ДИСКРЕТНЕ СТРУКТУРЕ 1

Жарко Мијајловић   Зоран Петровић   Маја Рославцев

С а д р ж а ј

1 Увод

Дискретне структуре, као област изучавања дискретне математике, представљају фамилију матаматичких структура са коначним или највише пребројивим доменима.

Математичке области које се у мањој или већој мери изучавају у овом курсу су:
Математичка логика-упознавање елемената исказног и предикатског рачуна;
Комбинаторика-опис комбинаторних функција на коначним скуповима;
Елементи теорије скупова-представљање основних скуповних операција и конструкција над скуповима;
Теорија бројева-испитивање особина целих бројева;
Теорија формалне израчунљивости-утврђује се концепт израчунљивости или алгоритма, као и разни алгоритамски системи (Тјурингова машина, опште рекурзивне функције, УР машина);
Теорија графова-изучавање највише пребројивих скупова на којима је дефинисана бинарна релација.

Значајне су примене дискретне математике у рачунарству. Наведимо пар примера. Програмски језик LISP заснован је на λ-рачуну, који представља алгоритамски систем. У дизајну и анализи логичких кола, која чине основу савремених дигиталних рачунара, користи се исказни рачун и с њим блиско повезане Булове алгебре. Такође, математичка логика нам даје средства помоћу којих утврђујемо коректност неког програма.

Бројевне структуре имају централно место у математици и можемо рећи да на њима почива целокупна математика. То су:

- $\mathbb{N}$ - структура природних бројева;
- $\mathbb{Z}$ - прстен целих бројева;
- $\mathbb{Q}$ - поље рационалних бројева;
- $\mathbb{R}$ - поље реалних бројева;
- $\mathbb{C}$ - поље комплексних бројева.

Пре него што опишимо сваку од ових структура детаљније, наведимо дефиниције алгебарске операције и структуре.

Дефиниција 1.1 *Алгебарска операција дужине n на скупу A, за природан број $n \geq 1$, је свако пресликавање $f : A^n \to A$. Ако је $n = 2$ онда f називамо бинарном операцијом, а ако је $n = 1$ унарном.*

Дефиниција 1.2 *Алгебарска структура је свака n-торка*

$$(A, f_1, f_2, \dots, f_k, a_1, a_2, \dots, a_m)$$

где је A непразан скуп, природни бројеви $m, k \geq 1$, $n = k + m + 1$, $f_1, f_2, \dots, f_k$ операције скупа A и $a_1, a_2, \dots, a_m \in A$. Скуп A се назива доменом, а елементи $a_1, a_2, \dots, a_m$ константама.

Наведене бројевне структуре јесу алгебарске структуре, са операцијама сабирања и множења. Алгебарску структуру можемо проширити додавши јој и неку релацију, најчешће релацију $\leq$.

1.1 Природни бројеви

Скуп природних бројева је $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. Сваки природни број n има свог директног наследника – број $n + 1$, који се понекад означава са n'. У скупу $\mathbb{N}$ постоји најмањи природан број – нула. Исто својство има и сваки непразан подскуп скупа $\mathbb{N}$:

Тврђење 1.3 ***Принцип најмањег елемента за скуп природних бројева*** *Ако је $X \subseteq \mathbb{N}$ и $X \neq \emptyset$, тада X има најмањи елемент.*

Даћемо једно неформално објашњење овог тврђења. Нека је скуп X описан неким аритметичким својством $\varphi(n)$. То значи да се $\varphi(n)$ може записати помоћу симбола аритметичких операција ($+$ и $\cdot$), симбола константи (бројеви $0, 1, 2, \ldots$) и логичких симбола. Како су могуће вредности променљиве n у изразу $\varphi(n)$ природни бројеви, то скуп X можемо представити као

$$X = \{n \in \mathbb{N} \,|\, \varphi(n)\}.$$

Уз набрајање природних бројева $n \in \mathbb{N}$, почев од нуле, за сваки члан n проверавамо истинитост исказа $\varphi(n)$, на основу чега закључујемо да ли тај елемент припада скупу X или не. Уочимо први природан број m за који важи да је $\varphi(m)$ тачан исказ. Такав елемент постоји, јер је X, према претпоставци, непразан скуп. Тада је m најмањи елемент скупа X.

Иако је појам природних бројева интуитивно врло јасан, формално заснивање природних бројева је озбиљан математички проблем. Наведимо један приступ.

Ставимо да је $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$,$4 = \{0, 1, 2, 3\}, \ldots$ Дакле, сваки природан број n је скуп својих претходника, то јест

$$n = \{0, 1, 2, \ldots, n - 1\}.$$

Иначе, реч *број* у српском језику је у етимолошкој вези са глаголом *бријати*, то јест сећи. Према томе, реч *број* би значила засек или зарез. Веза је јасна, ако се сетимо да су људи у давна времена за бројање користили урезивање цртица у неки материјал.

Структура природних бројева је $(\mathbb{N}, +, \cdot, \leq, 0)$, где су операције $+$ и $\cdot$ операције сабирања, односно множења природних бројева, 0 је константа, и $\leq$ је уређење природних бројева. Скуп позитивних природних бројева $\{1, 2, 3, \ldots\}$ обележавамо са $\mathbb{N}^+$.

1.2 Цели бројеви

Скуп целих бројева је $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots\}$. Структура $(\mathbb{Z}, +, -, \cdot, 0, 1)$ представља прстен целих бројева, где су $+$, $\cdot$ и $-$ операције сабирања, множења и промене знака. Наведену структуру можемо посматрати и као структуру $(\mathbb{Z}, +, \cdot, 0, 1)$, јер се операција промене знака може дефинисати помоћу операције $+$. Наиме, елемент $-x$ дефинишемо као елемент који сабран са x даје нулу.

1.3 Рационални бројеви

Скуп рационалних бројева је $\mathbb{Q} = \{\frac{m}{n} \,|\, m \in \mathbb{Z}, n \in \mathbb{N}^+\}$. Алгебарска структура $(\mathbb{Q}, +, \cdot, 0, 1)$ представља поље рационалних бројева. Операције $+$ и $\cdot$ су дефинисане као:

$$\begin{aligned} \frac{m}{n} + \frac{m'}{n'} &= \frac{mn' + m'n}{nn'} \\ \frac{m}{n} \cdot \frac{m'}{n'} &= \frac{mm'}{nn'}. \end{aligned}$$

1.4 Реални бројеви

Скуп реалних бројева $\mathbb{R}$ је скуп бројева са коначним или бесконачним децималним записом. Бројеви са коначним или бесконачно периодичним децималним записом су рационални бројеви, а бројеви са бесконачним децималним записом који није периодичан називају се ирационални бројеви. Скуп ирационалних бројева означавамо са $\mathbb{I}$. Јасно је да важи $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{I} \subset \mathbb{R}$, $\mathbb{R} \setminus \mathbb{Q} = \mathbb{I}$. Неки од ирационалних бројева су $\sqrt{2}$ и π.

Доказ да је $\sqrt{2}$ ирационалан број није компликован. Ако би $\sqrt{2}$ био рационалан број, могли бисмо да га представимо као $\sqrt{2} = \frac{p}{q}$, где су p и q узајамно прости цели бројеви. Квадрирањем ове једнакости добијамо да је $2 = \frac{p^2}{q^2}$, то јест $p^2 = 2q^2$. То значи да је p паран број, па је p облика $2k$, за $k \in \mathbb{Z}$. Тада је $q^2 = 2k^2$, па је и q паран број. Немогуће је да и p и q буду парни бројеви, јер смо претпоставили да су узајамно прости. Дакле, $\sqrt{2}$ мора бити ирационалан број. Насупрот овом доказу, доказ да је број π ирационалан није лак.

Структура $(\mathbb{R}, +, \cdot, \leq, 0, 1)$ представља уређено поље реалних бројева.

1.5 Комплексни бројеви

Скуп комплексних бројева је $\mathbb{C} = \{a + bi \,|\, a, b \in \mathbb{R}\}$, где је i ознака за имагинарну јединицу, то јест елемент који представља једно решење једначине $x^2 + 1 = 0$. Сабирање и множење комплексних бројева дефинише се на следећи начин:

$$\begin{aligned}(a+bi)+(a'+b'i) &= (a+a')+(b+b')i\\ (a+bi)\cdot(a'+b'i) &= (ab-a'b')+(ab'+a'b)i.\end{aligned}$$

Структура $(\mathbb{C}, +, \cdot, 0, 1)$, где су $+$ и $\cdot$ горе дефинисане операције, представља поље комплексних бројева. Приметимо да је сваки реалан број и комплексан, јер је $a = a + 0 \cdot i$.

Приметимо да важи да је $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Такође, операције $+$ и $\cdot$ су екстензије, то јест продужења одговарајућих операција са скупа природних бројева на скупове $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ редом.

1.6 Оператори $\sum$ и $\prod$

У математици се често разматрају збирови и производи бројева задатих на општи начин. На пример: $a_0 + a_1 + a_2 + \cdots + a_n$ и $a_0 \cdot a_1 \cdot a_2 \cdots a_n$, где симбол $\cdots$ означава све чланове који недостају. Оператори $\sum$ и $\prod$ олакшавају запис оваквих израза. Дефинишемо их на следећи начин:

$$\begin{aligned}\sum_{i=m}^{n} a_i &\stackrel{\text{def}}{=} a_m + a_{m+1} + \cdots + a_n\\ \prod_{i=m}^{n} a_i &\stackrel{\text{def}}{=} a_m \cdot a_{m+1} \cdots a_n.\end{aligned}$$

Специјално је $\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + \cdots + a_n$, и слично за производ. На пример $\sum_{i=3}^{7} a_i = a_3 + a_4 + a_5 + a_6 + a_7$. Ако је јасно у ком распону се врши сабирање или множење, можемо писати и $\sum_i a_i$ и $\prod_i a_i$.

Теорема 1.4 *Оператори $\sum$ и $\prod$ имају следеће особине:*

а) $\sum_i \alpha a_i = \alpha \sum_i a_i$;

б) $\sum_i (a_i + b_i) = \sum_i a_i + \sum_i b_i$ $\qquad$ $\prod_i a_i \cdot b_i = \prod_i a_i \cdot \prod_i b_i$

в) $\sum_{i=1}^{n} a_i = \sum_{j=1}^{n} a_j$ $\qquad$ $\prod_{i=1}^{n} a_i = \prod_{j=1}^{n} a_j$

г) $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij}$ $\qquad$ $\prod_{i=1}^{m} \prod_{j=1}^{n} a_{ij} = \prod_{j=1}^{n} \prod_{i=1}^{m} a_{ij}$

Доказ.

а)

$$\sum_{i=1}^{n} \alpha a_i = \alpha a_1 + \alpha a_2 + \cdots + \alpha a_n = \alpha(a_1 + a_2 + \cdots + a_n) = \alpha \sum_{i=1}^{n} a_i$$

б)

$$\begin{aligned}\sum_{i=1}^{n}(a_i + b_i) &= (a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n)\\ &= (a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n)\\ &= \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i\end{aligned}$$

в) Овде се ради само о промени индекса сумирања.

г)

$$\begin{aligned}\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = \sum_{i=1}^{m}(a_{i1} + a_{i2} + \cdots + a_{in}) &=\\ (a_{11} + a_{12} + \cdots + a_{1n}) &+\\ (a_{21} + a_{22} + \cdots + a_{2n}) &+\\ \vdots\\ (a_{m1} + a_{m2} + \cdots + a_{mn}) &= \quad \text{(сабирајући по колонама)}\\ (a_{11} + a_{21} + \cdots + a_{m1}) &+\\ (a_{12} + a_{22} + \cdots + a_{m2}) &+\\ \vdots\\ (a_{1n} + a_{2n} + \cdots + a_{mn}) &=\\ \sum_{j=1}^{n}(a_{1j} + a_{2j} + \cdots + a_{mj}) &= \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\end{aligned}$$

У доказима 1,2,4 смо имплицитно користили асоцијативни, комутативни и дистрибутивни закон за сабирање и множење. Докази за оператор $\prod$ изводе се слично. $\square$

Пример 1.5 *1.* $\sum_{i=1}^{7}(i+k) = \sum_{i=1}^{7} i + \sum_{i=1}^{7} k = \frac{7\cdot 8}{2} + 7k = 28 + 7k$

2. $\sum_{i=m}^{n} 1 = n - m + 1$, *за* $n \geq m$

3.

$$\begin{aligned}\sum_{i=1}^{n}(-1)^i &= (-1)^1 + (-1)^2 + (-1)^3 + \cdots + (-1)^n\\ &= -1 + 1 - 1 + 1 - \cdots + (-1)^n\\ &= \begin{cases} 0, & n \text{ паран}\\ -1, & n \text{ непаран}\end{cases}\end{aligned}$$

4. $\prod_{i=1}^{n}(-1)^i = (-1)^{1+2+\cdots+n} = (-1)^{\frac{n(n+1)}{2}}$

5. Ако је $n \geq 4$, *онда је*

$$\prod_{i=3}^{n} \log(tg(\frac{\pi}{i})) = \log(tg(\frac{\pi}{3})) \cdot \log(tg(\frac{\pi}{4})) \cdot \cdots \cdot \log(tg(\frac{\pi}{n})) = 0.$$

$\triangle$

1.7 Алгебарски идентитети

Алгебарски идентитети су формуле облика $u = v$, где су u и v алгебарски изрази (терми). Алгебарски израз $u = v$ је тачан или истинит у некој алгебарској структури ако се за задате вредности учествујућих променљивих у термима u и v вредности терма u и v поклапају. У горе наведеним бројевним структурама су тачни следећи идентитети:

1. $(x+y)^2 = x^2 + 2xy + y^2$
2. $x^2 - y^2 = (x+y)(x-y)$
3. $x^3 - y^3 = (x-y)(x^2 + xy + y^2)$
4. $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$
5. $x^3 + y^3 + z^3 = (x+y+z)(x^2 + y^2 + z^2 - xy - xz - yz) + 3xyz$
6. $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}), n \in \mathbb{N}, n \geq 2$
7. $x^{2n+1} + y^{2n+1} = (x+y)(x^{2n} - x^{2n-1}y + x^{2n-2}y^2 - \cdots - xy^{2n-1} + y^{2n}), n \in \mathbb{N}, n \geq 1$

Уведимо дефиниције: $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$, за $n \geq 1$, и $0! = 1$. Биномни коефицијенти су бројеви $\frac{n!}{k!(n-k)!}$, за $n, k \in \mathbb{N}$ и $n \geq k$. Означавамо их са $\binom{n}{k}$ или C_k^n. Биномна формула је

8. $(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$

Пример 1.6 *1. Ако у формули 6. ставимо $x = 1$ и $y = t$ добијамо*

$$1 + t + t^2 + \cdots + t^{n-1} = \frac{1 - t^n}{1 - t}.$$

2. Ако у 7. ставимо $x = 1$ и $y = t$ онда је

$$1 - t + t^2 - t^3 + \cdots - t^{2n-1} + t^{2n} = \frac{1 + t^{2n+1}}{1 + t}.$$

3. Из биномне формуле за $x = 1$ и $y = t$ следи

$$(1+t)^n = \sum_{k=0}^{n}\binom{n}{k}t^k.$$

Такође, за $x = 1$ и $y = 1$ добијамо

$$\sum_{k=0}^{n}\binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n,$$

и за $x = 1$ и $y = -1$:

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = \binom{n}{0} + \binom{n}{1} - \binom{n}{2} + \cdots + (-1)^n\binom{n}{n} = 0.$$

4. $\binom{n}{n-k} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$.

△

Дефиниција 1.7 *Нека су $a_1, \ldots, a_n$ позитивни реални бројеви. Тада је број:*

- $A(a_1, \ldots, a_n) = \frac{a_1 + \cdots + a_n}{n}$ *аритметичка средина бројева $a_1, \ldots, a_n$;*
- $G(a_1, \ldots, a_n) = \sqrt[n]{a_1 a_2 \cdots a_n}$ *геометријска средина бројева $a_1, \ldots, a_n$;*

- $H(a_1,\ldots,a_n)=\frac{n}{\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_n}}$ *хармонијска средина бројева* $a_1,\ldots,a_n$*;*

- $K(a_1,\ldots,a_n)=\sqrt{\frac{a_1^2+a_2^2+\cdots+a_n^2}{n}}$ *квадратна средина бројева* $a_1,\ldots,a_n$*.*

Пример 1.8 *Важи* $H(a_1,\ldots,a_n)\leq G(a_1,\ldots,a_n)\leq A(a_1,\ldots,a_n)\leq K(a_1,\ldots,a_n)$ *за све позитивне реалне бројеве* $a_1,\ldots,a_n$*.*

- Докажимо прво $G(a_1,\ldots,a_n)\leq A(a_1,\ldots,a_n)$.

  Нека је $n=2$. Како је $(x-y)^2\geq 0$ важи $x^2+y^2\geq 2xy$, за све $x,y\in\mathbb{R}$. Бројеви a_1,a_2 су позитивни, па у тој неједнакости можемо узети да је $x=\sqrt{a_1}, y=\sqrt{a_2}$. Добијамо $a_1+a_2\geq 2\sqrt{a_1}\sqrt{a_2}$, то јест $G(a_1,a_2)\leq A(a_1,a_2)$.

  Једноставан је доказ и за $n=3$. За све $x,y,z\in\mathbb{R}^+$ важи

  $$x^2+y^2\geq 2xy \qquad x^2+z^2\geq 2xz \qquad y^2+z^2\geq 2yz.$$

  Сабирањем неједнакости добијамо $2x^2+2y^2+2z^2\geq 2xy+2xz+2yz$, па је $x^2+y^2+z^2-xy-xz-yz\geq 0$. С обзиром на идентитет $x^3+y^3+z^3=(x+y+z)(x^2+y^2+z^2-xy-xz-yz)+3xyz$ закључујемо да је $x^3+y^3+z^3\geq 3xyz$. Одатле имамо и $a_1+a_2+a_3\geq 3\sqrt{a_1}\sqrt{a_2}\sqrt{a_3}$, а тиме и $G(a_1,a_2,a_3)\leq A(a_1,a_2,a_3)$.

  Неједнакост $G(a_1,a_2,a_3,a_4)\leq A(a_1,a_2,a_3,a_4)$ можемо добити двоструком применом неједнакости $G(a_1,a_2)\leq A(a_1,a_2)$. Наиме,

  $$\begin{aligned}\frac{a_1+a_2+a_3+a_4}{4}=\frac{\frac{a_1+a_2}{2}+\frac{a_3+a_4}{2}}{2} &\geq \frac{\sqrt{a_1a_2}+\sqrt{a_3+a_4}}{2}\\ &\geq \sqrt{\sqrt{a_1a_2}\sqrt{a_3a_4}}=\sqrt[4]{a_1a_2a_3a_4}.\end{aligned}$$

  Користећи идеју у претходном извођењу докажимо да важи следеће тврђење: ако за било којих n бројева важи неједнакост геометријске и аритметичке средине, тада је $G(a_1,a_2,\ldots,a_{2n})\leq A(a_1,a_2\ldots,a_{2n})$, за било који скуп од $2n$ позитивних реалних бројева. Дакле, ако је $G(a_1,\ldots,a_n)\leq A(a_1,\ldots,a_n)$ за све $a_1,\ldots,a_n\in\mathbb{R}^+$, онда имамо

  $$\begin{aligned}\frac{a_1+a_2+\cdots+a_{2n}}{2n} &= \frac{\frac{a_1+a_2+\cdots+a_n}{n}+\frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2}\geq\frac{\sqrt[n]{a_1\cdots a_n}+\sqrt[n]{a_{n+1}\cdots a_{2n}}}{2}\\ &\geq \sqrt{\sqrt[n]{a_1\cdots a_2}\,\sqrt[n]{a_{n+1}\cdots a_{2n}}}=\sqrt[2n]{a_1a_2\cdots a_{2n}}.\end{aligned}$$

  Можемо закључити да неједнакост аритметичке и геометријске средине важи за $n=2,4,8,16,\ldots$, то јест важи $G(a_1,\ldots,a_n)\leq A(a_1,\ldots,a_n)$ за $n=2^k, k\in\mathbb{N}^+$.

  Докажимо најзад да неједнакост важи за произвољно n. На основу претходног можемо претпоставити да је $n\neq 2^k$. Нека је m најмањи природан број тако да $2^{m-1}<n<2^m$ и нека је $l\in\mathbb{N}^+$ тако да $n+l=2^m$. Према већ доказаном важи

  $$\frac{a_1+a_2+\cdots+a_{2^m}}{2^m}\geq\sqrt[2^m]{a_1a_2\cdots a_{2^m}}.$$

  Ставимо $a_{n+1}=a_{n+2}=\cdots=a_{n+l}=\frac{a_1+a_2+\cdots+a_n}{n}$. Заменом у горњу неједнакост добијамо

  $$\frac{n\frac{a_1+a_2+\cdots+a_n}{n}+l\frac{a_1+a_2+\cdots+a_n}{n}}{n+l}\geq\sqrt[n+l]{a_1a_2\cdots a_n\left(\frac{a_1+a_2+\cdots+a_n}{n}\right)^l}.$$

  Сређивањем ове неједнакости добијамо

  $$\left(\frac{a_1+a_2+\cdots+a_n}{n}\right)^{n+l}\geq a_1a_2\cdots a_n\left(\frac{a_1+a_2+\cdots+a_n}{n}\right)^l,$$

то јест
$$\frac{a_1+a_2+\cdots+a_n}{n} \geq \sqrt[n]{a_1a_2\cdots a_n},$$
чиме је доказана неједнакост $G(a_1,\ldots,a_n) \leq A(a_1,\ldots,a_n)$ за све $a_1,\ldots,a_n \in \mathbb{R}^+$.

- Неједнакост $H(a_1,\ldots,a_n) \leq G(a_1,\ldots,a_n)$ следи из $G(\frac{1}{a_1},\ldots,\frac{1}{a_n}) \leq A(\frac{1}{a_1},\ldots,\frac{1}{a_n})$.
- Докажимо неједнакост $A(a_1,\ldots,a_n) \leq K(a_1,\ldots,a_n)$ за све $a_1,\ldots,a_n \in \mathbb{R}^+$. Важи $a_i^2 + a_j^2 \geq 2a_ia_j$ за све $i,j \in \{1,\ldots,n\}$. Тада

$$\begin{aligned}
\sum_{i=1}^n\sum_{j=1}^n\left(a_i^2+a_j^2\right) &\geq 2\sum_{i=1}^n\sum_{j=1}^n a_1a_j\\
\sum_{i=1}^n\sum_{j=1}^n\left(a_i^2+a_j^2\right) &= \sum_{i=1}^n\left(\sum_{j=1}^n a_i^2+\sum_{j=1}^n a_j^2\right) = \sum_{i=1}^n\left(na_i^2+\sum_{j=1}^n a_j^2\right)\\
&= \sum_{i=1}^n na_i^2+\sum_{i=1}^n\sum_{j=1}^n a_j^2 = n\sum_{i=1}^n a_i^2+n\sum_{j=1}^n a_j^2 = 2n\sum_{i=1}^n a_i^2\\
\left(\sum_{i=1}^n a_i\right)^2 &= \left(\sum_{i=1}^n a_i\right)\left(\sum_{i=1}^n a_i\right) = \left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^n a_j\right) = \sum_{i=1}^n\sum_{j=1}^n a_ia_j,
\end{aligned}$$

заменом две једнакости у првој неједнакости добијамо
$$2n\sum_{i=1}^n a_i^2 \geq 2\left(\sum_{i=1}^n a_i\right)^2,$$
а множењем ове неједнакости са $\frac{1}{n^2}$ добијамо
$$\frac{1}{n}\sum_i a_i^2 \geq \left(\frac{1}{n}a_i\right)^2$$
што је тражена неједнакост.

Ако у некој од неједнакости хармонијске, геометријске, аритметичке и квадратне средине важи једнакост, тада је $a_1 = \cdots = a_n$. На пример, важи $G(a_1,\ldots,a_n) = A(a_1,\ldots,a_n)$ акко $a_1 = \cdots = a_n$. Јасно је да из $a_1 = \cdots = a_n$ следи $G(a_1,\ldots,a_n) = A(a_1,\ldots,a_n)$. Обрнуто, докажимо да $G(a_1,\ldots,a_n) = A(a_1,\ldots,a_n)$ повлачи $a_1 = \cdots = a_n$. Претпоставимо супротно: није $a_1 = \cdots = a_n$. Без умањења општости можемо претпоставити да је $a_1 \neq a_2$. Тада је $\frac{a_1+a_2}{2} > \sqrt{a_1a_2}$, па је
$$\frac{a_1+a_2+\cdots+a_n}{n} = \frac{\frac{a_1+a_2}{2}+\frac{a_1+a_2}{2}+a_3+\cdots+a_n}{n} \geq \sqrt[n]{\frac{a_1+a_2}{2}a_3a_4\cdots a_n} > \sqrt{(a_1a_2)a_3\cdots a_n},$$
што је немогуће. Дакле, мора бити $a_1 = \cdots = a_n$. $\triangle$

Сви алгебарски идентитети 1-8, које смо навели на почетку, су последица неколико основних алгебарских идентитета које називамо алгебарским законима.

Нека је $(G,*,e)$ алгебарска структура, где је $*$ симбол бинарне операције, а e константа. Тада је:

1. $(x*y)*z = x*(y*z)$ асоцијативни закон
2. $x*e = x, e*x = x$ закони неутралног елемента
3. $x*x' = e, x'*x = e$ закони инверзног елемента

4. $x * y = y * x$ комутативни закон.

Ако је дата још једна бинарна операција $\circ$ на G, можемо говорити о дистрибутивним законима:

5. $x \circ (y * z) = (x \circ y) * (x \circ z)$ леви дистрибутивни закон ($\circ$ према $*$)

6. $(y * z) \circ x = (y \circ x) * (z \circ x)$ десни дистрибутивни закон ($\circ$ према $*$).

Алгебарски закони који ће такође бити споменути у наставку су:

- $x * x = x$ закон идемпотенције
- $x * x = e$ закон инволуције
- $x \circ (x * y) = x$ закон апсорпције
- $(x \circ y) * (y \circ z) * (z \circ x) = (x * y) \circ (y * z) \circ (z * x)$ Дедекиндов[1] закон

Дефиниција 1.9 *Алгебарска структура $(G, *, e)$ у којој за све $x, y, z \in G$ важи 1. и 2. и за свако $x \in A$ постоји x' тако да важи 3. назива се група. Ако важи још и 4. структуру G називамо Абелова или комутативна група.*

Дефиниција 1.10 *Прстен је алгебарска структура $(R, *, \circ, e, \iota)$ тако да је $(R, *, e)$ Абелова група, за структуру $(R, \circ, \iota)$ важе асоцијативни закон и закони неутралног елемента, као и дистрибутивни закони операције $\circ$ према $*$. Ако је операција $\circ$ комутативна, за R кажемо да је комутативни прстен. Ако важе закони инверзног елемента за операцију $\circ$ за све елементе из R сем e, онда кажемо да је R поље.*

Приметимо да је структура $\{\mathbb{Z}, +, \cdot, 0, 1\}$ комутативни прстен, а $(\mathbb{Q}, +, \cdot, 0, 1)$, $(\mathbb{R}, +, \cdot, 0, 1)$, $(\mathbb{C}, +, \cdot, 0, 1)$ су поља.

Задаци

2 Скупови

Појам скупа је интуитивно врло јасан, мада се прецизно описује тек аксиомама теорије скупова, које ће бити изложене у наставку. Раселов[2] парадокс нас брзо може убедити зашто није тако једноставно описати нешто што је скуп. Наиме, нека је S сачињен од елемената x за које важи $x \notin x$. Да ли је $S \in S$? Ако јесте, онда према томе како смо дефинисали S важи $S \notin S$, што је немогуће. С друге стране, ако није $S \in S$, онда S испуњава својство елемента од S, што је такође немогуће. Дакле, S није скуп.

Основна релација међу скуповима је већ поменута релација припадности. Скуп x припада скупу y записујемо као $x \in y$ и кажемо да је x елемент скупа y.

Наведимо сада аксиоме теорије скупова:

A1 (Аксиома екстензионалности) Два скупа су једнака ако имају исте елементе.

A2 (Аксиома празног скупа) Постоји скуп који нема ниједан елемент. Означаваћемо га са $\emptyset$.

A3 (Аксиома пара) За све скупове x и y постоји скуп $z = \{x, y\}$, чији су једини елементи скупови x и y.

[1] Richard Dedekind (1831-1916), немачки математичар
[2] Bertrand Russell (1872-1970), британски филозоф и математичар

A4 (Аксиома уније) За сваки скуп x постоји скуп z тако да $u \in z$ ако и само ако $u \in y$ за неки $y \in x$. Скуп z представља унију чланова скупа x и означаваћемо га са $\cup x$.

A5 (Аксиома партитивног скупа) За сваки скуп x постоји скуп $z = \mathcal{P}(x)$, који се састоји од свих подскупова од x.

A6 (Аксиома издвајања подскупа) За сваку формулу $\phi(x)$ и сваки скуп a $\{x \in a \mid \phi(x)\}$ је скуп.

A7 (Аксиома замене) Нека је $\psi(x, y)$ формула за коју важи да за свако x постоји највише једно y тако да је $\psi(x, y)$ испуњено. Тада је за сваки скуп a и $\{y \mid \psi(x, y)$ за неко $x \in a\}$ такође скуп.

A8 (Аксиома доброг заснивања или аксиома регуларности) Сваки непразан скуп A садржи елемент a такав да је $A \cap a = \emptyset$.

A9 (Аксиома бесконачности) Постоји скуп A који садржи $\emptyset$ и са сваким својим елементом x садржи и $x \cup \{x\}$.

A10 (Аксиома избора) Ако је дат скуп x чији су сви елементи непразни скупови, онда постоји функција $f : x \to \cup x$ таква да $f(z) \in z$, за све $z \in x$. Та функција назива се функција избора.

Теорија са аксиомама A1-A9 назива Зермело[3]-Френкелова[4] теорија скупова и скраћено означава са ZF. Зермело-Френкелова теорија са аксиомом избора скраћено се означава са ZFC.

Прву аксиому ћемо експлицитно најчешће користити у доказивању скуповних идентитета. Такође су нам битне аксиоме празног скупа и партитивног скупа, јер обезбеђују егзистенцију ових важних објеката. Шеста аксиома ће нам омогућити дефиниције нових скупова у односу на неке већ дате. На пример пресек два скупа, разлику два скупа и тако даље. Често ћемо у доказима теорема формирати нове скупове од датих на овај начин, користећи неке формуле које се односе на елементе датог скупа, и управо нам ова аксима обезбеђује коректност таквог поступка. На аксиому регуларности ћемо се вратити у шестој глави, која се односи на увођење природних бројева.

Скупове можемо задавати навођењем његових елемената или преко својства која њихови елементи испуњавају. Још једном, ако је задат скуп A, и φ је својство његових елемената задато математичким формулама, тада је $B = \{x \in A \mid \varphi(x)\}$ такође скуп, на основу шесте аксиоме.

Пример 2.1 *1.* $A = \{2, 3\}$

2. $B = \{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\}$

Приметимо да је $A = B$. △

Дефиниција 2.2 *Кажемо да је скуп A подскуп скупа B ако је сваки елемент скупа A уједно и елемент скупа B. Пишемо $A \subseteq B$. Ако је $A \subseteq B$ и $A \neq B$, онда пишемо $A \subset B$.*

Пример 2.3 *1. Празан скуп је подскуп сваког скупа.*

2. $\{x \in \mathbb{R} \mid x \geq 3\} \subset \{x \in \mathbb{R} \mid x \geq 1\}$.

3. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. △

[3]Ernst Zermelo (1871-1953), немачки математичар

[4]Abraham Fraenkel (1891-1965), израелски математичар

Користећи појам подскупа можемо увести једну карактеризацију једнакости скупова, коју ћемо често користити у задацима.

Теорема 2.4 *За произвољне скупове A и B важи: $A = B$ ако и само ако $A \subseteq B$ и $B \subseteq A$.*

Доказ. Јасно је да A и B имају исте елементе ако и само ако су сви елементи скупа A у B и сви елементи скупа B у A. $\square$

Дефиниција 2.5 *Пресек скупова A и B је скуп*

$$A \cap B = \{x \in A \mid x \in B\},$$

или, еквивалентно:

$$A \cap B = \{x \in B \mid x \in A\}.$$

Ако скупови A и B немају заједничких елемената, тада њихову унију означавамо са $A \sqcup B$ и називамо дисјунктном унијом тих скупова.

Дефиниција 2.6 *Унија скупова A и B је скуп*

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

Дефиниција 2.7 *Разлика скупова A и B је скуп*

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Дефиниција 2.8 *Симетрична разлика скупова A и B је скуп*

$$A \bigtriangleup B = (A \setminus B) \cup (B \setminus A).$$

Дефиниција 2.9 *Нека је $A \subseteq U$. Комплемент скупа A у скупу U је скуп*

$$A^c = \{x \in U \mid x \notin A\}.$$

Правилније је писати A^c_U, јер тако знамо у односу на који скуп посматрамо комплемент. У примерима и задацима који следе, подразумевамо да су сви скупови који се спомињу подскупови неког фиксног скупа, тако да ће бити довољно јасно писати само A^c.

Пример 2.10 *Нека је скуп $U = \{1,2,3,4,5,6,7,8,9,10\}$ и нека су $A = \{1,2,3,4\}$ и $B = \{2,3,7,8,9\}$ његови подскупови. Тада је*

$$\begin{array}{lcl@{\qquad}lcl} A \cap B & = & \{2,3\} & A \setminus B & = & \{1,4\} \\ A \cup B & = & \{1,2,3,4,7,8,9\} & B \setminus A & = & \{7,8,9\} \\ A^c & = & \{5,6,7,8,9,10\} & A \bigtriangleup B & = & \{1,4,7,8,9\} \end{array}$$

$\triangle$

Пример 2.11 *За операције $\cap, \cup, \bigtriangleup, \setminus$ и операцију комплемента скупа ^{c} важе следеће особине:*

1. $(A \cap B) \cap C = A \cap (B \cap C)$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $(A \bigtriangleup B) \bigtriangleup C = A \bigtriangleup (B \bigtriangleup C)$
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

6. $A \cap B = B \cap A$

7. $A \cup B = B \cup A$

8. $A \triangle B = B \triangle A$

9. $A \cap A = A$

10. $A \cup A = A$

11. $A \cap (A \cup B) = A$

12. $A \cup (A \cap B) = A$

13. $(A \cap B)^c = A^c \cup B^c$

14. $(A \cup B)^c = A^c \cap B^c$

15. $(A^c)^c = A$

16. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

17. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

18. $(A \cap B) \cup (B \cap C) \cup (C \cap A) = (A \cup B) \cap (B \cup C) \cap (C \cup A)$

Сетимо се да су скупови X и Y једнаки ако имају исте елементе. То можемо записати и овако: $X = Y$ ако важи: $x \in X$ ако и само ако $x \in Y$ за произвољно x. Некад је згодније доказивати скуповне идентитете користећи теорему 2.4. Наиме, $X = Y$ уколико је тачно: за свако x исказ $x \in X$ повлачи $x \in Y$ и за свако x исказ $x \in Y$ повлачи $x \in X$.

Докажимо једнакост 1. Важи следећи низ еквиваленција

$$\begin{array}{lll} x \in (A \cap B) \cap C & \text{акко} & x \in (A \cap B) \text{ и } x \in C \\ & \text{акко} & (x \in A \text{ и } x \in B) \text{ и } x \in C \\ & \text{акко} & x \in A \text{ и } (x \in B \text{ и } x \in C) \\ & \text{акко} & x \in A \text{ и } x \in B \cap C \\ & \text{акко} & x \in A \cap (B \cap C). \end{array}$$

Дакле, скупови $(A \cap B) \cap C$ и $A \cap (B \cap C)$ имају исте елементе, па су једнаки. Једнакост 4:

$$\begin{array}{lll} x \in A \cap (B \cup C) & \text{акко} & x \in A \text{ и } x \in B \cup C \\ & \text{акко} & x \in A \text{ и } (x \in B \text{ или } x \in C) \\ & \text{акко} & (x \in A \text{ и } x \in B) \text{ или } (x \in A \text{ и } x \in C) \\ & \text{акко} & x \in A \cap B \text{ или } x \in A \cap C \\ & \text{акко} & x \in (A \cap B) \cup (A \cap C). \end{array}$$

Једнакост 11:

$$\begin{array}{lll} \text{Из } x \in A \cap (A \cup B) & \text{следи} & x \in A \text{ и } x \in A \cup B \\ & \text{следи} & x \in A. \end{array}$$

С друге стране

$$\begin{array}{lll} x \in A & \text{следи} & x \in A \text{ и } x \in A \\ & \text{следи} & x \in A \text{ и } (x \in A \text{ или } x \in B) \\ & \text{следи} & x \in A \text{ и } (x \in A \cup B) \\ & \text{следи} & x \in A \cap (A \cup B). \end{array}$$

Знајући да важе следећа два идентитета

$$A \cap C \subseteq A \qquad A \subseteq A \cup C$$

за произвољне скупове A и C, доказ претходне једнакости може изгледати и овако:

$$A \cap (A \cup B) \subseteq A \qquad \left.\begin{array}{l} A \subseteq A \cup B \\ A \subseteq A \end{array}\right\} A \subseteq A \cap (A \cup B).$$

Једнакост 13:

$$\begin{array}{rll} x \in (A \cap B)^c & \text{акко} & x \notin A \cap B \\ & \text{акко} & \text{није } x \in A \cap B \\ & \text{акко} & \text{није } (x \in A \text{ и } x \in B) \\ & \text{акко} & (\text{није } x \in A) \text{ или } (\text{није } x \in B) \\ & \text{акко} & x \notin A \text{ или } x \notin B \\ & \text{акко} & x \in A^c \text{ или } x \in B^c \\ & \text{акко} & x \in A^c \cup B^c. \end{array}$$

Једнакост 15:

$$\begin{array}{rll} x \in (A^c)^c & \text{акко} & x \notin A^c \\ & \text{акко} & \text{није } x \in A^c \\ & \text{акко} & \text{није } x \notin A \\ & \text{акко} & \text{није } (\text{није } x \in A) \\ & \text{акко} & x \in A. \end{array}$$

Једнакост 16:

$$\begin{array}{rll} x \in A \setminus (B \cap C) & \text{акко} & x \in A \text{ и } x \notin B \cap C \\ & \text{акко} & x \in A \text{ и није } (x \in B \text{ и } x \in C) \\ & \text{акко} & x \in A \text{ и } (\text{није } x \in B \text{ или није } x \in C) \\ & \text{акко} & x \in A \text{ и } (x \notin B \text{ или } x \notin C) \\ & \text{акко} & (x \in A \text{ и } x \notin B) \text{ или } (x \in A \text{ и } x \notin C) \\ & \text{акко} & x \in A \setminus B \text{ или } x \in A \setminus C \\ & \text{акко} & x \in (A \setminus B) \cup (A \setminus C). \end{array}$$

На сличан начин могу се извести сви остали докази.

Једнакости 1-3 представљају асоцијативност операција пресека, уније и симетричне разлике. Једнакости 4 и 5: дистрибутивност пресека у односу на унију и обрнуто. Комутативност за $\cap, \cup, \triangle$ су идентитети 6-8; 9 и 10 је идемпотентност за пресек и унију. Закони апсорпције за пресек и унију су једнакости 11 и 12. Једнакости 13 и 14 се називају Де Моргановиi[5] закони. Једнакост 18 је Дедекиндов закон за пресек и унију. $\triangle$

Пример 2.12 *Одредити тражене партитивне скупове и доказати наведени идентитет:*

1. $\mathcal{P}(\{a, b\})$
2. $\mathcal{P}(\emptyset)$
3. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

[5] Augustus De Morgan (1806-1871), британски математичар

1. $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
2. $\mathcal{P}(\emptyset) = \{\emptyset\}$
3. Докажимо дату једнакост:

$$\begin{aligned} X \in \mathcal{P}(A \cap B) \quad & \text{акко} \quad X \subseteq A \cap B \\ & \text{акко} \quad X \subseteq A \text{ и } X \subseteq B \\ & \text{акко} \quad X \in \mathcal{P}(A) \text{ и } X \in \mathcal{P}(B) \\ & \text{акко} \quad X \in \mathcal{P}(A) \cap \mathcal{P}(B). \end{aligned}$$

$\triangle$

Тврђење 2.13 *За скупове a, b, c, d важи:*

$$\{a,b\} = \{c,d\} \text{ ако и само ако } (a = c \text{ и } b = d) \text{ или } (a = d \text{ и } b = c\}.$$

Доказ. Ако важи неки од два услова са десне стране, јасно је да је $\{a,b\} = \{c,d\}$. С друге стране, претпоставимо да је $\{a,b\} = \{c,d\}$. Како је $a \in \{a,b\}$, то је $a \in \{c,d\}$, па је $a = c$ или $a = d$. Нека је прво $a = c$. Важи $d \in \{c,d\}$, па $d \in \{a,b\}$, а тиме и $d = a$ или $d = b$. Ако је $b = d$ важи десна страна. Ако је $a = d$, имамо да је $a = c = d$. Из $b \in \{a,b\} = \{c,d\}$ следи $b = c = d$, па важи десна страна. Слично се доказује и други случај, када је $a = d$. $\square$

Дефиниција 2.14 *Уређени пар (a,b) скупова a и b је скуп $\{\{a\}, \{a,b\}\}$.*

Тврђење 2.15 *За уређене парове (a,b) и (c,d) важи:*

$$(a,b) = (c,d) \text{ акко } a = c \text{ и } b = d.$$

Доказ. Ако важи $a = c$ и $b = d$, онда је $(a,b) = \{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\} = (c,d)$. Нека је $(a,b) = (c,d)$. Онда је $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$. Према тврђењу 2.13, важи да је $(\{a\} = \{c\}$ и $\{a,b\} = \{c,d\})$ или $(\{a\} = \{c,d\}$ и $\{a,b\} = \{c\}.)$ Ако важи први део, мора бити $a = c$. Такође, важи $(a = c$ и $b = d)$ или $(a = d$ и $b = c)$. У првој случају имамо $a = c$ и$b = d$. У другом случају $d = a = c = b$, па је специјално и $a = c$ и $b = d$. Ако важи други део, онда је $a = b = c = d$, па опет важе тражене једнакости. $\square$

Дефиниција 2.16 *Декартов[6] производ скупова A и B је*

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

Пример 2.17 *Декартов производ скупова $A = \{1,2,3\}$ и $B = \{x,y\}$ је $A \times B = \{(1,x),(1,y),(2,x),(2,y),(3,x),(3,y)\}$.*

Како је $B \times A = \{(x,1),(x,2),(x,3),(y,1),(y,2),(y,3)\}$, видимо да не мора важити једнакост између скупова $A \times B$ и $B \times A$. $\square$

Пример 2.18 *Важи следећи идентитет $(A \cup B) \times C = (A \times C) \cup (B \times C)$.*

[6] René Descartes (1596-1650), француски филозоф и математичар

Приметимо да је елемент у $(A \cup B) \times C$ облика (a, c), где је $a \in A \cup B$, $c \in C$.

$$\begin{array}{lll}
\text{Из } (a,c) \in (A \cup B) \times C & \text{следи} & a \in A \cup B \text{ и } c \in C \\
& \text{следи} & (a \in A \text{ или } a \in B) \text{ и } c \in C \\
& \text{следи} & (a \in A \text{ и } c \in C) \text{ или } (a \in B \text{ и } c \in C) \\
& \text{следи} & (a,c) \in A \times C \text{ или } (a,c) \in B \times C \\
& \text{следи} & (a,c) \in (A \times C) \cup (B \times C).
\end{array}$$

С друге стране је

$$\begin{array}{lll}
x \in (A \times C) \cup (B \times C) & \text{следи} & x \in A \times C \text{ или } x \in B \times C \\
& \text{следи} & (x = (a,c) \text{ за } a \in A \text{ и } c \in C) \text{ или } (x = (b,d) \text{ за } b \in B \text{ и } d \in C) \\
& \text{следи} & x = (y,z) \text{ где је } y \in A \text{ или } B, \text{ а } z \in C \\
& \text{следи} & x = (y,z) \text{ где је } y \in A \cup B \text{ и } z \in C \\
& \text{следи} & x \in (A \cup B) \times C.
\end{array}$$

$\triangle$

Задаци

1. Доказати скуповни идентитет $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.
2. Доказати да је симетрична разлика скупова A и B једнака $(A \cup B) \setminus (A \cap B)$.
3. Доказати скуповни идентитет $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
4. Доказати скуповни идентитет $(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cup D)$.
5. Доказати да су следећа тврђења еквивалентна:
   (а) $A \subseteq B$
   (б) $A \cap B = A$
   (ц) $A \cup B = B$.
6. Показати да важи $A \cap (B \cup C) = (A \cap B) \cup C$ ако и само ако $C \subseteq A$.
7. Доказати да важи $C \subseteq A \cup B$ ако и само ако $B^c \cap C \subseteq A$.
8. Одредити $\mathcal{P}(\mathcal{P}(\emptyset))$.
9. Доказати да је $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Под којим условима важи једнакост?
10. Одредити формуле за $A \setminus B$ и $A \cup B$ преко операција пресека и комплемента.
11. Доказати да ако је $A \cap B = A \cap C$, онда не мора бити $B = C$.
12. Доказати скуповни идентитет $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.
13. Доказати скуповни идентитет $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

3 Релације

Добро познате су нам релације $\leq$, $=$, $\subseteq$. Можемо рећи да се појам релације бави остваривањем веза између неких елемената скупова које посматрамо. Прецизна дефиниција гласи овако.

Дефиниција 3.1 *Нека су A и B скупови. Релација ρ са скупа A у скуп B је сваки подскуп од $A \times B$. Дакле, $\rho \subseteq A \times B$. Ако је $A = B$ онда кажемо да је ρ бинарна релација на скупу A.*

Да је $(a, b) \in \rho$ пишемо и $a\rho b$.

Дефиниција 3.2 *Домен релације $\rho \subseteq A \times B$ је скуп*

$$\mathrm{Dom}(\rho) = \{a \in A \mid \textit{постоји } b \in B \textit{ тако да је } (a, b) \in \rho\}.$$

Слика релације ρ је

$$\mathrm{Im}(\rho) = \{b \in B \mid \textit{постоји } a \in A \textit{ тако да је } (a, b) \in \rho\}.$$

Дефиниција 3.3 *Инверзна релација релације $\rho \subseteq A \times B$ је*

$$\rho^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \rho\} \subseteq B \times A.$$

Приметимо да је домен релације ρ^{-1} слика релације ρ, као и да је слика од ρ^{-1} домен од ρ.

Дефиниција 3.4 *Композиција релација $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$ је релација*

$$\sigma \circ \rho = \{(a, c) \in A \times C \mid \textit{постоји } b \in B \textit{ тако да } (a, b) \in \rho \textit{ и } (b, c) \in \sigma\} \subseteq A \times C.$$

Пример 3.5 *Нека су скупови $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$ и $C = \{\alpha, \beta, \gamma\}$. Нека је дата релација ρ са скупа A на B са $\rho = \{(1, y), (2, z), (2, x), (3, y)\}$ и релација σ са B на C са $\sigma = \{(x, \beta), (y, \beta)\}$. Одредити домен, слику и инверзну релацију релације ρ, као и композицију $\sigma \circ \rho$.*

$$\begin{array}{rclrcl} \mathrm{Dom}(\rho) & = & \{1, 2, 3\} & \rho^{-1} & = & \{(y, 1), (z, 2), (x, 2), (y, 3)\} \\ \mathrm{Im}(\rho) & = & \{x, y, z\} & \sigma \circ \rho & = & \{(1, \beta), (2, \beta), (3, \beta)\} \end{array}$$

$\triangle$

Теорема 3.6 *Ако су дате релације $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$ и $\tau \subseteq C \times D$, тада важи $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$.*

Доказ. Приметимо да је $\tau \circ \sigma \subseteq B \times D$, $\sigma \circ \rho \subseteq A \times C$ и $(\tau \circ \sigma) \circ \rho, \tau \circ (\sigma \circ \rho) \subseteq A \times D$. Важи следећи низ импликација:

$$\begin{array}{rcl} (a, d) \in (\tau \circ \sigma) \circ \rho & \text{акко} & \text{постоји } b \in B \text{ тако да } (a, b) \in \rho \text{ и } (b, d) \in \tau \circ \sigma \\ & \text{повлачи} & \text{постоји } b \in B \text{ тако да } (a, b) \in \rho \\ & & \text{и постоји } c \in C \text{ тако да } (b, c) \in \sigma \text{ и } (c, d) \in \tau \\ & \text{повлачи} & (a, c) \in \sigma \circ \rho \text{ и } (c, d) \in \tau \\ & \text{повлачи} & (a, d) \in \tau \circ (\sigma \circ \rho). \end{array}$$

С друге стране

$$\begin{array}{rcl} (a, d) \in \tau \circ (\sigma \circ \rho) & \text{акко} & \text{постоји } c \in C \text{ тако да } (a, c) \in \sigma \circ \rho \text{ и } (c, d) \in \tau \\ & \text{повлачи} & \text{постоји } c \in C \text{ и постоји } b \in B \text{ тако да } (a, b) \in \rho \\ & & \text{и } (b, c) \in \sigma \text{ и } (c, d) \in \tau \\ & \text{повлачи} & (a, b) \in \rho \text{ и } (b, d) \in \tau \circ \sigma \\ & \text{повлачи} & (a, d) \in (\tau \circ \sigma) \circ \rho \end{array}$$

□

Теорема 3.7 *Нека су дате релације $\rho, \sigma \subseteq A \times B$ тада важи*

1. *Ако је $\rho \subseteq \sigma$, онда је $\rho^{-1} \subseteq \sigma^{-1}$.*
2. $(\rho^{-1})^{-1} = \rho$.

Доказ.

1. Нека је $(a,b) \in \rho^{-1}$. Тада је $(b,a) \in \rho$. Према претпоставци је $\rho \subseteq \sigma$, па и $(b,a) \in \sigma$, то јест $(a,b) \in \sigma^{-1}$.
2. Важи да је $(a,b) \in \rho$ ако и само ако $(b,a) \in \rho^{-1}$ ако и само ако $(a,b) \in (\rho^{-1})^{-1}$.

□

Теорема 3.8 *Ако су дате релације $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$, тада важи $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.*

Доказ. Приметимо прво да је $\sigma \circ \rho \subseteq A \times C$ и $(\sigma \circ \rho)^{-1} \subseteq C \times A$. Важи да је

$$\begin{aligned}
(c,a) \in (\sigma \circ \rho)^{-1} \quad & \text{акко} \quad (a,c) \in \sigma \circ \rho \\
& \text{акко} \quad \text{постоји } b \in B \text{ тако да } (a,b) \in \rho \text{ и } (b,c) \in \sigma \\
& \text{акко} \quad \text{постоји } b \in B \text{ тако да } (b,a) \in \rho^{-1} \text{ и } (c,b) \in \sigma^{-1} \\
& \text{акко} \quad (c,a) \in \rho^{-1} \circ \sigma^{-1}.
\end{aligned}$$

□

Како је релација скуп, јасно је шта је пресек или унија две релације.

