# I skyrius. AIBĖS IR ATVAIZDŽIAI

## Aibės sąvoka

**0. 1.** Šiuolaikinėje matematikoje aibių teorijos yra grindžiamos aksiomų sistemomis. Pagrindinėms algebros struktūroms išdėstyti labiausiai priimtina aibių teorija, pagrįsta Cermelo - Frenkelio (o taip pat ir Bernaiso - Gedelio) aksiomų sistema. Bet aksiomatiškai aibių teorijos mes nedėstysime, nes mūsų tikslams visiškai pakaks pačių elementariausių šios teorijos sąvokų.

Aibių teorijoje, kurią sukūrė Georgas Kantoras, aibės ir elemento priklausomumo aibei sąryšio sąvokos buvo grindžiamos intuicija. Pavyzdžiui, Cermelo - Frenkelio aibių teorijoje aibės ir elemento priklausomumo aibei sąryšio sąvokos yra laikomos pirminėmis, kurių pagrindinės savybės nusakomos aksiomomis. Georgas Kantoras pateikė tokį aibės apibrėžimą: "aibę suprasime kaip objektų, kuriuos vieną nuo kito gerai galime atskirti savo intuicija arba mintimis, sujungimą į vieną visumą".

Nors, kaip aibių teorijos raida rodo, intuicija pasikliauti negalima, mes visgi prisilaikysime Kantoro apibrėžimo. Tik pabrėšime, kad ne kiekviena kurių nors elementų ar objektų visuma sudaro aibę. Pavyzdžiui, tarę, kad visų aibių visuma yra aibė, neišvengtume paradoksų. Štai vienasiš žinomų paprasčiausias, Bertrano Raselo paradoksas. Pažymėkime raide $C$visų aibių, nesančių pačios savęs elementu, visumą. Pavyzdžiui, visų natūraliųjų skaičių aibė $\mathbb{N}$ nėra natūralusis skaičius, visų racionaliųjų skaičių aibė $\mathbb{Q}$ taip pat nėra racionalusis skaičius, t. y. šios aibės priklauso $C$. Tarę, kad $C$ yra aibė, išsiaiškinkime, ar aibė $C$ yra aibės $C$ elementas, ar ne. Jei aibė $C$ yra aibės $C$ elementas, tai aibė $C$ nepriklauso aibei $C$ pagal $C$ apibrėžimą. Jei aibė $C$ nėra aibės $C$ elementas, tai aibė $C$ priklauso $C$ pagal $C$ apibrėžimą. Kaip matome, tai tikrai labai paprastas paradoksas.

Dėl aptiktų Kantoro aibių teorijoje paradoksų matematikams iškilo problema pagrįsti aibių teoriją taip, kad joje nebūtų paradoksų, o Kantoro aibių teorijos esminiai pasiekimai, – kardinalų ir ordinalų teorija, – būtų išsaugoti. Nieko geriau nebuvo sugalvota, kaip kurti aibių teorijas aksiomatiškai. Vėliau apie tai kalbėsime kiek plačiau.

**0. 2.** Aptarsime aibių teorijos elementariausias sąvokas ir žymėjimus. Užrašai "$a \in A$" arba "$A \ni a$" yra skaitomi "$a$ yra aibės $A$ elementas" arba "$a$ priklauso aibei $A$". Užrašai "$a \notin A$" arba "$A \not\ni a$" yra skaitomi "$a$ nėra aibės $A$ elementas" arba "$a$ nepriklauso aibei $A$". Aibė, neturinti nei vieno elemento, yra vadinama tuščiąja ir yra žymima $\emptyset$. Baigtinę aibę, sudarytą iš elementų $x_1, x_2, \ldots, x_n$, sutarkime užrašyti $\{x_1, x_2, \ldots, x_n\}$.

**Aibės poaibio apibrėžimas.** Yra sakoma, kad aibė $A$ yra aibės $B$ poaibis ir žymima $A \subset B$ arba $B \supset A$, jei aibės $A$ kiekvienas elementas yra ir aibės $B$ elementas. Aibės poaibio apibrėžimas matematiniais simboliais yra užrašomas taip:

$$A \subset B \Longleftrightarrow: \forall a (a \in A \Rightarrow a \in B).$$

Užrašai "$A \not\subset B$" arba "$B \not\supset A$" yra skaitomi "aibė $A$ nėra aibės $B$ poaibis". Aibė $A$ nėra aibės $B$ poaibis, jei egzistuoja toks aibės $A$ elementas $a$, kuris nepriklauso aibei $B$. Apibrėžimą "aibė $A$ nėra aibės $B$ poaibis" matematiniais simboliais galime užrašyti taip:

$$A \not\subset B \Longleftrightarrow: \exists a(a \in A \wedge a \notin B).$$

Aibių įdėties sąryšis $\subset$ (arba $\supset$) turi sekančias savybes:

1. Jei $A \subset B$ ir $B \subset C$, tai $A \subset C$.Matematinių simbolių žymėjimais ši savybė atrodo taip:

$$((A \subset B) \wedge (B \subset C)) \Longrightarrow (A \subset C);$$

2. Kiekvienai aibei $A$, $\emptyset \subset A$. Matematinių simbolių žymėjimais ši savybė atrodo taip:

$$\forall A(\emptyset \subset A).$$

**Aibių lygybės apibrėžimas.** Aibės $A$ ir $B$ yra vadinamos lygiomis ir žymima $A = B$, jei $A \subset B$ ir $B \subset A$. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$(A = B) \Longleftrightarrow: ((A \subset B) \wedge (B \subset A)).$$

Aibių lygybės sąryšis $=$ turi sekančias savybes:

1. Kiekvienai aibei $A$, $A = A$;
2. Jei $A = B$, tai $B = A$. Matematiniais simboliais ši savybė užrašoma taip:

$$(A = B) \Longrightarrow (B = A);$$

3. Jei $A = B$, $B = C$, tai $A = C$. Matematiniais simboliais ši savybė užrašoma taip:

$$((A = B), (B = C)) \Longrightarrow (A = C).$$

**Aibės poaibiai.** Fiksuotos aibės $A$ visų poaibių visuma sudaro aibę, kuri yra žymima $\mathbf{P}(A)$ arba $2^A$. Taigi $X \subset A \Longleftrightarrow X \in \mathbf{P}(A)$.

Aibės $A$ poaibiai dažnai yra apibrėžiami kuria nors savybe $S$, kurią turintys aibės $A$ elementai ir sudaro aibės $A$ poaibį. Aibės $A$ elementų, turinčių savybę $S$, visumą žymėsime $\{x \in A | S(x)\}$. Pavyzdžiui, $\{x \in \mathbb{R} | x > 2\}$ yra realiųjų skaičių aibės poaibis, sudarytas iš realiųjų skaičių didesnių už 2. Aibių teorijoje, grindžiamoje aksiomų sistema, kruopščiai yra aptariamos savybių klasės, leistinos nagrinėjamojoje teorijoje. Tos savybės, kurias vėliau nagrinėsime mes, norėdami apibrėžti kurio nors aibės kai kuriuos poaibius, nesukels jokių loginių sunkumų.

## 1. Veiksmai su aibėmis

**1. 1. Aibių sumos (junginio) apibrėžimas.** Aibių $A$ ir $B$ suma (junginiu) yra vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso bent vienai aibių: $A$ ar $B$ ir žymima $A \cup B$. Mtematinių simbolių žymėjimais aibių suma yra apibrėžiama taip:

$$x \in A \cup B \Longleftrightarrow (x \in A) \vee (x \in B).$$

Aibių sumą galima ir taip apibrėžti: $A \cup B =: \{x | x \in A \vee x \in B\}$.

Panašiai galima apibrėžti ir užrašyti ir aibių šeimos sumą. Aibių šeima yra vadinama tokia aibių $A_\alpha$ visuma $\{A_\alpha\}_{\alpha \in I}$, kurios elementai "sunumeruoti" kurios nors aibės $I$ elementais $\alpha$. Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ aibės, kurių indeksai skirtingi, gali būti ir lygios.

**Aibių šeimos suma.** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ suma (junginys) apibrėžiama(s) taip:

$$\bigcup_{\alpha \in I} A_\alpha =: \{x | \exists \alpha \in I (x \in A_\alpha)\}.$$

**Aibių sumos savybės.** Bet kurioms aibėms $A$, $B$, $C$ teisingos lygybės:
1. $A \cup (B \cup C) = (A \cup B) \cup C$. Ši savybė yra vadinama aibių sudėties asociatyvumu;
2. $A \cup B = B \cup A$. Ši savybė yra vadinama aibių sudėties komutatyvumu;
3. $A \cup A = A$. Ši savybė yra vadinama aibių sudėties idempotentumo dėsniu.

**1. 2. Aibių sankirtos (sandaugos) apibrėžimas.** Aibių $A$ ir $B$ sankirta (sandauga) yra vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso ir aibei $A$ ir aibei $B$ ir yra žymima $A \cap B$. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$A \cap B = \{x | (x \in A) \wedge (x \in B)\}$$

arba

$$x \in A \cap B \Longleftrightarrow ((x \in A) \wedge (x \in B)).$$

**Aibių šeimos sankirta (sandauga).** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ sankirta (sandauga) apibrėžiama taip:

$$\bigcap_{\alpha \in I} A_\alpha =: \{x | \forall \alpha \in I (x \in A_\alpha)\}.$$

**Aibių sankirtos savybės.** Bet kurioms aibėms $A$, $B$, $C$ teisingos lygybės:
1. $(A \cap B) \cap C = A \cap (B \cap C)$ (aibių sankirtos asociatyvumo dėsnis);
2. $A \cap B = B \cap A$ (aibių sankirtos komutatyvumo dėsnis);
3. $A \cap A = A$ (aibių sankirtos idempotentumo dėsnis ).

**1. 3. Aibių skirtumo apibrėžimas.** Aibių $A$ ir $B$ skirtumu yra vadinama aibė, sudaryta iš visų tų aibės $A$ elementų, kurie nepriklauso aibei $B$, ir yra žymima $A \setminus B$. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$A \setminus B = \{x \in A | x \notin B$$

arba

$$x \in A \setminus B \Longleftrightarrow (x \in A) \wedge (x \notin B).$$

Akivaizdu, kad $A \setminus B \subset A$ ir

$$A \setminus B = A \Longleftrightarrow (A \cap B = \emptyset).$$

Pastebėsime, kad $A \cap B = A \setminus (A \setminus B)$.

**1. 4. Aibių simetrinio skirtumo apibrėžimas.** Aibių $A$ ir $B$ simetriniu skirtumu yra vadinama aibė

$$A \ominus B =: (A \setminus B) \cup (B \setminus A).$$

**1. 5. Distributyvumo dėsniai.** Aibių sudėtis ir sankirta yra susieti distributyvumo dėsniais. Bet kurioms aibėms $A$, $B$, $C$, teisingos lygybės:

1. $A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ (pirmasis distributyvumo dėsnis, siejantis aibių sudėtį ir sankirtą );

2. $A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (antrasis distributyvumo dėsnis, siejantis aibių sudėtį ir sankirtą ).

**Pratimai.**

1. Įrodykite anksčiau užrašytus distributyvumo dėsnius, siejančius aibių sudėtį ir sankirtą.

2. Įrodykite, kad bet kurioms aibėms $A$, $B$, $C$, teisingos lygybės:
1. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
2. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Šios lygybės yra vadinamos de Morgano dėsniais. De Morgano dėsnius galime užrašyti bendriausiuoju atveju:

$$A \setminus (\bigcap_{\alpha \in I} B_\alpha) = \bigcup_{\alpha \in I} (A \setminus B_\alpha)$$

ir

$$A \setminus (\bigcup_{\alpha \in I} B_\alpha) = \bigcap_{\alpha \in I} (A \setminus B_\alpha).$$

Įrodykite, kad bet kurioms aibėms $A$, $B$, $C$ yra teisingos lygybės:

1. $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)$. Kaip matome, aibių skirtumas ir sankirta yra susieti distributyvumo dėsniu.

2. $(A \ominus B) \ominus C = A \ominus (B \ominus C)$. Kaip matome, simetrinis aibių skirtumas yra asociatyvus.

