назива CAT-проблем (енг. satisfiability – задовољивост). Препоручујемо читаоцу да се путем интернета детаљније информише о овом проблему и његовом значају у савременој математици.

1.2. Таутологије

У уводном примеру 1 (стр. 2) најављен је значај исказних формула чија истинитосна вредност не зависи од валуације исказних слова.

2

Формула $p \vee \neg p$ је истинита и у случају да је $p = 0$, као и да је $p = 1$.

Дефиниција 2. *Исказна формула α је **таутологија** ако је за сваку валуацију исказних слова вредност формуле α једнака 1. Да је α таутологија означавамо $\models \alpha$.*

Пример 8. Формуле $p \wedge (p \Rightarrow q) \Rightarrow q$ и $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$ су таутологије (а самим тим и задовољиве):

p	$\wedge$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	q
0	0	0	1	0	**1**	0
0	0	0	1	1	**1**	1
1	0	1	0	0	**1**	0
1	1	1	1	1	**1**	1

$(p$	$\Rightarrow$	$q)$	$\wedge$	$\neg$	q	$\Rightarrow$	$\neg$	p
0	1	0	1	1	0	**1**	1	0
0	1	1	0	0	1	**1**	1	0
1	0	0	0	1	0	**1**	0	1
1	1	1	0	0	1	**1**	0	1

О значају таутологија, пре свега при описивању закона мишљења, биће речи касније. За сада, истичемо само да се таутологија $p \wedge (p \Rightarrow q) \Rightarrow q$ (тзв. modus ponens) препознаје у следећем свакодневном закључивању:

$$\frac{p \quad p \Rightarrow q}{q}(\text{MP})$$

1. Ана живи у Београду.
2. Ако Ана живи у Београду, онда Ана живи у Србији.

Дакле, Ана живи у Србији.

Такође, и таутологију modus tolens $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$ свакодневно користимо приликом закључивања:

$$\frac{p \Rightarrow q \quad \neg q}{\neg p}(\text{MT})$$

1. Ако Ана живи у Београду, онда Ана живи у Србији.
2. Ана не живи у Србији.

Дакле, Ана не живи у Београду.

Слободно говорећи, таутологије су (алгебарски) изрази којима се описују основни шаблони мишљења.

У наставку наводимо списак неких важних таутологија (читаоцима препуштамо проверу да су ове формуле заиста таутологије). Наведене формуле се лакше памте, ако се уочи да логичке операције можемо описати и на следећи начин уколико 0 и 1 схватимо као бројеве. Наиме, за $x, y \in \{0, 1\}$, важи $x \vee y = \max\{x, y\}$, $x \wedge y = \min\{x, y\}$, (при чему се ослањамо на уобичајени поредак $0 < 1$), као и да је $\neg x = 1 - x$ ('$-$' је знак за одузимање). Такође, ваља приметити да импликација $x \Rightarrow y$ има вредност 1 ако и само ако је $x \leqslant y$.

Списак важних таутологија:

Својства импликације:

$\models p \Rightarrow p$

$\models \bot \Rightarrow p \qquad \models p \Rightarrow \top$

$\models (p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$ *транзитивност импликације*

$\models (p \Rightarrow q) \vee (q \Rightarrow p)$ *линеарност импликације*

Својства конјункције:

$\models p \wedge q \Rightarrow p$ $\quad\quad$ $\models p \wedge q \Rightarrow q$

$\models (r \Rightarrow p) \Rightarrow ((r \Rightarrow q) \Rightarrow (r \Rightarrow p \wedge q))$ $\quad$ *формула $p \wedge q$ је највеће доње ограничење за p и q*

Својства дисјункције:

$\models p \Rightarrow p \vee q$ $\quad\quad$ $\models q \Rightarrow p \vee q$

$\models (p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r))$ $\quad$ *формула $p \vee q$ је најмање горње ограничење за p и q*

Својства конјункције и дисјункције:

$\models p \wedge p \Leftrightarrow p$	$\models p \vee p \Leftrightarrow p$	*закони идемпотентности*
$\models p \wedge (p \vee q) \Leftrightarrow p$	$\models p \vee (p \wedge q) \Leftrightarrow p$	*закони апсорпције*
$\models p \wedge q \Leftrightarrow q \wedge p$	$\models p \vee q \Leftrightarrow q \vee p$	*закони комутативности*
$\models p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	$\models p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$	*закони асоцијативности*
$\models p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	*закони дистрибутивности $\wedge$ према $\vee$*	
$\models p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	*закони дистрибутивности $\vee$ према $\wedge$*	

Својства негације:

$\models p \wedge \neg p \Rightarrow q$	*ex falso quodibet – из лажне претпоставке следи све (што желиш)*
$\models (p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$	*reduction ad absurdum – свођење на противречност*
$\models \neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	*Де Морганов закон*
$\models \neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$	*Де Морганов закон*
$\models (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	*закон контрапозиције*
$\models p \Leftrightarrow \neg\neg p$	*закон двојне негације*
$\models p \vee \neg p$	*закон искључења трећег*

Исказна слова се зову још и *исказне променљиве*. Уопште у математици, променљива је симбол везан за супституцију, тј. замену, без изузетка, свих јављања тог симбола истим изразом. Резултат супституције се зове супституциона инстанца, или просто **инстанца**. У некој исказној формули, уместо променљивих могу да се постављају произвољне исказне формуле, и добијене инстанце су онда опет исказне формуле. Користимо следеће ознаке:

- $[p/\varphi]$ означава *истовремену замену слова p формулом φ*;
- $\alpha[p/\varphi]$ означава *резултат замене слова p формулом φ у некој формули α.*

Пример 9. Ако је α формула $\neg(p \Rightarrow q) \Rightarrow p \wedge \neg q$, онда је:

- $\alpha[p/p \vee r]$ формула $\neg(p \vee r \Rightarrow q) \Rightarrow (p \vee r) \wedge \neg q$;
- $\alpha[q/r \Rightarrow \neg s \wedge t]$ формула $\neg(p \Rightarrow (r \Rightarrow \neg s \wedge t)) \Rightarrow p \wedge \neg(r \Rightarrow \neg s \wedge t)$;
- $\alpha[s/p \Rightarrow \neg r]$ формула α, тј. $\neg(p \Rightarrow q) \Rightarrow p \wedge \neg q$, јер се s не појављује у α.

Приметимо да је формула α, тј. $\neg(p \Rightarrow q) \Rightarrow p \wedge \neg q$ таутологија. Да ли су формуле $\alpha[p/p \vee r]$, $\alpha[q/r \Rightarrow \neg s \wedge t]$ и $\alpha[s/p \Rightarrow \neg r]$ такође таутологије?

$\neg$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	p	$\wedge$	$\neg$	q
0	0	1	0	**1**	0	0	1	0
0	0	1	1	**1**	0	0	0	1
1	1	0	0	**1**	1	1	1	0
0	1	1	1	**1**	1	0	0	1

Посебно истичемо једну очигледну чињеницу: *свака инстанца таутологије је такође таутологија.*

Теорема 1. *Ако је α таутологија, онда је и $\alpha[p/\varphi]$ такође таутологија, за било коју формулу φ.*

Пример 10. Знамо да су формуле

$$p \wedge (p \Rightarrow q) \Rightarrow q \text{ и } (p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$$

таутологије. Применом претходне теореме закључујемо да су и њихове инстанце

$$\varphi \wedge (\varphi \Rightarrow \psi) \Rightarrow \psi \text{ и } (\varphi \Rightarrow \psi) \wedge \neg\psi \Rightarrow \neg\varphi,$$

такође таутологије, за било које формуле φ и ψ.

Многе од таутологија са претходног списка јесу еквиваленције неке две формуле.

Дефиниција 3. *Формуле α и β су* ***еквивалентне****, у ознаци $\alpha \equiv \beta$, ако α и β имају исте истинитосне вредности за сваку валуацију, тј. ако је $\models \alpha \Leftrightarrow \beta$.*

Приметимо да је $\alpha \equiv \beta$ само други запис чињенице $\models \alpha \Leftrightarrow \beta$.

Ако је $\alpha \equiv \beta$, и у некој формуле се појављује α као потформула, онда се након замене сваког појављивања формуле α формулом β, добија нова формула еквивалентна полазној. Две еквивалентне формуле увек имају исте истинитосне вредности, па је јасно да свако појављивање једне у тих формула, у некој формули, можемо заменити другом, њој еквивалентном формулом. Ово запажање је познато као *теорема о замени еквивалената*[16]. Да бисмо је прецизније формулисали теорему уводимо следеће ознаке:

- $[\alpha/\beta]$ означава замену свих појављивања формуле α формулом β;
- $\varphi[\alpha/\beta]$ означава формулу добијену заменом свих појављивања потформуле α у формули φ формулом β.

[16] Замена еквивалената је у основи тзв. екивалентних трансформација било каквих алгебарских израза. На пример, знамо да је $x^2 - y^2 = (x-y)(x+y)$, тј. да су изрази $x^2 - y^2$ и $(x-y)(x+y)$ еквивалентни (имају исте вредности за све вредности променљивих x и y), а знамо и да ако појављивање израза $x^2 - y^2$ у неком сложеном изразу заменимо изразом $(x-y)(x+y)$, добијамо израз еквиваленатан полазном сложеном изразу.

Теорема 2. [***Теорема о замени еквивалената***] *Ако је $\alpha \equiv \beta$, онда је $\varphi \equiv \varphi[\alpha/\beta]$, за било коју формулу φ.*

Тврђење о замени еквивалената је засновано на истиносној функционалности. По истиносној функционалности, за израчунавање истиносне вредности свеједно је са којом смо од двеју еквивалентних исказних формула имали посла. Важна је само истинитосна вредност, а она се код еквивалентних исказних формула не разликује.[17] Тврђење о замени еквивалената нам каже да се еквивалентне формуле, мада нису једнаке, понашају исто ако нас занима само истинитосна вредност. Пошто увек имају исту истинитосну вредност, оне на исти начин утичу на истинитосну вредност контекста.

[17] Тврђење о замени еквивалената се прецизно доказује математичком индукцијом, која прати индуктивну дефиницију исказних формула (о чему ће касније бити речи). Овде се ради о индукцији по сложености формуле φ. Математичком индукцијом се иначе доказују слична тврђења која нешто тврде о свим формулама.

Примену тврђења о замени еквивалената прате и следећа очигледна својства.

Теорема 3. *Нека су α, β, γ произвољне исказне формуле.*

(P) $\alpha \equiv \alpha$, *тј.* $\models \alpha \Leftrightarrow \alpha$;

(C) ако је $\alpha \equiv \beta$, *онда је и* $\beta \equiv \alpha$ *(из* $\models \alpha \Leftrightarrow \beta$ *следи* $\models \beta \Leftrightarrow \alpha$*);*

(T) ако је $\alpha \equiv \beta$ *и* $\beta \equiv \gamma$, *онда је и* $\alpha \equiv \gamma$ *(из* $\models \alpha \Leftrightarrow \beta$ *и* $\models \beta \Leftrightarrow \gamma$, *следи* $\models \alpha \Leftrightarrow \gamma$*).*

(K) ако је $\alpha \equiv \beta$ *и* $\gamma \equiv \delta$, *онда је и* $\alpha * \gamma \equiv \beta * \delta$, *за било који везник* $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$ *(из* $\models \alpha \Leftrightarrow \beta$ *и* $\models \gamma \Leftrightarrow \delta$, *следи* $\models \alpha * \gamma \Leftrightarrow \beta * \delta$*).*

Издвајамо неке основне парове еквивалентних формула. За било које формуле α, β, γ важи:

$\mathbf{A}^\vee$	$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$	$\mathbf{A}^\wedge$	$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$
$\mathbf{K}^\vee$	$\alpha \vee \beta \equiv \beta \vee \alpha$	$\mathbf{K}^\wedge$	$\alpha \wedge \beta \equiv \beta \wedge \alpha$
$\mathbf{D}^\vee_\wedge$	$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	$\mathbf{D}^\wedge_\vee$	$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
$\mathbf{C}^\vee$	$\alpha \vee \neg\alpha \equiv \top$	$\mathbf{C}^\wedge$	$\alpha \wedge \neg\alpha \equiv \bot$
$\mathbf{N}^\vee$	$\alpha \vee \bot \equiv \alpha$	$\mathbf{N}^\wedge$	$\alpha \wedge \top \equiv \alpha$
$\mathbf{I}^\vee$	$\alpha \vee \alpha \equiv \alpha$	$\mathbf{I}^\wedge$	$\alpha \wedge \alpha \equiv \alpha$
$\mathbf{A}^\vee_\wedge$	$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$	$\mathbf{A}^\wedge_\vee$	$\alpha \wedge (\alpha \vee \beta) \equiv \alpha$
DM	$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$	**DM**	$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
	$\alpha \vee \top \equiv \top$		$\alpha \wedge \bot \equiv \bot$

$$\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$$
$$\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$$
$$\neg\neg\alpha \equiv \alpha$$
$$\vdots$$

Пример 11. Применом наведених еквиваленција доказаћемо да је формула $(p \vee q) \vee (\neg p \wedge \neg q)$ таутологија:

$$\begin{aligned}
(p \vee q) \vee (\neg p \wedge \neg q) &\equiv ((p \vee q) \vee \neg p) \wedge ((p \vee q) \vee \neg q) && [\mathbf{D}^\vee_\wedge] \\
&\equiv ((q \vee p) \vee \neg p) \wedge (p \vee (q \vee \neg q)) && [\mathbf{A}^\vee, \mathbf{K}^\vee] \\
&\equiv (q \vee (p \vee \neg p)) \wedge (p \vee \top) && [\mathbf{A}^\vee, \mathbf{C}^\vee] \\
&\equiv (q \vee \top) \wedge \top && [\mathbf{C}^\vee, \text{ очигледно } \alpha \vee \top \equiv \top] \\
&\equiv \top \wedge \top && [\text{ очигледно } \top \vee \top \equiv \top] \\
&\equiv \top
\end{aligned}$$

Слично се може показати да исказна формула $(p \vee q) \wedge (\neg p \wedge \neg q)$ није задовољива. $(p \vee q) \wedge (\neg p \wedge \neg q) \equiv \cdots \equiv \bot$

2. Математичка индукција

2.1. **Принцип математичке индукције**

3

Један од најзначајнијх производа људске мисли јесте *скуп* свих природних бројева 0, 1, 2, 3, 4, 5, 6, ... Бројање је једна од најзначајнијих вештина коју је човек стекао захваљујући свом чистом мишљењу, а не физичком раду.

Када аритметику називам само једним делом логике, тиме већ исказујем да појам броја сматрам сасвим независним од представа или интуиција простора и времена, да га, напротив сматрам непосредним производом чистих закона мишљења.
Дедекинд (1831—1916), Was sind und was sollen die Zahlen, 1888.

Бројање је базични појам аритметике. Предмет аритметике нису бројеви већ бројање. Идеја бројања је на природан начин повезана са прадавним начином бележења резултата бројања у тзв. *рецка-систему*: записи резултата бројања настају тако што полазећи од 0 (почетног резултата који претходи бројању) узастопно дописујемо (једну по једну) цртицу: $0, 0', 0'', 0''', 0'''', \ldots$ или

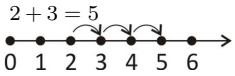
$$0, \overline{0}, \overline{\overline{0}}, \overline{\overline{\overline{0}}}, \overline{\overline{\overline{\overline{0}}}}, \ldots$$

У наставку, користимо овај други запис. Да бисмо поједноставили читање, користићемо и арапске цифре, да краће запишемо бројеве:

$$0, 1 = \overline{0}, 2 = \overline{\overline{0}}, 3 = \overline{\overline{\overline{0}}}, 4 = \overline{\overline{\overline{\overline{0}}}}, \ldots$$

Најважнији корак бележења резултата бројања јесте 'додавање нове цртице на текући резултат бројања'. На тај начин креирамо следбеника сваког броја. Нема никаквог ограничења: сваки број има свог следбеника.

Сабирање је операција која се природно надовезује на бројање: збир $m + n$ добијамо када почев од броја m избројимо још n бројева. Другим речима, збир $m + n$ је n-ти следбеник броја m. Сабирање се прецизно описује двема једнакостима:



$$\begin{array}{ll} m + 0 = m & [\text{Када се броју } m \text{ дода 0 резултат је } m.] \\ m + \overline{n} = \overline{m + n} & [\text{Ако је } m + n = k, \text{ онда је } m + \overline{n} = \overline{k}.] \end{array}$$

Наведене једнакости описују како се (било ком) броју m додају природни бројеви, тј. дефинишу функцију којом се природном броју x додељује јединствен природан број $m + x$, ту функцију краће означавамо $x \mapsto m + x$. Сабирање је бројање почев од неког задатог броја. Нпр. збир $2 + 3$ (тј. $\overline{\overline{0}} + \overline{\overline{\overline{0}}}$) је трећи следбеник броја 2:

$$\begin{aligned} \overline{\overline{0}} + \overline{\overline{\overline{0}}} &= \overline{\overline{\overline{0}} + \overline{\overline{0}}} \\ &= \overline{\overline{\overline{0}} + \overline{0}} \\ &= \overline{\overline{\overline{0}} + 0} \\ &= \overline{\overline{\overline{0}}} \end{aligned}$$

Користећи наведене једнакости изводимо општа својства сабирања. На пример, можемо ли доказати једнакост $0 + n = n$, за било који природан број n? Једноставно је проверити једнакост у било ком

конкретном случају:

$0 + 0 = 0$ је последица једнакости $m + 0 = m$ која је тачна за било који број m, па и када је m једнако 0;

$0 + \overline{0} = \overline{0 + 0} = \overline{0}$, јер је у претходном кораку показано $0 + 0 = 0$;

$0 + \overline{\overline{0}} = \overline{0 + \overline{0}} = \overline{\overline{0}}$, јер је у претходном кораку показано $0 + \overline{0} = \overline{0}$;

$0 + \overline{\overline{\overline{0}}} = \overline{0 + \overline{\overline{0}}} = \overline{\overline{\overline{0}}}$, јер је у претходном кораку показано $0 + \overline{\overline{0}} = \overline{\overline{0}}$;

$\vdots$

У овом низу доказа примећујемо: осим за прву једнакост $0 + 0 = 0$, при доказивању сваке једнакости користимо једнакост која јој претходи. Када за неко n докажемо да је $0 + n = n$, онда једноставно изводимо и следећу једнакост

$$0 + \overline{n} = \overline{0 + n} = \overline{n}.$$

Претходна запажања истичу суштину тзв. принципа математичке индукције.

$$\frac{\mathcal{S}(0), \mathcal{S}(0) \Rightarrow \mathcal{S}(1), \mathcal{S}(1) \Rightarrow \mathcal{S}(2), \mathcal{S}(2) \Rightarrow \mathcal{S}(3), \ldots}{\mathcal{S}(0), \mathcal{S}(1), \mathcal{S}(2), \mathcal{S}(3), \ldots}$$

Индуктивни корак заправо представља доказ да операција *следбеник* чува уочено својство.

Принцип математичке индукције: Нека је $\mathcal{S}$ ознака за неко својство природних бројева, и $\mathcal{S}(n)$ ознака да *број* n *има својство* $\mathcal{S}$. Из следећа два услова:

БИ (База индукције)
0 има својство $\mathcal{S}$, тј. $\mathcal{S}(0)$;

ИК (Индуктивни корак)
за свако n, ако n има својство $\mathcal{S}$, онда и $\overline{n}$ има својство $\mathcal{S}$, тј. $\mathcal{S}(n) \Rightarrow \mathcal{S}(\overline{n})$;

закључујемо да <u>сваки</u> природни број има својство $\mathcal{S}$.

Теорема 4. *За сваки природан број* n, $0 + n = n$.

Доказ. Сабирање је дефинисано двема једнакостима:

$$\begin{aligned} &(\text{Rec1})\ m + 0 = m \\ &(\text{Rec2})\ m + \overline{n} = \overline{m + n} \end{aligned}$$

Једнакост $0 + n = n$ посматрамо као $\mathcal{S}(n)$ из принципа математичке индукције.
(БИ) Да ли важи $\mathcal{S}(0)$, тј. $0 + 0 = 0$? Ова једнакост директно следи из (Rec1).
(ИК) Да ли, за произвољно n важи $\mathcal{S}(n) \Rightarrow \mathcal{S}(\overline{n})$? Другим речима, да ли из претпоставке да је $0 + n = n$ можемо извести једнакост $0 + \overline{n} = \overline{n}$?

Уводимо тзв. индуктивну претпоставку: Нека је n природан број такав да је $0 + n = n$. Применом ове претпоставке и (Rec2) долазимо до жељене једнакости:

$$\begin{aligned} 0 + \overline{n} &= \overline{0 + n} \text{ према (Rec2)} \\ &= \overline{n} \text{ према индуктивној претпоставци} \end{aligned}$$

Дакле, према принципу математичке индукције, за сваки природан број n тачна је једнакост $0 + n = n$. □

Теорема 5. *За све природне бројеве m, n, k важе једнакости:*

(1) $\overline{m} + n = m + \overline{n}$;

(2) $m + n = n + m$;

(3) $m + (n + k) = (m + n) + k$

Доказ. (1) Индукцијом по n:

(БИ) $\overline{m} + 0 = \overline{m}$ [према (Rec1)]
$= \overline{m + 0}$ [према (Rec1)]
$= m + \overline{0}$ [према (Rec2)]

(ИП) $\overline{m} + n = m + \overline{n}$

$\overline{m} + \overline{n} = \overline{\overline{m} + n}$ [према (Rec2)]
$= \overline{m + \overline{n}}$ [према ИП]
$= m + \overline{\overline{n}}$ [према (Rec2)]

(2) Индукцијом по n:

(БИ) Из $m + 0 = m$ и $0 + m = m$ следи да је $m + 0 = 0 + m$.

(ИП) $m + n = n + m$

$m + \overline{n} = \overline{m + n}$ [према (Rec2)]
$= \overline{n + m}$ [према ИП]
$= n + \overline{m}$ [према (Rec2)]
$= \overline{n} + m$ [према (1)]

(3) Индукцијом по k:

(БИ) Једноставно се доказује једнакост $(m + n) + 0 = m + (n + 0)$.

(ИП) $(m + n) + k = m + (n + k)$

$(m + n) + \overline{k} = \overline{(m + n) + k}$ [према (Rec2)]
$= \overline{m + (n + k)}$ [према ИП]
$= m + \overline{n + k}$ [према (Rec2)]
$= m + (n + \overline{k})$ [према (Rec2)] □

Чувени француски математичар Анри Поенкаре (1854—1912) своју књигу La Science l'Hypothèse почиње доказима основних својстава сабирања и истиче: Наведени докази аритметичких тврђења илуструју математичко резоновање par excellence, и морамо га ближе проучити.

Због асоцијативности сабирања, $m + (n + k) = (m + n) + k$, кратко пишемо $m + n + k$ остављајући могућност да се по потреби додају заграде које обухватају први и други сабирак, или заграде које обухватају други и трећи сабирак.

На сличан начин, као сабирање, уводимо и **множење**, прецизирајући познату 'интуитивну' једнакост: $m \cdot n = \underbrace{m + \cdots + m}_{n \text{ пута}}$. Множење описујемо следећим двема једнакостима:

$$m \cdot 0 = 0$$
$$m \cdot \overline{n} = (m \cdot n) + m$$

Према знаном договору да је множење приоритетније од сабирања, уместо $(m \cdot n) + m$, краће пишемо $m \cdot n + m$.

Теорема 6. *За све природне бројеве m, n, k важе једнакости:*

(1) $k \cdot (m + n) = k \cdot m + k \cdot n$

(2) $(k \cdot m) \cdot n = k \cdot (m \cdot n)$

(3) $\overline{m} \cdot n = m \cdot n + n$

(4) $m \cdot n = n \cdot m$

Доказ. (1) Индукцијом по n:
(БИ) Из $k \cdot (m + 0) = k \cdot m$ и $k \cdot m + k \cdot 0 = k \cdot m + 0 = k \cdot m$ следи да је $k \cdot (m + 0) = k \cdot m + k \cdot 0$.
(ИП) $k \cdot (m + n) = k \cdot m + k \cdot n$

$$\begin{aligned} k \cdot (m + \overline{n}) &= k \cdot \overline{m + n} \\ &= k \cdot (m + n) + k \\ &= (k \cdot m + k \cdot n) + k \quad [\text{према ИП}] \\ &= k \cdot m + (k \cdot n + k) \\ &= k \cdot m + k \cdot \overline{n} \end{aligned}$$

(3) Индукцијом по n:
(БИ) Једноставно се уочава да је једнакост $\overline{m} \cdot 0 = m \cdot 0 + 0$ тачна.
(ИП) $\overline{m} \cdot n = m \cdot n + n$

$$\begin{aligned} \overline{m} \cdot \overline{n} &= \overline{m} \cdot n + \overline{m} \\ &= (m \cdot n + n) + \overline{m} \quad [\text{према ИП}] \\ &= m \cdot n + (n + \overline{m}) \\ &= m \cdot n + (\overline{n} + m) \\ &= m \cdot n + (m + \overline{n}) \\ &= (m \cdot n + m) + \overline{n} \\ &= m \cdot \overline{n} + \overline{n} \end{aligned}$$

Једнакости (2) и (4) остављамо за вежбу. □

Начин на који смо увели сабирање и множење називамо **индуктивним**, одн. **рекурзивним** или **рекурентним** дефиницијама. Индуктивним дефиницијама уводимо веома богату класу аритметичких операција. У наставку, прелазимо на ознаке које су уобичајене у литератури, и уместо $\overline{n}$ пишемо $n + 1$. (Приметите да је $n + 1 = n + \overline{0} = \overline{n + 0} = \overline{n}$.)

Степеновање:[26]

$$\begin{cases} m^0 = 1 \\ m^{n+1} = m^n \cdot m \end{cases}$$

Факторијел:[27]

$$\begin{cases} 0! = 1 \\ (m+1)! = m! \cdot (m+1) \end{cases}$$

Биномни коефицијенти $\binom{\cdot}{2}$**:**

$$\begin{cases} \binom{0}{2} = 1 \\ \binom{m+1}{2} = \binom{m}{2} + m \end{cases}$$

Реч рекурзија потиче од латинске речи recurrere која значи *вратити се од* [recurrence ı који се враћа]. Дедекинд је у свом раду из 1888. користио термин *дефинисан индукцијом*, док је Хилберт (1904) употребио реч rekurrent(e), а касније (1923) и реч Rekursion.

[26] $m^n = \underbrace{m \cdot \ldots \cdot m}_{n \text{ пута}}$

[27] $m! = 1 \cdot 2 \cdot \ldots \cdot m$

▼ Вежбе

Принцип рекурзије	Принцип индукције
метод за **дефинисање** низа елемената неког скупа: $S_0, S_1, S_2, \ldots, S_n, S_{n+1}, \ldots$	метод за **доказивање** низа тврђења: $\mathcal{S}(0), \mathcal{S}(1), \mathcal{S}(2), \ldots, \mathcal{S}(n), \mathcal{S}(n+1), \ldots$
- S_0 је дефинисано ($S_0 = x$, где је x неки фиксиран елемент задатог скупа); - елемент S_{n+1} дефинишемо у зависности од n и елемента S_n, тј. за сваки природан број n имамо неку задату везу између S_{n+1} и S_n облика $S_{n+1} = F(S_n)$.	(БИ) $\mathcal{S}(0)$ је тачно; (ИК) истинитост исказа $\mathcal{S}(n+1)$ доказујемо користећи претпоставку $\mathcal{S}(n)$, тј. доказујемо да за сваки природан број n важи импликација: $\mathcal{S}(n) \Rightarrow \mathcal{S}(n+1)$.
Пример 1.	
Дат је низ бројева: $f_1 = 5$, $f_{n+1} = 5 + f_n$, $n \in \mathbb{N}$. Одредити f_5.	Доказати да за сваки природан број n важи: $5 \mid f_n$.

2.2 **Формалне граматике и формалне теорије**

4

Чувени амерички лингвиста Ноам Чомски је принцип индуктивног (рекурзивног) дефинисања препознао и као универзални принцип на коме почивају говорни језици. Испоставља се да је принцип рекурзије темељни принцип и језичке структуре. Ова чињеница лежи у основи развоја вештачких (формалних) језика међу којима се посебно значајно место заузимају програмски језици. У наставку издвајамо основне идеје, наводећи основне дефиниције и типичне примере.

▼ Алфабет

Полазиште у развоју било ког формалног језика представља избор **алфабета**. Уопштено, под *алфабетом* Σ подразумевамо било који непразан коначан скуп чије елементе називамо *симболима*. Сваки алфабет користимо да бисмо написали неки текст. Наводимо неколико познатих алфабета:

Основне идеје овог одељка потичу од Емила Поста (1943). Шта год да представљају *изрази* неког логичког система, одн. језика, они се у крајње уопштеној анализи своде на *низове симбола неког коначног алфабета*. Веома сложени логички и математички системи засновани су на правилима која одређују како се неки низови симбола могу трансформисати у неке друге низове симбола.

- $\Sigma_{\mathrm{U}} = \{1\}$ – *унарни алфабет*, који садржи само један симбол;
- $\Sigma_2 = \{0, 1\}$ – *бинарни алфабет*, веома важан за рачунарство;
- $\Sigma_{\mathrm{lat}} = \{a, b, c, \ldots, z\}$ – мала слова латинице;
- $\Sigma_{\mathrm{keyboard}} = \{\mathtt{A}, \mathtt{a}, \mathtt{Б}, \mathtt{б}, \ldots, \mathtt{З}, \mathtt{з}, \sqcup, >, <, (,), \ldots, !\}$ – алфабет свих симбола тастатуре (при чему $\sqcup$ означава бланко знак); итд.

▼ Речи

Ако је Σ алфабет, за $m \geqslant 2$, Σ^m је скуп свих коначних низова дужине m. Коначан низ $a_1, \ldots, a_m$ дужине m, називамо и

$\Sigma_2^0 = \{\varepsilon\}$, $\Sigma_2^1 = \{0, 1\}$,
$\Sigma_2^2 = \{00, 01, 10, 11\}$,
$\vdots$
$\Sigma_2^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$
$\Sigma_2^+ = \{0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$

- *реч над* Σ *дужине* m и тада пишемо $a_1 \cdots a_m$ (изостављамо запете), или
- *уређена* m*-торка* и тада пишемо $(a_1, \cdots, a_m)$.

Скуп Σ^1, тј. скуп свих речи над Σ дужине 1, идентификујемо са скупом Σ. Скуп Σ^0 је једночлани скуп чији ћемо елемент означавати са ε и при томе ћемо сматрати да је и ε реч над Σ и то *празна реч*. Скуп свих речи над алфабетом Σ означавамо Σ^*. Ако $w \in \Sigma^*$, тада јединствени m такав да $w \in \Sigma^m$ називамо дужином речи w и пишемо $|w| = m$.

Приметимо да ако алфабет Σ садржи k симбола, онда скуп Σ^m садржи k^m речи.

▼ Правила за трансформацију речи

Развој *рачуна* са речима данас заузима значајно место у алгебри, логици, геометрији, рачунарству. Основу свих тих рачуна чине правила за трансформације речи.

Сваки пар речи u и w, над неким алфабетом Σ, одређује *правило* које се означава $u \to w$ (или $[u/w]$). Свако правило чине две речи: реч са леве стране називамо *претходником*, а реч са десне стране *следбеником*. Правило $u \to w$ можемо применити на сваку реч v која садржи u као подреч, тј. на реч v облика $v_1 u v_2$, за неке (можда

празне) речи v_1 и v_2. Примена правила подразумева да подреч u заменимо речју w; пишемо:

$$v_1 u v_2 \to v_1 w v_2.$$

Дозвољена су и правила следећег облика:

- $u \to \varepsilon$, тј. брисање подречи u;
- $\varepsilon \to v$, тј. уметање речи v на било ком месту.

Када је задат неки коначан скуп правила, кажемо да се из v **изводи** реч v', ако постоји коначан низ речи

$$v = v_0 \to v_1 \to v_2 \to \cdots \to v'$$

такав да је свака реч, почевши од друге, добијена применом неког од правила на реч која јој претходи.

Неки скуп правила за трансформацију речи задатог алфабета назива се *Семи-Туов процес* или *систем преписивања* над тим алфабетом.

Пример 12. За алфабет $\Sigma = \{a, b\}$ посматрамо два правила $ab \to aa$ и $ba \to bb$. Ево једног извођења речи aaa из aba:

У свакој речи, подреч ab можемо заменити са aa, а подреч ba можемо заменити са bb.

$$aba \to abb \to aab \to aaa$$

Може ли се, применом датих правила, из $aaabb$ извести $aaaaa$? Може ли се из $aaabb$ извести $bbbbb$?

Пример 13. Над алфабетом $\{a, b, c\}$ дата су правила

$$c \to ac \qquad c \to b$$

Пример илуструје две важне примене принципа математичке индукције, које ћемо често примењивати проучавајући разне формалне системе: индукцију по сложености речи и индукцију по дужини доказа.

Није тешко уочити да се из c могу извести речи $a^n b$ или $a^n c$, за било које $n \geqslant 0$. Доказ ове чињенице спроводимо индукцијом по n.

БИ $n = 0$: јасно је да се из c могу извести речи b (директном применом правила $c \to b$) и c (без примене иједног правила).

ИК Претпоставимо да се за неко n, из c могу извести $a^n b$ и $a^n c$. Покажимо да се могу извести и речи $a^{n+1} b$ и $a^{n+1} c$; обе ове речи се добијају из $a^n c$ применом одговарајућих правила. Извођење речи $a^{n+1} c$:

$$\begin{array}{lcll} c & \to & a^n c & [\text{према ИП}] \\ & \to & a^n ac & [\text{применом } c \to ac] \end{array}$$

Извођење речи $a^{n+1} b$:

$$\begin{array}{lcll} c & \to & a^n c & [\text{према ИП}] \\ & \to & a^n ac & [\text{применом } c \to ac] \\ & \to & a^n ab & [\text{применом } c \to b] \end{array}$$

Докажимо и да се из c могу извести **само** речи облика $a^n c$ или $a^n b$, $n \geqslant 0$. Другим речима, ако је w реч која се може извести из c,

треба доказати да је w облика $a^n c$ или $a^n b$, $n \geqslant 0$. Доказ спроводимо **индукцијом по дужини извођења**.

БИ Ако је дужина извођења речи w из c једнака 0, тј. ниједно правило није примењено, онда је w заправо реч c, тј. реч $a^0 c$.

ИП Претпоставимо да тврђење важи за све речи дужине мање од k, за неки природан број k. Докажимо да важи и за извођење дужине k.

Претпоставимо да је дужина извођења речи w из c једнака k:

$$\underbrace{c \to \cdots \to w'}_{k-1 \text{ корака}} \to w$$

при чему је w' реч која се добија у претпоследњем кораку извођења. Према индуктивној претпоставци, w' је облика $a^n b$ или $a^n c$.

Међутим, реч w' облика $a^n b$, јер ова реч не садржи c и на њу се не може применити ниједно од датих правила. Дакле, w' је облика $a^n c$. Ако је последње примењено $c \to ac$, добијамо да је w облика $a^{n+1} c$. Ако је последње примењено правило $c \to b$, добијамо да је w облика $a^n b$.

▼ Језик одређен формалном граматиком

Формална граматика је посебна врста система преписивања над алфабетом у коме се разликују две врсте симбола:

- помоћни симболи – тзв. *променљиве*, међу којима је једна променљива издвојена као *полазни симбол*;
- крајњи симболи – тзв. *терминали*.

Над оваквим алфабетом, **формална граматика** је одређена коначним списком правилима са чије се леве стране налази бар једна променљива. **Језик** одређен формалном граматиком јесте скуп свих речи састављене од терминала које се могу извести из полазног симбола.

Уобичајено је (али не и неопходно) да се велика слова користе за означавање променљивих, а да се мала слова и ци означавају за означавање терминала.

> *Полазни симбол репрезентује сам језик, тј. скуп свих речи над терминалима које се могу извести из полазног симбола.*

Наводимо неколико примера формалних граматика.

Пример 14. 1) Палиндром је реч која се једнако чита и слева надесно и здесна налево. Палиндроми над $\{0,1\}$ су: 0, 010, 010010, итд. Наравно, и празна реч је палиндром. Скуп P **свих** палиндрома (укључујући и празну реч) над $\{0,1\}$ индуктивно дефинишемо на следећи начин:

- ε, 0 и 1 су палиндроми ($\varepsilon, 0, 1 \in P$);

Подсећамо, ε је празна реч.

- ако је w палиндром, онда су то и $0w0$ и $1w1$ (ако $w \in P$, онда $0w0, 1w1 \in P$).

Овој индуктивној дефиницији, у потпуности одговарају следећа правила над алфабетом $\{P, 0, 1\}$, где је P променљива, а 0 и 1 терминали:

$$P \to \varepsilon \qquad P \to 0 \quad P \to 1 \quad P \to 0P0 \quad P \to 1P1$$

Полазећи од симбола P можемо извести било који палиндром. Изведимо, на пример 0010100:

$$\begin{array}{rcll} P & \to & 0P0 & [\text{применом } P \to 0P0] \\ & \to & 00P00 & [\text{применом } P \to 0P0] \\ & \to & 001P100 & [\text{применом } P \to 1P1] \\ & \to & 0010100 & [\text{применом } P \to 0] \end{array}$$

Штавише, палиндроми су једине речи над $\{0, 1\}$ које се могу извести из P.

2) Посматрајмо следећа правила над алфабетом $\{I, +, -, x, y, z, (,)\}$, где је I променљива, а остали симболи су терминали:

$$I \to x \quad I \to y \quad I \to z \quad I \to 0 \quad I \to 1 \quad I \to -I \quad I \to (I + I)$$

Будући да сва правила са леве стране имају исти симбол I, све заједно их краће записујемо на следећи начин:

$$(*) \quad I \to x \mid y \mid z \mid 0 \mid 1 \mid -I \mid (I + I).$$

Није тешко уочити да из симбола I можемо извести било који израз у коме се појављују променљиве x, y или z, константе 0 или 1, знак за сабирање, и знак за супротни број, уз уобичајену употребу заграда. Изведимо, на пример израз $-(1 + x)$:

$$\begin{array}{rcll} I & \to & -I & [\text{применом } I \to -I] \\ & \to & -(I + I) & [\text{применом } I \to (I + I)] \\ & \to & -(1 + I) & [\text{применом } I \to 1] \\ & \to & -(1 + x) & [\text{применом } I \to x] \end{array}$$

3) Над алфабетом $\{F, \Rightarrow, \neg, \top, \bot, p, q, r, (,)\}$ посматрамо следећа правила:

$$F \to \top \quad F \to \bot \quad F \to p \quad F \to q \quad F \to r \quad F \to \neg F \quad F \to (F \Rightarrow F)$$

Није тешко уочити да из симбола F можемо извести било која исказна формула са словима p, q или r, логичким константама $\top$ и $\bot$, и у којој се од везника појављују само негација и импликација. Изведимо, на пример формулу $\neg(q \Rightarrow p)$:

$$\begin{array}{rcll} F & \to & \neg F & [\text{применом } F \to \neg F] \\ & \to & \neg(F \Rightarrow F) & [\text{применом } F \to (F \Rightarrow F)] \\ & \to & \neg(q \Rightarrow F) & [\text{применом } F \to q] \\ & \to & \neg(q \Rightarrow r) & [\text{применом } F \to r] \end{array}$$

Често се променљиве означавају неком карактеристичном скраћеницом (или чтиавом речју) уместо једним словом. На пример, уместо F погодније је писати скраћеницу For. Уз ово значавање, правила

$$\text{For} \to \top \mid \bot \mid p \mid q \mid r \mid \neg\text{For} \mid (\text{For} \Rightarrow \text{For})$$

Списак наведених правила прати следећу индуктивну дефиницију скупа I свих израза наведеног облика:

- променљиве x, y, z, и симболи 0 и 1 су изрази ($x, y, z, 0, 1 \in I$);
- ако је α израз, онда је и $-\alpha$ израз (тј. ако $\alpha \in I$, онда и $-\alpha \in I$);
- ако су α и β изрази, онда је $(\alpha + \beta)$ израз (тј. ако $\alpha, \beta \in I$, онда и $(\alpha + \beta) \in I$).

одсликавају индуктивну дефиницију скупа For исказних формула наведеног облика.

4)[36] Наводимо граматику која генерише један фрагмент граматике Енглеског језика. Приметимо да алфабет ове граматике чине читаве речи и посебно симбола за размак.

(1) Sentence → NounPhrase Verb NounPhrase
(2) NounPhrase → Noun
(3) NounPhrase → Adjective NounPhrase
(4) Noun → people (5) Verb → love
(6) Adjective → good (7) Adjective → charming
(8) Adjective → happy (9) Adjective → bad
(10) Adjective → obnoxious (11) Adjective → unhappy

Шта означавају наведена правила? На пример, правило (1) описује како састављамо Sentence: најпре наводимо NounPhrase, затим размак, па Verb, још један размак и најзад NounPhrase. Правила (2) и (3) описују две могућности да се састави NounPhrase: то може бити само Noun, или се саставља тако што се на Adjective надовеже размак и нека друга NounPhrase. Правила (4–11) представљају речник, који садржи једну именицу Noun (4), један глагол Verb (5) и шест придева Adjectives (6–11). Изведимо реченицу:

happy people love charming bad people

Sentence → NounPhrase Verb NounPhrase
→ Adjective NounPhrase Verb NounPhrase
→ Adjective Noun Verb NounPhrase
→ Adjective Noun Verb Adjective NounPhrase
→ Adjective Noun Verb Adjective Adjective NounPhrase
→ Adjective Noun Verb Adjective Adjective Noun
→ ⋮
→ happy people love bad charming people

[36] Граматика је преузета са такмичња NACLO - North American Computational Linguistics Olympiad

▼ Формалне теорије

Уопштавајући даље наведене системе, долазимо до формалних теорија. *Формалну теорију* чине:

- алфабет Σ (скуп симбола, који не мора бити коначан);
- скуп формула $\mathrm{For} \subseteq \Sigma^*$ (који је углавном одређен неком граматиком);
- скупом аксиома $\mathrm{Ax} \subseteq \mathrm{For}$ (из скупа свих формула издвајамо неке формуле које ћемо сматрати аксиомама);
- скупом правила извођења $\mathcal{P}$ облика:

$$(P): \frac{\alpha_1 \quad \cdots \quad \alpha_n}{\alpha},$$

где $\alpha_1, \ldots, \alpha_n, \alpha$ означавају неке формуле из For; формуле $\alpha_1, \ldots, \alpha_n$ називају се *премисе* (претпоставке), а формула α *закључак* правила.

Приликом задавања неке формалне теорије $\mathcal{F}$, наводимо сва четири скупа која одређују ту теорију и пишемо $\mathcal{F} = (\Sigma, \mathrm{For}, \mathrm{Ax}, \mathcal{P})$.

Дефиниција 4. *Коначан низ формула $\varphi_1, \ldots, \varphi_k$ је извођење (доказ) у формалној теорији $\mathcal{F}$ ако свака формула φ_i, $i = \overline{1,n}$, испуњава један од услова:*

1. *φ_i је аксиома, или*
2. *φ_i се може добити из неких од претходних формула $\varphi_1, \ldots, \varphi_{i-1}$ применом неког од правила извођења из $\mathcal{P}$.*

Формула φ је теорема формалне теорије $\mathcal{F}$, у ознаци $\vdash_{\mathcal{F}} \varphi$ ако постоји извођење у тој теорији чији је последњи члан формула φ.

Ако је из контекста јасно о којој формалној теорији је реч, уместо $\vdash_{\mathcal{F}} \varphi$ краће пишемо $\vdash \varphi$.

> *Уопштено говорећи, формалне теорије посматрамо као машине за производњу теорема.*

Пример 15. Формална теорија $\mathcal{F}$ одређена је на следећи начин:

- алфабет садржи три симбола, $\{|, +, =\}$;
- формуле су све речи облика $x + y = z$, где су x, y, z речи записане само симболом $|$;
- једина аксиома је $| + | = ||$;
- правила извођења су:

$$\text{(R1)}\ \frac{x + y = z}{x| + y = z|} \qquad \text{(R2)}\ \frac{x + y = z}{y + x = z}$$

Докажимо $\vdash_{\mathcal{F}} || + ||| = |||||$:

1.	$\| + \| = \|\|$	аксиома
2.	$\|\| + \| = \|\|\|$	применом правила (R1) на формулу 1.
3.	$\|\|\| + \| = \|\|\|\|$	применом правила (R1) на формулу 2.
4.	$\| + \|\|\| = \|\|\|\|$	применом правила (R2) на формулу 3.
5.	$\|\| + \|\|\| = \|\|\|\|\|$	применом правила (R1) на формулу 4.

Није тешко доказати да је:

$$\vdash_{\mathcal{F}} \underbrace{|\cdots|}_{k \text{ пута}} + \underbrace{|\cdots|}_{\ell \text{ пута}} = \underbrace{|\cdots|}_{m \text{ пута}} \quad \text{акко} \quad k + \ell = m$$

2.3 **Исказни рачун** Ł (**Формална теорија** Ł)

5

Посебно издвајамо формалну теорију познату као (Лукашијевичев) исказни рачун Ł:

- алфабет чине логички везници $\Rightarrow$, $\neg$, заграде (,) и исказна слова $p, q, r, \ldots, p_n, q_n, r_n, \ldots$;
- формуле су све исказне формуле изграђене на уобичејни начин (у којима се појављују само симболи уведеног афабета);
- аксиоме су следећег облика:

  A1 $\alpha \Rightarrow (\beta \Rightarrow \alpha)$

  A2 $(\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$

  A3 $(\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta)$

  где су α, β, γ произвољне формуле;
- једино правило извођења је модус поненс:

$$\frac{\alpha \qquad \alpha \Rightarrow \beta}{\beta}\ (MP)$$

  где су α, β произвољне формуле.

Лема 1. $\vdash_{\text{Ł}} \alpha \Rightarrow \alpha$, *за било коју формулу* α.