Теорема 3.9 *Ако су $\rho, \sigma \subseteq A \times B$ тада је:*

1. $(\sigma \cup \rho)^{-1} = \sigma^{-1} \cup \rho^{-1}$
2. $(\sigma \cap \rho)^{-1} = \sigma^{-1} \cap \rho^{-1}$.

Доказ.

1.

$$\begin{aligned}
(b,a) \in (\sigma \cup \rho)^{-1} \quad & \text{акко} \quad (a,b) \in \sigma \cup \rho \\
& \text{акко} \quad (a,b) \in \sigma \text{ или } (a,b) \in \rho \\
& \text{акко} \quad (b,a) \in \sigma^{-1} \text{ или } (b,a) \in \rho^{-1} \\
& \text{акко} \quad (b,a) \in \sigma^{-1} \cup \rho^{-1}.
\end{aligned}$$

2.

$$\begin{aligned}
(b,a) \in (\sigma \cap \rho)^{-1} \quad & \text{акко} \quad (a,b) \in \sigma \cap \rho \\
& \text{акко} \quad (a,b) \in \sigma \text{ и } (a,b) \in \rho \\
& \text{акко} \quad (b,a) \in \sigma^{-1} \text{ и } (b,a) \in \rho^{-1} \\
& \text{акко} \quad (b,a) \in \sigma^{-1} \cap \rho^{-1}.
\end{aligned}$$

□

Теорема 3.10 *Нека су $\rho_1, \rho_2 \subseteq A \times B$ и $\sigma \subseteq B \times C$.*

1. *Ако је* $\rho_1 \subseteq \rho_2$*, онда је* $\sigma \circ \rho_1 \subseteq \sigma \circ \rho_2$*.*

2. *Ако је* $A = B$ *и* $\rho_1 \subseteq \rho_2$*, онда је* $\rho_1 \circ \rho_1 \subseteq \rho_2 \circ \rho_2$*.*

3. $\sigma \circ (\rho_1 \cup \rho_2) = (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2)$*.*

4. $\sigma \circ (\rho_1 \cap \rho_2) \subseteq (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2)$*.*

Доказ.

1.

$$\begin{array}{rcl} (a,c) \in \sigma \circ \rho_1 & \text{акко} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_1 \text{ и } (b,c) \in \sigma \\ & \text{повлачи} & (a,b) \in \rho_2 \text{ и } (b,c) \in \sigma \\ & \text{повлачи} & (a,c) \in \sigma \circ \rho_2. \end{array}$$

2.

$$\begin{array}{rcl} (a,c) \in \rho_1 \circ \rho_1 & \text{акко} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_1 \text{ и } (b,c) \in \rho_1 \\ & \text{повлачи} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_2 \text{ и } (b,c) \in \rho_2 \\ & \text{повлачи} & (a,c) \in \rho_2 \circ \rho_2. \end{array}$$

3.

$$\begin{array}{rcl} (a,c) \in \sigma \circ (\rho_1 \cup \rho_2) & \text{акко} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_1 \cup \rho_2 \text{ и } (b,c) \in \sigma \\ & \text{акко} & \text{постоји } b \in B \text{ тако да } \ ((a,b) \in \rho_1 \text{ или } (a,b) \in \rho_2) \ \text{ и } (b,c) \in \sigma \\ & \text{акко} & \text{постоји } b \in B \text{ тако да } \ ((a,b) \in \rho_1 \text{ и } (b,c) \in \sigma) \\ & & \text{или } \ ((a,b) \in \rho_2 \text{ и } (b,c) \in \sigma) \\ & \text{акко} & (a,c) \in \sigma \circ \rho_1 \text{ или } (a,c) \in \sigma \circ \rho_2 \\ & \text{акко} & (a,c) \in (\sigma \circ \rho_1) \cup (\sigma \circ \rho_2). \end{array}$$

4.

$$\begin{array}{rcl} (a,c) \in \sigma \circ (\rho_1 \cap \rho_2) & \text{акко} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_1 \cap \rho_2 \text{ и } (b,c) \in \sigma \\ & \text{акко} & \text{постоји } b \in B \text{ тако да } (a,b) \in \rho_1 \text{ и } (a,b) \in \rho_2 \text{ и } (b,c) \in \sigma \\ & \text{следи} & (a,c) \in \sigma \circ \rho_1 \text{ и } (a,c) \in \sigma \circ \rho_2 \\ & \text{акко} & (a,c) \in (\sigma \circ \rho_1) \cap (\sigma \circ \rho_2). \end{array}$$

□

Размислите због чега у 4. не мора да важи једнакост – другим речима, нађите пример који то показује.

Дефиниција 3.11 *Нека је* ρ *бинарна релација на скупу* A*. Кажемо да је* ρ

- *рефлексивна, ако за свако* $a \in A$ *важи:* $(a,a) \in \rho$*;*
- *антирефлексивна, ако за свако* $a \in A$ *важи:* $(a,a) \notin \rho$*;*
- *симетрична, ако за све* $a, b \in A$ *важи:* $(a,b) \in \rho \Rightarrow (b,a) \in \rho$*;*
- *антисиметрична, ако је за све* $a, b \in A$ *важи:* $(a,b) \in \rho \wedge (b,a) \in \rho \Rightarrow a = b$*;*
- *транзитивна, ако је за све* $a, b, c \in A$ *важи:* $(a,b) \in \rho \wedge (b,c) \in \rho \Rightarrow (a,c) \in \rho$*.*

Напомена 3.12 Приметимо да се у дефиницији симетричне, антисиметричне и транзитивне релације појављује знак импликације. Исказ облика $x \Rightarrow y$ је тачан ако су тачни x и y, али и ако је x нетачно,а y има било коју вредност. Битно је узети у обзир овај коментар при испитивању особина неке релације. На пример, ако при испитивању антисиметричности закључимо да не постоје елементи a и b тако да $(a, b) \in \rho \wedge (b, a) \in \rho$, тада је лева страна импликације увек нетачна, па је цео исказ тачан и релација јесте антисиметрична.

Пример 3.13 *Нека је $A = \{a, b, c\}$. Испитати које од наведених особина задовољава бинарна релација $\rho \subseteq A \times A$, ако је:*

1. $\rho = \emptyset$;
2. $\rho = A \times A$;
3. $\rho = \{(a, a), (b, b), (a, b), (b, a)\}$;
4. $\rho = \{(a, c), (b, a)\}$.

1. Релација ρ није рефлексивна, јер, на пример $(a, a) \notin \rho$. Јесте антирефлексивна, јер за сваки елемент скупа A важи да није у релацији са самим собом. Леве стране импликација у дефиницији симетричности, антисиметричности и транзитивности су увек нетачне, па према претходној напомени ρ јесте симетрична, антисиметрична и транзитивна.
2. Најпре, $A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$. Лако се може закључити да је ρ рефлексивна, симетрична и транзитивна, а да није антирефлексивна. Није антисиметрична, јер је, на пример $(a, b) \in \rho$ и $(b, a) \in \rho$, а није $a = b$.
3. Релација није рефлексивна, јер $(c, c) \notin \rho$. Није ни антирефлексивна, јер је $(a, a) \in \rho$. Јесте симетрична и транзитивна. Није антисиметрична јер је $(a, b) \in \rho$ и $(b, a) \in \rho$ и $a \neq b$.
4. Није рефлексивна, али како важи да ниједан елемент није у релацији са самим собом, јесте антирефлексивна. Није симетрична, јер је, на пример, $(a, c) \in \rho$ а није $(c, a) \in \rho$. Није транзитивна, јер је $(b, a) \in \rho$ и $(a, c) \in \rho$, а није $(b, c) \in \rho$. Према претходној напомени, јесте антисиметрична.

$\triangle$

Приметимо да се може десити да релеција не буде ни рефлексивна ни антирефлексивна, али да не може истовремено бити и једно и друго. С друге стране, релација може бити и симетрична и антисиметрична, али може бити и да није симетрична и није антисиметрична. Пример за последње тврђење је скуп $A = \{x, y, z, t\}$ и релација $\rho = \{(x, y), (z, t), (t, z)\}$.

Нека је $\triangle_A = \{(a, a) \mid a \in A\}$. Како важи $(a, b) \in \triangle_A$ акко $a = b$, то је $\triangle_A$ релација једнакости на скупу A. Уз помоћ ове ознаке можемо преформулисати претходну дефиницију. Наиме, релација ρ је

- рефлексивна, ако је $\triangle_A \subseteq \rho$;
- антирефлексивна, ако је $\triangle_A \cap \rho = \emptyset$;
- симетрична, ако је $\rho \subseteq \rho^{-1}$;
- антисиметрична, ако је $\rho \cap \rho^{-1} \subseteq \triangle_A$;
- транзитивна, ако је $\rho \circ \rho \subseteq \rho$.

Јасно је зашто су ово алтернативне дефиниције рефлексивности и антирефлексивности. Приметимо да је важи и: релација је симетрична ако и само ако је $\rho^{-1} \subseteq \rho$, а тиме и $\rho^{-1} = \rho$. Објашњење за антисиметричност гласи овако: реченица 'Ако је $(a,b) \in \rho$ и $(b,a) \in \rho$, онда је $a = b$.' је еквивалентана са 'Ако је $(a,b) \in \rho$ и $(a,b) \in \rho^{-1}$, онда је $(a,b) \in \triangle_A$.' Објашњење за транзитивност: нека је ρ транзитивна. Ако је $(a,c) \in \rho \circ \rho$, онда постоји b тако да $(a,b) \in \rho$ и $(b,c) \in \rho$. Због транзитивности је $(a,c) \in \rho$, па је $\rho \circ \rho \subseteq \rho$. Обрнуто, нека је $\rho \circ \rho \subseteq \rho$. Ако је $(a,b) \in \rho$ и $(b,c) \in \rho$, онда је и $(a,c) \in \rho \circ \rho \subseteq \rho$, па је релација транзитивна.

Нека је дата релација ρ на скупу A. Ако ρ није рефлексивна, можемо је проширити тако да добијамо рефлексивну релацију. Наиме, $\rho^r = \rho \cup \triangle_A$ је најмања рефлексивна релација која садржи ρ. Слично је са $\rho^s = \rho \cup \rho^{-1}$ дефинисана најмања симетрична релација која садржи ρ. Наредна теорема објашњава како се од полазне релације добија транзитивна релација.

Нека је ρ^n ознака за $\underbrace{\rho \circ \rho \circ \cdots \circ \rho}_{n \text{ пута}}$.

Теорема 3.14 *Нека је ρ бинарна релација на скупу A. Најмања транзитивна релација која садржи ρ је релација $\rho^t = \bigcup_{n \geq 1} \rho^n$.*

Доказ. Како је $\rho^t = \rho \cup \rho^2 \cup \rho^3 \ldots$, важи да је $\rho \subseteq \rho^t$, то јест ρ^t садржи ρ.

Докажимо да је ρ^t транзитивна. Нека су $(a,b),(b,c) \in \rho^t$. Постоји број $n \geq 1$ тако да $(a,b) \in \rho^n$ и $m \geq 1$ тако да $(b,c) \in \rho^m$. Тада је $(a,c) \in \rho^m \circ \rho^n = \rho^{m+n} \subseteq \rho'$.

Дакле, доказали смо да је ρ^t транзитивна релација која садржи ρ. Да бисмо доказали да је најмања таква, довољно је показати да ако је $\rho \subseteq \tau$ транзитивна, онда мора бити $\rho^t \subseteq \tau$. Из $\rho \subseteq \tau$ и тврђења 3.10 следи $\rho \circ \rho \subseteq \tau \circ \tau$. Како је τ транзитивна, имамо да је $\tau \circ \tau \subseteq \tau$, па је $\rho^2 \subseteq \tau$. Слично је и $\rho^n \subseteq \tau$, за било који број $n \geq 1$, а тиме је и $\bigcup_{n \geq 1} \rho^n \subseteq \tau$, то јест $\rho^t \subseteq \tau$. □

3.1 Релације еквиваленције

Дефиниција 3.15 *Нека је ρ бинарна релација на скупу A. Кажемо да је ρ релација еквиваленције, ако је рефлексивна, симетрична и транзитивна.*

Релације еквиваленције обично означавамо са $\sim$.

Пример 3.16 *Следеће релације су релације еквиваленције:*

1. *Релација једнакости међу реалним бројевима: $=$.*
2. *Релација сличности у скупу троуглова еуклидске равни: $\sim$.*
3. *Једнакост апсолутних вредности реалних бројева, то јест релација $\sim$ дефинисана са: $x \sim y$ ако је $|x| = |y|$.*

△

Према алтернативним дефиницијама рефлексивности, симетричности и транзитивности, бинарна релација ρ на скупу A је релација еквиваленције ако важи

$$\triangle_A \subseteq \rho \qquad \rho \subseteq \rho^{-1} \qquad \rho \circ \rho \subseteq \rho.$$

Пример 3.17 *Релација ρ на скупу A је релација еквиваленције ако и само ако*

$$\triangle_A \subseteq \rho \qquad \rho = \rho^{-1} \qquad \rho \circ \rho = \rho.$$

Јасно је да ако важи наведено, онда ρ јесте релација еквиваленције. С друге стране, ако је ρ релација еквиваленције, онда је

$$\triangle_A \subseteq \rho \qquad \rho \subseteq \rho^{-1} \qquad \rho \circ \rho \subseteq \rho.$$

Према тврђењу 3.7 из $\rho \subseteq \rho^{-1}$ следи $\rho^{-1} \subseteq (\rho^{-1})^{-1} = \rho$. Дакле, важи $\triangle_A \subseteq \rho$ и $\rho = \rho^{-1}$. Треба још доказати $\rho \circ \rho = \rho$. Нека је $(a, b) \in \rho$. Како је $\triangle_A \subseteq \rho$, постоји $b \in A$ тако да $(a, b) \in \rho$ и $(b, b) \in \rho$, па је тада и $(a, b) \in \rho \circ \rho$. Дакле, важи $\rho \subseteq \rho \circ \rho$. $\triangle$

Дефиниција 3.18 *Нека је $\sim$ релација еквиваленције на скупу A. Класа еквиваленције елемента $a \in A$ је скуп*

$$C_a = \{x \in A \mid a \sim x\}.$$

Означавамо је и са $[a]$ и кажемо да је елемент a представник класе C_a.

Теорема 3.19 *Нека је $\sim$ релација еквиваленције на скупу A.*

1. *Све класе еквиваленције су непразни скупови.*
2. *Нека је $a, b \in A$. Ако је $C_a \cap C_b \neq \emptyset$, онда је $C_a = C_b$.*
3. *Унија свих класа еквиваленције је једнака скупу A.*

Доказ.

1. Како је за свако $a \in A$ испуњено $a \sim a$, то је $a \in C_a$, па је свака класа непразан скуп.
2. Како је $C_a \cap C_b \neq \emptyset$, постоји $x \in C_a \cap C_b$. Нека је $u \in C_a$. Докажимо да је $u \in C_b$. Важи
$$x \in C_a \Rightarrow a \sim x \qquad x \in C_b \Rightarrow b \sim x.$$
Из $u \in C_a$ следи да $a \sim u$. Због симетричности и транзитивности релације $\sim$ важи
$$\begin{matrix} a \sim u \\ a \sim x \end{matrix} \quad \Rightarrow \quad \begin{matrix} u \sim a \\ a \sim x \end{matrix} \quad \Rightarrow \quad u \sim x.$$
Даље је
$$\begin{matrix} u \sim x \\ b \sim x \end{matrix} \quad \Rightarrow \quad \begin{matrix} u \sim x \\ x \sim b \end{matrix} \quad \Rightarrow \quad u \sim b \quad \Rightarrow \quad b \sim u.$$
Последња релација значи да је $u \in C_b$, а како је u произвољан елемент, имамо да је $C_a \subseteq C_b$. Слично се докаже и обрнуто: $C_b \subseteq C_a$, па је $C_a = C_b$.
3. Нека је $a \in A$ било који елемент. Како је $a \sim a$, онда је $a \in C_a$, па и $a \in \bigcup_{x \in A} C_x$.

$\square$

Према претходној теореми, свака релација еквиваленције разбија скуп на коме је дефинисана на непразне, дисјунктне скупове чија унија је једнака целом скупу. Таква подела се назива партиција скупа.

Дефиниција 3.20 *Количнички скуп скупа A за релацију еквиваленције $\sim$ је $A/_\sim = \{C_x \mid x \in A\}$.*

Пример 3.21 *Нека је дефинисана бинарна релација на скупу $\mathbb{Z}$ са $x \sim y$ ако је $x - y$ дељив са 3. Доказати да је $\sim$ релација еквиваленције, одредити класе еквиваленције и количнички скуп.*

Како је за свако $x \in \mathbb{Z}$ број $x - x = 0$ дељив са 3, релација јесте рефлексивна. За све $x, y \in \mathbb{Z}$ важи да ако је број $x - y$ дељив са 3, онда је то и број $y - x$, па је $\sim$ симетрична. Треба још доказати транзитивност. Нека су $x, y, z \in \mathbb{Z}$ такви да су $x - y$ и $y - z$ дељиви са 3, онда је и број $x - z = (x - y) + (y - z)$ дељив са 3. Дакле, $\sim$ јесте релација еквиваленције.

Нека је $x \in \mathbb{Z}$ произвољни елемент. Одредимо његову класу C_x. Према дефиницији је

$$\begin{aligned} C_x &= \{y \in \mathbb{Z} \mid x \sim y\} = \{y \in \mathbb{Z} \mid x - y \text{ је дељив са } 3\} \\ &= \{y \in \mathbb{Z} \mid x - y = 3k, \text{ за неки број } k \in \mathbb{Z}\} = \{x - 3k \mid k \in \mathbb{Z}\}. \end{aligned}$$

Тако да је

$$\begin{aligned} C_0 &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ C_1 &= \{\dots, -8, -5, -2, 1, 4, 7, \dots\} \\ C_2 &= \{\dots, -7, -4, -1, 2, 5, 8, \dots\}. \end{aligned}$$

Приметимо да су ово све класе наведене релације, па је количнички скуп

$$A/_\sim = \{\{\dots, -6, -3, 0, 3, 6, \dots\}, \{\dots, -8, -5, -2, 1, 4, 7, \dots\}, \{\dots, -7, -4, -1, 2, 5, 8, \dots\}\}.$$

$\triangle$

3.2 Релације парцијалног уређења

Дефиниција 3.22 *Нека је ρ бинарна релација на скупу A. Кажемо да је ρ релација парцијалног уређења, ако је рефлексивна, антисиметрична и транзитивна.*

Релацију парцијалног уређења можемо означавати са $\preceq$. Скуп A на коме је дефинисана релација $\preceq$ називамо парцијално уређен скуп или посет.

Пример 3.23 *Следеће релације су релације парцијалног уређења:*

1. *Релација мање или једнако на скупу реалних бројева: $\leq$.*
2. *Релација дељивости на скупу природних бројева: $|$.*
3. *Релација инклузија на партитивном скупу неког скупа: $\subseteq$.*

$\triangle$

Пример 3.24 *Слично као у примеру 3.17, може се показати да је ρ релација поретка на скупу A ако и само ако*

$$\triangle_A \subseteq \rho \qquad \rho \cap \rho^{-1} = \triangle_A \qquad \rho \circ \rho = \rho.$$

$\triangle$

Дефиниција 3.25 *Нека је $\preceq$ релација парцијалног поретка на скупу A. Кажемо да је елемент $a \in A$*

- *минималан, ако је за сваки $x \in A$ тачно $x \preceq a \Rightarrow x = a$;*
- *максималан, ако је за сваки $x \in A$ тачно $a \preceq x \Rightarrow x = a$;*

- *најмањи, ако је за сваки $x \in A$ $a \preceq x$;*
- *највећи, ако је за сваки $x \in A$ $x \preceq a$.*

Приметимо да ако постоји најмањи елемент, тада је он једини такав. Претпоставимо супротно: a_1 и a_2 су најмањи. Тада је $a_1 \preceq a_2$, јер је a_1 најмањи, али и $a_2 \preceq a_1$ јер је a_2 најмањи. Како у питању релација поретка, важи антисимметричност, па из $a_1 \preceq a_2$ и $a_2 \preceq a_1$ следи да је $a_1 = a_2$. Слично се може доказати да постоји највише један највећи елемент.

Ако претпоставимо да постоји најмањи елемент a, тада је он и једини минимални елемент. Наиме, за свако $x \in A$ важи $a \preceq x$, па ако је $x \prec a$, због антисиметричности мора бити $x = a$. Према дефиницији, a јесте минимални елемент. Ако је b минимални елемент, онда је $x \preceq b \Rightarrow x = b$, за свако x, па и за a. Пошто је a најмањи, онда је $a \preceq b$, а тиме и $a = b$. Дакле, a је једини минимални елемент. Аналогно је тврђење за највећи елемент.

Пример 3.26 *Нека је дефинисана бинарна релација на скупу $A = \{2, 3, 5, 6, 15, 30\}$ са $x \preceq y$ ако је $x \mid y$. Доказати да је $\preceq$ релација парцијалног уређења на скупу A и одредити најмањи, највећи, минималне и максималне елементе, ако постоје.*

За сваки број $x \in A$ важи да $x \mid x$, па је $\prec$ рефлексивна. Јасно је и да је једино могуће да $x \mid y$ и $y \mid x$ ако је $x = y$, па је $\preceq$ антисиметрична. Ако су $x, y, z \in A$ и $x \mid y$ и $y \mid z$, мора бити да $x \mid z$, па важи транзитивност.

Не постоји елемент који дели све елементе скупа A, па нема најмањег. Број 30 је дељив свим елементима из A, па је то највећи елемент, а према претходним коментарима, и једини максимални. Како не постоје бројеви скупа A који деле 2,3 и 5, а различити су од њих, то ови елементи чине минималне елементе у односу на релацију $\preceq$. $\triangle$

Задаци

1. Нека су ρ, σ, τ бинарне релације на скупу A такве да $\rho \circ \sigma \subseteq \rho$ и $\rho \circ \sigma^{-1} \subseteq \rho$. Доказати да је $\rho \cap (\tau \circ \sigma) = (\rho \cap \tau) \circ \sigma$.

2. Нека су ρ и σ антисиметричне бинарне релације скупа A. Доказати да је:

   (а) ρ^{-1} и $\rho \cap \sigma$ су антисиметричне.

   (б) $\rho \cup \sigma$ је антисиметрична ако и само ако $\rho \cap \sigma^{-1} \subseteq \triangle_A$.

3. Нека је n природан број. Дефинишимо релацију $\sigma_n \in \mathbb{N} \times \mathbb{N}$ са: $(x, y) \in \sigma_n$ ако је $x + n \leq y$. Доказати да је:

   (а) σ_n је транзитивна.

   (б) $m \leq n$ ако и само ако $\sigma_n \subseteq \sigma_m$.

   (в) $\sigma_m \circ \sigma_n \subseteq \sigma_{m+n}$.

4. Нека је дата релација $\rho \subseteq \mathbb{R} \times \mathbb{R}$ са $(x, y) \in \rho$ ако је $x^2 + y^2 \leq 1$. Испитати да ли је ρ рефлексивна, антирефлексивна, симетрична, антисиметрична, транзитивна.

5. Нека је дата релација $\rho \subseteq \mathbb{R} \times \mathbb{R}$ са $(x, y) \in \rho$ ако је $x = |y|$. Испитати да ли је ρ рефлексивна, антирефлексивна, симетрична, антисиметрична, транзитивна.

6. Нека су ρ и σ релације еквиваленције на скупу A. Доказати да је $\sigma \circ \rho$ релација еквиваленције ако и само ако $\sigma \circ \rho = \rho \circ \sigma$.

7. Нека су ρ и σ релације поретка на скупу A. Доказати да је и $\rho \cap \sigma^{-1}$ релација поретка.

8. Доказати да је једина бинарна релација на непразном скупу A која је и релација еквиваленције и парцијалног уређења релација $\triangle_A$.

9. Нека је $\preceq$ релација парцијалног уређења скупа A.

   (а) Ако не постоји минимални (максимални) елемент или постоје бар два минимална (максимална) елемента, тада не постоји најмањи (највећи).

   (б) Ако је елемент a најмањи (највећи, минимални, максимални) у односу на $\preceq$, тада је a највећи (најмањи, максимални, минимални) у односу на релацију $\preceq^{-1}$.

10. Нека је на скупу $\mathbb{R}\times\mathbb{R}$ дефинисана релација $\sim$ са $x \sim y$ ако је $\cos x = \cos y$. Доказати да је $\sim$ релација еквиваленције. Ако је $\alpha \in \mathbb{R}$ произвољни елемент, наћи C_α.

11. Нека је скуп $A = \{0, 1, 2\}$ и $B = A\times A$. На скупу B је дефинисана релација $\sim$ са $(x, y) \sim (z, t)$ ако је $xy = zt$. Доказати да је $\sim$ релација еквиваленције и одредити количнички скуп.

12. Нека је $A = \{-6, -4, -2, 0, 1, 3, 5\}$ и $B = \{2, 4, 8, 16, 32\}$. Дефинишимо релацију $\preceq$ на скупу $C = A\times B$ на следећи начин: $(x, y) \preceq (z, t)$ ако је $|x| \leq |z|$ и $y \mid t$. Доказати да је $\preceq$ релација парцијалног уређења на скупу C и одредити најмањи, највећи, минималне и максималне елементе, ако постоје.

13. Нека је A неки непразни скуп и $B = \mathcal{P}(A) \setminus \{\emptyset\}$. На скупу B је дата релација $\preceq$ са $X \preceq Y$ ако је $X \subseteq Y$. Доказати да је $\preceq$ релација парцијалног уређења и одредити најмањи, највећи, минималне и максималне елементе, ако постоје.

4 Функције

За скупове A и B, функцију из A у B замишљамо као додељивање елементима скупа A елемената скупа B, по неком правилу. Увешћемо функцију преко појма релације. Лако се можемо уверити да се та дефиниција поклапа са нашом интуицијом.

Дефиниција 4.1 *Нека је $f \subseteq A \times B$ релација. Кажемо да је f функција ако за свако $a \in \mathrm{Dom}(f)$ постоји тачно једно $b \in B$ тако да $(a, b) \in f$.*

Ако је $f \subseteq A \times B$ функција, уместо $(a, b) \in f$ пишемо $b = f(a)$. Ако је $\mathrm{Dom}(f) = A$, пишемо $f\colon A \to B$ и кажемо да је A домен функције f, а B кодомен.

Ако је $f\colon A \to B$ функција, знамо да је f^{-1} инверзна релација. Занима нас под којим условима је f^{-1} функција, а и под којим условима је њен домен једнак скупу B, тј. када $f^{-1}\colon A \to B$. Како је

$$\begin{aligned}\mathrm{Dom}(f^{-1}) = \mathrm{Im}(f) &= \{b \in B \mid \text{постоји } a \in A \text{ тако да } (a, b) \in f\}\\ &= \{b \in B \mid \text{постоји } a \in A \text{ тако да } f(a) = b\},\end{aligned}$$

видимо да је неопходно да за свако $b \in B$ постоји $a \in A$ тако да $f(a) = b$. Такође, потребно је да за свако $b \in \mathrm{Dom}(f^{-1})$ постоји само једно $a \in A$ тако да $f(a) = b$. Другим речима, ако је $f(a_1) = f(a_2)$ мора бити $a_1 = a_2$. Овим смо мотивисали увођење следећих дефиниција:

Дефиниција 4.2 *Функција $f : A \to B$ је сурјекција, или "на" функција, ако важи*

$$\textit{за свако } b \in B \textit{ постоји } a \in A \textit{ тако да је } f(a) = b.$$

Дефиниција 4.3 *Функција $f : A \to B$ је инјекција, или "1-1" функција, ако важи*

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2, \text{ за све } a_1, a_2 \in A.$$

Дефиниција 4.4 *За функцију $f : A \to B$ кажемо да је бијекција ако је инјекција и сурјекција.*

Сада можемо да закључимо: ако је $f : A \to B$ бијекција, тада је f^{-1} такође функција.

Пример 4.5 *Нека су скупови*

$$\begin{array}{rclcrcl} A &=& \{1,2,3,4\} & \quad & B &=& \{x,y,z\} \\ C &=& \{a,b,c\} & & D &=& \{m,n,p,q\}. \end{array}$$

Дате су функције

$$\begin{array}{rcl} f : A & \to & B \\ \\ 1 & \mapsto & y \\ 2 & \mapsto & x \\ 3 & \mapsto & x \\ 4 & \mapsto & z \end{array} \qquad \begin{array}{rcl} g : C & \to & D \\ \\ a & \mapsto & p \\ b & \mapsto & m \\ c & \mapsto & n \end{array} \qquad \begin{array}{rcl} h : A & \to & D \\ \\ 1 & \mapsto & n \\ 2 & \mapsto & p \\ 3 & \mapsto & m \\ 4 & \mapsto & q. \end{array}$$

Испитати инјективност, сурјективност и бијективност наведених функција.

Функција f јесте сурјективна, а како је $f(2) = f(3)$ и $2 \neq 3$, није инјективн. Функција g јесте инјективн, али није сурјективна јер не постоји елемент из C који се слика у q. Функција h је инјекција и сурјекција, па је и бијекција. Инверзна функција је

$$h^{-1} : D \to A \qquad \begin{array}{rcl} m & \mapsto & 3 \\ n & \mapsto & 1 \\ p & \mapsto & 2 \\ q & \mapsto & 4. \end{array}$$

△

Дефиниција 4.6 *Нека су $f : A \to B$ и $g : B \to C$ функције. Композиција функција f и g је функција $g \circ f : A \to C$ тако да $(g \circ f)(x) = g(f(x))$.*

Пример 4.7 *Ако су ознаке као у претходном примеру, одредити композицију $f \circ h^{-1}$.*

Како је $h^{-1} : D \to A$ и $f : A \to B$, то је $f \circ h^{-1} : D \to B$.

$$\begin{array}{rcl} (f \circ h^{-1})(m) &=& f(3) = x \\ (f \circ h^{-1})(n) &=& f(1) = y \\ (f \circ h^{-1})(p) &=& f(2) = x \\ (f \circ h^{-1})(q) &=& f(4) = z. \end{array}$$

△

Пример 4.8 *Нека су дате инјективне функције $f : A \to B$ и $g : B \to C$. Доказати да је композиција $g \circ f$ такође инјекција.*

Нека је $(g \circ f)(a_1) = (g \circ f)(a_2)$. Треба доказати да је $a_1 = a_2$. Важи да је $g(f(a_1)) = g(f(a_2))$. Како је g "1-1", према дефиницији је $f(a_1) = f(a_2)$. Даље, како је f "1-1", то је $a_1 = a_2$. △

4.1 Директна и инверзна слика скупа

Дефиниција 4.9 *Нека је $f : X \to Y$ и $A \subseteq X$. Директна слика скупа A је скуп*

$$f[A] = \{f(x) \mid x \in A\}.$$

Дефиниција 4.10 *Нека је $f : X \to Y$ и $B \subseteq Y$. Инверзна слика скупа B је скуп*

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

Приметимо да важи:

$$\begin{array}{rll} y \in f[A] & \text{акко} & \text{постоји } x \in A \text{ тако да } f(x) = y; \\ x \in f^{-1}[B] & \text{акко} & f(x) \in B. \end{array}$$

Такође је

$$\begin{array}{rll} y \notin f[A] & \text{акко} & \text{за свако } x \in A\ f(x) \neq y; \\ x \notin f^{-1}[B] & \text{акко} & f(x) \notin B. \end{array}$$

Напомена 4.11 *Инверзна слика скупа $f^{-1}[B]$ је појам који је дефинисан без обзира на то да ли постоји инверзна функција f^{-1}.*

Пример 4.12 *Нека су скупови $A = \{1, 2, 3, 4, 5\}$ и $B = \{a, b, c, d, e, f\}$ и функција $f : A \to B$ задата са*

$$\begin{array}{ccccccccc} 1 & \mapsto & b & 2 & \mapsto & e & 3 & \mapsto & b \\ 4 & \mapsto & c & 5 & \mapsto & c. & & & \end{array}$$

Одредити $f[\{2, 4, 5\}]$ и $f^{-1}[\{a, b, c\}]$.

$$f[\{2, 4, 5\}] = \{c, e\} \qquad f^{-1}[\{a, b, c\}] = \{1, 3, 4, 5\}.$$

△

Пример 4.13 *Нека је $f : X \to Y$ функција и $A, B \subseteq X$, $C, D \subseteq Y$.*

1. *Важи да $f[\emptyset] = \emptyset$ и $f^{-1}[\emptyset] = [\emptyset]$.*
2. *Ако је $A \subseteq B$, онда је $f[A] \subseteq f[B]$.*
3. *Ако је $C \subseteq D$, онда је $f^{-1}[C] \subseteq f^{-1}[D]$.*

1. Ако претпоставимо да постоји елемент који припада левој страни неке од две једнакости, добијемо контрадикцију. Тако да оба скупа морају бити једнака празном скупу.

2.

$$\begin{array}{rll} y \in f[A] & \text{повлачи} & \text{постоји } x \in A \text{ тако да } f(x) = y \\ & \text{повлачи} & \text{постоји } x \in B \text{ тако да } f(x) = y, \text{ јер је } A \subseteq B \\ & \text{повлачи} & y \in f[B]. \end{array}$$

3.

$$\begin{array}{rll} x \in f^{-1}[C] & \text{повлачи} & f(x) \in C \\ & \text{повлачи} & f(x) \in D, \text{ јер је } C \subseteq D \\ & \text{повлачи} & x \in f^{-1}[D]. \end{array}$$

△

Пример 4.14 *Ако су $A, B \subseteq X$ и $f : X \to Y$ функција, доказати да је $f[A \cup B] = f[A] \cup f[B]$.*

Важи да

$$\begin{array}{rll} y \in f[A \cup B] & \text{акко} & \text{постоји } x \in A \cup B \text{ тако да } f(x) = y \\ & \text{следи} & x \in A \text{ или } x \in B \text{ тако да } f(x) = y \\ & \text{следи} & x \in A \text{ тако да } f(x) = y \text{ или } x \in B \text{ тако да } f(x) = y \\ & \text{следи} & y \in f[A] \text{ или } y \in f[B] \\ & \text{следи} & y \in f[A] \cup f[B]. \end{array}$$

С друге стране је

$$\begin{array}{rll} y \in f[A] \cup f[B] & \text{акко} & y \in f[A] \text{ или } y \in f[B] \\ & \text{следи} & \text{постоји } x \in A \subseteq A \cup B \text{ тако да } f(x) = y \\ & & \text{или постоји } z \in B \text{ тако да } f(z) = y \\ & \text{следи} & \text{постоји } x \in A \cup B \text{ тако да } f(x) = y \\ & \text{следи} & y \in f[A \cup B]. \end{array}$$

△

Пример 4.15 *Ако су $A, B \subseteq Y$ и $f : X \to Y$ функција, доказати да је $f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$.*

Важи да

$$\begin{array}{rll} x \in f^{-1}[A \setminus B] & \text{акко} & f(x) \in A \setminus B \\ & \text{акко} & f(x) \in A \text{ и } f(x) \notin B \\ & \text{акко} & x \in f^{-1}[A] \text{ и } x \notin f^{-1}[B] \\ & \text{акко} & x \in f^{-1}[A] \setminus f^{-1}[B]. \end{array}$$

△

4.2 Карактеристичне функције скупа

Ако су X и Y скупови, ознака за скуп функција из X у Y је

$$Y^X = \{f \mid f : X \to Y\}.$$

Дефиниција 4.16 *Нека је X било који скуп и $A \subseteq X$. Карактеристична функција скупа A је $\chi_A : X \to \{0, 1\}$ тако да*

$$\chi_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A. \end{cases}$$

На пример, важи $\chi_\emptyset = 0$ и $\chi_X = 1$.

Пример 4.17 *Нека је скуп $X\{a, b, c, d, e, f\}$ и $A = \{c, d, f\} \subseteq X$. Тада је карактеристична функција скупа A:*

$$\chi_A : X \to \{0,1\} \qquad \begin{array}{rcl} \chi_A(a) & = & 0 \\ \chi_A(b) & = & 0 \\ \chi_A(c) & = & 1 \end{array} \qquad \begin{array}{rcl} \chi_A(d) & = & 1 \\ \chi_A(e) & = & 0 \\ \chi_A(f) & = & 1. \end{array}$$

△

Теорема 4.18 *За скупове A и B важи: $A = B$ ако и само ако $\chi_A = \chi_B$.*

Доказ. Ако је $A = B$ јасно је да је $\chi_A = \chi_B$. Обрнуто, претпоставимо да је $\chi_A = \chi_B$. Нека је $x \in A$. Тада је $\chi_a(x) = 1$, а тиме и $\chi_B(x) = 1$, па је $x \in B$. Дакле, $A \subseteq B$. Докажимо и $B \subseteq A$. Нека је $x \in B$. Тада је $1 = \chi_B(x) = \chi_A(x)$, па је $x \in A$. $\square$

Теорема 4.19 *Функција $\Phi : \mathcal{P}(X) \to \{0,1\}^X$ дефинисана са $\Phi(A) = \chi_A$ је бијекција.*

Доказ. Нека је $\Phi(A) = \Phi(B)$. Тада је $\chi_A = \chi_B$, па према теореми 4.2 важи $A = B$. Дакле, Φ је инјективн.

Нека је $f : X \to \{0,1\}$ било која функција. Одредимо скуп A тако да $\Phi(A) = \chi_A = f$. Дефинишимо скуп $A \subseteq X$ са $A = \{x \in X \mid f(x) = 1\}$. Ако је $x \in A$ тада је $\chi_A(x) = 1$ С друге стране по томе како смо дефинисали скуп A важи $f(x) = 1$, тако да добијамо $\chi_A(x) = f(x)$. Нека је сада $x \notin A$. Тада важи $\chi_A(x) = 0$, али и $f(x) \neq 1$, то јест $f(x) = 0$. Можемо закључити да је за свако $x \in X$ $f(x) = \chi_A(x)$, а тиме је и $f = \chi_A$. $\square$

Нека су операције сабирања и множења на скупу $\{0,1\}$ дефинисане на следећи начин:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Тада можемо дефинисати збир $f+g$ и производ $f \cdot g$ функција $f, g \in \{0,1\}^X$ са:

$$\begin{aligned} (f+g)(x) &\stackrel{\text{def}}{=} f(x) + g(x) \\ (f \cdot g)(x) &\stackrel{\text{def}}{=} f(x) \cdot g(x). \end{aligned}$$

Приметимо да је у првом изразу први знак + симбол операције сабирања функција, а други знак + симбол операције сабирања у скупу $\{0,1\}$. Исто важи за множење. То што их исто означавамо не доводи до забуне, јер су операције дефинисане на различитим скуповима. Лако се може показати да важи комутативност и асоцијативност сабирања и множења функција, као и лева и десна дистрибутивност множења према сабирању. Наиме, за све функције $f, g, h \in \{0,1\}^X$ важи:

$$\begin{aligned} f+g &= g+f & \qquad f+(g+h) &= (f+g)+h \\ f \cdot g &= g \cdot f & f \cdot (g \cdot h) &= (f \cdot g) \cdot h \end{aligned}$$

$$\begin{aligned} f \cdot (g+h) &= f \cdot g + f \cdot h \\ (g+h) \cdot f &= g \cdot f + h \cdot f \end{aligned}$$

Све једнакости су последица чињенице да у кодомену функција f, g и h, то јест скупу $\{0,1\}$, важи све набројане особине операција + и $\cdot$. Иначе, ако у скупу Y са операцијом $*$ важи, на пример, комутативност, тада иста особина важи и у скупу Y^X. Специјално, за функције из $\{0,1\}^X$ важи и $f + f = 0$, где је функција $0 : X \to \{0,1\}$ тако да $0(x) = 0$. Такође је $f \cdot f = f$. Све наведене особине можемо да применимо на карактеристичне функције.

Покушајмо да пронађемо везу између функције $\chi_{A \cap B}$ и функција χ_A и χ_B. Важи да је

$$\chi_{A \cap B}(x) = \begin{cases} 0, & x \notin A \cap B \\ 1, & x \in A \cap B. \end{cases}$$

С друге стране

$$\begin{aligned} (\chi_A \cdot \chi_B)(x) = \chi_A(x) \cdot \chi_B(x) = 1 \quad & \text{акко} \quad \chi_A(x) = 1 \text{ и } \chi_B(x) = 1 \\ & \text{акко} \quad x \in A \text{ и } x \in B \\ & \text{акко} \quad x \in A \cap B \end{aligned}$$

Дакле, добили смо да је $\chi_{A\cap B} = \chi_A \cdot \chi_B$.

На сличан начин се могу доказати и следећи идентитети:

$$\begin{array}{rcl}
\chi_{A\cup B} & = & \chi_A + \chi_B + \chi_A\chi_B \\
\chi_{A\setminus B} & = & \chi_A + \chi_A\chi_B \\
\chi_{A\triangle B} & = & \chi_A + \chi_B \\
\chi_{A^c} & = & 1 + \chi_A.
\end{array}$$

Присетимо се још да је

$$\chi_A\chi_A = \chi_A \qquad \chi_A + \chi_A = 0.$$

Ове једнакости можемо користити за доказивање скуповних идентитета.

Пример 4.20 *Доказати да је:*

1. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
2. $(A \cap B) \cup (B \cap C) \cup (C \cap A) = (A \cup B) \cap (B \cup C) \cap (C \cup A)$.

1.

$$\begin{array}{rcl}
\chi_{(A\triangle B)\triangle C} & = & \chi_{A\triangle B} + \chi_C = \chi_A + \chi_B + \chi_C \\
\chi_{A\triangle(B\triangle C)} & = & \chi_A + \chi_{B\triangle C} = \chi_A + \chi_B + \chi_C
\end{array}$$

Дакле, имамо да је $\chi_{(A\triangle B)\triangle C} = \chi_{A\triangle(B\triangle C)}$, па је према тврђењу 4.2 $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

2.

$$\begin{array}{rcl}
\chi_{(A\cap B)\cup(B\cap C)\cup(C\cap A)} & = & \chi_{((A\cap B)\cup(B\cap C))\cup(C\cap A)} = \chi_{(A\cap B)\cup(B\cap C)} + \chi_{C\cap A} + \\
& & +\chi_{(A\cap B)\cup(B\cap C)}\chi_{C\cap A} \\
& = & \chi_{A\cap B} + \chi_{B\cap C} + \chi_{A\cap B}\chi_{B\cap C} + \chi_C\chi_A + \\
& & +(\chi_{A\cap B} + \chi_{B\cap C} + \chi_{A\cap B}\chi_{B\cap C})\chi_C\chi_A \\
& = & \chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_B\chi_B\chi_C + \chi_C\chi_A + \\
& & +(\chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_B\chi_B\chi_C)\chi_C\chi_A \\
& = & \chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_B\chi_C + \chi_C\chi_A + \\
& & +\chi_A\chi_B\chi_C\chi_A + \chi_B\chi_C\chi_C\chi_A + \chi_A\chi_B\chi_C\chi_C\chi_A \\
& = & \chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_B\chi_C + \chi_A\chi_C + \\
& & +\chi_A\chi_B\chi_C + \chi_A\chi_B\chi_C + \chi_A\chi_B\chi_C \\
& = & \chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_C.
\end{array}$$

$$\begin{array}{rcl}
\chi_{(A\cup B)\cap(B\cup C)\cap(C\cup A)} & = & \chi_{((A\cup B)\cap(B\cup C))\cap(C\cup A)} = \chi_{(A\cup B)\cap(B\cup C)}\chi_{C\cup A} \\
& = & \chi_{A\cup B}\chi_{B\cup C}\chi_{C\cup A} \\
& = & (\chi_A + \chi_B + \chi_A\chi_B)(\chi_B + \chi_C + \chi_B\chi_C)(\chi_C + \chi_A + \chi_C\chi_A) \\
& = & (\chi_A\chi_B + \chi_A\chi_C + \chi_A\chi_B\chi_C + \chi_B\chi_B + \chi_B\chi_C + \chi_B\chi_B\chi_C + \\
& & +\chi_A\chi_B\chi_B + \chi_A\chi_B\chi_C + \chi_A\chi_B\chi_B\chi_C)(\chi_C + \chi_A + \chi_C\chi_A) \\
& = & (\chi_A\chi_C + \chi_B + \chi_A\chi_B\chi_C)(\chi_C + \chi_A + \chi_C\chi_A) \\
& = & \chi_A\chi_C\chi_C + \chi_A\chi_C\chi_A + \chi_A\chi_C\chi_C\chi_A + \chi_B\chi_C + \chi_B\chi_A + \\
& & +\chi_B\chi_c\chi_A + \chi_A\chi_B\chi_C\chi_C + \chi_A\chi_B\chi_C\chi_A + \chi_A\chi_B\chi_C\chi_C\chi_A \\
& = & \chi_A\chi_B + \chi_B\chi_C + \chi_A\chi_C.
\end{array}$$

$\triangle$

Користећи карактеристичне функције скупа можемо доказати једну занимљиву теорему.

Теорема 4.21 *(Канторова[7] теорема) Нека је X произвољан скуп. Постоји ињекција из X у $\mathcal{P}(X)$, али не постоји бијекција између тих скупова.*

Доказ. Претпоставимо супротно: постоји бијекција $f : X \to \mathcal{P}(X)$. Тада је за $x \in X$ $f(x)$ елемент у $\mathcal{P}(X)$, то јест $f(x) \subseteq X$. Можемо дефинисати функцију $g : X \to \{0,1\}$ тако да $g(x) = \chi_{f(x)}(x) + 1$. Видимо да је $g \in \{0,1\}^X$, па према тврђењу 4.19 важи да постоји скуп $A \subseteq X$ тако да $g = \chi_A$. С друге стране, $A \in \mathcal{P}(X)$ и f је бијекција, а тиме и сурјекција, постоји $x_0 \in X$ тако да $f(x_0) = A$. Добили смо да је $g = \chi_A = \chi_{f(x_0)}$, то јест за свако $x \in X$ важи $\chi_{f(x)}(x) + 1 = g(x) = \chi_{f(x_0)}(x)$. За $x = x_0$ имамо $\chi_{f(x_0)}(x_0) + 1 = \chi_{f(x_0)}(x_0)$, то јест $0 = 1$. Ово је немогуће, па бијекција не постоји. □

Задаци

1. Нека су функције $f : X \to Y$ и $g : Y \to Z$ и композиција $g \circ f$ је сурјекција. Доказати да је g сурјекција.
2. Доказати да је $(g \circ f)[A] = g[f[A]]$ и $(g \circ f)^{-1}[B] = f^{-1}[g^{-1}[B]]$, за функције $f : X \to Y$ и $g : Y \to Z$ и скупове $A \subseteq X, B \subseteq Z$.
3. Ако су функције $f : X \to Y$ и $g : Y \to Z$ бијекције, доказати да је и $g \circ f$ бијекција.
4. Доказати је $f[A \cap B] \subseteq f[A] \cap f[B]$, где је $f : X \to Y$ функција и $A, B \subseteq X$. Примером показати да не мора да важи обрнуто.
5. Доказати је $f[A] \setminus f[B] \subseteq f[A \setminus B]$, где је $f : X \to Y$ функција и $A, B \subseteq X$. Примером показати да не мора да важи обрнуто.
6. Доказати да је $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$, где је $f : X \to Y$ функција и $A, B \subseteq Y$.
7. Доказати да је $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$, где је $f : X \to Y$ функција и $A, B \subseteq Y$.
8. Доказати да је $f[A] \cap B^c = f[A \setminus f^{-1}[B]]$, где је $f : X \to Y$, $A \subseteq X$ и $B \subseteq Y$.
9. Нека је $f : X \to Y$ сурјекција и $A, b \subseteq X$ тако да $A \cup B = X$. Доказати да је $f[A] \cup f[B] = Y$.
10. (а) Показати да је $f : X \to Y$ ињективн ако и само ако за сваки скуп $A \subseteq X$ важи $f^{-1}[f[A]] = A$.
    (б) Нека је функција $f : X \to Y$ ињекција. Доказати да постоји функција $g : \mathcal{P}(X) \to \mathcal{P}(Y)$ која је сурјективна.
11. (а) Показати да је $f : X \to Y$ сурјективна ако и само ако за сваки скуп $B \subseteq Y$ важи $f[f^{-1}[B]] = B$.
    (б) Нека је функција $f : X \to Y$ сурјекција. Доказати да постоји функција $g : \mathcal{P}(X) \to \mathcal{P}(Y)$ која је ињективн.
12. Користећи карактеристичне функције, доказати скуповни идентитет: $(A \cap B \cap C) \setminus D = (A \setminus D) \cap (B \setminus D) \cap (C \setminus D)$.
13. Користећи карактеристичне функције доказати да је $(A \setminus B) \setminus C = (B \setminus C) \setminus A$ ако и само ако је $A \cup C = B \cup C$.
14. Користећи карактеристичне функције доказати да је $(A \setminus B) \setminus C = A \setminus B$ ако и само ако је $A \cap C \subseteq B$.

[7] Georg Cantor (1845-1918), немачки математичар

5 Коначни и бесконачни скупови

Дефиниција 5.1 *Скуп X је коначан ако има n елемената, где је n природни број. Ако скуп није коначан, кажемо да је бесконачан.*

Следеће тврђење ће бити представљено без доказа.

Тврђење 5.2 *Скуп X је бесконачан ако и само ако постоји прави подскуп $X' \subset X$ тако да су X и X' у бијекцији.* $\square$

Тврђење 5.3 *Скуп природних бројева је бесконачан.*

Доказ. Посматрајмо пресликавање $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ задато са $f(n) = n + 1$. Ако је $f(n) = f(n')$, онда је $n + 1 = n' + 1$, па и $n = n'$. То значи да је f инјективн. Нека је сада $n \in \mathbb{N} \setminus \{0\}$. Тада је елемент $n - 1 \in \mathbb{N}$. Важи да је $f(n-1) = (n-1) + 1 = n$, па је f и сурјективна. Дакле, скуп $\mathbb{N}$ је у бијекцији са својим правим подскупом, па мора бити бесконачан. $\square$

Дефиниција 5.4 *Скуп X је пребројив ако постоји бијекција $f : X \to \mathbb{N}$. Ако је скуп коначан или пребројив, онда кажемо да је највише пребројив. Ако скуп није највише пребројив кажемо да је непребројив.*

На пример, скуп $\mathbb{N}$ је пребројив. Наиме, функција $f : \mathbb{N} \to \mathbb{N}$ задата са $f(n) = n$ је бијекција.

Пример 5.5 *1. Скуп $\mathbb{Z}$ је пребројив.*

2. Скуп $\mathbb{N} \times \mathbb{N}$ је пребројив.