3. $(A \ominus B) \cap C = (A \cap C) \ominus (B \cap C)$. Kaip matome, simetrinis aibių skirtumas ir aibių sankirta yra susieti distributyvumo dėsniu.

**Aibės papildinio apibrėžimas.** Aibės $A$ poaibio $X$ papildiniu iki aibės $A$ yra vadinama aibė $C_A X =: A \ominus X$.

Paprastumo dėlei praleisime apatinį indeksą $A$ tais atvejais, kai iš konteksto aišku, iki kokios aibės yra imamas papildinys.

Išvardinsime keletą paprastų aibė papildinio savybių. Tarkime, kad $X \subset A$, $Y \subset A$. Tuomet:

1. $C(CX) = X$;

2. $X \subset Y \Longrightarrow CX \supset CY$;

3. $C(X \cap Y) = CX \cup CY$;

4. $C(X \cup Y) = CX \cap CY$.

Aibės papildinio trečioji ir ketvirtoji savybės, – tai de Morgano dėsniai. Remdamiesi aibės papildinio pirmąja ir antrąja savybėmis, gauname, kad

$$X = Y \Longleftrightarrow CX = CY.$$

**Pavyzdžiai ir pratimai.**

1. Apibrėžkime $n\mathbb{Z} =: \{nk | k \in \mathbb{Z}\}$, čia $n$ – natūralusis skaičius. Įrodykite: $n\mathbb{Z} \subset m\mathbb{Z}$ tada ir tik tada, kai skaičius $m$ dalija skaičių $n$.

2. Įrodykite, kad $n\mathbb{Z} \cap m\mathbb{Z} = r\mathbb{Z}$, čia skaičius $r$ yra skaičių $m$ ir $n$ mažiausias bendrasis kartotinis.

3. Jei $n \in \mathbb{N}$, $r \in \mathbb{Z}$, tai apibrėžkime aibę $r + n\mathbb{Z} =: \{r + nk | k \in \mathbb{Z}\}$. Įrodykite, kad $r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z}$, $r_1, r_2 \in \mathbb{Z}$, tada ir tik tada, kai skaičius $n$ dalija $r_1 - r_2$. Įrodykite, jei $n$ nedalija $r_1 - r_2$, tai $(r_1 + n\mathbb{Z}) \cap (r_2 + n\mathbb{Z}) = \emptyset$.

4. Įrodykite, kad $\bigcup_{j=0}^{n-1} (j + n\mathbb{Z}) = \mathbb{Z}$.

5. Imkime $s \in \mathbb{Q}$ ir apibrėžkime aibę $s\mathbb{Z} =: \{sk | k \in \mathbb{Z}\}$. Įsitikinkite, kad aibė $\bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z}$, čia $p$ pirminis skaičius, yra sudaryta iš visų racionaliųjų skaičių, kurių skaitiklis gali būti bet koks sveikasis skaičius, o vardiklis – pirminio skaičiaus $p$ laipsnis, t. y.

$$\alpha \in \bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z} \Longleftrightarrow (\exists m \in \mathbb{Z})(\exists s \in \mathbb{N})(\alpha = \frac{m}{p^s}).$$

6. Įrodykite, kad bet kuriam natūraliajam skaičiui $m$ yra teisinga lygybė:

$$\bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z} = \bigcup_{j=m}^{\infty} \frac{1}{p^j}\mathbb{Z}.$$

7. Įsitikinkite, kad

$$\mathbb{Q} = \bigcup_{\substack{0 \le r < 1 \\ r \in \mathbb{Q}}} (r + \mathbb{Z}).$$

## 2. Sąryšis

**2. 1. Nesutvarkytosios poros (nesutvarkytieji dvejetai).** Kad ir kokie būtų objektai $x$ ir $y$, egzistuoja aibė $A$, kurios elementai yra $x$ ir $y$. Šią aibę sutarkime užrašyti $A =: \{x, y\}$ ir vadinti nesutvarkyta pora (arba nesutvarkytu dvejetu). Matematinių simbolių žymėjimais aibė $A$ yra apibrėžiama taip:

$$\forall x \forall y \exists! A((z \in A) \Longrightarrow (z = x) \vee (z = y)).$$

Savaime aišku, kad $\{x, y\} = \{y, x\}$. Jei $x = y$, tai aibę $\{x, x\}$ žymėsime $\{x\}$.

Panašiai galima apibrėžti nesutvarkytą trejetą, ketvertą ir t. t. .

**2. 2. Sutvarkytosios poros (sutvarkytieji dvejetai).** Apibrėšime sutvarkytosios poros Kuratovskio konstrukciją. Imkime bet kokius objektus $x$ ir $y$ ir sudarykime aibę $(x, y) =: \{\{x\}, \{x, y\}\}$. Atkreipkite dėmesį, kad pirmiausia iš objektų $x$ ir $y$ yra sudaromos aibės $\{x\}$ ir $\{x, y\}$, o iš tų aibių yra sudaroma aibė $\{\{x\}, \{x, y\}\}$. Akivaizdu, kad $(x, y) \neq (y, x)$, jei tik $x \neq y$. Aibę $(x, y)$ yra vadinama sutvarkytąja pora ( sutvarkytuoju dvejetu), $x$ – sutvarkytosios poros pirmuoju elementu, o $y$ – sutvarkytosios poros antruoju elementu. Labai svarbi sutvarkytosios poros ( sutvarkytojo dvejeto) pagrindinė savybė:

$$((x_1, y_1) = (x_2, y_2)) \Longleftrightarrow (x_1 = x_2) \wedge (y_1 = y_2)).$$

Dėl šios savybės ir yra apibrėžiama(s) sutvarkytoji pora (sutvarkytasis dvejetas). Teiginį "z yra sutvarkytoji pora" ar "z yra sutvarkytasis dvejetas" suprasime taip: egzistuoja tokie objektai $x$ ir $y$, kad $z = (x, y)$.

Panašiai galima apibrėžti sutvarkytuosius trejetus, ketvertus ir t. t. . Sutvarkytojo $n$-tuko $(x_1, x_2, \ldots, x_n)$ pagrindinė savybė yra tokia:

$$((x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)) \Longleftrightarrow ((x_1 = y_1) \wedge (x_2 = y_2) \wedge \ldots \wedge (x_n = y_n)).$$

**2. 3. Sąryšio apibrėžimas.** Aibė $R$, kurios elementai yra sutvarkytosios poros (sutvarkytieji dvejetai) yra vadinama binariuoju (dviviečiu) sąryšiu arba binariąja (dviviete) atitiktimi.

Šis apibrėžimas užrašytas matematinių simbolių žymėjimais atrodo taip:

$$(R - \text{sąryšis}) \Longleftrightarrow \forall z (z \in R \Longrightarrow z - \text{sutvarkytoji pora}).$$

Yra sakoma, kad elementas $x$ yra susietas sąryšiu $R$ su elementu $y$ ir tai žymima $xRy$, jei sutvarkytoji pora $(x, y) \in R$. Kitaip tariant, $xRy \Longleftrightarrow: (x, y) \in R$.

**2. 4. Sąryšio apibrėžimo ir kitimo sritys.** Visų sutvarkytųjų porų, priklausančių $R$, pirmųjų elementų aibė $D(R)$ yra vadinama sąryšio $R$ apibrėžimo sritimi, o tų sutvarkytųjų porų antrųjų elementų aibė $E(R)$ – sąryšio $R$ kitimo sritimi (arba sąryšio $R$ reikšmių aibe). Matematinių simbolių žymėjimais šie apibrėžimai atrodo taip:

$$D(R) =: \{x | \exists y ((x, y) \in R)\},$$

$$E(R) =: \{y | \exists x ((x, y) \in R)\}$$

Galime dar ir taip užrašyti:

$$D(R) =: \{x | \exists y (xRy)\},$$

$$E(R) =: \{y | \exists x (xRy)\}.$$

**2. 5. Atvirkštinis sąryšis sąryšiui $R$.** Sąryšis $R^{-1} =: \{(x, y) | yRx\}$ yra vadinamas atvirkštiniu sąryšiu sąryšiui $R$.

Galime ir taip užrašyti: $xR^{-1}y \Longleftrightarrow yRx$ arba $(x, y) \in R^{-1} \Longleftrightarrow (y, x) \in R$. Akivaizdu, kad $D(R^{-1}) = E(R)$, $E(R^{-1}) = D(R)$.

**2. 6. Sąryšių kompozicija (superpozicija).** Sąryšių $R_1$ ir $R_2$ kompozicija (superpozicija) yra vadinamas sąryšis

$$R_2 \circ R_1 =: \{(x, y) | \exists z (((x, z) \in R_1) \wedge ((z, y) \in R_2))\}.$$

Akivaizdu, kad $D(R_2 \circ R_1) \subset D(R_1)$, $E(R_2 \circ R_1) \subset E(R_2)$.

**Sąryšių kompozicijos (superpozicijos) savybės.** Bet kokiems sąryšiams $R_1$, $R_2$, $R_3$, teisingos lygybės:

1. $(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1)$;
2. $(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$;
3. $(R^{-1})^{-1} = R$.

**Pratimas.** Įrodykite sąryšių kompozicijos užrašytąsias savybes.

**2. 7. Sąryšio siaurinys.** Tarkime, $R$ – sąryšis, $D(R)$ – sąryšio $R$ apibrėžimo sritis. Kiekvienam aibės $D(R)$ poaibiui $X$ egzistuoja sąryšis $R\big|_X =: \{(x, y) \in R | x \in X\}$. Panašiai, kiekvienam sąryšio $R$ reikšmių srities $E(R)$ poaibiui $Y$ egzistuoja sąryšis ${}_Y\big|R =: \{(x, y) \in R | y \in Y\}$.

Sąryšis $R\big|_X$ yra vadinamas sąryšio $R$ siauriniu, gaunamu susiaurinant sąryšio $R$ apibrėžimo sritį $D(R)$ iki poaibio $X$. Panašiai, ${}_Y\big|R$ yra taip pat vadinamas sąryšio $R$ siauriniu, gaunamu susiaurinant sąryšio $R$ kitimo sritį $E(R)$ iki poaibio $Y$. Akivaizdu, kad

$$R\big|_X \subset R, D(R\big|_X) = X, E(R\big|_X) \subset E(R),$$

$${}_Y\big|R \subset R, D({}_Y\big|R) \subset D(R), E({}_Y\big|R) = Y.$$

Remdamiesi sąryšio siaurinio apibrėžimu, gauname:
1. Jei $X_1 \subset X_2 \subset D(R)$, tai $(R\big|_{X_2})\big|_{X_1} = R\big|_{X_1}$;
2. Jei $Y_1 \subset Y_2 \subset E(R)$, tai ${}_{Y_1}\big|({}_{Y_2}\big|R) = {}_{Y_1}\big|R$;
3. Jei $X \subset D(R)$, $Y \subset E(R)$, tai ${}_Y\big|(R\big|_X) = ({}_Y\big|R)\big|_X$.

**2. 8. Sąryšio plėtinys.** Sąryšis $S$ yra vadinamas sąryšio $R$ plėtiniu, jei $D(R) \subset D(S)$, $E(R) \subset E(S)$, $R = S\big|_{D(R)}$. Galima apibrėžti sąryšio $R$ plėtinį ir kita prasme: sąryšis $S$ yra sąryšio $R$ plėtinys, jei $R = {}_{E(R)}\big|S$.

**2. 9. Veiksmai su sąryšiais.** Kadangi sąryšiai yra aibės, tai veiksmai su sąryšiais tokie pat, kaip ir su aibėmis. Taigi galima apibrėžti sąryšių sumą, sankirtą, skirtumą ir t. t. .

**Išspręskite šiuos pratimus.** Bet kokiems sąryšiams $R_1$, $R_2$, $R_3$, yra teisingos lygybės:

1. $D(R_1 \cup R_2) = D(R_1) \cup D(R_2)$, $E(R_1 \cup R_2) = E(R_1) \cup E(R_2)$;

2. $D(R_1 \cap R_2) \subset D(R_1) \cap D(R_2)$, $E(R_1 \cap R_2) \subset E(R_1) \cap E(R_2)$;

3. $D(R_1 \setminus R_2) \supset D(R_1) \setminus D(R_2)$, $E(R_1 \setminus R_2) \supset E(R_1) \setminus E(R_2)$;

4. $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$, $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$, $(R_1 \setminus R_2)^{-1} = R_1^{-1} \setminus R_2^{-1}$;

5. $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$, $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$;

6. $(R_1 \cap R_2) \circ R_3 \subset (R_1 \circ R_3) \cap (R_2 \circ R_3)$, $R_1 \circ (R_2 \cap R_3) \subset (R_1 \circ R_2) \cap (R_1 \circ R_3)$.

