МАТЕМАТИЧКА ЛОГИКА

ЕЛЕМЕНТИ ТЕОРИЈЕ СКУПОВА

Зоран Петровић
Математички факултет
Београд

Жарко Мијајловић
Математички факултет
Београд

Садржај

Глава 1

Основни појмови

Скупове стално срећемо у математици. Радили смо са скуповима тачака у равни, посматрали скупове решења неких једначина и многе сличне објекте. Заправо, скоро све што радимо у математици засновано је, посредно или непосредно, на појму скупа. Скупове замишљамо као колекције објеката и термин колекција често се користи као синоним за појам скупа. Но, ту ипак треба бити обазрив. Наиме, ако се тако нехајно односимо према појму скупа, врло брзо можемо наићи на проблеме.

Размотримо следећи познати пример. У неком селу берберин брије све људе који се не брију сами и никога више. Поставља се питање: брије ли берберин сам себе? Ако је одговор *не* онда, пошто се не брије сам, мора бријати сам себе (као што је наведено). Дакле, то доводи до противречности. Но, ако је одговор *да*, такође имамо проблема, пошто је речено да он брије искључиво људе који се *не брију сами*, па и тада долазимо до противречности. Сажето говорећи, закључили смо да се он брије сам **ако и само ако** се не брије сам!

Ево још једног примера. Посматрајмо игре за два играча. Није нам важно која су тачно правила за те игре, једино се захтева да се у сваком тренутку зна који је играч на потезу и који су потези допуштени. Када није могуће повући ниједан потез, игра се завршава. Рећи ћемо да је игра *добро заснована* ако се она мора завршити после коначно много корака. Размотримо сада следећу игру (назовимо је Суперигра). У Суперигри први играч бира неку добро засновану игру и онда ту игру започиње други играч. Да ли је Суперигра добро заснована? Па, делује да јесте, јер ако први играч изабере било коју добро засновану игру, онда се та игра завршава после коначно много корака, а то значи да се и Суперигра завршава после коначно много корака. Али ако је Суперигра добро заснована, онда у другом потезу други играч може изабрати баш њу и онда је први играч опет бира и игра се никада не завршава.

У оба примера се појављује сличан проблем, назовимо га *самопози-*

вање. Оба ова примера су у вези са чувеним *Раселовим*[1] *парадоксом.* Наиме, посматрајмо колекцију S дефинисану са

$$x \in S \text{ акко } x \notin x.$$

Да ли $S \in S$? По дефиницији те колекције, добили бисмо да важи

$$S \in S \text{ акко } S \notin S,$$

што је контрадикција. Због тога закључујемо да тако дефинисану колекцију S не можемо сматрати скупом у математичком смислу и питати се од којих се елемената тај „скуп" састоји.

У даљем тексту бавићемо се описом метода за изградњу основних математичких објеката коришћењем скупова, али водећи рачуна о томе да избегнемо сличне парадоксе. Почнимо од почетка ...

1.1 Формирање скупова

Основна релација међу скуповима је релација припадности. Ознака за ту релацију је $\in$. Дакле, ако желимо да кажемо да скуп x припада скупу y онда пишемо

$$x \in y.$$

Ту ознаку први је користио Пеано[2]. Ако је $x \in y$, кажемо и да је x елемент од y. Ми се овде нећемо *детаљно* бавити аксиоматском теоријом скупова, али ћемо ипак истаћи основне принципе на којима почива теорија скупова. Ево и нашег првог принципа, *Аксиоме екстензије*, који потиче још од Лајбница[3].

$$\boxed{\text{Два објекта су једнака акко имају исте елементе.}}$$

Како од нечега морамо почети, то ћемо усвојити и следећу *Аксиому празног скупа.*

$$\boxed{\text{Постоји скуп који нема ниједан елемент.}}$$

Такав скуп називаћемо *празан скуп.* Празан скуп је по Аксиоми екстензије јединствен. Наиме ако су e_1 и e_2 скупови који немају елемената онда за сваки x важи

$$x \in e_1 \iff x \in e_2$$

јер су обе стране еквиваленције нетачне. Стога по Аксиоми екстензије закључујемо да је $e_1 = e_2$. Празан скуп ћемо означавати са $\emptyset$.

Покушаћемо да покажемо како се сви основни математички објекти могу приказати као скупови. Наравно, оног тренутка када су објекти

[1] Bertrand Arthur William Russell (1872–1970), британски логичар.

[2] Giuseppe Peano (1858–1932), италијански математичар.

[3] Gottfried Wilhelm von Leibniz (1646–1716), немачки математичар.

конструисани и њихова основна својства установљена, тада можемо у неким случајевима и заборавити како смо их конструисали и ослонити се у даљем раду са њима искључиво на њихова својства. Приметимо да нас претходне две аксиоме и упућују на то да је сваки објекат који разматрамо скуп. Наиме, ако бисмо разматрали неки објекат за који бисмо сматрали да није скуп, тј. да не садржи никакве елементе онда би он по претходне две аксиоме морао да буде празан скуп, дакле ипак је скуп!

За сада нам је на располагању само празан скуп. То заиста није много, па нам треба још принципа (аксиома) који нам показују како можемо формирати нове скупове. *Аксиома пара* тврди:

За све скупове x и y, постоји скуп z чији су једини елементи x и y.

Такав скуп ћемо означавати са $z = \{x, y\}$. Према томе, важи следеће

$$u \in \{x, y\} \text{ акко } u = x \text{ или } u = y.$$

Приметимо да за произвољни скуп x можемо формирати и скуп који њега има за једини елемент, дакле скуп $\{x\}$ (узимајући да је у претходном $y = x$). По Аксиоми екстензије важи

$$\{\, x, x \,\} = \{x\},$$

јер су то скупови који имају исте елементе. Наведимо сада један једноставан став који ћемо касније користити

Став 1.1 Важи следеће:

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

Доказ. Ово заиста није тешко показати. Пре свега, јасно је да ако је неки од два услова са десне стране еквиваленције испуњен, мора важити и тражена једнакост. Докажимо стога обратну импликацију. Нека је, дакле, $\{a, b\} = \{c, d\}$. Како $a \in \{a, b\}$ то мора бити $a \in \{c, d\}$, па је $a = c$ или $a = d$. Претпоставимо да је $a = c$ (други случај се аналогно ради). Како $d \in \{c, d\}$ то је и $d \in \{a, b\}$. Ако је $d = b$ добили смо оно што је требало. Претпоставимо зато да је $d = a$. Тада је $a = c = d$, па како и $b \in \{a, b\}$ то мора бити и $b = c = d$, тј. сви елементи су једнаки и следи тражени закључак. □

Следећа аксиома је веома природна, мада ће њена формулација вероватно бити помало необична за читаоце. То је *Аксиома уније.*

За сваки скуп x постоји скуп z тако да $u \in z$ акко $u \in y$ за неки $y \in x$

.

Тај скуп означавамо са $\cup x$. Дакле, он се састоји од елемената елемената од x. Можда делује помало збуњујуће, али не смемо заборавити да су сви објекти које разматрамо скупови, па су стога и елементи из x такође скупови који имају своје елементе. Но, није то ни толико тешко. Ако на пример узмемо било која два скупа x и y и формирамо скуп $z = \{x, y\}$ тада $\cup z$ није ништа друго него скуп свих u таквих да $u \in x$ или $u \in y$, а то је нешто на шта смо навикли — обична унија, да се тако изразимо. У том случају користимо и стандардно означавање

$$x \cup y \stackrel{def}{=} \cup\{x, y\}.$$

Можемо се запитати: Како стоји ствар са пресеком? Али, о пресеку мало касније.

До сада смо успевали да све што смо желели изразимо преко наше основне релације $\in$ и нисмо изводили нове релације. Уведимо сада релације $\subseteq$ и $\subset$ следећом дефиницијом.

$$x \subseteq y \stackrel{\text{def}}{\iff} \text{за сваки } z \text{ важи: ако } z \in x \text{ онда } z \in y.$$

У том случају се за скуп x каже да је он подскуп скупа y. Релација $\subset$ је изведена релација претходне и дефинисана је са

$$x \subset y \stackrel{\text{def}}{\iff} x \subseteq y \text{ и } x \neq y.$$

Ако је $x \subset y$, кажемо да је x *прави* подскуп од y.

Када смо увели појам подскупа датог скупа, можемо сада прећи и на *Аксиому партитивног скупа*.

За сваки скуп x постоји скуп $\mathcal{P}(x)$, који се састоји од свих подскупова од x.

До сада је све ишло глатко, али сада се морамо позабавити нечим суптилнијим. Наиме, навикли смо да у пракси формирамо скупове попут следећег

$$X = \{x : x(x+1) \geq 3\}.$$

Дакле, формирамо скуп који се састоји од елемената који испуњавају неко задато својство. Јасно је да морамо да будемо опрезни како то својство задајемо. На пример, већ смо видели да скуп не можемо задати са $S = \{x : x \notin x\}$. Једноставно, на овај начин добијамо „превише велики скуп“, да се тако изразимо. Но, можда неће довести до проблема да формирамо скуп попут следећег

$$T = \{x \in a : x \text{ задовољава неко својство}\},$$

где је a неки скуп. На овај начин нећемо добити превелике скупове, али размотримо ипак следећи пример. Нека је скуп W задат са

$$W = \{x \in \mathbb{N} : x \text{ се не може описати са мање од сто речи}\}.$$

Ако бисмо узели најмањи елемент тог скупа, јасно је да је он описан са мање од сто речи и добијамо контрадикцију. Но, јасно је да овде имамо проблем у томе каква својства допуштамо. Како нам је од интереса да градимо математичке објекте то се ограничавамо на својства која су задата формулама које се формирају на следећи начин.

Дефиниција 1.2 Дефинишемо скуп (добро формираних) формула са:

(1) $(u = v)$, $(u \in v)$ су формуле, где су u и/или v промењљиве или имена неких скупова (константе)

(2) ако су ϕ и ψ формуле то су и $\neg\phi$, $(\phi * \psi)$, где је $*$ било који логички везник;

(3) ако је ϕ формула, то су и $\forall x\phi$, $\exists x\phi$ формуле.

Свака формула се добија коначном применом ових правила.

Промењљиве ћемо најчешће означавати словима $x, y, z, \ldots$, као и индексираним словима (x_1, x_2 и слично). Оно што је важно истаћи је да су својства о којима је реч прецизно математички задата неким формулама. Ако се, у датој формули, неко појављивање неке промењљиве налази под дејством неког квантификатора, тада кажемо да је то појављивање везано. У супротном је слободно. На пример у формули $\forall x((y = x) \Rightarrow (y = z))$ сва појављивања промењљивих y и z су слободна, док је појављивање промењљиве x везано. За формулу кажемо да има слободну промењљиву, ако је бар једно појављивање бар једне промењљиве слободно. Ознака $\phi(x)$ означава да формула има највише једну слободну промењљиву и да то може бити само промењљива x. Ознака $\psi(x, y)$ одговара случају са две промењљиве. Наведимо сада *Аксиому издвајања подскупа.*

$$\boxed{\text{За сваку формулу } \phi(x)\text{: } \{x \in a : \phi(x)\} \text{ је скуп.}}$$

Дакле, из неког скупа можемо издвојити подскуп задат неком формулом. Ако је $\phi(x)$ било која формула са једном слободном промењљивом, видимо да је колекција свих објеката који задовољавају ту формулу у општем случају превелика да би је називали скупом, али пошто је могуће радити са таквим формулама онда је погодно (и то ћемо понекад и радити) разматрати и такву колекцију и називати је класом. Ако је рецимо испуњено $\phi(x) \Rightarrow \psi(x)$ онда је природно рећи да је класа одређена формулом $\phi(x)$ подкласа класе одређене формулом ψ. Како никада нећемо једну класу посматрати као *елемент* неке друге класе, то нећемо имати проблема са парадоксима.

Ево и неких једноставних примена ове аксиоме.

$$A \setminus B \overset{\text{def}}{=} \{x \in A : x \notin B\}.$$

На овај начин дефинишемо разлику скупова A и B. Дакле, разлику чине сви елементи из A који су издвојени формулом $x \notin B$ (прецизније говорећи, формулом $\neg(x \in B)$).

$$A \cap B \stackrel{\text{def}}{=} \{x \in A : x \in B\}.$$

Уопште можемо дефинисати и пресек $\cap a$ где је a било који *непразан* скуп са

$$\cap a \stackrel{\text{def}}{=} \{z \in \cup a : \forall y(y \in a \Rightarrow z \in y)\}.$$

Продискутујмо мало ову дефиницију. Наравно да бисмо желели да пресек дефинишемо као скуп свих елемената који леже у свим елементима датог скупа, без позивања на унију. Но, знамо да елементе можемо коректно да изаберемо (а да од њих после тога формирамо скуп) уколико они већ леже у неком скупу. Због тога је корисно узети унију.

Присетимо се Раселовог парадокса. Применимо идеју, коју смо тамо користили да докажемо следећи став.

Став 1.3 Сваки непразан скуп има подскуп, који није његов елемент.

Доказ. Нека је S произвољан непразан скуп. Посматрајмо подскуп скупа S задат са:

$$R_S = \{x \in S : x \notin x\}.$$

Претпоставимо да $R_S \in S$. Као у Раселовом парадоксу добијамо да важи: $R_S \in R_S$ ако и само ако $R_S \notin R_S$. Наиме, ако $R_S \notin R_S$, с обзиром да $R_S \in S$ добијамо да мора бити $R_S \in R_S$ (R_S задовољава дефиниционі услов скупа R_S). Обратно, ако $R_S \in R_S$, он је у подскупу скупа S у коме су они скупови који нису сопствени елементи, па добијамо $R_S \notin R_S$. Дакле, добили смо контрадикцију и закључујемо да R_S не припада скупу S. $\square$

Последица 1.4 Не постоји скуп који садржи све скупове.

Доказ. Према претходном ставу за сваки непразан скуп постоји скуп који није његов елемент. $\square$

Наведимо сада неке идентитете и релације међу скуповима.

$$A \cup A = A \tag{1.1}$$
$$A \cap A = A \tag{1.2}$$
$$A \subseteq B \iff A \cap B = A \tag{1.3}$$
$$A \subseteq B \iff A \cup B = B \tag{1.4}$$
$$A \subseteq A \cup B \tag{1.5}$$

$$
\begin{aligned}
A \cap B &\subseteq A && (1.6)\\
A \cap (B \cap C) &= (A \cap B) \cap C && (1.7)\\
A \cup (B \cup C) &= (A \cup B) \cup C && (1.8)\\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) && (1.9)\\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) && (1.10)\\
A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C) && (1.11)\\
A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) && (1.12)\\
(A \cap B) \cup (B \cap C) \cup (A \cap C) &= (A \cup B) \cap (B \cup C) \cap (A \cup C) && (1.13)
\end{aligned}
$$

Наравно да су нам то све добро позната својства попут асоцијативности, дистрибутивности, Де Моргановихa[4] закона. Можда је једино последњи идентитет мање познат — то је Дедекиндов[5] идентитет. Сви се ти идентитети (сем можда Дедекиндовог) једноставно доказују и била би добра вежба за читаоца да неке и покаже. Ми ћемо овде за илустрацију доказати следећу чињеницу

$$A \cap (B \cup C) = (A \cap B) \cup C \iff C \subseteq A$$

$\Longrightarrow$:

$$C \subseteq (A \cap B) \cup C = A \cap (B \cup C) \subseteq A$$

$\Longleftarrow$:

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

Проверите која су својства коришћена у овом доказу. Наведимо и дефиницију симетричне разлике скупова

$$A \triangle B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A).$$

Симетрична разлика скупова има правилније понашање од уније, а она се користи и у теорији мере, као што ће читаоци имати прилике да виде. На њу ћемо се вратити и касније.

1.2 Декартов производ скупова. Релације

Свима нам је добро познат појам уређеног пара. Како да коректно дефинишемо уређени пар, а да има својства која желимо? Ево како:

$$(x, y) \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}.$$

Став 1.5 За скупове a, b, c, d важи

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

[4] Augustus De Morgan (1806–1871), британски математичар.
[5] Julius Wilhelm Richard Dedekind (1831–1916), немачки математичар.

Доказ. Јасно је да ако важи $a = c$ и $b = d$ морају одговарајући уређени парови бити једнаки, јер су то скупови са истим елементима. Докажимо обратну импликацију. Нека је, дакле $(a, b) = (c, d)$, тј. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Према Ставу 1.1, тада мора бити $\{a\} = \{c\}$ и $\{a, b\} = \{c, d\}$, или $\{a\} = \{c, d\}$ и $\{a, b\} = \{c\}$. У првом случају, поновљеном применом истог става добијамо тражено, док је у другом случају ситуација још једноставнија, јер је тада $a = b = c = d$, па следи тражени закључак. □

Дакле, показали смо како се може задати уређени пар и у даљем можемо користити искључиво његово основно својство дато претходним ставом без позивања на дефиницију. Уређену тројку можемо задати са

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

и слично се могу задати произвољне уређене $n-$торке. Ако $x \in A$ и $y \in B$, проверимо где се налази уређени пар (x, y):

$$\begin{aligned} x \in A \text{ и } y \in B \quad &\Rightarrow \quad \{x\} \in \mathcal{P}(A) \text{ и } \{x, y\} \in \mathcal{P}(A \cup B) \\ &\Rightarrow \quad \{x\} \in \mathcal{P}(A \cup B) \text{ и } \{x, y\} \in \mathcal{P}(A \cup B) \\ &\Rightarrow \quad \{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(A \cup B)) \end{aligned}$$

Дакле, Декартов[6] производ скупова A и B можемо дефинисати на следећи начин

$$A \times B \stackrel{\text{def}}{=} \{w \in \mathcal{P}(\mathcal{P}(A \cup B)) : (\exists x \in A)(\exists y \in B)(w = (x, y))\}.$$

Напоменимо да је $(\exists x \in A)\phi$ заправо скраћени запис за $\exists x(x \in A \wedge \phi)$. Помоћу уређених $n-$торки дефинише се појам Декартовог производа од n скупова. Ако су сви скупови једнаки добијени скуп означавамо са A^n. Дефинишимо сада појам релације.

Дефиниција 1.6 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 $A = B$ добијамо појам бинарне релације на скупу A. Унарне релације на скупу A су подскупови од A, док се n-арне релације на A аналогно дефинишу као подскупови од A^n. Нама ће посебно бити интересантан случај бинарне релације на неком скупу.

У случају бинарне релације, уместо $(a, b) \in \rho$ чешће се користи запис $a \, \rho \, b$. Ми ћемо користити оба записа у зависности од ситуације. Подсетимо се својстава које нека бинарна релација може да има.

Дефиниција 1.7 Нека је ρ бинарна релација на скупу A. Релација ρ је

[6] René Descartes (1596–1650), француски математичар.

(P)	Рефлексивна ако	за све $a \in A$: $a\,\rho\,a$;
(AP)	Антирефлексивна ако	за све $a \in A$: $\neg(a\,\rho\,a)$;
(C)	Симетрична ако	за све $a, b \in A$: $a\,\rho\,b \Rightarrow b\,\rho\,a$;
(T)	Транзитивна ако	за све $a, b, c \in A$: $a\,\rho\,b$ и $b\,\rho\,c \Rightarrow a\,\rho\,c$;
(AC)	Антисиметрична ако	за све $a, b \in A$: $a\,\rho\,b$ и $b\,\rho\,a \Rightarrow a = b$.

Дефиниција 1.8 За релацију на скупу A кажемо да је **релација еквиваленције**, ако је она рефлексивна, симетрична и транзитивна. Најчешћа ознака за произвољну релацију еквиваленције је $\sim$. Скуп свих елемената, који су у релацији са неким елементом x зове се класа еквиваленције тог елемента и означава се са C_x.

За релацију кажемо да је **релација парцијалног уређења** на скупу A ако је она рефлексивна, антисиметрична и транзитивна. Ознака је $\leq$. Релација је **релација строгог поретка** ако је она антирефлексивна и транзитивна. Ознака: $<$.

Приметимо да, ако је на неком скупу задата релација парцијалног уређења $\leq$, тада је релација задата са

$$a < b \overset{\text{def}}{\iff} (a \leq b) \text{ и } a \neq b$$

једна релација строгог поретка, чиме се ове ознаке доводе у сагласност. Скуп P са задатом релацијом парцијалног уређења на њему назива се парцијално уређен скуп, скраћено **посет** (од енглеског назива *„partially ordered set“*).

Елемент m посета P је **највећи** елемент у том посету уколико за сваки $x \in P$ важи: $x \leq m$. Кажемо да је елемент m посета P **максималан** елемент уколико не постоји елемент $x \in P$ такав да је $m < x$. На сличан начин се дефинише и појам најмањег, односно минималног елемента у посету. Ако у посету постоји највећи елемент, онда је јасно да је он и максималан. С друге стране, у посету може постојати више максималних елемената, а ниједан највећи. Суштина је у томе да не морају свака два елемента у посету да буду упоредива. Погледајте задатке за вежбу.

Ако су свака два елемента упоредива ($a \leq b$ или $b \leq a$, за све $a, b \in P$) тада је скуп P линеарно (тотално) уређен. Линеарно уређен подскуп неког посета назива се **ланац**. Ако су у неком подскупу неког посета свака два различита елемента неупоредива, такав подскуп називамо **антиланац**. На пример, ако радимо са релацијом дељивости у скупу позитивних целих бројева, скуп свих простих бројева чини један антиланац. На ове појмове ћемо се касније поново вратити.

Како је релација скуп, то се непосредно дефинише појам пресека и уније две релације. Дефинишимо сада композицију две релације.

Дефиниција 1.9 Нека су $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$ две релације. Релација $\sigma \circ \rho \subseteq A \times C$ дефинише се са

$$a\,(\sigma \circ \rho)\,c \overset{\text{def}}{\iff} \text{ за неки } b \in B \text{ важи } a\,\rho\,b \text{ и } b\,\sigma\,c.$$

Овакав начин задавања композиције две релације мотивисан је дефиницијом композиције две функције. Наиме, видећемо како се функција може видети као специјалан случај релације и композиција функција ће се поклопити са композицијом релација. Инверзна релација је задата дефиницијом.

Дефиниција 1.10 Нека је $\rho \subseteq A \times B$

$$b\,\rho^{-1}\,a \stackrel{\text{def}}{\iff} a\,\rho\,b.$$

Приметимо да је $\rho^{-1} \subseteq B \times A$.

У следећем ставу наводе се нека својства операција дефинисаних над релацијама.

Став 1.11 Нека су $\rho, \rho_1, \rho_2, \sigma, \tau$ релације. Тада

1. $(\sigma \circ \rho) \circ \tau = \sigma \circ (\rho \circ \tau)$;
2. $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$;
3. $\rho_1 \subseteq \rho_2 \Rightarrow \sigma \circ \rho_1 \subseteq \sigma \circ \rho_2$;
4. $(\rho_1 \cap \rho_2)^{-1} = \rho_1^{-1} \cap \rho_2^{-1}$;
5. $(\rho_1 \cup \rho_2)^{-1} = \rho_1^{-1} \cup \rho_2^{-1}$;
6. $\sigma \circ (\rho_1 \cup \rho_2) = \sigma \circ \rho_1 \cup \sigma \circ \rho_2$;
7. $\sigma \circ (\rho_1 \cap \rho_2) \subseteq \sigma \circ \rho_1 \cap \sigma \circ \rho_2$.

Доказ. Ниједан од ових исказа није тежак за доказивање. Доказаћемо илустрације ради други, шести и седми.

$$\begin{aligned}
c\,(\sigma \circ \rho)^{-1}\,a &\iff a\,(\sigma \circ \rho)\,c \\
&\iff \text{ за неко } b\text{: } a\,\rho\,b \text{ и } b\,\sigma\,c \\
&\iff \text{ за неко } b\text{: } b\,\rho^{-1}\,a \text{ и } c\,\sigma^{-1}\,b \\
&\iff \text{ за неко } b\text{: } c\,\sigma^{-1}\,b \text{ и } b\,\rho^{-1}\,a \\
&\iff c\,(\rho^{-1} \circ \sigma^{-1})\,a.
\end{aligned}$$

$$\begin{aligned}
a\,\sigma \circ (\rho_1 \cup \rho_2)\,c &\iff \text{ за неко } b\text{: } a\,(\rho_1 \cup \rho_2)\,b \text{ и } b\,\sigma\,c \\
&\iff \text{ за неко } b\text{: } (a\,\rho_1\,b \text{ или } a\,\rho_2\,b) \text{ и } b\sigma\,c \\
&\iff \text{ за неко } b\text{: } (a\,\rho_1\,b \text{ и } b\,\sigma\,c) \text{ или } (a\,\rho_2\,b \text{ и } b\,\sigma\,c) \\
&\iff a\,(\sigma \circ \rho_1)\,c \text{ или } a\,(\sigma \circ \rho_2)\,c \\
&\iff a\,(\sigma \circ \rho_1 \cup \sigma \circ \rho_2)\,c.
\end{aligned}$$

Докажимо напокон и исказ 7. Нека је, дакле $a\,\sigma\circ(\rho_1\cap\rho_2)\,c$. Тада постоји неко b за које важи: $a\,\rho_1\cap\rho_2\,b$ и $b\,\sigma\,c$. Стога је за то b испуњено $a\,\rho_1\,b$, $b\,\sigma\,c$, као и $a\,\rho_2\,b$, $b\,\sigma\,c$, па је испуњено и $a\,(\sigma\circ\rho_1)\cap(\sigma\circ\rho_2)\,c$. □

Покушајмо да докажемо обратну импликацију. Претпоставимо дакле да је $a\,(\sigma\circ\rho_1)\cap(\sigma\circ\rho_2)\,c$. То значи да је $a\,(\sigma\circ\rho_1)\,c$ и $a\,(\sigma\circ\rho_2)\,c$. Из чињенице да је $a\,(\sigma\circ\rho_1)\,c$ закључујемо да постоји b_1 тако да важи $a\,\rho_1\,b_1$ и $b_1\,\sigma\,c$, док из $a\,(\sigma\circ\rho_2)\,c$ закључујемо да постоји b_2 тако да важи $a\,\rho_2\,b_2$ и $b_2\,\sigma\,c$. *У општем случају је* $b_1\neq b_2$ и зато обратна импликација не важи увек. Но, да бисмо се заиста уверили да у 7 једнакост не мора увек важити морамо навести пример. Пример је доста једноставан. Нека је наш основни скуп, на пример скуп $\mathbb{N}\setminus\{0\}$. За релацију σ узмимо релацију дељивости ($\,|\,$), за релацију ρ_1 релацију $\leq$, а за релацију ρ_2 релацију $\geq$. Тада се непосредно проверава:

$$\begin{aligned} |\circ\leq &= \leq\\ |\circ\geq &= (\mathbb{N}\setminus\{0\})^2\\ |\circ(\leq\cap\geq) &= |\,. \end{aligned}$$

Доказе које смо управо извели намерно смо исписали у текстуалном облику, без исписивања квантификатора. Заправо се у овим резултатима крију основна својства универзалних и егзистенцијалних квантификатора и добро је исписати их речима. Ово што смо сада урадили треба да послужи као мотивација за касније изучавање.

Једнакост је врло посебна релација еквиваленције, која је дефинисана на сваком скупу. Понекад ћемо, због прегледности, за њу користити ознаку $\triangle_A$, ако је посматрамо на скупу A. Дакле,

$$\triangle_A \stackrel{\text{def}}{=} \{(a,a) : a\in A\}.$$

Изразимо сада раније наведена својства релација у компактнијем запису.

Став 1.12 Релација ρ на скупу A, је

(Р)	рефлексивна	**акко**	$\triangle_A\subseteq\rho$
(АР)	антирефлексивна	**акко**	$\rho\cap\triangle_A=\emptyset$
(С)	симетрична	**акко**	$\rho\subseteq\rho^{-1}$
(Т)	транзитивна	**акко**	$\rho\circ\rho\subseteq\rho$
(АС)	антисиметрична	**акко**	$\rho\cap\rho^{-1}\subseteq\triangle_A$

Доказ. Све наведено непосредно следи из дефиниција и та провера се оставља читаоцу. □

Дефинишемо домен $\mathrm{Dom}(\rho)$ и слику $\mathrm{Im}(\rho)$ неке релације $\rho\subseteq A\times B$ на следећи начин

$$\begin{aligned} \mathrm{Dom}(\rho) &\stackrel{\text{def}}{=} \{a\in A : (\exists b\in B)(a,b)\in\rho\}\\ \mathrm{Im}(\rho) &\stackrel{\text{def}}{=} \{b\in B : (\exists a\in A)(a,b)\in\rho\}. \end{aligned}$$

За релацију је могуће дефинисати и још неке појмове, али ћемо дефинисање тих појмова дати тек у следећем одељку и то искључиво у случају функција, где имамо и највећу корист од њиховог увођења.

Запитајмо се на крају како се од дате релације ρ на скупу A може добити најмања релација еквиваленције која је садржи — релација еквиваленције ρ^e генерисана датом релацијом ρ. То се изводи у неколико корака

1. $\rho_1 = \rho \cup \triangle_A$;
2. $\rho_2 = \rho_1 \cup \rho_1^{-1}$;
3. $\rho^e = \bigcup_{n=1}^{\infty} \rho_2^n$

ρ^n се наравно дефинише као

$$\underbrace{\rho \circ \rho \circ \cdots \circ \rho}_{\text{n puta}}.$$

Није тешко објаснити разлоге због којих се изводе ове конструкције. Прва операција нам даје рефлексивну релацију, друга од постојеће направи симетричну, а трећа транзитивну.

1.3 Функције

Функције су посебан случај релација, али су као објекти од централног значаја за математику.

Дефиниција 1.13 Нека је $f \subseteq A \times B$ релација из A у B. Та релација је *функција* ако за свако $x \in \mathrm{Dom}(f)$ постоји тачно једно $y \in B$ такво да је $(x, y) \in f$. У том случају уместо $(x, y) \in f$, чешће се пише $y = f(x)$. Ако је $\mathrm{Dom}(f) = A$, онда користимо ознаку $f\colon A \to B$. Скуп B називамо кодоменом функције f.

Напомена 1.14 Зашто смо баш на овај начин дефинисали функцију? Наиме, зашто нисмо одмах дефинисали шта је то функција из A у B и онда написали да A зовемо домен, а B кодомен функције, као што смо углавном до сада навикли? Два су разлога. Први је у томе што дефинисање на овај начин и јесте врло природно пошто објашњава да је домен скуп свих оних елемената за које функција „може бити израчуната“, да се тако изразимо. Други разлог састоји се у следећем. Ми знамо да функција f^{-1} није увек дефинисана. Но, видели смо да релација f^{-1} *јесте* увек дефинисана. Наравно да желимо да се инверзна функција (када постоји) поклопи са инверзном релацијом (која увек постоји). Али желели бисмо и да сматрамо f^{-1} за функцију чак и када функција f није „на“ већ само „1–1“ (у овој напомени идемо мало испред уведених појмова, али ово је методска напомена која не утиче на развијање области како је презентирамо, него даје објашњење читаоцу, којем су многи од дефинисаних појмова већ познати). У том случају, пошто функција f није „на“ то домен релације f^{-1} није цео долазни скуп. Заправо је $\mathrm{Dom}(\rho^{-1}) = \mathrm{Im}(\rho)$, за сваку релацију ρ, па посебно и за функцију. Зато је боље на овај начин дефинисати функцију и посебно издвојити појам њеног домена. Тако смо наиме у могућности да разматрамо f^{-1} за било коју „1–1“ функцију $f\colon A \to B$ и тада је $f^{-1} : \mathrm{Im}(f) \to A$.

Дакле, функција је посебан случај релације. Следећи став даје потребне и довољне услове да би нека релација била функција.

Став 1.15 Нека је $\Phi \subseteq A \times B$. Тада важи

$$\Phi \text{ је функција са доменом } A \textbf{ акко } \triangle_A \subseteq \Phi^{-1} \circ \Phi \text{ и } \Phi \circ \Phi^{-1} \subseteq \triangle_B.$$

Доказ.
$\Longleftarrow$: Нека су дати услови испуњени и нека је x произвољан елемент из A. Како $(x,x) \in \triangle_A$, то из првог услова добијамо да постоји неко $y \in B$ за које важи: $(x,y) \in \Phi$ и $(y,x) \in \Phi^{-1}$, што се своди само на $(x,y) \in \Phi$. Отуда, за сваки $x \in A$ постоји $y \in B$ тако да $(x,y) \in \Phi$, па закључујемо да је домен релације Φ цео скуп A. Нека је за неке парове (x,y_1) и (x,y_2) испуњено: $(x,y_1) \in \Phi$ и $(x,y_2) \in \Phi$. Тада $(y_1,x) \in \Phi^{-1}$ и $(x,y_2) \in \Phi$, па, по дефиницији композиције две релације, закључујемо да $(y_1,y_2) \in \Phi \circ \Phi^{-1}$. Према другом услову, закључујемо да је $y_1 = y_2$, чиме је завршен доказ да је Φ функција.
$\Longrightarrow$: Доказ овог смера оставља се читаоцу за вежбу. $\square$

Нека $f\colon X \to Y$ и нека је $A \subseteq X$ и $B \subseteq Y$. *Инверзна слика* скупа B при функцији f дефинише се са

$$f^{-1}[B] \stackrel{\text{def}}{=} \{x \in X : f(x) \in B\}.$$

Видимо да је инверзна слика подскупа од Y дефинисана за сваку функцију f и да, према Аксиоми издвајања подскупа, заиста представља легитиман скуп. Дефинишимо сада *директну слику* скупа A при функцији f

$$f[A] \stackrel{\text{def}}{=} \{f(x) : x \in A\}.$$

Пажљив читалац неће пропустити овај тренутак да примети да нисмо сигурни да смо овако дефинисали један скуп. И заиста, због тога уводимо *Аксиому замене* који проглашава овако дефинисану колекцију за скуп. Заправо је Аксиома замене нешто општија и у том смислу је аналогна Аксиоми издвајања подскупа, о којој је раније било речи. Наиме, нека је $\psi(x,y)$ једна добро формирана формула која има две слободне промењљиве x и y. Ако је за њу тачно да за сваки скуп a постоји *највише један* скуп b за који је $\psi(a,b)$ испуњено и ако је A било који скуп онда важи

$$\boxed{\{y : \psi(x, y) \text{ за неко } x \in A\} \text{ је скуп.}}$$

Заправо нам за увођење појма директне слике скупа није неопходно да уводимо аксиму замене. Наиме, ако се пажљивије напише дефиниција директне слике скупа видимо да је

$$f[A] \stackrel{\text{def}}{=} \{y \in B : (\exists x)(x \in A \wedge y = f(x))\},$$

па чињеница да је директна слика заиста скуп *ипак* следи из Аксиоме издвајања подскупа. Но, нама је ипак потребно да и колекције формиране као у Аксиоми замене чине скуп, па је згодно ту аксиому увести у овом тренутку. Суштина Аксиоме замене је у томе да, ако све елементе неког скупа *заменимо* произвољним скуповима, тако добијена колекција објеката чини скуп. Не желимо да се ограничавамо искључиво на ситуацију у којој се елементи бирају из унапред задатог скупа.

Нека $f\colon X \to Y$. За $A \subseteq X$ дефинишемо *рестрикцију* функције f на подскуп A са

$$f|_A \stackrel{\text{def}}{=} \{(x, y) \in f : x \in A\}.$$

Тада $f|_A : A \to Y$ и $f|_A(a) = f(a)$ за све $a \in A$.

Фамилија скупова индексирана скупом индекса I је функција $F : I \to W$, где је W неки скуп. Ако скупове у фамилији означимо са $X_i = F(i)$, за $i \in I$, онда фамилију F, а и било коју функцију, записујемо и овако $\langle X_i : i \in I\rangle$. По Аксиоми замене може се формирати скуп

$$\{X_i : i \in I\}$$

и уместо $\bigcup\{X_i : i \in I\}$, односно $\bigcap\{X_i : i \in I\}$ пишемо

$$\bigcup_{i \in I} X_i,$$

односно

$$\bigcap_{i \in I} X_i.$$

Приметимо да је услов $x \in \bigcup_{i\in I} X_i$ ($x \in \bigcap_{i\in I} X_i$) еквивалентан услову: за неко (свако) $i \in I$ је $x \in X_i$.

Наводимо сада основна својства директне и инверзне слике скупова у оквиру следећег става.

Став 1.16 Нека $f\colon X \to Y$, $g\colon Y \to Z$ и нека су A,A',A_i, за $i \in I$, подскупови од X; B,B',B_i, за $i \in I$, подскупови од Y (I је неки скуп индекса), а C подскуп од Z. Тада важи

$$(g \circ f)[A] = g[f[A]] \tag{1.14}$$

$$(g \circ f)^{-1}[C] = f^{-1}[g^{-1}[C]] \tag{1.15}$$

$$f^{-1}\Big[\bigcup_{i\in I} B_i\Big] = \bigcup_{i\in I} f^{-1}[B_i] \tag{1.16}$$

$$
\begin{aligned}
f^{-1}\Big[\bigcap_{i\in I} B_i\Big] &= \bigcap_{i\in I} f^{-1}[B_i] && (1.17)\\
f^{-1}[B\setminus B'] &= f^{-1}[B]\setminus f^{-1}[B'] && (1.18)\\
f\Big[\bigcup_{i\in I} A_i\Big] &= \bigcup_{i\in I} f[A_i] && (1.19)\\
f\Big[\bigcap_{i\in I} A_i\Big] &\subseteq \bigcap_{i\in I} f[A_i] && (1.20)\\
f[A\setminus A'] &\supseteq f[A]\setminus f[A'] && (1.21)\\
f[f^{-1}[B]] &\subseteq B && (1.22)\\
f^{-1}[f[A]] &\supseteq A && (1.23)
\end{aligned}
$$

Доказ. Мада се сви ови резултати лако доказују извешћемо сваки доказ у потпуности.

Доказ за (1.14)

$$
\begin{aligned}
z\in g[f[A]] &\iff \text{за неко } y\in f[A],\ z=g(y)\\
&\iff \text{за неко } y\in f[A] \text{ и неко } x\in A,\ z=g(y) \text{ и } y=f(x)\\
&\iff \text{за неко } x\in A,\ z=g(f(x))\\
&\iff \text{за неко } x\in A,\ z=(g\circ f)(x),\\
&\iff z\in (g\circ f)[A].
\end{aligned}
$$

Доказ за (1.15)

$$
\begin{aligned}
x\in f^{-1}[g^{-1}[C]] &\iff f(x)\in g^{-1}[C]\\
&\iff g(f(x))\in C\\
&\iff (g\circ f)(x)\in C\\
&\iff x\in (g\circ f)^{-1}[C].
\end{aligned}
$$

Доказ за (1.16)

$$
\begin{aligned}
x\in f^{-1}\Big[\bigcup_{i\in I} B_i\Big] &\iff f(x)\in \bigcup_{i\in I} B_i\\
&\iff \text{за неко } i\in I,\ f(x)\in B_i\\
&\iff \text{за неко } i\in I,\ x\in f^{-1}[B_i]\\
&\iff x\in \bigcup_{i\in I} f^{-1}[B_i].
\end{aligned}
$$

Доказ за (1.17)

$$
x\in f^{-1}\Big[\bigcap_{i\in I} B_i\Big] \iff f(x)\in \bigcap_{i\in I} B_i
$$

$$\begin{aligned}
&\iff \text{за свако } i \in I,\ f(x) \in B_i \\
&\iff \text{за свако } i \in I,\ x \in f^{-1}[B_i] \\
&\iff x \in \bigcap_{i \in I} f^{-1}[B_i].
\end{aligned}$$

Доказ за (1.18)

$$\begin{aligned}
x \in f^{-1}[B \setminus B'] &\iff f(x) \in B \setminus B' \\
&\iff f(x) \in B \text{ и } f(x) \notin B' \\
&\iff x \in f^{-1}[B] \text{ и } x \notin f^{-1}[B'] \\
&\iff x \in f^{-1}[B] \setminus f^{-1}[B'].
\end{aligned}$$

Доказ за (1.19)

$$\begin{aligned}
y \in f\Big[\bigcup_{i \in I} A_i\Big] &\iff \text{за неко } x \in \bigcup_{i \in I} A_i,\ y = f(x) \\
&\iff \text{за неко } i \in I,\ y \in f[A_i] \\
&\iff y \in \bigcup_{i \in I} f[A_i].
\end{aligned}$$

Доказ за (1.20)

$$\begin{aligned}
y \in f\Big[\bigcap_{i \in I} A_i\Big] &\iff \text{за неко } x \in \bigcap_{i \in I} A_i,\ y = f(x) \\
&\Rightarrow \text{за свако } i \in I,\ y \in f[A_i] \\
&\iff y \in \bigcap_{i \in I} f[A_i].
\end{aligned}$$

Доказ за (1.21)

$$\begin{aligned}
y \in f[A] \setminus f[A'] &\iff y \in f[A] \text{ и } y \notin f[A'] \\
&\iff \text{за неко } x \in A,\ y = f(x) \text{ и } y \notin f[A'] \\
&\Rightarrow \text{за неко } x \in A, \text{ које није у } A',\ y = f(x) \\
&\iff y \in f[A \setminus A'].
\end{aligned}$$

Доказ за (1.22)

$$\begin{aligned}
y \in f[f^{-1}[B]] &\iff \text{за неко } x \in f^{-1}[B],\ y = f(x) \\
&\iff \text{за неко } x, \text{ такво да } f(x) \in B,\ y = f(x) \\
&\Rightarrow y \in B.
\end{aligned}$$

Доказ за (1.23)

$$\begin{aligned}
x \in A &\Rightarrow f(x) \in f[A] \\
&\iff x \in f^{-1}[f[A]].
\end{aligned}$$

□

Прокоментаришимо мало наведене доказе. Основна особина, која је коришћена на више места у овим доказима, је следећа

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

То није ништа друго до преформулација дефиниције инверзне слике скупа. Са друге стране, $f(x) \in f[A]$ **није** еквивалентно са $x \in A$. Погледајмо, наиме следећи једноставан пример. Нека је $f\colon \mathbb{R} \to \mathbb{R}$ дефинисано са $f(x) = x^2$. Ако је $A = (-\infty, 0]$ то је $f(2) = 4$ и $4 \in f[A](= [0, +\infty))$, а наравно $2 \notin A$. Дакле, овај пример показује зашто наведена еквиваленција не важи. Због свега реченог, инверзна слика се много боља „понаша“ у односу на скуповне операције од директне слике, што доводи до разних корисних особина функција. Добра би била вежба за читаоца да сада прекине читање овог текста и покуша да провери зашто не важе једнакости у свим случајевима.

Ако је читалац урадио како је саветовано, то је без сумње могао да увиди да су проблеми у томе што се два различита елемента могу сликати у исти, или што није сваки елемент слика неког другог. Ако за функцију f важи $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, за све x_1 и x_2 из домена те функције онда за ту функцију кажемо да је једна *инјекција*, или да је „1–1“. Уместо наведеног услова чешће се користи еквивалентан услов

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

за проверу да ли је нека функција „1–1“. Функција $f\colon X \to Y$ је *сурјекција*, односно „на“ ако је сваки елемент из Y слика неког елемента из X, тј. ако

$$(\forall y \in Y)(\exists x \in X)\, y = f(x).$$

Другим речима, $f[X] = Y$. Може се једноставно показати да у (1.22) једнакост важи за сваки скуп B *акко* је f „на“, док у (1.23), једнакост важи за свако A *акко* је f „1–1“. За функцију кажемо да је *бијекција* уколико је и „1–1“ и „на“. Уколико је $f\colon X \to Y$ бијекција, тада се једноставно проверава да је f^{-1} функција са доменом Y и да важи: $f^{-1} \circ f = \triangle_A$ и $f \circ f^{-1} = \triangle_B$ (проверити!). Убудуће ћемо релацију $\triangle_A$, која није ништа друго до релација једнакости на скупу A, означавати са Id_A, или са i_A, ако је посматрамо као идентичну функцију ($\mathrm{Id}_A(x) = x$) на скупу A.

Став 1.17 Нека $f\colon X \to Y$ и $g\colon Y \to Z$. Тада важи

а) $g \circ f$ је „1–1“ $\Rightarrow$ f је „1–1“;

б) $g \circ f$ је „на“ $\Rightarrow$ g је „на“.

Доказ.

а) Нека је $f(x_1) = f(x_2)$. Тада је и $g(f(x_1)) = g(f(x_2))$, тј. $(g\circ f)(x_1) = (g\circ f)(x_2)$ из чега следи (пошто је $g\circ f$ „1–1“) да је $x_1 = x_2$.

б) Нека је $z \in Z$ произвољан елемент. Треба показати да постоји $y \in Y$ такав да је $z = g(y)$. Како је по претпоставци $g\circ f$ „на“, то постоји $x \in X$ за које је $(g\circ f)(x) = z$. Пошто је $(g\circ f)(x) = g(f(x))$, то за тражено y можемо узети баш $f(x)$. □

Последица 1.18 Нека су $f\colon X \to Y$ и $g\colon Y \to X$ функције за које су $g\circ f$ и $f\circ g$ бијекције. Тада су и f и g бијекције.

Доказ. Како је $g\circ f$ бијекција, то је према претходном ставу g „на“, а f „1–1“, док из чињенице да је $f\circ g$ бијекција, следи да је f „на“, а g „1–1“. □

Нека су X и Y скупови. Уведимо следећу ознаку за скуп свих функција из X у Y

$$Y^X \overset{\text{def}}{=} \{f \mid f\colon X \to Y\}.$$

Ми ћемо се у следећој глави позабавити питањем увођења природних бројева у контексту теорије скупова, али овде укратко поменимо како се дефинишу најмањи природни бројеви. Дакле

$$\begin{array}{rcl} 0 & := & \emptyset \\ 1 & := & \{0\} \\ 2 & := & \{0,1\} \\ 3 & := & \{0,1,2\} \\ . & & \\ . & & \\ . & & \end{array}$$

Нека је X било који скуп и $A \subseteq X$. Дефинишемо *карактеристичну функцију* $\chi_A : X \to 2$, подскупа A, са

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

Став 1.19 Нека је X скуп. Функција $\Phi\colon \mathcal{P}(X) \to 2^X$, дефинисана са $\Phi(A) = \chi_A$, је бијекција.

Доказ. Докажимо прво да је Φ „1–1“. Дакле, нека је $\Phi(A) = \Phi(B)$. Треба доказати да је $A = B$.

$$\begin{array}{rcl} x \in A & \iff & \chi_A(x) = 1 \\ & \iff & \Phi(A)(x) = 1 \\ & \iff & \Phi(B)(x) = 1 \\ & \iff & \chi_B(x) = 1 \\ & \iff & x \in B. \end{array}$$

Дакле, Φ је „1–1“. Нека је $f: X \to 2$ било која функција. Узмимо за $A \subseteq X$ скуп дефинисан са

$$A = \{x \in X : f(x) = 1\}.$$

Доказаћемо да је $f = \chi_A$, што показује да је $\Phi(A) = f$. Тако добијамо да је Φ и „на“. Приметимо, пре свега да за сваке две функције $f, g: X \to 2$ важи

$$f = g \textbf{ акко } (\forall x \in X)(f(x) = 1 \iff g(x) = 1).$$

То следи из чињенице да су једине могуће вредности ових функција 0 односно 1, те чим таква функција не узима вредност 1 мора узети вредност 0, па је довољно да се скупови на којима такве две функције узимају вредност 1 поклапају да би се и функције поклопиле. Но,

$$\begin{aligned} \chi_A(x) = 1 \quad &\iff \quad x \in A \\ &\iff \quad f(x) = 1, \end{aligned}$$

па је заиста $f = \chi_A$. □

Овај резултат је од посебног значаја. Овде ћемо дати неке његове занимљиве примене на доказивање идентитета међу скуповима. Но, пре тога, дефинишимо две операције $+$ и $\cdot$ на скупу 2. Операција $\cdot$ је обично множење, док је операција $+$ сабирање, сем што узимамо да је $1 + 1 = 0$ („сабирање по модулу 2“). Тако дефинисане операције индукују и операције на функцијама $f, g: X \to 2$.

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

Како су операције сабирања и множења у скупу 2, комутативне и асоцијативне и како је операција множења дистрибутивна у односу на сабирање (што није тешко проверити), то та својства имају и операције на функцијама задате на претходни начин. Приметимо да је $f + f = 0$ (са 0 смо означили и функцију из X у 2 идентички једнаку нули), као и $f \cdot f = f$, за сваку функцију $f: X \to 2$.

Пример 1.20 Показати да важи:

(а) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;

(б) $A = B \cup C \iff A \triangle B \triangle C = B \cap C$;

(в) $x \in A \triangle B \triangle C \iff x$ припада једном или сва три скупа A, B, C.

Доказ. За скуп X узмимо скуп $A \cup B \cup C$. тако ће сви скупови које посматрамо бити подскупови од X и карактеристичне функције које користимо биће дефинисане на скупу X. Приметимо пре свега да важе следећи идентитети

$$\begin{aligned}\chi_{A\cap B} &= \chi_A\cdot\chi_B;\\ \chi_{A\triangle B} &= \chi_A+\chi_B;\\ \chi_{A\cup B} &= \chi_A+\chi_B+\chi_A\cdot\chi_B.\end{aligned}$$

Оставићемо читаоцу за вежбу да их сам провери. Коришћењем ових идентитета лако се доказује тражено.
Доказ за (а)

$$\begin{aligned}x\in(A\triangle B)\triangle C &\iff \chi_{(A\triangle B)\triangle C}(x)=1\\ &\iff (\chi_{A\triangle B}+\chi_C)(x)=1\\ &\iff \chi_{A\triangle B}(x)+\chi_C(x)=1\\ &\iff (\chi_A(x)+\chi_B(x))+\chi_C(x)=1\\ &\iff \chi_A(x)+(\chi_B(x)+\chi_C(x))=1\\ &\iff \chi_A(x)+(\chi_B+\chi_C)(x)=1\\ &\iff (\chi_A+(\chi_B+\chi_C))(x)=1\\ &\iff (\chi_A+\chi_{B\triangle C})(x)=1\\ &\iff \chi_{A\triangle(B\triangle C)}(x)=1\\ &\iff x\in A\triangle(B\triangle C).\end{aligned}$$

Дакле, асоцијативност симетричне разлике своди се на асоцијативност збира функција. Како је симетрична разлика асоцијативна операција, то убудуће не пишемо заграде у случају поновљене операције (као што је и стандардно у аналогним ситуацијама).
Доказ за (б)

$$\begin{aligned}A=B\cup C &\iff \chi_A=\chi_{B\cup C}\\ &\iff \chi_A=\chi_B+\chi_C+\chi_B\cdot\chi_C\\ &\iff \chi_A+\chi_B+\chi_C=\chi_B+\chi_C+\chi_B\cdot\chi_C+\chi_B+\chi_C\\ &\iff \chi_A+\chi_B+\chi_C=\chi_B\cdot\chi_C\\ &\iff \chi_{A\triangle B\triangle C}=\chi_{B\cap C}\\ &\iff A\triangle B\triangle C=B\cap C.\end{aligned}$$

Доказ за (в)

$$x\in A\triangle B\triangle C \iff \chi_A(x)+\chi_B(x)+\chi_c(x)=1.$$

Како је збир три броја који су сви 0 или 1 једнак 1 акко је број јединица 1 или 3, то тражени закључак следи непосредно.

Став 1.21 *(Канторова[7] теорема)* Нека је X произвољан скуп. Тада постоји инјекција скупа X у скуп $\mathcal{P}(X)$, али <u>не</u> постоји бијекција између тих скупова.

[7]Georg Ferdinand Ludwig Philipp Cantor (1845–1918), немачки математичар.

Доказ. Јасно је да је функција $g\colon X \to \mathcal{P}(X)$ дефинисана са $g(x) = \{x\}$ инјекција. Претпоставимо да постоји бијекција $f\colon X \to \mathcal{P}(X)$.