1. Дефинишимо пресликавање $f : \mathbb{N} \to \mathbb{Z}$ са:

$$f(n) = \begin{cases} k, & n = 2k \ (k = 0, 1, 2, \dots) \\ -k-1, & n = 2k+1 \ (k = 0, 1, 2, \dots) \end{cases}$$

Приметимо да је

$$\begin{array}{ll} 0 & \mapsto 0 \\ 1 & \longmapsto -1 \\ 2 & \mapsto 1 \\ 3 & \longmapsto -2 \\ 4 & \mapsto 2 \\ 5 & \longmapsto -3 \\ 6 & \mapsto 3 \\ & \dots \end{array}$$

Докажимо прво да је f "1-1". Нека је $f(n) = f(m)$. Ако су n и m парни, тада је $n = 2k_1$ и $m = 2k_2$, за неке $k_1, k_2 \in \mathbb{N}$. Онда је $f(n) = k_1$ и $f(m) = k_2$, па из претпостављене једнакости следи да је $k_1 = k_2$. Тиме је и $2k_1 = 2k_2$, па је $m = n$. Ако су n и m непарни, онда је $n = 2k_1 + 1$ и $m = 2k_2 + 1$, за $k_1, k_2 \in \mathbb{N}$. Тако да је $f(n) = -k_1 - 1$ и $f(m) = -k_2 - 1$, па је $-k_1 - 1 = -k_2 - 1$. Следи да је $k_1 = k_2$, а тиме и $n = m$. Још је остало проверити случај кад је један од бројева паран, а други непаран. Без умањења општости, претпоставимо да је n паран, а m непаран. Тада је $n = 2k_1$, а $m = 2k_1 + 1$. Следи да $k_1 = -k_2 - 1$, то јест $k_1 + k_2 = -1$, што је немогуће јер су бројеви k_1 и k_2 природни. Дакле, у сваком случају је закључак да је $m = n$, па је f инјекција.

Докажимо да је f "на". Нека је $m \in \mathbb{Z}$ приозвољан елемент. Треба пронаћи $n \in \mathbb{N}$, тако да $f(n) = m$. Ако је $m \geq 0$, онда је $f(n) = m$, за $n = 2m$. Ако је $m < 0$, ставимо $n = 2(-(m+1)) + 1$. Тада је $f(n) = -(-(m+1)) - 1 = m$.

Дакле, f је бијекција, па је $\mathbb{Z}$ пребројив.

2. Подсетимо се да је скуп $\mathbb{N}\times\mathbb{N} = \{(i,j) \mid i,j \in \mathbb{N}\}$. Можемо га представити и на следећи начин:

$$\begin{array}{ccccccccc}
(0,0) & & (0,1) & & (0,2) & & (0,3) & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \\
(1,0) & & (1,1) & & (1,2) & & (1,3) & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \\
(2,0) & & (2,1) & & (2,2) & & (2,3) & \cdots \\
& \swarrow & & \swarrow & & \swarrow & & \\
(3,0) & & (3,1) & & (3,2) & & (3,3) & \cdots \\
\vdots & \swarrow & \vdots & \swarrow & \vdots & \swarrow & \vdots & \ddots
\end{array}$$

Дефинишимо пресликавање $g : \mathbb{Z} \to \mathbb{N}$ тако да

$$\begin{array}{ccc}
(0,0) & \mapsto & 0 \\
(0,1) & \mapsto & 1 \\
(1,0) & \mapsto & 2 \\
(0,2) & \mapsto & 3 \\
(1,1) & \mapsto & 4 \\
(2,0) & \mapsto & 5 \\
\vdots & & \vdots
\end{array}$$

Дакле, додељујемо елементе скупа $\mathbb{N}$ елементима (i,j), почевши од $(0,0)$, у смеру дијагоналних стрелица, с лева на десно. Јасно је да скуп $\mathbb{N}\times\mathbb{N}$ можемо посматрати као низ: његов нулти члан је елемент $(0,0)$, први је $(0,1)$, други $(1,0)$, и тако даље. Приметимо да ако одредимо на ком месту у овом низу се налази елемент (i,j), онда знамо који природни број треба да му доделимо, да бисмо дефинисали пресликавање g. Пре елемента (i,j) у низу се налазе елементи који припадају дијагоналама од прве до $i+j$-те, као и елементи $(0,i+j),(1,i+j-1),\dots,(i-1,j+1)$. Видимо да k-та дијагонала има k елемената, док $i+j+1$-ва дијагонала до елемента (i,j) има i елемената. Тако да их пре елемента (i,j) има $1+2+\cdots+(i+j)+i$. Овај број је једнак $\frac{(i+j)(i+j+1)}{2}+i$. С обзиром на то да први елемент сликамо у нулу, (i,j) сликамо баш у број $\frac{(i+j)(i+j+1)}{2}+i$. Коначно, g је дефинисано са $g(i,j) = \frac{(i+j)(i+j+1)}{2}+i$. Формални доказ да је g бијекција ћемо прескочити.

$\triangle$

Тврђење 5.6 *Скуп свих коначних подскупова скупа природних бројева $\mathcal{P}_{fin}(\mathbb{N})$ јесте пребројив.*

Доказ. Дефинишимо функцију $f : \mathcal{P}_{\text{fin}}(\mathbb{N}) \to \mathbb{N}$ са:

$$\begin{aligned}
&f(\emptyset) = 0\\
&f(\{m_1,\dots,m_n\}) = 2^{m_1} + 2^{m_2} + \cdots 2^{m_n},
\end{aligned}$$

где је $\{m_1,\dots,m_n\} \subset \mathbb{N}$, такав да $m_i \neq m_j$, за $i \neq j$. Докажимо да је f инјекција. Нека је $f(\{m_1,\dots,m_k\}) = f(\{n_1,\dots,n_l\})$. У питању су природни бројеви и без умањења општости можемо претпоставити да је $m_1 > m_2 > \cdots > m_k$ и $n_1 > n_2 > \cdots > n_l$. Тада је $2^{m_1}+2^{m_2}+\cdots 2^{m_k} = 2^{n_1}+2^{n_2}+\cdots 2^{n_l}$. Претпоставимо да је $m_1 > n_1$. Користићемо једнакост $1+2^1+2^2+\cdots+2^i = 2^{i+1}-1$, која важи за свако $i \geq 1$; објашњење се може наћи у примеру 6.16. Пошто је $n_1 < m_1$, онда је $n_1+1 \leq m_1$, па је $2^{n_1+1} \leq 2^{m_1}$. Можемо закључити да је

$$2^{n_1}+2^{n_2}+\cdots 2^{n_l} \leq 2^{n_1}+2^{n_1-1}+\cdots 2^1+1 = 2^{n_1+1}-1 \leq 2^{m_1}-1 < 2^{m_1} \leq 2^{m_1}+2^{m_2}+\cdots 2^{m_k},$$

што је немогуће. Контрадикцију добијамо и ако претпоставимо да је $n_1 > m_1$. Дакле, мора бити $m_1 = n_1$. Тада је и $2^{m_1} = 2^{n_1}$, па можемо да скратимо овај сабирак у полазном збиру. Настављајући овај поступак добијамо да је $k = l$ и $m_i = n_i$ за свако $i \in \{1, \dots, k\}$. Доказали смо да је f "1-1", па је скуп $\mathcal{P}_{\text{fin}}(\mathbb{N})$ највише пребројив. Јасно је да коначних подскупова од $\mathbb{N}$ има бесконачно много, па $\mathcal{P}_{\text{fin}}(\mathbb{N})$ не може бити коначан. Дакле, наведени скуп је пребројив. $\square$

Тврђење 5.7 *Скуп реалних бројева $\mathbb{R}$ није пребројив.*

Доказ. Претпоставимо супротно: скуп $\mathbb{R}$ јесте пребројив. Како је функција $h : (0,1) \to \mathbb{R}$ задата са $h(x) = tg(\pi x - \frac{\pi}{2})$ бијекција, то је и скуп $(0,1)$ пребројив. Дакле, интервал $(0,1)$ је низ бројева $r_0, r_1, r_2, \dots$. Како сваки реални број можемо представити у децималном облику, на пример са $r_i = 0, x_{i0}x_{i1}x_{i2}\dots$, то је $(0,1)$ низ бројева:

$$\begin{array}{lcl} r_0 & = & 0, \boxed{x_{00}} x_{01}x_{02}x_{03}\dots \\ r_1 & = & 0, x_{10}\boxed{x_{11}} x_{12}x_{13}\dots \\ r_2 & = & 0, x_{20}x_{21}\boxed{x_{22}} x_{23}\dots \\ r_3 & = & 0, x_{30}x_{31}x_{32}\boxed{x_{33}} \dots \\ \vdots & & \vdots \end{array}$$

Уочимо елемент y задат са $y = 0, y_0y_1y_2\dots$, где је

$$y_i = \begin{cases} 1, & x_{ii} \neq 1 \\ 2, & x_{ii} = 1. \end{cases}$$

Добили смо елемент који припада скупу $(0,1)$, а није ниједан од $r_0, r_1, r_2, \dots$. То је немогуће, тако да скуп $\mathbb{R}$ не може бити пребројив. Како је скуп природних бројева бесконачан, а садржан је у скупу реалних бројева, то $\mathbb{R}$ није коначан, па је непребројив. $\square$

Теорема 5.8 *(Кантор - Бернштајнова[8] теорема) Ако постоји инјекција из X у Y и инјекција из Y у X, тада постоји бијекција између X и Y.*

Доказ. Због појединости овог доказа битно нам је да скупови X и Y буду дисјунктни. Ако нису, онда то сигурно важи за скупове $X \times \{0\}$ и $Y \times \{1\}$. Може се доказати да је X у бијекцији са $X \times \{0\}$, као и да је Y у бијекцији са $Y \times \{1\}$. Тако да ако постоји бијекција између $X \times \{0\}$ и $Y \times \{1\}$, онда сигурно постоји бијекција измађу X и Y. Тако да, без умањења општости, можемо претпоставити да су X и Y дисјунктни.

Нека су елементи $x \in X$ и $y \in Y$ такви да $f(x) = y$. Због једноставнијег изражавања у доказу, елемент x можемо звати родитељем елемента y. Слично, ако је $g(y') = x'$, кажемо да је y' родитељ елемента x'. Како су функције f и g инјекције, сваки елемент може имати највише једног родитеља. Назовимо $(z_0, z_1, \dots, z_n)$ низом предака за елемент z_0 ако је за сваки $i \in \{1, 2, \dots, n\}$ z_i родитељ за z_{i-1}. За било који елемент скупа X или Y важи да је максимална дужина његовог ланца предака паран или непаран број или да је његов ланац предака бесконачан. Означимо са $X_{\text{пар}}$ скуп свих елемената у X чији је максимални ланац предака паран број. Слично за $X_{\text{непар}}$ и X_∞. Тада је $X = X_{\text{пар}} \sqcup X_{\text{непар}} \sqcup X_\infty$. Takође је $Y = Y_{\text{пар}} \sqcup Y_{\text{непар}} \sqcup Y_\infty$. Сетимо се да ако за функцију $F : A \to B$ важи да $F[A] = B$, онда је F сурјекција. Приметимо да је

$$f[X_\infty] = Y_\infty \qquad f[X_{\text{пар}}] = Y_{\text{непар}} \qquad g[Y_{\text{пар}}] = X_{\text{непар}}.$$

[8] Felix Bernstein (1878-1956), немачки математичар

Тако да су рестрикције функције f на скупове X_∞ и $X_{\text{пар}}$ и рестрикција функције g на $Y_{\text{пар}}$ бијекције. Функцију $h : X \to Y$ дефинишимо са

$$h(x) = \begin{cases} f(x), & x \in X_{\text{пар}} \sqcup X_\infty \\ g^{-1}(x), & x \in X_{\text{непар}}. \end{cases}$$

Јасно је да је h тражена бијекција између скупова X и Y. $\square$

Пример 5.9 *Скуп $\mathbb{Q}$ је пребројив.*

Докажимо прво да је скуп $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ пребројив. Нека је $f : \mathbb{N} \to \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ дефинисана са $f(n) = (0, n+1)$, за $n \in \mathbb{N}$. Функција f је "1-1": ако је $f(n) = f(m)$, онда је $(0, n+1) = (0, m+1)$, па је $n = m$. Нека је $g : \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \to \mathbb{N}$ таква да

$$g(m, n) = \begin{cases} 2^{2|m|+1}3^n, & m < 0 \\ 2^{2m}3^n, & m \geq 0. \end{cases}$$

Докажимо и да је g "1-1". Нека је $g(m_1, n_1) = g(m_2, n_2)$, где су $m_1, m_2 \in \mathbb{Z}$ и $n_1, n_2 \in \mathbb{N} \setminus \{0\}$. Ако су m_1 и m_2 негативни, тада је $2^{2|m_1|+1}3^{n_1} = 2^{2|m_2|+1}3^{n_2}$. Тада мора бити $n_1 = n_2$ и $2|m_1| + 1 = 2|m_2| + 1$. Како су $m_1, m_2 < 0$, следи да је $m_1 = m_2$. Дакле, важи $(m_1, n_1) = (m_2, n_2)$. Ако су m_1, m_2 ненегативни, на сличан начин добијамо $(m_1, n_1) = (m_2, n_2)$. Ако је $m_1 < 0$, а $m_2 \geq 0$, онда је $2^{2|m_1|+1}3^{n_1} = 2^{2m_2}3^{n_2}$. Следи да је $2|m_1|+1 = 2m_2$, то јест $-2m_1+1 = 2m_2$. Ово би значило да је $2(m_1 + m_2) = 1$, што је немогуће јер је $m_1 + m_2$ цео број. У сваком случају је $(m_1, n_1) = (m_2, n_2)$, па је g "1-1".

Дакле, постоји инјекција из $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ у $\mathbb{N}$ и инјекција из $\mathbb{N}$ у $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$. Према теореми 5.8, постоји бијекција између ова два скупа. Дефинишимо сада пресликавање $h : \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \to \mathbb{Q}$ са $h(m, n) = \frac{m}{n}$. Јасно је да је h "на" пресликавање, па елемемата у $\mathbb{Q}$ не може бити више него у $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$, то јест има их највише пребројиво много. Како је $\mathbb{N} \subset \mathbb{Q}$ и $\mathbb{N}$ је бесконачан, то $\mathbb{Q}$ не може бити коначан. Дакле, $\mathbb{Q}$ је пребројив. $\triangle$

Пример 5.10 *Доказати да је скуп $2\mathbb{N} = \{0, 2, 4, \dots\}$ пребројив.*

Нека је $f : \mathbb{N} \to 2\mathbb{N}$ функција таква да $f(n) = 2n$. Дакле,

$$f : \qquad 0 \mapsto 0 \qquad 1 \mapsto 2 \qquad 2 \mapsto 4 \cdots$$

Нека је $f(n) = f(m)$, за $m, n \in \mathbb{N}$. Тада је $2n = 2m$, па је $n = m$. То значи да је f "1-1". Нека је $k \in 2\mathbb{N}$ било који елемнент. Следи да је $k = 2n$, за неко $n \in \mathbb{N}$. Важи да је $f(n) = 2n = k$, па је функција f "на". Дакле, f је бијекција.

Задаци

1. Доказати да је скуп $\mathbb{N}_{\geq 5} = \{5, 6, 7, \dots\}$ пребројив.
2. Доказати да је скуп $\mathbb{N} \setminus \{1, 3\}$ пребројив.
3. Доказати да је скуп $\{0, 1\} \times \mathbb{N}$ пребројив.
4. Доказати да је скуп $\{0, 1\} \times \{2, 3, 4\} \times \mathbb{N}$ пребројив.

6 Бројеви

Прве аксиоме теорије природних бројева су увели Пеано[9] и Дедекинд крајем 19. века. Докажимо за почетак пар тврђења која ће нам касније бити потребна.

[9] Giuseppe Peano (1858-1932), италијански математичар

Тврђење 6.1 *а) Не постоји скуп x тако да је $x \in x$.*
б) Не постоје скупови x и y тако да $x \in y$ и $y \in x$.
в) Не постоји низ скупова $x_0, x_1, x_2, \dots$, тако да је $x_0 \ni x_1 \ni x_2 \ni \dots$.

Доказ. а) Претпоставимо да је $x \in x$ за неки x . Посматрајмо скуп $A = \{x\}$. Из $x \in x$ и $x \in A$ следи да је $A \cap x \neq \emptyset$. Према аксиоми доброг заснивања, постоји $a \in A$ тако да $A \cap a = \emptyset$. С друге стране, једини елемент у A је x. Добили смо контрадикцију због аксиоме регуларности.
б) Нека је $x \in y$ и $y \in x$, за неке x и y. Нека је $A = \{x, y\}$. Како је $x \in A$ и $x \in y$, следи да је $A \cap y \neq \emptyset$. Такође, из $y \in A$ и $y \in x$ следи да $A \cap x \neq \emptyset$. Једини елементи у A су x и y, па опет добијамо противречност са аксиомом регуларности.
в) Претпоставимо да постоји такав низ и нека је скуп $A = \{x_0, x_1, x_2, \dots\}$. Како је $x_1 \in A$ и $x_1 \in x_0$, важи $A \cap x_0 \neq \emptyset$. Даље, из $x_2 \in A$ и $x_2 \in x_1$ следи $A \cap x_1 \neq \emptyset$. Настављајући овај поступак видимо да мора бити $A \cap x_i \neq \emptyset$, за све i. Као и у претходним доказима, због тога како је дефинисан скуп A добијамо контрадикцију са аксиомом регуларности. □

Тврђење 6.2 *Ако је $x \cup \{x\} = y \cup \{y\}$, онда је $x = y$.*

Доказ. Претпоставимо супротно: нека је $x \neq y$. Како је $x \in x \cup \{x\} = y \cap \{y\}$, то је $x \in y$ или $x \in \{y\}$, заправо $x \in y$ или $x = y$. Због претпоставке, мора бити $x \in y$. С друге стране из $y \in y \cup \{y\} = x \cup \{x\}$ следи да је $y \in x$ или $y = x$. Дакле, $y \in x$. Закључили смо да је $x \in y$ и $y \in x$. Због тврђења 6.2, ово је контрадикција. □

Пеанове аксиоме гласе овако:

П1 0 је природан број.

П2 Ако је x природан број, онда је и x' природан број.

П3 Ако су x и y природни бројеви и $x' = y'$, онда је $x = y$.

П4 За сваки природан број x, $x' \neq 0$.

П5 Нека је Φ својство природних бројева за које важи:

1) 0 има својство Φ;
2) Ако природан број x има својство Φ, тада и x' има својство Φ.

Тада сваки природни број има својство Φ.

У Пеановим аксиомама јављају се симболи 0 и $'$, где је 0 симбол константе, а $'$ унарни функцијски симбол. Приметимо да Пеанове аксиоме само описују својства природних бројева, али не говоре на коју структуру тачно се односе. Моделом природних бројева називамо било коју тројку $(N, 0, ')$ која задовољава те аксиоме. Један од познатијих модела природних бројева је Фон Нојманов[10] модел, који се ослања на теорију скупова. Наиме, природне бројеве можемо дефинисати на следћи начин:

$$0 := \emptyset,\ 1 := \{0\},\ 2 := \{0, 1\},\ 3 := \{0, 1, 2\}, \dots$$

Прецизније, $0 := \emptyset,\ n' = n \cup \{n\}$ и $\mathbb{N} := \{0, 1, 2, \dots\}$.

Теорема 6.3 *Фон Нојманов модел природних бројева задовољава Пеанове аксиоме.*

[10] John von Neumann (1903-1957), мађарски математичар

Доказ. Како је $0 \in N$ и ако је $n \in N$ онда је и $n' \in N$, тиме су задовољене аксиоме П1 и П2. Такође, јасно је да за сваки $n \in N$ $n' \neq 0$, што је П4. Проверимо аксиому П3. Нека су m и n природни бројеви тако да $m' = n'$. То значи да је $m \cup \{m\} = n \cup \{n\}$. Према тврђењу 6.2 важи $m = n$.

Нека је Φ произвољно својство природних бројева. Претпоставимо да је $\Phi(0)$ тачно (или да 0 има својство Φ) и да је $\forall x\,(\Phi(x) \Rightarrow \Phi(x'))$. Да бисмо доказали да важи П5, треба доказати да је, уз наведене претпоставке, $\Phi(n)$ тачно за сваки $n \in N$. Претпоставимо супротно: постоји $n \in N$ тако да није тачно $\Phi(n)$. То значи да n није 0. Приметимо да у Фон Нојмановом моделу важи следеће: $\forall n(n \neq \emptyset \Rightarrow \exists m\ n = m')$. Дакле, постоји природан број m тако да $n = n_1'$ и тиме је и нетачно $\Phi(n_1')$. Користећи претпоставку имамо да је нетачно и $\Phi(n_1)$. Слично, постоји n_2 тако да $n_1 = n_2'$ и није тачно $\Phi(n_2)$. На тај начин добијамо $n \ni n_1 \ni n_2 \ni \ldots$, што је немогуће према тврђењу 6.1. $\Box$

Можемо приметити да се у Фон Нојмановом моделу релација неједнакости између природних бројева поклапа са скуповном релацијом припадања, то јест важи $x < y$ ако и само ако $x \in y$ за све $x, y \in N$. Принцип најмањег елемента за природне бројеве

Из аксиоме индукције можемо извести још једно битно тврђење које нам омогућава извођење доказа о природним бројевима. Код тог тврђења, које називамо Принципом потпуне индукције, индуктивна хипотеза се састоји од свих исказа $\Phi(0), \Phi(1), \ldots, \Phi(n-1)$.

Теорема 6.4 ***Принцип потпуне индукције*** *Нека је Φ неко својство природних бројева. Тада се из Пеанових аксима може извести*

$$\forall n((\forall k < n)\Phi(k) \Rightarrow \forall n \Phi(n).$$

Дефинишимо операцију сабирања природних бројева:

Дефиниција 6.5 *За природне бројеве x и y је:*

$$\begin{aligned} x + 0 &:= x \\ x + y' &:= (x + y)'. \end{aligned}$$

Тврђење 6.6 *За све природне бројеве x, y и z важи:*

1. $(x + y) + z = x + (y + z)$
2. $x + 0 = 0 + x = x$
3. $x + 1 = 1 + x$
4. $x + y = y + x$
5. $x + y = 0 \Rightarrow x = 0 \vee y = 0$
6. $x + z = y + z \Rightarrow x = y$

Доказ.

1. Доказујемо индукцијом по z. Ако је $z = 0$, онда је по дефиницији сабирања
$$(x + y) + 0 = (x + y) \qquad y + 0 = 0.$$
Дакле, важи
$$(x + y) + 0 = x + y = x + (y + 0).$$

Претпоставимо да је $(x+y)+z = x+(y+z)$. Докажимо $(x+y)+z' = x+(y+z')$.

$$
\begin{array}{rcll}
(x+y)+z' & = & ((x+y)+z)' & \text{по дефиницији сабирања} \\
 & = & (x+(y+z))' & \text{по индуктивној претпоставци} \\
 & = & x+(y+z)' & \text{по дефиницији сабирања} \\
 & = & x+(y+z') & \text{по дефиницији сабирања.}
\end{array}
$$

2. По дефиницији је $x+0=x$. Индукцијом по x доказујемо $0+x=x$. Важи $0+0=0$. Претпоставимо $0+x=x$. Тада је $0+x'=(0+x)'=x'$.

3. Из низа једнакости

$$x+1 = x+0' = (x+0)' = x'$$

имамо да је $x+1=x'$. Тражену једнакост ћемо доказати индукцијом по x. За $x=0$ важи

$$1+0 = 1 = \text{ (дефиниција сабирања) } = 0+1 \text{ (особина 2).}$$

Нека је $x+1=1+x$. Тада је

$$
\begin{array}{rcll}
1+x' & = & (1+x)' & \text{по дефиницији сабирања} \\
 & = & (x+1)' & \text{по индуктивној претпоставци} \\
 & = & x+1' & \text{по дефиницији сабирања} \\
 & = & x+(1+1) & \text{јер важи } x'=x+1 \\
 & = & (x+1)+1 & \text{особина 1} \\
 & = & x'+1 & \text{јер важи } x'=x+1
\end{array}
$$

4. Користићемо индукцију по y. Према дефиницији и особини 2 редом, важи

$$x+0=x \qquad 0+x=x,$$

па је $x+0=0+x$. Ако је $x+y=y+x$, имамо да је

$$
\begin{array}{rcl}
x+y' & = & (x+y)' = (y+x)' = y+x' \\
 & = & y+(x+1) = y+(1+x) = (y+1)+x \\
 & = & y'+x.
\end{array}
$$

На сличан начин се докажу и тврђења 4 и 5. □

Дефинишимо сада операцију множења природних бројева:

Дефиниција 6.7 *За природне бројеве x и y је:*

$$
\begin{array}{rcl}
x \cdot 0 & := & 0 \\
x \cdot y' & := & x \cdot y + x.
\end{array}
$$

Тврђење 6.8 *За све природне бројеве x, y и z важи:*

1. $x \cdot (y+z) = x \cdot y + x \cdot z$
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
3. $0 \cdot x = 0$
4. $1 \cdot x = x$
5. $(x+y) \cdot z = x \cdot z + y \cdot z$
6. $x \cdot y = y \cdot x$

7. $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Доказ.

1. Индукцијом по z:

$$x \cdot (y+0) = x \cdot y = x \cdot y + 0 = x \cdot y + x \cdot 0.$$

Претпоставимо да је $x \cdot (y+z) = x \cdot y + x \cdot z$. Тада је

$$\begin{aligned} x \cdot (y+z') &= x \cdot (y+z)' = x \cdot (y+z) + x \\ &= (x \cdot y + x \cdot z) + x = x \cdot y + (x \cdot z + x) \\ &= x \cdot y + x \cdot z'. \end{aligned}$$

2. Индукцијом по z:

$$(x \cdot y) \cdot 0 = 0 = x \cdot 0 = x \cdot (y \cdot 0).$$

Претпоставимо да је $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Тада је

$$\begin{aligned} (x \cdot y) \cdot z' &= (x \cdot y) \cdot z + x \cdot y = x \cdot (y \cdot z) + x \cdot y = x \cdot (y \cdot z + y) \\ &= x \cdot (y \cdot z'). \end{aligned}$$

□

Дефиниција 6.9 *За бројеве $x, y \in \mathbb{N}$ за које је $x = y + z$, за неко $z \in \mathbb{N}$, дефинишемо разлику броја x и броја y као $x - y \stackrel{\text{def}}{=} z$.*

Приметимо да одузимање није операција на скупу природних бројева, јер разлика $x-y$ није дефинисана за све $x, y \in \mathbb{N}$. На пример, не постоји природни број z тако да је $1 = 3 + z$.

Математичка индукција представља важан метод за доказивање тврђења која се односе на природне бројеве. Подсетимо се како гласи:

Принцип математичке индукције Нека је Φ својство природних бројева за које важи:

1) тачно је $\Phi(0)$;

2) ако за природни број n тачно $\Phi(n)$, онда и тачно и $\Phi(n+1)$.

Тада је за сваки природни број n тачно $\Phi(n)$.

Услов 1. се назива база индукције, а услов 2. индуктивни корак. Формула $\Phi(n)$ у индуктивном кораку се назива индуктивна претпоставка. Има аритметичких тврђења која нису тачна за неколико најмањих природних бројева, али су тачна за све остале. У тим случајевима можемо користити мало измењени принцип матаматичке индукције, који гласи овако:

Нека је Φ својство природних бројева за које важи:

1) тачно је $\Phi(k)$;

2) ако за природни број $n \geq k$ тачно $\Phi(n)$, онда и тачно и $\Phi(n+1)$.

Тада је за сваки природни број $n \geq k$ тачно $\Phi(n)$.

Пример 6.10 *Користећи математичку индукцију доказати да за сваки природни број $n \geq 1$ важи идентитет*

$$1 + \cdots + n = \frac{n(n+1)}{2}.$$

Нека је $\Phi(n) : 1+\cdots+n = \frac{n(n+1)}{2}$. Проверавамо базу индукције: $\Phi(1) : 1 = \frac{1(1+1)}{2}$. Јасно је да је то тачан исказ, па је испуњен услов 1. Приметимо да овде користимо принцип математичке индукције, у коме је база индукције исказ $\Phi(k)$; у нашем случају је $k = 1$.

Даље, претпоставимо да је тачан исказ $\Phi(n) : 1+\cdots+n = \frac{n(n+1)}{2}$, за природан број $n \geq 1$. Треба доказати да је тачан исказ $\Phi(n+1) : 1+\cdots+n+(n+1) = \frac{(n+1)((n+1)+1)}{2}$. Важи следеће:

$$
\begin{aligned}
1+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1) \text{ користећи индуктивну претпоставку} \\
&= (n+1)(\frac{n}{2}+1) \\
&= (n+1)\frac{n+2}{2} \\
&= \frac{(n+1)((n+1)+1)}{2}.
\end{aligned}
$$

Овим смо доказали да је тачна импликација у индуктивном кораку, па према принципу математичке индукције наведена једнакост важи за све бројеве $n \geq 1$. △

Пример 6.11 *Доказати да је за све природне бројеве тачно да* $2^n > n$.

Овде је $\Phi(n) : 2^n > n$. За $n = 0$ исказ $\Phi(0)$ је $2^0 > 0$, што је тачно. Претпоставимо да је тачно $2^n > n$. Докажимо да је $2^{n+1} > n+1$. Важи да $2^{n+1} = 2 \cdot 2^n > 2n$, због индуктивне претпоставке. Такође је $2n \geq n+1$ еквивалентно са $n \geq 1$, што је тачно, па је и

$$2^{n+1} > 2n \geq n+1 \Rightarrow 2^{n+1} > n+1.$$

Дакле, важе услеви 1. и 2., па је $2^n > n$ за све природне бројеве. △

Пример 6.12 *Доказати да је број* $5^n + 2^{n+1}$ *дељив са 3, за све* $n \in \mathbb{N}$.

Ставимо да је $\Phi(n) :$ број $5^n + 2^{n+1}$ је дељив са 3. Број $5^0 + 2^{0+1} = 1+2 = 3$ је дељив са 3, па је тачно $\Phi(0)$. Претпоставимо да је број $5^n + 2^{n+1}$ дељив са 3. Докажимо да је $5^{n+1} + 2^{(n+1)+1}$ дељив са 3. Важи

$$5^{n+1} + 2^{(n+1)+1} = 5 \cdot 5^n + 2 \cdot 2^{n+1} = (3+2)5^n + 2 \cdot 2^{n+1} = 3 \cdot 5^n + 2(5^n + 2^{n+1}).$$

Број $2(5^n + 2^{n+1})$ је дељив са 3, јер је према индуктивној претпоставци $5^n + 2^{n+1}$ дељив са 3. Такође је број $3 \cdot 5^n$ дељив са 3, па и збир та два броја $3 \cdot 5^n + 2(5^n + 2^{n+1})$ дељив са 3. Дакле, $5^{n+1} + 2^{(n+1)+1}$ је дељив са 3. Тврђење је доказано. △

Пример 6.13 *Последња цифра броја* $2^{2^n} + 1$ *је 7, за све бројеве* $n \geq 2$.

Опишимо дати исказ као $\Phi(n) :$ последња цифра броја $2^{2^n}+1$ је 7. Важи да је $2^{2^2} + 1 = 16+1 = 17$, па је последња цифра 7, чиме је доказана база индукције $\Phi(2)$. Претпоставимо да је тачно $\Phi(n)$. Тада је 6 последња цифра броја 2^{2^n}. Можемо закључити и да је последња цифра квадрата тог броја такође 6. Дакле, $(2^{2^n})^2 = 2^{2^n \cdot 2} = 2^{2^{n+1}}$ се завршава са 6, па је последња цифра броја $2^{2^{n+1}} + 1$ 7. Дакле, доказан је индуктивни корак. △

Може се доказати и следећа варијанта принципа математичке индукције, коју називамо индукција са $k+1$ хипотеза.

Нека је Φ својство природних бројева за које важи:

1) тачни су искази $\Phi(0), \ldots, \Phi(k)$;

2) ако су за природни број n тачни искази $\Phi(n), \Phi(n+1), \ldots, \Phi(n+k)$, онда и тачно и $\Phi(n+k+1)$.

Тада је за сваки природни број n тачно $\Phi(n)$.

Пример 6.14 *Нека је $a_0 = 2, a_1 = 5$ и за све $n \geq 0$ важи формула $a_{n+2} = 5a_{n+1} - 6a_n$. Доказати да је $a_n = 2^n + 3^n$, за све $n \geq 0$.*

Користићемо претходно тврђење за $k = 1$, то јест индукцију са две хипотезе. За почетак, означимо са $\Phi(n) : a_n = 2^n + 3^n$. Искази $\Phi(0) : a_0 = 2^0 + 3^0 = 1 + 1 = 2$ и $\Phi(1) : a_1 = 2^1 + 3^1 = 2 + 3 = 5$ су тачни, јер је $a_0 = 2, a_1 = 5$ према тексту задатка. Дакле, доказана је база индукције. Претпоставимо да су тачни искази $\Phi(n)$ и $\Phi(n+1)$. То значи да је $a_n = 2^n + 3^n$ и $a_{n+1} = 2^{n+1} + 3^{n+1}$. Треба доказати да је $a_{n+2} = 2^{n+2} + 3^{n+2}$. Према формули у тексту, важи

$$\begin{aligned}
a_{n+2} &= 5a_{n+1} - 6a_n \\
&= 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n) \\
&= 5 \cdot 2^{n+1} + 5 \cdot 3^{n+1} - 6 \cdot 2^n - 6 \cdot 3^n \\
&= 2^n(5 \cdot 2 - 6) + 3^n(5 \cdot 3 - 6) \\
&= 2^n \cdot 4 + 3^n \cdot 9 \\
&= 2^n 2^2 + 3^n 3^2 \\
&= 2^{n+2} + 3^{n+2}.
\end{aligned}$$

Дакле, доказали смо и услов 2, па важи да је тачно $\Phi(n)$ за сваки $n \geq 0$. $\triangle$

Пример 6.15 *Аритметички низ је низ реалних бројева x_n одређен формулама $x_0 = a$, $x_{n+1} = x_n + d$, где су $a, d \in \mathbb{R}$. Одредити општи члан x_n тог низа и суму првих $n+1$ чланова $S_n = \sum_{i+0}^{n} x_i$.*

Тачне су једнакости:

$$\begin{aligned}
x_0 &= a \\
x_1 - x_0 &= d \\
x_2 - x_1 &= d \\
&\vdots \\
x_n - x_{n-1} &= d.
\end{aligned}$$

Сабирајући их добијамо

$$x_0 + (x_1 - x_0) + (x_2 - x_1) + \cdots + (x_n - x_{n-1}) = a + nd,$$

а скраћивањем одговарујућих чланова x_i закључујемо да је $x_n = a + nd$.

$$S_n = \sum_{i+0}^{n} x_i = \sum_{i=0}^{n} (a + id) = \sum_{i=0}^{n} a + d \sum_{i=0}^{n} i = (n+1)a + \frac{n(n+1)}{2} d = \frac{(n+1)(2a + nd)}{2}.$$

$\triangle$

Пример 6.16 *Геометријски низ је низ реалних бројева y_n одређен формулама $y_0 = b$, $y_{n+1} = y_n \cdot q$, где су $b, q \in \mathbb{R}$. Одредити општи члан y_n тог низа и суму првих $n+1$ чланова $S_n = \sum_{i+0}^{n} y_i$.*

Ако је $b = 0$, онда је и $y_n = 0$ и $S_n = 0$. Ако је $q = 0$, онда је $y_n = 0$, за $n > 0$ и $S_n = b$. Зато можемо претпоставити да је $b, q \neq 0$. Тада је

$$\begin{aligned} y_0 &= b \\ \frac{y_1}{y_0} &= q \\ \frac{y_2}{y_1} &= q \\ &\vdots \\ \frac{y_n}{y_{n-1}} &= q. \end{aligned}$$

Множећи претходне једнакости добијамо

$$y_0 \cdot \frac{y_1}{y_0} \cdot \frac{y_2}{y_1} \cdots \frac{y_n}{y_{n-1}} = b \cdot q^n,$$

а скраћивањем одговарујућих чланова y_i закључујемо да је $y_n = b \cdot q^n$. Ако је $q = 1$, онда је $y_n = b$ за свако n, па је и $S_n = (n+1)q$. Ако је $q \neq 1$, онда је

$$\begin{aligned} S_n &= \sum_{i+0}^{n} y_i = \sum_{i=0}^{n} (b \cdot q^i) = b(\sum_{i=0}^{n} q^i) = b(1 + q + q^2 + \cdots q^n) \cdot \frac{q-1}{q-1} \\ &= b\frac{q + q^2 + q^3 + \cdots + q^n + q^{n+1} - 1 - q - q^2 - q^3 - \cdots - q^n}{q-1} = b\frac{q^n - 1}{q-1}. \end{aligned}$$

△

Пример 6.17 *Нека је $a_0 = 1$ и за свако $n \geq 1$ важи формула $a_n = a_{n-1} + a_{n-2} + \cdots + a_1 + 2a_0$. Доказати да је $a_n = 2^n$ за сваки природни број n.*

Користићемо принцип потпуне индукције 6.4. Ставимо $\Phi(n) : a_n = 2^n$. Јасно је да за задати члан a_0 важи да је $a_0 = 2^0 = 1$. Претпоставимо да су тачни искази $\Phi(1), \ldots, \Phi(n-1)$. Тада је $a_1 = 2^1$, $a_2 = 2^2, \ldots, a_{n-1} = 2^{n-1}$. Докажимо да је тачно $\Phi(n)$. Према формули је $a_n = a_{n-1} + a_{n-2} + \cdots + a_1 + 2a_0 = 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2^1 + 2 \cdot 1$. Приметимо да је последњи израз сума геометријског низа са почетним чланом 2 и количником 2 увећана за $2 \cdot 1$, тако да је

$$a_n = S_{n-1} + 2 = b\frac{q^{n-1} - 1}{q-1} + 2 = 2\frac{2^{n-1} - 1}{2-1} + 2 = 2^n + 2 - 2 = 2^n.$$

Дакле, закључак је да је тачно $\Phi(n)$ за свако $n \in \mathbb{N}$. △

Пример 6.18 *Нека је низ реалних бројева x_n , $n \in \mathbb{N}$ задат формулама $x_0 = \alpha$, $x_{n+1} = \lambda + \mu x_n$, где су $\alpha, \lambda, \mu \in \mathbb{R}$.Одредити општи члан овог низа.*

Првих пар чланова низа x_n је:

$$\begin{aligned} x_0 &= \alpha \\ x_1 &= \lambda + \mu x_0 = \lambda + \alpha\mu \\ x_2 &= \lambda + \mu x_1 = \lambda + \mu(\lambda + \alpha\mu) = \lambda + \lambda\mu + \alpha\mu^2 \\ x_3 &= \lambda + \mu x_2 = \lambda + \mu(\lambda + \lambda\mu + \alpha\mu^2) = \lambda + \lambda\mu + \lambda\mu^2 + \alpha\mu^3 \end{aligned}$$

Одавде можемо наслутити да је

$$\begin{aligned} x_n &= \lambda + \lambda\mu + \lambda\mu^2 + \cdots + \lambda\mu^{n-1} + \alpha\mu^n, \quad \text{за } n = 1, 2, 3 \ldots \\ x_n &= \alpha\mu^n + \lambda(1 + \mu + \mu^2 + \cdots + \mu^{n-1}). \end{aligned}$$

Докажимо једнакост индукцијом:

$$n = 1 : x_1 = \lambda + \mu x_0 = \lambda + \alpha\mu = \lambda + \alpha\mu^1$$

$x_{n+1} = \lambda+\mu x_n = \lambda+\mu(\alpha\mu^n+\lambda(1+\mu+\mu^2+\cdots+\mu^{n-1}) = alpha\mu^{n+1}+\lambda(1+\mu+\mu^2+\cdots+\mu^n)$
Ако је $\mu \neq 1$

$$(\alpha + \frac{\lambda}{\mu - 1})\mu^n - \frac{\lambda}{1 - \mu}$$

△

Пример 6.19 *Аутомобил кошта 12000 €. Од банке се може узети кредит по следећим условима: уче71е је 20% и камата на месечном нивоу је 1%.*

1. *Колики је износ месечне рате ако купац жели да исплати кредит у 40 једнаких рата? Колика је укупна камата за овако договорен кредит?*
2. *Купац жели да износ месечне рате буде 200 €. У колико рата ће исплатити новац банци?*
3. *Који је најмањи износ рате?*

Уведимо ознаке:

$$\begin{aligned}
S &= 12000 \text{ вредност аутомобила}\\
q &= 0.01 \ \text{ месечна камата}\\
d &= 0.2 \cdot 12000 = 2400 \ \text{ уче71е}\\
S' &= S - d = 9600 \ \text{ износ кредита}\\
m &= 40 \ \text{ број рата}\\
x_n &= \text{износ преосталог кредита после } n \text{ месеци}\\
r &= ? \ \text{ месечна рата}
\end{aligned}$$

1. После $n + 1$. месеца преостали износ је преостали износ из претходног месеца увећан за месечну камату минус исплаћена рата: $x_{n+1} = x_n + qx_n - r$. Дакле, добијамо једначину

   $$x_{n+1} = (1 + q)x_n - r, \qquad x_0 = S'.$$

   Користећи ознаке из претходног примера:

   $$\alpha = x_0 = S' \qquad \lambda = -r \qquad \mu = 1 + q.$$

   Опште решење ове једначине је

   $$x_n = (\alpha + \frac{\lambda}{\mu - 1})\mu^n - \frac{\lambda}{1 - \mu} = (S' - \frac{r}{q})(1 + q)^n + \frac{r}{q}.$$

   Услов за исплату кредита у m рата је $x_m = 0$. Дакле

   $$x_m = (S' - \frac{r}{q})(1 + q)^m + \frac{r}{q} = 0,$$

   одакле добијамо да је $r = \frac{qS'}{1-(1+q)^{-m}}$, то јест $r = \frac{0.01\cdot 9600}{1-1.01^{-40}} \approx 292.37$€. Укупан износ који је купац исплатио банци је $S'' = m \cdot r = 40 \cdot 292.37 = 11694.8$, што значи да је исплаћена камата једнака $K = S''-S' = 11694.8-9600 = 2094.8$€.

2. Из услова $x_{m=0}$ добијамо $(S' - \frac{r}{q})(1 + q)^m + \frac{r}{q} = 0$, то јест $m = -\frac{\log(1-\frac{qS'}{r})}{, log(1+q)}$. Даље је $m = -\frac{\log(1-\frac{0.01\cdot 9600}{200})}{\log(1+0.01)} \approx 65.72$. Дакле, купац треба да плати 65 рата по 200€ и 66. рату у износу 144€.

3.

$\triangle$

Пример 6.20 *Нека је $S\{l_1, l_2, \ldots, l_n\}$ скуп од n правих у равни тако да се сваке две секу и никоје три се не секу у истој тачки. Нека је A_n број ограничених, а B_n број неограничених делова равни које те праве одређују. Одредити A_n и B_n. Упоредити те бројеве.*

$$\begin{aligned} A_{n+1} &= A_n + (n-1) \qquad k_1 = 0 \\ B_{n+1} &= B_n + 2 \qquad B_1 = 2 \end{aligned}$$

$$\sum_{i=1}^{n} A_{i+1} = \sum_{i=1}^{n} (A_i + (i-1))$$

$$\sum_{i=2}^{n+1} A_n = \sum_{i=1}^{n} A_i + \sum_{i=1}^{n} (i-1)$$

$$A_{n+1} + \sum_{i=2}^{n} A_i = A_1 + \sum_{i=2}^{n} A_i + \frac{n(n-1)}{2}$$

Добијамо да је $A_{n+1} = \frac{n(n-1)}{2}$ то јест $A_n = \frac{(n-1)(n-2)}{2}$. $B_n = 2n$. Важи $A_n < B_n$ за $1 \leq n \leq 6$ и $A_n > B_n$ за $n \geq 7$. $\triangle$

Пример 6.21 *Дато је n кружница у равни тако да се сваке две секу у тачно две тачке и никоје три се не секу у истој тачки. Одредити број ограничених делова равни које те кружнице одређују.*

$\triangle$

Дефиниција 6.22 *Фибоначијев[11] низ је низ природних бројева f_n задат са*

$$f_0 = 0 \qquad f_1 = 1 \qquad f_{n+2} = f_{n+1} + f_n, \text{ за све природне бројеве } n.$$

Дакле, задата су прва два члана низа, а сваки следећи је збир претходна два. Почетак тог низа изгледа овако: 0,1,1,2,3,5,8,13,21,54...

Пример 6.23 *Доказати да је $f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$, за све $n \geq 0$.*

Доказаћемо идентитет користећи математичку индукцију. За $n = 0$ важи $f_0 = 0 = 1 - 1 = f_2 - 1$, па имамо базу индукције. Претпоставимо да је тачна једнакост $f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$. Докажимо да је $f_0 + f_1 + f_2 + \cdots + f_n + f_{n+1} = f_{n+3} - 1$. Важи

$$f_0 + f_1 + f_2 + \cdots + f_n + f_{n+1} = f_{n+2} - 1 + f_{n+1} = f_{n+3} - 1,$$

при чему смо прву једнакост собили из индуктивне претпоставке, а другу из дефиниције Фибоначијевих бројева.

[11] Leonardo Fibonacci (1170-1250), италијански математичар

6.1 Дељивост

Дефиниција 6.24 *Нека су $a, b \in \mathbb{N}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{N}$ тако да је $b = a \cdot c$.*

На овај начин смо дефинисали једну релацију на скупу природних бројева. Зовемо је релацијом дељивости.

Теорема 6.25 *Релација $\mid$ је релација парцијалног поретка на скупу $\mathbb{N}$.*

Доказ. Нека је a било који природни број. Тада је $a = 1 \cdot a$, па важи да $a \mid a$. То значи да је реација $\mid$ рефлексивна.

Докажимо антисиметричност. Нека су $a, b \in \mathbb{N}$ и $a \mid b$ и $b \mid a$. Треба доказати да је $a = b$. Претпоставимо да су бројеви a и b различити од нуле. Ако јесу нула, онда је $a = 0 = b$. Даље, како је $a \mid b$, постоји $c \in \mathbb{N}$ тако да $b = ca$. С друге стране, из $b \mid a$ имамо да постоји $d \in \mathbb{N}$ тако да $a = db$. Дакле, важи $a = db = dca$, то јест $a(1 - dc) = 0$. Како $a \neq 0$, мора бити $dc = 1$, а пошто су d и c природни бројеви, имамо да је $d = c = 1$, а тиме је и $a = b$.

Нека су $a, b, c \in \mathbb{N}$ и $a \mid b$ и $b \mid c$. Тада постоје $d, e \in \mathbb{N}$ тако да $b = da$ и $c = eb$, а тиме је и $c = eb = eda$, па $a \mid c$. Доказали смо и транзитивност релације $\mid$, па је она релација парцијалног уређења. □

Тврђење 6.26 *Нека су a, b, c произвољни природни бројеви. Тада важи:*

1. $a \mid 0$
2. *Ако $a \mid b$ и $a \mid c$, онда $a \mid b + c$.*
3. *Ако $a \mid b$ и $a \mid c$, онда $a \mid b \cdot c$.*
4. *Ако $a \mid b$ онда $a \mid b^n$, за свако $n \in \mathbb{N} \setminus \{0\}$.*

Доказ.

1. Важи $0 = a \cdot 0$.
2. Како је $b = ax$ и $c = ay$, за $x, y \in \mathbb{N}$, онда је $b + c = ax + ay = a(x + y)$, па $a \mid b + c$.
3. Постоји $x \in \mathbb{N}$ тако да $b = ax$. Тада је и $bc = axc$, па $a \mid bc$.
4. Ово тврђење је последица претходног доказа. □

Теорема 6.27 *(о Еуклидском дељењу) Нека су $a, b \in \mathbb{N}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{N}$ који су јединствено одређени тако да је*

$$a = b \cdot q + r, \;\; 0 \leq r < b.$$

Доказ. Посматрајмо скуп $S = \{a - bq \in \mathbb{N} \mid q \in \mathbb{N}\}$. Јасно је да је $S \subseteq \mathbb{N}$, али и да је $S \neq \emptyset$, јер је за $q = 0$, бар елемент $a = a - b \cdot 0$ у S. Према принципу најмањег елемента за скуп природних бројева, важи да постоји најмањи елемент у S - означимо га са r. Дакле, $r = a - bq \in \mathbb{N}$, то јест $a = bq + r$. Треба проверити да ли је $r < b$. Претпоставимо супротно: нека је $r \geq b$. Тада постоји $r' \in \mathbb{N}$ тако да је $r = r' + b$. Даље имамо да је $r' = r - b = a - bq - b = a - b(q + 1)$, па $r' \in S$ и $r' < r$. Ово је немогуће, јер је r најмањи елемент скупа S. Дакле, мора бити $r < b$. То значи да је $a = bq + r$ и $0 \leq r < b$. Још треба доказати јединственост бројева r и q. Претпоставимо да је $a = bq_1 + r_1$ и $0 \leq r_1 < b$.

Треба доказати да је $r = r_1$ и $q = q - 1$. Без умањења општости можемо претпоставити да је $r \geq r_1$. Тада је $0 \leq r - r_1 < b$, али и

$$r - r_1 = a - bq - (a - bq_1) = bq_1 - bq = b(q_1 - q).$$

Како $b \mid r - r_1$, важи $b \leq r - r_1$ или $r - r_1 = 0$. Због $r - r_1 < b$ први део је немогућ, па је $r - r_1 = 0$, то јест $r = r_1$. Даље је $a - r = bq = bq_1$, па је $b(q - q_1) = 0$,а како b није 0, мора бити $q - q_1 = 0$, то јест $q = q_1$. $\square$

Релацију дељивости можемо увести и на скупу целих бројева. Ако су $a, b \in \mathbb{Z}$ кажемо да a дели b и пишемо $a \mid b$ ако постоји број $c \in \mathbb{Z}$ тако да је $b = a \cdot c$. Релација дељивости није релација парцијалног поретка на скупу $\mathbb{Z}$ јер није антисиметрична. Наиме, важи да је

$$-3 \mid 3 \quad \text{и} \quad 3 \mid (-3) \quad \text{али је} \quad 3 \neq -3.$$

Тврђење о Еуклидском дељењу у овом случају изгледа овако:

Теорема 6.28 *Нека су $a, b \in \mathbb{Z}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{Z}$ који су јединствено одређени тако да је*

$$a = q \cdot b + r, \;\; 0 \leq r < |b|.$$

Доказ. Користићемо тврђење 6.27. Разликујемо четири случаја:
I случај: $a \geq 0, b > 0$
Ово је заправо тврђење 6.27.
II случај: $a \geq 0, b < 0$
Број $|b|$ је природан број, па можемо применити тврђење 6.27 на бројеве a и $|b|$. Постоје једиствени бројеви $q, r \in \mathbb{N}$ тако да $a = |b|q + r$ и $0 \leq r < |b|$. Онда је $a = b(-q) + r = bq' + r$ и $q' \in \mathbb{Z}$.
III случај: $a \leq 0, b > 0$
Број $|a|$ је природан број, па је $|a| = bq + r$ и $0 \leq r < b$. Тада је $-a = bq + r$, то јест $a = b(-q) - r$. Ако је $r = 0$ твређење је доказано. Ако је $r \neq 0$, онда је $a = b(-q) - r = b(-q-1) + b - r = bq' + r'$, где су $q' = -q - 1 \in \mathbb{Z}$ и $0 \leq r' = b - r < |b|$.
IV случај: $a \leq 0, b < 0$
Бројеви $|a|, |b|$ су природни, па је $|a| = |b|q + r$ и $0 \leq r < |b|$. Даље је $-a = -bq + r$, то јест $a = bq - r$. Слично као у претходном случсју можемо наћи q' и r' тако да $bq' + r'$ и $0 \leq r' < |b|$. $\square$

На пример, при дељењу бројева 43 и -17 са 6 добијамо $43 = 7 \cdot 6 + 1$ и $-17 = (-3) \cdot 6 + 1$.