Доказ.

1.	$(\alpha \Rightarrow ((\alpha \Rightarrow \alpha) \Rightarrow \alpha)) \Rightarrow ((\alpha \Rightarrow (\alpha \Rightarrow \alpha)) \Rightarrow (\alpha \Rightarrow \alpha))$	аксиома A2
2.	$\alpha \Rightarrow ((\alpha \Rightarrow \alpha) \Rightarrow \alpha)$	аксиома A1
3.	$(\alpha \Rightarrow (\alpha \Rightarrow \alpha)) \Rightarrow (\alpha \Rightarrow \alpha)$	$MP(1,2)$
4.	$\alpha \Rightarrow (\alpha \Rightarrow \alpha)$	аксиома A1
5.	$\alpha \Rightarrow \alpha$	$MP(3,4)$

Наведени низ формула је извођење формуле $\alpha \Rightarrow \alpha$ у рачуну Ł. □

Природно се намеће проблем 'описати све теореме рачуна Ł'. Испоставља се да је исказна формула φ (над алфабетом рачуна Ł) теорема, тј. $\vdash_{\text{Ł}} \varphi$ акко је φ таутологија. Познато је да се исказни везници $\vee$, $\wedge$, $\Leftrightarrow$ могу изразити помоћу $\Rightarrow$ и $\neg$:

Скуп $\{\Rightarrow, \neg\}$ је потпун систем везника.

$$\begin{aligned} \alpha \vee \beta &\equiv \neg\alpha \Rightarrow \beta \\ \alpha \wedge \beta &\equiv \neg\alpha \vee \neg\beta \\ \alpha \Leftrightarrow \beta &\equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha) \end{aligned}$$

Самим тим, рачун Ł је 'машина' за производњу таутологија.

Теорема 7. [***Теорема сагласности***] *Ако је* $\vdash_{\text{Ł}} \varphi$, *онда је* φ *таутологија.*

Доказ. Довољно је доказати:

- Аксиоме A1, A2 и A3 јесу таутологије;
- Правило извођења (MP) *чува* таутологије, тј. ако су α и $\alpha \Rightarrow \beta$ таутологије, онда је и β таутологија.

Показаћемо само ово друго. Ако су α и $\alpha \Rightarrow \beta$, не може постојати валуација за коју би формула β била нетачна. Уколико би за неку валуацију β било нетачно, за ту валуацију би α било тачно (јер је α таутологија), па би импликација $\alpha \Rightarrow \beta$ била нетачна што је немогуће, јер је $\alpha \Rightarrow \beta$ таутологија. □

Важи и обрат претходне теореме: у формалној теорији Ł могу се извести само таутологије. Да бисмо то доказали уводимо концепт *извођења из хипотеза* и доказујемо једно веома важно тврђење.

Дефиниција 5. *Нека је* $\mathcal{F} = (\Sigma, \mathrm{For}, \mathrm{Ax}, \mathcal{P})$ *формална теорија и* $\Gamma \subseteq \mathrm{For}$. *Коначан низ формула* $\varphi_1, \ldots, \varphi_k$ *је извођење из хипотеза* Γ *у формалној теорији* $\mathcal{F}$ *ако свака формула* φ_i, $i = \overline{1,n}$, *испуњава један од услова:*

1. φ_i *је аксиома, или*
2. φ_i *је хипотеза (тј. формула из* Γ*), или*
3. φ_i *се може добити из неких од претходних формула низа* $\varphi_1, \ldots, \varphi_{i-1}$ *применом неког од правила извођења из* $\mathcal{P}$.

Формула φ *је последица хипотеза* Γ, *у ознаци* $\Gamma \vdash_{\mathcal{F}} \varphi$ *ако постоји извођење из* Γ *чији је последњи члан формула* φ.

Лема 2. *1) Ако је* $\Gamma \vdash_{Ł} \varphi$, *онда* $\Gamma, \theta \vdash_{Ł} \varphi$, *за било коју формулу* θ.
2) Ако је $\Gamma \vdash_{Ł} \theta$ *и* $\theta \vdash_{Ł} \varphi$, *онда* $\Gamma \vdash_{Ł} \varphi$.

Доказ. Тврђење 1) је очигледно. 2) Надовезивањем извођења $\Gamma \vdash_{Ł} \theta$ и извођења $\theta \vdash_{Ł} \varphi$, добијамо извођење $\Gamma \vdash_{Ł} \varphi$. □

Теорема 8. [***Став дедукције***] *Ако је* Γ *неки скуп формула и нека су* α, β *произвољне формуле.*

$$\Gamma, \alpha \vdash_{Ł} \beta \text{ акко } \Gamma \vdash_{Ł} \alpha \Rightarrow \beta$$

Доказ. ($\leftarrow$) Доказујемо прво једноставнији део, да из $\Gamma \vdash_{Ł} \alpha \Rightarrow \beta$ следи $\Gamma, \alpha \vdash_{Ł} \beta$.

Претпоставимо да $\Gamma \vdash_{Ł} \alpha \Rightarrow \beta$. Нека је $\varphi_1, \ldots, \varphi_m$ извођење формуле $\alpha \Rightarrow \beta$ из Γ (при чему је, наравно, φ_m формула $\alpha \Rightarrow \beta$). Тада је следећи низ формула извођење формуле β из Γ, α:

1.	φ_1	
	$\vdots$	
m.	$\alpha \Rightarrow \beta$	
$(m+1)$.	α	хипотеза
$(m+2)$.	β	$MP(m+1, m)$

($\rightarrow$) Претпоставимо $\Gamma, \alpha \vdash_{Ł} \beta$. Треба да докажемо да $\Gamma \vdash_{Ł} \alpha \Rightarrow \beta$.

Доказ спроводимо индукцијом по дужини извођења формуле β из хипотеза Γ, α.

(**БИ**) Претпоставимо да се извођења формуле β из хипотеза Γ, α састоји из само једне формуле. Тада та једина формула у извођењу мора бити управо формула β. Самим тим β је аксиома или је β

Водећа замисао у доказу овог дела јесте како извођење $\Gamma, \alpha \vdash_{Ł} \beta$ **прерадити** у извођење $\Gamma \vdash_{Ł} \alpha \Rightarrow \beta$. Ту прераду одређујемо индукцијом по дужини извођења $\Gamma, \alpha \vdash_{Ł} \beta$.

хипотеза, тј. $\beta \in \Gamma \cup \{\alpha\}$. Дакле, могућ је један од следећа три случаја:

- β **је аксиома** – тада је следећи низ формула извођење формуле $\alpha \Rightarrow \beta$ из Γ:
  1. β аксиома
  2. $\beta \Rightarrow (\alpha \Rightarrow \beta)$ аксиома A1
  3. $\alpha \Rightarrow \beta$ $MP(1,2)$

- β **припада** Γ – слично као у претходном случају добијамо извођење формуле $\alpha \Rightarrow \beta$ из Γ:
  1. β хипотеза
  2. $\beta \Rightarrow (\alpha \Rightarrow \beta)$ аксиома A1
  3. $\alpha \Rightarrow \beta$ $MP(1,2)$

- β **је заправо формула** α – онда, према претходној леми $\vdash_{\mathrm{L}} \alpha \Rightarrow \alpha$, а самим тим и $\Gamma \vdash_{\mathrm{L}} \alpha \Rightarrow \alpha$.

(**ИП**) Претпоставимо да за свако $k < n$, ако постоји извођење формуле β дужине k из Γ, α, онда постоји извођење формуле $\alpha \Rightarrow \beta$ из Γ.

Нека је $\varphi_1, \ldots, \varphi_n$ извођење дужине n формуле β из Γ, α; дакле φ_n је формула β. Тада, према претходној дефиницији: (1°) β је аксиома, или (2°) β припада Γ, или (3°) β је формула α, или

(4°) β је добијена применом (MP) неке формуле φ_i и φ_j, за неке $i, j < n$, при чему је формула φ_j заправо $\varphi_i \Rightarrow \beta$.

У случајевима (1°), (2°), (3°) закључујемо као у бази индукције. Преостаје да размотримо случај (4°). Тада извођење има следећи облик:

1. φ_1
   $\vdots$
i. φ_i
   $\vdots$
j. $\varphi_i \Rightarrow \beta$
   $\vdots$
n. β $MP(i,j)$

Првих i формула представљају извођење за φ_i из Γ, α, док првих j формула чине извођење за $\varphi_i \Rightarrow \beta$ из Γ, α. Према индуктивној хипотези $(i, j < n)$ постоје извођења и за $\alpha \Rightarrow \varphi_i$ и за $\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$ из скупа хипотеза Γ:
$\psi_1, \ldots, \psi_\ell$, при чему је ψ_ℓ формула $\alpha \Rightarrow \varphi_i$
$\theta_1, \ldots, \theta_k$, при чему је θ_k формула $\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$. Следећи низ формула чини извођење формуле $\alpha \Rightarrow \beta$ из Γ:

1.	ψ_1	
	$\vdots$	
ℓ.	$\alpha \Rightarrow \varphi_i$	
$(\ell+1)$.	θ_1	
	$\vdots$	
$(\ell+k)$.	$\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$	
$(\ell+k+1)$.	$(\alpha \Rightarrow (\varphi_i \Rightarrow \beta)) \Rightarrow ((\alpha \Rightarrow \varphi_i) \Rightarrow (\alpha \Rightarrow \beta))$	аксиома А2
$(\ell+k+2)$.	$(\alpha \Rightarrow \varphi_i) \Rightarrow (\alpha \Rightarrow \beta)$	$MP(\ell+k, \ell+k+1)$
$(\ell+k+3)$.	$\alpha \Rightarrow \beta$	$MP(\ell, \ell+k+2)$

Дакле, за свако извођење формуле β из Γ, α, постоји извођење формуле $\alpha \Rightarrow \beta$ из Γ. □

Лема 3. *У исказном рачуну* Ł *доказати:*

6

Користити став дедукције када год је то погодно.

(i) $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma \vdash_{Ł} \alpha \Rightarrow \gamma$
(ii) $\vdash_{Ł} (\alpha \Rightarrow \beta) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma))$
(iii) $\alpha, \neg\alpha \vdash_{Ł} \beta$
(iv) $\vdash_{Ł} \neg\neg\alpha \Rightarrow \alpha$
(v) $\vdash_{Ł} \alpha \Rightarrow \neg\neg\alpha$
(vi) $\vdash_{Ł} (\alpha \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$
(vii) $\alpha \Rightarrow \beta, \neg\alpha \Rightarrow \beta \vdash_{Ł} \beta$
(viii) $\alpha, \beta \vdash_{Ł} \alpha \Rightarrow \beta$
(ix) $\alpha, \neg\beta \vdash_{Ł} \neg(\alpha \Rightarrow \beta)$
(x) $\neg\alpha, \beta \vdash_{Ł} \alpha \Rightarrow \beta$
(xi) $\neg\alpha, \neg\beta \vdash_{Ł} \alpha \Rightarrow \beta$

Доказ.

(i) Довољно је доказати $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma, \alpha \vdash_{Ł} \gamma$ (према ставу дедукције):

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	α	хипотеза
3.	β	$MP(1,2)$
4.	$\beta \Rightarrow \gamma$	хипотеза
5.	γ	$MP(3,4)$

Управо доказано тврђење дозвољава да у извођењима користимо правило:

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \gamma}{\alpha \Rightarrow \gamma}\ (T)$$

које обележамо (T) и називамо *транзитивност импликације.*

(iii) Доказујемо да 'из противречних тврдњи можемо извести било који закључак':

1.	$\neg\alpha$	хипотеза
2.	α	хипотеза
3.	$\neg\alpha \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$	А1
4.	$\neg\beta \Rightarrow \neg\alpha$	$MP(2,3)$
5.	$(\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta)$	А3
6.	$\alpha \Rightarrow \beta$	$MP(4,5)$
7.	β	$MP(1,6)$

Приметимо да према ставу дедукције: важи и $\vdash_{Ł} \neg\alpha \Rightarrow (\alpha \Rightarrow \beta)$.

(iv) Докажимо $\neg\neg\alpha \vdash_{\text{Ł}} \alpha$

1.	$\neg\neg\alpha$	хипотеза
2.	$\neg\neg\alpha \Rightarrow (\neg\alpha \Rightarrow \neg\neg\neg\alpha)$	последица тврђења (iii) и става дедукције
3.	$\neg\alpha \Rightarrow \neg\neg\neg\alpha$	$MP(1,2)$
4.	$(\neg\alpha \Rightarrow \neg\neg\neg\alpha) \Rightarrow (\neg\neg\alpha \Rightarrow \alpha)$	A3
5.	$\neg\neg\alpha \Rightarrow \alpha$	$MP(4,5)$
6.	α	$MP(1,6)$

(v)

1.	$\neg\neg\neg\alpha \Rightarrow \neg\alpha$	према (iv)
2.	$(\neg\neg\neg\alpha \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \neg\neg\alpha)$	A3
3.	$\alpha \Rightarrow \neg\neg\alpha$	$MP(1,2)$

(vi) Доказујемо $\alpha \Rightarrow \beta \vdash_{\text{Ł}} \neg\beta \Rightarrow \neg\alpha$

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	$(\neg\neg\alpha \Rightarrow \neg\neg\beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$	A3
3.	$\neg\neg\alpha \Rightarrow \alpha$	према (iv)
4.	$\neg\neg\alpha \Rightarrow \beta$	према (i); $T(3,1)$
5.	$\beta \Rightarrow \neg\neg\beta$	према (v)
6.	$\neg\neg\alpha \Rightarrow \neg\neg\beta$	према (i); $T(4,5)$
7.	$\neg\beta \Rightarrow \neg\alpha$	$MP(6,2)$

(vii) Доказујемо $\alpha \Rightarrow \beta, \neg\alpha \Rightarrow \beta \vdash_{\text{Ł}} \beta$

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	$\neg\alpha \Rightarrow \beta$	хипотеза
3.	$\neg\beta \Rightarrow \neg\alpha$	према (vi)
4.	$\neg\beta \Rightarrow \beta$	према (i); $T(3,2)$
5.	$\neg\beta \Rightarrow (\beta \Rightarrow \neg(\beta \Rightarrow \beta))$	према (iii) и ставу дедукције (два пута)
6.	$\neg\beta \Rightarrow (\beta \Rightarrow \neg(\beta \Rightarrow \beta)) \Rightarrow ((\neg\beta \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)))$	A2
7.	$(\neg\beta \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta))$	$MP(5,6)$
8.	$\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)$	$MP(4,7)$
9.	$(\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)) \Rightarrow ((\beta \Rightarrow \beta) \Rightarrow \beta)$	A3
10.	$(\beta \Rightarrow \beta) \Rightarrow \beta$	$MP(8,9)$
11.	$\beta \Rightarrow \beta$	Лема 1
12.	β	$MP(11,10)$

(viii)

1.	β	хипотеза
2.	$\beta \Rightarrow (\alpha \Rightarrow \beta)$	A1
3.	$\alpha \Rightarrow \beta$	$MP(2,3)$

(ix)

1.	α	хипотеза
2.	$\neg\beta$	хипотеза
3.	$\alpha \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow \beta)$	из $\alpha, \alpha \Rightarrow \beta \vdash_{\text{Ł}} \beta$ и ставу дедукције
4.	$(\alpha \Rightarrow \beta) \Rightarrow \beta$	$MP(1,3)$
4.	$\neg\beta \Rightarrow \neg(\alpha \Rightarrow \beta)$	према (vi)
5.	$\neg(\alpha \Rightarrow \beta)$	$MP(2,5)$

(x)-(xi) Према (iii) важи $\neg\alpha \vdash_{\text{Ł}} \alpha \Rightarrow \beta$, па самим тим важи и $\neg\alpha, \beta \vdash_{\text{Ł}} \alpha \Rightarrow \beta$ и $\neg\alpha, \neg\beta \vdash_{\text{Ł}} \alpha \Rightarrow \beta$. □

Посебно истичемо тврђења (viii)-(xi) претходне леме.

(viii) $\alpha, \quad \beta \vdash \alpha \Rightarrow \beta$
(ix) $\alpha, \quad \neg\beta \vdash \neg(\alpha \Rightarrow \beta)$
(x) $\neg\alpha, \quad \beta \vdash \alpha \Rightarrow \beta$
(xi) $\neg\alpha, \quad \neg\beta \vdash \alpha \Rightarrow \beta$

α	β	$\alpha \Rightarrow \beta$
1	1	1
1	0	0
0	1	1
0	0	1

Ако је v нека валуација исказних слова и φ произвољна формула, нека је $v(\varphi)$ истинитосна вредност формуле φ при валуацији v и

$$\varphi^v = \begin{cases} \varphi, & \text{ако је } v(\varphi) = 1, \\ \neg\varphi, & \text{ако је } v(\varphi) = 0. \end{cases}$$

Уз ове ознаке, тврђења (viii)-(xi) сажето исказујемо у следећој последици.

Последица 1. Ако је v валуација, α, β исказне формуле, онда $\alpha^v, \beta^v \vdash_Ł (\alpha \Rightarrow \beta)^v$.

Последица 2. Нека је φ нека формула у којој се појављују само (не нужно сва) слова $p_1, \ldots, p_k$. Тада за сваку валуацију v важи: $p_1^v, \ldots, p_k^v \vdash_Ł \varphi^v$.

Доказ. Индукцијом по сложености формуле.

(БИ) Тврђење очигледно важи ако је φ исказно слово.

(ИП) Претпоставимо да тврђење важи за све формуле које су мање сложености од φ.

Нека је φ облика $\neg\alpha$. Према (ИП): $p_1^v, \ldots, p_k^v \vdash_Ł \alpha^v$. Разликујемо два случаја.

1. случај: Ако је $v(\alpha) = 0$, онда је $\alpha^v = \neg\alpha$ и $v(\varphi) = 1$, па је $\varphi^v = \varphi = \neg\alpha$, и тврђење је доказано.

2. случај: Ако је $v(\alpha) = 1$, онда је $\alpha^v = \alpha$ и $v(\varphi) = 0$, па је $\varphi^v = \neg\varphi$. Из $p_1^v, \ldots, p_k^v \vdash_Ł \alpha$ добијамо $p_1^v, \ldots, p_k^v \vdash_Ł \neg\neg\alpha$, односно $p_1^v, \ldots, p_k^v \vdash_Ł \neg\varphi$ (тј. $p_1^v, \ldots, p_k^v \vdash \varphi^v$)

Нека је φ облика $\alpha \Rightarrow \beta$. Према индуктивној претпоставци је $p_1^v, \ldots, p_k^v \vdash_Ł \alpha^v$ и $p_1^v, \ldots, p_k^v \vdash_Ł \beta^v$. Када применимо последицу 1 добијамо $p_1^v, \ldots, p_k^v \vdash_Ł (\alpha \Rightarrow \beta)^v$, тј. $p_1^v, \ldots, p_k^v \vdash_Ł \varphi^v$. □

Теорема 9. [***Теорема потпуности***] *Ако је φ таутологија, онда $\vdash_Ł \varphi$.*

Доказ. Нека су $p_1, \ldots, p_k$ слова која се појављују у φ. За било коју валуацију v слова $p_1, \ldots, p_k$ важи $\varphi^v = \varphi$, као и (последица 2) $p_1^v, \ldots, p_k^v \vdash \varphi$.

Нека је w произвољна валуација. Тада

$$p_1^w, \ldots, p_{k-1}^w, p_k \vdash \varphi \text{ и } p_1^w, \ldots, p_{k-1}^w, \neg p_k \vdash \varphi,$$

односно

$$p_1^w, \ldots, p_{k-1}^w \vdash p_k \Rightarrow \varphi \text{ и } p_1^w, \ldots, p_{k-1}^w \vdash \neg p_k \Rightarrow \varphi,$$

одакле следи $p_1^w, \ldots, p_{k-1}^w \vdash \varphi$. Настављајући овај поступак, добијамо $p_1^w, \ldots, p_{k-2}^w \vdash \varphi$ итд., до $\vdash \varphi$. □

Тврђење (vii) претходне леме оправдава употребу правила

$$\frac{\alpha \Rightarrow \beta \quad \neg\alpha \Rightarrow \beta}{\beta}$$

2.4 Природна дедукција у исказној логици

7

У исказном рачуну Ł главну улогу у генерисању извођења имају:

- правило *модус поненс* $\dfrac{\alpha \quad \alpha \Rightarrow \beta}{\beta}$, које одређује како у извођењима да користимо *импликације*, тј. формуле чији је главни знак $\Rightarrow$ и
- став дедукције – $\Gamma, \alpha \vdash \beta$ акко $\Gamma \vdash \alpha \Rightarrow \beta$; Став дедукције утврђује како да доказујемо *импликације*: да бисмо доказали $\Gamma \vdash \alpha \Rightarrow \beta$, довољно је доказати $\Gamma, \alpha \vdash \beta$.

Ова запажања веома су блиска идејама на којима је заснован један од најпознатијих формалних теорија које карактеришу исказну логику – **природна дедукција**[44]. Скуп аксиома овог формалног система је празан док су правила извођења дата следећим схемама (у смислу да α, β и γ могу бити произвољне формуле):

[44] Рачун природне дедукције увео је, 1935. године, Герхард Генцен с намером да природније опише уобичајено закључивање математичара

$$\frac{\alpha \quad \beta}{\alpha \wedge \beta}\ (\wedge_{\mathrm{U}})$$

Увођење конјункције ($\wedge_{\mathrm{U}}$): из претпоставки α, β (директно) закључујемо $\alpha \wedge \beta$. Можемо размишљати и овако: да бисмо доказали $\alpha \wedge \beta$ потребно је да докажемо сваки конјункт појединачно, и α и β. Другим речима доказ за $\alpha \wedge \beta$ добијамо спајањем доказа за α и доказа за β.

$$\frac{\alpha \wedge \beta}{\alpha}\ (\wedge^{\mathrm{L}}_{\mathrm{E}}) \qquad \frac{\alpha \wedge \beta}{\beta}\ (\wedge^{\mathrm{D}}_{\mathrm{E}})$$

Елиминација конјункције: из претпоставке $\alpha \wedge \beta$ закључујемо α (одн. β) применом правила ($\wedge^{\mathrm{L}}_{\mathrm{E}}$) (одн. ($\wedge^{\mathrm{D}}_{\mathrm{E}}$)).

Пример 16. Докажимо секвент $(p \wedge q) \wedge s, r \wedge t \vdash t \wedge q$.

1.	$(p \wedge q) \wedge s$	претпоставка
2.	$r \wedge t$	претпоставка
3.	$p \wedge q$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1 [формула $p \wedge q$ је добијена применом правила $\wedge^{\mathrm{L}}_{\mathrm{E}}$ на 1.]
4.	q	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	t	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 2
6.	$t \wedge q$	$\wedge_{\mathrm{U}}$, 5, 4

Наведени доказ можемо приказати и на следећи начин.

$$\dfrac{\dfrac{r \wedge t}{t}\wedge^{\mathrm{D}}_{\mathrm{E}} \quad \dfrac{\dfrac{(p \wedge q) \wedge s}{p \wedge q}\wedge^{\mathrm{L}}_{\mathrm{E}}}{q}\wedge^{\mathrm{D}}_{\mathrm{E}}}{t \wedge q}\wedge_{\mathrm{U}}$$

Уводна разматрања најављују правила увођења и елиминације импликације.

$$\frac{\alpha \Rightarrow \beta \quad \alpha}{\beta}\ (\Rightarrow_{\mathrm{E}})$$

Елиминација импликације (одн. модус поненс) ($\Rightarrow_{\mathrm{E}}$) описује како се у доказима користе тврдње формулисане у облику имликације.

$$\dfrac{\begin{array}{|l}\alpha \\ \vdots \\ \beta\end{array}}{\alpha \Rightarrow \beta}\ (\Rightarrow_{\mathrm{U}})$$

Увођење импликације ($\Rightarrow_{\mathrm{U}}$): да бисмо доказали импликацију $\alpha \Rightarrow \beta$ треба увести *додатну (привремену) претпоставку* α и доказати β, при чему је у том доказу дозвољено користити α, све остале претпоставке и међузакључке које смо већ извели. Доказ формуле β након увођења додатне претпоставке α истичемо вертикалном цртом и називамо *поддоказом*. Непосредно испод завршетка вертикалне линије наводимо закључак $\alpha \Rightarrow \beta$, ознаку правила ($\Rightarrow_{\mathrm{U}}$) и бројеве којима су нумерисани кораци поддоказа.

Пример 17. Докажимо $p \Rightarrow q, p \Rightarrow r \vdash p \Rightarrow q \wedge r$

1.	$p \Rightarrow q$	претпоставка
2.	$p \Rightarrow r$	претпоставка
3.	p	додатна претпоставка
4.	q	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	r	$\Rightarrow_{\mathrm{E}}$, 2, 3
6.	$q \wedge r$	$\wedge_{\mathrm{U}}$, 4, 5
7.	$p \Rightarrow q \wedge r$	$\Rightarrow_{\mathrm{U}}$, 3-6

$\vdots$			Када желимо да докажемо $\alpha \Rightarrow \beta$:
$j.$	α		уводимо додатну претпоставку α
$\vdots$	$\vdots$		и настојимо да докажемо β.
$k.$	β		Када успемо,
$k+1.$	$\alpha \Rightarrow \beta$	$\Rightarrow_{\mathrm{U}}$, j-k	изводимо жељени закључак.

$$\frac{\alpha \quad \neg\alpha}{\bot}(\neg_{\mathrm{E}})$$

Елиминација негације ($\neg_{\mathrm{E}}$): из претпоставки α, $\neg\alpha$ изводимо контрадикцију.

$$\begin{array}{|l} \alpha \\ \vdots \\ \bot \end{array} \over \neg\alpha (\neg_{\mathrm{U}})$$

Увођење негације ($\neg_{\mathrm{U}}$): ако из α докажемо контрадикцију, онда закључујемо $\neg\alpha$.

$$\begin{array}{|l} \neg\alpha \\ \vdots \\ \bot \end{array} \over \alpha (\bot_{\mathrm{c}})$$

Правило ($\bot_{\mathrm{c}}$): да бисмо доказали α, у класичној логици, довољно је извести контрадикцију из $\neg\alpha$.

$$\frac{\alpha}{\alpha \vee \beta}(\vee^{\mathrm{L}}_{\mathrm{U}}) \quad \frac{\beta}{\alpha \vee \beta}(\vee^{\mathrm{D}}_{\mathrm{U}})$$

Увођење дисјункције: из α (ако смо доказали α) изводимо закључак $\alpha \vee \beta$), за било коју формулу β, применом правила ($\vee^{\mathrm{L}}_{\mathrm{U}}$); на исти начин, из β изводимо закључак $\alpha \vee \beta$, за било коју формулу α, применом правила ($\vee^{\mathrm{D}}_{\mathrm{U}}$).

Елиминација дисјункције ($\vee_{\mathrm{E}}$) описује на који начин у доказима користимо формуле облика $\alpha \vee \beta$? Замислимо да желимо да докажемо γ претпостављајући $\alpha \vee \beta$. Будући да не знамо која је од формула α, β тачна (а једна мора бити), морамо спровести два одвојена доказа:

$$\begin{array}{|l|l} \alpha & \beta \\ \vdots & \vdots \\ \gamma & \gamma \end{array} \over \gamma (\vee_{\mathrm{E}})$$

- Најпре, претпостављамо да је α тачно и доказујемо γ.
- Затим, претпостављамо да је β тачно и доказујемо γ.

На основу ова два доказа и претпоставке $\alpha \vee \beta$ закључујемо γ, јер два поддоказа покривају обе могућности.

Еквиваленција два исказа $\alpha \Leftrightarrow \beta$ јесте заправо конјункција две обратне импликације $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, па се правила **увођења** и **елиминације еквиваленције** сама намећу.

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \alpha}{\alpha \Leftrightarrow \beta}(\Leftrightarrow_{\mathrm{U}}) \qquad \frac{\alpha \Leftrightarrow \beta}{\alpha \Rightarrow \beta}(\Leftrightarrow^{\mathrm{LD}}_{\mathrm{E}}) \qquad \frac{\alpha \Leftrightarrow \beta}{\beta \Rightarrow \alpha}(\Leftrightarrow^{\mathrm{DL}}_{\mathrm{E}})$$

Наведена правила карактеришу доказивост тзв. *секвената*

$$\varphi_1, \ldots, \varphi_k \vdash \psi$$

(тј. доказивост да из претпоставки $\varphi_1, \ldots, \varphi_k$ следи ψ). Секвенте доказујемо тако што формирамо низ који чине претпоставке $\varphi_1, \ldots, \varphi_k$

и (међу)закључци добијени применом правила дедукције на већ наведене формуле. Поступак завршавамо када добијемо жељени закључак ψ, а формирани низ називамо доказом формуле ψ из претпоставки $\varphi_1, \ldots, \varphi_k$, одн. *доказом* одговарајућег секвента.

Пример 18. Доказати $\vdash (p \Rightarrow q) \vee (p \Rightarrow r) \Rightarrow (p \Rightarrow q \vee r)$.

1.	$(p \Rightarrow q) \vee (p \Rightarrow r)$	додатна претпоставка
2.	$\quad p \Rightarrow q$	додатна претпоставка
3.	$\quad\quad p$	додатна претпоставка
4.	$\quad\quad q$	$\Rightarrow_{\mathrm{E}}$, 2, 3
5.	$\quad\quad q \vee r$	$\vee_{\mathrm{U}}^{\mathrm{L}}$, 4
6.	$\quad p \Rightarrow (q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 3-5
7.	$\quad p \Rightarrow r$	додатна претпоставка
8.	$\quad\quad p$	додатна претпоставка
9.	$\quad\quad r$	$\Rightarrow_{\mathrm{E}}$, 7, 8
10.	$\quad\quad q \vee r$	$\vee_{\mathrm{U}}^{\mathrm{D}}$, 9
11.	$\quad p \Rightarrow (q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 7-10
12.	$p \Rightarrow (q \vee r)$	$\vee_{\mathrm{E}}$, 1, 2-6, 7-11
13.	$(p \Rightarrow q) \vee (p \Rightarrow r) \Rightarrow (p \Rightarrow q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 1-12

Теорема 10. $\Gamma \vdash_{\text{Ł}} \varphi$ *акко* $\Gamma \vdash \varphi$ *(је доказив секвент применом правила природне дедукције).*

Специјално, формула φ је теорема у рачуну природне дедкуције, ако је доказив секвент $\vdash \varphi$ (са празним скупом претпоставки). Из претходне теореме и теореме потпуности закључујемо да се правилима природне дедукције могу доказати све таутологије, и само таутологије.

Да бисмо поједноставили доказивање секваната, списак правила проширујемо још неким **изведеним правилима**, чија се употреба, наравно, једноставно може елиминисати из сваког доказа.

$$\frac{\alpha \Rightarrow \beta \quad \neg\beta}{\neg\alpha}\ (\mathrm{MT})$$

Правило modus tolens (MT) може бити веома корисно при употреби тврдњи у облику импликације.

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\neg\beta$	претпоставка
3.	$\quad\alpha$	додатна прет.
4.	$\quad\beta$	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	$\quad\bot$	$\neg_{\mathrm{E}}$, 2, 4
6.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 3-5

$$\frac{\neg\neg\alpha}{\alpha}\ (\neg\neg_{\mathrm{E}}) \qquad \frac{\alpha}{\neg\neg\alpha}\ (\neg\neg_{\mathrm{U}})$$

Правило $(\neg\neg_{\mathrm{E}})$ нам дозвољава да обришемо два знака негације. Насупрот томе, правило $(\neg\neg_{\mathrm{U}})$ дозвољава да се испред сваке формуле допишу два знака негације.

Оправдавамо само правило $\neg\neg_{\mathrm{U}}$.

1.	α	претпоставка
2.	$\neg\alpha$	додатна прет.
3.	$\bot$	$\neg_{\mathrm{E}}$, 1, 2
4.	$\neg\neg\alpha$	$\neg_{\mathrm{U}}$, 2-3

Пример 19. Примену изведених правила једноставно можемо елиминисати из сваког доказа. То илуструјемо доказом секвента $p \Rightarrow \neg q, q \vdash \neg p$.

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\neg\neg q$	$\neg\neg_{\mathrm{U}}$, 2
4.	$\neg p$	MT, 1, 3

Без правила $\neg\neg_{\mathrm{U}}$ и MT дати секвент бисмо доказали на следећи начин.

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\neg q$	додатна претпоставка
4.	$\bot$	$\neg_{\mathrm{E}}$, 2, 3
5.	$\neg\neg q$	$\neg_{\mathrm{U}}$, 3-4
6.	p	додатна претпоставка
7.	$\neg q$	$\Rightarrow_{\mathrm{E}}$, 1, 6
8.	$\bot$	$\neg_{\mathrm{E}}$, 2, 7
9.	$\neg p$	$\neg_{\mathrm{U}}$, 6-8

Дисјунктивни силогизми
$\dfrac{\alpha \vee \beta \quad \neg\alpha}{\beta}$ (DS) $\quad \dfrac{\alpha \vee \beta \quad \neg\beta}{\alpha}$ (DS)

Оба правила означавамо на исти начин јер ће увек бити очигледно које од ова два правила користимо.

1.	$\alpha \vee \beta$	претпоставка
2.	$\neg\alpha$	претпоставка
3.	α	додатна претпоставка
4.	$\bot$	$\neg_{\mathrm{E}}$, 2, 3
5.	β	$\bot_{\mathrm{E}}$, 4
6.	β	додатна претпоставка
7.	β	$\vee_{\mathrm{E}}$, 1, 3-5, 6

Аналогно се доказује и секвент $\alpha \vee \beta, \neg\beta \vdash \alpha$, за било које формуле α, β.

Транзитивност импликације	Закони контрапозиције
$\dfrac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \gamma}{\alpha \Rightarrow \gamma}$ (T)	$\dfrac{\alpha \Rightarrow \beta}{\neg\beta \Rightarrow \neg\alpha}$ (K) $\quad \dfrac{\neg\alpha \Rightarrow \neg\beta}{\beta \Rightarrow \alpha}$ (K)

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\beta \Rightarrow \gamma$	претпоставка
3.	α	додатна прет.
4.	β	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	γ	$\Rightarrow_{\mathrm{E}}$, 2, 4
6.	$\alpha \Rightarrow \gamma$	$\Rightarrow_{\mathrm{U}}$, 3-5

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\neg\beta$	додатна прет.
3.	$\neg\alpha$	MT, 1, 2
4.	$\neg\beta \Rightarrow \neg\alpha$	$\Rightarrow_{\mathrm{U}}$, 2-3

Закон искључења трећег (tertium non datur)
$\dfrac{}{\alpha \vee \neg\alpha}$ (TND)

Према закону искључења трећег, у доказима можемо користити као претпоставку $\alpha \vee \neg\alpha$, за било коју формулу α.

1.	$\neg(\alpha \vee \neg\alpha)$	додатна претпоставка
2.	α	додатна претпоставка
3.	$\alpha \vee \neg\alpha$	$\vee^{\mathrm{L}}_{\mathrm{U}}$, 2
4.	$\bot$	$\neg_{\mathrm{E}}$, 1, 3
5.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 2-4
6.	$\alpha \vee \neg\alpha$	$\vee^{\mathrm{D}}_{\mathrm{U}}$, 5
7.	$\bot$	$\neg_{\mathrm{E}}$, 1, 6
8.	$\neg\neg(\alpha \vee \neg\alpha)$	$\neg_{\mathrm{U}}$, 1-7
9.	$\alpha \vee \neg\alpha$	$\neg\neg_{\mathrm{E}}$, 8

Де Морганови закони			
$\dfrac{\neg\alpha \vee \neg\beta}{\neg(\alpha \wedge \beta)}$ (DM)	$\dfrac{\neg\alpha \wedge \neg\beta}{\neg(\alpha \vee \beta)}$ (DM)	$\dfrac{\neg(\alpha \vee \beta)}{\neg\alpha \wedge \neg\beta}$ (DM)	$\dfrac{\neg(\alpha \wedge \beta)}{\neg\alpha \vee \neg\beta}$ (DM)

Свако од ова четири правила назваћемо Де Морган овим законом, јер приликом примене неће бити забуне.

1.	$\neg\alpha \vee \neg\beta$	претпоставка
2.	$\alpha \wedge \beta$	додатна прет.
3.	α	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 2
4.	$\neg\neg\alpha$	$\neg\neg_{\mathrm{U}}$,
5.	$\neg\beta$	DS, 1, 4
6.	β	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 2
7.	$\bot$	$\neg_{\mathrm{E}}$, 5, 6
8.	$\neg(\alpha \wedge \beta)$	$\neg_{\mathrm{U}}$, 2-7

1.	$\neg\alpha \wedge \neg\beta$	претпоставка
2.	$\neg\alpha$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1
3.	$\neg\beta$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 1
4.	$\alpha \vee \beta$	додатна прет.
5.	β	DS, 2, 4
6.	$\bot$	$\neg_{\mathrm{E}}$, 3, 5
7.	$\neg(\alpha \vee \beta)$	$\neg_{\mathrm{U}}$, 2-6

1.	$\neg(\alpha \vee \beta)$	претпоставка
2.	α	додатна прет.
3.	$\alpha \vee \beta$	$\vee^{\mathrm{L}}_{\mathrm{U}}$, 2
4.	$\bot$	$\neg_{\mathrm{E}}$, 1, 3
5.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 2-4
6.	β	додатна прет.
7.	$\alpha \vee \beta$	$\vee^{\mathrm{D}}_{\mathrm{U}}$, 6
8.	$\bot$	$\neg_{\mathrm{E}}$, 1, 7
9.	$\neg\beta$	$\neg_{\mathrm{U}}$, 6-8
10.	$\neg\alpha \wedge \neg\beta$	$\wedge_{\mathrm{U}}$, 5, 9

1.	$\neg(\alpha \wedge \beta)$	претпоставка
2.	α	додатна прет.
3.	β	додатна прет.
4.	$\alpha \wedge \beta$	$\wedge_{\mathrm{U}}$, 2, 3
5.	$\bot$	$\neg_{\mathrm{E}}$, 1, 4
6.	$\neg\beta$	$\neg_{\mathrm{U}}$, 3-5
7.	$\neg\alpha \vee \neg\beta$	$\vee^{\mathrm{D}}_{\mathrm{U}}$, 6
8.	$\neg\alpha$	додатна прет.
9.	$\neg\alpha \vee \neg\beta$	$\vee^{\mathrm{L}}_{\mathrm{U}}$, 8
10.	$\alpha \vee \neg\alpha$	TND
11.	$\neg\alpha \vee \neg\beta$	$\vee_{\mathrm{E}}$, 10, 2-7, 8-9

3. Чиста предикатска логика

Неформално говорећи, исказна логика се бави структуром реченица узимајући у обзир само начин на који су неки једноставни искази повезани логичким везницима, док је значење тих полазних исказа потпуно неважно. Тако, исказна логика није довољно изражајна да би се у њој размотрало следеће чувено закључивање:

> Сваки човек је смртан.
> Сократ је човек.
> **Дакле**, Сократ је смртан.

Предикатска логика омогућава да разматрамо и смисао полазних исказа. Пре него што детаљно опишемо поменуту логику, наводимо један пример у коме ћемо објаснити неке полазне идеје у развоју предикатске логике.

Пример 20. Природни језици нису погодни за прецизно изражавање смисла исказа. Да ли реченица *Сваки момак воли једну девојку* значи (1) *Постоји једна девојка коју воли сваки момак* или (2) *За сваког момка се може пронаћи једна девојка коју он воли*?

Потреба да се елиминишу двосмислености природног језика довела је, између осталог, до увођења тзв. *формалних језика* чије се реченице формирају према унапред утврђеним правилима. Реченице (1) и (2) формално ћемо изразити користећи:

- логичке везнике ($\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$),
- квантификаторе $\forall$ – *сваки* и $\exists$ – *неки*,
- променљиве $x, y, z, x_1, y_1, z_1, x_2, \ldots$ (којима ћемо означавати 'произвољно', 'неодређено' људско биће) и
- помоћне знаке: зарез и заграде.

Поред тога, потребно је да неким симболима означимо и особине *бити момак* и *бити девојка*, као и однос *волети*. Изјаву '*x је момак*' означавамо $M(x)$, '*x је девојка*' означавамо $D(x)$, док $V(x, y)$ значи '*x воли y*'.

Реченицама (1) и (2) редом одговарају следеће формуле:

$$\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y, x))) \text{ и } \forall x(M(x) \Rightarrow \exists y(D(y) \wedge V(x, y))),$$

Наводимо формализације још неколико реченица природног језика.

- Свако воли некога – $\forall x \exists y V(x, y)$
- Неко воли свакога – $\exists x \forall y V(x, y)$
- Неко не воли никога – $\exists x \forall y \neg V(x, y)$

3.1. **Предикатске формуле**

8

Језик предкатске логике развијен је у једном од најважнијих логичких дела – у књижици Begriffsschrift (Појмовно писмо) од стотинак страница које је написао Готлоб Фреге и објавио 1879. године[47]. Поднаслов овог дела је

формални језик за чисто мишљење, по узору на језик аритметике.

Уопштено говорећи, језиком предикатске логике описујемо извесне *објекте* помоћу унапред изабраних *предиката* (који могу представљати *својства* појединачних објеката, али и међусобне *везе* више објеката).

[47] Фрегеа је, по сопственом признању, водила Лајбницова идеја о универзалном језику, lingua charactera, чији је успех лежао у разборитом избору симбола. Фрегеов језик је вештачки језик одређен прецизним граматичким правилима, односно синтаксом. Слободно се може сматрати да је Begriffsschrift претеча свих програмских језика.

▼ Универзум објеката и предикати

Уопштено:

Универзум чине сви објекти о којима говоримо. Поједине, конкретне, одређене објекте универзума називаћемо *константама*.

Сваки предикат има своју *дужину*, тј. придружени број који одређује дужину низа објеката на који се предикат односи:

- *унарни предикати* представљају својства, одн. особине појединачних објеката;
- *бинарни предикати* представљају везе између два објекта, тј. особину двочланих низова објеката;
- *тернарни предикати* представљају везе између три објекта, тј. особину трочланих низова објеката;

...

- n-арни *предикати* представљају особину n-точланих низова објеката.

Претходни пример:

Универзум чине сви људи. Свака конкретна особа представља неку константу универзума који чине људи: `Абелар`, `Елоиза` итд.

Словима M и D су означена два унарна предиката која редом одговарају особинама *бити момак* и *бити девојка*. Изјаве *Абелар је момак* и *Елоиза је девојка* краће означавамо $M(\texttt{Абелар})$ и $D(\texttt{Елоиза})$.

Словом V означен је бинарни предикат који одговара вези *волети*. Изјаве *Абелар воли Елоизу* и *Елоиза воли Абелара* краће означавамо $V(\texttt{Абелар}, \texttt{Елоиза})$ и $D(\texttt{Елоиза}, \texttt{Абелар})$.

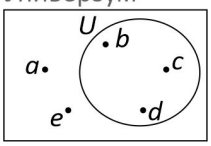
Избором предиката бирамо заправо основне (атомске) изјаве које користимо приликом описивања одговарајућег универзума.

Пример 21. Имајући на уму неки универзум, предикат одређене дужине дефинишемо додељивањем истинитосних вредности сваком исказу добијеном дејством предиката на низ објеката одговарајуће дужине. На 'малим' универзумима предикате можемо дефинисати на више начина: графички, табелом, набрајањем низова објеката који имају одговарајуће својство и сл.

Посматрајмо универзум од пет објекта: a, b, c, d, e.

Дефинишимо унарни предикат U.

Графички:
За унарне предикате користимо тзв. Венове дијаграме:



Табелом:
На више начина се може дефинисати табела:

исказ	0/1
$U(a)$	0
$U(b)$	1
$U(c)$	1
$U(d)$	1
$U(e)$	0

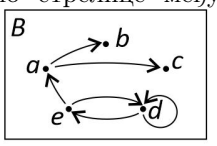
или

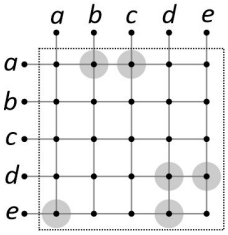
x	$U(x)$
a	0
b	1
c	1
d	1
e	0

Набрајањем:
Својство U имају објекти b, c и d; тј. тачни су искази $U(b)$, $U(c)$ и $U(c)$ (подразумева се да a и e немају својство U).

Дефинишимо бинарни предикат B.

Графички:
За бинарне предикате користимо стрелице међу објектима:





Табелом:
Бинарне предикате је најпрегледније задати табелом следећег облика:

B	a	b	c	d	e
a	0	1	1	0	0
b	0	0	0	0	0
c	0	0	0	0	0
d	0	0	0	1	1
e	1	0	0	1	0

Набрајањем:
Својство B имају следећи парови (a,b), (a,c), (d,d), (d,e), (e,a), (e,d); тј. тачни су искази $B(a,b)$, $B(a,c)$, $B(d,d)$, $B(d,e)$, $B(e,a)$, $B(e,d)$.

Некада је најједноставније предикат дефинисати прецизним описом на говорном језику. Дефинишемо један тернарни предикат.

Описно:
T је тернарни предикат дат на следећи начин: *уређена тројка објеката има особину T акко су свака два члана те тројке међусобно различита.*

Набрајањем:
Тачни су следећи искази: $T(a,b,c)$, $T(a,c,b)$, $T(b,a,c)$, $T(b,c,a)$, $T(c,a,b)$, $T(c,b,a)$, ..., $T(e,d,c)$; нетачни су: $T(a,a,a)$, $T(a,a,b)$, $T(a,b,a)$, $T(b,c,b)$, $T(b,a,b)$ итд.

Полазећи од наведених *атомских* исказа, употребом логичких везника формирамо сложеније исказе, чију истинитост једноставно рачунамо:

- $U(e) \wedge \neg B(b,a) \Rightarrow T(e,c,d)$ је тачан исказ;
- $B(d,e) \wedge B(e,a) \Rightarrow B(d,a)$ је нетачан исказ итд.

