УВОД У МАТЕМАТИЧКУ ЛОГИКУ

(зимски семестар школске 2018/19 године)

Небојша Икодиновић

– први део –

Садржај

1 Природна дедукција **5**

1.1 Искaзна логика и природна дедукција 5

Исказне формуле и појам последице 5

Основна правила дедукције 7

Задаци 21

1.2 Предикатска логика и природна дедукција 23

Задаци 37

2 Теорија скупова **40**

2.1 Аксиоме теорије скупова - I 40

2.2 Булове операције и Декартов производ 49

2.3 Релације 57

Важне бинарне релације 62

2.4 Функције 72

Важне функције 79

Функције из празног и у празан скуп 83

Директне и индиректне слике 84

Колекције и фамилије 86

2.5 Аксиоме теорије скупова - II 90

2.6 Скуп природних бројева 93

Општа теорема рекурзије 108

2.7 Кардиналност скупа 112

Коначни скупови 112

Бесконачни скупови 117

Пребројиви и непребројиви скупови 121

1

Природна дедукција

1.1 Исказна логика и природна дедукција

Исказне формуле и појам последице

Основни појам логике јесте појам *последице*, односно извођење *закључка* из некаквих *претпоставки*. Уместо

Из *претпоставка*$_1$,..., *претпоставка*$_n$ изводим *закључак*,

краће пишемо

$$\frac{\textit{претпоставка}_1, \ldots, \textit{претпоставка}_n}{\textit{закључак}}$$

или

$$\textit{претпоставка}_1, \ldots, \textit{претпоставка}_n \vdash \textit{закључак}.$$

Последњи запис називамо *секвентом*.

У овом одељку бавићемо се пре свега закључивањима у којима су претпоставке и закључци формулисани спајањем тзв. *декларативних реченица*, тј. *исказа* одређеним везницима. Под декларативним реченицама, одн. исказима, подразумевамо оне реченице чију истинитост на неки начин можемо утврдити, тј. рећи да ли су *тачне* или *лажне*. Исказе ћемо често означавати малим словима латинице p, q, r, ..., користећи по потреби и индексе $p_1, p_2, \ldots, q_1, \ldots$ Ове ознаке исказа називамо и *исказним словима*.

Полазећи од неких исказа, градимо сложеније исказе тако што **негирамо** ($\neg$) један од полазних исказа или два полазна исказа повезујемо везницима **и** ($\wedge$), **или** ($\vee$), **ако ... онда ...** ($\Rightarrow$), **акко** ($\Leftrightarrow$), користећи по потреби заграде на уобичајени начин. Да бисмо поједноставили записивање договарамо се о приоритету везника: $\neg$ је везник највећег приоритета, за њим следе $\vee$ и $\wedge$

који су једнаког приоритета, а за њима $\Rightarrow$ и $\Leftrightarrow$, такође једнаког приоритета. Приметите да поступамо потпуно аналогно као када формирамо бројевне изразе полазећи од променљивих и основних операција међу бројевима. „Логичке изразе“ изграђене од исказних слова употребом везника и заграда називамо **исказне формуле**.

Сложени искази су такође декларитивне реченице чија се истинитост једноставно може одредити ако за све полазне исказе (означене исказним словима) знамо да ли су тачни или нису. Истинитост сложених исказа одређујемо на основу познатих таблица (1 – тачно, 0 – нетачно):

$$\begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|c} & \neg \\ \hline 0 & 1 \\ 1 & 0 \end{array} \qquad \begin{array}{c|cc} \Rightarrow & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{c|cc} \Leftrightarrow & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array}$$

У овом одељку фамилијарност са наведеним таблицама није од пресудног значаја, и на таблице ћемо се ослањати само приликом интуитивног оправдавања правила дедукције која наводимо у наставку. Основно питање на које желимо да одговоримо јесте која правила користимо да бисмо неку исказну формулу извели као закључак (последицу) датог скупа претпоставки (премиса)?

Пример 1. Посматрајмо следећа четири *закључивања.*

(1) Ако авион не касни и има слободног таксија на аеродрому, Ана стиже на састанак. Ана није стигла на састанак. Авион не касни. **Дакле**, нема слободног таксија на аеродрому.

(2) Ако Пера положи алгебру и анализу, отац ће појести шешир. Отац није појео шешир. Пера је положио алгебру. **Дакле**, Пера није положио анализу.

(3) Ако четвороугао $ABCD$ има једнаке странице и једнаке углове, онда је $ABCD$ квадрат. $ABCD$ није квадрат. Странице четвроугла $ABCD$ су једнаке. **Дакле**, углови четвороугла $ABCD$ нису једнаки.

(4) Ако је n дељиво са 2 и са 3, онда је n дељиво са 6. Број n није дељив са 6. Број n јесте дељив са 2. **Дакле**, број n није дељив са 3.

У сва четири случаја уочавамо исти шаблон:

Претпоставке:	**Ако** p **и** q, **онда** r; **није** r; p	$p \wedge q \Rightarrow r$ $\neg r$ p
Образложење (?)	$\vdots$	$\vdots$
Закључак:	**није** q	$\neg q$

Употреба исказних слова нам омогућава да сажето опишемо реченице и фокусирамо се на механизам закључивања.

Ако авион не касни и има слободног таксија на аеродрому, Ана стиже на састанак. Ана није стигла на састанак. Авион не касни.

(**Формализација**) p: Авион не касни.
q: Има слободног таксија на аеродрому.
$\downarrow$ r: Ана стиже на састанак.

$p \wedge q \Rightarrow r, \neg r, p$

$\vdots$ **Закључивање (!)**

$\neg q$

$\downarrow$ **Повратак у неформални контекст**

Нема слободног таксија на аеродрому.

Наш основни задатак је да попунимо „празнину“ између претпоставки и закључка навођењем одговарајућих правила закључивања.

Извлачење закључка из неког скупа претпоставки јесте мисаона радња, тзв. *дедуктивно закључивање*, којој се посвећује велика пажња још од традиционалне логике па све до савремене математичке логике. Давно је формулисан општи услов који мора испуњавати свако правило дедуктивног закључивања. Услов је познат под називом salva veritate и гласи:

Приликом извођења закључака не сме се наносити штета истинитости, односно ако су претпоставке истините, онда је и закључак истинит.

Основна правила дедукције

Конјункција

Прва правила која наводимо односе се на конјункцију.

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

Из претпоставки α, β (директно) закључујемо $\alpha \wedge \beta$. Ако су тачни α и β, онда је тачна и конјункција $\alpha \wedge \beta$.

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. Наведено правило називамо и *правило увођења конјункције*, па га зато означавамо $(\wedge_{\mathrm{U}})$.

Наредна два правила омогућавају да у доказима користимо конјункције и назаву је *правила елиминације конјункције*.

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

Ако је тачна конјункција $\alpha \wedge \beta$, онда је тачан и конјункт α и конјункт β. Ако имамо доказ за $\alpha \wedge \beta$, онда даље закључујемо α (одн. β) тако што на $\alpha \wedge \beta$ примењујемо правило $(\wedge^{\mathrm{L}}_{\mathrm{E}})$ (одн. $(\wedge^{\mathrm{D}}_{\mathrm{E}})$).

Секвент $\varphi_1,\dots,\varphi_k \vdash \psi$ (тј. да из претпоставки $\varphi_1,\dots,\varphi_k$ следи ψ) доказујемо тако што формирамо низ који чине претпоставке $\varphi_1,\dots,\varphi_k$ 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 $\varphi_1,\dots,\varphi_k$, одн. *доказом* одговарајућег секвента. На који начин користимо правила, одн. како доказујемо секвенте илустровано је у наредном примеру.

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

Наведени доказ можемо приказати и на следећи начин.

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

У наставку углавном ћемо користити први запис.

Задатак 1. Доказати следеће секвенте:
(1) $p\wedge q\vdash q\wedge p$
(2) $p\wedge(q\wedge r)\vdash(p\wedge q)\wedge r$
(3) $(p\wedge q)\wedge r\vdash p\wedge(q\wedge r)$
(4) $p\vdash p\wedge p$

Двострука негација

Занимљиву дискусију која се може водити о двострукој негацији изостављамо, и прихватамо *класично* становиште да свака формула α и њена двострука негација $\neg\neg\alpha$ „тврде“ исто.

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

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. Овим правилима заправо изражавамо становиште да нема разлике између формуле и њене двоструке негације.

ПРИМЕР 3. Докажимо секвент $p, \neg\neg(q \wedge r) \vdash \neg\neg p \wedge r$.

1.	p	претпоставка
2.	$\neg\neg(q \wedge r)$	претпоставка
3.	$q \wedge r$	$\neg\neg_{\mathrm{E}}$, 2
4.	r	$\wedge_{\mathrm{E}}^{\mathrm{D}}$, 3
5.	$\neg\neg p$	$\neg\neg_{\mathrm{U}}$, 1
6.	$\neg\neg p \wedge r$	$\wedge_{\mathrm{U}}$, 5, 4

ЗАДАТАК 2. Доказати следеће секвенте:
(1) $p \wedge q \vdash \neg\neg p \wedge \neg\neg q$
(2) $\neg\neg p \wedge \neg\neg q \vdash p \wedge q$

Импликација

Наредно правило које уводимо јесте једно од најпознатијих правила закључивања познато под латинским називом modus ponens. Ми ћемо ово правило називати савременијим именом – *елиминација импликације*.

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

Правило $(\Rightarrow_{\mathrm{E}})$ говори о томе како се у доказима могу користити тврдње формулисане у облику имликације.

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

Правило modus tolens (MT) такође је веома корисно при употреби тврдњи у облику импликације.

НАПОМЕНА 1. Наведена правила постају очигледна када формуле заменимо декларативним реченицама говорног језика које су одговарајућег облика.

$\dfrac{\alpha \Rightarrow \beta \quad \alpha}{\beta}(\Rightarrow_{\mathrm{E}})$	1. Ако Аца живи у Београду, онда Аца живи у Србији. 2. Аца живи у Београду. **Дакле**, Аца живи у Србији.
$\dfrac{\alpha \Rightarrow \beta \quad \neg\beta}{\neg\alpha}(\mathrm{MT})$	1. Ако Аца живи у Београду, онда Аца живи у Србији. 2. Аца не живи у Србији. **Дакле**, Аца не живи у Београду.

Препоручујемо читаоцу да и остала правила која будемо уводили илуструје на аналоган начин.

Пример 4. Докажимо секвент $p \Rightarrow (q \Rightarrow r), p, \neg r \vdash \neg q$.

1.	$p \Rightarrow (q \Rightarrow r)$	претпоставка
2.	p	претпоставка
3.	$\neg r$	претпоставка
4.	$q \Rightarrow r$	$\Rightarrow_{\mathrm{E}}$, 1, 2
5.	$\neg q$	МТ, 4, 3

Снагу правила дедукције лепо илуструју најразноврснији примери закључивања у којима се она примењују.

Пример 5. Миле размишља коју девојку да позове.
(1) Ако позовем Ану, нећу звати Бојану.
(2) Ако не позовем Бојану, нећу звати ни Весну.
(3) Ако не позовем Гоцу, зваћу Весну.
(4) Ако позовем Гоцу, зваћу и Драгану.
(5) Ако позовем Драгану, нећу звати Ему.
Напослетку, позвао је Ему. Да ли ће Миле, у складу са својим размишљањем позвати Ану?

Формални доказ

1.	$a \Rightarrow \neg b$	претпоставка
2.	$\neg b \Rightarrow \neg v$	претпоставка
3.	$\neg g \Rightarrow v$	претпоставка
4.	$g \Rightarrow d$	претпоставка
5.	$d \Rightarrow \neg e$	претпоставка
6.	e	претпоставка
7.	$\neg\neg e$	$\neg\neg_{\mathrm{U}}$, 6
8.	$\neg d$	МТ, 5, 7
9.	$\neg g$	МТ, 4, 8
10.	v	$\Rightarrow_{\mathrm{E}}$, 3, 9
11.	$\neg\neg v$	$\neg\neg_{\mathrm{U}}$, 10
12.	$\neg\neg b$	МТ, 2, 11
13.	$\neg a$	МТ, 1, 12

Неформални доказ: Наведени формални доказ у потпуности одговара неформалном доказу који бисмо навели размишљући о задатку.

Како је Миле позвао Ему, према (5) следи да неће звати Драгану. Из (4) даље следи да неће звати Гоцу. Затим из (3), пошто неће звати Гоцу, зваће Весну, одакле према (2) закључујемо да ће звати Бојану. Најзад, из (1) следи да неће звати Ану.

Приметите да се у наведеном неформалном образложењу подразумевају правила двојне негације.

Наводимо и правило *увођења импликације* које говори како се доказују импликације.

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

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 истицаћемо вертикалном цртом и називати *поддоказом*. Непосредно испод завршетка вертикалне линије наводимо закључак $\alpha \Rightarrow \beta$, ознаку правила $(\Rightarrow_{\mathrm{U}})$ и бројеве којима су нумерисани кораци поддоказа. Наредна шема илуструје употребу правила $(\Rightarrow_{\mathrm{U}})$.

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

Пример 6. (1) Ако научим да доказујем, лако ћу положити логику. (2) Ако не размишљам, нећу положити логику. (3) Ако размишљам, лако ћу завршити математику.

Доказати: ако научим да доказујем, лако ћу завршити математику.

Треба заправо доказати секвент $d \Rightarrow l, \neg r \Rightarrow \neg l, r \Rightarrow m \vdash d \Rightarrow m$.

Формални доказ

1.	$d \Rightarrow l$	претпоставка
2.	$\neg r \Rightarrow \neg l$	претпоставка
3.	$r \Rightarrow m$	претпоставка
4.	$\mid\ d$	додатна прет.
5.	$\mid\ l$	$\Rightarrow_{\mathrm{E}}$, 1, 4
6.	$\mid\ \neg\neg l$	$\neg\neg_{\mathrm{U}}$, 5
7.	$\mid\ \neg\neg r$	MT, 2, 6
8.	$\mid\ r$	$\neg\neg_{\mathrm{E}}$, 7
9.	$\mid\ m$	$\Rightarrow_{\mathrm{E}}$, 3, 8
10.	$d \Rightarrow m$	$\Rightarrow_{\mathrm{U}}$, 4-9

Неформални доказ: Наведени формални доказ и овог пута одговара неформалном размишљању (уз подразумевање правила двојне негације.)

Претпоставимо да сам научио да доказујем. Тада ћу, према (1) лако положити логику, што значи, према (2), да размишљам. А пошто размишљам, из (3) следи да ћу завршити математику.

Пример 7. Докажимо секвент $\vdash p \Rightarrow p$.

1.	$\mid\ p$	додатна претпоставка
2.	$p \Rightarrow p$	$\Rightarrow_{\mathrm{U}}$, 1

У наведеном доказу, додатну претпоставку уводимо, јер желимо да докажемо импликацију облика $p \Rightarrow \cdots$. Оно што треба доказати читамо са десне стране жељене импликације $\cdots \Rightarrow p$. У овом случају, увођењем додатне претпоставке одмах долазимо до циља (p).

Негација и контрадикција

Правила двоструке негације мало говоре о самој негацији, тј. о *увођењу* и *елиминацији негације*. Пре него што уведемо одговарајућа правила, позабавимо се појмом *контрадикције*. Под контрадикцијом подразумевамо конјункцију било које формуле и њене негације, а сваки скуп претпоставки из кога се може извести нека формула и њена негација називамо *контрадикторним*. Погодно је увести посебан знак $\perp$ за контрадикцију (формулу која је сигурно нетачна).

$$\frac{\alpha \quad \neg\alpha}{\perp}(\neg_E) \qquad \frac{\begin{array}{|l}\alpha\\ \vdots\\ \perp\end{array}}{\neg\alpha}(\neg_U)$$

Из претпоставки α, $\neg\alpha$ изводимо контрадикцију. Поред тога, ако из α докажемо контрадикцију, онда закључујемо $\neg\alpha$.

$$\frac{\perp}{\alpha}(\perp_E)$$

Уводимо и правило према коме се из контрадикције може закључити било шта, тј. може се извести било која формула.

Пример 8. Детектив разматра следеће евидентне чињенице:
(1) Ако Пера није крив, крив је Лаза, а Мика није.
(2) Ако није крив Мика, није крив ни Лаза.
(3) Ако није крив Лаза, није крив ни Пера.
Ко је крив?

Најпре ћемо неформално, а затим и формално доказати да су криви сви. У формалном доказу, то ће значити да из претпоставки $\neg p \Rightarrow l \wedge \neg m$, $\neg m \Rightarrow \neg l$, $\neg l \Rightarrow \neg p$ изводимо и p и m и l (при чему слова p, m, l редом означавају исказе „Пера је крив“, „Мика је крив“, „Лаза је крив“).

Неформални доказ

Претпоставимо да Пера није крив. Тада, према (1), Лаза је крив, а Мика није крив. Пошто је Лаза крив, из (2) следи да је Мика крив, што је у супротности за претходним закључком да Мика није крив. Контрадикција! Дакле, погрешна је претпоставка да Пера није крив, што значи да Пера јесте крив. Сада, из (3) даље закључујемо да је крив и Лаза. Најзад, према (2) следи да је крив и Мика.

Формални доказ

1.	$\neg p \Rightarrow l \wedge \neg m$	претпоставка	
2.	$\neg m \Rightarrow \neg l$	претпоставка	
3.	$\neg l \Rightarrow \neg p$	претпоставка	
4.	$\neg p$	додатна прет.	
5.	$l \wedge \neg m$	$\Rightarrow_{\mathrm{E}}$, 1, 4	
6.	l	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 5	
7.	$\neg m$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 5	
8.	$\neg l$	$\Rightarrow_{\mathrm{E}}$, 2, 7	
9.	$\perp$	$\neg_{\mathrm{E}}$, 6, 8	
10.	$\neg\neg p$	$\neg_{\mathrm{U}}$, 4-9	
11.	p	$\neg\neg_{\mathrm{E}}$, 10	◀
12.	$\neg\neg l$	MT, 3, 10	
13.	l	$\neg\neg_{\mathrm{E}}$, 12	◀
14.	$\neg\neg m$	MT, 2, 12	
15.	m	$\neg\neg_{\mathrm{E}}$, 14	◀

Дисјункција

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

Ако знамо да је α тачно (ако смо доказали α), онда мора бити тачно и $\alpha \vee \beta$ (онда изводимо и закључак $\alpha \vee \beta$), за било коју формулу β. На исти начин, из β изводимо закључак $\alpha \vee \beta$, за било коју формулу α.

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:

- 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.

$$\frac{\alpha \vee \beta \quad \begin{array}{|c} \alpha \\ \vdots \\ \gamma \end{array} \quad \begin{array}{|c} \beta \\ \vdots \\ \gamma \end{array}}{\gamma}\,(\vee_{\mathrm{E}})$$

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

Задатак 3. Доказати секвент $\vdash (p \Rightarrow r) \wedge (q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r)$.

Еквиваленција

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.

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

Пример 10. Докажимо $\vdash \neg p \Leftrightarrow (p \Rightarrow \bot)$.

1.	$\neg p$	додатна претпоставка
2.	p	додатна претпоставка
3.	$\bot$	$\neg_{\mathrm{E}}$, 1, 2
4.	$p \Rightarrow \bot$	$\Rightarrow_{\mathrm{U}}$, 2-3
5.	$\neg p \Rightarrow (p \Rightarrow \bot)$	$\Rightarrow_{\mathrm{U}}$, 1-4
6.	$p \Rightarrow \bot$	додатна претпоставка
7.	p	додатна претпоставка
8.	$\bot$	$\Rightarrow_{\mathrm{U}}$, 7, 6
9.	$\neg p$	$\neg_{\mathrm{U}}$, 7-8
10.	$(p \Rightarrow \bot) \Rightarrow \neg p$	$\Rightarrow_{\mathrm{U}}$, 6-9
11.	$\neg p \Leftrightarrow (p \Rightarrow \bot)$	$\Leftrightarrow_{\mathrm{U}}$, 5, 9

Неколико изведених правила

Сва до сада наведена правила закључивања називаћемо *правилима закључивања исказне логике.* Међу њима су два правила која нисмо морали да наводимо, јер се могу извести из осталих. То су правила $\neg\neg_U$ и MT.

1.	α	претпоставка
2.	$\quad\mid \neg\alpha$	додатна прет.
3.	$\quad\mid \bot$	$\neg_E$, 1, 2
4.	$\neg\neg\alpha$	$\neg_U$, 2-3

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\neg\beta$	претпоставка
3.	$\quad\mid \alpha$	додатна прет.
4.	$\quad\mid \beta$	$\Rightarrow_E$, 1, 3
5.	$\quad\mid \bot$	$\neg_E$, 2, 4
6.	$\neg\alpha$	$\neg_U$, 3-5

Примену ова два правила једноставно можемо елиминисати из сваког доказа тако што тај доказ проширујемо навођењем горе наведених доказа прилагођених конкретном случају. То је илустровано у наредном примеру.

Пример 11. Доказимо секвент $p \Rightarrow \neg q, q \vdash \neg p$.

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\neg\neg q$	$\neg\neg_U$, 2
4.	$\neg p$	MT, 1, 3

Без правила $\neg\neg_U$ и MT дати секвент бисмо доказали на следећи начин.

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\quad\mid \neg q$	додатна претпоставка
4.	$\quad\mid \bot$	$\neg_E$, 2, 3
5.	$\neg\neg q$	$\neg_U$, 3-4
6.	$\quad\mid p$	додатна претпоставка
7.	$\quad\mid \neg q$	$\Rightarrow_E$, 1, 6
8.	$\quad\mid \bot$	$\neg_E$, 2, 7
9.	$\neg p$	$\neg_U$, 6-8

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

Дисјунктивни силогизми	
$\dfrac{\alpha \vee \beta \quad \neg\alpha}{\beta}$ (DS)	$\dfrac{\alpha \vee \beta \quad \neg\beta}{\alpha}$ (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.	$\perp$	$\neg_{\mathrm{E}}$, 2, 3
5.	β	$\perp_{\mathrm{E}}$, 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.	$\alpha \vee \neg\alpha$	$\vee_{\mathrm{U}}^{\mathrm{L}}$, 2
4.	$\perp$	$\neg_{\mathrm{E}}$, 1, 3
5.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 2-4
6.	$\alpha \vee \neg\alpha$	$\vee_{\mathrm{U}}^{\mathrm{D}}$, 5
7.	$\perp$	$\neg_{\mathrm{E}}$, 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 Моргановим законом, јер приликом примене неће бити забуне.

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

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

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

Пример 12. Докажимо секвент $p \wedge q \Rightarrow r, \neg r, p \vdash \neg q$ из примера 1.

1.	$p \wedge q \Rightarrow r$	претпоставка
2.	$\neg r$	претпоставка
3.	p	претпоставка
4.	$\neg(p \wedge q)$	MT, 1, 2
5.	$\neg p \vee \neg q$	DM, 4
6.	$\neg\neg p$	$\neg\neg_{\mathrm{U}}$, 3
7.	$\neg q$	DS, 5, 6

Посебно су корисна следећа изведена правила која се односе на еквиваленцију. У последњем правилу које наводимо, $*$ стоји уместо једног (било ког) везника $\wedge$, $\vee$ или $\Rightarrow$.

$$\frac{}{\alpha \Leftrightarrow \alpha} \qquad \frac{\alpha \Leftrightarrow \beta}{\beta \Leftrightarrow \alpha} \qquad \frac{\alpha \Leftrightarrow \beta \quad \beta \Leftrightarrow \gamma}{\alpha \Leftrightarrow \gamma} \qquad \frac{\alpha \Leftrightarrow \beta}{\neg\alpha \Leftrightarrow \neg\beta} \qquad \frac{\alpha \Leftrightarrow \beta \quad \alpha' \Leftrightarrow \beta'}{\alpha * \alpha' \Leftrightarrow \beta * \beta'}$$

Изведимо само прво и последње правило, у случају када је $*$ знак за конјункцију. Извођење осталих правила препуштамо читаоцима.