Дефиниција 6.29 *Број $d \in \mathbb{N}$ је заједнички делилац природних бројева a и b ако $d \mid a$ и $d \mid b$. За такав број d кажемо да је највећи заједнички делилац бројева a и b ако $d' \mid d$ за сваки заједнички делилац d' тих бројева. У том случају пишемо $d =$ нзд(a, b).*

Дефиниција 6.30 *Број $s \in \mathbb{N}$ је заједнички садржалац природних бројева a и b ако $a \mid s$ и $b \mid s$. За такав број s кажемо да је најмањи заједнички садржалац бројева a и b ако $s \mid s'$ за сваки заједнички садржалац s' тих бројева. У том случају пишемо $s =$ нзс(a, b).*

На пример, за бројеве 330 и 42 важи нзд$(330, 42) = 6$ и нзс$(330, 42) = 2310$.

Тврђење 6.31 *Ако је $a = bq + r$ онда је нзд$(a, b) =$ нзд(b, r).*

Доказ. Докажимо да је скуп S_1 заједничких делилаца бројева a и b једнак скупу S_2 заједничких делилаца бројева b и r. Нека је $d \in S_1$. Дакле, d дели a

и b. Онда d дели и bq, а тиме и $a - bq = r$, па је d елемент скупа S_2. Ако је $d \in S_2$, онда d дели b и r, а тиме и $a = bq + r$, па је $d \in S_1$. Тиме смо доказали да је $S_1 = S_2$. $\square$

Еуклидов алгоритам представља поступак за одређивање највећег заједничког делиоца датих целих бројева a и $b \neq 0$. Састоји се од узастопног примењивања теореме 6.28. Прво, број a при дељењу са b даје неки количник q_1 и остатак r_1. Ако је $r_1 \neq 0$, можемо поделити b са r_1. У том случају добијамо количник q_2 и остатак r_2. Ако је $r_2 \neq 0$ настављамо поступак са бројевима r_1 и r_2. Поступак се завршава када добијемо остатак који је једнак нули. Алгоритам можемо представити шемом

$$\begin{array}{rcll} a & = & bq_1 + r_1, & 0 \leq r_1 < |b| \\ b & = & r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\ \vdots & & & \\ r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n q_{n+1} + r_{n+1}, & 0 \leq r_{n+1} < r_n \end{array}$$

Како остаци $r_1, r_2, r_3 \ldots$ чине строго опадајући низ и сви су већи или једнаки од нуле, то јест важи

$$0 \leq \ldots r_{n+1} < r_n < \cdots < r_2 < r_1,$$

постоји $n \in \mathbb{N}$ тако да је $r_{n+1} = 0$. Тада важи:

Теорема 6.32 *Последњи ненула остатак у претходном поступку је највећи заједничи делилац бројева a и b.*

Д о к а з. Нека је r_n последњи ненула остатак. Тада је $r_{n+1} = 0$ у претходној шеми. Користећи тврђење 6.31 имамо да је

$$\begin{array}{rcl} \text{нзд}(a, b) & = & \text{нзд}(b, r_1) \\ & = & \text{нзд}(r_1, r_2) \\ & = & \text{нзд}(r_2, r_3) \\ & \ldots & \\ & = & \text{нзд}(r_{n-1}, r_n). \end{array}$$

Пошто је $r_{n+1} = 0$, онда је $r_{n-1} = r_n q_{n+1}$ и нзд$(r_{n-1}, r_n) = r_n$. Дакле, нзд$(a, b) = r_n$. $\square$

Ако ставимо нзд$(0, 0) = 0$, уз претходну теорему, јасно је да за свака два цела броја a и b постоји нзд(a, b).

Тврђење 6.33 *Ако је нзд$(a, b) = d$, онда постоје бројеви x и y тако да $ax + by = d$.*

Д о к а з. Посматрајмо шему за Еуклидов алгоритам. Како је $d = r_n = r_{n-2} - r_{n-1} q_n$, то је $d = x_1 r_{n-2} + y_1 r_{n-1}$, за неке $x_1, y_1 \in \mathbb{Z}$. Из претходне једнакости имамо да је $r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$, па је $d = x_2 r_{n-3} + y_2 r_{n-2}, x_2, y_2 \in \mathbb{Z}$. Настављајући на овај начин долазимо до једнакости $d = x_{n-2} r_1 + y_{n-2} r_2, x_2, y_2 \in \mathbb{Z}$. Коначно је

$$d = x_{n-1} b + y_{n-1} r_1 = x_n a + y_n b.$$

Ставимо $x = x_n$ и $y = y_n$ и добили смо тразену једнакост. $\square$

Пример 6.34 *Користећи Еуклидов алгоритам одредити највећи заједнички делилац бројева 2541 и 588 и одредити бројеве x и y тако да $2541x + 588y =$ нзд$(2541, 588)$.*

Важи да је

$$\begin{array}{rcll} 2541 & = & 588 \cdot 4 + 189, & 0 \leq 189 < 588 \\ 588 & = & 189 \cdot 3 + 21, & 0 \leq 21 < 189 \\ 189 & = & 21 \cdot 9. & \end{array}$$

Последњи ненула остатак је 21, па је нзд$(2541, 588) = 21$. Такође је

$$21 = 588 - 189 \cdot 3 = 588 - (2541 - 588 \cdot 4) \cdot 3 = (-3) \cdot 2541 + 11 \cdot 588.$$

$\triangle$

Претходни поступак можемо извести и користећи матрице. Уочимо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix},$$

где су a и b бројеви чији највећи заједнички делилц тражимо. Ову матрицу можемо трансформисати користећи следеће операције:

1. множење врсте целим бројем и додавање другој врсти;
2. множење врсте са -1;
3. замена места врстама.

На тај начин полазну матрицу можемо свести на облик

$$\begin{bmatrix} d & x & y \\ 0 & x' & y' \end{bmatrix},$$

где је $d =$ нзд(a, b), цели бројеви x и y су такви да $ax + by = d$, док нам $x', y' \in \mathbb{Z}$ нису битни. На пример, нека су $a = 1729$ и $b = 385$. Тада је

$$\begin{bmatrix} 1729 & 1 & 0 \\ 385 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 189 & 1 & -4 \\ 385 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 189 & 1 & -4 \\ 7 & -2 & 9 \end{bmatrix} \sim \begin{bmatrix} 0 & 55 & -247 \\ 7 & -2 & 9 \end{bmatrix} \sim \begin{bmatrix} 7 & -2 & 9 \\ 0 & 55 & -247 \end{bmatrix},$$

одакле видимо да је нзд$(1729, 395) = 7$ и $7 = (-2) \cdot 1729 + 9 \cdot 385$.

Дефиниција 6.35 *Бројеви $a, b \in \mathbb{Z}$ су узајамно прости ако је нзд$(a, b) = 1$.*

Тврђење 6.36 *Ако $a \mid bc$ и нзд$(a, b) = 1$ онда $a \mid c$.*

Доказ. Према тврђењу 6.33 важи нзд$(a, b) = 1 = ax + by$, за неке $x, y \in \mathbb{Z}$. Можемо помножити целу једнакост са c. Тада је $acx + bcy = c$. Како $a \mid acx$ и $a \mid bc$, а тиме и $a \mid bcy$, онда $a \mid acx + bcy$, то јест $a \mid c$. $\square$

6.2 Диофантове једначине

Дефиниција 6.37 *Диофантова*[12] *једначина је једначина са целобројним коефицијентима код које тражимо решења у скупу $\mathbb{Z}$.*

Пример 6.38 *Једначина $ax = b$, где су $a, b \in \mathbb{Z}$ и $a \neq 0$ је Диофантова једначина. Има решење у $\mathbb{Z}$ ако и само ако $a \mid b$.* $\triangle$

Посматрајмо једначину облика

$$ax + by = c.$$

Ако је $a = 0$ или $b = 0$ једначина се своди на ннаведени пример. Зато можемо претпоставити да је $a \neq 0$ и $b \neq 0$. Нека је $d =$ нзд(a, b). Ако d дели c

[12] Диофант (3. век нове ере), старогрчки математичар

једначина има решење. Наиме, постоји c_1 тако да $c = dc_1$. Према 6.33 постоје $u, v \in \mathbb{Z}$ тако да $au + bv = d$. Помножимо овај идентитет са c_1. Добијамо $auc_1 + bvc_1 = dc_1 = c$. Бројеви uc_1 и vc_1 су цели бројеви, па представљају једно решење полазне једначине.

Важи и обрнуто: ако једначина $ax + by = c$ има решења, онда је $d \mid c$. Нека су $x_0, y_0 \in \mathbb{Z}$ решења једначине, то јест $ax_0 + by_0 = c$. Како је $d \mid a$ и $d \mid b$ имамо и $d \mid ax_0$ и $d \mid y_0$, па је $d \mid ax_0 + by_0$. Дакле, $d \mid c$.

У случају да $d \mid c$, као што је већ речено, једно решење једначине је уређени пар (uc_1, vc_1), при чему бројеве u и v можемо да одредимо из Еуклидовог алгоритма. Како одредити сва решења ове једначине?

Имамо једнакости

$$au + bv = c \qquad ax + by = c.$$

Ако их одузмемо добијамо:

$$a(x-u) + b(y-v) = 0 \Rightarrow a(x-u) = -b(y-v).$$

Како је $d = \text{нзд}(a, b)$, постоје цели бројеви a_1 и b_1 тако да $a = a_1 d$ и $b = b_1 d$; јасно је да мора бити $\text{нзд}(a_1, b_1) = 1$. Даље, важе једнакости

$$\begin{aligned} da_1(x-u) &= -db_1(y-v) \\ a_1(x-u) &= -b_1(y-v). \end{aligned}$$

Видимо да $b_1 \mid a_1(x-u)$, а како су a_1 и b_1 узајамно прости, применом тврђења 6.36 добијамо да b_1 дели $x - u$, што значи да постоји $t \in \mathbb{Z}$ тако да $x - u = b_1 t$. Заменом у ?? добијамо $y - v = -a_1 t$. Дакле, ако је (x, y) произвољно решење једначине, имамо да је $x = u + b_1 t$, а $y = v - a_1 t$, за $t \in \mathbb{Z}$. Заменом ових једнакости у полазну једначину видимо да је $(u + b_1 t, v - a_1 t)$ решење за свако $t \in \mathbb{Z}$. Овим смо доказали:

Теорема 6.39 *Једначина $ax + by = c$, где је $a, b \neq 0$ има целобројна решења ако и само ако $\text{нзд}(a, b) \mid c$. У том случају опште решење ове једначине је*

$$\begin{aligned} x &= u\frac{c}{d} + \frac{b}{\text{нзд}(a,b)} \cdot t \\ y &= v\frac{c}{d} - \frac{a}{\text{нзд}(a,b)} \cdot t, \qquad t \in \mathbb{Z}, \end{aligned}$$

где су u и v решења једначине $au + bv = d$ добијена помоћу Еуклидовог алгоритма.
□

Пример 6.40 *Испитати да ли једначина $121x + 77y = 132$ има целобројна решења и ако има одредити опште решење.*

Можемо приметити да је $\text{нзд}(121, 77) = 11$, али потребно је наћи и бројеве u и v тако да $121u + 77v = \text{нзд}(121, 77)$.

$$\begin{bmatrix} 121 & 1 & 0 \\ 77 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 44 & 1 & -1 \\ 77 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 44 & 1 & -1 \\ -11 & -2 & 3 \end{bmatrix} \sim$$

$$\begin{bmatrix} 0 & -7 & 11 \\ -11 & -2 & 3 \end{bmatrix} \sim \begin{bmatrix} -11 & -2 & 3 \\ 0 & -7 & 11 \end{bmatrix} \sim \begin{bmatrix} 11 & 2 & -3 \\ 0 & -7 & 11 \end{bmatrix}$$

Дакле, $121 \cdot 2 + 77 \cdot (-3) = 11 = \text{нзд}(121, 77)$. Како је $11 \mid 132$, једначина има целобројна решења. Према претходној теореми опште решење једначине је дато са

$$\begin{aligned} x &= 2\frac{132}{11} + \frac{77}{11} \cdot t = 24 + 7t \\ y &= -3\frac{132}{11} - \frac{121}{11} \cdot t = -36 - 11t, \qquad t \in \mathbb{Z}. \end{aligned}$$

6.3 Прости бројеви

Дефиниција 6.41 *Цео број $p > 1$ је прост ако су једини делиоци тог броја 1 и p. Цео број $n > 1$ који није прост је сложен.*

На пример, бројеви 11 и 571 су прости, а 6 и 51 нису прости.
Ако је p прост и важи $p = a \cdot b$ онад мора бити $a = 1$ или $b = 1$.

Тврђење 6.42 *Постоји бесконачно много простих бројева.*

Доказ. Претпоставимо супротно: има их коначно много и нека су то бројеви $p_1, p_2, \ldots, p_n$. Нека је број $p = p_1 p_2 \cdots p_n + 1$. Како је $p > p_i$ за свако $i = \overline{1, n}$ онда је $p \neq p_i$ за $i = \overline{1, n}$. Дакле, p није прост број. Онда p мора бити сложен. То значи да је дељив неким простим бројем, заправо неким од бројева $p_1, p_2, \ldots, p_n$. Остатак при дељењу броја p са било којим од бројева p_i је један, па добијамо контрадикцију. Дакле, простих бројева има бесконачно много. $\square$

Тврђење 6.43 *Ако је p прост број и $p \mid ab$, онда је $p \mid a$ или $p \mid b$.*

Доказ. Нека је $p \mid ab$ и претпоставимо да $p \nmid a$. Ако би било нзд$(a, p) > 1$, како е p прост било би нзд$(a, p) = p$, то јест $p \mid a$, што није. Дакле, мора бити нзд$(a, p) = 1$. Применом тврђења 6.36 закључујемо да је $p \mid b$. $\square$
Важи и уопштеније тврђење: ако је p прост број и $p \mid a_1 a_2 \cdots a_k$, онда је тачно $p \mid a_1 \vee p \mid a_2 \vee \cdots \vee p \mid a_k$.

Тврђење 6.44 *Сваки природан број већи од 1 је прост или се може представити као производ простих бројева.*

Доказ. Користићемо принцип потпуне индукције. Нека је Φ својство природних бројева 'бити прост или производ простих'. Нека је $n > 1$ и претпоставимо да сваки природан број мањи од n задовољава својство Φ. Ако је n прост, онда је тачно $\Phi(n)$. Ако је n сложен, онда је $n = m_1 \cdot m_2$, где су m_1 и m_2 природни бројеви такви да $1 < m_1, m_2 < n$. Према индуктивној претпоставци, m_1 и m_2 су прости или производи простих, па је тиме и број n, као њихов производ, производ простих бројева. Дакле, и у овом случају је тачно $\Phi(n)$. Према теореми 6.4 својство Φ задовољава сваки породни број. $\square$

Теорема 6.45 *(Основна теорема аритметике) Сваки природни број већи од 1 може се представити у облику производа простих бројева на јединствен начин (до на редослед простих фактора).*

Доказ. Због претходне теореме, довољно је доказати да је представљање броја на просте факторе јединствено. Можемо претпоставити да постоје две факторизације природног броја n:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}.$$

Без умањења општости, претпоставимо да је $p_1 < p_2 < \cdots < p_k$ и $q_1 < q_2 < \cdots < q_l$. Дакле, важи

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}.$$

Како $p_1 \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда и $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$. Према коментару после тврдјења 6.43, важи $p_1 \mid q_i$ за неко $i \in \{1 \ldots, l\}$. Пошто су у питању прости бројеви, мора бити $p_1 = q_i$. Слично налазимо да је $p_2, p_3, \ldots, p_k \in \{q_1, q_2, \ldots, q_l\}$, то јест $\{p_1, p_2, \ldots, p_k\} \subseteq \{q_1, q_2, \ldots, q_l\}$. Такође, можемо показати да је $\{q_1, q_2, \ldots, q_l\} \subseteq \{p_1, p_2, \ldots, p_k\}$. Дакле, $\{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_l\}$, а уз услове $p_1 < p_2 < \cdots < p_k$ и $q_1 < q_2 < \cdots < q_l$ мора бити $k = l$ и $p_i = q_i$, за свако $i \in \{1, \ldots, k\}$.

Сада добијамо једнакост $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$. Ако би важило $\beta_1 > \alpha_1$, онда бисмо имали $p_2^{\alpha_2}\cdots p_k^{\alpha_k} = p_1^{\gamma_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$, за $\gamma_1 = \beta_1 - \alpha_1 > 0$. Тада је $p_1 \mid p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, па следи да је $p_1 = p_j$, за неко $j \neq 1$. То је немогуце, јер је $p_1 < p_j$, за свако $j \in \{2,\dots,k\}$. Дакле, важи $\beta_1 \leq \alpha_1$. На сличан начин можемо закључити да је $\alpha_1 \leq \beta_1$, па је онда $\alpha_1 = \beta_1$. Добијамо да је $p_2^{\alpha_2}\cdots p_k^{\alpha_k} = p_2^{\beta_2}\cdots p_k^{\beta_k}$. Настављајући наведени поступак добијамо $\alpha_2 = \beta_2, \dots, \alpha_k = \beta_k$. □

На пример, број 24255 прдстављамо у облику производа степена простих бројева на следећи начин: $24255 = 3^2 \cdot 5 \cdot 7^2 \cdot 11$.

6.4 Конгруенције

Дефиниција 6.46 *Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod m$ или $a \equiv_m b$ ако је $m \mid (a-b)$.*

На пример $16 \equiv -5 \equiv 2 \pmod 7$.

Тврђење 6.47 *Релација $\equiv_m$ је релација еквиваленције*

Доказ. Како је $x - x = 0$ и према тврђењу 6.26 $m \mid 0$, релација $\equiv_m$ је рефлексивна.

Ако је $x \equiv_m y$, онда је $m \mid x - y$, а тиме је и $m \mid -(x-y)$, то јест $m \mid y - x$. Дакле, $y \equiv_m x$, па је дата релације симетрична.

Нека је $x \equiv_m y$ и $y \equiv_m z$. Да бисмо доказали да је релација $\equiv_m$ транзитивна, потребно је доказати да $x \equiv_m z$. Из претпоставки следи да је $m \mid x - y$ и $m \mid y - z$. Бројеви $x - y$ и $y - z$ су дељиви са m, па је и њихов збир дељив са m, то јест $m \mid (x-y) + (y-z)$. □

Тврђење 6.48 *Ако је $a \equiv a_1 \pmod m$ и $b \equiv b_1 \pmod m$ онда је*

$$\begin{aligned} a + b &\equiv a_1 + b_1 \pmod m \\ a \cdot b &\equiv a_1 \cdot b_1 \pmod m \end{aligned}$$

Доказ. Према претпоставци, $m \mid a - a_1$ и $m \mid b - b_1$. Тада је и $m \mid (a - a_1) + (b - b_1)$, то јест $m \mid (a+b) - (a_1 + b_1)$. Следи да је $a + b \equiv_m a_1 + b_1$. Докажимо и другу једнакост. Приметимо да је

$$ab - a_1b_1 = ab - a_1b + a_1b - a_1b_1 = (a - a_1)b + a_1(b - b_1).$$

Важе следеће импликације:

$$\begin{aligned} m \mid a - a_1 &\Rightarrow m \mid (a - a_1)b \\ m \mid b - b_1 &\Rightarrow m \mid a_1(b - b_1), \end{aligned}$$

па је и

$$m \mid (a - a_1)b + a_1(b - b_1) \Rightarrow m \mid ab - a_1b \Rightarrow ab \equiv_m a_1b_1.$$

□

Тврђење 6.49 *Ако је $a \equiv a_1 \pmod m$ и k је природан број, тада је $a^k \equiv a_1^k \pmod m$.*

Доказ. Користићмо индукцију по k. За $k = 0$: $a^0 = 1 = a_1^0$, па је $a^0 \equiv_m a_1^0$. Претпоставимо да тврђење важи за природни број k: $a^k \equiv_m a_1^k$. Како је $a \equiv_m a_1$, према претходној теореми важи $a^{k+1} \equiv_m a_1^{k+1}$. □

Нека је $p(x) = p_0 + p_1x + \cdots + p_nx^n$ полином чији коефицијенти су цели бројеви, нека је $a \equiv b \pmod{m}$. Према претходном тврђењу је $p(a) \equiv p(b) \pmod{m}$.

Ево још једне примене овог тврђења. Нека је a природни број. Одредимо услов под којим је број a дељив са 3. Нека је $a = 10^na_n + 10^{n-1}a_{n-1} + \cdots 10^2a_2 + 10a_1 + a_0$. Како је $10 \equiv_3 1$, онда је и $10^k \equiv_3 1^k \equiv_3 1$, за свако k. Па важи $a \equiv_3 a_n + a_{n-1} + \cdots + a_1 + a_0$, то јест број је дељив са 3 ако је збир његових цифара дељив са 3.

Како је и $10 \equiv_9 1$, то је број дељив са 9 ако је збир његових цифара дељив са 9.

Одредимо под којим условима је број $a = 10^na_n + 10^{n-1}a_{n-1} + \cdots 10^2a_2 + 10a_1 + a_0$ дељив са 11. Важи $10 \equiv_{11} -1$, па је $10^k \equiv_{11} (-1)^k$, а тиме је број a дељив са 11 ако је број $(-1)^na_n + (-1)^{n-1}a_{n-1} + \cdots + (-1)a_1 + a_0$ дељив са 11. На пример, број 174625 је дељив са 11, јер је то и број $-1+7-4+6-2+5 = 11$.

Пример 6.50 *Одредити остатак при дељењу броја* 2^{30} *са 13.*

Користећи тврђење 6.48 закључујемо:

$$\begin{array}{lllllll}
2^1 & \equiv & 2 \pmod{13} & \qquad & 2^4 & \equiv & 8\cdot 2 \equiv 3 \pmod{13}\\
2^2 & \equiv & 2\cdot 2 \equiv 4 \pmod{13} & & 2^5 & \equiv & 3\cdot 2 \equiv 6 \pmod{13}\\
2^3 & \equiv & 4\cdot 2 \equiv 8 \pmod{13} & & 2^6 & \equiv & 6\cdot 2 \equiv 12 \equiv -1 \pmod{13}.
\end{array}$$

Према томе је
$$2^{30} \equiv (2^6)^5 \equiv (-1)^5 \equiv -1 \equiv 12 \pmod{13},$$
па је тражени остатак број 12. △

Тврђење 6.51 *Ако је* $ab \equiv ac \pmod{m}$ *и* нзд$(a,m) = 1$, *онда је* $b \equiv c \pmod{m}$.

Доказ. Важи да $m \mid ab - ac \Rightarrow m \mid a(b-c)$. Како је нзд$(a,m) = 1$, применом тврђења 6.36 добијамо да $m \mid b - c$, то јест $b \equiv c \pmod{m}$. □

Тврђење 6.52 *Нека за природне бројеве m и n веће од 1 и цео број a важи: $m \mid a$ и $n \mid a$. Ако су бројеви m и n узајамно прости, онда је $mn \mid a$.*

Доказ. Претпоставка је да је $a = ma_1$ и $n \mid a \Rightarrow n \mid ma_1$. Како је нзд$(m,n) = 1$, према тврђењу 6.36 n дели $a-1$ па је $a_1 = na_2$. Добили смо да је $a = ma_1 = mna_2$, па mn дели a. □

Нека је
$$a \equiv a_1 \pmod{m} \qquad a \equiv a_1 \pmod{n}.$$
Тада је $m \mid a - a_1$ и $n \mid a - a_1$. Ако су m и n узајамно прости, према претходном тврђењу је $a \equiv a_1 \pmod{mn}$.

Пример 6.53 *Решити једначину* $ax \equiv b \pmod{m}$, *где су* $a, b \in \mathbb{Z}$.

Тачан је следећи низ еквиваленција:

Постоји решење једначине $ax \equiv b \pmod{m}$	акко	$m \mid ax - b$, за неко x
	акко	$ax - b = m(-y)$, за неко x и y
	акко	једначина $ax + my = b$ има решење
	акко	нзд$(a,m) \mid b$.

Нека је $d =$ нзд(a,m). Ако је $d \mid b$, одредимо решење ове једначине. Нека је (x_0, y_0) решење једначине $ax+my = d$ одређено помоћу Еуклидовог алгоритма. Тада је $x_1 = x_0\frac{b}{d}$ једно решење полазне једначине $ax \equiv b \pmod{m}$. Ако је $d = 1$, онда су сва решења облика $x_1 + mt$, за $t \in \mathbb{Z}$.

Нека је $d > 1$. Докажимо да је x рашење једначине $ax \equiv b \pmod{m}$ ако и само ако је решење једначине $a'x \equiv b' \pmod{m'}$, где су $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Важи:

$$\begin{array}{lll}
\text{Ако је } ax \equiv b \pmod{m} & \text{онда} & m \mid ax - b \\
& \text{следи} & ax - b = m(-y), \text{ за неко } y \\
& \text{следи} & ax + my = b \\
& \text{следи} & ax + my = b / : d \\
& \text{следи} & \dfrac{a}{d}x + \dfrac{m}{d}y = \dfrac{b}{d} \\
& \text{следи} & a'x + m'y = b' \\
& \text{следи} & a'x \equiv b' \pmod{m'}.
\end{array}$$

С друге стране:

$$\begin{array}{lll}
\text{ако је } a'x \equiv b' \pmod{m'} & \text{онда} & m' \mid a'x - b' \\
& \text{следи} & a'x - b' = m'(-y), \text{ за неко } y \\
& \text{следи} & a'x + m'y = b' \\
& \text{следи} & a'x + m'y = b' / \cdot d \\
& \text{следи} & a'dx + m'dy = b'd \\
& \text{следи} & ax + my = b \\
& \text{следи} & ax \equiv b \pmod{m}.
\end{array}$$

Нека је x_0 најмањи позитивни број који је решење једначине $a'x \equiv b \pmod{m'}$. Тада су

$$x_0 \qquad x_0 + m' \qquad x_0 + 2m' \qquad \cdots \qquad x_0 + (d-1)m'$$

различита решења једначине $ax \equiv b \pmod{m}$, јер је $m = m'd$. Како је нзд$(a', b') = 1$, према претходном делу сва решења једначине $ax \equiv b \pmod{m}$ су $x_0 + m't$, за $t \in \mathbb{Z}$. Дакле, сва решења једначине $ax \equiv b \pmod{m}$ по модулу m су $y_i = x_0 + im'$, за $i \in \{0, 1, \ldots, d-1\}$. Приметимо да их има d. Дакле, опште решење дате једначине је $y_i + mt$, за $i \in \{0, 1, \ldots, d-1\}$ и $t \in \mathbb{Z}$. $\triangle$

Напомена 6.54 *Претходни пример даје услов за егзистенцију решења и начин за одређивање истог. У случају када је нзд$(a, m) = 1$ приметимо да је могуће пронаћи решење једначине $ax \equiv_m b$ тако што задајемо вредности за x, почевши на пример од 1, и проверавамо која од тих вредности задовољава једначину. Ово ћемо че71е користити када су у питању "мали" бројеви. На пример, ако је $m = 9$, довољно је проверити који од бројева $1, \ldots, 8$ је решење.*

Пример 6.55 *Испитати да ли следеће једначине имају решење и ако имају одредити га.*

1. $4x \equiv_{14} 9$
2. $7x \equiv_9 1$
3. $8x \equiv_{28} 12$

1. Како је нзд$(4, 14) = 2$ и $2 \nmid 9$, једначина нема решење.
2. Важи да нзд$(7, 9) = 1$ и $1 \mid 1$, па једначина има решење. Можемо закључити да је 4 једно решење једначине и без кори71ења Еуклидовог алгоритма. Тако да је опште решење једначине $4 + 9t$, за $t \in \mathbb{Z}$.
3. Једначина има решење јер нзд$(8, 28) = 4$ и $4 \mid 12$. Према претходном, треба одредити решење једначине $2x \equiv_7 3$. Приметимо да је $2 \cdot 5 \equiv 10 \equiv 3 \pmod{7}$. Сва решења су бројеви 5, 12, 19 и 24 по модулу 7.

$\triangle$

Теорема 6.56 *(Вилсонова теорема) Ако је p прост број тада је* $(p-1)! \equiv -1 \pmod{p}$.

Доказ. Ако је $p = 2$ или $p = 3$, тврђење тореме важи. Ако је p различито од 2 и 3, докажимо да за сваки број $a \in \{2, 3, \ldots, p-1\}$ постоји тачно једно $x \in \{2, 3, \ldots, p-1\}$ тако да $ax \equiv 1 \pmod{p}$. Последња једначина има решење ако и само ако нзд$(a, p) \mid 1$. Како је p прост и $a < p$, a и p су узајамно прости, па постоји $y \in \mathbb{Z}$ тако да $ay \equiv 1 \pmod{m}$. Постоји $x \in \{1, 2, \ldots p-1\}$ тако да $y \equiv_p x$. Дакле, $ax \equiv 1 \pmod{p}$. Не може бити $x = 1$, јер би тада било $p \mid a$, а то је немогуће. Ако би важило $ax_1 \equiv 1 \pmod{p}$, за неко $x_1 \in \{2, 3, \ldots, p-1\}$, онда је $ax \equiv_p ax_1$, па пошто су задовољени услови тврђења 6.51, важи $x \equiv_p x_1$. Претпоставимо да је $x \leq x_1$. Тада је $0 \leq x_1 - x$, али и $x_1 - x < p$, јер је $2 \leq x, x_1 \leq p-1$. Посто $p \mid x_1 - x$ и $0 \leq x_1 - x < p$, јасно је да мора бити $x = x_1$. Овим смо доказали јединственост броја x.

Проверимо да ли се може десити да је $x = a$. Тада је $a^2 \equiv_p 1$, то јест $p \mid a^2 - 1 \Rightarrow p \mid (a-1)(a+1)$. Пошто је p прост, према тврђењу 6.43, мора бити $p \mid a-1$ или $p \mid a+1$. Како је $a \in \{2, 3, \ldots, p-1\}$, онда је $1 \leq a \leq p-2$ и немогућ је да p дели $a-1$. Дакле, $p \mid a+1$. важи да је $3 \leq a+1 \leq p$, па мора бити $a + 1 = p$, то јест $a = p - 1$.

Можемо закључити следеће: ако је $a = p - 1$ постоји јединствени елемент $x(= p-1)$ тако да $ax \equiv 1 \pmod{p}$; ако је $a \in \{2, 3, \ldots, p-2\}$ постоји јединствени елемент $x \in \{2, 3, \ldots, p-2\}$ тако да $ax \equiv 1 \pmod{p}$ и $x \neq a$.

Сада посматрајмо једнакост $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$. За сваки од бројева $2, \ldots, p-2$ постоји неки у истом том скупу, који помножен са њим даје 1 по модулу p. Дакле,

$$(p-1)! \equiv 1 \cdot \underbrace{1 \cdots 1}_{\frac{p-3}{2} \text{ пута}} \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}.$$

$\square$

Приметимо да важи и обрат Вилсонове теореме: ако за неки природан број $p > 1$ важи да $(p-1)! \equiv 1 \pmod{p}$, онда p јесте прост број. Наиме, важи да је $p \mid (p-1)!+1$, па постоји $k \in \mathbb{Z}$ тако да $pk = (p-1)!+1$, то јест $pk + (-1)(p-1)! = 1$. Тада нзд$(p, (p-1)!) \mid 1$, па је нзд$(p, 1 \cdot 2 \cdots (p-1)) = 1$. Видимо да је за свако $i \in \{1, 2, \ldots, p-1\}$ број нзд$(i, p) = 1$, па је p прост.

Теорема 6.57 *(Кинеска теорема о остацима) Систем конгруенција*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

има решење ако нзд$(m_i, m_j) \mid (a_i - a_j)$ за све $i \neq j$. Ако је $\overline{x}$ неко решење тог система, онда је опште решење облика $x = \overline{x} +$ нзс$(m_1, \ldots m_k) \cdot t$, где је $t \in \mathbb{Z}$.

Доказ. Користићемо индукцију по броју конгруенција k. Ако је $k = 1$ имамо једну конгруенцију $x \equiv a_1 \pmod{m_1}$. Решења су $x = a_1 + mt$, за свако $t \in \mathbb{Z}$. Претпоставимо да је тврђење тачно за k конгруенција. Докажимо да важи за

$k+1$. Нека је дат систем конгруенција

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \\ x & \equiv & a_3 & \pmod{m_3} \\ & \dots & & \\ x & \equiv & a_k & \pmod{m_k} \\ x & \equiv & a_{k+1} & \pmod{m_{k+1}}, \end{array}$$

тако да важе услови нзд$(m_i, m_j) \mid (a_i - a_j)$ за све $i \neq j$. Према индуктивној хипотези, првих k конгруенција има решење и опште решење је облика $x = x_0 + \text{нзс}(m_1, \dots, m_k)y$, где је x_0 једно изборно решење и $y \in \mathbb{Z}$. Проверимо да ли ово решење задовољава и последњу конгруенцију, то јест да ли једначина $x_0 + \text{нзс}(m_1, \dots, m_k)y \equiv a_{k+1} \pmod{m_{k+1}}$ има решење. Дакле, тражимо $y \in \mathbb{Z}$ тако да нзс$(m_1, \dots, m_k)y \equiv a_{k+1} - x_0 \pmod{m_{k+1}}$. Према претходном, решење ове једначине постоји ако нзд(нзс$(m_1, \dots, m_k), m_{k+1}) \mid a_{k+1} - x_0$. Како је нзд(нзс$(m_1, \dots, m_k), m_{k+1})$ = нзс(нзд(m_1, m_{k+1}), нзд$(m_2, m_{k+1}), \dots,$ нзд(m_k, m_{k+1})), довољно је показати да нзд$(m_i, m_{k+1}) \mid a_{k+1} - x_0$, за сваки $i\{1, \dots, k\}$. Важи $a_{k+1} - x_0 = (a_{k+1} - a_i) + (a_i - x_0)$. Према претпоставци је нзд$(m_i, m_{k+1}) \mid a_i - a_{k+1}$. Такође, $x_0 \equiv a_i \pmod{m_i}$, за свако $i \in \{1, \dots, k\}$, то јест $m_i \mid a_i - x_0$, па је онда и нзд$(m_i, m_{k+1}) \mid a_i - x_0$. Самим тим нзд$(m_i, m_{k+1})$ дели и збир $(a_{k+1} - a_i) + (a_i - x_0)$. Дакле, доказали смо да систем од $k+1$ конгруенција има решење.

Треба одредити како изгледа опште решење система конгруенција. Нека је $\overline{x}$ једно решење тог система, а x произвољно. Тада је

$$\begin{array}{rcll} \overline{x} & \equiv & a_1 & \pmod{m_1} \\ \overline{x} & \equiv & a_2 & \pmod{m_2} \\ \overline{x} & \equiv & a_3 & \pmod{m_3} \\ & \dots & & \\ \overline{x} & \equiv & a_k & \pmod{m_k} \end{array} \qquad \begin{array}{rcll} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \\ x & \equiv & a_3 & \pmod{m_3} \\ & \dots & & \\ x & \equiv & a_k & \pmod{m_k}, \end{array}$$

а тиме и

$$\begin{array}{rcll} x & \equiv & \overline{x} & \pmod{m_1} \\ x & \equiv & \overline{x} & \pmod{m_2} \\ x & \equiv & \overline{x} & \pmod{m_3} \\ & \dots & & \\ x & \equiv & \overline{x} & \pmod{m_k}. \end{array}$$

Следи да $m_i \mid x - \overline{x}$, за свако i. То значи да нзс$(m_1, \dots m_k) \mid x - \overline{x}$, то јест да је $x - \overline{x} =$ нзс$(m_1, \dots m_k)t$, за неко $t \in \mathbb{Z}$. Такође, сваки број облика $\overline{x} +$ нзс$(m_1, \dots m_k)t$, за $t \in \mathbb{Z}$ јесте решење датог система конгруенција, пошто је нзс$(m_1, \dots m_k) \equiv 0 \pmod{m_i}$, за свако $i \in \{1, \dots, k\}$. □

Напомена 6.58 *Ако су бројеви m_i, m_j међусобно узајамно прости за $i \neq j$, онда важи да наведени систем конгруенција има решење за све a_i.*

Пример 6.59 *Решити систем конгруенција*

$$x \equiv_3 2 \qquad x \equiv_4 3 \qquad x \equiv_5 1.$$

Приметимо да је ово случај из претходне напомене, па систем има решење. Из прве једначине је $3 \mid x - 2$, па је решење облика $x = 3y + 2$, за неко $y \in \mathbb{Z}$. Заменимо то у другу једначину: $3y + 2 \equiv_4 3$, то јест $3y \equiv_4 1$. Пошто је нзд$(3,4) = 1$ и $1 \mid 1$ последње једначине има решење које је облика $y = 3 + 4z$, за $z \in \mathbb{Z}$. Тада је $x = 3y + 2 = 3(3 + 4z) + 2 = 11 + 12z$. Заменимо ову једнакост у трећу једначину датог система: $11 + 12z \equiv_5 1$, то јест $12z \equiv_5 0$, па је $5 \mid 12z$. Према тврђењу 6.36 је $z = 5t$, за $t \in \mathbb{Z}$. Дакле, $x = 11 + 12z = 11 + 60t$, $t \in \mathbb{Z}$ је опште решење полазног система. Приметимо да 11 јесте једно специјално решење система, као и да нзс$(3,4,5) = 60$, па се добијени резултат поклапа са тврђењем теореме.

Дефиниција 6.60 *Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m,n) = 1$. Функција φ се назива Ојлерова*[13] *функција.*

Лако можемо закључити да, ако је p прост број, онда је $\varphi(p) = p - 1$. Такође, за $k \geq 1$, $\varphi(p^k) = p^k - p^{k-1}$. Наиме, питање колико има бројева који су мањи од p^k и узајамно прости са њим своди се на питање колико има бројева мањих од p^k и дељивих са p. Сви бројеви који задовољавају последњи услов су $\{kp \mid 1 < kp < p^k\} = \{kp \mid 1 \leq k \leq p^{k-1}\}$ и има их p^{k-1}. Дакле, од свих p^k бројева одузимамо оне за које важи да је највећи заједнички делилац тог броја и броја p^k већи од 1 и добијамо да је $\varphi(p^k) = p^k - p^{k-1}$.

Означимо са $\Phi(n)$ скуп $\{k \mid 1 \leq k \leq n-1, \text{нзд}(k,n) = 1\}$. Тада је $\varphi(n) = |\Phi(n)|$.

Тврђење 6.61 *Нека су $m, n > 1$ природни бројеви такви да нзд$(m,n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.*

Доказ. Формираћмо пресликавање скупа $\Phi(mn)$ на скуп $\Phi(m) \times \Phi(n)$, које је бијекција. Дефинишимо $f : \Phi(mn) \to \Phi(m) \times \Phi(n)$ са $f(k) = (\rho_m(k), \rho_n(k))$. Преликавање је добро дефинисано, јер ако је k узајамно прост са mn, онда мора бити узајамно прост и са m и са n. Дакле, заиста је $(\rho_m(k), \rho_n(k)) \in \Phi(m) \times \Phi(n)$.

Докажимо да је f инјективно. Нека је $f(k) = f(\overline{k})$, то јест $(\rho_m(k), \rho_n(k)) = (\rho_m(\overline{k}), \rho_n(\overline{k}))$. Тада је $\rho_m(k) = \rho_m(\overline{k})$ и $\rho_n(k) = \rho_n(\overline{k})$, па $m \mid k - \overline{k}$ и $n \mid k - \overline{k}$. Премо тврђењу 6.52, имамо да је $mn \mid k - \overline{k}$. Како је $1 \leq k, \overline{k} \leq mn-1$ и бројеви k и $\overline{k}$ дају исти остатак при дељеју са mn, мора бити $k = \overline{k}$.

Нека је $(r,s) \in \Phi(m) \times \Phi(n)$. Посматрајмо систем конгруенција

$$\begin{aligned} x &\equiv r \pmod{m} \\ x &\equiv s \pmod{n}. \end{aligned}$$

Бројеви m и n су узајамно прости, па према теореми 6.57 постоји решење овог система. Како је нзс$(m,n) = mn$, постоји решење x_0 тако да $1 \leq x_0 < mn$. За број x_0 важи да при дељењу са m даје остатак r, а при дељењу са n остатак s. Треба проверити да x_0 припада скупу $\Phi(mn)$. Нека је $d =$ нзд(m, x_0). Из једначине $x_0 \equiv r \pmod{m}$ имамо да је $x_0 - r = mt$, за неко $t \in \mathbb{Z}$. Пошто $d \mid x_0$ и $d \mid m$, онда важи и $d \mid r$. Како је $r \in \Phi(m)$, онда је нзд$(r,m) = 1$, па из претходног разматрана следи да је $d = 1$. Дакле, бројеви m и x_0 су узајамно прости. Сличо се докаже и да су n и x_0 узајамно прости. Према тврђењу 6.33 постоје бројеви $u, v, p, q \in \mathbb{Z}$ тако да $mu + x_0v = 1$ и $np + x_0q = 1$. Множећи последње две једнакости добијамо $mn(up) + x_0(mnq + npv + x_0vq) = 1$, што значи да су mn и x_0 узајамно прости, па је $x_0 \in \Phi(mn)$. Дакле, видимо да је $f(x_0) = (r,s)$, па је функција f сурјективна.

Дакле, f је бијекција, па је $|\Phi(mn)| = |\Phi(m) \times \Phi(n)| = |\Phi(m)| \cdot |\Phi(n)|$. То управо значи да је $\varphi(mn) = \varphi(m)\varphi(n)$. □

Према теореми 6.45 сваки природни број n се на јединствен начин, до на редослед фактора, може представити у облику $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где су $p_1, \ldots, p_k$ различити прости бројеви.

[13] Leonhard Euler (1707-1783), швајцарски математичар

Теорема 6.62 *Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда је $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$.*

Доказ. Како су p_i различити прости бројеви, они су међусобно узајамно прости, па је према 6.61 $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$. Сетимо се да је за прост број p $\varphi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p})$. Имамо низ једнакости

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\cdots\varphi\left(p_k^{\alpha_k}\right) \\
&= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right) \\
&= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

□

Дефиниција 6.63 *Нека је $n > 1$ природни број. Скуп $\{r_1, \ldots, r_n\}$ природних бројева је потпуни систем остатака по модулу n ако је сваки цео број конгуентан по модулу n тачно једном од бројева r_i.*

Можемо приметити да је r_i није конгруентно по модулу n броју r_j, за $i \neq j$. Један пример за потпуни систем остатака по модулу n је $\{0, 1, 2, \ldots, n-1\}$.

Дефиниција 6.64 *Нека је $n > 1$ природни број. Скуп $\{r_1, \ldots, r_k\}$ природних бројева је редуковани систем остатака по модулу n ако је сваки цео број који је узајамно прост са n конгуентан по модулу n тачно једном од бројева r_i.*

Специјално важи да су сви r_i узајамно прости са n и да r_i није конгруентно по модулу n броју r_j, за $i \neq j$. Наравно, сваки редуковани систем остатака по модулу n има $\varphi(n)$ елемената. На пример, један редуковани систем остатака по модулу 12 је скуп $\{1, 5, 7, 11\}$ и тај скуп очигледно има $\varphi(12)$ елемената.

Теорема 6.65 *(Ојлерова теорема) Нека су a и n позитивни природни бројеви, такви да нзд$(a, n) = 1$. Тада важи $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Доказ. Нека је $\{r_1, \ldots, r_{\varphi(n)}\}$ један редуковани систем остатака по модулу n. Докажимо да је скуп $\{ar_1, \ldots, ar_{\varphi(n)}\}$ такође редуковани систем остатака по модулу n. Како је нзд$(a, n) = 1$ и нзд$(r_i, n) = 1$, мора бити и нзд$(ar_i, n) = 1$. То значи да су сви елементи скупа $\{ar_1, \ldots, ar_{\varphi(n)}\}$ узајамно прости са n. С друге стране, ако је $ar_i \equiv ar_j \pmod{n}$ и како важи нзд$(a, n) = 1$, према тврђењу 6.51 важи $r_i \equiv r_j \pmod{n} \Rightarrow i = j$. Дакле, бројеви наведеног скупа су различити по модулу n, узајамно су прости са n и има их $\varphi(n)$. Према томе, чине један редуковани систем остатака по модулу n.

Даље, како је и $\{r_1, \ldots, r_{\varphi(n)}\}$ редуковани систем остатака по модулу n, постоји пермутација σ индекса $\{1, 2, \ldots, \varphi(n)\}$, тако да је $ar_i \equiv r_\sigma(i) \pmod{n}$. Посматрајмо једначине

$$\begin{aligned}
ar_1 &\equiv r_\sigma(1) \pmod{n} \\
ar_2 &\equiv r_\sigma(2) \pmod{n} \\
&\cdots \\
ar_{\varphi(n)} &\equiv r_\sigma(\varphi(n)) \pmod{n}.
\end{aligned}$$

Ако их измножимо добијамо $a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_\sigma(1) r_\sigma(2) \cdots r_\sigma(\varphi(n)) \pmod{n}$. Како је σ пермутација индекса, производ $r_\sigma(1) r_\sigma(2) \cdots r_\sigma(\varphi(n))$ је једнак производу $r_1 r_2 \cdots r_{\varphi(n)}$. Дакле, $a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$, и знајући да је нзд$(r_1r_2\cdots r_{\varphi(n)}, n) = 1$, можемо искористити тврђење 6.51 да добијемо $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Последица 6.66 *(Мала Фермаова*[14] *теорема) Нека је p прост број и p не дели позитиван број a. Тада је $a^{p-1} \equiv 1 \pmod{p}$.*

Доказ. Јасно је да су a и p узајамно прости, па су испуњени услови теореме 6.65. Тада је $a^{\varphi(p)} \equiv 1 \pmod{p}$. Доказ је комплетан, ако се сетимо да за прост број важи $\varphi(p) = p - 1$. $\square$

Пример 6.67 *Одредити остатак при дељењу броја 4^{1000} са 7.*

Бројеви 4 и 7 су узајамно прости, па можемо применити теорему 6.65. Дакле, $4^{\varphi(7)} \equiv_7 1$, то јест $4^6 \equiv_7 1$. Како је $1000 \equiv_6 4$, то је $1000 = 6k + 4$, за неко $k \in \mathbb{Z}$. Приметимо да нам није битно који је тачно број k. Сада важи

$$4^{1000} \equiv 4^{6k+4} \equiv (4^6)^k \cdot 4^4 \equiv 1^k \cdot 16^2 \equiv 1 \cdot 2^2 \equiv 4 \pmod{7},$$

па је тражени остатак број 4.

Пример 6.68 *Одредити последњу цифру броја $33^{55^{77}}$.*

Заправо треба одредити остатак при дељењу датог броја са 10. Како је $33 \equiv_{10} 3$, важи $33^{55^{77}} \equiv_{10} 3^{55^{77}}$. Бројеви 3 и 10 су узајамно прости, па је $3^{\varphi(10)} \equiv_{10} 1$. Како је $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$, важи $3^4 \equiv_{10} 1$. Треба одредити остатак при дељењу 55^{77} са 4. Важи $55^{77} \equiv_4 3^{77}$. Бројеви 3 и 4 су узајамно прости, па можемо поново применити Ојлерову теорему: $3^{\varphi(4)} \equiv_4 1$, то јест $3^2 \equiv_4 1$. Приметимо још да је $77 \equiv_2 1$. Сада можемо да спојимо све закључке:

$$55^{77} \equiv 3^{77} \equiv 3^{2k+1} \equiv (3^2)^k \cdot 3 \equiv 3 \pmod{4}.$$

То значи да је број 55^{77} облика $4l + 3$, за $l \in \mathbb{Z}$. Вратимо се на полазни број:

$$33^{55^{77}} \equiv 3^{55^{77}} \equiv 3^{4l+3} \equiv (3^4)^l \cdot 3^3 \equiv 1 \cdot 27 \equiv 7 \pmod{10}.$$

Дакле, последња цифра датог броја је 7.

Задаци

1. Доказати да је $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
2. Доказати да за сваки број $n \geq 1$ важи $\frac{5}{1\cdot 2} + \frac{13}{2\cdot 3} + \cdots + \frac{2n^2+2n+1}{n(n+1)} = \frac{n(2n+3)}{n+1}$.
3. Доказати да за свако $n \geq 2$ важи $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+n} > \frac{13}{24}$.
4. Доказати да за свако $n \geq 2$ важи $\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$.
5. Доказати да за свако $n \geq 2$ важи $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$.
6. Доказати да је за сваки природни број n број $3 \cdot 5^{2n+1} + 2^{3n+1}$ дељив са 17.
7. Доказати да је број $n \cdot 4^{n+1} - (n+1)4^n + 1$ дељив са 9 за сваки $n \in \mathbb{N}$.
8. Нека је $a_0 = 1, a_1 = 4$ и за све $n \geq 0$ важи формула $a_{n+2} = 4a_{n+1} - 4a_n$. Доказати да је $a_n = 2^n + n \cdot 2^n$, за све $n \geq 0$.

[14] Pierre de Fermat (1601-1665), француски математичар

9. Користећи математичку индукцију доказати да је $\cos\frac{\pi}{2^n}$ ирационалан број, за сваки број $n \geq 1$.

10. Доказати да је $f_1 + 2f_2 + 3f_3 + \cdots + nf_n = nf_{n+2} - f_{n+3} + 2$, за све $n \geq 0$.

11. Доказати да је $f_n \geq \left(\frac{3}{2}\right)^{n-1}$ за свако $n \geq 6$.

12. Користећи Еуклидов алгоритам одредити највећи заједнички делилац бројева 18876 и 5775 и одредити бројеве x и y тако да $18876x + 5775y =$ нзд$(18876, 5775)$.

13. Испитати да ли једначина $6006x + 1955y = 30$ има целобројна решења и ако има одредити опште решење.

14. Одредити остатак при дељењу броја 17^{2012} са 7.

15. Решити једначину $15x \equiv_{33} 18$.

16. Решити систем конгруенција: $x \equiv_7 1 \qquad x \equiv_9 4 \qquad x \equiv_5 3$.

17. Одредити последње две цифре броја 2011^{4043}.