Први начин: Посматрајмо скуп дефинисан са

$$A = \{x \in X : x \notin f(x)\}.$$

Како је за свако $x \in X$, $f(x) \subseteq X$, то горња једнакост заиста задаје један подскуп од X. Но, пошто је функција f бијекција, постоји неки елемент $a \in A$, такав да је $f(a) = A$. Међутим тада добијамо

$$\begin{aligned} a \in A \quad &\Longleftrightarrow \quad a \notin f(a) \text{ по дефиницији скупа } A \\ &\Longleftrightarrow \quad a \notin A, \text{ јер је } f(a) = A. \end{aligned}$$

Према томе, добили смо контрадикцију и закључујемо да бијекција између ова два скупа не може постојати.

Други начин: Посматрајмо функцију $h\colon X \to 2$, задату са:

$$h(x) := \chi_{f(x)}(x) + 1.$$

Како је $f(x) \subseteq X$, има смисла овако дефинисати функцију. С обзиром да је придруживање $A \mapsto \chi_A$ бијекција скупа $\mathcal{P}(X)$ на скуп 2^X, то постоји $A \subseteq X$ за који је $h = \chi_A$. Како је f „на“, то постоји $x_0 \in X$ тако да је $A = f(x_0)$. Добијамо једнакост

$$\chi_{f(x_0)}(x) = \chi_{f(x)}(x) + 1,$$

која важи за свако $x \in X$. Ако за x узмемо баш x_0, добијамо

$$\chi_{f(x_0)}(x_0) = \chi_{f(x_0)}(x_0) + 1,$$

те је $0 = 1$. Ова контрадикција завршава доказ. □

1.4 Добра заснованост

У овом кратком одељку, најзад ћемо искључити могућност разматрања скупова који су сопствени елементи. Основу за то нам даје *Аксиома доброг заснивања*

> Сваки непразан скуп A садржи елемент a такав да је $A \cap a = \emptyset$.

Став 1.22 Важи следеће

а) Не постоји скуп x такав да $x \in x$;

б) Не постоје скупови x и y за које важи $x \in y \in x$;

в) Не постоје скупови x и y за које важи $(x, y) \in x$.

Доказ. Све набројано веома једноставно следи из наведене Аксиоме доброг заснивања.

Доказ за а) Ако је скуп x такав да је $x \in x$, тада би скуп $A = \{x\}$ противречио Аксиоми доброг заснивања (његов једини елемент x има непразан пресек са њим).

Доказ за б) Нека за скупове x и y важи $x \in y \in x$. Формирајмо скуп $A = \{x, y\}$. По Аксиоми доброг заснивања он садржи елемент дисјунктан са њим. Но, то не може бити елемент x пошто $y \in A \cap x$, а не може то бити ни елемент y, јер $x \in A \cap y$. Закључујемо да такви скупови не могу постојати.

Доказ за в) На исти начин, уколико је $(x, y) \in x$, за неке скупове x и y, формирањем скупа $A = \{x, \{x\}, (x, y)\}$ добијамо контрадикцију. $\square$

Осим овог става наведимо и следећи, који ће нам бити користан касније.

Став 1.23 Ако су скупови x и y такви да је $x \cup \{x\} = y \cup \{y\}$, тада је $x = y$.

Доказ. Како је $x \in x \cup \{x\}$ то $x \in y \cup \{y\}$. Ако је $x = y$ то је тврђење доказано. У супротном добијамо $x \in y$. Слично, $y \in y \cup \{y\}$, па $y \in x \cup \{x\}$ и ако је $y \neq x$ добијамо да је и $y \in x$, а видели смо да такви скупови не могу постојати. $\square$

1.5 Задаци за вежбу

1. Доказати следеће скуповне идентитете:
   (а) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   (б) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (в) $A \cap (A \cup B) = A$
   (г) $A \cup (A \cap B) = A$
   (д) $(A \cap B) \cup (B \cap C) \cup (A \cap C) = (A \cup B) \cap (B \cup C) \cap (A \cup C)$
2. Испитати да ли постоје скупови A, B, C за које важи: $A \cap B \neq \emptyset$, $A \cap C = \emptyset$ и $(A \cap B) \setminus C = \emptyset$.
3. Нека су A, B и C произвољни скупови. Доказати или оповргнути:
   (а) $A \setminus (B \setminus C) = (A \setminus B) \setminus C$ **акко** $A \cap C = \emptyset$.
   (б) $A \cup (B \setminus C) = (A \cup B) \setminus C$ **акко** $A \cap C = \emptyset$.
   (в) $A \cap (B \setminus C) = (A \cap B) \setminus C$.
   (г) $A \cup (B \cap C) = (A \cup B) \cap C$ **акко** $A \subseteq C$.
   (д) $A \cap (B \triangle C) = (A \cap B) \triangle C$ **акко** $C \subseteq A$.

(ђ) $A \cup (B \triangle C) = (A \cup B) \triangle C$ **акко** $A \cap C = \emptyset$.

(е) $A \setminus (B \triangle C) = (A \setminus B) \triangle C$ **акко** $A \cap C = B$.

(ж) $A \triangle (B \setminus C) = (A \triangle B) \setminus C$ **акко** $A \cap C = \emptyset$.

4. Нека $f\colon X \to Y$. Доказати или оповргнути:

   (а) $f[f^{-1}[f[A]]] = f[A]$ за сваки $A \subseteq X$;

   (б) $f^{-1}[f[f^{-1}[B]]] = f^{-1}[B]$ за сваки $B \subseteq Y$;

   (в) f је „1–1“ **акко** $f[A \cap B] = f[A] \cap f[B]$, за све $A, B \subseteq X$;

   (г) f је „1–1“ **акко** $f[A \triangle B] = f[A] \triangle f[B]$ за све $A, B \subseteq X$;

   (д) $f[A \cap f^{-1}[B]] = f[A] \cap B$ за све $A \subseteq X$ и $B \subseteq Y$;

   (ђ) $f[A \triangle f^{-1}[B]] = f[A] \triangle B$ за све $A \subseteq X$ и $B \subseteq Y$;

   (е) $f[f^{-1}[B] \setminus A] = B \setminus f[A]$ за све $A \subseteq X$ и $B \subseteq Y$.

5. Доказати да је $f\colon X \to Y$ „1–1“ **акко** постоји $g\colon Y \to X$ тако да је $g \circ f = \mathrm{Id}_X$.

6. Нека су X и Y скупови за које постоји функција $f\colon X \to Y$ која је „на“. Доказати да тада постоји и функција $g\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ која је „1–1“.

7. Нека $f, g\colon X \to Y$. Доказати или оповргнути

$$f = g \ \textbf{акко} \ f^{-1}[g[A]] \supseteq A \text{ за сваки } A \subseteq X$$

8. Испитати да ли постоји непразан скуп X са бар два елемента и функција $f\colon X \to X$ таква да је $f[A] \cap A = \emptyset$ за сваки $A \subseteq X$, који има највише два елемента.

9. Доказати:

   (а) Ако је $A \triangle B = C \triangle D$ онда је $A \triangle C = B \triangle D$;

   (б) $A \subseteq B \cup C \Longleftrightarrow A \setminus B \subseteq C$;

   (в) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$;

   (г) $(A_1 \cap \cdots \cap A_n) \triangle (B_1 \cap \cdots \cap B_n) \subseteq (A_1 \triangle B_1) \cup \cdots \cup (A_n \triangle B_n)$.

10. Доказати без коришћења карактеристичних функција:

$$C \subseteq A \Rightarrow (A \cap B) \triangle C = A \cap (B \triangle C).$$

11. Нека су A, B и C произвољни скупови. Доказати: $A \cap (B \triangle C) = B$ ако и само ако је $A \cap C = \emptyset$ и $B \subseteq A$.

12. Решити систем једначина

$$\begin{array}{rcl} A \cap X & = & B \\ A \cup X & = & C \end{array}$$

Посебно обратити пажњу на услове које „коефицијенти“ A, B и C морају да испуњавају да би систем имао решење.

13. Нека је A произвољан непразан скуп. Доказати или оповргнути: ако је $A \cap X = A \cap Y$ и $A \cup X = A \cup Y$ онда је $X = Y$.

14. Дати су скупови A и B. Одредити који услов ти скупови морају да задовољавају да би постојао скуп X такав да је $A \cap X = B \cup X$ и за скупове који тај услов задовољавају наћи све такве X.

15. Нека је X непразан скуп. На његовом партитивном скупу $\mathcal{P}(X)$ дефинишимо операцију $*$ са

$$A * B := A \triangle B^c.$$

   (а) Показати да је $(\mathcal{P}(X), *)$ Абелова[8] група.

   (б) Ако је $|X| = n$, показати да је горе дефинисана група изоморфна групи $(\mathbb{Z}_2)^n$.

16. Дат је скуп X и његови подскупови $A_0, \ldots, A_{n-1}$. Доказати да се од подскупова A_i, коришћењем операција уније, пресека и комплемента може добити највише 2^{2^n} подскупова скупа X, а затим и навести пример у коме се ова граница достиже.

17. Показати да за сваки скуп a важи $\{a\} \times \{a\} = \{\{\{a\}\}\}$.

18. Испитати да ли постоје скупови x, y, z за које важи $x \in y \in z \in x$.

19. Испитати да ли постоји скуп x такав да је $\{x\} \in x$.

20. Показати да не постоји скуп који садржи све једночлане скупове.

21. Испитати да ли постоји скуп x такав да је $\{x\} \subseteq x$.

22. Испитати да ли постоји скуп x такав да је $(x, x) \in x$.

23. Доказати: $a \neq \emptyset \Rightarrow a \neq a \times a$.

24. Нека су A, B, C, D непразни скупови. Доказати: $A \times B = C \times D$ ако и само ако је $A = C$ и $B = D$.

25. Доказати да не постоји непразан скуп A такав да је $(A \times A) \times A = A \times (A \times A)$.

[8]Niels Henrik Abel (1802–1829), норвешки математичар.

26. Знамо да постоји бијекција између $\mathcal{P}(X)$ и 2^X. Испитати да ли постоји непразан скуп X за који важи једнакост $\mathcal{P}(X) = 2^X$.

27. Дефинишимо $\langle x, y\rangle$ са

$$\langle x, y\rangle \stackrel{\text{def}}{=} \{\{\emptyset, \{x\}\}, \{\{y\}\}\}.$$

Показати да је основна особина уређеног пара

$$\langle x, y\rangle = \langle u, v\rangle \iff x = u \text{ и } y = v$$

испуњена и при овој дефиницији (ово је алтернативна дефиниција уређеног пара).

28. Нека је на непразном скупу X дефинисана бинарна релација ρ која има следећа својства

(а) $\forall y \exists x (x \,\rho\, y)$;

(б) $\forall x \forall y \forall z (x \,\rho\, y \wedge x \,\rho\, z \Rightarrow y \,\rho\, z)$.

Испитати да ли ρ мора бити релација еквиваленције.

29. Нека су ρ и σ бинарне релације на скупу A. Доказати или оповргнути:

$$\rho^2\sigma^2 = (\rho\sigma)^2 \Rightarrow \rho\sigma = \sigma\rho.$$

30. Нека су $f, g \colon X \to X$ функције за које је

$$(f \circ g) \circ (f \circ g) = (f \circ f) \circ (g \circ g).$$

Испитати да ли из тих претпоставки следи да је $f \circ g = g \circ f$.

31. Нека је $\rho = \{(x, y) \in \mathbb{R}^2 : x^3 = y^2 + 3y + 1\}$. Одредити домен и слику релације ρ.

32. Нека је $\rho = \{(x, y) \in \mathbb{R}^2 : -1 \leq x - y \leq 2, -1 \leq x + y \leq 5\}$. Наћи домен и слику релације ρ.

33. Нека су ρ и σ две релације еквиваленције на скупу A. Показати да је релација $\sigma \cap \rho$ *увек* релација еквиваленције, док је релација $\sigma \circ \rho$ релација еквиваленције ако и само ако је $\sigma \circ \rho = \rho \circ \sigma$.

34. Нека је U непразан скуп и $C \subseteq U$. Дефинишимо релацију $\sim_C$ на скупу $\mathcal{P}(U)$ са:

$$A \sim_C B \textbf{ акко } A \triangle B \subseteq C.$$

Доказати да је $\sim_C$ једна релација еквиваленције и наћи класу еквиваленције датог скупа A.

35. Нека је $m \geq 2$ цео број. Дефинишемо бинарну релацију $\equiv_m$ на $\mathbb{Z}$ (релација конгруенције по модулу m) са: $a \equiv_m b$ ако и само ако $m \mid (a - b)$. Доказати да је $\equiv_m$ релација еквиваленције и показати да је

$$\equiv_m \cap \equiv_n \, = \, \equiv_{\mathrm{NZS}(m,n)}, \quad \equiv_m \circ \equiv_n \, = \, \equiv_{\mathrm{NZD}(m,n)} .$$

36. Наћи најмању релацију еквиваленције, која садржи релацију ρ дефинисану на скупу позитивних целих бројева са:

$$a \, \rho \, b \textbf{ акко } \mathrm{NZD}(a, b) = 1.$$

37. На скупу $\mathcal{L}$, свих правих у еуклидској[9] равни, посматрајмо релацију $\perp$, тј. релацију ортогоналности. Наћи најмању релацију еквиваленције, која садржи релацију $\perp$.

38. На скупу свих равни у еуклидском простору посматрајмо релацију ортогоналности $\perp$. Наћи најмању релацију еквиваленције, која садржи ову релацију.

39. На скупу $\mathcal{K}$, свих кружница у равни, дефинисана је релација ρ са: $k_1 \, \rho \, k_2$ ако и само ако се кружнице k_1 и k_2 додирују. Наћи најмању релацију еквиваленције, која садржи ову релацију.

40. Наћи најмању релацију еквиваленције, која садржи релацију стандардног уређења $\leq$ на скупу целих бројева.

41. На скупу $\mathbb{R}^2$ дефинишимо релацију $\preceq$ парцијалног уређења са: $(a, b) \preceq (c, d)$ ако и само ако је $a \leq c$ и $b \leq d$, где је са $\leq$ означена стандардна релација поретка на $\mathbb{R}$.

    (а) Доказати да је овако заиста дефинисана једна релација парцијалног уређења.

    (б) Посматрајмо „троугао“ $T = \{(x, y) \in \mathbb{R}^2 : x \geq 0, y \geq 0, x + 2y \leq 1\}$. Наћи максималне и минималне елементе у T. Да ли у T постоји највећи, односно најмањи елемент?

[9] $E\upsilon\kappa\lambda\epsilon\iota\delta\eta\sigma$ (око 325 – око 265 п.н.е.), грчки математичар.

Глава 2

Коначни и бесконачни скупови

2.1 Аксиома бесконачности и природни бројеви

Погледајмо мало „са стране“ оно што смо до сада урадили. Користећи до сада уведене аксиоме, у могућности смо да конструишемо искључиво коначне скупове. Наиме, пошли смо од празног скупа и вршили унирање скупова, формирање скупова од два елемента, формирање скупа свих подскупова, издвајање подскупова и слично. Ниједна од тих операција не може „направити“ бесконачан скуп. Да би се још више убедили у то, проверимо да ли можда можемо наћи неки математички објекат који испуњава до сада наведене аксиоме.

Објекат који тражимо није тешко наћи. За то нам је потребан неки скуп V и нека бинарна релација на њему која представља *интерпретацију* за $\in$. За скуп V узећемо скуп природних бројева, а релацију ε на скупу V дефинишемо на следећи начин. Нека је m било који природан број. Тада се m може на јединствен начин записати у облику

$$m = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k},$$

тако да важи $m_1 > m_2 > \ldots > m_k$ (бинарни запис броја n). Тада дефинишемо релацију ε са

$$n \,\varepsilon\, m \overset{\text{def}}{\iff} n = m_i, \text{ за неко } i.$$

Видимо да сваки природан број „садржи“, у смислу овако уведене релације ε, највише коначно много елемената. На пример 0 одговара празном скупу. Ако су x и y два различита броја онда скупу $\{x, y\}$ одговара број $2^x + 2^y$ и слично. Заправо се лако може проверити да су за ову структуру испуњене све аксиоме.

Нема много смисла градити теорију скупова да бисмо онда искључиво разматрали коначне скупове у оквиру те теорије. Стога нам је потребна и аксиома која гарантује постојање бар једног бесконачног скупа (ми ћемо иначе тек касније увести дефиницију појма бесконачног скупа, а бесконачност је и иначе врло суптилан појам). То је *Аксиома бесконачности.*

Постоји скуп A који садржи 0 и са сваким својим елементом x садржи и $x \cup \{x\}$.

Формалнији запис је

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

Теорема 2.1 Постоји тачно један скуп ω за који важи:

(1) $0 \in \omega$;

(2) $(\forall x \in \omega) x \cup \{x\} \in \omega$;

(3) Ако је $C \subseteq \omega$ подскуп који задовољава (1) и (2), онда је $C = \omega$.

Доказ. Аксиома бесконачности тврди да постоји скуп који испуњава прва два својства. За тражени скуп ω довољно је узети скуп који је пресек скупа свих подскупова тог скупа, који задовољавају та два својства. Непосредно се проверава да тако добијени скуп испуњава и треће тражено својство. □

Скуп ω из наведене теореме није ништа друго до *скуп природних бројева.* Наравно да смо навикли да скуп природних бројева означавамо са $\mathbb{N}$, али ћемо се ипак за сада задржзати на уведеној ознаци. Са $s(m)$, или са m' означаваћемо скуп $m \cup \{m\}$ и звати га *следбеник од* m. Сетимо се да је у Ставу 1.23 доказано да је функција $f{:}\,\omega \to \omega$ задата са $f(m) = m'$ једна инјекција. Својство (3) скупа природних бројева издвојићемо у облику добро познатог принципа (математичке) индукције.

Теорема 2.2 Нека је $C \subseteq \omega$ скуп за који важи:

(1) $0 \in C$;

(2) $\forall m(m \in C \Rightarrow m' \in C)$.

Тада је $C = \omega$.

Подсетимо се да за сада у употреби имамо релацију $\in$ и релацију $\subseteq$, која је непосредно изведена из ње. Ми знамо да у скупу природних бројева осим релације $<$ имамо и операције сабирања и множења. У наредном тексту показаћемо како се ова релација и те операције могу увести и извести њихова основна својства.

Лема 2.3 Нека су $m, n \in \omega$ и нека $n \in m$. Тада $n \subseteq m$.

Доказ. У доказу користимо горе формулисани принцип индукције. Нека је $C = \{m \in \omega : (\forall n \in \omega)(n \in m \Rightarrow n \subseteq m)\}$. Тада 0 припада C јер 0 не садржи ниједан елемент, па је тражена импликација тривијално тачна. Нека $m \in C$. Треба проверити да ли $m' \in C$. Претпоставимо да $n \in m' = m \cup \{m\}$. Ако је $n = m$, то закључак следи. У супротном $n \in m$ па , како $m \in C$ то добијамо да је $n \subseteq m \subset m'$, те закључујемо да је и у овом случају $n \subseteq m'$. Како скуп C испуњава услове предвиђене принципом индукције, добијамо да је $C = \omega$ што се и тражило. $\square$

Став 2.4 Нека су $m, n \in \omega$. Тада важи следеће

$$m \in n \textbf{ акко } m \subset n.$$

Доказ. Нека је $m \in \omega$ произвољан елемент. Формирајмо скуп

$$C = \{n \in \omega : m \in n \text{ акко } m \subset n\}.$$

Испитајмо пре свега да ли 0 припада C. Како је 0 празан скуп, то су обе релације нетачне увек, па је еквиваленција тачна и добијамо да 0 припада C. Нека је $n \in C$. Треба показати да и n' припада C, тј. да за n' важи

$$m \in n' \iff m \subset n'.$$

Претпоставимо да $m \in n' = n \cup \{n\}$. Ако $m \in n$, то закључујемо (пошто по претпоставци $n \in C$) да је $m \subset n$, па је и $m \subset n'$. У случају да је $m = n$, то добијамо да је $m = n \subseteq n \cup \{n\}$, а како $n \notin n$, то добијамо да је $m \subset n \cup \{n\}$. За доказ другог смера, претпоставимо да је $m \subset n'$. Поставља се питање: да ли $n \in m$? Ако би $n \in m$ било испуњено, онда би по Леми 2.3 добили да је $n \subseteq m$ и осим тога би важило $\{n\} \subseteq m$, па бисмо добили да је $n' = n \cup \{n\} \subseteq m \subset n'$ што није могуће. Закључујемо да $n \notin m$. Пошто је $m \subset n'$, а m не садржи n, то је $m = n$ или је $m \subset n$. Уколико је $m = n$, тада непосредно добијамо $m \in n'$, а уколико је $m \subset n$ из претпоставке да $n \in C$, добијамо да је $m \in n \subseteq n'$, тј. $m \in n'$. Закључујемо да и n' припада C, па је по принципу индукције $C = \omega$. $\square$

Став 2.5 Нека су $m, n \in \omega$. Тада

$$m \in n \vee m = n \vee n \in m.$$

Доказ. Као и у претходним случајевима, формирајмо скуп C. Овај пут за скуп C узимамо

$$C = \{m \in \omega : (\forall n \in \omega)(m \in n \vee m = n \vee n \in m)\}.$$

Проверимо најпре да $0 \in C$. У ту сврху, нека је $n \in \omega$ произвољан елемент. За $n = 0$ је јасно, а ако је $n \neq 0$, тада је $0 \subset n$ те, према претходном ставу $0 \in n$. Дакле, $0 \in C$. Претпоставимо да $m \in C$ и нека је $n \in \omega$ произвољан елемент. Треба показати да важи

$$m' \in n \vee m' = n \vee n \in m'.$$

Претпоставили смо да $m \in C$. То значи да можемо да разликујемо три случаја:

$\underline{m \in n}$ Тада је, по претходном ставу $m \subset n$ и добијамо $m' = m \cup \{m\} \subseteq n$. Или је $m' = n$, или је $m' \subset n$. У првом случају добијамо тражено, док у другом случају, још једна примена претходног става даје $m' \in n$, па и тада добијамо оно што нам је требало.

$\underline{m = n}$ Овде непосредно добијамо да $n \in m \cup \{m\} = m'$.

$\underline{n \in m}$ И овде је све јасно, јер следи да $n \in m'$. $\square$

Доказали смо довољно особина природних бројева (то јест елемената скупа ω) да можемо да дефинишемо релацију строгог уређења на том скупу са

$$m < n \overset{\text{def}}{\iff} m \in n.$$

Тада је ова релација антирефлексивна (јер за све $m \in \omega$ важи: $m \notin m$), транзитивна (што следи из резултата: $m \in n \iff m \subset n$), а такође важи и *закон трихотомије*: за све $m, n \in \omega$

$$m < n \vee m = n \vee n < m,$$

тј. свака два елемента су упоредива. Ако релација поретка има такво својство онда за њу кажемо да је релација *линеарног* уређења. Приметимо да се релација $\leq$ стандардно дефинише са $m \leq n \iff m < n \vee m = n$. Тада важи и $m < n \iff s(m) \leq n$. Дакле, на скупу ω релација $<$ заправо је релација $\in$, а поклапа се и са релацијом $\subset$! То необично својство је заправо типично за посебан тип скупова (у које спада и скуп природних бројева). Такве скупове, који се називају ординали, изучаваћемо касније и они представљају природан продужетак бројања када, да се тако изразимо, у бројању „потрошимо“ све природне бројеве.

Наведимо сада други принцип индукције, који је познат и под називом *потпуне индукције*, или под нетачним називом *трансфинитне индукције* (трансфинитна индукција је индукција по ординалима и њена сличност са ниже формулисаним принципом донекле оправдава лошу употребу тог појма).

Теорема 2.6 Нека је $C \subseteq \omega$ за који важи следеће. За сваки природан број m испуњен је услов: ако је сваки природан број n који је мањи од m у скупу C, онда и m мора припадати C. Симболима

$$(\forall m \in \omega)((\forall n < m) n \in C \Rightarrow m \in C).$$

Тада је $C = \omega$.

Доказ. Овај доказ није тако једноставан као претходни докази. Наиме, нећемо показати да $0 \in C$ и да из $n \in C$ следи $n' \in C$. Уместо тога, уводимо помоћни скуп D са $D = \{m \in \omega : (\forall n < m)(n \in C)\}$. Ако покажемо да је $D = \omega$, лако добијамо да је и $C = \omega$. Наиме, претпоставимо да смо показали да је $D = \omega$ и нека је $m \in \omega$ произвољан елемент. Како је $m < m'$, а $m' \in D$, јер је наравно $m' \in \omega$, а $D = \omega$, то, *по дефиницији* скупа D (погледајте ту дефиницију поново!) следи да $m \in C$. Дакле, $\omega \subseteq C \subseteq \omega$, па је $C = \omega$. Према томе, скуп D јесте користан.

Докажимо сада да је $D = \omega$. Овај доказ *јесте* као и претходни. Наиме, $0 \in D$, јер не постоји елемент мањи од 0, па је тражени услов тривијално испуњен. Нека је $m \in D$. Треба показати да је $m' = m \cup \{m\}$ такође у D. Ако се још једном подсетимо дефиниције скупа D онда видимо шта треба радити. Узмимо било који елемент n такав да је $n < m'$. Тада постоје две могућности. Или је $n < m$, у ком случају користимо претпоставку да $m \in D$ да бисмо закључили да $n \in C$. У другом случају је $n = m$ и сада (најзад!) користимо услов који је испуњен за скуп C. Наиме, како је $m \in D$ то је $(\forall k < m) k \in C$. По услову који скуп C задовољава, закључујемо да и $n = m \in C$. Према томе, за скуп D испуњени су тражени услови за примену принципа индукције, па је према томе, $D = \omega$ што завршава тражени доказ. $\square$

Наведимо сада још једно веома важно својство скупа природних бројева у оквиру следеће теореме.

Теорема 2.7 Сваки непразан подскуп скупа природних бројева има најмањи елемент.

Доказ Нека је A подскуп скупа ω и претпоставимо да A *нема* најмањи елемент. У доказу користимо управо доказани принцип потпуне индукције. Наиме, показаћемо да је скуп C дефинисан са $C = \omega \setminus A$ једнак ω из чега закључујемо да је $A = \emptyset$ (дакле, једини подскуп од ω који *нема* најмањи елемент је празан скуп, тј. скуп који уопште нема елемената). Нека је $m \in \omega$ произвољан природан број и нека је $(\forall n < m) n \in C$. Уколико $m \notin C$ закључујемо да $m \in A$, а како A нема најмањи елемент то у A постоји елемент мањи од m, што противречи претпоставци. Дакле, закључујемо да $m \in C$, па скуп задовољава услов за потпуну индукцију. Према томе, $C = \omega$, чиме је доказ завршен. $\square$

Дефиниција 2.8 За парцијално уређени скуп кажемо да је **добро уређен**, ако у њему сваки непразан подскуп има најмањи елемент.

Видимо да је скуп природних бројева добро уређен. О добро уређеним скуповима и њиховим својствима биће речи у даљем излагању. Из добре уређености скупа природних бројева следи принцип потпуне индукције.

Сада ћемо се позабавити дефинисањем операција сабирања и множења природних бројева и доказивањем основних својстава тих операција. Операције ћемо дефинисати методом *рекурзије*, који у најједноставнијем случају гласи: функција се на јединствен начин може задати на скупу ω, уколико се зада на 0 и зада се правило којим се од вредности у n (или од вредности у свим m, за $m < n$) добија вредност у n' (односно у n). Правило о коме је реч је такође задато функцијом (можда и од више аргумената). Ми се нећемо детаљније бавити засниванјем тог правила, које ће читаоцу сигурно бити јасно из наведених примера.

Сабирање дефинишемо на следећи начин. Нека је $m \in \omega$, тада

$$m + 0 \stackrel{\text{def}}{=} m \tag{2.1}$$

$$m + n' \stackrel{\text{def}}{=} (m + n)'. \tag{2.2}$$

Заправо радимо следеће. За дато m дефинишемо функцију $plus_m$ (која треба да представља сабирање са m) на ω са $plus_m(0) = m$ и $plus_m(n') = (plus_m(n))'$. Принцип рекурзије каже да је тако добро дефинисана једна функција на скупу ω и да је она овим једначинама јединствено задата. Убудуће ова прецизирања нећемо посебно давати.

Подсетимо се да је $1 \stackrel{\text{def}}{=} 0'$, $2 \stackrel{\text{def}}{=} 1'$ итд. Тада је

$$\begin{array}{rcll} m+1 & = & m+0' & \text{по дефиницији јединице} \\ & = & (m+0)' & \text{по } (2.2) \\ & = & m' & \text{по } (2.1) \end{array}$$

Следећи став описује добро нам позната својства сабирања природних бројева.

Став 2.9 Нека су $m, n, p \in \omega$. Тада

(1) $(m + n) + p = m + (n + p)$;

(2) $0 + m = m$;

(3) $m + 1 = 1 + m$;

(4) $m + n = n + m$.

Доказ. Користимо принцип индукције, али на „традиционалнији начин“. Доказ за (1): индукцијом по p

$$\begin{array}{rcll} (m+n)+0 & = & m+n & \text{по } (2.1) \\ & = & m+(n+0) & \text{по } (2.1). \end{array}$$

Нека је тврђење тачно за p, тј. нека је

$$(m + n) + p = m + (n + p). \tag{2.3}$$

Тада

$$\begin{array}{rcll} (m+n)+p' & = & ((m+n)+p)' & \text{по } (2.2) \\ & = & (m+(n+p))' & \text{по } (2.3) \\ & = & m+(n+p)' & \text{по } (2.2) \\ & = & m+(n+p') & \text{по } (2.2). \end{array}$$

Доказ за (2): индукцијом по m

$$0 + 0 = 0 \text{ по } (2.1)$$

Претпоставимо $0 + m = m$.

$$\begin{aligned} 0 + m' &= (0 + m)' && \text{по } (2.2) \\ &= m' && \text{по претпоставци.} \end{aligned}$$

Доказ за (3): Видели смо да је $m + 1 = m'$. Треба дакле доказати $1 + m = m'$. За $m = 0$ то је јасно ($1 + 0 = 1$ и $0' = 1$). Нека је то тачно за m. Тада је

$$1 + m' = (1 + m)' = (m')',$$

што је и требало показати.
Доказ за (4): У овом доказу користићемо (3), што је, наравно, специјалан случај за (4). Радићемо индукцијом по n. Пре свега $m+0 = m = 0 + m$ (последња једнакост је заправо једнакост (2)). Претпоставимо да је тврђење тачно за n. Тада

$$\begin{aligned} m + n' &= (m + n)' && \text{по дефиницији} \\ &= (n + m)' && \text{по претпоставци} \\ &= n + m' && \text{по дефиницији} \\ &= n + (1 + m) && \text{по } (3) \\ &= (n + 1) + m && \text{по } (1) \\ &= n' + m && \text{по раније доказаном.} \end{aligned}$$

□

Следећи став дајемо без доказа. Предлажемо да читалац уради (једноставан) доказ овог става за вежбу.

Став 2.10 (1) За сваки природан број n, различит од нуле, постоји природан број m такав да је $n = m + 1$.
(2) $m + n = 0 \Rightarrow m = n = 0$.
(3) $m + p = n + p \Rightarrow m = n$.

Операција множења се дефинише на следећи начин.

$$m \cdot 0 \stackrel{\text{def}}{=} 0 \tag{2.4}$$

$$m \cdot n' \stackrel{\text{def}}{=} m \cdot n + m \tag{2.5}$$

Став 2.11 Нека су $m, n, p \in \omega$. Тада

(1) $m \cdot (n + p) = m \cdot n + m \cdot p$;

(2) $(m \cdot n) \cdot p = m \cdot (n \cdot p)$;

(3) $0 \cdot m = 0$;

(4) $1 \cdot m = m$;

(5) $(m + n) \cdot p = m \cdot p + m \cdot n$;

(6) $m \cdot n = n \cdot m$;

(7) $m \cdot n = 0 \Rightarrow m = 0 \vee n = 0$.

Доказ. Овај пут ће докази бити сажетији него у ранијим случајевима, пошто нам је метод већ добро познат.
Доказ за (1) За $p = 0$: $m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$. Нека је тврђење тачно за p. Тада

$$\begin{aligned} m \cdot (n + p') &= m \cdot (n + p)' \\ &= m \cdot (n + p) + m \\ &= (m \cdot n + m \cdot p) + m \\ &= m \cdot n + (m \cdot p + m) \\ &= m \cdot n + m \cdot p'. \end{aligned}$$

Доказ за (2) За $p = 0$ је јасно. Нека је тачно за p. Тада

$$\begin{aligned} (m \cdot n) \cdot p' &= (m \cdot n) \cdot p + m \cdot n \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= m \cdot (n \cdot p + n) \\ &= m \cdot (n \cdot p'). \end{aligned}$$

Доказ за (3) Једноставно.
Доказ за (4) Једноставно.
Доказ за (5) За $p = 0$ је јасно. Ако је тачно за p добијамо

$$\begin{aligned} (m + n) \cdot p' &= (m + n) \cdot p + (m + n) \\ &= (m \cdot p + n \cdot p) + (m + n) \\ &= m \cdot p + (n \cdot p + (m + n)) \\ &= m \cdot p + ((n \cdot p + m) + n) \\ &= m \cdot p + ((m + n \cdot p) + n) \\ &= (m \cdot p + (m + n \cdot p)) + n \\ &= ((m \cdot p + m) + n \cdot p) + n \\ &= (m \cdot p' + n \cdot p) + n \\ &= m \cdot p' + (n \cdot p + n) \\ &= m \cdot p' + n \cdot p'. \end{aligned}$$

Доказ за (6) За $n = 0$ следи из дефиниције и (3). Ако је тачно за n тада

$$\begin{aligned} m \cdot n' &= m \cdot n + m \\ &= n \cdot m + m \\ &= n \cdot m + 1 \cdot m \\ &= (n+1) \cdot m \\ &= n' \cdot m. \end{aligned}$$

Доказ за (7) Нека је $m \cdot n = 0$ и $n \neq 0$. Тада према Ставу 2.10 постоји k такав да је $n = k + 1$. Тада је

$$0 = m \cdot n = m \cdot (k+1) = m \cdot k + m \cdot 1 = m \cdot k + m,$$

одакле, према истом ставу следи да је $m = 0$. □

Овим се завршава увођење и утврђивање основних својстава природних бројева.

2.2 Коначни, пребројиви и непребројиви скупови

Започнимо овај одељак следећим једноставним ставом.

Став 2.12 Ако постоји бијекција $f: m \to n$, где $m, n \in \omega$, тада је $m = n$.

Доказ. Доказаћемо наведено тврђење индукцијом по m. Ако је $m = 0$, онда је јасно да мора и n бити једнако нули, па тврђење следи. Претпоставимо да је тврђење тачно за m и све $n \in \omega$ и нека је $f: m' \to n$ бијекција. Како је $m' \neq 0$, то мора бити и $n \neq 0$. Према Ставу 2.10, $n = p + 1$ за неко p. Дакле, f је бијекција између $m' = m \cup \{m\}$ и $p + 1 = p' = p \cup \{p\}$. Проверимо где се при тој бијекцији слика елемент m. Ако је $f(m) = p$, то је $f[m] = p$ (обратити пажњу на ознаке: у првом случају се ради о вредности функције f у тачки m, док је у другом случају у питању *директна слика* скупа m при пресликавању f) и рестрикција $f|_m$ функције f на скуп m представља бијекцију између m и p. По индуктивној претпоставци добијамо да је $m = p$, па је и $m' = p' = n$, што је и требало показати. У случају да је $f(m) \neq p$, дефинишемо функцију $g: n \to n$ са

$$g(x) = \begin{cases} p, & x = f(m) \\ f(m), & x = p \\ x, & \text{иначе} \end{cases}$$

Јасно је да је функција $g: n \to n$ бијекција и да је за функцију $h = g \circ f$, $h(m) = p$ (функција g је и уведена да би се то постигло). Но, на функцију h можемо применити претходно закључивање чиме се доказ завршава. □

Дефиниција 2.13 За скуп X кажемо да је коначан ако за неки природан број n постоји бијекција $f\colon X \to n$.

На основу претходног става, природан број који је у бијекцији са скупом X (ако постоји) јединствен је и тада пишемо

$$|X| = n$$

и кажемо да скуп X има n елемената (наравно да то одговара нашем добро развијеном појму о броју елемената коначног скупа).

За скуп кажемо да је *бесконачан* ако није коначан. Појам бесконачности је од непроцењивог значаја у скоро свим математичким дисциплинама и то је врло суптилан појам. За сада само приметимо да постоји алтернативна дефиниција појма бесконачног скупа: скуп је бесконачан ако постоји бијекција између тог скупа и неког његовог правог подскупа. Ми за сада *нисмо* у могућности да докажемо еквивалентност тако уведене дефиниције са оном коју смо већ дали, али ћемо се касније и тиме позабавити. Докажимо за сада само следећи став.

Став 2.14 Нека је скуп X коначан и A прави подскуп од X. Тада не постоји бијекција између X и A.

Доказ. Како је X коначан и тиме у бијекцији са неким природним бројем, то је довољно претпоставити да је $X = n$, за неко $n \in \omega$. Доказаћемо тврђење индукцијом по n. Ако је $n = 0$, онда се и нема шта доказивати пошто празан скуп нема правих подскупова. Претпоставимо стога да је тврђење тачно за n и нека је $f\colon n' \to A$ бијекција између n' и неког његовог правог подскупа. Нека је $f(n) = a$. Ако је $a = n$, то рестрикција $f|_n$ задаје бијекцију између n и његовог правог подскупа $A \setminus \{n\}$ (подсетимо се да је $n' = n \cup \{n\}$). По претпоставци је то немогуће, па стога ни f не може бити бијекција. Ако је $a \neq n$, то као и у претходном доказу можемо увести помоћну бијекцију g са доменом A такву да композиција $g \circ f$ задовољава претходни услов, тако да се овај случај своди на већ разматрани. Читаоцу се препоручује да сам провери неопходне детаље. $\square$

До краја ове главе, за скуп природних бројева користићемо уобичајену ознаку $\mathbb{N}$. Приметимо да су операције одузимања и дељења *парцијално* дефинисане на $\mathbb{N}$. Наиме, ако је $m \geq n$, онда је $m - n$ број за који важи $(m-n)+n = m$ (читалац може проверити на основу којих резултата тврдимо да он постоји и да је јединствено одређен). Слично, дефинишемо релацију *дељивости* на скупу $\mathbb{N}$, са

$$a \mid b \stackrel{\text{def}}{\iff} (\exists c \in \mathbb{N}) b = a \cdot c.$$

У случају $a \neq 0$, тај број c јединствено је одређен и означавамо га са $\frac{b}{a}$.

Последица 2.15 Скуп природних бројева је бесконачан.

Доказ. Функција $f\colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$ дефинисана са $f(n) = n + 1$ успоставља бијекцију између скупа $\mathbb{N}$ и његовог правог подскупа $\mathbb{N} \setminus \{0\}$. Према претходном ставу закључујемо да скуп $\mathbb{N}$ не може бити коначан. $\square$

Како смо закључили да је скуп природних бројева бесконачан то следећа дефиниција има смисла.

Дефиниција 2.16 За скуп X кажемо да је пребројив уколико постоји бијекција $f\colon X \to \mathbb{N}$.

Став 2.17 Сваки подскуп пребројивог скупа или је пребројив или је коначан.

Доказ. Нека је X пребројив скуп и $A \subseteq X$. Како постоји бијекција $f\colon X \to \mathbb{N}$, то уместо скупа X и његовог подскупа A, можемо посматрати $\mathbb{N}$ и $f[A] \subseteq \mathbb{N}$. Дакле, довољно је показати да је сваки подскуп од $\mathbb{N}$ коначан или пребројив. Нека је $B \subseteq \mathbb{N}$. Дефинишемо функцију $h \subseteq \mathbb{N} \times B$, са

$$h(0) = \begin{cases} \min B, & \text{ако је } B \neq \emptyset \\ \text{није дефинисано}, & \text{ако је } B = \emptyset. \end{cases}$$

$$h(n') = \begin{cases} \min(B \setminus h[n]), & \text{ако је } h \text{ дефинисана на } n \text{ и } B \setminus h[n] \neq \emptyset \\ \text{није дефинисано}, & \text{иначе.} \end{cases}$$

Са $\min D$ означавамо најмањи елемент у непразном скупу D који постоји јер је скуп природних бројева добро уређен. Дакле, постоје две могућности: или је $\mathrm{Dom}(f) = \mathbb{N}$, у ком случају је h бијекција између $\mathbb{N}$ и B, или је $\mathrm{Dom}(h) = m$, за неко $m \in \mathbb{N}$ и тада је h бијекција између m и B. $\square$

Овај став делује врло једноставно и можда се појединим читаоцима може учинити и сувишан, али видећемо касније како једно слично питање доводи до озбиљних последица.

За скуп ћемо убудуће рећи да је *највише пребројив* ако је коначан или пребројив. Видели смо да то заправо значи да постоји инјекција тог скупа у скуп природних бројева.

Став 2.18 Скуп $\mathbb{N} \times \mathbb{N}$ је пребројив скуп.

Доказ. Представимо скуп $\mathbb{N} \times \mathbb{N}$ на следећи начин.

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

Како успоставити бијекцију између скупа $\mathbb{N}$ и скупа $\mathbb{N}\times\mathbb{N}$? Стрелице на слици указују на поступак:

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

Дакле, елементе „пребројавамо" дуж дијагоналних стрелица. Када завршимо са једном дијагоналом, прелазимо на прву суседну са десне стране. Делује јасно да је тако успостављена једна бијекција. Но, како да нађемо формулу за функцију која успоставља ову бијекцију? Покушајмо да то урадимо. Прва дијагонала има само један елемент – $(0,0)$; друга – два елемента $(0,1)$ и $(1,0)$, трећа – три итд. Конструишемо тражену бијекцију $g\colon\mathbb{N}\times\mathbb{N}\to\mathbb{N}$. Где се слика елемент (i,j)? Пре свега „редни број" дијагонале на којој се он налази је $i+j$ (почињемо од 0). Према томе, пре њега долазе сви елементи са дијагонала нижег реда, тј. реда $0,1,2,\ldots,i+j-1$, као и елементи: $(0,i+j),(1,i+j-1),\ldots,(i-1,j+1)$. Број елемената „испред" елемента (i,j) је дакле

$$1+2+3+\cdots+(i+j)+i=\frac{(i+j)(i+j+1)}{2}+i.$$

(Прва дијагонала има један члан, друга – два, итд; на „његовој" дијагонали има i чланова „испред" њега). Како пребројавање почиње од нуле то је „редни број" елемента (i,j) баш горе наведени број. Према томе, дефинишемо $g\colon\mathbb{N}\times\mathbb{N}\to\mathbb{N}$, са

$$g(i,j)\stackrel{\text{def}}{=}\frac{(i+j)(i+j+1)}{2}.$$

Према до сада размотреном, јасно је да g успоставља бијекцију између $\mathbb{N}\times\mathbb{N}$ и $\mathbb{N}$. Али, да бисмо се још више убедили, покажимо да је функција g, задата горњом формулом, заиста бијекција.

g је „на": Нека је $m\in\mathbb{N}$ произвољан елемент. Ако посматрамо вредности функције $h\colon\mathbb{N}\to\mathbb{N}$, дефинисане са $h(n)=\frac{n(n+1)}{2}$, видимо да је $h(n)>m$, за довољно велико n (довољно је узети $n=m+1$). Нека је n_0 најмањи природан број за који важи $h(n_0)>m$. Тада је $h(n_0-1)\leq m$ (приметимо да је $n_0\neq 0$, јер је за све m $h(0)=0\leq m$). Нека је

$i = m - h(n_0 - 1)$, а $j = n_0 - 1 - i$. Наравно, питамо се да ли је j добро дефинисан, тј. да ли је $n_0 - 1 \geq i$. Ако би било $i > n_0 - 1$, то бисмо имали $m - h(n_0 - 1) > n_0 - 1$ из чега следи

$$\begin{aligned} m &> h(n_0 - 1) + n_0 - 1 \\ &= \frac{(n_0 - 1)n_0}{2} + n_0 - 1 \\ &= (n_0 - 1)(\frac{n_0}{2} + 1) \\ &= \frac{(n_0 - 1)(n_0 + 2)}{2}. \end{aligned}$$

Међутим, $\frac{(n_0-1)(n_0+2)}{2} = \frac{n_0^2+n_0-2}{2} = \frac{n_0(n_0+1)}{2} - 1$, па бисмо добили $m+1 > h(n_0)$, тј. $m \geq h(n_0)$, што противречи избору броја n_0. Дакле, заиста је $i \leq n_0 - 1$ и j је добро дефинисано. Израчунајмо $g(i, j)$

$$\begin{aligned} g(i, j) &= g(i, n_0 - 1 - i) \\ &= \frac{(i + (n_0 - 1 - i))(i + (n_0 - 1 - i) + 1)}{2} + i \\ &= h(n_0 - 1) + m - h(n_0 - 1) \\ &= m. \end{aligned}$$

Дакле, g је „на“.

g је „1–1: Нека је $g(i, j) = g(i_1, j_1)$. Уведимо ознаке $n = i+j$ и $n_1 = i_1+j_1$. Ако је $n \neq n_1$, тада је $n > n_1$ или $n < n_1$. Нека је нпр. $n > n_1$. Тада

$$\begin{aligned} g(i_1, j_1) &= g(i, j) \\ &= h(n) + i \\ &\geq h(n_1 + 1) + i \\ &= \frac{(n_1 + 1)(n_1 + 2)}{2} + i \\ &= \frac{n_1^2 + 3n_1 + 2}{2} + i \\ &= \frac{n_1^2 + n_1 + 2(n_1 + 1)}{2} + i \\ &= \frac{n_1(n_1 + 1)}{2} + n_1 + 1 + i \\ &= h(n_1) + n_1 + 1 + i \\ &= h(n_1) + i_1 + j_1 + 1 + i \\ &> h(n_1) + i_1 \\ &= g(i_1, j_1). \end{aligned}$$

Према томе, не може бити $n > n_1$. Наравно да не може бити ни $n_1 > n$, те закључујемо да је $n = n_1$. Тада

$$h(n) + i = g(i, j) = g(i_1, j_1) = h(n_1) + i_1,$$

па добијамо да је $i = i_1$, из чега затим следи и $j = j_1$, те је функција g и „1–1“. $\square$

Као што видимо, није баш тако лако наћи бијекцију између два скупа. Срећом, касније ћемо доказати теорему која ће нам омогућити да закључимо да *постоји* бијекција између нека два скупа, а да је не морамо експлицитно конструисати. Но, у овом одељку још немамо ту теорему па смо приморани на експлицитне конструкције. Но, наравно да су експлицитне конструкције занимљиве и саме по себи. На крају одељка даћемо још један такав доказ.

Дефиниција 2.19 За скуп кажемо да је непребројив, ако није највише пребројив.

Другим речима за скуп који није ни коначан ни пребројив кажемо да је *непребројив*. У даљем ћемо подразумевати да су читаоцу добро позната основна својства реалних бројева, која је уосталом много пута до сада имао прилике да користи. Показаћемо да је скуп реалних бројева непребројив.

Претпоставимо супротно. Како скуп $\mathbb{R}$ сигурно није коначан ($\mathbb{N} \subset \mathbb{R}$), то ћемо претпоставити да је он пребројив. Како постоји бијекција између скупа $\mathbb{R}$ и отвореног интервала $(0, 1)$ (нађите ту бијекцију – можда ће вам у том покушају помоћи и функција тангенс), то добијамо да је и интервал $(0, 1)$ пребројив. Дакле, постоји бијекција $f\colon \mathbb{N} \to (0, 1)$. Стога је

$$(0, 1) = \{r_0, r_1, r_2, \ldots\}.$$

Сваки r_i се може на јединствен начин записати у децималном облику

$$r_i = 0.x_{i0}x_{i1}x_{i2}\ldots,$$

при чему претпостављамо да се запис не завршава са бесконачно много деветки, као и да се може завршавати са бесконачно много нула. Према томе

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

Посматрајмо сада „дијагоналне“ елементе у развојима (означене елементе) и формирајмо реални број $y \in (0, 1)$ тако да је $y = 0.y_0y_1y_2\ldots$, при чему је

$$y_i = \begin{cases} 5, & x_{ii} \neq 5 \\ 7, & x_{ii} = 5 \end{cases}$$

Тада је за све i: $y \neq r_i$ јер је $y_i \neq x_{ii}$. Стога $y \in (0,1) \setminus \{r_0, r_1, r_2, \ldots\} = \emptyset$, чиме смо добили контрадикцију. Закључујемо да скуп $(0,1)$, а тиме ни скуп $\mathbb{R}$, није пребројив.

Претходни поступак познат је под називом „Канторов дијагонални поступак“. Ми ћемо касније показати да постоји бијекција између скупа $\mathbb{R}$ и скупа $\mathcal{P}(\mathbb{N})$, а подсетимо се да не постоји бијекција између скупа X и $\mathcal{P}(X)$ ни за један скуп X. То је још један доказ чињенице да скуп $\mathbb{R}$ није пребројив.

Дакле, скуп реалних бројева је непребројив. Поставља се питање: да ли за скуп $\mathbb{R}$ важи став аналоган Ставу 2.17? Прецизније, да ли за скуп $\mathbb{R}$ важи следеће.

Нека је $A \subseteq \mathbb{R}$. Тада је A или коначан, или пребројив, или у бијекцији са $\mathbb{R}$.

Испоставља се да је то питање далеко сложеније него што се на први поглед може чинити. То питање се заправо своди на чувену *Канторову Континуум хипотезу*: сваки непребројив подскуп од $\mathbb{R}$ у бијекцији је са $\mathbb{R}$. Ми ћемо се касније вратити та ово питање, а за сада само споменимо да је континуум хипотезу немогуће ни доказати ни оповргнути коришћењем наведених аксиома теорије скупова.

Овај одељак завршавамо следећим примером.

Пример 2.20 Скуп $\mathcal{P}_{\text{fin}}(\mathbb{N})$ свих коначних подскупова од $\mathbb{N}$ је пребројив.

Први начин: Подсетимо се пре свега на чињеницу, која нам је из других курсева добро позната, а коју овом приликом нећемо доказивати. Број $k-$точланих подскупова скупа од n елемената је $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$.