## 3. Funkcinis sąryšis (funkcija). Atvaizdis

**3. 1. Apibrėžimas.** Sąryšis $R$ yra vadinamas funkciniu sąryšiu arba funkcija, jei $R$ tenkina sąlygą:

$$(\forall x \forall y \forall z)(((x, y) \in R) \wedge ((x, z) \in R) \Longrightarrow (y = z)).$$

Galime pasakyti ir taip: R yra funkcija, jei aibei $R$ nepriklauso dviejų skirtingų sutvarkytų dvejetų su vienu ir tuo pačiu pirmuoju elementu.

Funkcijas žymėsime raidėmis $f$, $g$, $h$, ir t. t. .

**Pastabos.**

1. Jei $f$ funkcija, tai bendruoju atveju $f^{-1}$ nėra funkcija. Pavyzdžiui, $f = \{(x, x^2)|x \in \mathbb{R}\}$ yra funkcija, bet $f^{-1} = \{(x^2, x)|x \in \mathbb{R}\}$ nėra funkcija, nes $(1, 1) \in f^{-1}$ ir $(1, -1) \in f^{-1}$, tuo tarpu šių sutvarkytų dvejetų pirmieji elementai yra lygūs, o antrieji – nėra lygūs. Panašiai, $g = \{(x, \sin x)|x \in \mathbb{R}\}$ yra funkcija, o $g^{-1}$ nėra funkcija.

2. Funkcijų $f$ ir $g$ sąjunga (suma) $f \cup g$ bendruoju atveju nėra funkcija. Pavyzdžiui, $f = \{(1, 2)\}$, $g = \{(1, 3)\}$ yra funkcijos, tuo tarpu $f \cup g = \{(1, 2), (1, 3)\}$ nėra funkcija, nes sutvarkytų dvejetų $(1, 2)$ ir $(1, 3$, priklausančių $f \cup g$, pirmieji elementai yra lygūs, o antrieji elementai nėra lygūs.

3. Funkcijų $f$ ir $g$ sankirta $f \cap g$, jei tik netuščia, visuomet yra funkcija.

**3. 2. Atvaizdžio apibrėžimas.** Funkcija $f$ yra vadinama atvaizdžiu iš aibės $A$ į aibę $B$, jei $D(f) = A$, $E(f) \subset B$. Šiuo atveju taip pat yra sakoma, kad $f$ yra atvaizdis, apibrėžtas aibėje $A$ ir įgyjantis reikšmes aibėje $B$. Atvaizdis $f$ iš aibės $A$ į aibę $B$ yra žymimas $f : A \to B$ arba $A \xrightarrow{f} B$. Jei $(a, b) \in f$, tai elementas $b \in B$ yra vadinamas elemento $a \in A$ vaizdu ir yra žymimas $f(a)$.

Dažnai yra naudojami ir tokie atvaizdžio $f$ iš aibės $A$ į aibę $B$ žymėjimai: $A \ni a \mapsto f(a) \in B$ arba $A \to B$, $a \mapsto f(a)$. Šie žymėjimai dažniausiai naudojami tais atvejais, kai apibrėžiamas atvaizdis $f$, nurodant aibės $A$ elemento $a$ vaizdą $f(a) \in B$ formule ar kuria nors vienareikšmiškai nusakoma taisykle ir t. t. . Pavyzdžiui, $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, $\sin : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin x$ ir t. t. .

Tarkime, kad $f$ yra atvaizdis iš aibės $A$ į aibę $B$. Tuomet kiekvienam $a \in A$ egzistuoja vienintelis $b \in B$ toks, kad $(a, b) \in f$ (arba $afb$). Todėl literatūroje dažnai atvaizdis $f : A \to B$ yra vadinamas taisykle $f$, kuria remiantis kiekvienam aibės $A$ elementui $a$ yra priskiriamas vienas ir tik vienas aibės $B$ elementas $b$, kuris yra žymimas $f(a)$ ir vadinamas elemento $a$ vaizdu.

**3. 3.** Tarkime, kad $f : A \to B$ yra atvaizdis, $X \subset A$, $Y \subset B$. Aibė $f(X) =: \{f(x)|x \in X\}$, sudaryta iš aibės $A$ poaibio $X$ elementų vaizdų, yra vadinama aibės $A$ poaibio $X$ vaizdu. Jei $X = \{a\}$, tai vietoje $f(\{a\})$ rašysime $f(a)$.

Aibės $A$ poaibio $X$ vaizdą $f(X)$ galime ir taip apibrėžti: $f(X) = E(f\big|_X)$ arba $f(X) = \{b \in B|(\exists x \in X)(f(x) = b)\}$.

**Apibrėžimas.** Aibė $f^{-1}(Y) =: \{a \in A|f(a) \in Y\}$, sudaryta iš visų tokių aibės $A$ elementų, kurių vaizdai priklauso $Y$, $Y \subset B$, yra vadinama aibės $B$ poaibio $Y$ pilnuoju pirmavaizdžiu ( dažniausiai žodis "pilnuoju" yra praleidžiamas). Jei $Y = \{b\}$, tai vietoje $f^{-1}(\{b\})$ rašysime $f^{-1}(b)$.

Aibės $B$ poaibio $Y$ pilnąjį pirmavaizdį $f^{-1}(Y)$ galime ir taip apibrėžti: $f^{-1}(Y) = D({}_Y\big|f)$ arba $f^{-1}(Y) = E(f^{-1}\big|_Y)$.

**3. 4. Atvaizdžių kompozicija.** Sakykime, kad $f : A \to B$ ir $g : B \to C$ yra atvaizdžiai. Tuomet remdamiesi atvaizdžio apibrėžimu, gauname, kad funkcijų $g$ ir $f$ kompozicija $g \circ f$ yra atvaizdis $g \circ f : A \to C$, kuris yra vadinamas atvaizdžių $f$ ir $g$ kompozicija.

Jei $f : A \to B$ ir $g : B \to C$ – atvaizdžiai, tai kiekvienam $a \in A$, $(g \circ f)(a) = g(f(a))$.

**Pratimas.** Sakykime, kad $f : A \to B$, $g : B \to C$, $h : C \to D$ yra atvaizdžiai. Įrodykite, kad $h \circ (g \circ f) = (h \circ g) \circ f$. Rendamiesi šia lygybe, matome, kad atvaizdžių kopozicija yra asociatyvus dėsnis.

**3. 5. Apibrėžimas.** Visų atvaizdžių iš aibės $A$ į aibę $B$ visuma sudaro aibę, kuri yra žymima $B^A$. Pagal apibrėžimą

$$f \in B^A \Longleftrightarrow f : A \to B - \text{ atvaizdis.}$$

**Pratimai.**

Tarkime, kad $f : A \to B$ yra atvaizdis, $X_1, X_2 \subset A$, $Y_1, Y_2 \subset B$. Įrodykite lygybes:

1. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$;
2. $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$;
3. $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$;
4. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$;
5. $f^{-1}(Y_1 \setminus Y_2) = f^{-1}(Y_1) \setminus f^{-1}(Y_2)$;
6. $f^{-1}(Y_1 \ominus Y_2) = f^{-1}(Y_1) \ominus f^{-1}(Y_2)$;
7. $f(f^{-1}(Y_1)) = Y_1$;
8. $f^{-1}(f(X_1)) \supset X_1$.

**Pastaba.** Jei $f$ yra atvaizdis iš aibės $A$ į aibę $B$, tai, remdamiesi aibės vaizdo ir aibės pilnojo pirmavaizdžio apibrėžimu, matome, kad $f$ generuoja atvaizdį iš aibės $\mathbf{P}(A)$ į aibę $\mathbf{P}(B)$, o $f^{-1}$, gal ir nebūdamas atvaizdžiu iš aibės $E(f)$ į aibę $A$, generuoja atvaizdį iš aibės $\mathbf{P}(B)$ į aibę $\mathbf{P}(A)$, kuriuos žymime $f$ ir $f^{-1}$. Induktyviai būtų galima apibrėžti atvaizdžius

$$\mathbf{P}^n(f) : \mathbf{P}^n(A) \to \mathbf{P}^n(B), n \in \mathbb{Z}, n \geq 1,$$

generuotus atvaizdžio $f : A \to B$ ir atvaidžius

$$\mathbf{P}^n(f^{-1}) : \mathbf{P}^n(B) \to \mathbf{P}^n(A), n \in \mathbb{Z}, n \geq 1,$$

genruotus atvaizdžio $f^{-1} : \mathbf{P}(B) \to \mathbf{P}(A)$, čia $\mathbf{P}^n(A) = \underbrace{\mathbf{P}(\mathbf{P}(\ldots(\mathbf{P}}_{n}(A))\ldots))$.

**3. 6. Aibių Dekarto sandauga.** Aibių $A$ ir $B$ Dekarto sandauga yra vadinama aibė $A \times B$, sudaryta iš visų sutvarkytų dvejetų $(a, b)$, $a \in A$, $b \in B$.

Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

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

Egzistuoja kanoniniai atvaizdžiai

$$pr_1 : A \times B \to A, pr_1((a, b)) = a$$

ir

$$pr_2 : A \times B \to A, pr_1((a, b)) = b,$$

kurie yra vadinami aibių $A$ ir $B$ Dekarto sandaugos $A \times B$ projekcijomis į pirmąjį ir antrąjį dauginamuosius $A$ ir $B$.

Panašiai galima apibrėžti aibių $A_1$, $A_2$, ... , $A_n$ Dekarto sandaugą $A_1 \times A_2 \times \ldots \times A_n$ ir projekcijas $pr_j : A_1 \times A_2 \times \ldots \times A_n \to A_j$, $1 \leq j \leq n$. Jei $A_1 = A_2 = \ldots = A_n$, tai vietoje

$$\underbrace{A \times A \times \ldots \times A}_{n},$$

yra rašoma $A^n$.

Kadangi

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_j \in A, \ 1 \leq j \leq n\},$$

tai $A^n$ galima sutapatinti su visų atvaizdžių iš $\{1, 2, \ldots, n\}$ į $A$ aibe. Kaip matome, žymėjimas $A^n$ yra suderintas su žymėjimu $B^A$ (žr.[ 2. 14.]).

**Aibių šeimos Dekarto sandauga.** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ Dekarto sandauga yra vadinama aibė $\prod\limits_{\alpha \in I} A_\alpha$, sudaryta iš visų atvaizdžių $f$, apibrėžtų aibėje $I$ ir, kiekvienam $\alpha \in I$, įgyjančių reikšmę $f(\alpha) \in A_\alpha$. Egzistuoja kanoninės projekcijos

$$pr_\alpha : \prod_{\alpha \in I} A_\alpha \to A_\alpha, \ pr_\alpha(f) = f(\alpha), \ f \in \prod_{\alpha \in I} A_\alpha, \ \alpha \in I.$$

**3. 7. Atvaizdžio grafikas.** Tarkime, kad $f : A \to B$ yra atvaizdis. Aibės $A \times B$ poaibis $\Gamma_f = \{(a, f(a)) | a \in A\}$ yra vadinamas atvaizdžio $f$ grafiku.

**Pastaba.** Remdamiesi atvaizdžio $f$ apibrėžimu, matome, kad $f$ ir $\Gamma_f$ kaip aibės yra lygios. Kalbant apie atvaizdžio $f$ grafiką $\Gamma_f = f$, svarbu, kad $\Gamma_f = f$ yra nagrinėjamas kaip aibės $A \times B$ poaibis. Savaime suprantama, kad atvaizdžio grafikas $\Gamma_f \subset A \times B$ vienareikšmiškai apibrėžia patį atvaizdį $f : A \to B$.