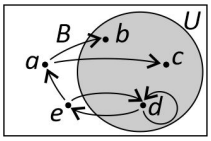
▼ Променљиве и исказне функције

Променљиве $x, y, z, x_1, y_1, z_1, \ldots$ користимо да означимо произвољне, неодређене објекте универзума. Када променљиве користимо

као аргуманате предиката, не добијамо исказ већ тзв. *исказну функцију*. Полазећи од оваквих *атомских* исказних функција, применом исказних везника ($\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$) на уобичајени начин, градимо сложеније исказне функције. Било којом заменом промењивих конкретним објектима универзума добијамо исказ, чију истинитосну вредност рачунамо према дефиницији предиката. Наравно, уколико се једна промењива појављује више пута у истој исказној функцији, увек је замењујемо истим објектом.

Пример 22. Нека су универзум и предикати одређени као у претходном примеру. Дефинишимо неколико исказних функција.

Универзум: a, b, c, d, e.
Предикати U и B су дефинисани графички:



Истинитосне функције:
У зависности од x одређујемо истинитосну вредност за $U(x) \Rightarrow B(x,x)$:

x	$U(x) \Rightarrow B(x,x)$	$U(x) \vee \neg B(x,x)$	$U(x) \wedge B(x,x)$
a	1		
b	0		
c	0		
d	1		
e	1		

Истинитосна вредност исказне функције $U(x) \wedge U(y) \Rightarrow \neg B(x,y)$ зависи од вредности x и y.

x	a	a	a	a	a	b	b	b	b	b	c	c	c	c	c	d	d	d	d	d	e	e	e	e	e
y	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e
$U(x) \wedge U(y) \Rightarrow \neg B(x,y)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
$\neg(U(x) \vee U(y)) \wedge B(x,y)$																									
$\neg U(x) \wedge B(x,y) \Rightarrow U(y)$																									
$B(x,y) \vee B(y,x)$																									
$B(x,y) \vee \neg B(x,y)$																									

▼ Квантификатори; слободна и везана појављивања промењиве

Значајно већа изражајна моћ предикатске логике, у односу на исказну логику, долази од употребе *квантификатора*. Користимо две врсте квантификатора:

- универзални квантификатор, који означавамо $\forall$ и значи 'за сваки' (за произвољан, за било који и сл.)
- егзистенцијани квантификатор, који означавамо $\exists$ и значи 'за неки' (постоји, за бар један и сл.)

Уопштено, **предикатске формуле** градимо користећи:

- *нелогичке симболе*, тј. симболе константи и предикатске симболе, са придруженим дужинама, који су изабрани у складу са контекстом;

- *логичке симболе*, који се користе у било ком контексту,
  - бесконачан скуп променљивих $x, y, z, x_1, y_1, z_1, \ldots$;
  - логичке везнике: $\wedge$, $\vee$, $\neg$, $\Rightarrow$ и $\Leftrightarrow$;
  - логичке константе: $\bot$, $\top$;
  - квантификаторе: $\forall$ (универзални) и $\exists$ (егзистенцијални);
  - помоћне знаке, тј. уобичајени симболи за зарез и заграде.

Овако изабран алфабет одређује тзв. *чист предикатски језик*.

Дефиниција 6. *(1)* ***Атомске формуле*** *градимо тако што предикатским симболом повежемо одговарајући број симбола који се односе на објекте универзума (константе и/или променљиве).*
(2) ***Предикатске формуле*** *градимо следећим правилима:*

- *логичке константе $\bot$ и $\top$, као и све атомске формуле јесу формуле;*
- *ако је α формула, онда је и $\neg\alpha$ формула;*
- *ако су α, β формуле и $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$, онда је и $(\alpha * \beta)$ формула;*
- *ако је α формула и x променљива, онда су $\forall x\alpha$ и $\exists x\alpha$ формуле.*

Када квантификатор са неком променљивом поставимо испред формуле, тада сва појављивања те променљиве у поменутој формули постају *везана* и кажемо да су под *дејством постављеног квантификатора*. Уколико неко појављивање променљиве у формули није под дејством ниједног квантификатора, кажемо да је *слободно*.

Пример 23. Одредимо везана и слободна појављивања променљивих у формули $\exists x(V(x,y) \Rightarrow M(x) \vee D(y)) \wedge \neg\forall y V(y,y)$. Стрелице на наредној слици показују на слободна појављивања променљивих.

$$\exists x(V(x,\underset{\downarrow}{y}) \Rightarrow M(x) \vee D(\underset{\downarrow}{y})) \wedge \neg\forall y V(y,y)$$

Појављивања осталих променљивих су везана.

Променљива је слободна у некој формули ако има слободно појављивање у тој формули. Када желимо да истакнемо да су све слободне променљиве формуле α неке (не нужно све) од променљивих $x_1, \ldots, x_n$, онда пишемо $\alpha(x_1, \ldots, x_n)$.

Пример 24. Ако са α означимо формулу

$$\exists x(V(x,y) \Rightarrow M(x) \vee D(y)) \wedge \neg\forall y V(y,y)$$

(из претходног примера), онда бисмо је, ради истицања слободних променљивих, могли означити $\alpha(y)$, али и $\alpha(y,z)$, $\alpha(y,x_1,\ldots,x_n)$ и слично – важно је само да се променљива y појави на списку променљивих у загради.

Свака формула са слободним променљивама на изабраном универзуму дефинише једну истинитосну функцију чији су аргументи објекти универзума, а вредности су 0 или 1. Када слободним променљивама неке формуле доделимо конкретне објекте, истинитосну вредност добијеног исказа одређујемо применом истинитосних таблица за логичке везнике и следећих правила за квантификаторе:

- Ако су слободним променљивама формуле $\forall x\alpha$ додељени неки објекти универзума, онда је $\forall x\alpha$ тачна за те вредности променљивих, ако је за **сваки** (било који) објекат универзума додељен променљивој x формула α тачна;

  $\forall x\alpha(x)$ је тачно, ако је $\alpha(c)$ тачно, за сваки објекат c универзума.

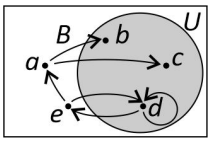
- Ако су слободним променљивама формуле $\exists x\alpha$ додељени неки објекти универзума, онда је $\exists x\alpha$ тачна за те вредности променљивих, ако је за **неки** (бар један) објекат универзума додељен променљивој x формула α тачна;

  $\exists x\alpha(x)$ је тачно, ако је $\alpha(c)$ тачно, за неки објекат c универзума.

Пример 25. Поново се ослањамо на универзум и предикате одређене у претходна два примера.

Универзум: a, b, c, d, e.

Предикати U и B су дефинисани графички:



Истинитосна вредност формула $U(x) \Rightarrow B(x,x)$ и $B(x,x) \Rightarrow U(x)$ зависи од x:

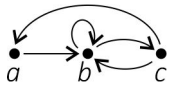
x	$U(x) \Rightarrow B(x,x)$	$B(x,x) \Rightarrow U(x)$
a	1	1
b	0	1
c	0	1
d	1	1
e	1	1

Из табела датих исказних функција закључујемо и да тачне следеће формуле без слободних променљивих:

$$\exists x(U(x) \Rightarrow B(x,x)), \qquad \neg\forall x(U(x) \Rightarrow B(x,x)), \qquad \forall x(B(x,x) \Rightarrow U(x))$$

Посебно истичемо да за тачност претходних формула није потребно додељивање вредности променљивима.

Пример 26. Над универзумом који чине три објекта a, b и c, задат је бинарни предикат R (сликом доле лево, одн. табелом доле десно).



R	a	b	c
a	0	1	0
b	0	1	1
c	1	1	0

Испитајмо истинитосне вредности формула $\forall y\, R(x,y)$ и $\forall y\, R(y,x)$, за разне вредности слободне променљиве x. Наравно, за изабрано x, треба за све вредности променљиве y испитати истинтосне вредности формула $R(x,y)$, одн. $R(y,x)$.

Формуле постају разумљивије, ако $R(x,y)$ читамо као реченицу

из x иде стрелица ка y.

Тада:

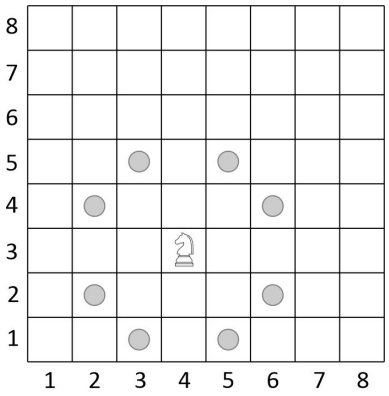
- $\forall y R(x,y)$ значи

x	y	$R(x,y)$	$\forall y\, R(x,y)$	$R(y,x)$	$\forall y\, R(y,x)$
	a	0		0	
a	b	1	0	0	0
	c	0		1	
	a	0		1	
b	b	1	0	1	1
	c	1		1	
	a	1		0	
c	b	1	0	1	0
	c	0		0	

Закључујемо да су тачне и следеће формуле без слободних променљивих:

- $\neg\exists x\forall y\, R(x,y)$ (не постоји тачка из које полазе стрелица ка свим тачкама универзума);
- $\exists x\forall y\, R(y,x)$ (постоји тачка у коју долазе стрелице из свих тачака универзума)

Пример 27. Употреба променљивих значајно повећава изражајну моћ предикатског језика. Значај променљивих илуструјемо репрезентацијом информација о кретању скакача на шаховској табли. Поља табле означавамо паром бројева од 1 до 8.



Узимајући да универзум чине бројеви 1, 2, 3, 4, 5, 6, 7, 8; посматрамо предикат дужине 4 (тј. 4-арни предикат): $S(x_1,x_2,x_3,x_4)$

'дозвољено је да скакач пређе са поља (x_1,x_2) на поље (x_3,x_4).'

Један начин да наведемо све допустиве потезе јесте да их излистамо:

$$(*)\quad S(1,1,2,3), S(1,1,3,2),\ldots$$

Листа је прилично дугачка и садржи 336 чињеница. Ситуацију можемо поправити, и листу знатно скратити ако опишемо неке опште чињенице о кретању скакача. На пример, следеће свойство симетричности, скраћује горњу листу на пола:

(σ_1) $\forall x_1\forall x_2\forall x_3\forall x_4(S(x_1,x_2,x_3,x_4)\Rightarrow S(x_3,x_4,x_1,x_2))$.

Уз додатне опште услове, може се изоставити још више појединачних чињеница листе $(*)$.

(σ_2) $\forall x_1\forall x_2\forall x_3\forall x_4(S(x_1,x_2,x_3,x_4)\Rightarrow S(x_1,x_4,x_3,x_2))$

(σ_3) $\forall x_1\forall x_2\forall x_3\forall x_4(S(x_1,x_2,x_3,x_4)\Rightarrow S(x_2,x_1,x_4,x_3))$

(σ_4) $\forall x_1\forall x_2\forall x_3\forall x_4(S(x_1,x_2,x_3,x_4)\Rightarrow S(x_3,x_2,x_1,x_4))$

Интуитивно је јасно да из $S(4,3,5,1)$,

- на основу (σ_1) закључујемо $S(4,1,5,3)$;
- на основу (σ_2) закључујемо $S(5,1,4,3)$;
- на основу (σ_3) закључујемо $S(3,4,1,5)$;
- на основу (σ_4) закључујемо $S(5,3,4,1)$.

Пример 28. Нека универзум чине бројеви: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Бинарни предикат '... мањи од ...' означавамо $<$, и користимо тзв. *инфиксну* нотацију: пишемо $x < y$ уместо $<(x,y)$.

Уместо навођења истинитости сваког од 100 исказа, приказаних у табели десно, довољно је навести следећих девет конкретних веза

$$(*)\quad 0<1,\ 1<2,\ 2<3,\ 3<4,\ 4<5,\ 5<6,\ 6<7,\ 7<8,\ 8<9.$$

и неколико општих особина:

(O_1) $\forall x \neg x < x$

(O_2) $\forall x \forall y (x < y \Rightarrow \neg\, y < x)$

(O_3) $\forall x \forall y \forall z (x < y \wedge y < z \Rightarrow x < z)$

Ослањајући се на 'здраворазумску логику', једноставно уочавамо да се из списка $(*)$ и особина (O_1), (O_2), (O_3) може закључити, на пример: $3 < 8$; $\neg\, 5 < 2$; $\neg\, 7 < 7$ итд.

$<$	0	1	2	3	4	5	6	7	8	9
0	0	1	1	1	1	1	1	1	1	1
1	0	0	1	1	1	1	1	1	1	1
2	0	0	0	1	1	1	1	1	1	1
3	0	0	0	0	1	1	1	1	1	1
4	0	0	0	0	0	1	1	1	1	1
5	0	0	0	0	0	0	1	1	1	1
6	0	0	0	0	0	0	0	1	1	1
7	0	0	0	0	0	0	0	0	1	1
8	0	0	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0

3.2. **Правила дедукције за квантификаторе**

9

Поред правила дедукције за исказну логику, која примењујемо и на предикатске формуле, користимо и правила за квантификаторе.

Важно место у правилима дедукције која се односе на квантификаторе заузима тзв. *супституција* слободних променљивих симболима константи или неким другим променљивама.

Ако је α нека формула, x променљива и c симбол константе, онда са $\alpha[x/c]$ означавамо формулу добијену заменом свих слободних појављивања променљиве x симболом константом c. Наравно, ако x није слободно у α, онда је формула $\alpha[x/c]$ истоветна формули α.

Приликом замене слободне променљиве неком другом променљивом морамо бити обазривији. Наиме, када у α свако слободно појављивање променљиве x замењујемо променљивом y, ниједно појављивање променљиве y након замене x са y, не сме да постане везано. У наредном примеру, илуструјемо разлоге овог ограничења.

Пример 29. Ако се ослонимо на интерпретацију из примера 20, онда се формула

$$\alpha(y):\ \forall x\, V(x,y) \text{ – свака особа воли особу } y$$

битно не разликује од формуле

$$\alpha(y)[y/z]:\ \forall x\, V(x,z) \text{ – свака особа воли особу } z;$$

у оба случаја истинитост добијених формула зависи од вредности које доделимо промењливој y, одн. z. Исто важи ако y заменимо било којом другом променљивом, **осим** променљивом x, јер би то изазвало драстичну промену значења:

$$\alpha(y)[y/x]:\ \forall x\, V(x,x) \text{ – свака особа воли себе.}$$

Нема много разлике да ли квадратну функцију опишемо једнакошћу $f(y) = y^2$ или $f(z) = z^2$.

Важно. Кажемо да је променљива x слободна за y у формули α ако ниједно појављивање променљиве y настало заменом x са y не постаје везано, а са $\alpha[x/y]$ означавамо формулу добијену након описане замене. У наставку, када год напишемо $\alpha[x/y]$ подразумеваћемо да је променљива x слободна за y у формули α. Када је јасно да је у формули α променљива x замењена променљивом y, уместо $\alpha[x/y]$ краће пишемо $\alpha(y)$.

Приметимо да је x увек слободно за x и да је формула $\alpha[x/x]$ истоветна формули α. Приметимо и да уколико се променљива x не појављује слободно у формули α, тада је формула $\alpha[x/y]$ идентична формули α.

Правила $\forall x_{\mathrm{E}}$ и $\exists x_{\mathrm{U}}$

Пре него што наведемо наслovљена правила, мотивисаћемо их неким интуитивним аргументима. Нека је P унарни предикатски симбол. Ако замислимо да су низом $c_1, c_2, c_3, \ldots$ набројани сви објекти универзума, тада формула $\forall x P(x)$ 'тврди':

$$P(c_1) \wedge P(c_2) \wedge P(c_3) \wedge \cdots, \tag{1}$$

а $\exists x P(x)$ 'тврди':

$$P(c_1) \vee P(c_2) \vee P(c_3) \vee \cdots . \tag{2}$$

Ова запажања нас наводе да правила дедукције о квантификаторима повежемо са одговарајућим правилима за конјункцију и дисјункцију.

Правило '$(\wedge_{\mathrm{E}})$'

$$\frac{P(c_1) \wedge P(c_2) \wedge P(c_3) \wedge \cdots}{P(c_i)}\ (\wedge_{\mathrm{E}})$$

тесно је повезано са следећим размишљањем: ако је тачно $\forall x \alpha$, тада ће бити тачна и формула добијена када се у α променљива x замени било којим објектом.

$$\frac{\forall x \alpha}{\alpha[x/v]}\ (\forall_{\mathrm{E}})$$

Из $\forall x \alpha$ закључујемо $\alpha[x/v]$, при чему је v симбол константе или променљива за коју је x слободно у α.

Будући да на располагању имамо неграничено много променљивих, за сваку формулу α можемо пронаћи променљиву v тако да након замене x са v у α, ниједно појављивање променљиве v не постаје везано.

Пример 30.

$$\forall x(\texttt{Човек}(x) \Rightarrow \texttt{Смртан}(x)), \texttt{Човек}(\texttt{Сократ}) \vdash \texttt{Смртан}(\texttt{Сократ})$$

1.	$\forall x(\texttt{Човек}(x) \Rightarrow \texttt{Смртан}(x))$	претпоставка
2.	$\texttt{Човек}(\texttt{Сократ})$	претпоставка
3.	$\texttt{Човек}(\texttt{Сократ}) \Rightarrow \texttt{Смртан}(\texttt{Сократ})$	$\forall x_{\mathrm{E}}$, 1 $[x/\texttt{Сократ}]$
4.	$\texttt{Смртан}(\texttt{Сократ})$	$\Rightarrow_{\mathrm{E}}$, 3, 2

Правило '$(\vee_{\mathrm{U}})$'

$$\frac{R(c_i)}{R(c_1) \vee R(c_2) \vee R(c_3) \vee \cdots}\ (\vee_{\mathrm{U}})$$

тесно је повезано са следећим размишљањем: ако је тачно $\alpha[x/v]$ за неки објекат v, онда је тачна и формула $\exists x \alpha$.

$$\frac{\alpha[x/v]}{\exists x \alpha}\ (\exists_{\mathrm{U}})$$

Из $\alpha[x/v]$, за неки симбол константе или променљиву v, закључујемо $\exists x \alpha$.

Пример 31.

$$\forall x(\texttt{Човек}(x) \Rightarrow \texttt{Смртан}(x)), \texttt{Човек}(\texttt{Сократ}) \vdash \exists x \texttt{Смртан}(x)$$

1.	$\forall x(\texttt{Човек}(x) \Rightarrow \texttt{Смртан}(x))$	претпоставка
2.	$\texttt{Човек}(\texttt{Сократ})$	претпоставка
3.	$\texttt{Човек}(\texttt{Сократ}) \Rightarrow \texttt{Смртан}(\texttt{Сократ})$	$\forall x_{\mathrm{E}}$, 1 $[x/\texttt{Сократ}]$
4.	$\texttt{Смртан}(\texttt{Сократ})$	$\Rightarrow_{\mathrm{E}}$, 3, 2
5.	$\exists x \texttt{Смртан}(x)$	$\exists x_{\mathrm{U}}$, 4

Правила $\forall x_{\mathrm{U}}$ и $\exists x_{\mathrm{E}}$

Увођење универзалног и елиминација егзистенцијалног квантификатора су донекле компликованија правила.

Неформално, када треба да докажемо тврдњу облика $\forall x\alpha$, доказ започињемо речима 'нека је x произвољан објекат ...', при чему водимо рачуна да је једино што знамо о x-у то да припада одговарајућем универзуму; уколико се деси да је ознака x већ резервисана, онда узимамо неку другу, **свежу** променљиву v и кажемо 'нека је v произвољан објекат ...' Слично томе, када знамо да је тачно $\exists x\alpha$, онда ћемо одговарајући елемент означити неким 'свежим' словом које није већ резервисано.

У оба правила се појављују поддокази снабдевени тзв. *свежом променљивом* која се у формулама ван поддоказа не појављује слободно.

$$\dfrac{\begin{array}{|l} v \\ \vdots \\ \alpha[x/v] \end{array}}{\forall x\alpha}\ (\forall x_{\mathrm{U}})$$

Ако се коришћењем *свеже* променљиве може доказати $\alpha[x/v]$, онда се може закључити $\forall x\alpha$.

Кључна чињеница за претходно правило јесте да је v свежа променљива, тј. да се не појављује нигде ван одговарајућег поддоказа, па пошто ништа не претпостављамо о v, сваки објекат ће 'проћи' на његовом месту. Следећа шема илуструје употребу правила $(\forall x_{\mathrm{U}})$.

$\vdots$			Када желимо да докажемо $\forall x\alpha$,
$j.$	v		уводимо свежу променљиву v мислећи на 'нека је v произвољан објекат универзума'.
$\vdots$	$\vdots$		Из свега осталог настојимо да докажемо $\alpha[x/v]$.
$k.$	$\alpha[x/v]$		Када успемо,
$k+1.$	$\forall x\alpha$	$(\forall x_{\mathrm{U}})$, j-k	изводимо жељени закључак.

Пример 32. Докажимо секвент
$\forall x(A(x) \Rightarrow B(x)), \forall x(B(x) \Rightarrow C(x)) \vdash \forall x(A(x) \Rightarrow C(x))$.

1.	$\forall x(A(x) \Rightarrow B(x))$	претпоставка
2.	$\forall x(B(x) \Rightarrow C(x))$	претпоставка
3.	v	уводимо свежу променљиву
4.	$A(v) \Rightarrow B(v)$	$\forall x_{\mathrm{E}}$, 1
5.	$B(v) \Rightarrow C(v)$	$\forall x_{\mathrm{E}}$, 2
6.	$A(v) \Rightarrow C(v)$	транзитивност импликације, 4, 5
7.	$\forall x(A(x) \Rightarrow C(x))$	$\forall x_{\mathrm{U}}$, 3-6

Задатак **1.** Доказати секвенте:
(1) $\vdash \forall x(A(x) \Rightarrow A(x))$
(2) $\forall x(A(x) \Rightarrow B(x)), \forall x(B(x) \Rightarrow A(x)) \vdash \forall x(A(x) \Leftrightarrow B(x))$
(3) $\vdash \forall x(A(x) \Leftrightarrow A(x))$
(4) $\forall x(A(x) \Leftrightarrow B(x)) \vdash \forall x(B(x) \Leftrightarrow A(x))$
(5) $\forall x(A(x) \Leftrightarrow B(x)), \forall x(B(x) \Leftrightarrow C(x)) \vdash \forall x(A(x) \Leftrightarrow C(x))$

Пример 33. Докажимо секвент $\forall x \neg P(x) \vdash \forall x(P(x) \Rightarrow Q(x))$.

1.	$\forall x \neg P(x)$	претпоставка
2.	$\quad v$	уводимо свежу променљиву
3.	$\quad\quad P(v)$	додатна претпоставка
4.	$\quad\quad \neg P(v)$	$\forall x_{\mathrm{E}}$, 1
5.	$\quad\quad \bot$	$\neg_{\mathrm{E}}$, 3, 4
6.	$\quad\quad Q(v)$	$\bot_{\mathrm{E}}$, 5
7.	$\quad P(v) \Rightarrow Q(v)$	$\Rightarrow_{\mathrm{U}}$, 3-6
8.	$\forall x(P(x) \Rightarrow Q(x))$	$\forall x_{\mathrm{U}}$, 2-7

Задатак **2.** Доказати $\forall x \neg P(x), \forall x \neg Q(x) \vdash \forall x(P(x) \Leftrightarrow Q(x))$.

Уведимо најзад правило $(\exists x_{\mathrm{E}})$. Грубо речено: ако знамо да је $\exists x\alpha$ тачно, онда је α тачно за бар једну 'вредност' x, па би требало обавити закључивање по случајевима за све могуће вредности, што постижемо користећи свежу променљиву v као 'генеричку' вредност која репрезентује све могуће вредности.

$$\dfrac{\exists x\alpha \qquad \begin{array}{|l} v \quad \alpha[x/v] \\ \vdots \\ \gamma \end{array}}{\gamma}\ (\exists x_{\mathrm{E}})$$

Ако из $\alpha[x/v]$ докажемо формулу γ у којој се не појављује v, онда γ мора бити тачно без обзира на 'вредност' v. И овога пута, од суштинске важности је да се v не појављује слободно нигде ван одговарајућег поддоказа, па самим тим ни у γ.

Следећа шема илуструје коришћење правила $(\exists x_{\mathrm{E}})$.

$\vdots$			
$i.$	$\exists x\alpha$		
$\vdots$			Када желимо да искористимо $\exists x\alpha$,
$j.$	$\quad v \;\; \alpha[x/v]$	дод. прет.	уводимо ознаку v за објекат који задовољава α.
$\vdots$	$\quad\quad \vdots$		Из $\alpha[x/v]$ и свега осталог настојимо да докажемо γ у коме се v не појављује слободно.
$k.$	$\quad\quad \gamma$		Када успемо,
$k+1.$	γ	$(\exists x_{\mathrm{E}})$, i, j-k	изводимо жељени закључак.

Пример 34. Докажимо секвент:

$$\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y,x))), M(\texttt{Миле}) \vdash \exists z V(\texttt{Миле}, z)$$

Неформално

Да бисмо што јасније образложили наведени секвент, ослонићемо се на интерпретацију наведену у примеру 20. Из претпоставке да постоји девојка коју воли сваки момак и претпоставке да је Миле момак, јасно је да постоји девојка коју Миле воли, јер то потврђује управо девојка коју сви воле, па и Миле.

Формално

1.	$\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y,x)))$	претпоставка
2.	$M(\texttt{Миле})$	претпоставка
3.	$c \quad D(c) \wedge \forall y(M(y) \Rightarrow V(y,c))$	додатна претпоставка
4.	$\forall y(M(y) \Rightarrow V(y,c))$	$\wedge_{\mathrm{E}}^{\mathrm{D}}$, 3
5.	$M(\texttt{Миле}) \Rightarrow V(\texttt{Миле},c)$	$\forall x_{\mathrm{E}}$, 4
6.	$V(\texttt{Миле},c)$	$\Rightarrow_{\mathrm{E}}$, 5, 2
7.	$\exists z V(\texttt{Миле},z)$	$\exists z_{\mathrm{U}}$, 6
8.	$\exists z V(\texttt{Миле},z)$	$\exists x_{\mathrm{E}}$, 1, 3-7

Пример 35. Нека је B бинарни предикатски симбол. Докажимо секвент $\forall x B(x,x) \vdash \forall x \exists y B(x,y)$.

1.	$\forall x B(x,x)$	претпоставка
2.	v	уводимо свежу променљиву
3.	$B(v,v)$	$\forall x_{\mathrm{E}}$, 1
4.	$\exists y B(v,y)$	$\exists y_{\mathrm{U}}$, 3 ($B(v,v)$ је истоветна формули $B(v,y)[y/v]$)
5.	$\forall x \exists y B(x,y)$	$\forall x_{\mathrm{U}}$, 2-4

У наредна два примера посебну пажњу посвећујемо неформалним доказима. У математици је уобичајено да се докази наводе у неформалном облику, што ћемо и ми чинити у наредним поглављима. Наравно, у неформалним доказима углавном не наводимо правила дедукције која користимо, али их свакако имамо на уму, јер на основу њих и састављамо неформални доказ.

Пример 36. Нека универзум чине све тачке неке равни. Да бисмо описали распоред међу тачкама користићемо тернарни (дужине три) предикатски симбол O: $O(x,y,z)$ значи 'тачка y је између тачака x и z'. Доказати да из 'очигледне истине'
$\forall x \forall y \forall z(O(x,y,z) \Rightarrow O(z,y,x) \wedge \neg O(y,z,x))$
(Ако је y између x и z, онда је y између z и x и није z између y и x.)
следи $\forall x \forall y \forall z(O(x,y,z) \Rightarrow \neg O(z,x,y))$.
Неформално

Претпоставимо да је $\forall x \forall y \forall z(O(x,y,z) \Rightarrow O(z,y,x) \wedge \neg O(y,z,x)) \cdots (*)$
.

Нека су a, b, c произвољне тачке.
Да бисмо доказали импликацију $O(a,b,c) \Rightarrow \neg O(c,a,b)$,
претпоставимо да је $O(a,b,c)$. (Треба доказати $\neg O(c,a,b)$.)
Претпоставимо (супротно), да је $O(c,a,b)$.
Из $(*)$ и $O(c,a,b)$ следи $O(b,a,c)$ и $\neg O(a,b,c)$
(На $(*)$ смо применили $[x/c],[y/b],[z/a]$.)
$O(a,b,c)$ и $\neg O(a,b,c)$ дају контрадикцију.
Дакле, $\neg O(c,a,b)$.
Дакле, $O(a,b,c) \Rightarrow \neg O(c,a,b)$.
Дакле, $\forall x \forall y \forall z(O(x,y,z) \Rightarrow \neg O(z,x,y))$.
Формално

1.	$\forall x\forall y\forall z(O(x,y,z) \Rightarrow O(z,y,x) \wedge \neg O(y,z,x))$	претпоставка
2.	a, b, c	
3.	$O(a,b,c)$	додатна претпоставка
4.	$O(c,a,b)$	додатна претпоставка
5.	$O(c,a,b) \Rightarrow O(b,a,c) \wedge \neg O(a,b,c)$	$\forall xyz_{\mathrm{E}}$, 1
6.	$O(b,a,c) \wedge \neg O(a,b,c)$	$\Rightarrow_{\mathrm{E}}$, 5, 4
7.	$\neg O(a,b,c)$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 6
8.	$\bot$	$\neg_{\mathrm{E}}$, 3, 7
9.	$\neg O(c,a,b)$	$\neg_{\mathrm{U}}$, 4-8
10.	$O(a,b,c) \Rightarrow \neg O(c,a,b)$	$\Rightarrow_{\mathrm{U}}$, 3-9
11.	$\forall x\forall y\forall z(O(x,y,z) \Rightarrow \neg O(z,x,y))$	$(\forall xyz_{\mathrm{U}})$, 2-10

Формула α је **теорема предикатске логике** ако је доказив секвент $\vdash \alpha$. Наводимо неколико важних теорема предикатске логике.

Два суседна квантификатора исте врсте могу заменити места
$\vdash \forall x\forall y\alpha \Leftrightarrow \forall y\forall x\alpha$ $\quad$ $\vdash \exists x\exists y\alpha \Leftrightarrow \exists y\exists x\alpha$

$\vdash \exists x\forall y\alpha \Rightarrow \forall y\exists x\alpha$

Де Морганови закони за квантификаторе
$\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha$ $\quad$ $\vdash \neg\forall x\alpha \Leftrightarrow \exists x\neg\alpha$

'$\forall$ пролази кроз $\wedge$, а $\exists$ кроз $\vee$'
$\vdash \forall x(\alpha \wedge \beta) \Leftrightarrow \forall x\alpha \wedge \forall x\beta$ $\quad$ $\vdash \exists x(\alpha \vee \beta) \Leftrightarrow \exists x\alpha \vee \exists x\beta$

$\vdash \forall x\alpha \vee \forall x\beta \Rightarrow \forall x(\alpha \vee \beta)$ $\quad$ $\vdash \exists x(\alpha \wedge \beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$

Ако x нема слободно појављивање у β!
$\vdash \forall x(\alpha \vee \beta) \Leftrightarrow \forall x\alpha \vee \beta$ $\quad$ $\vdash \exists x(\alpha \wedge \beta) \Leftrightarrow \exists x\alpha \wedge \beta$

Докажимо Де Морганов закон $\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha$. Наводимо само доказе секвената $\neg\exists x\alpha \vdash \forall x\neg\alpha$ и $\forall x\neg\alpha \vdash \neg\exists x\alpha$.

Де Морганови закон $\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha$

1.	$\neg\exists x\alpha$	претпоставка
2.	v	
3.	$\alpha[x/v]$	додатна прет.
4.	$\exists x\alpha$	$\exists x_{\mathrm{U}}$, 3
5.	$\bot$	$\neg_{\mathrm{E}}$, 4, 1
6.	$\neg\alpha[x/v]$	$\neg_{\mathrm{U}}$, 3-5
7.	$\forall x\neg\alpha$	$\forall x_{\mathrm{U}}$, 2-6

1.	$\forall x\neg\alpha$	претпоставка
2.	$\exists x\alpha$	додатна прет.
3.	$v\ \alpha[x/v]$	додатна прет.
4.	$\neg\alpha[x/v]$	$\forall x_{\mathrm{E}}$, 1
5.	$\bot$	$\neg_{\mathrm{E}}$, 4, 3
6.	$\bot$	$\exists x_{\mathrm{E}}$, 2, 3-5
7.	$\neg\exists x\alpha$	$\neg_{\mathrm{U}}$, 2-6

Задатак **3.** Доказати секвенте:
(а) $\vdash \forall x\forall y\alpha \Leftrightarrow \forall y\forall x\alpha$
(б) $\vdash \exists x\exists y\alpha \Leftrightarrow \exists y\exists x\alpha$
(в) $\vdash \exists x\forall y\alpha \Rightarrow \forall y\exists x\alpha$

Де Морганов закон $\vdash \neg\forall x\alpha \Leftrightarrow \exists x\neg\alpha$ једноставно изводимо из

претходног. Доказ наводимо у облику еквиваленцијског ланца:

$$\neg\forall x\alpha \Leftrightarrow \neg\forall x\neg\neg\alpha \Leftrightarrow \neg\neg\exists x\neg\alpha \Leftrightarrow \exists x\neg\alpha$$

Задатак **4.** У облику еквиваленцијског ланца навести доказе секвената $\vdash \exists x\alpha \Leftrightarrow \neg\forall x\neg\alpha$ и $\vdash \forall x\alpha \Leftrightarrow \neg\exists x\neg\alpha$.

Да бисмо доказали да '$\forall$ пролази кроз $\wedge$' доказаћемо секвенте $\forall x(\alpha\wedge\beta)\vdash\forall x\alpha\wedge\forall x\beta$ и $\forall x\alpha\wedge\forall x\beta\vdash\forall x(\alpha\wedge\beta)$.

Доказ за $\forall x(\alpha\wedge\beta)\vdash\forall x\alpha\wedge\forall x\beta$

1.	$\forall x(\alpha\wedge\beta)$	претпоставка
2	x	Докажимо најпре $\forall x\alpha$.
3.	$\alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
4.	α	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 3
5.	$\forall x\alpha$	$\forall x_{\mathrm{U}}$, 2-4
6.	x	Докажимо даље $\forall x\beta$.
7.	$\alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
8.	β	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 7
9.	$\forall x\beta$	$\forall x_{\mathrm{U}}$, 6-8
10.	$\forall x\alpha\wedge\forall x\beta$	$\wedge_{\mathrm{U}}$, 5, 9

Доказ за $\forall x\alpha\wedge\forall x\beta\vdash\forall x(\alpha\wedge\beta)$

1.	$\forall x\alpha\wedge\forall x\beta$	претпоставка
2.	$\forall x\alpha$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1
3.	$\forall x\beta$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 1
4.	x	
5.	α	$\forall x_{\mathrm{E}}$, 2
6.	β	$\forall x_{\mathrm{E}}$, 3
7.	$\alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 5, 6
8.	$\forall x(\alpha\wedge\beta)$	$\forall x_{\mathrm{U}}$, 4-7

Доказ да '$\exists$ пролази кроз $\vee$' наводимо у облику еквиваленцијског ланца.

$$\begin{aligned}
\exists x(\alpha\vee\beta) &\Leftrightarrow \neg\neg\exists x(\alpha\vee\beta)\\
&\Leftrightarrow \neg\forall x\neg(\alpha\vee\beta)\\
&\Leftrightarrow \neg\forall x(\neg\alpha\wedge\neg\beta)\\
&\Leftrightarrow \neg(\forall x\neg\alpha\wedge\forall x\neg\beta)\\
&\Leftrightarrow \neg\forall x\neg\alpha\vee\neg\forall x\neg\beta\\
&\Leftrightarrow \exists x\neg\neg\alpha\vee\exists x\neg\neg\beta\\
&\Leftrightarrow \exists x\alpha\vee\exists x\beta
\end{aligned}$$

Под претпоставком да x нема слободно појављивање у β, доказаћемо $\exists x(\alpha\wedge\beta)\vdash\exists x\alpha\wedge\beta$ и $\exists x\alpha\wedge\beta\vdash\exists x(\alpha\wedge\beta)$.

Доказ за $\exists x(\alpha\wedge\beta)\vdash\exists x\alpha\wedge\beta$, када x није слободно у β.

1.	$\exists x(\alpha\wedge\beta)$	претпоставка
2	$v\ \ \alpha[x/v]\wedge\beta$	додатна прет. ($\beta[x/v]$ је истоветно формули β)
3.	$\alpha[x/v]$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 2
4.	β	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	$\exists x\alpha$	$\exists x_{\mathrm{U}}$, 3
6.	$\exists x\alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 5, 4
7.	$\exists x\alpha\wedge\beta$	$\exists x_{\mathrm{E}}$, 1, 2-6

Доказ за $\exists x\alpha\wedge\beta\vdash\exists x(\alpha\wedge\beta)$, када x није слободно у β.

1.	$\exists x\alpha\wedge\beta$	претпоставка
2.	$\exists x\alpha$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1
3.	β	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 1
4	$v\ \ \alpha[x/v]$	додатна прет.
5.	$\alpha[x/v]\wedge\beta$	$\wedge_{\mathrm{U}}$, 4, 3
6.	$\exists x(\alpha\wedge\beta)$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 5 ($\beta[x/v]$ је истоветно формули β)
7.	$\exists x(\alpha\wedge\beta)$	$\exists x_{\mathrm{E}}$, 2, 4-6

Задатак **5.** У облику еквиваленцијског ланца навести доказе секвената:
(1) $\vdash \forall x(\alpha \Rightarrow \beta) \Leftrightarrow (\exists x\alpha \Rightarrow \beta)$, под претпоставком да се x не појављује слободно у формули β.
(2) $\vdash \forall x(\alpha \Rightarrow \beta) \Leftrightarrow (\alpha \Rightarrow \forall x\beta)$, под претпоставком да се x не појављује слободно у формули α.

4. ZF теорија скупова

Појам скупа је један од најважнијих појмова савремене математике. Правила грађења скупова и основна својства прецизирамо аксиомама замишљеног универзума чије објекте називамо *скупови*. Велике заслуге у развоју тих аксиома имали су Цермело[56] и Френкел[57], па се списак аксиома који у наставку излажемо зове и *Цермело-Френкелова теорија скупова* и означава **ZF**.

[56] Ернест Цермело (1871-1953) (Ernst Zermelo)

[57] Абрахам Френкел (1891-1965) (Abraham Fraenkel)

Универзум скупова описујемо користећи два бинарна предиката $\in$ (припадање) и $=$ (једнакост). Променљиве ћемо означавати малим и великим словима латинице са или без индекса. Уместо $\in(\cdot,\cdot)$ и $=(\cdot,\cdot)$ користићемо тзв. инфиксну нотацију $\cdot\in\cdot$ и $\cdot=\cdot$. За негације атомских формула користимо краће ознаке: уместо $\neg x\in y$ и $\neg x=y$ редом пишемо $x\notin y$ и $x\neq y$.

Основна, унапред претпостављена, својства универзума називамо *аксиомама теорије скупова*. Све дедуктивне последице које изводимо из аксиома називамо *теоремама теорије скупова*. При доказивању теорема користимо правила дедукције и примењујемо их на аксиоме и теореме које смо већ доказали. Иако су аксиоме и теореме заправо формуле изабраног предикатског језика, ми ћемо их формулисати и на говорном (српском) језику, јер то значајно олакшава разумевање онога што се њима тврди. Ипак, формулације ће пратити и одговарајуће формуле, осим у случајевима када су оне веома компликоване и тешко читљиве. Доказе теорема углавном ћемо наводити у неформалном облику, при чему ћемо за оне једноставније (у првим одељцима ове главе) наводити и формалне варијанте.

4.1. Пет аксиома (екстензионалности, празног скупа, пара, уније и партитивног скупа) и једна схема аксиома (издвајања)

10

▼ Аксиома екстензионалности. Инклузија.

Прва аксиома коју наводимо описује везу између $\in$ и $=$.

Аксиома екстензионалности
Два скупа су једнака акко и само ако имају исте елементе.

$$\forall a \forall b(a = b \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in b))$$

Најпре доказујемо неке очекиване особине једнакости.

Теорема 11. *(1) За сваки скуп a важи $a = a$.*
(2) За све скупове a и b, из $a = b$ следи $b = a$.
(3) За све скупове a, b, c, из $a = b$ и $b = c$ следи $a = c$.

Доказ. (1) Нека је a произвољан скуп. Једноставно се може доказати формула $\forall x(x \in a \Leftrightarrow x \in a)$ (видети поддоказ 5-9 доказа наведеног у наредној напомени), из које према аксиоми екстензионалности добијамо $a = a$.

Наведени доказ је неформална варијанта формалног доказа секвента $\forall a \forall b(a = b \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in b)) \vdash \forall a\,(a = a)$:

1.	$\forall a \forall b(a = b \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in b))$	аксиома екстензионалности (Ax1)
2.	a	(Желимо да докажемо $\forall a(a = a)$.)
3.	$a = a \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in a)$	$\forall a_{\mathrm{E}} \forall b_{\mathrm{E}}$, 1
4.	$\forall x(x \in a \Leftrightarrow x \in a) \Rightarrow a = a$	$\Leftrightarrow_{\mathrm{E}}^{\mathrm{DL}}$, 3
5.	x	(Желимо да докажемо $\forall x(x \in a \Leftrightarrow x \in a)$.)
6.	$x \in a$	
7.	$x \in a \Rightarrow x \in a$	$\Rightarrow_{\mathrm{U}}$, 6
8.	$x \in a \Leftrightarrow x \in a$	$\Leftrightarrow_{\mathrm{U}}$, 7
9.	$\forall x(x \in a \Leftrightarrow x \in a)$	$\forall x_{\mathrm{U}}$, 5-8
10.	$a = a$	$\Rightarrow_{\mathrm{E}}$, 4, 9
11.	$\forall a(a = a)$	$\forall a_{\mathrm{U}}$, 2, 10

(2) Нека су a и b произвољни скупови. Из $a = b$, према аксиоми екстензионалности следи $\forall x(x \in a \Leftrightarrow x \in b)$, одакле се једноставно може извести $\forall x(x \in b \Leftrightarrow x \in a)$. Из последње формуле, према наведеној аксиоми, добијамо $b = a$.

(3) Нека су a, b и c произвољни скупови. Претпоставимо да важи $a = b$ и $b = c$. Према аксиоми екстензионалности имамо $\forall x(x \in a \Leftrightarrow x \in b)$ и $\forall x(x \in b \Leftrightarrow x \in c)$, одакле изводимо $\forall x(x \in a \Leftrightarrow x \in c)$. Најзад, из последње формуле, применом аксиоме екстензионалности, добијамо $a = c$. □

Напомена 1. Формални докази секвената који се помињу у доказима тврдњи (2) и (3) претходне леме:
(2) $\forall x(x \in a \Leftrightarrow x \in b) \vdash \forall x(x \in b \Leftrightarrow x \in a)$
(3) $\forall x(x \in a \Leftrightarrow x \in b), \forall x(x \in b \Leftrightarrow x \in c) \vdash \forall x(x \in a \Leftrightarrow x \in c)$
потпуно су аналогни доказима секвената из задатка 1.1 под (4) и (5).

Неформално, уколико су сви елементи скупа a уједно и елементи скупа b, кажемо да је a *подскуп* од b, одн. b је *надскуп* од a, и пишемо $a \subseteq b$, одн. $b \supseteq a$. Однос међу скуповима означен симболом $\subseteq$ назива се *инклузија*. Такође, кажемо да је a *строги подскуп* од b (b је *строги надскуп* од a) ако је $a \subseteq b$ ($b \supseteq a$) и $a \neq b$, и пишемо $a \subset b$ ($b \supset a$). Прецизније:

- формула $a \subseteq b$ (као и формула $b \supseteq a$) је скраћени запис формуле $\forall x(x \in a \Rightarrow x \in b)$;
- формула $a \subset b$ је скраћени запис формуле $a \subseteq b \wedge a \neq b$.

Теорема 12. *(1) За сваки скуп a важи $a \subseteq a$.*
(2) За све скупове a и b, из $a \subseteq b$ и $b \subseteq a$ следи $a = b$.
(3) За све скупове a, b, c, из $a \subseteq b$ и $b \subseteq c$ следи $a \subseteq c$.

Доказ. Следеће секвенте није тешко доказати (докази су потпуно аналогни доказима секвената из примера **1**.32 и задатка **1**.1 под (1) и (2)):
(1) $\forall x(x \in a \Rightarrow x \in a)$
(2) $\forall x(x \in a \Rightarrow x \in b), \forall x(x \in b \Rightarrow x \in a) \vdash \forall x(x \in a \Leftrightarrow x \in b)$
(3) $\forall x(x \in a \Rightarrow x \in b), \forall x(x \in b \Rightarrow x \in c) \vdash \forall x(x \in a \Rightarrow x \in c)$
одакле непосредно (уз примену аксиоме екстензионалности за тврђење (2)) следе тврђења наведена у леми. □

▼ Аксиома празног скупа

Аксиома празног скупа
Постоји скуп који нема елемената.
$\exists y \forall x(x \notin y)$

Скуп чије постојање тврди аксиома празног скупа мора, према аксиоми екстензионалности, бити јединствен. Заиста, означимо са y_1 и y_2 скупове за које важи

$$\forall x(\neg x \in y_1) \text{ и } \forall x(\neg x \in y_2).$$

Из ове две формуле једноставно изводимо $\forall x(x \in y_1 \Leftrightarrow x \in y_2)$, одакле, користећи аксиому екстензионалности, закључујемо да је $y_1 = y_2$.

Напомена 2. Формални доказ секвента

$$\forall x(\neg x \in y_1), \forall x(\neg x \in y_2) \vdash \forall x(x \in y_1 \Leftrightarrow x \in y_2).$$

наведен је на маргини и потпуно је аналоган извођењу секвента из задатка **1**.2.