1.	$\vert\ \alpha$	додатна прет.
2.	$\alpha \Rightarrow \alpha$	$\Rightarrow_{\mathrm{U}}$, 1
3.	$\alpha \Leftrightarrow \alpha$	$\Leftrightarrow_{\mathrm{U}}$, 2, 2

Одговарајуће извођење за последње правило само ћемо укратко описати. Из претпоставки $\alpha \Leftrightarrow \beta$ и $\alpha' \Leftrightarrow \beta'$, применом правила $\Leftrightarrow_{\mathrm{E}}^{\mathrm{DL}}$ и $\Leftrightarrow_{\mathrm{E}}^{\mathrm{LD}}$, добијамо $\alpha \Rightarrow \beta$, $\beta \Rightarrow \alpha$, $\alpha' \Rightarrow \beta'$ и $\beta' \Rightarrow \alpha'$. Ако додатно претпоставимо $\alpha \wedge \alpha'$, према $\wedge_{\mathrm{E}}^{\mathrm{L}}$ и $\wedge_{\mathrm{E}}^{\mathrm{D}}$ редом добијамо α и α'. Примењујући $\Rightarrow_{\mathrm{E}}$ на $\alpha \Rightarrow \beta$ и α, добијамо β, а на $\alpha' \Rightarrow \beta'$ и α' добијамо β'. Најзад, користећи $\wedge_{\mathrm{U}}$ изводимо $\beta \wedge \beta'$. Овиме смо доказали $\alpha \wedge \alpha' \Rightarrow \beta \wedge \beta'$. Аналогно се доказује обратна импликација $\beta \wedge \beta' \Rightarrow \alpha \wedge \alpha'$.

Неке теореме исказне логике

Приликом доказивања секвената посебно је корисно користити следеће две опште тврдње које су заједно познате као **став дедукције**. Нека је Γ неки низ претпоставки.

1. Ако је доказив секвент $\Gamma, \alpha \vdash \beta$, онда је доказив и секвент $\Gamma \vdash \alpha \Rightarrow \beta$.

2. Ако је доказив секвент $\Gamma \vdash \alpha \Rightarrow \beta$, онда је доказив и секвент $\Gamma, \alpha \vdash \beta$.

Кратко ћемо образложити оба тврђења. Доказ секвента $\Gamma, \alpha \vdash \beta$ једноставно се може „доградити“ у доказ секвента $\Gamma \vdash \alpha \Rightarrow \beta$.

Доказ за $\Gamma, \alpha \vdash \beta$		
	$\vdots$	претпоставке из Γ
$i.$	α	претпоставка
	$\vdots$	међузакључци
$j.$	β	закључак

$\rightsquigarrow$

Доказ за $\Gamma \vdash \alpha \Rightarrow \beta$		
	$\vdots$	претпоставке из Γ
$i.$	$\vert\ \alpha$	додатна претпоставка
	$\vert\ \vdots$	
$j.$	$\vert\ \beta$	
$j+1.$	$\alpha \Rightarrow \beta$	$\Rightarrow_{\mathrm{U}}$, i-j

Такође, из доказа за $\Gamma \vdash \alpha \Rightarrow \beta$, једноставно добијамо и доказ за $\Gamma, \alpha \vdash \beta$.

Доказ за $\Gamma \vdash \alpha \Rightarrow \beta$		
	$\vdots$	претпоставке из Γ
	$\vdots$	
$j.$	$\alpha \Rightarrow \beta$	закључак

$\rightsquigarrow$

Доказ за $\Gamma, \alpha \vdash \beta$		
	$\vdots$	претпоставке из Γ
	$\vdots$	
$j.$	$\alpha \Rightarrow \beta$	закључак
$j+1.$	α	претпоставка
$j+2.$	β	$\Rightarrow_{\mathrm{E}}$, j, $j+1$

Пример 13. Докажимо да је $\vdash \neg p \vee q \Rightarrow (p \Rightarrow q)$.

Према тврђењу 1 става дедукције (примењеном два пута) довољно је доказати $\neg p \vee q, p \vdash q$. Овај последњи секвент је директно доказив применом правила DS. Дакле, доказив је и секвент $\neg p \vee q \vdash p \Rightarrow q$, као и $\vdash \neg p \vee q \Rightarrow (p \Rightarrow q)$.

Можемо доказати и $\vdash (p \Rightarrow q) \Rightarrow \neg p \vee q$, односно $p \Rightarrow q \vdash \neg p \vee q$.

1.	$p \Rightarrow q$	претпоставка
2.	$p \vee \neg p$	TND
3.	$\mid\ p$	додатна претпоставка
4.	$\mid\ q$	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	$\mid\ \neg p \vee q$	$\vee_{\mathrm{U}}^{\mathrm{D}}$, 4
6.	$\mid\ \neg p$	додатна претпоставка
7.	$\mid\ \neg p \vee q$	$\vee_{\mathrm{U}}^{\mathrm{L}}$, 6
8.	$\neg p \vee q$	$\vee_{\mathrm{E}}$, 2, 3-5, 6-7

Дакле, пошто смо доказали $\vdash \neg p \vee q \Rightarrow (p \Rightarrow q)$ и $\vdash (p \Rightarrow q) \Rightarrow \neg p \vee q$, на основу правила $(\Leftrightarrow_{\mathrm{U}})$ закључујемо да је доказиво $\vdash (p \Rightarrow q) \Leftrightarrow \neg p \vee q$.

Формула α је **теорема исказне логике** ако је доказив секвент $\vdash \alpha$.

Издвајамо неке познате теореме исказне логике којима су исказане еквивалентности неке две формуле.

(1) $\vdash \alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge \gamma$	(2) $\vdash \alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$
(3) $\vdash \alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$	(4) $\vdash \alpha \vee \beta \Leftrightarrow \beta \vee \alpha$
(5) $\vdash \alpha \wedge \alpha \Leftrightarrow \alpha$	(6) $\vdash \alpha \vee \alpha \Leftrightarrow \alpha$
(7) $\vdash \alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$	(8) $\vdash \alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
(9) $\vdash \neg(\alpha \wedge \beta) \Leftrightarrow \neg\alpha \vee \neg\beta$	(10) $\vdash \neg(\alpha \vee \beta) \Leftrightarrow \neg\alpha \wedge \neg\beta$
(11) $\vdash (\alpha \Rightarrow \beta) \Leftrightarrow \neg\alpha \vee \beta$	(12) $\vdash \neg\neg\alpha \Leftrightarrow \alpha$

Наведене теореме исказне логике веома су корисне и углавном ћемо их прећутно подразумевати. Прве две теореме познате су под називом *асоцијативност* конјункције, одн. дисјункције. Због ових теорема смемо писати $\alpha \wedge \beta \wedge \gamma$ и $\alpha \vee \beta \vee \gamma$, јер је свеједно како су заграде постављене. Теореме (3) и (4) познате су као *комутативност* конјункције, одн. дисјункције, и дозвољавају нам да у конјункцијама (дисјункцијама) конјунктима (дисјунктима) мењамо места. Теореме (5) и (6) се називају *законима идемпотентности*. Теореме (7) и (8) изражавају тзв. *дистрибутивност* конјункције према дисјункцији, одн. дисјункције према конјункцији. (9) и (10) су већ познати Де Морганови закони. Најзад, (11) (без неког посебног назива) и (12) (закон двојне негације) у неким случајевима омогућавају да се исказна формула трансформише у једноставнији облик.

Пример 14. Докажимо $\vdash \neg(\alpha \Rightarrow \beta) \Leftrightarrow \alpha \wedge \neg\beta$.

Дати секвент једноставно можемо доказати применом изведених правила која се односе на еквиваленцију и коришћењем одговарајућих теорема исказне логике наведених изнад. Доказ наводимо изостављајући детаљна објашњења.

$$\dfrac{\dfrac{\dfrac{(\alpha \Rightarrow \beta) \Leftrightarrow \neg\alpha \vee \beta}{\neg(\alpha \Rightarrow \beta) \Leftrightarrow \neg(\neg\alpha \vee \beta)} \quad \neg(\neg\alpha \vee \beta) \Leftrightarrow \neg\neg\alpha \wedge \neg\beta}{\neg(\alpha \Rightarrow \beta) \Leftrightarrow \neg\neg\alpha \wedge \neg\beta} \qquad \dfrac{\neg\neg\alpha \Leftrightarrow \alpha \quad \neg\beta \Leftrightarrow \neg\beta}{\neg\neg\alpha \wedge \neg\beta \Leftrightarrow \alpha \wedge \neg\beta}}{\neg(\alpha \Rightarrow \beta) \Leftrightarrow \alpha \wedge \neg\beta}$$

Уобичајено је да се докази овог типа наводе у скраћеном облику формирањем тзв. *еквиваленцијског ланца*, при чему се правила еквиваленције не наводе (већ се подразумевају), а евентуално се наводе само коришћене исказне теореме или њихови називи:

$$\begin{aligned}
\neg(\alpha \Rightarrow \beta) &\Leftrightarrow \neg(\neg\alpha \vee \beta) \quad (\text{јер је } \vdash (\alpha \Rightarrow \beta) \Leftrightarrow \neg\alpha \vee \beta)\\
&\Leftrightarrow \neg\neg\alpha \wedge \neg\beta \quad (\text{Де Морганов закон})\\
&\Leftrightarrow \alpha \wedge \neg\beta \quad (\text{Закон двојне негације})
\end{aligned}$$

Задаци

$$\frac{\alpha \land \beta}{\alpha}\,(\land_E^L) \qquad \frac{\alpha \land \beta}{\beta}\,(\land_E^D) \qquad \frac{\alpha \quad \beta}{\alpha \land \beta}\,(\land_U)$$

$$\frac{\neg\neg\alpha}{\alpha}\,(\neg\neg_E) \qquad \frac{\alpha}{\neg\neg\alpha}\,(\neg\neg_U)$$

$$\frac{\alpha \Rightarrow \beta \quad \alpha}{\beta}\,(\Rightarrow_E) \qquad \frac{\alpha \Rightarrow \beta \quad \neg\beta}{\neg\alpha}\,(\mathrm{MT}) \qquad \frac{\begin{array}{|l}\alpha\\ \vdots\\ \beta\end{array}}{\alpha \Rightarrow \beta}\,(\Rightarrow_U)$$

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \alpha}{\alpha \Leftrightarrow \beta}\,(\Leftrightarrow_U) \qquad \frac{\alpha \Leftrightarrow \beta}{\alpha \Rightarrow \beta}\,(\Leftrightarrow_E^{LD}) \qquad \frac{\alpha \Leftrightarrow \beta}{\beta \Rightarrow \alpha}\,(\Leftrightarrow_E^{DL})$$

$$\frac{\alpha \quad \neg\alpha}{\bot}\,(\neg_E) \qquad \frac{\begin{array}{|l}\alpha\\ \vdots\\ \bot\end{array}}{\neg\alpha}\,(\neg_U) \qquad \frac{\bot}{\alpha}\,(\bot_E)$$

$$\frac{\alpha}{\alpha \lor \beta}\,(\lor_U^L) \qquad \frac{\beta}{\alpha \lor \beta}\,(\lor_U^D) \qquad \frac{\alpha \lor \beta \quad \begin{array}{|l}\alpha\\ \vdots\\ \gamma\end{array} \quad \begin{array}{|l}\beta\\ \vdots\\ \gamma\end{array}}{\gamma}\,(\lor_E)$$

$$\frac{\alpha \lor \beta \quad \neg\alpha}{\beta}\,(\mathrm{DS}) \qquad \frac{\alpha \lor \beta \quad \neg\beta}{\alpha}\,(\mathrm{DS})$$

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \gamma}{\alpha \Rightarrow \gamma}\,(\mathrm{T}) \qquad \frac{\alpha \Rightarrow \beta}{\neg\beta \Rightarrow \neg\alpha}\,(\mathrm{K}) \qquad \frac{\neg\alpha \Rightarrow \neg\beta}{\beta \Rightarrow \alpha}\,(\mathrm{K}) \qquad \frac{}{\alpha \lor \neg\alpha}\,(\mathrm{TND})$$

$$\frac{\neg\alpha \lor \neg\beta}{\neg(\alpha \land \beta)}\,(\mathrm{DM}) \qquad \frac{\neg(\alpha \land \beta)}{\neg\alpha \lor \neg\beta}\,(\mathrm{DM}) \qquad \frac{\neg\alpha \land \neg\beta}{\neg(\alpha \lor \beta)}\,(\mathrm{DM}) \qquad \frac{\neg(\alpha \lor \beta)}{\neg\alpha \land \neg\beta}\,(\mathrm{DM})$$

1. Доказати следеће секвенте:

(1) $\neg p \Rightarrow q, \neg p \vee (\neg q \Rightarrow r), \neg q \vdash r$

(2) $\neg p \vee q \Rightarrow r, s \vee \neg q, \neg t, p \Rightarrow t, \neg p \wedge r \Rightarrow \neg s \vdash \neg q$

(3) $p \wedge q \Rightarrow r, r \Rightarrow s, q \wedge \neg s \vdash \neg p$

(4) $p \Rightarrow q, r \vee s, \neg s \Rightarrow \neg t, \neg q \vee s, \neg s, \neg p \wedge r \Rightarrow u, w \vee t \vdash u \wedge w$

(5) $c \vee e \Rightarrow \neg m, r \Rightarrow m, c \vdash \neg r$

(6) $\neg a \Rightarrow (b \Rightarrow \neg c), c \Rightarrow \neg a, \neg d \vee a \Rightarrow c, \neg d \vdash \neg b$

(7) $e \Rightarrow f, \neg g \Rightarrow \neg f, h \Rightarrow i, e \vee h \vdash g \vee i$

2. Доказати:

(1) $\vdash p \Rightarrow (q \Rightarrow p)$

(2) $\vdash (p \Rightarrow q) \wedge (p \Rightarrow r) \Rightarrow (p \Rightarrow q \wedge r)$

(3) $\vdash (p \Rightarrow q) \wedge (r \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q)$

3. Ако на журку не дође Сања и дође Никола, онда ће доћи и Ема. Ако дође Васа, онда неће доћи Никола и доћи ће Ема. Ако не дође Филип и дође Никола, онда неће доћи Сања. Ако не дође Васа и дође Ема, онда неће доћи Никола. Никола долази на журку. Ко ће још доћи на журку?

4. Аладин се налази испред две пећине A и B. На улазу у пећину A пише „у једној од нас крије се благо“, а на улазу у B „у A нема блага“. Аладин зна да су обе изјаве тачне или су обе лажне. У којој пећини се налази благо?

1.2 Предикатска логика и природна дедукција

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 15. 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*,
- промењиве $x, y, z, x_1, y_1, z_1, x_2, \ldots$ (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 – $\exists x \forall y \neg V(x,y)$

ЗАДАТАК 4. Превести на српски и следећу реченицу:
$\exists x (D(x) \wedge \forall y (M(y) \Rightarrow \neg V(x,y)))$.

Наравно, важно је правилно преводити и са српског на формални језик, па за вежбу дајемо две реченице на српском:
• *Сваког момка воли бар једна девојка и бар једна девојка га не воли.*
• *Свака девојка воли сваког момка који њу воли.*

Предикатске формуле

Сврха претходног примера је да илуструје са каквим формулама радимо у предикатској логици. Уопштено говорећи, при формализацији у предикатској логици узимамо у обзир:

- извесне објекте о којима желимо да говоримо, као и
- шта желимо о њима да говоримо – која *својства* (особине) објеката су нам важна, и које *везе* међу објектима посматрамо; својства и везе називамо *предикатима*.

Универзум (универзум говора) чине сви објекти о којима говоримо. У претходном примеру, универзум чине сви људи. *Променљиве* $x, y, z, x_1, \dots$ користимо да означимо произвољне, неодређене објекте универзума. Поједине, конкретне, одређене објекте универзума називаћемо *константама*. Свака конкретна особа представља неку константу универзума који чине људи.

При формирању предикатских формула користимо и унапред изабране симболе за *особине* објеката и *везе* међу њима. Ове симболе називамо *предикатским симболима*. Подразумева се и да је сваком предикатском симболу придружена тзв. *дужина*, тј. број објеката на које се односи. У претходном примеру, предикатски симболи су M, D, V, при чему су њихове дужине редом 1, 1, 2. Наравно, број и врста предиката могу бити и другачији у зависности од ситуације коју описујемо. Предикатске симболе дужине 1 називаћемо *унарним*, а предикатске симболе дужине 2 називамо *бинарним.* У наредним примерима углавном нећемо наглашавати дужину одговарајућих предикатских симбола, јер ће то из контекста бити јасно.

Атомичне (елементарне) формуле градимо тако што предикатским симболом повежемо одговарајући број симбола који се односе на објекте универзума (константе и/или променљиве).

Пример 16. Користећи предикатске симболе из претходног примера, M, D, V и две константе `Mika` и `Ana`, запишимо неке елементарне формуле:

$$M(x), M(y), M(\texttt{Mika}),\ D(x), D(\texttt{Ana}), V(x,\texttt{Ana}), V(x,x_1), \ldots$$

Полазећи од атомичних формула, употребом везника $(\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow)$, на уобичајени начин, и квантификатора $(\forall, \exists)$ формирамо предикатске формуле. Квантификаторе користимо тако што испред већ формиране предикатске формуле, постављамо један од квантификатора заједно са неком променљивом. 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 17. 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. Појављивања осталих променљивих су везана.

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

Кажемо да је променљива 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 18. 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.

Правила дедукције за квантификаторе

Поред правила дедукције која примењујемо и на предикатске формуле, користимо и у предикатској логици, користимо и правила за квантификаторе.

Супституција

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

Ако је α нека формула, x променљива и c константа, онда са $\alpha[c/x]$ означавамо формулу добијену заменом свих слободних појављивања променљиве x константом c. Наравно, ако x није слободно у α, онда је формула $\alpha[c/x]$ 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, настало заменом x са y, не сме да постане везано. У наредном примеру, илуструјемо разлоге овог ограничења.

Пример 19. Ако се ослонимо на интерпретацију из примера 15, онда се формула

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

битно не разликује од формуле

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

Исто важи ако y заменимо било којом другом променљивом, **осим** променљивом x, јер би то изазвало драстичну промену значења:

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

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 $\alpha[y/x]$ означавамо формулу добијену након описане замене. У наставку, када год напишемо $\alpha[y/x]$ подразумеваћемо да је променљива x слободна за y у формули α. Приметимо да је x увек слободно за x и да је формула $\alpha[x/x]$ истоветна формули α.

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

Пре него што наведемо насловљена правила, мотивисаћемо их неким интуитивним аргументима. Нека је P неки 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.

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

Ако је $\forall x \alpha$ тачно, тада мора бити тачна и формула $\alpha[v/x]$ добијена из α заменом свих слободних појављивања променљиве x у формули α са v, при чему је v константа или променљива за коју је x слободно у α.

Будући да на располагању имамо неограничено 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.

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

Пример 20.

$$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x)), \texttt{Covek}(\texttt{Sokrat}) \vdash \texttt{Smrtan}(\texttt{Sokrat})$$

1.	$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x))$	претпоставка
2.	$\texttt{Covek}(\texttt{Sokrat})$	претпоставка
3.	$\texttt{Covek}(\texttt{Sokrat}) \Rightarrow \texttt{Smrtan}(\texttt{Sokrat})$	$\forall x_{\mathrm{E}}$, 1
4.	$\texttt{Smrtan}(\texttt{Sokrat})$	$\Rightarrow_{\mathrm{E}}$, 3, 2

Правило „($\vee_U$)“

$$\frac{R(c_i)}{R(c_1) \vee R(c_2) \vee R(c_3) \vee \cdots} \ (\vee_U)$$

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

$\boxed{\dfrac{\alpha[v/x]}{\exists x\alpha}\ (\exists_U)}$ Ако је $\alpha[v/x]$ тачно, за неку константу или променљиву v, тада мора бити тачно $\exists x\alpha$.

Пример 21.

$$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x)), \texttt{Covek}(\texttt{Sokrat}) \vdash \exists x \texttt{Smrtan}(x)$$

1.	$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x))$	претпоставка
2.	$\texttt{Covek(Sokrat)}$	претпоставка
3.	$\texttt{Covek(Sokrat)} \Rightarrow \texttt{Smrtan(Sokrat)}$	$\forall x_E$, 1
4.	$\texttt{Smrtan(Sokrat)}$	$\Rightarrow_E$, 3, 2
5.	$\exists x \texttt{Smrtan}(x)$	$\exists x_U$, 4

Правила $\forall x_U$ и $\exists x_E$

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.

$$\boxed{\dfrac{\begin{array}{|c} v \\ \vdots \\ \alpha[v/x] \end{array}}{\forall x\alpha}\ (\forall x_U)}$$

Ако се коришћењем *свеже* променљиве може доказати $\alpha[v/x]$, 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 $\alpha[v/x]$.
$k.$	$\alpha[v/x]$		Када успемо,
$k+1.$	$\forall x\alpha$	$(\forall x_{\mathrm{U}})$, j-k	изводимо жељени закључак.

Пример 22. 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.	$\quad v$	уводимо свежу променљиву
4.	$\quad A(v) \Rightarrow B(v)$	$\forall x_{\mathrm{E}}$, 1
5.	$\quad B(v) \Rightarrow C(v)$	$\forall x_{\mathrm{E}}$, 2
6.	$\quad A(v) \Rightarrow C(v)$	транзитивност импликације, 4, 5
7.	$\forall x(A(x) \Rightarrow C(x))$	$\forall x_{\mathrm{U}}$, 3-6

Задатак 5. 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 23. 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 претпоствка
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 6. Доказати секвент $\forall x \neg P(x), \forall x \neg Q(x) \vdash \forall x(P(x) \Leftrightarrow Q(x))$.

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.

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

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

ПРИМЕР 24. Докажимо секвент:

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

Неформално

Да бисмо што јасније образложили наведени секвент, ослонићемо се на интерпретацију наведену у примеру 15. 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.	$\exists x(D(x) \land \forall y(M(y) \Rightarrow V(y,x)))$	претпоставка
2.	$M(\texttt{Mile})$	претпоставка
3.	$v \quad D(v) \land \forall y(M(y) \Rightarrow V(y,v))$	додатна претпоставка
4.	$\quad \forall y(M(y) \Rightarrow V(y,v))$	$\land^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	$\quad M(\texttt{Mile}) \Rightarrow V(\texttt{Mile},v)$	$\forall x_{\mathrm{E}}$, 4
6.	$\quad V(\texttt{Mile},v)$	$\Rightarrow_{\mathrm{E}}$, 5, 2
7.	$\quad \exists z V(\texttt{Mile},z)$	$\exists z_{\mathrm{U}}$, 6
8.	$\exists z V(\texttt{Mile},z)$	$\exists x_{\mathrm{E}}$, 1, 3-7

Пример 25. 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.	$\quad B(v,v)$	$\forall x_{\mathrm{E}}$, 1
4.	$\quad \exists y B(v,y)$	$\exists y_{\mathrm{U}}$, 3 ($B(v,v)$ је истоветна формули $B(v,y)[v/y]$)
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 26. 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"
$\forall x \forall y \forall z (O(x,y,z) \Rightarrow O(z,y,x) \land \neg O(y,z,x))$
(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 $\forall x \forall y \forall z (O(x,y,z) \Rightarrow O(z,y,x) \land \neg O(y,z,x)) \cdots (*)$.
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 $[c/x], [b/y], [a/z]$.)
$O(a,b,c)$ 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

Пример 27. Доказати да из
(1) $\forall x \exists y V(x,y)$
(2) $\forall x \forall y \forall u \forall v (V(x,u) \wedge V(y,v) \Rightarrow V(u,v) \vee V(v,u))$
(3) $\forall x \forall y \forall z (V(x,y) \wedge V(y,z) \Rightarrow V(x,z))$
следи $\forall x \forall y \exists z (V(x,z) \wedge V(y,z))$.