**Pavyzdys.** Atvaizdžio $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $x \in \mathbb{R}$, grafikas $\Gamma_f = \{(x, x^2) | x \in \mathbb{R}\}$ yra plokštumos $\mathbb{R}^2$ kreivė, kuri yra vadinama parabole.

**3. 8. Injektyvus atvaizdis (injekcija).** Atvaizdis $f : A \to B$ yra vadinamas injektyviu atvaizdžiu arba injekcija, jei bet kuriems $x, y \in A$,

$$f(x) = f(y) \Longrightarrow x = y.$$

Galima injektyvų atvaizdį apibrėžti ir taip: atvaizdis $f : A \to B$ yra vadinamas injektyviu atvaizdžiu arba injekcija, jei bet kuriems $x, y \in A$,

$$x \neq y \Longrightarrow f(x) \neq f(y).$$

Injektyvų atvaizdį galima ir taip apibūdinti: kiekvienam $y \in f(A)$, elemento $y$ pilnasis pirmavaizdis $f^{-1}(y)$ yra sudarytas tik iš vieno elemento.

Jei $f : A \to B$ yra injektyvus atvaizdis, tai apibrėžtas atvaizdis $f^{-1} : f(A) \to A$, $f^{-1}(f(a)) = a$, $a \in A$.

**3. 9. Siurjektyvus atvaizdis (siurjekcija).** Atvaizdis $f : A \to B$ yra vadinamas siurjektyviu atvaizdžiu arba siurjekcija, jei $f(A) = B$.

Atvaizdis $f : A \to B$ yra siurjektyvus, jei kiekvienam $b \in B$, egzistuoja toks $a \in A$, kad $f(a) = b$.

**3. 10. Bijektyvus atvaizdis (bijekcija).** Atvauzdis $f : A \to B$ yra vadinamas bijektyviu atvaizdžiu arba bijekcija, jei $f$ yra imjektyvus ir siurjektyvus atvaizdis.

**Pratimai.**

Sakykime, kad $f : A \to B$, $g : B \to C$ yra atvaizdžiai.

1. Įrodykite: jei $f, g$ yra injektyvūs atvaizdžiai, tai ir $g \circ f$ yra injektyvus atvaizdis.

2. Įrodykite: jei $f, g$ yra siurjektyvūs atvaizdžiai, tai ir $g \circ f$ yra siurjektyvus atvaizdis.

3. Įrodykite: jei $g \circ f$ yra injektyvus atvaizdis, tai ir atvaizdis $f$ yra injektyvus. Pateikite pavyzdį, kad $g \circ f$ būtų injektyvus atvaizdis, bet atvaizdis $g$ nebūtų injektyvus.

4. Įrodykite: jei $g \circ f$ yra siurjektyvus atvaizdis, tai ir atvaizdis $g$ yra siurjektyvus. Pateikite tokį pavyzdį, kad $g \circ f$ būtų siurjektyvus atvaizdis, bet atvaizdis $f$ nebūtų siurjektyvus.

5. Įrodykite: jei $g \circ f$ yra injektyvus atvaizdis, $f$ – siurjektyvus atvaizdis, tai atvaizdis $f$ yra bijektyvus, o $g$ – injektyvus atvaizdis.

6. Įrodykite: jei $g \circ f$ yra siurjektyvus atvaizdis, $g$ – injektyvus atvaizdis, tai atvaizdis $f$ yra siurjektyvus, o $g$ – bijektyvus atvaizdis.

**3. 11. Aibių ekvivalentumas.** Aibės $A$ ir $B$ yra vadinamos ekvivalenčiomis, jei egzistuoja bijekcija $f : A \to B$.

Pavyzdžiui, baigtinės aibės, turinčios vieną ir tą patį elementų skaičių, yra ekvivalenčios. Baigtinės aibės $A$ elementų skaičių žymėsime $|A|$.

Anksčiau sutarėme aibės $A$ visų poaibių aibę žymėti $\mathbf{P}(A)$ arba $2^A$. Dabar pagrįsime žymėjimą $2^A$.

**Teorema.** Aibės $\mathbf{P}(A)$ ir $\{0,1\}^A$ yra ekvivalenčios (žr.[2. 14.]).

**Įrodymas.** Tarkime, kad $X \in \mathbf{P}(A)$, t. y. $X \subset A$. Tuomet aibės $A$ poaibiui $X$ priskirkime atvaizdį $f_X : A \to \{0,1\}$,

$$f(a) = \begin{cases} 0, & \text{jei } a \in X, \\ 1, & \text{jei } a \notin X. \end{cases}$$

Taigi apibrėžėme atvaizdį:

$$F : \mathbf{P}(A) \to \{0,1\}^A, \ \ F(X) = f_X, \ \ X \in \mathbf{P}(A).$$

Įrodysime, kad $F$ yra bijekcija.

Pirmiausia įsitikinsime, kad $F$ yra injektyvus atvaizdis. Vadinasi, reikia įrodyti, kad, jei $X \neq Y$, tai ir $F(X) = f_X \neq f_Y = F(Y)$. Norint įrodyti, kad $f_X \neq f_Y$, reikia nurodyti bent vieną tokį aibės $A$ elementą $a$, kad būtų $f_X(a) \neq f_Y(a)$. Tad sakykime, kad $X, Y \in \mathbf{P}(A)$, $X \neq Y$. Kadangi $X \neq Y$, tai bent viena iš šių aibių yra netuščia. Tarkime, kad $X \neq \emptyset$. Jei $X \not\subset Y$, tai ezistuoja toks $a \in X$, kad $a \notin Y$. Šiuo atveju $F(X) = f_X \neq f_Y = F(Y)$, nes $f_X(a) = 0 \neq 1 = f_Y(a)$. Jei $X \subset Y$, tai egzistuoja toks $a \in Y$, kad $a \notin X$. Ir šiuo atveju $f_X(a) = 1 \neq 0 = f_Y(a)$, t. y. $F(X) = f_X \neq f_Y = F(Y)$. Taigi įrodėme, kad

$$F : \mathbf{P}(A) \to \{0,1\}^A$$

yra injektyvus atvaizdis.

Dabar įsitikinsime, kad $F$ yra siurjektyvus atvaizdis. Tuo tikslu reikia įrodyti, kad bet kuriam $g \in \{0,1\}^A$ egzistuoja toks $X \in \mathbf{P}(A)$, kad $F(X) = f_X = g$. Apibrėžkime $X$ taip:

$$X =: \{x \in A | g(x) = 0\}.$$

Akivaizdu, kad $f_X = g$. $\triangle$

Įrodysime dar vieną svarbią teoremą.

**Teorema.** Aibės $A$ ir $\mathbf{P}(A)$ nėra ekvivalenčios aibės.

**Įrodymas.** Šią teoremą įrodysime taip vadinamu G. Kantoro įstrižainės metodu.

Tarkime, kad $A$ ir $\mathbf{P}(A)$ yra ekvivalenčios. Vadinasi, egzistuoja bijekcija $f : A \to \mathbf{P}(A)$. Apibrėžkime aibę $X =: \{x \in A | x \notin f(x)\}$. Taigi $X \subset A$, t. y. $X \in \mathbf{P}(A)$, o $f^{-1}(X)$ yra aibės $A$ elementas. Pažymėkime $a = f^{-1}(X)$. Išsiaiškinkime, ar $a \in X$, ar $a \notin X$. Jei $a \in X = f(a)$, tai, pagal aibės $X$ apibrėžimą, gauname, kad $a \notin f(a) = X$. Jei $a \notin X$, tai vėl, remdamiesi aibės $X$ apibrėžimu, gauname, kad $a \in X$. Vadinasi, prielaida, kad aibės $A$ ir $\mathbf{P}(A)$ yra ekvivalenčios, prieštaringa.

G. Kantoro įstrižainės metodu įrodoma, kad natūraliųjų skaičių aibė $\mathbb{N}$ ir realiųjų skaičių intervalas $\{x \in \mathbb{R} | 0 < x < 1\}$ nėra ekvivalenčios aibės, kitaip tariant, realiųjų skaičių intervalas $\{x \in \mathbb{R} | 0 < x < 1\}$ ( vadinasi, ir visų realiųjų skaičių aibė) nėra skaiti aibė (skaičia aibe yra vadinama aibė, ekvivalenti natūraliųjų skaičių aibei).

**Pratimai.**

1. Įrodykite: jei $A$ ir $B$ yra baigtinės aibės, tai $|A^B| = |A|^{|B|}$.

2. Įrodykite: jei $A$ ir $B$ yra baigtinės aibės, tai $|A \times B| = |A||B|$.

3. Įrodykite: aibės $(A^B)^C$ ir $A^{B \times C}$ yra ekvivalenčios.

Jei $A$, $B$, $C$ yra baigtinės aibės, tai, remiantis 1-uoju ir 2-uoju pratimais, akivaizdu, kad $\left|(A^B)^C\right| = \left|A^{B \times C}\right|$. Šiuo atveju matome, kad aibės $(A^B)^C$ ir $A^{B \times C}$ yra ekvivalenčios. Bendruoju atveju pasinaudokite nurodymu: jei $f \in (A^B)^C$, tai kiekvienam $c \in C$, $f(c) \in A^B$, t. y. bet kuriems $c \in Cirb \in B$, $(f(c))(b) \in A$. Tuomet atvaizdžiui $f$ priskirkite atvaizdį $\tilde{f} \in A^{B \times C}$, apibrėžiamą lygybe: $\tilde{f}(b, c) = (f(c))(b)$. Įsitikinkite, kad atvaizdis

$$(A^B)^C \ni f \to \tilde{f} \in A^{B \times C}$$

yra bijekcija.

**3. 12. Aibė $\mathcal{A}utA$.** Visų bijekcijų $f : A \to A$ aibę žymėsime $\mathcal{A}utA$. Akivaizdu, kad:

1. $f, g \in \mathcal{A}utA \Longrightarrow f \circ g \in \mathcal{A}utA$ (žr.[ 2. 19.]);

2. $\mathrm{id} \in \mathcal{A}utA$ (atvaizdis id apibrėžiamas taip: $\mathrm{id} : A \to A$, $\mathrm{id}(a) = a$, $a \in A$. Įsitikinkite, kad $f \circ \subset d = \mathrm{id} \circ f = f$, $f \in \mathcal{A}utA$;

3. $f \in \mathcal{A}utA \Longrightarrow f^{-1} \in \mathcal{A}utA$, $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$.

## 4. Ekvivalentumo sąryšis. Faktoraibė

**4. 1. Ekvivalentumo sąryšio apibrėžimas.** Aibės $A \times A$ poaibis $R$ yra vadinamas ekvivalentumo sąryšiu, apibrėžtu aibėje $A$, jei

1. Kiekvienam $a \in A$, $(a, a) \in R$ (sąryšio $R$ refleksyvumo savybė);
2. $(a, b) \in R \Longrightarrow (b, a) \in R$ (sąryšio $R$ simetriškumo savybė);
3. $(a, b) \in R, (b, c) \in R \Longrightarrow (a, c) \in R$ (sąryšio $R$ tranzityvumo savybė).

**Pastaba.** Ekvivalentumo sąryšį $R$, apibrėžtą aibėje $A$, paprastumo dėlei vadinsime ekvivalentumo sąryšiu aibėje $A$.

Ekvivalentumo sąryšį $R \subset A \times A$ aibėje $A$ galima apibrėžti ir taip:

1'. $\Delta(A) \subset R$, $\Delta(A) =: \{(a, a) | a \in A\}$ – aibės $A \times A$ poaibis, kuris yra vadinamas aibės $A \times A$ įstrižaine;

2'. $R = R^{-1}$ (žr. [ 2. 5.]);
3'. $R \circ R \subset R$ (žr. [ 2. 6.]).
Akivaizdu, kad $R \circ R = R$.

Aibės $A$ elementai $a$ ir $b$ yra susieti ekvivalentumo sąryšiu $R$, jei $(a, b) \in R$. Elementai $a, b \in A$, susieti ekvivalentumo sąryšiu $R$, yra vadinami ekvivalenčiais ir vietoje žymėjimų $aRb$ ar $(a, b) \in R$ yra naudojami tokie: $a \underset{R}{\sim} b$ arba $a \equiv b (\mathrm{mod}\ R)$.