1.	$\forall x(\neg x \in y_1)$	
2.	$\forall x(\neg x \in y_2)$	
3.	$\quad x$	
4.	$\quad x \in y_1$	
5.	$\quad \neg x \in y_1$	$\forall x_{\mathrm{E}}$, 1
6.	$\quad \bot$	$\neg_{\mathrm{E}}$, 4, 5
7.	$\quad x \in y_2$	$\bot_{\mathrm{E}}$, 6
8.	$x \in y_1 \Rightarrow x \in y_2$	$\Rightarrow_{\mathrm{U}}$, 4-7
9.	$\quad x \in y_2$	
10.	$\quad \neg x \in y_2$	$\forall x_{\mathrm{E}}$, 2
11.	$\quad \bot$	$\neg_{\mathrm{E}}$, 9, 10
12.	$\quad x \in y_1$	$\bot_{\mathrm{E}}$, 11
13.	$x \in y_2 \Rightarrow x \in y_1$	$\Rightarrow_{\mathrm{U}}$, 9-12
14.	$x \in y_1 \Leftrightarrow x \in y_2$	$\Leftrightarrow_{\mathrm{U}}$, 8, 13
15.	$\forall x(x \in y_1 \Leftrightarrow x \in y_2)$	$\forall x_{\mathrm{U}}$, 3-14

Јединствени скуп који нема елемената означавамо $\emptyset$ и називамо **празан скуп**. Дакле, $\forall x\,(x \notin \emptyset)$. У наставку, ознаку $\emptyset$ користимо као симбол *константе* универзума скупова.

Постојање и јединственост празног скупа тврди следећа формула, која је, као што смо показали последица уведених аксиома:

$$\exists y \underbrace{\forall x(x \notin y)}_{\varphi(y)} \wedge \forall y_1 \forall y_2 (\underbrace{\forall x(x \notin y_1)}_{\varphi[y/y_1]} \wedge \underbrace{\forall x(x \notin y_2)}_{\varphi[y/y_2]} \Rightarrow y_1 = y_2).$$

Уопште, формуле облика

$$(*) \qquad \exists y \varphi(y) \wedge \forall y_1 \forall y_2 (\varphi[y/y_1] \wedge \varphi[y/y_2] \Rightarrow y_1 = y_2),$$

које краће означавамо $\exists! y \varphi(y)$, тврде да постоји јединствени објекат y који задовољава извесну формулу φ.

Теорема 13. *За сваки скуп a важи $\emptyset \subseteq a$.*

Доказ. Треба доказати формулу $\forall x(x \in \emptyset \Rightarrow x \in a)$.

1.	$\forall x(\neg x \in \emptyset)$	
2.	$\quad x$	
3.	$\quad x \in \emptyset$	
4.	$\quad \neg x \in \emptyset$	$\forall x_{\mathrm{E}}$, 1
5.	$\quad \bot$	$\neg_{\mathrm{E}}$, 3, 4
6.	$\quad x \in a$	$\bot_{\mathrm{E}}$, 5
7.	$x \in \emptyset \Rightarrow x \in a$	$\Rightarrow_{\mathrm{U}}$, 3-6
8.	$\forall x(x \in \emptyset \Rightarrow x \in a)$	$\forall x_{\mathrm{U}}$, 2-7

□

▼ 'Неприхватљива аксиома'. Раселов парадокс

Почетке проучавања теорије скупова често је пратило наивно прихватање појединих аксиома (полазних претпоставки), које су изгледале 'интуитивно јасне', али се касније испостављало да доводе до противречности. Најпознатија 'наивна аксиома' јесте: за свако својство постоји скуп који садржи само оне објекте који имају то својство.[60]

Природно је прихватати да *својства* буду неке формуле теорије скупова. Формулу $\alpha(x, \cdots)$ можемо сматрати својством скупа x, допуштајући могућност да α садржи неке друге променљиве (наведене уместо тачкица $\cdots$). Ако се променљива y не појављује слободно у $\alpha(x, \cdots)$, онда се 'наивна аксиома' може формулисати на следећи начин:

$$(\text{НАИВНО!}) \qquad \forall \cdots \exists y \forall x(x \in y \Leftrightarrow \alpha(x, \cdots));$$

за произвољне скупове $\cdots$, постоји скуп y који садржи само оне x за које се може утврдити веза $\alpha(x, \cdots)$.

Приметимо најпре, да за сваку формулу α, скуп y чије постојање тврди формула (НАИВНО!) мора бити јединствен према аксиоми екстензионалности. Заиста, ако y_1 и y_2 означавају скупове такве да је

$$\forall x(x \in y_1 \Leftrightarrow \alpha(x, \cdots)) \text{ и } \forall x(x \in y_2 \Leftrightarrow \alpha(x, \cdots)),$$

онда се једноставно може извести $\forall x(x \in y_1 \Leftrightarrow x \in y_2)$, а због аксиоме екстензионалности и $y_1 = y_2$.

[60] Овом 'наивном аксиомом' се заправо уводи један нов начин задавања скупова. Поред једноставног набрајања елемената унутар витичастих заграда, 'наивна аксиома' оправдава дефинисање скупа својством, и сходно томе употребу ознаке $\{x \mid \alpha(x)\}$ за скуп свих објеката x који имају својство $\alpha(x)$. Неприхватљивост 'наивне аксиоме' показао је Бертран Расел (1872-1970) изабравши својство *не бити сам себи елемент*, тј. бирајући да $\alpha(x)$ буде $x \notin x$.

Можемо ли за свако α, формулу (НАИВНО!) прихватити као аксиому? Одговор је негативан, као што показује чувени Раселов парадокс.

Раселов парадокс. Нека је $\alpha(x, a_1, \ldots, a_n)$ формула $x \notin x$. Означимо ову формулу са $\rho(x)$. Тада (ρ^*) постаје: $\exists y \forall x(x \in y \Leftrightarrow x \notin x)$. Међутим, из ове формуле једноставно изводимо контрадикцију:

1.	$\exists y \forall x(x \in y \Leftrightarrow x \notin x)$	
2.	$v \quad \forall x(x \in v \Leftrightarrow x \notin x)$	
3.	$\quad v \in v \Leftrightarrow v \notin v$	$\forall x_{\mathrm{E}}$, 2
	$\quad \vdots$	
i.	$\quad \bot$	
$i+1$.	$\bot$	$\exists x_{\mathrm{E}}$, 1, 2-i

Контрадикција је свакако нешто што не смемо дозволити. Дакле, схема (НАИВНО!) је неприхватљива у општем случају.

▼ Схема издвајања. Аксиоме: пара, уније и партитивног скупа

Све наслоњене аксиоме су облика

$$\forall \cdots \exists y \forall x(x \in y \Leftrightarrow \alpha(x, \cdots)),$$

али само за неке посебно изабране формуле $\alpha(x, \cdots)$ у којима се y не појављује слободно.

СХЕМА ИЗДВАЈАЊА $\forall a \forall a_1 \cdots \forall a_n \exists y \forall x(x \in y \Leftrightarrow x \in a \wedge \varphi(x, a, a_1, \ldots, a_n))$

Да бисмо једноставније објаснили значење аксиоме издвајања, посматраћемо њен специјалан случај

$$\forall a \exists y \forall x(x \in y \Leftrightarrow x \in a \wedge \varphi(x, a)).$$

Схема издвајања заправо одређује бесконачно много аксиома – по једну аксиому, за сваку формулу $\varphi(x, \cdots)$. Уопштено говорећи, за свако задато својство $\varphi(x, \cdots)$, само из постојећих скупова могу се издавајати елементи који задовољавају то својство и од тих елемената формирати нови скуп.

$$\{x \in a \mid \varphi(x, \cdots)\}$$

Овим обликом аксиоме се тврди да за сваки скуп a и било коју формулу $\varphi(x, a)$ можемо формирати скуп (издвојити подскуп од a) који ће садржавати само оне елементе x из a за које се може утврдити $\varphi(x, a)$. Пошто такав скуп мора бити јединствен, уводимо посебну ознаку за њега $\{x \mid x \in a \wedge \varphi(x, a)\}$ или $\{x \in a \mid \varphi(x, a)\}$. Приметимо да је $\{x \mid x \in a \wedge \varphi(x, a)\} \subseteq a$. Истичемо и следећу еквиваленцију:

$$t \in \{x \mid x \in a \wedge \varphi(x, a)\} \Leftrightarrow t \in a \wedge \varphi(t, a).$$

АКСИОМА ПАРА $\forall a_1 \forall a_2 \exists y \forall x(x \in y \Leftrightarrow x = a_1 \vee x = a_2)$

Аксиома пара тврди да за свака два скупа a_1 и a_2 постоји скуп y чији су једини елементи a_1 и a_2. Већ смо истакли да се може извести $\forall a_1 \forall a_2 \exists! y \forall x(x \in y \Leftrightarrow x = a_1 \vee x = a_2)$. Јединствени скуп који садржи a_1 и a_2 као једине елементе означавамо $\{a_1, a_2\}$. Специјално, за произвољан a_1, скуп $\{a_1, a_1\}$ означавамо $\{a_1\}$ и називамо га **синглтоном** (или једночланим скупом). Уведене ознаке користитимо при записивању формула, при чему имамо на уму да ове ознаке можемо елеминисати помоћу следећих еквиваленција:

$$x \in \{a_1, a_2\} \Leftrightarrow x = a_1 \vee x = a_2 \quad \text{и} \quad x \in \{a_1\} \Leftrightarrow x = a_1 \vee x = a_1 \Leftrightarrow x = a_1.$$

Аксиома партитивног скупа $\forall a \exists y \forall x (x \in y \Leftrightarrow \forall t (t \in x \Rightarrow t \in a))$

Подсећамо да је $x \subseteq a$ скраћење за $\forall t (t \in x \Rightarrow t \in a)$, па аксиому партитивног скупа можемо записати и у следећем облику: $\forall a \exists y \forall x (x \in y \Leftrightarrow x \subseteq a)$. Дакле, ова аксиома тврди да за сваки скуп a постоји скуп који садржи све подскупове скупа a и других елемената нема. Тај јединствени скуп означавамо $\mathcal{P}(a)$ и називамо **партитивни скуп** од a. Посебно истичемо еквиваленцију коју ћемо користити при раду са партитивним скуповима:

$$x \in \mathcal{P}(a) \Leftrightarrow x \subseteq a.$$

Аксиома уније $\forall a \exists y \forall x (x \in y \Leftrightarrow \exists t (t \in a \wedge x \in t))$

Аксиомом уније се тврди да за сваки скуп a постоји скуп који садржи све елементе елемената скупа a и других елемената нема. Тај јединствени скуп означавамо $\bigcup a$ или $\bigcup\limits_{t \in a} t$ и називамо **унијом** скупа a.

$$x \in \bigcup a \Leftrightarrow \exists t (t \in a \wedge x \in t)$$

Корисно је имати на уму следеће:

- на пример, ако $\{a, b, c\} \in X$, онда $a, b, c \in \bigcup X$;
- на пример, ако $a, b, c \in X$, онда $\{a, b, c\} \in \mathcal{P}(X)$.

Пример 37. Полазећи од празног скупа $\emptyset$, наводимо неке од скупова које можемо изградити применом наведених аксиома.

Користећи аксиому пара добијамо скупове:

$$\{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\{\emptyset\}\}\},\ \{\emptyset, \{\emptyset\}\},\ \{\emptyset, \{\{\emptyset\}\}\},\ \{\{\emptyset\}, \{\{\emptyset\}\}\}\ \text{итд.}$$

Користећи аксиому партитивног скупа:

$$\mathcal{P}(\emptyset) = \{\emptyset\},\ \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\},\ \mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}\ \text{итд.}$$

Користећи аксиому издвајања, на пример, из скупа $\mathcal{P}(\{\emptyset, \{\emptyset\}\})$ формулом $\emptyset \in x \vee \{\emptyset\} \in x$ можемо 'издвојити' скуп

$$\{x \mid x \in \mathcal{P}(\{\emptyset, \{\emptyset\}\}) \wedge (\emptyset \in x \vee \{\emptyset\} \in x)\} = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

Применом аксиоме уније можемо формирати, на пример, скуп $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$. Заиста, формирајмо синглтон $\{\emptyset\}$ и пар $\{\{\emptyset\}, \{\{\emptyset\}\}\}$, а затим од ових скупова нови пар $\{\{\emptyset\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}\}$. Тада је

$$\bigcup \{\{\emptyset\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}.$$

Слободније речено, ако су скупови задати навођењем елемената унутар витичастих заграда, онда $\bigcup a$ добијамо брисањем витичатих заграда које се односе на елементе скупа a (и избацивањем празног скупа уколико је он елемент од a):

ако је $a = \{\{\emptyset\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}\}$, онда је $\bigcup a = \{\cancel{\{}\emptyset\cancel{\}}, \cancel{\{}\{\emptyset\}, \{\{\emptyset\}\}\cancel{\}}\}$

До сада смо наведене аксиоме користили да бисмо доказали постојање извесних скупова. У наставку ћемо доказати нешто другачији резултат: да не постоји скуп који садржи све скупове.

Теорема 14. *Не постоји скуп који садржи све скупове.*

Доказ. Потребно је да из наведених аксиома изведемо формулу $\neg\exists y\forall x(x \in y)$. Уместо формалног извођења, наводимо само основне кораке доказа.

Претпоставимо супротно ономе што треба доказати, тј. да постоји скуп свих скупова, $\exists y\forall x(x \in y)$. Означимо са v такав скуп, $\forall x(x \in v)$. (Није тешко показати да овакав скуп v мора бити јединствен.) Према аксиоми издвајања можемо формирати скуп $u = \{x \mid x \in v \wedge x \notin x\}$. Из $\forall x(x \in u \Leftrightarrow x \in v \wedge x \notin x)$, изводимо

$$(*) \qquad u \in u \Leftrightarrow u \in v \wedge u \notin u.$$

Према закону искључења трећег, $u \in u$ или $u \notin u$.

Ако $u \in u$, користећи импликацију $u \in u \Rightarrow u \in v \wedge u \notin u$, добијену из $(*)$, изводимо $u \in v \wedge u \notin u$, тј. $u \notin u$. Контрадикција.

Нека $u \notin u$. Из $\forall x(x \in v)$ закључујемо да $u \in v$ (v садржи све скупове, па самим тим садржи и u), па имамо $u \in v \wedge u \notin u$. Користећи импликацију $u \in v \wedge u \notin u \Rightarrow u \in u$, добијену из $(*)$, изводимо $u \in u$. Контрадикција.

Изведене контрадикције обарају полазну претпоставку да постоји скуп свих скупова. Дакле, $\neg\exists y\forall x(x \in y)$. □

Последица 1. *За сваки скуп постоји скуп који му не припада.*

Доказ. Тврђење следи из претходне теореме и Де Морганових закона за квантификаторе: $\neg\exists y\forall x(x \in y) \Leftrightarrow \forall y\exists x(x \notin y)$. □

За било који скуп a, унија $\bigcup a$ садржи само оне елементе који припадају бар једном елементу из a. Ако је a непразан скуп, онда из једног елемента скупа a можемо издвојити само оне елементе који припадају свим елементима из a:

$$(*) \qquad x \in \bigcap a \;\Leftrightarrow\; \forall t(t \in a \Rightarrow x \in t).$$

Овако одређен скуп $\bigcap a$ је јединствен и називамо га **пресеком** скупа a. Уместо $\bigcap a$ понекада се пише и $\bigcap\limits_{t\in a} t$. Важно је имати на уму да је дефинисан само пресек непразног скупа. Пресек празног скупа није дефинисан, јер би се у том случају еквиваленцијом $(*)$ тврдило да је $\bigcap\emptyset$ заправо скуп свих скупова (једноставно је доказати формулу $\forall t(t \in \emptyset \Rightarrow x \in t)$).

4.2. **Булове операције. Декартов производ**

11

Већ смо нагласили да ћемо као промењиве користити и велика слова латинице, што је у математичкој литератури уобичајено, па ћемо у наставку све чешће тако поступати. Подсећамо на уведене аксиоме и основне последице.

Формула $\exists! y\varphi$ (постоји јединствено y тако да φ) јесте краћи запис за:

$\exists y\varphi \wedge \forall y_1 \forall y_2 (\varphi[y/y_1] \wedge \varphi[y/y_2] \Rightarrow y_1 = y_2)$.

Аксиома екстензионалности:	$\forall A \forall B (A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B))$
Аксиома празног скупа:	$\exists y \forall x (x \notin y)$
Лема (i)	$\exists! y \forall x (x \notin y)$
Дефиниција.	... $\emptyset$
Аксиома пара:	$\forall a_1 \forall a_2 \exists P \, \forall x \, (x \in P \Leftrightarrow x = a_1 \vee x = a_2)$
Лема (ii)	$\forall a_1 \forall a_2 \exists! P \, \forall x (x \in P \Leftrightarrow x = a_1 \vee x = a_2)$
Дефиниција.	... $\{a_1, a_2\}$
Аксиома уније:	$\forall \mathcal{A} \exists U \, \forall x \, (x \in U \Leftrightarrow \exists S (S \in \mathcal{A} \wedge x \in S))$
Лема (iii)	$\forall \mathcal{A} \exists! U \, \forall x (x \in U \Leftrightarrow \exists S (S \in \mathcal{A} \wedge x \in S))$
Дефиниција.	... $\bigcup \mathcal{A} = \bigcup\limits_{S \in \mathcal{A}} S = \{x \mid \exists S (S \in \mathcal{A} \wedge x \in S)\}$
Аксиома партитивног скупа:	$\forall A \exists \mathcal{P} \, \forall S \, (S \in \mathcal{P} \Leftrightarrow S \subseteq A)$
Лема (iv)	$\forall A \exists! \mathcal{P} \, \forall S (S \in \mathcal{P} \Leftrightarrow S \subseteq A)$
Дефиниција.	... $\mathcal{P}(A) = \{S \mid S \subseteq A\} = \{S \mid \forall x (x \in S \Rightarrow x \in A)\}$
Схема издвајања:	$\forall A \forall a_1 \cdots \forall a_n \exists Y \, \forall x \, (x \in Y \Leftrightarrow x \in A \wedge \varphi(x, A, a_1, \ldots, a_n))$
Лема (v)	$\forall A \forall a_1 \cdots \forall a_n \exists! Y \, \forall x (x \in Y \Leftrightarrow x \in A \wedge \varphi(x, A, a_1, \ldots, a_n))$
Дефиниција.	... $Y = \{x \mid x \in A \wedge \varphi(x, A, a_1, \ldots, a_n)\}$ $= \{x \in A \mid \varphi(x, A, a_1, \ldots, a_n)\}$

▼ Булове (скуповне) операције

Лема 4. *Следећа тврђења су последице уведених аксиома:*

1. $\forall A \forall B \exists! Y \forall x (x \in Y \Rightarrow x \in A \wedge x \in B)$
2. $\forall A \forall B \exists! Y \forall x (x \in Y \Rightarrow x \in A \wedge x \notin B)$
3. $\forall A \forall B \exists! Y \forall x (x \in Y \Rightarrow x \in A \vee x \in B)$

Доказ. Тврђења 1) и 2) су директне последице схеме издвајања и аксиоме екстензионалности (тј. последице леме (v)) узимајући да је $\varphi_1(x, A, B)$ формула $x \in B$, одн. да је $\varphi_2(x, A, B)$ формула $x \notin B$:

$$\forall A \forall B \exists! Y \forall x (x \in Y \Rightarrow \underbrace{x \in A \wedge x \in B}_{x \in A \wedge \varphi_1(x,A,B)}), \text{ одн. } \forall A \forall B \exists! Y \forall x (x \in Y \Rightarrow \underbrace{x \in A \wedge x \notin B}_{x \in A \wedge \varphi_2(x,A,B)})$$

3) Нека је $Y = \bigcup\{A, B\}$. За било које x имамо:

$$\begin{aligned}
x \in Y &\Leftrightarrow x \in \bigcup \{A, B\} \\
&\Leftrightarrow \exists t (t \in \{A, B\} \wedge x \in t) \\
&\Leftrightarrow \exists t ((t = A \vee t = B) \wedge x \in t) \\
&\Leftrightarrow \exists t ((t = A \wedge x \in t) \vee (t = B \wedge x \in t)) \\
&\Leftrightarrow \exists t (t = A \wedge x \in t) \vee \exists t (t = B \wedge x \in t) \\
&\Leftrightarrow x \in A \vee x \in B.
\end{aligned}$$

Дакле, за дате скупове A и B, постојање и јединственост скупа Y следи из аксиома екстензионалности, пара и уније. $\square$

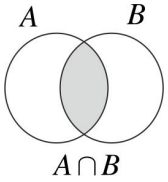
Напомена 3. У претходном еквиваленцијском ланцу користили смо еквиваленцију $\exists t(t = A \wedge x \in t) \Leftrightarrow x \in A$ коју није тешко доказати. Наводимо скраћени доказ импликације $\exists t(t = A \wedge x \in t) \Rightarrow x \in A$.

1.	$\exists t(t = A \wedge x \in t)$	претпоставка
2.	$t \;\; t = A \wedge x \in t$	
3.	$t = A$	$\wedge_{\mathrm{E}}^{\mathrm{L}}$, 2
4.	$x \in t$	$\wedge_{\mathrm{E}}^{\mathrm{D}}$, 2
5.	$t = A \Leftrightarrow \forall u(u \in t \Leftrightarrow u \in A)$	аксиома
$\cdots i.$	$x \in t \Leftrightarrow x \in A$	из 3 и 5 применом $\Leftrightarrow_{\mathrm{E}}^{\mathrm{LD}}$, $\Rightarrow_{\mathrm{E}}$, $\forall u_{\mathrm{E}}$
$i+1.$	$x \in A$	из 4 и i применом $\Leftrightarrow_{\mathrm{E}}^{\mathrm{LD}}$, $\Rightarrow_{\mathrm{E}}$
$i+2.$	$x \in A$	$\exists x_{\mathrm{E}}$, 1, 2-$i+1$

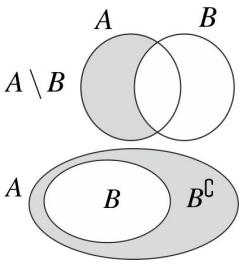
Обратну импликацију $x \in A \Rightarrow \exists t(t = A \wedge x \in t)$ је још лакше доказати.

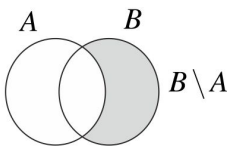
1.	$x \in A$	
$\cdots i.$	$A = A$	
$i+1.$	$A = A \wedge x \in A$ [Ова формула је заправо $(t = A \wedge x \in t)[A/t]$]	$\wedge_{\mathrm{U}}$, 1, i
$i+2.$	$\exists t(t = A \wedge x \in t)$	$\exists t_{\mathrm{U}}$, $i+1$

Дефиниција 7. *1)* ***Пресек*** *скупова A и B јесте скуп $A \cap B$ који садржи само оне елементе који припадају и скупу A и скупу B, и других елемената осим ових нема. Пресек скупова A и B означавамо $A \cap B$: $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Скупови A и B су* ***дисјунктни*** *ако је $A \cap B = \emptyset$.*



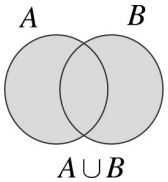
2) ***Разлика*** *скупова A и B јесте скуп који садржи само оне елементе који припадају скупу A, а не припадају скупу B, и других елемената осим ових нема. Специјално, ако је $B \subseteq A$, разлику $A \setminus B$ називамо* ***комплементом*** *скупа B у односу на A. Када је у неком контексту јасно у односу на који скуп A се одређују комплементи, онда уместо $A \setminus B$ пишемо $B^{\complement}$.*





3) ***Унија*** *скупова A и B јесте скуп $A \cup B$ који садржи само оне елементе који припадају скупу A или скупу B (бар једном од скупова A, B), и других елемената осим ових нема:*

$$A \cup B = \bigcup\{A, B\} = \{x \mid x \in A \vee x \in B\}.$$



Теорема 15. *За произвољне скупове A, B, C важи:*

1. $A \cap A = A$	*2.* $A \cup A = A$
3. $A \cap B = B \cap A$	*4.* $A \cup B = B \cup A$
5. $A \cap (B \cap C) = (A \cap B) \cap C$	*6.* $A \cup (B \cup C) = (A \cup B) \cup C$
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	*8.* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
9. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$	*10.* $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Доказ. Све наведене једнакости једноставно доказујемо формирањем еквиваленцијских ланаца у којима користимо одговарајуће теореме предикатске логике. Наводимо само неколико доказа, а остале препуштамо читаоцима.

Једнакост (1) $A \cap A = A$ потврђује ланац

$$x \in A \cap A \Leftrightarrow x \in A \wedge x \in A \Leftrightarrow x \in A,$$

у коме је друга еквиваленицција позната теорема исказне логике $\alpha \wedge \alpha \Leftrightarrow \alpha$.

Једнакост (8) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ потврђује ланац

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee x \in B \cap C \Leftrightarrow x \in A \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\qquad [\vdash \alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \beta)] \\ &\Leftrightarrow x \in A \cup B \wedge x \in A \cup C \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

Једнакост (10) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ потврђује ланац

$$\begin{aligned} x \in A \setminus (B \cup C) &\Leftrightarrow x \in A \wedge \neg x \in B \cup C \Leftrightarrow x \in A \wedge \neg(x \in B \vee x \in C) \\ &\Leftrightarrow x \in A \wedge (\neg x \in B \wedge \neg x \in C) \\ &\qquad [\vdash \neg(\alpha \vee \beta) \Leftrightarrow \neg\alpha \wedge \neg\beta] \\ &\Leftrightarrow (x \in A \wedge \neg x \in B) \wedge (x \in A \wedge \neg x \in C) \\ &\qquad [\vdash \alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge (\alpha \wedge \gamma)] \\ &\Leftrightarrow x \in A \setminus B \wedge x \in A \setminus C \\ &\Leftrightarrow x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

Корисно је приметити да сваком од наведених скуповних идентитета одговара једна сродна таутологија. □

Теорема 16. *За произвољне скупове A, B, C важи:*
1. $A \cap B \subseteq A$, $A \cap B \subseteq B$, *2.* $A \subseteq A \cup B$, $B \subseteq A \cup B$,
3. Ако је $C \subseteq A$ и $C \subseteq B$, онда је $C \subseteq A \cap B$,
4. Ако је $A \subseteq C$ и $B \subseteq C$, онда је $A \cup B \subseteq C$,
5. Ако је $B \subseteq C$, онда је $A \setminus C \subseteq A \setminus B$.

Доказ. Тврдње (1) и (2) директно следе из дефиниција инклузије, пресека и уније, и следећих теорема предикатске логике:
(1) $x \in A \wedge x \in B \Rightarrow x \in A$, $x \in A \wedge x \in B \Rightarrow x \in B$,
(2) $x \in A \Rightarrow x \in A \vee x \in B$, $x \in B \Rightarrow x \in A \vee x \in B$.
(3) Из $C \subseteq A$ и $C \subseteq B$, тј. $\forall x(x \in C \Rightarrow x \in A)$ и $\forall x(x \in C \Rightarrow x \in B)$, закључујемо $\forall x(x \in C \Rightarrow x \in A \wedge x \in B)$, тј. $\forall x(x \in C \Rightarrow x \in A \cap B)$, па је $C \subseteq A \cap B$.
(4) Из $A \subseteq C$ и $B \subseteq C$, тј. $\forall x(x \in A \Rightarrow x \in C)$ и $\forall x(x \in B \Rightarrow x \in C)$, закључујемо $\forall x(x \in A \vee x \in B \Rightarrow x \in C)$, тј. $\forall x(x \in A \cup B \Rightarrow x \in C)$, па је $A \cup B \subseteq C$.
(5) Из $B \subseteq C$, тј. $\forall x(x \in B \Rightarrow x \in C)$, према закону контрапозиције имамо $\forall x(x \notin C \Rightarrow x \notin B)$, а одатле и $\forall x(x \in A \wedge x \notin C \Rightarrow x \in A \wedge x \notin B)$, па је $A \setminus C \subseteq A \setminus B$. □

Последица 2. *Ако је $B \subseteq A$ и $C \subseteq A$, онда је:*
(1) $(B \cap C)^{\complement} = B^{\complement} \cup C^{\complement}$ *и* $(B \cup C)^{\complement} = B^{\complement} \cap C^{\complement}$,
(2) из $B \subseteq C$ следи $C^{\complement} \subseteq B^{\complement}$.

Пример 38. Докажимо да је $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Треба доказати еквиваленцију:

$$X \in \mathcal{P}(A \cap B) \Leftrightarrow X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B),$$

односно, према дефиниције партитивног скупа,

$$X \subseteq A \cap B \Leftrightarrow X \subseteq A \wedge X \subseteq B.$$

Импликацију $X \subseteq A \cap B \Rightarrow X \subseteq A \wedge X \subseteq B$, доказујемо уз помоћ леме 16 (1) и леме 12 (3): ако је $X \subseteq A \cap B$, онда, због $A \cap B \subseteq A$ и $A \cap B \subseteq B$, мора бити и $X \subseteq A$ и $X \subseteq B$. Обратна импликација, $X \subseteq A \wedge X \subseteq B \Rightarrow X \subseteq A \cap B$, јесте заправо тврдња теореме 16 (3).

Испитајмо да ли управо доказана једнакост важи уколико пресек заменимо унијом. Импликацију $X \subseteq A \vee X \subseteq B \Rightarrow X \subseteq A \cup B$ није тешко доказати: ако је $X \subseteq A$, онда, због $A \subseteq A \cup B$, добијамо $X \subseteq A \cup B$, а ако је $X \subseteq B$, онда, због $B \subseteq A \cup B$, опет добијамо $X \subseteq A \cup B$. Дакле, за било које скупове важи A и B важи $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Међутим, ако је $X \subseteq A \cup B$, скуп X *не мора бити* подскуп ниједног од скупова A, B. На пример, ако је $A = \{0, 1\}$, $B = \{1, 2\}$ и $X = \{0, 2\}$, биће $X \subseteq A \cup B$, али $X \not\subseteq A$ и $X \not\subseteq B$. Другачије записано, $X \in \mathcal{P}(A \cup B)$, $X \notin \mathcal{P}(A)$ и $X \notin \mathcal{P}(B)$. Приметимо да смо наведеним избором скупова A, B, X заправо доказали прву формулу следећег еквиваленцијског ланца:

$$\begin{aligned}
& \exists A \exists B \exists X (X \in \mathcal{P}(A \cup B) \wedge X \notin \mathcal{P}(A) \wedge X \notin \mathcal{P}(B)) \\
\Leftrightarrow\ & \exists A \exists B \exists X \neg(\neg X \in \mathcal{P}(A \cup B) \vee (X \in \mathcal{P}(A) \vee X \in \mathcal{P}(B)) \\
\Leftrightarrow\ & \exists A \exists B \neg \forall X (X \in \mathcal{P}(A \cup B) \Rightarrow (X \in \mathcal{P}(A) \vee X \in \mathcal{P}(B)) \\
\Leftrightarrow\ & \exists A \exists B \neg (\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)) \\
\Leftrightarrow\ & \neg \forall A \forall B (\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B))
\end{aligned}$$

▼ Уређене n-торке. Декартов производ

Уређен пар скупова a и b, у ознаци (a, b), замишљамо као целину коју чине a и b наведени одређеним редоследом – зна се који објекат је *први* (леви) члан целине, а који је *други* (десни) члан целине. Кључна особина уређених парова јесте да из $(a, b) = (c, d)$ следи $a = c$ и $b = d$.

Дефиниција 8. *Уређен пар скупова a и b је скуп $\{\{a\}, \{a, b\}\}$, тј. $(a, b) \stackrel{\text{def}}{=} \{\{a\}, \{a, b\}\}$, при чему је a прва координата и b друга координата.*

Приметимо да уређен пар (a, b) није исто што и пар $\{a, b\}$. Докажимо да за овако уведене уређене парове важи наведена особина.

Теорема 17. *Нека су a, b, c и d било који скупови. Тада:*

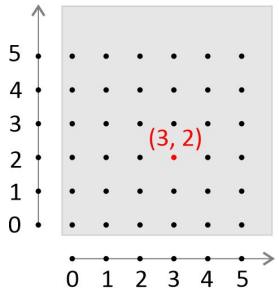
$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

$$\{a, b\} = \{c, d\} \quad \Leftrightarrow \quad (a = c \wedge b = d) \vee (a = b \wedge b = c).$$

Доказ. Посебно доказујемо сваку импликацију.
($\Leftarrow$) Ако је $a = c$ и $b = d$, онда је $\{a\} = \{c\}$ и $\{a, b\} = \{c, d\}$, па је и $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, тј. $(a, b) = (c, d)$.
($\Rightarrow$) Нека је $(a, b) = (c, d)$, тј. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Знамо да су два скупа једнака ако имају исте елементе, па из претпостављене једнакости закључујемо да важе једнакости наведене у сваком од следећа два случаја. Доказаћемо да у оба случаја мора бити $a = c \wedge b = d$.
1. случај: $\{a\} = \{c\}$, $\{a, b\} = \{c, d\}$. Из $\{a\} = \{c\}$ следи да је $a = c$, а одатле и $\{a, b\} = \{c, d\}$, па је и $b = d$.
2. случај: $\{a\} = \{c, d\}$, $\{a, b\} = \{c\}$. Из $\{a\} = \{c, d\}$ следи $a = c = d$, а из $\{a, b\} = \{c\}$ да је $a = b = c$. Самим тим, свакако важи $a = c$ и $b = d$. □

Лема 5. *За свака два скупа A и B постоји јединствени скуп који садржи уређене парове чије прве координате припадају скупу A, а друге координате припадају скупу B (и других елемената нема):*

$$\forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b)))$$



Доказ. Уређени парови чије прве координате припадају скупу A, а друге координате припадају скупу B припадају скупу $\mathcal{P}(\mathcal{P}(A \cup B))$. Заиста,

ако $a \in A$ и $b \in B$,	тада	$a, b \in A \cup B$,
	одакле следи	$\{a\}, \{a, b\} \subseteq A \cup B$,
	тј.	$\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$.
	па даље имамо	$\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$,
	односно	$(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Наравно, скуп $\mathcal{P}(\mathcal{P}(A \cup B))$ садржи и свакакве друге елементе (који нису уређени парови, као и уређене парове чије координате не испуњавају постављени услов), па је потребно применити аксиому издвајања да бисмо формирали тражени (јединствен) скуп:

$$Y = \{x \mid x \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b))\}.$$

Посебно истичемо да су у доказу овог тврђења употребљене аксиоме: екстензионалности, пара, уније, партитивног скупа и схема издвајања. □

Дефиниција 9. ***Декартов производ*** *скупова A и B јесте скуп уређених парова чије прве координате припадају скупу A, а друге скупу B. Декартов производ скупова A и B означавамо $A \times B$ и пишемо:*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Пример 39. Декартов производ скупова $A = \{0, 1, 2\}$ и $B = \{0, 1\}$ јесте скуп $A \times B = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}$. Приметимо да је $B \times A = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$, као и да је $A \times B \neq B \times A$.

Можемо формирати и следеће Декартове производе:
$A \times A = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$,
$B \times B = \{(0,0),(0,1),(1,0),(1,1)\}$.

Будући да празан скуп нема елементе, не можемо формирати уређене парове чија једна координата долази из празног скупа. Одавде следи да за сваки скуп A важе једнакости

$$A \times \emptyset = \emptyset = \emptyset \times A.$$

Лема 6. *За све скупове A, B, C важе једнакости:*
(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
(3) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Доказ. (1) Доказ наводимо у облику следећег еквиваленцијског ланца:

$$\begin{aligned}
(x,y) \in A \times (B \cup C) &\Leftrightarrow x \in A \wedge y \in B \cup C \\
&\Leftrightarrow x \in A \wedge (y \in B \vee y \in C) \\
&\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\
&\Leftrightarrow (x,y) \in A \times B \vee (x,y) \in A \times C \\
&\Leftrightarrow (x,y) \in (A \times B) \cup (A \times C)
\end{aligned}$$

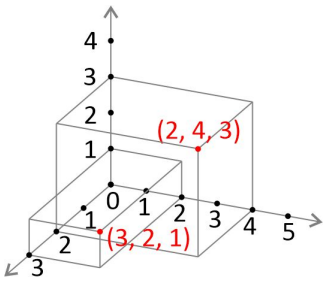
□

За произвољне a, b, c, уређени пар $((a,b),c)$ краће означавамо (a,b,c) и називамо **уређеном тројком**, и a, b, c редом називамо првом, другом, трећом координатом уређене тројке (a,b,c). Следећи еквиваленцијски ланац доказује основну особину уређених тројки:

$$\begin{aligned}
(a,b,c) = (a_1,b_1,c_1) &\Leftrightarrow (a,b) = (a_1,b_1) \wedge c = c_1 \\
&\Leftrightarrow a = a_1 \wedge b = b_1 \wedge c = c_1.
\end{aligned}$$

Скуп свих уређених тројки чија прва координата припада скупу A, друга скупу B, и трећа скупу C јесте скуп $(A \times B) \times C$, који се краће означава $A \times B \times C$. Слично као за Декартове производе два скупа, пишемо

$$A \times B \times C = \{(a,b,c) \mid a \in A \wedge b \in B \wedge c \in C\}.$$



Потпуно аналогно уводимо уређене четворке, петорке итд:

$$(a,b,c,d) \stackrel{\text{def}}{=} ((a,b,c),d),\ (a,b,c,d,e) \stackrel{\text{def}}{=} ((a,b,c,d),e),\ \ldots,$$

и Декартове производе више од три скупа:

$$A \times B \times C \times D = \{(a,b,c,d) \mid a \in A \wedge b \in B \wedge c \in C \wedge d \in D\},\ \ldots$$

Ако је A било који скуп, Декартове производе $A \times A$, $A \times A \times A$, $A \times A \times A$ итд. називамо **Декартовим степенима** и краће их означавамо A^2, A^3, A^4 итд.

– Скупови $(A \times B) \times C$ и $A \times (B \times C)$ нису једнаки, па зато у запису $A \times B \times C$ не изостављамо заграде због асоцијативности, већ по договору. Према општем договору о изостављању заграда у означавању Декартовог производа подразумева се да је $A_1 \times A_2 \times A_3 \times A_4 \times \cdots \times A_n$ краћи запис за

$$(\cdots(((A_1 \times A_2) \times A_3) \times A_4) \times \cdots) \times A_n,$$

а не да се заграде могу постављати произвољно.

4.3. **Релације. Функције**

12

Да бисмо поједноставили записивање формула, усвајамо следеће договоре: за било коју формулу α,

- $(\forall x \in X)\,\alpha$ означава $\forall x(x \in X \Rightarrow \alpha)$;
- $(\exists x \in X)\,\alpha$ означава $\exists x(x \in X \wedge \alpha)$;
- $(\exists! x \in X)\,\alpha$ означава $\exists! x(x \in X \wedge \alpha)$.

Није тешко доказати следећу еквиваленцију

$$(\exists! x \in X)\,\alpha \Leftrightarrow (\exists x \in X)\,\alpha \wedge (\forall x_1 \in X)(\forall x_1 \in X)(\alpha[x/x_1] \wedge \alpha[x/x_2] \Rightarrow x_1 = x_2).$$

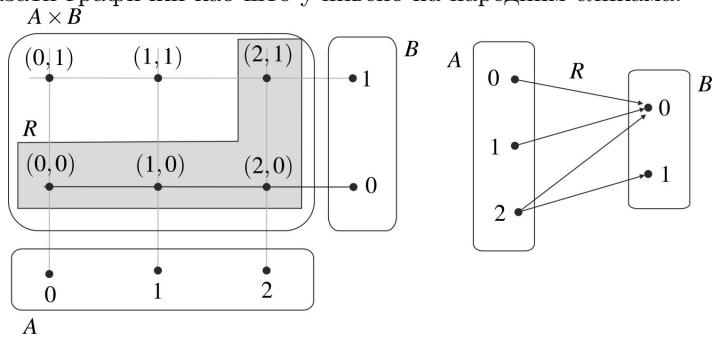
Сличне договоре примењујемо у обичном тексту:

'за сваки $x \in X$'	значи	'за сваки x који припада X';
'постоји $x \in X$'	значи	'постоји x који припада X';
'скуп $X \subseteq A$'	значи	'скуп X који је подскуп скупа A'.

Дефиниција 10. *Сваки подскуп од $X \times Y$ назива се **бинарна релација** између X и Y. Специјално, подскуп од $X \times X$ назива се бинарна релација скупа X.*

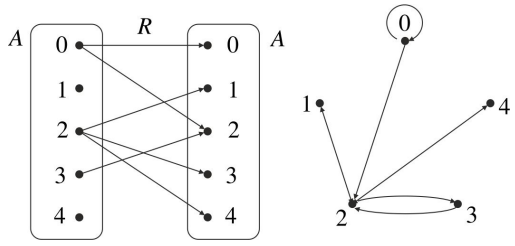
Дакле, $\mathcal{P}(A \times B)$ је скуп свих релација између A и B.

Пример 40. Ако је $A = \{0,1,2\}$ и $B = \{0,1\}$, онда је $R = \{(0,0),(1,0),(2,0),(2,1)\}$ бинарна релација између A и B. У једноставним случајевима, као што је овај, погодно је релацију R приказати графички као што учињено на наредним сликама.

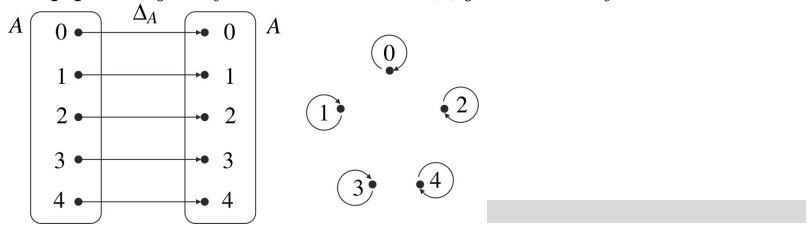


Наводимо још неколико релација из A у B: $P = \{(1,2)\}$, $Q = \{(0,0),(0,1)\}$, $S = \{(0,1),(1,1),(2,1)\}$ итд. Приметимо и да су $\emptyset$ и $A \times B$ такође две бинарне релације између A и B; $\emptyset$ називамо **празном релацијом**, а $A \times B$ **пуном** релацијом.

Пример 41. Нека је R нека релација скупа A, $R \subseteq A \times A$. Да бисмо графички приказали R не морамо два пута 'цртати' скуп A. На пример, релацију $R = \{(0,0),(0,2),(2,1),(2,3),(2,4),(3,2)\}$ скупа $A = \{0,1,2,3,4\}$ графички можемо приказати као на наредним сликама, при чему је очигледно како је слика десно настала.



Релација $\Delta_A = \{(0,0),(1,1),(2,2),(3,3),(4,4)\} \subseteq A \times A$ је важан пример релације скупа A – назива се *дијагонала скупа* A.



Дефиниција 11. ***Дијагонала*** *скупа* X *је скуп*

$$\Delta_X = \{(x,y) \mid (x,y) \in X \times X \wedge x = y\} = \{(x,x) \mid x \in X\}.$$

Напомена 4. Није тешко аксиомама оправдати постојање скупа Δ_X. Из скупа $X \times X$ издвајамо (ослањајући се, наравно, на схему издвајања) уређене парове чије су координате исте.

$$\Delta_X = \{z \in X \times X \mid (\exists x \in X)\, z = (x,x)\}$$

Сваки скуп R чији су елементи уређени парови јесте заправо бинарна релација скупа $\bigcup\bigcup R$. Заиста, координате било ког пара (a,b) из R припадају скупу $\bigcup\bigcup R$: ако $(a,b) = \{\{a\},\{a,b\}\} \in R$, онда $\{a\},\{a,b\} \in \bigcup R$, па $a,b \in \bigcup\bigcup R$. Дакле, сваки скуп R уређених парова можемо сматрати бинарном релацијом: $R \subseteq (\bigcup\bigcup R) \times (\bigcup\bigcup R)$. Скуп свих првих координата уређених парова из R назива се *домен* релације R и обележава се $\mathrm{dom}(R)$, а скуп свих других координата назива се *кодомен* релације R и обележава $\mathrm{codom}(R)$ или $\mathrm{ran}(R)$.

$$\mathrm{dom}(R) = \{a \in \bigcup\bigcup R \mid \exists b\,(b \in \bigcup\bigcup R \wedge (a,b) \in R)\}$$

$$\mathrm{ran}(R) = \{b \in \bigcup\bigcup R \mid \exists a\,(a \in \bigcup\bigcup R \wedge (a,b) \in R)\}$$

Дефиниција 12. *Релација* F *између скупова* X *и* Y, $F \subseteq X \times Y$ *је* ***функција*** *из* X *у* Y, *у ознаци* $F : X \to Y$, *ако за свако* x *из* X *постоји јединствено* y *из* Y *тако да* $(x,y) \in F$, *што можемо изразити и следећим условима:*

(**F1**) $\mathrm{dom}(F) = X$, *тј. за свако* $x \in X$ *постоји* $y \in Y$ *тако да* $(x,y) \in F$,

(**F2**) *за свако* $x \in X$ *и све* $y_1, y_2 \in Y$, *из* $(x,y_1) \in F$ *и* $(x,y_2) \in F$ *следи* $y_1 = y_2$.

Према претходној дефиницији, запис $F : X \to Y$ је скраћење за формулу

$$(\forall x \in X)(\exists! y \in Y)(x, y) \in F,$$

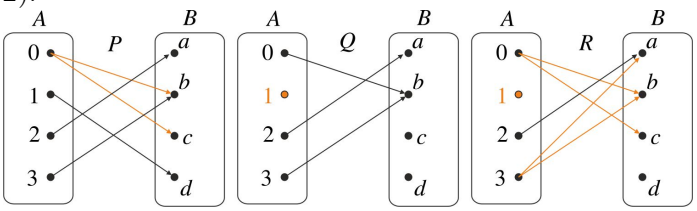
односно за конјункцију следеће две формуле:

(**F1**) $(\forall x \in X)(\exists y \in Y)(x, y) \in F$,

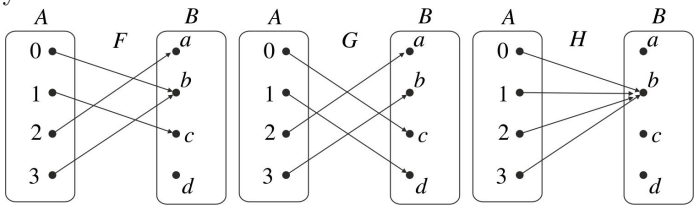
(**F2**) $(\forall x \in X)(\forall y_1 \in Y)(\forall y_2 \in Y)((x, y_1) \in F \wedge (x, y_2) \in F \Rightarrow y_1 = y_2)$.