18. Доказати да је број $3333^{7777} + 7777^{3333}$ дељив са 10.

19. Одредити остатак при дељењу броја $5^{5^{5^5}}$ са 17.

20. Одредити остатак при дељењу 1943^{1942} са 5, 7 и 35.

7 Булове алгебре

Задаци

8 Исказна логика

Исказ је реченица која је или тачна или нетачна. За исказ који је тачан кажемо и да има исказну вредност $\top$(те) или 1, а за исказ који није тачан кажемо да има исказну вредност $\perp$(не те) или 0. Од исказа се могу формирати сложени искази. Основна особина сложених исказа је то да је његова истинитосна вредност потпуно одређена истинитосном вредношћу исказа који фигуришу у њему. Сложени искази се формирају уз помоћ исказних операција које ћемо навести.

Дефиниција 8.1 *Конјункција исказа p и q је исказ $p \wedge q$ ("p и q"). Тачан је ако су тачни и p и q. У свим осталим случајевима је нетачан.*

Дефиниција 8.2 *Дисјункција исказа p и q је исказ $p \vee q$ ("p или q"). Нетачан је ако су нетачни и p и q. У свим осталим случајевима је тачан.*

Дефиниција 8.3 *Импликација исказа p и q је исказ $p \Rightarrow q$ ("p повлачи q"). Нетачан је ако је тачан p и нетачан q. У свим осталим случајевима је тачан.*

Исказ $p \Rightarrow q$ још читамо и "ако p онда q" и "из p следи q".

Дефиниција 8.4 *Еквиваленција исказа p и q је исказ $p \Leftrightarrow q$ ("p ако и само ако q"). Тачан је ако p и q имају једнаке истинитосне вредности - оба су тачна или су оба нетачна. У осталим случајевима је нетачан.*

Дефиниција 8.5 *Негација исказа p је исказ $\neg p$ ("не p"). Тачан је ако је p нетачан.*

Дефиниција 8.6 *Ексклузивна дисјункција исказа p и q је исказ* $p \veebar q$ *("или p или q"). Тачан је ако p и q имају различите истинитосне вредности - p тачно и q нетачно или p нетачно и q тачно. У осталим случајевима је нетачан.*

Претходне дефиниције су дате таблицама:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

p	q	$p \veebar q$
0	0	0
0	1	1
1	0	1
1	1	0

p	$\neg p$
0	1
1	0

Исказна алгебра састоји се од логичких константи, исказних слова и логичких везника. Логичке константе су $\top$ и $\bot$. Као и у претходним дефиницијама исказе означавамо уз помоћ исказних слова (или исказних промењљивих), најче71е су то слова $p, q, r, s, t \dots$ или $p_0, p_1, p_2 \dots$. Скуп исказних слова ћемо означавати са P. Скуп логичких везника је $\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \veebar\}$. Дефинишимо сада исказне формуле.

Дефиниција 8.7 *1. Исказна слова и логичке константе су исказне формуле.*
2. Ако су A и B исказне формуле, тада су исказне формуле и

$$\neg A \qquad A \wedge B \qquad A \vee B \qquad A \Rightarrow B \qquad A \Leftrightarrow B \qquad A \veebar B.$$

Исказне формуле се добијају једино коначном применом правила 1 и 2.

Напомена 8.8 *У дефиницијама 8.1 – 8.6 описали смо шта је конјункција два исказа, дисјункција два исказа, и тако даље. Исто је са формулама:*

- *конјункција формула A и B је формула која је тачна када су тачне формуле A и B;*
- *дисјункција* $A \vee B$ *је нетачна једино ако су обе формуле нетачне;*
- *импликација* $A \Rightarrow B$ *је нетачна једино ако је A тачна, а B нетачна;*
- *еквиваенција* $A \Leftrightarrow B$ *је тачна ако формуле A и B имају исте истинитоне вредности;*
- *негација* $\neg A$ *је тачна кад је A нетачна;*
- *ексклузивна дисјункција* $A \veebar B$ *је тачна кад формуле A и B имају различите истинитосне вредности.*

Скуп свих формула ћемо означавати са For.

Дефиниција 8.9 *Валуација је било која функција* $v : P \to \{0, 1\}$.

Пример 8.10 *Нека је* $P = \{p, q, r\}$. *Са* $v(p) = 0$, $v(q) = 1$ *и* $v(r) = 0$ *је задата једна валуација.*

Ако је $v : P \to \{0,1\}$ било која валуација, можемо је продужити до функције $v : For \to \{0,1\}$ на следећи начин:

$$\begin{array}{rcl}
v(c) & = & c, \text{ ако је } c \text{ логичка константа} \\
v(\neg A) & = & \neg v(A) \\
v(A \wedge B) & = & v(A) \wedge v(B) \\
v(A \vee B) & = & v(A) \vee v(B) \\
v(A \Rightarrow B) & = & v(A) \Rightarrow v(B) \\
v(A \Leftrightarrow B) & = & v(A) \Leftrightarrow v(B) \\
v(A \veebar B) & = & v(A) \veebar v(B), \text{ за све } A, B \in For.
\end{array}$$

Пример 8.11 *Неко је валуација као у претходном примеру и формула* $(p \vee q) \Rightarrow (p \vee r)$*. Одредити истинитосну вредност ове формуле*

$$\begin{array}{rcl}
v(p \vee q) \Rightarrow (p \vee r)) & = & v(p \vee q) \Rightarrow v(p \vee r) \\
& = & (v(p) \vee v(q)) \Rightarrow (v(p) \vee v(r)) \\
& = & (0 \vee 1) \Rightarrow (0 \vee 0) \\
& = & 1 \Rightarrow 0 \\
& = & 0,
\end{array}$$

што значи да дата формула није тачна и валуацији v. Приметимо да ако задамо другу валуцију $v' : P \to \{0,1\}$ са $v'(p) = 0$, $v'(q) = 0$ и $v'(r) = 1$ добијамо

$$\begin{array}{rcl}
v'(p \vee q) \Rightarrow (p \vee r)) & = & v'(p \vee q) \Rightarrow v'(p \vee r) \\
& = & (v'(p) \vee v'(q)) \Rightarrow (v'(p) \vee v'(r)) \\
& = & (0 \vee 0) \Rightarrow (0 \vee 1) \\
& = & 0 \Rightarrow 1 \\
& = & 1,
\end{array}$$

што значи да је формула тачна у валуацији v'. △

При записивању формула користе се правила о приоритету логичких операција, уведених да би запис био једноставнији. Највећи приоритет има операција $\neg$, средњег приоритета су операције $\wedge$ и $\vee$, а најмањег операције $\Rightarrow, \Leftrightarrow, \veebar$. Са леве стране су дате формуле без примене правила о приоритету операција, а са десне исте те формуле записане уз помоћ наведених правила. Нагласимо да је и једно и друго исправно, предност другог записа је у једноставности.

$$\begin{array}{cc}
(\neg p) \wedge q & \neg p \wedge q \\
(p \vee q) \Leftrightarrow r & p \vee q \Leftrightarrow r \\
((p \veebar q) \wedge (\neg r)) \Rightarrow (p \vee (q \wedge r)) & (p \veebar q) \wedge \neg r \Rightarrow p \vee (q \wedge r)
\end{array}$$

Важне су нам формуле које су тачне у свим валуацијама својих промењљивих.

Дефиниција 8.12 *Формула A је таутологија ако је $v(A) = 1$ за све валуације v. Ако за сваку валуацију v важи $v(A) = 0$, онда кажемо да је A контрадикција.*

Дефиниција 8.13 *Формула A је задовољива ако постоји валуација v тако да је $v(A) = 1$. Скуп формула Φ је задовољив ако постоји валуација v тако да је $v(A) = 1$ за све формуле $A \in \Phi$.*

Дефиниција 8.14 *Подформула формуле A је једно од следећег:*

1. *A је подформула формуле A.*

2. *Ако је $\neg B$ подформула од A, тада је и B подформула од A.*

3. *Ако је $B * C$ подформула од A, где је $*$ један од симбола $\wedge, \vee, \Rightarrow, \Leftrightarrow, \veebar$, онда су и B и C подформуле од A.*

Пример 8.15 *Одредити све подформуле формуле $\neg p \wedge q \Rightarrow (r \Rightarrow q)$.*

$$\begin{array}{lcl} \neg p \wedge q & \Rightarrow & (r \Rightarrow q) \\ \neg p \wedge q & & r \Rightarrow q \\ \neg p \quad q & & r \quad q \\ \ \ p & & \end{array}$$

$\triangle$

Пример 8.16 *Доказати да је формула $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ таутологија.*

Како се у датој формули јављају три исказна слова, постоји укупно $2 \cdot 2 \cdot 2 = 8$ различитих валуација тих променљивих. Испитиваћемо тачност формуле у свакој од тих валуација. То се најпрегледније може представити таблицом.

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$	$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
0	0	0	0	0	0	0	1
0	0	1	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	1	1
1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1

У свакој валуацији дата формула има вредност 1, па јесте таутологија.

Постоји још један начин прављења истинитосне таблице:

$(p$	$\vee$	$q)$	$\vee$	r	$\Leftrightarrow$	p	$\vee$	$(q$	$\vee$	$r)$
0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	1	1	0	1	0	1	1
0	1	1	1	0	1	0	1	1	1	0
0	1	1	1	1	1	0	1	1	1	1
1	1	0	1	0	1	1	1	0	0	0
1	1	0	1	1	1	1	1	0	1	1
1	1	1	1	0	1	1	1	1	1	0
1	1	1	1	1	1	1	1	1	1	1

Овде се испод сваког појављивања исказног слова налазе одговарајуће вредности у валуацијама. Такође, резултат примене неке логичке операције се пише испод симбола за ту операцију. Тако се испод првог знака $\vee$ са леве стране налазе истинитосне вредности за подформулу $p \vee q$, испод другог знака $\vee$ се налазе истинитосне вредости за подформулу $(p \vee q) \vee r$, и тако даље. Да је формула таутологија, примећујемо из чињенице да се у таблици испод симбола $\Leftrightarrow$ налазе само јединице. $\triangle$

Пример 8.17 *Доказати да је формула $F = (p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ таутологија.*

Користићемо метод свођења на апсурд. Претпоставимо да формула није таутологија. Тада постоји валуација v тако да $v\big((p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))\big) = 0$. Импликација је једино нетачна ако је подформула $F_1 = (p \Rightarrow (q \Rightarrow r))$ тачна у тој валуацији, а $F_2 = ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ нетачна у тој валуацији . Пошто је $v(F_2) = 0$, мора бити $F_2' = p \Rightarrow q$ тачна у v, а $F_2'' = p \Rightarrow r$ нетачна у v. Из $v(F_2'') = 0$ следи да је $v(p) = 1$ и $v(r) = 0$. Важи $v(F_2') = 1$, то јест $v(p \Rightarrow q) = 1$, а како је $v(p) = 1$, онда је и $v(q) = 1$. Вратимо се на подформулу F_1:

$$\begin{aligned}
v\big((p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))\big) &= 0\\
(v(p) \Rightarrow (v(q) \Rightarrow v(r))) \Rightarrow ((v(p) \Rightarrow v(q)) \Rightarrow (v(p) \Rightarrow v(r))) &= 0\\
(1 \Rightarrow (1 \Rightarrow 0)) \Rightarrow ((1 \Rightarrow 1) \Rightarrow (1 \Rightarrow 0)) &= 0\\
(1 \Rightarrow 0) \Rightarrow (1 \Rightarrow 0) &= 0\\
0 \Rightarrow 0 &= 0\\
1 &= 0,
\end{aligned}$$

што је немогуће. $\triangle$

Пример 8.18 *Доказати да су следеће формуле таутологије:*

1. $p \wedge 1 \Leftrightarrow p$
2. $p \wedge 0 \Leftrightarrow 0$
3. $p \vee 1 \Leftrightarrow 1$
4. $p \vee 0 \Leftrightarrow p$
5. $(1 \Rightarrow p) \Leftrightarrow p$
6. $(0 \Rightarrow p) \Leftrightarrow 1$
7. $(p \Rightarrow 1) \Leftrightarrow 1$
8. $(p \Rightarrow 0) \Leftrightarrow \neg p$

Сви примери се могу лако доказати. Ове кратке таутологије ћемо често користити у другим доказима. $\triangle$

Пример 8.19 *Наведимо неке битне таутологије:*

$p \wedge p \Leftrightarrow p$	*закон идемпотентности за конјункцију*
$p \vee p \Leftrightarrow p$	*закон идемпотентности за дисјункцију*
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	*закон асоцијативности за конјункцију*
$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	*закон асоцијативности за дисјункцију*
$p \wedge q \Leftrightarrow q \wedge p$	*закон комутативности за конјункцију*
$p \vee q \Leftrightarrow q \vee p$	*закон комутативности за дисјункцију*
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	*закон дистрибуције конјункције према дисјункцији*
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	*закон дистрибуције дисјункције према конјункцији*
$\neg\neg p \Leftrightarrow p$	*закон двоструке негације*
$p \vee \neg p$	*закон искључења трећег*
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	*Де Морганов закон*
$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	*Де Морганов закон*
$(p \wedge q) \Rightarrow p$	*слабљење конјункције*
$p \Rightarrow (p \vee q)$	*увођење дисјункције*
$p \Rightarrow p$	*закон рефлексивности за импликацију*
$p \Leftrightarrow p$	*закон рефлексивности за еквиваленцију*
$p \wedge (p \vee q) \Leftrightarrow p$	*закон апсорпције конјункције према дисјункцији*
$p \vee (p \wedge q) \Leftrightarrow p$	*закон апсорпције дисјункције према којункцији*
$(p \wedge (p \Rightarrow q)) \Rightarrow q$	*модус поненс*
$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$	*правило уклањања импликације*
$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$	*правило уклањања еквиваленције*
$(p \veebar q) \Leftrightarrow \neg(p \Leftrightarrow q)$	*правило уклањања ексклузивне дисјункције*
$((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Rightarrow (p \Leftrightarrow r)$	*закон транзитивности за еквиваленцију*
$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	*закон контрапозиције*
$(\neg p \Rightarrow (q \wedge \neg q)) \Rightarrow p$	*правило свођења на апсурд*
$(p \vee q) \wedge (q \vee r) \wedge (r \vee p) \Leftrightarrow$	
$(p \wedge q) \vee (q \wedge r) \vee (r \wedge p)$	*Дедекиндов закон*

Свака од ових таутологија може се лако доказати, на пример кори71ењем методе таблице истинитости. △

Напомена 8.20 *Нека је φ било која таутологија у којој се појављују исказна слова $p_1, p_2, \ldots, p_k$. Ако заменимо симболе тих исказних слова са симболима било којих исказних формула $A_1, A_2, \ldots, A_k$, добијамо формулу која је такође таутологија. На пример, формула $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ је таутологија за било које исказне формуле A и B. За избор $A = p \Leftrightarrow q$ и $B = p \vee r$ добијамо таутологију $\neg((p \Leftrightarrow q) \wedge (p \vee r)) \Leftrightarrow \neg(p \Leftrightarrow q) \vee \neg(p \vee r)$. За ту формулу кажемо да је изведена из таутологије $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$.*

Пример 8.21 *Доказати да је формула $(p \Rightarrow (q \vee r)) \Leftrightarrow (p \Rightarrow q) \vee (p \Rightarrow r))$ таутологија.*

Користићемо методу дискусије по исказном слову. Нека је v било која валуација наведених исказних слова. Ако је $v(p) = 1$ добијамо да је

$$\begin{aligned}
v\big((p \Rightarrow (q \vee r)) \Leftrightarrow (p \Rightarrow q) \vee (p \Rightarrow r))\big) &= v\big((p \Rightarrow (q \vee r))\big) \Leftrightarrow v\big((p \Rightarrow q) \vee (p \Rightarrow r))\big) \\
&= (v(p) \Rightarrow v(q \vee r)) \Leftrightarrow (v(p) \Rightarrow v(q)) \vee (v(p) \Rightarrow v(r))) \\
&= (1 \Rightarrow v(q \vee r)) \Leftrightarrow (1 \Rightarrow v(q)) \vee (1 \Rightarrow v(r))) \\
&\quad \text{(користићемо пример 8.18 (5))} \\
&= v(q \vee r) \Leftrightarrow (v(q) \vee v(r)) \\
&= v\big(q \vee r \Leftrightarrow q \vee r\big) \\
&\quad \text{(користићемо закон рефлексивности} \\
&\quad \text{за } \Leftrightarrow \text{ и напомену 8.20)} \\
&= v(1) = 1.
\end{aligned}$$

Дакле, у том случају је формула тачна. Ако је $v(p) = 0$, онда је слично

$$\begin{aligned} v\big((p \Rightarrow (q \vee r)) \Leftrightarrow (p \Rightarrow q) \vee (p \Rightarrow r))\big) &= (v(p) \Rightarrow v(q \vee r)) \Leftrightarrow (v(p) \Rightarrow v(q)) \vee (v(p) \Rightarrow v(r))) \\ &= (0 \Rightarrow v(q \vee r)) \Leftrightarrow (0 \Rightarrow v(q)) \vee (0 \Rightarrow v(r))) \\ &\quad \text{(користићемо пример 8.18 (6))} \\ &= 1 \Leftrightarrow (1 \vee 1) = 1 \Leftrightarrow 1 = 1. \end{aligned}$$

У овом случају је формула такође тачна, тако да закључујемо да јесте таутологија. △

Пример 8.22 *Нека су A, B, C, D исказне формуле такве да су формуле $A \vee B$, $A \Rightarrow C$, $B \Rightarrow D$ таутологије. Доказати да је $C \vee D$ таутологија.*

Прво приметимо да овде не можемо користити методу истинитосних таблица, јер су дате формуле, а не исказна слова. Претпоставимо да формула $C \vee D$ није таутологија. То значи да постоји валуација v тако да $v(C \vee D) = 0$. Мора бити $v(C) = 0$ и $v(D) = 0$, јер је једино у том случају дисјункција нетачна. Како је $A \Rightarrow C$ таутологија, онда је та формула тачна у свакој валуацији, па и у v. Следи да $v(A \Rightarrow C) = 1$, а како је $v(C) = 0$, важи да $v(A) = 0$. Даље, $A \vee B$ је таутологија, па је $v(A \vee B) = 1$, а заједно са претходним добијамо да $v(B) = 1$. Искористимо још чињеницу да је $B \Rightarrow D$ таутологија. Важи $v(B \Rightarrow D) = 1$, а онда је и $v(D) = 1$. Вратимо се на почетак: имали смо да је $v(D) = 0$. Добијамо да је формула D и тачна и нетачна у валуацији v, што је немогуће. Следи да је полазна претпоставка била погрешна, то јест $C \vee D$ јесте таутологија. △

Пример 8.23 *Доказати скуповни идентитет $A \setminus (B \cup C) = (A \setminus B) \setminus C$ користеци исказну логику.*

Сетимо се да су два скупа X и Y једнака ако имају исте елементе, то јест ако је $(\forall x) x \in X \Leftrightarrow x \in Y$. Тада је

$$\begin{aligned} A \setminus (B \cup C) = (A \setminus B) \setminus C \quad &\text{акко} \quad (\forall x) x \in A \setminus (B \cup C) \Leftrightarrow x \in (A \setminus B) \setminus C \\ &\text{акко} \quad (\forall x) x \in A \wedge (x \notin B \cup C) \Leftrightarrow (x \in A \setminus B) \wedge x \notin C \\ &\text{акко} \quad (\forall x) x \in A \wedge \neg(x \in B \cup C) \Leftrightarrow (x \in A \wedge x \notin B) \wedge \neg(x \in C) \\ &\text{акко} \quad (\forall x) x \in A \wedge \neg(x \in B \vee x \in C) \Leftrightarrow (x \in A \wedge \neg x \in B) \wedge \neg(x \in C). \end{aligned}$$

Израз $x \in A$ је може имати вредност тачно ил нетачно, па је $x \in A$ исказ. Назовимо га p. Слично, исказе $x \in B$ и $x \in C$ можемо означити са q и r. Добијамо формулу $F = p \wedge \neg(q \vee r) \Leftrightarrow (p \wedge \neg q) \wedge \neg r$. Скуповни идентитет је тачан ако и само ако за свако x важи последња еквиваленција, то јест ако и само ако је формула F таутологија. Проверимо да ли је F таутологија помоћу истинитосне таблице.

p	$\wedge$	$\neg$	$(q$	$\vee$	r	$\Leftrightarrow$	$(p$	$\wedge$	$\neg$	$q)$	$\wedge$	$\neg$	$r)$
0	0	1	0	0	0	1	0	0	1	0	0	1	0
0	0	0	0	1	1	1	0	0	1	0	0	0	1
0	0	0	1	1	0	1	0	0	0	1	0	1	0
0	0	0	1	1	1	1	0	0	0	1	0	0	1
1	1	1	0	0	0	1	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1	1	1	0	0	0	1
1	0	0	1	1	0	1	1	0	0	1	0	1	0
1	0	0	1	1	1	1	1	0	0	1	0	0	1

То смо могли закључити и на другачији начин. Како је $\neg(q \vee r) \Leftrightarrow \neg q \wedge \neg r$, формула је еквивалентна са $p \wedge (\neg q \wedge \neg r) \Leftrightarrow (p \wedge \neg q) \wedge \neg r$. Последња формула је таутологија због асоцијативности коњукције. У сваком случају, следи да је полазна скуповна једнакост тачна. $\triangle$

Приметимо да основне дефиниције операција над скуповима можемо описати и логичким језиком:

$$\begin{array}{rcl}
A = B & \text{акко} & (\forall x) x \in A \Leftrightarrow x \in B \\
A \subseteq B & \text{акко} & (\forall x) x \in A \Rightarrow x \in B \\
A \cap B & = & \{x \mid x \in A \wedge x \in B\} \\
A \cup B & = & \{x \mid x \in A \vee x \in B\} \\
A \setminus B & = & \{x \mid x \in A \wedge \neg x \in B\} \\
A \triangle B & = & \{x \mid x \in A \veebar x \in B\} \\
A^c & = & \{x \mid \neg x \in A\}
\end{array}$$

То нам омогућава да користимо исказну логику у доказивању скуповних идентитета.

Пример 8.24 *Низови исказних формула су дати са*

$$\begin{array}{ll}
A_0 = p & A_{n+1} = A_n \wedge B_n \\
B_0 = q & B_{n+1} = B_n \Rightarrow A_n,
\end{array}$$

где су p и q исказна слова. Доказати да A_n и B_n нису таутологије ни за једно $n \geq$.

Посматрајмо прво формуле A_n. Како је A_0 исказно слово, постоји валуација v у којој је $v(p) = v(A_0) = 0$. Докажимо да је свака формула A_n нетачна у валуацији v. Како је A_{n+1} конјункција претходне формуле A_n и формуле B_n, ако је A_n нетачно у v, мора бити и A_{n+1} јер је конјукција натечна чим је нетачна једна од формула које је формирају. Зато ћемо у доказу користити математичку индукцију. За $n = 0$ је $v(A_0) = v(p) = 0$. Претпоставимо да је $v(A_n) = 0$. Докажимо да је $v(A_{n+1}) = 0$. Важи

$$v(A_{n+1}) = v(A_n \wedge B_n) = v(A_n) \wedge v(B_n) = 0 \wedge v(B_n) = 0.$$

Како за сваку формулу A_n постоји валуација (и то једна те иста валуација v) тако да је $v(A_n) = 0$, то значи да ниједна од тих формула на може бити таутологија.

Докажимо сада да формуле B_n нису таутологије. Јасно је да постоју валуација v тако да $v(A_0) = 0$. У претходном делу смо доказали да је у тој валуацији нетачна и свака друга формула A_n. У тој валуацији такође важи:

$$\begin{array}{rcl}
v(B_1) & = & v(B_0 \Rightarrow A_0) = v(B_0) \Rightarrow v(A_0) = v(B_0) \Rightarrow 0 = \neg v(B_0) \\
v(B_2) & = & v(B_1 \Rightarrow A_1) = v(B_1) \Rightarrow v(A_1) = \neg v(B_0) \Rightarrow 0 = \neg\neg v(B_0) = v(B_0) \\
v(B_3) & = & v(B_2 \Rightarrow A_2) = v(B_2) \Rightarrow v(A_2) = v(B_0) \Rightarrow 0 = \neg v(B_0) \\
v(B_4) & = & v(B_3 \Rightarrow A_3) = v(B_3) \Rightarrow v(A_3) = \neg v(B_0) \Rightarrow 0 = \neg\neg v(B_0) = v(B_0) \\
\ldots & &
\end{array}$$

Ако изаберемо валуацију v_1 тако да $v_1(A_0) = 0$ и $v_1(B_0) = 0$ видимо да су у тој валуацији нетачне све формуле B_k за паран број k. Ако изаберемо валуацију v_2 тако да $v_2(A_0) = 0$ и $v_2(B_0) = 1$, онда су у тој валуацији нетачне формуле B_k за непаран број k. Докажимо ово математичком индукцијом. Како су $p = A_0$ и $q = B_0$ исказна слова, постоји v_1 тако да $v_1(A_0) = 0$ и $v_1(B_0) = 0$. Већ смо закључили да је $v_1(A_n) = 0$ за свако n. Докажимо да је $v_1(B_{2m}) = 0$ за свако природни број м. За $m = 0$ је $v_1(B_0) = 0$. Претпоставимо да је $v_1(B_{2m}) = 0$. Докажимо да је $v_1(B_{2(m+1)}) = 0$. Важи

$$\begin{array}{rcl}
v_1(B_{2(m+1)}) & = & v_1(B_{2m+2}) = v_1(B_{2m+1}) \Rightarrow v_1(A_{2m+1}) = v_1(B_{2m} \Rightarrow A_{2m}) \Rightarrow 0 \\
& = & (v_1(B_{2m}) \Rightarrow 0) \Rightarrow 0 = (0 \Rightarrow 0) \Rightarrow 0 = 1 \Rightarrow 0 = 0
\end{array}$$

Слично, постоји v_2 тако да $v_2(A_0) = 0$ и $v_2(B_0) = 1$ и користећи математичку индукцију може се доказати да је $v_2(B_{2m+1}) = 0$ за сваки природни број m. Тако да за сваку формулу B_n постоји валуација (v_1 или v_2) у којој је та формула нетачна, па ниједна од наведених није таутологија. $\triangle$

8.1 Метод таблоа

Дефиниција 8.25 *Ако је A исказна формула, онда су $\top A$ и $\bot A$ означене формуле. Формула $\top A$ је тачна у некој валуацији ако је тачна A у тој валуацији, а нетачна иначе. Формула $\bot A$ је тачна у некој валуацији ако је A нетачна у тој валуацији, а нетачна иначе.*

Формулу $\top A$ читамо "тачно је A", а формулу $\bot A$ читамо "нетачно је A".

Постоје две групе правила за формирање таблоа:

- правила која не доводе до гранања (...и...); називају се α правила, а одговарајуће формуле су формуле типа α. Правила типа α су:

$$\begin{array}{c} \top(\neg A) \\ | \\ \bot A \end{array} \qquad \begin{array}{c} \bot(\neg A) \\ | \\ \top A \end{array} \qquad \begin{array}{c} \top(A \land B) \\ | \\ \top A \\ | \\ \top B \end{array} \qquad \begin{array}{c} \bot(A \lor B) \\ | \\ \bot A \\ | \\ \bot B \end{array} \qquad \begin{array}{c} \bot(A \Rightarrow B) \\ | \\ \top A \\ | \\ \bot B \end{array}$$

- правила која доводе до гранања (...или...); називају се β правила, а одговарајуће формуле су формуле типа β. Правила типа β су:

$$\begin{array}{c} \bot(A \land B) \\ \swarrow \quad \searrow \\ \bot A \quad \bot B \end{array} \qquad \begin{array}{c} \top(A \lor B) \\ \swarrow \quad \searrow \\ \top A \quad \top B \end{array} \qquad \begin{array}{c} \top(A \Rightarrow B) \\ \swarrow \quad \searrow \\ \bot A \quad \top B \end{array}$$

Приметимо да су правила за конструкцију таблоа неког од облика:

$$\begin{array}{c} \alpha \\ | \\ \alpha_1 \end{array} \qquad \begin{array}{c} \alpha \\ | \\ \alpha_1 \\ | \\ \alpha_2 \end{array} \qquad \begin{array}{c} \beta \\ \swarrow \quad \searrow \\ \beta_1 \quad \beta_2 \end{array}$$

Дефиниција 8.26 *Табло за формулу A је бинарно дрво у чијем сваком чвору се налазе означене формуле и који се конструише на следећи начин:*

- *У корену дрвета је формула $\bot A$.*
- *Ако нека грана од корена до листа садржи формулу типа α која није искори71ена у тој грани, онда листу те гране додајемо један чвор са означеном формулом α_1 или два чвора један за другим са означеним формулама α_1 и α_2 (у зависности од врсте α формуле).*
- *Ако нека грана од корена до листа садржи формулу типа β која није искори71ена у тој грани, онда листу те гране додајемо два чвора која воде из тог листа са означеним формулама β_1 и β_2.*

Дефиниција 8.27 *Кажемо да је грана таблоа за исказну формулу A затворена ако се на њој налазе формуле $\top B$ и $\bot B$. Табло за формулу A је затворен ако је свака његова грана затворена.*

Може се доказати да је исказна формула таутологија ако и само ако је табло за ту формулу затворен.

Пример 8.28 *Методом таблоа доказати да је формула* $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$ *таутологија.*

$$1.\bot (p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$$
$$2.\top (p \Rightarrow q) \ \ (1)$$
$$3.\bot (\neg q \Rightarrow \neg p) \ \ (1)$$
$$4.\top (\neg q) \ \ (3)$$
$$5.\bot (\neg p) \ \ (3)$$
$$6.\bot (q) \ \ (4)$$
$$7.\top (p) \ \ (5)$$

- $8.\bot(p)$ (2) — $X(7,8)$
- $9.\top(q)$ (2) — $X(6,9)$

Приметимо да се, јасноће ради, после сваке формуле пише из које је изведена, као и да на крају сваке гране пишемо због којих формула се грана затвара. Затарање гране, као што се види из примера, означавамо са X. $\triangle$

Пример 8.29 *Методом таблоа доказати да је формула* $(p \vee (q \wedge r)) \Rightarrow ((p \vee q) \wedge (p \wedge r))$ *таутологија.*

$$1.\bot\big((p \vee (q \wedge r)) \Rightarrow ((p \vee q) \wedge (p \wedge r))\big)$$
$$2.\top (p \vee (q \vee r)) \ \ (1)$$
$$3.\bot ((p \vee q) \wedge (p \wedge r)) \ \ (1)$$

- $4.\bot(p \vee q)$ (3)
  - $6.\bot(p)$ (4)
  - $7.\bot(q)$ (4)
    - $10.\top(p)$ (2) — $X(6,10)$
    - $11.\top(q \wedge r)$ (2)
      - $12.\top(q)$ (11)
      - $13.\top(r)$ (11) — $X(7,12)$
- $5.\bot(p \vee r)$ (3)
  - $8.\bot(p)$ (5)
  - $9.\bot(r)$ (5)
    - $14.\top(p)$ (2) — $X(8,14)$
    - $15.\top(q \wedge r)$ (2)
      - $16.\top(q)$ (15)
      - $17.\top(r)$ (15) — $X(9,17)$

$\triangle$

8.2 Логичка еквивалентност

Дефиниција 8.30 *Формуле A и B су логички еквивалентне ако за сваку валуацију v важи $v(A) = v(B)$. Пишемо $A \equiv B$.*

Дакле, формуле су логички еквивалентне ако имају једнаке истинитосне таблице. Важи и да је $A \equiv B$ ако и само ако је $A \Leftrightarrow B$ таутологија. Лако се може проверити да је $\equiv$ релација еквиваленције на скупу свих исказаних формула For.

Пример 8.31 *Одредити све логички нееквивалентне формуле A у којима фигуришу искључиво исказна слова p и q тако да је формула $q \Rightarrow ((A \wedge p) \vee (A \wedge q))$ таутологија.*

Користећи пример 8.18 попуњавамо истинитосну таблицу:

	p	q	$A \wedge p$	$A \wedge q$	$(A \wedge p) \vee (A \wedge q)$	$q \Rightarrow ((A \wedge p) \vee (A \wedge q))$
v_1	0	0	0	0	0	1
v_2	0	1	0	$v_2(A)$	$v_2(A)$	$v_2(A)$
v_3	1	0	$v_3(A)$	0	$v_3(A)$	1
v_4	1	1	$v_4(A)$	$v_4(A)$	$v_4(A)$	$v_4(A)$

Да би формула $q \Rightarrow ((A \wedge p) \vee (A \wedge q))$ била таутологија, неопходно је да формула A буде тачна у валуацијама v_2 и v_4. Дакле, све формуле у којима фигуришу исказна слова p и q и тачне су у валуацијама v_2 и v_4 испуњавају услов задатка. Вредности тих формула су:

$$v_1(A) = * \qquad v_2(A) = 1 \qquad v_3(A) = * \qquad v_4(A) = 1, \text{ где је } * \in \{0, 1\}.$$

Потребно је одредити све такве логички нееквивалентне формуле, то јест све формуле које задовољавају услов задатка, а имају различите истинитосне таблице. Према претходном, све могуће таблице за фомулу A су

	A	A_1	A_2	A_3	A_4
v_1	$*$	0	0	1	1
v_2	1	1	1	1	1
v_3	$*$	0	1	0	1
v_4	1	1	1	1	1

Ставимо

$$A_1 = q \qquad A_2 = p \vee q \qquad A_3 = p \Rightarrow q \qquad A_4 = 1.$$

Овако задате формуле $A_1 - A_4$ имају одговарајуће таблице и јасно је да било која друга формула која задовољавају дати услов мора бити логички екввалентна некој од A_1, A_2, A_3, A_4. $\triangle$

Задаци

1. Користећи истинитосну таблицу доказати да је фотмула $((p \Rightarrow \neg q) \Rightarrow (r \wedge \neg p)) \Rightarrow (p \Rightarrow q)$ таутологија.

2. Методом свођења на апсурд доказати да је формула $((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow (q \wedge r))$ таутологија.

3. Методом дискусије по исказном слову доказати да је формула $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$ таутологија.

4. Нека су A, B, C, D формуле исказне логике. Ако су формуле $A \Leftrightarrow D$ и $A \veebar B$ таутологије, а $C \Leftrightarrow D$ контрадикција, доказати да је $B \Rightarrow C$ таутологија.

5. Доказати скуповни идентитет $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ користећи исказну логику.

6. Низови исказних формула су дати са

$$\begin{aligned} A_0 &= p \qquad & A_{n+1} &= (A_n \Rightarrow B_n) \Rightarrow A_n \\ B_0 &= q \qquad & B_{n+1} &= A_n \Rightarrow B_n, \end{aligned}$$

где су p и q исказна слова. Доказати да A_n и B_n нису таутологије ни за једно $n \geq$.

7. Методом таблоа доказати да је формула $(p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ таутологија.

8. Методом таблоа доказати да је формула $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ таутологија.

9. Методом таблоа доказати да је формула $(((p \Rightarrow r) \wedge (q \Rightarrow r)) \wedge (p \vee q)) \Rightarrow r$ таутологија.

10. Одредити све логички нееквивалентне формуле A у којима фигуришу искључиво исказна слова p и q тако да је формула $(A \vee p) \Rightarrow (A \vee \neg q)$ таутологија.

9 Формални системи

Формални систем или формална теорија је одређен када су испуњени следећи услови:

1. Дат је највише пребројив скуп симбола или азбука. Низ симбола представља реч.

2. Неки подскуп скупа свих речи је скуп формула. При том је дат и поступак помоћу ког се одређује да ли је нека реч формула или не.

3. Скуп аксиома је неки подскуп скупа свих формула.

4. Дат је коначан број правила изводења. Ако су $A_1, A_2, \ldots, A_{n-1}, A_n$ било које формуле, тада правило извођења α (дужине n) одлучује да ли из формула $A_1, A_2, \ldots, A_{n-1}$ следи формула A_n. Ако да, онда пишемо

$$\alpha : \frac{A_1, A_2, \ldots, A_{n-1}}{A_n}.$$

   Кажемо и да је A_n директна последица формула $A_1, A_2, \ldots, A_{n-1}$.

Дефиниција 9.1 *Коначни низ формула $A_1, A_2, \ldots, A_n$ неког формалног система је извођење или доказ ако за сваку формулу A_i важи да је или аксиома или је директна последица неких претходних формула тог низа (по неком правилу извођења).*

Дефиниција 9.2 *Формула A је теорема ако постоји извођење $A_1, A_2, \ldots, A_n$ тако да је $A_n = A$. Пишемо $\vdash A$.*

Дефиниција 9.3 *Формула A је последица скупа формула Γ ако постоји низ формула $A_1, A_2, \ldots, A_n$ тако да је $A_n = A$ и ако за сваку формулу A_i важи да је или аксиома или једна од формула скупа Γ или је директна последица неких претходних формула тог низа (по неком правилу извођења). Пишемо $\Gamma \vdash A$.*

Ако је $\Gamma = \{F_1, F_2, \ldots, F_k\}$ онда формуле $F_1, F_2, \ldots, F_k$ зовемо хипотезама и пишемо $F_1, F_2, \ldots, F_k \vdash A$.

Пример 9.4 *Нека се азбука формалног система $\mathcal{S}$ састоји од слова a и b. Нека су формуле речи облика $aba^m b^n$, где је a^m скраћени запис за $\underbrace{aa\ldots a}_{m \text{ пута}}$. Аксиоме су формуле $abab$, aba^2b и $abab^2$. Правила извођења су*

$$\alpha : \frac{aba^m b^n}{a^m bab^n}, \qquad \beta : \frac{aba^m b^n}{ab^n a^m b}, \qquad \gamma : \frac{aba^m b^n}{aba^{m+1} b^{n+1}}.$$

Доказати да је a^3b^4ab теорема у овом формалном систему.

Важи:

1.$abab^2$	аксиома
2.aba^2b^3	правило извођења γ примењено на формулу 1
3.aba^3b^4	правило извођења γ примењено на формулу 2
4.a^3bab^4	правило извођења α примењено на формулу 3
5.a^3b^4ab	правило извођења β примењено на формулу 4

Ово је једно извођење где је последња формула у низу a^3b^4ab, па наведена формула јесте теорема. △

Већ смо представили исказну логику. Формални систем који описује исказни рачун означавамо са $\mathcal{L}$ и називамо још Лукашиевичев[15] рачун. Симболи рачуна $\mathcal{L}$ су

$$\neg, \Rightarrow, (,), p, q, r, s \dots$$

Симболе $p, q, r, \dots$ називамо исказним словима. Исказне формуле се дефинишу на следећи начин:

1. Исказна слова су исказне формуле.
2. Ако су A и B исказне формуе, онда су и $\neg A$ и $A \Rightarrow B$ исказне формуле.

Исказне формуле се могу добити једино коначном применом 1 и 2.
Аксиоме исказног рачуна су:

Л1 $A \Rightarrow (B \Rightarrow A)$,

Л2 $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$,

Л3 $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$,

где су A, B, C произвољне формуле.
Једино правило извођења рачуна $\mathcal{L}$ је правило модус поненс:

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

Читамо "из A и $A \Rightarrow B$ по модус поненсу изводимо B".
Операције $\wedge, \vee, \Leftrightarrow$ дефинишемо са:

- $A \wedge B$ је замена за $\neg(A \Rightarrow \neg B)$;
- $A \vee B$ је замена за $\neg A \Rightarrow B$;
- $A \Leftrightarrow B$ је замена за $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Тврђење 9.5 *Формула $A \Rightarrow A$ је теорема.*

Доказ. Важи:

1.$(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$	аксиома Л2
2.$A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$	аксиома Л2
3.$(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$	МП на формуле 1 и 2
4.$A \Rightarrow (A \Rightarrow A)$	аксиома Л1
5.$A \Rightarrow A$	МП на формуле 3 и 4

Последња формула у овом извођењу је $A \Rightarrow A$, па наведена формула јесте теорема. □

[15] Jan Łukasiewicz (1878-1956), пољски математичар

Теорема 9.6 *(Теорема о дедукцији) Нека је Γ скуп формула исказне логике, а A нека формула. Ако је $\Gamma, A \vdash B$, онда је $\Gamma \vdash A \Rightarrow B$.*

Доказ. Докажимо за почетак једно помоћно тврђење. Нека је $\Gamma \subset For$ и $C, D \in For$. Ако је $\Gamma \vdash C$ онда је $\Gamma \vdash D \Rightarrow C$.

Из $\Gamma \vdash C$ следи да постоји низ формула $C_1, \ldots, C_k$ тако да $C_k = C$ и који представља извођење за C из Γ. Тада је

$$
\begin{array}{rll}
1. & C_1 & \\
2. & C_2 & \\
\vdots & & \\
k. & C & \\
k+1. & C \Rightarrow (D \Rightarrow C) & \text{аксиома Л1} \\
k+2. & D \Rightarrow C & \text{МП на формуле } k \text{ и } k+1,
\end{array}
$$

па постоји извођење за $D \Rightarrow C$ из Γ, то јест $\Gamma \vdash D \Rightarrow C$.

Вратимо се на доказ теореме. Изве71емо га индукцијом по дужини извођења формуле B из Γ и A. Нека је $n = 1$. Како B мора бити последња формула у том извођењу, она је и једина. Онда важи да је B аксиома или $B \in \Gamma$ или $B = A$. Ако је B аксиома или $B \in \Gamma$ сигурно важи $\Gamma \vdash B$. Сетимо се тврђења са почетка: за било коју формулу, па и A, важи $\Gamma \vdash A \Rightarrow B$. Ако је $A = B$ онда из 9.5 следи да је $A \Rightarrow B$ теорема, а тиме и $\Gamma \vdash A \Rightarrow B$.

Претпоставимо да тврђење важи за све формуле B чије извођење из Γ и A је дужине мање од n, то јест ако је извођење $\Gamma, A \vdash B$ дужине мање од n, онда је $\Gamma \vdash A \Rightarrow B$. Нека је сада B таква да је дужина извођења те формуле из Γ и A једнака n. Докажимо да се из Γ може извести формула $A \Rightarrow B$. Дакле, из Γ и A се изводи B и нека је тај доказ састављен од формула $B_1, \ldots, B_n$, где је $B_n = B$. То значи да важи једно од следећег:

- B је аксиома;
- $B \in \Gamma$;
- $B = A$;
- Постоје бројеви i и j који су мањи од n тако да је формула B_j једнака $B_i \Rightarrow B$.

Ако важи неки од прва три случаја, добијамо $\Gamma \vdash A \Rightarrow B$ на исти начин као у бази индукције. Последњи случај заправо каже да је B добијена применом модус поненса на формуле B_i и $B_i \Rightarrow B$ које су део тог извођења. Како су i и j мањи од n, можемо применити индуктивну претпоставку: $\Gamma, A \vdash B_i$ и $\Gamma, A \vdash B_i \Rightarrow B$ и извођења су дужине мање од n; следи да је $\Gamma \vdash A \Rightarrow B_i$ и $\Gamma \vdash A \Rightarrow (B_i \Rightarrow B)$. Посматрајмо извођења формула $A \Rightarrow B_i$ и $A \Rightarrow (B_i \Rightarrow B)$ из Γ и допунимо тај доказ до доказа тражене формуле.

$$
\begin{array}{rll}
1 & \ldots & \\
\vdots & & \\
k. & A \Rightarrow B_i & \\
\vdots & & \\
k+l. & A \Rightarrow (B_i \Rightarrow B) & \\
k+l+1. & (A \Rightarrow (B_i \Rightarrow B)) \Rightarrow ((A \Rightarrow B_i) \Rightarrow (A \Rightarrow B)) & \text{аксиома Л2} \\
k+l+2. & (A \Rightarrow B_i) \Rightarrow (A \Rightarrow B) & \text{МП}(k+l, k+l+1) \\
k+l+3. & A \Rightarrow B & \text{МП}(k, k+l+2)
\end{array}
$$

Дакле, из Γ следи $A \Rightarrow B$, па је тврђење теореме доказано. $\square$

Пример 9.7 *Доказати да је $\neg A, A \vdash B$ за било које формуле A и B.*

1.$\neg A$	хипотеза
2.A	хипотеза
3.$\neg A \Rightarrow (\neg B \Rightarrow \neg A)$	аксиома Л1
4.$\neg B \Rightarrow \neg A$	МП(1,3)
5.$(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$	аксиома Л3
6.$A \Rightarrow B$	МП(4,5)
7.B	МП(2,6)

Користећи теорему о дедукцији можемо закључити да је $A \vdash \neg A \Rightarrow b$, а још једном применом исте теореме и $\vdash A \Rightarrow (\neg A \Rightarrow B)$. Слично је и $\vdash \neg A \Rightarrow (A \Rightarrow B)$. Тако да смо из овог примера добили две важне теореме које ћемо користити у наставку. △

Тврђење 9.8 *Ако је* Γ *скуп исказних формула и* $\Gamma, \neg A \vdash B$ *и* $\Gamma, \neg A \vdash \neg B$ *онда је* $\Gamma \vdash A$.

Доказ. На основу претходног примера закључујемо да је $\vdash \neg B \Rightarrow (B \Rightarrow \neg(A \Rightarrow A))$. Из чињенице да $\Gamma, \neg A \vdash \neg B$ и примене правила модус поненс на претходне две формуле добијамо да $\Gamma, \neg A \vdash B \Rightarrow \neg(A \Rightarrow A)$. Применом модус поненса на ову формулу и $\Gamma, \neg A \vdash B$ добијамо да $\Gamma, \neg A \vdash \neg(A \Rightarrow A)$. На основу теореме дедукције имамо да $\Gamma \vdash \neg A \Rightarrow \neg(A \Rightarrow A)$. Одатле и из аксиоме Л3 $(\neg A \Rightarrow \neg(A \Rightarrow A)) \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ седи да $\Gamma \vdash (A \Rightarrow A) \Rightarrow A$. Из тврђења 9.5 следи да је теорема $A \Rightarrow A$. Још једним кори71ењем модус поненса добијамо да $\Gamma \vdash A$, што је и требало доказати. □

Пример 9.9 *Доказати да је* $(\neg A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow \neg B) \Rightarrow A)$ *теорема.*

Користицемо претходно тврђење. Нека је Γ скуп формула $\neg A \Rightarrow B$ и $\neg A \Rightarrow \neg B$. Важи да $\Gamma, \neg A \vdash B$ јер

1.$\neg A \Rightarrow B$	хипотеза
2.$\neg A$	хипотеза
3.B	МП(1,2).

Такође је $\Gamma, \neg A \vdash \neg B$ јер

1.$\neg A \Rightarrow \neg B$	хипотеза
2.$\neg A$	хипотеза
3.$\neg B$	МП(1,2).

Сада применом 9.8 добијамо да је $\Gamma \vdash A$, то јест $\neg A \Rightarrow B, \neg A \Rightarrow \neg B \vdash A$. После двоструке примене теореме о дедукцији следи да $\vdash (\neg A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow \neg B) \Rightarrow A)$. △

Пример 9.10 *Доказати да је* $\neg\neg A \Rightarrow A$ *теорема.*

На основу теореме о дедукцији довољно је доказати да $\neg\neg A \vdash A$. Нека је Γ формула $\neg\neg A$. Тада је $\Gamma, \neg A \vdash \neg A$, као и $\Gamma, \neg A \vdash \neg\neg A$. Ако означимо $\neg A$ са B, јасно је да из примене тврђења 9.8 добијамо да $\Gamma \vdash A$, то јест $\neg\neg A \vdash A$. Докажимо последњи израз и на други начин.

1.$\neg\neg A$	хипотеза
2.$\neg\neg A \Rightarrow (\neg A \Rightarrow \neg\neg\neg A)$	теорема из примера 9.7
3.$\neg A \Rightarrow \neg\neg\neg A$	МП(1,2)
4.$(\neg A \Rightarrow \neg\neg\neg A) \Rightarrow (\neg\neg A \Rightarrow A)$	аксиома Л3
5.$\neg\neg A \Rightarrow A$	МП(3,4)
6.A	МП(1,5).

Приметимо да у доказу, сем аксиома и евентуалних хипотеза, можемо користити и неку већ доказану теорему. △

Пример 9.11 *Доказати* $\vdash A \Rightarrow \neg\neg A$.

$1.A$	хипотеза
$2.\neg\neg\neg A \Rightarrow \neg A$	теорема из претходног примера
$3.(\neg\neg\neg A \Rightarrow \neg A) \Rightarrow (A \Rightarrow \neg\neg A)$	аксиома Л3
$4.A \Rightarrow \neg\neg A$	МП(2,3)
$5.\neg\neg A$	МП(1,4).

$\triangle$

Пример 9.12 *Доказати да* $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$.

На основу 9.6 довољно је доказати да $A \Rightarrow B, B \Rightarrow C, A \vdash C$.

$1.A \Rightarrow B$	хипотеза
$2.B \Rightarrow C$	хипотеза
$3.A$	хипотеза
$4.B$	МП(1,2)
$5.C$	МП(4,2)

$\triangle$

Пример 9.13 *Доказати да* $\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$.

Нека је Γ формула $A \Rightarrow B$. Доказали смо да је $\neg\neg A \Rightarrow A$ теорема, па на основу 9.12 следи да $\Gamma \vdash \neg\neg A \Rightarrow B$. Такође је доказано да $\vdash B \Rightarrow \neg\neg B$, па на основу истог примера имамо да $\vdash \neg\neg A \Rightarrow \neg\neg B$. Применом модус поненса на ову формулу и аксиому Л3 $(\neg\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg B \Rightarrow \neg A)$ добијамо да $\Gamma \vdash \neg B \Rightarrow \neg A$, то јест $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$, па је онда на основу 9.6 формула $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ теорема. $\triangle$

Дефиниција 9.14 *Формула A је логичка последица скупа формула Γ ако за сваку валуацију v, за коју је $v(F) = 1$ за све формуле $F \in \Gamma$, важи $v(A) = 1$. У том случају пишемо $\Gamma \models A$.*

Приметимо да је A логичка последица празног скупа формула ако и само ако је A таутологија. Тада пишемо $\models A$.