Šiais naujais žymėjimais ekvivalentumo sąryšio $R$ aibėje $A$ savybės užrašomos taip: bet kuriems $a, b, c \in A$

1". $a \underset{R}{\sim} a$ arba $a \equiv a (\mathrm{mod}\ R)$;
2". $a \underset{R}{\sim} b \Longrightarrow b \underset{R}{\sim} a$ arba $a \equiv b (\mathrm{mod}\ R) \Longrightarrow b \equiv a (\mathrm{mod}\ R)$;
3". $a \underset{R}{\sim} b, b \underset{R}{\sim} c \Longrightarrow a \underset{R}{\sim} c$ arba $a \equiv b (\mathrm{mod}\ R), b \equiv c (\mathrm{mod}\ R) \Longrightarrow a \equiv c (\mathrm{mod}\ R)$.

**Pastaba.** Konkrečių ekvivalentumo sąryšių aibėse atvejais galimi ir kitokie žymėjimai.

**Pavyzdžiai.**

1. Tarkime, $A$ – netuščia aibė, $R = \Delta(A)$ – aibės $A \times A$ įstrižainė. $R$ yra ekvivalentumo sąryšis aibėje $A$ ir

$$a \underset{R}{\sim} b \Longleftrightarrow a = b.$$

Tai vienas iš dviejų kraštutinių atvejų.

2. Tarkime, $A$ – netuščia aibė, $R = A \times A$. $R$ yra ekvivalentumo sąryšis aibėje $A$ ir šiuo atveju bet kurie aibės $A$ elementai yra ekvivalentūs. Tai kitas kraštutinis atvejis.

3. Tarkime, $n$ – fiksuotas natūralusis skaičius, $n \geq 1$, $R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} |\ n|(a - b)\}$ (jei sveikasis skaičius $a$ dalija sveikąjį skaičių $b$, tai rašome $a|b$, jei $a$ nedalija skaičiaus $b$, tai rašome $a \not| b$). $R_n$ yra ekvivalentumo sąryšis aibėje $\mathbb{Z}$, nes bet kuriems $a, b, c \in \mathbb{Z}$, $R_n$ tenkina ekvivalentumo sąryšio apibrėžimo sąlygas:

1. $a \underset{R_n}{\sim} a$, nes $n|(a - a) = 0$;
2. $a \underset{R_n}{\sim} b \Longrightarrow b \underset{R_n}{\sim} a$, nes, jei $n|(a - b)$, tai $n|(b - a)$ (kadangi $b - a = (-1)(a - b)$);
3. $a \underset{R_n}{\sim} b, b \underset{R_n}{\sim} c \Longrightarrow a \underset{R_n}{\sim} c$, nes, jei $n|(a - b), n|(b - c)$, tai $n|(a - c)$ (kadangi $a - c = (a - b) + (b - c)$).

Ekvivalentumo sąryšio $R_n$ aibėje $\mathbb{Z}$ atveju vietoje $a \underset{R_n}{\sim} b$ dažnai rašoma $a \equiv b (\mathrm{mod}\ n)$. Šį žymėjimą naudojo K. F. Gausas.

4. Tarkime, $A$ – plokštumos $\mathbb{R}^2$ visų tiesių aibė. Tegu $R = \{(a, b) \in A \times A |\ a||b\}$, čia $a||b$ žymi, kad tiesės $a$ ir $b$ yra lygiagrečios. Tiesės $a$ ir $b$ yra lygiagrečios pagal apibrėžimą, jei $a = b$ arba $a$ ir $b$ neturi bendrų taškų. Akivaizdu, kad $R$ yra ekvivalentumo sąryšis aibėje $A$.

5. Tarkime, kad $A$ – plokštumoje $\mathbb{R}^2$ visų trikampių aibė,

$$R = \{(a, b) \in A \times A \mid \text{ plotas a=plotui b}\},$$

$R$ – ekvivalentumo sąryšis aibėje $A$.

6. Tarkime, kad $A$ – plokštumoje $\mathbb{R}^2$ visų trikampių aibė,

$$R = \{(a, b) \in A \times A | \ a \sim b\},$$

čia $a \sim b$ žymi, kad trikampis $a$ yra panašus trikampiui $b$. Akivaizdu, kad $R$ yra ekvivalentumo sąryšis.

**4. 2. Ekvivalentumo klasės apibrėžimas.** Tarkime, $R$ yra ekvivalentumo sąryšis aibėje $A$. Elemento $a \in A$ ekvivalentumo klase $R$ atžvilgiu yra vadinamas aibės $A$ poaibis $\{x \in A | \ x \underset{R}{\sim} a\}$, sudarytas iš aibės $A$ elementų, ekvivalenčių elementui $a$ ir yra žymimas $a(\text{mod } R)$.

Remdamiesi ekvivalentumo sąryšio apibrėžimu, gauname:

1. Jei $x, y \in a(\text{mod } R)$, tai $x$ ir $y$ yra ekvivalentūs. Matematinių simbolių žymėjimais šis teiginys yra užrašomas taip:

$$x, y \in a(\text{mod } R) \Longrightarrow x \equiv y(\text{mod } R).$$

Iš tikrųjų, jei $x, y \in a(\text{mod } R)$, tai $x \equiv a(\text{mod } R)$, $y \equiv a(\text{mod } R)$, t. y. $x \equiv a(\text{mod } R)$, $a \equiv y(\text{mod } R)$. Taigi ir $x \equiv y(\text{mod } R)$.

2. Jei $x \equiv y(\text{mod } R)$ ir $y \in a(\text{mod } R)$, tai ir $x \in a(\text{mod } R)$. Matematinių simbolių žymėjimais šis teiginys užrašomas taip:

$$x \equiv y(\text{mod } R), y \in a(\text{mod } R) \Longrightarrow x \in a(\text{mod } R).$$

Dabar įrodysime vieną iš svarbiausių aibės $A$ elementų ekvivalentuno klasių savybių.

**Teiginys.** Tarkime, $R$ yra ekvivalentumo sąryšis aibėje $A$. Tuomet aibės $A$ elementų $a$ ir $b$ ekvivalentumo klasės $a(\text{mod } R)$ ir $b(\text{mod } R)$ arba sutampa arba neturi bendrų elementų.

**Įrodymas.** Jei $a(\text{mod } R) \cap b(\text{mod } R) = \emptyset$, tai teiginys įrodytas. Tarkime, kad $c \in a(\text{mod } R) \cap b(\text{mod } R)$. Tuomet $c \in a(\text{mod } R)$, $c \in b(\text{mod } R)$. Remdamiesi 2-ąja ir 3-iąja ekvivalentumo sąryšio apibrėžimo savybėmis, gauname, kad $a \equiv b(\text{mod } R)$.

Jei $x \in a(\text{mod } R)$, tai $x \equiv a(\text{mod } R)$. Kadangi $a \equiv b(\text{mod } R)$, tai, remiantis 3-iąja ekvivalentumo sąryšio apibrėžimo savybe, galima parašyti $x \equiv b(\text{mod } R)$. Kaip matome, jei $x \in a(\text{mod } R)$, tai $x \in b(\text{mod } R)$. Taigi $a(\text{mod } R) \subset b(\text{mod } R)$. Panašiai įrodoma, kad

$b(\mathrm{mod}\ R) \subset a(\mathrm{mod}\ R)$. Taigi, jei $a(\mathrm{mod}\ R) \cap b(\mathrm{mod}\ R) \neq \emptyset$, tai $a(\mathrm{mod}\ R) = b(\mathrm{mod}\ R)$. $\triangle$

**1. Išvada.** Tarkime, $R$ yra ekvivalentumo sąryšis aibėje $A$. Tuomet $a(\mathrm{mod}\ R) = b(\mathrm{mod}\ R)$ tada ir tik tada, kai $a \equiv b(\mathrm{mod}\ R)$.

**2. Išvada.** Tarkime, $R$ yra ekvivalentumo sąryšis aibėje $A$. Jei $x \in a(\mathrm{mod}\ R)$, tai $x(\mathrm{mod}\ R) = a(\mathrm{mod}\ R)$.

**4. 3.** Jei $R$ ekvivalentumo sąryšis aibėje $A$, tai skirtingos aibės $A$ elementų ekvivalentumo klasės suskaido aibę $A$ į netuščius, neturinčius bendrų elementų poaibius. Iš tikrųjų, kiekvienas aibės $A$ elementas $a$ patenka tik į vieną ekvivalentumo klasę $a(\mathrm{mod}\ R)$, o skirtingos elementų ekvivalentumo klasės neturi bendrų elementų.

**Teiginys.** Kiekvienam netuščios aibės $A$ skaidiniui netuščiais, neturinčiais bendrų elementų, poaibiais egzistuoja toks ekvivalentumo sąryšis aibėje $A$, kad aibės $A$ elementų ekvivalentumo klasės sutampa su aibės $A$ skaidinio poaibiais.

**Įrodymas.** Sakykime, kad $A = \bigcup\limits_{\alpha \in I} A_\alpha$ yra aibės $A$ skaidinys netuščiais, neturinčiais bendrų elementų, poaibiais $A_\alpha$, $\alpha \in I$, t. y., kiekvienam $\alpha \in I$, $A_\alpha \neq \emptyset$ ir jei $\alpha \neq \beta$, $\alpha, \beta \in I$, tai $A_\alpha \cap A_\beta = \emptyset$. Apibrėžkime sąryšį $R$ aibėje $A$ taip: $a \underset{R}{\sim} b$ tada ir tik tada, kai ezistuoja toks $\alpha \in I$, kad $a, b \in A_\alpha$. Remdamiesi $R$ apibrėžimu, matome:

1. Kiekvienam $a \in A$, $a \underset{R}{\sim} a$;
2. Jei $a \underset{R}{\sim} b$, tai $b \underset{R}{\sim} a$;
3. Jei $a \underset{R}{\sim} b$, $b \underset{R}{\sim} c$, tai $a \underset{R}{\sim} c$.

Taigi $R$ yra ekvivalentumo sąryšis aibėje $A$. Be to, akivaizdu, kad aibės $A$ elemento $a$ ekvivalentumo klasė yra $A_\alpha$, jei $a \in A_\alpha$. $\triangle$

**4. 4.** Yra glaudus ryšys tarp ekvivalentumo sąryšių $R$ aibėje $A$ ir siurjekcijų $f : A \to B$.

Sakykime, kad $f : A \to B$ – siurjekcija. Tuomet $A = \bigcup\limits_{b \in B} f^{-1}(b)$ yra aibės $A$ skaidinys netuščiais, neturinčiais bendrų elementų, poaibiais. Toks skaidinys, kaip įrodėme (žr.[4. 3.]), apibrėžia ekvivalentumo sąryšį aibėje $A$.

Sakykime, kad $R$ – ekvivalentumo sąryšis aibėje $A$, $A = \bigcup\limits_{\alpha \in I} A_\alpha$ – aibės $A$ skaidinys aibės $A$ elementų ekvivalentumo klasėmis, t. y. kiekvienam $\alpha \in I$, $A_\alpha \neq \emptyset$ ir jei $\alpha \neq \beta$, $\alpha, \beta \in I$, tai $A_\alpha \cap A_\beta = \emptyset$, $A_\alpha$, $\alpha \in I$ – aibės $A$ elementų ekvivalentumo klasės. Tuomet atvaizdis $f : A \to B$, $B = \{A_\alpha \mid \alpha \in I\}$, $f(a) = A_\alpha$, jei $a \in A_\alpha$, yra siurjekcija.

**4. 5. Faktoraibės apibrėžimas.** Tarkime, kad $R$ – ekvivalentumo sąryšis aibėje $A$, $A = \bigcup\limits_{\alpha \in I} A_\alpha$ – aibės $A$ skaidinys skirtingomis aibės $A$ elementų ekvivalentumo klasėmis. Aibė $\{A_\alpha \mid \alpha \in I\}$, kurios elementai yra aibės $A$ elementų ekvivalentumo klasės, yra vadinama aibės $A$ faktoraibe pagal ekvivalentumo sąryšį $R$ ir yra žymima $A/R$. Egzistuoja kanoninė siurjekcija $j : A \to A/R$, $j(a) = A_\alpha$, jei $a \in A_\alpha \subset A$, $\alpha \in I$, t. y. atvaizdis $j$ kiekvienam aibės $A$ elementui $a$ priskiria šio elemento ekvivalentumo klasę, – faktoraibės $A/R$ elementą $A_\alpha$.