Неформално

Нека су a и b произвољни објекти.
Како, због (1), $\exists y V(a,y)$, нека је a' објекат такав да $V(a,a')$. Важи и $\exists y V(b,y)$, па нека је b' објекат такав да је $V(b,b')$. Из (2) следи да је $V(a',b')$ или $V(b',a')$.

Први случај: $V(a',b')$. Из $V(a,a')$ и $V(a',b')$, према (3) следи $V(a,b')$. Како је и $V(b,b')$, закључујемо $\exists z (V(a,z) \wedge V(b,z))$.

Други случај: $V(b',a')$. Из $V(b,b')$ и $V(b',a')$, према (3) следи $V(b,a')$. Како је и $V(a,a')$, закључујемо $\exists z (V(a,z) \wedge V(b,z))$.

Дакле, $\exists z (V(a,z) \wedge V(b,z))$, па како су a и b произвољни, коначно добијамо $\forall x \forall y \exists z (V(x,z) \wedge V(y,z))$.

Формалан доказ препуштамо читаоцима.

Неке теореме предикатске логике

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

Када смо навели правило $(\forall x_{\mathrm{U}})$, посебно смо истакли да v мора бити свежа променљива која се не појављује слободно нигде ван поддоказа (наравно, може се слободно појављивати у формулама подоказа).

У формалним доказима, које смо до сада наводили, правило $(\forall x_{\mathrm{U}})$ смо примењивали након што смо у поддоказу извели $\alpha[v/x]$, за неку свежу променљиву v. Међутим, формула $\alpha(v)$ са слободном променљивом v може бити и претпоставка, па нам није потребан поддоказ да бисмо је извели. Уколико v није слободно у осталим претпоставкама (низа Γ), онда је v свежа променљива поддоказа који чини сâмо навођење претпоставке $\alpha(v)$.

$$\begin{array}{lll} & \vdots & v \text{ није слободно у } \Gamma \\ i. & \alpha(v) & \text{претпоставка} \end{array} \quad\rightsquigarrow\quad \begin{array}{rl|l} & \vdots & v \text{ није слободно у } \Gamma \\ i. & \multicolumn{1}{|l}{v} & \\ i+1. & \multicolumn{1}{|l}{\quad\alpha(v)} & \text{претпоставка} \\ i+2. & \forall x\alpha[x/v] & \forall x_{\mathrm{U}},\ i\text{-}i+1 \end{array}$$

Из претходног разматрања следи: *Ако v није слободно у формулама из Γ, онда $\Gamma, \alpha(v) \vdash \forall x\alpha[x/v]$.* Специјално, $\alpha(v) \vdash \forall x\alpha[x/v]$. Ово запажање ћемо искористити да изведемо два правила која ће нам бити од користи при формирању еквиваленцијских ланаца у предикатској логици.

$$\boxed{\dfrac{\alpha \Leftrightarrow \beta}{\forall x\alpha \Leftrightarrow \forall x\beta} \qquad \dfrac{\alpha \Leftrightarrow \beta}{\exists x\alpha \Leftrightarrow \exists x\beta}}$$

$$\begin{array}{rll} 1. & \alpha \Leftrightarrow \beta & \\ 2. & \forall x(\alpha \Leftrightarrow \beta) & \forall x_{\mathrm{U}}, 1 \\ 3. & \mid \forall x\alpha & \\ 4. & \mid\mid v & \\ 5. & \mid\mid \quad \alpha[v/x] & \forall x_{\mathrm{E}}, 3 \\ 6. & \mid\mid \quad \alpha[v/x] \Leftrightarrow \beta[v/x] & \forall x_{\mathrm{E}}, 2 \\ 7. & \mid\mid \quad \alpha[v/x] \Rightarrow \beta[v/x] & \Leftrightarrow_{\mathrm{U}}^{\mathrm{LD}}, 6 \\ 8. & \mid\mid \quad \beta[v/x] & \Rightarrow_{\mathrm{E}}, 5, 7 \\ 9. & \mid \forall x\beta & \forall x_{\mathrm{U}}, 4\text{-}8 \\ 10. & \forall x\alpha \Rightarrow \forall x\beta & \Rightarrow_{\mathrm{U}}, 3\text{-}9 \\ & \vdots & \\ 18. & \forall x\beta \Rightarrow \forall x\alpha & \\ 19. & \forall x\alpha \Leftrightarrow \forall x\beta & \Leftrightarrow_{\mathrm{U}}, 10, 18 \end{array}$$

$$\begin{array}{rll} 1. & \alpha \Leftrightarrow \beta & \\ 2. & \forall x(\alpha \Leftrightarrow \beta) & \forall x_{\mathrm{U}}, 1 \\ 3. & \mid \exists x\alpha & \\ 4. & \mid\mid v\ \alpha[v/x] & \\ 5. & \mid\mid \quad \alpha[v/x] \Leftrightarrow \beta[v/x] & \forall x_{\mathrm{E}}, 2 \\ 6. & \mid\mid \quad \alpha[v/x] \Rightarrow \beta[v/x] & \Leftrightarrow_{\mathrm{U}}^{\mathrm{LD}}, 5 \\ 7. & \mid\mid \quad \beta[v/x] & \Rightarrow_{\mathrm{E}}, 4, 6 \\ 8. & \mid\mid \quad \exists x\beta & \exists x_{\mathrm{U}}, 7 \\ 9. & \mid \exists x\beta & \exists x_{\mathrm{E}}, 3, 4\text{-}8 \\ 10. & \exists x\alpha \Rightarrow \exists x\beta & \Rightarrow_{\mathrm{U}}, 3\text{-}9 \\ & \vdots & \\ 18. & \exists x\beta \Rightarrow \exists x\alpha & \\ 19. & \exists x\alpha \Leftrightarrow \exists x\beta & \Leftrightarrow_{\mathrm{U}}, 10, 18 \end{array}$$

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
$\vdash \forall x \forall y \alpha \Leftrightarrow \forall y \forall x \alpha$ $\qquad$ $\vdash \exists x \exists y \alpha \Leftrightarrow \exists y \exists x \alpha$

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

Де Органови закони за квантификаторе
$\vdash \neg \exists x \alpha \Leftrightarrow \forall x \neg \alpha$ $\qquad$ $\vdash \neg \forall x \alpha \Leftrightarrow \exists x \neg \alpha$

„$\forall$ пролази кроз $\wedge$, а $\exists$ кроз $\vee$“
$\vdash \forall x(\alpha \wedge \beta) \Leftrightarrow \forall x \alpha \wedge \forall x \beta$ $\qquad$ $\vdash \exists x(\alpha \vee \beta) \Leftrightarrow \exists x \alpha \vee \exists x \beta$

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

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

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

Задатак 7. 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 8. 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	$\mid x$	Докажимо најпре $\forall x\alpha$.
3.	$\mid\quad \alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
4.	$\mid\quad \alpha$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 3
5.	$\forall x\alpha$	$\forall x_{\mathrm{U}}$, 2-4
6.	$\mid x$	Докажимо даље $\forall x\beta$.
7.	$\mid\quad \alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
8.	$\mid\quad \beta$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 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.	$\mid x$	
5.	$\mid\quad \alpha$	$\forall x_{\mathrm{E}}$, 2
6.	$\mid\quad \beta$	$\forall x_{\mathrm{E}}$, 3
7.	$\mid\quad \alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 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	$\mid v\quad \alpha[v/x]\wedge\beta$	додатна прет. ($\beta[v/x]$ је истоветно формули β)
3.	$\mid\quad \alpha[v/x]$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 2
4.	$\mid\quad \beta$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	$\mid\quad \exists x\alpha$	$\exists x_{\mathrm{U}}$, 3
6.	$\mid\quad \exists x\alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 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.	$\exists x\alpha$	$\wedge_{\mathrm{E}}^{\mathrm{L}}$, 1
3.	β	$\wedge_{\mathrm{E}}^{\mathrm{D}}$, 1
4	v $\alpha[v/x]$	додатна прет.
5.	$\alpha[v/x] \wedge \beta$	$\wedge_{\mathrm{U}}$, 4, 3
6.	$\exists x(\alpha \wedge \beta)$	$\wedge_{\mathrm{E}}^{\mathrm{D}}$, 5 ($\beta[v/x]$ је истоветно формули β)
7.	$\exists x(\alpha \wedge \beta)$	$\exists x_{\mathrm{E}}$, 2, 4-6

Задатак 9. 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.

Задаци

$$\frac{\forall x\alpha}{\alpha[v/x]}\ (\forall x_{\mathrm{E}}) \qquad \frac{\begin{array}{|ll} v & \vdots \\ & \alpha[v/x] \end{array}}{\forall x\alpha}\ (\forall x_{\mathrm{U}})$$

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

$$\frac{\neg\forall x\alpha}{\exists x\neg\alpha}\ (\mathrm{DM}) \qquad \frac{\neg\exists x\alpha}{\forall x\neg\alpha}\ (\mathrm{DM})$$

5. Имајући на уму универзум свих људи, користећи унарни предикат $\texttt{D}$, бинарни предикат $\texttt{P}$, са значењима:
$\texttt{D}(x)$ – „x је добар (човек)“ и
$\texttt{P}(x,y)$ – „x има пријатеља y“,
и константу $\texttt{Ana}$ изразити формулама следеће реченице:

(1) Свако ко има пријатеља је добар.

(2) Постоји неко чији су сви пријатељи добри.

(3) Неки Анини пријатељи нису добри.

(4) Сви Анини пријатељи су добри.

(5) Сви добри људи су Анини пријатељи.

(6) Сви пријатељи свих Аниних пријатеља, такође су и Анини пријатељи.

(7) Неки пријатељи неких Аниних пријатеља нису добри.

(8) Сваки Анин пријатељ има пријатеље који су добри.

(9) Неким Аниним пријатељима, Ана није пријатељ.

(10) Постоје Анини пријатељи који немају пријатеље.

6. Доказати:

(1) $\forall x(P(x) \Rightarrow Q(x)), \forall x P(x) \vdash \forall x Q(x)$

(2) $\forall x(P(x) \Rightarrow Q(x)), \exists x P(x) \vdash \exists x Q(x)$

7. Доказати:

(1) $\forall x(\texttt{Som}(x) \Rightarrow \texttt{Riba}(x)), \neg\texttt{Riba}(\texttt{Dambo}) \vdash \neg\texttt{Som}(\texttt{Dambo})$

(2) $\forall x(M(x) \Rightarrow \exists y(D(y) \land V(x,y))), M(\texttt{Mile}) \vdash \exists z V(\texttt{Mile}, z)$

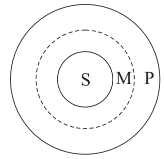
8. [Аристотелови силогизми] Посматрајмо следећа четири типа тврдњи:

(A) **сви** S **јесу** P: $\forall x(S(x) \Rightarrow P(x))$ (E) **ниједан** S **није** P: $\forall x(S(x) \Rightarrow \neg P(x))$

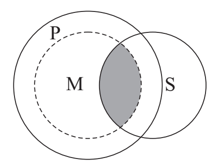
(I) **неки** S **јесу** P: $\exists x(S(x) \wedge P(x))$ (O) **неки** S **нису** P: $\exists x(S(x) \wedge \neg P(x))$

Правилима дедукције доказати да из претпоставки изнад црте изводимо закључак испод црте.

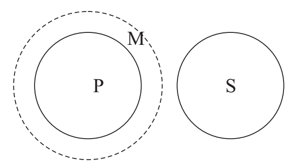
$$(1)\quad \dfrac{\begin{array}{l}\text{сви } M \text{ јесу } P\\ \text{сви } S \text{ јесу } M\end{array}}{\text{сви } S \text{ јесу } P}$$



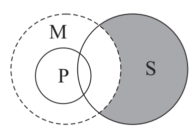
$$(2)\quad \dfrac{\begin{array}{l}\text{сви } M \text{ јесу } P\\ \text{неки } M \text{ јесу } S\end{array}}{\text{неки } S \text{ јесу } P} \qquad (3)\quad \dfrac{\begin{array}{l}\text{сви } M \text{ јесу } P\\ \text{неки } S \text{ јесу } M\end{array}}{\text{неки } S \text{ јесу } P}$$



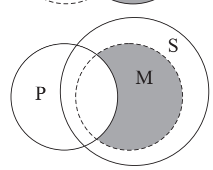
$$(4)\quad \dfrac{\begin{array}{l}\text{сви } P \text{ јесу } M\\ \text{ниједан } S \text{ није } M\end{array}}{\text{ниједан } S \text{ није } P} \qquad (5)\quad \dfrac{\begin{array}{l}\text{сви } P \text{ јесу } M\\ \text{ниједан } M \text{ није } S\end{array}}{\text{ниједан } S \text{ није } P}$$



$$(6)\quad \dfrac{\begin{array}{l}\text{сви } P \text{ јесу } M\\ \text{неки } S \text{ нису } M\end{array}}{\text{неки } S \text{ нису } P}$$

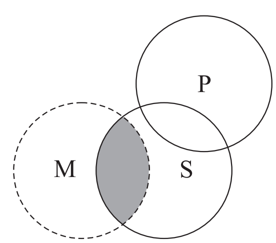


$$(7)\quad \dfrac{\begin{array}{l}\text{неки } M \text{ нису } P\\ \text{сви } M \text{ јесу } S\end{array}}{\text{неки } S \text{ нису } P}$$



$$(8)\quad \dfrac{\begin{array}{l}\text{ниједан } M \text{ није } P\\ \text{неки } M \text{ јесу } S\end{array}}{\text{неки } S \text{ нису } P} \qquad (9)\quad \dfrac{\begin{array}{l}\text{ниједан } M \text{ није } P\\ \text{неки } S \text{ јесу } M\end{array}}{\text{неки } S \text{ нису } P}$$

$$(10)\quad \dfrac{\begin{array}{l}\text{ниједан } P \text{ није } M\\ \text{неки } S \text{ јесу } M\end{array}}{\text{неки } S \text{ нису } P} \qquad (11)\quad \dfrac{\begin{array}{l}\text{ниједан } P \text{ није } M\\ \text{неки } M \text{ јесу } S\end{array}}{\text{неки } S \text{ нису } P}$$



9. Доказати:

(1) $\forall x(A(x) \Rightarrow B(x)), \exists x \neg B(x) \vdash \exists x \neg A(x)$

(2) $\forall x(A(x) \vee B(x) \Rightarrow C(x)), \exists x \neg C(x) \vdash \exists x \neg A(x)$

(3) $\forall x(N(x) \wedge S(x) \Rightarrow C(x)), \forall x(T(x) \Rightarrow N(x)), \exists x(T(x) \wedge \neg C(x)) \vdash \exists x \neg S(x)$

(4) $\forall x(N(x) \Rightarrow B(x)), \exists x(N(x) \wedge D(x)) \vdash \exists x(B(x) \wedge D(x))$

(5) $\forall x((A(x) \Rightarrow R(x)) \vee T(x)), \exists x(T(x) \Rightarrow P(x)), \forall x(A(x) \wedge \neg P(x)) \vdash \exists x R(x)$

(6) $\forall x \exists y(E(x) \Rightarrow M(x) \vee N(y)), \neg \forall x M(x), \forall x E(x) \vdash \exists x N(x)$

10. Доказати:

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

(2) $\forall x (A(x) \Rightarrow B(x)) \vdash \forall x (\exists y (A(y) \wedge C(x,y)) \Rightarrow \exists y (B(x) \wedge C(x,y)))$

11. Доказати:

(1) $\forall x \forall y (R(x,y) \Rightarrow \neg R(y,x)) \vdash \forall x \neg R(x,x)$

(2) $\forall x \neg R(x,x), \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow R(x,z)) \vdash \forall x \forall y (R(x,y) \Rightarrow \neg R(y,x))$

(3) $\forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow \neg R(x,z)) \vdash \forall x \neg R(x,x)$

(4) $\forall x \exists y R(x,y), \forall x \forall y (R(x,y) \Rightarrow R(y,x)), \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow R(x,z)) \vdash \forall x R(x,x)$

12. Из претпоставки

$\exists x \exists y (A(x) \wedge A(y) \wedge \neg R(x,y))$ и

$\forall x \forall y (B(x) \wedge B(y) \Rightarrow R(x,y))$

неформално извести $\exists x (A(x) \wedge \neg B(x))$.

13. Из претпоставки

$\exists x (F(x) \wedge \forall y (G(y) \Rightarrow H(x,y)))$ и

$\forall x (F(x) \Rightarrow \forall y (B(y) \Rightarrow \neg H(x,y)))$

неформално извести $\forall x (G(x) \Rightarrow \neg B(x))$.

14. Из претпоставки

$\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_2,x_3,x_4,x_1))$ и

$\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_3,x_1,x_2,x_4))$

неформално извести сваку од следећих формула:

(1) $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_3,x_4,x_1,x_2))$

(2) $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_4,x_1,x_2,x_3))$

(3) $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_2,x_3,x_1,x_4))$

(4) $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_1,x_2,x_4,x_3))$

2

Теорија скупова

2.1 Аксиоме теорије скупова - I

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 атомичних 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.

Аксиома екстензионалности

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

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

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

Одмах можемо доказати неке очекиване особине једнакости.

Теорема 1. (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 $a = a$.

Напомена 1. 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.	$\forall x (x \in a \Leftrightarrow x \in a) \Rightarrow a = a$	$\Leftrightarrow^{\mathrm{DL}}_{\mathrm{E}}$, 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 2. 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**.5 под (4) и (5).

Инклузија

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*. Формално, $a \subseteq b$ (као и $b \supseteq a$) је скраћени запис формуле $\forall x(x \in a \Rightarrow x \in b)$. 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 $a \subset b$ ($b \supset a$). Формално, $a \subset b$ је скраћени запис формуле $a \subseteq b \wedge a \neq b$.

ТЕОРЕМА 2. (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**.22 и задатка **1**.5 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. $\square$

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 3. Наводимо и формални доказ секвента

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

1.	$\forall x(\neg x \in y_1)$	
2.	$\forall x(\neg x \in y_2)$	
3.	x	
4.	$x \in y_1$	
5.	$\neg x \in y_1$	$\forall x_{\mathrm{E}}$, 1
6.	$\perp$	$\neg_{\mathrm{E}}$, 4, 5
7.	$x \in y_2$	$\perp_{\mathrm{E}}$, 6
8.	$x \in y_1 \Rightarrow x \in y_2$	$\Rightarrow_{\mathrm{U}}$, 4-7
9.	$x \in y_2$	
10.	$\neg x \in y_2$	$\forall x_{\mathrm{E}}$, 2
11.	$\perp$	$\neg_{\mathrm{E}}$, 9, 10
12.	$x \in y_1$	$\perp_{\mathrm{E}}$, 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

Приметимо да је ово извођење потпуно аналогно извођењу секвента из задатка **1**.6.

Јединствени скуп који нема елемената означавамо са $\emptyset$ и називамо га **празним скупом**. 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:

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

Уопште, формуле облика

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

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

ТЕОРЕМА 3. 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.	x	
3.	$x \in \emptyset$	
4.	$\neg x \in \emptyset$	$\forall x_{\mathrm{E}}$, 1
5.	$\perp$	$\neg_{\mathrm{E}}$, 3, 4
6.	$x \in a$	$\perp_{\mathrm{E}}$, 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

□

Аксиоме пара, издвајања, уније и партитивног скупа

Све насловљене аксиоме, које наводимо у овом одељку, јесу облика

$$(\alpha^*) \qquad \forall a_1 \cdots \forall a_n \exists y \forall x(x \in y \Leftrightarrow \alpha(x, a_1, \ldots, a_n)),$$

где ће $\alpha(x, a_1, \ldots, a_n)$ бити нека формула специјалног облика, у којој се y не појављује слободно и свака променљива која се слободно појављује у овој формули јесте нека (не нужно и свака) од променљивих $x, a_1, \ldots, a_n$. Интуитивно, наведени облик разумемо на следећи начин: ако су $a_1, \ldots, a_n$ произвољни скупови, тада постоји скуп y који садржи само оне x за које се може утврдити веза $\alpha(x, a_1, \ldots, a_n)$. За сваку формулу α, скуп y чије постојање тврди формула (α^*) мора бити јединствен према аксиоми екстензионалности. Заиста, ако за произвољно изабране $a_1, \ldots, a_n$, са y_1 и y_2 означимо скупове такве да је

$$\forall x(x \in y_1 \Leftrightarrow \alpha(x, a_1, \ldots, a_n)) \text{ и } \forall x(x \in y_2 \Leftrightarrow \alpha(x, a_1, \ldots, a_n)),$$

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

Поставља се питање, можемо ли за свако α, формулу (α^*) 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:

$$\begin{array}{rl|ll} 1. & \multicolumn{2}{l}{\exists y \forall x (x \in y \Leftrightarrow x \notin x)} & \\ 2. & & v \ \forall x (x \in v \Leftrightarrow x \notin x) & \\ 3. & & \quad v \in v \Leftrightarrow v \notin v & \forall x_{\mathrm{E}},\ 2 \\ & & \quad \vdots & \\ i. & & \quad \perp & \\ i+1. & \multicolumn{2}{l}{\perp} & \exists x_{\mathrm{E}},\ 1,\ 2\text{-}i \end{array}$$

Контрадикција је свакако нешто што не смемо дозволити. Дакле, шема (α^*) је неприхватљива у општем случају. Смемо је користити само за формуле $\alpha(x, a_1, \ldots, a_n)$ специјалног облика:

- $x = a_1 \vee x = a_2$,
- $x \in a \wedge \varphi(x, a, a_1, \ldots, a_n)$, за било коју формулу $\varphi(x, a, a_1, \ldots, a_n)$,
- $\forall t (t \in x \Rightarrow t \in a)$,
- $\exists t (t \in a \wedge x \in t)$.

$\boxed{\text{Аксиома пара } \forall a_1 \forall a_2 \exists y \forall x (x \in y \Leftrightarrow x = a_1 \vee x = a_2)}$

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:

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

$\boxed{\text{Аксиома издвајања } \forall a \forall a_1 \cdots \forall a_n \exists y \forall x (x \in y \Leftrightarrow x \in a \wedge \varphi(x, a, a_1, \ldots, a_n))}$

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

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

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:

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

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

Сетимо се да $x \subseteq a$ схватамо као скраћење формуле $\forall t(t \in x \Rightarrow t \in a)$, 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:

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

$\boxed{\text{Аксиома уније } \forall a \exists y \forall x (x \in y \Leftrightarrow \exists t (t \in a \wedge x \in t))}$

Аксиома уније 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.

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

Пример 1. Полазећи од празног скупа $\emptyset$, наводимо неке од скупова које можемо изградити применом наведених аксиома.