Да бисмо доказали пребројивост наведеног скупа, показаћемо пре свега да су за свако $n \in \mathbb{N}$ сви скупови $\mathcal{P}_n(\mathbb{N})$ n-точланих подскупова од $\mathbb{N}$ пребројиви. Дефинишемо функције $f_n : \mathcal{P}_n(\mathbb{N}) \to \mathbb{N} \setminus \{0\}$ са

$$f_n(\{x_0, x_1, \ldots, x_{n-1}\}) = \binom{x_0}{1} + \binom{x_1}{2} + \cdots \binom{x_{n-1}}{n},$$

ако је $x_0 < x_1 < \cdots < x_{n-1}$. На пример $f_4(\{7,3,2,9\}) = \binom{2}{1} + \binom{3}{2} + \binom{7}{3} + \binom{9}{4}$. Показаћемо да је f_n бијекција. Приметимо најпре да је

$$f_n(\{x-n+1, x-n+2, \ldots, x\}) = \binom{x+1}{n} - 1.$$

То није тешко показати. Подсетимо се основног својства биномних коефицијената

$$\binom{y}{k} + \binom{y}{k+1} = \binom{y+1}{k+1}.$$

Ако се читалац можда не сећа ове релације, може је у сваком случају лако проверити. Сада добијамо

$$\begin{aligned}
& 1 + f_n(\{x-n+1, x-n+2, \dots, x\}) \\
= \; & 1 + \binom{x-n+1}{1} + \binom{x-n+2}{2} + \binom{x-n+3}{3} + \cdots \binom{x}{n} \\
= \; & \binom{x-n+1}{0} + \binom{x-n+1}{1} + \binom{x-n+2}{2} + \cdots + \binom{x}{n} \\
= \; & \binom{x-n+2}{1} + \binom{x-n+2}{2} + \binom{x-n+3}{3} + \cdots \binom{x}{n} \\
= \; & \binom{x-n+3}{2} + \binom{x-n+3}{3} + \cdots \binom{x}{n} \\
= \; & \binom{x-n+4}{3} + \cdots + \binom{x}{n} \\
\vdots \; & \quad \vdots \\
= \; & \binom{x}{n-1} + \binom{x}{n} \\
= \; & \binom{x+1}{n}.
\end{aligned}$$

Читалац за вежбу може овај доказ извести индукцијом. Ми ћемо сада индукцијом показати да за свако $m \in \mathbb{N} \setminus \{0\}$ једначина

$$f_n(\{x_0, \dots, x_{n-1}\}) = m, \tag{2.6}$$

где је $x_0 < x_1 < \cdots < x_{n-1}$ и $n \geq 1$ има јединствено решење. То је заправо преформулација тврђења да је функција f_n бијекција. Ако је $n = 1$ онда се наша једначина своди на $f_1(\{x_0\}) = m$ и резултат тривијално следи. Претпоставимо да је тврђење тачно за n и разматрајмо једначину

$$f_{n+1}(\{x_0, x_1, \dots, x_n\}) = m.$$

Јасно је да постоји јединствено y за које важи

$$\binom{y}{n} \leq m < \binom{y+1}{n}.$$

Проверити зашто је ово тачно! Како је

$$f_{n+1}(\{x_0, x_1, \dots, x_n\}) \leq f_{n+1}(\{x_n - n + 1, x_n - n + 2, \dots, x_n\}) = \binom{x_n + 1}{n} - 1,$$

то за x_n <u>морамо</u> узети наведено y. Наиме, ако је $x_n < y$, онда

$$f_{n+1}(\{x_0, x_1, \dots, x_n\}) \leq \binom{x_n + 1}{n} - 1 \leq \binom{y}{n} - 1 < \binom{y}{n} \leq m,$$

па једнакост $f_{n+1}(\{x_0, x_1, \ldots, x_n\}) = m$ не би могла важити. Не може бити ни $x_n > y$, јер је у том случају

$$f_{n+1}(\{x_0, x_1, \ldots, x_n\}) \geq \binom{x_n}{n} \geq \binom{y+1}{n} > m.$$

Пошто смо добили да је $x_n = y$, то се једначина 2.6 своди на једначину

$$f_{n-1}(\{x_0, x_1, \ldots, x_{n-1}\}) = m - \binom{y}{n},$$

а она, по индуктивној претпоставци има јединствено решење. Дакле и наша једначина има јединствено решење, те су све функције f_n бијекције. Да бисмо показали да је $\mathcal{P}_{\text{fin}}(\mathbb{N})$ пребројив формирајмо функцију

$$f\colon \mathcal{P}_{\text{fin}}(\mathbb{N}) \to \mathbb{N} \times \mathbb{N}$$

на следећи начин. Сваки елемент (сем празног скупа) из $\mathcal{P}_{\text{fin}}(\mathbb{N})$ је облика $\{x_0, x_1, \ldots, x_{n-1}\}$ за неко n и неке $x_0 < x_1 < \cdots < x_{n-1}$. Тада

$$f(\{x_0, x_1, \ldots, x_{n-1}\}) \stackrel{\text{def}}{=} (f_n(\{x_0, x_1, \ldots, x_{n-1}\}), n).$$

Додајмо још да вредност на празном скупу можемо задати са $f(\emptyset) = (0, 0)$. Сада се непосредно проверава да је тако добијена функција једна инјекција (проверити!). Према томе скуп $\mathcal{P}_{\text{fin}}(\mathbb{N})$ је највише пребројив, а како сигурно није коначан (сваки од скупова $\mathcal{P}_n(\mathbb{N})$ је пребројив) то закључујемо да је он пребројив.
Други начин: Функција $f\colon \mathcal{P}_{\text{fin}}(\mathbb{N}) \to \mathbb{N}$ задата са

$$f(S) = \sum_{n \in S} 2^n,$$

где је $S \in \mathcal{P}_{\text{fin}}(\mathbb{N})$ и где сматрамо да је $f(\emptyset) = 0$, јесте бијекција. Препуштамо читаоцу да докаже ту чињеницу.

2.3 Кантор–Бернштајнова теорема

Уведимо пре свега неке ознаке и терминологију. За скупове X и Y кажемо да имају исти кардинални број и пишемо $|X| = |Y|$, ако постоји бијекција између њих. Ако постоји инјекција из X у Y, онда пишемо $|X| \leq |Y|$. Наравно да $|X| < |Y|$ означава чињеницу да постоји инјекција из X у Y, али не и бијекција. На пример, до сада смо показали:

$$|X| < |\mathcal{P}(X)| \tag{2.7}$$

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}| \tag{2.8}$$

$$|\mathbb{N}| < |\mathbb{R}| \tag{2.9}$$

Јасно је да, ако важи $|X| \leq |Y|$ и $|Y| \leq |Z|$, онда важи и $|X| \leq |Z|$ (композиција инјекција је инјекција), као и $|X| \not< |X|$, али да ли је релација $\leq$ и антисиметрична (нећемо се за сада питати на ком објекту је та релација заиста дефинисана)? Одговор на то даје Кантор–Бернштајнова[1] теорема.

Теорема 2.21 Нека су X и Y скупови. Тада важи

$$|X| \leq |Y| \text{ и } |Y| \leq |X| \Rightarrow |X| = |Y|.$$

Доказ. Дакле, претпоставка је да постоје „1–1“ функције $f\colon X \to Y$ и $g\colon Y \to X$. Наш је задатак да покажемо да постоји бијекција $h\colon X \to Y$. Приметимо пре свега да можемо претпоставити да су скупови X и Y дисјунктни. Наиме ако нису дисјунктни, постоји стандардни „трик“, или ако се тако некоме више свиђа, метод, да се од њих формирају скупови исте кардиналности, а дисјунктни. Наиме можемо ставити $X_1 = X \times \{1\}$ и $Y_1 = Y \times \{2\}$. Тада су скупови X_1 и Y_1 дисјунктни. У даљем се враћамо на ознаке X и Y за наше скупове и претпостављамо да су дисјунктни. Даћемо два доказа ове теореме. Она по свом значају то и заслужује, а сваки од ова два доказа је по нечему интересантан и поучан, па је корисно да се читаоци упознају са оба доказа. Основна идеја у оба доказа је иста. Скуп X представићемо у облику дисјунктне уније скупова и онда ће наша бијекција на неким члановима уније бити дефинисана помоћу f, а на другим помоћу g. Подсетимо се још и чињенице, да је за „1–1“ функцију f дефинисана функција f^{-1}, тако да је $\mathrm{Dom}(f^{-1}) = \mathrm{Im}(f)$.

Први доказ. За $x \in X$ рећи ћемо да је родитељ од $y \in Y$, ако је $f(x) = y$. Слично се дефинишу родитељи елемената из X (у том случају наравно користимо функцију g). Приметимо да сваки елемент може имати највише једног родитеља, јер су функције „1–1“. За низ $(z_0, z_1, \ldots, z_n)$ кажемо да представља ланац предака за елемент z_0, ако је за свако $i \in \{1, \ldots, n\}$ елемент z_i родитељ елемента z_{i-1}. За овај ланац предака кажемо да је дужине n. Наравно да могу постојати и ланци предака бесконачне дужине. На основу тога можемо закључити да је за сваки елемент z из X, односно Y испуњен један од следећа три услова.

1. Максимална дужина ланца предака за z је паран број;
2. Максимална дужина ланца предака за z је непаран број;
3. Ланац предака за z је бесконачан.

У складу са тим скупове X и Y представљамо у облику дисјуктне уније

$$\begin{array}{rcl} X & = & X_{\mathrm{par}} \sqcup X_{\mathrm{nepar}} \sqcup X_{\infty} \\ Y & = & Y_{\mathrm{par}} \sqcup Y_{\mathrm{nepar}} \sqcup Y_{\infty} \end{array}$$

[1]Felix Bernstein (1878–1956), немачки математичар.

где је са, нпр. X_{par} означен скуп свих елемената из X код којих је максимална дужина ланца предака парна. Ознака $\sqcup$ је ознака која се користи када се жели истаћи да је унија о којој се ради, унија дисјунктних скупова. Како је максимална дужина ланца предака родитеља за 1 мања од дужине ланца предака потомка, то је јасно да важи

$$\begin{array}{rcl} f[X_{\mathrm{par}}] & = & Y_{\mathrm{nepar}} \\ f[X_\infty] & = & Y_\infty \\ g[Y_{\mathrm{par}}] & = & X_{\mathrm{nepar}}. \end{array}$$

и да су одговарајуће рестрикције функција f односно g на наведене скупове заправо бијекције. Стога функцију $h\colon X \to Y$, можемо дефинисати са

$$h(x) = \left\{ \begin{array}{cl} f(x) & x \in X_{\mathrm{par}} \sqcup X_\infty \\ g^{-1}(x) & x \in X_{nepar}. \end{array} \right.$$

Јасно је да је тако дефинисана функција h бијекција, чиме је наш доказ завршен.

Други доказ. Докажимо, пре свега, следећу лему.

Лема 2.22 Нека је X било који скуп и $\Phi\colon \mathcal{P}(X) \to \mathcal{P}(X)$ „монотона“ функција, тј. функција за коју важи следеће

$$A \subseteq B \Rightarrow \Phi(A) \subseteq \Phi(B).$$

Тада постоји *фиксна тачка* за функцију Φ, тј. постоји $Z \subseteq X$, такав да је $\Phi(Z) = Z$.

Одмах ћемо задати скуп Z:

$$Z = \bigcup_{A \subseteq \Phi(A)} A.$$

Докажимо да је $Z = \Phi(Z)$. Нека је $z \in Z$. По дефиницији скупа Z закључујемо да $z \in A$, за неки скуп A такав да је $A \subseteq \Phi(A)$. Стога $z \in \Phi(A)$, а како је $A \subseteq Z$, то је и $\Phi(A) \subseteq \Phi(Z)$, па закључујемо да $z \in \Phi(Z)$. Према томе доказали смо да је $Z \subseteq \Phi(Z)$. Из те чињенице добијамо да је $\Phi(Z) \subseteq \Phi(\Phi(Z))$, па скуп $\Phi(Z)$ испуњава услове за припадност фамилији скупова која се користи у дефиницији скупа Z. Како је Z унија свих елемената те фамилије (а међу њима се, према претходном, налази и скуп $\Phi(Z)$), то је $Z \supseteq \Phi(Z)$, чиме смо завршили доказ леме. $\Diamond$

Дефинишемо функцију $\Phi\colon \mathcal{P}(X) \to \mathcal{P}(X)$, са

$$\Phi(A) = X \setminus g[Y \setminus f[A]].$$

Приметимо да смо у дефинисању функције Φ користили директну слику скупа при задатој функцији ($f[A]$, односно $g[Y \setminus f[A]]$). $\Phi(A)$ је *вредност* функције Φ у тачки A, док је $f[A]$ директна слика скупа A при f. Треба обратити пажњу на ту финесу. Функција Φ испуњава услове за примену претходне леме

$$\begin{aligned} A \subseteq B &\Rightarrow f[A] \subseteq f[B] \\ &\Rightarrow Y \setminus f[A] \supseteq Y \setminus f[B] \\ &\Rightarrow g[Y \setminus f[A]] \supseteq g[Y \setminus f[B]] \\ &\Rightarrow X \setminus g[Y \setminus f[A]] \subseteq X \setminus g[Y \setminus f[B]] \\ &\Rightarrow \Phi(A) \subseteq \Phi(B). \end{aligned}$$

Према претходној леми, постоји $Z \subseteq X$, такав да је $\Phi(Z) = Z$, тј. за скуп Z важи

$$X \setminus g[Y \setminus f[Z]] = Z,$$

односно

$$X \setminus Z = g[Y \setminus f[Z]]. \tag{2.10}$$

Дефинишемо функцију $h: X \to Y$ са

$$h(x) = \begin{cases} f(x) & x \in Z \\ g^{-1}(x) & x \notin Z. \end{cases}$$

Приметимо да је на основу 2.10 функција h добро дефинисана. Покажимо да је h бијекција. Ако су x_1 и x_2 елементи из Z такви да је $x_1 \neq x_2$, тада из инјективности функције f следи $h(x_1) = f(x_1) \neq f(x_2) = h(x_2)$. Слично се добија ако су x_1 и x_2 оба ван Z. Претпоставимо стога да $x_1 \in Z$ и $x_2 \notin Z$. Тада је $g^{-1}(x_2) \in Y \setminus f[Z]$, а $f(x_1) \in f[Z]$, па је опет $h(x_1) \neq h(x_2)$. Закључујемо да је h „1–1“. Ако је $y \in Y$ произвољан елемент, то је он или у $f[Z]$ или у $Y \setminus f[Z]$. У првом случају је $y = f(x)$, за неко $x \in Z$, па је, по дефиницији функције h, $h(x) = f(x) = y$. У другом случају $x = g(y) \notin Z$ (према 2.10) те је $y = h(x)$. У сваком случају добијамо да је $z \in h[X]$, тј. функција h је сурјекција. □

У наредном одељку дајемо неке примене ове теореме. Видећемо да се резултат да је $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ веома једноставно доказује њеним коришћењем.

2.4 Разни примери

Докажимо пре свега два става, која ћемо користити у даљем излагању.

Став 2.23 Ако постоји сурјекција $f: \mathbb{N} \to X$, онда је скуп X највише пребројив.

Доказ. Дефинишемо функцију $g: X \to \mathbb{N}$, са

$$g(x) = \min f^{-1}[\{x\}].$$

Приметимо да је функција g добро дефинисана, јер је $\mathbb{N}$ добро уређен, па најмањи елемент у скупу $f^{-1}[\{x\}]$ (који није празан, јер је f „на“) увек постоји. За $x \in X$ важи $f(g(x)) = x$, тј. $f \circ g = \mathrm{Id}_X$, из чега добијамо да је g „1–1“. □

Став 2.24 а) $|(A^B)^C| = |A^{B\times C}|$;
б) $|A| = |A_1|$ и $|B| = |B_1| \Rightarrow |A^B| = |A_1^{B_1}|$ и $|A \times B| = |A_1 \times B_1|$.

Доказ. а) $\Phi\colon (A^B)^C \to A^{B\times C}$ је дефинисано са $\Phi(f)(b,c) = f(c)(b)$, за $f \in (A^B)^C$. Слично дефинишемо $\Psi\colon A^{B\times C} \to (A^B)^C$ са $\Psi(F)(c)(b) = F(b,c)$, за $F \in A^{B\times C}$. Директно се може проверити да је $\Psi \circ \Phi = \mathrm{Id}_{(A^B)^C}$, односно $\Phi \circ \Psi = \mathrm{Id}_{A^{B\times C}}$, из чега следи тражени закључак. Доказ резултата под б) оставља се читаоцу за вежбу. □

Позабавимо се сада неким примерима. У оквиру њих поново ћемо доказати поједине резултате које смо већ обрадили.

Пример 2.25 $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

$f\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ дефинисано са $f(n) = (n, 0)$ је „1–1“. $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ дефинисано са $g(m,n) = 2^m 3^n$ је такође „1–1“ (проверити!). Из Кантор–Бернштајнове теореме добијамо тражено.

Пример 2.26 Пребројива унија пребројивих скупова је пребројив скуп.

Нека је $\{A_n : n \in \mathbb{N}\}$ пребројив скуп при чему је за свако $n \in \mathbb{N}$ скуп A_n пребројив. Према томе, постоје $f_n : \mathbb{N} \to A_n$ које су бијекције. Дефинишемо

$$f\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$$

са $f(m,n) = f_n(m)$. Јасно је да је f „на“ (не мора бити „1–1“ пошто скупови A_n не морају бити дисјунктни). Како је $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$ то постоји и сурјекција $g\colon \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$. Према Ставу 2.23 добијамо да је скуп $\bigcup_{n\in\mathbb{N}} A_n$ највише пребројив. Како очигледно није коначан, то мора бити пребројив.

Пример 2.27 $\mathbb{Q}$ је пребројив.

Покажимо најпре да је скуп $\mathbb{Z}$ пребројив. Функција $f\colon \mathbb{Z} \to \mathbb{N}$ задата са

$$f(m) = \begin{cases} 2|m| + 1 & m < 0 \\ 2m & m \geq 0 \end{cases}$$

представља тражену бијекцију. Дефинишимо сада

$$g\colon \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \to \mathbb{Q}$$

са $g(m,n) = \frac{m}{n}$. Тада је g „на“ и као и у претходном (како $\mathbb{Q}$ није коначан — садржи скуп $\mathbb{N}$) закључујемо да је $\mathbb{Q}$ пребројив.

Пример 2.28 $\mathcal{P}_{\mathrm{fin}}(\mathbb{N})$ је пребројив.

Индукцијом једноставно закључујемо да је за свако $n \in \mathbb{N} \setminus \{0\}$, скуп $\mathbb{N}^n$ пребројив. Тада је, по примеру 2.26 и скуп $\bigcup_{n\in\mathbb{N}\setminus\{0\}} \mathbb{N}^n$ пребројив. Дефинишимо

$$f\colon \bigcup_{n\in\mathbb{N}\setminus\{0\}} \mathbb{N}^n \to \mathcal{P}_{\mathrm{fin}}(\mathbb{N}) \setminus \{\emptyset\}$$

са

$$f(m_1, m_2, \ldots, m_n) = \{m_1, m_2, \ldots, m_n\}.$$

Јасно је да је f „на“ и тврђење следи.

Напомена 2.29 Наравно да важи и : $\mathcal{P}_{\mathrm{fin}}(A)$ је пребројив за сваки пребројив скуп A.

Пример 2.30 $|\mathbb{N}^{\mathbb{N}}| = |2^{\mathbb{N}}|$.

Јасно је да постоји инјекција $\Phi\colon 2^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$. Наиме, ако са $i : 2 \to \mathbb{N}$ означимо инклузију ($2 \subset \mathbb{N}$), тада се Φ може дефинисати са $\Phi(f) = i \circ f$. Φ је наравно „1–1“. Дефинишимо сада инјекцију $\Psi\colon \mathbb{N}^{\mathbb{N}} \to 2^{\mathbb{N}}$. Низу природних бројева треба придружити низ нула и јединица. Учинимо то на следећи начин. Нека је дат низ $(a_0, a_1, a_2, \ldots)$, где су сви a_i природни бројеви. Том низу можемо придружити следећи низ нула и јединица

$$(\underbrace{1, 1, \ldots 1}_{a_0+1}, 0, \underbrace{1, 1, \ldots 1}_{a_1+1}, 0, \ldots).$$

Тиме смо дефинисали $\Psi\colon \mathbb{N}^{\mathbb{N}} \to 2^{\mathbb{N}}$. Како је јасан поступак којим се на јединствен начин од задатог низа нула и јединица добија низ природних бројева (не одговара *сваком* низу нула и јединица низ природних бројева — не тврдимо да је функција Ψ „на“!) то је Ψ „1–1“ Читаоцу се за вежбу препоручује да установи тај поступак. На пример, низ $(1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0 \ldots)$ потиче од низа $(2, 3, 0, 0, 1, \ldots)$.

Пример 2.31 $|\mathbb{R}| = |2^{\mathbb{N}}|$.

Како је $|\mathbb{R}| = |(0, 1)|$, то је довољно показати $|(0, 1)| = |2^{\mathbb{N}}|$. Нека је $x \in (0, 1)$ произвољан елемент и $x = 0.x_1x_2x_3\ldots$, децимални запис за x. При томе претпостављамо да се децимални запис не завршава са бесконачно много деветки, нпр. $0.1249999\ldots = 0.125000\ldots$. Тада је придруживање

$$(0, 1) \ni x \mapsto (x_1, x_2, x_3, \ldots) \in \mathbb{N}^{\mathbb{N}}$$

„1–1“. Инјекцију $2^{\mathbb{N}}$ у $(0, 1)$ можемо дефинисати како следи. Елемент из $2^{\mathbb{N}}$ је низ нула и јединица $(a_0, a_1, a_2, \ldots)$, где $a_i \in 2$ за све i. Том елементу придружујемо елемент $x \in (0, 1)$ чији је *децимални* запис $0.a_0a_1a_2\ldots$. Може се додуше десити да смо тако добили 0 која не припада $(0, 1)$, али $|[0, 1)| = |(0, 1)|$. Наиме, $|(0, 1)| = |(a, b)|$ за све $a, b \in \mathbb{R}$, такве да је

$a < b$. Тражена бијекција $h\colon (0,1) \to (a,b)$ је дата са $h(t) = (1-t)a + tb$. Према томе,

$$|(0,1)| \leq |[0,1)| \leq |(0,2)| = |(0,1)|.$$

Пример 2.32 Означимо са $C(\mathbb{R})$ скуп свих непрекидних функција $f\colon \mathbb{R} \to \mathbb{R}$. Тада је $|C(\mathbb{R})| = |\mathbb{R}|$.

Свака непрекидна функција из $\mathbb{R}$ у $\mathbb{R}$ потпуно је одређена вредностима које узима на скупу $\mathbb{Q}$ (или на било ком свуда густом скупу). То је основна идеја коју користимо за доказ наведене чињенице. Формалније, дефинишемо

$$\Phi\colon C(\mathbb{R}) \to \mathbb{R}^{\mathbb{Q}}$$

са $\Phi(f) = f|_{\mathbb{Q}}$. Нека је $\Phi(f) = \Phi(g)$ за неке $f, g \in C(\mathbb{R})$. Показаћемо да је $f = g$, тј. да за све $x \in \mathbb{R}$ важи $f(x) = g(x)$. Нека је $x \in \mathbb{R}$ произвољан. Ако $x \in \mathbb{Q}$, онда је

$$f(x) = f|_{\mathbb{Q}}(x) = \Phi(f)(x) = \Psi(g)(x) = g|_{\mathbb{Q}}(x) = g(x).$$

Ако $x \notin \mathbb{Q}$, онда постоји низ (x_n) рационалних бројева који конвергира ка x. Како је $\Phi(f) = \Phi(g)$, то је $f(x_n) = g(x_n)$, за све $n \in \mathbb{N}$. Због непрекидности функција f и g, $f(x_n) \to f(x)$ и $g(x_n) \to g(x)$. Из јединствености граничне вредности низа добијамо $f(x) = g(x)$. Према томе, f је „1–1“ и добили смо $|C(\mathbb{R})| \leq |\mathbb{R}^{\mathbb{Q}}|$. Са друге стране, $|\mathbb{R}^{\mathbb{Q}}| = |(2^{\mathbb{N}})^{\mathbb{Q}}|$, према примеру 2.31 и Ставу 2.24, а $|(2^{\mathbb{N}})^{\mathbb{Q}}| = |2^{\mathbb{N}\times\mathbb{Q}}|$ према Ставу 2.24, те уз чињеницу да је скуп $\mathbb{Q}$ пребројив добијамо, применом истог става, да је $|2^{\mathbb{N}\times\mathbb{Q}}| = |2^{\mathbb{N}}|$, а $|2^{\mathbb{N}}| = \mathbb{R}$, према примеру 2.31. Дакле, $|C(\mathbb{R})| \leq |\mathbb{R}|$. Наравно да важи и $|\mathbb{R}| \leq |C(\mathbb{R})|$. Наиме, сваком реалном броју можемо придружити константну функцију. Закључујемо да је $|C(\mathbb{R})| = |\mathbb{R}|$.

Пример 2.33 Скуп свих алгебарских бројева је пребројив.

Подсетимо се да се под алгебарским бројем подразумева сваки комплексан број који је нула неког полинома са рационалним коефицијентима. Са $Z(p)$ означаваћемо скуп свих нула полинома p. За скуп алгебарских бројева, у ознаци $\overline{\mathbb{Q}}$, дакле важи

$$\overline{\mathbb{Q}} = \bigcup_{p\in\mathbb{Q}[X]\setminus\{0\}} Z(p).$$

Сваки од скупова $Z(p)$ је коначан док је скуп $\mathbb{Q}[X]$ пребројив. Заправо постоји сурјекција $\Phi\colon \bigcup_{n\in\mathbb{N}\setminus\{0\}} \mathbb{Q}^n \to \mathbb{Q}[X]$ која $n-$торци рационалних бројева додељује полином са тим коефицијентима. Према томе, $\overline{\mathbb{Q}}$ је пребројива унија коначних скупова, па тиме и пребројив скуп (јасно је да није коначан).

Пример 2.34 $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Као и раније радићемо са интервалом $(0,1)$ уместо $\mathbb{R}$. Ињекција $\Psi\colon (0,1)\times(0,1)\to(0,1)$ може се задати на следећи начин

$$\Psi((0.x_1x_2x_3x_4\ldots),(0.y_1y_2y_3y_4\ldots)) = (0.x_10y_10x_20y_20\ldots).$$

Пример 2.35 Нека је $\mathcal{S}$ пребројив скуп тачака у равни. Показати да постоји права у тој равни која не садржи ниједну од тачака из $\mathcal{S}$.

Како је $|\mathbb{R}\times\mathbb{R}| = |\mathbb{R}| > |\mathcal{S}|$, то закључујемо да је $\mathbb{R}^2\setminus\mathcal{S}\neq\emptyset$. Изаберимо било коју тачку x_0 из тог скупа и нека је ℓ било која права која пролази кроз ту тачку и изаберимо једну од полуравни одређених правом ℓ. Ако поставимо кружницу са центром у тачки x_0 произвољног полупречника онда можемо закључити да је свака права која пролази кроз x_0 и није једнака ℓ, јединствено одређена тачком у којој сече онај део кружнице који лежи у изабраној полуравни. Дакле, скуп $\mathcal{P}$ свих таквих правих је у бијекцији са скупом $(0,\pi)$ (тачке на кружници су одређене углом). Како је тај скуп непребројив то је и скуп $\mathcal{P}$ непребројив. Скуп свих правих које пролазе кроз x_0 и неку од тачака из $\mathcal{S}$ је највише пребројив, јер је $\mathcal{S}$ пребројив. Закључујемо да постоји права кроз x_0 која не садржи ниједну од тачака из $\mathcal{S}$.

2.5 Задаци за вежбу

1. Нека су A и B коначни скупови. Доказати: $|A\cup B| = |A|+|B|-|A\cap B|$.

2. Генералисати претходни задатак на случај n коначних скупова.

3. Нека су $A_1,\ldots,A_n$ подскупови коначног скупа V. Одредити формулу која одређује број елемената у скупу $V\setminus(A_1\cup\ldots\cup A_n)$ (број елемената који не припадају ниједном од скупова A_n).

4. Нека је $|A| = m$ и $|B| = n$ и $B\subseteq A$. Одредити број скупова C за које је $B\subseteq C\subseteq A$.

5. Нека је $|X| = m$ и $|Y| = n$. Показати

   (а) Број функција из X у Y је n^m;

   (б) Број „1–1“ функција из X у Y је $n(n-1)\cdots(n-m+1)$;

   (в) Број сурјекција из X у Y је

   $$\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^m.$$

6. Нека је са p_n означен број релација еквиваленције на скупу од n елемената. Показати да важи следећа формула
$$p_{n+1} = \sum_{j=0}^{n} \binom{n}{j} p_j,$$
при чему додатно дефинишемо да је $p_0 = 1$.

7. Колико има различитих линеарних уређења на скупу од n елемената?

8. Нека у посету P има $mn + 1$ елемената, где су $m, n > 0$. Показати да у P постоји антиланац са $m + 1$ елемената или ланац са $n + 1$ елемената.

9. Дат је низ од $mn + 1$ различитих бројева. Доказати да он садржи растући подниз дужине $m + 1$ *или* опадајући подниз дужине $n + 1$.

10. Посматрајмо посет $(\mathcal{P}(\mathbb{N}), \subseteq)$. Да ли он садржи ланац кардиналности $\mathfrak{c}$? Да ли он садржи антиланац кардиналности $\mathfrak{c}$?

11. Доказати да су у сваком посету свака два различита максимална елемента неупоредива. Доказати да у коначном посету за сваки елемент x постоји *максималан* елемент m такав да је $x \leq m$.

12. Означимо са P скуп свих низова природних бројева који су једнаки 0 почев од неког члана, тј.
$$P = \{\langle x_n \rangle \in \mathbb{N}^{\mathbb{N}} \,|\, (\exists m \in \mathbb{N})(\forall n \geq m) x_n = 0\}.$$
На P је уведено парцијално уређење са
$$\langle x_n \rangle \leq_P \langle y_n \rangle \overset{\text{def}}{\iff} (\forall n \in \mathbb{N}) x_n \leq y_n.$$
Доказати да је $(P, \leq_P) \cong (\mathbb{N} \setminus \{0\}, |)$, где је са $|$ означена релација дељивости у скупу природних бројева.

13. Нека је $|A| = n$. Одредити број аутоморфизама посета $(\mathcal{P}(A), \subseteq)$.

14. У посету $(P, \leq)$ елемент $s(x)$ $(p(x))$ је следбеник (претходник) елемента x уколико не постоји $y \in P$ такав да је $x < y < s(x)$ $(p(x) < y < x)$. Дефинисати уређење на скупу реалних бројева у коме сваки елемент има и следбеника и претходника.

15. Доказати да не постоје скупови $x_0, x_1, x_2, \ldots$ такви да $x_0 \ni x_1 \ni x_2 \ni \cdots$.

16. Доказати да је посет добро уређен ако и само ако не постоји бесконачни опадајући низ у том посету.

17. Испитати да ли постоји непразан скуп x такав да је $\cup x = x$.

18. Испитати да ли постоји коначан непразан скуп x такав да је $\cup x = x$.

19. Испитати да ли постоји непразан скуп x такав да је $\cup(\cap x) = x$.

20. Испитати да ли постоји непразан скуп x такав да је $\cup(\cap x) \supseteq x$.

21. Испитати да ли постоји скуп x, који има бар два елемента и за који је $\cap(\cup x) = x$.

22. Испитати да ли постоји непразан скуп x такав да је $\cap x \neq \emptyset$ и $\cap(\cap x) = \cap x$.

23. Испитати да ли постоје непразни скупови x и y тако да је бар један од њих коначан и да важи $\cup x = y$ и $\cup y = x$.

24. Нека је скуп X коначан и $f\colon X \to X$. Доказати

    (а) f је „1–1“ **акко** f је бијекција;

    (б) f је „на“ **акко** f је бијекција.

25. Нека је $f\colon X \to X$ функција за коју важи: $f^2 = f$ и f је „1–1“. Испитати да ли је f обавезно бијекција.

26. Нека су $f, g\colon X \to X$ такве да је $f \circ g \circ f$ „1–1“ и $g \circ f \circ g$ „на“. Доказати или оповргнути: f и g су бијекције.

27. Нека су $f, g\colon X \to X$ функције за које важи:

    (а) $g \circ f \circ g \circ f = g \circ f$;

    (б) g је „1–1“;

    (ц) f је „на“.

    Испитати да ли из тих претпоставки следи да су и f и g бијекције.

28. Нека су $f, g, h\colon X \to X$ функције за које важи:

    (а) $h \circ g \circ g \circ f$ је бијекција;

    (б) $g \circ h \circ f \circ g$ је бијекција.

    Испитати да ли из тих претпоставки следи да је h бијекција.

29. Нека је X скуп са бар три елемента и $f\colon X \longrightarrow X$ функција за коју важи: за свака два двочлана скупа A и B

$$f[A] = f[B] \Rightarrow A = B.$$

    Доказати или оповргнути: f је „1–1“.

30. Нека је функција $f\colon X \to Y$ таква да за сваки непразан $B \subseteq Y$ постоји $A \subseteq X$ тако да је $f[A] \cap B \neq \emptyset$. Испитати да ли f мора бити „на“.

31. Нека $f\colon X \to Y$, $A \subseteq X$, $B, C \subseteq Y$. Испитати да ли из чињенице $f[A] \subseteq B \setminus C$ можемо закључити да је $A \cap f^{-1}[C] = \emptyset$.

32. Нека $f\colon X \to Y$. Доказати да је f „на“ акко за све $A, B \subseteq Y$ важи: $f[f^{-1}[A] \setminus f^{-1}[B]] = A \setminus B$.

33. Нека $f\colon X \to Y$. Доказати: f је „1–1“ **акко** за сваки скуп Z и функције $g_1, g_2 : Z \to X$ важи: $f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$.

34. Нека $f\colon X \to Y$. Доказати: f је „на“ **акко** за сваки скуп Z и функције $g_1, g_2 : Y \to Z$ из $g_1 \circ f = g_2 \circ f$ следи $g_1 = g_2$.

35. Доказати да је $\mathbb{N} \times \mathbb{N} \subseteq \mathcal{P}_{\mathrm{fin}}(\mathcal{P}_{\mathrm{fin}}(\mathbb{N}))$ (користити дефиницију уређеног пара). Можете ли ову чињеницу искористити (уз коришћење још неког резултата) за доказ пребројивости скупа $\mathbb{N} \times \mathbb{N}$?

36. Нека је $\mathcal{S}$ било који непребројив подскуп скупа реалних бројева. Доказати да $\mathcal{S}$ садржи непребројиво много ирационалних бројева.

37. Нека је $\mathcal{S}$ пребројив подскуп равни. Доказати да у тој равни постоји кружница која не садржи ниједну тачку из $\mathcal{S}$.

38. Нека је k кружница у равни. Доказати да k садржи тачку чије су обе координате ирационални бројеви.

39. Нека је $\mathcal{K}$ скуп кружница у равни са следећим својством. За сваку тачку P праве $y = 0$, постоји кружница из скупа $\mathcal{K}$, која ту праву додирује у тачки P. Доказати да се неке две кружнице из скупа $\mathcal{K}$ секу.

40. Доказати да се сваки пребројив подскуп A равни може представити у облику уније $A = B \cup C$, где у B има само коначно много тачака са сваке „вертикалне“ праве, а у C само коначно много тачака са сваке „хоризонталне“ праве.

41. Доказати да је бесконачан скуп A пребројив ако и само ако се $A \times A$ може представити у облику уније $B \cup C$ при чему су скупови $\{(x, y) \in A \times A : x = x_0\} \cap B$ и $\{(x, y) \in A \times A : y = y_0\} \cap C$ коначни за све $x_0, y_0 \in A$.

42. Доказати да у равни постоји пребројив скуп правих $\mathcal{F}$ са особином : свака права те равни сече бесконачно много правих из скупа $\mathcal{F}$.

43. Нека је $\mathcal{S} \subseteq \mathbb{R}^3$ такав да је растојање између било које две различите тачке из $\mathcal{S}$ бар 1. Доказати да је скуп $\mathcal{S}$ највише пребројив.

44. Доказати да за скуп $C_+(\mathbb{R})$ свих функција из $\mathbb{R}$ у $\mathbb{R}$ које су непрекидне са десне стране важи: $|C_+(\mathbb{R})| = |C(\mathbb{R})|$.

45. Доказати да је скуп тачака прекида монотоне функције највише пребројив.

46. Нека је на скупу $\mathbb{N}\times\mathbb{N}$ дефинисано парцијално уређење $\ll$ са

$$(m,n) \ll (p,q) \overset{\text{def}}{\Longleftrightarrow} m \leq p \wedge n \leq q.$$

Доказати да не постоји бесконачан подскуп од $\mathbb{N}\times\mathbb{N}$ чија су свака два елемента неупоредива (не постоји бесконачни антиланац). Шта се може рећи за аналогни поредак на $\mathbb{Z}\times\mathbb{Z}$?

47. Шаховски скакач се креће по целобројним тачкама у равни чинећи сваког секунда нестандардан скок. Нама није позната ни позиција скакача ни тачан скок који врши. Ако сваког минута можемо да означимо по једну целобројну тачку у равни, доказати да ћемо после коначно много времена успети да означимо позицију у којој се скакач у том тренутку налази („да га погодимо“).

48. Показати да се раван не може „покрити“ са мање од $\mathfrak{c}$ правих.

49. Показати да скуп $\mathbb{R}$ не може бити унија пребројиво много скупова који су сви кардиналности мање од $\mathfrak{c}$.

50. Ако је $A \subseteq \mathbb{R}^2$ такав да свака хоризонтална права сече A у коначно много тачака, онда постоји вертикална права која сече комплемент A^c по скупу кардиналности $\mathfrak{c}$.

51. Постоји континуум много подскупова $A_\gamma \subseteq \mathbb{N}$ таквих да је за $\gamma_1 \neq \gamma_2$ скуп $A_{\gamma_1} \cap A_{\gamma_2}$ коначан.

52. Ако је $A \subseteq \mathbb{R}$ такав да за свако $a \in A$ постоји $\delta_a > 0$ тако да је $(a, a+\delta_a) \cap A = \emptyset$ или $(a-\delta_a, a) \cap A) = \emptyset$, доказати да је A пребројив.

53. Ако је A непребројив подскуп од $\mathbb{R}$ онда он садржи строго опадајући низ који конвергира ка тачки у A.

54. Доказати да је сваки добро уређен подскуп од $\mathbb{R}$ пребројив.

Глава 3

Аксиома избора. Ординали и кардинали

3.1 Ординали

Све објекте које смо до сада дефинисали, читалац је већ имао прилике да упозна. Додуше, вероватно није разматрао конструкцију природних бројева и ригорозно доказивање њихових својстава. Вероватно се и није превише задржавао на разматрању питања шта можемо сматрати скупом и томе слично. Но, у овом одељку упознаћемо нешто заиста ново. Процес бројања почиње од 0 и наставља се са 1, 2, 3, ... и тако доводи до природних бројева. Поставимо питање: може ли се наставити и „даље“? Видећемо да се може и показати шта то „даље“ заправо значи. Тако ћемо доћи до појма *ординалних (редних) бројева*, или краће *ординала*.

Основно својство природних бројева садржано је у принципу индукције односно у добром уређењу. Подсетимо се да је неки скуп добро уређен уколико сваки његов непразан подскуп има најмањи елемент. Ако је $(X, \leq)$ неки добро уређени скуп, дефинишемо почетни комад X_a од X, одређен елементом $a \in X$, са:

$$X_a \stackrel{\text{def}}{=} \{x \in X : x < a\}.$$

Дефиниција 3.1 Добро уређени скуп $(X, \leq)$ је *ординал* ако је за сваки елемент $a \in X$ испуњено

$$X_a = a.$$

Дакле, за сваки елемент a ординала X важи: $a = \{x \in X : x < a\}$. То је помало необична особина и са правом се можемо запитати да ли такви скупови уопште постоје. Проверимо како би они могли да изгледају. Нека је X непразан ординал. Означимо са x_0 његов најмањи елемент. Тада важи:

$$x_0 = X_{x_0} = \{x \in X : x < x_0\} = \emptyset.$$

Према томе, у сваком ординалу налази се $0 = \emptyset$ и то као најмањи елемент. Који је следећи елемент? Ако га означимо са x_1 ($x_1 = \min(X \setminus \{0\})$), добијамо:

$$x_1 = X_{x_1} = \{x \in X : x < x_1\} = \{0\}.$$

Подсетимо се да смо 1 дефинисали као $\{0\}$. Сада већ слободније настављамо даље:

$$\min(X \setminus \{0, 1\}) = x_2 = X_{x_2} = \{x \in X : x < x_2\} = \{0, 1\},$$

а то је по нашој дефиницији 2. Према томе, сваки ординал почиње природним бројевима. Ако је тај ординал коначан скуп, онда он није ништа друго до неки природан број. Скуп свих природних бројева ω такође је ординал: за свако $n \in \omega$ важи: $\{m \in \omega : m < n\} = n$. Као што знамо $n + 1 = n \cup \{n\}$. Заправо, за сваки ординал x, скуп $s(x) = x \cup \{x\}$ такође је ординал (при чему дефинишемо $x > y$ за све $y \in x$). Наиме, за $y \in x$ важи

$$\begin{aligned} s(x)_y &= \{z \in s(x) : z < y\} \\ &= \{z \in x : z < y\} \quad (x \not< y) \\ &= x_y \\ &= y, \text{ јер је } x \text{ ординал,} \end{aligned}$$

а важи и

$$s(x)_x = \{z \in s(x) : z < x\} = x.$$

Ординал $s(x)$ назива се следбеник ординала x.

Наведимо још једну особину ординала. Наиме, елемент ординала такође је ординал. Проверимо да ли је то заиста тако. Нека је x било који ординал и $y \in x$. Како је x ординал, то је $y = x_y$ и ако је $z \in y$ тада $z \in x_y$, па $z \in x$ и $z < y$. Добијамо

$$\begin{aligned} y_z &= \{u \in y : u < z\} \\ &= \{u \in x_y : u < z\} \\ &= \{u \in x : u < y \text{ и } u < z\} \\ &= \{u \in x : u < z\} \\ &= x_z \\ &= z, \text{ јер је } x \text{ ординал.} \end{aligned}$$

Ако су x и y елементи неког ординала u (па, према претходном, и сами ординали) такви да је $x < y$ тада важи: $x = u_x \subset u_y = y$. Такође је и $x \in u_y = y$, па је и $x \in y$. Будимо још прецизнији.

Став 3.2 (а) Свака почетни комад ординала је ординал.
(б) Ако су x и y ординали и $y \subset x$, тада је y почетни комад од x.
(в) Ако су x и y различити ординали тада је један од њих почетни комад оног другог.

Доказ. (а) Ако је u ординал и $x \in u$, тада је $u_x = x$, што је, како смо видели један ординал.
(б) Нека је $y \subset x$ и $a = \min(x \setminus y)$. Ако је $z < a$, тада $z \in y$ (јер је a најмањи у $x \setminus y$), тј. $x_a \subseteq y$. Претпоставимо да $z \in y$. Ако је $z = a$ тада $a \in y$ што противречи избору елемента a. Ако је $z > a$, онда је $a \in x_z = z = y_z$, тј. $a \in y$, што поново противречи избору a. Закључујемо да је $z < a$, тј. $y \subseteq x_a$ (овде смо користили чињеницу да је сваки добро уређен скуп и тотално уређен, тј. да за свака два елемента a и b из тог скупа важи: $a < b \vee a = b \vee a > b$).
(в) Нека је $x \neq y$. Претпоставимо да $x \not\subset y$ и $y \not\subset x$. Посматрајмо њихов пресек $z = x \cap y$. По претпоставци, $z \neq x$ и $z \neq y$. Међутим, z јесте ординал. Наиме, нека је $a \in z$. Тада је $a = x_a \subseteq x$, пошто је x ординал, а такође је и $a = y_a \subseteq y$, јер је y ординал. Тада

$$
\begin{aligned}
u \in a \quad &\iff \quad u \in x_a \wedge u \in y_a \\
&\iff \quad (u < a \wedge u \in x) \wedge (u < a \wedge u \in y) \\
&\iff \quad (u < a) \wedge u \in x \cap y \\
&\iff \quad u \in z_a.
\end{aligned}
$$

Како је непразан подскуп добро уређеног скупа и сам добро уређен (зашто?) то закључујемо да је z ординал. Но, пошто је $z \subset x$ и $z \subset y$, то је $z = x_a$ за неко $a \in x$ и $z = y_b$, за неко $b \in y$. Тада је $a = x_a = z = y_b = b$, па $a = b \in x \cap y = z$, што није могуће (добили бисмо да $a \in x_a$, тј. $a < a$). □

Став 3.3 Унија скупа ординала је ординал.

Доказ. Нека је X скуп који се састоји искључиво од ординала. Означимо његову унију са A. Дакле, $A = \bigcup X$. Видели смо да су елементи ординала ординали, па се у A налазе само ординали. Дефинишимо релацију поретка $<$ на A са

$$x < y \overset{\text{def}}{\iff} x \text{ је почетни комад од } y.$$

Да ли је $<$ транзитивна релација на скупу A? Претпоставимо да је $x < y$ и $y < z$. Тада је $x = y_a$, за неко $a \in y$ и $y = z_b$ за неко $b \in z$. Добијамо

$$
\begin{aligned}
x &= y_a \\
&= (z_b)_a \\
&= z_a,
\end{aligned}
$$

па је $x < z$. Према претходном ставу, за свака два елемента $x, y \in A$, важи:

$$x < y \vee x = y \vee y < x.$$

Заправо је A добро уређен. Наиме, нека је B непразан подскуп од A и b било који елемент из B. Ако је b најмањи у B онда смо показали да B има најмањи елемент. У супротном, сви елементи мањи од b су почетни комади од b (дефиниција уређења на A), а тиме и елементи у b (b је ординал) и међу њима постоји најмањи елемент, јер је b добро уређен. Тај елемент је најмањи и у B.

Остаје да за сваки $a \in A$ проверимо једнакост $A_a = a$. Како је $A = \bigcup X$, то је $a \in x$, за неко $x \in X$. Како се у X налазе искључиво ординали, то је и x ординал и важи: $a = x_a$, те је $a < x$ (по дефиницији поретка на A). Показаћемо да је $A_a = x_a$ што нам даје тражену једнакост.

Претпоставимо да $u \in A_a$. То значи да је $u < a$, а како је $a < x$ закључујемо да $u \in x_a$. Уколико $u \in x_a$, то закључујемо да је $u \in x$ и $u < a$. Но, $x \subset A$, па добијамо да $u \in A$ и $u < a$, тј. $u \in A_a$. $\square$

Анализирајмо шта смо до сада постигли. Ако на ординалима дефинишемо релацију $<$ са:

$$x < y \overset{\text{def}}{\iff} x \text{ је почетни комад од } y$$

тада добијамо

$$x < y \iff x \subset y.$$

Међутим, $x < y \iff x = y_a$, за неко $a \in y$. Како је y ординал, то је $y_a = a$,те $x \in y$. Дакле, поредак на ординалима дат је релацијом $\in$, која се поклапа са $\subset$, која се поклапа са релацијом „бити почетни комад од“!

Теорема 3.4 (Бурали–Форти[1]) Ординали не чине скуп.

Доказ. Претпоставимо да колекција свих ординала чини скуп O. Читаоцу се оставља за проверу чињеница да је тада скуп O добро уређен. Но,

$$O_x = \{z \in O : z < x\} = \{z \in O : z \in x\} = x.$$

Закључујемо да је и O ординал, те $O \in O$, што, као што знамо није могуће. $\square$

Мада ординали не чине скуп, понекад ћемо говорити о *класи* свих ординала и означавати је са On.

Следећи задатак који себи постављамо је следећи. Показати да је сваки добро уређен скуп изоморфан тачно једном ординалу. Но, нисмо дефинисали појам изоморфизма. Јасно је како то дефинишемо.

[1] Cesare Burali-Forti (1861–1931), италијански математичар.

Дефиниција 3.5 За добро уређен скупове $(X, \leq_X)$ и $(Y, \leq_Y)$, кажемо да су изоморфни ако постоји бијекција $f\colon X \to Y$, таква да

$$x_1 \leq_X x_2 \iff f(x_1) \leq_Y f(x_2).$$

Став 3.6 Нека је X добро уређен, $Y \subseteq X$ и $f\colon X \to Y$ изоморфизам. Тада је $f(x) \geq x$ за све $x \in X$.

Доказ. Нека је $E = \{x \in X : f(x) < x\}$. Ако је E непразан, он има најмањи елемент e. Како $e \in E$, то је $f(e) < e$. Тада је и $f(f(e)) < f(e)$ ($f(f(e)) \neq f(e)$, јер је f „1–1“), па и $f(e) \in E$, а како је $f(e) < e$, то добијамо контрадикцију. □

Последица 3.7 Ако су X и Y добро уређени и $f, g\colon X \to Y$ изоморфизми, онда је $f = g$.

Доказ. $g^{-1} \circ f\colon X \to X$ је изоморфизам. Према претходном ставу, $(g^{-1} \circ f)(x) \geq x$, односно $f(x) \geq g(x)$ за све $x \in X$. Слично је и $g(x) \geq f(x)$, па закључујемо да је за све $x \in X$ $f(x) = g(x)$, тј. $f = g$. □

Последица 3.8 Добро уређен скуп никада није изоморфан неком свом почетном комаду.

Доказ. Ако је $f\colon X \to X_a$ изоморфизам, тада је $f(a) \geq a$, па $f(a) \notin X_a$ чиме добијамо контрадикцију. □

Последица 3.9 Ако су ординали X и Y изоморфни, тада је $X = Y$.

Доказ. У супротном, један од њих је почетни комад оног другог па би добро уређен скуп био изоморфан свом почетном комаду. □

Видимо да су ординали веома ригидни објекти у односу на релацију изоморфизма. Два различита ординала никада нису изоморфна, а сваки аутоморфизам $f\colon X \to X$ ординала X је идентитет.

Да бисмо доказали тражени резултат морамо још пажљивије прићи појму добро уређеног скупа. Наиме, на добро уређеном скупу неке се чињенице успешно могу доказивати индукцијом. Тачније, важи следећа теорема.

Теорема 3.10 (*Принцип индукције*) Нека је X добро уређен скуп и P својство које елементи из X могу задовољавати. Ако је за сваки елемент $x \in X$ тачно да испуњавање својства P за сваки елемент $y < x$ нужно повлачи испуњење својства P за x, тада је својство P испуњено за све $x \in X$.

Доказ. Са $P(x)$ означићемо чињеницу да елемент x испуњава својство P. Ми претпостављамо да важи следеће:

$$(\forall x \in X)((\forall y < x)P(y) \Rightarrow P(x)).$$

Треба показати да је тада тачно и $(\forall x \in X)P(x)$.

Претпоставимо супротно, тј. нека је

$$S = \{x \in X : \neg P(x)\} \neq \emptyset.$$

Тада он има најмањи елемент x_0. Како је x_0 најмањи такав да својство није испуњено, то закључујемо

$$(\forall y < x_0) P(y).$$

Но тада, по претпоставци, добијамо да је и $P(x_0)$. Закључујемо да скуп S мора бити празан што доказује теорему. $\square$

Као што видимо, индукција није метод који је резервисан искључиво за природне бројеве. Тај метод се може примењивати и у случају произвољног добро уређеног скупа. Формулишимо најзад у облику теореме резултат који желимо да докажемо.

Теорема 3.11 Сваки добро уређен скуп изоморфан је тачно једном ординалу.

Пре доказа теореме доказаћемо следећу лему.

Лема 3.12 Нека је X добро уређени скуп такав да је за све $a \in X$ почетни комад X_a изоморфан ординалу. Тада је X изоморфан ординалу.

Доказ. Са $f_a : X_a \to Z(a)$ означимо изоморфизам између почетног комада X_a и ординала $Z(a)$. Претходни резултати показују да су $Z(a)$ и f_a јединствено одређени. Формирајмо скуп

$$W = \{Z(a) : a \in X\}.$$

То је заиста скуп према Аксиоми замене. Тако добијамо функцију

$$f \colon X \to W$$

дефинисану са $f(a) = Z(a)$. Доказаћемо да важи:

$$x < y \Rightarrow f(x) \subset f(y).$$

Наиме, сигурно је $Z(x) \neq Z(y)$, јер су изоморфни различитим почетним комадима од X. Како су то ординали, то је један од њих почетни комад оног другог. Но, ако је $Z(y)$ почетни комад од $Z(x)$, то би X_y било изоморфно почетном комаду од X_x, тј. неком свом почетном комаду што је, како смо видели раније, немогуће. Дакле, $Z(x) \subset Z(y)$. Закључујемо да је W изоморфан са X, па тиме и добро уређен (стриктан поредак на W је наравно релација „бити почетни комад од“ — подсетимо се да су елементи у W ординали). Но,

$$\begin{aligned} W_{Z(y)} &= \{Z(x) : Z(x) \subset Z(y)\} \\ &= \{Z(x) : Z(x) \in Z(y)\} \\ &= Z(y). \end{aligned}$$

Наиме, претпоставимо да $u \in Z(y)$. Тада је $u = Z(y)_u$. Како је $f_y : X_y \to Z(y)$ изорфизам, то постоји $t \in X_y$ такво да је $f_y(t) = u$. Но, тада је $X_t = (X_y)_t \cong Z(y)_u = u$. Како је ординал изоморфан скупу X_t јединствено одређен, то мора бити $u = Z(t)$. Закључујемо да је W ординал. □

Доказ теореме. Јасно је да је потребно само доказати да је X изоморфан ординалу. Јединственост следи из претходних резултата.