**Pavyzdžiai.**

1. Jei $A \neq \emptyset$, $R = \Delta(A) = \{(a, a) \mid a \in A\}$ – aibės $A \times A$ įstrižainė, tai $A/R = A$.

2. Jei $A \neq \emptyset$, $R = A \times A$, tai $A/R = \{A\}$ – aibė, sudaryta iš vieno elemento $A$.

3. Jei $A = \mathbb{Z}$, $R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid n|(a - b)\}$, $n$ – sveikasis teigiamas skaičius, $n \geq 1$, [žr.4. 1., 3 pvz.], tai aibės $\mathbb{Z}$ elemento $i$ ekvivalentumo klasė yra $i + n\mathbb{Z} = \{i + nl \mid l \in \mathbb{Z}\}$. K. F. Gauso žymėjimais ekvivalentumo klasė $i + n\mathbb{Z}$ yra žymima $i(\text{mod } n)$. Priminsime, kad $i + n\mathbb{Z} = j + n\mathbb{Z}$ tada ir tik tada, kai $n|(i - j)$. Faktoraibė $\mathbb{Z}/R_n$ yra dar žymima $Z_n$ arba $\mathbb{Z}/n\mathbb{Z}$. Taigi $Z_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$.

4. $A = \mathbb{R}^2 = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\}$. Apibrėžkime ekvivalentumo sąryšį $R$ aibėje $\mathbb{R}^2$: $(\alpha, \beta) \underset{R}{\sim} (\gamma, \delta)$ tada ir tik tada, kai $\alpha^2 + \beta^2 = \gamma^2 + \delta^2$. Aibės $\mathbb{R}^2$ elementų ekvivalentumo klasės yra apskritimai plokštumoje $\mathbb{R}^2$, kurių centrai koordinačių pradžioje $(0, 0)$ ir taškas $(0, 0)$. Faktoraibė $A/R$ ekvivalenti aibei $\mathbb{R}_+ = \{\alpha \mid \alpha \geq 0\}$. Tai įrodoma taip: apibrėžiame siurjekciją $f : \mathbb{R}^2 \to \mathbb{R}_+$, $f((\alpha, \beta)) = \alpha^2 + \beta^2$. Tuomet $\mathbb{R}^2 = \bigcup\limits_{r \geq 0} f^{-1}(r)$, $f^{-1}(r)$ – spindulio $r \geq 0$ apskritimas, kurio centras yra taške $(0, 0)$. Atvaizdis $f$ generuoja bijekciją $\bar{f} : \mathbb{R}^2/R \to \mathbb{R}_+$, $\bar{f}(f^{-1}(r)) = r$, $r \geq 0$.

**4. 6.** Tarkime, kad $R$ ekvivalentumo sąryšis aibėje $A$, $f : A \to B$ – toks atvaizdis, kad $f(a) = f(b)$, kai $a(\text{mod } R) = b(\text{mod } R)$. Tuomet egzistuoja toks atvaizdis $\bar{f} : A/R \to B$, kad diagrama

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "j"'] & & B \\ & A/R \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

yra komutatyvi, t. y., kiekvienam $a \in A$, $f(a) = (\bar{f} \circ j)(a)$. Atvaizdį $\bar{f} : A/R \to B$ apibrėžkime taip:

$$\bar{f}(a(\text{mod } R)) =: f(a), \quad a \in A.$$

Atvaizdis $\bar{f}$ apibrėžtas korektiškai. Įsitikinkite, kad atvaizdis $\bar{f}$ tenkina anksčiau suformuluotą savybę.

## 5. Tvarkos sąryšiai. Sutvarkytosios aibės

**5. 1. Tvarkos sąryšio apibrėžimas.** Binarusis sąryšis $R$ yra vadinamas antirefleksyviuoju tvarkos sąryšiu, jei

1. $(a, b) \in R \Longrightarrow (b, a) \notin R$;
2. $(a, b), (b, c) \in R \Longrightarrow (a, c) \in R$.

Pastebėsime, kad $(a, a) \notin R$.

**Apibrėžimas.** Aibė $A$ yra vadinama antirefleksyviai sutvarkytąja aibe antirefleksyviojo tvarkos sąryšio $R$ atžvilgiu, jei $A \subset D(R) \cup E(R)$. Čia $D(R), E(R)$ – sąryšio $R$ apibrėžimo ir reikšmių sritys. Sutvarkytoji tvarkos sąryšio $R$ atžvilgiu aibė yra žynima $(A, R)$, o tvarkos sąryšis $R$ dažnai yra vadinamas tvarka aibėje $A$.

**Apibrėžimas.** Aibė $A$ yra vadinama antirefleksyviai sutvarkytąja aibe sąryšio $R \subset A \times A$ atžvilgiu, jei

1. $(a, b) \in R \Longrightarrow (b, a) \notin R$;
2. $(a, b), (b, c) \in R \Longrightarrow (a, c) \in R$.

Sutvarkytoji aibė $R$ atžvilgiu aibė yra žynima $(A, R)$, o sąryšis $R$ dažnai yra vadinamas tvarka aibėje $A$.

**Pastabos.**

1. Jei $(A, R)$ antirefleksyviai sutvarkytoji aibė, tai dažnai vietoje $R$ rašoma $<$.

2. Antirefleksyviai sutvarkytąją aibę $(A, R)$ atitinka refleksyviai sutvarkytoji aibė $(A, R')$, čia $R' =: R \cup \Delta(A)$, $\Delta(A) = \{(a, a) \mid a \in A\}$. Teisingas ir toks teiginys: kiekvieną refleksyviai sutvarkytąją aibę $(A, R')$ atitinka antirefleksyviai sutvarkutoji aibė $(A, R)$, čia $R =: R' \setminus \Delta(A)$. Dažnai vietoje refleksyviojo sąryšio žymėjimo $R'$ yra rašoma $\leq$.

3. Jei $B$ yra refleksyviai ar antirefleksyviai sutvarkytosios aibės $(A, R)$ poaibis, tai $B$ yra taip pat refleksyviai ar antirefleksyviai sutvarkytoji tvarkos sąryšio $R$ atžvilgiu aibė. Dažnai rašoma, kad tvarkos sąryšis $R$ aibėje $A$ indukuoja tvarkos sąryšį aibės $A$ poaibyje $B$.

Nagrinėsime tik refleksyviai sutvarkytąsias aibes $(A, R)$.

**Pavyzdžiai.**

1. Sakykime, $A$ – netuščia aibė, $\mathbf{P}(A)$ – aibės $A$ visų poaibių aibė. Aibė $\mathbf{P}(A)$ aibių įdėties sąryšio $\subset$ atžvilgiu yra sutvarkytoji aibė.

2. Aibės $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sąryšio $\leq$ atžvilgiu yra sutvarkytosios aibės.

3. Aibė $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ dalybos sąryšio $\mid$ atžvilgiu yra sutvarkytoji aibė.

4. Aibė $\{a, b, c\}$ sąryšio $R = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}$ atžvilgiu yra sutvarkytoji aibė.

5. Aibė $\{a, b, c, d, e, f\}$ sąryšio

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, c), (b, c), (c, d),$$

$$(c, e), (a, d), (a, e), (b, d), (b, e), (a, f), (b, f), (c, f), (d, f), (e, f)\}$$

atžvilgiu yra sutvarkytoji aibė.

Pasitelkę ženklą "$\leq$", tvarkos sąryšį $R$ dar galime ir taip apibūdinti:

$$a \leq c \leq d \leq f, \quad b \leq c \leq e \leq f.$$

Sakykime, $(A, R)$ – sutvarkytoji aibė. Aibės $A$ elementai yra vadinami palyginamais, jei $(a, b)$ ar $(b, a)$ priklauso sąryšiui $R$. Kaip žinome, jei $a \neq b$, tai tik vienas iš dviejų sutvarkytųjų dvejetų $(a, b)$ ar $(b, a)$ gali priklausyti $R$. Refleksyviai sutvarkytosios aibės $(A, R)$ atveju $(a, b) \in R$ ir $(b, a) \in R$ tada ir tik tada, kai $a = b$. Bendruoju atveju sutvarkytoje aibėje $(A, R)$ yra nepalyginamų elementų. Pavyzdžiui, trečiajame pavyzdyje 2 ir 3 nepalyginami, nes $2 \not| 3$(t. y. 2 nedalija 3).

**5. 2. Tiesiškai ir visiškai sutvarkytosios aibės.**

**Apibrėžimas.** Sutvarkytoji aibė $(A, R)$ yra vadinama tiesiškai sutvarkyta aibe, jei bet kurie aibės $A$ elementai yra palyginami. Kitaip tariant, bet kuriems aibės $A$ elementams $a$ ir $b$, vienas ir tik vienas iš dviejų sutvarkytųjų dvejetų $(a, b)$ ir $(b, a)$ būtinai priklauso $R$.

**Pavyzdžiai.**

1. Sutvarkytosios aibės $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ yra tiesiškai sutvarkytos aibės.

2. Sutvarkytoji aibė $(\mathbf{P}(A), \subset)$, čia $A$ – netuščia aibė, nėra tiesiškai sutvarkyta aibė.

**Apibrėžimas.** Sutvarkytosios aibės $(A, \leq)$ elementas $a$ yra vadinamas maksimaliuoju, jei neegzistuoja toks aibės $A$ elementas $b$, kad $b \neq a$ ir $a \leq b$. Panašiai galima apibrėžti sutvarkytosios aibės $(A, \leq)$ minimalųjį elementą.

**Pavyzdžiai.**

1. Sutvarkytose aibėse $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ neegzistuoja nei vieno maksimalaus, nei vieno minimalus elemento.

2. Sutvarkytoje aibėje $(\mathbb{N}, \leq)$ egzistuoja minimalus elementas 0, bet neegzistuoja nei vieno maksimalaus elemento.

3. Sutvarkytoje aibėje $(\{a, b, c\}, R)$, čia $R = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}$ egzistuoja du maksimalūs elementai $b$ ir $c$ ir vienas minimalus elementas $a$.

4. Sutvarkytoje aibėje $(\{a, b, c, d, e\}, R)$, čia

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (b, c), (c, d), (c, e), (a, d), (a, e), (b, d), (b, e)\}$$

egzistuoja du maksimalūs elementai $d$ ir $e$ ir du minimalūs elementais $a$ ir $b$.

5. Sutvarkytoje aibėje $(\{a, b, c, d, e, f\}, R)$, čia

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, c), (b, c), (c, d),$$

$$(c, e), (a, d), (a, e), (b, d), (b, e), (a, f), (b, f), (c, f), (d, f), (e, f)\},$$

egzistuoja vienas maksimalus elementas $e$ ir du minimalūs elementai $a$ ir $b$.

**Apibrėžimas.** Sutvarkytosios aibės $(A, \leq)$ elementas $a$ yra vadinamas galiniu, jei kiekvienam aibės elementui $b$, $b \leq a$.

**Pastaba.** Akivaizdu, kad sutvarkytosios aibės $(A, \leq)$ galinis elementas yra šios aibės vienintelis maksimalus elementas. Teisingas ir atvirkščias teiginys: jei sutvarkytoje aibėje $(A, \leq)$ egzistuoja vienintelis maksimalus elementas, tai jis yra ir galinis šios aibės elementas.

**Apibrėžimas.** Sutvarkytosios aibės $(A, \leq)$ elementas $a$ yra vadinamas pradiniu, jei kiekvienam aibės elementui $b$, $a \leq b$.

Akivaizdu, kad sutvarkytosios aibės $(A, \leq)$ pradinis elementas yra šios aibė vienintelis mminimalus elementas. Teisingas ir atvirkščias teiginys: jei sutvarkytoje aibėje $(A, \leq)$ egzistuoja vienintelis mminimalus elementas, tai jis yra ir pradinis šios aibės elementas.