Користећи аксиому пара: $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, $\{\emptyset,\{\emptyset\}\}$, $\{\emptyset,\{\{\emptyset\}\}\}$, $\{\{\emptyset\},\{\{\emptyset\}\}\}$ итд. Приметимо да су сви наведени скупови међусобно различити.

Користећи аксиому партитивног скупа: $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset,\{\emptyset\}\}$, $\mathcal{P}(\{\emptyset,\{\emptyset\}\}) = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}$ 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

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

Да би се лакше уочило да претходна једнакост важи, подвлачимо елементе скупа чију унију тражимо, а надвлачимо елементе елемената истог скупа:

$$\{\,\underline{\{\overline{\emptyset}\}},\,\underline{\{\overline{\{\emptyset\}},\overline{\{\{\emptyset\}\}}\}}\,\}.$$

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 $\bigcup a = \{\cancel{\{}\emptyset\cancel{\}},\cancel{\{}\{\emptyset\},\{\{\emptyset\}\}\cancel{\}}\}$

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 $\{a,b,c\} \in \mathcal{P}(X)$.

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 4. Не постоји скуп који садржи све скупове.

Доказ. Из наведених аксиома извешћемо формулу $\neg\exists y\forall x(x \in y)$. Уместо формалног извођења, наводимо само основне кораке доказа.

Претпоставимо супротно, 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 $\exists y \forall x (x \in y)$. Дакле, $\neg \exists y \forall x (x \in y)$. □

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

Доказ. Тврђење директно следи из претходне теореме и Де Моргановиx 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 непразних скупова. 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 $\forall t (t \in \emptyset \Rightarrow x \in t)$).

На крају овог одељка уводимо ознаке за неколико скупова које ћемо касније често користити у примерима. Те скупове означићемо познатим симболима за природне бројеве (из разлога који ће касније бити сасвим јасни): $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$, $3 = \bigcup \{2, \{2\}\} = \{0,1,2\}$, $4 = \bigcup \{3, \{3\}\} = \{0,1,2,3\}$ итд.

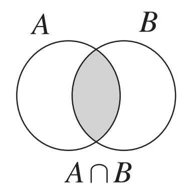
Задатак 1. За било које скупове a, b, c, оправдати постојање и јединственост скупа $\{a,b,c\}$.

Задатак 2. Доказати да за сваки скуп a важи једнакост $a = \bigcup \mathcal{P}(a)$.

2.2 Булове операције и Декартов производ

Већ смо нагласили да ћемо као промењљиве користити и велика слова латинице, што је у математичкој литератури уобичајено, па ћемо у наставку све чешће тако поступати. Користећи наведене аксиоме, уводимо тзв. Булове (скуповне) операције.

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.

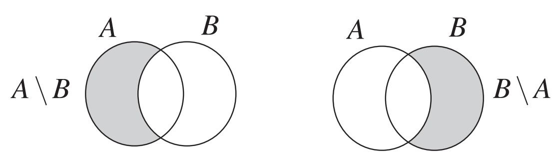


Формално, из уведених аксиома се доказује:

$$\forall A \forall B \exists ! Y \forall x (x \in Y \Rightarrow \underbrace{x \in A \wedge x \in B}_{x \in A \wedge \alpha(x,A,B)}).$$

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 $A \cap B = \emptyset$.

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.

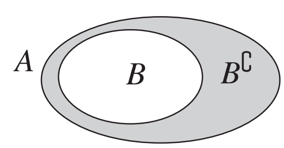


Из уведених аксиома се доказује:

$$\forall A \forall B \exists ! Y \forall x (x \in Y \Rightarrow x \in A \wedge x \notin B)$$

Разлику скупова A и B означавамо $A \setminus B$: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

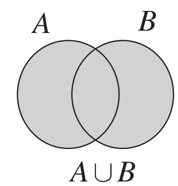
Специјално, ако је $B \subseteq A$, разлику $A \setminus B$ називамо **комплементом** скупа B у односу на A. Када је у неком контексту јасно у односу на који скуп A се одређују комплементи, онда уместо $A \setminus B$ пишемо $B^{\complement}$.



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.

Формално, унија два скупа се уводи на следећи начин: $A \cup B = \bigcup \{A, B\}$. За било које x имамо:

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



Наведеним еквиваленцијским ланцем оправдан је уобичајени запис

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

Напомена 4. 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
$i+2.$	$\exists t (t = A \wedge x \in t)$	$\exists t_{\mathrm{U}}$, $i+1$

Теорема 5. 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 еквиваленииција 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

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

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

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

□

Теорема 6. 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 $A \setminus C \subseteq A \setminus B$. $\square$

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 2. 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 6 (1) и леме 2 (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 6 (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 $X \nsubseteq A$ и $X \nsubseteq B$. 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:

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

Уређен пар скупова a и b, у ознаци (a,b), замишљамо као целину коју чине a и b наведени одређеним редоследом – јасно се зна 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 $b = d$.

Формално, уређен пар скупова a и b можемо дефинисати као скуп $\{\{a\},\{a,b\}\}$: $(a,b) \stackrel{\text{def}}{=} \{\{a\},\{a,b\}\}$. Приметимо да уређен пар (a,b) није исто што и пар $\{a,b\}$. За уређени пар (a,b), скуп a се назива *прва координата*, а скуп b *друга координата*. Докажимо да за овако уведене уређене парове важи наведена особина.

Теорема 7. Нека су a, b, c и d било који скупови. Тада:

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

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 $b = d$. □

Декартов производ скупова A и B јесте скуп уређених парова чије прве координате припадају скупу A, а друге скупу B. Да бисмо оправдали постојање једног оваквог скупа, најпре ћемо одредити скуп у коме се (између осталог) налазе сви уређени парови наведеног облика, а затим ћемо из тог скупа издвојити само жељене уређене парове.

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. $\{a\},\{a,b\} \in \mathcal{P}(A \cup B)$. 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 скупове (који нису уређени парови, као и уређене парове чије координате не испуњавају постављени услов), али применом аксиоме издвајања можемо формирати најављени Декартов производ који ћемо означавати $A \times B$:

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

У математичкој литератури врло често се Декартов производ $A \times B$ задаје као скуп $\{(a,b) \mid a \in A \wedge b \in B\}$, што је оправдано јер знамо да су сви елементи скупа $A \times B$ уређени парови и то управо они чија прва координата долази из A, а друга из B. Када желимо да докажемо да извесни уређени пар (x,y) припада $A \times B$, довољно је да докажемо $x \in A$ и $y \in B$.

$$(x,y) \in A \times B \Leftrightarrow x \in A \wedge y \in B$$

Пример 3. 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 1. 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.

НАПОМЕНА 5. 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.

2.3 Релације

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

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

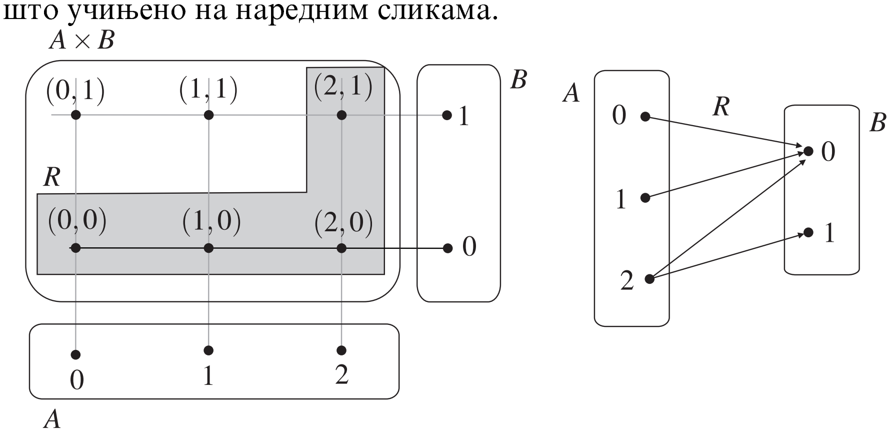
Сличне договоре примењујемо у обичном тексту: „за сваки (постоји) $x \in X$“ значи „за сваки (постоји) x који припада X“. Такође, „скуп $X \subseteq A$“ значи „скуп X који је подскуп скупа A“.

До сада смо нове појмове уводили у обичном тексту истичући их масним словима. У наставку, за сваки важан појам наводимо издвојену дефиницију.

Дефиниција 1. 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.

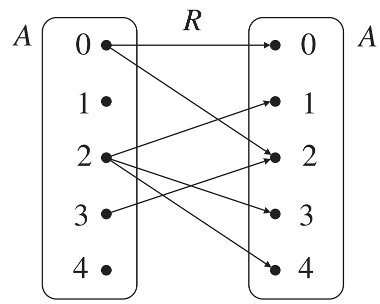
Дакле, $\mathcal{P}(A \times B)$ је скуп свих релација између A и B.

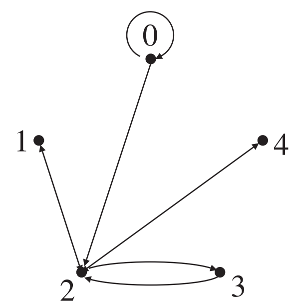
Пример 4. Ако је $A = \{0,1,2\}$ и $B = \{0,1\}$, онда је $R = \{(0,0),(1,1),(2,0),(2,1)\}$ бинарна релација између A и B. У једноставним случајевима, као што је овај, погодно је релацију R приказати графички као што учињено на наредним сликама.



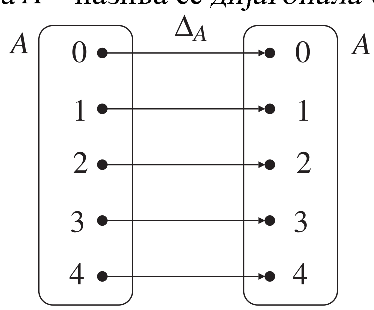
Наводимо још неколико релација из A у B: $P = \{(1,2)\}$, $Q = \{(0,0),(0,1)\}$, $S = \{(0,1),(1,1),(2,1)\}$ итд. Приметимо и да су $\emptyset$ и $A \times B$ такође две бинарне релације између A и B; $\emptyset$ називамо **празном релацијом**, а $A \times B$ **пуном** релацијом.

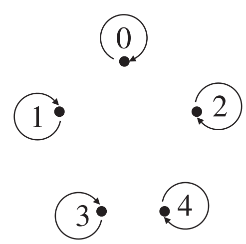
Пример 5. Нека је R нека релација скупа A, $R \subseteq A \times A$. Да бисмо графички приказали R не морамо два пута „цртати“ скуп A. На пример, релацију $R = \{(0,0),(0,2),(2,1),(2,3),(2,4),(3,2)\}$ скупа $A = \{0,1,2,3,4\}$ графички можемо приказати као на наредним сликама, при чему је очигледно како 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 2. **Дијагонала** скупа X је скуп

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

Дефиниција 3. 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 6. Није тешко аксиомама оправдати постојање скупа Δ_X. Из скупа $X \times X$ издвајамо (ослањајући се, наравно, на аксиому издвајања) уређене парове чије су координате исте.

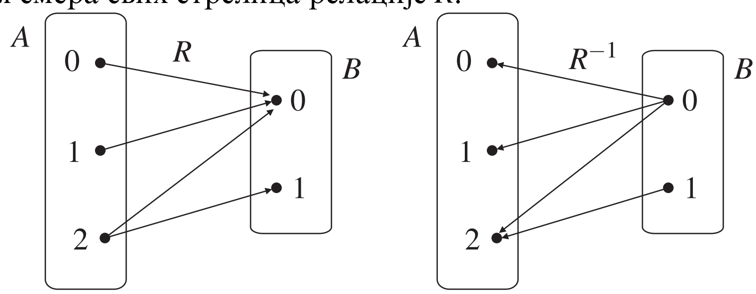
$$\Delta_X = \{z \in X \times X \mid (\exists x \in X)\, z = (x,x)\}$$

Користећи се сличним аргументима, ако је $R \subseteq X \times Y$, онда је

$$R^{-1} = \{z \in Y \times X \mid (\exists x \in X)(\exists y \in Y)(z = (y,x) \wedge (x,y) \in R)\}.$$

ПРИМЕР 6. 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.



ДЕФИНИЦИЈА 4. Нека је $R \subseteq X \times Y$ и $Q \subseteq Y \times Z$. Релација $Q \circ R \subseteq X \times Z$ дата са

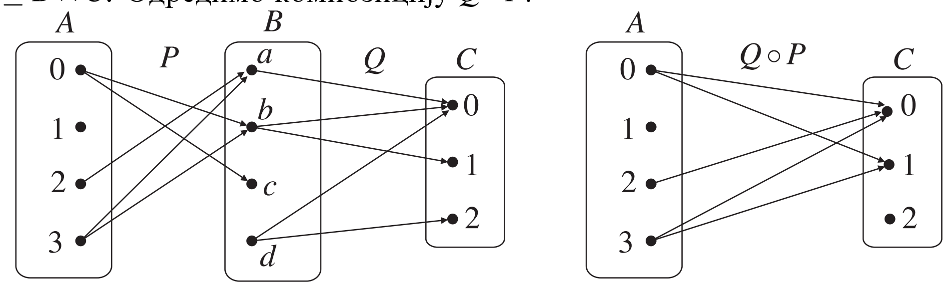
$$Q \circ R = \{(x,z) \in X \times Z \mid \exists y \in Y((x,y) \in R \wedge (y,z) \in Q)\}$$

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

НАПОМЕНА 7. Аксиомом издвајања једноставно се може 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 7. 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 8. 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) $(R^{-1})^{-1} = R$,
(3) $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$,
(4) $P \circ (Q \circ R) = (P \circ Q) \circ R$

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 4 на страни 50.
(2) Из $R \subseteq X \times X$, следи да је $R^{-1} \subseteq Y \times X$, па је $(R^{-1})^{-1} \subseteq X \times Y$. Остаје још да за произвољан уређен пар (x,y) из $X \times Y$ докажемо еквиваленцију $(x,y) \in (R^{-1})^{-1} \Leftrightarrow (x,y) \in R$:

$$(x,y) \in (R^{-1})^{-1} \Leftrightarrow (y,x) \in R^{-1} \Leftrightarrow (x,y) \in R.$$

(3) Нека је $R \subseteq X \times Y$ и $Q \subseteq Y \times Z$. Тада је $Q \circ R \subseteq X \times Z$, па је $(Q \circ R)^{-1} \subseteq Z \times X$. Такође, $R^{-1} \subseteq Y \times X$ и $Q^{-1} \subseteq Z \times Y$, одакле закључујемо $R^{-1} \circ Q^{-1} \subseteq Z \times X$. Остаје још да за сваки уређени пар (z,x) из $Z \times X$ докажемо еквиваленцију $(z,x) \in (Q \circ R)^{-1} \Leftrightarrow (z,x) \in R^{-1} \circ Q^{-1}$:

$$\begin{aligned}
(z,x) \in (Q \circ R)^{-1} \quad & \Leftrightarrow \quad (x,z) \in Q \circ R \\
& \Leftrightarrow \quad (\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q) \\
& \Leftrightarrow \quad (\exists y \in Y)((y,x) \in R^{-1} \wedge (z,y) \in Q^{-1}) \\
& \Leftrightarrow \quad (\exists y \in Y)((z,y) \in Q^{-1} \wedge (y,x) \in R^{-1}) \\
& \Leftrightarrow \quad (z,x) \in R^{-1} \circ Q^{-1}
\end{aligned}$$

(4) 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 $(x,u) \in P \circ (Q \circ R) \Leftrightarrow (x,u) \in (P \circ Q) \circ R$:

$$\begin{aligned}
(x,u) \in P \circ (Q \circ R) \quad & \Leftrightarrow \quad (\exists z \in Z)((x,z) \in Q \circ R \wedge (z,u) \in P) \\
& \Leftrightarrow \quad (\exists z \in Z)(\underline{(x,z) \in Q \circ R} \wedge (z,u) \in P) \\
& \Leftrightarrow \quad (\exists z \in Z)(\underline{(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q)} \wedge (z,u) \in P) \\
& \Leftrightarrow \quad (\exists z \in Z)(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q \wedge (z,u) \in P) \\
& \Leftrightarrow \quad (\exists y \in Y)\underline{(\exists z \in Z)}((x,y) \in R \wedge \underline{(y,z) \in Q} \wedge \underline{(z,u) \in P}) \\
& \Leftrightarrow \quad (\exists y \in Y)((x,y) \in R \wedge \underline{\exists z(z \in Z \wedge (y,z) \in Q \wedge (z,u) \in P)}) \\
& \Leftrightarrow \quad (\exists y \in Y)((x,y) \in R \wedge \underline{(y,u) \in P \circ Q}) \\
& \Leftrightarrow \quad (x,u) \in (P \circ Q) \circ R
\end{aligned}$$

□

НАПОМЕНА 8. 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.

Теорема 9. 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 $Q \circ R \subseteq Q_1 \circ R$.

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 $\mathrm{ran}(R)$.

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

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

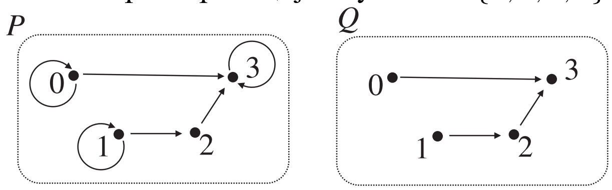
Важне бинарне релације

У овом пододељку издвајамо најважније врсте бинарних релација.

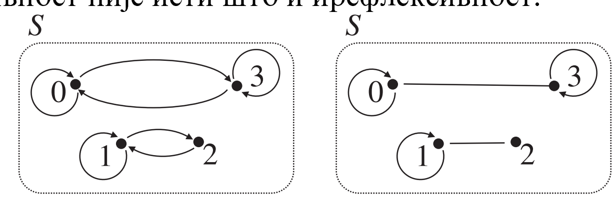
Дефиниција 5. Нека је $R \subseteq X \times X$. Релација R је:

- **рефлексивна** ако је $\Delta_X \subseteq R$, тј. за свако x из X важи $(x,x) \in R$;
- **ирефлексивна** (или **антирефлексивна**) ако је $\Delta_X \cap R = \emptyset$, тј. за свако x из X важи $(x,x) \notin R$;
- **симетрична** ако је $R \subseteq R^{-1}$, тј. за све $x,y \in X$, из $(x,y) \in R$ следи $(y,x) \in R$;
- **антисиметрична** ако је $R \cap R^{-1} \subseteq \Delta_X$, тј. за све $x,y \in X$, из $(x,y) \in R$ и $(y,x) \in R$ следи $x = y$;
- **транзитивна** ако је $R \circ R \subseteq R$, тј. за све $x,y,z \in X$, из $(x,y) \in R$ и $(y,z) \in R$ следи $(x,z) \in R$;
- **линеарна** ако је $R \cup R^{-1} = X \times X$, тј. за све $x,y \in X$, $(x,y) \in R$ или $(y,x) \in R$.

Пример 8. Да бисмо графички илустровали наведене особине, посматраћемо неколико бинарних релација скупа $X = \{0, 1, 2, 3\}$.

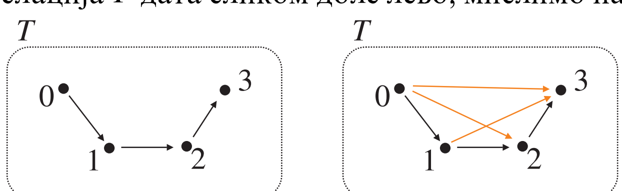


Релација P није рефлексивна, јер постоји $x \in X$ такав да $(x, x) \notin P$: $(2, 2) \notin P$. Али, релација P није ни ирефлексивна. Релација Q није рефлексивна, али је ирефлексивна, јер за свако $x \in X$ важи $(x, x) \notin Q$. Приметимо да нерефлексивност није исти што и ирефлексивност.



Симетричност релације значи да између свака два елемента или не постоји ниједна стрелица или постоје две супротно оријентисане, па једноставно уочавамо да је S симетрична релација. Да бисмо поједноставили цртеже, у случају симетричних релација две стрелице које повезују исти пар елемената, замењујемо једном дужи. Код антисиметричних релација између свака два различита елемента може постојати највише једна стрелица; присуство или одсуство петљи није повезано са особином антисиметричности. Релације P и Q су антисиметричне.

Имајући на уму графичке репрезентације релација, транзитивност значи да за сваке две надовезане стрелице (крај једне стрелице исти је као почетак друге стрелице), постоји стрелица која директно повезује почетак прве и крај друге. Транзитивне релације поједностављено приказујемо тако што изостављамо сваку стрелицу између x и z уколико постоји y и стрелице које повезују x са y и y са z. На пример, када кажемо да је транзитивна релација T дата сликом доле лево, мислимо на приказ десно.



Наравно, ако се не истакне да је T транзитивна релација, онда се на слици лево не подразумевају никакве додатне стрелице.

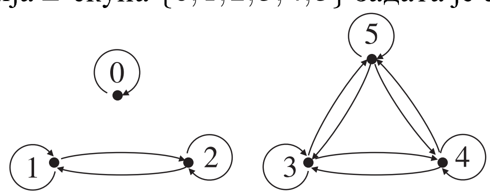
Пример 9. Ако је R бинарна релација скупа X, $R \subseteq X \times X$, и $A \subseteq X$, онда је $R \cap (A \times A)$ очигледно једна бинарна релација скупа A. Ова релација се означава R_A и назива *рестрикција* релације R на A.

Свако од својстава *рефлексивност*, *симетричност*, *антисиметричност*, *транзитивност* и *линеарност* је универзално, у смислу да је описано формулом у којој се појављују искључиво универзални квантификатори и то на почетку формуле. Одавде није тешко закључити да ако R има било које од набројаних својстава, тада то својство има и релација R_A скупа A, за било које $A \subseteq X$. Наравно, нека од рестрикција релације R може имати својства која нема релација R.

Релације еквиваленције

Дефиниција 6. Релација $R \subseteq X \times X$ је **релација еквиваленције** ако је рефлексивна, симетрична и транзитивна.

Пример 10. Релација E скупа $\{0,1,2,3,4,5\}$ задата је следећим графом.



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.

Пример 11. За сваки скуп X, релација $\Delta_X = \{(x,x) \mid x \in X\} \subseteq X \times X$, јесте једна релација еквиваленције, која се назива и једнакост на скупу X (видети пример 5).

Дефиниција 7. 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,

$$X/E = \{[x]_E \mid x \in X\}.$$

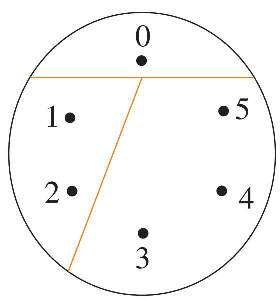
НАПОМЕНА 9. Класе еквиваленције се у литератури и другачије означавају. На пример, уместо $[x]_E$ пише се и x/E, или C_x у случајевима када је јасно о којој релацији еквиваленције је реч.

ПРИМЕР 12. 1) Одредимо класе еквиваленције релације из примера 10.

$$[0]_E = \{0\}, [1]_E = [2]_E = \{1,2\}, [3]_E = [4]_E = [5]_E = \{3,4,5\}.$$

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. Штавише, за сваку класу еквиваленције C, пресек $R \cap (C \times C)$ је једна *пуна релација* скупа C.

2) Класе еквиваленције одређене релацијом Δ_X јесу једночлани скупови: $[x]_{\Delta_X} = \{x\}$, $x \in X$.

ТЕОРЕМА 10. Нека је $E \subseteq S \times S$ релација еквиваленције.

1. За свако $x \in S$, $x \in [x]_E$, па је самим тим $[x]_E \neq \emptyset$.