Доказаћемо да је за свако $a \in X$ почетни комад X_a изоморфан ординалу. Применом леме добијамо тражени резултат.

Означимо дакле са $P(a)$ својство „X_a је изоморфно ординалу“. Ако је за сваки $b < a$, $P(b)$ испуњено, онда примена леме даје : X_a је изоморфно ординалу (јер сваки почетни комад од X_a је облика $(X_a)_b$, за неко $b < a$, а $(X_a)_b = X_b$, што је по претпоставци изоморфно ординалу). Према принципу индукције, закључујемо да је за све $a \in X$, испуњено $P(a)$, што се и тражило. □

Позабавимо се мало садржајем претходне теореме. Удаљимо се за тренутак од добро уређених скупова. Ако желимо да упоредимо „величину“ два објекта (под „величином“ можемо подразумевати разна својства објеката у зависности од околности — то може бити дужина, тежина, запремина и слично), како поступамо? Можемо их непосредно упоредити и проверити да ли је један, нпр. дужи од другог. *Или* их можемо упоредити са неким *еталоном мере.* На пример, са оном полугом која се чува у близини Париза и представља еталон мере за дужину. Оно што наша претходна теорема показује је да су ординали *еталони мере* за добро уређене скупове! Два добро уређена скупа су изоморфна *акко* су изоморфна истом ординалу. Изоморфизам између два добро уређ ена скупа јесте бијекција, али не било која бијекција него она која чува поредак. Ако заборавимо поредак и питамо се само да ли постоји бијекција између два скупа и тражимо еталон мере за тако нешто, долазимо до појма кардинала. Али о њима ће бити речи касније.

Пре него што пређемо на аритметику са ординалним бројевима, позабавимо се мало трансфинитном индукцијом, тј. индукцијом по ординалима. Пре свега, приметимо да се у доказу Става 3.3 крије и доказ следеће чињенице.

- Сваки непразан скуп који се састоји искључиво од ординала има најмањи елемент.

Читаоцу се за вежбу оставља да провери како се овај резултат може доказати. Узимајући тај резултат у обзир, очекујемо индукцију по ординалима. И заиста, важи следећа теорема.

Теорема 3.13 Нека је P неко својство ординала. Претпоставимо да је за сваки ординал x испуњено следеће: ако је $P(y)$ тачно за све $y < x$, тада је тачно и $P(x)$. Тада је $P(x)$ тачно за све ординале x.

Доказ. Ми већ знамо да принцип индукције важи у добро уређеним скуповима. Да бисмо доказали да је $P(x)$ тачно за ординал x, довољно је узети неки добро уређени скуп који га садржи и затим применити индукцију у том добро уређеном скупу. Најједноставнији добро уређени скуп који садржи x је $s(x) = x \cup \{x\}$. □

Приметимо да смо морали бити пажљиви при овом доказу. Наиме, видели смо да ординали не чине скуп, па не можемо радити индукцију у „скупу свих ординала“. За то смо искористили „трик“ да било који ординал „убацимо“ у добро уређени скуп где се индукција може применити. Овако формулисана индукција аналогна је потпуној индукцији код природних бројева. Да ли постоји формулација овог принципа, који подсећа на „обичну“ индукцију код природних бројева (прелазак са n на $n+1$)? Постоји, али нам је за ту формулацију потребна и једна једноставна класификација ординала.

Дефиниција 3.14 За ординал α кажемо да је *следбеник*, ако постоји ординал β такав да је $\alpha = s(\beta)$. За ординал λ кажемо да је *гранични* ако је $\lambda = \bigcup_{\alpha<\lambda} \alpha$.

Став 3.15 Сваки ординал $\alpha \neq 0$ или је следбеник, или је гранични ординал.

Доказ. Приметимо да смо у формулацији користили тзв. ексклузивну дисјункцију „или, ..., или“. Дакле, тачно једно од наведена два својства је испуњено. Покажимо пре свега да следбеник никада није гранични ординал. У ту сврху, нека је $\alpha = s(\beta) = \beta \cup \{\beta\}$. Тада

$$\bigcup_{\gamma<\alpha} \gamma = \beta < \alpha.$$

Према томе, α није гранични. Претпоставимо да је $\lambda \neq 0$ и да није следбеник. Показаћемо да је λ гранични ординал. Формирајмо ординал μ са

$$\mu = \bigcup_{\alpha<\lambda} \alpha.$$

(Зашто је μ ординал?) Јасно је да је $\mu \subseteq \lambda$. Претпоставимо да је $\mu \subset \lambda$. То значи да је $\mu < \lambda$, те је $\lambda \geq s(\mu)$ (зашто?) и пошто λ није следбеник, добијамо $s(\mu) < \lambda$. Следи да је $s(\mu) \leq \mu$, што није могуће ($\mu \notin \mu$). Закључујемо да мора бити $\mu = \lambda$, тј.

$$\lambda = \bigcup_{\alpha<\lambda} \alpha,$$

што значи да је ординал λ гранични. □

Дакле, постоје три типа ординала

- 0;
- следбеници;
- гранични ординали.

Приметимо да смо већ почели да користимо неке типичне ознаке за ординале. Наиме, произвољне ординале обично ћемо означавати словима α, β, γ, док је ознака λ углавном резервисана за граничне ординале. Формулишимо сада принцип индукције у најављеном облику (тај облик је често и погоднији за примену од претходног).

Теорема 3.16 Нека је P неко својство ординала. Претпоставимо да

1. $P(0)$ важи;
2. За сваки ординал α важи: ако $P(\alpha)$ онда $P(s(\alpha))$;
3. Ако је λ гранични ординал и $P(\alpha)$ важи за све $\alpha < \lambda$, тада важи и $P(\lambda)$.

Тада је $P(\alpha)$ испуњено за сваки ординал α.

Доказ. Ову теорему нећемо доказивати — даћемо само упутство, а доказ препуштамо читаоцу за (добру) вежбу. Посматрајте својство Q задато са:

$$Q(\alpha) \text{ важи} \stackrel{\text{def}}{\Longleftrightarrow} P(\beta) \text{ важи за све } \beta \leq \alpha$$

и примените трансфинитну индукцију за доказивање да је $Q(\alpha)$ испуњено за све ординале α. Да ли вас ова идеја на нешто подсећа? $\square$

3.2 Ординална аритметика

Како се сабирају и множе ординали? Даћемо две дефиниције, за које ће се касније показати да су еквивалентне. Предност у оваквом приступу је у томе што понекад, за доказивање неких својстава, а уопште и у раду са ординалима, можемо користити једну дефиницију, а понекад другу.

Дефиниција 3.17 Нека су $(X, \leq_X)$ и $(Y, \leq_Y)$ уређени скупови. Дефинишемо *уређену суму* и *уређени производ* тих скупова. Нека је $S = X \times \{0\} \bigcup Y \times \{1\}$. Дефинишемо уређење на S са

- $(\forall x, x_1 \in X)((x,0) <_S (x_1,0) \stackrel{\text{def}}{\Longleftrightarrow} x <_X x_1)$
- $(\forall y, y_1 \in Y)((y,1) <_S (y_1,1) \stackrel{\text{def}}{\Longleftrightarrow} y <_Y y_1)$
- $(\forall x \in X)(\forall y \in Y)(x,0) <_S (y,1)$

Уређена сума $(X, \leq_X)$ и $(Y, \leq_Y)$ је $(S, \leq_S)$.
Нека је $P = X \times Y$. Дефинишемо уређење на P са

$$(x, y) <_P (x_1, y_1) \overset{\text{def}}{\iff} y <_Y y_1 \vee (y = y_1 \wedge x <_X x_1).$$

Уређени производ $(X, \leq_X)$ и $(Y, \leq_Y)$ је $(P, \leq_P)$.

Прокоментаришимо укратко претходну дефиницију. Идеја уређене суме два скупа је јасна — скуп X стављамо „испред“ скупа Y. Пошто скупови X и Y можда нису дисјунктни (а како намеравамо да тако дефинишемо сабирање међу ординалима, који *сигурно* нису дисјунктни ту могућност морамо узети у обзир), то смо уместо њих посматрали скупове $X \times \{0\}$ и $Y \times \{1\}$, који јесу дисјунктни. Што се тиче производа, ту смо користили лексикографски поредак, али гледано са десна на лево. Видећемо касније због чега је то згодно. Уређена сума (производ) ординала α и β у (привременој) ознаци $\alpha +_u \beta$ $(\alpha \cdot_u \beta)$ дефинише се као јединствени ординал који је изоморфан уређеној суми (производу) скупова α и β. Приметимо одмах да сабирање ординала није комутативно. Наиме

$$1 +_u \omega = \omega \neq \omega +_u 1.$$

Наиме, $1 +_u \omega$ добијамо када „испред“ свих природних бројева ставимо још један елемент, но тај новодобијени уређени скуп је изоморфан ω (једноставна транслација остварује изоморфизам), док је $\omega +_u 1$ добијено када се „иза“ свих природних бројева дода још један елемент. Тај скуп има највећи елемент (тај додати елемент је највећи), а скуп природних бројева нема највећи елемент, па не могу бити изоморфни.

Пређимо сада на другу дефиницију.

Дефиниција 3.18 Дефинишемо збир и производ ординала.
Дефиниција збира

S1 $\alpha + 0 = \alpha$;

S2 $\alpha + s(\beta) = s(\alpha + \beta)$;

S3 $\alpha + \lambda = \bigcup_{\gamma < \lambda} (\alpha + \gamma)$ за гранични ординал λ.

Дефиниција производа

P1 $\alpha \cdot 0 = 0$;

P2 $\alpha \cdot s(\beta) = \alpha \cdot \beta + \alpha$;

P3 $\alpha \cdot \lambda = \bigcup_{\gamma < \lambda} (\alpha \cdot \gamma)$ за гранични ординал λ.

Приметимо да је ова дефиниција врло слична дефиницији коју смо дали за сабирање и множење природних бројева. То се могло и очекивати, јер ординали представљају наставак природних бројева „иза коначног подручја“. Овде смо користили рекурзију по ординалима и чињеницу да је сваки ординал или 0 или следбеник или гранични ординал. Стога се и појављују три случаја, а не само два као код природних бројева.

Коришћењем друге дефиниције добијамо

$$\begin{aligned}\omega\cdot 2 &= \omega\cdot 1' \\ &= \omega\cdot 1+\omega \\ &= \omega\cdot 0'+\omega \\ &= (\omega\cdot 0+\omega)+\omega \\ &= \omega+\omega,\end{aligned}$$

те видимо да се $\omega\cdot 2$ добија када се „иза“ свих природних бројева дода још један примерак истог скупа. У овом доказу смо користили чињеницу да је $0+\omega=\omega$. Зашто је то тачно?

Са друге стране

$$\begin{aligned}2\cdot\omega &= \bigcup_{n\in\omega}(2\cdot n) \\ &= \omega,\end{aligned}$$

што показује да не важи ни комутативност множења.

Став 3.19 За све ординале α и β важи

1. $\alpha +_u \beta = \alpha+\beta$;
2. $\alpha \cdot_u \beta = \alpha\cdot\beta$.

Доказ. Извешћемо само доказ за сабирање. Доказ за множење препуштамо читаоцу. Нека је α произвољан ординал. Доказаћемо да важи

$$\alpha +_u \beta = \alpha+\beta,$$

индукцијом по β. Према нашој другој формулацији принципа индукције за ординале разликујемо три случаја.

1. $\beta=0$: У овом случају све је јасно — оба збира дају α.

2. Претпоставићемо да је тврђење тачно за ординал β. Треба да га докажемо и за $s(\beta)$. Знамо да је

$$\begin{aligned}\alpha+s(\beta) &= s(\alpha+\beta) \\ &= \alpha+\beta\cup\{\alpha+\beta\}.\end{aligned}$$

По претпоставци је $\alpha+\beta=\alpha +_u \beta$. Наш задатак је да покажемо да је јединствени ординал који је изоморфан уређеној суми ординала α и

$s(\beta)$ баш ординал $\alpha+\beta\cup\{\alpha+\beta\}$. Уређена сума ординала α и $s(\beta)$ добија се када се „иза“ ординала α, постави ординал $s(\beta) = \beta \cup \{\beta\}$. Но, то је исто као да иза ординала α поставимо прво цео ординал β, а затим додамо још и елемент β, тј. то је уређена сума ординала $\alpha+_u\beta = \alpha+\beta$ и једночланог скупа $\{\beta\}$. То није ништа друго до $\alpha+\beta\cup\{\alpha+\beta\}$ (подсетимо се да је $\gamma < \alpha + \beta$, за све ординале $\gamma \in \alpha + \beta$).

3. Нека је λ гранични ординал и претпоставимо да је тврђење тачно за све ординале $\gamma < \lambda$, тј. за све $\gamma < \lambda$ важи

$$\alpha +_u \gamma = \alpha + \gamma.$$

Погледајмо како се формирају оба ова скупа. Пре свега, $\alpha +_u \lambda$ добијамо када иза ординала α поставимо цео ординал λ. Са друге стране, по дефиницији је

$$\alpha + \lambda = \bigcup_{\gamma<\lambda} (\alpha + \gamma).$$

Но, по претпоставци је $\alpha + \gamma = \alpha +_u \gamma$, за све $\gamma < \lambda$. Дакле, скупови из наведене уније се добијају када иза ординала α постављамо ординале из λ (подсетимо се да је $\gamma < \lambda \iff \gamma \in \lambda$). Како је $\lambda = \bigcup_{\gamma<\lambda} \gamma$, то се наведена унија формира од растуће колекције скупова чија унија није ништа друго до $\alpha +_u \lambda$ ($\alpha +_u \gamma \subset \alpha +_u \gamma_1$, ако је $\gamma \subset \gamma_1$). $\square$

У оквиру следећег става наводимо најважније особине овако дефинисаних операција. Доказе препуштамо читаоцима. Они су углавном слични одговарајућим доказима за природне бројеве, једино се случај граничних ординала разликује. За тај случај можете искористити метод који смо користили у доказу претходног става.

Став 3.20 Нека су $\alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2, \gamma$ ординали. Тада важи

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;
2. $\alpha + 0 = \alpha = 0 + \alpha$;
3. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$;
4. $\alpha \cdot 0 = 0 = 0 \cdot \alpha$;
5. $\alpha \cdot 1 = \alpha = 1 \cdot \alpha$;
6. $\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$;
7. Не постоји ординал β такав да важи: $\alpha < \beta < \alpha + 1$;
8. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$;
9. $\alpha \leq \alpha + \beta$, $\alpha \leq \beta + \alpha$;
10. $\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta$;

11. $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$;
12. $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$;
13. $\gamma \neq 0 \Rightarrow (\alpha < \beta \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta)$;
14. $\gamma \cdot \alpha < \gamma \cdot \beta \Rightarrow \alpha < \beta$;
15. $\gamma \neq 0 \Rightarrow (\gamma \cdot \alpha = \gamma \cdot \beta \Rightarrow \alpha = \beta)$;
16. Ако је $\alpha_1 + \beta_1 \leq \alpha_2 + \beta_2$ и $\beta_2 < \beta_1$, онда је $\alpha_1 < \alpha_2$. □

Као што је операција одузимања дефинисана за неке парове природних бројева, то је случај са операцијом одузимања и код ординала. Наиме, претпоставимо да је $\alpha \leq \beta$. Дефинишемо $\beta - \alpha$ са:

$$\gamma = \beta - \alpha \overset{\text{def}}{\Longleftrightarrow} \alpha + \gamma = \beta.$$

Поставља се питање добре дефинисаности ове операције. Наиме, да ли је заиста тачно да за све ординале α и β за које важи $\alpha \leq \beta$ постоји ординал γ такав да је $\alpha + \gamma = \beta$? И да ли је тај ординал γ јединствен?

Став 3.21 Нека су α и β ординали такви да је $\alpha \leq \beta$. Тада постоји тачно један ординал γ такав да $\alpha + \gamma = \beta$.

Доказ. Тачка 6 претходног става показује да, ако такав ординал постоји, он мора бити јединствен. Позабавимо се питањем његовог постојања. Како је $\alpha + \beta \geq \beta$ и $\beta \in s(\beta)$, то је скуп

$$M = \{\gamma \in s(\beta) : \alpha + \gamma \geq \beta\}$$

непразан. Како је $M \subseteq s(\beta)$, а $s(\beta)$ добро уређен скуп (као и сваки други ординал), то у M постоји најмањи елемент. Означимо га са γ_0. Тврдимо да је $\alpha + \gamma_0 = \beta$. У супротном, $\alpha + \gamma_0 > \beta$. Ординал γ_0 сигурно није 0 (зашто?), па за њега остају две могућности — или је он следбеник, или је гранични ординал. Претпоставимо да је $\gamma_0 = s(\delta)$. Тада добијамо

$$\beta < \alpha + \gamma_0 = \alpha + s(\delta) = s(\alpha + \delta),$$

из чега закључујемо да је $\beta \leq \alpha + \delta$, па би ординал δ припадао скупу M и био мањи од ординала γ_0, који је најмањи елемент у том скупу! Закључујемо да ординал γ_0 не може бити следбеник. Претпоставимо да је он гранични ординал. У том случају је $\gamma_0 = \bigcup_{\delta < \gamma_0} \delta$. За све $\delta < \gamma_0$ мора важити: $\alpha + \delta < \beta$ (по дефиницији скупа M). Стога је

$$\alpha + \gamma_0 = \bigcup_{\delta < \gamma_0} (\alpha + \delta) \leq \beta,$$

но то противречи претпоставци да је $\alpha + \gamma_0 > \delta$. Закључујемо да је претпоставка погрешна и да мора бити $\alpha + \gamma_0 = \beta$. □

Доказаћемо сада следећи став, чији би се други део могао звати и „став о дељењу са остатком“.

Став 3.22 а) Ако је $\gamma < \alpha \cdot \beta$ онда постоје ординали $\delta < \alpha$ и $\varepsilon < \beta$ такви да је $\gamma = \alpha \cdot \varepsilon + \delta$ и они су јединствено одређени.
б) Нека је $\beta > 0$. Тада за сваки ординал α постоје јединствено одређени ординали γ и $\delta < \beta$ такви да је $\alpha = \beta \cdot \gamma + \delta$.

Доказ а) Подсетимо се да је ординал $\alpha \cdot \beta$ дефинисан као ординал који је изоморфан уређеном производу скупова α и β. Како је $\gamma < \alpha \cdot \beta$, то закључујемо да је γ изоморфан неком почетном комаду $(\alpha \times \beta)_{(\delta,\varepsilon)}$ ($\alpha \times \beta$ је уређени производ ординала α и β). Проверимо како изгледа тај почетни комад.

$$\begin{aligned}
(\alpha \times \beta)_{(\delta,\varepsilon)} &= \{(x,y) \in \alpha \times \beta : (x,y) < (\delta,\varepsilon)\} \\
&= \{(x,y) \in \alpha \times \beta : y < \varepsilon \vee (y = \varepsilon \wedge x < \delta)\} \\
&= \{(x,y) \in \alpha \times \beta : y < \varepsilon\} \cup \{(x,y) \in \alpha \times \beta : y = \varepsilon \wedge x < \delta\} \\
&= \alpha \times \beta_\varepsilon \cup \alpha_\delta \times \{\varepsilon\}.
\end{aligned}$$

Уређење у скупу $\alpha \times \beta$ смо због једноставности означавали са $<$. Приметимо да је сваки елемент у скупу $\alpha \times \beta_\varepsilon$ мањи (у смислу поретка на скупу $\alpha \times \beta$) од сваког елемента из скупа $\alpha_\delta \times \{\varepsilon\}$. Стога закључујемо да поредак на скупу $\alpha \times \beta$ индукује поредак на скупу $\alpha \times \beta_\varepsilon \cup \alpha_\delta \times \{\varepsilon\}$ који представља уређену суму скупова $\alpha \times \beta_\varepsilon$ и $\alpha_\delta \times \{\varepsilon\}$, док тај поредак на скупу $\alpha \times \beta_\varepsilon$ индукује уређени производ тих скупова. Према томе, ординал γ који је изоморфан том почетном комаду, није ништа друго до $\alpha \cdot \varepsilon + \delta$ ($\beta_\varepsilon = \varepsilon, \alpha_\delta = \delta$), што се и тражило.

Пређимо сада на доказ јединствености. У ту сврху, претпоставимо да је

$$\alpha \cdot \varepsilon_1 + \delta_1 = \gamma = \alpha \cdot \varepsilon_2 + \delta_2,$$

при чему важи: $\delta_1, \delta_2 < \alpha$ и $\varepsilon_1, \varepsilon_2 < \beta$. Претпоставимо да је $\varepsilon_1 < \varepsilon_2$. Тада је $\varepsilon_1 + 1 \leq \varepsilon_2$. Добијамо

$$\begin{aligned}
\gamma &= \alpha \cdot \varepsilon_1 + \delta_1 \\
&< \alpha \cdot \varepsilon_1 + \alpha \\
&= \alpha \cdot \varepsilon_1 + \alpha \cdot 1 \\
&= \alpha \cdot (\varepsilon_1 + 1) \\
&\leq \alpha \cdot \varepsilon_2 \\
&\leq \alpha \cdot \varepsilon_2 + \delta_2 \\
&= \gamma.
\end{aligned}$$

(Овде смо користили нека својства из Става 3.20.) Према томе, добијамо да је $\gamma < \gamma$. Закључујемо да *није* $\varepsilon_1 < \varepsilon_2$. На исти начин се показује да не може бити ни $\varepsilon_2 < \varepsilon_1$, па мора бити $\varepsilon_1 = \varepsilon_2$. Но, тада, на основу Става 3.20 добијамо да је и $\delta_1 = \delta_2$ чиме је доказана јединственост.

б) Како је $\alpha = 1 \cdot \alpha < \beta \cdot (\alpha + 1)$, то на основу претходног добијамо да постоје јединствено одређени ординали γ и δ такви да је $\delta < \beta$ и $\alpha = \beta \cdot \gamma + \delta$. □

Операција степеновања ординала ординалом уводи се следећом дефиницијом.

Дефиниција 3.23 Степеновање ординала задато је са:

E1 $\alpha^0 = 1$;

E2 $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$;

E3 $\alpha^\lambda = \bigcup_{\gamma<\lambda} \alpha^\gamma$, за гранични ординал λ.

Остављамо да читаоци за вежбу докажу следећа својства управо дефинисаног степеновања

1. $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
2. $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$

Према томе $\omega^2 = \omega \cdot \omega$, тј. ω^2 представља скуп који се добија када се пребројиво много копија скупа ω постави једна иза друге. Интересантно је приметити да је тај ординал изоморфан једном подскупу скупа рационалних бројева. Наиме посматрајмо скуп

$$S = \{m - \frac{1}{n} : m, n \in \mathbb{N}, m \geq 1, n \geq 2\},$$

уз стандардну релацију уређења међу рационалним бројевима. Показаћемо да је тај посет изоморфан ординалу ω^2. У ту сврху је довољно доказати следеће:

$$m - \frac{1}{n} < m_1 - \frac{1}{n_1} \Longleftrightarrow m < m_1 \vee (m = m_1 \wedge n < n_1).$$

$\Longrightarrow$: Нека је $m - \frac{1}{n} < m_1 - \frac{1}{n_1}$. Тада добијамо

$$\begin{aligned} m &< m_1 + \frac{1}{n} - \frac{1}{n_1} \\ &< m_1 + \frac{1}{n} + \frac{1}{n_1} \\ &\leq m_1 + \frac{1}{2} + \frac{1}{2} \\ &= m_1 + 1. \end{aligned}$$

Према томе добијамо да је $m < m_1 + 1$. Тада је $m < m_1$ или $m = m_1$. Уколико је $m < m_1$ добијамо тражено, а ако је $m = m_1$, то добијамо да је $-\frac{1}{n} < -\frac{1}{n_1}$, из чега закључујемо да је $n < n_1$.

$\Longleftarrow$: Претпоставимо да је $m < m_1$. Тада је

$$m - \frac{1}{n} + \frac{1}{n_1} < m + \frac{1}{2} + \frac{1}{2} = m + 1 \leq m_1,$$

из чега добијамо да је $m - \frac{1}{n} < m_1 - \frac{1}{n_1}$.

Остављамо читаоцу за вежбу да исту анализу понови и у случају ординала $\omega^3, \omega^4, \ldots$ Скуп ω^ω је (подсетимо се да је ординал ω гранични) задат са

$$\omega^\omega = \bigcup_{n \in \omega} \omega^n.$$

Размислите и о њему.
За додатну илустрацију рада са ординалима урадићемо пар примера.

Пример 3.24 Сваки бесконачни ординал може се написати у облику $\lambda + n$, где је λ гранични ординал, а $n \in \omega$.

Ову чињеницу није тешко доказати. Наиме, претпоставимо да постоји неки ординал α, који није траженог облика и означимо са β најмањи бесконачни ординал који није траженог облика (тада је $\beta \in s(\alpha)$). Ординал β сигурно није 0, јер је бесконачан. Он није ни гранични ординал, јер гранични ординал јесте траженог облика. Остаје могућност да је ординал β следбеник, тј. $\beta = \gamma + 1$, за неки ординал γ. Како је ординал γ бесконачан, а уз то је и $\gamma < \beta$, то закључујемо да је $\gamma = \lambda + n$ за неки гранични ординал λ и $n \in \omega$, но тада је и $\beta = \lambda + (n + 1)$, што противречи избору ординала β.

Пример 3.25 Ординал λ је гранични ако и само ако је $\lambda = \omega \cdot \alpha$ за неки ординал $\alpha \neq 0$.

Применићемо горе наведени „став о дељењу са остатком“. Нека је λ неки гранични ординал. Према споменутом ставу, постоје ординали α и $\delta < \omega$, такви да је $\lambda = \omega \cdot \alpha + \delta$. Како је $\delta < \omega$ и ординал λ гранични,то закључујемо да мора бити $\delta = 0$ (у супротном $\lambda = s(\omega \cdot \alpha + \delta - 1)$) и добијамо $\lambda = \omega \cdot \alpha$.

Посматрајмо ординал $\omega \cdot \alpha$ за неки ординал $\alpha \neq 0$ и претпоставимо да је $\omega \cdot \alpha = \gamma + 1$. Дакле, $\gamma < \omega \cdot \alpha$, па постоје ординали $n < \omega$ и $\varepsilon < \alpha$ такви да је $\gamma = \omega \cdot \varepsilon + n$. Но, тада је

$$\gamma + 1 = \omega \cdot \varepsilon + (n + 1) < \omega \cdot \varepsilon + \omega = \omega \cdot (\varepsilon + 1) \leq \omega \cdot \alpha = \gamma + 1.$$

Ова контрадикција показује да је ординал $\omega \cdot \alpha$ гранични.

Пример 3.26 Нека је γ произвољни ординал. Доказати да се ординал ω^γ не може представити у облику збира два ненула ординала.

Претпоставимо да је $\omega^\gamma = \alpha + \beta$ и $\beta \neq 0$. Доказаћемо да је $\alpha = 0$. Разликујемо три случаја.

$\underline{\gamma = 0}$ Ако је $\omega^0 = \alpha + \beta$ и $\beta \neq 0$, то из чињенице да је $\omega^0 = 1$, следи да мора бити $\alpha = 0$ и $\beta = 1 = \omega^0$.

γ је следбеник Нека је $\gamma = s(\delta)$. Тада је $\alpha + \beta = \omega^\gamma = \omega^\delta \cdot \omega$. Како је $\beta \neq 0$, закључујемо да је $\alpha < \omega^\delta \cdot \omega$. Према Ставу 3.22 закључујемо да постоје $\varepsilon < \omega$ и $\tau < \omega^\delta$ такви да је $\alpha = \omega^\delta \cdot \varepsilon + \tau$. Тада је

$$\alpha < \omega^\delta \cdot \varepsilon + \omega^\delta = \omega^\delta \cdot (\varepsilon + 1).$$

Како је $\varepsilon + 1 + \omega = \omega$ (зашто?) то добијамо

$$\begin{aligned} \alpha + \beta &= \omega^\gamma \\ &= \omega^\delta \cdot \omega \\ &= \omega^\delta \cdot (\varepsilon + 1 + \omega) \\ &= \omega^\delta \cdot (\varepsilon + 1) + \omega^\delta \cdot \omega \\ &= \omega^\delta \cdot (\varepsilon + 1) + \omega^\gamma \end{aligned}$$

Како је $\alpha < \omega^\delta \cdot (\varepsilon + 1)$, то закључујемо да је $\beta \geq \omega^\gamma$. То, уз чињеницу да је $\omega^\gamma = \alpha + \beta$, даје $\omega^\gamma = \beta$.

γ је гранични ординал Дакле, $\alpha + \beta = \omega^\gamma = \bigcup_{\delta < \gamma} \omega^\delta$. Ако би било $\alpha \geq \omega^\delta$ за све $\delta < \gamma$ добили бисмо да је $\alpha \geq \bigcup_{\delta < \gamma} \omega^\delta = \omega^\gamma$. Но, $0 < \beta \Rightarrow \alpha < \alpha + \beta$, па бисмо добили

$$\omega^\gamma \leq \alpha < \alpha + \beta = \omega^\gamma.$$

Закључујемо да постоји $\delta < \gamma$ такав да је $\omega^\delta > \alpha$. Нека је δ_0 најмањи такав. Како $\delta_1 \leq \delta_2 \Rightarrow \omega^{\delta_1} \leq \omega^{\delta_2}$ (показати да то важи), то је

$$\omega^\gamma = \bigcup_{\delta < \gamma} \omega^\delta = \bigcup_{\delta_0 \leq \delta < \gamma} \omega^\delta.$$

Показаћемо да је $\beta \geq \omega^\delta$ за све δ такве да $\delta_0 \leq \delta < \gamma$. Покажимо то пре свега за ординале δ који су следбеници. Тај доказ је врло сличан доказу претходног случаја. Наиме, нека је $\delta = s(\delta_1)$. Тада је $\alpha < \omega^{\delta_1} \cdot \omega$, па је, као у претходном случају $\alpha < \omega^{\delta_1} \cdot (\varepsilon + 1)$ за неки $\varepsilon < \omega$. Осим тога

$$\begin{aligned} \alpha + \beta &\geq \omega^\delta \\ &= \omega^{\delta_1} \cdot \omega \\ &= \omega^{\delta_1} \cdot (\varepsilon + 1 + \omega) \\ &= \omega^{\delta_1} \cdot (\varepsilon + 1) + \omega^\delta, \end{aligned}$$

што, уз наведену чињеницу да је $\alpha < \omega^{\delta_1} \cdot (\varepsilon + 1)$, даје $\beta \geq \omega^\delta$. Како стоји ствар са граничним ординалима δ? Приметимо да смо заправо доказали следеће

$$\beta \geq \omega^{\delta} \text{ за све следбенике који су мањи од } \gamma.$$

Наиме, за ординале мање од δ_0 неједнакост следи из неједнакости за веће ординале. Претпоставимо да постоји неки гранични ординал λ, такав да је $\lambda < \gamma$ и да је $\beta < \omega^{\lambda}$. Нека је λ_0 најмањи такав. То значи да за све ординале τ који су мањи од λ_0 важи $\beta \geq \omega^{\tau}$ (подсетимо се да смо то доказали за све следбенике, а наравно да је тачно и за 0). Но, тада је и

$$\omega^{\lambda_0} = \bigcup_{\tau < \lambda_0} \omega^{\tau} \leq \beta.$$

Закључујемо да је $\beta \geq \omega^{\delta}$ за све ординале $\delta < \gamma$, па је и $\beta \geq \bigcup_{\delta < \gamma} \omega^{\delta} = \omega^{\gamma}$. Према томе, добијамо $\beta = \omega^{\gamma}$ што се и тражило.

3.3 Аксиома избора и њени еквиваленти

У овом тренутку би за читаоца било добро да поново погледа формулацију и доказ Става 2.23. Поставља се природно питање: да ли важи општији став од наведеног? Будимо прецизнији: да ли је тачно да постојање сурјекције из X у Y гарантује постојање инјекције из Y у X, где су X и Y *произвољни скупови*? Покушајмо да докажемо то тврђење. По претпоставци постоји $f\colon X \to Y$, тако да је f „на“. За доказ је *довољно* показати да постоји $g\colon Y \to X$ тако да је $f \circ g = \mathrm{Id}_Y$. У ту сврху, нека је $y \in Y$ произвољно. Како је f „на“, то скуп $f^{-1}[\{y\}]$ није празан. *Изаберимо* било који елемент x из тог скупа и дефинишимо вредност функције g у тачки y са $g(y) = x$. Ако то урадимо за сваки елемент из скупа Y добићемо тражену функцију g. Рекло би се, ништа једноставније од тога. Но, ми смо овде користили избор елемента из неког скупа, заправо избор *по једног елемента из сваког од међусобно дисјунктних скупова* $f^{-1}[\{y\}]$, $y \in Y$. Чини се да је само по себи очигледно да то увек можемо да урадимо, али ипак није тако. Наиме, ниједна од до сада наведених аксиома не гарантује нам да се тако нешто може извести.

Погледајмо још један пример. Несумњиво сте већ имали прилике да се упознате са директним, или Декартовим производом било које фамилије скупова. Подсетимо се тога. Нека је, дакле, $\mathcal{F} = \{A_i : i \in I\}$ и претпоставимо да је $A_i \neq \emptyset$, за све $i \in I$. Декартов производ

$$\prod_{i \in I} A_i$$

ове фамилије скупова дефинише се са:

$$\prod_{i \in I} A_i \stackrel{\text{def}}{=} \{f\colon I \to \bigcup_{i \in I} A_i \,|\, f(i) \in A_i, \text{ за све } i \in I\}.$$

Поставља се питање: да ли је $\prod_{i \in I} A_i \neq \emptyset$? Опет се чини да је то нешто само по себи очигледно, али није. Оно о чему смо заправо у претходним редовима дискутовали тиче се *Аксиоме избора* и ми смо се кроз ова два примера упознали са две њене формулације.

Наведимо сада експлицитно те две формулације.

Прва формулација Аксиоме избора (постојање изборног скупа) Нека је $\mathcal{F}$ скуп међусобно дисјунктних, непразних скупова. Тада постоји скуп C такав да је $C \cap X$ једночлан за све $X \in \mathcal{F}$. Тај скуп се назива изборни скуп или трансверзала.

Друга формулација Аксиоме избора (постојање функције избора) Ако је дат скуп $\mathcal{F}$ чији су сви елементи непразни скупови онда постоји функција $f\colon \mathcal{F} \to \cup\mathcal{F}$ таква да $f(X) \in X$, за све $X \in \mathcal{F}$. Та функција се назива функција избора.

Није тешко уверити се да су ове две формулације еквивалентне. Ако претпоставимо да постоји изборни скуп за сваки скуп дисјунктних и непразних скупова онда је лако конструисати тражену функцију избора за скуп $\mathcal{F}$ који се састоји од непразних, али не обавезно дисјунктних скупова. Наиме, добро је познат „трик“ како се од скупова који не морају бити дисјунктни „праве“ скупови који *јесу* дисјунктни. Формирајмо, наиме, скуп $\mathcal{F}' = \{X \times \{X\} : X \in \mathcal{F}\}$. Новодобијени скупови $X \times \{X\}$ јесу дисјунктни и сада нам постојање изборног скупа даје и функцију избора.

У супротном, ако претпоставимо да је могуће задати функцију избора, онда је јасно да се тражени изборни скуп може формирати као слика скупа $\mathcal{F}$ при функцији избора.

У даљем ћемо чешће користити формулацију која гарантује постојање функције избора.

Аксиома избора представља вероватно најсуптилнију од свих аксиома теорије скупова које смо имали прилике да разматрамо. Мада има доста једноставну формулацију, она се ипак не може доказати из других аксиома. Велики део савремене математике било би врло тешко развијати без ове аксиоме, а са друге стране она има и неке, да се тако изразимо „нежељене“ последице. У даљем тексту упознаћемо се са неким еквивалентима Аксиоме избора, као и непосредним последицама које из ње (односно њених еквивалената) проистичу.

Овде ћемо навести само два еквивалента Аксиоме избора који ће нам бити од користи у даљем раду и у применама. То су *Цорнова*[2] *лема* и *Принцип доброг уређења.*

[2]Max August Zorn (1906–1993), немачки (и амерички) математичар.

Цорнова лема Ако у неком посету сваки ланац има мајоранту онда тај посет поседује максимални елемент.

Подсетимо се да под посетом подразумевамо парцијално уређени скуп, док је ланац онај његов подскуп чија су свака два елемента упоредива. За неки елемент a кажемо да је *мајоранта*, или горње ограничење, скупа L ако је $x \leq a$, за све $x \in L$. Максималан елемент m у посету P је наравно онај за који не постоји елемент $x \in P$ такав да $x > m$.

Принцип доброг уређења Сваки скуп може се добро уредити.

Обратите пажњу на чињеницу колико се формулација Цорнове леме чини сложенијом од формулације принципа доброг уређења. Упркос томе, Цорнова лема се веома много користи за доказивање егзистенције многих објеката и њено коришћење је врло једноставно.

Докажимо сада наведену еквивалентност.

Теорема 3.27 Следећа тврђења су међусобно еквивалентна.

(1) Принцип доброг уређења;

(2) Аксиома избора;

(3) Цорнова лема.

Доказ. Као и обично, у ситуацијама када треба доказати еквивалентност неких тврђења, важно је добро одабрати поредак доказивања. Ми смо овде одабрали да докажемо тражено по следећој схеми.

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1).$$

(1) $\Rightarrow$ (2): Нека је $\mathcal{F}$ скуп чији су сви елементи непразни скупови. Треба наћи функцију избора. У ту сврху добро уредимо скуп $\cup\mathcal{F}$. То можемо урадити, јер смо претпоставили да принцип доброг уређења важи. Сада је лако наћи функцију избора — $f\colon \mathcal{F} \to \cup\mathcal{F}$ дефинишемо са

$$f(X) = \min X.$$

(2) $\Rightarrow$ (3): Нека је $(P, \leq)$ непразан парцијално уређен скуп у коме сваки ланац има мајоранту. Треба показати да тада P садржи максимални елемент. Претпоставићемо да то није тачно. Уз ту претпоставку и коришћење Аксиоме избора конструисаћемо „1–1“ функцију F из класе On свих ординала у скуп P. Постојање такве функције гарантује, уз коришћење Аксиоме замене, да је On скуп, а видели смо да то није тачно. Тиме добијамо контрадикцију. Пређимо сада на конструкцију тражене функције.

Нека је f функција избора за фамилију свих непразних подскупова од P. Како имамо три типа ординала то тако и дефинишемо функцију

F. За вредност $F(0)$ можемо изабрати било који елемент из P. Како је функција f функција која за нас „врши избор“ то дефинишемо

$$F(0) \stackrel{\text{def}}{=} f(P).$$

Претпоставимо да је $F(\alpha)$ дефинисано за ординал α и наш је задатак да дефинишемо $F(s(\alpha))$.

$$F(s(\alpha)) \stackrel{\text{def}}{=} f(\{x \in P : x > F(\alpha)\}).$$

Наиме, скуп $\{x \in P : x > F(\alpha)\}$ је непразан, јер по претпоставци P не садржи максималан елемент те за сваки елемент постоји елемент који је већи од њега. Такав избор нам гарантује да је $F(s(\alpha)) > F(\alpha)$. На крају дефинишимо $F(\lambda)$, за гранични ординал λ, под претпоставком да је $F(\alpha)$ дефинисано за све $\alpha < \lambda$. Опет ћемо се при дефинисању $F(\lambda)$ водити идејом да важи $F(\lambda) > F(\alpha)$, за све $\alpha < \lambda$. Приметимо, пре свега да је $F[\lambda]$ ланац. Наиме, може се доказати, индукцијом у добро уређеном скупу λ да важи: $\alpha < \beta \Rightarrow F(\alpha) < F(\beta)$. Према томе, $F[\lambda]$ је ланац. Како је то тако, а у P сваки ланац има мајоранту (по претпоставци), то је скуп тих мајоранти непразан. Означимо га са M и дефинишимо

$$F(\lambda) \stackrel{\text{def}}{=} f(M).$$

Према томе дефинисали смо F и она испуњава својство

$$\alpha < \beta \Rightarrow F(\alpha) < F(\beta),$$

за све ординале α и β. То завршава тражени доказ.
(3) $\Rightarrow$ (1): Преостало нам је да покажемо како се, уз помоћ Цорнове леме, може сваки непразан скуп добро уредити. Нека је X дати скуп. Означимо са W следећи скуп

$$W = \{(Y, \leq_Y) : Y \subseteq X, \text{ а } \leq_Y \text{ је добро уређење на } Y\}.$$

Дакле, скуп W састоји се од свих могућих добрих уређења на подскуповима од X. Јасно је да је W непразан. Наиме, сваки једночлани подскуп од X јесте добро уређен и то, наравно, на јединствен начин. Када би се међу добро уређеним подскуповима од X који се налазе у W „крио“ и сам X (са неким добрим уређењем) то бисмо добили тражено. Да бисмо могли да применимо Цорнову лему, потребно је увести неко уређење на W. Тражено уређење дефинише се на природан начин:

$$(Y, \leq_Y) \prec (Z, \leq_Z) \stackrel{\text{def}}{\iff} Y = Z_z \text{ и } \leq_Y = \leq_Z \cap (Y \times Y).$$

Дакле, Y је почетни комад од Z и уређење на Y је рестрикција уређења на Z. На овај начин смо добили један посет $(W, \preceq)$ на који ћемо применити Цорнову лему. Наиме, нека је L неки ланац у W. Треба показати да он има мајоранту у W. Пре свега, ланац у W представља скуп добрих уређења на неким подскуповима од X тако да су свака два упоредива. Означимо са M следећу унију

$$M = \bigcup_{(Y,\leq_Y)\in L} Y.$$

Дефинишемо уређење $\leq_M$ на M на следећи начин. Нека су y и z произвољни елементи из M. Тада $y \in Y$ и $z \in Z$, за неке Y и Z такве да $(Y,\leq_Y),(Z,\leq_Z)\in L$. Како су свака два елемента упоредива то је $Y \subseteq Z$ или $Z \subseteq Y$. Нека је, нпр. $Y \subseteq Z$. Тада $y, z \in Z$ и дефинишемо

$$y \leq_M z \overset{\text{def}}{\iff} y \leq_Z z.$$

Поставља се питање добре дефинисаности ове релације. Наиме, ако ти елементи припадају и неком скупу V, шта се дешава ако покушамо да дефинишемо да је $y \leq_M z \iff y \leq_V z$? Но, V и Z су упоредиви и осим тога је релација на оном мањем рестрикција релације на оном већем па тако не добијамо никакву противречност. Релација $\leq_M$ је заиста добро дефинисана. Остаје да проверимо да смо тако добили један добро уређени скуп. Нека је U непразан подскуп од M. Тада је $U \cap Y_0 \neq \emptyset$, за неки Y_0 такав да $(Y_0,\leq_{Y_0})\in L$. Како је скуп Y_0 добро уређен и $U \cap Y_0$ његов непразан подскуп то он има најмањи елемент. Означимо га са u_0. Доказаћемо да је u_0 најмањи елемент у U. Нека је u произвољан елемент из U. Тада $u \in Y$ за неки скуп Y. Како су Y и Y_0 упоредиви (један је почетни комад другог) разликујемо два случаја.
1) Y је почетни комад од Y_0. У то случају, како је u_0 најмањи елемент у $U \cap Y_0$, он мора бити мањи и од u ($u \in U \cap Y_0$).
2) Y_0 је почетни комад од Y. Тада је $Y_0 = Y_y$ за неки $y \in Y$. Тада је и $u_0 < y$. Ако је $u < y$ онда $u \in Y_0$, тј. $u \in Y_0 \cap U$, па је сигурно $u_0 \leq u$ (u_0 је најмањи елемент у том скупу). Ако је $u \geq y$, то је $u > u_0$ ($u_0 < y$). У сваком случају добијамо $u_0 \leq u$. Како је u био произвољни елемент из U то закључујемо да је u_0 заиста најмањи елемент у том скупу чиме је завршен доказ добре уређености скупа M. По самој дефиницији скупа M, јасно је да је $(Y,\leq_Y) \preceq (M,\leq_M)$ за све $(Y,\leq_Y)\in L$, тј. заиста је $(M,\leq_M)$ мајоранта ланца L. Према Цорновој леми скуп W мора поседовати максималан елемент $(M_0,\leq_{M_0})$. Ако је $M_0 \neq X$ то постоји неки елемент $x \in X \setminus M_0$. На скупу $M' = M_0 \cup \{x\}$ можемо дефинисати поредак тако што елемент x прогласимо већим од свих елемената из M_0. Јасно је да смо тако добили добро уређен скуп $(M',\leq_{M'})$ такав да је $(M_0,\leq_{M_0}) \prec (M',\leq_{M'})$, што је у супротности са чињеницом да је $(M_0,\leq_{M_0})$ максималан елемент у W. Закључујемо да је $M_0 = X$ чиме је завршен доказ тврђења да се скуп X може добро уредити. $\square$

Пре него што у наредном одељку пређемо на неке непосредне последице Аксиоме избора наведимо још пар речи о принципу доброг уређења. Наиме, према принципу доброг уређења, сваки скуп може се добро уредити. Како нам је познато да је сваки добро уређени скуп изоморфан тачно једном ординалу, то принцип доброг уређења даје да сваки скуп X можемо приказати у облику

$$X = \{x_\alpha : \alpha < \mu\},$$

за неки ординал μ. Видећемо како се ова чињеница може искористити.

3.4 Неке последице Аксиоме избора

Овде се нећемо трудити да будимо превише исцрпни. Наиме, навешћемо само пар непосредних последица Аксиоме избора, које ће нам пре свега послужити за илустрацију како се у пракси примењује Аксиома избора и њени наведени еквиваленти. Читалац је имао, или ће имати прилике да упозна још неке директне последице ове аксиоме.

Први пример који наводимо тиче се егзистенције базе у векторском простору. Верујемо да читалац у курсу линеарне алгебре није имао прилике да се упозна са овим доказом у случају *произвољног* векторског простора, па овај доказ попуњава ту могућу празнину у читаочевом математичком образовању.

Теорема 3.28 Сваки векторски простор има базу.

Доказ. Претпоставићемо да су читаоцу познати основни појмови и чињенице из линеарне алгебре (заправо очекујемо да му је и доста више од тога познато, али се само основне ствари у овом доказу користе!). У доказу ћемо користити принцип доброг уређења. Дакле, задат је векторски простор V и треба показати да он има базу. Према принципу доброг уређења

$$V \setminus \{0\} = \{v_\alpha : \alpha < \mu\},$$

за неки ординал μ. Базу ћемо конструисати на прилично директан начин. Нека је $B_0 = \emptyset$. Ако је B_α дефинисано, за неки ординал $\alpha < \mu$, тада дефинишемо $B_{s(\alpha)}$ са

$$B_{s(\alpha)} = \begin{cases} B_\alpha, & \text{ако је } v_\alpha \text{ линеарна комбинација вектора из } B_\alpha \\ B_\alpha \cup \{v_\alpha\}, & \text{иначе} \end{cases}$$

За крај, нека је $\lambda(\leq \mu)$ гранични ординал. Тада дефинишемо

$$B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha.$$

Тражена база је $B = B_\mu$. Да бисмо то показали треба показати да је тај скуп линеарно независна генератриса. То није тешко показати. Наиме, ако је $v_\beta \neq 0$ произвољни елемент из V, тада је он или у $B_{s(\beta)}$, па јесте линеарна комбинација вектора из B, или није, у ком случају је, по конструкцији скупова B_α, он линеарна комбинација неких елемената из B_β. Дакле, B је заиста једна генератриса. Уколико претпоставимо да тај скуп није скуп линеарно независних вектора, то постоји нетривијална линеарна комбинација *коначно* много вектора из тог скупа. Нека је v_β, вектор из тог коначног скупа вектора са највећим индексом. Како је он линеарна комбинација вектора са мањим индексима, то закључујемо да се он не би смео ни појављивати у скупу $B_{s(\beta)}$, па тиме ни у скупу B. Дакле, скуп B заиста представља једну базу простора V. $\square$

Напомена: Пажљив читалац је могао да примети да смо ми заправо доказали да постоји линеарно независна генератриса. База је фамилија, а не само скуп — сетите се дефиниције базе из линеарне алгебре, односно матрице преласка са базе на базу; база је била уређена n-торка вектора, а не скуп вектора. Но, чим имамо линеарно независну генератрису, имамо и базу. Стандардни је трик да векторе индексирамо њима самима! Наиме, ако имамо скуп S, онда имамо и фамилију F индексирану скупом S: за $F : S \to S$ се може узети Id_S.

Пре следеће примене Аксиоме избора подсетимо се да је *максимални идеал* прстена A идеал M такав да је $M \neq A$ и, осим тога, не постоји идеал I за који важи: $M \subset I \subset A$.

Теорема 3.29 Сваки прстен са јединицом има максимални идеал.

Доказ. У доказу примењујемо Цорнову лему. Означимо са $\mathcal{I}$ скуп свих идеала прстена A који нису једнаки A. Јасно је да је скуп $\mathcal{I}$ уређен релацијом $\subseteq$. Нека је $\mathcal{L}$ ланац у $\mathcal{I}$. Ако је $\mathcal{L} = \emptyset$ онда је идеал $\{0\}$ мајоранта за тај ланац. Ако је $\mathcal{L} \neq \emptyset$, нека је $J = \bigcup \mathcal{L}$. Показаћемо да је J један идеал прстена A. У ту сврху, претпоставимо да су x_1 и x_2 из J. Тада $x_1 \in I_1$, а $x_2 \in I_2$, за неке идеале $I_1, I_2 \in \mathcal{L}$. Но, како је $\mathcal{L}$ ланац, то је $I_1 \subseteq I_2$ или $I_2 \subseteq I_1$. У сваком случају (узимајући већи од њих) закључујемо да су елементи x_1 и x_2 у неком идеалу из $\mathcal{L}$. Одатле следи да је и елемент $x_1 + x_2$ у том идеалу, па тиме и у J. Ако је $x \in J$ и $a \in A$, онда је $x \in I$, за неки идеал $I \in \mathcal{L}$, па је и $ax, xa \in I$ (јер је I идеал), па тиме и у J. Закључујемо да је J заиста идеал. Како је јасно да је $I \subseteq J$ за сваки идеал $I \in \mathcal{L}$ то је J једна мајоранта за $\mathcal{L}$. Према томе, сваки ланац у $\mathcal{I}$ има мајоранту, па по Цорновој леми добијамо да $\mathcal{I}$ има максимални елемент. Но, јасно је да је максимални елемент у $\mathcal{I}$ заправо максимални идеал у A чиме је доказ завршен. $\square$

У претходна два примера примене Аксиоме избора видели смо како се користе њена два еквивалента. У следећем примеру видећемо како директно коришћење Аксиоме избора доводи до једне занимљиве последице. Овај пример се обично наводи у књигама које се баве теоријом мере, али ми га овде наводимо ради илустрације примене Аксиоме избора. Рецимо пре свега, да је идеја да се појмови дужине, површине, запремине прошире на произвољне подскупове на правој, равни, простору веома природна. Но, видећемо да такав покушај не може успети чак ни на правој. Наравно, пре свега морамо увести одговарајући појам мере (која генералише дужину интервала). Дакле, мера ће за нас бити функција μ која подскуповима реалне праве додељује ненегативне реалне бројеве (укључујући и ∞) и која испуњава следећа својства:

- $A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$;

- За све реалне бројеве a, b такве да је $a < b$ важи: $\mu([a,b]) = \mu((a,b)) = b - a$;

- μ је $\sigma-$адитивна, тј. за дисјунктне скупове $X_n, n \in \mathbb{N}$ важи:
$$\mu(\bigcup_{n\in\mathbb{N}} X_n) = \sum_{n\in\mathbb{N}} \mu(X_n);$$

- Мера μ је транслаторно инваријантна, тј. за сваки $r \in \mathbb{R}$ важи: $\mu(A + r) = \mu(A)$, при чему је $A + r = \{x + r : x \in A\}$.