Дефиниција 9.15 *Скуп формула Γ је конзистентан ако не постоји формула A тако да $\Gamma \vdash A$ и $\Gamma \vdash \neg A$.*

Теорема 9.16 *(Теорема о сагласности)*

1. *Ако је $\vdash A$, онда је A таутологија.*
2. *Ако је $\Gamma \vdash A$, онда је $\Gamma \models A$.*
3. *Ако је Γ задовољив скуп формула, онда је и конзистентан.*

Доказ. 1) Ово је специјални случај тврђења под 2), када за Γ ставимо празан скуп.
2) Изве71емо доказ индукцијом по дужини извођења n за A из Γ. Нека је $n = 1$. Тада је једина формула у том извођењу A, па мора бити да је A аксиома или $A \in \Gamma$. Нека је v валуација таква да $v(F) = 1$ за сваку формулу $F \in \Gamma$. Ако је $A \in \Gamma$ јасно је да је $v(A) = 1$, а ако је A аксиома, тачна је у свакој валуацији, па и у v. Дакл,е $\Gamma \models A$. Претпоставимо да је тврђење тачно за све формуле чије је извођење дужине мање од n. Нека је A таква да $\Gamma \vdash A$ и то извођење је дужине n. Ако је A аксиома или $A \in \Gamma$, као у бази индукције, може се доказати да $\Gamma \models A$. Једино још остаје случај када је A добијена из претходних формула у низу применом правила модус поненс. Тада постоји формула B тако да $B, B \Rightarrow A$ имају извођења из Γ дужине мање од n. Према

индуктивној хипотези је $\Gamma \models B$ и $\Gamma \models B \Rightarrow A$. Нека је v валуација таква да $v(F) = 1$ за све $F \in \Gamma$. Важи да $v(B) = 1$ и $v(B \Rightarrow A) = 1$, па је онда $v(A) = 1$, што значи да $\Gamma \models A$.
3) Претпоставимо да је Γ задовољив скуп формула и да није конзистентан. Тада постоји формула A тако да $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. Према делу под 2) је $\Gamma \models A$ и $\Gamma \models \neg A$. Нека је v валуација тако да $v(F) = 1$ за све $F \in \Gamma$. Из $\Gamma \models A$ следи да $v(A) = 1$, а из $\Gamma \models \neg A$ следи да $v(\neg A) = 1$, то јест $v(A) = 0$. Добили смо контрадикцију, па скуп Γ мора бити конзистентан. □

Теорема 9.17 *(Теорема о потпуности)*

1. *Ако је формула A таутологија, онда је A и теорема.*
2. *Ако је $\Gamma \models A$, онда је и $\Gamma \vdash A$.*
3. *Ако је Γ конзистентан скуп формула, онда је и задовољив.*

Доказ. □

Приметимо да на основу теореме о потпуности и теореме о сагласности следи да је формула таутологија ако и само ако је теорема.

Теорема 9.18 *(Став компактности) Скуп формула Γ је задовољив ако и само ако је задовољив сваки његов коначи подскуп.*

Доказ. Ако је Γ задовољив, постоји валуација v тако да је $v(F) = 1$ за сваку $F \in \Gamma$. Ако је Γ' коначан подскуп од Γ тада је и $v(F) = 1$ за све $F \in \Gamma'$, па је сваки коначан подскуп од Γ задовољив.

Претпоставимо сада да је сваки коначан подскуп од Γ задовољив. Треба доказати да то важи и за Γ. Претпоставимо супротно: Γ није задовољив. Према теореми 9.17, Γ није конзистентан, па постоји формула A тако да $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. Како је извођење неке формуле коначан низ формула, то постоји коначан подскуп $\Gamma' \subseteq \Gamma$ тако да $\Gamma' \vdash A$ и $\Gamma' \vdash \neg A$. На основу теореме 9.16 следи да $\Gamma' \models A$ и $\Gamma' \models \neg A$. Важи да је Γ' као коначан подскуп од Γ задовољив, па постоји валуација v тако да $v(F) = 1$ за све $F \in \Gamma'$. Тада из $\Gamma' \models A$ следи да $v(A) = 1$, а из $\Gamma' \models \neg A$ следи да $v(\neg A) = 1$, то јест $v(A) = 0$. Добили смо контрадикцију, па Γ мора бити задовољив. □

Дефиниција 9.19 *Формална теорија је одлучива ако постоји алгритам који за сваку формулу A одлучује да ли је теорема или не.*

Теорема 9.20 *Исказни рачун је одлучив.*

Доказ. □

Задаци

1. Доказати да је $A \wedge B \vdash A$.
2. Доказати да је $A \wedge B \vdash B \wedge A$.
3. Доказати да је $A \vdash A \vee B$, као и $B \vdash A \vee B$.
4. Доказати да је $A \vee B \vdash B \vee A$.
5. Доказати да је $A \Rightarrow B, \neg A \Rightarrow B \vdash B$.
6. Доказати да је $\neg(A \vee B) \vdash \neg A \wedge \neg B$.

7. Доказати да је $B \vee B \vdash B$.
8. Доказати да је $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ теорема.
9. Нека су A, B, C исказне формуле и $A, B \vdash \neg(C \Rightarrow C)$. Доказати да је $A \vdash \neg B$.

10 Предикатска логика

Елементи језика предикатске логике су:

- скуп променљивих *Var* (променљиве ћемо обично означавати са $x, y, z, \dots$);
- логички везници: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
- квантификатори $\forall$ и $\exists$;
- интерпункцијски знаци: , , (,);
- знак једнакости $=$;
- скуп функцијских (или операцијских) симбола *Fun* (обично ћемо их означавати са $f, g, h, \dots$);
- скуп релацијских (или предикатских) симбола *Rel* (обично ћемо их означавати са $p, q, r, \dots$);
- скуп константи *Const* (обично ћемо их означавати са $a, b, c, \dots$).

Релацијски и функцијски симболи имају своју дужину која је природан број $n > 0$ и која се заједнички назива арност релације или функције. Означавамо је са ar. Дефинишимо сада терм (или израз), атомичку формулу и формулу.

Дефиниција 10.1 *1) Променљиве и константе су терми.*
2) Ако су $t_1, \dots, t_n$ терми и f функцијски симбол арности n онда је $f(t_1, \dots, t_n)$ терм.
Терми се могу добити једино коначном применом правила 1 и 2. Скуп терма означвамо са Term.

Дефиниција 10.2 *1) Ако су t_1 и t_2 терми, онда је $t_1 = t_2$ атомичка формула.*
2) Ако су $t_1, \dots, t_n$ терми и p релацијски симбол арности n, онда је $p(t_1, \dots, t_n)$ атомичка формула.

Дефиниција 10.3 *1) Атомичка формула је формула.*
2) Ако су A и B формуле, онда су формуле и

$$\neg A \qquad A \wedge B \qquad A \vee B \qquad A \Rightarrow B \qquad A \Leftrightarrow B \qquad (\forall x)A \qquad (\exists x)A.$$

Формуле се добијају једино коначном применом правила 1 и 2. Скуп формула означавамо са For.

У предикатској логици, при запису највећи приоритет имају операција $\neg, \forall, \exists$, средњег приоритета су операције $\wedge$ и $\vee$, а најмањег операције $\Rightarrow, \Leftrightarrow$. Тако да формуле $(\forall x)A$ и $(\exists x)A$ можемо писати и $\forall x A$ и $\exists x A$.

Пример 10.4 *Нека је L језик предикатске логике задат са $Fun = \{f, g\}$, $Rel = \{p, q\}$ и $Const\{a\}$, где је $ar(f) = ar(q) = 1$ и $ar(g) = ar(p) = 2$. Испитати који од следећих низова симбола је терм, који формула, а који ни једно ни друго.*

$\forall x \forall y p(x, y)$	формула
$g(f(x), a)$	терм
$\forall x f(x)$	ни једно ни друго, јер је $f(x)$ терм
$g(x, y) = a$	формула (атомичка)
$p(x, q(x))$	ни једно ни друго, јер је $q(x)$ формула
$\forall x(p(x, y) \Rightarrow g(x, y))$	ни једно ни друго, јер је p релацијски симбол, а g функцијски

$\triangle$

Дефиниција 10.5 *Нека је L језик предикатске логике. Структура језика L у ознаци $\mathbb{M}$ се састоји од:*

- *непразног скупа M;*
- *функције $f^{\mathbb{M}} : M^n \to M$ арности n за сваки функцијски симбол $f \in Fun$;*
- *релације $p^{\mathbb{M}}$ арности n на скупу M за сваки релацијски симбол $p \in Rel$;*
- *елемента $a^{\mathbb{M}} \in M$ за сваки симбол константе $a \in Const$.*

Дакле, $\mathbb{M} = \big(M, \ldots, f^{\mathbb{M}}, \ldots, p^{\mathbb{M}}, \ldots, a^{\mathbb{M}}\big)$.

Пример 10.6 *Нека је L језик предикатске логике задат са $Fun = \{f, g\}$, $Rel = \{p, q\}$ и $Const\{a\}$, где је $ar(f) = ar(q) = 1$ и $ar(g) = ar(p) = 2$. Дефинишимо L-структуру $\big(\mathbb{N}, f^{\mathbb{N}}, g^{\mathbb{N}}, p^{\mathbb{N}}, q^{\mathbb{N}}, a^{\mathbb{N}}\big)$ на скупу природних бројева $\mathbb{N}$ са:*

$$\begin{array}{rl} f^{\mathbb{N}}(x) = x + 1 & p^{\mathbb{N}}(x, y) = 1 \text{ ако је } x \leq y \\ g^{\mathbb{N}}(x, y) = x + y & q^{\mathbb{N}}(x) = 1 \text{ ако је } x \text{ прост број} \\ a^{\mathbb{N}} = 0 & \end{array}$$

Дефиниција 10.7 *Валуација v за скуп променљивих Var у односу на домен M је свако пресликавање $v : Var \to M$. Ако је $v(x) = a \in M$, онда кажемо да је a вредност променљиве x у валуацији v. Нека су v и w две валуације за исти скуп променљивих и у односу на исти домен. Кажемо да су v и w x-близу, ако је $v(y) = w(y)$ за сваку променљиву y која је различита од x и пишемо $v \sim_x w$.*

Ако је дат домен M, објаснимо како се валуација v може продужити са скупа Var на скуп $Term$. Ако је t терм тако да:

- $t = x$ за $x \in Var$, онда је $v(t) = v(x)$;
- $t = a$ за $a \in Const$, онда је $v(t) = a^{\mathbb{M}}$;
- $t = f(t_1, \ldots, t_n)$ за $f \in Fun$, онда је $v(t) = f^{\mathbb{M}}(v(t_1), \ldots, v(t_n))$.

Пример 10.8 *Нека је језик L и структура тог језика задата као у примеру 10.6. Одредити вредност терма $g(x, a), f(g(x, y)), g(f(x), f(a))$ при валуацији $v = \begin{pmatrix} x & y & \cdots \\ 2 & 7 & \cdots \end{pmatrix}$.*

Важи:

$$\begin{array}{rcl} v(g(x,a)) & = & g^{\mathbb{N}}(v(x), v(a)) = g^{\mathbb{N}}(2, a^{\mathbb{N}}) = g^{\mathbb{N}}(2, 0) = 2 + 0 = 2 \\ v(f(g(x,y))) & = & f^{\mathbb{N}}(v(g(x,y))) = f^{\mathbb{N}}(g^{\mathbb{N}}(v(x), v(y))) = f^{\mathbb{N}}(g^{\mathbb{N}}(2,7)) = f^{\mathbb{N}}(2+7) \\ & = & f^{\mathbb{N}}(9) = 9 + 1 = 10 \\ v(g(f(x), f(a))) & = & g^{\mathbb{N}}(v(f(x)), v(f(a))) = g^{\mathbb{N}}(f^{\mathbb{N}}(v(x)), f^{\mathbb{N}}(v(a))) = g^{\mathbb{N}}(f^{\mathbb{N}}(2), f^{\mathbb{N}}(a^{\mathbb{N}})) \\ & = & g^{\mathbb{N}}(2+1, f^{\mathbb{N}}(0)) = g^{\mathbb{N}}(3, 0+1) = g^{\mathbb{N}}(3,1) = 3 + 1 = 4. \end{array}$$

$\triangle$

Истинитосна вредност формуле у валуацији v и L-структури $\mathbb{M}$ се дефинише на следећи начин:
-ако је A атомична формула тако да:

- A је $t_1 = t_2$ за терме t_1 и t_2, онда је $v(A) = 1$ ако је $v(t_1) = v(t_2)$;
- A је $p(t_1, \ldots, t_n)$ за релацијски симбол p, онда је $v(A) = 1$ ако је $(v(t_1), \ldots, v(t_n)) \in p^{\mathbb{M}}$;

-ако је F формула тако да:

- $F = \neg A$ за формулу A, онда је $v(F) = 1$ ако је $v(A) = 0$;
- $F = A \wedge B$ за формуле A и B, онда је $v(F) = 1$ једино ако $v(A) = 1$ и $v(B) = 1$;
- $F = A \vee B$ за формуле A и B, онда је $v(F) = 0$ једино ако је $v(A) = 0$ и $v(B) = 0$;
- $F = A \Rightarrow B$ за формуле A и B, онда је $v(F) = 0$ једино ако је $v(A) = 1$ и $v(B) = 0$;
- $F = A \Leftrightarrow B$ за формуле A и B, онда је $v(F) = 1$ ако је $v(A) = v(B)$;
- $F = (\forall x)A$ за формулу A, онда је $v(F) = 1$ ако за сваку валуацију w тако да $w \sim_x v$ важи $w(A) = 1$;
- $F = (\exists x)A$ за формулу A, онда је $v(F) = 1$ ако постоји валуација w тако да $w \sim_x v$ и $w(A) = 1$.

Приметимо да још важи:

- ако је $F = (\forall x)A$, онда је $v(F) = 0$ ако постоји валуација $w \sim_x v$ тако да $w(A) = 0$;
- ако је $F = (\exists x)A$, онда је $v(F) = 0$ ако за сваку валуацију $w \sim_x v$ важи $w(A) = 0$.

У случају да за неку формулу A важи $v(A) = 1$ за неку валуацију v и L-структуру $\mathbb{M}$, онда кажемо да је формула A тачна у тој валуацији L-структуре $\mathbb{M}$. У супротном кажемо да је нетачна.

Пример 10.9 *Нека је језик L и структура тог језика задата као у примеру 10.6. Испитати тачност формула $g(x,a) = f(f(a)), p(g(x,y), f(a)), q(f(x)) \Rightarrow p(x,x)$ при валуацији $v = \begin{pmatrix} x & y & \cdots \\ 2 & 3 & \cdots \end{pmatrix}$.*

Важи:

$$\begin{array}{rcl} v(g(x,a)) & = & g^{\mathbb{N}}(2,0) = 2 + 0 = 2 \\ v(f(f(a))) & = & f^{\mathbb{N}}(v(f(a))) = f^{\mathbb{N}}(f^{\mathbb{N}}(0)) = f^{\mathbb{N}}(1) = 2, \end{array}$$

па је $v(g(x,a)) = v(f(f(a)))$, а тиме је и $v(g(x,a) = f(f(a))) = 1$. Даље је

$$\begin{array}{rcl} v(g(x,y)) & = & g^{\mathbb{N}}(v(x), v(y)) = 2 + 3 = 5 \\ v(f(a)) & = & f^{\mathbb{N}}(0) = 1, \end{array}$$

па како како није $(5,1) \in p^{\mathbb{N}}$, то јест није $5 \leq 1$, онда је $v(p(g(x,y), f(a))) = 0$. Слично је $v(f(x)) = f^{\mathbb{N}}(2) = 2+1 = 3$, па како је 3 прост број, важи $v(q(f(x))) = 1$. Такође је $2 \leq 2$, па је $v(p(x,x)) = 1$. Сада имамо да

$$v(q(f(x)) \Rightarrow p(x,x)) = v(q(f(x))) \Rightarrow v(p(x,x)) = 1 \Rightarrow 1 = 1.$$

Дакле, прва и трећа формула су тачне у валуацији v, а друга формула није тачна у тој валуацији. $\triangle$

Дефиниција 10.10 *Ако се појављивање променљиве x у формули A налази под дејством квантификатора, онда кажемо да је то појављивање променљиве везано. У супротном је слободно. Променљива је везана (слободна) у формули A ако има бар једно везано (слободно) појављивање.*

Пример 10.11 *Нека је p и q релацијски симболи језика L арности 2 и 1 редом. За сва појављивања променљивих x и y у формулама $p(x,y), \forall x p(x,y), \exists x p(x,y) \Rightarrow q(x), \exists y(p(x,y) \Rightarrow \forall x p(x,y))$ одредити да ли су слободна или везана.*

$p(x,y)$	појављивање променљивих x, y је слободно
$\forall x p(x,y)$	прво појављивање променљиве x је везано, као и друго, док је појављивање променљиве y слободно
$\exists x p(x,y) \Rightarrow q(x)$	променљива x: прво појављивање везано, друго везано, треће слободно; променљива y: појављивање је слободно
$\exists y(p(x,y) \Rightarrow \forall x p(x,y))$	променљива x: прво појављивање слободно, друго везано, треће везано; променљива y: прво појављивање везано, друго везано, треће везано

$\triangle$

Нека је x променљива која се појављује у формули A. Приметимо да вредности те формуле у валуацији v зависи од $v(x)$ само ако променљива x има слободна појављивања у тој формули. У формули $\forall x p(x,y)$ из претходног примера, вредност формуле не зависи од $v(x)$ јер x има само везана појављивања, али зависи од $v(y)$, јер је појављивање те променљиве слободно. Иначе, вредност формуле зависи само од слободних променљивих које се у њој појављују.

Дефиниција 10.12 *Формула у којој нема слободних променљивих се назива реченица.*

На основу претходног закључујемо да ако је A реченица, онда $v(A)$ уопште не зависи од валуације v.

Дефиниција 10.13 *Ако за неку L-структуру $\mathbb{M}$ и формулу A важи да је $v(A) = 1$ за сваку валуацију $v : Var \to \mathbb{M}$, онда кажемо да је L-структура $\mathbb{M}$ модел за формулу A. Ако не важи $v(A) = 1$ за сваку валуацију $v : Var \to \mathbb{M}$, онда кажемо да је L-структура $\mathbb{M}$ контрамодел за формулу A.*

Дефиниција 10.14 *Ако је свака L-структура модел за формулу A, онда кажемо да је A ваљана.*

Пример 10.15 *Нека је језик L и структура тог језика задата као у примеру 10.6. Испитати да ли је $\mathbb{N}$ модел или контрамодел за реченице $\forall x q(x), \forall x p(x, f(x))$, $\forall x \forall y (f(x) = f(y)), \forall x \forall y \forall z (p(x,y) \Leftrightarrow p(g(x,z), g(y,z)), \forall x(g(x,a) = x), \exists x \forall y p(y,x)$.*

Формула $\forall x q(x)$ значи да је сваки природан број прост. Ово није тачно, па је $\mathbb{N}$ контрамодел за ову формулу. Формула $\forall x p(x, f(x))$ каже да за сваки природни број x важи да је $x \le x+1$, што је тачно, тако да је $\mathbb{N}$ модел за дату формулу. Следећа формула каже да за је за свака два природна броја x и y $x+1 = y+1$, што не важи, па имамо један контрамодел дате формуле. За све природне бројеве x, y и z важи да је $x \le y$ ако и само ако $x+z \le y+z$, па је $\mathbb{N}$ модел за формулу $\forall x \forall y \forall z (p(x,y) \Leftrightarrow p(g(x,z), g(y,z))$. За сваки природни број важи да је $x + 0 = x$, па важи исти закључак као у претходном случају. Није тачно да постоји природни број тако да су сви остали природни бројеви мањи од њега, па је ова L-структура контрамодел за последњу формулу. $\triangle$

Пример 10.16 *Нека је језик L и структура тог језика задата као у примеру 10.6. Реченицама датог језика изразити следећа својства структуре $\mathbb{N}$:*

1. *Постоји природни број који је мањи или једнак од свих природних бројева.*

2. *Ако природни број није нула, онда постоји број чији је то следбеник.*

1. $\exists x \forall y p(x, y)$

2. $\forall x (p(f(a), x) \Rightarrow \exists y x = f(y)$

$\triangle$

Пример 10.17 *Дефинисати језик првог реда у коме је могуће изрећи аксиоме комутативне групе.*

Нека је језик L задат са: f је функцијски симбол арности 2 и e је симбол константе. Аксиоме се могу представити на следећи начин:

1. $\forall x \forall y \forall z f(f(x, y), z) = f(x, f(y, z))$

2. $\forall x f(x, e) = x$

3. $\forall x \exists y f(x, y) = e$

4. $\forall x \forall y f(x, y) = f(y, x)$

$\triangle$

Пример 10.18 *Нека је $\mathcal{L}$ језик првог реда задат са: $Rel = \{p, q\}, Fun = \{f, g, h\}, Const = \{a\}$, при чему је $ar(p) = ar(f) = 2$ и $ar(q) = ar(g) = ar(h) = 1$. На скупу $\mathbb{N}$ је задата L-структура тако да*

$$\begin{array}{ll} f^{\mathbb{N}}(x, y) = x + y & p^{\mathbb{N}}(x, y) = 1 \text{ ако је } x \leq y \\ g^{\mathbb{N}}(x) = 5x & q^{\mathbb{N}}(x) = 1 \text{ ако је } x \text{ прост број} \\ h^{\mathbb{N}}(x) = x^2 & c^{\mathbb{N}} = 3. \end{array}$$

Одредити валуације v_1 и v_2 у којима је формула $\forall y\, p(x, f(y, a)) \Rightarrow p(h(y), g(x))$ тачна, односно нетачна.

Приметимо да тачност претпоставке $\forall y\, p(x, f(y, c))$ не зависи од валуације у којој је y. Импликација је тачна ако је претпоставка нетачна или ако је последица тачна, тако да можемо да тражимо решење на два начина. Ако тражимо валуацију у којој је последица тачна, онда из

$$v_1(p(h(y), g(x))) = p^{\mathbb{N}}(h^{\mathbb{N}}(v_1(y)), g^{\mathbb{N}}(v_1(x))) = p^{\mathbb{N}}(v_1(y))^2), 5v_1(x)) = 0,$$

следи да мора бити $v_1(y))^2 \leq 5v_1(x)$. Једна таква валуација је, на пример $v_1 = \begin{pmatrix} x & y & \cdots \\ 1 & 1 & \cdots \end{pmatrix}$. Ако тражимо, с друге стране, валуацију у којој је претпоставка нетачна, онда је $v_1(\forall y\, p(x, f(y, a))) = 0$ ако постоји валуација $w \sim_y v_1$ тако да $w(p(x, f(y, a))) = 0$. Ово последње важи ако и само ако $p^{\mathbb{N}}(w(x), w(y) + 3) = 0$, то јест ако није $w(x) \leq w(y) + 3$. Видимо да је довољно да вредност променљиве x буде већа или једнака од 4, па таква валуација постоји. Вредност променљиве y не утиче на резултат, па ту можемо задати било шта. Једна валуација за коју је испуњено све наведено је $v_1 = \begin{pmatrix} x & y & \cdots \\ 4 & 1 & \cdots \end{pmatrix}$.

Треба још одредити валуацију у којој је формула нетачна. Неопходно је да у тој валуацији претпоставка буде тачна, а последица нетачна. Дакле, треба да је $v_2(\forall y\, p(x, f(y, c))) = 1$ и $v_2(p(h(y), g(x))) = 0$. Други услов значи да није $v_2(y))^2 \leq 5v_2(x)$, што важи за, на пример, $v_2 = \begin{pmatrix} x & y & \cdots \\ 0 & 1 & \cdots \end{pmatrix}$. За сваку валуацију $w \sim_y v_2$ важи да $0 = w(x) \leq w(y) + 3$, па и $w(p(x, f(y, c))) = 1$. Тако да је $v_2(\forall y\, p(x, f(y, a))) = 1$, па наведена валуација v_2 задовољава све тражене услове. $\triangle$

Пример 10.19 *Доказати да је формула* $F = \forall x \forall y \forall z((p(x) \wedge p(y)) \Rightarrow p(z))$ *ваљана.*

Треба доказати да је произвољна L-структура модел за F. Претпоставим супротно: постоји L-структура $\mathbb{M}$ и валуација $v : Var \rightarrow M$ тако да $v(F) = 0$. Дакле, $v\big(\forall x \forall y \forall z((p(x) \wedge p(y)) \Rightarrow p(z))\big) = 0$. Тада постоји валуација $v' \sim_x v$ тако да $v'\big(\forall y \forall z((p(x) \wedge p(y)) \Rightarrow p(z))\big) = 0$. Даље, постоји валуација $v'' \sim_y v'$ тако да $v''\big(\forall z((p(x) \wedge p(y)) \Rightarrow p(z))\big) = 0$. Коначно, за сваку валуацију $v''' \sim_z v''$ важи да $v'''\big((p(x) \wedge p(y)) \Rightarrow p(z)\big) = 0$. Следи да за сваку такву v''' важи да

$$\begin{array}{rrr} & v'''(p(x) \wedge p(y)) = 1 & v'''(p(z)) = 0 \\ v'''(p(x)) = 1 & v'''(p(y)) = 1 & v'''(p(z)) = 0 \\ p^{\mathbb{M}}(v'''(x)) = 1 & p^{\mathbb{M}}(v'''(y)) = 1 & p^{\mathbb{M}}(v'''(z)) = 0 \end{array}$$

нека је $v''' : Var \rightarrow \mathbb{M}$ таква да

$$v'''(x) = v''(x) \qquad v'''(y) = v''(y) \qquad v'''(z) = v''(x).$$

Тада је $p^{\mathbb{M}}(v''(x)) = 1, p^{\mathbb{M}}(v''(y)) = 1$ и $p^{\mathbb{M}}(v''(x)) = 0$. Добили смо да је истовремено $p^{\mathbb{M}}(v''(x)) = 1$ и $p^{\mathbb{M}}(v''(x)) = 0$, што је немогуће, па полазна формула јесте ваљана. $\triangle$

Пример 10.20 *Доказати да је формула* $F = \forall x(p(x) \wedge q(x)) \Leftrightarrow (\forall x p(x) \wedge \forall x q(x))$ *ваљана.*

Претпоставим да F није ваљана: тада постоји L-структура $\mathbb{M}$ и валуација $v : Var \rightarrow M$ тако да $v(F) = 0$, то јест $v\big(\forall x(p(x) \wedge q(x)) \Leftrightarrow (\forall x p(x) \wedge \forall x q(x))\big) = 0$. Сада имамо две могућности:

$$\begin{array}{ll} 1) v(\forall x(p(x) \wedge q(x))) = 1 & v(\forall x p(x) \wedge \forall x q(x)) = 0 \\ 2) v(\forall x(p(x) \wedge q(x))) = 0 & v(\forall x p(x) \wedge \forall x q(x)) = 1 \end{array}$$

У првом случају из друге релације да је $v(\forall x p(x)) = 0$ (случај $1'$) или $v(\forall x q(x)) = 0$ (случај $1''$). За $1'$: постоји валуација $v' \sim_x v$ тако да $v'(p(x)) = 0$. Из $v(\forall x(p(x) \wedge q(x))) = 1$ следи да за сваку валуацију $w \sim_x v$ важи да $w(p(x) \wedge q(x)) = 1$. Можемо узети $w = v'$. Тада је $v'(p(x) \wedge q(x)) = 1$, то јест $v'(p(x)) = 1$ и $v'(q(x)) = 1$. Закључак са почетка случаја $1'$ је да $v'(p(x)) = 0$, што је контрадикција. Случај $1''$: постоји валуација $v'' \sim_x v$ тако да $v''(q(x)) = 0$. Поново се позивајући на прву препоставку случаја 1, добијамо да $v''(p(x)) = 1$ и $v''(q(x)) = 1$, што је поново контрадикција. Тако да је случај 1 немогућ.

У другом случају из друге релације следи да $v(\forall x p(x)) = 1$ и $v(\forall x q(x)) = 1$. Како је $v(\forall x(p(x) \wedge q(x))) = 0$ постоји $v' \sim_x v$ тако да $v'(p(x) \wedge q(x)) = 0$. Тада је $v'(p(x)) = 0$ (случај $2'$) или $v'(q(x)) = 0$ (случај $2''$). За $2'$: како је $v(\forall x p(x)) = 1$ онда је за сваку валуацију $w \sim_x v$ тачно $w(p(x)) = 1$. Нека је $w = v'$. Онда је $v'(p(x)) = 1$, што је контрадикција. За $2''$: на сличан начин из $v(\forall x q(x)) = 1$ следи да је $v'(q(x)) = 1$, што је немогуће. Дакле, и у другом случају смо добили контрадикцију, тако да полаза формула јесте ваљана. $\triangle$

Пример 10.21 *Доказати да формула* $F = \forall x \exists y p(x, y) \Rightarrow \exists y \forall x p(x, y)$ *није ваљана.*

Да формула није ваљана, значило би да постоји L-структура $\mathbb{M}$ која није модел за F, то јест структура $\mathbb{M}$ и валуација v тако да $v(F) = 0$. Одредићемо једну такву структуру $\mathbb{M}$ и то је онда један контрамодел за дату формулу. Нека је $M = \mathbb{N}$ и $p^{\mathbb{N}} = \leq$. Претпоставимо супротно: за сваку валуацију $v : Var \rightarrow \mathbb{N}$ је $v(F) = 1$. Тада из $v(\forall x \exists y p(x, z) \Rightarrow \exists y \forall x p(x, y))$ следи да $v(\forall x \exists y p(x, y)) = 0$ или $v(\exists y \forall x p(x, y)) = 1$. Први случај: постоји валуација $v' \sim_x v$ тако да $v'(\exists y p(x, y)) = 0$. Одатле следи да за сваку валуацију $v'' \sim_y v'$

важи $v''(p(x,y)) = 0$. Нека је $v'' : Var \to \mathbb{N}$ задата са $v''(x) = v'(x)$ и $v''(y) = v'(x)+1$. Тада је $p^{\mathbb{N}}(v'(x), v'(x)+1) = 0$, то јест није $v'(x) \leq v'(x)+1$, што је немогуће јер су у питању природни бројеви.

У другом случају постоји валуација $v' \sim_y v$ тако да $v'(\forall x p(x,y)) = 1$. То значи да за сваку $v'' \sim_x v'$ важи $v''(p(x,y)) = 1$. Нека је $v''(y) = v'(y)$ и $v''(x) = v'(y)+1$. Тада је $p^{\mathbb{N}}(v'(y)+1, v'(y)) = 1$, то јест $v'(y)+1 \leq v'(y)$, што није могуће. Следи да је формула F нетачна у свакој валуацији овако задате структуре, и тиме је одређен и један контрамодел за F. $\triangle$

10.1 Метод таблоа

Метод таблоа за исказни рачун ћемо проширити тако да важи и за формуле предикатске логике, то јест помоћу ове методе ће бити могуће доказивање ваљаности предикатских формула. Слично као у случају исказне логике, у корену бинарног дрвета је формула $\perp F$ и користимо правила α и β за гранање дрвета. Сем те две врсте правила уводимо и правила која се односе на формуле са кванторима:

- γ правила, и одговарајуће формуле су формуле типа γ. То су:

$$\begin{array}{c} \top((\forall x)p(x)) \\ | \\ \top(p(a)) \end{array} \qquad a \text{ је било који симбол константе}$$

$$\begin{array}{c} \perp((\exists x)p(x)) \\ | \\ \perp(p(a)) \end{array} \qquad a \text{ је било који симбол константе}$$

- δ правила, и одговарајуће формуле су формуле типа δ. То су:

$$\begin{array}{c} \top((\exists x)p(x)) \\ | \\ \top(p(a)) \end{array} \qquad a \text{ је нови симбол константе}$$

$$\begin{array}{c} \perp((\forall x)p(x)) \\ | \\ \perp(p(a)) \end{array} \qquad a \text{ је нови симбол константе}$$

Може се доказати да је ако је табло за предикатску формулу затворен, онда је та формула ваљана.

Пример 10.22 *Методом таблоа доказати да је формула $\forall y(\forall x p(x) \Rightarrow p(y))$ ваљана.*

$$\begin{array}{c} 1.\perp((\forall y)((\forall x)p(x) \Rightarrow p(y))) \\ | \\ 2.\perp((\forall x)p(x) \Rightarrow p(a))\ \ (1)] \\ | \\ 3.\top((\forall x)p(x))\ \ (2) \\ | \\ 4.\perp(p(a))\ \ (2) \\ | \\ 5.\top(p(a))\ \ (3) \\ X(4,5) \end{array}$$

$\triangle$

Пример 10.23 *Методом таблоа доказати да је формула $\forall x \forall y((p(x,y) \vee q(x)) \Rightarrow r(x)) \Rightarrow (\exists x \neg r(x) \Rightarrow \exists x \forall y \neg p(x,y))$ ваљана.*

$$1.\bot\big((\forall x)(\forall y)((p(x,y)\vee q(x))\Rightarrow r(x))\Rightarrow((\exists x)\neg r(x)\Rightarrow(\exists x)(\forall y)\neg p(x,y))$$

$$2.\top\big((\forall x)(\forall y)((p(x,y)\vee q(x))\Rightarrow r(x))\big)\ \ (1)$$

$$3.\bot\big((\exists x)\neg r(x)\Rightarrow(\exists x)(\forall y)\neg p(x,y)\big)\ \ (1)$$

$$4.\top((\exists x)\neg r(x))\ \ (3)$$

$$5.\bot((\exists x)(\forall y)\neg p(x,y))\ \ (3)$$

$$6.\top(\neg r(a))\ \ (4)$$

$$7.\bot(r(a))\ \ (6)$$

$$8.\top((\forall y)((p(a,y)\vee q(a))\Rightarrow r(a)))\ \ (2)$$

$$9.\bot((\forall y)\neg p(a,y))\ \ (5)$$

$$10.\bot(\neg p(a,b))\ \ (9)$$

$$11.\top(p(a,b))\ \ (10)$$

$$12.\top((p(a,b)\vee q(a))\Rightarrow r(a))\ \ (8)$$

$$13.\bot(p(a,b)\vee q(a))\ \ (12) \qquad\qquad 14.\top(r(a))\ \ (12)$$

$$\qquad\qquad\qquad\qquad\qquad\qquad X(7,14)$$

$$15.\bot(p(a,b))\ \ (13)$$

$$16.\bot(q(a))\ \ (13)$$

$$X(11,15)$$

$\triangle$

Задаци

1. Нека је L језик предикатске логике задат са $Fun=\{f,g\}$, $Rel=\{p,q\}$ и $Const=\{a\}$, где је $ar(f)=ar(q)=1$ и $ar(g)=ar(p)=2$. Нека је L-структура $\big(\mathbb{Z},f^{\mathbb{Z}},g^{\mathbb{Z}},p^{\mathbb{Z}},q^{\mathbb{Z}},a^{\mathbb{Z}}\big)$ на скупу целих бројева $\mathbb{Z}$ са:

$$\begin{array}{rl} f^{\mathbb{Z}}(x)=-x & p^{\mathbb{Z}}(x,y)=1 \text{ ако је } x\mid y \\ g^{\mathbb{Z}}(x,y)=x\cdot y & q^{\mathbb{Z}}(x)=1 \text{ ако је } x \text{ позитиван број} \\ a^{\mathbb{N}}=1 & \end{array}$$

   (а) Одредити вредности терма $f(g(g(x,y),f(a)))$ и $g(f(y),z)$ у валуацији $v=\begin{pmatrix} x & y & z & \cdots \\ 2 & 3 & 4 & \cdots \end{pmatrix}$.

   (б) Одредити тачност формула $q(f(g(x,y)))\Leftrightarrow q(y)$ и $\neg p(f(x),z)\vee q(f(a))$ у валуацији $w=\begin{pmatrix} x & y & z & \cdots \\ -2 & -3 & 4 & \cdots \end{pmatrix}$.

   (ц) Одредити да ли је ова структура модел или контрамодел за реченице $\forall x\exists y p(x,y)\Rightarrow\forall x q(g(x,f(x)))$ и $\forall x(q(x)\vee q(a))$.

   (д) Реченицама датог језика изразити следећа својства ове структуре:
   -Сваки цео број је дељив са 1.
   -Ако цео број није нула, онда је он позитиван или је супротни број тог броја позитиван.

2. Нека је L-структура $\big(\mathbb{Z},f^{\mathbb{Z}},g^{\mathbb{Z}},p^{\mathbb{Z}},q^{\mathbb{Z}},a^{\mathbb{Z}}\big)$ задата као у претходном задатку. Ако је могуће, одредити валуације v_1 и v_2 у којима је формула $\exists y q(f(y))\Leftrightarrow p(a,g(x,y))$ тачна, односно нетачна.

3. Нека је L језик предикатске логике задат са $Fun = \{f, g, h\}$, $Rel = \{p, q\}$ и $Const = \{a\}$, где је $ar(h) = ar(q) = 1$ и $ar(f) = ar(g) = ar(p) = 2$. Нека је L-структура $\left(\mathcal{P}(\mathbb{N}), f^{\mathcal{P}(\mathbb{N})}, g^{\mathcal{P}(\mathbb{N})}, h^{\mathcal{P}(\mathbb{N})}, p^{\mathcal{P}(\mathbb{N})}, q^{\mathcal{P}(\mathbb{N})}, a^{\mathcal{P}(\mathbb{N})}\right)$ задата на партитивном скупу скупа природних бројева $\mathcal{P}(\mathbb{N})$ са:

$$\begin{array}{rr} f^{\mathcal{P}(\mathbb{N})}(x,y) = x \setminus y & p^{\mathcal{P}(\mathbb{N})}(x,y) = 1 \text{ ако је } x \subseteq y \\ g^{\mathcal{P}(\mathbb{N})}(x,y) = x \cap y & q^{\mathcal{P}(\mathbb{N})}(x) = 1 \text{ ако је } x \text{ коначан скуп} \\ h^{\mathcal{P}(\mathbb{N})}(x) = x^c & a^{\mathcal{P}(\mathbb{N})} = \emptyset \end{array}$$

(а) Одредити вредности терма $g(f(z, x), y)$ и тачност формуле $q(h(a)) \vee \neg p(f(x, z), g(x, y))$ у валуацији
$v = \begin{pmatrix} x & y & z & \cdots \\ \{1,3,5,7,\dots\} & \{2,4,6,8,\dots\} & \{0,1,2,3,4,5\} & \cdots \end{pmatrix}$.

(б) Одредити валуацију v_1 у којој је формула $\forall x p(x, y) \wedge \exists y q(g(x, y))$ тачна.

(ц) Одредити валуацију v_2 у којој је формула $\forall x \forall y p(h(x), h(g(x, y))) \Rightarrow p(h(y), h(f(x, y)))$ нетачна.

4. Доказати да је формула $\exists x \forall y p(x, y) \Rightarrow \forall y \exists x p(x, y)$ ваљана.

5. Доказати да је формула $\forall x(p(x) \Rightarrow \forall y q(x, y)) \wedge \exists x p(x) \Rightarrow \exists x q(x, x)$ ваљана.

6. Доказати да формула $\forall x(p(x, f(x)) \Rightarrow p(f(x), x))$ није ваљана и при том наћи контрамодел коначног домена.

7. Наћи један модел формуле $\forall x(p(x) \Rightarrow p(f(x)))$.

8. Методом таблоа доказати да је формула $\forall x(p(x) \Rightarrow q(x)) \Rightarrow (\forall x p(x) \Rightarrow \forall x q(x))$ ваљана.

9. Методом таблоа доказати да је формула $\forall x((p(x) \vee q(x)) \Rightarrow r(x)) \Rightarrow (\exists x \neg r(x) \Rightarrow \exists x \neg p(x))$ ваљана.

10. Методом таблоа доказати да је формула $\forall x \exists y \exists z(p(x, z) \Rightarrow q(x, y)) \Rightarrow (\forall x \forall z p(x, z) \Rightarrow \forall x \exists y q(x, y))$ ваљана.

11. Методом таблоа доказати да је формула $(H \wedge K) \Rightarrow L$ ваљана, где је $H = \forall x(p(x) \Rightarrow \exists y(q(x, y) \vee r(x, y)))$, $K = \exists x \forall y \neg r(x, y)$ и $L = \forall x p(x) \Rightarrow \exists x \exists y q(x, y)$.

11 Решења задатака

Глава 1

Глава 2

1. Важи

$$\begin{array}{lll} x \in (A \cap B) \triangle (A \cap C) & \text{акко} & x \in (A \cap B) \setminus (A \cap C) \text{ или } x \in (A \cap C) \setminus (A \cap B) \\ & \text{акко} & (x \in A \text{ и } x \in B \text{ и није } x \in A \cap C) \text{ или} \\ & & (x \in A \text{ и } x \in C \text{ и није } x \in A \cap B) \\ & \text{акко} & (x \in A \text{ и } x \in B \text{ и } (x \notin A \text{ или } x \notin C)) \text{ или} \\ & & (x \in A \text{ и } x \in C \text{ и } (x \notin A \text{ или } x \notin B)) \\ & \text{акко} & (x \in A \text{ и } x \in B \text{ и } x \notin A) \text{ или } (x \in A \text{ и } x \in B \text{ и } x \notin C) \text{ или} \\ & & (x \in A \text{ и } x \in C \text{ и } x \notin A) \text{ или } (x \in A \text{ и } x \in C \text{ и } x \notin B) \\ & \text{акко} & (x \in A \text{ и } x \in B \text{ и } x \notin C) \text{ или } (x \in A \text{ и } x \in C \text{ и } x \notin B) \\ & \text{акко} & (x \in A \text{ и } x \in B \setminus C) \text{ или } (x \in A \text{ и } x \in C \setminus B) \\ & \text{акко} & x \in A \text{ и } (x \in B \setminus C \text{ или } x \in C \setminus B) \\ & \text{акко} & x \in A \text{ и } x \in (B \setminus C) \cup (C \setminus B) \\ & \text{акко} & x \in A \cap (B \triangle C). \end{array}$$

2. Како је $A \triangle B = (A \setminus B) \cup (B \setminus A)$, имамо да је

$$\begin{aligned}
x \in (A \setminus B) \cup (B \setminus A) \quad & \text{акко} \quad (x \in A \text{ и } x \notin B) \text{ или } (x \in B \text{ и } x \notin A) \\
& \text{акко} \quad (x \in A \text{ или } (x \in B \text{ и } x \notin A)) \text{ и} \\
& \phantom{\text{акко}} \quad (x \notin B \text{ или } (x \in B \text{ и } x \notin A)) \\
& \text{акко} \quad (x \in A \text{ или } x \in B) \text{ и } (x \in A \text{ или } x \notin A) \text{ и} \\
& \phantom{\text{акко}} \quad (x \notin B \text{ или } x \in B) \text{ и } (x \notin B \text{ или } x \notin A)) \\
& \text{акко} \quad (x \in A \text{ или } x \in B) \text{ и } (x \notin B \text{ или } x \notin A)) \\
& \text{акко} \quad x \in A \cup B \text{ и } x \notin A \cap B \\
& \text{акко} \quad x \in (A \cup B) \setminus (A \cap B).
\end{aligned}$$

3.

$$\begin{aligned}
x \in A \setminus (B \setminus C) \quad & \text{акко} \quad x \in A \text{ и } x \notin B \setminus C \\
& \text{акко} \quad x \in A \text{ и није } x \in B \setminus C \\
& \text{акко} \quad x \in A \text{ и није } (x \in B \text{ и } x \notin C) \\
& \text{акко} \quad x \in A \text{ и } (x \notin B \text{ или } x \in C) \\
& \text{акко} \quad (x \in A \text{ и } x \notin B) \text{ или } (x \in A \text{ и } x \in C) \\
& \text{акко} \quad x \in A \setminus B \text{ или } x \in A \cap C \\
& \text{акко} \quad x \in (A \setminus B) \cup (A \cap C).
\end{aligned}$$

4.

$$\begin{aligned}
x \in (A \setminus B) \cap (C \setminus D) \quad & \text{акко} \quad x \in A \setminus B \text{ и } x \in C \setminus D \\
& \text{акко} \quad x \in A \text{ и } x \notin B \text{ и } x \in C \text{ и } x \notin D \\
& \text{акко} \quad x \in A \text{ и } x \in C \text{ и } x \notin B \text{ и } x \notin D \\
& \text{акко} \quad x \in A \cap C \text{ и } x \notin B \cup D \\
& \text{акко} \quad x \in (A \cap C) \setminus (B \cup D)
\end{aligned}$$

5. Довољно је доказати да из 1. следи 2.,из 2. следи 3. и из 3. следи 1.
(а)⇒(б) Претпоставимо да је $A \subseteq B$. Треба доказати да је $A \cap B = A$. Ако је $x \in A \cap B$, јасно је да је $x \in A$, па имамо $A \cap B \subseteq A$. Нека је $x \in A$. Због претпоставке је $A \subseteq B$, па $x \in B$. Дакле, $x \in A$ и $x \in B$, па је $x \in A\cap$, чиме смо доказали $A \subseteq A \cap B$. Пошто важи и обрнута инклузија, имамо $A \cap B = A$.
(б)⇒(в) Претпоставимо да је $A \cap B = A$. Треба доказати да је $A \cup B = B$. Сигурно је $B \subseteq A \cup B$. Нека је $x \in A \cup B$. Тада је $x \in A$ (што је једнако $A \cap B$ према претпоставци) или $x \in B$. Дакле, $x \in A \cap B$ или $x \in B$. Следи да је ($x \in A$ и $x \in B$) или $x \in B$, па мора бити да је $x \in B$. Овим смо доказали да је $A \cup B \subseteq B$.
(в)⇒(а) Претпоставимо да је $A \cup B = B$. Докажимо да је $A \subseteq B$. Нека је $x \in A$. Тада је и $x \in A \cup B$, а према претпоставци последњи скуп је једнак B, па имамо $x \in B$.

6. Претпоставимо прво да важи једнакост $A \cap (B \cup C) = (A \cap B) \cup C$. Докажимо да је $C \subseteq A$.

$$\begin{aligned}
\text{Из } x \in C \quad & \text{следи} \quad x \in (A \cap B) \cup C \\
& \text{следи} \quad x \in A \cap (B \cup C) \text{ на основу претпостављене једнакости} \\
& \text{следи} \quad x \in A.
\end{aligned}$$

Претпоставимо сада да је $C \subseteq A$. Докажимо да важи наведена једнакост.

$$\begin{array}{lll}
x \in A \cap (B \cup C) & \text{акко} & x \in A \text{ и } (x \in B \text{ или } x \in C) \\
& \text{акко} & (x \in A \text{ и } x \in B) \text{ или } (x \in A \text{ и } x \in C) \\
& \text{акко} & x \in A \cap B \text{ или } x \in A \cap C \\
& & \text{користећи претходни задатак важи } A \cap C = C \text{ акко } C \subseteq A \\
& \text{акко} & x \in A \cap B \text{ или } x \in C \\
& \text{акко} & x \in (A \cap B) \cup C.
\end{array}$$

7. Претпоставимо да је $C \subseteq A \cup B$. Докажимо $B^c \cap C \subseteq A$.

$$\begin{array}{lll}
x \in B^c \cap C & \text{следи} & x \in B^c \text{ и } x \in C \\
& \text{следи} & x \notin B \text{ и } x \in A \cup B \text{ из претпоставке} \\
& \text{следи} & x \notin B \text{ и } (x \in A \text{ или } x \in B) \\
& \text{следи} & (x \in B \text{ и } x \in A) \text{ или } (x \notin B \text{ и } x \in B) \\
& \text{следи} & x \in B \text{ и } x \in A \\
& \text{следи} & x \in A.
\end{array}$$

Ако претпоставимо $B^c \cap C \subseteq A$, онда је

$$\begin{array}{lll}
x \in C & \text{следи} & x \in B^c \cup C \\
& \text{следи} & x \in A \text{ из претпоставке} \\
& \text{следи} & x \in A \cup B.
\end{array}$$

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

9. Докажимо прво да је $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

$$\begin{array}{lll}
X \in \mathcal{P}(A) \cup \mathcal{P}(B) & \text{следи} & X \in \mathcal{P}(A) \text{ или } X \in \mathcal{P}(B) \\
& \text{следи} & X \subseteq A \text{ или } X \subseteq B \\
& \text{следи} & X \subseteq A \cup B.
\end{array}$$

Претпоставимо да је $A \subseteq B$ или $B \subseteq A$. Тада је $A \cup B = B$ или $A \cup B = A$ респективно. Ако је $A \cup B = B$, онда је

$$\begin{array}{lll}
X \in \mathcal{P}(A \cup B) & \text{следи} & X \subseteq A \cup B \\
& \text{следи} & X \subseteq B \\
& \text{следи} & X \in \mathcal{P}(B) \\
& \text{следи} & X \in \mathcal{P}(A) \cup \mathcal{P}(B).
\end{array}$$

Слично, ако је $A \cup B = A$, добијамо да из $X \in \mathcal{P}(A \cup B)$ следи $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Дакле, закључујемо да ако је $A \subseteq B$ или $B \subseteq A$, онда је $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.

10. Приметимо да је $x \in A \setminus B$ ако и само ако $x \in A$ и није $x \in B$, што можемо записати као $x \in A$ и $x \in B^c$, па је $A \setminus B = A \cap B^c$. Даље, посматрајмо скуп $(A^c \cap B^c)^c$. Према Де Моргановим законима и особини $(A^c)^c = A$, важи
$$(A^c \cap B^c)^c = (A^c)^c \cup (B^c)^c = A \cup B.$$

11. Нека су скупови $A = \{1, 2\}, B = \{2, 3\}, C = \{2, 4\}$. Тада је $A \cap B = \{2\} = A \cap C$, али је очидледно $B \neq C$.

12.

$$\begin{aligned}(a,c)\in(A\cap B)\times(C\cap D)) \quad &\text{акко} \quad a\in A\cap B \text{ и } c\in C\cap D\\ &\text{акко} \quad a\in A \text{ и } a\in B \text{ и } c\in C \text{ и } x\in D\\ &\text{акко} \quad (a,c)\in A\times C \text{ и } (a,c)\in B\times D\\ &\text{акко} \quad (a,c)\in (A\times C)\cap(B\times D).\end{aligned}$$

13.

$$\begin{aligned}(a,b)\in A\times(B\setminus C) \quad &\text{акко} \quad a\in A \text{ и } b\in B\setminus C\\ &\text{акко} \quad a\in A \text{ и } b\in B \text{ и } c\notin C\\ &\text{акко} \quad (a,b)\in A\times B \text{ и } (a,b)\notin A\times C\\ &\text{акко} \quad (a,b)\in (A\times B)\setminus(A\times C).\end{aligned}$$

Глава 3

1. Дакле, претпоставка је да је $\rho\circ\sigma\subseteq\rho$ и $\rho\circ\sigma^{-1}\subseteq\rho$.

$$\begin{aligned}(a,b)\in\rho\cap(\tau\circ\sigma) \quad &\text{следи} \quad (a,b)\in\rho \text{ и } (a,b)\in\tau\circ\sigma\\ &\text{следи} \quad (a,b)\in\rho \text{ и постоји } c\in A \text{ тако да } (a,c)\in\sigma \text{ и } (c,b)\in\tau\\ &\text{следи} \quad c\in A:(a,b)\in\rho \text{ и } (c,a)\in\sigma^{-1} \text{ и } (c,b)\in\tau\\ &\text{следи} \quad c\in A:(c,b)\in\rho\circ\sigma^{-1}\subseteq\rho \text{ и } (a,c)\in\sigma \text{ и } (c,b)\in\tau\\ &\text{следи} \quad c\in A:(c,b)\in\rho \text{ и } (a,c)\in\sigma \text{ и } (c,b)\in\tau\\ &\text{следи} \quad c\in A:(c,b)\in\rho\cap\tau \text{ и } (a,c)\in\sigma\\ &\text{следи} \quad (a,b)\in(\rho\cap\tau)\circ\sigma.\end{aligned}$$

$$\begin{aligned}(a,b)\in(\rho\cap\tau)\circ\sigma \quad &\text{следи} \quad \text{постоји } c\in A \text{ тако да } (a,c)\in\sigma \text{ и } (c,b)\in\rho\cap\tau\\ &\text{следи} \quad c\in A:(a,c)\in\sigma \text{ и } (c,b)\in\rho \text{ и } (c,b)\in\tau\\ &\text{следи} \quad (a,b)\in\tau\circ\sigma \text{ и } (a,b)\in\rho\circ\sigma\subseteq\rho\\ &\text{следи} \quad (a,b)\in\tau\circ\sigma \text{ и } (a,b)\in\rho\\ &\text{следи} \quad (a,b)\in\rho\cap(\tau\circ\sigma) \text{ и } (a,b)\in\rho.\end{aligned}$$

2. (а) Нека је $(a,b),(b,a)\in\rho^{-1}$. Тада је $(b,a),(a,b)\in\rho$, па је $a=b$, што значи да је ρ^{-1} антисиметрична. Ако је $(a,b),(b,a)\in\rho\cap\sigma$, онда је $(b,a),(a,b)\in\rho$, па је $a=b$, а тиме је и $\rho\cap\sigma$ антисиметрична.