2. За све $x, y \in S$ важи $(x, y) \in E$ акко $[x]_E = [y]_E$.

3. За све $x, y \in S$ важи $[x]_E \neq [y]_E$ акко $[x]_E \cap [y]_E = \emptyset$.

4. $S = \bigcup S/E = \bigcup_{x \in S} [x]_E$.

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, $[x]_E \neq [y]_E$. $\square$

ДЕФИНИЦИЈА 8. **Партиција** (или **разбијање**) скупа S је скуп $\Pi \subseteq \mathcal{P}(S)$ који задовољава следеће услове:

1. за свако $X \in \Pi$ важи $X \neq \emptyset$;

2. за све $X, Y \in \Pi$, ако је $X \neq Y$, онда је $X \cap Y = \emptyset$;

3. $S = \bigcup \Pi$

Према теореми 10, свака релација еквиваленције E на неком скупу A одређује партицију A/E скупа A.

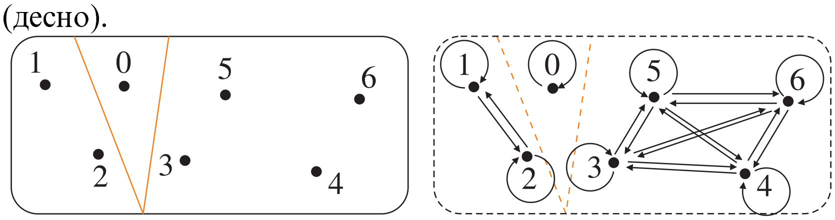
ТЕОРЕМА 11. Нека су E_1 и E_2 две релације еквиваленције скупа S такве да је $S/E_1 = S/E_2$. Тада је $E_1 = E_2$.

ДОКАЗ. Доказаћемо да је $E_1 \subseteq E_2$. Претпоставимо да $(x,y) \in E_1$. Тада $y \in [x]_{E_1} \in S/E_1$. Како је $S/E_1 = S/E_2$, закључујемо да $[x]_{E_1} \in S/E_2$, тј. да је $[x]_{E_1} = [x']_{E_2}$, за неко $x' \in S$. Из $x \in [x]_{E_1} = [x']_{E_2}$, следи да $(x',x) \in E_2$, па је $[x]_{E_2} = [x']_{E_2}$. Дакле, $y \in [x]_{E_1} = [x']_{E_2} = [x]_{E_2}$, одакле добијамо да $(x,y) \in E_2$.

Инклузија $E_1 \supseteq E_2$ се доказује аналогно. □

Свака партиција неког скупа одређује једну релацију еквиваленције такву да је одговарајући количнички скуп задата партиција (што тврди наредна теорема). Штавише, та релација еквиваленције је јединствена према претходној теореми. Релацију еквиваленције реконструишемо из партције тако што на сваком елементу партиције дефинишемо пуну релацију, а затим узмемо унију тих пуних релација: ако је Π партиција скупа S, онда она одређује релацију еквиваленције $E = \bigcup\{P \times P \mid P \in \Pi\}$. Другим речима, два елемента су у релацији E ако и само ако припадају истом члану партиције.

ПРИМЕР 13. Релација еквиваленције која је одређена партицијом $\Pi = \{\{0\},\{1,2\},\{3,4,5,6\}\}$, скупа $\{0,1,2,3,4,5,6\}$, приказана је на наредној слици (десно).



ТЕОРЕМА 12. За сваку партицију Π скупа S, постоји јединствена релација еквиваленције E таква да је $\Pi = S/E$.

Доказ. (*Егзистенција*) Нека је $E \subseteq S \times S$ дефинисано на следећи начин:

$$(x,y) \in E \overset{\text{def}}{\Leftrightarrow} \text{ постоји } X \in \Pi \text{ тако да } x,y \in X.$$

(Рефлексивност) Нека је $x \in S$ произвољан. Тада је $x \in S = \bigcup \Pi$, па постоји $X \in \Pi$ такав да $x \in X$, и самим тим $(x,x) \in E$.

(Симетричност) Нека $x,y \in S$. Ако $(x,y) \in E$, онда постоји $X \in \Pi$ такав да $x,y \in X$, одакле тривијално следи и да $(y,x) \in E$.

(Транзитивност) Нека $x,y,z \in S$. Претпоставимо да $(x,y) \in E$ и $(y,z) \in E$. Тада постоје $X_1, X_2 \in \Pi$ такви да $x,y \in X_1$ и $y,z \in X_2$. Очигледно је $X_1 \cap X_2 \neq \emptyset$, одакле следи да мора бити $X_1 = X_2$. Дакле, оба елемента x и z припадају једном скупу из Π, па према томе $(x,z) \in E$.

По дефиницији релације E следи да су класе еквиваленције ове релације скупови из Π. Заиста, ако је $x \in S$ произвољан, тада постоји $X \in \Pi$ такав да $x \in X$ и сви елементи из S који су у релацији са x морају припадати скупу X, па је $[x]_E = X$. Наравно, и сваки скуп из Π је класа неког елемента, јер је непразан.

(*Јединственост*) следи директно из претходне теореме. Заиста, ако постоји још једна релација еквиваленције E' таква да је $X/E' = \Pi$, онда је $X/E' = X/E$, па према претходној теореми следи да је $E = E'$. □

Према претходној теореми, релације еквиваленције можемо дефинисати само задавањем партиције.

Релације поретка

Дефиниција 9. Релација $R \subseteq X \times X$ је:

- **релација поретка**, односно **уређење** ако је рефлексивна, антисиметрична и транзитивна;
- **релација линеарног поретка**, односно **линеарно уређење** ако је рефлексивна, антисиметрична, транзитивна и за све $x,y \in X$ важи $(x,y) \in R$ или $(y,x) \in R$;
- **релација строгог поретка**, односно **строго уређење** ако је ирефлексивна и транзитивна.

ТЕОРЕМА 13. 1) Ако је $\preccurlyeq$ уређење скупа X, онда је релација $\prec$ дата са:

$$x \prec y \text{ акко } x \preccurlyeq y \wedge x \neq y,$$

строго уређење скупа X.
2) Ако је $\prec$ строго уређење скупа X, онда је релација $\preccurlyeq$ дата са:

$$x \preccurlyeq y \text{ акко } x \prec y \vee x = y,$$

уређење скупа X.

ДОКАЗ. 1) (Ирефлексивност) Релација $\prec$ је ирефлексивна, јер је конјункција $x \preccurlyeq x \wedge x \neq x$ нетачна за свако x.

(Транзитивност) Нека је $x \prec y$ и $y \prec z$. Тада је

$$x \preccurlyeq y, x \neq y, y \preccurlyeq z, y \neq z.$$

Како је $\preccurlyeq$ транзитивна, из $x \preccurlyeq y$ и $y \preccurlyeq z$, следи да је $x \preccurlyeq z$. Остаје још да се докаже да је $x \neq z$. Претпоставимо супротно, да је $x = z$. Тада је $x \preccurlyeq y$ и $y \preccurlyeq x$, па због антисиметричности релације $\preccurlyeq$ важи $x = y$, што није могуће јер је $x \neq y$.

2) (Рефлексивност) Релација $\preccurlyeq$ је рефлексивна, јер за свако x важи $x = x$, а самим тим и $x \prec x \vee x = x$.

(Антисиметричност) Претпоставимо да је $x \preccurlyeq y$ и $y \preccurlyeq x$. Треба да докажемо да је $x = y$. Претпоставимо супротно да је $x \neq y$. Тада мора бити $x \prec y$ и $y \prec x$. Међутим, из транзитивности релације $\prec$ следи да је $x \prec x$, што није могуће, јер је $\prec$ ирефлексивна релација.

(Транзитивност) Претпоставимо да је $x \preccurlyeq y$ и $y \preccurlyeq z$. Треба доказати да је $x \preccurlyeq z$. Разликујемо неколико случајева.

1. случај. Ако је $x = y$ и $y = z$, онда је $x = z$, па важи $x \preccurlyeq z$.

2. случај. Ако је $x \prec y$ и $y = z$, онда је и $x \prec z$, па је $x \preccurlyeq z$.

3. случај. Ако је $x = y$ и $y \prec z$, онда је и $x \prec z$, па је $x \preccurlyeq z$.

4. случај. Ако је $x \prec y$ и $y \prec z$, онда због транзитивности релације $\prec$ важи $x \prec z$, а самим тим и $x \preccurlyeq z$. □

НАПОМЕНА 10. Ако је нека релација поретка приказана графички, брисањем свих петљи добијамо одговарајућу релацију строгог поретка. Важи и обрнуто, додавањем свих петљи на приказ релације строгог поретка, добијамо приказ одговарајуће релације поретка.

Релације строгог поретка углавном се означавају знацима попут $<$, $\prec$, $\lhd$, $\sqsubset$ и слично, а њима одговарајуће релације поретка додавањем цртице испод знака: $\leqslant$ (или $\leq$), $\preceq$ (или $\preccurlyeq$), $\unlhd$, $\sqsubseteq$. У наставку ћемо овај договор о означавању подразумевати.

Пример 14. За било који скуп X, инклузија одређује једну релацију поретка на скупу $\mathcal{P}(X)$:
(R) за све $A \in \mathcal{P}(X)$ важи $A \subseteq A$,
(AS) за све $A, B \in \mathcal{P}(X)$, из $A \subseteq B$ и $B \subseteq A$ следи $A = B$,
(T) за све $A, B, C \in \mathcal{P}(X)$, из $A \subseteq B$ и $B \subseteq C$ следи $A \subseteq C$.

Овој релацији ($\subseteq$) одговара релација одређена строгом инклузијом ($\subset$).

Дефиниција 10. Нека је $\leqslant$ релација поретка на скупу X.

- Елемент $a \in X$ је $\leqslant$-**најмањи** ако за свако $x \in X$ важи $a \leqslant x$.
- Елемент $a \in X$ је $\leqslant$-**највећи** ако за свако $x \in X$ важи $x \leqslant a$.
- Елемент $a \in X$ је $\leqslant$-**минималан** ако не постоји $x \in X$ такав да је $x < a$. (Наравно, $<$ означава строги поредак који одговара поретку $\leqslant$).
- Елемент $a \in X$ је $\leqslant$-**максималан** ако не постоји $x \in X$ такав да је $a < x$.

У случајевима када је јасно за коју релацију поретка $\leqslant$ одређујемо елементе уведене претходном дефиницијом, у називима тих елемената изостављамо префикс „$\leqslant$-“. Истичемо неке значајне чињенице у вези са претходном дефиницијом.

- Ако, у односу на неки поредак, постоји најмањи елемент, онда је он јединствен. Исто важи и за највећи елемент.
- Најмањи елемент, ако постоји, уједно је и (једини) минималан елемент; највећи елемент је једини максималан елемент.
- Могуће је да у односу на неко уређење постоји више минималних, одн. максималних елемената.

Пример 15. Посматрајмо релације одређене инклузијом на неким скуповима.

- $\subseteq$ на скупу $\mathcal{P}(\{0,1,2\})$: најмањи елемент $\emptyset$, па је самим тим и једини минималан елемент; највећи елемент је $\{0,1,2\}$, па је уједно и једини максималан елемент.
- $\subseteq$ на скупу $\mathcal{P}(\{0,1,2\}) \setminus \{\emptyset\}$: најмањи елемент не постоји, а минимални елементи су $\{0\}$, $\{1\}$, $\{2\}$; највећи елемент је $\{0,1,2\}$, па је и једини максималан елемент.
- $\subseteq$ на скупу $\mathcal{P}(\{0,1,2\}) \setminus \{\{0,1,2\}\}$: најмањи елемент $\emptyset$, па је и једини минималан елемент; највећи елемент не постоји, а максимални елементи су $\{0,1\}$, $\{1,2\}$, $\{0,2\}$.
- $\subseteq$ на скупу $\mathcal{P}(\{0,1,2\}) \setminus \{\emptyset, \{0,1,2\}\}$: не постији ни најмањи ни највећи елемент; минимални елементи су $\{0\}$, $\{1\}$, $\{2\}$, а максимални $\{0,1\}$, $\{1,2\}$, $\{0,2\}$.

2.4 Функције

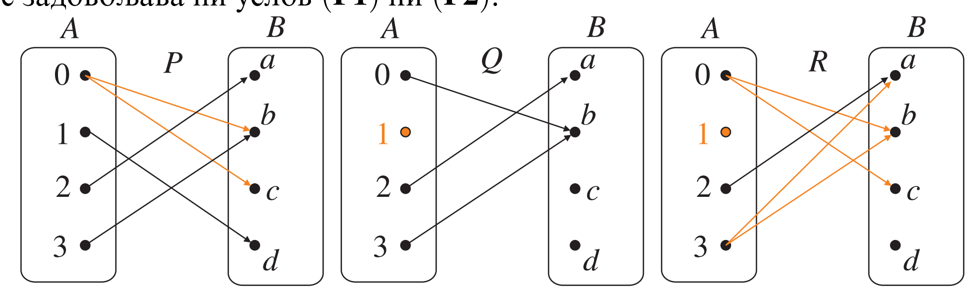
ДЕФИНИЦИЈА 11. Релација F између скупова X и Y, $F \subseteq X \times Y$ је **функција** из X у Y, у означи $F : X \to Y$, ако за свако x из X постоји јединствено y из Y тако да $(x,y) \in F$, што можемо изразити и следећим условима:

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

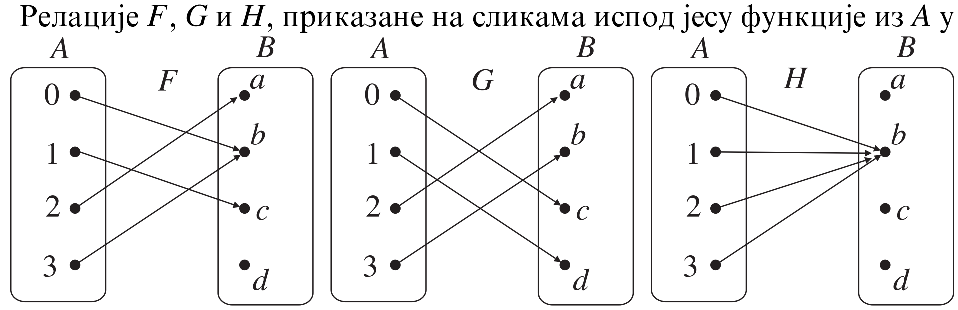
(**F2**) за свако $x \in X$ и све $y_1, y_2 \in Y$, из $(x,y_1) \in F$ и $(x,y_2) \in F$ следи $y_1 = y_2$.

ПРИМЕР 16. 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“:

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

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

У наредној леми наводимо једну корисну реформулацију наведена два услова.

Напомена 11. Теореме које изводимо пре свега као помоћна тврђења која нам олакшавају доказивање значајнијих резултата називаћемо *лемама*.

Лема 2. Нека је $F \subseteq X \times Y$ (и $F^{-1} \subseteq Y \times X$ одговарајућа инверзна релација). $F : X \to Y$ акко $\Delta_X \subseteq F^{-1} \circ F$ и $F \circ F^{-1} \subseteq \Delta_Y$.

Доказ. $(\Rightarrow)$ Претпоставимо да $F : X \to Y$. Треба доказати: (1) $\Delta_X \subseteq F^{-1} \circ F$ и (2) $F \circ F^{-1} \subseteq \Delta_Y$.

(1) Приметимо најпре да је $F^{-1} \circ F \subseteq X \times X$. Да бисмо доказали (1), бирамо произвољно x из X, и настојимо да докажемо $(x,x) \in F^{-1} \circ F$. Пошто је F функција, према услову (**F1**), за свако $x \in X$ постоји $y \in Y$ такав да $(x,y) \in F$. Тада је $(y,x) \in F^{-1}$, одакле следи да $(x,x) \in F^{-1} \circ F$.

(2) Приметимо да је $F \circ F^{-1} \subseteq Y \times Y$. Нека су y_1 и y_2 произвољни елементи из Y такви да $(y_1,y_2) \in F \circ F^{-1}$. Треба доказати да је $y_1 = y_2$.

Из $(y_1,y_2) \in F \circ F^{-1}$ следи да постоји $x \in X$ такав да $(y_1,x) \in F^{-1}$ и $(x,y_2) \in F$. Тада је и $(x,y_1) \in F$. Из услова (**F2**) закључујемо да мора бити $y_1 = y_2$.

$(\Leftarrow)$ Претпоставимо да је $\Delta_X \subseteq F^{-1} \circ F$ и $F \circ F^{-1} \subseteq \Delta_Y$. Треба показати услове (**F1**) и (**F2**).

(**F1**) Нека је x произвољан елемент из X. Како је $\Delta_X \subseteq F^{-1} \circ F$, закључујемо да $(x,x) \in F^{-1} \circ F$, одакле следи да постоји y из Y такав да $(x,y) \in F$ и $(y,x) \in F^{-1}$.

(**F2**) Нека су $x \in X$ и $y_1, y_2 \in Y$ произвољни такви да $(x,y_1) \in F$ и $(x,y_2) \in F$. Из $(x,y_1) \in F$ следи да $(y_1,x) \in F^{-1}$, па $(y_1,y_2) \in F \circ F^{-1}$. Како је $F \circ F^{-1} \subseteq \Delta_Y$, закључујемо да $(y_1,y_2) \in \Delta_Y$, тј. $y_1 = y_2$. □

НАПОМЕНА 12. Из доказа претходне леме видимо да услову **(F1)** одговара инклузија $\Delta_X \subseteq F^{-1} \circ F$, а услову **(F2)** инклузија $F \circ F^{-1} \subseteq \Delta_Y$. Ово можемо веома једноставно и формално извести:

$$\begin{aligned}
\Delta_X \subseteq F^{-1} \circ F &\Leftrightarrow (\forall x \in X)\,(x,x) \in F^{-1} \circ F \\
&\Leftrightarrow (\forall x \in X)(\exists y \in Y)\,((x,y) \in F \wedge \underline{(y,x) \in F^{-1}}) \\
&\Leftrightarrow (\forall x \in X)(\exists y \in Y)\,((x,y) \in F \wedge \underline{(x,y) \in F}) \\
&\Leftrightarrow (\forall x \in X)(\exists y \in Y)\,(x,y) \in F \quad (\mathbf{F1})
\end{aligned}$$

$$\begin{aligned}
F \circ F^{-1} \subseteq \Delta_Y &\Leftrightarrow (\forall y_1 \in Y)(\forall y_2 \in Y)(\underline{(y_1,y_2) \in F \circ F^{-1}} \Rightarrow (y_1,y_2) \in \Delta_Y) \\
&\Leftrightarrow (\forall y_1 \in Y)(\forall y_2 \in Y)(\underline{(\exists x \in X)\left((y_1,x) \in F^{-1} \wedge (x,y_2) \in F\right)} \Rightarrow y_1 = y_2) \\
&\Leftrightarrow (\forall y_1 \in Y)(\forall y_2 \in Y)(\underline{(\exists x \in X)\,((x,y_1) \in F \wedge (x,y_2) \in F)} \Rightarrow y_1 = y_2) \\
&\Leftrightarrow (\forall y_1 \in Y)(\forall y_2 \in Y)(\forall x \in X)((x,y_1) \in F \wedge (x,y_2) \in F \Rightarrow y_1 = y_2) \quad (\mathbf{F2})
\end{aligned}$$

У последњој еквиваленцији другог ланца искористили смо следећу чињеницу (видети задатак **1**.9): ако се x не појављује слободно у формули β, онда је формула $(\exists x\alpha \Rightarrow \beta) \Leftrightarrow \forall x(\alpha \Rightarrow \beta)$ теорема предикатске логике.

Ако $F : X \to Y$, онда 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 ћемо префикс F изостављати када је из контекста јасно о којој функцији F је реч. За x из X, запис $F(x)$ можемо користити и самостално као ознаку одговарајућег елемента из Y – ознаку F-слике елемента x.

Рестрикције

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 $f\,|_A$ и назива **рестрикција** функције f на (подскуп домена) A. Дакле, $f \mid A : A \to Y$. За $x \in A$ важи $f\,|_A\,(x) = f(x)$, док за $x \in X \setminus A$, запис $f\,|_A\,(x)$ нема смисла.

ПРИМЕР 17. Нека $f : \{0,1,2,3\} \to \{a,b,c\}$:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & c & a & b \end{pmatrix}.$$

Тада

$$f\,|_{\{0,1,2\}} = \begin{pmatrix} 0 & 1 & 2 \\ b & c & a \end{pmatrix}, f\,|_{\{1,3\}} = \begin{pmatrix} 1 & 3 \\ c & b \end{pmatrix}, \text{ итд.}$$

Лема 3. Ако $f : X \to Y$ и $\emptyset \neq B \subseteq A \subseteq X$, онда је $(f\,|_A)\,|_B = f\,|_B$.

Доказ. Из $f\,|_A = f \cap (A \times X)$ и $(f\,|_A)\,|_B = f\,|_A \cap (B \times X)$ следи да је

$$(f\,|_A)\,|_B = f\,|_A \cap (B \times X) = f \cap (A \times X) \cap (B \times X).$$

Како је $B \subseteq A$, закључујемо да је $B \times X \subseteq A \times X$, тј. $(A \times X) \cap (B \times X) = B \times X$. Дакле, $(f\,|_A)\,|_B = f \cap (B \times X) = f\,|_B$. □

Композиција функција

Композиција две функције, такође је функција.

Теорема 14. 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 $z_1 = z_2$. □

Напомена 13. Према леми 2, претходну теорему можемо доказати и на следећи начин.

Ако $F : X \to Y$ и $G : Y \to Z$, онда је $\Delta_X \subseteq F^{-1} \circ F$, $F \circ F^{-1} \subseteq \Delta_Y$ и $\Delta_Y \subseteq G^{-1} \circ G$, $G \circ G^{-1} \subseteq \Delta_Z$. Треба да докажемо $\Delta_X \subseteq (G \circ F)^{-1} \circ (G \circ F)$ и $(G \circ F) \circ (G \circ F)^{-1} \subseteq \Delta_Z$. Користећи теореме 8 и 9 имамо:

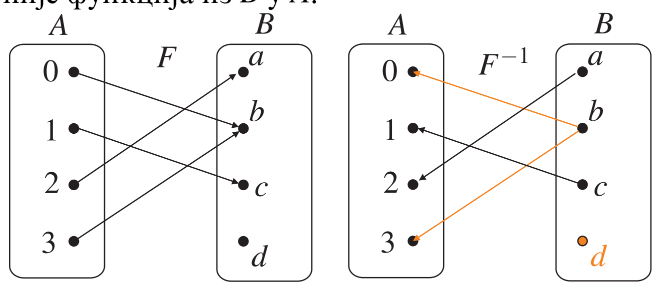
$$\begin{aligned}
(G \circ F)^{-1} \circ (G \circ F) &= (F^{-1} \circ G^{-1}) \circ (G \circ F) = F^{-1} \circ (G^{-1} \circ (G \circ F)) \\
&= F^{-1} \circ ((G^{-1} \circ G) \circ F) \supseteq F^{-1} \circ (\Delta_Y \circ F) = F^{-1} \circ F \\
&\supseteq \Delta_X
\end{aligned}$$

$$
\begin{aligned}
(G\circ F)\circ(G\circ F)^{-1} &= (G\circ F)\circ(F^{-1}\circ G^{-1}) = G\circ(F\circ(F^{-1}\circ G^{-1}))\\
&= G\circ((F\circ F^{-1})\circ G^{-1}) \subseteq G\circ(\Delta_Y\circ G^{-1}) = G\circ G^{-1}\\
&\subseteq \Delta_Z
\end{aligned}
$$

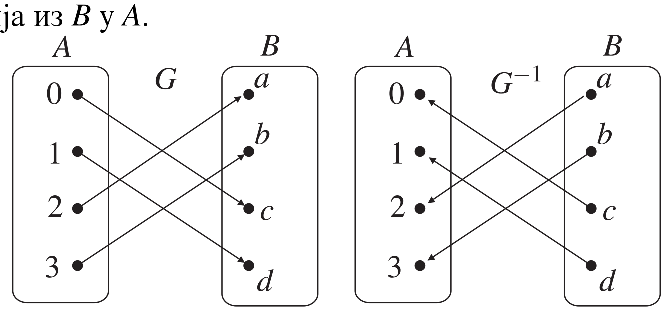
Ако $F : X \to Y$ и $G : Y \to Z$, тада за x из X, елемент $(G\circ F)(x)$, тј. $G\circ F$-слику елемента x означавамо и са $G(F(x))$.