Ми овде нећемо дискутовати како се таква једна функција може дефинисати, али ћемо се позабавити питањем да ли уопште постоји функција μ са тим својствима, а која је дефинисана на целом $\mathcal{P}(\mathbb{R})$. За скуп A кажемо да је *мерљив*, ако постоји $\mu(A)$. Следећи став даје негативан одговор на горе постављено питање.

Став 3.30 Постоји ограничен подскуп у $\mathbb{R}$ који није мерљив.

Доказ. Ово заправо није тешко ни доказати. Дефинишимо најпре релацију $\sim$ на одсечку $[0, 1]$ са
$$x \sim y \overset{\text{def}}{\iff} x - y \in \mathbb{Q}.$$
Јасно је да је тако дефинисана једна релација еквиваленције. Ако са $\mathcal{C}$ означимо скуп свих класа еквиваленције, онда по Аксиоми избора, постоји скуп S такав да је $S \cap C$ једночлан, за сваки $C \in \mathcal{C}$.

Скупови $S_r = S + r$, где је r рационалан број из одсечка $[-1, 1]$ су дисјунктни. Наиме, ако је $S_r \cap S_s \neq \emptyset$, за $r \neq s$, тада постоје бројеви x, y из S за које је $x+r = y+s$. Но, из ове једнакости следи $x-y = s-r \in \mathbb{Q}$, тј. $x \sim y$ што није могуће према избору скупа S ($x \neq y$, јер $r \neq s$). Посматрајмо скуп $\mathbb{S}$ дефинисан са
$$\mathbb{S} = \bigcup_{r\in[-1,1]\cap\mathbb{Q}} S_r.$$
Према претходном важи
$$[0, 1] \subseteq \mathbb{S} \subseteq [-1, 2]$$

(проверите зашто је ово тачно). Тврдимо да скуп S није мерљив. У супротном, претпоставимо да је $\mu(S) = m$. Постоје две могућности: или је m једнак нули, или не. Ако је различит од нуле, онда из чињенице да је $\mathbb{S} \subseteq [-1, 2]$, $\sigma-$адитивности и осталих својстава мере добијамо да је $\infty \leq 3$. Слично, претпоставка да је $m = 0$ даје $1 = \mu([0, 1]) \leq \sum_{r \in [-1,2] \cap \mathbb{Q}} 0 = 0$. Закључујемо да скуп S не може бити мерљив. □

3.5 Кардинали

Кардиналност неког скупа представља проширење појма „број елемената у скупу" на случај бесконачних скупова. Раније смо се бавили тим појмом недовољно га прецизирајући, а сада ћемо тај појам заиста и увести следећом дефиницијом.

Дефиниција 3.31 *Кардиналност* скупа X је најмањи ординал κ за који постоји бијекција $f\colon \kappa \to X$. Уколико је κ кардиналност скупа X, користимо ознаку $|X| = \kappa$. *Кардинални број*, или кратко *кардинал*, је ординал κ, такав да не постоји ординал $\alpha < \kappa$ такав да постоји бијекција између κ и α.

Из ове дефиниције може се лако проверити да је кардиналност сваког скупа кардинал и да за сваки кардинал κ важи: $|\kappa| = \kappa$. Дакле, кардинали су посебни ординали по овој дефиницији. Јасно је да нису сви ординали и кардинали. На пример, $\omega < \omega + 1$ и како постоји бијекција између ω и $\omega + 1$ (конструишите је!) можемо закључити да $\omega + 1$ није кардинал. Следећа теорема додатно појашњава који су ординали уједно и кардинали.

Теорема 3.32 (а) Сваки коначни ординал је кардинал.
(б) ω је кардинал.
(в) Сваки бесконачни кардинал је гранични ординал.

Доказ. Како су прва два дела већ раније обрађена , то нам преостаје само да докажемо последњи део.

У ту сврху, довољно је показати да ординал облика $\alpha + 1$, где је $\alpha \geq \omega$ није кардинал. Заправо ћемо показати да постоји бијекција $f\colon \alpha \to \alpha + 1$. Бијекцију f и није тешко конструисати. Она је одређена са

$$
\begin{aligned}
f(0) &= \alpha; \\
f(n+1) &= n, \text{ за } n \in \omega; \\
f(\gamma) &= \gamma, \text{ за } \omega \leq \gamma < \alpha.
\end{aligned}
$$

□

Докажимо сада следећи став који оправдава терминологију коју смо раније користили.

Став 3.33 Нека су X и Y скупови. Тада је $|X| \leq |Y|$ акко постоји „1–1“ функција $f\colon X \to Y$.

Доказ. Уведимо ознаке $|X| = \kappa$ и $|Y| = \lambda$. Јасно је да $\kappa \leq \lambda$ имплицира постојање тражене „1–1“ функције. Концентришимо се на други смер. По претпоставци, постоје бијекције $i : \kappa \to X$ и $j : \lambda \to Y$. Нека је $g = j^{-1} \circ f \circ i$ и $U = g[\kappa]$. Како је $U \subseteq \lambda$, а λ је ординал, то је скуп U добро уређен и постоји јединствени ординал γ који је изоморфан добро уређеном скупу U. По дефиницији кардиналности скупа, мора бити $|U| \leq \gamma$. Но, како постоји „1–1“ функција из γ у λ, то мора бити $\gamma \leq \lambda$. Сада, узевши све у обзир добијамо

$$\kappa = |\kappa| = |U| \leq \gamma \leq \lambda,$$

што се и тражило. □

Позабавимо се кардиналном аритметиком. Дефинишимо најпре збир, производ и степен кардинала.

Дефиниција 3.34 Нека су κ и λ кардинали.

1. $\kappa + \lambda \stackrel{\text{def}}{=} |(\kappa \times \{0\}) \cup (\lambda \times \{0\})|$;
2. $\kappa \cdot \lambda \stackrel{\text{def}}{=} |\kappa \times \lambda|$;
3. $\kappa^\lambda \stackrel{\text{def}}{=} |\{f | f\colon \lambda \to \kappa\}|$.

Јасно је да уместо скупова κ и λ у претходној дефиницији можемо користити са десне стране и произвољне скупове X и Y одговарајуће кардиналности. Како смо раније показали $|\mathcal{P}(X)| = |\{f | f\colon X \to 2\}|$. Према горњој дефиницији закључујемо да је $|\mathcal{P}(X)| = 2^{|X|}$. Приметимо да се овако уведене операције не поклапају са операцијама које смо увели на ординалима и зато је потребно истицати да ли радимо само са кардиналима, или са ординалима. Операције се поклапају у случају коначних ординала. Наведимо основна својства овако уведених операција у облику става који се врло једноставно доказује и чији ћемо доказ изоставити.

Став 3.35 Нека су κ, λ и μ произвољни кардинали. Тада:

1. $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$;
2. $\kappa + \lambda = \lambda + \kappa$;
3. $(\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$;
4. $\kappa \cdot \lambda = \lambda \cdot \kappa$;
5. $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$;
6. $\kappa^\lambda \cdot \kappa^\mu = \kappa^{\lambda+\mu}$;

7. $\kappa^\lambda \cdot \mu^\lambda = (\kappa \cdot \mu)^\lambda$;

8. $(\kappa^\lambda)^\mu = \kappa^{\lambda\cdot\mu}$.

На својства из претходног става већ смо се навикли у раду са бројевима и за сада ништа необично нисмо добили. Следећа теорема представља главни резултат овог одељка. Но пре њене формулације, наведимо ознаку коју ћемо користити за ознаку кардиналности пребројивог скупа: $\aleph_0$ (чита се „алеф нула“). Дакле, ако желимо да истакнемо да је неки кардинал κ бесконачан, то записујемо овако: $\kappa \geq \aleph_0$. Приметимо да заправо имамо три ознаке за скуп природних бројева: $\mathbb{N}$, ω и $\aleph_0$. Зависи од контекста коју ћемо ознаку користити.

Теорема 3.36 Ако је $\kappa \geq \aleph_0$, онда је $\kappa \cdot \kappa = \kappa$.

Доказ. Нека је скуп A кардиналности κ, тј. $|A| = \kappa$. Како је јасно да је $\kappa \leq \kappa \cdot \kappa$, то је довољно доказати да је $\kappa \cdot \kappa \leq \kappa$, односно да постоји „1–1“ функција $f\colon A \times A \to A$. Доказ те чињенице изводимо користећи Цорнову лему.

Нека је скуп Φ задат са:

$$\Phi = \{(B, \phi_B) : B \subseteq A, |B| \geq \aleph_0, \phi_B : B \times B \to B \text{ је „1–1“}\}.$$

Скуп Φ није празан, јер смо већ доказали да је $\aleph_0 \cdot \aleph_0 = \aleph_0$. На њему можемо задати релацију поретка са

$$(B, \phi_B) \prec (B', \phi_{B'}) \overset{\text{def}}{\Longleftrightarrow} B \subset B' \text{ и } \phi_B \text{ је рестрикција од } \phi_{B'}.$$

Јасно је да ова релација јесте једна релација поретка и тако је $(\Phi, \prec)$ један посет. Нека је $\mathcal{L}$ непразан ланац у том посету (јасно је како наћи мајоранту празног ланца — узмимо било који елемент из нашег посета). Нека је

$$C = \bigcup_{(B,\phi_B)\in\mathcal{L}} B.$$

Функцију $\phi_C : C \times C \to C$ задајемо на следећи начин.

$$\phi_C(c', c'') = \phi_B(c', c''), \text{ ако } c', c'' \in B.$$

Поставља се питање добре дефинисаности функције ϕ_C. Нека су c' и c'' произвољни елементи из C. По дефиницији скупа C закључујемо да постоје скупови B' и B'' такви да $c' \in B'$, $c'' \in B''$ и $(B', \phi_{B'}), (B'', \phi_{B''}) \in \mathcal{L}$, за неке функције $\phi_{B'}$ и $\phi_{B''}$. Како су $(B', \phi_{B'}), (B'', \phi_{B''})$ елементи једног ланца, то су они упоредиви, а по дефиницији релације поретка, то значи да је један од њих подскуп другог и да је одговарајућа функција рестрикција оне друге. Дакле, заиста постоји елемент (B, ϕ_B) ланца $\mathcal{L}$ такав да $c', c'' \in B$. Ако постоји и неки други елемент (B_1, ϕ_{B_1})

тог ланца, такав да $c', c'' \in B_1$ то је $\phi_B(c', c'') = \phi_{B_1}(c', c'')$, јер су ти елементи упоредиви. Закључујемо да је функција ϕ_C заиста добро дефинисана. Није тешко проверити да $(C, \phi_C) \in \Phi$ и да је $(B, \phi_B) \preceq (C, \phi_C)$ за све (B, ϕ_B) из $\mathcal{L}$.

Показали смо да у посету $(\Phi, \prec)$ сваки ланац има мајоранту. По Цорновој леми закључујемо да у том посету постоји максимални елемент, означимо га са (B_0, ϕ_{B_0}). Постоје две могућности: или је $|B_0| = \kappa$, или је $|B_0| < \kappa$. Уколико је испуњена прва могућност онда је доказ теореме завршен, јер је $\phi_{B_0} : B_0 \times B_0 \to B_0$ „1–1“, па добијамо да је $\kappa \cdot \kappa \leq \kappa$. Претпоставимо стога да је $|B_0| = \lambda < \kappa$. Како је функција ϕ_{B_0} „1–1“, то њено постојање показује да је $\lambda \cdot \lambda = \lambda$. Тада за сваки природан број $n > 0$ важи

$$\lambda \leq n \cdot \lambda \leq \lambda \cdot \lambda = \lambda,$$

па закључујемо да је за све $n > 0$ тачно $n \cdot \lambda = \lambda$. Посебно, $2 \cdot \lambda = \lambda < |A|$, па закључујемо да постоји скуп B_1 кардиналности λ такав да је $B_1 \cap B_0 = \emptyset$ и да је $B_0 \cup B_1 \subset A$ (зашто?). Конструисаћемо „1–1“ функцију $\phi : (B_0 \cup B_1) \times (B_0 \cup B_1) \to (B_0 \cup B_1)$. Пре свега

$$(B_0 \cup B_1) \times (B_0 \cup B_1) = (B_0 \times B_0) \cup (B_0 \times B_1) \cup (B_1 \times B_0) \cup (B_1 \times B_1).$$

Сви скупови у наведеној унији су дисјунктни те је

$$\begin{aligned} |(B_0 \times B_1) \cup (B_1 \times B_0) \cup (B_1 \times B_1)| &= \lambda \cdot \lambda + \lambda \cdot \lambda + \lambda \cdot \lambda \\ &= \lambda + \lambda + \lambda \\ &= 3 \cdot \lambda \\ &= \lambda \\ &= |B_1|. \end{aligned}$$

Дакле, постоји бијекција $g \colon (B_0 \times B_1) \cup (B_1 \times B_0) \cup (B_1 \times B_1) \to B_1$. Функцију ϕ дефинишемо са

$$\phi(x, y) = \begin{cases} \phi_0(x, y), & (x, y) \in B_0 \times B_0 \\ g(x, y), & \text{иначе.} \end{cases}$$

Но, постојање функције ϕ противречи максималности елемента (B_0, ϕ_{B_0}). Закључујемо да се друга могућност и не појављује и тиме је доказ теореме завршен. $\square$

Наведимо неколико последица ове теореме.

Последица 3.37 Нека је $1 \leq \kappa \leq \lambda$ и $\lambda \geq \aleph_0$. Тада:

$$\kappa + \lambda = \kappa \cdot \lambda = \lambda.$$

Доказ. $\lambda \leq \kappa + \lambda \leq \lambda + \lambda = \lambda$; $\lambda \leq \kappa \cdot \lambda \leq \lambda \cdot \lambda = \lambda$. $\square$

Последица 3.38 Нека је κ бесконачни кардинал. Ако са κ^+ означимо најмањи кардинал већи од κ тада је

$$\kappa^+ = |\{\alpha \in \kappa^+ : \kappa \leq \alpha\}|.$$

Доказ.

$$\begin{aligned}
\kappa^+ &= |\kappa^+| \\
&= |\{\alpha \in \kappa^+ : \alpha < \kappa^+\}| \\
&= |\{\alpha \in \kappa^+ : \alpha < \kappa\}| + |\{\alpha \in \kappa^+ : \kappa \leq \alpha\}| \\
&= |\kappa| + |\{\alpha \in \kappa^+ : \kappa \leq \alpha\}| \\
&= \kappa + |\{\alpha \in \kappa^+ : \kappa \leq \alpha\}|
\end{aligned}$$

Како је $\kappa < \kappa^+$, закључујемо $|\{\alpha \in \kappa^+ : \kappa \leq \alpha\}| = \kappa^+$. □

Последица 3.39 Нека је $\kappa \geq \aleph_0$, $\lambda \leq \kappa$, $|I| \leq \lambda$ и $|A_i| \leq \kappa$ за све $i \in I$. Тада $|\bigcup_{i \in I} A_i| \leq \kappa$.

Доказ. $|\bigcup_{i \in I} A_i| \leq |I| \cdot \kappa \leq \lambda \cdot \kappa = \kappa$. □

Последица 3.40 Нека је X бесконачни скуп кардиналности κ. Доказати да је скуп свих његових коначних подскупова, у ознаци $\mathcal{P}_{\mathrm{fin}}(X)$, такође кардиналности κ.

Доказ. Приметимо да је за све $n \in \mathbb{N}$, $n > 0$, $|X^n| = \kappa$ (користити индукцију). Узимајући за скупове A_n из претходне последице баш скупове X^n, добијамо да је $|\bigcup_{n \in (\mathbb{N} \setminus \{0\})} X^n| \leq \kappa$. Како постоји функција $f \colon \bigcup_{n \in (\mathbb{N} \setminus \{0\})} X^n \to \mathcal{P}_{\mathrm{fin}}(X)$ која је „на“ то је тражени резултат доказан (додатно образложити!). □

Последица 3.41 Нека је $2 \leq \kappa \leq \lambda$ и $\lambda \geq \aleph_0$. Тада је $\kappa^\lambda = 2^\lambda$.

Доказ. Нека су скупови X и Y такви да је $|X| = \lambda$ и $|Y| = \kappa$. Тада је

$$\kappa^\lambda = |\{f | f \colon X \to Y\}|.$$

Но, ако $f \colon X \to Y$, онда је $f \subseteq X \times Y$, тј. $f \in \mathcal{P}(X \times Y)$. Према томе, $\{f | f \colon X \to Y\} \subseteq \mathcal{P}(X \times Y)$, па је

$$\kappa^\lambda \leq 2^{|X \times Y|} = 2^{|X| \cdot |Y|} = 2^{\kappa \cdot \lambda} = 2^\lambda.$$

Како је $\kappa \geq 2$, то је $\kappa^\lambda \geq 2^\lambda$ и доказ је завршен. □

Раније смо доказали да је $|2^{\mathbb{N}}| = |\mathbb{R}|$. За кардиналност скупа реалних бројева користи се посебна ознака $|\mathbb{R}| = \mathfrak{c}$ и $\mathfrak{c}$ се назива кардиналност континуума. С тим у вези је и позната *континуум хипотеза.* Пре него што је наведемо уведимо следеће ознаке. За сваки ординал α дефинише се кардинал $\aleph_\alpha$ на следећи начин.

- $\aleph_0 = \omega$;
- $\aleph_{\alpha+1} = \aleph_\alpha^+$;
- $\aleph_\lambda = \bigcup_{\alpha < \lambda} \aleph_\alpha$ за гранични ординал λ.

Са првом ознаком смо се већ раније упознали. Видимо да кардинале на овај начин можемо индексирати ординалима. Како је за сваки кардинал κ, $2^\kappa > \kappa$, то добијамо да је за сваки ординал α тачно: $2^{\aleph_\alpha} \geq \aleph_{\alpha+1}$. Можемо се запитати: за које ординале α овде важи једнакост? Континуум хипотеза (CH) није ништа друго до претпоставка: $2^{\aleph_0} = \aleph_1$ (уколико једнакост претпоставимо за све α онда се ради о генералисаној континуум хипотези (GCH)). Како знамо да је $2^{\aleph_0} = \mathfrak{c}$, то се континуум хипотеза може преформулисати и овако: „Да ли постоји непребројив подскуп скупа $\mathbb{R}$, који није кардиналности $\mathfrak{c}$?“ Тридесетих година прошлог века Курт Гедел[3] је показао да се ова хипотеза не може опорвгнути коришћењем осталих аксиома теорије скупова (укључујући и Аксиому избора), док је 1963. године Пол Коен[4] доказао да се она не може ни доказати уз помоћ тих аксиома. Дакле, остале аксиоме нам ништа не могу рећи о континуум хипотези.

Наведимо још два примера за крај овог одељка.

Пример 3.42 Нађи све кардинале κ и λ за које је $\kappa \cdot \lambda^2 = 9^\lambda$.

Приметимо пре свега да ниједан од ових кардинала не може бити једнак 0. Разликујемо четири случаја.
1. $\kappa, \lambda < \aleph_0$: У том случају су κ и λ природни бројеви већи од нуле и означаваћемо их са m и n респективно. Наша једначина у том запису изгледа овако

$$m \cdot n^2 = 9^n.$$

Како је $9 = 3^2$ то добијамо да је $m \cdot n^2 = 3^{2n}$. Према теореми о јединствености приказа природних бројева у облику производа простих (коју у овој књизи нисмо доказивали, али је читаоцима свакако позната) и из чињенице да је 3 прост број, закључујемо да и m и n морају бити степени броја 3, тј. $m = 3^s$ и $n = 3^t$ за неке природне бројеве s и t. Једначина постаје

$$3^s \cdot 3^{2t} = 3^{2\cdot 3^t}.$$

Добијамо да је $s + 2t = 2 \cdot 3^t$. Како је $2 \cdot 3^t > 2 \cdot 2^t > 2 \cdot t$ за све $t \in \mathbb{N}$, то закључујемо да се за t може узети произвољан природни број и тада је $s = 2 \cdot 3^t - 2t$. Дакле, решење је у овом случају дато са:

$$\boxed{(\kappa, \lambda) = (3^{2\cdot 3^t - 2t}, 3^t),\ t \in \mathbb{N}}$$

2. $\kappa \geq \aleph_0, \lambda < \aleph_0$: У овом случају са десне стране једнакости добијамо коначни кардинал, док са леве добијамо бесконачни, па закључујемо да решења у овом случају нема.
3. $\kappa < \aleph_0, \lambda \geq \aleph_0$: Добијамо $\lambda = 2^\lambda$ (зашто?), а та једнакост није испуњена ни за један кардинал λ.
4. $\kappa \geq \aleph_0, \lambda \geq \aleph_0$: Добијамо $\max\{\kappa, \lambda\} = 2^\lambda$ одакле закључујемо да λ може бити произвољан бесконачни кардинал, а за κ узимамо 2^λ:

[3] Kurt Gödel (1906–1978), аустријски (и амерички) математичар.
[4] Paul Joseph Cohen, амерички математичар (р. 1934), добитник Филдсове медаље (1966).

$$\boxed{(\kappa,\lambda)=(2^\lambda,\lambda),\ \lambda\geq\aleph_0}$$

Пример 3.43 (Уз CH) Наћи све кардинале κ, λ и μ за које је $\kappa^\lambda+\mu=\mathfrak{c}$.

Из наведених услова добијамо да је $\kappa^\lambda\leq\mathfrak{c}$ и $\mu\leq\mathfrak{c}$.
1. $\mu=\mathfrak{c}$: У овом случају задатак се своди на налажење кардинала κ и λ за које је $\kappa^\lambda\leq\mathfrak{c}$. То се дешава уколико је $\kappa\leq\mathfrak{c}$ и $\lambda\leq\aleph_0$ — подсетимо се да смо раније доказали да је $\mathfrak{c}^{\aleph_0}=\mathfrak{c}$ (када смо то доказали?).
2. $\mu<\mathfrak{c}$: Потребно је наћи кардинале κ и λ за које важи: $\kappa^\lambda=\mathfrak{c}$. Јасно је да мора важити: $\kappa\geq 2$. Ако је $2\leq\kappa\leq\aleph_0$, онда је $\lambda=\aleph_0$, а ако је $\kappa>\aleph_0$, онда мора бити $\kappa=\mathfrak{c}$ и $1\leq\lambda\leq\aleph_0$.

Следећи пример је заправо теорема пољског математичара Мазуркиевича[5] из 1914. године.

Пример 3.44 Постоји подскуп S равни $\mathbb{R}^2$ такав да свака права те равни има тачно две тачке из скупа S.

Доказ. Означимо са $\mathcal{L}$ скуп свих правих у равни. Знамо да је $|\mathcal{L}|=\mathfrak{c}$. Стога можемо овај скуп записати у облику $\mathcal{L}=\{l_\alpha:\alpha<\mathfrak{c}\}$. Формирамо скупове S_α за $\alpha\leq\mathfrak{c}$ на следећи начин. Нека су A_0 и B_0 било које две различите тачке на правој l_0. За S_0 узимамо $S_0=\{A_0,B_0\}$. Посматрамо праву l_1. Права l_0 сече праву l_1 највише у једној тачки. Ако је то нека од тачака A_0 или B_0 онда за S_1 узимамо скуп $S_1=S_0\cup\{C_1\}$, где је C_1 било која тачка праве l_1 која није на правој l_0, а ако у пресеку ових правих нема тачака из скупа S_0 (можда је пресек и празан скуп), онда за S_1 узимамо $S_1=S_0\cup\{C_1,D_1\}$ где су C_1 и D_1 било које две различите тачке са праве l_1, које нису на правој l_0. Сада би идеја доказа требало да буде јасна. Претпоставимо да је скуп S_α, за ординал $\alpha<\mathfrak{c}$, задат тако да за све $\gamma\leq\alpha$ права l_γ има тачно две тачке из S_α, да у S_α не постоје три неколинеарне тачке и да је $|S_\alpha|\leq|\alpha|$ у случају бесконачног ординала α. Скуп L_α, свих правих одређених тачкама из S_α, такође је кардиналности мање од $\mathfrak{c}$. Разматрамо праву $l_{\alpha+1}$. Како се две различите праве секу највише у једној тачки, то је

$$|((\cup_{\beta\leq\alpha}l_\alpha)\cup(\cup_{l\in L_\alpha}l))\cap l_{\alpha+1}|\leq|\alpha|<\mathfrak{c}=|l_{\alpha+1}|,$$

то на правој $l_{\alpha+1}$ имамо „довољно“ тачака за додавање. Скуп $S_{\alpha+1}$ задајемо на следећи начин. Ако се у пресеку $l_{\alpha+1}$ и горе наведене уније правих налазе две тачке скупа S_α (према конструкцији не може их бити више од две), онда је $S_{\alpha+1}=S_\alpha$. Ако је само једна, онда са праве $l_{\alpha+1}$ изаберимо неку тачку $A_{\alpha+1}$ различиту од те и тада је $S_{\alpha+1}=S_\alpha\cup\{A_{\alpha+1}\}$. Најзад, у случају да на $l_{\alpha+1}$ нема тачака из S_α, узмимо било које две различите тачке $A_{\alpha+1}$ и $B_{\alpha+1}$ са праве $l_{\alpha+1}$ и тада је $S_{\alpha+1}=S_\alpha\cup\{A_{\alpha+1},B_{\alpha+1}\}$. Из конструкције је јасно да у скупу $S_{\alpha+1}$ не постоје три неколинеарне тачке и да за све $\gamma\leq\alpha+1$, права l_γ

[5] Stefan Mazurkiewicz (1888–1945), пољски математичар.

садржи тачно две тачке из скупа $S_{\alpha+1}$ У случају граничног ординала λ за S_λ узимамо, као што се и очекује, $S_\lambda = \cup_{\gamma<\lambda} S_\gamma$. Тражени скуп је $S_\mathfrak{c}$ (подсетимо се да је $\mathfrak{c}$ као кардинал заправо гранични ординал). $\square$

Препоручујемо да читалац за вежбу покуша да докаже да постоји скуп тачака у равни такав да свака кружница у равни има тачно три тачке из тог скупа.

Теорема 3.45 Простор $\mathbb{R}^3$ је унија дисјунктних кружница полупречника 1.

Доказ. Наравно, под кружницом подразумевамо најобичнију кружницу у некој равни.

Нека је $\mathbb{R}^3 = \{p_\alpha : \alpha < \mathfrak{c}\}$. За $\alpha \leq \mathfrak{c}$ формирамо скупове C_α чији су елементи кружнице полупречника 1, које су дисјунктне тако да за свако $\alpha < \mathfrak{c}$ важи:

$$\{p_\gamma : \gamma \leq \alpha\} \subseteq \cup C_\alpha,$$

тј. свака тачка p_γ за $\gamma \leq \alpha$ садржана је у некој кружници из C_α. Осим тога захтевамо да је $|C_\alpha| \leq |\alpha|$, у случају бесконачног ординала α.

Нека је k_0 било која кружница, која садржи p_0. За C_0 узимамо $C_0 = \{k_0\}$. Претпоставимо да је C_α изабран и уочимо тачку $p_{\alpha+1}$. Уколико p_α „лежи“ на некој кружници из C_α узимамо да је $C_{\alpha+1} = C_\alpha$. У супротном, уочимо раван π која садржи тачку $p_{\alpha+1}$ и не садржи ниједну од кружница из C_α. Ово је могуће извести пошто је кардиналност скупа C_α мања од $\mathfrak{c}$, а $\mathfrak{c}$ је наравно кардиналност скупа свих равни које садрже дату тачку. У равни π скуп свих кружица полупречника 1 је кардиналности $\mathfrak{c}$. С друге стране, како π не садржи ниједну кружницу из C_α, то у π има највише $2 \cdot |\alpha|$ тачака које се налазе у унији кружица из C_α.

Наш задатак се своди на следеће: у равни је дата тачка p и скуп тачака S такав да је $|S| < \mathfrak{c}$. Наћи кружницу која је полупречика 1, која садржи p и која не сече скуп S. Посматрајмо скуп свих кружница које садрже тачку p и које су полупречника 1. Како кроз две дате тачке у равни пролазе тачно две кружнице (из те равни) полупречника 1, то се тачка из скупа S може налазити на највише две такве кружнице. Дакле, потребно нам је више од $2 \cdot |S|$ кружница, а $2 \cdot |S| < \mathfrak{c}$, те их имамо довољно, тј. сигурно постоји кружница k полупречника 1, која садржи тачку p и која нема тачака из S.

Сада за скуп $C_{\alpha+1}$ узимамо скуп $C_\alpha \cup \{k\}$, где је k кружница изабрано како је управо описано. У случају граничног ординала λ, узимамо $C_\lambda = \cup_{\alpha<\lambda} C_\alpha$. Јасно је да ћемо у овој конструкцији „покупити“ све тачке из $\mathbb{R}^3$, односно тражени скуп кружница је скуп $C_\mathfrak{c}$. $\square$

Читалац може за вежбу да покуша да докаже да је скуп $\mathbb{R}^3 \setminus \mathbb{Q}^3$ дисјунктна унија кружница, као и да $\mathbb{R}^2$ <u>није</u> дисјунктна унија кружница.

3.6 Задаци за вежбу

1. Доказати да постоји функција $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, таква да је $f(x+y) = f(x)+f(y)$ за све реалне бројеве x и y, а која *није* линеарна, тј. *није* облика $f(x) = ax$ за неко $a \in \mathbb{R}$.

2. Посматрајмо $\mathbb{R}$ као векторски простор над $\mathbb{Q}$. Доказати да је свака његова база кардиналности $\mathfrak{c}$.

3. Доказати да су Абелове групе $\mathbb{R}$ и $\mathbb{R} \oplus \mathbb{R}$ изоморфне.

4. За скуп M кажемо да је *транзитиван* ако за сваки скуп x важи: $x \in M \Rightarrow x \subset M$. Доказати да је дефиницији ординала наведеној у тексту еквивалентна следећа дефиниција: M је ординал **акко** је M транзитиван скуп који је линеарно уређен релацијом $\in$.

5. Доказати да је скуп M транзитиван **акко** $\bigcup(M \cup \{M\}) = M$.

6. Наћи подскуп скупа рационалних бројева који је (подразумевајући стандардни поредак на рационалним бројевима) изоморфан ординалу ω^3. Можете ли наћи подскуп изоморфан ординалу ω^ω?

7. Наћи пример ординала α, β и γ таквих да је $\alpha \neq \beta$ и $\alpha+\gamma = \beta+\gamma$.

8. Дати су ординали $\alpha > 1$ и β. Доказати да је $\alpha^\beta \geq \alpha \cdot \beta$.

9. Одредити све ординале α за које је $1 + \alpha = \alpha$.

10. Доказати $\alpha + \beta = \beta \Longleftrightarrow \alpha \cdot \omega \leq \beta$.

11. Нека је $\alpha > 1$. Наћи најмањи ординал β различит од 0 такав да је $\alpha \cdot \beta = \beta$.

12. Упоредити следеће ординале:

    (а) $2 \cdot (\omega + 1)$ и $(\omega + 1) \cdot 2$;

    (б) $\omega \cdot (\omega + 1)$ и $(\omega + 1) \cdot \omega$.

13. Решити следеће једначине:

    (а) $\omega + \alpha = \omega$;

    (б) $\alpha + \omega = \omega$;

    (в) $\alpha \cdot \omega = \omega$;

    (г) $\omega \cdot \alpha = \omega$;

    (д) $\alpha + \beta = \omega$;

    (ђ) $\alpha \cdot \beta = \omega$.

14. Решити једначину $\alpha + \beta = \omega^2 + 1$.

15. Ако су α и β ординали и $k \in \mathbb{N}$, при чему је $k > 0$, онда из једнакости $\alpha^k = \beta^k$ следи да је $\alpha = \beta$.

16. Нека је α произвољни ординал. Ако је за све ординале β испуњено: $\alpha + \beta = \beta + \alpha$, онда је $\alpha = 0$.

17. Ако $k, n \in \omega$, при чему је $k > 1$ и λ гранични ординал, доказати да је $(\lambda \cdot n)^k = \lambda^k \cdot n$.

18. Нека је $n \in \omega$ и α бесконачни ординал. Тада је $(\alpha+n)\cdot\beta = \alpha\cdot\beta+n$ уколико је β следбеник, а $(\alpha + n) \cdot \beta = \alpha \cdot \beta$ уколико је β гранични ординал или 0.

19. За дати ординал $\alpha > 0$, одредити све природне бројеве n такве да је $\alpha = n \cdot \beta$, за неки ординал β.

20. Доказати да за сваки ординал α постоји само коначно много ординала γ таквих да је $\alpha = \beta + \gamma$ за неки ординал β.

21. Доказати да за сваки ординал $\alpha \neq 0$ постоји само коначно много ординала γ таквих да је $\alpha = \beta \cdot \gamma$ за неки ординал β.

22. Показати да једначина $\alpha^2 + \omega = \beta^2$ нема решења.

23. Одредити бесконачно много решења једначине $\alpha^2+\omega^2 = \beta^2$ таквих да је α бесконачан ординал.

24. Наћи сва решења једначине $\alpha^2 \cdot 2 = \beta^2$.

25. Показати да за сваки природан број $k \geq 1$ постоји бесконачан низ ординала, који чине аритметички низ, при чему је сваки члан тог низа k-ти степен (неког ординала).

26. Посматрајмо $n+1$ ординала $1, 2, 2^2 \ldots, 2^{n-1}, \omega$. Показати да се њиховим сумирањем (користећи различите поретке при сумирању), може добити тачно 2^n различитих вредности.

27. За сваки природан број $n \geq 1$, наћи n ординала тако да су сви њихови производи (при свим могућим пермутацијама) различити.

28. Показати да за сваки непразан скуп ординала постоји највећи заједнички <u>леви</u> делилац.

29. Показати да је ординал α дељив са леве стране ординалима $\omega+2$ и $\omega + 3$ ако и само ако је дељив са леве стране ординалом ω^2.

30. Показати да је ординал α дељив са десне стране са 2 и 3 ако и само ако је дељив са десне стране са 6.

31. Показати да је ординал α дељив са десне стране са $\omega + 2$ и $\omega + 3$ ако и само ако је дељив са десне стране са $\omega + 6$.

32. Нека је $n > 1$. Доказати да је $n^{\omega^\omega} = \omega^{\omega^\omega}$.

33. Ако је $n \in \omega$, онда је $(\omega + n)^\omega = \omega^\omega$.

34. Доказати да за сваки ординал α и ординал $\gamma > 1$ важи: $\alpha \leq \gamma^\alpha$.

35. Доказати да за сваки гранични ординал λ важи: $1^\lambda + 2^\lambda = 3^\lambda$.

36. Доказати да су за сваки бесконачни ординал α, ординали α и 2^α исте кардиналности.

37. Доказати да се сваки ординал $\alpha \neq 0$ може на јединствен начин записати у облику

$$\alpha = 2^{\beta_0} + 2^{\beta_1} + \cdots + 2^{\beta_n}, \qquad \text{при чему је } \beta_0 > \beta_1 > \cdots > \beta_n.$$

38. Представити ординал $\omega^\omega + \omega^5 \cdot 3 + \omega^2 + 6$ у облику наведеном у претходном задатку.

39. Нека је ординал $\gamma \geq 2$. Доказати да се сваки ординал $\alpha \neq 0$ може на јединствен начин приказати у облику

$$\alpha = \gamma^{\xi_0} \cdot \eta_0 + \gamma^{\xi_1} \cdot \eta_1 + \cdots + \gamma^{\xi_n} \cdot \eta_n,$$

за неке ординале ξ_i, η_j, при чему је $\xi_0 > \xi_1 > \cdots > \xi_n$ и за све $j = \overline{1,n}$ важи: $1 \leq \eta_j < \gamma$.

40. Нека су α и γ произвољни ординали, при чему је $\gamma \neq 0$. Означимо са ${}^\alpha\gamma$ скуп свих функција $f\colon \alpha \to \gamma$ за које је $f(\beta) \neq 0$ само за коначно много $\beta \in \alpha$. На овом скупу уведимо релацију поретка $\preceq$ на следећи начин. Ако је $f \neq g$, онда је

$$f \prec g \ \textbf{акко}\ f(\xi) < g(\xi), \text{ где је } \xi = \max\{\beta \in \alpha : f(\beta) \neq g(\beta)\}.$$

Доказати да је скуп ${}^\alpha\gamma$, са овом релацијом уређења, један добро уређен скуп, који је изоморфан ординалу γ^α.

41. Под операцијом „замене основе c основом d“ подразумевамо следећу трансформацију: $a_k c^k + \cdots + a_1 c^1 + a_0 \mapsto a_k d^k + \cdots + a_1 d^1 + a_0$ где је за све $i \in \{0, \ldots, k\}$ $0 \leq a_i < c$ (запис природног броја у основи c „посматрамо“ као запис у основи d). Узмимо произвољан природан број, запишимо га, на пример, у декадном систему и затим вршимо следеће трансформације: одузмимо од њега 1 и заменимо основу 10 основом 11; поново одузмимо 1 и заменимо основу 11 основом 12, итд. Показати да се после коначно много корака мора добити 0, без обзира на то који природни број на почетку бирамо.

42. Замислимо следећу „финансијску игру“. На почетку имамо коначан број новчаница, које могу бити различите вредности (наравно, претпостављамо да има само коначно много различитих вредности новчаница!). Сваког дана обавезно одлазимо у мењачницу и мењамо једну новчаницу за *произвољан број* (коначан!) новчаница, али обавезно мањег апоена од ње. За новчаницу најмање могуће вредности не добијамо ниједну новчаницу. Доказати да ћемо после коначно много дана остати без иједне новчанице.

43. На листу хартије добили смо исписан низ нула и јединица (наравно да их има коначно много!). На том низу понављамо следећу трансформацију: било који пар 01 који се појављује у низу заменимо јединицом иза које следи произвољан, коначан број нула. Ако се пар 01 не појављује поступак се завршава. Да ли се поступак обавезно завршава после коначно много корака?

44. Ако су κ, λ и μ кардинали, доказати: $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

45. Навести пример кардиналног броја κ са особином: $\kappa^{\mathfrak{c}} = \kappa$.

46. Одредити све кардиналне бројеве $\kappa > 0$ такве да је $\mathfrak{c}^\kappa = 2^\kappa$.

47. Наћи све кардинале κ за које је $\kappa^{\kappa^\kappa} = 2^\kappa$.

48. Одредити све кардинале κ и λ за које је $\kappa^\lambda = \aleph_0$.

49. Нека је λ кардинал. Доказати: $2^\lambda \geq \aleph_0 \Rightarrow 2^\lambda \geq \mathfrak{c}$.

50. Одредити све кардинале κ и λ тако да важи: $\kappa \cdot \lambda = 2^\kappa + \aleph_0$.

51. Одредити све кардинале κ и λ за које је: $\kappa^2\lambda^2 = \kappa^3 + \lambda^2$.

52. Одредити све кардинале κ и λ за које важи: $\kappa \cdot \lambda^2 = 7^\lambda$.

53. Одредити све кардинале κ, λ за које је $7^\kappa\lambda^7 = \kappa^3\lambda^2$.

54. Одредити све кардинале κ и λ такве да је: $11^\kappa\kappa^2 = \kappa^9\lambda^5$.

55. Одредити све кардинале κ и λ за које је : $13^\kappa\lambda^3 = \kappa^3\lambda^8$.

56. Одредити све кардинале κ, λ за које је $\kappa^2\lambda + 3^\kappa = \lambda^3$.

57. Одредити све кардинале κ, λ за које је $3^\kappa\lambda = \lambda + 4\lambda^5$.

58. Одредити све кардинале κ, λ за које је $3^\kappa = \lambda^3\kappa + \kappa$.

59. Одредити све кардинале κ, λ за које је $5^{2\lambda} = \lambda\kappa + \kappa$.

60. Нека је
$$\prod_{i \in I} A_i = \bigsqcup_{i \in I} B_i.$$
Показати да за бар један индекс i важи $|B_i| \geq |A_i|$.

61. Уочимо кардинал $\alpha = \aleph_0 + 2^{\aleph_0} + 2^{2^{\aleph_0}} + \cdots$. Доказати:

    (а) Кардинал α је најмањи кардинал који је већи од кардиналности свих скупова: $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N})), \ldots$

    (б) За кардинал α важи: $\alpha^{\aleph_0} = 2^\alpha$.

62. Доказати Кенигову[6] неједнакост: ако су, за све $i \in I$ дати ординали κ_i и λ_i такви да је $\kappa_i < \lambda_i$, онда је
$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i.$$

63. Нека је A пребројив подскуп од $\mathbb{R}$. Испитати да ли постоји $x \in \mathbb{R}$ такав да је
$$\{x + a : a \in A\} \cap A = \emptyset.$$

64. Хауздорфов принцип максималности гласи: У сваком посету сваки ланац је садржан у неком максималном ланцу. Доказати да је Хауздорфов принцип максималности еквивалентан Цорновој леми.

65. Непразан скуп A је *коначног карактера* ако за њега важи следеће. За сваки скуп X: X је у A **акко** сваки коначан подскуп од X је у A. Доказати да су следећи скупови коначног карактера

    (а) $\mathcal{F} = \{Z \subseteq \mathcal{P}(A) : (\forall S, T \in Z)(S \neq T \Rightarrow S \cap T = \emptyset)\}$, где је A произвољан скуп.

    (б) $\mathcal{F} = \{f \subseteq A \times B : f$ је функција$\}$, где су A и B произвољни скупови.

    (ц) $\mathcal{F} = \{f \subseteq A \times B : f$ је „1–1“ функција$\}$, где су A и B произвољни скупови.

66. Тјукијева[7] лема је следеће тврђење: Сваки скуп коначног карактера садржи елемент који је максималан у односу на инклузију. Доказати:

    (а) Тјукијева лема је последица Цорнове леме.

    (б) Постојање изборне функције за фамилију непразних скупова је последица Тјукијеве леме.

    На овај начин показујемо да је и Тјукијева лема еквивалент Аксиоми избора.

67. Нека је $y = ax^2 + bx + c$ нека парабола. Доказати да она садржи бесконачно много тачака чије су обе координате ирационални бројеви.

[6] Julius König (1849–1913), мађарски математичар.
[7] John Wilder Tukey (1915–2000), амерички математичар.

68. Одредити кардиналност скупа свих тачака у равни које припадају кривој задатој једначином

$$x^3 + 3xy^2 - 4y^5 = 2,$$

а код којих је бар једна координата рационалан број.

69. Нека је $\mathbb{K}$ пребројив скуп кружница у равни. Доказати да је скуп тачака у равни које не припадају ниједној од кружница из $\mathbb{K}$ кардиналности $\mathfrak{c}$.

70. У равни је дат пребројив скуп правих Π. Одредити кардиналности скупа свих кружница које имају полупречник рационалне дужине и које не додирују ниједну праву из Π.

71. Нека $f\colon X \to Y$. Доказати да је f „на“ акко за сваки скуп Z и сваку функцију $h\colon Z \to Y$ постоји функција $g\colon Z \to X$ за коју је $h = f \circ g$.

72. За функцију $f\colon \mathbb{N} \to \mathbb{N}$ кажемо да је *мултипликативно периодична* ако

$$(\exists k \geq 2)(\forall m \in \mathbb{N})(f(km) = f(m)).$$

Одредити кардиналност скупа свих мултипликативно периодичних функција из $\mathbb{N}$ у $\mathbb{N}$.

73. Одредити кардиналност скупа свих бинарних релација на скупу $\mathcal{P}(\mathbb{R})$.

74. Одредити кардиналност скупа свих релација на скупу природних бројева.

75. Одредити кардиналност скупа свих релација еквиваленције на $\mathbb{N}$.

76. Одредити кардиналност скупа $\mathcal{F}$, где је

$$\mathcal{F} = \{f\colon \mathbb{N} \to \mathbb{N} \mid f \text{ је „на“}\}$$

77. Одредити кардиналност скупа $\mathcal{F}$, где је

$$\mathcal{F} = \{f\colon \mathbb{N} \to \mathbb{Z} \mid f \text{ је „1–1“}\}$$

78. Одредити кардиналност скупа $\mathcal{F}$, где је

$$\mathcal{F} = \{f\colon \mathbb{N} \to \mathbb{N} \mid f \text{ је бијекција}\}$$

79. Одредити кардиналност скупа свих нерастућих, бесконачних низова природних бројева.

80. Одредити кардиналност скупа свих аутоморфизама посета $(\mathbb{N} \setminus \{0\}, |)$.

81. На $\mathbb{R}$ је дефинисана релација еквиваленције $\sim$ са: $x \sim y$ **акко** $x - y$ је алгебарски број. Одредити кардиналност скупа $\mathbb{R}/_{\sim}$ (скупа свих класа еквиваленције).

82. На $\mathbb{R}$ је дефинисана релација еквиваленције $\sim$ са:

$$x \sim y \overset{\text{def}}{\iff} \sin x = \sin y.$$

Одредити кардиналност $\mathbb{R}/_{\sim}$.

83. Нека је $\mathcal{F} = \{f | f\colon \mathbf{R} \to \mathbf{R}\}$. Уведимо релацију $\sim$ на скупу $\mathcal{F}$ са

$$f \sim g \overset{\text{def}}{\iff} (\forall m \in \mathbf{N})(f(m) = g(m)).$$

Показати да је наведена релација једна релација еквиваленције и одредити кардиналност скупа $\mathcal{F}/_{\sim}$, свих класа еквиваленције.

84. Показати да је кардиналност скупа свих функција $f\colon [0,1] \to [0,1]$, које су прекидне бар у једној тачки, већа од $\mathfrak{c}$.

85. Одредити кардиналност скупа свих *највише пребројивих* подскупова од $\mathbb{R}$.

Глава 4

Решења задатака

4.1 Задаци из прве главе

1. Користићемо карактеристичне функције. Нека је $U = A \cup B \cup C$. Карактеристичну функцију рачунамо у односу на скуп U.

   (а) Израчунајмо најпре карактеристичну функцију скупа са леве стране.

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

   Карактеристична функција скупа са десне стране је

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

   Како су карактеристичне функције једнаке, то су и скупови једнаки.

   (б) Овај пут је карактеристична функција скупа о коме је реч једнака $\chi_A + \chi_B\chi_C + \chi_A\chi_B\chi_C$.

   (в) $\chi_{A\cap(A\cup B)} = \chi_A(\chi_A + \chi_B + \chi_A\chi_B) = \chi_A\chi_A + \chi_A\chi_B + \chi_A\chi_B = \chi_A$. Овде смо наравно користили својство $\chi_X\chi_X = \chi_X$.

   (г) Доказ се изводи као у претходном случају.

   (д) Наравно да се и овде доказ може извести коришћењем карактеристичних функција (изведите и тај доказ), но урадићемо то без њиховог коришћења. Са L, односно D означимо скуп који се налази са леве, односно са десне стране наведеног идентитета. Нека $x \in L$. Без губљења општости можемо претпоставити да $x \in B \cap C$. То значи да $x \in A \cup B$ (јер је у B), $x \in B \cup C$ (заправо је у оба скупа) и $x \in A \cup C$ (јер је у C). Закључујемо да $x \in D$. За доказ другог смера претпоставимо да $x \in D$ и нпр. $x \in A$. Уколико $x \notin B$, то из $x \in D$ закључујемо да $x \in C$, па $x \in A \cap C$. У супротном, тј. $x \in B$ добијамо да $x \in A \cap B$. У сваком случају $x \in L$. Слично се закључује и у осталим случајевима. Приметимо да овај идентитет не представља ништа друго до два различита описа подскупа од U који се састоји од оних елемената који леже у *бар* два од скупова A, B и C.

2. Не постоје. Претпоставимо супротно, тј. нека су A, B, C скупови са наведеним својствима. Нека је $x \in A \cap B$ произвољан елемент (по претпоставци је овај скуп непразан). Тада x мора бити у C, јер би у супротном припадао $(A \cap B) \setminus C$, а тај је скуп по претпоставци празан. Дакле, $x \in A \cap C$ што противречи претпоставци.

3. Користимо метод карактеристичних функција. Нека је $U = A \cup B \cup C$.

   (а) $\chi_{A \setminus (B \setminus C)} = \chi_{(A \setminus B) \setminus C}$ ако и само ако је $0 = \chi_{A \cap C}$ (проверити!), што је еквивалентно са $A \cap C = \emptyset$.

   (б) На сличан начин добијамо да је еквиваленција испуњена.

   (в) Карактеристичне функције два наведена подскупа су увек једнаке.

   (г) Поређењем карактеристичних функција добијамо да су скупови једнаки ако и само ако је $\chi_A = \chi_{A \cap C}$ што је еквивалентно са $A \subseteq C$.

   (д) Слично претходном случају.

   (ђ) Поређењем карактеристичних функција добијамо да тражена једнакост међу скуповима важи ако и само ако је $\chi_A \chi_C = 0$, тј. ако је $A \cap C = \emptyset$.

   (е) Добијамо да је наведена једнакост испуњена ако и само ако је $\chi_B + \chi_A \chi_C = 0$, што је еквивалентно са $\chi_B = \chi_{A \cap C}$, тј. $B = A \cap C$.

   (ж) Слично случају (ђ).

4. (а) Знамо да је $f[f^{-1}[B]] \subseteq B$ за сваки $B \subseteq Y$. Добијамо да је $f[f^{-1}[f[A]]] \subseteq f[A]$. Но, такође је и $f^{-1}[f[A]] \supseteq A$, па следи да је и $f[A] \subseteq f[f^{-1}[f[A]]]$, чиме је доказ завршен.

   (б) Као и у претходном, из чињенице да је $f^{-1}[f[A]] \supseteq A$ добијамо да је $f^{-1}[f[f^{-1}[B]]] \supseteq f^{-1}[B]$, док из $f[f^{-1}[B]] \subseteq B$ добијамо $f^{-1}[f[f^{-1}[B]]] \subseteq f^{-1}[B]$.

(в) Претпоставимо најпре да је функција f „1–1“. Познато нам је да је инклузија $f[A \cap B] \subseteq f[A] \cap f[B]$ испуњена за сваку функцију f и све подскупове A, B, те нам само преостаје да докажемо обратну инклузију. У ту сврху, нека је $y \in f[A] \cap f[B]$. По дефиницији директне слике скупа, закључујемо да постоје $x_1 \in A$ и $x_2 \in B$ такви да је $y = f(x_1) = f(x_2)$. Но, како је по претпоставци функција f „1–1“, то мора бити $x_1 = x_2 \in A \cap B$, па добијамо да $y \in f[A \cap B]$. Остаје да покажемо да из наведеног услова следи да је функција „1–1“. Претпоставимо да је $f(x_1) = f(x_2)$, за неке $x_1, x_2 \in X$. Посматрајмо скупове $A = \{x_1\}$ и $B = \{x_2\}$. Према услову је $f[A \cap B] = f[A] \cap f[B]$, и добијамо да је $f[A \cap B] = \{f(x_1)\}$. То значи да је скуп $A \cap B = \{x_1\} \cap \{x_2\}$ непразан, а то је могуће једино ако је $x_1 = x_2$.

(г) $\Longrightarrow$: Претпоставимо да је f „1–1“. Нека $y \in f[A \triangle B]$. Према томе $y = f(x)$, за неко $x \in A \triangle B = A \setminus B \cup B \setminus A$. Претпоставимо да $x \in A \setminus B$ (на исти начин резонујемо и у другом случају). То значи да $y \in f[A]$ ($x \in A \Rightarrow y = f(x) \in f[A]$) и $y \notin f[B]$. Наиме, уколико $y \in f[B]$, то је $y = f(x_1)$, за неко $x_1 \in B$, при чему је $x \neq x_1$, јер $x \notin B$. Но, тада добијамо да је $f(x) = f(x_1)$, при чему је $x \neq x_1$, што противречи претпоставци да је f „1–1“. Закључујемо да $y \in f[A] \setminus f[B]$, те $y \in f[A] \triangle f[B]$. Нека $y \in f[A] \triangle f[B]$, нпр. $y \in f[B] \setminus f[A]$. Тада је $y = f(x)$, за неко $x \in B$. Но, $x \notin A$, јер $y \notin f[A]$. Дакле, $y \in f[B \setminus A]$, те $y \in f[A \triangle B]$. Приметимо да нам у овом делу није била потребна претпоставка да је f „1–1“.