   (б) Претпоставимо да је $\rho\cup\sigma$ антисиметрична. Нека је $(a,b)\in\rho\cap\sigma^{-1}$. Тада је $(a,b)\in\rho$ и $(a,b)\in\sigma^{-1}$, то јест $(a,b)\in\rho$ и $(b,a)\in\sigma$. Имамо да је $(a,b),(b,a)\in\rho\cup\sigma$, а та релација је антисиметрична, па мора бити $a=b$, Дакле,$(a,b)\in\triangle_A$.

   Претпоставимо да је $\rho\cap\sigma^{-1}\subseteq\triangle_A$. Нека је $(a,b),(b,a)\in\rho\cup\sigma$. Имамо четири случаја. Први је да $(a,b),(b,a)\in\rho$, а тада из симетричности ρ следи да је $a=b$. Други је да $(a,b),(b,a)\in\sigma$. Слично је и тада $a=b$. Трећи случај је да $(a,b)\in\rho$ и $(b,a)\in\sigma$. Тада је $(a,b)\in\rho$ и $(a,b)\in\sigma^{-1}$, па је $(a,b)\in\rho\cap\sigma^{-1}$. Према претпоставци, важи $\rho\cap\sigma^{-1}\subseteq\triangle_A$, па је $(a,b)\in\triangle_A$, то јест $a=b$. Четврти случај је $(b,a)\in\rho$ и $(a,b)\in\sigma$. Овде се, слично као у трећем случају, изведе да је $a=b$. Пошто је $a=b$ у сваком случају, онда је $\rho\cup\sigma$ антисиметрична.

3. (а) Нека су $(x,y),(y,z)\in\sigma_n$. Тада је $x+n\leq y$ и $y+n\leq z$. Следи да је $y\leq z-n$, па је $x+n\leq y\leq z-n\leq z$. Дакле, $(x,z)\in\sigma_n$, па како су x,y,z произвољни природни бројеви, следи да је релација σ_n транзитивна.

(б) Претпоставимо да је $m \leq n$. Нека је $(x, y) \in \sigma_n$. Тада је $x + n \leq y$. Посматрајмо број $x+m$. Важи да је $x+m \leq x+n \leq y$. Дакле, $(x, y) \in \sigma_m$. Претпоставимо да је $\sigma_n \subseteq \sigma_m$. Тада важи $x+n \leq y \Rightarrow x+m \leq y$, за све $x, y \in \mathbb{N}$. Нека је $x = 0$ и $y = n$. Важи да је $0+n \leq n$, па је и $0+m \leq n$, то јест $m \leq n$.

(в)

$$\begin{array}{lll} \text{Из } (x,y) \in \sigma_m \circ \sigma_n & \text{следи} & \text{постоји } z \in \mathbb{N} \text{ тако да } (x,z) \in \sigma_n \text{ и } (z,y) \in \sigma_m \\ & \text{следи} & z \in \mathbb{N} : x+n \leq z \text{ и } z+m \leq y \\ & \text{следи} & x+m+n \leq z+m \leq y \\ & \text{следи} & (x,y) \in \sigma_{m+n}. \end{array}$$

4. За $x = 1$ важи $1^2 + 1^2 = 2 > 1$, па $(1, 1) \notin \rho$, што значи да ρ није рефлексивна. Важи да је $0^2 + 0^2 = 0 \leq 1$, па је $(0, 0) \in \rho$, па ρ није ни антирефлексивна. Због комутативности сабирања реалних бројева важи $x^2 + y^2 \leq 1 \Rightarrow y^2 + x^2 \leq 1$, па је ρ симетрична. Важи да је $(\frac{1}{2})^2 + (\frac{1}{3})^2 \leq 1$ и $(\frac{1}{3})^2 + (\frac{1}{2})^2 \leq 1$, али је $\frac{1}{2} \neq \frac{1}{3}$. Дакле, ρ није антисиметрична. Није ни транзитивна: $1^2 + 0^2 \leq 1$ и $0^2 + 1^2 \leq 1$, али није $1^2 + 1^2 \leq 1$.

5. Није рефлексивна, јер је, на пример, $-1 \neq |-1| = 1$, па није $(-1, -1) \in \rho$. Није антирефлексивна: $1 = |1|$, па је $(1, 1) \in \rho$. Није симетрична: $1 = |-1|$ и $-1 \neq |1|$, што значи да је $(1, -1) \in \rho$ и $(-1, 1) \notin \rho$. Даље, нека је $(x, y), (y, x) \in \rho$. Тада је $x = |y|$ и $y = |x|$, па су и x и y ненегативни бројеви. Такође је $x = |y| = y$, па је релација антисиметрична. Нека је $(x, y), (y, z) \in \rho$. То значи да је $x = |y|$ и $y = |z|$, па су x и y ненегативни бројеви, а онда је и $x = y = |z|$. Дакле, ρ је транзитивна.

6. Користимо карактеризацију релације еквиваленције дате у примеру 3.17. Претпоставимо прво да је $\sigma \circ \rho = \rho \circ \sigma$. Нека је $(a, a) \in \triangle_A$. Релације ρ и σ су релације еквиваленције, па је $\triangle_A \subseteq \rho$ и $\triangle_A \subseteq \sigma$. Тада је елемент $a \in A$ је такав да $(a, a) \in \rho$ и $(a, a) \in \sigma$, па је $(a, a) \in \sigma \circ \rho$. Дакле, $\triangle_A \subseteq \sigma \circ \rho$. Такође, важи $\rho^{-1} = \rho$ и $\sigma^{-1} = \sigma$, па је према 3.8

$$(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1} = \rho \circ \sigma = \sigma \circ \rho.$$

Доказали смо и да је $(\sigma \circ \rho)^{-1} = \sigma \circ \rho$. Да би $\sigma \circ \rho$ била релација еквиваленције, треба још доказати да $(\sigma \circ \rho) \circ (\sigma \circ \rho) = \sigma \circ \rho$. Користећи претпоставку и тврђење 3.6 важи

$$(\sigma \circ \rho) \circ (\sigma \circ \rho) = \sigma \circ \rho \circ \sigma \circ \rho = \sigma \circ \rho \circ \rho \circ \sigma = \sigma \circ \rho \circ \sigma = \sigma \circ \sigma \circ \rho = \sigma \circ \rho.$$

Претпоставимо сада да је $\sigma \circ \rho$ релација еквииваленције. Докажимо да је $\sigma \circ \rho = \rho \circ \sigma$. Важи

$$\sigma \circ \rho = (\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1} = \rho \circ \sigma.$$

7. Релације ρ и σ су релације поретка, па је $\triangle_A \subseteq \rho$ и $\triangle_A \subseteq \sigma$. Тиме је и $\triangle_A \subseteq \sigma^{-1}$, па и $\triangle_A \subseteq \rho \cap \sigma^{-1}$. Даље је

$$\begin{aligned} (\rho \cap \sigma^{-1}) \cap (\rho \cap \sigma^{-1})^{-1} &= (\rho \cap \sigma) \cap (\rho^{-1} \cap \sigma) = \rho \cap \sigma^{-1} \cap \rho^{-1} \cap \sigma \\ &= (\rho \cap \rho^{-1}) \cap (\sigma \cap \sigma^{-1}) \subseteq \triangle_A \cap \triangle_A = \triangle_A \end{aligned}$$

Остало је још да се докаже транзитивност. Нека су $(a, b), (b, c) \in \rho \cap \sigma^{-1}$. Тада је $(a, b), (b, c) \in \rho$, па и $(a, c) \in \rho$. Такође је $(a, b), (b, c) \in \sigma^{-1}$, па $(b, a), (c, b) \in \sigma$, а тиме и $(c, a) \in \sigma \Rightarrow (a, c) \in \sigma^{-1}$. Следи да је $(a, c) \in \rho \cap \sigma^{-1}$.

8. Нека је $\rho \subseteq A \times A$ релација која задовољава тражене услове. Нека је $(a, b) \in \rho$ произвољни елемент. Како је ρ симетрична, важи $(b, a) \in \rho$. Дакле, имамо $(a, b), (b, a) \in \rho$, која је антисиметрична, па је $a = b$. То значи да је $(a, b) \in \triangle_A$, па је $\rho \subseteq \triangle_A$. Због рефлексивности релације ρ важи $\triangle_A \subseteq \rho$, п амора бити $\triangle_A = \rho$.

9. (а) У оба случаја претпоставимо супротно: постоји најмањи (највећи) елемент a. Тада је, према коментару после дефиниције, a и једини минимални (максимални). Добили смо контрадикцију.

   (б) Претпоставимо да је a најмањи елемент у односу на $\prec$. Тада је за свако $x \in A$ $a \prec x$. Ово је еквивалентно са изјавом да је за свако $x \in A$ $x \prec^{-1} a$. То управо значи да је a највећи у односу на $\prec^{-1}$. Ако је a минимални у односу на $\prec$, то значи да за свако $x \in A$ важи $x \prec a \Rightarrow x = a$. То је еквивалентно исказу: за свако $x \in A$ је $a \prec^{-1} x \Rightarrow x = a$. Последње управо значи да је a максимални у односу на $\prec^{-1}$. Слично се докаже и остатак тврђења.

10. За свако $x \in \mathbb{R}$ важи $\cos x = \cos x$, па је $\sim$ рефлексивна. Такође, за све $x, y \in \mathbb{R}$ важи да $\cos x = \cos y \Rightarrow \cos y = \cos x$, па је $\sim$ и симетрична. За $x, y, z \in \mathbb{R}$: ако је $\cos x = \cos y$ и $\cos y = \cos z$, онда је $\cos x = \cos z$, па важи транзитивност. Дакле, $\sim$ је релација еквиваленције. Даље, важи

$$C_\alpha = \{x \in \mathbb{R} \mid \cos x = \cos \alpha\} = \{x \in \mathbb{R} \mid x = \pm\alpha + 2k\pi, \text{ за } k \in \mathbb{Z}\} = \{\pm\alpha + 2k\pi \mid k \in \mathbb{Z}\}.$$

11. За сваки елемнент $(x, y) \in B$ важи да је $xy = xy$, па је $\sim$ рефлексивна. Ако је $(x, y) \sim (z, t)$ онда је $xy = zt$, па и $zt = xy$, а тиме и $(z, t) \sim (x, y)$. Нека је $(x, y) \sim (z, t)$ и $(z, t) \sim (r, s)$. Тада је $xy = zt$ и $zt = rs$, па је $xy = rs$, то јест $(x, y) \sim (r, s)$. Дакле, релација $\sim$ је релација еквиваленције. Приметимо да је

$$\begin{aligned} C_{(0,0)} &= \{(0,0), (0,1), (0,2), (1,0), (2,0)\} = C_{(0,1)} = C_{(0,2)} = C_{(1,0)} = C_{(2,0)} \\ C_{(1,1)} &= \{(1,1)\} \\ C_{(1,2)} &= \{(1,2), (2,1)\} = C_{(2,1)} \\ C_{(2,2)} &= \{(2,2)\}, \end{aligned}$$

па је количнички скуп једнак

$$B/\sim = \{\{(0,0), (0,1), (0,2), (1,0), (2,0)\}, \{(1,1)\}, \{(1,2), (2,1)\}, \{(2,2)\}\}.$$

12. Како је за све $(x, y) \in C$ $|x| \leq |x|$ и $y \mid y$, онда је $(x, y) \prec (x, y)$, па је $\prec$ рефлексивна. Нека је $(x, y) \prec (z, t)$ и $(z, t) \prec (x, y)$. Тада је

$$|x| \leq |z| \qquad y \mid t \qquad |z| \leq |x| \qquad t \mid y.$$

Према томе како су дефинисани скупови A и B јасно је да је $x = z$ и $y = t$. Дакле, $(x, y) = (z, t)$, па је $\prec$ антисиметрична. Проверимо и транзитивност. Нека су $(x, y), (z, t), (r, s) \in C$ такви да $(x, y) \prec (z, t)$ и $(z, t) \prec (r, s)$. Тада је

$$|x| \leq |z| \qquad y \mid t \qquad |z| \leq |r| \qquad t \mid s.$$

Следи да је $|x| \leq |r|$ и $y \mid s$, па је $(x, y) \prec (r, s)$.

Како је за све $(x, y) \in C$ $|0| \leq |x|$ и $2 \mid y$, онда је елемент $(0, 2)$ најмањи. Такође је за све (x, y) $|x| \leq |-6|$ и $y| \mid 32$, па је $(-6, 32)$ највећи елемент. Самим тим, једини минимални је $(0, 2)$ и једини максимални $(-6, 32)$.

13. За сваки скуп важи да је $X \subseteq X$, па је $\prec$ рефлексивна. Такође, према тврђењу 2.4, ако је $X \subseteq Y$ и $Y \subseteq X$, онда је $X = Y$. Нека су још $X, Y, Z \in A$. Ако је $X \subseteq Y$ и $Y \subseteq Z$, онда је $X \subseteq Z$.

    Јасно је да је сваки елемент $X \in A$ такав да $X \subseteq B$, па је B највећи елемент. Тада је и једини максимални B. Ако је скуп A једночлан, на пример $A = \{a\}$, онда је $B = \mathcal{P}(\{a\})\emptyset = \{\{a\}\}$ и тада постоји најмањи елемент: то је $\{a\}$. Ако скуп A има бар два елемента, онда је, на пример, $A = \{a_1, a_2, \dots\}$. Ако је X најмањи елемент, онда мора бити $X \subseteq \{a_1\}$ и $X \subseteq \{a_2\}$, што је немогуће. Дакле, у том случају најмањи не постоји. Ако је A једночлан, једини минимални је $\{a\}$. Ако има бар два елемента, онда важи: ако је $b \in A$ било који елемент, тада је тачно да за свако $X \in B$ $X \subseteq \{b\} \Rightarrow X = \{b\}$. Дакле, сви једночлани скупови су минимални.

Глава 4

1. Нека је $z \in Z$ произвољни елемент. Треба доказати да постоји $y \in Y$ тако да $g(y) = z$. Како је $g \circ f$ "на", то постоји $x \in X$ тако да $(g \circ f)(x) = z$, то јест $g(f(x)) = z$. Ставимо $f(x) = y$. Тада важи $g(y) = z$.

2.

$$\begin{aligned} z \in (g \circ f)[A] \quad & \text{акко} \quad \text{постоји } x \in A \text{ тако да } (g \circ f)(x) = z \\ & \text{акко} \quad \text{постоји } x \in A \text{ тако да } g(f(x)) = z \\ & \text{акко} \quad \text{постоји } x \in A \text{ и } f(x) = y \text{ и } g(y) = z \\ & \text{акко} \quad \text{постоји } y \in Y \text{ тако да } y \in f[A] \text{ и } g(y) = z \\ & \text{акко} \quad z \in g[f[A]]. \end{aligned}$$

$$\begin{aligned} x \in (g \circ f)^{-1}[B] \quad & \text{акко} \quad (g \circ f)(x) \in B \\ & \text{акко} \quad g(f(x)) \in B \\ & \text{акко} \quad f(x) \in g^{-1}[B] \\ & \text{акко} \quad x \in f^{-1}[g^{-1}[B]]. \end{aligned}$$

3. Пошто су f и g бијекције, онда су и "1-1" и "на". Према већ урађеном примеру, када су f и g "1-1", онда је и $g \circ f$ "1-1". Треба доказати да је $g \circ f$ "на". Нека је $z \in Z$. Како је g "на", онда постоји $y \in Y$ тако да $g(y) = z$. Такође, из $y \in Y$ и f је "на" следи да постоји $x \in X$ тако да $f(x) = y$. Сада имамо $(g \circ f)(x) = g(f(x)) = g(y) = z$. Дакле, постоји $x \in X$ тако да $(g \circ f)(x) = z$, па је $g \circ f$ "на", а како је и "1-1", онда је бијекција.

4.

$$\begin{aligned} y \in f[A \cap B] \quad & \text{акко} \quad \text{постоји } x \in A \cap B \text{ тако да } f(x) = y \\ & \text{следи} \quad x \in A \text{ и } x \in B \text{ тако да } f(x) = y \\ & \text{следи} \quad y \in f[A] \text{ и } y \in f[B] \\ & \text{следи} \quad y \in f[A] \cap f[B]. \end{aligned}$$

    Нека је $X = \{1, 2, 3, 4\}$ и $Y = \{\alpha, \beta\}$ и f таква да $f(1) = f(2) = f(3) = f(4) = \alpha$. Нека је још $A = \{1, 2\}$ и $B = \{3, 4\}$. Видимо да је $f[A \cap B] = f[\emptyset] = \emptyset$, а $f[A] \cap f[B] = \{\alpha\} \cap \{\alpha\} = \{\alpha\}$, па никако не може бити $f[A] \cap f[B] \subseteq f[A \cap B]$.

5.

$$\begin{aligned} y \in f[A] \setminus f[B] \quad & \text{акко} \quad y \in f[A] \text{ и } y \notin f[B] \\ & \text{следи} \quad \text{постоји } x \in A \text{ и } f(x) = y \text{ и } x \notin B \\ & \text{следи} \quad x \in A \setminus B \text{ и } f(x) = y \\ & \text{следи} \quad y \in f[A \setminus B]. \end{aligned}$$

Нека је $X = \{1,2,3,4\}$ и $Y = \{\alpha,\beta\}$ и f таква да $f(1) = f(3) = \alpha$ и $f(2) = f(4) = \beta$. Нека је још $A = \{1,2,3\}$ и $B = \{1,2\}$. Тада је $f[A \setminus B] = f[\{3\}] = \{\alpha\}$ и $f[A] \setminus f[B] = \{\alpha,\beta\} \setminus \{\alpha,\beta\} = \emptyset$. Дакле, немогуће је да $f[A \setminus B] \subseteq f[A] \setminus f[B]$.

6.

$$\begin{aligned} x \in f^{-1}[A \cap B] \quad & \text{акко} \quad f(x) \in A \cap B \\ & \text{акко} \quad f(x) \in A \text{ и } f(x) \in B \\ & \text{акко} \quad x \in f^{-1}[A] \text{ и } x \in f^{-1}[B] \\ & \text{акко} \quad x \in f^{-1}[A] \cap f^{-1}[B]. \end{aligned}$$

7.

$$\begin{aligned} x \in f^{-1}[A \cup B] \quad & \text{акко} \quad f(x) \in A \cup B \\ & \text{акко} \quad f(x) \in A \text{ или } f(x) \in B \\ & \text{акко} \quad x \in f^{-1}[A] \text{ или } x \in f^{-1}[B] \\ & \text{акко} \quad x \in f^{-1}[A] \cup f^{-1}[B]. \end{aligned}$$

8.

$$\begin{aligned} y \in f[A] \cup B^c \quad & \text{следи} \quad y \in f[A] \text{ и } y \in B^c \\ & \text{следи} \quad \text{постоји } x \in A : f(x) = y \text{ и } y \notin B \\ & \text{следи} \quad x \in A : f(x) = y \text{ и } f(x) \notin B \\ & \text{следи} \quad x \in A : f(x) = y \text{ и } x \notin f^{-1}[B] \\ & \text{следи} \quad x \in A \setminus f^{-1}[B] \text{ и } f(x) = y \\ & \text{следи} \quad f(x) \in f[A \setminus f^{-1}[B]] \text{ и } f(x) = y \\ & \text{следи} \quad y \in f[A \setminus f^{-1}[B]]. \end{aligned}$$

$$\begin{aligned} y \in f[A \setminus f^{-1}[B]] \quad & \text{следи} \quad \text{постоји } x \in A \setminus f^{-1}[B] : f(x) = y \\ & \text{следи} \quad \text{постоји } x \in A : f(x) = y \text{ и } y \notin B \\ & \text{следи} \quad x \in A \text{ и } x \notin f^{-1}[B] \text{ и } f(x) = y \\ & \text{следи} \quad x \in A \text{ и } f(x) \notin B \text{ и } f(x) = y \\ & \text{следи} \quad f(x) \in f[A] \text{ и } f(x) \in B^c \text{ и } f(x) = y \\ & \text{следи} \quad y \in f[A] \text{ и } y \in B^c \\ & \text{следи} \quad y \in f[A] \cup B^c. \end{aligned}$$

9. Како је $f[A] \subseteq Y$ и $f[B] \subseteq Y$, мора бити $f[A] \cup f[B] \subseteq Y$. Треба доказати и обрнуто.

$$\begin{aligned} \text{Из } y \in Y \quad & \text{следи} \quad \text{постоји } x \in X \text{ тако да } f(x) = y, \text{ јер је } f\text{"на"} \\ & \text{следи} \quad x \in A \cup B \text{ и } f(x) = y, \text{ јер је } A \cup B = X \\ & \text{следи} \quad x \in A \text{ или } x \in B; f(x) = y \\ & \text{следи} \quad f(x) \in f[A] \text{ или } f(x) \in f[B]; f(x) = y \\ & \text{следи} \quad y \in f[A] \cup f[B]. \end{aligned}$$

10. (a) Претпоставимо прво да је f "1-1". Треба доказати да је за сваки скуп $A \subseteq X$ $f^{-1}[f[A]] = A$. Нека је $A \subseteq X$ приозвољан скуп. Инклузија $A \subseteq f^{-1}[f[A]]$ важи и без претпоставке да је f "1-1". Наиме, ако је $x \in A$ онда је $f(x) \in f[A]$, па и $x \in f^{-1}[f[A]]$. С друге стране

$$\begin{aligned} x \in f^{-1}[f[A]] \quad & \text{акко} \quad f(x) \in f[A] \\ & \text{следи} \quad \text{постоји } y \in A \text{ тако да } f(x) = f(y) \\ & \text{следи} \quad x = y \in A, \text{ јер је } f \text{ "1-1"} \\ & \text{следи} \quad x \in A. \end{aligned}$$

Претпоставимо сада да је за сваки скуп $A \subseteq X$ $f^{-1}[f[A]] = A$. Треба доказати да је f "1-1". Нека је $f(x_1) = f(x_2)$, за $x_1, x_2 \in X$. Важи

$$f(x_1) \in f[\{x_1\}] = f[\{x_2\}] \Rightarrow x_1 \in f^{-1}[f[\{x_2\}]].$$

Према претпоставци је $f^{-1}[f[\{x_2\}]] = \{x_2\}$. Дакле, $x_1 \in \{x_2\}$, па мора бити $x_1 = x_2$, што значи да је f "1-1".

(б) Дефинишимо функцију $g : \mathcal{P}(Y) \to \mathcal{P}(X)$ на следећи начин: за $B \in \mathcal{P}(Y)$ $g(B) = f^{-1}[B]$. Пошто је $B \subseteq Y$ и $f : X \to Y$, то је $f^{-1}[B] \subseteq X$, а тиме и $f^{-1} \in \mathcal{P}(X)$. Дакле, функција g је добро дефинисана. Докажимо да је "на". Нека је $A \in \mathcal{P}(X)$, то јест $A \subseteq X$. Како је f "1-1", преме претходном делу је $f^{-1}[f[A]] = A$. Тада је $g(f[A]) = f^{-1}[f[A]] = A$. Дакле, скуп $f[A]$ се слика у A са g, па је g сурјекција.

11. (а) Нека је f "на". Треба доказати да је за сваки скуп $B \subseteq Y$ $f[f^{-1}[B]] = B$. Инклузија $f[f^{-1}[B]] \subseteq B$ важи и без претпоставке да је f "на".

$$\begin{aligned} y \in f[f^{-1}[B]] \quad & \text{акко} \quad \text{постоји } x \in f^{-1}[B] \text{ тако да } f(x) = y \\ & \text{следи} \quad f(x) \in B \text{ и } f(x) = y \\ & \text{следи} \quad y \in B. \end{aligned}$$

Докажимо и обрнуто:

$$\begin{aligned} y \in B \quad & \text{следи} \quad \text{постоји } x \in X \text{ тако да } f(x) = y \in B, \text{ јер је } f \text{ "1-1"} \\ & \text{следи} \quad x \in f^{-1}[B] \text{ и } f(x) = y \\ & \text{следи} \quad f(x) \in f[f^{-1}[B]] \text{ и } f(x) = y \\ & \text{следи} \quad y \in f[f^{-1}[B]]. \end{aligned}$$

Претпоставимо сада да је за сваки скуп $B \subseteq Y$ $f[f^{-1}[B]] = B$. Треба доказати да је f "на". Нека је $y \in Y$. Тада је $f[f^{-1}[Y]] = Y$, па је $y \in f[f^{-1}[Y]]$. То значи да постоји $x \in f^{-1}[Y] = X$ тако да $f(x) = y$. Нашли смо елемент из X који се слика у y, па је f "на".

(б) Дефинишимо функцију $g : \mathcal{P}(Y) \to \mathcal{P}(X)$ као и у претходном задатку: за $B \in \mathcal{P}(Y)$ $g(B) = f^{-1}[B]$. Јасно је да је g добро дефинисана. Докажимо да је "1-1". Нека је $g(B_1) = g(B_2)$. Тада је $f^{-1}[B_1] = f^{-1}[B_2]$, па и $f[f^{-1}[B_1]] = f[f^{-1}[B_2]]$. Из претходног дела следи да је $B_1 = B_2$.

12.

$$\begin{aligned} \chi_{(A\cap B\cap C)\setminus D} &= \chi_{A\cap B\cap C} + \chi_{A\cap B\cap C}\chi_D \\ &= \chi_A\chi_B\chi_C + \chi_A\chi_B\chi_C\chi_D \end{aligned}$$

$$\begin{aligned} \chi_{(A\setminus D)\cap(B\setminus D)\cap(C\setminus D)} &= \chi_{A\setminus D}\chi_{B\setminus D}\chi_{C\setminus D} \\ &= (\chi_A + \chi_A\chi_D)(\chi_B + \chi_B\chi_D)(\chi_C + \chi_C\chi_D) \\ &= (\chi_A\chi_B + \chi_A\chi_B\chi_D + \chi_A\chi_D\chi_B + \chi_A\chi_D\chi_B\chi_D)(\chi_C + \chi_C\chi_D) \\ &= (\chi_A\chi_B + \chi_A\chi_B\chi_D)(\chi_C + \chi_C\chi_D) \\ &= \chi_A\chi_B\chi_C + \chi_A\chi_B\chi_C\chi_D + \chi_A\chi_B\chi_D\chi_C + \chi_A\chi_B\chi_C\chi_D \\ &= \chi_A\chi_B\chi_C + \chi_A\chi_B\chi_C\chi_D \end{aligned}$$

Видимо да је $\chi_{(A\cap B\cap C)\setminus D} = \chi_{(A\setminus D)\cap(B\setminus D)\cap(C\setminus D)}$, па важи тражена једнакост.

13. Претпоставимо да је $(A \setminus B) \setminus C = (B \setminus C) \setminus A$. Тада важи

$$\begin{aligned}
\chi_{(A\setminus B)\setminus C} = \chi_{(B\setminus C)\setminus A} \quad &\text{следи} \quad \chi_{A\setminus B} + \chi_{A\setminus B}\chi_C = \chi_{B\setminus C} + \chi_{B\setminus C}\chi_A \\
&\text{следи} \quad \chi_A + \chi_A\chi_B + \chi_A\chi_C + \chi_A\chi_B\chi_C = \\
&\qquad\quad = \chi_B + \chi_B\chi_C + \chi_B\chi_A + \chi_B\chi_C\chi_A \\
&\text{следи} \quad \chi_A + \chi_A\chi_C = \chi_B + \chi_B\chi_C \\
&\text{следи} \quad \chi_A + \chi_C + \chi_A\chi_C = \chi_B + \chi_C + \chi_B\chi_C \\
&\text{следи} \quad \chi_{A\cup C} = \chi_{B\cup C},
\end{aligned}$$

па је према тврђењу 4.2 $A \cup C = B \cup C$.

Претпоставимо да је $A \cup C = B \cup C$.

$$\begin{aligned}
\chi_{A\cup C} = \chi_{B\cup C} \quad &\text{следи} \quad \chi_A + \chi_C + \chi_A\chi_C = \chi_B + \chi_C + \chi_B\chi_C \\
&\text{следи} \quad \chi_A + \chi_A\chi_C = \chi_B + \chi_B\chi_C \\
&\text{следи} \quad \chi_A + \chi_A\chi_B + \chi_A\chi_C + \chi_A\chi_B\chi_C = \\
&\qquad\quad = \chi_B + \chi_B\chi_C + \chi_A\chi_B + \chi_A\chi_B\chi_C \\
&\text{следи} \quad \chi_{A\setminus B} + (\chi_A + \chi_A\chi_B)\chi_C = \\
&\qquad\quad = \chi_{B\setminus C} + (\chi_B + \chi_B\chi_C)\chi_A \\
&\text{следи} \quad \chi_{A\setminus B} + \chi_{A\setminus B}\chi_C = \chi_{B\setminus C} + \chi_{B\setminus C}\chi_A \\
&\text{следи} \quad \chi_{(A\setminus B)\setminus C} = \chi_{(B\setminus C)\setminus A},
\end{aligned}$$

па је $(A \setminus B) \setminus C = (B \setminus C) \setminus A$.

14. Претпоставимо да је $(A \setminus B) \setminus C = A \setminus B$. Тада из

$$\begin{aligned}
\chi_{(A\setminus B)\setminus C} = \chi_{A\setminus B} \quad &\text{следи} \quad \chi_{A\setminus B} + \chi_{A\setminus B}\chi_C = \chi_{A\setminus B} \\
&\text{следи} \quad \chi_A + \chi_A\chi_B + (\chi_A + \chi_A\chi_B)\chi_C = \chi_A + \chi_A\chi_B \\
&\text{следи} \quad \chi_A\chi_C + \chi_A\chi_B\chi_C = 0 \\
&\text{следи} \quad \chi_A\chi_C = \chi_A\chi_B\chi_C \\
&\text{следи} \quad \chi_{A\cap C} = \chi_{A\cap B\cap C} \\
&\text{следи} \quad A \cap C = A \cap B \cap C \\
&\text{следи} \quad A \cap B \subseteq C.
\end{aligned}$$

Ако је $A \cap B \subseteq C$, онда важи да је $A \cap C = A \cap C \cap B$, па из

$$\begin{aligned}
\chi_{A\cap C} = \chi_{A\cap C\cap B} \quad &\text{следи} \quad \chi_A\chi_C = \chi_A\chi_B\chi_C \\
&\text{следи} \quad \chi_A\chi_C + \chi_A\chi_B\chi_C = 0 \\
&\text{следи} \quad (\chi_A + \chi_A\chi_B)\chi_C = 0 \\
&\text{следи} \quad \chi_{A\setminus B} + \chi_{A\setminus B}\chi_C = \chi_{A\setminus B} \\
&\text{следи} \quad \chi_{(A\setminus B)\setminus C} = \chi_{A\setminus B} \\
&\text{следи} \quad (A \setminus B) \setminus C = A \setminus B.
\end{aligned}$$

Глава 5

1. Нека је $f : \mathbb{N}_{\geq 5} \to \mathbb{N}$ задата са $f(n) = n - 5$. Дакле,

$$f: \qquad 5 \mapsto 0 \qquad 6 \mapsto 1 \qquad 7 \mapsto 2 \cdots$$

Ако је $f(n) = f(m)$, за неке $n, m \in \mathbb{N}_{\geq 5}$, онда је $n - 5 = m - 5$, па је $n = m$. То значи да је f "1-1", треба још доказати да је "на". Нека је $n \in \mathbb{N}$ било који елемент. Тада је број $n + 5$ сигурно елемент скупа $\mathbb{N}_{\geq 5}$. Важи да $f(n + 5) = n + 5 - 5 = n$.

2. Задајмо функцију $f : \mathbb{N} \setminus \{1, 3\} \to \mathbb{N}$ са:

$$\begin{array}{ccc} 0 & \mapsto & 0 \\ 2 & \mapsto & 1 \\ 4 & \mapsto & 2 \\ 5 & \mapsto & 3 \\ 6 & \mapsto & 4 \\ & \dots & \end{array}$$

Прецизније

$$f: \qquad 0 \mapsto 0 \qquad 2 \mapsto 1 \qquad k \mapsto k-2, \text{ за свако } k \geq 4.$$

Скупови $\{0, 2\}$ и $\{0, 1\}$ су у бијективној вези преко фунције f. Слично као у претходном задатку се докаже да се преко f скуп $\mathbb{N}_{\geq 4}$ слика бијективно на скуп $\mathbb{N}_{\geq 2}$.

3. Нека је $f : \{0, 1\} \times \mathbb{N} \to \mathbb{N}$ таква да

$$\begin{array}{rcl} f : (0, n) & \to & 2n \\ (1, n) & \to & 2n + 1. \end{array}$$

Заправо, важи да

$$\begin{array}{ccccccc} (0,0) & \mapsto & 0 & \quad & (1,0) & \mapsto & 1 \\ (0,1) & \mapsto & 2 & & (1,1) & \mapsto & 3 \\ (0,2) & \mapsto & 4 & & (1,3) & \mapsto & 5 \\ & \dots & & & & \dots & \end{array}$$

Нека је $f(i, n) = f(j, m)$, где су $i, j \in \{0, 1\}$ и $n, m \in \mathbb{N}$. Ако је $i \neq j$, тада је на пример $i = 0$ и $j = 1$, па добијамо $2n = 2m + 1$, што не важи ни за које природне бројеве n и m. Ако је $i = j = 0$ онда је $2n = 2m$, па $n = m$, а тиме и $(i, n) = (j, m)$. Слично, ако је $i = j = 1$, важи $2n + 1 = 2m + 1$, па је опет $(i, n) = (j, m)$. дакл,е f је "1-1". Нека је $k \in \mathbb{N}$ било који број. Ако је паран, облика је $k = 2n$, за $n \in \mathbb{N}$. Тада је $f(0, n) = 2n = k$. Ако је k напаран, посроји $m \in \mathbb{N}$ тако да $k = 2m + 1$. У том случају је $f(1, m) = 2m + 1 = k$, па је функција f "на".

4. Дефинишимо функцију $f : \{0, 1\} \times \{2, 3, 4\} \times \mathbb{N} \to \mathbb{N}$ тако да је за свако $n \in \mathbb{N}$

$$\begin{array}{ccccccc} (0,2,n) & \mapsto & 6n & \quad & (1,2,n) & \mapsto & 6n+1 \\ (0,3,n) & \mapsto & 6n+2 & & (1,3,n) & \mapsto & 6n+3 \\ (0,4,n) & \mapsto & 6n+4 & & (1,4,n) & \mapsto & 6n+5 \end{array}$$

Нека је $f(i_1, j_1, n_1) = f(i_2, j_2, n_2)$, где су $i_1, i_2 \in \{0, 1\}$, $j_1, j_2 \in \{2, 3, 4\}$ и $n_1, n_2 \in \mathbb{N}$. Ако би било $i_1 \neq i_2$ онда би $f(i_1, j_1, n_1) = f(i_2, j_2, n_2)$ истовремено био и паран и непаран број, што је немогуће. Дакле, мора бити $i_1 = i_2$. Слично, ако би било $j_1 \neq j_2$, опет бисмо добили немогуће једнакости. На пример, да је $j_1 = 2$ и $j_2 = 3$ и $i_1 = i_2 = 0$ било би $6n_1 = f(0, 2, n_1) = f(0, 3, n_2) = 6n_2 + 2$. Тиме добијамо једнакост $6(n_1 - n_2) = 2$, која не важи ни за које природне бројеве n_1 и n_2. Закључујемо да мора бити и $j_1 = j_2$. Сада се лако закључи и да у сваком од тих случајева мора бити $n_1 = n_2$. То значи да је $(i_1, j_1, n_1) = (i_2, j_2, n_2)$, па је f "1-1". Докажимо и да је f "на". Нека је k било који природан број. Његов остатак при дељењу са 6 је $i \in \{0, 1, 2, 3, 4, 5\}$. Тада се k може представити као $k = 6n + i$. Ако је, на пример $i = 3$, онда је $f(1, 3, n) = 6n + 3 = k$. Тако да, који год да је остатак i, постоји елемент из $\{0, 1\} \times \{2, 3, 4\} \times \mathbb{N} \to \mathbb{N}$ који се слика у k.

Глава 6

1. Нека је $\Phi(n): 1+3+5+\cdots+(2n-1)=n^2$. Тачно је $1=1^2$, па имамо базу индукције. Претпоставимо да је тачно $\Phi(n)$. Докажимо тачност исказа $\Phi(n+1): 1+3+5+\cdots+(2n-1)+(2(n+1)-1)=(n+1)^2$. Важи

$$\begin{aligned} 1+3+5+\cdots+(2n-1)+(2n+1) &= n^2+2n+1 \\ &= (n+1)^2. \end{aligned}$$

2. За $n=1$ важи $\frac{5}{1\cdot 2}=\frac{5}{2}=\frac{1(2\cdot 1+3)}{1+1}$, па је доказана база индукције. Претпоставимо да је тачно $\Phi(n): \frac{5}{1\cdot 2}+\frac{13}{2\cdot 3}+\cdots+\frac{2n^2+2n+1}{n(n+1)}=\frac{n(2n+3)}{n+1}$. Треба доказати да је тачно $\Phi(n+1): \frac{5}{1\cdot 2}+\frac{13}{2\cdot 3}+\cdots+\frac{2n^2+2n+1}{n(n+1)}+\frac{2(n+1)^2+2(n+1)+1}{(n+1)((n+1)+1}=\frac{(n+1)(2(n+1)+3}{(n+1)+1}$. Важи

$$\begin{aligned} & \frac{5}{1\cdot 2}+\frac{13}{2\cdot 3}+\cdots+\frac{2n^2+2n+1}{n(n+1)}+\frac{2(n+1)^2+2(n+1)+1}{(n+1)((n+1)+1} \\ = & \frac{n(2n+3)}{n+1}+\frac{2(n+1)^2+2(n+1)+1}{(n+1)((n+1)+1} \\ = & \frac{n(2n+3)(n+2)+2(n+1)^2+2(n+1)+1}{(n+1)(n+2)} \\ = & \frac{2n^3+4n^2+3n^2+6n+2n^2+4n+2+2n+2+1}{(n+1)(n+2)} \\ = & \frac{2n^3+9n^2+12n+5}{(n+1)(n+2)} \\ = & \frac{(n+1)(2n^2+7n+5)}{(n+1)(n+2)} \\ = & \frac{(n+1)(2n+5)}{n+2} \\ = & \frac{(n+1)(2(n+1)+3)}{(n+1)+1}. \end{aligned}$$

3. За $n=2$ важи $\frac{1}{2+1}+\frac{1}{2+2}=\frac{1}{3}+\frac{1}{4}=\frac{14}{24}>\frac{13}{24}$. Претпоставимо да је тачно $\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{n+n}>\frac{13}{24}$. Треба доказати да је $\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\cdots+\frac{1}{(n+1)+(n+1)}>\frac{13}{24}$. Важи

$$\begin{aligned} & \frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\cdots+\frac{1}{(n+1)+n-1}+\frac{1}{(n+1)+n}+\frac{1}{(n+1)+(n+1)}= \\ & \frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{n+n}+\frac{1}{n+n+1}+\frac{1}{n+1+n+1}= \\ & \frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{n+n}+\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}> \\ & \frac{13}{24}+\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}= \\ & \frac{13}{24}+\frac{2n+2+2n+1-2(2n+1)}{(2n+1)(2n+2)} \\ & \frac{13}{24}+\frac{2n+2+2n+1-4n-2}{(2n+1)(2n+2)} \\ & \frac{13}{24}+\frac{1}{(2n+1)(2n+2)}>\frac{13}{24}. \end{aligned}$$

Прву неједнакост смо добили из индуктивне претпоставке, а другу из неједнакости $\frac{1}{(2n+1)(2n+2)}>0$.

4. Како је $\frac{4^2}{2+1} = \frac{16}{3}$, а $\frac{(2\cdot 2)!}{(2!)^2} = \frac{4!}{4} = 6 = \frac{18}{3}$, онда је јасно да неједакост важи за $n = 2$. Претпоставимо да је тачно $\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$. Докажимо да је $\frac{4^{n+1}}{n+1+1} < \frac{((2(n+1))!}{((n+1)!)^2}$.

$$\begin{aligned}
\frac{((2(n+1))!}{((n+1)!)^2} &= \frac{(2n+2)!}{((n+1)n!)^2} \\
&= \frac{(2n+2)(2n+1)(2n)!}{(n+1)^2(n!)^2} \\
&= \frac{(2n+2)(2n+1)}{(n+1)^2} \cdot \frac{(2n)!}{(n!)^2} \\
&= \frac{2(2n+1)}{n+1} \cdot \frac{(2n)!}{(n!)^2} \\
&> \frac{2(2n+1)}{n+1} \cdot \frac{4^n}{n+1}.
\end{aligned}$$

У последњем кораку смо искористили индуктивну претпоставку. Наведена неједнакост за $n+1$ је сада еквивалентна са $\frac{2(2n+1)}{n+1} \cdot \frac{4^n}{n+1} \geq \frac{4^{n+1}}{n+1+1}$, па имамо низ еквиваленција:

$$\begin{aligned}
\frac{2(2n+1)}{n+1} \cdot \frac{4^n}{n+1} \geq \frac{4^{n+1}}{n+1+1} \quad &\text{акко} \quad \frac{4n+2}{(n+1)^2} \geq \frac{4}{n+2} \\
&\text{акко} \quad (4n+2)(n+2) \geq 4(n+1)^2 \\
&\text{акко} \quad 4n^2 + 10n + 4 \geq 4n^2 + 8n + 4 \\
&\text{акко} \quad 10n \geq 8n \\
&\text{акко} \quad 2n \geq 0.
\end{aligned}$$

Последња неједнакост је тачна, јер је n природан број. Дакле,

$$\frac{((2(n+1))!}{((n+1)!)^2} > \frac{2(2n+1)}{n+1} \cdot \frac{4^n}{n+1} \geq \frac{4^{n+1}}{n+1+1}.$$

5. За $n = 2$ имамо исказ $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}$, то јест $1 + \frac{1}{\sqrt{2}} > \sqrt{2}$. Еквивалентни исказ добијамо када последњи помножимо са $\sqrt{2}$: $\sqrt{2} + 1 > 2$, што је тачно, тако да смо доказали базу индукције. Претпоставимо да је тачно $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$. Докажимо да је $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} > \sqrt{n+1}$. Користећи индуктивну претпоставку добијамо $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} > \sqrt{n} + \frac{1}{\sqrt{n+1}}$. Докажимо да је $\sqrt{n} + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1}$. Тачан је следећи низ еквиваленција:

$$\begin{aligned}
\sqrt{n} + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1} \quad &\text{акко} \quad \frac{1 + \sqrt{n}\sqrt{n+1}}{\sqrt{n+1}} \geq \sqrt{n+1} \\
&\text{акко} \quad 1 + \sqrt{n}\sqrt{n+1} \geq n+1 \\
&\text{акко} \quad \sqrt{n(n+1)} \geq n \\
&\text{акко} \quad n(n+1) \geq n^2 \text{ јер су дати изрази ненегативни} \\
&\text{акко} \quad n^2 + n \geq n \\
&\text{акко} \quad n \geq 0.
\end{aligned}$$

Како је последња неједнакост тачна, јер је n природан број, онда је тачна и полазна неједнакост, а тиме је и

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} > \sqrt{n} + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1}.$$

6. Ако је $n=0$ број $3\cdot 5^1+2^1=17$ је дељив са 17. Претпоставимо да је $3\cdot 5^{2n+1}+2^{3n+1}$ дељив са 17. Докажмо да је $3\cdot 5^{2(n+1)+1}+2^{3(n+1)+1}$ дељив са 17. Важи

$$\begin{aligned}3\cdot 5^{2(n+1)+1}+2^{3(n+1)+1} &= 25\cdot 3\cdot 5^{2n+1}+8\cdot 2^{3n+1}=(17+8)\cdot 3\cdot 5^{2n+1}+8\cdot 2^{3n+1}\\ &= 17(3\cdot 5^{2n+1})+8(3\cdot 5^{2n+1}+2^{3n+1}).\end{aligned}$$

Први сабирак је очигледно дељив са 17, а према индуктивној претпоставци и други је. Тако да је и збир та два броја дељив са 17.

7. За $n=0$ је $0\cdot 4^{0+1}-(0+1)4^1+1=0$, па како је $9\mid 0$, доказана је база индукције. Нека је $f(n)=n\cdot 4^{n+1}-(n+1)4^n+1$. Претпоставимо да је $f(n)$ дељив са 9. Докажимо да је $f(n+1)$ дељив са 9. Приметимо да је

$$\begin{aligned}f(n+1)-f(n) &= (n+1)4^{n+2}-(n+2)4^{n+1}+1-(n\cdot 4^{n+1}-(n+1)4^n+1)\\ &= 4n\cdot 4^{n+1}+4^{n+2}-n\cdot 4^{n+1}-4(n+1)4^n-4^{n+1}+(n+1)4^n+1-1\\ &= 3(n\cdot 4^{n+1})-3((n+1)4^n)+4^{n+2}-4^{n+1}\\ &= 3(n\cdot 4^{n+1})-3((n+1)4^n)+3-3+4^{n+1}(4-1)\\ &= 3(n\cdot 4^{n+1}-(n+1)4^n+1)+3(4^{n+1}-1)\\ &= 3f(n)+3(4^{n+1}-1).\end{aligned}$$

Дакле, $f(n+1)=4f(n)+3(4^{n+1}-1)$. Према индуктивној претпоставци је $f(n)$ дељив са 9. Довољно је још доказати да је $4^{n+1}-1$ дељив са 3, за свако n. Тада ће $f(n+1)$ бити збир два броја дељива са 9.

Користићемо математичку индукцију да бисмо доказали да је $4^{n+1}-1$ дељив са 3. За $n=0$ је $3\mid 4-1$. Претпоставимо да $3\mid 4^{n+1}$. Како је

$$4^{n+2}-1=4^{n+1}\cdot 4-1+4-4=4(4^{n+1}-1)+3,$$

користећи индуктивну претпоставку добијамо да је $4^{n+2}-1$ дељив са 3.

8. Нека је $\Phi(n): a_n=2^n+n2^n$. Искази $\Phi(0): a_0=2^0+0\cdot 2^0=1$ и $\Phi(1): a_1=2^1+1\cdot 2^1=4$ су тачни према услову задатка. Претпоставимо да је тачно $\Phi(n)$ и $\Phi(n+1)$, то јест да је $a_n=2^n+n2^n$ и $a_{n+1}=2^{n+1}+(n+1)2^{n+1}$. Тада је

$$\begin{aligned}a_{n+2} &= 4a_{n+1}-4a_n\\ &= 4(2^{n+1}+(n+1)2^{n+1})-4(2^n+n2^n)\\ &= 2^2(2^{n+1}+(n+1)2^{n+1})-2^2(2^n+n2^n)\\ &= 2^{n+3}+(n+1)2^{n+3}-2^{n+2}-n2^{n+2}\\ &= 2^{n+2}(2-1)+n2^{n+2}(2-1)+2^{n+3}\\ &= 2^{n+2}+2^{n+2}(n+2),\end{aligned}$$

што значи да је тачно $\Phi(n+2)$.

9. За $n=1$ је $\cos\frac{\pi}{2^1}=\frac{\sqrt{2}}{2}$, што јесте ирационалан број. Претпоставимо да је $\cos\frac{\pi}{2^n}$ ирационалан. Треба доказати да исто важи и за $\cos\frac{\pi}{2^{n+1}}$. Претпоставимо супротно: број $\cos\frac{\pi}{2^{n+1}}$ је рационалан. Тада је и број $\left(\cos\frac{\pi}{2^{n+1}}\right)^2$ такође рационалан. Како важи $\left(\cos\frac{\pi}{2^{n+1}}\right)^2=\left(\cos\left(\frac{1}{2}\cdot\frac{\pi}{2^n}\right)\right)^2=\frac{1+\cos\frac{\pi}{2^n}}{2}$, онда је и број $\frac{1+\cos\frac{\pi}{2^n}}{2}$ рационалан. То значи да је број $\cos\frac{\pi}{2^n}$ рационалан, што је немогуће, према индуктивној претпоставци. Дакле, мора бити да је $\cos\frac{\pi}{2^{n+1}}$ ирационалан.