Пример 42. На наредним сликама представљено је неколико релација између скупова $A = \{0, 1, 2, 3\}$ и $B = \{a, b, c, d\}$.

Релације P, Q и R нису функције из A у B. Релација P не испуњава услов (**F2**), према коме елемент домена не може бити почетак више од једне стрелице: $(0, b) \in P$, $(0, c) \in P$ и $b \neq c$. Релација Q не испуњава услов (**F1**), према коме сваки елемент домена мора бити почетак неке стрелице: елемент 1 није прва координата ниједног уређеног пара из Q. Релација R не задовољава ни услов (**F1**) ни (**F2**).



Релације F, G и H, приказане на сликама испод јесу функције из A у B.

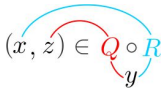


Ове функционалне релације краће описујемо следећим 'табелама':

$$F = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & c & a & b \end{pmatrix}, G = \begin{pmatrix} 0 & 1 & 2 & 3 \\ c & d & a & b \end{pmatrix}, H = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & b & b & b \end{pmatrix}.$$

Ако $F : X \to Y$, уместо $(x, y) \in F$ пишемо $F(x) = y$ или $x \overset{F}{\mapsto} y$. Елементи скупа X називају се *оригинали* или *аргументи* функције F. За сваки x из X, елемент y из Y такав да је $F(x) = y$ називамо *F-сликом* аргумента x, при чему префикс F изостављамо када је из контекста јасно о којој функцији F је реч. За x из X, запис $F(x)$ користитимо и самостално као ознаку одговарајућег елемента из Y – ознаку F-слике елемента x.

▼ Композиција релација. Композиција функција



Дефиниција 13. *Нека је $R \subseteq X \times Y$ и $Q \subseteq Y \times Z$. Релација $Q \circ R \subseteq X \times Z$ дата са*

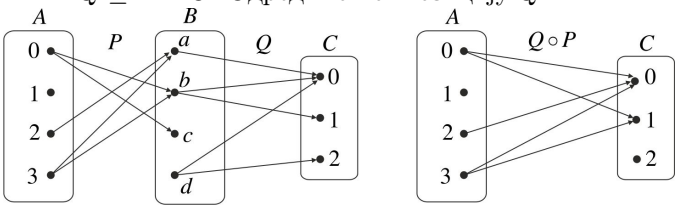
$$Q \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y((x, y) \in R \wedge (y, z) \in Q)\}$$

назива се ***композиција*** *релација R и Q.*

Напомена 5. Схемом издвајања једноставно је оправдати постојање скупа који је композиција релација $R \subseteq X \times Y$ и $Q \subseteq Y \times Z$:

$$Q \circ R = \{u \in X \times Y \mid (\exists x \in X)(\exists y \in Y)(\exists z \in Z)(u = (x, z) \wedge (x, y) \in R \wedge (y, z) \in Q)\}.$$

Пример 43. На слици доле лево приказане су две релације $P \subseteq A \times B$ и $Q \subseteq B \times C$. Одредимо композицију $Q \circ P$.



Ослањајући се на дате графове релација уочавамо да (x, z) припада релацији $Q \circ P$ ако постоји стрелица из x у неки елемент скупа Y и стрелица из тог истог елемента у z, тј. ако су x и z повезани двема надовезаним стрелицама (крај једне стрелице поклапа се са почетком друге стрелице).

Теорема 18. *Нека је $R \subseteq X \times Y$, $Q \subseteq Y \times Z$ и $P \subseteq Z \times U$. Тада је:*
(1) $R \circ \Delta_X = R = \Delta_Y \circ R$,
(2) $P \circ (Q \circ R) = (P \circ Q) \circ R$

Доказ. (1) Очигледно су $R \circ \Delta_X$ и $\Delta_Y \circ R$ подскупови од $X \times Y$. Доказе жељених једнакости наводимо у облику следећих еквиваленцијских ланаца:

$$\begin{aligned}(x, y) \in R \circ \Delta_X &\Leftrightarrow (\exists t \in X)((x, t) \in \Delta_X \wedge (t, y) \in R)\\ &\Leftrightarrow (\exists t \in X)(x = t \wedge (t, y) \in R)\\ &\Leftrightarrow (x, y) \in R\end{aligned}$$

$$\begin{aligned}(x, y) \in \Delta_Y \circ R &\Leftrightarrow (\exists t \in Y)((x, t) \in R \wedge (t, y) \in \Delta_Y)\\ &\Leftrightarrow (\exists t \in Y)((x, t) \in R \wedge t = y)\\ &\Leftrightarrow (x, y) \in R\end{aligned}$$

Оправдање последњих еквиваленција у наведеним ланцима сасвим је аналогно оном које је наведено у напомени 3 на страни 58.
(2) Нека је $R \subseteq X \times Y$, $Q \subseteq Y \times Z$ и $P \subseteq Z \times U$. Тада је $Q \circ R \subseteq X \times Z$, па је $P \circ (Q \circ R) \subseteq X \times U$. Такође, $P \circ Q \subseteq Y \circ U$, па је

$(P \circ Q) \circ R \subseteq X \times U$. Остаје још да за сваки уређени пар (x, u) из $X \times U$ докажемо еквиваленцију $(x, u) \in P \circ (Q \circ R) \Leftrightarrow (x, u) \in (P \circ Q) \circ R$:

$$\begin{aligned}
(x,u) \in P \circ (Q \circ R) &\Leftrightarrow (\exists z \in Z)((x,z) \in Q \circ R \wedge (z,u) \in P) \\
&\Leftrightarrow (\exists z \in Z)(\underline{(x,z) \in Q \circ R} \wedge (z,u) \in P) \\
&\Leftrightarrow (\exists z \in Z)(\underline{(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q)} \wedge (z,u) \in P) \\
&\Leftrightarrow (\exists z \in Z)(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q \wedge (z,u) \in P) \\
&\Leftrightarrow (\exists y \in Y)\underline{(\exists z \in Z)}((x,y) \in R \wedge \underline{(y,z) \in Q} \wedge \underline{(z,u) \in P}) \\
&\Leftrightarrow (\exists y \in Y)((x,y) \in R \wedge \underline{\exists z(z \in Z \wedge (y,z) \in Q \wedge (z,u) \in P)}) \\
&\Leftrightarrow (\exists y \in Y)((x,y) \in R \wedge \underline{(y,u) \in P \circ Q}) \\
&\Leftrightarrow (x,u) \in (P \circ Q) \circ R
\end{aligned}$$

□

Напомена 6. Када се променљива v не појављује слободно у формули α, тада је

$$\vdash \exists v(\alpha \wedge \beta) \Leftrightarrow \alpha \wedge \exists v\beta,$$

што смо користили у доказу тврђења (4). Поред тога, користили смо и

$$\vdash \exists v_1 \exists v_2 \varphi \Leftrightarrow \exists v_2 \exists v_3 \varphi,$$

као и асоцијативност конјункције.

Задатак **6.** Нека је $R, R_1 \subseteq X \times Y$ и $Q, Q_1 \subseteq Y \times Z$.
(1) Ако је $R \subseteq R_1$, онда је $Q \circ R \subseteq Q \circ R_1$.
(2) Ако је $Q \subseteq Q_1$, онда је $Q \circ R \subseteq Q_1 \circ R$.

Композиција две функције, такође је функција.

Теорема 19. *Нека је $F : X \to Y$ и $G : Y \to Z$. Тада $G \circ F : X \to Z$.*

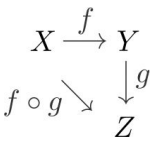
Доказ. Јасно је да мора бити $G \circ F \subseteq X \times Z$. Проверимо услове (**F1**) и (**F2**).
(**F1**) Нека је $x \in X$ произвољно изабран елемент. Будући да $F : X \to Y$, постоји елемент $y \in Y$ такав да је $(x, y) \in F$. Даље, пошто $G : Y \to Z$, постоји елемент $z \in Z$ такав да је $(y, z) \in G$. Одавде, следи да $(x, z) \in G \circ F$.
(**F2**) Нека су $x \in X$, $z_1, z_2 \in Z$ произвољно изабрани елементи, такви да је $(x, z_1) \in G \circ F$ и $(x, z_2) \in G \circ F$.

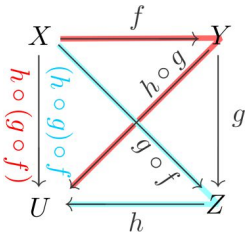
Из $(x, z_1) \in G \circ F$ следи да постоји $y_1 \in Y$ такав да $(x, y_1) \in F$ и $(y_1, z_1) \in G$.

Из $(x, z_2) \in G \circ F$ следи да постоји $y_2 \in Y$ такав да $(x, y_2) \in F$ и $(y_2, z_2) \in G$.

Пошто $F : X \to Y$, из $(x, y_1) \in F$ и $(x, y_2) \in F$, закључујемо да $y_1 = y_2$. Најзад, пошто $G : Y \to Z$, из $y_1 = y_2$, $(y_1, z_1) \in G$ и $(y_2, z_2) \in G$, закључујемо да $z_1 = z_2$. □

Ако $f : X \to Y$ и $g : Y \to Z$, тада за x из X, елемент $(g \circ f)(x)$, тј. $g \circ f$-слику елемента x означавамо и са $g(f(x))$.





Према теореми 18 (2), ако $f : X \to Y$, $g : Y \to Z$ и $h : Z \to U$, једнакост

$$(h \circ g) \circ f = h \circ (g \circ f)$$

допушта да композицију ове три функције означавамо $h \circ g \circ f : X \to U$.

▼ Инверзна релација. 1-1 функција, на-функција, бијекција

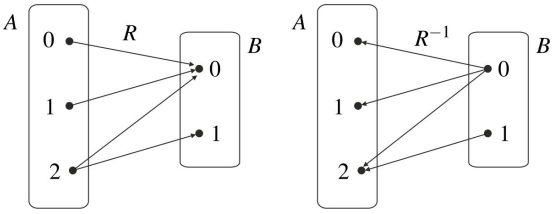
Дефиниција 14. *Нека је $R \subseteq X \times Y$. Релација $R^{-1} \subseteq Y \times X$ дата са $R^{-1} = \{(y, x) \mid (x, y) \in R\}$ назива се* ***инверзна релација*** *релације R.*

Напомена 7. Није тешко аксиомама оправдати постојање скупа који је инверзна релација неке дате делације $R \subseteq X \times Y$:

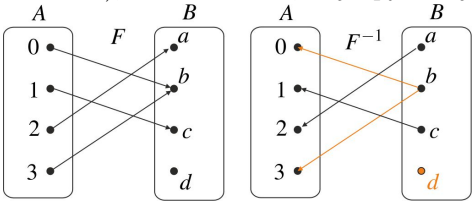
$$R^{-1} = \{z \in Y \times X \mid (\exists x \in X)(\exists y \in Y)(z = (y, x) \wedge (x, y) \in R)\}.$$

Пример 44. Нека је $A = \{0, 1, 2\}$ и $B = \{0, 1\}$.

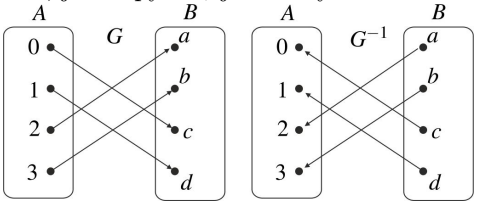
Ако је $R \subseteq A \times B$ и $R = \{(0, 0), (1, 0), (2, 0), (2, 1)\}$, онда је $R^{-1} \subseteq B \times A$ и $R^{-1} = \{(0, 0), (0, 1), (0, 2), (1, 2)\}$. Графички приказ релације R^{-1} добијамо променом смера свих стрелица релације R.



Пример 45. Инверзна релација функције не мора бити функција. Инверзна релација функције $F : A \to B$ (приказане на наредној слици лево), $F^{-1} \subseteq B \times A$, није функција из B у A.



Инверзна релација функције $G : A \to B$ (слика доле лево), $G^{-1} \subseteq B \times A$, јесте функција из B у A.



Ако $F : X \to Y$, релација $F^{-1} \subseteq Y \times X$ је функција из Y у X ако важи:

$$(\forall y \in Y)(\exists! x \in X)(y, x) \in F^{-1}, \text{ тј. } (\forall y \in Y)(\exists! x \in X)(x, y) \in F.$$

Последња формула заправо представља услов који мора да задовољи функција F да би њој инверзна релација такође била функција. Тај услов еквивалентан је конјункцији следећа два услова:

(**S**) $(\forall y \in Y)(\exists x \in X)(x, y) \in F$, тј. за свако y из Y постоји x из X такав да $(x, y) \in F$ (сваки y из Y јесте слика неког елемента из X);

(**I**) $(\forall y \in Y)(\forall x_1 \in X)(\forall x_2 \in X)((x_1, y) \in F \wedge (x_2, y) \in F \Rightarrow x_1 = x_2)$, тј. ако x_1 и x_2 из X имају исте слике, онда су они једнаки.

Услов (**I**) можемо формулисати и у следећем облику:

(**I**) $(\forall x_1 \in X)(\forall x_2 \in X)(F(x_1) = F(x_2) \Rightarrow x_1 = x_2)$,

односно, ослањајући се на закон контрапозиције,

(**I**) $(\forall x_1 \in X)(\forall x_2 \in X)(x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2))$.

Углавном ћемо користити једну од ове последње две формулације.

Дефиниција 15. *Нека $F : X \to Y$.*

1. *F је **на-функција** или **сурјекција**, у ознаци $F : X \overset{\text{на}}{\to} Y$, ако задовољава услов (**S**).*[75]
2. *F је **1-1 функција** или **инјекција**, у ознаци $F : X \overset{1-1}{\to} Y$, ако задовољава услов (**I**).*
3. *F је **бијекција** или **обострано-једнозначна коресподенција**, у ознаци $F : X \overset{1-1}{\underset{\text{на}}{\to}} Y$, ако $F : X \overset{1-1}{\to} Y$ и $F : X \overset{\text{на}}{\to} Y$.*

[75] Ако $F : X \overset{\text{на}}{\to} Y$, кажемо да је F функција из скупа X на скуп Y.

Задатак **7.** Нека $f : X \to Y$ и $g : Y \to Z$.

(1) Ако $f : X \overset{1-1}{\to} Y$ и $g : Y \overset{1-1}{\to} Z$, онда $g \circ f : X \overset{1-1}{\to} Z$.

(2) Ако $f : X \overset{\text{на}}{\to} Y$ и $g : Y \overset{\text{на}}{\to} Z$, онда $g \circ f : X \overset{\text{на}}{\to} Z$.

(3) Ако $f : X \overset{1-1}{\underset{\text{на}}{\to}} Y$ и $g : Y \overset{1-1}{\underset{\text{на}}{\to}} Z$, онда $g \circ f : X \overset{1-1}{\underset{\text{на}}{\to}} Z$.

На основу претходних разматрања изводимо следећи закључак.

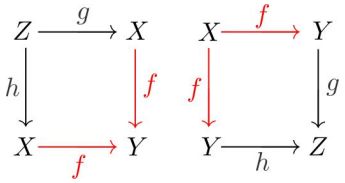
Теорема 20. *Нека $F : X \to Y$.*

1. *Инверзна релација функције F је функција акко је F бијекција.*
2. *Ако је F бијекција, онда је и F^{-1} бијекција.*

Напомена 8. Ако $F : X \to Y$, за y из Y смемо користити запис $F^{-1}(y)$ само ако знамо да је F бијекција, јер само тада то има смисла.

Задатак **8.** (1) $f : X \overset{1-1}{\to} Y$ акко за све $g, h : Z \to X$, из $f \circ g = f \circ h$ следи $g = h$.

(2) $f : X \overset{\text{на}}{\to} Y$ акко за све $g, h : Y \to Z$, из $g \circ f = h \circ f$ следи $g = h$.



▼ Важни примери релација и функција

13

Функције заузимају веома значајно место у свим математичким областима што донекле потврђује велики број синонима који се користе: пресликавања, трансформације, оператори итд.

Рестрикције

Ако је R бинарна релација скупа X, тј. $R \subseteq X \times X$, онда је за сваки непразан подскуп A од X, скуп $R \cap (A \times A)$ бинарна релација скупа A. Ова релација се обележава $R \mid_A$ и назива се **рестрикција** релације R на A.

Слично, ако $f : X \to Y$, тада је за сваки непразан подскуп A од X ($\emptyset \neq A \subseteq X$), скуп $f \cap (A \times Y)$ функција из A у Y. Ова функција се обележава $f \mid_A$ и назива **рестрикција** функције f на (подскуп домена) A. Дакле, $f \mid_A : A \to Y$. За $x \in A$ важи $f \mid_A (x) = f(x)$, док за $x \in X \setminus A$, запис $f \mid_A (x)$ нема смисла.

Пример 46. Нека $f : \{0,1,2,3\} \to \{a,b,c\}$:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & c & a & b \end{pmatrix}.$$

Тада је $f \mid_{\{0,1,2\}} = \begin{pmatrix} 0 & 1 & 2 \\ b & c & a \end{pmatrix}$, $f \mid_{\{1,3\}} = \begin{pmatrix} 1 & 3 \\ c & b \end{pmatrix}$, итд.

Лема 7. *Ако $f : X \to Y$ и $\emptyset \neq B \subseteq A \subseteq X$, онда је $(f \mid_A) \mid_B = f \mid_B$.*

Доказ. Из $f \mid_A = f \cap (A \times Y)$ и $(f \mid_A) \mid_B = f \mid_A \cap (B \times Y)$ следи да је

$$(f \mid_A) \mid_B = f \mid_A \cap (B \times Y) = f \cap (A \times Y) \cap (B \times Y).$$

Како је $B \subseteq A$, закључујемо да је $B \times Y \subseteq A \times Y$, тј. $(A \times Y) \cap (B \times Y) = B \times Y$. Дакле, $(f \mid_A) \mid_B = f \cap (B \times Y) = f \mid_B$. □

Идентичко пресликавање

Очигледно је Δ_X (дијагонала скупа X) једна фунција из X у X, $\Delta_X : X \to X$. Ова функција је веома заступљена у математици и у литератури се среће доста њених ознака id_X, I_X, Id_X, 1_X итд, при чему се индекс X изоставља када је јасно на који скуп X се односи. Ми ћемо користити ознаку $\mathrm{id}_X : X \to X$. Приметимо да је $\mathrm{id}_X(x) = x$, за свако $x \in X$. Очигледно, функција id_X је бијекција. Посебно истичемо следеће својство.

Теорема 21. *Ако $f : X \to Y$ и $g : Y \to X$ и важи $g \circ f = \mathrm{id}_X$ и $f \circ g = \mathrm{id}_Y$, онда су f и g бијекције, једна другој инверзне.*

Релације аквиваленције. Количнички скуп

Једнакост је основна релација сваког непразног скупа. У универзуму скупова, бинарни предикат $=$ одређује на сваком непразном скупу X релацију једнакости, коју смо означавали Δ_X; природнија је ознака $=_X$, при чему је уобичајено да се изоставља индекс, јер је увек јасно који скуп се посматра.

Издвајамо три основне особине једнакости које користимо за увођење веома важне врсте бинарних релација – релација еквиваленције:

- за свако x из X, $x = x$ – *рефлексивност*
- за све x, y из X, из $x = y$ следи $y = x$ – *симетричност*
- за све x, y, z из X, из $x = y$ и $y = z$ следи $y = x$ – *транзитивност*.

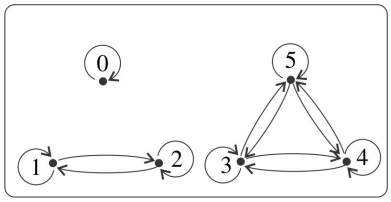
Дефиниција 16. *Бинарна релација E скупа X, $E \subseteq X \times X$, јесте* ***релација еквиваленције*** *ако је:*

- *рефлексивна* – $(\forall x \in X)\,(x, x) \in E$ *(или еквивалентно, ако је* $\Delta_X \subseteq E$*,),*
- *симетрична* – $(\forall x, y \in X)\,((x, y) \in E \Rightarrow (y, x) \in E)$ *(или еквивалентно, ако је* $E \subseteq E^{-1}$*),*
- *транзитивна* – $(\forall x, y, z \in X)\,((x, y) \in E \wedge (y, z) \in E \Rightarrow (x, z) \in E)$ *(или еквивалентно, ако је* $E \circ E \subseteq E$*).*

Инфиксна нотација је много чешћа за бинарне релације; поред тога, релације еквиваленције се углавном означавају знацима који подсећају на знак једнакости, попут: $\approx$, $\sim$, $\cong$, $\simeq$, $\equiv$, $\doteq$, итд.

$$\frac{}{x \sim x} \qquad \frac{x \sim y}{y \sim x} \qquad \frac{x \sim y \quad y \sim z}{x \sim z}$$

Пример 47. Релација E скупа $\{0, 1, 2, 3, 4, 5\}$ задата је графом десно.



Није тешко уочити да је E релација еквиваленције. Релација је рефлексивна, јер око сваког елемента уочавамо петљу. Симетрична је зато што за сваку стрелицу која повезује нека два елемента постоји супротно усмерена стрелица која повезује исте елементе. Транзитивна је, јер за свака два елемента повезана двема надовезаним стрелицама (крај једне поклапа се са почетком друге стрелице) постоји стрелица која их директно повезује.

Дефиниција 17. *Нека је $E \subseteq X \times X$ релација еквиваленције. За сваки елемент $x \in X$ скуп*

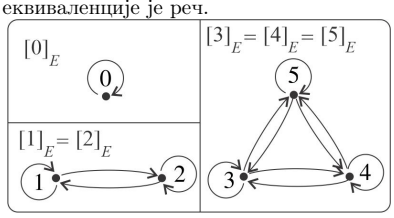
$$[x]_E = \{y \in X \mid (x, y) \in E\}$$

назива се ***класа еквиваленције*** *елемента x у односу на релацију E. Скуп свих класа еквиваленције назива се* ***количнички скуп*** *и обележава се X/E. Дакле,*

$$X/E = \{[x]_E \mid x \in X\}.$$

Класе еквиваленције се у литератури и другачије означавају. На пример, уместо $[x]_E$ пише се и x/E, или C_x у случајевима када је јасно о којој релацији еквиваленције је реч.

Пример 48. Одредимо класе еквиваленције релације из примера 47.



$$[0]_E = \{0\}, [1]_E = [2]_E = \{1, 2\}, [3]_E = [4]_E = [5]_E = \{3, 4, 5\}.$$

Количнички скуп је

$$\{0, 1, 2, 3, 4, 5\}/E = \{[0]_E, [1]_E, [2]_E, [3]_E, [4]_E, [5]_E\} = \{\{0\}, \{1, 2\}, \{3, 4, 5\}\}$$

Очигледно да је класама еквиваленције скуп $\{0, 1, 2, 3, 4, 5\}$ **разбијен** на непразне дисјунктне подскупове чија је унија наведени скуп.

Класе еквиваленције једнакости су једночлани скупови.

Теорема 22. *Нека је $E \subseteq X \times X$ релација еквиваленције.*

1. *За свако $x \in X$, $x \in [x]_E$, па је самим тим $[x]_E \neq \emptyset$.*
2. *За све $x, y \in X$ важи $(x, y) \in E$ акко $[x]_E = [y]_E$.*
3. *За све $x, y \in X$ важи $[x]_E \neq [y]_E$ акко $[x]_E \cap [y]_E = \emptyset$.*
4. *$X = \bigcup X/E = \bigcup_{x \in X} [x]_E$.*

Доказ. 1. Тврђење следи директно из дефиниције класе еквиваленције и чињенице да је релација еквиваленције рефлексивна.

2. ($\Rightarrow$) Претпоставимо да $(x, y) \in E$. Треба доказати да је $[x]_E = [y]_E$.

Ако $z \in [x]_E$, онда $(x, z) \in E$. Због симетричности релације E, из $(x, y) \in E$ следи да $(y, x) \in E$. Како је E транзитивна релација из $(y, x) \in E$ и $(x, z) \in E$ следи $(y, z) \in E$, тј. $z \in [y]_E$. Дакле, $[x]_E \subseteq [y]_E$. Обрнута инклузија се доказује на исти начин.

($\Leftarrow$) Претпоставимо да је $[x]_E = [y]_E$. Због рефлексивности релације E имамо да $y \in [y]_E$, па $y \in [x]_E$ што значи да $(x, y) \in E$.

3. ($\Rightarrow$) Нека је $[x]_E \neq [y]_E$, тј. $(x, y) \notin E$ (према тврђењу под 2). Треба доказати да је $[x]_E \cap [y]_E = \emptyset$. Претпоставимо супротно, да је $[x]_E \cap [y]_E \neq \emptyset$, тј. да постоји z такав да је $z \in [x]_E \cap [y]_E$. Тада $z \in [x]_E$ и $z \in [y]_E$, тј. $(x, z) \in E$ и $(y, z) \in E$. Због симетричности релације E имамо да $(z, y) \in E$. Узимајући у обзир транзитивност релације E из $(x, z) \in E$ и $(z, y) \in E$ закључујемо да $(x, y) \in E$ што је супротно полазној претпоставци.

($\Leftarrow$) Претпоставимо да је $[x]_E \cap [y]_E = \emptyset$. Ако би било $[x]_E = [y]_E$, имали бисмо да је $[x]_E = [y]_E = [x]_E \cap [y]_E = \emptyset$, што је немогуће према тврђењу под 1. Дакле, $[x]_E \neq [y]_E$. □

Дефиниција 18. *Ако је E релација еквиваленције скупа X, функција $k : X \to X/E$, дефинисана са $k(x) = [x]_E$ назива се количничко (фактор) пресликавање.*

Задатак **9.** Ако $f : X \to Y$, доказати да је

$$\ker(f) = \{(x_1, x_2) \in X \times X \mid f(x_1) = f(x_2)\}$$

релација еквиваленције скупа X; ова релација се назива *језгро* функције f.

Пројекције

За било које скупове A и B, функције

- $\pi_A : A \times B \to A$, $\pi_A(x, y) = x$ и
- $\pi_B : A \times B \to B$, $\pi_B(x, y) = y$,

називају се *пројекције*. Пројекције су увек на функције.

Бинарне операције

Ако је S неки скуп, свака функција из $S \times S$ у S назива се *бинарна операција* скупа S.

14

Пример 49. Бинарну операцију $* : \{0,1,2\} \times \{0,1,2\} \to \{0,1,2\}$ скупа $\{0,1,2\}$ дату са

$$* = \begin{pmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) & (2,0) & (2,1) & (2,2) \\ 0 & 0 & 1 & 1 & 2 & 0 & 0 & 2 & 1 \end{pmatrix}$$

представљамо и тзв. Кејлијевом таблицом.

$*$	0	1	2
0	0	0	1
1	1	2	0
2	0	2	1

Уобичајено је да се уместо $*(x,y)$ пише $x * y$. Када год је задата нека бинарна операција на скупу,

• рачунамо вредности израза: на пример, $(0 * 1) * ((2 * 2) * 1) = 0 * (0 * 1) = 0 * 0 = 0$;

• решавамо једначине: на пример, решења једначине $x * 1 = 2$ су 1 и 2 ($x = 1$ или $x = 2$);

• трагамо за законима које задовољава дата операција: на приме, за сваки $x \in \{0,1,2\}$ важи: $(x * x) * x = ((x * x) * x) * x$.

Уобичајено је да се бинарне операције означавају разним специјалним симболима $+$, $\cdot$, $*$, $\star$, $\oplus$ итд, као и да се користи тзв. *инфиксна нотација* – ознаку операције наводимо између аргумената (за разлику од префиксне нотације где се ознака операције наводи испред аргумената).

Дефиниција 19. *Операција $* : S \times S \to S$ је:*

- ***комутативна** ако за све $x, y \in S$ важи $x * y = y * x$;*
- ***асоцијативна** ако за све $x, y, z \in S$ важи $x * (y * z) = (x * y) * z$.*

Гробо говорећи, комутативност неке операције значи да било која два аргумента смеју да замене места, а да се резултат не промени. Асоцијативност дозвољава изостављање заграда: уместо $x * (y * z)$ и $(x * y) * z$ пишемо $x * y * z$, јер је свеједно како су заграде постављене. Наравно, запис $x * y * z$ је недопустив уколико операција $*$ није асоцијативна.

Пример 50. Операција $* : \{0,1,2\} \times \{0,1,2\} \to \{0,1,2\}$ дефинисана у претходном примеру није комутативна, јер је, на пример, $0 * 1 = 0$ и $1 * 0 = 1$. Није ни асоцијативна, јер је, на пример, $1 * (1 * 2) = 1 * 0 = 1$ и $(1 * 1) * 2 = 2 * 2 = 0$.

Операција $\star : \{0,1,2\} \times \{0,1,2\} \to \{0,1,2\}$ дата Кејлијевом таблицом:

$\star$	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

јесте комутативна (што се једноставно уочава, јер је таблица симетрична у односу на главну дијагоналу), али није асоцијативна: $0 \star (1 \star 2) = 0 \star 2 = 1$ и $(0 \star 1) \star 2 = 1 \star 2 = 2$.

Пример 51. Наредним таблицама уводимо две важне бинарне операције скупа $\{0, 1\}$:

$+_2$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Операција $+_2$ се назива *сабирање по модулу* 2, а $\cdot$ *множење* (по модулу 2). Обе операције су комутатвне и обе су асоцијативне. У асоцијативност се једноставно можемо уверити директном провером свих могућих случајева. На пример, асоцијативност операције $+_2$ потврђују резултати приказани у наредној табели:

x	y	z	$y +_2 z$	$x +_2 (y +_2 z)$	$x +_2 y$	$(x +_2 y) +_2 z$
0	0	0	0	**0**	0	**0**
0	0	1	1	**1**	0	**1**
0	1	0	1	**1**	1	**1**
0	1	1	0	**0**	1	**0**
1	0	0	0	**1**	1	**1**
1	0	1	1	**0**	1	**0**
1	1	0	1	**0**	0	**0**
1	1	1	0	**1**	0	**1**

Пример 52. Ако је S било који скуп, на скупу $\mathcal{P}(S)$ природно је посматрати операције пресека, уније и разлике, јер за све $X, Y \in \mathcal{P}(S)$, скупови $X \cap Y$, $X \cup Y$ и $X \setminus Y$ такође припадају $\mathcal{P}(S)$. Зато унију, пресек и разлику можемо посматрати и као операције (било ког) партитивног скупа $\mathcal{P}(S)$, и писати $\cup, \cap, \setminus : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$. Слично томе, и комплемент у односу на скуп S јесте функција из $\mathcal{P}(S)$ у себе $\complement : \mathcal{P}(S) \to \mathcal{P}(S)$.

Скуп свих функција из A у B, у ознаци B^A добијамо издвајањем из скупа $\mathcal{P}(A \times B)$ оних релација између A и B које су функције.

Пример 53. Ако је S било који скуп, композиција две функције из S^S такође је функција из S^S, па самим тим композиција представља једну бинарну релацију скупа S^S, тј. $\circ : S^S \times S^S \to S^S$.

Специјално, за $S = \{0, 1\}$, скуп S^S садржи следеће елементе:

$$\mathrm{id}_S = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad f = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad h = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

а операцији композиције одговара следећа Кејлијева таблица:

$\circ$	id_S	f	g	h
id_S	id_S	f	g	h
f	f	f	f	f
g	g	h	id_S	f
h	h	h	h	h

За било који скуп S, операција $\circ$ на S^S је асоцијативна, што директно следи из теореме 18 (3). Да композиција, у општем случају, није комутативна, једноставно уочавамо из претходне таблице ($f \circ g \neq g \circ f$).

Карактеристичне функције

Ако је S било који скуп, функције из S у двочлани скуп $\{0,1\}$ представљају својеврсне репрезентације подскупова од S. Наиме, било који подскуп $A \subseteq S$ репрезентује његова *карактеристична функција* $\chi_A : S \to \{0,1\}$,

$$\chi_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

Ако 1 схватимо као 'да' и 0 као 'не', онда вредност $\chi_A(x)$ представља одговор на питање да ли x припада A.

Пример 54. Ако је $S = \{0,1,2,3,4\}$, онда је:

$$\chi_{\{0,2,4\}} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \ \chi_\emptyset = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ итд.}$$

Свака функција $f : S \to \{0,1\}$ одређује један подскуп скупа S чија је карактеристична функција управо f; реч је о подскупу $\{x \in S \mid f(x) = 1\}$.

Посебно, свака бинарна релација скупа S, $R \subseteq S \times S$ може се посматрати и као функција $\chi_R : S \times S \to \{0,1\}$.

Како за сваки $A \subseteq S$ важи $(\forall x \in S)(x \in A \Leftrightarrow \chi_A(x) = 1)$, закључујемо да су подскупови $A_1, A_2 \subseteq S$ једнаки ако и само ако $(\forall x \in S)(\chi_{A_1}(x) = \chi_{A_2}(x))$. Ово запажање може бити веома корисно приликом доказивања скуповних идентитета, што је илустровано у следећем примеру.

Пример 55. Симетрична разлика скупова A и B јесте скуп $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Докажимо да за било која три скупа A, B, C важи $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

Нека је $S = A \cup B \cup C$. Није тешко уочити да за било које $X, Y \subseteq S$, и све $x \in S$ важи $\chi_{X \triangle Y}(x) = \chi_X(x) +_2 \chi_Y(x)$. Како је $A, B, C \subseteq S$

и $+_2$ асоцијативна операција имамо да за све $x \in S$ важи:

$$\begin{aligned}\chi_{A\triangle(B\triangle C)}(x) &= \chi_A(x) +_2 \chi_{B\triangle C}(x)\\ &= \chi_A(x) +_2 (\chi_B(x) +_2 \chi_C(x))\\ &= (\chi_A(x) +_2 \chi_B(x)) +_2 \chi_C(x)\\ &= \chi_{A\triangle B}(x) +_2 \chi_C(x)\\ &= \chi_{(A\triangle B)\triangle C}(x),\end{aligned}$$

одакле следи жељена једнакост.

Празна функција (из празног скупа у неки скуп)

Функције из празног и у празан скуп

Очигледно је да не постоје функције из (било ког) непразног скупа у празан скуп. Заиста, ако је $f \subseteq X \times \emptyset$, из $X \times \emptyset = \emptyset$ закључујемо да је и $f = \emptyset$, а једноставно можемо показати $\emptyset \neq X \overset{\text{не постоји}}{\longrightarrow} \emptyset$

$$\neg(\forall x \in X)(\exists! y \in \emptyset)\,(x, y) \in \emptyset.$$

Да ли постоје функције из празног скупа у неки непразан скуп? Ако је X било који скуп, тада је $\emptyset \times X = \emptyset$, и једини подскуп од $\emptyset \times X$ јесте празан скуп. Како је $\emptyset \subseteq \emptyset \times X$, питамо се да ли $\emptyset$ можемо сматрати функцијом из $\emptyset$ у X. Одговор је потврдан уколико можемо да докажемо

$(*)$ $\quad (\forall x \in \emptyset)(\exists! y \in X)\,(x, y) \in \emptyset$ тј. $\forall x(x \in \emptyset \Rightarrow (\exists! y \in X)\,(x, y) \in \emptyset)$.

Из $\forall x\,(x \notin \emptyset)$ следи да се $(*)$ може доказати, тј. $\emptyset$ јесте, и то једина, функција из $\emptyset$ у X. Штавише, $\emptyset : \emptyset \overset{1-1}{\to} X$, што се једноставно доказује истим аргументима као раније. Међутим, ако је $X \neq \emptyset$, онда 'празна функција' $\emptyset$ није на функција, јер се за (било који) елемент y из X не може пронаћи елемент x у $\emptyset$ (јер празан скуп уопште нема елемената) такав да $(x, y) \in \emptyset$. Али, ако је $X = \emptyset$, онда тривијално следи да је 'празна функција' и на функција, тј. $\emptyset : \emptyset \overset{1-1}{\underset{\text{на}}{\to}} \emptyset$. $\emptyset \overset{\emptyset}{\longrightarrow} X$

Директне и индиректне слике

Било која функција $f : X \to Y$, одређује две нове функције:

- једну из $\mathcal{P}(X)$ у $\mathcal{P}(Y)$, за коју користимо исту ознаку f, али аргумент (подскуп од X) наводимо у угластим заградама:

$$f[A] = \{y \in Y \mid (\exists a \in A) f(a) = y\}, \text{ за } A \subseteq X.$$

- другу из $\mathcal{P}(Y)$ у $\mathcal{P}(X)$, за коју користимо ознаку f^{-1} (која у овом контексту нема никакве везе са појмом инверзне функције), а аргумент (подскуп од Y) наводимо у угластим заградама:

$$f^{-1}[B] = \{x \in X \mid f(x) \in B\}, \text{ за } B \subseteq Y.$$

Скуп $f[A] = \{y \in Y \mid (\exists a \in A) f(a) = y\} \subseteq Y$ називамо **директна слика** скупа $A \subseteq X$; $f[A]$ је подскуп од Y који садржи само оне елементе који су f-слике елемената из A. Будући да су сви елементи скупа $f[A]$ облика $f(a)$, $a \in A$, пишемо и $f[A] = \{f(a) \mid a \in A\}$.

Скуп $f^{-1}[B] = \{x \in X \mid f(x) \in B\} \subseteq X$ називамо **индиректна слика** скупа $B \subseteq Y$; $f^{-1}[B]$ је подскуп од X који садржи само оне елементе из X чије f-слике припадају скупу B.

Пример 56. Нека $f : \{0,1,2\} \to \{a,b,c\}$:

$$f = \begin{pmatrix} 0 & 1 & 2 \\ b & a & a \end{pmatrix}.$$

Одредимо директне слике свих подскупова домена:
$f[\emptyset] = \emptyset,\ f[\{0\}] = \{b\},\ f[\{1\}] = \{a\},\ f[\{2\}] = \{a\},$
$f[\{0,1\}] = \{a,b\},\ f[\{1,2\}] = \{a\},\ f[\{0,2\}] = \{a,b\},\ f[\{0,1,2\}] = \{a,b\}$. Одредимо и индиректне слике свих подскупова кодомена:
$f^{-1}[\emptyset] = \emptyset,\ f^{-1}[\{a\}] = \{1,2\},\ f^{-1}[\{b\}] = \{0\},\ f^{-1}[\{c\}] = \emptyset,$
$f^{-1}[\{a,b\}] = \{0,1,2\},\ f^{-1}[\{a,c\}] = \{1,2\},\ f^{-1}[\{b,c\}] = \{0\},$
$f^{-1}[\{a,b,c\}] = \{0,1,2\}$.

Посебно наглашавамо да се, на пример, $f^{-1}[\{a\}]$ битно разликује од записа $f^{-1}(a)$, који у овом случају нема смисла јер f није бијекција.

Теорема 23. *Нека $f : X \to Y$. За произвољне скупове $A, A_1, A_2 \subseteq X$ и $B, B_1, B_2 \subseteq Y$ важи:*

(1) $A \subseteq f^{-1}[f[A]]$; *(2)* $f[f^{-1}[B]] \subseteq B$;
(3) $A_1 \subseteq A_2 \Rightarrow f[A_1] \subseteq f[A_2]$; *(4)* $B_1 \subseteq B_2 \Rightarrow f^{-1}[B_1] \subseteq f^{-1}[B_2]$;
(5) $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$; *(6)* $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$;
(7) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$; *(8)* $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$.

Доказ. (1) Ако $x \in A$, онда је очигледно $f(x) \in f[A]$. Како је $f(x) \in f[A]$ еквивалентно са $x \in f^{-1}[f[A]]$, непосредно изводимо жељени закључак.
(2) Ако $y \in f[f^{-1}[B]]$, онда је $y = f(x)$, за неко $x \in f^{-1}[B]$. Како је $x \in f^{-1}[B]$ еквивалентно са $f(x) \in B$, закључујемо $y = f(x) \in B$.
(3) Нека је $A_1 \subseteq A_2$. Претпоставимо да $y \in f[A_1]$. Тада је $y = f(x)$, за неко $x \in A_1$. Будући да је $A_1 \subseteq A_2$, из $y = f(x)$ и $x \in A_1 \subseteq A_2$ закључујемо да $y \in f[A_2]$.
(4) Нека је $B_1 \subseteq B_2$. Претпоставимо да $x \in f^{-1}[B_1]$, одн. $f(x) \in B_1$. Из $f(x) \in B_1 \subseteq B_2$, закључујемо да $x \in f^{-1}[B_2]$.
(5) Ова инклузија директно следи из (3). Како је $A_1 \cap A_2 \subseteq A_1$ и $A_1 \cap A_2 \subseteq A_2$, према (3) следи $f[A_1 \cap A_2] \subseteq f[A_1]$ и $f[A_1 \cap A_2] \subseteq f[A_2]$, а одавде и $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$.
(6) Инклузију $f^{-1}[B_1 \cap B_2] \subseteq f^{-1}[B_1] \cap f^{-1}[B_2]$ директно добијамо из (4). Докажимо да је и $f^{-1}[B_1 \cap B_2] \supseteq f^{-1}[B_1] \cap f^{-1}[B_2]$. Ако $x \in f^{-1}[B_1] \cap f^{-1}[B_2]$, онда $x \in f^{-1}[B_1]$ и $x \in f^{-1}[B_2]$, одн. $f(x) \in B_1$ и $f(x) \in B_2$. Дакле, $f(x) \in B_1 \cap B_2$, што је еквивалентно са $x \in f^{-1}[B_1 \cap B_2]$.

(7) Једнакост доказује следећи еквиваленцијски ланац:

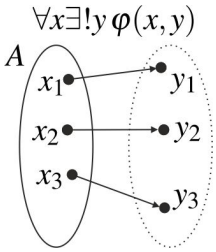
$$\begin{aligned} y \in f[A_1 \cup A_2] &\Leftrightarrow \exists x(x \in A_1 \cup A_2 \wedge y = f(x)) \\ &\Leftrightarrow \exists x((x \in A_1 \vee x \in A_2) \wedge y = f(x)) \\ &\Leftrightarrow \exists x((x \in A_1 \wedge y = f(x)) \vee (x \in A_2 \wedge y = f(x)) \\ &\Leftrightarrow \exists x(x \in A_1 \wedge y = f(x)) \vee \exists x(x \in A_2 \wedge y = f(x)) \\ &\Leftrightarrow y \in f[A_1] \vee y \in f[A_2] \\ &\Leftrightarrow y \in f[A_1] \cup f[A_2] \end{aligned}$$

(8) Једнакост доказује следећи еквиваленцијски ланац:

$$\begin{aligned} x \in f^{-1}[B_1 \cup B_2] &\Leftrightarrow f(x) \in B_1 \cup B_2 \\ &\Leftrightarrow f(x) \in B_1 \vee f(x) \in B_2 \\ &\Leftrightarrow x \in f^{-1}[B_1] \vee x \in f^{-1}[B_2] \\ &\Leftrightarrow x \in f^{-1}[B_1] \cup f^{-1}[B_2]. \end{aligned}$$

4.4. **Аксиоме: замене, регуларности и бесконачности** 15

▼ Аксиома замене



Важан метод дефинисања функција омогућава нам нова аксиома –аксиома замене. Пре него што је наведемо, описаћемо ситуације у којима је користимо. Претпоставимо да смо, за неку формулу $\varphi(x,y)$, доказали $\forall x\exists!y\varphi(x,y)$. Ако је A било који скуп, тада мора да важи и $\forall x \in A\exists!y\varphi(x,y)$, што значи да за сваки x из A постоји јединствен y за који је $\varphi(x,y)$. Све ово указује на могућност да се формулом φ дефинише једна функција са доменом A. Међутим, да би на овај начин била дефинисана функција, неопходно је да знамо у ком скупу се налазе те јединствене 'слике' елемената из A. Аксиома замене нас ослобађа сваке бриге по овом питању, јер тврди да за сваку формулу $\varphi(x,y)$ за коју се може утврдити $\forall x\exists!y\varphi(x,y)$ и сваки скуп A постоји скуп који садржи само оне скупове y за које $\exists x \in A\varphi(x,y)$.

Аксиома замене
$\forall x\exists!y\varphi(x,y) \Rightarrow \forall A\exists B\forall y(y \in B \Leftrightarrow \exists x(x \in A \wedge \varphi(x,y)))$

▼ Аксиома регуларности

Аксиомом регуларности се тврди да сваки непразан скуп садржи елемент са којим нема заједничких елемената.

Аксиома регуларности
$\forall X(X \neq \emptyset \Rightarrow \exists x(x \in X \wedge x \cap X = \emptyset))$

Теорема 24. *(1) Не постоји скуп x такав да $x \in x$.*
(2) Не постоје скупови x и y такви да $x \in y \in x$.