$\Longleftarrow$: Претпоставимо да је $f[A \triangle B] = f[A] \triangle f[B]$ за све $A, B \subseteq X$ и нека је $f(x_1) = f(x_2)$. Посматрајмо шта нам горња једнакост даје у случају да је $A = \{x_1\}$ и $B = \{x_2\}$. Тада је $f[A] \triangle f[B] = \{f(x_1\} \triangle \{f(x_2\} = \emptyset$, јер је $f(x_1) = f(x_2)$. Но, тада је и $f[\{x_1\} \triangle \{x_2\}] = \emptyset$, што је једино могуће у случају да је $\{x_1\} \triangle \{x_2\} = \emptyset$ из чега добијамо да је $x_1 = x_2$. Закључујемо да је функција f „1–1“.

(д) $\subseteq$: Нека $y \in f[A \cap f^{-1}[B]]$. То значи да је $y = f(x)$, за неко $x \in A \cap f^{-1}[B]$. Из чињенице да $x \in f^{-1}[B]$ добијамо да $y = f(x) \in B$, тј. $y \in f[A] \cap B$.

$\supseteq$: Нека $y \in f[A] \cap B$. Дакле, $y = f(x)$, за неко $x \in A$. Како $f(x) = y \in B$, то добијамо да $x \in f^{-1}[B]$, па $x \in A \cap f^{-1}[B]$ те $y \in f[A \cap f^{-1}[B]]$.

(ђ) Показаћемо контрапримером да идентитет не важи у општем случају. Нека је $X = \{0, 1\}$, $Y = \{0\}$ и $f(0) = f(1) = 0$. Ако је $A = \{0\}$, $B = \{0\}$, добијамо да је

$$f[A \triangle f^{-1}[B]] = f[\{0\} \triangle \{0, 1\}] = f[\{1\}] = \{0\},$$

док је $f[A] \triangle B = \{0\} \triangle \{0\} = \emptyset$.

(e) Исти контрапример и у овом случају показује да идентитет није увек испуњен.

5. $\Longrightarrow$: Претпоставимо да је $f: X \to Y$ „1–1“. Нека је a произвољни елемент из X. Тражену функцију $g: Y \to X$ дефинишемо са

$$g(y) = \begin{cases} x, & \text{ако је } y = f(x), \\ a, & \text{иначе.} \end{cases}$$

Како је функција f „1–1“, то је g добро дефинисана функција и $g(f(x)) = x$ за све $x \in X$, тј. $g \circ f = \mathrm{Id}_X$.

$\Longleftarrow$: Нека је $g \circ f = \mathrm{Id}_X$ и $f(x_1) = f(x_2)$. Тада је

$$x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2.$$

6. Функцију $g: \mathcal{P}(Y) \to \mathcal{P}(X)$ дефинишемо са: $g(A) = f^{-1}[A]$, за $A \subseteq X$. Обратите пажњу на ознаке! Нисмо написали да је $g = f^{-1}$. Поновите дефиницију инверзне слике скупа, ако вам ово није јасно. Није тешко доказати да је функција g заиста „1–1“. Ако је $g(A) = g(B)$, то значи да је $f^{-1}[A] = f^{-1}[B]$ из чега следи да је $f[f^{-1}[A]] = f[f^{-1}[B]]$. Но, функција f је „на “ по претпоставци, те добијамо да је $A = B$ (зашто?).

7. Јасно је да из $f = g$ следи да је $f^{-1}[g[A]] = f^{-1}[f[A]] \supseteq A$. Остаје да докажемо други смер. Нека је $x \in X$ произвољни елемент. Посматрајмо скуп $A = \{x\}$. По претпоставци је $\{x\} \subseteq f^{-1}[g[\{x\}]]$. Дакле, по дефиницији инверзне слике скупа, $f(x) \in g[\{x\}] = \{g(x)\}$, тј. $f(x) = g(x)$. Како је x био произвољни елемент, закључујемо да је за све $x \in X$ $f(x) = g(x)$ те је $f = g$ чиме смо доказали наведено тврђење.

8. Нека $f: X \to X$ и нека је $x \in X$ произвољан елемент. За подскуп A узмимо $A = \{x, f(x)\}$. Тада $f(x) \in f[A] \cap A$, те закључујемо да тражени скуп и функција не постоје.

9. (a) Користићемо карактеристичне функције. Посматрамо скуп $U = A \cup B \cup C \cup D$.

$$\begin{aligned} A \triangle B = C \triangle D \quad &\Rightarrow \quad \chi_{A \triangle B} = \chi_{C \triangle D} \\ &\Rightarrow \quad \chi_A + \chi_B = \chi_C + \chi_D \\ &\Rightarrow \quad \chi_A + \chi_B + \chi_B + \chi_C = \chi_C + \chi_D + \chi_B + \chi_C \\ &\Rightarrow \quad \chi_A + \chi_C = \chi_B + \chi_D. \end{aligned}$$

Овде смо користили чињеницу да је $\chi_X + \chi_X = 0$ за сваки $X \subseteq U$.

(б) $\Longrightarrow$: Нека $x \in A \setminus B$. Како је, по претпоставци, $A \subseteq B \cup C$, то $x \in B \cup C$, но, како $x \notin B$, закључујемо да $x \in C$.

$\Longleftarrow$: Нека $x \in A$. Постоје две могућности: $x \in B$, или $x \notin B$. У првом случају $x \in B \cup C$, што се и тражи, док у другом случају $x \in A \setminus B$, па по претпоставци следи да $x \in C$. У сваком случају добијамо да $x \in B \cup C$.

(в) Нека је $U = A \cup B \cup C$. Са X^c, где је $X \subseteq U$ означимо комплемент у односу на скуп U, тј. $X^c := U \setminus X$. Подсетимо се да тада важи $X \setminus Y = X \cap Y^c$.

$$\begin{aligned} A \setminus (B \setminus C) &= A \cap (B \cap C^c)^c \\ &= A \cap (B^c \cup C) \\ &= (A \cap B^c) \cup (A \cap C) \\ &= (A \setminus B) \cup (A \cap C). \end{aligned}$$

У горњем доказу смо користили раније позната својства комплемента, пресека и уније скупова.

(г) Нека $x \in (A_1 \cap \ldots \cap A_n) \triangle (B_1 \cap \ldots \cap B_n)$. То значи да x припада тачно једном од скупова $A_1 \cap \ldots \cap A_n$, односно $B_1 \cap \ldots \cap B_n$. Можемо, без губљења општости, претпоставити да $x \in A_1 \cap \ldots \cap A_n$ и $x \notin B_1 \cap \ldots \cap B_n$. Како $x \notin B_1 \cap \ldots \cap B_n$, то $x \notin B_i$, за неко $i \in \{1, \ldots, n\}$. Но, тада $x \in A_i \triangle B_i$ (x припада сваком од скупова A_k), па стога x припада и наведеној унији.

10. Претпоставка је да је $C \subseteq A$.

$\subseteq$: Нека $x \in (A \cap B) \triangle C$. Из те претпоставке закључујемо да постоје две могућности.

(а) x је и у A и у B, а није у C. Но, тада је x и у A и у $B \setminus C$, па тиме и у $A \cap (B \triangle C)$.

(б) x јесте у C, али није у пресеку $A \cap B$. Но, по претпоставци је $C \subseteq A$, па закључујемо да $x \notin B$. Но, све то значи да x јесте у A и у $C \setminus B$, па тиме и у $A \cap (B \triangle C)$.

$\supseteq$: Нека је x из скупа $A \cap (B \triangle C)$. То значи да је x сигурно у A. Остају две могућности.

(а) $x \in B \setminus C$. Тада је x у $(A \cap B) \setminus C$, па тиме и у $(A \cap B) \triangle C$.

(б) $x \in C \setminus B$. Но, у овом случају је x у C, а није у пресеку $A \cap B$, па видимо да се налази у $(A \cap B) \triangle C$.

11. Приметимо да је $\chi_{A \cap (B \triangle C)} = \chi_A \chi_B + \chi_A \chi_C$. Дакле, уколико је $A \cap (B \triangle C) = B$ добијамо да је $\chi_A \chi_B + \chi_B = \chi_A \chi_C$, тј. $B \setminus A = A \cap C$. Претпоставимо да овај скуп није празан и нека је x неки његов елемент. Тада добијамо да $x \in A$, јер $x \in A \cap C$, али и да $x \notin A$,

пошто $x \in B \setminus A$. Јасно је да то није могуће и добијамо да мора бити $B \setminus A = A \cap C = \emptyset$, тј. $B \subseteq A$ и $A \cap C = \emptyset$. Провера обратне импликације оставља се читаоцу као лака вежба.

12. Уколико систем једначина има решење то из прве једначине добијамо да је $B \subseteq A$, а из друге $A \subseteq C$. У даљем ћемо претпоставити да су ти услови испуњени. Користимо карактеристичне функције. Добијамо систем једначина

$$\begin{aligned} \chi_A \chi_X &= \chi_B \\ \chi_A + \chi_X + \chi_A \chi_X &= \chi_C \end{aligned}$$

Коришћењем прве једначине, добијамо да је

$$\chi_A + \chi_X + \chi_B = \chi_C$$

односно

$$\chi_X = \chi_A + \chi_B + \chi_C.$$

Закључујемо да је $X = A \triangle B \triangle C$. Када ништа више не бисмо знали о скуповима A, B и C могли бисмо решење да оставимо и у овом облику, међутим ми знамо да је $B \subseteq A \subseteq C$. Тада је $A \triangle B = A \setminus B$ и

$$\begin{aligned} X &= (A \triangle B) \triangle C \\ &= (A \setminus B) \triangle C \\ &= C \setminus (A \setminus B) \\ &= (C \setminus A) \cup B. \end{aligned}$$

13. Решићемо овај задатак на два начина — коришћењем карактеристичних функција и директно.

Први начин Нека је $U = A \cup X \cup Y$. Из претпоставки следи да је

$$\chi_A \chi_X = \chi_A \chi_Y, \quad \chi_A + \chi_X + \chi_A \chi_X = \chi_A + \chi_Y + \chi_A \chi_Y.$$

Добијамо да је $\chi_X = \chi_Y$, па је $X = Y$.

Други начин Претпоставимо да $x \in X$. Тада $x \in A \cup X = A \cup Y$. Претпоставимо да $x \notin Y$. Тада $x \in A$, па следи да $x \in A \cap X = A \cap Y$, те ипак $x \in Y$. Дакле, доказали смо да из $x \in X$ следи да $x \in Y$, тј. $X \subseteq Y$. Наравно да се и друга инклузија лако доказује.

14. Како је $B \subseteq B \cup X = A \cap X \subseteq A$, то закључујемо да је $B \subseteq A$ потребан услов за постојање скупа X. Осим тога, јасно је да је $B \subseteq B \cup X = A \cap X \subseteq X$, па је $B \cup X = X$. Следи да је $A \cap X = X$, тј. $X \subseteq A$. Но, сваки скуп X такав да је $B \subseteq X \subseteq A$ задовољава дату једначину и тако добијамо тражено решење.

15. (а) Овај део је најлакше урадити коришћењем карактеристичних функција. Подсетимо се да је

$$\chi_{A\triangle B} = \chi_A + \chi_B; \quad \chi_{A^c} = 1 + \chi_A.$$

Одавде лако изводимо $\chi_{A*B} = \chi_A + \chi_{B^c} = \chi_A + \chi_B + 1$. За проверу асоцијативности израчунајте $\chi_{(A*B)*C}$ и $\chi_{A*(B*C)}$. Добија се исти резултат у оба случаја (наравно да у том доказу користимо комутативност и асоцијативност сабирања у скупу карактеристичних функција!). Комутативност је јасно испуњена. Да бисмо открили који је подскуп неутрал за операцију $*$ треба наћи E такав да је $A * E = A$ (операција $*$ је комутативна, па не морамо проверавати и $E * A = A$). Но, то се своди на $1 + \chi_A + \chi_E = \chi_A$, односно на $\chi_E = 1$ (подсетимо се да је $\chi_Z + \chi_Z = 0$ за сваки $Z \in \mathcal{P}(X)$). Закључујемо да је $E = X$. Како је $\chi_A * \chi_A = 1 = \chi_X$, то добијамо да је сваки елемент сам свој инверз, па према томе сваки елемент заиста има инверз и ово је Абелова група.

(б) У случају да је $|X| = n$, добијамо да је $|\mathcal{P}(X)| = 2^n$. Но, у коначној Абеловој групи $(\mathcal{P}(X), *)$ сваки елемент сем неутрала је реда 2 ($A*A = X$). Према основној теореми о коначним Абеловим групама, свака од њих је сума цикличних. Како се овде појављују искључиво елементи реда 2, то та група мора бити сума цикличних група које су све изоморфне $\mathbb{Z}_2$. Како је $|\mathcal{P}(X)| = 2^n$ то она мора бити изоморфна баш групи $(\mathbb{Z}_2)^n$ (број елемената у овој групи је 2^n).

16. Посматрајмо најпре неки конкретан случај, нпр. нека је $n = 2$ и A_0, A_1 су подскупови скупа X. Које све подскупове можемо добити на наведени начин? Наведимо их: A_0, A_0^c, A_1, A_1^c, $A_0 \cup A_1$, $A_0 \cup A_1^c$, $A_0^c \cup A_1$, $A_0^c \cup A_1^c$, $\emptyset (= A_0 \cap A_0^c)$, $A_0 \cap A_1$, $A_0^c \cap A_1$, $A_0 \cap A_1^c$, $A_0^c \cap A_1^c$, $X (= A_0 \cup A_0^c)$, $(A_0 \cap A_1^c) \cup (A_0^c \cap A_1)$, $(A_0 \cap A_1) \cup (A_0^c \cap A_1^c)$. Наравно, можда међу овим скуповима има једнаких, а осим тога треба проверити да ли смо неки скуп „испустили“.

Уведимо следеће ознаке. Ако је $B \subseteq X$, онда нека је $B^1 := B$, а $B^0 := B^c$. Ако је $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}) \in 2^n$, нека је

$$A(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}) := A_0^{\varepsilon_0} \cap A_1^{\varepsilon_1} \cdots \cap A_{n-1}^{\varepsilon_{n-1}}.$$

Приметимо да ови скупови чине једно разбијање скупа X, тј. то су међусобно дискјунктни подскупови од X чија је унија X. Како је број n-торки 2^n, то смо добили разбијање скупа X на 2^n међусобно дисјунктних подскупова. Бирањем које од тих подскупова унирамо, добијамо укупно (највише) 2^{2^n} различитих скупова.

Није тешко доказати да су ово сви могући скупови које можемо добити на наведени начин. Наиме, ако је скуп A тако добијен, онда важи следеће. За свако $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ из 2^n:

$$A \cap A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}) \neq \emptyset \Rightarrow A \cap A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}) = A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$$

То се може, на пример, доказати индукцијом по броју коришћења операције уније при формирању скупа A. Доказ препуштамо читаоцу. Када је ово доказано, онда је јасно да је сваки добијени скуп унија неких скупова $A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$.

Пример у коме се постиже тачно 2^{2^n} различитих скупова је следећи. Нека је $X = \{0, 1, \dots, 2^n - 1\}$ (наравно да је заправо $X = 2^n$). Нека скуп A_i чине они бројеви из X код којих се у бинарном запису на i-тој позицији налази 1. (На пример, за $n = 4$, $X = \{0, 1, \dots, 15\}$, $A_0 = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $A_1 = \{2, 3, 6, 7, 10, 11, 14, 15\}$, $A_2 = \{4, 5, 6, 7, 12, 13, 14, 15\}$, $A_3 = \{8, 9, 10, 11, 12, 13, 14, 15\}$.) Јасно је да је сваки од скупова $A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ једночлан. Заправо је $A(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}) = \{\varepsilon_0 \cdot 2^0 + \varepsilon_1 \cdot 2^1 + \dots + \varepsilon_{n-1} \cdot 2^{n-1}\}$. Стога су сви могући скупови које добијамо унијом ових међусобно различити.

17. Ово наравно није тешко проверити:

$$\{a\} \times \{a\} = \{(a, a)\} = \{\{\{a\}, \{a, a\}\}\} = \{\{\{a\}, \{a\}\}\} = \{\{\{a\}\}\}.$$

18. Овде користимо идеју коју смо већ имали прилике да видимо. Дакле, претпоставимо да наведени скупови постоје и посматрајмо скуп $A = \{x, y, z\}$ (овај скуп се може видети као унија скупова $\{x, y\}$ и $\{z\}$ за које знамо да постоје). Према Аксиоми доброг заснивања у A постоји елемент дисјунктан са њим. То не може бити елемент x, јер $z \in A \cap x$. То не може бити елемент y, јер $x \in A \cap y$. Но, то не може бити ни елемент z, јер $y \in A \cap z$. Како смо добили контрадикцију закључујемо да тражени скупови не постоје.

19. Уколико би постојао такав скуп x добили бисмо да важи: $x \in \{x\}$ и $\{x\} \in x$, тј. постојали би скупови x и y такви да је $x \in y$ и $y \in x$, а знамо да то није тачно.

20. Претпоставимо да постоји скуп u који садржи све једночлане скупове. Тада би важило: $\{u\} \in u$. Према претходном задатку то није могуће.

21. Уколико би постојао такав скуп x, како $x \in \{x\}$, добили бисмо да $x \in x$, а то није могуће.

22. Претпоставимо да такав скуп x постоји. Како је $(x, x) = \{\{x\}\}$, то добијамо да важи $x \in \{x\} \in \{\{x\}\} \in x$, тј. постоје скупови x, y, z такви да је $x \in y \in z \in x$, а то није могуће.

    Напомена: Наравно да смо могли користити и резултат из текста по коме не постоје скупови x, y такви да је $(x, y) \in x$, но изабрали смо да дамо директан доказ.

23. Претпоставимо да је a непразан скуп такав да је $a = a \times a$. Формирајмо скуп $A = a \cup (\cup a)$ (подсетите се дефиниције уније). Према Аксиоми доброг заснивања закључујемо да постоји $x \in A$ такав да $x \cap A = \emptyset$. Разликујемо два случаја.

    (а) $x \in a$. Како је по претпоставци $a = a \times a$, то постоје $y, z \in a$ такви да је $x = (y, z) = \{\{y\}, \{y, z\}\}$. Добијамо да $\{y\} \in x \in a$, тако да $\{y\} \in \cup a$ по дефиницији уније. Дакле и $\{y\} \in A$, а како већ припада x, то добијамо контрадикцију.

    (б) $x \in \cup a$. То значи да постоји неки $w \in a$, такав да $x \in w \in a$. Како је по претпоставци $a = a \times a$, то је $w = (u, v) = \{\{u\}, \{u, v\}\}$, за неке $u, v \in a$. Стога је $x = \{u\}$ или $x = \{u, v\}$. У сваком случају, $u \in x$, а по претходном $u \in a \subseteq A$, па би скуп $x \cap A$ био непразан. Дошли смо до контрадикције.

24. Јасно је да уколико је $A = C$ и $B = D$ важи и $A \times C = B \times D$. Потребно је доказати други смер. Наравно, то није тешко. Како су ово непразни скупови то можемо изабрати неки елемент из сваког од њих, нпр. нека је $b_0 \in B$. Претпоставимо да је $a \in A$ произвољан елемент. Тада уређени пар (a, b_0) припада $A \times B = C \times D$. Дакле, $(a, b_0) \in C \times D$, те следи да $a \in C$. Тако смо доказали да је $A \subseteq C$. На сличан начин се доказују и остале инклузије и добијамо да је заиста $A = B$, $C = D$.

25. Претпоставимо да за неки непразан скуп A важи: $(A \times A) \times A = A \times (A \times A)$. Према претходном задатку добијамо да мора бити $A = A \times A$, а на основу 23. задатка знамо да то није могуће.

26. Претпоставимо да је за неки непразан скуп X испуњено $\mathcal{P}(X) = 2^X$. Како је скуп X непразан то постоји неко $x_0 \in X$. Посматрајмо подскуп $\{x_0\}$. По претпоставци је $\mathcal{P}(X) = 2^X$, те закључујемо да $\{x_0\} \in 2^X$. Дакле, $\{x_0\} = f$, где $f \colon X \to 2$. Но, тада добијамо

$$\{x_0\} \in \{\{x_0\}, \{x_0, f(x_0)\}\} = (x_0, f(x_0)) \in f = \{x_0\}$$

што, како знамо, није могуће.

27. Јасно је да је довољно доказати само један смер. Претпоставимо стога да је $\langle x, y\rangle = \langle u, v\rangle$. Користећи дефиницију, чињеницу да је скуп $\{\emptyset, \{x\}\}$ двочлан (скуп $\{x\}$ сигурно није празан), као и резултат из текста (који тачно?) добијамо да је $\{\emptyset, \{x\}\} = \{\emptyset, \{u\}\}$ и $\{\{y\}\} = \{\{v\}\}$. Одавде, поновном применом истог резултата, као и Аксиоме екстензије добијамо да је $x = u$ и $y = v$, што се и тражило.

28. Покажимо најпре да је релација рефлексивна. Нека је $a \in X$ произвољан елемент. Прво својство релације „каже“ да за сваки елемент из X постоји елемент са којим је он у релацији. Према

томе и за наведено a постоји елемент x такав да је $x\,\rho\,a$. Но, друго својство даје $x\,\rho\,a \wedge x\,\rho\,a \Rightarrow a\,\rho\,a$. Дакле, релација јесте рефлексивна. Симетричност сада није тешко проверити. Наиме, нека је $a\,\rho\,b$; како је и $a\,\rho\,a$, то из другог својства следи да је $b\,\rho\,a$. Из симетричности и другог својства следи транзитивност.

29. Оно што не треба радити је следеће. Исписати дату једнакост у „погодном“ облику $\rho\,\rho\,\sigma\,\sigma = \rho\,\sigma\,\rho\,\sigma$, а затим скратити ρ са леве стране и σ са десне! Наравно да ово не смемо радити са релацијама! Ако је тај трик „радио“ код група, не значи да се може свуда користити. Заправо, баш чињеница да се ово не може тако урадити би требало да нас наведе да тражимо контрапример. Нека је $A = \{0,1,2\}$, $\rho = \{(0,0),(0,1),(0,2)\}$ и $\sigma = \{(0,0),(1,0),(2,0)\}$. Дакле, релације смо изабрали тако да је $0\rho x$ за све $x \in A$, док је $x\sigma 0$ за све $x \in A$ док остали парови елемената не улазе у релације. Проверимо да ли су испуњени тражени услови. Нека је $x\rho^2 y$ за неке $x, y \in A$. То значи да мора постојати $z \in A$ такав да је $x\rho z$ и $z\rho y$. Но, тада x мора бити 0 и добијамо да је $\rho^2 = \rho$ (зашто?). На сличан начин се добија да је $\sigma^2 = \sigma$. Одредимо $\rho\sigma$. Нека је $x\,\rho\sigma\,y$. То значи да постоји z такво да је $x\sigma z$ и $z\rho y$. Но, видимо да за произвољан избор елемената x и y постоји такво z, то је 0. Закључујемо да је $\rho\sigma = A^2$. Из свега до сада виђеног добијамо да је $\rho^2\sigma^2 = (\rho\sigma)^2$. Одредимо $\sigma\rho$. Нека је $x\,\sigma\rho\,y$. То значи да постоји z такво да је $x\rho z$ и $z\sigma y$. Но, то је могуће само под условом да је $x = 0$ и $y = 0$ (једини елемент x за који постоји z такав да је $x\rho z$ је 0). Према томе, $\sigma\rho = \{(0,0)\}$ и $\rho\sigma \neq \sigma\rho$.

30. Скраћивање наравно не долази у обзир, као ни у претходном задатку. Анализирајмо мало дату ситуацију. Видимо да је у услову који функције f и g испуњавају функција f та која „напада“ композицију неких функција и са леве и са десне стране знака једнакости. Према томе, ако је функција f *константна*, онда је наведена једнакост тачна *независно од функције* g. Но, сада је лако наћи контрапример. За скуп X можемо узети било који скуп са бар два елемента, док функције f и g могу бити било које константне, али *различите* функције. Тада ће услов задатка бити испуњен, но неће важити да је $f \circ g = g \circ f$. Размислите како бисте могли да искористите ово решење за решавање претходног задатка.

31. На основу дефиниције, $x \in \mathrm{Dom}(\rho)$ ако и само ако постоји $y \in \mathbb{R}$ тако да је $x^3 = y^2 + 3y + 1$, тј. тако да је $y^2 + 3y + (1 - x^3) = 0$. Другим речима, интересује нас за које $x \in \mathbb{R}$ ова једначина (по y) има реално решење. Но, то је квадратна једначина и није тешко установити да она има реално решење ако и само ако је $x \geq -\sqrt[3]{\frac{9}{4}}$, те је $\mathrm{Dom}(\rho) = [-\sqrt[3]{\frac{9}{4}}, +\infty)$. С друге стране, $y \in \mathrm{Im}(\rho)$ ако и само

ако постоји $x \in \mathbb{R}$ тако да је $x^3 = y^2 + 3y + 1$. Но, ово је испуњено за све $y \in \mathbb{R}$, па је $\mathrm{Im}(\rho) = \mathbb{R}$.

32. Релација ρ је заправо један паралелограм у равни који одређују праве $x - y = -1$, $x - y = 2$, $x + y = 1$, $x + y = 5$ (нацртајте слику). Домен заправо чине све тачке са x-осе за које одговарајуће вертикалне праве секу овај скуп, док слику чине све тачке са y-осе тако да одговарајуће хоризонталне праве секу дати скуп. Решавањем одговарајућих система једначина налазимо темена овог паралелограма и то су $(-1, 0), (1/2, -3/2), (7/2, 3/2), (2, 3)$. Добијамо да је $\mathrm{Dom}(\rho) = [-1, 7/2]$, а $\mathrm{Im}(\rho) = [-3/2, 3]$. Проверите ово!

33. Како је $\triangle_A \subseteq \sigma$ и $\triangle_A \subseteq \rho$, то је $\triangle_A \subseteq \sigma \cap \rho$. Такође је $(\sigma \cap \rho)^{-1} = \sigma^{-1} \cap \rho^{-1} = \sigma \cap \rho$. На крају, $(\sigma \cap \rho) \circ (\sigma \cap \rho) \subseteq \sigma \circ \sigma \subseteq \sigma$ и $(\sigma \cap \rho) \circ (\sigma \cap \rho) \subseteq \rho \circ \rho \subseteq \rho$, те је $(\sigma \cap \rho) \circ (\sigma \cap \rho) \subseteq (\sigma \cap \rho)$. Закључујемо да је $\sigma \cap \rho$ релација еквиваленције.

    Ако је $\sigma \circ \rho$ релација еквиваленције, мора бити $(\sigma \circ \rho)^{-1} = \sigma \circ \rho$. Но, $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1} = \rho \circ \sigma$. Према томе, ако је $\sigma \circ \rho$ релација еквиваленције, релације σ и ρ комутирају.

    Претпоставимо да је $\sigma \circ \rho = \rho \circ \sigma$. Докажимо да је $\sigma \circ \rho$ релација еквиваленције.

    Рефлексивност: $\triangle_A = \triangle_A \circ \triangle_A \subseteq \sigma \circ \rho$.

    Симетричност: $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1} = \rho \circ \sigma = \sigma \circ \rho$.

    Транзитивност:

    $(\sigma \circ \rho) \circ (\sigma \circ \rho) = \sigma \circ (\rho \circ \sigma) \circ \rho = \sigma \circ (\sigma \circ \rho) \circ \rho = (\sigma \circ \sigma) \circ (\rho \circ \rho) \subseteq \sigma \circ \rho$.

34. Коришћењем карактеристичних функција добијамо:

$$A \triangle B \subseteq C \text{ акко } (A \triangle B) \cap C = A \triangle B \text{ акко } \chi_A \chi_C + \chi_B \chi_C = \chi_A + \chi_B$$

$$\text{акко } \chi_A + \chi_A \chi_C = \chi_B + \chi_B \chi_C \text{ акко } A \setminus C = B \setminus C.$$

    Сада није тешко показати да је $\sim_C$ релација еквиваленције. Класа скупа A је $\{(A \setminus C) \cup D : D \subseteq C\}$. Наиме, јасно је да је $((A \setminus C) \cup D) \setminus C = A \setminus C$ за сваки $D \subseteq C$. Осим тога, ако је $B \setminus C = A \setminus C$, онда је $B = (B \setminus C) \cup (B \cap C) = (A \setminus C) \cup D$, где је $D = B \cap C \subseteq C$.

35. Лако се проверава да је $\equiv_m$ релација еквиваленције. Нека то читаоци сами ураде за вежбу. Ми ћемо доказати да важе наведене једнакости међу релацијама.

    Пре свега, уколико је $a(\equiv_m \cap \equiv_n)b$ то значи да и m и n деле разлику $a - b$, а то је еквивалентно са $\mathrm{NZS}(m, n) \mid (a - b)$.

    Нешто је теже доказати резултат за композицију. Уколико је $a(\equiv_m \circ \equiv_n)b$, то постоји цео број c такав да је $a \equiv_n c$ и $c \equiv_m b$. Дакле, за неке целе бројеве k, l је $a = c + nk$, $b = c + ml$. Добијамо да је $a-b=nk-ml$. Но, одавде следи да $\mathrm{NZD}(m,n) \mid (a-b)$. Претпоставимо да $\mathrm{NZD}(m,n) \mid (a-b)$. Ако са d означимо $\mathrm{NZD}(m,n)$, онда за неки цео број r важи $a-b=dr$. Но, добро је позната чињеница да постоје цели бројеви p и q за које је $mp+nq=d$. Множењем са r добијамо да је $mpr+nqr=dr=a-b$. Нека је $c=a-mpr$. Тада је јасно да $m \mid (a-c)$. Но, $c-b=a-mpr-b=nqr$, па $n \mid (c-b)$.

36. Лако се показује да је $\rho \circ \rho$ пуна релација, тј. да су свака два позитивна цела броја у тој релацији. Наиме, како је сваки број узајамно прост са 1, то је $a\,\rho\,1$ и $1\,\rho\,b$ за произвољне a, b, те је $a(\rho \circ \rho)b$. Закључујемо да је најмања релација еквиваленције, која садржи релацију ρ заправо пуна релација.

37. Није тешко уверити се да је $\perp \circ \perp = \|$. Но, релација $\perp \cup \|$ *јесте* релација еквиваленције (проверите ово), те је стога то и најмања релација еквиваленције, која садржи релацију $\perp$.

38. У овом случају добијамо сасвим другачији резултат. Наиме, за сваке две равни у простору, постоји трећа раван која је ортогонална на обе (подсетите се мало знања из средњошколске геометрије). Стога је релација $\perp \circ \perp$ пуна релација, а то је и тражена релација еквиваленције.

39. Опет нам знање средњошколске геометрије помаже. Наиме, за сваке две кружнице k_1 и k_2 постоји кружница k тако да k додирује и кружницу k_1 и кружницу k_2 (докажите ово). Стога је опет тражена релација заправо пуна релација.

40. Како је $\leq^{-1} = \geq$, а релација $\leq \circ \geq$ је пуна релација (за свака два цела броја a и b постоји цео број c који је већи од оба), то је тражена релација поново пуна релација.

41. Лако се проверава да је овако дефинисана једна релација парцијалног уређења на $\mathbb{R}^2$. Како је за свако $(x,y) \in T$ испуњено $(0,0) \preceq (x,y)$, то је координатни почетак најмањи елемент у T, а тиме и једини минимални елемент.

    Нека је $(x,y) \in T$ и нека је $x+2y < 1$ (дакле (x,y) није на хипотенузи нашег троугла). Уколико је $y' = \frac{1-x}{2}$, онда се лако може проверити да $(x,y') \in T$ и да је $(x,y) \prec (x,y')$. Наиме, $x+2y' = x+2\frac{1-x}{2} = 1$, а $x \leq x$ и $y < y' = \frac{1-x}{2}$. Дакле, елемент (x,y) за који је $x+2y<1$ није максималан елемент у T. Но, *сваки* елемент са хипотенузе јесте максималан. Наиме, ако је $x+2y=1$ и $(x,y) \prec (u,v)$, онда је $x \leq u$ и $y \leq v$ при чему је бар једна од ових неједнакости строга. Стога је $1 = x+2y < u+2v$ и добијамо да $(u,v) \notin T$. Дакле, заиста је сваки елемент са хипотенузе максималан и у овом посету не постоји највећи елемент.

4.2 Задаци из друге главе

1. Можда је најједноставнији начин за решавање овог задатка следећи. Нека је

$$\begin{aligned} |A \setminus B| &= a \\ |B \setminus A| &= b \\ |A \cap B| &= p. \end{aligned}$$

Како скупови $A \setminus B$, $B \setminus A$ и $A \cap B$ чине *разбијање* скупа $A \cup B$, тј. њихова *дисјунктна* унија је тај скуп, то добијамо

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |B \setminus A| + |A \cap B| \\ &= a + b + p \\ &= (a+p) + (b+p) - p \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

2. Погледајмо, пре свега, како би тражена формула изгледала за случај од три скупа. Користимо претходни задатак.

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \end{aligned}$$

$$= |A| + |B| - |A \cap B| + |C| - (|A \cap C| + |B \cap C| - |A \cap C \cap B \cap C|)$$

$$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Сада не би требало да буде тешко *погодити* општу формулу:

$$|A_1 \cup \cdots \cup A_n| =$$

$$= |A_1| + \cdots + |A_n| - (|A_1 \cap A_2| + \cdots + |A_{n-1} \cap A_n|) \pm \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

Прецизније:

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

Доказ изводимо индукцијом. За случај $n = 2$, па и $n = 3$ доказ је изведен. Претпоставимо да је формула доказана за n скупова и докажимо је за $n + 1$ скупова. Најпре добијамо

$$|(A_1 \cup \cdots \cup A_n) \cup A_{n+1}| = |A_1 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup \cdots \cup A_n) \cap A_{n+1}|.$$

Према индуктивној хипотези знамо да је

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

Уведимо ознаке $B_i = A_i \cap A_{n+1}$. Тада из индуктивне хипотезе (примењене на случај од n скупова $B_1, \ldots, B_n$) добијамо

$$\begin{aligned} |(A_1 \cup \cdots \cup A_n) \cap A_{n+1}| &= |(A_1 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})| \\ &= |B_1 \cup \cdots \cup B_n| \end{aligned}$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_k}|$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots A_{i_k} \cap A_{n+1}|.$$

Добили смо да је број елемената скупа $A_1 \cup \cdots \cup A_{n+1}$ једнак

$$\begin{aligned} &\sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| + |A_{n+1}| \\ + &\sum_{k=1}^{n} (-1)^{k} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots A_{i_k} \cap A_{n+1}|. \end{aligned}$$

Анализирајмо то што смо добили. У првој суми врши се сумирање по свим двојкама, тројкама,..., n-торкама скупова међу којима *није* скуп A_{n+1} уз наравно сабирање броја елемената у појединачним скуповима. Тој суми додајемо број елемената у скупу A_{n+1}, а затим додајемо суму у којој се сумира по свим двојкама, тројкама,..., $(n+1)$-торкама скупова у којима се *обавезно* појављује скуп A_{n+1}. Ако погледамо који се знаци налазе уз одговарајуће чланове у сумама, јасно је да смо добили тражени резултат. Препоручујемо читаоцу да сам напише формулу за број елемената у унији од $n+1$ скупова $A_1, \ldots, A_{n+1}$ и упореди са оним што смо добили.

3. Јасно је да резултат у овом случају следи из претходног задатка. Како је
$$|V \setminus (A_1 \cup \cdots \cup A_n)| = |V| - |A_1 \cup \cdots \cup A_n|,$$
то, користећи претходни резултат, добијамо
$$|V \setminus (A_1 \cup \cdots \cup A_n)| = |V| + \sum_{k=1}^{n} (-1)^{k} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|.$$

4. Означимо са $\mathcal{S}$ скуп свих тражених скупова. Функција $f\colon \mathcal{S} \to \mathcal{P}(A \setminus B)$ дефинисана са $f(C) = C \setminus B$ је бијекција (проверити!). Због тога добијамо да је $|\mathcal{S}| = |\mathcal{P}(A \setminus B)| = 2^{m-n}$.

5. (а) Ово није тешко. Ако је $X = \{x_1, x_2, \ldots, x_m\}$ и $Y = \{y_1, y_2, \ldots, y_n\}$ то се сваки елемент $x_i \in X$ може пресликати у било који од $y_j \in Y$, тј. за сваки елемент из X има n могућности, па је укупан број могућности, тј. функција из X у Y баш n^m.

   (б) Уколико је $m > n$ јасно је да „1–1“ функција из X у Y не може постојати. Претпоставимо стога да је $m \leq n$. Елемент x_1 може се сликати у било који елемент из Y, па за њега има n могућности. За елемент x_2 већ не постоји толики избор, пошто се не сме сликати у исти елемент у који се слика x_1. За њега дакле има $n-1$ могућности. За x_3 има $n-2$ итд. Закључујемо да је укупан број „1–1“ функција из X у Y једнак $n(n-1)\cdots(n-m+1)$. Приметимо да нам ова формула даје резултат 0 у случају да је $m > n$, тако да је она исправна за све случајеве.

   (ц) Ово је већ нешто сложенији задатак. Да бисмо одредили број сурјекција из X на Y поступимо на следећи начин. Означимо са A_i скуп свих функција из X у Y које „не погађају“ елемент y_i, тј. нека је

$$A_i := \{f \colon X \longrightarrow Y \mid y_i \notin \mathrm{Im}(f)\}.$$

Јасно је да је функција f „на“ **акко** не припада ниједном од скупова A_i, тј. сваки y_i јесте у слици функције f. Како не постоји функција f која је „на“ у случају да је $m < n$, то у даљем претпостављамо да је $m \geq n$. Користићемо формулу из једног од претходних задатака пошто покушавамо да одредимо број елемената неког скупа (у нашем случају скупа свих функција из X у Y) који нису ни у једном од скупова A_i. Приметимо да је $|A_1| = |A_2| = \cdots |A_n|$. Општије

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = |A_{j_1} \cap \cdots \cap A_{j_k}|,$$

за произвољне k-торке $i_1 < \cdots < i_k$ и $j_1 < \cdots < j_k$.

Погледајмо најпре колико има елемената у скупу A_1. Ту се налазе све функције код којих се ниједан елемент не слика у y_1, дакле има их исто као и функција из скупа X у скуп $Y \setminus \{y_1\}$, те је $|A_1| = (n-1)^m$. У скупу $A_1 \cap A_2$ има исто елемената као и функција из скупа X у скуп $Y \setminus \{y_1, y_2\}$, тј. $(n-2)^m$. Напокон $|A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)^m$. За коначан одговор довољно је приметити да k-торки $i_1 < \cdots < i_k$ има $\binom{n}{k}$. Примењујући претходно доказану формулу добијамо да је број функција из X у Y које су „на“

$$n^m + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)^m,$$

што је и требало доказати.

6. Приметимо, пре свега, да свакој релацији еквиваленције на скупу X одговара једна партиција тог скупа, тј. колекција дисјунктних скупова чија је унија скуп X. Наиме, класе еквиваленције представљају тражену партицију. Но, важи и обратно, свакој партицији одговара једна релација еквиваленције — дефинишемо да су два елемента у релацији акко припадају истом члану партиције. Према томе, уместо релација еквиваленције посматраћемо партиције датог скупа. Нека је $X = \{x_1, \ldots, x_n, x_{n+1}\}$. Концентришимо се на елемент x_{n+1}. Каква год да је партиција скупа X, елемент x_{n+1} мора се налазити у неком елементу те партиције. Елемент те партиције може имати 1, 2,..., $n+1$ чланова. Пребројимо колико има партиција у којима се елемент x_{n+1} налази у $(k+1)$-чланом подскупу партиције. Пре свега број начина да се из скупа од n преосталих елемената скупа X изабере k да би се формирао $(k+1)$-члани подскуп је $\binom{n}{k}$. На преосталом скупу од $n-k$ елемената могу се правити произвољне партиције и њих има p_{n-k}. Како k може бити било који број од 0 до n, то је

$$\begin{aligned} p_{n+1} &= \sum_{k=0}^{n} \binom{n}{k} p_{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{n-k} p_{n-k} \\ &= \sum_{j=0}^{n} \binom{n}{j} p_j. \end{aligned}$$

7. Ово није тешко. Најмањи елемент може бити било који елемент, следећи по реду било који сем овог, итд. Одговор је $n \cdot (n-1) \cdot (n-2) \cdots 1 = n!$. Наравно да је то број пермутација скупа од n елемената.

8. Претпоставимо да у посету P има највише n елемената који су пар по пар упоредиви. Издвојимо m таквих максималних скупова упоредивих елемената (ланаца). Тако смо „покупили“ највише mn елемената из P. Ако сада из сваког од тих скупова изаберемо по један елемент и још један који не припада ниједном од њих (а то је могуће пошто укупно има $mn+1$ елемената), то смо добили скуп од $m+1$ међусобно неупоредивих елемената, дакле један антиланац.

   Напомена: Због симетрије следи да у том посету постоји антиланац са $n+1$ елемената, или ланац са $m+1$ елемената.

9. Први начин: Претпоставимо да је максимална дужина растућег подниза нашег низа m. Формирајмо максималне растуће поднизе тог низа почев од првог члана. Када формирамо један подниз,

следећи започињемо од првог неискоришћеног члана почетног низа. Поновимо тај поступак док не добијемо n растућих поднизова. Ако са $x_1, x_2, \dots x_n$ означимо њихове последње чланове, онда се можемо уверити да они чине опадајући подниз, тј. $x_1 > x_2 > \cdots > x_n$. Наиме, ако би било $x_1 < x_2$, онда би низ који се завршава са x_1 било могуће продужити бар чланом x_2, а то по конструкцији није могуће. Слично важи и за остале. Како почетни низ има $mn{+}1$ чланова, а ми смо овим поступком покрили њих највише mn, то постоји неки члан низа, који није ни у једном од ових растућих низова. Означимо са x_{n+1} „први“ такав члан низа (дакле, члан низа са најмањим индексом у почетном низу који се не појављује у овим растућим низовима — наравно да његов индекс у почетном низу не мора бити баш $n+1$). Но, он се није појавио у првом растућем низу, што значи да је мањих од неког члана тог низа, па тиме и од највећег, тј. x_1. Како се није појавио ни у другом, то такође значи да је мањи и од x_2 итд. Закључујемо да је x_{n+1} мањи од свих x_k па на тај начин добијамо опадајући низ $x_1 > \cdots > x_{n+1}$ дужине $n+1$.

Други начин: Ако је (x_k) дати низ бројева, нека је $P = \{a_k : 1 \leq k \leq mn+1\}$, скуп од $mn+1$ елемената. На скупу P уводимо парцијално уређење $\prec$ на следећи начин. Ако је $k < l$, онда је

$$a_k \prec a_k \text{ акко } x_k < x_l.$$

Сада искористимо претходни задатак.

10. Сваки реалан број x дефинише подскуп скупа рационалних бројева $D_x := \{r \in \mathbb{Q} : r < x\}$. Како је испуњено: $x < y$ **акко** $D_x \subset D_y$, то на тај начин добијамо у $\mathcal{P}(\mathbb{Q})$ ланац кардиналности $\mathfrak{c}$. Коришћењем чињенице да постоји бијекција између $\mathbb{N}$ и $\mathbb{Q}$ добијамо да и у $\mathcal{P}(\mathbb{N})$ постоји ланац те кардиналности. Пример антиланца кардиналности $\mathfrak{c}$ налазимо на следећи начин. Присетимо се да постоји бијекција између скупа свих парних природних бројева и скупа свих непарних природних бројева, као и да је кардиналност скупа парних природних бројева $\aleph_0$. Нека је $f\colon 2\mathbb{N} \longrightarrow 2\mathbb{N}+1$ бијекција задата са $f(2n) = 2n+1$. Ако је $A \subseteq 2\mathbb{N}$ онда посматрајмо скуп $(2\mathbb{N} \setminus A) \cup f[A]$. Приметимо да су скупови $(2\mathbb{N} \setminus A) \cup f[A]$ и $(2\mathbb{N} \setminus B) \cup f[B]$ *неупоредиви* у смислу инклузије ако је $A \neq B$. Наиме, како су скупови $2\mathbb{N} \setminus A$ и $f[A]$ дисјунктни (у једном су парни, а у другом непарни природни бројеви), то из $(2\mathbb{N} \setminus A) \cup f[A] \subseteq (2\mathbb{N} \setminus B) \cup f[B]$ следи да мора бити $2\mathbb{N} \setminus A \subseteq 2\mathbb{N} \setminus B$ и $f[A] \subseteq f[B]$. Из првог услова добијамо да је $A \supseteq B$, а из другог $A \subseteq B$ (f је бијекција). Према томе, следи да мора бити $A = B$. Како подскупова од $2\mathbb{N}$ има $\mathfrak{c}$ и тих неупоредивих подскупова има $\mathfrak{c}$ и то је тражени антиланац кардиналности $\mathfrak{c}$.

11. Ако су a и b елементи неког посета и $a < b$, онда a не може

бити максималан елемент. Стога су свака два максимална елемента неупоредива. Претпоставимо да је P коначни посет и $x \in P$ произвољни елемент. Ако је x максималан, онда је тражени резултат доказан. У супротном постоји елемент $x_1 \in P$ такав да је $x < x_1$. Уколико је x_1 максималан добијамо тражени елемент, у противном настављамо претходни поступак, тј. узимамо елемент x_2 такав да је $x_1 < x_2$. Ако је $|P| = n$, онда се овај поступак може поновити највише $n-1$ пута и у последњем кораку добијамо тражени максимални елемент.

12. Нека је $p_0, p_1, \ldots$ низ који се састоји од свих простих бројева (они могу бити поређани у растући поредак, али и не морају — за овај доказ нам то није битно). Изоморфизам $f\colon P \longrightarrow \mathbb{N}\setminus\{0\}$ дефинисан је са
$$f(\langle x_n \rangle) \stackrel{\text{def}}{=} \prod_{n \in N} p_n^{x_n}.$$
Приметимо да је овај производ увек коначан, јер су сви фактори сем њих коначно много једнаки 1. Ово јесте бијекција због основне теореме аритметике. Но, $f(\langle x_n \rangle) | f(\langle y_n \rangle)$ повлачи да се сваки прост број који се налази у факторизацији броја $f(\langle x_n \rangle)$, тј. они p_k за које је $x_k \neq 0$, нужно налази и у факторизацији броја $f(\langle y_n \rangle)$ и то са експонентом који није већи, тј. за те x_k важи: $x_k \leq y_k$. Но, то управо значи да је $\langle x_n \rangle \leq_P \langle y_n \rangle$. Јасно је да из $\langle x_n \rangle \leq_P \langle y_n \rangle$ следи да $f(\langle x_n \rangle) | f(\langle y_n \rangle)$.

13. Показаћемо да је аутоморфизам наведеног посета одређен његовим вредностима на једночланим скуповима. Из тог резултата следи да је број аутоморфизама $n!$ — једночланих подскупова има n и свака бијекција на скупу свих једночланих подскупова продужује се на јединствен начин до аутоморфизма посета $\mathcal{P}(A)$. За доказ наведеног резултата довољно је да докажемо да је за $C, D \subseteq A$ испуњено: $f(C \cup D) = f(C) \cup f(D)$, за сваки аутоморфизам f. Докажимо то. Како је $C \subseteq C \cup D$ и f аутоморфизам, то је $f(C) \subseteq f(C \cup D)$. На исти начин добијамо и да је $f(D) \subseteq f(C \cup D)$, па је $f(C) \cup f(D) \subseteq f(C \cup D)$. Но, $f(C) \cup f(D) = f(E)$ за неки $E \subseteq A$, јер је f бијекција. Из чињенице да је $f(C) \subseteq f(E$ добијамо $C \subseteq E$, а аналогно је и $D \subseteq E$. Тако је $C \cup D \subseteq E$, па је $f(C \cup D) \subseteq f(E) = f(C) \cup f(D)$. Обратна инклузија је већ доказана, те закључујемо да је $f(C \cup D) = f(C) \cup f(D)$.

14. Ако са $[x]$ ($\{x\}$) означимо цео (разломљени) део броја x, дефинишемо релацију уређења $\preceq$ са:
$$x \prec y \textbf{ акко } \{x\} < \{y\} \text{ или је } \{x\} = \{y\} \text{ и } [x] < [y].$$
Тада је $x - 1$ претходник, а $x + 1$ броја x. Наиме, подсетимо се да је $\{x\} = x - [x]$, као и да је $[x + m] = [x] + m$ за сваки $m \in \mathbb{Z}$ и сваки

$x \in \mathbb{R}$. Претпоставимо да постоји $y \in \mathbb{R}$ такав да је $x \prec y \prec x+1$. Како је $\{x+1\} = x+1-[x+1] = x-[x] = \{x\}$, то не може бити $\{x\} < \{y\}$ (јер би тада важило и $\{x+1\} < \{y\}$), но тада мора бити $[x] < [y] < [x+1] = [x]+1$, што наравно није могуће.

15. Претпоставимо да такви скупови постоје и формирајмо скуп $A = \{x_0, x_1, \ldots\}$. Овај скуп постоји према Аксиоми замене (зашто?). Према Аксиоми доброг заснивања мора постојати елемент у том скупу који је дисјунктан са њим. Но, $x_{i+1} \in x_i \cap A$ за све $i \in \mathbb{N}$, те таквог елемента нема. Закључујемо да скупови са наведеним својством не могу постојати.

16. Нека је посет P добро уређен. Претпоставимо да постоји бесконачни опадајући низ $x_0 > x_1 > \cdots > x_n > \cdots$ у том посету. Формирајмо скуп $A = \{x_0, x_1, \ldots, x_n, \ldots\}$. То је непразан подскуп у P, те како је P добро уређен, A има најмањи елемент. Нека је то x_k. То значи да је за све $n \in \mathbb{N}$ испуњено $x_k \leq x_n$. Но, низ (x_n) је опадајући, па за $n > k$ важи: $x_n < x_k$.

    Претпоставимо да не постоји бесконачни опадајући низ у посету P и нека је A непразан подскуп од P, који нема најмањи елемент. Нека је x_0 било који елемент из A. Како x_0 није најмањи елемент у A (у A по претпоставци не постоји најмањи елемент), нека x_1 било који елемент мањи од x_0. Претпоставимо да смо елементе $x_0, \ldots, x_n \in A$ изабрали тако да за њих важи $x_0 > x_1 > \cdots > x_n$. Како A нема најмањи елемент то сигурно постоји $x_{n+1} \in A$ такав да је $x_{n+1} < x_n$. На тај начин конструишемо бесконачни опадајући низ у скупу A, па тиме и у посету P.

17. Одговор је потврдан. Наиме, $\cup\mathbb{N} = \mathbb{N}$ и за тражени скуп можемо узети скуп природних бројева.

18. Нека је $x = \{a_1, \ldots, a_n\}$ коначан, непразан скуп за који је $\cup x = x$. Дакле, $a_1 \cup \cdots \cup a_n = \{a_1, \ldots, a_n\}$. Закључујемо да за сваки $i \in \{1, \ldots n\}$ постоји неки $j \in \{1, \ldots n\}$ такав да је $a_i \in a_j$. Дефинишимо функцију $f\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ са:

    $$f(i) = \min\{j \in \{1, \ldots, n\} : a_i \in a_j\}\}.$$

    Дакле, за све $i \in \{1, \ldots, n\}$ важи: $a_i \in a_{f(i)}$. Скуп $\{1, f(1), f(f(1)), \ldots\}$ је коначан, по постоје неки k и l такви да је $k < l$ и $f^k(1) = f^l(1)$, где смо са f^k означили композицију функције f са самом собом k пута. Тада добијамо:

    $$a_{f^k(1)} \in a_{f^{k+1}(1)} \in \cdots \in a_{f^l(1)} = a_{f^k(1)},$$

    а то није могуће. Закључујемо да тражени скуп не постоји.