1-1 и на функције

Пример 18. 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 $(\forall y\in Y)(\exists! x\in X)(y,x)\in F^{-1}$, 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 12. Нека $F : X \to Y$.

1. F је **на-функција** или **сурјекција**, у ознаци $F : X \overset{\text{na}}{\to} Y$, ако задовољава услов (**S**).
2. F је **1-1 функција** или **инјекција**, у ознаци $F : X \overset{\text{1-1}}{\to} Y$, ако задовољава услов (**I**).
3. F је **бијекција** или **обострано-једнозначна коресподенција**, у ознаци $F : X \underset{\text{na}}{\overset{\text{1-1}}{\to}} Y$, ако $F : X \overset{\text{1-1}}{\to} Y$ и $F : X \overset{\text{na}}{\to} Y$.

Ако $F : X \overset{\text{na}}{\to} Y$, кажемо да је F функција из скупа X на скуп Y.

ЛЕМА 4. Нека $F : X \to Y$.

1. $F : X \overset{\text{1-1}}{\to} Y$ акко $\Delta_X = F^{-1} \circ F$.
2. $F : X \overset{\text{na}}{\to} Y$ акко $\Delta_Y = F \circ F^{-1}$.

ДОКАЗ. Ако $F : X \to Y$, онда према леми 2 важи $\Delta_X \subseteq F^{-1} \circ F$ и $F \circ F^{-1} \subseteq \Delta_Y$.
(1) $(\Rightarrow)$ Нека $F : X \overset{\text{1-1}}{\to} Y$. Треба доказати да је $\Delta_X \supseteq F^{-1} \circ F$. Приметимо да је $F^{-1} \circ F \subseteq X \times X$. Претпоставимо да $(x_1, x_2) \in F^{-1} \circ F$. Тада постоји y из Y такав да $(x_1, y) \in F$ и $(y, x_2) \in F^{-1}$, тј. $(x_2, y) \in F$. Како је F 1-1 функција, закључујемо да је $x_1 = x_2$, односно $(x_1, x_2) \in \Delta_X$.

$(\Leftarrow)$ Нека је $\Delta_X = F^{-1} \circ F$. Да бисмо доказали да је F 1-1 функција, претпоставимо да $(x_1, y) \in F$ и $(x_2, y) \in F$. Тада имамо $(x_1, y) \in F$ и $(y, x_2) \in F^{-1}$, па $(x_1, x_2) \in F^{-1} \circ F = \Delta_X$, одакле изводимо жељени закључак: $x_1 = x_2$.
(2) $(\Rightarrow)$ Нека $F : X \overset{\text{na}}{\to} Y$. Треба доказати да је $F \circ F^{-1} \supseteq \Delta_Y$, тј. да за било који y из Y важи $(y, y) \in F \circ F^{-1}$. Нека је y из Y произвољан. Како је F на

функција, постоји x из X такав да $(x,y) \in F$, а самим тим је и $(y,x) \in F^{-1}$, одакле следи да $(y,y) \in F \circ F^{-1}$.

($\Leftarrow$) Нека је $F \circ F^{-1} \supseteq \Delta_Y$. Тада за било који y из Y важи $(y,y) \in F \circ F^{-1}$, што значи да постоји x из X да је $(y,x) \in F^{-1}$ и $(x,y) \in F$. Дакле, $F : X \overset{\text{na}}{\to} Y$. $\square$

Ако $f : X \overset{\text{1-1}}{\to} Y$, онда за сваки непразан подскуп A од X важи $f\,|_A : A \overset{\text{1-1}}{\to} Y$. У општем случају, рестрикције на-функција не морају бити на-функције.

Задатак 3. Нека $f : X \to Y$ и $g : Y \to Z$.
(1) Ако $f : X \overset{\text{1-1}}{\to} Y$ и $g : Y \overset{\text{1-1}}{\to} Z$, онда $g \circ f : X \overset{\text{1-1}}{\to} Z$.
(2) Ако $f : X \overset{\text{na}}{\to} Y$ и $g : Y \overset{\text{na}}{\to} Z$, онда $g \circ f : X \overset{\text{na}}{\to} Z$.
(3) Ако $f : X \underset{\text{na}}{\overset{\text{1-1}}{\to}} Y$ и $g : Y \underset{\text{na}}{\overset{\text{1-1}}{\to}} Z$, онда $g \circ f : X \underset{\text{na}}{\overset{\text{1-1}}{\to}} Z$.

Последица 3. *$F : X \underset{\text{na}}{\overset{\text{1-1}}{\to}} Y$ акко $\Delta_X = F^{-1} \circ F$ и $\Delta_Y = F \circ F^{-1}$.*

Ако је $F \subseteq X \times Y$, па је $F^{-1} \subseteq Y \times X$, једнакости $\Delta_X = F^{-1} \circ F$ и $\Delta_Y = F \circ F^{-1}$ заправо кажу да су и F и F^{-1} функције, при чему су обе бијекције.

На основу претходних разматрања изводимо следећу значајну последицу.

Последица 4. *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 14. 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.

Корисно је приметити и следеће. Ако $F : X \to Y$ и за $G \subseteq Y \times X$ важи $G \circ F = \Delta_X$ и $F \circ G = \Delta_Y$, онда су F и G једна другој инверзне релације, и штавише, обе су бијекције. Заиста, уколико је $G \circ F = \Delta_X$ и $F \circ G = \Delta_Y$, онда је:
$$F^{-1} = F^{-1} \circ \Delta_Y = F^{-1} \circ (F \circ G) = (F^{-1} \circ F) \circ G \supseteq \Delta_X \circ G = G$$
и
$$F^{-1} = \Delta_X \circ F^{-1} = (G \circ F) \circ F^{-1} = G \circ (F \circ F^{-1}) \subseteq G \circ \Delta_Y = G,$$
одакле следи $G = F^{-1}$, а самим тим и $G^{-1} = (F^{-1})^{-1} = F$.

Важне функције

Функције заузимају веома значајно место у свим математичким областима што донекле потврђује велики број синонима који се користе: пресликавања, трансформације, оператори итд. У наставку ћемо издвојити неке најважније примере функција.

Идентичко пресликавање

Очигледно је Δ_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 следећу последицу претходних разматрања.

Последица 5. *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.*

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.

Фактор пресликавања

Ако је E релација еквиваленције скупа S, онда се функција $k : S \to S/E, k(x) = [x]_E$ назива *фактор пресликавање.* Фактор пресликавања су на функције.

Бинарне операције

Ако је S неки скуп, свака функција из $S \times S$ у S назива се *бинарна операција* скупа S.

Пример 19. 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	2
1	1	2	0
2	0	2	0

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 13. 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 $x*(y*z) = (x*y)*z$.

Грубо 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 20. 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 21. 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 22. 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 функционалне.

Пример 23. 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 8 (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 24. 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 $\{x \in S \mid f(x) = 1\}$.

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 прилико доказивања скуповних идентитета, што је илустровано у следећем примеру.

Пример 25. 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.

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 $\neg(\forall x \in X)(\exists! y \in \emptyset)\,(x, y) \in \emptyset$. 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

$$(*) \qquad (\forall x \in \emptyset)(\exists! y \in X)\,(x, y) \in \emptyset.$$

Последња формула је скраћење за $\forall x(x \in \emptyset \Rightarrow (\exists! y \in X)\,(x, y) \in \emptyset)$, па како важи $\forall x\,(x \notin \emptyset)$, уочавамо да се $(*)$ може доказати, тј. $\emptyset$ јесте, и то једина, функција из $\emptyset$ у X. Штавише, $\emptyset : \emptyset \xrightarrow{1\text{-}1} X$, што се једноставно може доказати коришћењем истих аргумената 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. $\emptyset : \emptyset \xrightarrow[\text{na}]{\text{1-1}} \emptyset$.

Директне и индиректне слике

Нека $f : X \to Y$. **Директна слика** скупа $A \subseteq X$ јесте подскуп од Y који садржи само оне елементе који су f-слике елемената из A. Тај скуп означавамо $f[A]$ и знамо да постоји према аксиоми издвајања:

$$f[A] = \{y \in Y \mid (\exists a \in A) f(a) = y\} \subseteq Y.$$

Будући да су сви елементи скупа $f[A]$ облика $f(a)$, $a \in A$, пишемо и $f[A] = \{f(a) \mid a \in A\}$. **Индиректна слика** скупа $B \subseteq Y$ јесте подскуп од X који садржи само оне елементе из X чије f-слике припадају скупу B. Овај скуп означавамо $f^{-1}[B]$. Дакле,

$$f^{-1}[B] = \{x \in X \mid f(x) \in B\} \subseteq X.$$

Приметите да употреба ознаке f^{-1} у наведеном контексту нема никакве везе са појмом инверзне функције.

Пример 26. 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 15. Нека $f: X \to Y$. Тада 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) Навешћемо формалан доказ наведене једнакости, јер верујемо да ће он јасније истаћи суштину доказа.

$$
\begin{aligned}
y \in f[A_1 \cup A_2] \quad & \Leftrightarrow \quad \exists x(x \in A_1 \cup A_2 \wedge y = f(x)) \\
& \Leftrightarrow \quad \exists x((x \in A_1 \vee x \in A_2) \wedge y = f(x)) \\
& \Leftrightarrow \quad \exists x((x \in A_1 \wedge y = f(x)) \vee (x \in A_2 \wedge y = f(x))) \\
& \Leftrightarrow \quad \exists x(x \in A_1 \wedge y = f(x)) \vee \exists x(x \in A_2 \wedge y = f(x)) \\
& \Leftrightarrow \quad y \in f[A_1] \vee y \in f[A_2] \\
& \Leftrightarrow \quad y \in f[A_1] \cup f[A_2]
\end{aligned}
$$

(8) Једнакост доказује следећи еквиваленцијски ланац:

$$
\begin{aligned}
x \in f^{-1}[B_1 \cup B_2] \quad &\Leftrightarrow \quad f(x) \in B_1 \cup B_2 \\
&\Leftrightarrow \quad f(x) \in B_1 \vee f(x) \in B_2 \\
&\Leftrightarrow \quad x \in f^{-1}[B_1] \vee x \in f^{-1}[B_2] \\
&\Leftrightarrow \quad x \in f^{-1}[B_1] \cup f^{-1}[B_2].
\end{aligned}
$$

□

Колекције и фамилије

У многим примерима скупова које смо формирали од $0, 1, 2, 3, \ldots$, није нам било важно то што су $0, 1, 2, 3, \ldots$ и сами скупови. Међутим, у неким ситуацијама биће веома битно то што су елементи скупа такође скупови. Када желимо посебно да истакнемо да ћемо користити чињеницу да су елементи неког скупа такође скупови, онда тај скуп називамо и *колекцијом* (скупова). Другим речима, колекција није ништа друго до скуп за који желимо да нагласимо да су и његови елементи скупови. Реч колекција је, дакле, синоним за скуп, а разлози за употребу ове речи су пре свега психолошко-језичке природе: психолошки, јер се тиме наглашава начин на који ћемо посматрати одговарајући скуп, а језички, јер „колекција скупова“ боље звучи од „скуп скупова“. Скупове које ћемо називати колекцијама често ћемо означавати калиграфским словима $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ итд.

У литератури се често функције чије кодомене називамо колекцијама, $A : I \to \mathcal{A}$ (I је неки скуп), називају *фамилије*. Чак се фамилијом назива и директна слика домена такве функције, тј. $A[I]$. За $i \in I$, уместо $A(i)$ пише се A_i, и при тој нотацији је $A[I] = \{A_i \mid i \in I\}$. Једини разлог увођења и употребе свих ових термина јесте да подржи интуицију и поједностави изражавање. Тако, када чујемо (прочитамо)

„. . . фамилија $\{A_i \mid i \in I\}$ . . . “,

треба да имамо на уму читаву причу која се прећутно подразумева – „дата фамилија је заправо директна слика функције A из I у неку колекцију скупова . . . “, као и да је та фамилија такође једна колекција скупова чији су елементи индексирани елементима скупа I.

У складу са претходим разматрањима, природно је за сваку фамилију $\{A_i \mid i \in I\}$ посматрати *унију*, у ознаци $\bigcup\limits_{i \in I} A_i$, и *пресек*, у ознаци $\bigcap\limits_{i \in I} A_i$. Будући да је наведена фамилија настала од функције $A : I \to \mathcal{A}$, за неку колекцију скупова $\mathcal{A}$, онда је $\bigcup\limits_{i\in I} A_i = \bigcup A[I]$ и $\bigcap\limits_{i\in I} A_i = \bigcap A[I]$. Приметимо и следеће:

$$\begin{aligned}
x \in \bigcup_{i\in I} A_i &\Leftrightarrow x \in \bigcup A[I] \\
&\Leftrightarrow \exists X\,(X \in A[I] \wedge x \in X) \\
&\Leftrightarrow \exists X\,((\exists i \in I)\,X = A(i) \wedge x \in X) \\
&\Leftrightarrow (\exists i \in I)\,\exists X\,(X = A_i \wedge x \in X) \\
&\Leftrightarrow (\exists i \in I)\,x \in A_i
\end{aligned}$$

$$\begin{aligned}
x \in \bigcap_{i\in I} A_i &\Leftrightarrow x \in \bigcap A[I] \\
&\Leftrightarrow \forall X\,(X \in A[I] \Rightarrow x \in X) \\
&\Leftrightarrow \forall X\,((\exists i \in I)X = A(i) \Rightarrow x \in X) \\
&\Leftrightarrow \forall X\,(\forall i \in I)\,(X = A_i \Rightarrow x \in X) \\
&\Leftrightarrow (\forall i \in I)\,\forall X\,(X = A_i \Rightarrow x \in X) \\
&\Leftrightarrow (\forall i \in I)\,x \in A_i
\end{aligned}$$

Специјално, ако $A : I \to \mathcal{P}(X)$, тада фамилију $\{A_i \mid i \in I\}$ називамо *фамилијом подскупова* скупа X. Уместо „фамилија $\{A_i \mid i \in I\}$“ писаћемо само „фамилија A_i, $i \in I$“.

Теорема 16. Нека $f : X \to Y$.
(1) За било коју фамилију A_i, $i \in I$ подскупова од X важи:

$$f\left[\bigcup_{i\in I} A_i\right] = \bigcup_{i\in I} f[A_i] \text{ и } f\left[\bigcap_{i\in I} A_i\right] \subseteq \bigcap_{i\in I} f[A_i].$$

(2) За било коју фамилију B_i, $i \in I$ подскупова од Y важи:

$$f^{-1}\left[\bigcup_{i\in I} B_i\right] = \bigcup_{i\in I} f^{-1}[B_i] \text{ и } f^{-1}\left[\bigcap_{i\in I} B_i\right] = \bigcap_{i\in I} f^{-1}[B_i].$$

Напомена 15. Свака функција $f : X \to Y$ одређује функције $F^+ : \mathcal{P}(X) \to \mathcal{P}(Y)$ и $F^- : \mathcal{P}(Y) \to \mathcal{P}(X)$, дате са $F^+(A) \stackrel{\text{def}}{=} f[A]$, $A \in \mathcal{P}(X)$ и $F^-(B) \stackrel{\text{def}}{=} f^{-1}[B]$, $B \in \mathcal{P}(Y)$.

За сваку фамилију $A : I \to \mathcal{P}(X)$ (подскупова од X) потпуно је одређена фамилија $F^+ \circ A : I \to \mathcal{P}(Y)$ (подскупова од Y), при чему је $F^+ \circ A(i) = f[A_i]$, $i \in I$. Такође, свака фамилија $B : I \to \mathcal{P}(Y)$ (подскупова од Y) одређује фамилију $F^- \circ B : I \to \mathcal{P}(X)$ (подскупова од X), при чему је $F^- \circ B(i) = f^{-1}[B_i]$, $i \in I$. Тврђења наведена у претходној теореми можемо формулисати и у следећем облику:

(1) $$F^+\left(\bigcup A[I]\right) = \bigcup F^+ \circ A[I] \text{ и } F^+(\left(\bigcap A[I]\right) \subseteq \bigcap F^+ \circ A[I],$$

односно

(2) $$F^-\left(\bigcup B[I]\right) = \bigcup F^- \circ B[I] \text{ и } F^-\left(\bigcap B[I]\right) = \bigcap F^- \circ B[I].$$

Доказ. (1) Изоставићемо детаљна објашњења, и наводимо само одговарајуће еквиваленцијске ланце из којих се види да суштину доказа чини „игра“ квантификаторима.

$$\begin{aligned}
y \in f\left[\bigcup_{i\in I} A_i\right] &\Leftrightarrow \exists x(x \in \bigcup_{i\in I} A_i \wedge y = f(x))\\
&\Leftrightarrow \exists x((\exists i \in I)\, x \in A_i \wedge y = f(x))\\
&\Leftrightarrow \exists x\,(\exists i \in I)(x \in A_i \wedge y = f(x))\\
&\Leftrightarrow (\exists i \in I)\,\exists x\,(x \in A_i \wedge y = f(x))\\
&\Leftrightarrow (\exists i \in I)\, y \in f[A_i]\\
&\Leftrightarrow y \in \bigcup_{i\in I} f[A_i]
\end{aligned}$$

$$\begin{aligned}
y \in f\left[\bigcap_{i\in I} A_i\right] &\Leftrightarrow \exists x(x \in \bigcap_{i\in I} A_i \wedge y = f(x))\\
&\Leftrightarrow \exists x((\forall i \in I)\, x \in A_i \wedge y = f(x))\\
&\Leftrightarrow \exists x\,(\forall i \in I)(x \in A_i \wedge y = f(x))\\
&\Rightarrow (\forall i \in I)\,\exists x\,(x \in A_i \wedge y = f(x))\\
&\Leftrightarrow (\forall i \in I)\, y \in f[A_i]\\
&\Leftrightarrow y \in \bigcap_{i\in I} f[A_i]
\end{aligned}$$

(2) Докази ових једнакости једноставнији су од доказа тврдњи под (1).

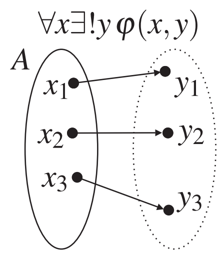
$$\begin{aligned}
x \in f^{-1}\left[\bigcup_{i\in I} B_i\right] &\Leftrightarrow f(x) \in \bigcup_{i\in I} B_i \\
&\Leftrightarrow (\exists i \in I)\, f(x) \in B_i \\
&\Leftrightarrow (\exists i \in I)\, x \in f^{-1}[B_i] \\
&\Leftrightarrow x \in \bigcup_{i\in I} f^{-1}[B_i]
\end{aligned}
\qquad
\begin{aligned}
x \in f^{-1}\left[\bigcap_{i\in I} B_i\right] &\Leftrightarrow f(x) \in \bigcap_{i\in I} B_i \\
&\Leftrightarrow (\forall i \in I)\, f(x) \in B_i \\
&\Leftrightarrow (\forall i \in I)\, x \in f^{-1}[B_i] \\
&\Leftrightarrow x \in \bigcap_{i\in I} f^{-1}[B_i]
\end{aligned}$$

$\square$

2.5 Аксиоме теорије скупова - II

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

Наредном аксиомом – аксиомом регуларности – тврди се 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 17. (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 18. 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, $x = y$. □

Ослањајући се на прву групу аксиома (одељак 2.1) за сваки скуп x постоји јединствени скуп y такав да је $y = x \cup \{x\}$. Скуп $x \cup \{x\}$ називаћемо *следбеником* скупа x и обележавати га x'. Специјално, ако се сетимо скупова[1)] које смо увели на крају одељка 2.1, имамо да је:

$$0' = 1,\ 1' = 2,\ 2' = 3,\ 3' = 4,\ 4' = 5 \ldots$$

Како је $x \neq x \cup \{x\}$ (заправо $x \subset x \cup \{x\}$), за свако x, полазећи од празног скупа $(0 = \emptyset)$, описаним поступком генеришемо нове скупове. 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

Аксиома бесконачности
Постоји скуп који садржи 0 и следбеника сваког свог елемента.

$$\exists I(0 \in I \wedge \forall x(x \in I \Rightarrow x \cup \{x\} \in I))$$

Напомена 16. 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 $[I]' \subseteq I$.

[1)] $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0,1\} = \{\emptyset,\{\emptyset\}\}$, $3 = \bigcup\{2,\{2\}\} = \{0,1,2\}$ итд.

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 $\omega \overset{\text{def}}{=} \bigcap \mathcal{I}(I)$. 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 19. (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 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 и њему ће бити посвећен наредни одељак.

2.6 Скуп природних бројева

Скуп ω уведен у претходном одељку 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).

Принцип математичке индукције

Суштински најважнија својства скупа природних бројева наведена су у теореми 19. Тврђење (2) поменуте теореме назива се **принцип математичке индукције**. Примену овог принципа илуструјемо доказивањем следећих важних тврђења.

ТЕОРЕМА 20. (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 $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n)$, формираћемо скуп

$$S = \{n \in \mathbb{N} \mid (\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n)\}$$

и доказати да је $S = \mathbb{N}$, применом принципа математичке индукције.

(**BI**) Докажимо најпре да $0 \in S$, тј. да важи $(\forall m \in \mathbb{N})(m \in 0 \Rightarrow m \subseteq 0)$. Како је $0 = \emptyset$ и знамо да за свако m важи $m \notin 0$, онда се из претпоставке $m \in 0$ изводи било шта (применом $(\perp_{\mathrm{E}})$), па и $m \subseteq 0$. Дакле, $0 \in S$.

(**IK**) Претпоставимо да $n \in S$, тј. да важи

$$(\mathrm{IP}) \qquad (\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n).$$

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 $(*)$. □

НАПОМЕНА 17. 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.

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 $n' \in S$.

Описани поступак можемо скратити тако што не формирамо скуп S већ доказујемо следеће формуле:

(**BI**) $\varphi[0/n]$

(**IK**) $(\forall n \in \mathbb{N})(\varphi(n) \Rightarrow \varphi[n'/n])$,

и из њих изводимо $(\forall n \in \mathbb{N})\, \varphi(n)$. За описани доказ ове формуле кажемо да је спроведен *индукцијом по* n.

Уколико треба доказати формулу облика

$$(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})\varphi(m,n), \tag{Φ}$$

због еквивалентности ове формуле са $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})\varphi(m,n)$, можемо поступити двојако.

Први начин	*Други начин*
Формирамо скуп $S = \{m \in \mathbb{N} \mid (\forall n \in \mathbb{N})\varphi(m,n)\}$ и настојимо да докажемо $S = \mathbb{N}$.	Формирамо скуп $S = \{n \in \mathbb{N} \mid (\forall m \in \mathbb{N})\varphi(m,n)\}$ и настојимо да докажемо $S = \mathbb{N}$.