Доказ. (1) Ако би постојао скуп x такав да $x \in x$, онда скуп $\{x\}$ не би садржао елемент са којим нема заједничких елемената, јер $x \in x \cap \{x\}$, што је супротно аксиоми регуларности.
(2) Претпоставимо да постоје скупови x и y такви да је $x \in y \in x$, тј. $x \in y$ и $y \in x$. Тада, супротно аксиоми регуларности, скуп $\{x,y\}$ не садржи елемент са којим нема заједничких елемената: $x \cap \{x,y\} \neq \emptyset$, јер $y \in x \cap \{x,y\}$, и $y \cap \{x,y\} \neq \emptyset$, јер $x \in y \cap \{x,y\}$. □

Теорема 25. *За било које скупове x и y, из $x \cup \{x\} = y \cup \{y\}$ следи $x = y$.*

Доказ. Нека је $x \cup \{x\} = y \cup \{y\}$. Претпоставимо супротно ономе што треба доказати да је $x \neq y$. Како $x \in y \cup \{y\}$ и $x \neq y$, закључујемо да $x \in y$. Слично томе, из $y \in x \cup \{x\}$ и $x \neq y$ следи $y \in x$. Међутим, није могуће да $x \in y$ и $y \in x$, према претходној теореми (2). Дакле, $x = y$. □

Скуп $x \cup \{x\}$ називамо *следбеником* скупа x и обележавамо га x'. Полазећи од празног скупа, редом уводимо *следбенике* добијених

скупова које из разумљивих разлога можемо идентификовати са природним бројевима:

$$\begin{aligned} 0 = \emptyset \quad & 1 = 0' = \emptyset \cup \{\emptyset\} = \{0\} \\ & 2 = 1' = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} \\ & 3 = 2' = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\} \\ & 4 = 3' = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\} \\ & \dots \end{aligned}$$

Интуитивно је јасно да генерисање нових скупова на описани начин неограничено можемо продужавати – за сваки добијени скуп, поступак можемо наставити увођењем његовог следбеника. Наредна аксиома заправо тврди да постоји скуп у коме ће се наћи сви скупови који се могу добити на описани начин. Будући да је описани поступак веома близак *бројању*, наредна аксиома ће бити кључна за увођење скупа природних бројева.

▼ Аксиома бесконачности. Скуп природних бројева

Аксиома бесконачности
Постоји скуп који садржи 0 и следбеника сваког свог елемента.

$$\exists I(0 \in I \wedge \forall x(x \in I \Rightarrow x \cup \{x\} \in I))$$

Према аксиоми замене, за сваки скуп A постоји скуп B који садржи све следбенике елемената из A, па се природно дефинише функција $' : A \to B$, која је заправо 1-1 функција према претходној теореми (што је последица аксиоме регуларности). Скуп B можемо означити и са $[A]'$, где је $[A]' = \{a' \mid a \in A\}$. Аксиома бесконачности заправо тврди да постоји бар један скуп I који садржи 0 и важи $[I]' \subseteq I$.

Сваки скуп који садржи 0 и следбеника сваког свог елемента називамо **индуктивним скупом**. Аксиомом бесконачности се тврди да постоји бар један индуктиван скуп. Не можемо тврдити да постоји јединствен индуктиван скуп, али колико год да их има сви садрже као подскуп један исти индуктиван скуп, тзв. *најмањи индуктиван скуп*.

Ако је I неки индуктиван скуп, означимо са $\mathcal{I}(I)$ скуп свих индуктивних подскупова од I:

$$\begin{aligned} \mathcal{I}(I) &= \{X \mid X \subseteq I \wedge \text{ '}X \text{ је индуктиван'}\} \\ &= \{X \mid X \subseteq I \wedge 0 \in X \wedge \forall x(x \in X \Rightarrow x' \in X)\}. \end{aligned}$$

Нека је $\omega \stackrel{\text{def}}{=} \bigcap \mathcal{I}(I)$. Доказаћемо да је ω индуктиван скуп и то најмањи у следећем смислу: ако је S индуктиван и $S \subseteq \omega$, онда је $S = \omega$, односно не постоји строги подскуп од ω који је индуктиван, што ћемо у наставку показати.

Теорема 26. *(1) ω је индуктиван скуп.*
(2) Ако је $S \subseteq \omega$ и важи:

(BI) $0 \in S$,

(IK) *ако $x \in S$, онда $x' \in S$,*

онда је $S = \omega$

Доказ. (1) Будући да $0 \in X$, за сваки $X \in \mathcal{I}(I)$, следи да $0 \in \bigcap \mathcal{I}(I) = \omega$.

Остаје још да се покаже да ω садржи следбеника сваког свог елемента. Нека је $x \in \omega$ произвољан. Из $x \in \omega = \bigcap \mathcal{I}(I)$, следи да

$x \in X$, за сваки $X \in \mathcal{I}(I)$. Како је сваки $X \in \mathcal{I}(I)$ индуктиван, сваки од њих садржи и x'. Дакле, $x \in \bigcap \mathcal{I}(I) = \omega$.
(2) Нека је $S \subseteq \omega$ такав да важе услови (BI) и (IK) – значи S је индуктиван подскуп од ω. Како је $\omega \subseteq I$, скуп S је и индуктиван подскуп од I, тј. $S \in \mathcal{I}(I)$, па је $\bigcap \mathcal{I}(I) \subseteq S$, тј. $\omega \subseteq S$, одакле следи да је $S = \omega$. □

Остаје још да покажемо да за било који (други) индуктиван скуп I_1 важи $\omega \subseteq I_1$, или еквивалентно $\omega \cap I_1 = \omega$. Очигледно је $\omega \cap I_1 \subseteq \omega$. Једноставно је уверити се да скуп $\omega \cap I_1$ задовољава услове (BI) и (IK), па према претходној теореми (2) мора важити $\omega \cap I_1 = \omega$. Одавде непосредно закључујемо и да је $\omega = \bigcap \mathcal{I}(I_1)$. Скуп ω заузима веома значајно место у математици – скуп ω називамо **скупом природних бројева** и обележавамо га и $\mathbb{N}$. Будући да је ова друга ознака много уобичајенија, углавном ћемо њу користити у наставку. Знамо да $\mathbb{N}$ садржи 0, 1, 2, 3, 4, итд. и да функција *следбеник* $' : \mathbb{N} \to \mathbb{N}$ има следеће особине:

- за свако $n \in \mathbb{N}$, $n' \neq 0$ (следбеник није на функција);
- за све $m, n \in \mathbb{N}$, из $m' = n'$ следи $m = n$ (следбеник јесте 1-1 функција).

Основно својство скупа природних бројева изражено је особином (2) теореме 26 – **принципом математичке индукције**. Неколико начина примене овог принципа илуструјемо доказивањем следећих важних тврђења.

Принцип математичке индукције користимо за доказивање формула облика $(\forall n \in \mathbb{N})\,\varphi(n)$. Доказ изводимо тако што формирамо скуп $S = \{n \in \mathbb{N} \mid \varphi(n)\}$ и настојимо да докажемо:

(**BI**) *базу индукције*, тј. да $0 \in S$ и

(**IK**) *индуктивни корак*, тј. да из $n \in S$ следи $n' \in S$. Пошто у индуктивном кораку треба доказати импликацију, претпостављамо $n \in S$, што се назива *индуктивна претпоставка* и настојимо да докажемо $n' \in S$.

Теорема 27. *(1) За све природне бројеве m, n важи $m \in n \Rightarrow m \subseteq n$.*
(2) За све природне бројеве m, n важи $m \in n \Leftrightarrow m \subset n$.
(3) За све природне бројеве m, n важи $m \in n \vee m = n \vee n \in m$.

Доказ. (⋆) (1) Да бисмо доказали

$$(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n),$$

формирамо скуп

$$S = \{n \in \mathbb{N} \mid (\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n)\}$$

и доказујемо да је $S = \mathbb{N}$, применом принципа математичке индукције.

Доказ применом принципа математичке индукције можемо скратити тако што не формирамо скуп S већ доказујемо формуле:

(**BI**) $\varphi(n/0)$

(**IK**) $(\forall n \in \mathbb{N})(\varphi(n) \Rightarrow \varphi(n/n'))$.

(**BI**) Докажимо да $0 \in S$, тј. $(\forall m \in \mathbb{N})(m \in 0 \Rightarrow m \subseteq 0)$. Како је $0 = \emptyset$ и знамо да за свако m важи $m \notin 0$, онда се из претпоставке $m \in 0$ изводи било шта ($\bot_{\mathrm{E}}$), па и $m \subseteq 0$. Дакле, $0 \in S$.
(**IK**) Претпоставимо да $n \in S$, тј.

$$(\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n). \tag{IP}$$

Треба да докажемо $n' \in S$, тј. $(\forall m \in \mathbb{N})(m \in n' \Rightarrow m \subseteq n')$. Из $m \in n' = n \cup \{n\}$ следи да $m \in n$ или $m = n$. У случају да је $m \in n$,

према (IP) закључујемо $m \subseteq n$, па је $m \subseteq n \cup \{n\} = n'$. У случају $m = n$, непосредно закључујемо да $m = n \subseteq n'$.

Дакле, $S = \mathbb{N}$.

(2) И у овом случају користимо принцип математичке индукције, али ћемо поступити мало другачије у односу на доказ тврђења (1).

Нека је m произвољан природан број и

$$S_m = \{n \in \mathbb{N} \mid m \in n \Leftrightarrow m \subset n\}.$$

Доказаћемо да је $S_m = \mathbb{N}$.

(**BI**) Знамо да $m \notin 0$ и $m \not\subset 0$ (празан скуп нема праве подскупове), одакле једноставно изводимо $m \in 0 \Leftrightarrow m \subset 0$. Дакле, $0 \in S_m$.

(**IK**) Претпоставимо да $n \in S_m$, тј. (IP) $m \in n \Leftrightarrow m \subset n$.

Докажимо $m \in n' \Leftrightarrow m \subset n'$.

Ако $m \in n' = n \cup \{n\}$, онда $m \in n$ или $m = n$. У случају да $m \in n$, према (IP) следи $m \subset n$, а тиме и $m \subset n'$, јер је $n \subset n'$. У случају да је $m = n$, онда је очигледно $m \subset n'$.

Нека је $m \subset n' = n \cup \{n\}$. Докажимо најпре да $n \notin m$. Ако би било $n \in m$, имали бисмо $\{n\} \subseteq m$ и, према (1), $n \subseteq m$, одакле следи $n' = n \cup \{n\} \subseteq m \subset n'$, што је немогуће. Дакле, $n \notin m$, па из $m \subset n \cup \{n\}$, следи $m \subseteq n$, тј. $m \subset n$ или $m = n$. У случају да је $m \subset n$, према (IP) закључујемо да $m \in n$, а самим тим и $m \in n'$. У случају да је $m = n$, директно добијамо $m = n \in n'$.

Дакле, $S_m = \mathbb{N}$ за сваки природан број m, одакле следи жељено тврђење.

(3) Нека је $S = \{m \in \mathbb{N} \mid (\forall n \in \mathbb{N})(m \in n \vee m = n \vee n \in m)\}$.

(**BI**) Докажимо $(\forall n \in \mathbb{N})(0 \in n \vee 0 = n \vee n \in 0)$.

Очигледно је да за било које $n \in \mathbb{N}$ важи $n = 0$ или $n \neq 0$. У случају да је $n = 0$, директно изводимо $0 \in n \vee 0 = n \vee n \in 0$. Уколико је $n \neq 0$, тада је $\emptyset = 0 \subset n$, па према тврђењу (2) закључујемо $0 \in n$, а тиме и $0 \in n \vee 0 = n \vee n \in 0$. Дакле, $0 \in S$.

(**IK**) Претпоставимо да $m \in S$, тј. (IP) $(\forall n \in \mathbb{N})(m \in n \vee m = n \vee n \in m)$.

Да бисмо доказали

$$(*) \qquad (\forall n \in \mathbb{N})(m' \in n \vee m' = n \vee n \in m'),$$

изаберимо произвољан $n \in \mathbb{N}$. Тада према (IP) важи $m \in n \vee m = n \vee n \in m$. Разликујемо три случаја.

1. случај: $m \in n$. Тада је, према (2), $m \subset n$, па је $m' = m \cup \{m\} \subseteq n$. Уколико је $m' \subset n$, онда, поново према (2), важи $m' \in n$, па самим тим важи $(*)$. Формула $(*)$ свакако важи и уколико је $m' = n$.

2. случај: $m = n$. Тврђење $(*)$ важи јер $n \in n' = m'$.

3. случај: $n \in m$. Непосредно добијамо $n \in m'$, па важи $(*)$. □

Уколико треба доказати формулу облика

$$(\Phi) \qquad (\forall m \in \mathbb{N})(\forall n \in \mathbb{N})\varphi(m, n),$$

због еквивалентности ове формуле са $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})\varphi(m, n)$, можемо поступити двојако:

1) За произвољно изабран $m \in \mathbb{N}$, формирамо скуп $S_m = \{n \in \mathbb{N} \mid \varphi(m, n)\}$ и индукцијом доказујемо $S_m = \mathbb{N}$. Када успемо, закључујемо $(\forall m \in \mathbb{N})\, S_m = \mathbb{N}$.

2) За произвољно изабран $n \in \mathbb{N}$, формирамо скуп $S_n = \{m \in \mathbb{N} \mid \varphi(m, n)\}$ и индукцијом доказујемо $S_n = \mathbb{N}$. Када успемо, закључујемо $(\forall n \in \mathbb{N})\, S_n = \mathbb{N}$.

У сваком од наведених случајева непосредно следи (Φ). У првом случају (Φ) доказујемо *индукцијом по n при фиксираном m*, а у другом случају *индукцијом по m при фиксираном n*.

Уколико треба доказати формулу облика

$$(\Phi) \qquad (\forall m \in \mathbb{N})(\forall n \in \mathbb{N})\varphi(m, n),$$

због еквивалентности ове формуле са $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})\varphi(m, n)$, можемо формирати скуп:

1) $S = \{n \in \mathbb{N} \mid (\forall m \in \mathbb{N})\varphi(m, n)\}$ или

2) $S = \{m \in \mathbb{N} \mid (\forall n \in \mathbb{N})\varphi(m, n)\}$

и доказати $S = \mathbb{N}$. Ако S дефинишемо на први (одн. други) начин, каже се да формулу Φ доказујемо *индукцијом по m* (одн. *индукцијом по n*). На који начин ћемо поступити углавном се опредељујемо према формули $\varphi(m, n)$.

▼ Уређење и аритметичке операције скупа $\mathbb{N}$

16

Скуп који садржи елементе свих својих елемената назива се **транзитиван** скуп. Другим речима T је тразитиван ако важи $(\forall x \in T)\forall t(t \in x \Rightarrow t \in T)$. Ова формула је еквивалентна формули $\forall x(x \in T \Rightarrow x \subseteq T)$, односно $(\forall x \in T)\, x \subseteq T$ или $\bigcup T \subseteq T$. Према претходној теореми (1), сваки природан број је транзитиван. Очигледно је и $\mathbb{N}$ транзитиван скуп.

Претходна теорема показује да припадање ($\in$), односно строга инклузија ($\subset$) на уобичајени начин уређује скуп природних бројева:

$$0 \in 1 \in 2 \in 3 \in 4 \in 5 \cdots, \quad \text{односно} \quad 0 \subset 1 \subset 2 \subset 3 \subset 4 \subset 5 \cdots$$

Заиста, знамо да:

- за сваки природан број n важи $n \notin n$ (ово је последица аксиоме регуларности – теорема 24 (1), али се може извести и без ове аксиоме, као последица претходне теореме (2));
- за све природне бројеве k, m, n, ако $k \in m$ и $m \in n$, онда $k \in n$ (ово је директна последица претходне теореме (2)).

Дакле, бинарна релација $\{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m \in n\}$ јесте *строго уређење скупа природних бројева* и обележава се $<$. Релацију $\leqslant$, тзв. *уређење* скупа $\mathbb{N}$ уводимо на следећи начин:

$$m \leqslant n \overset{\text{def}}{\Leftrightarrow} m < n \vee m = n.$$

Наравно, $\leqslant$ наслеђује основна својства инклузије $\subseteq$. За све $k, m, n \in \mathbb{N}$:

- $n \leqslant n$;
- $m \leqslant n \wedge n \leqslant m \Rightarrow m = n$;
- $k \leqslant m \wedge m \leqslant n \Rightarrow k \leqslant n$.

Последица 3. *За све природне бројеве m, n важи*
(1) $m \leqslant n \Leftrightarrow m \subseteq n$;
(2) $m \leqslant n \vee n \leqslant m$; (поредак $\leqslant$ је линеаран)
(3) $m < n \Leftrightarrow m' \leqslant n$;
(4) $m < n' \Leftrightarrow m \leqslant n$;
(5) $m < n \Leftrightarrow m' < n'$ (функција следбеник је монотона).

Доказ. (1) Према претходној теореми (2) имао да је:

$$m \leqslant n \;\Leftrightarrow\; m < n \vee m = n \;\Leftrightarrow\; m \subset n \wedge m = n \;\Leftrightarrow\; m \subseteq n.$$

(2) Директно из тврђења (3) претходне теореме.
(3) Ако је $m < n$, тј. $m \in n$, онда је $\{m\} \subseteq n$ и, према теореми 27 (1), $m \subseteq n$, па је $m' = m \cup \{m\} \subseteq n$, тј. $m' \leqslant n$.

Из $m' \leqslant n$ следи $m' < n$ или $m' = n$, и у оба случаја, будући да је $m < m'$, закључујемо $m < n$.
(4) и (5) Доказе остављамо за вежбу. □

Теорема 28. [***Принцип потпуне индукције***] *Нека је $S \subseteq \mathbb{N}$. Ако важи*

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S),$$

онда је $S = \mathbb{N}$.

Доказ. Формулу $(\forall k < n)\, k \in S$ можемо записати и на следећи начин: $(\forall k \in n)\, k \in S$.

Приметимо најпре да важи

(**BI**) $$(\forall k < 0)\, k \in S.$$

Ова формула је заправо скраћење за $\forall k\,(k \in 0 \Rightarrow k \in S)$, што се једноставно доказује, јер знамо да за свако k важи $k \notin 0$.

Није тешко уочити, а ни формално доказати, да је формула

$$(\forall k < n)\, k \in S \Rightarrow n \in S$$

еквивалентна формули

(**IK**) $$(\forall k < n)\, k \in S \Rightarrow (\forall k < n')\, k \in S.$$

Из (**BI**) и (**IK**), према принципу математичке индукције, следи

$$(\forall n \in \mathbb{N})(\forall k < n)\, k \in S.$$

Најзад, из последње формуле и претпоставке $S \subseteq \mathbb{N}$ закључујемо $S = \mathbb{N}$. □

Теорема 29. *Сваки непразан подскуп скупа природних бројева има најмањи елемент.*

Доказ. Нека је X подскуп од $\mathbb{N}$ који нема најмањи елемент. Доказаћемо да X мора бити празан, тј. да је $\mathbb{N} \setminus X = \mathbb{N}$. Ову једнакост доказујемо применом принципа потпуне индукције.

Нека је n природан број такав да је $(\forall k < n)\, k \in \mathbb{N} \setminus X$. Ако би број n припадао X, онда би он био најмањи елемент скупа X, јер сваки k мањи од n припада $\mathbb{N} \setminus X$. Дакле, $n \in \mathbb{N} \setminus X$. Према принципу потпуне индукције закључујемо да је $\mathbb{N} \setminus X = \mathbb{N}$, односно $X = \emptyset$. □

Принцип потпуне индукције заправо тврди да за сваки $S \subseteq \mathbb{N}$ важи:

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S) \Rightarrow (\forall n \in \mathbb{N})\, n \in S.$$

Наравно, за сваки $S \subseteq \mathbb{N}$ важи

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S^{\complement} \Rightarrow n \in S^{\complement}) \Rightarrow (\forall n \in \mathbb{N})\, n \in S^{\complement},$$

одн. применом закона контрапозиције:

$$\neg(\forall n \in \mathbb{N})\, n \in S^{\complement} \Rightarrow \neg(\forall n \in \mathbb{N})((\forall k < n)\, k \in S^{\complement} \Rightarrow n \in S^{\complement}).$$

Последња формула се једноставно трасформише у еквивалентну формулу

$$\underbrace{(\exists n \in \mathbb{N})\, n \in S}_{S \text{ је непразан}} \Rightarrow \underbrace{(\exists n \in \mathbb{N})((\forall k < n)\, k \notin S \wedge n \in S)}_{S \text{ има најмањи елемент}},$$

којом се тврди да *сваки непразан подскуп од* $\mathbb{N}$ *има најмањи елемент.*

Дефиниција 20. *Уређење* $\leqslant$ *неког скупа* X *је* ***добро*** *ако сваки непразан подскуп од* X *има најмањи елемент у односу на* $\leqslant$.

Дакле, скуп природних бројева је добро уређен скуп.

Бинарна релација $\leqslant$ неког скупа X је *уређење*, ако за све $x, y, z \in X$:

(P) $x \leqslant x$;

(AC) $x \leqslant y \wedge y \leqslant x \Rightarrow x = y$;

(T) $x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$.

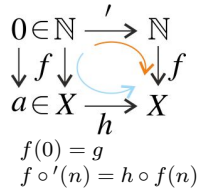
▼ Теорема рекурзије. Основне аритметичке операције

део питања 18

Теорема рекурзије омогућава да дефинишемо функције чији је домен $\mathbb{N}$, на начин који потпуно одговара 'природи' скупа $\mathbb{N}$.

Теорема 30. [***Принцип рекурзије***] *Нека је X неки скуп, $g \in X$ и $h : X \to X$. Тада постоји јединствена функција $f : \mathbb{N} \to X$ таква да је*

$$(\text{Rec}) \left| \begin{array}{l} f(0) = g, \\ f(n') = h(f(n)),\ n \in \mathbb{N}. \end{array} \right.$$



Доказ. (⋆) **Егзистенција**.

Скуп $F \subseteq \mathbb{N} \times X$ називаћемо (g,h)-скупом ако су задовољени следећи услови:

1) $(0, g) \in F$ и

2) за све $n \in \mathbb{N}$ и $x \in X$, ако $(n, x) \in F$, онда и $(n', h(x)) \in F$.

Очигледно је $\mathbb{N} \times X$ један (g,h)-скуп, па је непразна колекција $\mathcal{F}$ свих (g,h)-скупова. Нека је $f = \bigcap \mathcal{F}$. Тада је $f \subseteq \mathbb{N} \times X$. Доказаћемо да је f заправо тражена функција. Доказ ове чињенице је дугачак само зато што ћемо неколико пута проверавати услове 1) и 2), тј. доказивати да је неки скуп заиста (g,h)-скуп. Да бисмо олакшали читање, ове провере су издвојене из остатка доказа.

Подсећамо: f је функција из A у B, у ознаци $f : A \to B$, ако је $f \subseteq A \times B$ и за свако $a \in A$ постоји јединствено $b \in B$ тако да је $(a, b) \in f$. Ако $f : A \to B$, уместо $(a, b) \in f$ пишемо $f(a) = b$.

Докажимо најпре да је $f = \bigcap \mathcal{F}$ један (g,h)-скуп.

1) За свако $F \in \mathcal{F}$ важи $(0, g) \in F$, одакле следи да $(0, g) \in \bigcap \mathcal{F} = f$.
2) Претпоставимо да $(n, x) \in f = \bigcap \mathcal{F}$. Тада за свако $F \in \mathcal{F}$, $(n, x) \in F$, па и $(n', h(x)) \in F$ (јер F (g,h)-скуп). Дакле, $(n', h(x)) \in \bigcap \mathcal{F} = f$.

Даље, доказујемо да је f функција из $\mathbb{N}$ у X, одн. да за свако $k \in \mathbb{N}$ постоји јединствено $y \in X$ тако да $(k, y) \in f$.

(**BI**) Доказујемо базу индукције ($k = 0$). Како је f један (g,h)-скуп, знамо да $(0, g) \in f$. Претпоставимо да постоји још једно $g_1 \in X$ такво да $(0, g_1) \in f$ и $g \neq g_1$. Нека је $f_1 = f \setminus \{(0, g_1)\}$. Докажимо да је f_1 један (g,h)-скуп.

1) $(0, g) \in f_1$, јер је из f избачен само елемент $(0, g_1)$ и $g_1 \neq g$.
2) Претпоставимо да за неке $n \in \mathbb{N}$ и $x \in X$, $(n, x) \in f_1$. Будући да тада $(n, x) \in f$ имамо и да $(n', h(x)) \in f$. Како је $(n', h(x)) \neq (0, g_1)$, јер је $0 \neq n'$, следи да $(n', h(x)) \in f_1$.

Дакле, $f' \in \mathcal{F}$, па је $f = \bigcap \mathcal{F} \subsetneq f_1$, што је контрадикција.

(**IK**) Доказујемо индуктивни корак.

IP Претпоставимо да за $k \in \mathbb{N}$ постоји тачно један $y \in X$ такав да је $(k, y) \in f$.

Пошто је f један (g,h)-скуп, имамо да $(k', h(y)) \in f$. Претпоставимо да постоји и $y_1 \in X$ такав да $(k', y_1) \in f$ и $y_1 \neq h(y)$. Нека је $f_1 = f \setminus \{(k', y_1)\}$. Докажимо да је f_1 један (g,h)-скуп.

1) $(0, g) \in f'$, јер је из f избачен само елемент (k', y_1) који је сигурно различит од $(0, g)$, будући да је $0 \neq k'$.
2) Претпоставимо да за $n \in \mathbb{N}$ и $x \in X$, $(n, x) \in f_1$. Из $(n, x) \in f$ следи $(n', h(x)) \in f$. Докажимо да је $(n', h(x)) \neq (k', y_1)$. Неједнакост је очигледно тачна ако је $n' \neq k'$. Ако је $n' = k'$, онда је и $n = k$, па је $x = y$ (јер је y једини елемент из X такав да $(k, y) \in f$). Према избору елемента y_1 имамо да је $y_1 \neq h(y) = h(x)$, одакле следи $(n', h(x)) \neq (k', y_1)$.

Дакле, $f = \bigcap \mathcal{F} \subsetneqq f'$, што је контрадикција.

Доказ математичком индукцијом је завршен; доказали смо да је f функција из $\mathbb{N}$ у X. Ова функција задовољава једнакости (Rec), јер је f (g, h)-скуп:

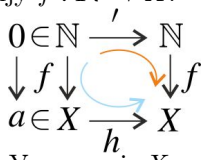
Из услова 1) произлази $f(0) = g$;

Према услову 2), из $f(n) = x$ следи да је $f(n') = h(x)$, тј. $f(n') = h(f(n))$.

Јединственост.

Претпоставимо да функције $f_1, f_2 : \mathbb{N} \to X$ задовољавају једнакости (Rec). Доказаћемо да су оне једнаке, тј. да за свако $n \in \mathbb{N}$ важи $f_1(n) = f_2(n)$. Доказ изводимо математичком индукцијом.
(**BI**) $f_1(0) = g = f_2(0)$
(**IK**) Претпоставимо да за неко $n \in \mathbb{N}$ важи $f_1(n) = f_2(n)$. Тада је $f_1(n') = h(f_1(n)) = h(f_2(n)) = f_2(n')$. □

Скуп природних бројева $\mathbb{N}$ је суштински одређен својим (почетним) елементом 0 и функцијом (следбеник) $' : \mathbb{N} \to \mathbb{N}$. Теорема рекурзије тврди да за било који скуп X, изабрани елемент $a \in X$ и функцију $h : X \to X$, једнакости (Rec) одређују јединствену функцију $f : \mathbb{N} \to X$.



$f(0) = a$
$f(n') = h(f(n))$, тј. $f \circ ' (n) = h \circ f\,(n)$

Уколико је X неки скуп, свака функција из $\mathbb{N}$ у X назива се и **низ** у скупу X. Низови су веома важни у свим областима математике, па се усвајају разни договори о ознакама. Аргумент функције (низа) $f : \mathbb{N} \to X$ често се записује као индекс слова којим је функција означена: уместо $f(n)$ пише се f_n. У складу са тим, уместо '$f : \mathbb{N} \to X$ ' пише се '$(f_n)_{n \in \mathbb{N}}$'. Поред тога, следбеник елемента $n \in \mathbb{N}$, уместо n' означава се $n + 1$. Уз ове договоре, теорема рекурзије тврди да за изабране $a \in X$ и $h : X \to X$, постоји јединствени низ $(f_n)_{n \in \mathbb{N}}$ одређен једнакостима:

$$(\text{Rec}) \begin{cases} f_0 = a, \\ f_{n+1} = h(f_n),\ n \in \mathbb{N}. \end{cases}$$

За низ одређен једнакостима (Rec) кажемо да је **рекурзивно** (рекурентно, индуктивно) дефинисан.

Из претходне теореме изводимо и следећу варијанту принципа рекурзије.

Теорема 31. [***Принцип рекурзије*** **– II**] *Нека* $g : S \to X$ *и* $h : S \times X \to X$. *Тада постоји јединствена функција* $f : S \times \mathbb{N} \to X$ *таква да за свако* $s \in S$*:*

$$\text{(Rec)} \quad \left| \begin{array}{l} f(s,0) = g(s), \\ f(s,n') = h(s, f(s,n)),\ n \in \mathbb{N}. \end{array} \right.$$

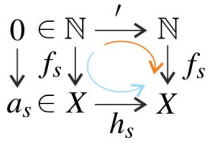
Доказ. Друга варијанта принципа рекурзије блиско је повезана са првом. Заиста, ако $g : S \to X$ и $h : S \times X \to X$, тада за свако $s \in S$:

- функција g 'бира' један елемент из X – бира $g(s)$ који ћемо означити g_s, и
- h одређује функцију $h_s : X \to X$, $h_s(x) \stackrel{\text{def}}{=} h(s,x)$, $x \in X$.

Према првој варијанти принципа рекурзије, за свако $s \in S$, постоји јединствена функција $f_s : \mathbb{N} \to X$ таква да:

$$\left| \begin{array}{l} f_s(0) = g_s, \\ f_s(n') = h_s(f_s(n)),\ n \in \mathbb{N}. \end{array} \right.$$

Све функције f_s, $s \in S$, одређују ('подизањем индекса у аргумент') јединствену функцију $f : S \times \mathbb{N} \to X$, $f(s,n) \stackrel{\text{def}}{=} f_s(n)$ која задовољава услове (Rec). □



Прва варијанта се може сматрати специјалним случајем друге ако изаберемо да S буде синглтон. Нека је $S = \{0\}$. Функцијом $g : \{0\} \to X$ заправо бирамо један елемент из X; нека је $g(0) = g$. Функцију $h : \{0\} \times X \to X$ можемо поистоветити са природно дефинисаном функцијом из X у X: $x \mapsto h(0,x)$, $x \in X$.

Основне рачунске операције уводимо применом друге варијанте теореме рекурзије, узимајући да је $S = X = \mathbb{N}$.

Сабирање. Нека је $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ функција дефинисана са $h(x,y) = y'$. Према другој варијанти принципа рекурзије, постоји јединствена функција $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ која задовољава једнакости:

$$\left| \begin{array}{l} +(m,0) = \mathrm{id}_{\mathbb{N}}(m), \\ +(m,n')) = h(m,+(m,n)), \end{array} \right. \quad \text{односно} \quad \left| \begin{array}{l} +(m,0) = m, \\ +(m,n') = s(+(m,n)). \end{array} \right.$$

h је композиција следбеника $' : \mathbb{N} \to \mathbb{N}$ и друге пројекције $\pi_2 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\pi_2(x,y) = y$: $h = ' \circ \pi_2$.

$\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ је идентичка функција, $\mathrm{id}_{\mathbb{N}}(n) = n$.

Ако уместо $+(m,n)$ пишемо $m+n$, претходне једнакости постају:

$$\text{(Rec+)} \quad \left| \begin{array}{l} m+0 = m, \\ m+n' = (m+n)'. \end{array} \right.$$

Није тешко уочити да је $n' = n+1$, за сваки природан број n.

Множење. Помоћу константне функције $\mathbf{0} : \mathbb{N} \to \mathbb{N}$, $\mathbf{0}(n) = 0$, и сабирања $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, уводимо множење $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ следећим једнакостима:

$$\text{(Rec}\cdot\text{)} \quad \left| \begin{array}{l} \cdot(m,0) = \mathbf{0}(m), \\ \cdot(m,n') = +(m,\cdot(m,n)), \end{array} \right. \quad \text{односно} \quad \left| \begin{array}{l} m \cdot 0 = 0, \\ m \cdot n' = m + (m \cdot n). \end{array} \right.$$

Степеновање $\exp : \mathbb{N}^+ \times \mathbb{N} \to \mathbb{N}$, при чему је $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ и уместо $\exp(m,n)$ пишемо m^n, дефинишемо следећим једнакостима:

$$\left| \begin{array}{l} m^0 = 1, \\ m^{n+1} = m \cdot m^n. \end{array} \right.$$

Сва позната својства ових операција и њихове везе са уређењем доказујемо математичком индукцијом.

Теорема 32. *За било које природне бројеве k, m, n важи:*
(1) $m + n = n + m$ *(сабирање је комутативно);*
(2) $k + (m + n) = (k + m) + n$ *(сабирање је асоцијативно);*
(3) $m \cdot 1 = m$ *(неутрал за множење је* 1*);*
(4) $m \cdot n = n \cdot m$ *(множење је комутативно);*
(5) $k \cdot (m \cdot n) = (k \cdot m) \cdot n$ *(множење је асоцијативно);*
(6) $k \cdot (m + n) = k \cdot m + k \cdot n$ *(леви закон дистрибутивности);*
(7) $1^m = 1$*;*
(8) $m^1 = m$*, под условом* $m \neq 0$*;*
(9) $k^{m+n} = k^m \cdot k^n$*, под условом* $k \neq 0$*;*
(10) $(k \cdot m)^n = k^n \cdot m^n$*, под условом* $k, m \neq 0$*;*
(11) $(k^m)^n = k^{m \cdot n}$*, под условом* $k \neq 0$*.*

Теорема 33. *За све* $k, m, n \in \mathbb{N}$ *важи:*
(1) $k < m \Leftrightarrow k + n < m + n$
(2) $k = m \Leftrightarrow k + n = m + n$
(3) $m + n = 0 \Leftrightarrow m = n = 0$
(4) $0 < n \wedge k < m \Rightarrow k \cdot n < m \cdot n$
(5) $0 < n \wedge k \cdot n = m \cdot n \Rightarrow k = m$
(6) $0 < n \wedge k \cdot n < m \cdot n \Rightarrow k < m$
(7) $m \cdot n = 0 \Leftrightarrow m = 0 \vee n = 0$
(8) $m \cdot n = 1 \Leftrightarrow m = 1 \wedge n = 1$

4.5. Кардиналност скупа

▼ Коначни скупови. Основни комбинаторни принципи

17

Један одосновних комбинаторних принципа познат је под називом *принцип кутлица и кутија* или *Дирихлеов принцип*:

> Ако m куглица распоредимо у n кутија, при чему је $m > n$, онда се у бар једној кутији налазе бар две куглице; другим речима, распоређивање куглица не може бити 1-1 (једнозначно).

Теорема 34. [***Дирихлеов принцип***] *За свака два природна броја m и n, ако је $m > n$, онда не постоји 1-1 функција из m у n.*

Доказ. Доказ изводимо индукцијом по n.
(**BI**) Ако је $m > 0$, тада уопште не постоји функција из m у 0 ($m \neq \emptyset$ и $0 = \emptyset$), па тврђење тривијално важи.
(**IK**) (IP) Нека је n природан број такав да за било које $m > n$ не постоји 1-1 функција из m у n. Доказаћемо да тада за свако $m > n'$, такође не постоји 1-1 функција из m у n'.

Претпоставимо супротно: нека је $m > n'$ и $f : m \overset{1-1}{\to} n'$. Одавде следи да n ($n \in n'$) мора бити f-слика неког елемента из m, јер би у супротном постојала 1-1 функција из m у n, што није могуће. Такође, из $m > n'$, следи да постоји природан број k такав да је $m = k'$; $f : k \cup \{k\} \overset{1-1}{\to} n \cup \{n\}$. Како је $k' > n'$, према последици 3 (5) имамо да је $k > n$, па не постоји 1-1 функција из k у n. Разликујемо два случаја: $f(k) = n$ и $f(k) \neq n$.
1. случај: $f(k) = n$. Тада $f\,|_k \colon k \overset{1-1}{\to} n$, што је немогуће према (IP).
2. случај: $f(k) \neq n$. Тада је $f(\ell) = n$, за неко $\ell \in k$, тј. $\ell < k$. Дефинишимо функцију $h : k' \to n'$ на следећи начин:

$$h(x) = \begin{cases} f(x), & x \in k \wedge x \neq \ell \\ f(k), & x = \ell, \\ n, & x = k. \end{cases}$$

Није тешко уочити да $h : k' \overset{1-1}{\to} n'$ и да је $h(k) = n$. Међутим, тада $h\,|_k \colon k \overset{1-1}{\to} n$, што није могуће према (IP). □

Последица 4. *Нека су m и n произвољни природни бројеви.*
(1) Постоји 1-1 функција из m у n ако и само ако је $m \leqslant n$.
(2) Постоји бијекција између m и n ако и само ако је $m = n$.

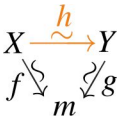
Као што је добро познато, природним бројевима изражавамо 'број' ('количину') елемената коначних скупова.

Дефиниција 21. *Скуп X је **коначан** ако постоји бијекција између X и неког природног броја n, и у том случају пишемо $|X| = n$.*

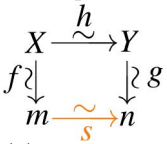
Према последици 4 (2), за сваки коначан скуп X постоји *јединствен* природан број n такав да је $|X| = n$ и тада кажемо да је n *број елемената* скупа X, одн. *кардиналност* скупа X једнака је n. Очигледно је $|n| = n$ за било који природан број n.

Теорема 35. *Нека су X и Y неки коначни скупови. Тада важи:*
(1) $|X| = 0 \Leftrightarrow X = \emptyset$;
(2) $|X| = |Y|$ *ако и само ако постоји бијекција између* X *и* Y.
(3) $|X| \leqslant |Y|$ *ако само ако постоји 1-1 функција из* X *у* Y.

Доказ. (1) Тврђење директно следи из разматрања о функцијама из празног и у празан скуп са стране 77.
(2) Будући да су X и Y коначни скупови, постоје природни бројеви m и n и бијекције $f : X \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} m$ и $g : Y \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} n$.
($\Rightarrow$) Претпоставимо да је $m = n$. Треба да дефинишемо бијекцију између X и Y. На наредној слици, знаком $\sim$ изнад стрелице означавамо да је одговарајућа функција бијекција.



Функција $h : X \to Y$, дата са $h(x) = g^{-1} \circ f(x)$, јесте бијекција.
($\Leftarrow$) Нека је $h : X \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} Y$ нека бијекција између X и Y. Тада се, аналогно претходном случају, дефинише бијекција између m и n, што према последици 4 (2) значи да је $m = n$, тј. $|X| = |Y|$.



(3) Доказ остављамо за вежбу. □

Теорема 36. *Нека је n било који природан број.*
(1) Сваки подскуп a од n је коначан и важи $|a| \leqslant n$.
(2) За сваки $a \subset n$ не постоји бијекција између n и a.
(3) За сваку функцију f из n у n важи: $f : n \overset{1-1}{\to} n$ акко $f : n \overset{\text{на}}{\to} n$.

Доказ. (1) (**BI**) Једини подскуп од 0, тј. од $\emptyset$, јесте $\emptyset$ па тврђење очигледно важи.
(IP) Нека је n природан број за који важи тврђење.
Претпоставимо да је $a \subseteq n' = n \cup \{n\}$. Разликујемо два случаја.
1. *случај:* $n \notin a$. Тада је $a \subseteq n$, па према (IP) скуп a је коначан и $|a| \leqslant n < n'$.
2. *случај:* $n \in a$. Тада је $a_1 = a \setminus \{n\} \subseteq n$, па из (IP) следи да је a_1 коначан скуп и $|a_1| \leqslant n$. Нека је $|a_1| = m$, за неко $m \leqslant n$, и $f : a_1 \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} m$. Дефинишимо функцију $h : a \to m'$:

$$h(x) = \begin{cases} f(x), & x \in a_1, \\ m, & x = n. \end{cases}$$

Није тешко уочити да је h бијекција, па је $|a| = m' \leqslant n'$.
(2) (**BI**) Не постоје прави подскупови од 0, па тврђење тривијално важи.
(IP) Нека је n природан број за који важи тврђење.

Претпоставимо да је $a \subset n' = n \cup \{n\}$ и $f : a \overset{1-1}{\underset{\text{на}}{\rightarrow}} n'$. Разликујемо два случаја.
1. *случај:* $n \notin a$. Тада је $a \subseteq n$, $a_1 = a \setminus \{f^{-1}(n)\} \subset a \subseteq n$ и $f\mid_{a_1} : a_1 \overset{1-1}{\underset{\text{на}}{\rightarrow}} n$, што је немогуће према (IP).
2. *случај:* $n \in a$. Разликујемо два подслучаја.

2.1. *случај:* $f(n) = n$. Тада је $a_1 = a \setminus \{n\} \subset n$ и $f\mid_{a_1} : a_1 \overset{1-1}{\underset{\text{на}}{\rightarrow}} n$, па поново долазимо до контрадикције са (IP).

2.2. *случај:* $f(n) \neq n$. Тада $f(n) = k$, за неко $k \in n$. Такође, постоји $\ell \in n$ такав да је $f(\ell) = n$. Нека је $h : a \to n$ функција дефинисана са

$$h(x) = \begin{cases} f(x), & x \in a \setminus \{\ell, n\}, \\ n, & x = n, \\ k, & x = \ell. \end{cases}$$

Једноставно се уочава да $h : a \overset{1-1}{\underset{\text{на}}{\rightarrow}} n'$ и да је $h(n) = n$, па се поново изводи контрадикција као у претходном случају.
(3) Ако је $n = 0$ тврђење тривијално важи. Претпоставимо зато да је $n \neq 0$.
($\Rightarrow$) Нека $f : n \overset{1-1}{\rightarrow} n$. Очигледно је $f[n] \subseteq n$. Не може бити $f[n] \subset n$, јер би тада било $f : n \overset{1-1}{\underset{\text{на}}{\rightarrow}} f[n]$, што је немогуће према тврђењу (2). Дакле, $f[n] = n$, тј. f је на функција.
($\Leftarrow$) Претпоставимо $f : n \overset{\text{на}}{\rightarrow} n$. Тада је за свако $k \in n$, скуп $f^{-1}[\{k\}]$ непразан подскуп од n, па има (јединствен) најмањи елемент, који ћемо означити $\min f^{-1}[\{k\}]$. Лако се проверава да је функција $g : n \to n$, $g(k) = \min f^{-1}[\{k\}]$, $k \in n$, заправо 1-1 функција: ако је $k_1 \neq k_2$, онда је $f^{-1}[\{k_1\}] \cap f^{-1}[\{k_2\}] = \emptyset$, па мора бити $\min f^{-1}[\{k_1\}] \neq \min f^{-1}[\{k_2\}]$, тј. $g(k_1) \neq g(k_2)$. Самим тим, према делу доказа ($\Rightarrow$), функција g мора бити и на функција, односно $g : n \overset{1-1}{\underset{\text{на}}{\rightarrow}} n$. Приметимо да је $f \circ g = \mathrm{id}_n$, тј. $f(g(k)) = k$, за свако $k \in n$.

На основу изведених закључака, доказујемо да је f 1-1 функција. Нека је $f(k_1) = f(k_2)$. Тада постоје јединствени ℓ_1 и ℓ_2 такви да је $g(\ell_1) = k_1$ и $g(\ell_2) = k_2$. Из $f(g(\ell_1)) = f(g(\ell_2))$, следи да је $\ell_1 = \ell_2$, па мора бити и $k_1 = k_2$. □

Последица 5. *Нека је X коначан скуп.*
(1) Сваки подскуп A од X је коначан и важи $|A| \leqslant |X|$.
(2) За сваки $A \subset X$ не постоји бијекција између X и A.
(3) За сваку функцију f из X у X важи: $f : X \overset{1-1}{\rightarrow} X$ акко $f : X \overset{\text{на}}{\rightarrow} X$.

Доказ. Сва тврђења су једноставне последице претходне теореме. Укратко ћемо описати само доказ тврђења (1). Остала два остављамо за вежбу.

(1) Нека је n природан број и $f : X \overset{1-1}{\underset{\text{на}}{\rightarrow}} n$. Тада је $f[A] \subseteq n$, па је $f[A]$ коначан скуп и $|f[A]| \leqslant n = |X|$. Одавде изводимо жељени закључак, јер су скупови $f[A]$ и A исте кардиналности (функција f одређује једну бијекцију између A и $f[A]$). □

Теорема 37. *Нека су X и Y произвољни коначни скупови.*
(1) [***Принцип збира***] *Ако је $X \cap Y = \emptyset$, онда је $|X \cup Y| = |X| + |Y|$.*
(2) [***Принцип производа***] $|X \times Y| = |X| \cdot |Y|$.

Доказ. Наведена тврђења можемо формулисати и на следећи начин: за свака два природна броја m и n, и свака два скупа X и Y,
(1) ако је $|X| = m$, $|Y| = n$ и $X \cap Y = \emptyset$, онда је $|X \cup Y| = m + n$;
(2) ако је $|X| = m$ и $|Y| = n$, онда је $|X \times Y| = m \cdot n$.

На основу ових реформулација тврђења уочавамо да доказе можемо спровести и индукцијом по n (при фиксираном m).

Нека је m произвољан природан број.
(1) (**BI**) Нека је $|X| = m$, $|Y| = 0$ и $X \cap Y = \emptyset$. Из $|Y| = 0$ следи да је $Y = \emptyset$ (теорема 35 (1)), па је $X \cup Y = X$ и $|X \cup Y| = |X| = m = m + 0$.

(IP) Нека је n природан број такав да за све скупове X и Y, из $|X| = m$, $|Y| = n$ и $X \cap Y = \emptyset$ следи $|X \cup Y| = m + n$.

Претпоставимо да је $|X| = m$, $|Y| = n'$ и $X \cap Y = \emptyset$. Тада постоји бијекција $f : Y \to n'$. Нека је $Y_1 = Y \setminus \{f^{-1}(n)\}$. Користећи бијекцију f непосредно можемо дефинисати бијекцију између Y_1 и n, одакле следи да је $|Y_1| = n$. Како је $X \cap Y_1 = \emptyset$, према (IP) закључујемо да постоји бијекција $g : X \cup Y_1 \overset{1-1}{\underset{\text{на}}{\rightarrow}} m + n$. Дефинишимо, најзад, функцију $h : X \cup Y \to (m + n)'$:

$$h(x) = \begin{cases} g(x), & x \in X \cup Y_1, \\ m + n, & x = f^{-1}(n). \end{cases}$$

Очигледно је h бијекција, а како је $(m + n)' = m + n'$, тврђење је доказано.
(2) (**BI**) Нека је $|X| = m$, $|Y| = 0$. Из $|Y| = 0$ следи да је $Y = \emptyset$, па је $X \times Y = \emptyset$ и $|X \times Y| = 0 = m \cdot 0$.