19. Претпоставимо да такав скуп x постоји и нека је $y \in x$ произвољан елемент у x. Тада $y \in \cup(\cap x)$, те $y \in z$ за неки $z \in \cap x$. Како $z \in \cap x$, то је z у сваком елементу из x, па и у y. Дакле, постоје скупови y, z такви да $y \in z$ и $z \in y$. Знамо да такви скупове не могу постојати, те закључујемо да не постоји ни скуп x са траженим својством.

20. Задатак се ради на исти начин као и претходни — узимамо скуп $y \in x$; како је по претпоставци $x \subseteq \cup(\cap x)$, то $y \in \cup(\cap x)$ итд.

21. Како x садржи бар два елемента, то $\cup x \neq \emptyset$ (бар један елемент из x није празан скуп) и нека је $y \in \cup x$. То значи да постоји $z \in x$ такав да $y \in z$. Како је $z \in x$, а по претпоставци је $x = \cap(\cup x)$, то z припада свако елементу из $\cup x$, па је стога $z \in y$. Дакле, добили смо да постоје y, z такви да $y \in z$ и $z \in y$ што није могуће. Дакле, ни скуп x са траженим својством не постоји.

22. По претпоставци је $\cap x \neq \emptyset$, па има смисла разматрати $\cap(\cap x)$. Означимо са y скуп $\cap x$. Скуп y није празан и уколико постоји скуп x са траженим својством добијамо да постоји и скуп $y \neq \emptyset$ такав да је $\cap y = y$. Покажимо да такав скуп не може постојати. У супротном, нека је z произвољан елемент из y. Тада, како је $\cap y = y$, z припада сваком елементу из y, па тиме и самом z. Добијамо да постоји z такав да $z \in z$, што је немогуће.

23. Приметимо најпре да је унија бесконачно много различитих скупова бесконачан скуп. Наиме, уколико би тај скуп био коначан онда би имао бесконачно много подскупова (сви скупови из наведене уније су његови подскупови), а то није могуће. Закључујемо да ако је један од скупова x, y коначан, то мора бити и други. Нека је стога
$$x = \{a_1, \ldots, a_m\} \text{ и } y = \{b_1, \ldots, b_n\}.$$
По претпоставци је
$$a_1 \cup \cdots \cup a_m = \{b_1, \ldots, b_n\} \text{ и } b_1 \cup \cdots \cup b_n = \{a_1, \ldots, a_m\}.$$
Стога, као и у задатку 16. постоје функције $f\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ и $g\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ тако да је $a_i \in b_{f(i)}$ и $b_j \in a_{g(j)}$ за све могуће вредности индекса i и j. Добијамо низ
$$a_1 \in b_{f(1)} \in a_{g(f(1))} \in b_{f(g(f(1)))} \in \cdots$$
Даље поступамо као у том задатку.

24. (a) Приметимо да треба доказати само један смер еквиваленције. Други је тривијално тачан. У ту сврху, претпоставимо да је скуп X коначан и да је $f\colon X \longrightarrow X$ једна „1–1“ функција. Тада постоји бијекција између скупа X и његовог подскупа $f[X]$.

Како је показано да коначан скуп никада није у бијекцији са неким својим *правим* подскупом, то мора бити $f[X] = X$, те је f и „на“.

(б) Како је скуп X коначан то је он у бијекцији са неким природним бројем и без губитка општости можемо претпоставити да је $X = n$ за неки природан број n. Ако је функција $f\colon X \longrightarrow X$ „на“, можемо дефинисати функцију $g\colon X \longrightarrow X$, која је „1–1“ са: $g(x) = \min f^{-1}[\{x\}]$. Према претходном је g бијекција. Но, за g и f важи: $f \circ g = \mathrm{id}_X$. Како је g бијекција то је $f = g^{-1}$ и сама бијекција.

25. Нека је $x \in X$ произвољно. Из једнакости $f(f(x)) = f(x)$ и чињенице да је f „1–1“ добијамо да је $f(x) = x$. Како је то тачно за све $x \in X$, добијамо да је f заправо идентична функција, а тиме наравно и бијекција.

26. Приметимо да из чињенице да је $f \circ g \circ f$ „1–1“ добијамо да је f такође „1–1“, док из чињенице да је $g \circ f \circ g$ „на“ добијамо да је и g „на“. Но, општи резултати нам не дају ништа више. То, наравно не значи да тражено тврђење није тачно, можда нам треба мало више рада да бисмо га доказали, али ипак указује да треба потражити контрапример. Њега заправо није тешко наћи. Нека је $X = \mathbb{N}$, а функције f и g дефинисане са

$$g(x) = \begin{cases} 0, & x = 0 \\ x - 1, & x > 0 \end{cases}$$

док је $f(x) = x + 1$. Видимо да функција f јесте „1–1“, али није „на“, док функција g јесте „на“, али није „1–1“. Приметимо да је $g \circ f = i_{\mathbb{N}}$. Одатле добијамо да је $f \circ g \circ f = f$, те та композиција јесте „1–1“, док је $g \circ f \circ g = g$, те је ова композиција „на“, али функције f и g ипак нису бијекције. Закључујемо да тражено тврђење није тачно.

27. Не следи. Из чињенице да је $g \circ f \circ g \circ f = g \circ f$ и да је g „1–1“ добијамо да је $f \circ g \circ f = f$. Из овог резултата и чињенице да је f „на“ добијамо да је $f \circ g = \mathrm{id}_{\mathbb{N}}$. Но, из овога можемо само добити да је g „1–1“, а f „на“, а то већ знамо. Ова анализа нас упућује на то да потражимо контрапример. Уколико погледамо решење претходног задатка видимо да нам оно даје тражени контрапример, једино што ће нам у овом случају за функцију f послужити функција g из претходног задатка, а за функцију g функција f!

28. Ако мало изанализирамо ситуацију, видимо да се лако може доћи до закључка да је f „1–1“, h „на“ и g бијекција. То нас може

упутити на то да потражимо контрапример. Како смо показали да g *мора* бити бијекција, а идентична функција је најједноставнија бијекција, то проверимо шта се добија у случају да је g идентитет. Наша два услова се своде само на један: $h \circ f$ је бијекција. Сада погледајте претходне примере и нађите контрапример.

29. Претпоставимо да f није „1–1“. Дакле, постоје елементи $x_1, x_2 \in X$ такви да је $x_1 \neq x_2$ и $f(x_1) = f(x_2)$. Како искористити дате податке? Па, то заиста не би требало да буде тешко. Видимо да би нам било корисно да имамо два двочлана подскупа са наведеним својством. Са друге стране, скуп X има бар три елемента. Када се о томе мало размисли, јасно је шта треба чинити. Нека је x_3 било који елемент скупа X који је различит од x_1 и x_2. Такав постоји пошто X садржи бар три елемента. Посматрајмо двочлане подскупове A и B скупа X задате са: $A = \{x_1, x_3\}$ и $B = \{x_2, x_3\}$. Добијамо
$$f[A] = \{f(x_1), f(x_3)\} = \{f(x_2), f(x_3)\} = f[B].$$
Но, тада мора бити $A = B$, а то није тачно. Закључујемо да f мора бити „1–1“.

30. Доказаћемо да је f „на“. Нека је $y \in Y$ произвољан. Посматрајмо непразан скуп $B = \{y\} \subseteq Y$. По претпоставци задатка, постоји $A \subseteq X$ такав да је $f[A] \cap B \neq \emptyset$. Но, како је $B = \{y\}$, то значи да тај y мора бити у $f[A]$, односно он је слика неког елемента из A при функцији f. Према томе, сваки елемент из Y је слика неког из X при f, а то управо значи да је f „на“.

31. Одговор је потврдан. Нека $x \in A \cap f^{-1}[C]$. Тада $x \in A$ и $x \in f^{-1}[C]$, тј. $f(x) \in C$. Но, по претпоставци $f[A] \subseteq B \setminus C$, па ниједан елемент из $f[A]$, а такав је $f(x)$, не припада C. Закључујемо да је скуп $A \cap f^{-1}[C]$ празан.

32. $\Rightarrow$: Нека је f „на“. Подсетимо се да је $f^{-1}[A] \setminus f^{-1}[B] = f^{-1}[A \setminus B]$ (ово важи, чак и ако f није „на“). Такође је $f[f^{-1}[A \setminus B]] = A \setminus B$ јер је f „на“.

    $\Leftarrow$: Ако за скуп B узмемо празан скуп, онда се наведени услов своди на $f[f^{-1}[A]] = A$, а то је добро познати услов из кога следи да је наведена функција f „на“.

33. $\Rightarrow$: Нека је f „1–1“ и $g_1, g_2 : Z \to X$ функције за које важи: $f \circ g_1 = f \circ g_2$. Дијаграм који је погодан за разматрање овог проблема је следећи
$$Z \xrightarrow{g_1, g_2} X \xrightarrow{f} Y.$$
Нека је $z \in Z$ било који елемент. Тада је $f(g_1(z)) = (f \circ g_1)(z) = (f \circ g_2)(z) = f(g_2(z))$. Како је f по претпоставци „1–1“ добијамо

да мора бити $g_1(z) = g_2(z)$. Како ово важи за свако $z \in Z$, то закључујемо да је $g_1 = g_2$.

$\Leftarrow$: Нека су $x_1, x_2 \in X$ такви да је $f(x_1) = f(x_2)$. За скуп Z узмимо било који једночлан скуп, нпр. нека је $Z = \{0\}$. Функције $g_1, g_2 : Z \to X$ дефинишимо са $g_i(0) = x_i$. Тада је $f \circ g_1 = f \circ g_2$ (поклапају се на јединем елементу домена), па из услова задатка добијамо да мора бити $g_1 = g_2$. Тада је $x_1 = g_1(0) = g_2(0) = x_2$ и закључујемо да је функција f „1–1“.

34. $\Rightarrow$: Нека је f „на“ и $g_1, g_2 : Y \to Z$ функције за које важи: $g_1 \circ f = g_2 \circ f$. Ако је $y \in Y$, онда, на основу претпоставке да је f „на“, следи да постоји $x \in X$ тако да је $y = f(x)$. Но, тада је

$$g_1(y) = g_1(f(x)) = (g_1 \circ f)(x) = (g_2 \circ f)(x) = g_2(f(x)) = g_2(y).$$

$\Leftarrow$: Претпоставимо да f није „на“. Тада постоји $y_0 \in Y$, које није у слици од f. Нека је $Z = \{0, 1\}$ и нека су функције $g_1, g_2 : Y \to Z$ задате на следећи начин:

$$g_1(y) = 0, \text{ за све } y \in Y; \quad g_2(y) = \begin{cases} 0, & y \neq y_0 \\ 1, & y = y_0. \end{cases}$$

Очигледно је да је $g_1 \circ f = g_2 \circ f$, док је $g_1 \neq g_2$.

35. Посматрајмо уређени пар $(m, n) \in \mathbb{N} \times \mathbb{N}$. По дефиницији уређеног пара $(m, n) = \{m, \{m, n\}\}$. Но, $\{m, n\} \in \mathcal{P}_{\text{fin}}(\mathbb{N})$ и стога $(m, n) \in \mathcal{P}_{\text{fin}}(\mathcal{P}_{\text{fin}}(\mathbb{N}))$, те је доказана наведена инклузија. Но, скуп $\mathcal{P}_{\text{fin}}(\mathbb{N})$ је пребројив — бијекција је дата са $f(\{m_1, m_2, \ldots, m_n\}) = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_n}$, $f(\emptyset) = 0$. На исти начин се добија да је и скуп $\mathcal{P}_{\text{fin}}(A)$ пребројив за сваки пребројив скуп A, па закључујемо да скуп $\mathbb{N} \times \mathbb{N}$ мора бити највише пребројив. Како он није коначан, то мора бити пребројив.

36. Овај задатак није тежак. Разбијмо скуп $\mathcal{S}$ на следећи начин

$$\mathcal{S} = (\mathcal{S} \cap \mathbb{Q}) \sqcup (\mathcal{S} \cap \mathbb{Q}^c).$$

Како је скуп $\mathcal{S}$ непребројив по претпоставци, скуп $\mathcal{S} \cap \mathbb{Q}$ највише пребројив, као подскуп пребројивог, а унија дисјунктна, то скуп $\mathcal{S} \cap \mathbb{Q}^c$ мора бити непребројив.

37. Нека је M било која тачка у равни. Скуп $\{d(M, S) : S \in \mathcal{S}\}$, где је са $d(M, S)$ означено растојање између тачака M и S, је највише пребројив. Како је скуп позитивних реалних бројева непребројив, то постоји $r > 0$ који није у том скупу, а то управо значи да кружница са центром у тачки M и полупречника r не садржи ниједну тачку из скупа $\mathcal{S}$.

38. Нека је кружница k дата једначином $(x-a)^2+(y-b)^2 = r^2$. Довољно је да покажемо да су скупови $k\cap(\mathbb{Q}\times\mathbb{Q}^c)$ и $k\cap(\mathbb{Q}^c\times\mathbb{Q})$ пребројиви (зашто?). Због симетрије, довољно је то показати за нпр. први скуп. За било који рационалан број $q \in Q$ постоје *највише два* ирационална броја y_1 и y_2 који задовољавају једначину $(q-a)^2 + (y-b)^2 = r^2$. Стога је

$$k \cap (\mathbb{Q} \times \mathbb{Q}^c) = \cup_{r\in\mathbb{Q}}\{r\} \times A_r,$$

где је сваки A_r највише двочлан. Како пребројива унија коначних скупова овај скуп је највише пребројив.

39. За сваку тачку P са x-осе изаберимо у кружници k_P из скупа $\mathcal{K}$, која додирује x-осу у тачки P, неку тачку са рационалним координатама. Како тачака са рационалним координатама има пребројиво много, а одговарајућих кружница k_P непребројиво много, то се за неке две кружнице те тачке са рационалним координатама поклапају, а то управо значи да се те кружнице секу.

40. Скупови X и Y свих првих, односно свих других координата тачака из A су највише пребројиви. Ради једноставнијег записа претпоставимо да су пребројиви, тј. нека је $X = \{x_n : n \in \mathbb{N}\}$ и $Y = \{y_n : n \in \mathbb{N}\}$ (слично се ради уколико је један од њих коначан). Формирајмо скупове B и C на следећи начин.

$$B = \{(x_m, y_n) \in A : n \le m\}, \quad C = \{(x_m, y_n) \in A : n > m\}.$$

Јасно је да је $A = B \cup C$. Нека је $x = x_k$ нека вертикална права, која сече скуп A. Тада се у B налазе само оне тачке (x_k, y_n) са те праве за које је $n \le k$, а њих има највише $k+1$. Слично, нека је $y = y_l$ нека хоризонтална права, која сече скуп A. Тада се у C налазе само оне тачке (x_m, y_l) са те праве за које је $m < l$, а њих има највише l.

41. Јасно је да из пребројивости скупа A следи да се скуп $A\times A$ може представити у траженом облику. Доказ се изводи на исти начин као у претходном задатку.

Докажимо да из чињенице да се скуп $A \times A$ може приказати у облику уније $B \cup C$ са наведеним својствима, следи да је скуп A пребројив. Претпоставимо да то није тако, тј. нека је A непребројив. Уочимо било који пребројив подскуп $K \subset A$ и посматрајмо скуп $(A \times K) \cap C$. С једне стране, како за свако $y \in K$ постоји само коначно много $x \in A$ таквих да је $(x, y) \in C$ (на основу својства скупа C), то је тај скуп пребројива унија коначних скупова, па је стога пребројив. С друге стране, за сваки $x \in A$ постоји $y_x \in K$ тако да $(x, y_x) \in C$. Наиме, скуп свих оних $y \in K$ таквих да $(x, y) \in B$ је коначан за фиксирано x (својство скупа B). Како је K

бесконачан, то постоји $y_x \in K$ са наведеним својством. То значи да је дефинисана функција $\phi : A \to (A \times K) \cap C$ ($\phi(x) = (x, y_x)$), која је „1–1“, па закључујемо да је скуп $(A \times K) \cap C$ непребројив (по претпоставци је скуп A непребројив). Добијена контрадикција завршава доказ.

42. У тражени скуп $\mathcal{F}$ уврстићемо све праве паралелне координатним осама чији је пресек са оном другом осом рационалан број, тј. праве чије су једначине облика $x = a$, односно $y = b$, где су a, b произвољни рационални бројеви. Јасно је да тих правих има пребројиво много. Ако је ℓ произвољна права у равни, онда постоје две могућности: или је она паралелна некој од координатних оса или није. Уколико јесте, то она сече све праве из скупа $\mathcal{F}$ које су паралелне другој оси, а уколико није, то она сече *све* праве из скупа $\mathcal{F}$.

43. Претпоставимо супротно, тј. нека је скуп $\mathcal{S}$ непребројив. Посматрајмо отворене кугле са центрима у тачкама скупа $\mathcal{S}$ полупречника $\frac{1}{3}$. Јасно је да су те кугле дисјунктне, јер ако $x \in \mathrm{K}(s, \frac{1}{3}) \cap \mathrm{K}(t, \frac{1}{3})$, где су s, t различите тачке из $\mathcal{S}$, онда је
$$d(s,t) \leq d(s,x) + d(x,t) < \frac{1}{3} + \frac{1}{3} = \frac{2}{3} < 1,$$
а то противречи претпоставци. Са друге стране, у свакој од тих кугли може се изабрати тачка са рационалним координатама (подсетимо се да је скуп свих рационалних бројева свуда густ у скупу свих реалних бројева). Но, тако изабране тачке морају бити различите за различите кугле, па би их било непребројиво много, што није могуће, јер је скуп тачака чије су све координате рационални бројеви пребројив скуп. Тако смо добили контрадикцију и закључујемо да скуп $\mathcal{S}$ мора бити највише пребројив.

44. Доказаћемо да је заправо $|C_+(\mathbb{R})| = |\mathbb{R}|$. Доказ се не разликује битно од доказа који је већ изведен у тексту и који се односи на непрекидне функције. Једина модификација је у томе што формирамо опадајуће низове рационалних бројева који конвергирају ирационалним бројевима. Ово је могуће учинити, јер су рационални свуда густи у $\mathbb{R}$, а корисно је, јер радимо са функцијама које су непрекидне са десне стране. Остатак доказа се спроводи на исти начин као и у тексту.

45. Претпоставимо да је функција f нпр. растућа (доказ се на исти начин изводи и у случају да је функција опадајућа). Ако са $f(x+0)$ и $f(x-0)$ означимо десни односно леви лимес функције f у тачки x то, како је функција растућа, добијамо $f(x-0) = \sup_{z<x} f(z)$ и $f(x+0) = \inf_{z>x} f(z)$. Из овога изводимо две чињенице. Прво: $f(x-0) \leq f(x) \leq f(x+0)$, а друго да је за $x < y$ испуњено да

је $f(x+0) \leq f(y-0)$. Ова друга чињеница се доказује низом неједнакости

$$f(x+0) = \inf_{z>x} f(z) \leq \inf_{x<z<y} f(z) \leq \sup_{x<z<y} f(z) \leq \sup_{z<y} f(z) = f(y-0),$$

а нека се читалац сам убеди у важење прве. Дакле, функција f је прекидна у тачки x **акко** је $f(x-0) < f(x+0)$, тј. $(f(x-0), f(x+0)) \neq \emptyset$. Ако са $\mathcal{D}(f)$ означимо скуп тачака прекида функције f то можемо дефинисати једно „1–1" пресликавање $\Phi\colon \mathcal{D}(f) \to \mathbb{Q}$ на следећи начин. Нека је x тачка прекида; тада из чињенице да је интервал $(f(x-0), f(x+0))$ непразан и чињенице да су рационални бројеви свуда густи у скупу реалних бројева, добијамо да постоји неки рационалан број $\Phi(x) \in (f(x-0), f(x+0))$. Према горе доказаном резултату, ако су $x < y$ тачке прекида, то су одговарајући интервали дисјунктни, па је $\Phi(x) \neq \Phi(y)$. Но, како је $\Phi\colon \mathcal{D}(f) \to \mathbb{Q}$ „1–1", то скуп $\mathcal{D}(f)$ мора бити највише пребројив.

46. Претпоставимо да бесконачни скуп са наведеним својством постоји и означимо га са S. Нека је (m_0, n_0) било који елемент из S. За сваки елемент $(m,n) \in S$, различит од (m_0, n_0), важи: $m < m_0 \wedge n > n_0$ или $m > m_0 \wedge n < n_0$, јер су елементи $(m_0, n_0), (m,n)$ неупоредиви. Како је скуп S бесконачан то постоји бесконачно много елемената из S који задовољавају први услов или постоји бесконачно много елемената из S који задовољавају други услов Претпоставимо да их има бесконачно много који задовољавају други услов и означимо тај скуп са S_1, тј.

$$S_1 := \{(m,n) |\, m > m_0 \wedge n < n_0\}.$$

Сада понављамо поступак: бирамо било који елемент $(m_1, n_1) \in S_1$. За било који други елемент $(m,n) \in S_1$ важи $m < m_1 \wedge n > n_1$ или $m > m_1 \wedge n < n_1$. Скуп S_1 је бесконачан, па као и раније добијамо да има бесконачно много његових елемената који испуњавају први услов или бесконачно много његових елемената који испуњавају други услов. Но, да ли може бити бесконачно много елемената који испуњавају први услов? Наиме, не радимо са било којим елементима него са елементима из S_1. Сваки елемент $(m,n) \in S_1$ који испуњава први услов заправо мора бити такав да је $m_0 < m < m_1$ и $n_1 < n < n_0$ (погледајте дефиницију скупа S_1). Но, таквих елемената има само коначно много. Према томе скуп

$$S_2 := \{(m,n) \in S_1 |\, m > m_1 \wedge n < n_1\}$$

је бесконачан. Понављањем поступка видимо да заправо конструишемо низ скупова S_k и низ (m_k, n_k) за који је низ n_k строго опадајући низ природних бројева! Узвичник је наравно стављен због тога што такав низ не моше постојати. Закључујемо да и бесконачан скуп S такође не може постојати.

Како стоји ствар са $\mathbb{Z}\times\mathbb{Z}$? Ако погледамо претходни доказ видимо да кључну улогу игра низ парова у којима прва компонента расте, а друга опада. Но, у $\mathbb{Z}\times\mathbb{Z}$ није тешко конструисати такав низ. Заправо је скуп $T = \{(m,-m) | \, m \in \mathbb{Z}\}$ пример бесконачног скупа са неупоредивим елементима.

47. Позиција скакача је задата паром координата (a,b), а скок је такође задат паром (p,q). Дакле, ако се скакач у датом тренутку налази на позицији (a,b), онда се после једне секунде налази на позицији $(a+p, b+q)$. Сви ови бројеви су цели бројеви и кретање скакача је потпуно одређено четворком (a,b,p,q) (сетимо се физике — кретање је потпуно одређено вектором положаја и вектором брзине). Овде, дакле, имамо пример тзв. дискретног динамичког система. У сваком случају, скуп свих могућих кретања скакача је задат скупом $S = \mathbb{Z}^4 = \{(a_n, b_n, p_n, q_n) : n \in \mathbb{N}\}$ (скуп S је пребројив те смо његове чланове поређали у низ). Уколико је кретање скакача задато четворком $(a_{n_0}, b_{n_0}, p_{n_0}, q_{n_0})$, онда се после k минута скакач налази на позицији $(a_{n_0}+60kp_{n_0}, b_{n_0}+60kq_{n_0})$. Ми у i-том минуту означавамо тачку $(a_i + 60ip_i, b_i + 60iq_i)$. У n_0-том минуту ћемо „погодити“ скакача.

48. Претпоставимо да постоји скуп правих $\mathcal{L}$ тако да $\cup\mathcal{L} = \mathbb{R}^2$ и да је $|\mathcal{L}| < \mathfrak{c}$. Тада сигурно постоји права p, која није паралелна ниједној од правих из $\mathcal{L}$ (зашто?). Како та права сече сваку од правих из $\mathcal{L}$ у једној тачки, то је $|p \cap (\cup\mathcal{L})| \leq |\mathcal{L}| < \mathfrak{c}$, но то противречи претпоставци да је $\cup\mathcal{L} = \mathbb{R}^2$ (знамо да је $|p| = \mathfrak{c}$).

49. Претпоставимо да је $\mathbb{R} = \cup_{n\in\mathbb{N}} A_n$ при чему је $|A_n| < |\mathbb{R}|$. Знамо да је $|\mathbb{R}^{\mathbb{N}}| = \mathfrak{c}$ $(|\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|)$. То значи да постоје и скупови A_n^* такви да је $\mathbb{R}^{\mathbb{N}} = \cup_{n\in\mathbb{N}} A_n^*$ при чему је $|A_n^*| < \mathfrak{c}$. Нека је $\tilde{A}_n$ пројекција скупа A_n^* на n-ту координату, тј. $\tilde{A}_n$ је скуп свих $a \in \mathbb{R}$ за које постоји низ $(a_k) \in \mathbb{R}^{\mathbb{N}}$ који се налази у A_n^* и такав да је $a = a_n$. Како је $|A_n^*| < \mathfrak{c}$, то је и $|\tilde{A}_n| < \mathfrak{c}$, па постоји $x_n \in \mathbb{R} \setminus \tilde{A}_n$. Тада је јасно да низ (x_n), овако изабраних тачака, не припада унији $\cup_{n\in\mathbb{N}} A_n^*$, која је по претпоставци једнака $\mathbb{R}^{\mathbb{N}}$. Наиме, ако $(x_n) \in A_k^*$, онда $x_k \in \tilde{A}_k$, а x_k је тако изабран да *не* припада $\tilde{A}_k$.

50. Претпоставимо да свака вертикална права сече скуп A^c по скупу кардиналности мање од $\mathfrak{c}$. Посматрајмо вертикалне праве $x = n$, где $n \in \mathbb{N}$ и нека је њихова унија V. На основу претходног задатка, $|V \cap A^c| < \mathfrak{c}$ (скуп кардиналности $\mathfrak{c}$ не може бити унија пребројиво много скупова мање кардиналности). Ако је $y_0 \in \mathbb{R}$ произвољан број, онда је скуп $\{(n, y_0) : n \in \mathbb{N}\}$ бесконачан скуп, а како свака хоризонтална права има само коначно много тачака из A, то за бесконачно много $n \in \mathbb{N}$, $(n, y_0) \in A^c$. Другим речима, свака хоризонтална права сече скуп $V \cap A^c$, па закључујемо да је $|V \cap A^c| \geq \mathfrak{c}$.

51. За реалан број $x \in (0,1)$ нека је $A_x = \{[10x], [10^2 x], \ldots, [10^n x], \ldots\}$. Нпр. ако је $x = \pi/10$, онда је $A_x = \{3, 31, 314, 3141, 31415, \ldots\}$. Јасно је да два различита броја x и y имају различите децималне записе, па је пресек скупова A_x и A_y коначан скуп.

52. Нека је A_1 скуп свих $a \in A$ за које постоји $\delta_a > 0$ такав да је $(a, a+\delta_a) \cap A = \emptyset$, док је A_2 скуп свих оних елемената $a \in A$ за које постоји $\delta_a > 0$ тако да је $(a - \delta_a, a) \cap A = \emptyset$. Покажимо да је скуп A_1 пребројив. Наиме, ако су a и b два различита елемента из A_1, онда је $(a, a+\delta_a) \cap (b, b+\delta_b) = \emptyset$ ($b \notin (a, a+\delta_a)$, па се ови интервали не могу сећи). Но, свака колекција дисјунктних интервала у $\mathbb{R}$ нужно је пребројива (сваки од њих садржи неки рационалан број, а како су они дисјунктни то садрже различите рационалне бројеве) те закључујемо да је скуп A_1 пребројив. На аналогни начин се показује да је и скуп A_2 пребројив, а како је $A = A_1 \cup A_2$, то тражени резултат следи.

53. Како је A непребројив, то на основу претходног задатка закључујемо да постоји $a \in A$ тако да је $(a, a+\delta) \cap A \neq \emptyset$ за све $\delta > 0$. Сада је лако конструисати строго опадајући низ тачака из A који конвергира ка a. За a_0 узмимо било који елемент из $(a, a+1) \cap A$. За a_1 узмимо било који елемент из $(a, \min\{a_0, a+1/2\}) \cap A$. Ако су $a_0, \ldots, a_n$ изабрани, онда за a_{n+1} узимамо било који елемент из скупа $(a, a+\min\{a_n, a_0+1/(n+1)\}) \cap A$. Добили смо опадајући низ (a_n), који конвергира ка a ($a < a_n < a + 1/(n+1)$).

54. Погледати 16. задатак и претходни задатак.

4.3 Задаци из треће главе

1. Посматрајмо $\mathbb{R}$ као векторски простор над пољем $\mathbb{Q}$. Како сваки векторски простор има базу, то и $\mathbb{R}$, као векторски простор над $\mathbb{Q}$, има базу. Нека је α било који базни елемент. Дефинишимо $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ са $f(x) = \alpha$-та координата вектора x. Јасно је да важи $f(x+y) = f(x) + f(y)$. Такође је $f(\alpha) = 1$, а f не може бити множење константом пошто је $f(x)$ рационалан број за све x ($\mathbb{R}$ смо посматрали као векторски простор над $\mathbb{Q}$ те су стога координате сваког вектора рационални бројеви). Наиме, ако би било $f(x) = ax$ за све $x \in \mathbb{R}$ и неко a, онда бисмо добили $f(\frac{1}{a}\sqrt{2}) = \sqrt{2} \notin \mathbb{Q}$ ($a \neq 0$, јер смо видели да је $f(\alpha) = 1$).

2. Нека је B било која база за $\mathbb{R}$ над $\mathbb{Q}$ и нека је $|B| = \kappa$. Уочимо скуп $\mathcal{B} = \bigcup_{n \in \mathbb{N}\setminus\{0\}} \mathbb{Q}^n \times B^n$. Дефинишимо функцију $f\colon \mathcal{B} \to \mathbb{R}$ са:

$$f((r_1, \ldots, r_n), (b_1 \ldots, b_n)) := r_1 b_1 + \cdots r_n b_n.$$

Како је B база за $\mathbb{R}$ над $\mathbb{Q}$, то f мора бити „на“. Но, $|\mathcal{B}| = \kappa$ (уверите се у то!), те закључујемо да је $\mathfrak{c} \leq \kappa$. Како је обратна неједнакост тривијално задовољена (зашто?), то добијамо $\kappa = \mathfrak{c}$, што се и тражило.

3. У претходном задатку смо добили да је кардиналност базе за $\mathbb{R}$ над $\mathbb{Q}$ баш $\mathfrak{c}$. Но, базу за $\mathbb{R} \oplus \mathbb{R}$ чине елементи облика (b', b''), где b', b'' припадају некој бази B за $\mathbb{R}$ над $\mathbb{Q}$. Кардиналност овог скупа је $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$. Но, ако су дата два векторска простора над истим пољем са базама исте кардиналности они морају бити изоморфни (бијекција на базама се на јединствен начин продужује до изоморфизма векторских простора — као и у случају простора коначне димензије). Стога су $\mathbb{R}$ и $\mathbb{R} \oplus \mathbb{R}$ изоморфни као векторски простори (над $\mathbb{Q}$), а тиме и као Абелове групе.

   <u>Напомена</u>: $\mathbb{R} \oplus \mathbb{R} \cong \mathbb{R} \times \mathbb{R}$ (изоморфизам векторских простора над $\mathbb{Q}$).

4. Доказ ове еквиваленције није тежак. Претпоставимо најпре да је M ординал и $x \in M$. По дефиницији ординала мора бити $x = M_x$, па је заиста $x \subset M$. Да је ординал линеарно уређен релацијом $\in$ већ смо показали у тексту.

   За доказ другог смера еквиваленције, претпоставимо да је M транзитиван скуп који је линеарно уређен релацијом $\in$. Да бисмо показали да је M ординал, прво треба да докажемо да је M добро уређен релацијом $\in$ (наравно, којом би другом?). Нека је A непразан подскуп од M, који нема најмањи елемент и x_0 произвољан елемент из A. Како A нема најмањи елемент, то постоји $x_1 \in A$ такав да $x_1 \in x_0$. Ни x_1 није најмањи елемент у A (по претпоставци нема таквог!), па постоји $x_2 \in A$ такав да је $x_2 \in x_1$. На тај начин конструишемо низ скупова (x_n) такав да је $x_{n+1} \in x_n$ за све $n \in \mathbb{N}$. Но, видели смо да такав низ скупова не може постојати (у ком задатку је то урађено?). Закључујемо да је M добро уређен. Остаје да се провери да је $M_x = x$. Но, то је тривијално тачно! Наиме, релација поретка на M је релација $\in$, па треба „проверити“ да за сваки скуп $y \in M$ важи: $y \in x \iff y \in x$.

   На самом крају, једна кратка напомена. Можда сте се запитали зашто се за скуп каже да је транзитиван уколико је испуњен наведени услов. Разлог је једноставан — ако је наведени услов испуњен, онда је релација $\in$ на том скупу транзитивна! Релација $\subset$ увек је транзитивна, али наравно да релација $\in$ не мора бити.

5. Приметимо најпре да је за сваки скуп M испуњено да је $M \subseteq \bigcup(M \cup \{M\})$. Обратна инклузија је она која нас интересује.

   $\Longrightarrow$: Претпоставимо да је скуп M транзитиван и да $x \in \bigcup(M \cup \{M\})$. Дакле, постоји неки скуп A такав да $x \in A \in M \cup \{M\}$. Ако је $A = M$ онда је све јасно. Остаје могућност да $A \in M$. Но, тада добијамо $x \in A \in M$, те из транзитивности скупа закључујемо да $x \in M$.

$\Longleftarrow$: Нека је за скуп M испуњено $M = \bigcup(M \cup \{M\})$ и нека $x \in M$. Ако $a \in x$, онда добијамо да $a \in x \in M \cup \{M\}$, па по дефиницији уније закључујемо да $a \in \bigcup(M \cup \{M\})$. Но, из претпоставке добијамо да то значи да $a \in M$, те закључујемо да је $x \subset M$ (јасно је да је $x \neq M$, јер $x \notin x$).

6. Погледајмо најпре доказ који је спроведен у главном тексту и који се тиче ординала ω^2. Нека је $\gamma < \omega^2 = \omega \cdot \omega$. Користећи став о дељењу са остатком добијамо да је $\gamma = \omega \cdot m + n$, где су $m, n < \omega$. Сада се уређајни изоморфизам између ω^2 и скупа S у тексту остварује са $f(\gamma) = m + 1 - \frac{1}{n+2}$. Приметимо да се у тексту наводи да је $m \geq 1$ и $n \geq 2$, но m у овом доказу је из ω, тј. $m \geq 0$. Тада је $m + 1 \geq 1$, а слично важи и за n. Анализирајмо још мало шта смо добили. Посматрајмо нпр. бројеве 2 и 3. Идеја је да се између 2 и 3 „уметне“ још један скуп изоморфан ω (као уосталом и између било која друга два природна броја!). Ми смо убацили бројеве облика $3 - \frac{1}{n}$, где смо захтевали да је $n \geq 2$ из очигледног разлога (не желимо да се деси да је $3 - \frac{1}{n} \leq 2$. Дакле

$$2 < 3 - \frac{1}{2} < 3 - \frac{1}{3} < 3 - \frac{1}{4} < \cdots < 3.$$

Ако желимо да добијемо скуп изоморфан са ω^3, морамо између свака два узастопна елемента из S убацити још један скуп уређајно изоморфан ω. Нека су узастопни елементи $m - \frac{1}{n}$ и $m - \frac{1}{n+1}$. Њихова разлика је једнака $\frac{1}{n(n+1)}$. Сада је јасно шта треба урадити. Посматрајмо скуп $T \subset \mathbb{Q}$ задат са

$$T \stackrel{\mathrm{def}}{=} \{m - \frac{1}{n} - \frac{1}{n(n+1)p} : m \geq 1, n \geq 2, p \geq 2\}.$$

Читаоцима остављамо да докажу да је T изоморфан ω^3. Не би требало да буде тешко да се на сличан начин добије подскуп од $\mathbb{Q}$ изоморфан ω^k, за $k \in \omega$. Но, $\omega^\omega = \cup_{k \in \omega} \omega^k$.

7. Нека је $\alpha = \omega$, $\beta = \omega + 1$, $\gamma = \omega$. Тада је $\alpha \neq \beta$, но

$$\alpha + \gamma = \omega + \omega = \omega + (1 + \omega) = (\omega + 1) + \omega = \beta + \gamma.$$

8. Доказаћемо наведени резултат индукцијом по ординалу β. Како се примењује индукција по ординалима? Присетимо се наведеног у тексту. . Ако је $\beta = 0$ тражена неједнакост је испуњена. Сада још треба да докажемо да ако је тврђење тачно за ординал β тачно је и за следећи ординал, $\beta + 1$ и у случају да је β гранични треба показати да из претпоставке да је тврђење тачно за сваки ординал мањи од β, то важи и за β.

Урадимо најпре први случај. Како је неједнакост испуњена за β то је $\alpha^\beta \geq \alpha \cdot \beta$. Но, $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$ по дефиницији степена ординала.

Одавде, коришћењем једног резултата из текста (којег тачно?), добијамо да је $\alpha^{\beta+1} \geq \alpha \cdot \beta \cdot \alpha$. Сада видимо да би било корисно да имамо следећи резултат: $\alpha > 1, \beta > 1 \Rightarrow \alpha \cdot \beta \geq \alpha + \beta$. Докажите то индукцијом по β. Користећи тај резултат добијамо

$$\alpha^{\beta+1} \geq \alpha \cdot \beta + \alpha = \alpha \cdot \beta + \alpha \cdot 1 = \alpha \cdot (\beta + 1).$$

Ситуација са граничним ординалом је заправо једноставнија. Нека је β гранични и претпоставимо да за сваки $\gamma < \beta$ важи $\alpha^\gamma \geq \alpha \cdot \gamma$. Тада је и

$$\bigcup_{\gamma<\beta} \alpha^\gamma \geq \bigcup_{\gamma<\beta} \alpha \cdot \gamma,$$

односно (подсетите се дефиниције производа и степена у случају граничних ординала) $\alpha^\beta \geq \alpha \cdot \beta$.

9. Наравно да наведена једнакост не може бити испуњена за коначан ординал α. Нека је, у даљем, $\alpha \geq \omega$. Присетимо се да је $1+\omega = \omega$. Овај резултат можемо да искористимо. Наиме, како је $\alpha \geq \omega$, то постоји ординал β такав да је $\omega + \beta = \alpha$. Тада је

$$1 + \alpha = 1 + (\omega + \beta) = (1 + \omega) + \beta = \omega + \beta = \alpha.$$

Према томе, једнакост је испуњена ако и само ако је $\alpha \geq \omega$.

10. $\Longrightarrow$: Претпоставимо да је $\alpha + \beta = \beta$. Индукцијом се непосредно доказује да је тада и $\alpha \cdot n + \beta = \beta$ за све природне бројеве n (изведите сами овај доказ). Но, тада добијамо да је за сваки $n \in \mathbb{N}$ испуњено: $\alpha \cdot n \leq \beta$. Но, ако се подсетимо дефиниције множења ординала, из овог резултата се непосредно закључује да је $\alpha \cdot \omega \leq \beta$.

$\Longleftarrow$: Како је $\alpha \cdot \omega \leq \beta$, то постоји ординал γ такав да је $\beta = \alpha \cdot \omega + \gamma$. Тада је

$$\alpha + \beta = \alpha + (\alpha \cdot \omega + \gamma) = (\alpha + \alpha \cdot \omega) + \gamma = \alpha \cdot (1 + \omega) + \gamma = \alpha \cdot \omega + \gamma = \beta.$$

11. Из једнакости $\alpha \cdot \beta = \beta$ индукцијом доказујемо да је за све $n \in \mathbb{N}$ испуњено $\alpha^n \cdot \beta = \beta$ (урадите то!). Но, одавде следи да је за све $n \in \mathbb{N}$: $\alpha^n \leq \beta$. Дакле, тражени ординал мора бити већи од свих α^n. Уколико је $\alpha < \omega$, добијамо да је $\beta = \omega$. У случају $\alpha \geq \omega$ показаћемо да је $\beta = 1 + \alpha + \alpha^2 + \cdots$ тражени ординал (прецизније: $\beta = \sup_{n \geq 1}(1 + \alpha + \cdots + \alpha^n)$). Јасно је да тражени ординал не може бити мањи од овог — докажите ово користећи оно што смо до сада доказали. Но,

$$\alpha \cdot (1 + \alpha + \cdots) = \alpha \cdot 1 + \alpha \cdot \alpha + \cdots = \alpha + \alpha^2 + \cdots = 1 + \alpha + \alpha^2 + \cdots = \beta.$$

Напомена: $\alpha^n \cdot \alpha^\omega = \alpha^{n+\omega} = \alpha^\omega$, па је $\beta \leq \alpha^\omega$ и наведени супремум сигурно постоји ($1 + \alpha + \cdots + \alpha^n < \alpha^\omega$).

12. (а) Пре свега, $2 \cdot (\omega + 1) = 2 \cdot \omega + 2 \cdot 1 = \omega + 2$. Но, $(\omega + 1) \cdot 2 = (\omega+1) \cdot (1+1) = (\omega+1) + (\omega+1) = \omega+\omega+1$. Видимо да је овај ординал већи од претходног.

(б) За први ординал добијамо $\omega \cdot (\omega+1) = \omega^2 + \omega$. Да бисмо други ординал упоредили са овим докажите најпре (индукцијом) да је $(\omega + 1) \cdot n = \omega \cdot n + 1$. Одавде добијамо неједнакости

$$\omega \cdot n \leq (\omega + 1) \cdot n \leq \omega \cdot (n + 1).$$

Уколико применимо унију по свим $n \in \mathbb{N}$ и подсетимо се дефиниције производа ординала добијамо да је $(\omega+1) \cdot \omega = \omega^2$. Дакле, први ординал је већи.

13. (а) Јасно је да мора бити $\alpha = 0$, пошто је у противном $\omega + \alpha > \omega$.

(б) Знамо да је за сваки $n \in \mathbb{N}$ испуњено $n+\omega = \omega$. Дакле, α може бити ма који коначан ординал. Уколико је α бесконачан, то постоји ординал γ такав да је $\alpha = \omega + \gamma$. Тада је $\alpha + \omega = \omega + \gamma + \omega > \omega$.

(в) Ако је $\alpha \cdot \omega = \omega$, онда је

$$\omega = \alpha \cdot \omega = \cup_{n<\omega} \alpha \cdot n.$$

Између осталог добијамо да је $\alpha \subset \omega$, па α мора бити коначан. Но, за све коначне ординале α, једнакост $\alpha \cdot \omega = \omega$ јесте испуњена.

(г) Јасно је да α не може бити 0 и да може бити 1. Уколико је $\alpha > 1$, онда је $\alpha = 2 + \beta$ за неки ординал β. Тада је $\omega \cdot \alpha = \omega \cdot (2 + \beta) = \omega \cdot 2 + \omega \cdot \beta = \omega + \omega + \omega \cdot \beta > \omega$.

(д) Јасно је да мора бити $\alpha, \beta \leq \omega$ и да је бар један од њих једнак ω. Тада резултат следи из претходних случајева.

(ђ) Као и у претходној једначини, резултат се може добити из већ разматраних једначина. Урадите то.

14. Како је $\alpha \leq \omega^2 + 1$, то постоје следеће могућности за α:

1. $\alpha = \omega^2 + 1$;
2. $\alpha = \omega^2$;
3. $\alpha = \omega \cdot n + m$, за неке $m, n \in \omega$ (сваки ординал мањи од ω^2 је овог облика — проверите зашто је ово тачно).

Тада је јасно да у првом случају мора бити $\beta = 0$, а у другом $\beta = 1$. Размотримо трећи случај. Јасно је да је $\beta \leq \omega^2 + 1$. Докажимо да заправо мора бити испуњено $\beta = \omega^2 + 1$. У супротном, нека је $\beta \leq \omega^2$. Како је $\omega + \omega^2 = \omega^2$ $(\omega + \omega^2 = \omega \cdot 1 + \omega \cdot \omega = \omega \cdot (1 + \omega) = \omega \cdot \omega = \omega^2)$, то је и $n + \omega^2 = \omega^2$ $(n+\omega^2 = n+\omega+\omega^2 = \omega+\omega^2 = \omega^2)$, па добијамо да је тада $\omega \cdot n + m + \omega^2 = \omega \cdot n + \omega \cdot \omega = \omega \cdot (n+\omega) = \omega \cdot \omega = \omega^2$.

Дакле, тада је $\omega \cdot n + m + \beta \leq \omega^2 < \omega^2 + 1$. Закључујемо да мора бити $\beta = \omega^2 + 1$.

15. Погледајте Став 3.20 и особину 13.

16. Покажимо најпре да за произвољни ординал α постоји ординал β такав да је $\alpha + \beta = \beta$. У ту сврху заправо можемо узети ординал $\alpha \cdot \omega$ (или било који ординал већи од овога). Наиме, $\alpha + \alpha \cdot \omega = \alpha \cdot 1 + \alpha \cdot \omega = \alpha \cdot (1 + \omega) = \alpha \cdot \omega$. Дакле, за тако одабрани ординал β важи да је $\beta + \alpha = \beta$ и из ове једнакости закључујемо да мора бити $\alpha = 0$.

    Напомена: Погледајте и 10. задатак.

17. Доказ се изводи индукцијом по k. Приметимо да је λ, као гранични ординал, облика $\lambda = \omega \cdot \alpha$. Стога је $n \cdot \lambda = n \cdot \omega \cdot \alpha = \omega \cdot \alpha = \lambda$.

    Уколико је $k = 1$, онда је тврђење тривијално. Претпоставимо да је тврђење тачно за k и проверимо га за $k + 1$:

    $$(\lambda \cdot n)^{k+1} = (\lambda \cdot n)^k \cdot (\lambda \cdot n) = (\lambda^k \cdot n) \cdot (\lambda \cdot n) = \lambda^k \cdot (n \cdot \lambda) \cdot n = \lambda^k \cdot \lambda \cdot n = \lambda^{k+1} \cdot n.$$

18. Докажимо најпре да је за бесконачни ординал α и природне бројеве n, m, при чему је $m \geq 1$, испуњено: $(\alpha + n) \cdot m = \alpha \cdot m + n$. Ово се једноставно доказује индукцијом по m. За $m = 1$, све је јасно. Претпоставимо да тврђење важи за m и докажимо га за $m + 1$:

    $$(\alpha + n) \cdot (m + 1) = (\alpha + n) \cdot m + (\alpha + n) = \alpha \cdot m + n + \alpha + n.$$

    Како је α бесконачан, то је $\alpha = \omega + \beta$ за неки ординал β и тада је $n + \alpha = n + \omega + \beta = \omega + \beta = \alpha$. Добијамо:

    $$(\alpha + n) \cdot (m + 1) = \alpha \cdot m + \alpha + n = \alpha \cdot (m + 1) + n.$$

    Сада није тешко показати да је $(\alpha + n) \cdot \omega = \alpha \cdot \omega$ за сваки бесконачни ординал α:

    $$\begin{aligned}(\alpha + n) \cdot \omega &= \cup_{m<\omega}(\alpha + n) \cdot m \\ &= \cup_{m\geq 1}(\alpha \cdot m + n) \\ &\subseteq \cup_{m\geq 1}(\alpha \cdot m + \alpha) \\ &= \cup_{m\geq 1}\alpha \cdot (m + 1) \\ &= \alpha \cdot \omega.\end{aligned}$$

    Ординал β можемо написати у облику $\beta = \omega \cdot \gamma + m$ за неки ординал γ и $m \in \omega$ (зашто је ово могуће урадити?). Уколико је β следбеник, тј. $m \neq 0$ добијамо:

    $$\begin{aligned}(\alpha + n) \cdot \beta &= (\alpha + n) \cdot (\omega \cdot \gamma + m) \\ &= (\alpha + n) \cdot \omega \cdot \gamma + (\alpha + n) \cdot m \\ &= \alpha \cdot \omega \cdot \gamma + \alpha \cdot m + n \\ &= \alpha \cdot (\omega \cdot \gamma + m) + n \\ &= \alpha \cdot \beta + n.\end{aligned}$$

У случају да је β гранични ординал (или 0), тј. $m = 0$, добијамо:

$$(\alpha + n) \cdot \beta = (\alpha + n) \cdot \omega \cdot \gamma = \alpha \cdot \omega \cdot \gamma = \alpha \cdot \beta.$$

19. Ординал α је облика $\alpha = \omega \cdot \gamma + k$ за неки ординал γ и $k \in \omega$. Уколико је $\beta = \omega \cdot \delta + l$ ($l \in \omega$), онда једнакост $\alpha = n \cdot \beta$ даје:

$$\omega \cdot \gamma + k = \omega \cdot \gamma + nl,$$

те мора бити $k = nl$. Закључујемо да су тражени природни бројеви заправо делиоци броја k.

20. Претпоставимо да постоји бесконачно много таквих ординала γ. То значи да постоји бесконачан строго растући низ ординала (γ_n) тако да је $\alpha = \beta_n + \gamma_n$ за неке ординале β_n. Но, тада је низ (β_n) један бесконачан строго опадајући низ ординала (како је $\gamma_n < \gamma_{n+1}$, то мора бити $\beta_n > \beta_{n+1}$ — погледајте својства ординала), а то није могуће (зашто?).

<u>Напомена:</u> Како је $\omega = n + \omega$, за $n \in \omega$, то се може десити да за дати ординал α постоји бесконачно много ординала γ за које постоји ординал β такав да је $\alpha = \gamma + \beta$.

21. Погледати претходни задатак.

22. Претпоставимо да наведена једначина има решење, тј. да постоје ординали α и β такви да је $\alpha^2 + \omega = \beta^2$. Уколико би α био коначан ординал, добили бисмо да је $\omega = \beta^2$ за неки ординал β, а јасно је да то није могуће (зашто?). Стога је $\alpha \geq \omega$. Како је $\beta^2 = \alpha^2 + \omega$, то је $\beta^2 > \alpha^2$, те следи да је $\beta > \alpha$ (видети Став 3.20). Дакле,

$$\alpha^2 + \omega = \beta^2 \geq (\alpha + 1)^2 \geq \alpha \cdot (\alpha + 1) = \alpha^2 + \alpha.$$

Дакле, мора бити $\omega \geq \alpha$, а како је α бесконачни ординал, то закључујемо да је $\alpha = \omega$. Дакле,

$$\omega^2 + \omega = \beta^2 \geq (\omega + 1)^2 = \omega^2 + \omega + 1.$$

Ова контрадикција показује да једначина нема решења.