**Apibrėžimas.** Sutvarkytosios aibės $(A, \leq)$ poaibis $B$ yra vadinamas aprėžtu iš viršaus, jei egzistuoja toks aibės $A$ elementas $a$, kad kiekvienam poaibio $B$ elementui $b$, $b \leq a$. Panašiai galima suformuluoti poaibio, aprėžto iš apačios, apibrėžimą.

**Apibrėžimas.** Tiesiškai sutvarkyta aibė $(A, \leq)$ yra vadinama visiškai sutvarkyta, jei kiekvienas šios aibės poaibis indukuotos tvarkos atžvilgiu turi minimalų elementą.

Suformuluosime aibių teorijoje svarbią aksiomą, vadinamą ėmimo, parinkimo arba Cermelo aksioma, o taip pat Cermelo teoremą ir Corno lemą.

**Cermelo aksioma.** Sakykime, $\{X_\alpha\}_{\alpha \in I}$ – netuščių aibių šeima, kurios aibės su skirtingais indeksais neturi bendrų elementų. Tuomet egzistuoja tokia aibė $A$, kuri su kiekviena duotos aibių šeimos aibe turi vieną ir tik vieną bendrą elementą.

Ši Cermelo aksioma ekvivalenti ir kitaip formuluojamam teiginiui.

**Teorema.** Tegu $\{X_\alpha\}_{\alpha \in I}$ – netuščių aibių šeima. Tuomet šios aibių šeimos sandauga $\prod\limits_{\alpha \in I} X_\alpha$ – netuščia aibė.

**Cermelo teorema.** Kiekvienoje netuščioje aibėje $A$ galima apibrėti tvarką $R$, kurios atžvilgiu $A$ yra visiškai sutvarkyta aibė.

**5. 3. Corno lema.** Tarkime, $(A, \leq)$ – sutvarkytoji aibė. Jei kiekvienas aibės $A$ indukuotos tvarkos atžvilgiu tiesiškai sutvarkytas poaibis yra aprėžtas iš viršaus, tai aibėje $A$ egzistuoja bent vienas maksimalus aibės $A$ elementas.

Analogiškai galima performuluoti sąlygą taip, kad būtume tikri, jog sutvarkytoje aibėje $(A, \leq)$ egzistuoja bent vienas minimalus elementas.

Cermelo aksioma sukėlė daug diskusijų ir konstruktyviosios matematikos atstovams yra nepriimtina. Bet be Cermelo aksiomos nebūtų galima įrodyti, pavyzdžiui, daug matematinės analizės svarbių faktų.

Cermelo aksioma, Cermelo teorema, suformuluotoji teorema apie netuščių aibių šeimos sankirtą ir Corno lema yra Cermelo-Frenkelio aibių teorijos sistemoje ekvivalentūs teiginiai. Vieną iš šių teiginių priėmę kaip aksiomą, kitus tris teiginius galima įrodyti kaip teoremas. Šių teiginių čia surašyti pavadinimai susiformavo istoriškai ir tokie išliko. Algebroje egzistencijos teoremoms įrodyti patogiausia remtis Corno lema. Vėliau, skyriuje, kuriame nagrinėjami žiedai, remdamiesi Corno lema, įrodysime, kad kiekviename komutatyviame žiede su vienetu egzistuoja maksimalus idealas (o kiekvienas maksimalus idealas yra ir pirminis). Taip pat, remdamiesi Corno lema, įrodysime, kad kiekvienoje tiesinėje erdvėje virš kūno $k$ egzistuoja bazė ir kiekvienam tiesinės erdvės tiesiniam poerdviui egzistuoja bent vienas papildomas tiesinis poerdvis. Remiantis Corno lema, funkcinėje analizėje įrodoma svarbi Chano-Banacho teorema apie pusnormės, apibrėžtos normuotos erdvės tiesiniame poerdvyje, pratęsimą į visą erdvę. Visų svarbių faktų, įrodomų remiantis Corno lema, neįmanoma suminėti.

**5. 4. Kryptinės aibės.**

**Apibrėžimas.** Sutvarkytoji aibė $(A, \leq)$ yra vadinama kryptine su kryptimi į dešinę, jei bet kuriems aibės $A$ elementams $a$ ir $b$ egzistuoja toks aibės $A$ elementas $c$, kad $a \leq c$, $b \leq c$.

Analogiškai galima apibrėžti kryptinės aibės su kryptimi į kairę sąvoką.

**Pavyzdžiai.**

1. Sutvarkytoji aibė $(A, \leq)$, kurioje egzistuoja galinis elementas, yra kryptinė aibė su kkryptimi į dešinę.

2. Sutvarkytosios aibės $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ yra kryptinės aibės su kryptimi tiek į dešinę, tiek į kairę.

3. Sutvarkytoji aibė $(\mathbf{P}(A), \subset)$ yra kryptinė aibė su kryptimi tiek į dešinę, tiek į kairę.

4. $I = [01]$ – uždaras intervalas. Parinkę šio intervalo taškus

$$0 = x_0 < x_1 < x_2 < \ldots < x_n = 1,$$

gauname intervalo $[0, 1]$ baigtinį skaidinį

$$[01] = \bigcup_{j=1}^{n} [x_{j-1} x_j],$$

kurį sutarkime žymėti $a = (I, \{x_0, x_1, \ldots, x_n\})$ Nagrinėkime intervalo $I$ visų baigtinių skaidinių aibę $A$. Aibėje $A$ apibrėžkime tvarkos sąryšį taip: jei

$$a = (I, \{x_0, x_1, \ldots, x_r\}),\ b = (I, \{y_0, y_1, \ldots, y_s\}),\ r, s \in \mathbb{N},$$

tai

$$a \leq b \Longleftrightarrow \{x_0, x_1, \ldots, x_r\} \subset \{y_0, y_1, \ldots, y_s\}.$$

Galite įsitikinti, kad $(A, \leq)$ kryptinė aibė su kryptimi į dešinę. Ši kryptinė aibė svarbi apibrėžiant Rymano integralą.

Kryptinės aibės svarbios apibrėžinant grupių, žiedų, modulių virš žiedų šeimų injektyvines ir projektyvines ribas.

**5. 5. Sutvarkytųjų aibių tipas.**

**Apibrėžimas.** Sakykime, $(A, \leq)$ ir $(B, \leq)$ – sutvarkytosios aibės. Atvaizdis $f : A \to B$ yra vadinamas monotoniniu, jei bet kuriems $a_1, a_2 \in A$, $a_1 \leq a_2$, $f(a_1) \leq f(a_2)$.

**Teiginys.** Jei $(A, \leq)$, $(B, \leq)$ ir $(C, \leq)$ – sutvarkytosios aibės, $f : A \to B$ ir $g : B \to C$ – monotoniniai atvaizdžiai, tai $g \circ f : A \to C$ yra monotoninis atvaizdis.

**Įrodymas.** Šio teiginio įrodymas akivaizdus.

**Apibrėžimas.** Sutvarkytosios aibės $(A, \leq)$ ir $(B, \leq)$ yra vadinamos vieno ir to paties tipo, jei egzistuoja tokia bijekcija $f : A \to B$, kad $f$ ir $f^{-1}$ monotoniniai atvaizdžiai.

**Pavyzdžiai.**

1. Sutvarkytosios aibės $(\mathbb{R}_+^*, \leq)$ ir $(\mathbb{R}, \leq)$ yra vieno ir to paties tipo. Iš tikrųjų, $\ln : \mathbb{R}_+^* \to \mathbb{R}$ – bijekcija ir bet kuriems $a, b \in \mathbb{R}_+^*$, $a \leq b$ tada ir tik tada, kai $\ln a \leq \ln b$.

2. Sutvarkytosios aibės $(\mathbb{Q}_+^*, \leq)$ ir $(\mathbb{Q}, \leq)$ yra vieno ir to paties tipo. Iš tikrųjų. Apibrėžkime atvaizdį $f : \mathbb{Q}_+^* \to \mathbb{Q}$ taip:

$$f(x) = \begin{cases} x - 1, & \text{jei} \quad\ \ x \geq 1, \\ -\frac{1}{x} + 1, & \text{jei } 0 < x \leq 1 \end{cases}.$$

$f$ – bijekcija, $f$, $f^{-1}$ – monotoniniai atvaizdžiai.

3. Sutvarkytosios aibės $(]-\frac{\pi}{2} \frac{\pi}{2}[, \leq)$ ir $(\mathbb{R}, \leq)$ yra vieno ir to paties tipo. $\mathrm{tg} : ]-\frac{\pi}{2} \frac{\pi}{2}[ \to \mathbb{R}$ – bijekcija ir bet kuriems $x, y \in ]-\frac{\pi}{2} \frac{\pi}{2}[$, $\mathrm{tgx} \leq \mathrm{tgy}$ tada ir tik tada, kai $x \leq y$.

4.Sutvarkytosios aibės $(-\mathbb{N}, \leq)$ ir $(\mathbb{N}, \leq)$, čia $-\mathbb{N} =: \{-n \mid n \in \mathbb{N}\}$, yra skirtingų tipų, nes sutvarkytoje aibėje $-\mathbb{N}$ egzistuoja galinis elementas, o sutvarkytoje aibėje $\mathbb{N}$ galinio elemento neegzistuoja.

**Apibrėžimas.** Tarkime, $(A, \leq)$ – sutvarkytoji aibė. Bijekcija $f : A \to A$ yra vadinama sutvarkytosios aibės $(A, \leq)$ automorfizmu, jei $f$, $f^{-1}$ – monotoniniai atvaizdžiai. Sutvarkytosios aibės $(A, \leq)$ visų automorfizmų aibę žymėsime $\mathcal{A}ut(A, \leq)$.

Aibėje $\mathcal{A}ut(A, \leq)$ apibrėžtas kompozicijos dėsnis $\circ$. Šis kompozicijos dėsnis tenkina sąlygas:

1. $\circ$ – asociatyvus kompozicijos dėsnis;
2. $\mathrm{id} \in \mathcal{A}ut(A, \leq)$;
3. $f \in \mathcal{A}ut(A, \leq) \Longrightarrow f^{-1} \in \mathcal{A}ut(A, \leq)$.

Aibė $\mathcal{A}ut(A, \leq)$ kompozicijos dėsnio $\circ$, tenkinančio išvardytas sąlygas, atžvilgiu yra vadinama grupė. Kitaip tariant, sutvarkytosios aibės automorfizmas, – tai tos aibės simetrija. Visos sutvarkytosios aibės simetrijos atvaizdžių kompozicijos atžvilgiu sudaro gupę. Vėliau grupes nagrinėsime detaliau.

## 6. Cermelo-Frenkelio aibių teorijos aksiomatika

Cermelo-Frenkelio aibių teorijos Z F sistema gali būti aprašoma štai taip. Ši sistema yra sudaryta iš kintamųjų $x, y, \ldots$, kuriais žymimos aibės, ir pirmykščio predikato $\in$, reiškiančio priklausomumo sąryšį ("priklauso"). Atomarinės formulės turi pavidalą: $x \in y$. Iš atomarinių formulių naudojant elementariosios logikos jungtis: $\Longrightarrow$ – implikaciją ("jei ..., tai ..."), $\urcorner$ – neigimą ("ne"), $\vee$ – disjunkciją ("arba"), $\wedge$ – konjunkciją ("ir") ir kvantorius: $\forall$ – bendrumo kvantorių ("kiekvienam"), $\exists$ – egzistavimo kvantorių ("egzistuoja") sudaromos kitos formulės ir teiginiai. Matematinėje logikoje užrašas "$\equiv$" žymi ekvivalentumą ("jei, ..., tai ... ir atvirkščiai"). Be to, priimamos elementariosios logikos aksiomos bei išvedimo taisyklės. Aibių teorijos Z F sistemos aksiomos yra sekančios:

Z F 1. Aibių lygumo aksioma. Šia aksioma teigiama, kad dvi aibės yra lygios, jei jos sudarytos iš vienų ir tų pačių elementų. Lygybės ženklas = pakeičia užrašą $(\forall z).(z \in x \equiv z \in y)$. Aksioma simbolių kalba užrašoma taip:

$$x = y \Longrightarrow (\forall w).(x \in w \Longrightarrow y \in w).$$

Z F 2. Sąjungos arba poros aksioma. Jei $x$ ir $y$ – aibės, tai $\{x, y\}$ taip pat yra aibė, t. y.

$$(\exists w).(\forall z).(z \in w \equiv (z = x \vee z = y)).$$

Z F 3. Išskyrimo aksioma. Kiekvienai aibei $z$ ir kiekvienai Z F sistemos formulei $F(x)$ egzistuoja aibės $z$ poaibis, kuriam priklauso tos ir tik tos aibės $x$, kurioms teisinga formulė $F(x)$. Simbolių kalba aksioma užrašoma taip:

$$(\forall z).(\exists y).(\forall x).(x \in y \equiv (x \in z \wedge F(x))),$$

čia $y$ neįeina į $F(x)$.