(IP) Нека је n природан број такав да за све скупове X и Y, из $|X| = m$ и $|Y| = n$ следи $|X \times Y| = m \cdot n$.

Претпоставимо да је $|X| = m$ и $|Y| = n'$. Тада постоји бијекција $f : Y \to n'$. Нека је $y = f^{-1}(n)$ и $Y_1 = Y \setminus \{y\}$. Како је $|Y_1| = n$, према (IP) закључујемо да је $|X \times Y_1| = m \cdot n$. Једноставно је уочити да је $|X \times \{y\}| = |X| = m$ (на пример, $h : X \times \{y\} \overset{1-1}{\underset{\text{на}}{\rightarrow}} X$, $h(x, y) = x$, $x \in X$). Како је $Y = \{y\} \cup Y_1$ (и $y \notin Y_1$), то је $X \times Y = (X \times \{y\}) \cup (X \times Y_1)$ и $(X \times \{y\}) \cap (X \times Y_1) = \emptyset$, па према (1) добијамо

$$|X \times Y| = |X \times \{y\}| + |X \times Y_1| = m + m \cdot n = m \cdot n'.$$

□

Последица 6. *(1) Ако су X и Y коначни скупови, онда је*

$$|X \cup Y| + |X \cap Y| = |X| + |Y|.$$

(2) Унија два коначна скупа је коначан скуп.
(3) Декартов производ два коначна скупа је коначан скуп.

▼ Бесконачни скупови. Кантор-Бернштајнова теорема

18

Нису сви скупови коначни. На пример, да скуп $\mathbb{N}$ није коначан можемо се уверити на више начина. Наводимо само два.

- Скуп $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ је прави подскуп од $\mathbb{N}$ и постоји бијекција између $\mathbb{N}$ и $\mathbb{N}^+$; на пример, функција $f : \mathbb{N} \to \mathbb{N}^+$, $f(n) = n'$, $n \in \mathbb{N}$, јесте бијекција. Према последици 5 (2), скуп $\mathbb{N}$ не може бити коначан.
- Функција следбеник $' : \mathbb{N} \to \mathbb{N}$ је 1-1 функција, али није на функција (0 није следбеник ниједног природног броја), па према последици 5 (3) закључујемо да $\mathbb{N}$ није коначан.

Дефиниција 22. *Скуп је **бесконачан** ако није коначан.*

Упоређивање бесконачних скупова по 'броју' елемената дефинишемо по узору на тврдње (2) и (3) теореме 35, које се односе на коначне скупове.

Дефиниција 23. *(1) Скупови A и B су **исте кардиналности** (имају исти број елемената), у ознаци $|A| = |B|$ ако постоји бијекција између A и B.*
(2) Кардиналност скупа A је мања од или једнака кардиналности скупа B, у ознаци $|A| \leqslant |B|$ ако постоји 1-1 функција из A у B.

Теорема 38. *За произвољне скупове A, B, C важи:*
(1) $|A| = |A|$;
(2) ако је $|A| = |B|$, онда је $|B| = |A|$;
(3) ако је $|A| = |B|$ и $|B| = |C|$, онда је $|A| = |C|$.

Доказ. (1) $\mathrm{id}_A : A \overset{1-1}{\underset{\text{на}}{\rightarrow}} A$.
(2) Ако $f : A \overset{1-1}{\underset{\text{на}}{\rightarrow}} B$, онда $f^{-1} : B \overset{1-1}{\underset{\text{на}}{\rightarrow}} A$.
(3) Ако $f : A \overset{1-1}{\underset{\text{на}}{\rightarrow}} B$ и $g : B \overset{1-1}{\underset{\text{на}}{\rightarrow}} C$, онда $g \circ f : A \overset{1-1}{\underset{\text{на}}{\rightarrow}} C$. □

Теорема 39. *За произвољне скупове A, B, C важи:*
(1) $|A| \leqslant |A|$;
(2) ако је $|A| \leqslant |B|$ и $|B| \leqslant |C|$, онда је $|A| \leqslant |C|$.

Доказ. Тврђење (1) директно следи из претходне теореме. Тврђење (2) важи јер из $f : A \overset{1-1}{\rightarrow} B$ и $g : B \overset{1-1}{\rightarrow} C$ следи $g \circ f : A \overset{1-1}{\rightarrow} C$. □

Теорема 40. [***Кантор-Бернштајнова теорема***] *Нека су A и B било који скупови. Ако је $|A| \leqslant |B|$ и $|B| \leqslant |A|$, онда је $|A| = |B|$.*

Најпре доказујемо једну корисну лему.

Лема 8. *Нека је A било који скуп и $F : \mathcal{P}(A) \to \mathcal{P}(A)$ функција која задовољава следећи услов:*

$$(*) \qquad (\forall X, Y \in \mathcal{P}(A))\, X \subseteq Y \Rightarrow F(X) \subseteq F(Y).$$

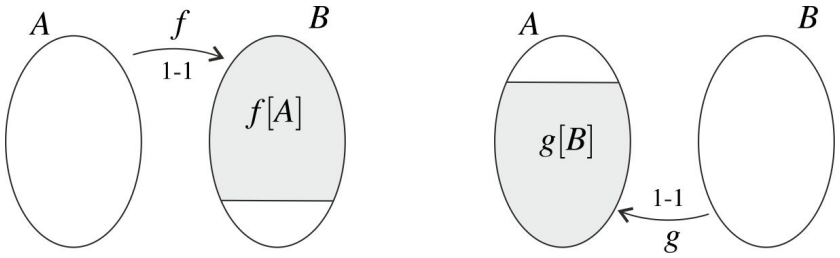
Тада постоји $E \subseteq A$ такав да је $F(E) = E$.

Доказ. Нека је $\mathcal{E} = \{X \mid X \subseteq A \wedge X \subseteq F(X)\}$ и $E = \bigcup \mathcal{E}$. Доказаћемо да је E *фиксна тачка* функције F, тј. $F(E) = E$. Приметимо најпре да важи:

$$E = \bigcup_{X\in\mathcal{E}} X \subseteq \bigcup_{X\in\mathcal{E}} F(X) \overset{(!)}{\subseteq} F(\bigcup_{X\in\mathcal{E}} X) = F(E).$$

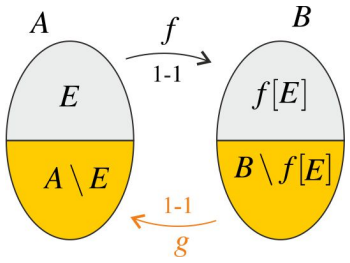
Инклузија означена знаком узвика важи јер за свако $X \in \mathcal{E}$, $X \subseteq \bigcup X$ и $F(X) \subseteq F(\bigcup X)$, према $(*)$. Из услова $(*)$ добијамо и да је $F(E) \subseteq F(F(E))$, одакле следи да $F(E) \in \mathcal{E}$, па је $F(E) \subseteq \bigcup \mathcal{E} = E$. Дакле, $F(E) = E$. □

Доказ. [**Кантор-Бернштајнова теорема**] Нека $f : A \overset{1-1}{\to} B$ и $g : B \overset{1-1}{\to} A$. Очигледно је да се помоћу функције f може дефинисати бијекција између скупова A и $f[A]$, а помоћу функције g бијекција међу скуповима B и $g[B]$. Међутим, могуће је да скупови $f[A]$ и $g[B]$ буду прави подскупови, редом од B и A.



Наравно, слично запажање важи и за подскупове од A, одн. B: ако је $X \subseteq A$, онда је f одређује једну бијекцију између X и $f[X]$, а ако је $Y \subseteq B$, онда g одређује бијекцију између Y и $g[Y]$. Кључно питање је да ли постоји подскуп $E \subseteq A$ такав да g одређује бијекцију између $B \setminus f[E]$ и $A \setminus E$, тј. да важи

$$g[B \setminus f[E]] = A \setminus E, \text{ одн. } E = A \setminus g[B \setminus f[E]].$$



Другим речима, треба испитати да ли постоји фиксна тачка функције $F : \mathcal{P}(A) \to \mathcal{P}(A)$, $F(X) = A \setminus g[B \setminus f[X]]$, $X \in \mathcal{P}(A)$. Према претходној леми, довољно је проверити да ли важи услов $(*)$. За било које $X_1, X_2 \subseteq A$ важи:

$$\begin{aligned} X_1 \subseteq X_2 &\Rightarrow f[X_1] \subseteq f[X_2] \\ &\Rightarrow B \setminus f[X_1] \supseteq B \setminus f[X_2] \\ &\Rightarrow g[B \setminus f[X_1]] \supseteq g[B \setminus f[X_2]] \\ &\Rightarrow A \setminus g[B \setminus f[X_1]] \subseteq A \setminus g[B \setminus f[X_2]] \\ &\Leftrightarrow F(X_1) \subseteq F(X_2). \end{aligned}$$

Дакле, према поменутој леми, постоји скуп E такав да је $F(E) = E$, тј. $g[B \setminus f[E]] = A \setminus E$. Приметимо да за свако $x \in A \setminus E$, постоји јединствени (јер је g 1-1 функција) елемент из B чија је g-слика једнака x; тај јединствени елемент из B означићемо са $g^{-1}(x)$. Сада није тешко дефинисати жељену бијекцију. Нека је $h : A \to B$ функција дата са:

$$h(x) = \begin{cases} f(x), & x \in E, \\ g^{-1}(x), & x \in A \setminus E \end{cases}$$

Доказ да је h бијекција остављамо за вежбу. □

Упоређивање бесконачних скупова по кардиналности (по броју елемената) има смисла, јер се испоставља да постоје разне 'врсте бесконачности' и да од сваког бесконачног скупа постоји неки 'бесконачнији', тј. веће кардиналности.

Дефиниција 24. *Кадриналност скупа A је мања од кардиналности скупа B, у ознаци $|A| < |B|$, ако је $|A| \leqslant |B|$ и $|A| \neq |B|$.*

Теорема 41. *За сваки скуп A, $|A| < |\mathcal{P}(A)|$.*

Доказ. Није тешко уочити да је $|A| \leqslant |\mathcal{P}(A)|$. Заиста, функција $f : A \to \mathcal{P}(A)$, $f(x) = \{x\}$, $x \in A$, јесте 1-1 функција.

Остаје још да покажемо да не постоји бијекција између A и $\mathcal{P}(A)$. Претпоставимо супротно, да $h : A \overset{1-1}{\underset{\text{на}}{\rightarrow}} \mathcal{P}(A)$. Дефинишимо скуп

$$K = \{x \in A \mid x \notin h(x)\}.$$

Очигледно $K \in \mathcal{P}(A)$, па пошто је h на функција, постоји $k \in A$ такав да је $h(k) = K$. Да ли k припада или не припада скупу K?
1. *могућност*: $k \in K$. Из $h(k) = K$ следи $k \in h(k)$, што према дефиницији скупа K, значи да $k \notin K$. Контрадикција.
1. *могућност*: $k \notin K$. Из $h(k) = K$ следи $k \notin h(k)$, што према дефиницији скупа K, значи да $k \in K$. Контрадикција.

Из добијених контрадикција закључујемо да не постоји бијекција између A и $\mathcal{P}(A)$. □

Напомена 9. Доказ последње теореме је стар преко сто година. Важна непосредна последица овог тврђења је да не постоји скуп свих скупова. Ако би постојао такав скуп V, тада бисмо имали да је $\mathcal{P}(V) \subseteq V$ (јер је сваки подскуп од V истовремено и елемент V) па и $|\mathcal{P}(V)| \leqslant |V|$. Такође, сви једночлани скупови не образују скуп, јер ако би K био скуп свих једночланих скупова, тада би за сваки скуп x било $x \in \{x\} \in K$, тј. $x \in \cup K$, па би скуп $\cup K$ садржавао све скупове. Интересантно је, такође, размотрити какве последице има неједнакост $|x| < |\mathcal{P}(x)|$, уколико је x бесконачан скуп.

Упоређивање скупова бројева по кардиналности је главни 'кривац' настанка теорије скупова јер се њеним првим резултатима сматрају Канторове теореме $|\mathbb{N}| = |\mathbb{Q}|$ и $|\mathbb{N}| < |\mathbb{R}|$. Слободније речено,

последња неједнакост нам говори да постоји нека врста бесконачности вишег реда, тј. да и од бесконачних скупова има строго 'бројнијих', будући да је скуп $\mathbb{N}$ бесконачан. Штавише, користећи доказану неједнакост $|x| < |\mathcal{P}(x)|$, можемо конструисати бесконачан, строго растући по кардиналности, низ бесконачних скупова.

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots < |\underbrace{\mathcal{P}(\cdots\mathcal{P}(\mathcal{P}}_{n}(\mathbb{N}))\cdots)| < \cdots$$

▼ Пребројиви и непребројиви скупови

19

Дефиниција 25. *Скуп X је **пребројив** ако је $|X| = |\mathbb{N}|$.*

Да је X пребројив означава се и $|X| = \aleph_0$.

Теорема 42. *Сваки подскуп пребројивог скупа је коначан или пребројив.*

Доказ. Доказаћемо да је сваки бесконачан подскуп од $\mathbb{N}$ пребројив. Из тога једноставно закључујемо да наведено тврђење важи.

Нека је A бесконачан подскуп од $\mathbb{N}$. Будући да је $|A| \leqslant |\mathbb{N}|$ (функција $f : A \to \mathbb{N}$, $f(a) = a$, $a \in A$, јесте 1-1 функција), према Кантор-Бернштајновој теореми треба још показати да је $|\mathbb{N}| \leqslant |A|$.

Дефинишимо најпре један низ подскупова од A. Применом теореме рекурзије дефинишемо $E : \mathbb{N} \to \mathcal{P}(A)$:

$$\begin{cases} E_0 = \emptyset, \\ E_{n+1} = E_n \cup \{\min(A \setminus E_n)\}. \end{cases}$$

Једноставно се доказују следеће чињенице:

- за свако $n \in \mathbb{N}$, E_n је коначан подскуп од A, па је и $A \setminus E_n \neq \emptyset$;
- E је строго растући (у односу на инклузију) низ, тј. за све $m, n \in \mathbb{N}$, из $m < n$ следи $E_m \subset E_n$;
- за свако $n \in \mathbb{N}$ и свако $m > n$, $\min(A \setminus E_n) \in E_m$.

Нека је $h : \mathbb{N} \to A$, $h(n) = \min(A \setminus E_n)$. Докажимо да је h 1-1 функција. Претпоставимо да је $n_1 \neq n_2$. Без губљења општости можемо узети да је $n_1 < n_2$. Из $h(n_1) = \min(A \setminus E_{n_1}) \in E_{n_2}$, закључујемо да мора бити $h(n_1) \neq h(n_2)$. □

Дефиниција 26. *Скуп је **највише пребројив** ако је коначан или пребројив. Бесконачан скуп је **непребројив** ако није највише пребројив.*

Из претходне теореме следи да је сваки подскуп пребројивог скупа највише пребројив.

Теорема 43. *Скуп A је највише пребројив акко је $|A| \leqslant |\mathbb{N}|$.*

Теорема 44. *Ако постоји функција из $\mathbb{N}$ на скуп A, $f : \mathbb{N} \overset{\text{na}}{\to} A$, онда је A највише пребројив.*

Доказ. Нека $f : \mathbb{N} \overset{\text{на}}{\to} A$. Тада је за свако $a \in A$, скуп

$$f^{-1}[\{a\}] = \{n \in \mathbb{N} \mid f(n) = a\}$$

непразан подскуп од $\mathbb{N}$, па самим тим има најмањи елемент. Нека је $g : A \to \mathbb{N}$ функција дефинисана са: $g(a) = \min f^{-1}[\{a\}]$, $a \in A$. Функција g је 1-1 функција, јер ако је $a_1 \neq a_2$, онда је $f^{-1}[\{a_1\}] \cap f^{-1}[\{a_2\}] = \emptyset$, па мора бити $g(a_1) \neq g(a_2)$. Дакле, $|A| \leqslant |\mathbb{N}|$. □

У наставку ћемо доказати неке чињенице у вези са пребројивим скуповима које се често користе (подразумевају) у многим математичким областима.

Теорема 45. *(1) Скуп $\mathbb{N} \times \mathbb{N}$ је пребројив. Уопште, Декартов производ два пребројива скупа је пребројив.*
(2) За свако $n \geqslant 3$, скуп $\mathbb{N}^n$ је пребројив.
(3) Пребројива унија пребројивих скупова је пребројив скуп.
(4) Скуп коначних низова пребројивог скупа је пребројив.
(5) Скуп коначних подскупова пребројивог скупа је пребројив.

Доказ. (1) Није тешко показати да су функције:

- $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $f(n) = (n, 0)$,
- $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $g(m, n) = 2^m \cdot 3^n$,

1-1 функције, па је $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, према Кантор-Бернштајновој теореми.
(2) Једноставно се доказује индукцијом.
(3) Пребројива фамилијом пребројивих скупова јесте заправо низ скупова $(A_n)_{n\in\mathbb{N}}$, од којих је сваки пребројив, $|A_n| = |\mathbb{N}|$, за свако $n \in \mathbb{N}$. Треба доказати да је скуп $A = \bigcup_{n\in\mathbb{N}} A_n$ такође пребројив.

За свако $n \in \mathbb{N}$, скуп A_n је пребројив, па постоји бијекција $f_n : \mathbb{N} \overset{1-1}{\underset{\text{на}}{\to}} A_n$. Дефинишимо функцију $f : \mathbb{N} \times \mathbb{N} \to A$ на следећи начин:

$$f(m, n) = f_m(n),\ (m, n) \in \mathbb{N} \times \mathbb{N}.$$

Функција f је на функција: за свако $a \in A = \bigcup_{n\in\mathbb{N}} A_n$, постоји $m \in \mathbb{N}$ такав да $a \in A_m$. Како је f_m бијекција између $\mathbb{N}$ и A_m, даље следи да постоји $n \in \mathbb{N}$ такав да је $f_m(n) = a$, па је $f(m, n) = a$. Према теореми 44 закључујемо да је A највише пребројив скуп, односно пребројив, јер очигледно није коначан.
(4) Тврђење директно следи из (2) и (3): $\bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ је пребројив.
(5) Сваком коначном низу на природан начин придружујемо коначан скуп (чији су елементи чланови низа):

Нпр:
$(1, 2) \mapsto \{1, 2\}$
$(1, 2, 1, 1) \mapsto \{1, 2\}$
$(0, 0, 0) \mapsto \{0\}$ ...

$$(x_1, \ldots, x_k) \mapsto \{x_1, \ldots, x_k\}$$

при чему, празном низу придружујемо празан скуп. На овај начин, дефинисана је функција из скупа свих коначних низова природних бројева **на** скуп свих коначних подскупова природних бројева. Према (4) и Теореми 44 изводимо жељени закључак. □

5. Операцијско-релацијске структуре

Појам математичке структуре заузима централно место у савременој математици. Уопштено говорећи, математичку структуру чини неки скуп, такозвани *домен*, *носач* или *универзум* структуре, **заједно са** релацијама и операцијама дефинисаним над доменом. Издвајамо један пример типичне структуре, коју чине:

Иако се идеја структуре, у извесном смислу, среће и у радовима Лајбница, верује се да је Шредер 1895. године први пут дефинисао појам апстрактне структуре.

- скуп $\mathbb{N}^+ = \{1, 2, 3, 4, \ldots\}$,
- бинарне операције: сабирање $(+)$, множење $(\cdot)$, степеновање $(\uparrow)$, при чему ћемо уместо $m \uparrow n$ краће писати m^n, и
- константа 1.

Ову структуру краће означавамо као уређену петорку, наводећи све оно што је чини: $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$. Средином шездесетих година, Алфред Тарски је проучавао законитости које важе у овој структури, полазећи од основних идентитета које је назвао *средњошколским идентитетима*:

HSI – High School Identities

$$(HSI)\ \begin{cases} \forall x \forall y (x + y = y + x) \\ \forall x \forall y \forall z (x + (y + z) = (x + y) + z) \\ \forall x (x \cdot 1 = x) \\ \forall x \forall y (x \cdot y = y \cdot x) \\ \forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\ \forall x \forall y \forall z (x \cdot (y + z) = x \cdot y + x \cdot z) \\ \forall x (x^1 = x) \\ \forall x (1^x = 1) \\ \forall x \forall y \forall z (x^{y+z} = x^y \cdot x^z) \\ \forall x \forall y \forall z ((x \cdot y)^z = x^z \cdot y^z) \\ \forall x \forall y \forall z ((x^y)^z = x^{y \cdot z}) \end{cases}$$

Занимљиво је да наведене идентитете задовољавају и разне друге структуре *истог типа*. Једна таква структура је $(\{0, 1\}, +, \cdot, \uparrow, 1)$, са доменом $\{0, 1\}$ над којим су дате три бинарне операције (дефинисане наредним таблицама) и константа 1:

Подсећамо на следеће парове еквивалентних исказних формула:
$x \vee y \equiv y \vee x$
$x \vee (y \vee z) \equiv (x \vee y) \vee z$
$x \wedge 1 \equiv x$
$x \wedge y \equiv y \wedge x$
$x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z$
$x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$
$1 \Rightarrow x \equiv x$
$x \Rightarrow 1 \equiv 1$
$y \vee z \Rightarrow x \equiv (y \Rightarrow x) \wedge (z \Rightarrow x)$
$z \Rightarrow x \wedge y \equiv (z \Rightarrow x) \wedge (z \Rightarrow y)$
$z \Rightarrow (y \Rightarrow x) \equiv z \wedge y \Rightarrow x$

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$\uparrow$	0	1
0	1	0
1	1	1

Није тешко уочити да операције $+$ и $\cdot$ заправо представљају редом дисјункцију и конјункцију над $\{0, 1\}$, а да $x \uparrow y$, тј. x^y заправо одговара исказној формули $y \Rightarrow x$. Једноставно је проверовати да у структури $(\{0, 1\}, +, \cdot, \uparrow, 1)$ важе све HSI законитости. Све структуре одговарајућег типа, које задовољавају HSI законитости називају се HSI алгебрама.

5.1. **Бројевне структуре**

20

Најважније примере структура чине оне над скуповима бројева. Овај одељак садржи кратак опис неких основних конструкција.

▼ Цели бројеви

Ако су m и n природни бројеви такви да је $m \leqslant n$, онда постоји само један (због закона скраћивања) природан број k такав да је $n = m + k$; овај број означавамо са $n - m$ и називамо разликом природних бројева n и m. Уколико је пак $n < m$, тада **не постоји** природан број k који можемо додати броју m да бисмо добили n. Другим речима, једначине по x, као што су на пример $2 + x = 1$, $13 + x = 8$,..., немају решења међу природним бројевима. Ово се најчешће узима као главни разлог уводјења негативних бројева: -1 [као решење једначина $1 + x = 0$, $2 + x = 1$, $3 + x = 2$, ...], -2, -3, ... Свака једначина по x, облика $a + x = b$, једнозначно је одређена уредјеним паром природних бројева (a, b), и зато скуп свих једначина наведеног облика идентификујемо са скупом $\mathbb{N} \times \mathbb{N}$. На скупу $\mathbb{N} \times \mathbb{N}$ дефинишемо бинарну релацију $\sim$ на следећи начин:

$$(a, b) \sim (c, d) \overset{\text{def}}{\Leftrightarrow} a + d = b + c.$$

Дефиниција релације $\sim$ потпуно је у складу са нашим искуством и намерама: две једначине $a + x = b$ и $c + x = d$ имају *исто* решење акко је $b - a = d - c$, тј. $a + d = b + c$.

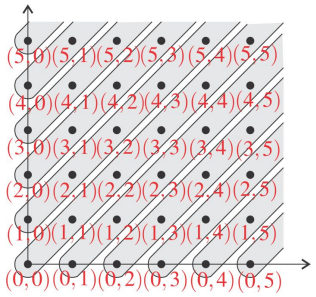
Лема 9. *Релација $\sim$ је релација еквиваленције на скупу $\mathbb{N} \times \mathbb{N}$.*

Доказ. (Р) Из $a + b = a + b$ следи $(a, b) \sim (a, b)$.

(С) Ако је $(a, b) \sim (c, d)$, онда је $a + d = b + c$. Из последње једнакости једноставно се добија $c + b = d + a$, па је $(c, d) \sim (a, b)$.

(Т) Нека је $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$. Из једнакости $a + d = b + c$ и $c + f = d + e$ добијамо:

$$(*) \qquad (a + d) + (c + f) = (b + c) + (d + e).$$



Применом комутативности и асоцијативности изводимо:

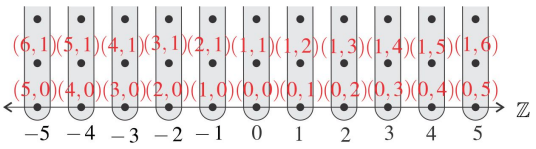
$$(a+d)+(c+f) = \cdots = (a+f)+(c+d) \quad \text{и} \quad (b+c)+(d+e) = \cdots = (b+e)+(c+d).$$

Из једнакости $(*)$ и последње две једнакости добијамо $(a + f) + (c + d) = (b + e) + (c + d)$, и најзад, применом закона скраћивања: $a + f = b + e$. Дакле, $(a, b) \sim (e, f)$. □

Количнички скуп $\mathbb{N} \times \mathbb{N}/\sim$ називамо скупом целих бројева и означавамо $\mathbb{Z}$. За сваки природан број a:

Решење једначине $0 + x = a$ је a; решење једначине $a + x = 0$ означавамо $-a$.

- класу $[(0, a)]_\sim$ краће означавамо a;
- класу $[(a, 0)]_\sim$ краће означавамо $-a$.



Сабирање и множење целих бројева уводимо ослањајући се на следеће:

1) ако су цели бројеви x и y решења једначине $a+x=b$ и $c+y=d$, онда је $x+y$ решење једначине $(a+c)+z=b+d$;

2) ако су цели бројеви x и y решења једначине $a+x=b$ и $c+y=d$, онда је $x\cdot y$ решење једначине $(ad+bc)+z=ac+bd$.

Запажање 2) се "наивно"може оправдати на следећи начин: из $x=b-a$ и $y=d-c$ следи:

$$\begin{aligned} xy &= (b-a)(d-c) \\ &= bd-ad-bc+ac \\ &= (ac+bd)-(ad+bc) \end{aligned}$$

Додатно, потребно је показати да: збир и производ целих бројева не зависи од избора једначина које их одређују.

Лема 10. *Ако је* $(a,b)\sim(a_1,b_1)$ *и* $(c,d)\sim(c_1,d_1)$, *онда је:*

- $(a+c,b+d)\sim(a_1+c_1,b_1+d_1)$;
- $(ad+bc,ac+bd)\sim(a_1d_1+b_1c_1,a_1c_1+b_1d_1)$.

Сабирање и множење целих бројева, $+_{\mathbb{Z}},\cdot_{\mathbb{Z}}:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ дефинишемо једнакостима:

$$[(a,b)]_\sim +_{\mathbb{Z}} [(c,d)]_\sim \stackrel{\text{def}}{=} [(a+b,c+d)]_\sim, \quad [(a,b)]_\sim \cdot_{\mathbb{Z}} [(c,d)]_\sim \stackrel{\text{def}}{=} [(ad+bc,ac+bd)]_\sim.$$

На пример, користећи договорно краће означавање:

Једнакост $[(5,3)]_\sim=[(2,0)]_\sim$, следи из $(5,3)\sim(2,0)$, тј. $5+0=3+2$.

$$\begin{aligned} 3+_{\mathbb{Z}}(-5) &= [(0,3)]_\sim +_{\mathbb{Z}} [(5,0)]_\sim \\ &= [(0+5,3+0)]_\sim = [(5,3)]_\sim = [(2,0)]_\sim \\ &= -2 \\ 3\cdot_{\mathbb{Z}}(-5) &= [(0,3)]_\sim +_{\mathbb{Z}} [(5,0)]_\sim \\ &= [(0\cdot 0+3\cdot 5, 0\cdot 5+3\cdot 0)]_\sim = [(15,0)]_\sim \\ &= -15 \\ (-3)\cdot_{\mathbb{Z}}(-5) &= [(3,0)]_\sim +_{\mathbb{Z}} [(5,0)]_\sim \\ &= [(3\cdot 0+0\cdot 5, 3\cdot 5+0\cdot 0)]_\sim = [(0,15)]_\sim \\ &= 15 \end{aligned}$$

итд.

Бинарну релацију $\leqslant_{\mathbb{Z}}$ уводимо на следећи начин:

$$[(a,b)]_\sim \leqslant_{\mathbb{Z}} [(c,d)]_\sim \stackrel{\text{def}}{\Leftrightarrow} b+c\leqslant a+d,$$

где је $\leqslant$ уредјење природних бројева. Веома је једноставно доказати коректност ове дефиниције, тј. да из $(a,b)\sim(a_1,b_1)$ и $(c,d)\sim(c_1,d_1)$, следи: $[(a,b)]_\sim\leqslant_{\mathbb{Z}}[(c,d)]_\sim$ акко $[(a_1,b_1)]_\sim\leqslant_{\mathbb{Z}}[(c_1,d_1)]_\sim$. Тада је, на пример:

- $-3\leqslant_{\mathbb{Z}}5$, тј.$[(3,0)]_\sim\leqslant_{\mathbb{Z}}[(0,5)]_\sim$, јер је $0+0\leqslant 3+5$,
- $-5\leqslant_{\mathbb{Z}}-3$, тј.$[(5,0)]_\sim\leqslant_{\mathbb{Z}}[(3,0)]_\sim$, јер је $0+3\leqslant 5+0$,
- $3\leqslant_{\mathbb{Z}}5$, тј.$[(0,3)]_\sim\leqslant_{\mathbb{Z}}[(0,5)]_\sim$, јер је $3+0\leqslant 0+5$, ...

Уобичајено је да се индекс $\mathbb{Z}$ изоставља у ознакама $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$, $\leqslant_{\mathbb{Z}}$, тј. да за сабирање, множење и уређење целих бројева користе исте ознаке као за сабирање, множење и уређење природних бројева, што

је давно усвојен обичај у случајевима када се *увођењем нових бројева, операција и релација са њима, поштују операције и релације старих бројева, тј. када је сачуван рад са старим бројевима.*

Ово начело проширивања скупова бројева познато је и као Хенкелов принцип перманенције.

На скупу целих бројева уводимо и унарну операцију *супротан број* $-:\mathbb{Z}\to\mathbb{Z}$,

$$-[(a,b)]_\sim \overset{\text{def}}{=} [(b,a)]_\sim.$$

Веома је једноставно доказати коректност ове дефиниције: ако је $(a,b)\sim(a_1,b_1)$, онда је $(b,a)\sim(b_1,a_1)$.

Лема 11. *За произвољне* $x,y,z\in\mathbb{Z}$*:*

$x+(y+z)=(x+y)+z$	$x\cdot(y\cdot z)=(x\cdot y)\cdot z$
$x+y=y+x$	$x\cdot y=y\cdot x$
$x+0=x$	$x\cdot 1=x,\ x\cdot 0=0$
$x+(-x)=0$	$x\cdot(y+z)=x\cdot y+x\cdot z$
$x\leqslant x$	$x\leqslant y\wedge y\leqslant x\Rightarrow x=y$
$x\leqslant y\wedge y\leqslant z\Rightarrow x\leqslant z$	$x\leqslant y\vee y\leqslant x$
$x\leqslant y\Rightarrow x+z\leqslant y+u$	$x\leqslant y\wedge 0\leqslant z\Rightarrow x\cdot z\leqslant y\cdot z$

▼ Рационални бројеви

Ако су a и b цели бројеви, при чему је $a>0$, једначина $a\cdot x=b$ не мора имати решења у скупу целих бројева. Поступајући као раније, скуп целих бројева проширујемо новим бројевима – решењима једначина наведеног типа. Једначину наведениг облика идентификоваћемо са уређеним паром $(a,b)\in\mathbb{N}^+\times\mathbb{Z}$. У наведеном контексту уобичајеније је да уређени пар $(a,b)\in\mathbb{N}^+\times\mathbb{Z}$ означавамо као разломак $\frac{b}{a}$. Да би се поједноставило читање, корисно је у причи која следи уређене парове преводити у разломке. Да бисмо олакшали читање, повремено ћемо понављати

На скупу $\mathbb{N}^+\times\mathbb{Z}$ дефинишемо бинарну релацију $\approx$ на следећи начин:

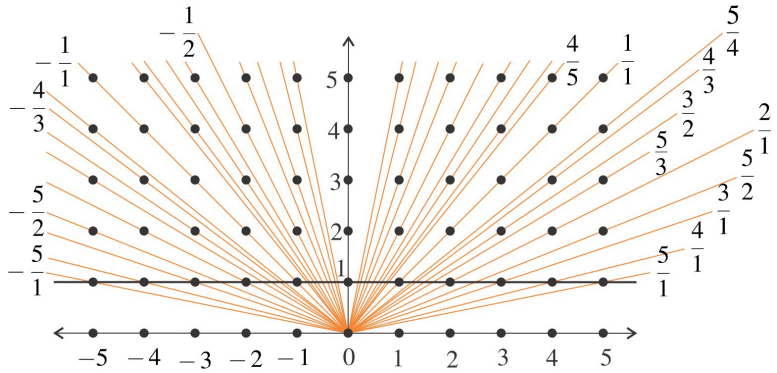
$$(a,b)\approx(c,d)\ \overset{\text{def}}{\Leftrightarrow}\ a\cdot d=b\cdot c.$$

Да бисмо истакли аналогију са увођењем целих бројева, подсећамо на дефиницију релације $\sim$: $(a,b)\sim(c,d)\ \overset{\text{def}}{\Leftrightarrow}\ a+d=b+c$. Релација $\approx$ је заправо једнакост међу разломцима:

$$\frac{b}{a}=\frac{d}{c}\ \Leftrightarrow\ ad=bc.$$

Лема 12. *Релација* $\approx$ *је релација еквиваленције на скупу* $\mathbb{N}^+\times\mathbb{Z}$.

Количнички скуп $\mathbb{N}^+\times\mathbb{Z}/\approx$ називамо скупом целих бројева и означавамо $\mathbb{Q}$.



Сабирање и множење рационалних бројева, $+_{\mathbb{Q}}, \cdot_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, супротан елемент $-_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$, и бинарну релацију $\leqslant_{\mathbb{Q}}$ дефинишемо на следећи начин:

- $[(a,b)]_\approx +_{\mathbb{Q}} [(c,d)]_\approx \stackrel{\text{def}}{=} [(ac, bc+ad)]_\approx$; $\quad \frac{b}{a} + \frac{d}{c} = \frac{bc+ad}{ac}$
- $[(a,b)]_\approx \cdot_{\mathbb{Q}} [(c,d)]_\approx \stackrel{\text{def}}{=} [(ac, bd)]_\approx$; $\quad \frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$
- $-_{\mathbb{Q}}[(a,b)]_\approx \stackrel{\text{def}}{=} [(a,-b)]_\approx$; $\quad -\frac{b}{a} = \frac{-b}{a}$
- $[(a,b)]_\approx \leqslant_{\mathbb{Q}} [(c,d)]_\approx \stackrel{\text{def}}{\Leftrightarrow} bd \leqslant ac$. $\quad \frac{b}{a} \leqslant_{\mathbb{Q}} \frac{c}{d} \Leftrightarrow bd \leqslant ac$

Проверу коректности наведених дефиниција препуштамо читаоцима.

Лема 13. *За произвољне* $x, y, z \in \mathbb{Q}$*:*

$x + (y+z) = (x+y) + z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
$x + y = y + x$	$x \cdot y = y \cdot x$
$x + 0 = x$	$x \cdot 1 = x,\ x \cdot 0 = 0$
$x + (-x) = 0$	$x \cdot (y+z) = x \cdot y + x \cdot z$
$(*)\ \ x \neq 0 \Rightarrow (\exists u \in \mathbb{Q})\, x \cdot u = 1$	
$x \leqslant x$	$x \leqslant y \wedge y \leqslant x \Rightarrow x = y$
$x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$	$x \leqslant y \vee y \leqslant x$
$x \leqslant y \Rightarrow x + z \leqslant y + u$	$x \leqslant y \wedge 0 \leqslant z \Rightarrow x \cdot z \leqslant y \cdot z$

5.2. **Структуре и њихов вокабулар**

Операцијско-релацијску структуру чини скуп заједно са неким својим операцијама, релацијама и елементима (константама).

21

$S^n = \underbrace{S \times \cdots \times S}_{n \text{ пута}}$ је скуп свих уређених n-торки елемената из S.

Дефиниција 27. *Нека је S произвољан непразан скуп и $n \geqslant 1$.*

(1) Свака функција из S^n у S, назива се n-арна операција скупа S. Посебно, функције из S у S називамо унарним операцијама; функције из $S \times S$ у S називамо бинарним операцијама.

(2) Сваки подскуп од S^n, назива се n-арна релација скупа S. Посебно, подскупове од S називамо унарним релацијама; подскупове од $S \times S$ називамо бинарним релацијама. Ако је $R \subseteq S^n$ и $a_1, \ldots, a_n \in S$, уместо $(a_1, \ldots, a_n) \in R$ пишемо $R(a_1, \ldots, a_n)$ и читамо 'елементи $a_1, \ldots, a_n$ су у релацији R'. Сваку n-арну релацију можемо посматрати као функцију из S^n у двочлани скуп $\{0, 1\}$ исказних вредности (0 за 'нетачно', 1 за 'тачно'), и самим тим исказе

$$\text{'}R(a_1, \ldots, a_n) \text{ је тачно'} \quad \text{и} \quad \text{'}R(a_1, \ldots, a_n) \text{ је нетачно'}$$

записати као једнакости

$$R(a_1, \ldots, a_n) = 1 \quad \text{и} \quad R(a_1, \ldots, a_n) = 0.$$

Напомена 10. Појам n-арне операције можемо уопштити и у случају када је $n = 0$. За било који скуп S, скуп S^n можемо посматрати као скуп свих n-точланих низова елемената из S; сходно томе, скуп S^0 можемо посматрати као скуп свих низова дужине 0. Будући да постоји само један низ дужине 0, скуп S^0 је једночлан, па неку функцију из S^0 у S одређује избор само једног елемента из S (у који пресликавамо једини елемент скупа S^0). Зато елементе (константе) из S посматрамо и као 0-арне операције скупа S.

Структуре задајемо тако што наведемо, у облику низа, све оно што је чини. Структуре често означавамо масним словима $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$, по потреби са индексима, при чему углавном користимо слова којима су означени домени (носачи) тих структура, $A, B, C, \ldots$, са одговарајућим индексима. Кардиналност структуре је кардиналност његовог домена: кажемо да је нека структура коначна (пребројива, непребројива) ако је њен домен коначан (пребројив, непребројив).

Пример:
Стандардну структуру природних бројева чини скуп природних бројева $\mathbb{N}$, заједно са релацијом уређења $\leqslant$, унарном операцијом следбеник $' : \mathbb{N} \to \mathbb{N}$, (бинарним операцијама) сабирањем и множењем $+, \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, и константом 0: $\mathbf{N} = (\mathbb{N}, \leqslant, ', +, \cdot, 0)$. $\mathbf{N}$ је пример пребројиве структуре.

Вокабулар структуре
Симболи којима означавамо релације, операције и константе неке структуре називамо *вокабуларом* те структуре.

Вокабулар структуре $\mathbf{N}$ чине симболи: $\leqslant, ', +, \cdot, 0$

Вокабулар заједно са логичким симболима чине алфабет тзв. *језика првог реда* који користимо за описивање структуре:

ЛОГИЧКИ СИМБОЛИ
променљиве:
$x, y, z, x_1, y_1, z_1, \ldots$

знак једнакости: $=$
логичке константе: $\bot$, $\top$
логички везници: (унарни) $\neg$,
(бинарни) $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$
квантификатори: $\forall$, $\exists$
помоћни знаци: лева и десна заграда, запета

ВОКАБУЛАР СТРУКТУРЕ
симболи константи;
симболи операција, при чему је за сваки симбол одређена његова дужина;
симболи релација, при чему је за сваки симбол одређена његова дужина.

Логички симболи су непроменљиви део језика првог реда, док симболе вокабулара одређује тип структуре коју посматрамо.

Изрази
Изразе градимо индуктивно, на уобичајен начин, користећи променљиве, симболе константи, симболе операција и помоћне знаке:

- Променљиве и симболи константи су изрази;
- Ако је F симбол операције дужине n и ако су $t_1, \ldots, t_n$ изрази, онда је $F(t_1, \ldots, t_n)$ израз. Специјално, ако је F симбол бинарне операције, и t_1, t_2 изрази, онда је уместо $F(t_1, t_2)$ углавном пишемо $t_1 F t_2$, користећи по потреби и заграде $(t_1 F t_2)$.

Примери израза над вокабуларом структуре $\mathbf{N}$: 0, $0'$, $0' \cdot (0')'$, $(x + 0)'$, $x + y$, $0' \cdot (x + 0')$, $x \cdot x + y \cdot y$, итд. Приликом записивања израза користимо уобичајене конвенције о брисању заграда, нпр. попут усвајања приоритета међу операцијама, да би се изоставило писање заграда.

Ако је t неки израз, са $V(t)$ означићемо скуп оних променљивих које учествују у грађењу израза t. Наравно, за сваки израз t, скуп $V(t)$ је коначан:

- $V(v) = \{v\}$, за променљиву v; $V(c) = \emptyset$, за симбол константе c;
- $V(F(t_1, \ldots, t_n)) = V(t_1) \cup \cdots \cup V(t_n)$, за симбол операције F дужине n и изразе $t_1, \ldots, t_n$.

Атомске формуле

Логичке константе сматрамо атомским формулама. Сложеније *атомске формуле* добијамо повезивањем два израза знаком једнакости, одн. повезивањем одговарајућег броја израза симболом релације.

- Логичке константе $\bot$ и $\top$ су атомске формуле;
- Ако си t_1 и t_2 изрази, онда је $t_1 = t_2$ атомска формула;
- Ако је R симбол релације дужине n и ако су t_1, $\ldots$, t_n изрази, онда је $R(t_1, \ldots, t_n)$ атомска формула.

Примери атомских формула над вокабуларом структуре $\mathbf{N}$: $0 = 0$, $0 \leqslant 0'$, $(x \cdot 0) \leqslant (x + 0)$, $x + y = y + x$ итд.

Формуле

Формуле дефинишемо индуктивно, полазећи од атомских формула и повезујући их логичким везницима, одн. постављањем квантификатора са променљивом.

- Атомске формуле су формуле;
- Ако је α формула, онда је $\neg\alpha$ такође формула;
- Ако су α и β формуле и $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$, онда је $(\alpha * \beta)$ формула;
- Ако је α формула, v нека променљива, онда су $\forall v\alpha$ и $\exists v\alpha$ формуле.

Примери формула над вокабуларом структуре $\mathbf{N}$: $0 = x$, $0 = 0 \wedge \neg 0' \leqslant 0$, $0' \leqslant x \Rightarrow x \leqslant (x \cdot x)$, $\neg\exists x(x + 0') = 0$, $\forall x \forall y(x + y = y + x)$ итд.

Слободна и везана појављивања променљивих

Појављивање променљиве у формули може бити *слободно* или *везано*. Свако појављивање променљиве које није под дејством квантификатора назива се слободним, а она појављивања која јесу под дејством квантификатора називају се везаним.

Све променљиве које имају слободна појављивања у некој формули називају се **слободне променљиве** те формуле. Скуп свих слободних променљивих формуле α означавамо $\mathrm{Fr}(\alpha)$ и прецизно дефинишемо индукцијом по сложености формуле:

- $\mathrm{Fr}(\bot) = \mathrm{Fr}(\top) = \emptyset$;
- $\mathrm{Fr}(t_1 = t_2) = V(t_1) \cup V(t_2)$;
- $\mathrm{Fr}(R(t_1, \ldots, t_n)) = V(t_1) \cup \cdots \cup V(t_n)$;
- $\mathrm{Fr}(\neg\alpha) = \mathrm{Fr}(\alpha)$;

- $\mathrm{Fr}(\alpha * \beta) = \mathrm{Fr}(\alpha) \cup \mathrm{Fr}(\beta)$, $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$;
- $\mathrm{Fr}(\forall x\alpha) = \mathrm{Fr}(\exists x\alpha) = \mathrm{Fr}(\alpha) \setminus \{x\}$.

За сваку формулу α, скуп $\mathrm{Fr}(\alpha)$ је коначан.

Вредност израза

Изразима, над вокабуларом неке структуре $\mathbf{S}$, дефинишу се нове функције, заправо операције над S, на сасвим природан начин. Ако је $V(t) \subseteq \{x_1, \ldots, x_n\}$, онда израз t означавамо $t(x_1, \ldots, x_n)$ када желимо да истакнемо су све променљиве које учествују у грађењу израза t неке од променљивих $x_1, \ldots, x_n$. Додељујући променљивама $x_1, \ldots, x_n$ редом неке вредности $a_1, \ldots, a_n$ из S, добијамо јединствену вредност $t(a_1, \ldots, a_n) \in S$:

$$S^n \ni (a_1, \ldots, a_n) \mapsto t(a_1, \ldots, a_n) \in S;$$

на овај начин је дефинисана једна функција (заправо n-арна операција) из S^n у S.