10. За $n=0$ је $0\cdot f_0=0=0\cdot f_2-f_3+2$. Претпоставимо да је $f_1+2f_2+3f_3+\cdots+nf_n=nf_{n+2}-f_{n+3}+2$. Докажимо да је $f_1+2f_2+3f_3+\cdots+nf_n+(n+1)f_{n+1}=$

$(n+1)f_{n+3} - f_{n+4} + 2$.

$$\begin{aligned} f_1 + 2f_2 + 3f_3 + \cdots + nf_n + (n+1)f_{n+1} &= nf_{n+2} - f_{n+3} + 2 + (n+1)f_{n+1} \\ &= (n+1)f_{n+2} - f_{n+2} + (n+1)f_{n+1} - f_{n+3} + 2 \\ &= (n+1)(f_{n+2} + f_{n+1}) - (f_{n+2} + f_{n+3}) + 2 \\ &= (n+1)f_{n+3} - f_{n+4} + 2. \end{aligned}$$

11. Користићемо индукцију са две хипотезе. За $n = 6$ је $\left(\frac{3}{2}\right)^5 = \frac{729}{32} \le 8 = f_6$, а за $n = 7$ је $\left(\frac{3}{2}\right)^6 = \frac{6561}{64} \le 13 = f_7$, па имамо базу индукције. Претпоставимо да је $f_n \ge \left(\frac{3}{2}\right)^{n-1}$ и $f_{n-1} \ge \left(\frac{3}{2}\right)^{n-2}$. Докажимо да је $f_{n+1} \ge \left(\frac{3}{2}\right)^{n}$. Важи

$$\begin{aligned} f_{n+1} = f_n + f_{n-1} &\ge \left(\frac{3}{2}\right)^{n-1} + \left(\frac{3}{2}\right)^{n-2} = \left(\frac{3}{2}\right)^{n-2}\left(\frac{3}{2} - 1\right) \\ &= \left(\frac{3}{2}\right)^{n-2} \cdot \frac{5}{2} = \left(\frac{3}{2}\right)^{n-2} \cdot \frac{10}{4} \\ &> \left(\frac{3}{2}\right)^{n-2} \cdot \frac{9}{4} = \left(\frac{3}{2}\right)^{n-2} \cdot \left(\frac{3}{2}\right)^{2} = \left(\frac{3}{2}\right)^{n}. \end{aligned}$$

12. Важи да је

$$\begin{aligned} 18876 &= 5775 \cdot 3 + 1551, & 0 &\le 1551 < 5775 \\ 5775 &= 1551 \cdot 3 + 1122, & 0 &\le 1122 < 1551 \\ 1551 &= 1122 \cdot 1 + 429, & 0 &\le 429 < 1122 \\ 1122 &= 429 \cdot 2 + 264, & 0 &\le 264 < 429 \\ 429 &= 264 \cdot 1 + 165, & 0 &\le 165 < 264 \\ 264 &= 165 \cdot 1 + 99, & 0 &\le 99 < 165 \\ 165 &= 99 \cdot 1 + 66, & 0 &\le 66 < 99 \\ 99 &= 66 \cdot 1 + 33, & 0 &\le 33 < 66 \\ 66 &= 33 \cdot 2, \end{aligned}$$

па је нзд$(18876, 5775) = 33$. Такође из

$$\begin{aligned} 33 &= 99 - 66 = 99 - (165 - 99) = -165 + 2(264 - 165) \\ &= 2 \cdot 264 - 3(429 - 264) = -3 \cdot 429 + 5(1122 - 2 \cdot 429) \\ &= 5 \cdot 1122 - 13(1551 - 1122) = -13 \cdot 1551 + 18(5775 - 3 \cdot 1551) \\ &= 18 \cdot 5775 - 67(18876 - 3 \cdot 5775) \\ &= -67 \cdot 18876 + 219 \cdot 5775, \end{aligned}$$

следи да је нзд$(18876, 5775) = -67 \cdot 18876 + 219 \cdot 5775$.

13. Одредимо прво нзд$(6006, 1955)$.

$$\begin{bmatrix} 6006 & 1 & 0 \\ 1955 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 141 & 1 & -3 \\ 1955 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 141 & 1 & -3 \\ 122 & -13 & 40 \end{bmatrix} \sim$$

$$\begin{bmatrix} 19 & 14 & -43 \\ 122 & -13 & 40 \end{bmatrix} \sim \begin{bmatrix} 19 & 14 & -43 \\ 8 & -97 & 298 \end{bmatrix} \sim \begin{bmatrix} 3 & 208 & -639 \\ 8 & -97 & 298 \end{bmatrix} \sim$$

$$\begin{bmatrix} 3 & 208 & -639 \\ 2 & -513 & 1576 \end{bmatrix} \sim \begin{bmatrix} 1 & 721 & -2215 \\ 2 & -513 & 1576 \end{bmatrix} \sim \begin{bmatrix} 1 & 721 & -2215 \\ 0 & * & * \end{bmatrix}.$$

Дакле, $1 =$ нзд$(6006, 1955) = 721 \cdot 6006 - 2215 \cdot 1955$. Како је $1 \mid 30$, према теореми 6.39 дата једначина има целобројна решења и опште решење је дато са

$$\begin{aligned} x &= 721\frac{30}{1} + \frac{1955}{1} \cdot t = 21630 + 1955t \\ y &= -2215\frac{30}{1} - \frac{6006}{1} \cdot t = -66450 - 6006t, \qquad t \in \mathbb{Z}. \end{aligned}$$

Можемо увести смену $t' = t + 11$, и тада је опште решење дато са

$$\begin{aligned} x &= 125 + 1955t \\ y &= -384 - 6006t, \qquad t' \in \mathbb{Z}. \end{aligned}$$

14. Приметимо да је $17 \equiv_7 3$, па је тражени остатак једнак остатку броја 3^{2012} при дељењу са 7. Даље је

$$\begin{aligned} 3^1 &\equiv 3 \pmod 7 & 3^4 &\equiv 6 \cdot 3 \equiv 4 \pmod 7 \\ 3^2 &\equiv 3 \cdot 3 \equiv 2 \pmod 7 & 3^5 &\equiv 4 \cdot 3 \equiv 5 \pmod 7 \\ 3^3 &\equiv 2 \cdot 3 \equiv 6 \pmod 7 & 3^6 &\equiv 5 \cdot 3 \equiv 1 \pmod 7. \end{aligned}$$

Следи да је

$$17^{2012} \equiv 3^{2012} \equiv 3^{335 \cdot 7 + 2} \equiv (3^7)^{335} \cdot 3^2 \equiv 1^{335} \cdot 9 \equiv 1 \cdot 2 \equiv 2 \pmod 7,$$

па је тражени остатак 2.

15. Како је $\text{нзд}(15, 33) = 3$ и $3 \mid 18$ једначина има решење. Решење једначине $5x \equiv_{11} 3$ је $x \equiv_{11} 10$, па су решења полазне једначине $x \equiv_{33} 10$, $x \equiv_{33} 21$ и $x \equiv_{33} 32$.

16. На основу напомене 6.58 закључујемо да систем има решење. Из прве једначине следи да је $x = 7y + 1$, за $y \in \mathbb{Z}$. Заменом у другу једначину добијамо $7y + 1 \equiv_9 4$. Једно решење ове једначине је 3, па је опште решење $y = 3 + 9z$, за $z \in \mathbb{Z}$. Тада је $x = 7y + 1 = 7(3 + 9z) + 1 = 22 + 63z$. Заменом ове једнакости у трећу једначину добијамо $22 + 63z \equiv_5 3$. Како је $22 \equiv_5 2$ и $63 \equiv_5 3$, једначина је еквивалентна са $2 + 3z \equiv_5 3$, то јест $3z \equiv_5 1$. Опште решење ове једначине је $2 + 5t$, за $t \in \mathbb{Z}$. Добили смо да је $x = 22 + 63z = 22 + 63(2 + 5t) = 148 + 315t$, што је решење полазног система.

17. Последње две цифре датог броја знамо ако нађемо његов остатак при дељењу са 100. Како је $2011 \equiv_{100} 11$, то је $2011^{4043} \equiv_{100} 11^{4043}$. Бројеви 11 и 100 су узајамно прости и $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = 2(2-1) \cdot 5(5-1) = 40$, па је према теореми 6.65 $11^{40} \equiv_{100} 1$. Даље треба одредити остатак при дељењу броја 4043 са 40. То је 3, па је $4043 = 40k + 3$, за $k \in \mathbb{Z}$. Коначно је

$$2011^{4043} \equiv 11^{4043} \equiv 11^{40k+3} \equiv (11^{40})^k \cdot 11^3 \equiv 1 \cdot 121 \cdot 11 \equiv 21 \cdot 11 \equiv 31 \pmod{100},$$

па су две последње цифре датог броја 3 и 1.

18. Треба доказати да је остатак при дељењу датог броја са 10 једнак нули. Одредимо прво остатак при дељењу 3333^{7777} са 10. Како је $3333 \equiv_{10} 3$, важи $3333^{7777} \equiv_{10} 3^{7777}$. Из $\text{нзд}(3, 10) = 1$ и $\varphi(10) = 4$ следи да је $3^4 \equiv_{10} 1$. Такође је $7777 \equiv_4 1$, па је $7777 = 4k + 1$, за неко $k \in \mathbb{Z}$. Даље је

$$3333^{7777} \equiv 3^{7777} \equiv 3^{4k+1} \equiv (3^4)^k \cdot 3^1 \equiv 3 \pmod{10}.$$

Сличан је поступак и за други сабирак: $7777^{3333} \equiv_{10} 7^{3333}$. Из $\text{нзд}(7, 10)$ следи да $7^4 \equiv_{10} 1$. Како је и $3333 \equiv_4 1$, важи

$$7777^{3333} \equiv 7^{3333} \equiv 7^{4l+1} \equiv (7^4)^l \cdot 7^1 \equiv 7 \pmod{10}.$$

Сада можемо закључити да је

$$3333^{7777} + 7777^{3333} \equiv 3 + 7 \equiv 0 \pmod{10}.$$

19. Како је нзд$(5,17) = 1$ и $\varphi(17) = 16$, важи $5^{16} \equiv_{17} 1$. Треба одредити остатак при дељењу 5^{5^5} са 16. Важи да је нзд$(5,16)$ и $\varphi(16) = \varphi(2^4) = 2^3(2-1) = 8$, па је $5^8 \equiv_{16} 1$. Даље је потребно одредити остатак при дељењу 5^5 са 8. Бројеви 5 и 8 су узајамно прости и $\varphi(8) = \varphi(2^3) = 4$, па је $5^4 \equiv_8 1$. Из последњег израза закључујемо да је

$$5^5 \equiv 5^4 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \pmod 8.$$

Даље је

$$5^{5^5} \equiv 5^{8k+5} \equiv (5^8)^k \cdot 5^5 \equiv 1 \cdot 5^5 \equiv 25 \cdot 25 \cdot 5 \equiv 9 \cdot 9 \cdot 5 \equiv 81 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \pmod{16}.$$

Вратимо се на почетак:

$$5^{5^{5^5}} \equiv 5^{16l+5} \equiv (5^16)^l \cdot 5^5 \equiv 1 \cdot 5^5 \equiv 25 \cdot 25 \cdot 5 \equiv 8 \cdot 8 \cdot 5 \equiv 64 \cdot 5 \equiv 13 \cdot 5 \equiv 65 \equiv 14 \pmod{17}.$$

Дакле, остатак је број 14.

20. Важи да је $1943^{1942} \equiv_5 3^{1942}$. Бројеви 3 и 5 су узајамно прости и $\varphi(5) = 4$, па је $3^4 \equiv_5 1$. При том је $1942 \equiv_4 2$, па је $1942 = 4k + 2$, за неко $k \in \mathbb{Z}$. Тада је

$$1943^{1942} \equiv 3^{1942} \equiv 3^{4k+2} \equiv (3^4)^k \cdot 3^2 \equiv 9 \equiv 4 \pmod 5.$$

Слично је $1943^{1942} \equiv_7 4^{1942}$ и $4^6 \equiv_7 1$. Из $1942 \equiv_6 4$ следи

$$1943^{1942} \equiv 4^{1942} \equiv 4^{6l+4} \equiv (4^6)^l \cdot 4^4 \equiv 16^2 \equiv 2^2 \equiv 4 \pmod 7.$$

Треба још одредити остатак при дељењу са 35. Овде можемо искористити Кинеску теорему 6.57. Уочимо систем конгруенција

$$x \equiv_5 4 \qquad x \equiv_7 4.$$

Бројеви 5 и 7 су узајамно прости, па решење система постоји. Одредимо опште решење система. Из прве једначине следи да је $x = 5y + 4$, за неко $y \in \mathbb{Z}$. Тада је $5y + 4 \equiv_7 4$, то јест $5y \equiv_7 0$, па је $y = 7t$, за $t \in \mathbb{Z}$. Заменом у прву једнакост добијамо $x = 5y + 4 = 5(7t) + 4 = 4 + 35t$. Приметимо да смо и одмах могли да уочимо да је 4 решење, па како је нзс$(5,7) = 35$ према теореми је опште решење облика $4 + 35t$. Даље, сетимо се да је број 1943^{1942} такође једно решење система. То значи да је 1943^{1942} једнак 4 по модулу 35, то јест $1943^{1942} \equiv_{35} 4$.

Глава 7

Глава 8

1. Означимо формулу $((p \Rightarrow \neg q) \Rightarrow (r \wedge \neg p)) \Rightarrow (p \Rightarrow q)$ са F.

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

2. Претпоставимо да дата формула није таутологија. Тада постоји валуација v тако да $v\big(((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow (q \wedge r))\big) = 0$. Следи да је $v\big(((p \Rightarrow q) \wedge (p \Rightarrow r))\big) = 1$, а $v\big((p \Rightarrow (q \wedge r))\big) = 0$. Због друге једнакости важи да $v(p) = 1$ и $v(q \wedge r) = 0$. Вратимо се на прву једнакост: конјункција је тачна ако су тачне обе формуле које у њој фигуришу. Тако да је $v(p \Rightarrow q) = 1$ и $v(p \Rightarrow r) = 1$. Како је исказ p тачан у валуацији v, следи да мора бити $v(q) = 1$ и $v(r) = 1$. Тада је и $v(q \wedge r) = 1$. Добијамо контрадикцију, јер смо већ закључили да је $v(q \wedge r) = 0$. Дакле, полазна формула јесте таутологија.

3. Спроведимо дискусију по исказном слову q. Нека је v било која валуација наведених исказних слова. Ако је $v(q) = 1$, онда је $v(p \Rightarrow q) = 1$ и $v(q \wedge r) = v(r)$. Добијамо да је
$$\begin{aligned}
v\big((p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))\big) &= v(p \Rightarrow q) \Rightarrow (v(p \wedge r) \Rightarrow v(q \wedge r)) \\
&= 1 \Rightarrow (v(p \wedge r)) \Rightarrow v(r)) \\
&= 1 \Rightarrow v((p \wedge r) \Rightarrow r) \\
&\ \text{(користићемо пример 8.19} \\
&\ \ \text{(слабљење конјункције))} \\
&= 1 \Rightarrow 1 = 1.
\end{aligned}$$
Ако је $v(q) = 0$, онда је $v(p \Rightarrow q) = \neg v(p)$ и $v(q \wedge r) = 0$. Следи да
$$\begin{aligned}
v\big((p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))\big) &= \neg v(p) \Rightarrow v((p \wedge r) \Rightarrow 0) \\
&\ \text{(користићемо пример 8.18 (8))} \\
&= \neg v(p) \Rightarrow \neg v(p \wedge r) \\
&\ \text{(користићемо Де Морганов закон:} \\
&\ v(\neg(p \wedge r)) = v(\neg p \vee \neg r)) \\
&= v(\neg p \Rightarrow \neg p \vee \neg r) \\
&\ \text{(користићемо пример 8.19} \\
&\ \ \text{(увођење дисјункције))} \\
&= 1.
\end{aligned}$$
Формула је тачна у оба случаја, па је таутологија.

4. Претпоставимо супротно: $B \Rightarrow C$ није таутологија. Тада постоји валуација v тако да $v(B \Rightarrow C) = 0$, што значи да је $v(B) = 1$ и $v(C) = 0$. Како је $A \veebar B$ таутологија, тачна је у свим валуацијама, па је и $v(A \vee B) = 1$. Формула $A \veebar B$ је тачна када су истинитосне вредности наведених формула различите, па како је $v(B) = 1$ мора бити $v(A) = 0$. С обзиром на тај закључак, као и да је $A \Leftrightarrow D$ таутологија, из $v(A \Leftrightarrow D) = 1$ следи да је $v(D) = 0$. Дато је и да је $C \Leftrightarrow D$ контрадикција. То значи да је та формула нетачна у свакој валуацији, па је тиме и $v(C \Leftrightarrow D) = 0$. Из $v(D) = 0$ следи да је $v(C) = 1$. Добијамо контрадикцију, јер је почетни закључак био да $v(C) = 0$. Дакле, $B \Rightarrow C$ мора бити таутологија.

5. Важи да
$$\begin{aligned}
A \cap (B \bigtriangleup C) = (A \cap B) \bigtriangleup (A \cap C) \quad &\text{акко} \quad (\forall x) x \in A \cap (B \bigtriangleup C) \Leftrightarrow x \in (A \cap B) \bigtriangleup (A \cap C) \\
&\text{акко} \quad (\forall x) x \in A \wedge x \in B \bigtriangleup C \Leftrightarrow x \in A \cap B \veebar x \in A \cap C \\
&\text{акко} \quad (\forall x) x \in A \wedge (x \in B \veebar x \in C) \Leftrightarrow \\
&\phantom{\text{акко}} \quad (x \in A \wedge x \in B) \veebar (x \in A \wedge x \in C).
\end{aligned}$$
Означимо исказе $x \in A$, $x \in B$ и $x \in C$ редом са p, q и r. Треба доказати

да је формула $p \wedge (q \veebar r) \Leftrightarrow (p \wedge q) \veebar (p \wedge r)$ таутологија.

p	$\wedge$	$(q$	$\veebar$	$r)$	$\Leftrightarrow$	$(p$	$\wedge$	$q)$	$\veebar$	$(p$	$\wedge$	$r)$
0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	1	1	1	0	0	0	0	0	0	1
0	0	1	1	0	1	0	0	1	0	0	0	0
0	0	1	0	1	1	0	0	1	0	0	0	1
1	0	0	0	0	1	1	0	0	0	1	0	0
1	1	0	1	1	1	1	0	0	1	1	1	1
1	1	1	1	0	1	1	1	1	1	1	0	0
1	0	1	0	1	1	1	1	1	0	1	1	1

Следи да је тачна полазна скуповна једнакост.

6. Нека је валуација v таква да $v(p) = v(A_0) = 0$. Докажимо математичком индукцијом да је $v(A_n) = 0$. База индукције је задовољена. Претпоставимо да је $v(A_n) = 0$. Тада је

$$\begin{aligned} v(A_{n+1}) &= v((A_n \Rightarrow B_n) \Rightarrow A_n) = (v(A_n) \Rightarrow v(B_n)) \Rightarrow v(A_n) \\ &= (0 \Rightarrow v(B_n)) \Rightarrow 0 = 1 \Rightarrow 0 = 0. \end{aligned}$$

Дакле, за сваку формулу A_n постоји валуација $v(A_n) = 0$, па онда да ниједна од тих формула није таутологија.

Докажимо сада и следеће: ако је $v(p) = v(A_0) = 1$, онда је и $v(A_n) = 1$ за свако n. Претпоставимо да је формуле $v(A_n) = 1$, за неко $n > 0$. Тада је

$$\begin{aligned} v(A_{n+1}) &= v((A_n \Rightarrow B_n) \Rightarrow A_n) = (v(A_n) \Rightarrow v(B_n)) \Rightarrow v(A_n) \\ &= = (1 \Rightarrow v(B_n)) \Rightarrow 1 = v(B_n) \Rightarrow 1 = 1. \end{aligned}$$

Пређимо на доказ да формуле B_n нису таутологије. Нека је валуација v таква да $v(A_0) = 1$ и $v(B_0) = 0$. Тада је, према претходном, $v(A_n) = 1$ за свако n. Докажимо индукцијом да је $v(B_n) = 0$ за свако $n \geq 0$. За $n = 0$ је $v(B_0) = 0$. Претпоставимо да је $v(B_n) = 0$. Важи

$$v(B_{n+1}) = v(A_n \Rightarrow B_n) = v(A_n) \Rightarrow v(B_n) = 1 \Rightarrow 0 = 0,$$

па је и $v(B_{n+1}) = 0$. Тако да ни формуле B_n нису таутологије.

7.

$1.\bot\big((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)\big)$

$2.\top((p \Rightarrow q) \wedge (q \Rightarrow r))$ (1)

$3.\bot(p \Rightarrow r)$ (1)

$4.\top(p)$ (3)

$5.\bot(r)$ (3)

$6.\top(p \Rightarrow q)$ (2)

$7.\top(q \Rightarrow r)$ (2)

$8.\bot(p)$ (6) $\quad$ $9.\top(q)$ (6)

$X(4,8)$

$10.\bot(q)$ (7) $\quad$ $11.\top(r)$ (7)

$X(9,10)$ $\quad$ $X(5,11)$

8.

$1.\bot\big((p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))\big)$

$2.\top(p \Rightarrow (q \Rightarrow r))$ (1)

$3.\bot((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ (1)

$4.\top(p \Rightarrow q)$ (3)

$5.\bot(p \Rightarrow r)$ (3)

$6.\top(p)$ (5)

$7.\bot(r)$ (5)

$8.\bot(p)$ (4) $X(6,8)$ | $9.\top(q)$ (4)

$10.\bot(p)$ (2) $X(6,10)$ | $11.\top(q \Rightarrow r)$ (2)

$12.\bot(q)$ (11) $X(9,12)$ | $13.\top(r)$ (11) $X(7,13)$

9.

$1.\bot\big((((p \Rightarrow r) \wedge (q \Rightarrow r)) \wedge (p \vee q)) \Rightarrow r\big)$

$2.\top\big(((p \Rightarrow r) \wedge (q \Rightarrow r)) \wedge (p \vee q)\big)$ (1)

$3.\bot(r)$ (1)

$4.\top((p \Rightarrow r) \wedge (q \Rightarrow r))$ (2)

$5.\top(p \vee q)$ (2)

$6.\top(p \Rightarrow r)$ (4)

$7.\top(q \Rightarrow r)$ (4)

$8.\top(p)$ (5) | $9.\top(q)$ (5)

$10.\bot(p)$ (6) $X(8,10)$ | $11.\top(r)$ (6) $X(3,11)$ | $12.\bot(q)$ (7) $X(,9,12)$ | $13.\top(r)$ (7) $X(3,13)$

10. Направимо истинитосну таблицу за формулу $(A \vee p) \Rightarrow (A \vee \neg q)$.

	p	q	$A \vee p$	$\neg q$	$A \vee \neg q$	$(A \vee p) \Rightarrow (A \vee \neg q)$
v_1	0	0	$v_1(A)$	1	1	1
v_2	0	1	$v_2(A)$	0	$v_2(A)$	1
v_3	1	0	1	1	1	1
v_4	1	1	1	0	$v_4(A)$	$v_4(A)$

Видимо да било која формула која је тачна у v_4 задовољава тражени услов. Тада су све могуће таблице за фомулу A

	A	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
v_1	$*$	0	0	0	1	0	1	1	1
v_2	$*$	0	0	1	0	1	0	1	1
v_3	$*$	0	1	0	0	1	1	0	1
v_4	1	1	1	1	1	1	1	1	1

Ставимо

$$\begin{array}{cccc} A_1 = p \wedge q & A_2 = p & A_3 = q & A_4 = p \Leftrightarrow q \\ A_5 = p \vee q & A_6 = q \Rightarrow p & A_7 = p \Rightarrow q & A_8 = 1. \end{array}$$

Наведене формуле су све међусобно нееквивалентне формуле које задовољавају тражени услов.

Глава 9

1. Према дефиницији је $A \wedge B = \neg(A \Rightarrow \neg B)$, а према теореми дедукције довољно је доказати да $\vdash \neg(A \Rightarrow \neg B) \Rightarrow A$. Важи:

1.$\neg A \Rightarrow (A \Rightarrow \neg B)$	теорема из примера 9.7
2.$(\neg A \Rightarrow (A \Rightarrow \neg B)) \Rightarrow (\neg(A \Rightarrow \neg B) \Rightarrow \neg\neg A)$	теорема из примера 9.13
3.$\neg(A \Rightarrow \neg B) \Rightarrow \neg\neg A$	МП(1,2)
4.$\neg\neg A \Rightarrow A$	теорема
5.$\neg(A \Rightarrow \neg B) \Rightarrow A$	применом 9.12 на 3 и 4.

2. Треба доказати да је $\neg(A \Rightarrow \neg B) \vdash \neg(B \Rightarrow \neg A)$, то јест да је $\neg(A \Rightarrow \neg B) \Rightarrow \neg(B \Rightarrow \neg A)$. Докажимо прво да је $B \Rightarrow \neg A \vdash A \Rightarrow \neg B$.

1.$B \Rightarrow \neg A$	хипотеза
2.$(B \Rightarrow \neg A) \Rightarrow (\neg\neg A \Rightarrow \neg B)$	теорема из примера 9.13
3.$\neg\neg A \Rightarrow \neg B$	МП(1,2)
4.$A \Rightarrow \neg\neg A$	теорема
5.$A \Rightarrow \neg B$	применом 9.12 на 3 и 4.

Сада је

1.$(B \Rightarrow \neg A) \Rightarrow (A \Rightarrow \neg B)$	теорема
2.$((B \Rightarrow \neg A) \Rightarrow (A \Rightarrow \neg B)) \Rightarrow (\neg(A \Rightarrow \neg B) \Rightarrow \neg(B \Rightarrow \neg A))$	теорема из примера 9.13
3.$\neg(A \Rightarrow \neg B) \Rightarrow \neg(B \Rightarrow \neg A)$	МП(1,2).

3. Како је $A \vee B = \neg A \Rightarrow B$, према теореми 9.6 треба доказати да је $A \Rightarrow (\neg A \Rightarrow B)$, што је закључак примера 9.7. С друге стране је

1.B	хипотеза
2.$B \Rightarrow (\neg B \Rightarrow \neg\neg A)$	теорема
3.$\neg B \Rightarrow \neg\neg A$	МП(1,2)
4.$(\neg B \Rightarrow \neg\neg A) \Rightarrow (\neg A \Rightarrow B)$	Л3
5.$\neg A \Rightarrow B$	МП(3,4),

па је $B \vdash A \vee B$.

4. Треба доказати да је $\neg A \Rightarrow B \vdash \neg B \Rightarrow A$, то јест да $\neg A \Rightarrow B, \neg B \vdash A$. Важи:

1.$\neg A \Rightarrow B$	хипотеза
2.$\neg B$	хипотеза
3.$(\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg\neg A)$	теорема
4.$\neg B \Rightarrow \neg\neg A$	МП(1,3)
5.$\neg\neg A \Rightarrow A$	теорема
6.$\neg B \Rightarrow A$	применом 9.12 на 4 и 5
7.A	МП(2,6).

5.

1.$A \Rightarrow B$	хипотеза
2.$\neg A \Rightarrow B$	хипотеза
3.$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$	теорема
4.$\neg B \Rightarrow \neg A$	МП(1,3)
5.$\neg B \Rightarrow B$	применом 9.12 на 4 и 2
6.$\neg B \Rightarrow (B \Rightarrow \neg(B \Rightarrow B))$	теорема
7.$(\neg B \Rightarrow (B \Rightarrow \neg(B \Rightarrow B))) \Rightarrow ((\neg B \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(B \Rightarrow B)))$	Л2
8.$(\neg B \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(B \Rightarrow B))$	МП(6,7)
9.$\neg B \Rightarrow \neg(B \Rightarrow B)$	МП(5,8)
10.$(\neg B \Rightarrow \neg(B \Rightarrow B)) \Rightarrow ((B \Rightarrow B) \Rightarrow B)$	Л3
11.$(B \Rightarrow B) \Rightarrow B$	МП(9,10)
12.$B \Rightarrow B$	теорема
13.B	МП(11,12)

6. Треба доказати $\neg(\neg A \Rightarrow \neg B) \vdash \neg(\neg A \Rightarrow \neg\neg B)$. Можемо прво доказати да $(\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg A \Rightarrow \neg B)$, то јест $\neg A \Rightarrow \neg\neg B \vdash \neg A \Rightarrow \neg B$:

1.$\neg A \Rightarrow \neg\neg B$	хипотеза
2.$\neg\neg B \Rightarrow B$	теорема
3.$\neg A \Rightarrow B$	транзитивност(1,2).

Даље је

1.$(\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg A \Rightarrow \neg B)$	теорема
2.$((\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg A \Rightarrow \neg B)) \Rightarrow (\neg(\neg A \Rightarrow \neg B) \Rightarrow \neg(\neg A \Rightarrow \neg\neg B))$	Л3
3.$\neg(\neg A \Rightarrow \neg B) \Rightarrow \neg(\neg A \Rightarrow \neg\neg B)$	МП(1,2).

7. Доказаћемо да је $\neg B \Rightarrow B \vdash B$:

1.$\neg B \Rightarrow B$	хипотеза
2.$\neg B \Rightarrow (B \Rightarrow \neg(B \Rightarrow B))$	теорема
3.$(\neg B \Rightarrow (B \Rightarrow \neg(B \Rightarrow B))) \Rightarrow ((\neg B \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(B \Rightarrow B))$	Л2
4.$(\neg B \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(B \Rightarrow B)$	МП(2,3)
5.$\neg B \Rightarrow \neg(B \Rightarrow B)$	МП(1,4)
6.$(\neg B \Rightarrow \neg(B \Rightarrow B)) \Rightarrow ((B \Rightarrow B) \Rightarrow B)$	Л3
7.$(B \Rightarrow B) \Rightarrow B$	МП(5,6)
8.$B \Rightarrow B$	теорема
9.B	МП(7,8).

8. Према 9.6 треба доказати да $(A \Rightarrow B) \Rightarrow A \vdash A$.

1.$(A \Rightarrow B) \Rightarrow A$	хипотеза
2.$\neg A \Rightarrow (A \Rightarrow B)$	теорема
3.$\neg A \Rightarrow A$	транзитивност(1,2)
4.$\neg A \Rightarrow (A \Rightarrow \neg(A \Rightarrow A))A$	теорема
5.$(\neg A \Rightarrow (A \Rightarrow \neg(A \Rightarrow A))) \Rightarrow ((\neg A \Rightarrow A) \Rightarrow (\neg A \Rightarrow \neg(A \Rightarrow A)))$	Л2
6.$(\neg A \Rightarrow A) \Rightarrow (\neg A \Rightarrow \neg(A \Rightarrow A))$	МП(4,5)
7.$\neg A \Rightarrow \neg(A \Rightarrow A)$	МП(3,6)
8.$(\neg A \Rightarrow \neg(A \Rightarrow A)) \Rightarrow ((A \Rightarrow A) \Rightarrow A)$	Л3
9.$(A \Rightarrow A) \Rightarrow A$	МП(7,8)
10.$A \Rightarrow A$	теорема
11.A	МП(9,10).

9. Ако је $A, B \vdash \neg(C \Rightarrow C)$ следи да $A \Rightarrow (B \Rightarrow \neg(C \Rightarrow C))$. Тако да је

1.A	хипотеза
2.$A \Rightarrow (B \Rightarrow \neg(C \Rightarrow C))$	претпоставка
3.$B \Rightarrow \neg(C \Rightarrow C)$	МП(1,2)
4.$(B \Rightarrow \neg(C \Rightarrow C)) \Rightarrow (\neg\neg(B \Rightarrow B) \Rightarrow \neg A)$	Л3
5.$\neg\neg(B \Rightarrow B) \Rightarrow \neg A$	МП(3,4)
6.$(B \Rightarrow B) \Rightarrow \neg\neg(B \Rightarrow B)$	теорема
7.$(B \Rightarrow B) \Rightarrow \neg A$	транзитивност(5,6)
8.$B \Rightarrow B$	теорема
9.$\neg A$	МП(7,8).

Глава 10

1. (а)

$$\begin{aligned}
v(f(g(g(x,y),f(a)))) &= f^{\mathbb{Z}}(g^{\mathbb{Z}}(g^{\mathbb{Z}}(v(x),v(y)),f^{\mathbb{Z}}(v(a))) \\
&= f^{\mathbb{Z}}(g^{\mathbb{Z}}(g^{\mathbb{Z}}(2,3),f^{\mathbb{Z}}(1)) = f^{\mathbb{Z}}(g^{\mathbb{Z}}(2\cdot 3,-1)) \\
&= f^{\mathbb{Z}}(6\cdot(-1)) = -(-6) = 6 \\
v(g(f(y),z)) &= g^{\mathbb{Z}}(f^{\mathbb{Z}}(v(y)),v(z)) = g^{\mathbb{Z}}(f^{\mathbb{Z}}(3),4) \\
&= g^{\mathbb{Z}}(-3,4) = -3\cdot 4 = -12
\end{aligned}$$

(б)

$$\begin{aligned}
v(q(f(g(x,y))) \Leftrightarrow q(y)) &= v(q(f(g(x,y)))) \Leftrightarrow v(q(y)) \\
&= q^{\mathbb{Z}}(f^{\mathbb{Z}}(g^{\mathbb{Z}}(v(x),v(y)))) \Leftrightarrow q^{\mathbb{Z}}(v(y)) \\
&= q^{\mathbb{Z}}(f^{\mathbb{Z}}(g^{\mathbb{Z}}(-2,-3))) \Leftrightarrow q^{\mathbb{Z}}(-3) \\
&= q^{\mathbb{Z}}(-6) \Leftrightarrow 0 = 0 \Leftrightarrow 0 \\
v(\neg p(f(x),z) \vee q(f(a))) &= v(\neg p(f(x),z)) \vee v(q(f(a)) \\
&= \neg v(p(f(x),z)) \vee q^{\mathbb{Z}}(f^{\mathbb{Z}}(v(a))) \\
&= p^{\mathbb{Z}}(f^{\mathbb{Z}}(v(x)),v(z)) \vee q^{\mathbb{Z}}(f^{\mathbb{Z}}(1)) \\
&= p^{\mathbb{Z}}(f^{\mathbb{Z}}(-2),4) \vee q^{\mathbb{Z}}(-1) \\
&= p^{\mathbb{Z}}(2,4) \vee 0 = 1 \vee 0 = 1
\end{aligned}$$

(ц) Формула $\forall x \exists y p(x,y)$ значи да за сваки цео број x постоји цео број y тако да је $x \leq y$, што је тачно. С друге стране није за свако $x \in \mathbb{Z}$ тачно да је $x \cdot (-x) = -x^2$ позитиван број, па формула $\forall x q(g(x, f(x)))$ није тачна. Тако да је истинитосна вредност реченице $\forall x \exists y p(x,y) \Rightarrow \forall x q(g(x, f(x)))$ једнака $1 \Rightarrow 0 = 0$, то јест наведена структура је контрамодел за дату реченицу. Формула $\forall x(q(x) \vee q(a))$ значи да за сваки цео број x важи да је x позитиван или да је број 1 позитиван. Како је 1 позитиван, формула је тачна у овој L-структури.

(д) Прва реченица се може написати у облику формуле $\forall x p(a,x)$. Сто се тице друге реченице, приметимо да је цео број x једнак 0 ако и само ако је $x = -x$. Тако да ту реченицу можемо записти са $\forall x(\neg x = f(x) \Rightarrow q(x) \vee q(f(x)))$.

2. Формула $\exists y q(f(y))$ значи да постоји цео број y тако да је $-y$ позитиван број. За $y = -1$, на пример, важи да је $-(-1)) = 1$ позитиван, па је ова формула тачна у свакој валуацији. Дакле, да бисмо одредили валуацију v_1 у којој је дата еквиваленција тачна, потребно је одредити валуацију у којој је формула $p(a, g(x,y))$ тачна, то јест треба одредити какве вредности треба да имају x и y па да је тачно $1 \leq v_1(x)v_1(y)$. То важи за, на пример $v_1 = \begin{pmatrix} x & y & \cdots \\ 2 & 1 & \cdots \end{pmatrix}$. С друге стране да би дата еквиваленција

била нетачна у некој валуацији v_2, треба да буде $v_2(p(a, g(x,y))) = 0$, $1 > v_2(x)v_2(y)$. Видимо да важи за $v_2 = \begin{pmatrix} x & y & \cdots \\ -2 & 1 & \cdots \end{pmatrix}$.

3. (а)

$$\begin{aligned} v(g(f(z,x),y)) &= g^{\mathcal{P}(\mathbb{N})}(f^{\mathcal{P}(\mathbb{N})}(v(z),v(x)),v(y))) \\ &= g^{\mathcal{P}(\mathbb{N})}(f^{\mathcal{P}(\mathbb{N})}(\{0,1,2,3,4,5\},\{1,3,5,\dots\}),\{2,4,6,\dots\})) \\ &= g^{\mathcal{P}(\mathbb{N})}(\{0,1,2,3,4,5\}\setminus\{1,3,5,\dots\},\{2,4,6,\dots\})) \\ &= g^{\mathcal{P}(\mathbb{N})}(\{0,2,4\},\{2,4,6,\dots\})) \\ &= \{0,2,4\}\cap\{2,4,6,\dots\} = \{2,4\} \end{aligned}$$

$$\begin{aligned} v(q(h(a)) \lor \neg p(f(x,z),g(x,y))) &= q^{\mathcal{P}(\mathbb{N})}(h^{\mathcal{P}(\mathbb{N})}(a^{\mathcal{P}(\mathbb{N})})) \lor \\ &\quad \neg p^{\mathcal{P}(\mathbb{N})}(f^{\mathcal{P}(\mathbb{N})}(v(x),v(z))), g^{\mathcal{P}(\mathbb{N})}(v(x),v(y)) \\ &= q^{\mathcal{P}(\mathbb{N})}(h^{\mathcal{P}(\mathbb{N})}(\emptyset)) \lor \\ &\quad \neg p^{\mathcal{P}(\mathbb{N})}(f^{\mathcal{P}(\mathbb{N})}(\{1,3,5,\dots\},\{0,1,2,3,4,5\})), \\ &\quad g^{\mathcal{P}(\mathbb{N})}(\{1,3,5,\dots\},\{2,4,6,\dots\}) \\ &= q^{\mathcal{P}(\mathbb{N})}(\emptyset^c) \lor \\ &\quad \neg p^{\mathcal{P}(\mathbb{N})}(\{1,3,5,\dots\}\setminus\{0,1,2,3,4,5\}, \\ &\quad \{1,3,5,\dots\}\cap\{2,4,6,\dots\}) \\ &= q^{\mathcal{P}(\mathbb{N})}(\mathbb{N}) \lor \neg p^{\mathcal{P}(\mathbb{N})}(\{7,9,11,\dots\},\emptyset) \\ &= 0 \lor \neg 0 = 0 \lor 1 = 1 \end{aligned}$$

Последње једнакост следи из чињенице да је скуп $\mathbb{N}$ бесконачан и да било који непразни скуп није подскуп празног скупа.

(б) Потребно је наћи валуацију у којој су тачне формуле $\forall x p(x,y)$ и $\exists y q(g(x,y))$. Ако ставимо $v_1(y) = \mathbb{N}$ онда је за сваку валуацију $w \sim_x v_1$ тачно да $w(x) \subseteq w(y) = \mathbb{N}$, јер је домен партитивни скуп скупа природних бројева. По другом делу формуле постоји скуп чији пресек са неким другим скупом је коначан. Овде је довољно узети да је x у валуацији v_1 било који коначан скуп. Нека је, на пример $v_1(x) = \{1,2\}$. Дакле, постоји валуација $u \sim_y v_1 (u = v_1)$ тако да је $u(x) \cap u(y) = \{1,2\} \cap \mathbb{N} = \{1,2\}$ коначан скуп. Овим је валуација v_1 у којој је дата формула тачна одређена са $v_1 = \begin{pmatrix} x & y & \cdots \\ \{1,2\} & \mathbb{N} & \cdots \end{pmatrix}$.

(ц) Како је $A^c \subseteq A^c \cup B^c = (A \cap B)^c$ за све скупове A и B, па и за произвољне подскупове скупа природних бројева, то је претпоставка $\forall x \forall y p(h(x), h(g(x,y)))$ дате формуле тачна у свакој валуацији. Треба наћи валуацијуу у којој је последица $p(h(y), h(f(x,y)))$ нетачна, да би цела импликација била нетачна. Дакле, треба наћи v_2 тако да је нетачна скупована једнакост $v_2(y)^c \subseteq (v_2(x) \setminus v_2(y))^c$. Ако је $v_2 = \begin{pmatrix} x & y & \cdots \\ \{0\} & \emptyset & \cdots \end{pmatrix}$, јасно је да не важи $\mathbb{N} = \emptyset^c \subseteq (\{0\} \setminus \emptyset)^c = \{0\}^c = \{1,2,3,\dots\}$.

4. Претпоставимо супротно: постоји структура $\mathbb{M}$ датог језика и валуација $v : Var \to M$ тако да је $v(\exists x \forall y p(x,y) \Rightarrow \forall y \exists x p(x,y)) = 0$. Тада је $v(\exists x \forall y p(x,y)) = 1$ и $v(\forall y \exists x p(x,y)) = 0$. Постоји валуација $v' \sim_x v$ тако да $v'(\forall y p(x,y)) = 1$ и постоји $w' \sim_y v$ тако да $w'(\exists x p(x,y)) = 0$. Даље, за сваку $v'' \sim_y v'$ важи $v''(p(x,y)) = 1$ и за сваку $w'' \sim_x w'$ важи $w''(p(x,y)) = 0$. Мора бити $v''(x) = v'(x)$ и $w''(y) = w'(y)$, али за $v''(y)$ и $w''(x)$ можемо узети било шта. Нека је $v''(y) = w'(y)$ и $w''(x) = v'(x)$. Тада је $v''(x) = v'(x) = w''(x)$ и $v''(y) = v'(y) = w''(y)$, па је $v'' = w''$. Одатле и из једнакости $v''(p(x,y)) = 1$ и $w''(p(x,y)) = 0$, добијамо контрадикцију.

5. Претпоставимо да постоји структура $\mathbb{M}$ датог језика и валуација $v : Var \to M$ тако да је $v(\forall x(p(x) \Rightarrow \forall y q(x,y)) \land \exists x p(x) \Rightarrow \exists x q(x,x)) = 0$. Следи да је $v(\forall x(p(x) \Rightarrow \forall y q(x,y)) \land \exists x p(x)) = 1$, то јест $v(\forall x(p(x) \Rightarrow \forall y q(x,y))) = 1$ и $v(\exists x p(x)) = 1$, као и да је $v(\exists x q(x,x)) = 0$. Једноставности ради, можемо писати да $v = \begin{pmatrix} x & y & \cdots \\ x_v & y_v & \cdots \end{pmatrix}$. Из $v(\exists x p(x)) = 1$ следи да постоји валуација $u \sim_x v$ тако да $u(p(x)) = 1$. Тада је $u = \begin{pmatrix} x & y & \cdots \\ x_u & y_v & \cdots \end{pmatrix}$. За сваку валуацију $v' \sim_x v$ је $v'(p(x) \Rightarrow \forall y q(x,y)) = 1$. Можемо узети $v' = \begin{pmatrix} x & y & \cdots \\ x_u & y_v & \cdots \end{pmatrix}$, то јест $v' = u$. Тада из $u(p(x)) \Rightarrow u(\forall y q(x,y))) = 1$ и $u(p(x)) = 1$ следи да је $u(\forall y q(x,y))) = 1$. Последња једнакост значи да за сваку $u' \sim_y u$ важи $u'(q(x,y)) = 1$, то јест $q^{\mathbb{M}}(u'(x), u'(y)) = 1$. Имали смо и да је $v(\exists x q(x,x)) = 0$, па за сваку $w \sim_x v$ важи $w(q(x,x)) = 0$, то јест $q^{\mathbb{M}}(w(x), w(x)) = 0$. Ставимо да $u' = \begin{pmatrix} x & y & \cdots \\ x_u & x_u & \cdots \end{pmatrix}$ и $w = \begin{pmatrix} x & y & \cdots \\ x_u & y_v & \cdots \end{pmatrix}$. Тада је $q^{\mathbb{M}}(x_u, x_u) = 1$ из $q^{\mathbb{M}}(u'(x), u'(y)) = 1$ и $q^{\mathbb{M}}(x_u, x_u) = 0$ из $q^{\mathbb{M}}(w(x), w(x)) = 0$. Ово је контрадикција.

6. Нека је $M = \{a, b\}$ и структура датог језика $\mathbb{M} = \{M, p^{\mathbb{M}}, f^{\mathbb{M}}\}$, где су релација $p^{\mathbb{M}}$ и функција $f^{\mathbb{M}}$ задате таблицама:

$p^{\mathbb{M}}$	a	b
a	1	1
b	0	0

$$f^{\mathbb{M}} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Претпоставимо да је дата формула тачна у свакој валуацији v, то јест $v(\forall x(p(x, f(x)) \Rightarrow p(f(x), x))) = 1$. Тада је за сваку валуацију $v' \sim_x v$ тачно $v'(p(x, f(x)) \Rightarrow p(f(x), x)) = 1$. Како $v'(x)$ може бити било шта, ставимо $v'(x) = a$. Следи да

$$\begin{aligned} v'(p(x, f(x)) \Rightarrow p(f(x), x)) &= p^{\mathbb{M}}(v'(x), f^{\mathbb{M}}(v'(x))) \Rightarrow p^{\mathbb{M}}(f^{\mathbb{M}}(v'(x)), v'(x)) \\ &= p^{\mathbb{M}}(a, f^{\mathbb{M}}(a)) \Rightarrow p^{\mathbb{M}}(f^{\mathbb{M}}(a), a) \\ &= p^{\mathbb{M}}(a, b) \Rightarrow p^{\mathbb{M}}(b, a) = 1 \Rightarrow 0 = 0, \end{aligned}$$

што је контрадикција. Дакле, постоји валуација у којој ова формула није тачна и са $\mathbb{M}$ је дат један контрамодел те формуле, који је коначног домена.

7. Нека је $M = \mathbb{N}$ и структура датог језика $\{\mathbb{N}, p^{\mathbb{N}}, f^{\mathbb{N}}\}$, где су релација $p^{\mathbb{N}}$ и функција $f^{\mathbb{N}}$ дате са:

$$p^{\mathbb{M}}(x) = 1 \text{ ако је } x > 3 \qquad f^{\mathbb{M}}(x) = x + 1.$$

Претпоставимо да постоји валуација v тако да $v(forallx(p(x) \Rightarrow p(f(x)))) = 0$. Тада постоји $v' \sim_x v$ тако да $v'(p(x) \Rightarrow p(f(x))) = 0$, то јест $p^{\mathbb{N}}(v'(x)) \Rightarrow p^{\mathbb{N}}(f^{\mathbb{N}}(v'(x))) = 0$. Даље, следи да је $p^{\mathbb{N}}(v'(x)) = 1$ и $p^{\mathbb{N}}(f^{\mathbb{N}}(v'(x))) = 0$. Нека је $v'(x) = m$. Из $p^{\mathbb{N}}(m) = 1$ следи да је $m > 3$. Из $p^{\mathbb{N}}(f^{\mathbb{N}}(m)) = p^{\mathbb{N}}(m+1) = 0$ следи да није $m+1 > 3$, то јест да је $m+1 \leq 3$. Како ни за један природни број m не важи да $m > 3$ и $m + 1 \leq 3$, добили смо контрадикцију. Дакле, задата структура јесте модел ове формуле.

8.

$$1.\bot((\forall x)(p(x) \Rightarrow q(x)) \Rightarrow ((\forall x)p(x) \Rightarrow (\forall x)q(x)))$$

$$2.\top((\forall x)(p(x) \Rightarrow q(x))) \;\; (1)$$

$$3.\bot((\forall x)p(x) \Rightarrow (\forall x)q(x)) \;\; (1)$$

$$4.\top((\forall x)p(x) \;\; (3)$$

$$5.\bot((\forall x)q(x)$$

$$6.\bot(q(a)) \;\; (5)$$

$$7.\top(p(a)) \;\; (4)$$

$$8.\top(p(a) \Rightarrow q(a)) \;\; (2)$$

$$9.\bot(p(a)) \;\; (8) \qquad 10.\top(q(a)) \;\; (8)$$

$$X(7,9) \qquad X(6,10)$$

9.

$$1.\bot((\forall x)((p(x) \vee q(x)) \Rightarrow r(x)) \Rightarrow ((\exists x)\neg r(x) \Rightarrow (\exists x)\neg p(x)))$$

$$2.\top((\forall x)((p(x) \vee q(x)) \Rightarrow r(x))) \;\; (1)$$

$$3.\bot((\exists x)\neg r(x) \Rightarrow (\exists x)\neg p(x)) \;\; (1)$$

$$4.\top((\exists x)\neg r(x)) \;\; (3)$$

$$5.\bot((\exists x)\neg p(x)) \;\; (3)$$

$$6.\top(\neg r(a)) \;\; (4)$$

$$7.\bot(r(a)) \;\; (6)$$

$$8.\bot(\neg p(a)) \;\; (5)$$

$$9.\top(p(a)) \;\; (\text{п(a)})$$

$$10.\top((p(a) \vee q(a)) \Rightarrow r(a)) \;\; (2)$$

$$11.\bot(p(a) \vee q(a)) \;\; (10) \qquad 12.\top(r(a)) \;\; (10)$$

$$X(7,12)$$

$$13.\bot(p(a)) \;\; (11)$$

$$14.\bot(q(a)) \;\; (11)$$

$$X(9,13)$$

10. $1.\bot((\forall x)(\exists y)(\exists z)(p(x,z) \Rightarrow q(x,y)) \Rightarrow ((\forall x)(\forall z)p(x,z) \Rightarrow (\forall x)(\exists y)q(x,y)))$

$$
\begin{array}{c}
2.\top((\forall x)(\exists y)(\exists z)(p(x,z) \Rightarrow q(x,y)))\ \ (1) \\
| \\
3.\bot((\forall x)(\forall z)p(x,z) \Rightarrow (\forall x)(\exists y)q(x,y))\ \ (1) \\
| \\
4.\top((\forall x)(\forall z)p(x,z))\ \ (3) \\
| \\
5.\bot((\forall x)(\exists y)q(x,y))\ \ (3) \\
| \\
6.\bot((\exists y)q(a,y))\ \ (5) \\
| \\
7.\top((\exists y)(\exists z)(p(a,z) \Rightarrow q(a,y)))\ \ (2) \\
| \\
8.\top((\forall z)p(a,z))\ \ (4) \\
| \\
9.\top((\exists z)(p(a,z) \Rightarrow q(a,b)))\ \ (7) \\
| \\
10.\bot(q(a,b))\ \ (6) \\
| \\
11.\top(p(a,c) \Rightarrow q(a,b))\ \ (9) \\
| \\
12.\top(p(a,c))\ \ (8) \\
\swarrow \qquad \searrow \\
\begin{array}{cc}
13.\bot(p(a,c))\ \ (11) & 14.\top(q(a,b))\ \ (11) \\
X(12,13) & X(10,14)
\end{array}
\end{array}
$$

11.

$1.\bot((H \wedge K) \Rightarrow L)$

$2.\top(H \wedge K)\ \ (1)$

$3.\bot((\forall x)p(x) \Rightarrow (\exists x)(\exists y)q(x,y))\ \ (1)$

$4.\top((\forall x)(p(x) \Rightarrow (\exists y)(q(x,y) \vee r(x,y))))\ \ (2)$

$5.\top((\exists x)(\forall y)\neg r(x,y))\ \ (2)$

$6.\top((\forall x)p(x))\ \ (3)$

$7.\bot((\exists x)(\exists y)q(x,y))\ \ (3)$

$8.\top((\forall y)\neg r(a,y))\ \ (5)$

$9.\top(p(a) \Rightarrow (\exists y)(q(a,y) \vee r(a,y)))\ \ (4)$

$10.\top(p(a))\ \ (6)$

$11.\bot((\exists y)q(a,y))\ \ (7)$

$12.\bot(p(a))\ \ (9)$	$13.\top((\exists y)(q(a,y) \vee r(a,y)))\ \ (9)$
$X(10,12)$	$14.\top(q(a,b) \vee r(a,b))\ \ (13)$
	$15.\bot(q(a,b))\ \ (11)$
	$16.\top(\neg r(a,b))\ \ (8)$
	$17.\bot(r(a,b))\ \ (16)$

$18.\top(q(a,b))\ \ (14)$	$19.\top(r(a,b))\ \ (14)$
$X(15,17)$	$X(17,19)$

Теорема 11.1

Доказ. □

Тврђење 11.2

Доказ. □

Последица 11.3

Доказ. □

Пример 11.4

△

Дефиниција 11.5