Z F 4. Poaibių aibės arba laipsnio aksioma. Kiekvienai aibei egzistuoja jos poaibių aibė:

$$(\forall z).(\exists y).(\forall x).(x \in y \equiv (\forall w).(w \in x \Longrightarrow w \in z)).$$

Z F 5. Sumos aksioma. Kiekvienai aibei egzistuoja aibė-suma:

$$(\forall z).(\exists y).(\forall x).(x \in y \equiv (\exists w).(x \in w \wedge w \in z)).$$

Z F 6. Cermelo arba parinkimo aksioma. Ši aksioma dar yra vadinama sandaugos aksioma. Jei $x$ – aibė, kurios elementai netuščios, neturinčios bendrų elementų aibės, tai jos aibė-suma turi bent vieną poaibį, kuris su kiekvienu $x$ elementu turi tik vieną bendrą elementą:

$$(\forall x).\Big((\forall y).(\forall z).((y \in x \wedge z \in x) \Longrightarrow$$

$$\Longrightarrow \big((\exists w).w \in y \wedge \urcorner(\exists w).(w \in y \wedge w \in z)\big)) \Longrightarrow$$

$$\Longrightarrow (\exists u).(\forall y).(y \in x \Longrightarrow (\exists v).(\forall t).\big(t = v \equiv (t \in u \wedge t \in y))\big)\Big).$$

Z F 7. Begalybės aksioma. Egzistuoja aibė, kuriai priklauso tuščia aibė ir kurios kiekvienam elementui $x$ aibė $\{x\}$, sudaryta iš vieno elemento, taip pat priklauso jai. Simbolių kalba aksioma atrodo taip:

$$(\exists z).\big(\emptyset \in z \wedge (\forall x).(x \in z \Longrightarrow \{x\} \in z)\big).$$

Z F 8. Apribojimo aksioma. Kiekvienam tokiai Z F sistemos formulei $F(x)$, kad $(\exists x)F(x)$, egzistuoja tokia aibė $y$, kad $F(y)$ teisinga, bet nei vienam jos elementui (daliai[?]) $z$ $F(z)$ nėra teisinga. Simbolių kalba:

$$(\exists x).F(x) \Longrightarrow (\exists y).(F(y) \wedge (\forall z)\urcorner\big(z \in y \wedge F(z)\big)).$$

.

Z F 9. Pakeitimo aksioma. Jei tarp dviejų klasių yra abipus vienreikšmė atitinkamybė ir viena iš šių klasių yra aibė, tai ir kita klasė yra aibė. Simbolių kalba:

$$(\forall x).(\forall y).(\forall w).(\big(F(x,y) \wedge F(z,w)\big) \Longrightarrow \big((x = z) \equiv (y = w)\big)).$$

Šioje Z F aibių teorijos sistemoje galima įrodyti, kad egzistuoja vienintelė natūraliųjų skaičių aibė, tenkinanti Peano aksiomas. Po to galima apibrėžti racionaliųjų skaičių aibę ir Dedekindo piūviais – realiųjų skaičių aibę.

Bet ši Z F aibių teorijos sistemos kalba formali. Norint suteikti šiai kalbai prasmę, būtina nagrinėti šios aksiomų sistemos interpretaciją. Pirmiausia, pasirodo, kad ši aksiomų sistema turi be galo daug interpretacijų. Kita vertus, egzistuoja tokios interpretacijos, kuriose natūraliųjų skaičių aibės, žiūrint iš išorės, nėra ekvivalenčios tarpusavy ir nėra ekvivalenčios intuityviai suvokiamai natūraliųjų skaičių aibei. Taigi susidarė nepaprastai įdomi situacija. Kolkas nėra žinoma nei viena aibių teorijos aksiomų sistema, kuri turėtų vienintelę interpretaciją ir kuri būtų tiek galinga, kad jos terminais būtų galima suformuluoti šiuolaikinės matematikos teorijas.

## AIBIŲ TEORIJOS RAIDOS TRUMPA APŽVALGA

G. Kantoras (Georg Cantor, 1845–1918), tyrinėdamas trigonometrines eilutes, 1872 m. pabandė klasifikuoti trigonometrinių eilučių teorijoje nagrinėjamas "ypatingas" aibes. Taip pradėjęs tyrinėti aibes, G. Kantoras 1872–1897 m. m. sukūrė aibių teoriją.

Paprastomis aibių teorijos sąvokomis, kaip elemento priklausomumo visumai (aibei), visumos dalis , visumos dalių bendra dalis ir panašiai, matematikai ir filosofai visais laikais naudojosi sąmoningai. Šios sąvokos suvokiamos intuityviai ir dėl jų nebuvo diskutuojama. Todėl nesukėlė jokių diskusijų ir aibės apibrėžimas, kurį pateikė G. Kantoras: aibę suprasime kaip objektų, kuriuos vieną nuo kito gerai galime atskirti savo intuicija arba mintimis, sujungimą į vieną visumą.

Nepapratai svarbus G. Kantoro atradimas – tai visiškai sutvarkytosios aibės. Remdamasis visiškai sutvarkytų aibių teorija, jis išvystė kardinalinių skaičių aritmetiką, suformulavo transfiničiosios indukcijos principą (tai matematinės indukcijos principo apibendrinimas) ir kontinuumo hipotezę. Be to, G. Kantoras yra bendrosios topologijos ir mato teorijos pradininkas. Visi šie atradimai, dėl kurių G. Kantoras ir yra vadinamas aibių teorijos kūrėju, matematikoje pasirodė pirmą kartą

Aibių teorija, kurią kūrė G. Kantoras, atrodė labai keistai to laiko matematikos požiūriu. Nors įrodymai ir griežti, bet rezultatai neįtikėtini ir keisti. Iki to laiko nieko panašaus matematikoje nebuvo. Todėl daugelis to laiko žymių matematikų aibių teorijos nepripažino. Ypač aštriai šią teoriją kritikavo L. Kronekeris (Leopold Kronecker, 1823–1891). Tik K. Veijerštrasas (Carl Weierstrass, 1815–1897) gana palankiai vertino savo mokinio veiklą. Bet palaipsniui aibių teorija buvo pradėta taikyti daugelyje matematikos sričių, XIX a. pabaigoje taikymų susilaukė transfiničiosios indukcijos principas, o po 1904 m. įrodytos E. Cermelo (E. Zermelo, 1871–1953) įžymiosios teoremos (kiekvienoje aibėje galima apibrėžti visiškai sutvarkytosios aibės struktūrą) transfiničiosios indukcijos principas tapo svarbiu visose šiuolaikinės matematikos srityse.

Kai aibių teorija tapo šiuolaikinės matematikos pagrindu, joje buvo aptikti paradoksai, kurie sukrėtė šiuos pagrindus.

Štai Bertrano Raselo (Bertrand Russell, 1872 – ?) paradoksas, paprasčiausias iš žinomų paradoksų: pažymėkime $C$ visų aibių, nesančių pačios savęs elementu, visumą. Tarę, kad $C$ yra aibė, pabandykime išsiaiškinti, ar $C$ yra $C$ elementas, ar ne? Jei $C$ yra $C$ elementas, tai $C$ nepriklauso $C$ pagal $C$ apibrėžimą. Jei $C$ nėra $C$ elementas, tai $C$ priklauso $C$ pagal $C$ apibrėžimą. Kaip matome, iš tikrųjų paprastas paradoksas.

Šis paradoksas rodo, kad aibės apibrėžimas, pagrįstas intuicija, nėra korektiškas, o intuicija besąlygiškai pasitikėti negalima. Jau B. Bolcano (B. Bolzano, 1781–1848) ir K. Veijerštrasas anksčiau buvo sukonstravę tolydžių funkcijų, nediferencijuojamų nei viename taške, pavyzdžius, rodančius, kad remiantis vien tik intuicija galima labai klysti. Taigi aibių teoriją reikėjo peržiūrėti ir griežtai pagrįsti.

Matematikai, norėdami išvengti paradoksų ir išsaugoti G. Kantoro aibių teorijos laimėjimus, stengėsi aibių teoriją pagrįsti aksiomatiškai. Taip buvo sukurtos įvairios aibių teorijos sistemos: Raselo tipų teorija (1908), Cermelo (1908), Cermelo-Frenkelio (1922), Noimano-Bernaiso (1925, 1937, 1941–1943), Bernaiso-Giodelio (1940) sistemos, Kuaino "Naujieji pagrindai". Labiausiai pritaikytos šiuolaikinės matematikos tikslams – tai Cermelo-Frenkelio ir Bernaiso-Giodelio aibių teorijų sistemos.

Kuriant matematinę teoriją aksiomatiškai, iškyla vienas iš fundamentaliausių klausimų: kaip įrodyti, kad aksiomatiškai grindžiama teorija yra neprieštaringa? Į šį klausimą atsakymas yra žinomas, jei kalbama ne apie aibių, o apie kurią nors kitą matematinę teoriją, grindžiamą aksiomatiškai. Norint įrodyti aksiomatiškai grindžiamos teorijos neprieštaringumą, reikia nurodyti matematinį modelį, tenkinantį duotą aksiomų sistemą. Matematinių modelių, tenkinančių duotas aksiomų sistemas, konstravimas, kiek yra žinoma, atliekamas aibių teorijos terminais. Jei kalbama apie aibių teoriją, grindžiamą aksiomų sistema, tai šios teorijos neprieštaringumui įrodyti šis kelias netinkamas. Jei pabandytume taip išspręsti aibių teorijos, grindžiamos aksiomatiškai, neprieštaringumą, patektume į užburtą ratą: aibių teorijos terminais konstruotume modelį aibių teorijos neprieštaringumui įrodyti.

D. Hilbertas pasiūlė programą šiam sudėtingam klausimui išspręsti. Aibių bei kitų matematinių teorijų nepaprastai sudėtinga semantika. Jis pasiūlė formalizuoti aksiomatiškai kuriamą teoriją, t. y. atsisakyti aiškinti matematinių simbolių, naudojamų aksiomų sistemoje, prasmę, o jų savybes grįsti tik aksiomomis ir apibrėžti taisykles, kaip jais operuoti. Remiantis logikos išvedimo taisyklėmis ir aksiomomis, formaliai įrodytos teoremos turi prasmę bet kurioje aksiomatizuotos teorijos interpretacijoje. D. Hilbertas tikėjosi, kad tuo keliu eidamas, įrodys aibių teorijos neprieštaringumą. Jis ir P. Bernaisas atkakliai ėmėsi įgyvendinti šią programą. Jo ir jo mokinio P. Bernaiso tyrimų rezultatai, vykdant šią programą, susumuoti jų fundamentaliame dviejų tomų veikale "Įrodymų teorija".

Bet tikslo jie nepasiekė. Po 1934 m. K. Giodelio įrodytos metamatematikos teoremos tapo aišku, kad D. Hilberto programa neįgyvendinama. K. Giodelio teorema teigia, kad kievienoje terijoje, grindžiamoje pakankamai "galinga" formalia aksiomų sistema, galima suformuluoti teiginį šios teorijos terminais, kurio šios teorijos terminais negalima nei įrodyti, nei paneigti.

Savaime suprantama, kad aibių teorijoje, o taip pat ir visoje matematikoje susidarė gana įdomi situacija. Be to, aibių teorijos, grindžiamos formalia aksiomų sistema, egzistuoja be galo daug interpretacijų. Kolkas nėra žinoma nei vienos aibių teorijos aksiomų sistemos, kuri turėtų tik vienintelę interpretaciją ir būtų tiek galinga, kad joje būtų galima suformuluoti visas žinomas šiuolaikinės matematikos teorijas.