Вредност израза (функције)

Најједноставније функције дефинисане изразима јесу пројекције и константе функције (тј. функције одређене најједноставнијим изразима):

$$(x_1, \ldots, x_n) \mapsto x_i, (1 \leqslant i \leqslant n) \text{ и } (x_1, \ldots, x_n) \mapsto c.$$

Сложеније функције одређују неки изрази $t_1, \ldots, t_m$, такви да је $V(t_1), \ldots, V(t_m) \subseteq \{x_1, \ldots, x_n\}$ и неки симбол операције F дужине m:

$$(x_1, \ldots, x_n) \mapsto F(t_1, \ldots, t_m).$$

Функције дефинисане изразима можемо описати и на следећи начин: полазећи од пројекција и константних функција,

$$(x_1, \ldots, x_n) \mapsto x_i, (1 \leqslant i \leqslant n) \text{ и } (x_1, \ldots, x_n) \mapsto c,$$

сложеније функције генеришемо тзв. супституцијама – постављањем већ дефинисаних функција као аргумената неког симбола операције.

Примери функција дефинисаних изразима над вокабуларом структуре $\mathbf{N}$:

- $t_1(x) = 0$ – константна функција (једног аргумента);
- $t_2(x, y) = 0'$ – константна функција (два аргумента);
- $t_3(x_1, x_2, x_3) = x_2$ – пројекција (на другу координату);
- $t_4(x, y) = x' \cdot (y + 0')$
- $t_5(x_1, x_2, x_3) = x_1' \cdot (x_2 + 0')$ итд.

Вредности израза t_5 за неке валуације променљивих:

- $t_5(2, 1, 4) = 2' \cdot (1 + 0') = 6$
- $t_5(3, 3, 3) = 3' \cdot (3 + 0') = 16$
- $t_5(7, 13, 31) = 7' \cdot (13 + 0') = 112$ итд.

Тачност формуле

Ако је $\mathrm{Fr}(\alpha) \subseteq \{x_1, \ldots, x_n\}$, онда формулу α означавамо и са $\alpha(x_1, x_2, \ldots, x_n)$ када желимо да истакнемо чињеницу да су све слободне променљиве формуле α неке од променљивих $x_1, x_2, \ldots, x_n$. Додељујући променљивама $x_1, \ldots, x_n$ редом неке вредности $a_1, \ldots, a_n$ из M, добијамо јединствену *истинитосну* вредност $\alpha(a_1, \ldots, a_n)$:

$$S^n \ni (a_1, \ldots, a_n) \mapsto \alpha(a_1, \ldots, a_n) \in \{0, 1\};$$

на овај начин је дефинисана једна функција из S^n у $\{0,1\}$, тј. једна n-арна релација скупа S.

Истинитосна вредност формуле

Полазећи од основних релација које одређују атомске формуле, сложеније релације градимо користећи исказне везнике и квантификаторе заједно са променљивама:

- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\neg\theta(x_1,\ldots,x_n)$, онда је за $a_1,\ldots,a_n \in S$,
$$\alpha(a_1,\ldots,a_n) = \neg\theta(a_1,\ldots,a_n);$$
- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\theta_1(x_1,\ldots,x_n) * \theta_2(x_1,\ldots,x_n)$, $* \in \{\wedge,\vee,\Rightarrow,\Leftrightarrow\}$, онда је за $a_1,\ldots,a_n \in S$,
$$\alpha(a_1,\ldots,a_n) = \theta_1(a_1,\ldots,a_n) * \theta_2(a_1,\ldots,a_n);$$
- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\forall x\theta(x,x_1,\ldots,x_n)$, онда је за $a_1,\ldots,a_n \in S$,
$$\alpha(a_1,\ldots,a_n) = \min_{a\in S}\theta(a,a_1,\ldots,a_n);$$
- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\exists x\theta(x,x_1,\ldots,x_n)$, онда је за $a_1,\ldots,a_n \in S$,
$$\alpha(a_1,\ldots,a_n) = \max_{a\in S}\theta(a,a_1,\ldots,a_n).$$

Примери релација дефинисаних изразима над вокабуларом структуре $\mathbf{N}$:

- $\alpha_1(x)$ је формула $0'' \leqslant x$; нпр. $\alpha_1(0)$ је нетачно ($\alpha_1(0) = 0$), а $\alpha_1(4)$ је тачно ($\alpha_1(4) = 1$) итд.
- $\alpha_2(x,y)$ је формула $x' = y$; нпр. $\alpha_2(3,2)$ је нетачно ($\alpha_2(3,2) = 0$), а $\alpha_2(2,3)$ је тачно ($\alpha_2(2,3) = 1$) итд.
- $\alpha_3(x_1,x_2)$ је $x_1 \leqslant x_2' \Rightarrow x_1' \leqslant x_2$; нпр. $\alpha_2(2,1)$ је нетачно, $\alpha_2(2,5)$ је тачно, $\alpha_2(5,2)$ је тачно, итд.
- $\alpha_4(x,y)$ је $x' \leqslant y \Rightarrow x \leqslant y'$; нпр. $\alpha_4(0,0)$, $\alpha_4(0,1)$, $\alpha_4(1,0)$, $\alpha_4(0,2)$, $\alpha_4(2,0)$ су тачни искази;
- $\alpha_5(x,y)$ је формула $\exists z\,(x + z = y)$; нпр. $\alpha_5(3,0)$ је нетачно, $\alpha_5(0,3)$ је тачно, итд.
- $\alpha_6(x)$ је формула $\forall y\,(x \cdot y = x)$; нпр. $\alpha_5(0)$ је тачно, $\alpha_5(1)$ је нетачно, итд.

Задатак **10.** На вокабулару структуре $\mathbf{N}$ дате су формуле:

- $\alpha(x,y)$ је $\neg x = 0 \wedge \neg y = 0 \wedge \exists z\,(x \cdot z = y)$
- $\beta(x)$ је $0'' \leqslant x \wedge \exists y \exists z\,(x = y \cdot z \Rightarrow y = 1 \vee y = 1)$
- $\gamma(x,y)$ је $\exists z(x + (z + z) = y \vee y + (z + z) = x)$.

Одреди, ако постоје, једну валуацију променљивих за коју је формула тачна, и једну валуацију променљивих за коју је формула нетачна.

Тачност реченице

Формула σ је **реченица** ако нема слободних променљивих, тј. ако је $\mathrm{Fr}(\alpha) = \emptyset$. На (не)истинитост реченице у некој структури не утичу валуације променљивих. Да је реченица σ тачна у некој структури $\mathbf{S}$, записујемо $\mathbf{S} \models \sigma$ и кажемо да је структура $\mathbf{S}$ *модел* реченице σ. Ако реченица σ није тачна у $\mathbf{S}$ пишемо $\mathbf{S} \not\models \sigma$ и кажемо да је $\mathbf{S}$ *контрамодел* реченице σ. Приметимо да ако $\mathbf{S} \not\models \sigma$, онда $\mathbf{S} \models \neg\sigma$.

Пример 57. $(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x \forall y (x + y = 0 \Rightarrow x = 0 \wedge y = 0)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x (\neg x = 0 \Rightarrow \exists y (x = y'))$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \exists y \forall x (x \cdot y = x)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \neg \exists x (x \cdot x = 0'')$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \exists x (x \cdot x = 0'''')$
итд.

Задатак **11.** Koje od следећих реченица су тачне у $(\mathbb{N}, \leqslant, ', +, \cdot, 0)$?

1. $\forall x \forall y \forall z (x \cdot y = x \cdot z \Rightarrow y = z)$
2. $\exists x \, (x \cdot x = x'')$
3. $\forall x \forall y \exists z (x = y \vee x + z = y \vee y + z = x)$

5.3. **Различите интерпретације једног вокабулара. Теорије.**

22

Најједноставнија класификација (операцијско-релацијских) структура врши се према вокабулару, тј. према броју и дужини релација и операција, као и броју константи које учествују у њиховој дефиницији. За структуре које имају исти вокабулар кажемо да су истог типа.

Пример 58. Посматрајмо неколико структура које имају иста својства као: адитивне структуре целих бројева $(\mathbb{Z}, +, -, 0)$ и рационалних бројева $(\mathbb{Q}, +, -, 0)$:

Слово A означава закон **а**социјативности; слово N постојање **н**еутралног елемента; слово I чињеницу да сваки елемент има тзв. **и**нверз.

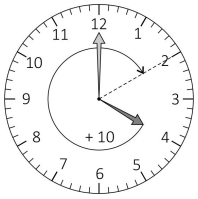
$$\begin{array}{ll} \text{(A)} & \forall x \forall y \forall z\ (x + (y + z) = (x + y) + z) \\ \text{(N)} & \forall x\ (x + 0 = x) \\ \text{(I)} & \forall x\ (x + (-x) = 0) \end{array}$$

и као мултипликативна структура рационалних бројева $(\mathbb{Q} \setminus \{0\}, \cdot, ^{-1}, 1)$

$$\begin{array}{ll} \text{(A)} & \forall x \forall y \forall z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\ \text{(N)} & \forall x\ (x \cdot 1 = x) \\ \text{(I)} & \forall x\ (x \cdot x^{-1} = 1) \end{array}$$

1. Структура

$$(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, \oplus, \ominus, 12)$$



карактерише тзв. аритметику часовника. Бинарна операција $\oplus$ скупа $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, дефинисана је на следећи начин:

$$x \oplus y = \begin{cases} x + y, & x + y \leqslant 12, \\ x + y - 12, & x + y > 12. \end{cases}$$

$\oplus$	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Није тешко проверити да је $\oplus$ асоцијативна операција,

(A) $\forall x \forall y \forall z\ (x \oplus (y \oplus z) = (x \oplus y) \oplus z)$;

да је 12 неутрални елемент за $\oplus$,

(N) $\forall x\ (x \oplus 12 = x)$;

и да сваки елемент има инверзни елемент одређен табелом:

x	1	2	3	4	5	6	7	8	9	10	11	12
$\ominus x$	11	10	9	8	7	6	5	4	3	2	1	12

,

при чему је

(I) $\forall x\ (x \oplus (\ominus x) = 12)$.

2. Наведимо још једну структуру истог типа. За било који скуп X,

• композиција две бијекције $f : X \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} X$ и $g : X \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} X$ такође је једна бијекција $f \circ g : X \to X$,

• идентичко пресликавање је бијекција, $\mathrm{id}_X : X \overset{1-1}{\underset{\text{на}}{\rightrightarrows}} X$, и

• за сваку бијекцију $f : X \overset{1-1}{\underset{\text{на}}{\rightarrow}} X$ постоји инверзна бијекција $f^{-1} : X \overset{1-1}{\underset{\text{на}}{\rightarrow}} X$.

Ако са S_X означимо скуп свих бијекција (пермутација) скупа X, онда је композиција $\circ$ одређује једну бинарну операцију скупа S_X, инверз $^{-1}$ одређује једну унарну операцију на S_X и id_X је један елемент (скупа) S_X. У структури $(S_X, \circ, ^{-1}, \mathrm{id}_X)$ тачне су следеће реченице:

(A) $\forall f \forall g \forall h\ (f \circ (g \circ h) = (f \circ g) \circ h)$

(N) $\forall f\ (f \circ \mathrm{id}_X = f)$

(I) $\forall f\ (f \circ f^{-1} = \mathrm{id}_X)$

3. Најзад, нека је S било који скуп. На скупу $\mathcal{P}(S)$ посматрајмо тзв. *симетричну разлику*: $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$ и нека је $\mathbf{I}$ унарна операција на $\mathcal{P}(S)$ дефинисана са $\mathbf{I}(A) = A$. У структури $(\mathcal{P}(S), \triangle, \mathbf{I}, \emptyset)$ тачне су следеће реченице:

(A) $\forall X \forall Y \forall Z\ (X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z)$

(N) $\forall X\ (X \triangle \emptyset = X)$

(I) $\forall X\ (X \triangle \mathbf{I}(X) = \emptyset)$

Ако је $X = \{1, 2, 3\}$, све бијекције (пермутације) скупа X су:

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\circ$	σ_1	σ_2	σ_3	τ_1	τ_2	τ_3
σ_1						
σ_2						
σ_3						
τ_1						
τ_2						
τ_3						

У претходном примеру илустрован је веома важан начин увођења операцијско-релацијских структура. Међу структурама истог типа (тј. структурама које имају исти тип вокабулара) издвајамо оне које задовољавају неке изабране особине, тј. задовољавају одређене *теорије*.

Дефиниција 28. *Теорија неког вокабулара јесте било који скуп реченица тог вокабулара.*

Наводимо неке важне примере теорија.

Теорија група. Вокабулар група чини симбол једне бинарне операције, симбол једне унарне операције и симбол једне константе; често се у општем случају користе следећи симболи: $*$, $^{-1}$, e. Теорију група чине следеће реченице:

(A) $\forall x \forall y \forall z\ (x * (y * z) = (x * y) * z)$

(N) $\forall x\ (x * e = x)$

(I) $\forall x\ (x * x^{-1} = e)$

Група је свака структура $(G, *, ^{-1}, e)$ која задовољава наведене аксиоме. У претходном примеру наведено је неколико примера група.

Теорија Булових алгебри. Вокабулар чине симболи две бинарне операције $\curlyvee$ и $\curlywedge$, симбол једне унарне операције $^{\mathrm{c}}$ и два симбола константе 0 и 1. Теорија Булових алгебри садржи следеће реченице:

$\mathbf{A}^{\curlyvee}$	$\forall x\forall y\forall z(x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z)$	$\mathbf{A}^{\curlywedge}$	$\forall x\forall y\forall z(x \curlywedge (y \curlywedge z) = (x \curlywedge y) \curlywedge z)$
$\mathbf{K}^{\curlyvee}$	$\forall x\forall y(x \curlyvee y = y \curlyvee x)$	$\mathbf{K}^{\curlywedge}$	$\forall x\forall y(x \curlywedge y = y \curlywedge x)$
$\mathbf{D}^{\curlyvee}_{\curlywedge}$	$\forall x\forall y\forall z(x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z))$	$\mathbf{D}^{\curlywedge}_{\curlyvee}$	$\forall x\forall y\forall z(x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z))$
$\mathbf{C}^{\curlyvee}$	$\forall x(x \curlyvee x^{\complement} = 1)$	$\mathbf{C}^{\curlywedge}$	$\forall x(x \curlywedge x^{\complement} = 0)$
$\mathbf{N}^{\curlyvee}$	$\forall x(x \curlyvee 0 = x)$	$\mathbf{N}^{\curlywedge}$	$\forall x(x \curlywedge 1 = x)$

Булова алгебра је свака структура $(B, \curlyvee, \curlywedge, ', 0, 1)$ у којој су тачне наведене реченице.

Пример 59. Ако је S било који скуп, $(\mathcal{P}(S), \cup, \cap, ^{\complement}, \emptyset, S)$ јесте Булова алгебра, јер за све $X, Y, Z \in \mathcal{P}(S)$ важи:

$\mathbf{A}^{\cup}$	$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$\mathbf{A}^{\cap}$	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$
$\mathbf{K}^{\cup}$	$X \cup Y = Y \cup X$	$\mathbf{K}^{\cap}$	$X \cap Y = Y \cap X$
$\mathbf{D}^{\cup}_{\cap}$	$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$\mathbf{D}^{\cap}_{\cup}$	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
$\mathbf{N}^{\cup}$	$X \cup \emptyset = X$	$\mathbf{N}^{\cap}$	$X \cap S = X$
$\mathbf{C}^{\cup}$	$X \cup X^{\complement} = S$	$\mathbf{C}^{\cap}$	$X \cap X^{\complement} = \emptyset$

Алгебра $(\{0,1\}, \vee, \wedge, \neg, 0, 1)$, са уобичајеним логичким везницима, такође је једна Булова алгебра, јер за све $p, q, r \in \{0,1\}$ важи:

$\mathbf{A}^{\vee}$	$p \vee (q \vee r) = (p \vee q) \vee r$	$\mathbf{A}^{\wedge}$	$p \wedge (q \wedge r) = (p \wedge q) \wedge r$
$\mathbf{K}^{\vee}$	$p \vee q = q \vee p$	$\mathbf{K}^{\wedge}$	$p \wedge q = q \wedge p$
$\mathbf{D}^{\vee}_{\wedge}$	$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$	$\mathbf{D}^{\wedge}_{\vee}$	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
$\mathbf{N}^{\vee}$	$p \vee 0 = p$	$\mathbf{N}^{\wedge}$	$p \wedge 1 = p$
$\mathbf{C}^{\vee}$	$p \vee \neg p = 1$	$\mathbf{C}^{\wedge}$	$p \wedge \neg p = 0$

Занимљив пример Булове алгебре добијамо разматрајући скуп D_n свих природних делилаца неког природног броја n који је производ различитих простих бројева (дакле, n није дељив квадратом неког простог броја). Није тешко показати, користећи елементарна својства најмањег заједничког садржаоца и највећег заједничког делиоца, да је $\mathbf{D}_n = (D_n, \mathrm{nzs}, \mathrm{nzd}, n/, 1, n)$ једна Булова алгебра (комплемент елемента $x \in D_n$ је n/x), тј. да за било које x, y, z важе следеће једнакости:

$\mathbf{A}^{\curlyvee}$	$\mathrm{nzs}(x, \mathrm{nzs}(y, z)) = \mathrm{nzs}(\mathrm{nzs}(x, y), z)$	$\mathbf{A}^{\curlywedge}$	$\mathrm{nzd}(x, \mathrm{nzd}(y, z)) = \mathrm{nzd}(\mathrm{nzd}(x, y), z)$
$\mathbf{K}^{\curlyvee}$	$\mathrm{nzs}(x, y) = \mathrm{nzs}(y, x)$	$\mathbf{K}^{\curlywedge}$	$\mathrm{nzd}(x, y) = \mathrm{nzd}(y, x)$
$\mathbf{D}^{\curlyvee}_{\curlywedge}$	$\mathrm{nzs}(x, \mathrm{nzd}(y, z)) = \mathrm{nzd}(\mathrm{nzs}(x, y), \mathrm{nzs}(x, z))$	$\mathbf{D}^{\curlywedge}_{\curlyvee}$	$\mathrm{nzd}(x, \mathrm{nzs}(y, z)) = \mathrm{nzs}(\mathrm{nzd}(x, y), \mathrm{nzd}(x, z))$
$\mathbf{C}^{\curlyvee}$	$\mathrm{nzs}\left(x, \frac{n}{x}\right) = n$	$\mathbf{C}^{\curlywedge}$	$\mathrm{nzd}\left(x, \frac{n}{x}\right) = 1$
$\mathbf{N}^{\curlyvee}$	$\mathrm{nzs}(x, 1) = x$	$\mathbf{N}^{\curlywedge}$	$\mathrm{nzd}(x, n) = x$

Теорија уређења. Вокабулар чини симбол једне бинарне релације $\leqslant$. Теорију уређења чине следеће реченице:

(R) $\forall x\ (x \leqslant x)$

(AS) $\forall x\forall y\ (x \leqslant y \wedge y \leqslant x \Rightarrow x = y)$

(T) $\forall x\forall y\forall z\ (x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z)$

Уређење је структура $(P, \leqslant)$ која задовољава наведене аксиоме. Примери уређења су $(\mathbb{N}, \leqslant)$ и $(\mathcal{P}(S), \subseteq)$, за било који скуп S.

Теорија линеарних уређења. Вокабулар чини симбол једне бинарне релације $\leqslant$. Теорију линеарних уређења чине следеће реченице:

(R) $\forall x\ (x \leqslant x)$

(AS) $\forall x \forall y\ (x \leqslant y \wedge y \leqslant x \Rightarrow x = y)$

(T) $\forall x \forall y \forall z\ (x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z)$

(L) $\forall x \forall y\ (x \leqslant y \vee y \leqslant x)$

Уређење је структура $(P, \leqslant)$ која задовољава наведене аксиоме. Структура $(\mathbb{N}, \leqslant)$ је пример линеарног уређења, док $(\mathcal{P}(S), \subseteq)$, када је $|S| \geqslant 2$, није линеарно уређење.

▼ Семантичка и синтаксна последица

23

Један од најважнијих логичких концепата јесте појам *последице*. Уводимо две врсте последице – *семантичку последицу* и *синтаксну последицу*.

Дефиниција 29. *Нека је* Γ *нека теорија (скуп реченица). Реченица* α *је* ***семантичка последица*** *теорије* Γ*, у ознаци* $\Gamma \models \alpha$*, ако за сваку структуру* $\mathbf{S}$*,*

$$\textit{из } \mathbf{S} \models \gamma,\ \textit{за свако } \gamma \in \Gamma, \textit{следи да } \mathbf{S} \models \alpha.$$

Уместо $\emptyset \models \alpha$ *пишемо* $\models \alpha$*.*

Ако је $\models \alpha$, тј. α је тачно у свим структурама одговарајућег вокабулара, кажемо да је α ваљана реченица.

Посебно истичемо да знак $\models$ користимо двојако:

- као ознаку односа између структуре и реченице; $\mathbf{S} \models \alpha$ значи да је α **тачно** у структури $\mathbf{S}$;
- као ознаку односа између скупа реченица и једне реченице; $\Gamma \models \alpha$ значи да је α **семантичка последица** скупа формула Γ.

Пример 60. Посматрајмо тврђење

($\star$) *У свакој групи важи десни закон канцелације (скраћивања).*

Нека Γ_{GR} означава теорију група. Десни закон канцелације, на језику теорије група, изражавамо следећом реченицом

$$\sigma: \quad \forall x \forall y \forall z (x * z = y * z \Rightarrow x = y)$$

Уз ове ознаке, $\Gamma_{\mathrm{GR}} \models \sigma$ је само други запис за тврђење ($\star$).

Докажимо ($\star$). Нека је $(G, *, ^{-1}, e)$ произвољна група.

1. Изаберимо произвољне елементе x, y, z из G, такве да је $x * z = y * z$.

Тада је

2. $(x * z) * z^{-1} = (y * z) * z^{-1}$,

3. $x * (z * z^{-1}) = y * (z * z^{-1})$, [из претходног према закону асоцијативности]

4. $x * e = y * e$, [из претходног јер је $z * z^{-1} = e$]

5. $x = y$, [из претходног јер је $x * e = x$ и $y * e = y$]

6. $\forall x \forall y \forall z (x * z = y * z \Rightarrow x = y)$. [јер су x, y, z произвољни елементи]

Иако током овог доказа, замишљамо да радимо са неком конкретном (произвољно изабраном) групом, али ниједног тренутка нисмо имали потребу да прецизирамо о којој је заиста групи реч, већ смо искључиво користили законитости које група задовољава по дефиницији, као и добро позната својства једнакости и операција (функција). Другим речима, значајне су само аксиоме теорије група, док 'семантика' није од пресудног значаја.

Претходни пример указује на концепт синтаксне последице, који је већ разматран у систему природне дедукције. Наводимо кратак резиме правила природне дедукције која смо до сада разматрали и најављујемо нова правила за језик првог реда.

- Прво смо разматрали правила природне дедукције за *исказну логику* чије су формуле грађене од исказних слова, логичке константе $\bot$ и логичких везника $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\neg$.
- Затим смо разматрања проширили на формуле *предикатске логике*, у којој су исказна слова замењена атомским формулама и додати су квантификатори $\forall$ и $\exists$; претходним правилима додата су и правила за квантификаторе.
- У наставку разматрамо формуле *језика првог реда*, које садрже богатији скуп атомских формула: релацијским симболима се повезују изрази (који могу да сарже и операцијске знаке, а не само променљиве и симболе константи, као у случају предикатске логике), и додатно, као атомске формуле се појављују и једнакости; уз одговарајућа уопштења правила за квантификаторе, додајемо и правила за једнакост.

Дефиниција 30. *Ако је* Γ *нека теорија (скуп реченица). Реченица* α *је* ***синтаксна последица*** *теорије* Γ*, ако се секвент* $\Gamma \vdash \alpha$ *може добити применом правила исказне логике (страна 29) и следећих правила за квантификаторе и једнакости, коначан број пута:*

$(\forall x_{\mathrm{E}})$ $\dfrac{\forall x \alpha}{\alpha[x/t]}$ $\qquad$ $(\exists x_{\mathrm{U}})$ $\dfrac{\alpha[x/t]}{\exists x \alpha}$

$(\forall x_{\mathrm{U}})$ $\dfrac{\begin{array}{|l} v \\ \vdots \\ \alpha[x/v] \end{array}}{\forall x \alpha}$ $\qquad$ $(\exists x_{\mathrm{E}})$ $\dfrac{\exists x \alpha \quad \begin{array}{|ll} v & \alpha[x/v] \\ & \vdots \\ & \gamma \end{array}}{\gamma}$

$(=_{\mathrm{U}})$ $\dfrac{}{t = t}$ $\qquad$ $(=_{\mathrm{E}})$ $\dfrac{\alpha[x/t] \quad t = u}{\alpha[x/u]}$

Важно! (1) Формула $\alpha[x/t]$ означава формулу која је добија истовременом заменом свих слободних појављивања променљиве x у формули α изразом t, при чему се ниједна променљива израза t није везана.

(2) У поддоказима правила $(\forall x_{\mathrm{U}})$ и $(\exists x_{\mathrm{E}})$, појављује се тзв. *свежа променљива* v која се у формулама ван поддоказа не појављује слободно.

Лема 14. *1.* $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$

2. $\vdash \forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$

Доказ. (1) Изводимо секвент $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$:

1.	x_1, x_2	Уводимо свеже променљиве да бисмо доказали $\forall x_1 \forall x_2 \cdots$;
2.	$\quad x_1 = x_2$	додатна претпоставка;
		Нека је $\alpha(x)$ формула $x = x_1$;
3.	$\quad x_1 = x_1$	$(=_{\mathrm{U}})$; једнакост $x_1 = x_1$ је заправо формула $\alpha[x/x_1]$;
4.	$\quad x_2 = x_1$	$(=_{\mathrm{E}})$, 2, 3; једнакост $x_2 = x_1$ је заправо формула $\alpha[x/x_2]$;
5.	$x_1 = x_2 \Rightarrow x_2 = x_1$	$(\Rightarrow_{\mathrm{U}})$, 2-4;
6.	$\forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$	$\forall x_{1\mathrm{U}}$, $\forall x_{2\mathrm{U}}$ 1-5

(2) Изводимо секвент $\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$:

1.	x_1, x_2, x_3	Уводимо свеже променљиве;
2.	$\quad x_1 = x_2 \wedge x_2 = x_3$	додатна претпоставка;
		Нека је $\alpha(x)$ формула $x_1 = x$;
3.	$\quad x_1 = x_2$	$(\wedge_{\mathrm{E}}^{\mathrm{L}})$; једнакост $x_1 = x_2$ је формула $\alpha[x/x_2]$;
4.	$\quad x_2 = x_3$	$(\wedge_{\mathrm{E}}^{\mathrm{D}})$;
5.	$\quad x_1 = x_3$	$(=_{\mathrm{E}})$, 3, 4; једнакост $x_1 = x_3$ је формула $\alpha[x/x_3]$;
6.	$x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3$	$(\Rightarrow_{\mathrm{U}})$, 2-5;
7.	$\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$	$\forall x_{1\mathrm{U}}$, $\forall x_{2\mathrm{U}}$, $\forall x_{3\mathrm{U}}$ 1-6

□

Изведена правила могу знатно да олакшају доказивање секвената. У наредној леми дајемо неколико изведених правила која се односе на једнакости.

Лема 15.

$$\frac{t_1 = t_2}{t_2 = t_1}(=_{\mathrm{S}}) \qquad \frac{t_1 = t_2 \quad t_2 = t_3}{t_1 = t_3}(=_{\mathrm{T}}) \qquad \frac{t_1 = t_2}{t[x/t_1] = t[x/t_2]}(=_{\mathrm{sup}})$$

Доказ. Наводимо само доказ правила $(=_{\mathrm{sup}})$. Наравно, $t[x/t_1]$ је израз добијен истовременом заменом свих појављивања променљиве x у t изразом t_1.

Нека је $\alpha(y)$ формула $t[x/t_1] = t[x/y]$.

1.	$\quad t_1 = t_2$	претпоставка;
2.	$\quad t[x/t_1] = t[x/t_1]$	$(=_{\mathrm{U}})$; једнакост $t[x/t_1] = t[x/t_1]$ је формула $\alpha[y/t_1]$;
3.	$\quad t[x/t_1] = t[x/t_2]$	$(=_{\mathrm{E}})$, 1, 2; једнакост $t[x/t_1] = t[x/t_2]$ је заправо формула $\alpha[y/t_2]$.

□

Пример 61. Претпоставимо да вокабулар садржи један бинарни операцијски знак, који ћемо означавати двема вертикалним цртама $|\ |$ (између којих долазе аргументи), и два тернарна знака које ћемо означавати са $\angle$ и $\triangle$ (и који очекују три аргумента са десне стране). Нека је T_{cong} теорија чије су аксиоме универзална затворења следећих формула:

Универзално затворење формуле $\alpha(x_1, \ldots, x_k)$ јесте реченица $\forall x_1 \ldots \forall x_k \alpha(x_1, \ldots, x_k)$.

γ_1 $|xy| = |yx|$,

γ_2 $\angle xyz = \angle zyx$,

γ_3 $\triangle xyz = \triangle uvw \Rightarrow |xy| = |uv| \wedge |yz| = |vw| \wedge |zx| = |wu|$,

γ_4 $\triangle xyz = \triangle uvw \Rightarrow \angle xyz = \angle uvw \wedge \angle yzx = \angle vwu \wedge \angle zxy = \angle wuv$,

γ_5 $|xy| = |uv| \wedge \angle xyz = \angle uvw \wedge |yz| = |vw| \Rightarrow \triangle xyz = \triangle uvw$.

Доказаћемо

$$T_{\text{cong}} \vdash |ab| = |ac| \Rightarrow \angle abc = \angle acb.$$

Према правилу $(\Rightarrow_{\text{U}})$, доказивање жељеног секвента сводимо на

$$T_{\text{cong}}, |ab| = |ac| \vdash \angle abc = \angle acb.$$

Дакле, скуп претпоставки Γ садржи γ_1, γ_2, γ_3, γ_4, γ_5 и $|ab| = |ac|$.

1. $|ab| = |ac|$ — претпоставка, тј. (ax)
2. $|ac| = |ab|$ — из 1 према $(=_{\text{S}})$
3. $|ab| = |ba|$ — активирањем γ_1 правилом $(\forall_{\text{E}})$ при $[x/a]$, $[y/b]$
4. $|ba| = |ab|$ — из 3 према $(=_{\text{S}})$
5. $|ba| = |ac|$ — из 4, 1 према $(=_{\text{T}})$
6. $|ac| = |ca|$ — активирањем γ_1 правилом $(\forall_{\text{E}})$ при $[x/a]$, $[y/c]$
7. $|ba| = |ca|$ — из 5, 6 према $(=_{\text{T}})$
8. $\angle bac = \angle cab$ — активирањем γ_2 правилом $(\forall_{\text{E}})$ при $[x/b]$, $[y/a]$, $[z/c]$
9. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab|$ — из 7, 8, 2 применом $(\wedge_{\text{U}})$ два пута
10. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab| \Rightarrow \triangle bac = \triangle cab$ активирањем γ_5 правилом $(\forall_{\text{E}})$ при $[x/b]$, $[y/a]$, $[z/c]$, $[u/c]$, $[v/a]$, $[z/b]$
11. $\triangle bac = \triangle cab$ — из 9, 10 према $(\Rightarrow_{\text{E}})$
12. $\triangle cab = \triangle bac$ — из 11 према $(=_{\text{S}})$
13. $\triangle cab = \triangle bac \Rightarrow \angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$, активирањем γ_4 правилом $(\forall_{\text{E}})$ при $[x/c]$, $[y/a]$, $[z/b]$, $[u/b]$, $[v/a]$, $[w/c]$
14. $\angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$ — из 12, 13 према $(\Rightarrow_{\text{E}})$
15. $\angle abc = \angle acb$ — из 14 према $(\wedge^{\text{l}}_{\text{E}})$ и $(\wedge^{\text{d}}_{\text{E}})$.

Иако су сематичка последица $(\models)$ и синтаксна последица $(\vdash)$ дефинисане на сасвим различите начине, поседују низ заједничких особина.

Теорема 46. [***Теорема сагласности***] *Ако је* $\Gamma \vdash \alpha$, *онда је* $\Gamma \models \alpha$.

[**Теорема сагласности**] Ако се формула α се може доказати (извести) из претпоставки Γ, онда је α тачно у свим моделима скупа Γ.

Специјално, ако је α формула $\bot$, онда:

$$\text{Из } \Gamma \vdash \bot \text{ следи } \Gamma \models \bot.$$

Ако $\Gamma \vdash \bot$, кажемо да је Γ *противречан* скуп формула; $\Gamma \models \bot$ значи да Γ нема модел, тј. не постоји структура у којој су тачне све формуле из Γ. Краће речено: *Противречан скуп формула нема модел.* Претходна теорема се често користи да би се показало да се нека реченица **не може** доказати из датих претпоставки. Теорему сагласности можемо формулисати и у овом облику:

$$\text{Ако } \Gamma \not\models \alpha, \text{ онда } \Gamma \nvdash \alpha.$$

$\Gamma \not\models \alpha$ значи да постоји структура $\mathbf{S}$ која задовољава све реченице скупа Γ, али не задовољава α, тј. $\mathbf{S} \models \Gamma$ и $\mathbf{S} \not\models \alpha$. На овај начин се на пример, доказује да чувена Аксиома паралелности није последица осталих аксиома еуклидске геометрије. Овом приликом наводимо знатно једноставнији пример: да комутативност није последица осталих аксиома аксиома теорије група.

Пример 62. Докажимо да се закон комутативности, тј. формула $\forall x \forall y(x * y = y * x)$ не може извести из аксиома теорије група T_{GR}. Да бисмо доказали да $T_{\mathrm{GR}} \nvdash \forall x \forall y(x * y = y * x)$, довољно је доказати да $T_{\mathrm{GR}} \not\models \forall x \forall y(x * y = y * x)$, за шта је довољно да конструишемо групу чија бинарна операција није комутативна. Једна од њих је група $(S_3, \circ, ^{-1}, \sigma_1)$, где је S_3 скуп свих пермутација (бијекција) скупа $\{1, 2, 3\}$ чију су елементи:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Да група није комутативна показују једнакости:

$$\tau_3 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_2, \ \tau_2 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3.$$

Доста важних математичких истраживања и нових математичких области је настало управо због немогућности да се извесна тврђења докажу из неких датих претпоставки. Историја математике је пуна потрага за доказима, за које се испоставило да не постоје. Ипак, из тих безнадежних потрага за доказима често су се рађале сасвим нове математичке теорије. Илустрације ради, наводимо један занимљив проблем који се односи на HSI-алгебре поменуте на почетку овог поглавља. Тарски је крајем 60-их година прошлог века поставио проблем који је данас познат као Тарскијев средњошколски проблем: *Да ли се из HSI теорије може извести сваки идентитет који је тачан у $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$?* Вилки је 1980. године дао негативан одговор тако што је показао да је идентитет

$$\big((1+x)^y + (1+x+x^2)^y\big)^x \cdot \big((1+x^3)^x + (1+x^2+x^4)^x\big)^y$$
$$= \big((1+x)^x + (1+x+x^2)^x\big)^y \cdot \big((1+x^3)^y + (1+x^2+x^4)^y\big)^x$$

тачан у $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$, али није последица HSI теорије. Тарскијев проблем и Вилкијево решење покренули су разне, још увек актуелне правце истраживања HSI алгебри.

$$(HSI) \begin{cases} \forall x \forall y(x + y = y + x) \\ \forall x \forall y \forall z(x + (y + z) = (x + y) + z) \\ \forall x(x \cdot 1 = x) \\ \forall x \forall y(x \cdot y = y \cdot x) \\ \forall x \forall y \forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\ \forall x \forall y \forall z(x \cdot (y + z) = x \cdot y + x \cdot z) \\ \forall x(x^1 = x) \\ \forall x(1^x = 1) \\ \forall x \forall y \forall z(x^{y+z} = x^y \cdot x^z) \\ \forall x \forall y \forall z((x \cdot y)^z = x^z \cdot y^z) \\ \forall x \forall y \forall z((x^y)^z = x^{y \cdot z}) \end{cases}$$

Питање за крај поглавља: да ли важи обрат теореме сагласности? Ако је $\Gamma \models \alpha$, да ли је $\Gamma \vdash \alpha$? До позитивног одговора на ово питање долазимо тек увођењем нове аксиоме теорије скупова – аксиоме изобора, која је тема наредног поглавља.

7. Аксиома избора

24

ZFC = ZF + AC

ZFC је теорија **ZF** проширена Аксиомом избора (Axiom of choice), краће (AC).

> Аксиома избора
> Ако је $\mathcal{A}$ скуп чији су сви елементи непразни, онда постоји (тзв. *изборна*) функција $f : \mathcal{A} \to \cup\mathcal{A}$ таква да за све $X \in \mathcal{A}$, $f(X) \in X$.

Једноставна последица Аксиоме избора јесте следеће тврђење:

(AC*) за сваки скуп A постоји функција $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да за све X, $\emptyset \neq X \subseteq A$, важи $f(X) \in X$.

Није тешко уочити да из (AC*) следи Аксиома избора. Заиста, нека је $\mathcal{A}$ произвољан скуп чији су елементи непразни скупови. Нека је $A = \cup\mathcal{A}$. Тада, према (AC*) постоји функција $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да за све X, $\emptyset \neq X \subseteq A$, важи $f(X) \in X$. Како је $\mathcal{A} \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$, директно следи да је $f \restriction \mathcal{A}$ изборна функција за $\mathcal{A}$.

Лема 16. *Ако $g : X \overset{\text{на}}{\to} Y$, онда је $|Y| \leq |X|$.*

Доказ. Треба наћи функцију $h : Y \overset{1-1}{\to} X$. За свако $y \in Y$ нека је $G_y = g^{-1}[\{y\}]$. Будући да је g на-функција, следи да је $G_y \neq \emptyset$ за свако $y \in Y$. Нека је $\mathcal{G} = \{G_y \mid y \in Y\}$ и f изборна функција за $\mathcal{G}$, тј. $f : \mathcal{G} \to \cup\mathcal{G}$ и $f(G_y) \in G_y$. Функцију $h : Y \to X$ дефинишемо на следећи начин: $h(y) = f(G_y)$, $y \in Y$. Једноставно закључујемо да је h 1-1 функција: ако су y_1 и y_2 два различита елемента из Y, онда су G_{y_1} и G_{y_2} дисјунктни, па је $h(y_1) \neq h(y_2)$. □

Приметимо да је лема 44 специјалан случај претходне леме. Међутим, за разлику од претходног доказа у којем се користи (AC), лема 44 је доказана захваљујући добром уређењу $\leq$ скупа $\mathbb{N}$. Аналоган доказ, без позивања на (AC), може се спровести за било који скуп X који је добро уређен неком релацијом.

Дефиниција 31. *Уређење $\preceq$ неког скупа X је **добро** ако сваки непразан подскуп од X има најмањи елемент у односу на $\preceq$.*

Лема 17. [*без* (AC)] *Неке је $\preceq$ добро уређење скупа X. Тада за сваки скуп Y, ако постоји $f : X \overset{\text{на}}{\to} Y$, онда је $|Y| \leq |X|$.*

Природно је поставити питање да ли се сваки скуп Y може добро уредити, одн. да ли са на сваком скупу Y може дефинисати нека бинарна релација која је добро уређење.

Теорема 47. [***Цермелова лема*** (WO)] *Сваки скуп се може добро уредити.*

Цермелова лема очигледно важи за највише пребројиве (коначне и пребројиве) скупове, и то можемо показати без Аксиоме избора.

Међутим, да бисмо добро уредили неки непребројив скуп, неопходно је позивање на Аксиому избора.

Није тешко уочити да је Аксиома избора последица Цермелове леме. Заправо, Цермелова лема је еквивалентна Аксиоми избора.
(WO) $\Rightarrow$ (AC) Чињеница да је $\leq$ добро уређење скупа Y значи да сваки непразан подскуп има најмањи елемент, па постоји функција $\min : \mathcal{P}(Y) \setminus \{\emptyset\} \to Y$ таква да за све X, $\emptyset \neq X \subseteq Y$, $\min(X) \in X$ и $\min(X) \leq x$, за свако $x \in X$.

Аксиома избора има још доста еквивалентних формулација. Једна од најпознатијих је свакако Цорнова лема.

Дефиниција 32. *Нека је $(P, \leq)$ уређење (тј. $\leq$ је релација поретка на скупу P).*

(1) Скуп $L \subseteq P$ је ланац ако су свака два елемента из L упоредива у односу на $\leq$, тј. за све $x, y \in L$ важи $x \leq y$ или $y \leq x$.

(2) Скуп $X \subseteq P$ је одозго ограничен ако постоји елемент $a \in P$ такав да за све $x \in X$ важи $x \leq a$.

(3) Елемент $a \in P$ је максималан ако не постоји елемент $x \in P$ такав да је $a \leq x$ и $a \neq x$.

Теорема 48. [***Цорнова лема*** (ZL)] *Нека је $(P, \leq)$ уређење. Ако је сваки ланац у P одозго ограничен, онда у $(P, \leq)$ постоји максималан елемент.*

Испоставља се да је и ово тврђење еквивалентно Аксиоми избора. Ту чињеницу ћемо детаљно доказати пре свега да бисмо илустровали примену Цорнове леме. Аксиома избора се у другим областима математике најчешће користи у форми Цорнове леме.
(ZL) $\Rightarrow$ (AC) ($\star$) Нека је A произвољан скуп. Треба показати да постоји функција $F : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да $F(X) \in X$, за све $X \in \mathcal{P}(A) \setminus \{\emptyset\}$. Следимо следећу стратегију:

- Посматрамо скуп $\mathcal{F}$ свих 'апроксимација' жељене изборне функције; тј. изборне функције дефинисане на неким подскуповима од $\mathcal{P}(A) \setminus \{\emptyset\}$;
- дефинишемо природно уређење међу апроскимацијама; интуитивно значење поретка $f \preceq g$ је 'g проширује f' (домен функције f је садржан у домену функције g и функције f и g имају исте вредности на заједничким елементима домена);
- доказујемо да сваки ланац (све бољих 'апроксимација') има горње ограничење; то горње ограничење ће бити унија свих функција ланца;
- максималан елемент уређења $(\mathcal{F}, \prec)$, који постоји према Цорновој леми, јесте жељена изборна функција.

Нека је $\mathcal{F}$ скуп свих функција избора f таквих да је $\mathrm{dom}(f) \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$ и $f(x) \in x$, за све $x \in \mathrm{dom}(f)$. Скуп $\mathcal{F}$ је непразан, јер

за сваки коначан подскуп од $\mathcal{P}(A) \setminus \{\emptyset\}$ постоји функција избора. Дефинишимо на скупу $\mathcal{F}$ релацију $\preceq$ на следећи начин:

$$f \preceq g \overset{\text{def}}{\Leftrightarrow} \operatorname{dom}(f) \subseteq \operatorname{dom}(g) \wedge \forall x \in \operatorname{dom}(f)\,(f(x) = g(x)).$$

Није тешко проверити да је $\preceq$ уређење скупа $\mathcal{F}$. Докажимо да је сваки ланац $\mathcal{L}$, уређења $(\mathcal{F}, \preceq)$, ограничен одозго.

Нека је $\mathcal{L}$ ланац у $(\mathcal{F}, \preceq)$ и $L = \bigcup_{\ell \in \mathcal{L}} \operatorname{dom}(\ell)$. Очигледно је $L \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$. За свако $x \in L$, постоји $\ell \in \mathcal{L}$ таква да $x \in \operatorname{dom}(\ell)$. Штавише, ако $x \in \operatorname{dom}(\ell_1)$ и $x \in \operatorname{dom}(\ell_2)$, за неке $\ell_1, \ell_2 \in \mathcal{L}$, тада мора бити $\ell_1(x) = \ell_2(x)$, јер је $\mathcal{L}$ ланац па важи $\ell_1 \preceq \ell_2$ или $\ell_2 \preceq \ell_1$, а самим тим:

1. $\operatorname{dom}(\ell_1) \subseteq \operatorname{dom}(\ell_2)$ и $\ell_1(t) = \ell_2(t)$, за све $t \in \operatorname{dom}(\ell_1)$, или
2. $\operatorname{dom}(\ell_2) \subseteq \operatorname{dom}(\ell_1)$ и $\ell_1(t) = \ell_2(t)$, за све $t \in \operatorname{dom}(\ell_2)$.

Другим речима, за свако $x \in L$ постоји јединствени елемент $y \in A$ такав да је $\ell(x) = y$, за свако $\ell \in \mathcal{L}$ чији домен садржи x. Нека је $h : L \to A$ одговарајућа функција: ако за $x \in L$ изаберемо неко (било које) $\ell \in \mathcal{L}$ такво да $x \in \operatorname{dom}(\ell)$, онда је $h(x) = \ell(x) \in x$. Према томе, $h \in \mathcal{F}$. Очигледно, за свако $\ell \in \mathcal{L}$ важи $\ell \preceq h$, јер је $\operatorname{dom}(\ell) \subseteq L = \operatorname{dom}(h)$ и $h(x) = \ell(x)$, за све $x \in \operatorname{dom}(\ell)$.

Доказали смо да сваки ланац у $(\mathcal{F}, \preceq)$ има горње ограничење. Према Цорновој леми, постоји максималан елемент у $(\mathcal{F}, \preceq)$: нека је то функција F. Тада је $\operatorname{dom}(F) \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$ и $F(x) \in x$, за свако $x \in \operatorname{dom}(F)$. Ако би било $\operatorname{dom}(F) \subset \mathcal{P}(A)$, постојао би $x_0 \in \mathcal{P}(A) \setminus \{\emptyset\}$ такав да $x_0 \notin \operatorname{dom}(F)$. Будући да је $x_0 \neq \emptyset$, нека је t произвољан елемент из x_0. Тада је функција $F^+ : \operatorname{dom}(F) \cup \{x_0\} \to A$ дефинисана са:

$$F^+(x) = \begin{cases} F(x), & x \in \operatorname{dom}(F), \\ t, & x = x_0, \end{cases}$$

такође функција избора, тј. $F^+ \in \mathcal{D}$, што је немогуће јер је $F \precneqq F^+$, а F је максималан елемент. Дакле, $\operatorname{dom}(F) = \mathcal{P}(A) \setminus \{\emptyset\}$. □