Ако поступимо на први начин, кажемо да смо формулу (Φ) доказали *индукцијом по* m, а у другом случају да смо (Φ) доказали *индукцијом по* n. Размотримо мало детаљније један од ова два начина – на пример, први. Да бисмо индукцијом (по m) доказали $S = \mathbb{N}$, треба доказати $(\forall n \in \mathbb{N})\varphi(0,n)$, као и $(\forall n \in \mathbb{N})\varphi(m',n)$ под претпоставком $(\forall n \in \mathbb{N})\varphi(m,n)$. Наравно, може се догодити да је индукција потребна и у доказима ових формула. На који начин ћемо поступити углавном се опредељујемо према формули $\varphi(m,n)$.

У неким случајевима, формулу (Φ) је погодно доказивати и на следеће начине.

Први начин	*Други начин*
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 $(\forall n \in \mathbb{N})\, S_n = \mathbb{N}$, одакле непосредно следи (Φ).	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 $(\forall m \in \mathbb{N})\, S_m = \mathbb{N}$, одакле непосредно следи (Φ).

У првом случају (Φ) доказујемо *индукцијом по m при фиксираном n*, а у другом случају *индукцијом по n при фиксираном m*,

Уређење природних бројева. Принцип потпуне индукције

Претходна теорема показује да припадање $(\in)$, односно строга инклузија $(\subset)$ на уобичајени начин уређује скуп природних бројева:

$$0 \in 1 \in 2 \in 3 \in 4 \in 5 \cdots, \text{ односно } 0 \subset 1 \subset 2 \subset 3 \subset 4 \subset 5 \cdots$$

Заиста, знамо да:

- за сваки природан број n важи $n \notin n$ (ово је последица аксиоме регуларности – теорема 17 (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 $<$. *Поредак* $\leqslant$ скупа $\mathbb{N}$ уводимо као у теореми 13:

$$m \leqslant n \overset{\text{def}}{\Leftrightarrow} m < n \vee m = n.$$

ПОСЛЕДИЦА 6. *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 20 (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. □

У вези са уређењем природних бројева је и следеће веома значајно тврђење.

Теорема 21. [**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 $(\forall k < n)\, k \in S$ схватамо, наравно, као $(\forall k \in n)\, k \in S$.

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 22. 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 $X = \emptyset$. $\square$

НАПОМЕНА 18. 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 14. 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.

Теорема рекурзије

Теорема рекурзије омогућава да дефинишемо функције чији је домен $\mathbb{N}$, на начин који потпуно одговара „природи“ скупа $\mathbb{N}$.

Теорема 23. [**Теорема рекурзије – I**] Нека је X било који скуп, $a \in X$ и $h : X \to X$. Тада постоји јединствена функција $f : \mathbb{N} \to X$ таква да је

$$\text{(Rec)} \begin{cases} f(0) = a, \\ f(n') = h(f(n)), n \in \mathbb{N}. \end{cases}$$

Доказ. Докажимо најпре да постоји функција $f : \mathbb{N} \to X$ која задовољава једнакости (Rec).

Скуп $F \subseteq \mathbb{N} \times X$ назваћемо (a,h)-скупом ако су задовољени следећи услови:

1) $(0,a) \in F$ 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 (a,h)-скуп, па је непразна колекција $\mathcal{F}$ свих (a,h)-скупова. Нека је $f = \bigcap \mathcal{F}$. Тада је $f \subseteq \mathbb{N} \times X$. Докажимо да је f један (a,h)-скуп.

1) За свако $F \in \mathcal{F}$ важи $(0,a) \in F$, одакле следи да $(0,a) \in \bigcap \mathcal{F} = f$.

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 (a,h)-скуп. Дакле, $(n', h(x)) \in \bigcap \mathcal{F} = f$.

Показаћемо да је f функција из $\mathbb{N}$ у X. Математичком индукцијом доказујемо да за свако $k \in \mathbb{N}$ <u>постоји јединствено</u> $y \in X$ тако да $(k,y) \in f$.

BI Како је f један (a,h)-скуп, знамо да $(0,a) \in f$. Претпоставимо да постоји још једно $a_1 \in X$такво да $(0,a_1) \in f$ и $a \neq a_1$. Нека је $f_1 = f \setminus \{(0,a_1)\}$. Докажимо да је f_1 један (a,h)-скуп.

1) $(0,a) \in f_1$, јер је из f избачен само елемент $(0,a_1)$ и $a_1 \neq a$.
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 $(n', h(x)) \neq (0,a_1)$, јер је $0 \neq n'$, за било које n, следи да $(n', h(x)) \in f_1$.

Дакле, $f_1 \in \mathcal{F}$, па је $f = \bigcap \mathcal{F} \subset f_1$, што је контрадикција. Тиме смо доказали да је aједини елемент из X такав да $(0,a) \in f$.

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 (a,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 (a,h)-скуп.

1) $(0,a) \in f'$, јер је из f избачен само елемент (k',y_1) који је сигурно различит од $(0,a)$, будући да је $0 \neq k'$.
2) Претпоставимо да за $n \in \mathbb{N}$ и $x \in X$, $(n,x) \in f_1$. С обзиром на то да $(n,x) \in f$ имамо да $(n',h(x)) \in f$. Докажимо да важи неједнакост $(n',h(x)) \neq (k',y_1)$. Неједнакост је очигледно тачна ако је $n' \neq k'$. Уколико је $n' = k'$, мора бити и $n = k$, па је и $x = y$ (јер је y једини елемент из X такав да $(k,y) = (n,x) \in f$). Према избору елемента y_1 имамо да је $y_1 \neq h(y) = h(x)$, па је $(n',h(x)) \neq (k',y_1)$.

Дакле, $f = \bigcap \mathcal{F} \subset f_1$, што је контрадикција. Закључујемо да је $h(y)$ једини елемент из X такав да $(k',h(y)) \in f$.

Доказали смо да је f функција из $\mathbb{N}$ у X. Ова функција задовољава једнакости (Rec) јер је f (a,h)-скуп:

Из услова 1) произлази $f(0) = a$;

Према услову 2), из $f(n) = x$ следи да је $f(n') = h(x)$, тј. $f(n') = h(f(n))$.

Остаје још да докажемо да је јединствена функција која задовољава једнакости (Rec).

Претпоставимо да функције $f_1, f_2 : \mathbb{N} \to X$ задовољавају једнакост (Rec). Доказаћемо да су оне једнаке, тј. да за сваки $n \in \mathbb{N}$ важи $f_1(n) = f_2(n)$. Доказ изводимо математичком индукцијом.

BI $f_1(0) = a = f_2(0)$.

IK Доказујемо индуктивни корак.

IP Претпоставимо да за неко $n \in \mathbb{N}$ важи $f_1(n) = f_2(n)$.

Тада је $f_1(n') = h(f_1(n)) = h(f_2(n)) = f_2(n')$.

□

Као што смо видели, скуп природних бројева $\mathbb{N}$ је суштински одређен својим (почетним) елементом 0 и функцијом (следбеника) $' : \mathbb{N} \to \mathbb{N}$. 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 $f : \mathbb{N} \to X$.

$$\begin{tikzcd} 0 \in \mathbb{N} \arrow[r, "'"] \arrow[d, "f"] & \mathbb{N} \arrow[d, "f"] \\ a \in X \arrow[r, "h"'] & X \end{tikzcd} \qquad \begin{array}{l} f(0) = a \\ f(n') = h(f(n)), \text{ тј. } f \circ {}' (n) = h \circ f(n) \end{array}$$

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 $n+1$ (ова ознака ће и у овој књизи ускоро бити прихваћена). 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:

$$(\mathrm{Rec}) \begin{cases} f_0 = a, \\ f_{n+1} = h(f_n), \; n \in \mathbb{N}. \end{cases}$$

За низ одређен једнакостима (Rec) кажемо да је **рекурзивно** (рекурентно, индуктивно) дефинисан.

Аналогно се може доказати и следећа општија варијанта теореме рекурзије. Кључне идеје доказа су исте као у доказу претходне теореме само су прилагођене ширем контексту, па је овај доказ технички незнатно сложенији.

Теорема 24. [**Теорема 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 $s \in S$:

$$(\mathrm{Rec}) \begin{cases} f(s,0) = g(s), \\ f(s,n') = h(s, f(s,n)), \; n \in \mathbb{N}. \end{cases}$$

Друга варијанта теореме 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 са a_s, а функција h одређује функцију $h_s : X \to X$, $h_s(x) \overset{\text{def}}{=} h(s,x)$, $x \in X$.

$$\begin{tikzcd} 0 \in \mathbb{N} \arrow[r, "'"] \arrow[d, "f_s"] & \mathbb{N} \arrow[d, "f_s"] \\ a_s \in X \arrow[r, "h_s"'] & X \end{tikzcd}$$

Према првој варијанте теореме рекурзије, за свако $s \in S$, постоји јединствена функција $f_s : \mathbb{N} \to X$ таква да:

$$(\mathrm{Rec}) \begin{cases} f_s(0) = a_s, \\ f_s(n') = h_s(f_s(n)), \; n \in \mathbb{N}. \end{cases}$$

Све функције f_s, $s \in S$, дефинишу („подизањем индекса у аргумент“) функцију $f : S \times \mathbb{N} \to X$, $f(s,n) \stackrel{\text{def}}{=} f_s(n)$, чије постојање и јединственост тврди претходна теорема.

Такође, прва варијанта се може сматрати специјалним случајем друге ако изаберемо да S буде синглтон. Нека је, на пример, $S = \{0\}$. Функцијом $g : \{0\} \to X$ заправо бирамо један елемент из X; нека је $g(0) = a$. Функцију $h : \{0\} \times X \to X$ можемо поистоветити са природно дефинисаном функцијом из X у X: $x \mapsto h(0,x)$, $x \in X$.

Сабирање и множење природних бројева

Основне рачунске операције уводимо применом друге варијанте теореме рекурзије, узимајући да је $S = X = \mathbb{N}$.

Нека је $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ функција дата са $h(x,y) = y'$, $(x,y) \in \mathbb{N} \times \mathbb{N}$. Очигледно је h композиција функције следбеник $'$: $\mathbb{N} \to \mathbb{N}$ и друге пројекције $\pi_2 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\pi_2(x,y) = y$: $h = {}' \circ \pi_2$. Према другој варијанти теореме рекурзије, постоји јединствена функција $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ која задовољава једнакости:

$$\begin{cases} +(m,0) = \mathrm{id}_{\mathbb{N}}(m), \\ +(m,n') = h(m,+(m,n)). \end{cases} \quad \text{односно} \quad \begin{cases} +(m,0) = m, \\ +(m,n') = (+(m,n))'. \end{cases}$$

Уместо $+(m,n)$ пишемо $m+n$, па при тој нотацији, претходне једнакости постају:

$$(\mathrm{Rec}+) \qquad \begin{cases} m+0 = m, \\ m+n' = (m+n)'. \end{cases}$$

Напомена 19. Овако уведено сабирање верно одсликава нашу интуицију према којој одређивање збира $m+n$ посматрамо као одређивање n-тог следбеника броја m, тј. збир $m+n$ рачунамо тако што полазећи од m „избројимо“ n наредних бројева:

$$m+n = m^{\overbrace{\prime\prime\cdots\prime}^{n \text{ пута}}}.$$

На пример, $4+3$ према једнакостима (Rec+) рачунамо:

$$4+3 = 4+2' = (4+2)' = (4+1')' = (4+1)'' = (4+0')'' = (4+0)''' = 4'''.$$

Полазећи од константне функције $\mathbf{0} : \mathbb{N} \to \mathbb{N}$, $\mathbf{0}(n) = 0$, и сабирања $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, множење $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ дефинишемо једнакостима:

$$(\mathrm{Rec}\cdot) \qquad \begin{cases} \cdot(m,0) = \mathbf{0}(m), \\ \cdot(m,n') = +(m, \cdot(m,n)). \end{cases} \quad \text{односно} \begin{cases} m \cdot 0 = 0, \\ m \cdot n' = m + (m \cdot n). \end{cases}$$

Напомена 20. Као и у случају сабирања, једнакости (Rec·) потпуно одговарају нашој интуицији о множењу. На пример,

$$\begin{aligned} 4 \cdot 3 &= 4 \cdot 2' = 4 + (4 \cdot 2) = 4 + (4 \cdot 1') = 4 + (4 + (4 \cdot 1)) \\ &= 4 + (4 + (4 \cdot 0')) = 4 + (4 + (4 + (4 \cdot 0))) = 4 + (4 + (4 + 0)) = 4 + (4 + 4). \end{aligned}$$

Уопште,

$$m \cdot n = \underbrace{m + (m + (m + \cdots (m + m)}_{n \text{ пута}} \cdots)).$$

Наравно, заграде у горњем изразу ћемо изостављати тек пошто се уверимо да је сабирање асоцијативно.

У наставку доказујемо добро познате особине сабирања и множења.

Полазећи од једнакости (Rec+), које ћемо означити (I) и (II), најпре доказујемо једнакости (I^+) и (II^+):

$$\begin{array}{llll} (\mathrm{I}) & m + 0 = m, & (\mathrm{I}^+) & 0 + m = m, \\ (\mathrm{II}) & m + n' = (m+n)'; & (\mathrm{II}^+) & m' + n = (m+n)'. \end{array}$$

а затим и да је сабирање асоцијативно и комутативно.

Теорема 25. За било које природне бројеве k, m, n важи:
(I^+) $0 + m = m$;
(II^+) $m' + n = (m+n)'$;
(A^+) $k + (m+n) = (k+m) + n$ (сабирање је асоцијативно);
(K^+) $m + n = n + m$ (сабирање је комутативно).

Доказ. Доказе изводимо математичком индукцијом, при чему ћемо на почетку сваког доказа навести на који начин га спроводимо.

(I^+) Индукцијом по m.

BI Из (I) директно следи $0 + 0 = 0$.

IK Претпоставимо (IP) $0+m=m$. Тада је $0+m'=(0+m)'\overset{(IP)}{=}m'$, што је и требало доказати.

(II^+) Индукцијом по n при фиксираном m.

BI Из (I) следи $m'+0=m'=(m+0)'$.

IK Претпоставимо (IP) $m'+n=(m+n)'$. Тада је

$$m'+n'\overset{(II)}{=}(m'+n)'\overset{(IP)}{=}(m+n)''\overset{(II)}{=}(m+n')'.$$

(A^+) Индукцијом по n при фиксираним k,m.

BI $k+(m+0)\overset{(I)}{=}k+m\overset{(I)}{=}(k+m)+0$

IK (IP) $k+(m+n)=(k+m)+n$

$$k+(m+n')\overset{(II)}{=}k+(m+n)'\overset{(II)}{=}(k+(m+n))'\overset{(IP)}{=}((k+m)+n)'\overset{(II)}{=}(k+m)+n'$$

(K^+) Индукцијом по n при фиксираном m.

BI $m+0\overset{(I)}{=}m\overset{(I^+)}{=}0+m$

IK (IP) $m+n=n+m$

$$m+n'\overset{(II)}{=}(m+n)'\overset{(IP)}{=}(n+m)'\overset{(II^+)}{=}n'+m$$

$\square$

Због (I) и (I^+) кажемо да је 0 **неутрал** за сабирање.

Асоцијативност сабирања нам омогућава да у изразима $k+(m+n)$ и $(k+m)+n$ изостављамо заграде и пишемо само $k+m+n$. Поред тога, због комутативности у последњем изразу било која два сабирка могу заменити места. Често је веома заморно доследно се позивати на законе комутативности и асоцијативности. На пример, детаљан доказ једнакости $(a+b)+(c+d)=(a+c)+(d+b)$ је:

$$\begin{aligned}(a+b)+(c+d) &\overset{(A^+)}{=} ((a+b)+c)+d \overset{(A^+)}{=} (a+(b+c))+d\\ &\overset{(K^+)}{=} (a+(c+b))+d \overset{(A^+)}{=} ((a+c)+b)+d\\ &\overset{(A^+)}{=} (a+c)+(b+d) \overset{(K^+)}{=} (a+c)+(d+b).\end{aligned}$$

Ми ћемо доказе налик овом избегавати у наставку, и истицати само да је одговарајућа једнакост последица комутативности и асоцијативности.

Сада ћемо доказати и неке особине множења ослањајући се на договор да је множење приоритетније од сабирања, што нам омогућава изостављање појединих заграда. На пример, уместо $a+(b\cdot c)$ пишемо $a+b\cdot c$.

Теорема 26. За све природне бројеве k,m,n важи:
($N^\bullet$) $0\cdot m=0$;
($J^\bullet$) $m\cdot 1=m=1\cdot m$ (неутрал за множење је 1);
(D_l) $k\cdot(m+n)=k\cdot m+k\cdot n$ (леви закон дистрибутивности);
(D_d) $(k+m)\cdot n=k\cdot n+m\cdot n$ (десни закон дистрибутивности);
($A^\bullet$) $k\cdot(m\cdot n)=(k\cdot m)\cdot n$ (множење је асоцијативно);
($K^\bullet$) $m\cdot n=n\cdot m$ (множење је комутативно).

Доказ. Означимо једнакости (Rec$\cdot$):

$$\begin{aligned}&(\mathrm{I}^\bullet)\ m\cdot 0=0,\\&(\mathrm{II}^\bullet)\ m\cdot n'=m+(m\cdot n).\end{aligned}$$

($N^\bullet$) Индукцијом по m.

BI Из ($\mathrm{I}^\bullet$) следи $0\cdot 0=0$.

IK (IP) $0\cdot m=0$

$$0\cdot m'\overset{(\mathrm{II}^\bullet)}{=}0+0\cdot m\overset{(\mathrm{IP})}{=}0+0\overset{(\mathrm{I})}{=}0$$

($J^\bullet$) Једнакост $m\cdot 1=m$ једноставно изводимо из (Rec$\cdot$) и (Rec$+$):

$$m\cdot 1=m\cdot 0'=m+m\cdot 0=m+0=m.$$

Једнакост $1\cdot m=m$ доказујемо индукцијом по m.

BI Из ($\mathrm{I}^\bullet$) следи $1\cdot 0=0$.

IK (IP) $1\cdot m=m$

$$1\cdot m'\overset{(\mathrm{II}^\bullet)}{=}1+1\cdot m\overset{(\mathrm{IP})}{=}1+m\overset{(\mathrm{II}^+)}{=}(0+m)'\overset{(\mathrm{I}^+)}{=}m'$$

(D_l) Индукцијом по n при фиксираним k,m.

BI $k\cdot(m+0)\overset{(\mathrm{I})}{=}k\cdot m\overset{(\mathrm{I})}{=}k\cdot m+0\overset{(\mathrm{I}^\bullet)}{=}k\cdot m+k\cdot 0$

IK (IP) $k\cdot(m+n)=k\cdot m+k\cdot n$

$$\begin{aligned}k\cdot(m+n')&\overset{(\mathrm{II})}{=}k\cdot(m+n)'\overset{(\mathrm{II}^\bullet)}{=}k+k\cdot(m+n)\overset{(\mathrm{IP})}{=}k+(k\cdot m+k\cdot n)\\&\overset{(\mathrm{AK}^+)}{=}k\cdot m+(k+k\cdot n)\overset{(\mathrm{II}^\bullet)}{=}k\cdot m+k\cdot n'\end{aligned}$$

$(\mathrm{D_d})$ Индукцијом по n при фиксираним k,m. У доказу изостављамо објашења појединих једнакости.

BI $(k+m)\cdot 0 = 0 = k\cdot 0 = k\cdot 0 + 0 = k\cdot 0 + m\cdot 0$

IK (IP) $(k+m)\cdot n = k\cdot n + m\cdot n$

$$\begin{aligned}(k+m)\cdot n' &= (k+m)+(k+m)\cdot n \overset{(\mathrm{IP})}{=} (k+m)+(k\cdot n+m\cdot n)\\ &\overset{(\mathrm{AK^+})}{=} (k+k\cdot n)+(m+m\cdot n) = k\cdot n' + m\cdot n'\end{aligned}$$

$(\mathrm{A^\bullet})$ Индукцијом по n при фиксираним k,m.

BI $k\cdot(m\cdot 0) = k\cdot 0 = 0 = (k\cdot m)\cdot 0$

IK (IP) $k\cdot(m\cdot n) = (k\cdot m)\cdot n$

$$\begin{aligned}k\cdot(m\cdot n') &= k\cdot(m+m\cdot n) \overset{(\mathrm{D_l})}{=} k\cdot m + k\cdot(m\cdot n)\\ &\overset{(\mathrm{IP})}{=} k\cdot m + (k\cdot m)\cdot n = (k\cdot m)\cdot n'\end{aligned}$$

$(\mathrm{K^\bullet})$ Индукцијом по n при фиксираном m.

BI $m\cdot 0 = 0 \overset{(\mathrm{N^\bullet})}{=} 0\cdot m$

IK (IP) $m\cdot n = n\cdot n$

$$\begin{aligned}m\cdot n' &= m+m\cdot n \overset{(\mathrm{IP})}{=} m+n\cdot m\\ &\overset{(\mathrm{J^\bullet})}{=} 1\cdot m + n\cdot m \overset{(\mathrm{D_d})}{=} (1+n)\cdot n = n'\cdot m\end{aligned}$$

□

У наставку одаљка доказујемо нека тврђења о вези сабирања и множења са уређењем.

ТЕОРЕМА 27. 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) $m+n=0 \Leftrightarrow m=n=0$.

ДОКАЗ. (1) Индукцијом по n при фиксираним k,m.

BI Очигледно: $k<m \Leftrightarrow k+0<m+0$.

IK (IP) $k<m \Leftrightarrow k+n<m+n$

Како је $k+n' = (k+n)'$, $m+n' = (m+n)'$ и према теореми 6 (4) важи

$$k+n < m+n \Leftrightarrow (k+n)' < (m+n)',$$

на основу индуктивне претпоставке долазимо до жељеног тврђења.
(2) Импликација $k = m \Rightarrow k+n = m+n$ је очигледна. Докажимо обратно.

Претпоставимо да је $k+n = m+n$. Ако би било $k < m$, према (1) би важило $k+n < m+n$, а ако би било $m < k$, опет према (1), важило би $m+n < k+n$. У оба случаја, закључци противрече претпоставци, па мора бити $m = n$.
(3) Импликација $m = 0 \wedge n = 0 \Rightarrow m+n = 0$ је очигледна.

Претпоставимо да је $m+n = 0$. Ако би било $0 < m$, онда бисмо због $0 \leqslant n$, према (1) и (2), имали $0 < m = m+0 \leqslant m+n = 0$, што је немогуће. Дакле, $m = 0$, па самим тим мора бити и $n = 0$. □

ТЕОРЕМА 28. За све $k,m,n \in \mathbb{N}$ важи:
(1) $0 < n \wedge k < m \Rightarrow k \cdot n < m \cdot n$;
(2) $0 < n \wedge k \cdot n = m \cdot n \Rightarrow k = m$;
(3) $0 < n \wedge k \cdot n < m \cdot n \Rightarrow k < m$;
(4) $m \cdot n = 0 \Leftrightarrow m = 0 \vee n = 0$;
(5) $m \cdot n = 1 \Leftrightarrow m = 1 \wedge n = 1$.

ДОКАЗ. (1) Доказ спроводимо индукцијом по n при фиксираним k,m.

BI Очигледно: $0 < 0 \wedge k < m \Rightarrow k \cdot 0 < m \cdot 0$.

IK (IP) $0 < n \wedge k < m \Rightarrow k \cdot n < m \cdot n$

Претпоставимо да је $k < m$. Знамо да је $0 < n'$, тј. $0 \leqslant n$, па је $n = 0$ или $0 < n$. Ако је $n = 0$, тада је:

$$k \cdot 0' = k \cdot 1 = k < m = m \cdot 1 = m \cdot 0'.$$

Уколико је $0 < n$, према (IP) имамо да је $k \cdot n < m \cdot n$. Узимајући у обзир комутативност сабирања, применом тврђења (1) претходне теореме (два пута) закључујемо да је

$$k \cdot n' = k + k \cdot n < m + k \cdot n < m + m \cdot n = m \cdot n'.$$

Дакле, доказали смо $0 < n' \wedge k < m \Rightarrow k \cdot n' < m \cdot n'$.

Преостала тврђења су једноставне последице управо доказаног, па их препуштамо читаоцима. □

Општа теорема рекурзије

Ако за неку формулу $\varphi(x,y)$ знамо да важи $\forall x \exists ! y \varphi(x,y)$, оправдано је уместо $\varphi(x,y)$ писати $\varphi(x) = y$, тј. за произвољан x, јединствени y за који је $\varphi(x,y)$ означити $\varphi(x)$. Овај договор значајно поједностављује рад са оваквим формулама и у доброј мери подржава интуицију у вези са тврдњама наведеног облика. Наравно, не можемо тврдити да је формулом φ одређена нека функција, између осталог и зато што би њен „домен“ требало да садржи све скупове, а знамо да овакав „домен“ није скуп. Ипак ништа нас не спречава да замишљамо да φ одређује једну *уопштену функцију* која сваком скупу додељује један једини скуп. Дакле, уопштене функције нису скупови (па самим тим нису ни обичне функције).

Пример 27. До сада смо доста пута прећуно подразумевали сличне договоре.

Доказали смо да важи

$$\forall x \exists ! y \underbrace{(\forall z(z \in y \Leftrightarrow z \subseteq x))}_{\psi(x,y)},$$

па смо одмах након тог доказа усвојили договор да уместо $\psi(x,y)$ пишемо $y = \mathcal{P}(x)$. Слово $\mathcal{P}$ свакако можемо замишљати као ознаку *уопштене функције* која сваком скупу додељује његов партитивни скуп.

Потпуно исту идеју смо применили и на (доказану) формулу

$$\forall x \exists ! y \underbrace{(\forall z(z \in y \Leftrightarrow \exists t(t \in x \wedge z \in t)))}_{\theta(x,y)},$$

када смо уместо $\theta(x,y)$ писали $y = \bigcup x$. Овога пута, знак $\bigcup$ је ознака *уопштене функције* која сваком скупу додељује његову унију.

Уопштене функције могу имати и више аргумената. Знамо да важи формула

$$\forall x \forall y \exists ! z(\forall t(t \in z \Leftrightarrow t \in x \wedge t \in y)),$$

па се може увести уопштена функција два арумента која сваком пару скупова додељује њихов пресек. Слично томе, унију, разлику и Декартов производ два скупа можемо посматрати као уопштену функцију дужине два.

Уопштене функције се често називају и *скуповне операције*.

Веома важан метод дефинисања низова заснован је на уопштењу теореме рекурзије које ћемо укратко описати. Нека је X било који скуп и Φ *уопштена функција* одређена формулом $\varphi(x,y)$, за коју наравно знамо да важи $\forall x \exists! y \varphi(x,y)$. Полазећи од X, узастопним применама уопштене функције Φ постепено формирамо низ

$$F_0 = X, F_1 = \Phi(X), F_2 = \Phi(F_1) = \Phi(\Phi(X)), F_3 = \Phi(F_2) = \Phi(\Phi(\Phi(X))), \ldots$$

који задовољава једнакости:

$$(*) \qquad \begin{cases} F_0 = X \\ F_{n'} = \Phi(F_n). \end{cases}$$

Штавише, чини се да је наведени низ јединствено одређен једнакостима $(*)$. Но, без обзира на јаку интуицију, треба доказати да постоји скуп $\mathcal{F}$ чији су елементи сви чланови низа, као и да постоји јединствена функција $F : \mathbb{N} \to \mathcal{F}$ која задовољава једнакости $(*)$.

Укратко ћемо изложити само основну идеју траженог доказа. Најпре се доказује да постоје тзв. коначне апроксимације функције F, тј. доказује се да за свако $n \in \mathbb{N} \setminus \{0\}$ постоји скуп $\mathcal{F}_n$ и функција $f_n : n \to \mathcal{F}_n$ таква да важи:

$$\begin{aligned} &f_n(0) = X \\ &f_n(k') = \Phi(f_n(k)), \text{ за свако } k' < n. \end{aligned}$$

Коначне апроксимације можемо описати и на следећи начин:

$$\begin{aligned} &f_0 = \{(0,X)\}, \\ &f_1 = \{(0,X),(1,\Phi(X))\}, \\ &f_2 = \{(0,X),(1,\Phi(X)),(2,\Phi(\Phi(X)))\}, \\ &\vdots \end{aligned}$$

Приметимо да сваку коначну апроксимацију (осим прве) одређује претходна апроксимација и утврђени начин како се та претходна апроксимација проширује. Од коначних апроксимација дефинишемо тражену функцију F узимајући да је $\mathcal{F} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$ и $F : \mathbb{N} \to \mathcal{F}$, $F(n) = f_{n'}(n)$.

ТЕОРЕМА 29. [**Општа теорема рекурзије**] Ако је Φ уопштена функција, за сваки скуп X постоји скуп $\mathcal{F}$ и јединствено одређени низ $F : \mathbb{N} \to \mathcal{F}$

такав да важи:

$$\text{(Rec)} \qquad \begin{cases} F_0 = X \\ F_{n'} = \Phi(F_n). \end{cases}$$

Важно је приметити да овако формулисана теорема није изразива формулом теорије скупова, јер се имплицитно подразумева да почиње речима *за сваку уопштену функцију* Φ ..., тј. *за сваку формулу* φ *такву да важи* $\forall x \exists! y \varphi(x,y)$ ..., а оваква врста квантификовања није дозвољена на језику теорије скупова. Зато, претходну теорему треба схватити као схему која за сваку фиксирану уопштену функцију Φ даје једну теорему теорије скупова.

Приликом примене опште теореме рекурзије, уобичајено је да се за задато X и Φ, каже да је једнакостима (Rec) задат (јединствени) низ скупова F_n, $n \in \mathbb{N}$, и да се без посебног образлагања формира скуп чији су једини елементи чланови овог низа; овај скуп углавном означавамо као фамилију скупова $\{F_n \mid n \in \mathbb{N}\} = \{F_0, F_1, F_2, F_3, \ldots\}$.

Пример 28. За сваки скуп A, једнакостима (1) је одређен јединствени низ:

$$\begin{cases} S_0 = A \\ S_{n'} = \{S_n\}, \end{cases}$$

одакле закључујемо да постоји скуп

$$(1) \qquad \{S_n \mid n \in \mathbb{N}\} = \{A, \{A\}, \{\{A\}\}, \{\{\{A\}\}\}, \ldots\}.$$

За сваки скуп A, једнакостима (2) је одређен јединствени низ:

$$(2) \qquad \begin{cases} V_0 = A \\ V_{n'} = \mathcal{P}(V_n), \end{cases}$$

одакле закључујемо да постоји скуп

$$\{V_n \mid n \in \mathbb{N}\} = \{A, \mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \mathcal{P}(\mathcal{P}(\mathcal{P}(A))), \ldots\}.$$

Самим тим постоји и скуп $P_\omega = \bigcup_{n \in \mathbb{N}} P_n$. Специјално, ако је $A = \emptyset$, онда се скуп P_ω назива *комбинаторни универзум*.

За сваки скуп A, једнакостима (2) је одређен јединствени низ:

$$(2) \qquad \begin{cases} A_0 = A \\ A_{n'} = A_n \times A, \end{cases}$$

одакле закључујемо да постоји скуп

$$\{A_n \mid n \in \mathbb{N}\} = \{A, A \times A, A \times A \times A, A \times A \times A \times A, \ldots\}.$$

Није тешко приметити да је за свако $n \in \mathbb{N}$ скуп A_n заправо Декартов степен A^n (скуп свих уређених n-торки елемената из A). Наравно, постоји и скуп $\bigcup_{n \in \mathbb{N}} A^n$, који се назива *скуп непразних коначних низова елемената из* A.

Коначни низови

У последњем примеру, скуп непразних коначних низова елемената из A уведен је као унија Декартових степена A^n, $n \in \mathbb{N}^+$, при чему је $A^1 = A$. За свако $n \in \mathbb{N}^+$, уређену n-торку из A^n називамо и **коначним низом дужине** n елемената скупа A. Међутим, под коначним низом дужине n елемената из A можемо сматрати и било коју функцију из n у A. Очигледно је да свака уређена n-трока $(a_1, \ldots, a_n) \in A^n$, одређује јединствену функцију из n у A: $a : n \to A$, $a(n) = a_n$. Тачно је и обрнуто: свака функција из n у A одређује јединствену n-торку елемената из A. Претходна запажања можемо проширити и на случај $n = 0$. Знамо да постоји само једна (празна) функција из 0 у A, па по договору можемо узети да је $A^0 = \{\emptyset\}$.

Дакле, за било које $n \in \mathbb{N}$, ознаку A^n користимо и да за скуп свих уређених n-торки (уз договор да је 0-торка заправо $\emptyset$), али и за скуп свих функција из n у A, јер између ова два скупа постоји бијекција која нам омогућава да једноставно прелазимо са једног на друго значење. Поменуту бијекцију заправо можемо посматрати као превод једног контекста на други, и обратно. Скуп $A^{<\omega} = \bigcup_{n \in \mathbb{N}} A^n$ називамо скуп свих коначних низова елемената из A, при чему празан скуп посматран као елемент скупа A^0 називамо и *празан низ*.

2.7 Кардиналност скупа

Коначни скупови

ТЕОРЕМА 30. [**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 $f : m \overset{1\text{-}1}{\to} n'$. 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 $m = k'$; $f : k \cup \{k\} \overset{1\text{-}1}{\to} n \cup \{n\}$. Како је $k' > n'$, према последици 6 (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 $f\,|_k : k \overset{1\text{-}1}{\to} n$, 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:

$$h(x) = \begin{cases} f(x), & x \in k \wedge x \neq \ell \\ f(k), & x = \ell, \\ \quad n, & x = k. \end{cases}$$

Није тешко уочити да $h : k' \overset{1\text{-}1}{\to} n'$ и да је $h(k) = n$. Међутим, тада $h\,|_k : k \overset{1\text{-}1}{\to} n$, што није могуће према (IP). □

ПОСЛЕДИЦА 7. *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 15. Скуп X је **коначан** ако постоји бијекција између X и неког природног броја n, и у том случају пишемо $|X| = n$.

Према последици 7 (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 31. 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 83.

(2) Будући да су X и Y коначни скупови, постоје природни бројеви m и n и бијекције $f : X \overset{1\text{-}1}{\underset{\text{na}}{\to}} m$ и $g : Y \overset{1\text{-}1}{\underset{\text{na}}{\to}} n$.

$(\Rightarrow)$ 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.

$$\begin{tikzcd} X \arrow[rr, "h"', "\sim"] \arrow[dr, "f"', "\wr"] & & Y \arrow[dl, "g", "\wr"'] \\ & m & \end{tikzcd}$$

Функција $h : X \to Y$, дата са $h(x) = g^{-1} \circ f(x)$, јесте бијекција.

$(\Leftarrow)$ Нека је $h : X \overset{1\text{-}1}{\underset{\text{na}}{\to}} Y$ нека бијекција између X и Y. Тада се, аналогно претходном случају, дефинише бијекција између m и n, што према последици 7 (2) значи да је $m = n$, тј. $|X| = |Y|$.

$$\begin{tikzcd} X \arrow[r, "h", "\sim"'] \arrow[d, "f"', "\wr"] & Y \arrow[d, "g", "\wr"'] \\ m \arrow[r, "\sim", "s"'] & n \end{tikzcd}$$

(3) Доказ остављамо за вежбу. $\square$

Теорема 32. 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: $f : n \overset{1\text{-}1}{\to} n$ акко $f : n \overset{\text{na}}{\to} n$.

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 $f : a_1 \overset{1\text{-}1}{\underset{\text{na}}{\to}} m$. 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 $f : a \overset{1\text{-}1}{\underset{\text{na}}{\to}} n'$. 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 $f\,|_{a_1} : a_1 \overset{1\text{-}1}{\underset{\text{na}}{\to}} n$, 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 $f\,|_{a_1} : a_1 \overset{1\text{-}1}{\underset{\text{na}}{\to}} n$, 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 $h : a \overset{1\text{-}1}{\underset{\text{na}}{\to}} n'$ 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 $f : n \overset{1\text{-}1}{\to} n$. Очигледно је $f[n] \subseteq n$. Не може бити $f[n] \subset n$, јер би тада било $f : n \overset{1\text{-}1}{\underset{\text{na}}{\to}} f[n]$, што је немогуће према тврђењу (2). Дакле, $f[n] = n$, тј. f је на функција.

($\Leftarrow$) Претпоставимо $f : n \overset{\text{na}}{\to} n$. 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 $g : n \overset{1\text{-}1}{\underset{\text{na}}{\to}} n$. 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 $k_1 = k_2$. $\square$

Последица 8. *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: $f : X \overset{1\text{-}1}{\to} X$ акко $f : X \overset{\text{na}}{\to} X$.

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 $f : X \overset{1\text{-}1}{\underset{\text{na}}{\to}} n$. 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 $f[A]$). $\square$

Теорема 33. 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 31 (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 $g : X \cup Y_1 \xrightarrow[\text{na}]{\text{1-1}} m + n$. 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, $h : X \times \{y\} \xrightarrow[\text{na}]{\text{1-1}} X$, $h(x,y) = x$, $x \in X$). 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 9. *(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

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 8 (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 8 (3) закључујемо да $\mathbb{N}$ није коначан.

Дефиниција 16. Скуп је **бесконачан** ако није коначан.

Упоређивање бесконачних скупова по „броју“ елемената дефинишемо по узору на тврдње (2) и (3) теореме 31, које се односе на коначне скупове.

Дефиниција 17. (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 34. 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) $\mathrm{id}_A : A \xrightarrow[\text{na}]{\text{1-1}} A$.
(2) Ако $f : A \xrightarrow[\text{na}]{\text{1-1}} B$, онда $f^{-1} : B \xrightarrow[\text{na}]{\text{1-1}} A$.
(3) Ако $f : A \xrightarrow[\text{na}]{\text{1-1}} B$ и $g : B \xrightarrow[\text{na}]{\text{1-1}} C$, онда $g \circ f : A \xrightarrow[\text{na}]{\text{1-1}} C$. $\square$

Теорема 35. 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 $f : A \overset{1\text{-}1}{\to} B$ и $g : B \overset{1\text{-}1}{\to} C$ следи $g \circ f : A \overset{1\text{-}1}{\to} C$. □

Теорема 36. [**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 5. Нека је A било који скуп и $F : \mathcal{P}(A) \to \mathcal{P}(A)$ функција која задовољава следећи услов:

$$(*) \qquad (\forall X, Y \in \mathcal{P}(A))\, X \subseteq Y \Rightarrow F(X) \subseteq F(Y).$$

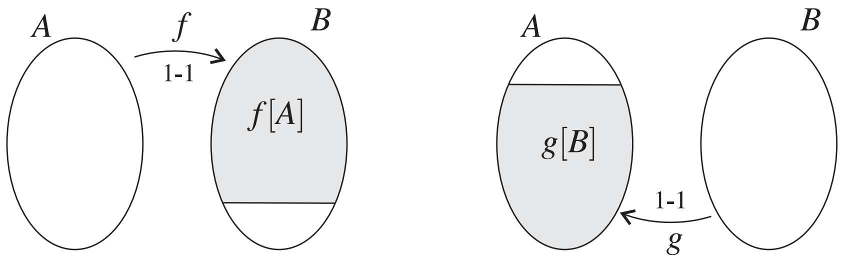
Тада постоји $E \subseteq A$ такав да је $F(E) = E$.

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:

$$E = \bigcup_{X \in \mathcal{E}} X \subseteq \bigcup_{X \in \mathcal{E}} F(X) \overset{(!)}{\subseteq} F\Big(\bigcup_{X \in \mathcal{E}} X\Big) = F(E).$$

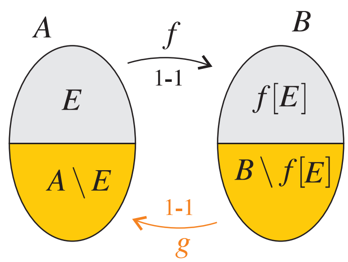
Инклузија означена знаком узвика важи јер за свако $X \in \mathcal{E}$, $X \subseteq \bigcup X$ и $F(X) \subseteq F(\bigcup X)$, према $(*)$. Из услова $(*)$ добијамо и да је $F(E) \subseteq F(F(E))$, одакле следи да $F(E) \in \mathcal{E}$, па је $F(E) \subseteq \bigcup \mathcal{E} = E$. Дакле, $F(E) = E$. □

Доказ. [**Кантор-Бернштајнова теорема**] Нека $f : A \overset{1\text{-}1}{\to} B$ и $g : B \overset{1\text{-}1}{\to} A$. 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. $\square$

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 18. Кадриналност скупа A је мања од кардиналности скупа B, у ознаци $|A| < |B|$, ако је $|A| \leqslant |B|$ и $|A| \neq |B|$.

Теорема 37. 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 $h : A \xrightarrow[\text{na}]{\text{1-1}} \mathcal{P}(A)$. 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 21. 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

Дефиниција 19. Скуп X је **пребројив** ако је $|X| = |\mathbb{N}|$.

Да је X пребројив означава се и $|X| = \aleph_0$.

Теорема 38. 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. Полазећи од $\emptyset \in \mathcal{P}(A)$ и $h : \mathcal{P}(A) \to \mathcal{P}(A)$, $h(X) = X \cup \{\min(A \setminus X)\}$, применом теореме рекурзије дефинишемо $E : \mathbb{N} \to \mathcal{P}(A)$:

$$\begin{cases} E(0) = \emptyset, \\ E(n') = h(E(n)); \end{cases} \text{тј.} \begin{cases} E(0) = \emptyset, \\ E(n') = E(n) \cup \{\min(A \setminus E(n))\}. \end{cases}$$

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 20. 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 39. Скуп A је највише пребројив акко је $|A| \leqslant |\mathbb{N}|$.

Теорема 40. Ако постоји функција из $\mathbb{N}$ на скуп A, $f : \mathbb{N} \xrightarrow{\text{na}} A$, онда је A највише пребројив.

Доказ. Нека $f : \mathbb{N} \xrightarrow{\text{na}} A$. Тада је за свако $a \in A$, скуп $f^{-1}[\{a\}]$ непразан подскуп од $\mathbb{N}$, па 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 41. (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) Нека је $f : \mathbb{N} \to \mathbb{N}$ функција дефинисана са:

$$\begin{cases} f(0) = 0, \\ f(x+1) = f(x) + x. \end{cases}$$

Једноставно се доказује да следећа особина: за све $x, y \in \mathbb{N}^+$, из $x < y$ следи $f(x) < f(y)$. Уместо $f(x)$ пишемо $\binom{x}{2}$.

Доказаћемо да је функција $K : \mathbb{N}^2 \to \mathbb{N}$ дефинисана са

$$K_2(x,y) = \binom{x+y+1}{2} + x$$

бијекција.

Доказажимо најпре да за свака два пара $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$,

$$\text{из } x_1 + y_1 < x_2 + y_2 \text{ следи да је } K(x_1, y_1) < K(x_2, y_2).$$

Заиста, ако је $x_1 + y_1 < x_2 + y_2$, онда је $x_1 + y_1 + 1 \leqslant x_2 + y_2$, па имамо да је

$$\begin{aligned} K(x_2, y_2) &= \binom{x_2+y_2+1}{2} + x_2 \geqslant \binom{x_2+y_2+1}{2} \\ &\geqslant \binom{x_1+y_1+1+1}{2} = \binom{x_1+y_1+1}{2} + x_1 + y_1 + 1 \\ &> \binom{x_1+y_1+1}{2} + x_1 = K(x_1, y_1). \end{aligned}$$

Овадве закључујемо да за свака два пара $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$, из $K(x_1, y_1) = K(x_2, y_2)$ следи да је $x_1 = x_2$ и $y_1 = y_2$, тј. да је $(x_1, y_1) = (x_2, y_2)$. Тиме је доказано да је функција K 1-1 функција.

Докажимо да је K и на функција. Нека је z произвољан природан број. Посматрајмо скуп

$$S = \left\{ n \in \mathbb{N} : z < \binom{n+2}{2} \right\}.$$

Скуп S је непразан (јер је $\binom{\cdot}{2}$ строго растућа функција на $\mathbb{N}^+$) па има најмањи елемент. Нека је $n_0 = \min S$. Тада је n_0 највећи природан број такав да је $\binom{n_0+1}{2} \leqslant z$. Како је $\binom{n_0+2}{2} = \binom{n_0+1}{2} + n_0 + 1$, имамо да је

$$\binom{n_0+1}{2} \leqslant z < \binom{n_0+1}{2} + n_0 + 1,$$

одакле следи да је
$$0 \leqslant z - \binom{n_0+1}{2} \leqslant n_0.$$
Нека је $x_0 = z - \binom{n_0+1}{2}$ и $y_0 = n_0 - x_0$. Како је
$$z = \binom{n_0+1}{2} + x_0 = \binom{x_0+y_0+1}{2} + x_0 = K_2(x_0, y_0),$$
доказ је завршен.

(2) Једноставно се доказује индукцијом.

(3) Под пребројивом фамилијом пребројивих скупова подразумевамо директну слику функције $A : I \to \mathcal{A}$, при чему је I неки пребројив скуп, и за свако $i \in I$, скуп A_i је пребројив скуп. Без губљења општости можемо претпоставити да је $I = \mathbb{N}$.

За свако $n \in \mathbb{N}$, скуп A_n је пребројив, па постоји бијекција $f_n : \mathbb{N} \xrightarrow[\text{na}]{\text{1-1}} A_n$. Нека је $A = \bigcup_{n\in\mathbb{N}} A_n$. 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 40 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) Означимо $\mathcal{P}_{\text{fin}}(\mathbb{N})$ скуп свих коначних подскупова од $\mathbb{N}$.

За $n \in \mathbb{N}$, скуп $\mathbb{N}^n$ посматрамо као скуп свих функција из n у $\mathbb{N}$. Није тешко уочити да је тада за свако $x \in \mathbb{N}^n$, $\operatorname{ran}(x) = x[n]$ један коначан подскуп од $\mathbb{N}$. Дефинишимо функцију $f : \bigcup_{n\in\mathbb{N}} \mathbb{N}^n \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ на следећи начин:
$$f(x) = \operatorname{ran}(x).$$
Функција f је на функција: за свако $X \in \mathcal{P}_{\text{fin}}(\mathbb{N})$ постоје n и $h : n \xrightarrow[\text{na}]{\text{1-1}} X$, па $h \in \mathbb{N}^n$ и $\operatorname{ran}(h) = X$. Према теореми 40 закључујемо да је $\mathcal{P}_{\text{fin}}(\mathbb{N})$ пребројив скуп, јер није коначан. $\square$