23. Тражена решења добијамо на основу следећих једнакости:

$$(\omega \cdot n)^2 + \omega^2 = \omega^2 \cdot n + \omega^2 = \omega^2 \cdot (n + 1) = (\omega \cdot (n + 1))^2.$$

24. Како $\sqrt{2} \notin \mathbb{Q}$, то су једина решења једначине за коначне ординале α и β, дата са: $\alpha = 0, \beta = 0$. Дакле, нека су α и β бесконачни

ординали и можемо их записати у облику $\alpha = \lambda + n$, $\beta = \mu + m$, где су λ и μ гранични ординали, а $m, n \in \omega$. Тада је

$$\begin{aligned}
\alpha^2 \cdot 2 &= (\lambda + n) \cdot (\lambda + n) \cdot 2 \\
&= ((\lambda + n) \cdot \lambda + (\lambda + n) \cdot n) \cdot 2 \\
&= (\lambda \cdot \lambda + \lambda \cdot n + n) \cdot 2 \\
&= (\lambda \cdot \lambda + \lambda \cdot n) \cdot 2 + n \\
&= \lambda \cdot (\lambda + n) \cdot 2 + n \\
&= \lambda \cdot (\lambda \cdot 2 + n) + n \\
&= \lambda^2 \cdot 2 + \lambda \cdot n + n,
\end{aligned}$$

док је $\beta^2 = \mu^2 + \mu \cdot m + m$ (користили смо раније доказана својства ординала). Добијамо једнакост

$$\lambda^2 \cdot 2 + \lambda \cdot n + n = \mu^2 + \mu \cdot m + m.$$

Како су ординали λ и μ гранични, то су и ординали $\lambda^2 \cdot 2 + \lambda \cdot n, \mu^2 + \mu \cdot m$ гранични, те мора бити $n = m$. Следи да је

$$\lambda^2 \cdot 2 + \lambda \cdot n = \mu^2 + \mu \cdot n. \quad (*)$$

Очигледно је да је $\lambda \leq \mu \leq \lambda \cdot 2$. Претпоставимо да је $\mu < \lambda \cdot 2$. То значи да је $\mu = \lambda + \tau$, за неки ординал $\tau < \lambda$. Добијамо:

$$\begin{aligned}
\mu^2 + \mu \cdot n &\leq \lambda \cdot 2 \cdot (\lambda + \tau) + \lambda \cdot 2 \cdot n \\
&= \lambda \cdot 2 \cdot \lambda + \lambda \cdot 2 \cdot \tau + \lambda \cdot 2 \cdot n \\
&= \lambda \cdot \lambda + \lambda \cdot 2 \cdot (\tau + n) \\
&\leq \lambda \cdot \lambda + \lambda \cdot 2 \cdot \lambda \\
&= \lambda^2 + \lambda^2 \\
&= \lambda^2 \cdot 2.
\end{aligned}$$

Овде смо користили чињеницу да је $2 \cdot \lambda = \lambda$ за сваки гранични ординал λ (зашто је ово тачно?), као и чињеницу да из $\tau < \lambda$ следи да је за све $n \in \omega$ испуњено $\tau + n < \lambda$, пошто је λ гранични ординал. Дакле, да би једнакост $(*)$ била испуњена, мора бити $n = 0$. Добијамо да је $\lambda^2 \cdot 2 = \mu^2$, а на основу претходних резултата следи да тада мора бити $\mu = \lambda \cdot 2$. Закључујемо да су сва нетривијална решења почетне једначине дата са: $\alpha = \lambda, \beta = \lambda \cdot 2$, где је λ произвољни гранични ординал.

25. Приметимо да важи једнакост $\omega^k \cdot n = (\omega \cdot n)^k$. Стога ординали $\omega^k, \omega^k \cdot 2, \omega^k \cdot 3, \ldots$ чине тражени аритметички низ.

26. Како је $m + \omega = \omega$, за сваки $m \in \omega$ и како природни бројеви међусобно комутирају, то се свака сума наведених ординала своди

на суму $s_1 + \omega + s_2 = \omega + s_2$, где је s_1 сума свих датих природних бројева који се у наведеној суми налазе испред ω, а s_2 сума оних који се налазе „иза“. Једна од њих је потпуно одређена другом, а поредак самих природних бројева у тим сумама је небитан. Само је битно који се природних бројеви налазе „испред“, а који „иза“. Како подскупова скупа $\{1, 2, \dots, 2^n\}$ има тачно 2^n, толико има и различитих сума.

27. Докажимо да за ординале $\omega+i_1, \omega+i_2, \dots, \omega+i_n$, где су $i_1, i_2, \dots, i_n$ природни бројеви различити од 0, важи:

$$(\omega + i_1)(\omega + i_2) \cdots (\omega + i_n) = \omega^n + \omega^{n-1} \cdot i_n + \cdots + \omega \cdot i_2 + i_1.$$

Ово није тешко доказати индукцијом по n. Тврђење је тривијално за $n = 1$. Нека је оно тачно за n бројева; докажимо га за $n + 1$ бројева. Имамо:

$$(\omega+i_1)(\omega+i_2)\cdots(\omega+i_{n+1}) = (\omega+i_1)(\omega^n+\omega^{n-1}i_{n+1}+\cdots+\omega\cdot i_3+i_2),$$

на основу индуктивне хипотезе. Знамо да је $(\omega + n) \cdot \alpha = \omega \cdot \alpha + n$ у случају да је α следбеник и применом овог својства добијамо тражено.

Користећи добијени израз за горњи производ, лако се индукцијом показује да из

$$(\omega + i_1)(\omega + i_2) \cdots (\omega + i_n) = (\omega + j_1)(\omega + j_2) \cdots (\omega + j_n)$$

следи да је $(i_1, i_2, \dots, i_n) = (j_1, j_2, \dots, j_n)$. Дакле, ординали $\omega + 1, \omega + 2, \dots, \omega + n$ представљају тражене ординале.

28. Нека су $\alpha, \beta, \gamma, \delta$ било који ординали и нека је $\alpha = \beta+\gamma$. Јасно је да уколико δ слева дели β и γ, онда δ дели и α слева. Претпоставимо да δ дели α и β слева. Докажимо да δ тада слева дели и γ. Користимо дељење са остатком. Постоје ординали γ_1 и ψ такви да је $\gamma = \delta \cdot \gamma_1 + \psi$ при чему је $\psi < \delta$. Дакле важи једнакости:

$$\alpha = \delta \cdot \alpha_1; \quad \alpha = \delta \cdot (\beta_1 + \gamma_1) + \psi,$$

за неке ординале α_1 и β_1. На основу става о дељењу са остатком, ово је могуће једино уколико је $\psi = 0$.

Сада је лако показати да постоји највећи заједнички леви делилац за произвољна два ординала — овај се резултат добија применом Еуклидовог алгоритма (како?). Приметимо да се поступак мора завршити зато што не постоји бесконачан опадајући низ ординала.

За произвољни скуп ординала поступамо на следећи начин. Нека су α и β произвољна два ординала из тог скупа. Они имају највећи заједнички леви делилац δ. Уколико δ дели све остале ординале из тог скупа (наравно са леве стране), онда је он тражени највећи заједнички леви делилац. У супротном он не дели неки елемент из тог скупа и нека је δ_1 највећи заједнички леви делилац тог елемента и δ. Тада је $\delta_1 < \delta$. Поступак понављамо. Он се мора зауставити пошто не постоји бесконачан опадајући низ ординала. Последњи делилац који смо добили у овом поступку је тражени највећи заједнички леви делилац.

29. Како је $\omega^2 = (\omega+2)\cdot\omega$ и $\omega^2 = (\omega+3)\cdot\omega$, то из чињенице да ω^2 дели слева ординал α следи да су и $\omega+3$ и $\omega+2$ леви делиоци од α.

    Претпоставимо да су $\omega + 2$ и $\omega + 3$ леви делиоци од α, а да то ω^2 није. Тада је $\alpha = \omega^2 \cdot \alpha_1 + \omega \cdot n + m$ за неки ординал α_1 и неке природне бројеве m и n, који нису оба једнаки 0 (зашто ови бројеви постоје?). Добијамо да је $\omega\cdot n+m$ слева дељив и са $\omega+2$ и са $\omega+3$, те је сигурно $n \geq 1$. Како је $\omega\cdot n+m = (\omega+2)\cdot(n-1)+(\omega+m)$, то $\omega + 2$ слева дели $\omega + m$, а то је могуће једино у случају да је $m = 2$. На сличан начин, користећи $\omega + 3$, добијамо да је $m = 3$. Ова контрадикција завршава доказ.

30. Јасно је да дељивост са 6 повлачи дељивост са 2 и са 3. Размотримо обратну импликацију.

    Претпоставимо да су 2 и 3 десни делиоци ординала α, тј. да постоји ординали β, γ такви да је $\alpha = \beta\cdot 2 = \gamma\cdot 3$. Нека је δ_0 највећи заједнички леви делилац ординала β и γ. Скраћивањем слева са δ_0 добијамо да је $\beta_0 \cdot 2 = \gamma_0 \cdot 3$ за неке ординале β_0, γ_0, који немају заједничких левих делилаца. Јасно је да тврђење следи уколико је бар један од њих коначан (тада мора и други бити коначан). Претпоставимо стога да су они бесконачни и да је $\beta_0 = \lambda_0 + m_0$, $\gamma_0 = \mu_0 + n_0$ за неке граничне ординале λ_0, μ_0 и природне бројеве m_0, n_0 од којих бар један није једнак 0 (ординали β_0 и γ_0 немају заједничних левих делилаца, а сваки гранични ординал је слева дељив са ω). Добијамо $\lambda_0\cdot 2+m_0 = \mu_0\cdot 3+n_0$, те мора бити $m_0 = n_0$ и $\lambda_0\cdot 2 = \mu_0\cdot 3$. Нека је δ_1 највећи заједнички леви делилац ординала λ_0, γ_0. Скраћивањем са δ_1, добијамо да је $\beta_1 \cdot 2 = \gamma_1 \cdot 3$ за неке ординале β_1 и γ_1, који немају заједничких левих делилаца. Како је $\beta_0 = \delta_1 \cdot \beta_1 + m_0$ и $m_0 > 0$, то добијамо да је $\beta_1 < \beta_0$. Такође је и $\gamma_1 < \gamma_0$. Понављањем поступка добијамо опадајуће низове ординала (β_n) и (γ_n). Како не постоји бесконачни опадајући низ ординала, то се поступак завршава после коначно много корака, тј. после коначно много корака добијају се коначни ординали и резултат тада лако следи (завршите овај доказ — испишите шта се на крају добија).

31. Задатак се ради аналогно претходном задатку.

32. Како је $n^\omega = \bigcup_{k<\omega} n^k = \omega$, то је $n^{\omega^k} = n^{\omega\cdot\omega^{k-1}} = (n^\omega)^{\omega^{k-1}} = \omega^{\omega^{k-1}}$. Ако је $\gamma < \omega^\omega = \bigcup_{k<\omega} \omega^k$, то је за неки $k < \omega$, $\gamma < \omega^k$ (релација $<$

на ординалима поклапа се са релацијом ϵ). Одавде следи да је

$$n^{\omega^\omega} = \bigcup_{\gamma<\omega^\omega} n^\gamma = \bigcup_{1\leq k<\omega} n^{\omega^k} = \bigcup_{1\leq k<\omega} \omega^{\omega^{k-1}} = \omega^{\omega^\omega}.$$

33. Јасно је да је за $n = 0$ једнакост тривијално испуњена. Претпоставимо стога да је $n \geq 1$. Знамо да је:

$$(\omega + n)^k = \omega^k + \omega^{k-1} \cdot n + \cdots + \omega \cdot n + n,$$

за све $k \geq 1$, те за $k \geq 1$ важи неједнакост $(\omega+n)^k < \omega^{k+1}$. Тражени идентитет сада лако следи.

34. Мада је у 8. задатку доказан резултат из кога тражени резултат следи, ипак ћемо и њега директно доказати. Доказаћемо тражено тврђење индукцијом по α. Уколико је $\alpha = 0$, тврђење се своди на $0 \leq 1$. Претпоставимо да је тврђење тачно за све ординале $\beta < \alpha$.

1) Нека је ординал α следбеник, тј. $\alpha = \beta + 1$ за неки ординал β. Приметимо да је увек испуњена неједнакост $\gamma^\delta < \gamma^{\delta+1}$. Наиме, $\gamma^{\delta+1} = \gamma^\delta \cdot \gamma$. Подсетимо се да је $\gamma^\delta \cdot \gamma$ ординал који је изоморфан уређеном производу $\gamma^\delta \times \gamma$ и да је γ^δ изоморфан почетном комаду $(\gamma^\delta \times \gamma)_{(0,1)}$. Наиме, ако је $(\delta, \varepsilon) \in (\gamma^\delta \times \gamma)_{(0,1)}$, то је, на основу дефиниције уређеног производа, $\varepsilon < 1$, или је $\varepsilon = 1$ и $\delta < 0$. Како неједнакост $\delta < 0$ никада није испуњена, то закључујемо да је $(\delta, \varepsilon) \in (\gamma^\delta \times \gamma)_{(0,1)}$ ако и само ако је $\varepsilon = 0$, а то показује да је одговарајући почетни комад изоморфан ординалу γ^δ.

Како је $\alpha = \beta + 1$, то је $\beta < \alpha$, те је $\beta \leq \gamma^\beta$. Но, тада је $\beta < \gamma^{\beta+1}$ (према претходно доказаном), па је $\alpha = \beta + 1 \leq \gamma^{\beta+1} = \gamma^\alpha$.

2) Претпоставимо да је α гранични ординал. Тада је

$$\alpha = \bigcup_{\beta<\alpha} \beta \leq \bigcup_{\beta<\alpha} \gamma^\beta = \gamma^\alpha.$$

35. Како је λ гранични ординал, то је $\lambda = \omega \cdot \alpha$ за неки ординал α. Пре свега, јасно је да је $1^\lambda = 1$. Но, ако је $n \geq 2$ тада је $n^\lambda = n^{\omega\cdot\alpha} = (n^\omega)^\alpha = \omega^\alpha$. Тражена једнакост се своди на $1 + \omega^\alpha = \omega^\alpha$, а знамо да је та једнакост испуњена.

36. Како је $2^\omega = \omega$, тврђење је тачно за $\alpha = \omega$.

Нека је $\alpha = \beta+1$ и претпоставимо да је тврђење тачно за ординал β. Тада је

$$|2^\alpha| = |2^{\beta+1}| = |2^\beta \cdot 2| = |2^\beta| \cdot 2 = |\beta| \cdot 2 = |\beta| = |\alpha|.$$

Нека је α гранични ординал и претпоставимо да је тврђење тачно за све ординале $\beta < \alpha$. Тада је $2^\alpha = \bigcup_{\omega\leq\beta<\alpha} 2^\beta$. Овде имамо унију

$|\alpha|$ бесконачних скупова од којих је сваки кардиналности највише $|\alpha|$ ($|2^\beta| = |\beta| \leq |\alpha|$). Стога је та унија кардиналности највише $|\alpha| \cdot |\alpha| = |\alpha|$. Како је $\alpha \subseteq 2^\alpha$, то је $|\alpha| \leq |2^\alpha|$, те су ови ординали заиста исте кардиналности.

37. Заиста је интересантно колико је доказ овог тврђења сличан, готово идентичан, одговарајућем тврђењу за природне бројеве. Нека је β_0 највећи ординал за који је $2^{\beta_0} \leq \alpha$. Тада је $\alpha < 2^{\beta_0+1} = 2^{\beta_0} \cdot 2 = 2^{\beta_0} + 2^{\beta_0}$, па је $\alpha = 2^{\beta_0} + \alpha_0$, при чему је $\alpha_0 < 2^{\beta_0} \leq \alpha$. Уколико је $\alpha_0 = 0$, добили смо тражено представљање ординала α, у супротном настављамо поступак. Добијамо да је $\alpha_0 = 2^{\beta_1} + \alpha_1$ за неке ординале β_1 и α_1, при чему је $\alpha_1 < \alpha_0 < \alpha$. Тада је $\alpha = 2^{\beta_0} + 2^{\beta_1} + \alpha_1$, где је очигледно $\beta_0 > \beta_1$. Продужавањем поступка, добијамо строго опадајући низ ординала (α_k). Како не постоји бесконачан, строго опадајући низ ординала, поступак се мора завршити и добијамо да је $\alpha = 2^{\beta_0} + \cdots + 2^{\beta_n}$ за неко $n \in \omega$ и неки коначан опадајући низ ординала (β_i).

    Да бисмо доказали јединственост оваквог представљања, претпоставимо да је

$$2^{\beta_0} + 2^{\beta_1} + \cdots + 2^{\beta_n} = 2^{\gamma_0} + 2^{\gamma_1} + \cdots + 2^{\gamma_m},$$

    при чему су низови (β_i) и (γ_j) строго опадајући низови ординала. Индукцијом по n лако се може показати да важи неједнакост

$$2^{\beta_1} + \cdots + 2^{\beta_n} < 2^{\beta_0}.$$

    Уколико претпоставимо да је $\beta_0 > \gamma_0$, добијамо

$$2^{\gamma_0} + 2^{\gamma_1} + \cdots + 2^{\gamma_m} < 2^{\gamma_0} + 2^{\gamma_0} = 2^{\gamma_0+1} \leq 2^{\beta_0} \leq 2^{\beta_0} + 2^{\beta_1} + \cdots + 2^{\beta_n}.$$

    Дакле, наведена једнакост не би била испуњена. На исти начин се показује да не може бити ни $\gamma_0 > \beta_0$. Закључујемо да мора бити $\beta_0 = \gamma_0$. Скраћивањем са 2^{β_0} и коришћењем индукције завршава се доказ.

38. Приметимо да је $\omega^\omega = (2^\omega)^\omega = 2^{\omega\cdot\omega} = 2^{\omega^2}$. За ординал ω^5 важи: $\omega^5 = (2^\omega)^5 = 2^{\omega\cdot 5}$. Тражена презентација је

$$\omega^\omega + \omega^5 \cdot 3 + \omega^2 + 6 = 2^{\omega^2} + 2^{\omega\cdot 5+1} + 2^{\omega\cdot 5} + 2^{\omega\cdot 2} + 2^2 + 2^1.$$

39. Доказ је сличан доказу о представљању ординала као збира степена двојке. Нека је γ^{ξ_0} највећи степен ординала γ, који није већи од α. Тада је $\alpha < \gamma^{\xi_0+1} = \gamma^{\xi_0} \cdot \gamma$. То значи да постоје ординали η_0 и α_0 такви да је $\alpha = \gamma^{\xi_0} \cdot \eta_0 + \alpha_0$ за неке ординале η_0, α_0, при чему је $\eta_0 < \gamma$ и $\alpha_0 < \alpha$. Уколико је $\alpha_0 = 0$, тражена презентација је добијена, у супротном настављамо поступак користећи α_0. Као и

у претходној конструкцији, добија се строго опадајући низ ординала (α_i), који мора бити коначан, те се поступак завршава после коначно много корака и добија се тражена презентација.

Претпоставимо да је

$$\gamma^{\xi_0} \cdot \eta_0 + \gamma^{\xi_1} \cdot \eta_1 + \cdots + \gamma^{\xi_n} \cdot \eta_n = \gamma^{\phi_0} \cdot \psi_0 + \gamma^{\phi_1} \cdot \psi_1 + \cdots + \gamma^{\phi_m} \cdot \psi_m,$$

при чему су низови ординала (ξ_i) и (ϕ_i) строго опадајући, а преостали ординали су мањи од γ. Да бисмо доказали да мора бити $n = m$ и да за све $i = \overline{1, n}$ важи да је $\xi_i = \phi_i$ и $\eta_i = \psi_i$, покажимо да је

$$\gamma^{\xi_1} \cdot \eta_1 + \cdots + \gamma^{\xi_n} \cdot \eta_n < \gamma^{\xi_0}.$$

Овај се доказ лако изводи индукцијом по n. Уколико је $n = 1$, то из чињенице да је $\eta_1 < \gamma$, следи да је

$$\gamma^{\xi_1} \cdot \eta_1 < \gamma^{\xi_1} \cdot \gamma = \gamma^{\xi_1 + 1} \leq \gamma^{\xi_0}.$$

Претпоставимо да је тврђење тачно за n и доказујемо га за $n+1$.

$$\gamma^{\xi_1} \cdot \eta_1 + \gamma^{\xi_2} \cdot \eta_2 + \cdots + \gamma^{\xi_{n+1}} \cdot \eta_{n+1} < \gamma^{\xi_1} \cdot \eta_1 + \gamma^{\xi_1} = \gamma^{\xi_1} \cdot (\eta_1 + 1).$$

Но, $\gamma^{\xi_1} \cdot (\eta_1 + 1) \leq \gamma^{\xi_1} \cdot \gamma = \gamma^{\xi_1 + 1} \leq \gamma^{\xi_0}$. Претпоставимо да је $\xi_0 > \phi_0$. Тада је

$$\gamma^{\phi_0} \cdot \psi_0 + \gamma^{\phi_1} \cdot \psi_1 + \cdots + \gamma^{\phi_m} \cdot \psi_m < \gamma^{\phi_0} \cdot \psi_0 + \gamma^{\phi_0} = \gamma^{\phi_0} \cdot (\psi_0 + 1).$$

Како је $\psi_0 < \gamma$, то је $\gamma^{\phi_0} \cdot (\psi_0 + 1) \leq \gamma^{\phi_0} \cdot \gamma = \gamma^{\phi_0 + 1} \leq \gamma^{\xi_0}$. Дакле, заиста мора бити $\xi_0 = \phi_0$. Препоручујемо читаоцу да сам заврши доказ јединствености тако што ће показати да мора бити и $\eta_0 = \psi_0$ и применити индукцију.

Напомена: Овај приказ ординала назива се *представљање ординала у основи* γ. Јасно је зашто је овај назив оправдан. У случају да је $\gamma = \omega$, говори се о *нормалној форми* датог ординала.

40. Приметимо најпре да наведени максимум сигурно постоји, пошто постоји само коначно много $\beta \in \alpha$ за које је $f(\beta) \neq g(\beta)$ (све функције узимају вредност 0 за све сем коначно много елемената).

Уколико је $\alpha = 0$, онда је ${}^{\alpha}\gamma = \{\emptyset\} = 1$.

Претпоставимо да је тврђење тачно за α; докажимо га за $\alpha + 1$. Дефинишемо функцију

$$\Phi : {}^{\alpha+1}\gamma \to {}^{\alpha}\gamma \times \gamma,$$

са: $\Phi(f) = (f_{|\alpha}, f(\alpha))$, где је са $f_{|\alpha}$ означена рестрикција функције f на α (присетимо се да је $\alpha + 1 = \alpha \cup \{\alpha\}$). Јасно је да је Φ једна бијекција. Како су ${}^{\alpha}\gamma$ и γ уређени скупови, посматрамо производ

${}^{\alpha}\gamma \times \gamma$ као производ уређених скупова. Докажимо да је Φ изоморфизам. Ово ће показати да је трђење тачно за $\alpha+1$ уколико је тачно за α (подсетите се дефиниције производа ординала). Нека су $f, g \in^{\alpha+1} \gamma$, при чему је $f \neq g$. Треба доказати да је $f \prec g$ ако и само ако је $(f_{|\alpha}, f(\alpha)) <_P (g_{|\alpha}, g(\alpha))$, где је са $<_P$ означена релација поретка у уређеном производу скупова.

1) $f(\alpha) < g(\alpha)$: Очигледно је да је тада $f \prec g$, но такође је $(f_{|\alpha}, f(\alpha)) <_P (g_{|\alpha}, g(\alpha))$ (подсетите се уређеног производа скупова).

2) $f(\alpha) = g(\alpha)$: Из дефиниције релације $\prec$ следи да је $f \prec q$ ако и само ако је $f(\xi) < g(\xi)$, где је ξ највећи елемент из $\alpha+1$, у коме функције f и g узимају различите вредности. Но, како је $f(\alpha) = g(\alpha)$, то је јасно да $\xi \in \alpha$. Овим смо показали да је у овом случају $f \prec g$ ако и само ако је $f_{|\alpha} \prec g_{|\alpha}$, но то управо значи да је $(f_{|\alpha}, f(\alpha)) <_P (g_{|\alpha}, g(\alpha))$.

За крај доказа, претпоставимо да је α гранични ординал и да је тврђење испуњено за све ординале $\beta < \alpha$. Приметимо да се свака функција $f \in^{\beta} \gamma$, може видети и као функција из ${}^{\alpha}\gamma$, тако што се на $\alpha \setminus \beta$ додефинише као идентички једнака нули. Формалније гледано, за све $\beta < \alpha$, дефинишемо „1–1“ функцију $\Phi_\beta :^{\beta}\gamma \to^{\alpha}\gamma$ са $\Phi(f) = \hat{f}$, где је $\hat{f} : \alpha \to \gamma$ функција чија се рестрикција на β једнака f, а за све $\delta \in \alpha \setminus \beta$ је $\hat{f}(\delta) = 0$. Јасно је да Φ_β чува поредак, те можемо сматрати да је ${}^{\beta}\gamma \subset {}^{\alpha}\gamma$.

Нека је $\beta < \alpha$ и $f \in^{\alpha}\gamma$ функција задата са: $f(\beta+1) = 1$, а $f(\delta) = 0$ за све $\delta \neq \beta$. Посматрајмо почетни комад $({}^{\alpha}\gamma)_f$. Ако $g \in^{\beta}\gamma$, онда је јасно да је $g \prec f$ $(g(\beta+1) = 0 < f(\beta+1)$, а за веће ординале и g и f узимају вредност 0). Обратно, ако претпоставимо да је $g \prec f$, онда мора бити $g(\delta) = 0$ за све ординале $\delta > \beta+1$ (иначе би било $f \prec g$), а такође мора бити и $g(\beta+1) = 0$, пошто би у случају да је $g(\beta) \geq 1$ следило да је или $f \prec g$, или $f = g$ (f је различито од 0 само у $\beta+1$). Закључујемо да је $({}^{\alpha}\gamma)_f =^{\beta}\gamma$. Како је, осим тога, јасно да је ${}^{\alpha}\gamma = \bigcup_{\beta<\alpha} {}^{\beta}\gamma$ (свака функција из ${}^{\alpha}\gamma$ је нула почев од неког ординала), а претпоставили смо да је ${}^{\beta}\gamma$ изоморфан ординалу γ^β за све ординале $\beta < \alpha$, следи да је и ${}^{\alpha}\gamma$ изоморфан са γ^α (подсетите се дефиниције степена ординала).

41. Применимо следећи трик: на сваки број у низу применимо замену основе, али тако да коначну основу c заменимо основом ω. Дакле, ако се у неком кораку број записује у основи c на следећи начин: $a_k c^k + a_{k-1}c^{k-1} + \cdots + a_1 c + a_0$, ми му придружујемо ординал $\omega^k \cdot a_k + \omega^{k-1} \cdot a_{k-1} + \cdots + \omega \cdot a_1 + a_0$. Претпоставимо да се поступак наведен у задатку никада не завршава, тј. да никада не добијамо 0. У том случају нашем низу бројева придружили смо на горе описани начин бесконачан *строго* опадајући низ ординала. Покажимо ово. Претпоставимо да смо у неком кораку добили ординал $\omega^k \cdot a_k + \omega^{k-1} \cdot a_{k-1} + \cdots + \omega \cdot a_1 + a_0$, где је $a_0 > 0$. У следећем кораку

добијамо ординал $\omega^k \cdot a_k + \omega^{k-1} \cdot a_{k-1} + \cdots + \omega \cdot a_1 + (a_0 - 1)$ (проверите зашто је то тако). У случају да смо после неког корака добили ординал $\omega^k \cdot a_k + \omega^{k-1} \cdot a_{k-1} + \cdots + \omega^i \cdot a_i$, за неко $i \geq 1$ при чему је $a_i \neq 0$, то значи да смо у процесу замене основа дошли до броја $a_k c^k + \cdots + a_i c^i$ за неко i. По правилу одузимамо 1 и прелазимо на вишу основу. Но, $c^i - 1 = (c-1)(c^{i-1} + \cdots + c + 1)$, па је $a_i c^i - 1 = (a_i - 1)c^i + c^i - 1 = (a_i - 1)c^i + (c-1)c^{i-1} + \cdots + (c-1)c + (c-1)$. Одговарајући члан у низу ординала је тада $\omega^k \cdot a_k + \cdots + \omega^i \cdot (a_i - 1) + \omega^{i-1} \cdot (c-1) + \cdots \omega \cdot (c-1) + (c-1)$ и он јесте мањи од претходно наведеног члана.

Како бесконачан строго опадајући низ ординала не може постојати, наведени поступак се мора завршити после коначно много корака, што значи да се после коначно много корака добија 0.

42. Нека је k број могућих вредности новчаница у оптицају. Посматрајмо уређени производ $\mathbb{N}^k$ (подсетите се дефиниције уређеног производа скупова — поредак је лексикографски гледано са десна на лево). Ако на почетку имамо n_1 новчаница најмање вредности, n_2 следеће вредности, ..., n_k новчаница највеће могуће вредности, онда се наш „финансијски почетак“ у овој „игри“ може видети као k-торка елемената из $\mathbb{N}^k$. Но, ако је $(n'_1, \ldots, n'_k)$ k-торка која настаје од $(n_1, \ldots, n_k)$ после посете мењачници, онда је $(n'_1, \ldots, n'_k) < (n_1, \ldots, n_k)$ према дефиницији уређеног производа скупова. Како је скуп $\mathbb{N}^k$ добро уређен (уређени производ добро уређених скупова је добро уређен), то се овај поступак не може бесконачно много пута понављати и на крају долазимо до k-торке $(0, \ldots, 0)$, односно, једноставно говорећи, остајемо без пара!

    Можете ли применити идеју из решења претходног задатка да дате друго решење овог задатка?

43. Да. Већ смо се мало привикли на задатке овог типа, па нам неће бити тешко да проблем „кодирамо“ на такав начин да се увиди да се све завршава после коначног броја корака. Пребројимо најпре колико има јединица (ако их нема, онда се не може ни започети са трансформацијама). Нека их има $k+1$. Са a_k означимо број нула које претходе првој јединици (ако их нема, онда је наравно $a_k = 0$). Са a_{k-1} означимо број нула између прве две јединице (све посматрамо са леве стране), итд. Са a_0 означавамо број нула испред претпоследње и последње јединице. Нуле које се налазе иза последње јединице не утичу на поступак и њих потпуно можемо да игноришемо (важно је уочити у сваком задатку шта су битни, а шта небитни подаци). Нашем низу нула и јединица придружујемо ординал $\omega^k \cdot a_k + \omega^{k-1} \cdot a_{k-1} + \cdots + \omega \cdot a_1 + a_0$. На пример, низу 001100101000 придружујемо ординал $\omega^3 \cdot 2 + \omega \cdot 2 + 1$, док низу 1000111001 придружујемо ординал $\omega^3 \cdot 3 + 2$. Ако овај поступак применимо на низове који се појављују у задатку поново

добијамо опадајући низ ординала и закључак се изводи као и у ранијем задатку. Појаснимо зашто заиста добијамо опадајући низ. Ако смо изабрали пар 01, где је јединица, нпр. $l-$та са леве стране ($l \geq 2$), онда после трансформације и „кодирања“ добијамо ординал

$$\omega^k \cdot a_k + \cdots + \omega^{k-l+2} \cdot a_{k-l+2} + \omega^{k-l+1} \cdot (a_{k-l+1} - 1) + \omega^{k-l} \cdot (a_{k-l} + m) + \cdots + a_0,$$

где је m непознати број нула које смо дописали иза јединице ($a_{k-l+1} \geq 1$ јер се на одговарајућем месту појављује 01). Јасно је да овај ординал мањи од почетног. Слична провера се може извршити и у случају $l = 1$.

44. Нека су скупови A, B и C такви да је $|A| = \kappa$, $|B| = \lambda$ и $|C| = \mu$ и да су скупови B и C дисјунктни. Тада, користећи чињеницу да је $A \times (B \cup C) = A \times B \cup A \times C$ добијамо тражени резултат.

45. Нека је $\kappa = 2^{\mathfrak{c}}$. Тада је

$$\kappa^{\mathfrak{c}} = (2^{\mathfrak{c}})^{\mathfrak{c}} = 2^{\mathfrak{c} \cdot \mathfrak{c}} = 2^{\mathfrak{c}} = \kappa.$$

46. Пре свега, јасно је да је $\kappa \geq \aleph_0$. У супротном, 2^κ је коначан кардинал и он не може бити једнак бесконачном кардиналу $\mathfrak{c}^\kappa$. Како је $\mathfrak{c} = 2^{\aleph_0}$, то добијамо $\mathfrak{c}^\kappa = (2^{\aleph_0})^\kappa = 2^{\aleph_0 \cdot \kappa}$, а како је $\kappa \geq \aleph_0$, то је $2^{\aleph_0 \cdot \kappa} = 2^\kappa$. Закључујемо да је тражена једнакост тачна за све $\kappa \geq \aleph_0$.

47. За $\kappa = 0$ је $\kappa^\kappa = 1$, те је $\kappa^{\kappa^\kappa} = 0^1 = 0$, док је $2^\kappa = 1$, те једнакост не важи. За $\kappa = 1$ лева страна је једнака 1, а десна 2, те ни тада једнакост не важи. За $\kappa \geq 2$ добијамо $\kappa^{\kappa^\kappa} \geq 2^{2^\kappa} > 2^\kappa$. Закључујемо да тражена једнакост није испуњена ни за један кардинал κ.

48. Уколико је $\lambda = 0$, добијамо да је $\kappa^\lambda = 1 \neq \aleph_0$. Дакле, у даљем је $\lambda > 0$. Ако је $\kappa = 0$ то је $\kappa^\lambda = 0 \neq \aleph_0$, а ако је $\kappa = 1$ то је $\kappa^\lambda = 1 \neq \aleph_0$. Дакле, у даљем је $\kappa \geq 2$. За $\lambda \geq \aleph_0$ добијамо $\kappa^\lambda \geq 2^{\aleph_0} > \aleph_0$. Према томе, λ мора бити коначан кардинал. Ако је и κ коначан, то би и κ^λ био коначан. Закључујемо да је κ бесконачан, а λ коначан и у том случају добијамо да је $\kappa^\lambda = \kappa$. Тако смо и добили решење: једнакост важи **акко** је $\kappa = \aleph_0$, а λ коначан, различит од 0.

49. За λ постоје две могућности: или је коначан или бесконачан. Ако је коначан, онда је 2^λ такође коначан па наведена неједнакост није испуњена. Према томе, λ мора бити бесконачан и у том случају добијамо да је $2^\lambda \geq 2^{\aleph_0} = \mathfrak{c}$.

50. Јасно је да ни κ ни λ не смеју бити једнаки нули, као и да је бар један од њих бесконачан (образложити зашто ово мора да важи).

У том случају је $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$. У случају да је $\kappa \geq \lambda$, добијамо да је $\kappa = 2^\kappa + \aleph_0$, што наравно није могуће јер је $2^\kappa > \kappa$. Закључујемо да је $\lambda > \kappa$ и $\lambda = 2^\kappa + \aleph_0$. Сада постоје две могућности: κ је коначан и онда је $\lambda = \aleph_0$ и κ је бесконачан. У овом другом случају добијамо да је $\lambda = 2^\kappa$ и тиме су све могућности исцрпљене.

51. Уколико је $\kappa = 0$ онда је $0 = \lambda^2$, па је и $\lambda = 0$. На исти начин добијамо $\lambda = 0 \Rightarrow \kappa = 0$. У даље претпостављамо да су и κ и λ различити од 0. Ако је бар један од њих бесконачан онда се тражена једнакост своди на $\max\{\kappa, \lambda\} = \max\{\kappa, \lambda\}$, те је у том случају испуњена. Претпоставимо, стога, да су и κ и λ коначни: $\kappa = m \in \mathbb{N}$ и $\lambda = n \in \mathbb{N}$. Пребацивањем једног од израза на другу страну и факторизацијом добијамо $(m^2 - 1)n^2 = m^3$. Но, $m^2 - 1$ и m^3 су узајамно прости (сваки прост делилац од m^3 уједно је и делилац од m, па тада не може делити $m^2 - 1$). Позната је следећа чињеница из аритметике: $a \,|\, bc, \mathrm{NZD}(a, b) = 1 \Rightarrow a \,|\, c$. Применом овог резултата добијамо да $m^3 \,|\, n^2$, те после скраћивања добијамо $(m^2 - 1)k = 1$ за неки природан број k. Но, јасно је да је ово немогуће за природне бројеве m, k $(m^2 - 1 \neq 1)$. Тако закључујемо да решења у овом случају и нема.

52. Како се овај задатак не разликује битно од задатка урађеног у оквиру примера у тексту, то ће решење бити мање детаљно презентирано. Пре свега, приметимо да ни κ ни λ никако не могу бити једнаки нули (зашто?). У даљем претпостављамо да су они различити од 0. Размотримо следеће случајеве.

    $\underline{\kappa \geq \aleph_0, \lambda \geq \aleph_0}$: У овом случају добијамо да мора бити $\max\{\kappa, \lambda\} = 2^\lambda$, те закључујемо да λ може бити произвољан бесконачни кардинал, а $\kappa = 2^\lambda$.

    $\underline{\kappa \geq \aleph_0, \lambda < \aleph_0}$: У овом случају немамо решење јер са десне стране добијамо бесконачан, а са леве коначан кардинал.

    $\underline{\kappa < \aleph_0, \lambda \geq \aleph_0}$: Ни у овом случају нема решења јер би се добило да је $2^\lambda = \lambda$, а *добро* знамо да је то немогуће.

    $\underline{\kappa < \aleph_0, \lambda < \aleph_0}$: Како је 7 прост број то је $\kappa = 7^s$, а $\lambda = 7^t$ и наведена једнакост своди се на $s + 2t = 7^t$. Како је $7^t > 4^t = 2^{2t} > 2t$, то је s за ма који избор природног броја t и сам природан број, па је у том случају решење дато са: $(\kappa, \lambda) = (7^{7^t - 2t}, 7^t)$, где је $t \in \mathbb{N}$.

53. Приметимо, пре свега да је за $\lambda = 0$ тражена једнакост испуњена за све кардинале κ, као и да из претпоставке $\kappa = 0$ следи да је $\lambda = 0$. Дакле, у даљем претпостављамо да су и κ и λ различити од 0.

    Размотримо четири случаја.

(а) $\kappa \geq \aleph_0$, $\lambda \geq \aleph_0$: У овом случају лева страна је једнака $\max\{2^\kappa, \lambda\}$, а десна $\max\{\kappa, \lambda\}$. Како је $2^\kappa > \kappa$, то закључујемо да λ мора бити највећи од свих кардинала који се овде појављују и да је то и довољно да једнакост буде испуњена. Дакле, у овом случају је $\lambda \geq 2^\kappa$, док је κ произвољан бесконачни кардинал.

(б) $\kappa \geq \aleph_0$, $\lambda < \aleph_0$: Сада је (присетимо се да смо претпоставили да λ није 0) лева страна једнака 2^κ, а десна κ, па у овом случају једнакост не може бити испуњена.

(ц) $\kappa < \aleph_0$, $\lambda \geq \aleph_0$: Овде су ($\kappa \neq 0$) и лева и десна страна једнакости једнаке λ, па је једнакост испуњена за све такве кардинале.

(д) $\kappa < \aleph_0$, $\lambda < \aleph_0$: Дакле, овде радимо са природним бројевима, па пређимо на одговарајуће ознаке — нека је $\kappa = m$, а $\lambda = n$. Претпоставили смо да ти природни бројеви нису једнаки 0, па после скраћивања добијамо $7^m n^5 = m^3$. Ако само мало размислимо, увериһемо се да овако нешто никада не може бити испуњено. Остаје само да то докажемо. Како да то урадимо? Па, вероватно је најједноставније доказати да је $7^m > m^3$ и то се може без икаквих проблема урадити индукцијом по m. Урадите то за вежбу.

54. Пре свега, једнакост је испуњена за $\kappa = 0$ и произвољан кардинал λ. Такође, $\lambda = 0 \Rightarrow \kappa = 0$. У даљем претпостављамо да тражени кардинали нису 0. Уколико је κ бесконачан, а λ коначан решења нема, јер бисмо у том случају добили $2^\kappa = \kappa$. У случају да је κ коначан, а λ бесконачан, решења такође нема, јер је у том случају на левој страни једнакости коначан, а на десној бесконачан кардинал. У случају да су оба бесконачна, добијамо $2^\kappa = \max\{\kappa, \lambda\}$ те је у том случају κ произвољан бесконачан, а $\lambda = 2^\kappa$. Остаје најзанимљивији случај — када су оба кардинала коначни. Дакле, $\kappa = m, \lambda = n$. Добијамо, после скраћивања, $11^m = m^7 n^5$. Као и раније, закључујемо да су и m и n степени простог броја 11: $m = 11^s, n = 11^t$. Тада мора бити $11^s = 7s + 5t$. Лако је показати (урадите то!) да је $11^s > 7s$ за свако $s \in \mathbb{N}$. Остаје да се види када је тај број дељив са 5. Дакле, колико је $11^s - 7s$ модуло 5? Но,

$$11^s - 7s \equiv_5 1^s - 2s \equiv_5 1 + 3s.$$

Треба дакле решити једначину

$$3s + 1 \equiv 0 \bmod 5.$$

Како је $2 \cdot 3 \equiv_5 1$, то после множења са 2 једначину сводимо на

$$s + 2 \equiv 0 \bmod 5,$$

односно,

$$s \equiv 3 \bmod 5.$$

Овде смо користили чињеницу да је $2+3 \equiv_5 0$. Према томе, у овом случају добијамо да је

$$\kappa = 11^{5l+3}, \lambda = 11^{\frac{11^{5l+3}-7\cdot(5l+3)}{5}},$$

где је $l \in \mathbb{N}$ произвољан.

55. Концентрисаћемо се само на случај $\kappa = m \in \mathbb{N}, \lambda = n \in \mathbb{N}$, где је $m, n \neq 0$ (остале случајеве препуштамо читаоцу за вежбу). После скраћивања добијамо да је $13^m = m^3 n^5$. Стога мора бити $m = 13^s$, $n = 13^t$, и добијамо да нам се траже s и t за које је $13^s = 3s + 5t$. Лако се показује да је $13^s - 3s > 0$ (пошто је лако, покажите); остаје само да се испита за које је s та разлика дељива са 5. Но,

$$13^s - 3s \equiv 3^s - 3s \bmod 5.$$

Како су 5 и 3 узајамно прости, то нас интересује за које s број 5 дели $3^{s-1} - s$. Ово је нешто сложенија ситуација него у претходном примеру, јер се s појављује и у експоненту. Како је $3^4 \equiv_5 1$ (мала Фермаова[1] теорема или у овом посебном случају прост рачун!), то је експонент модуло 5 периодичан са периодом 4. Како је само s модуло 5 периодично са периодом 5, то нас заправо интересује како се s понаша модуло 20. Формирајмо следећу табелу:

$s \bmod 20$	$3^{s-1} - s \bmod 5$
1	$1-1=0$
2	$3-2$
3	$9-3$
4	$27-4=2-4$
5	$6-5=1-0$
6	$3-1$
7	$9-2$
8	$27-3=2-3$
9	$6-4$
10	$18-5=3-0$
11	$9-1$
12	$27-2=2-2=0$
13	$6-3$
14	$18-4=3-4$
15	$9-5=4-0$
16	$12-1$
17	$36-2=1-2$
18	$3-3=0$
19	$9-4$
20	$27-5$

[1] Pierre de Fermat (1601–1665), француски математичар.

Како је она формирана? Нас интересује разлика два израза од којих је први експоненцијалан, а други линеаран. Стога смо узастопне разлике формирали тако што смо први члан у разлици множили са 3, а у другом члану разлике смо додавали јединицу и све смо то редуковали модуло 5 када су бројеви постајали превелики за наш укус. Видимо да се 0 појављује у случајевима када је $s \equiv 1$, 12 и 18 mod 20. Остављамо читаоцима да испишу коначно решење.

56. Као и у претходном задатку дајемо решење само за случај коначних кардинала. Дакле, треба наћи природне бројеве m, n такве да је $m^2 n + 3^m = n^3$. Јасно је да n не сме бити 0, као и да $m = 0 \Rightarrow n = 1$. У даљем претпостављамо да они нису 0. После мало сређивања видимо да се једначина своди на

$$3^m = n(n-m)(n+m).$$

Како је 3 прост број, то закључујемо да су сви фактори са десне стране степени тројке, тј. $n = 3^s$, $n - m = 3^t$ и $n + m = 3^u$, за неке природне бројеве s, t и u. Ако мало размислите, видећете да је то сумњиво. Приметимо пре свега да мора бити $t < s < u$, јер $m \neq 0$. Ако саберемо друге две једнакости и искористимо чињеницу да је $n = 3^s$, добијамо $2 \cdot 3^s = 3^t + 3^u$. Ако скратимо са 3^t (то је најмањи од свих степена тројке који се ту појављују), добијамо $2 \cdot 3^{s-t} = 1 + 3^{u-t}$. Но, и 3^{s-t} и 3^{u-t} су дељиви са 3, а 1 то није. Закључујемо да решења у коначном случају и нема.

57. Ако је $\lambda = 0$ онда наведена једнакост важи за сваки кардинал κ, док $\kappa = 0 \Rightarrow \lambda = 0$. У даљем претпостављамо да су κ и λ различити од 0.

Без обзира што смо претпоставили да је $\lambda \neq 0$, не можемо, сем у конашном случају скратити са λ. Морамо пажљивије поступати да не бисмо изгубили неко решење. Уколико су и κ и λ бесконачни то добијамо $\max\{2^\kappa, \lambda\} = \lambda$, те закључујемо да тада мора бити $\lambda \geq 2^\kappa$ при чему је κ произвољан бесконачни кардинал. Јасно је да решења нема у случају да је κ бесконачан, а λ коначан (зашто?). Такође је једнакост испуњена за сваки коначан $\kappa \neq 0$ и сваки бесконачан λ. Остаје нам само случај када су оба коначна и различита од нуле. Дакле, $\kappa = m \in \mathbb{N}$ и $\lambda = n \in \mathbb{N}$. После скраћивања са n добијамо $3^m = 1 + 4n^4$. Може ли ова једнакост бити испуњена за неке $m, n \neq 0$? Није тешко убедити се да не може. Заправо, израз са десне стране никада није дељив са 3. У то се можемо уверити ако редом проверавамо случајеве $n \equiv 0, 1, 2 \mod 3$. Добили бисмо да је израз са десне стране редом конгруентан са $1, 2, 2$ модуло 3, па није дељив са 3. Други начин би био да факторишемо наш израз $1 + 4n^4 = (1 + 2n^2)^2 - 4n^2 = (2n^2 - 2n + 1)(2n^2 + 2n + 1)$ и да потом анализирамо факторе. Учините то за вежбу. У сваком случају добили смо да решења у коначном случају нема (сем наравно за $\lambda = 0$ о чему је било речи раније). Читаоцу за вежбу такође препоручујемо да провери шта бисмо добили уколико бисмо у случају када је λ бесконачан кардинал скратили са λ.

58. Радимо само за коначне, наравно. После сређивања добијамо да треба наћи природне бројеве m и n за које је $3^m = m(n+1)(n^2-n+1)$. Одавде добијамо да је $m = 3^s$, $n+1 = 3^t$ и $n^2-n+1 = 3^u$. Ако из претпоследње једнакости изразимо n и заменимо у последњој добијамо да је
$$3^{2t} - 3^{t+1} + 3 = 3^u.$$
За $t = 0$ добијамо да је $n = 0$ и $3^m = m$ што није могуће. Такође, за $u = 0$ добијамо $n = 1$, или $n = 0$, но ни то није могуће, јер би тада добили $2 = 3^t$. Закључујемо да је горњу једнакост могуће скратити са 3 и добијамо
$$3^{2t-1} - 3^t + 1 = 3^{u-1}.$$
Чини се да су овде све степени тројке сем јединице и да смо добили контрадикцију, али није баш тако. Можда је $u = 1$. Проверимо: $u = 1 \Rightarrow n(n-1) = 2 \Rightarrow n = 2$. И заиста, ако $n = 2$ заменимо у полазну једнакост добијамо $3^m = 9m$, односно $3^{m-2} = m$. Ово *јесте* испуњено за $m = 3$ и само тада (проверите да је $3^{m-2} > m$ за $m > 3$). Према томе, једно решење је дато са $(m, n) = (3, 2)$. Но, то уједно и једино решење, јер ако u није 1, онда заиста добијамо контрадикцију (навести зашто).

59. У овом задатку нема ништа посебно ново у односу на претходне. Једино треба приметити да у случају да је $\lambda \geq \aleph_0$ важи $5^{2\lambda} = 5^\lambda = 2^\lambda$, док у случају да су оба кардинала коначна, κ, као и $\lambda + 1$ морају бити степени броја 5 (факторишите израз на десној страни у коначном случају).

60. Означимо са $\pi_j : \prod_{i \in I} A_i \to A_j$ пројекцију на j-ти фактор у производу. Ако је за неко j, $\pi_j[B_j] = A_j$ онда за то j важи и $|B_j| \geq |A_j|$ (зашто?). У супротном, за свако $j \in I$ постоји $x_j \in A_j$ који није у слици скупа B_j при одговарајућој пројекцији. Уочимо елемент $x = (x_i)_{i \in I}$. Тај елемент није ни у једном од скупова B_i. Наиме, $x \in B_j \Rightarrow x_j = \pi_j(x) \in \pi_j[B_j]$, што противречи избору елемента x_j. Како $x \notin \bigsqcup_{i \in I} B_i$, а тај скуп представља цео производ то добијамо контрадикцију.

61. (a) Јасно је да је α већи или једнак од кардиналности сваког од скупова који су наведени пошто је сума свих тих кардиналности. Но, он не може бити ни једнак некој од тих кардиналности пошто оне чине стриктно растући низ (ако би

био једнак кардиналности неког од наведених скупова, онда би морао да буде мањи од кардиналности следећег скупа у низу, а и она се појављује у његовој дефиницији). Осим тога, ако је κ кардинал који је већи од кардиналности свих наведених скупова онда је јасно да је $\kappa \geq \alpha$. Стога је α најмањи такав (видети и доказ дела под б за додатно појашњење).

(б) Приметимо да важи следеће: $|A^{B \sqcup C}| = |A^B \times A^C|$ — свака функција дефинисана на $B \sqcup C$ потпуно је одређена својим вредностима на B и C. И за општи случај исто важи:

$$|A^{\sqcup_{i\in I} B_i}| = |\prod_{i \in I} A^{B_i}|.$$

Ако са $\mathcal{P}^n(\mathbb{N})$ означимо низ скупова дефинисан са:

$$\mathcal{P}^0(\mathbb{N}) = \mathbb{N}; \quad \mathcal{P}^{n+1}(\mathbb{N}) = \mathcal{P}(\mathcal{P}^n(\mathbb{N})),$$

онда је

$$2^\alpha = |2^{\sqcup_{n\in\mathbb{N}}(P^n(\mathbb{N})\times\{n\})}| = |\prod_{n\in\mathbb{N}} 2^{\mathcal{P}^n(\mathbb{N})\times\{n\}}| = |\prod_{n\in\mathbb{N}} \mathcal{P}^{n+1}(\mathbb{N})|.$$

Но, за све $n \in \mathbb{N}$ је $|\mathcal{P}^{n+1}(\mathbb{N})| < \alpha$, па је $|\prod_{n\in\mathbb{N}} \mathcal{P}^{n+1}(\mathbb{N})| \leq \alpha^{\aleph_0}$. Како је $\alpha^{\aleph_0} \leq (2^\alpha)^{\aleph_0} = 2^{\alpha\cdot\aleph_0} = 2^\alpha$, то тражени закључак следи.

62. Нека су за $i \in I$ дати међусобно дисјунктни скупови A_i такви да је $|A_i| = \kappa_i$, док су за све $i \in I$, дати скупови B_i такви да је $|B_i| = \lambda_i$. Треба показати да постоји „1–1" функција из $\bigcup_{i\in I} A_i$ у $\prod_{i\in I} B_i$, али да не постоји бијекција између ових скупова.

Како је $|A_i| < |B_i|$, то постоје функције $f_i : A_i \to B_i$, које јесу „1–1", али које не могу бити „на". Нека је $(b_i^0) \in \prod_{i\in I}(B_i \setminus f_i[A_i])$ један, произвољно изабрани елемент. Дефинишемо функцију $f\colon \bigcup_{i\in I} A_i \to \prod_{i\in I} B_i$ са:

$$f(x)_i = \begin{cases} f_i(x), & x \in A_i \\ b_i^0, & x \notin A_i. \end{cases}$$

Покажимо да је f „1–1". Претпоставимо да је $f(x) = f(x')$.

1) За неко $i \in I$: $x, x' \in A_i$. У овом случају добијамо да мора бити $f_i(x) = f_i(x')$, но како је f_i „1–1" функција, следи да је $x = x'$.

2) $x \in A_i$, $x' \in A_j$ за неке $i \neq j$. Како је по претпоставци $f(x) = f(x')$, то добијамо да је $f_i(x) = f(x)_i = f(x')_i = b_i^0$, а то није могуће, јер су тачке b_i^0 тако изабране да $b_i^0 \neq f_i[A_i]$. Дакле, овај случај није могућ и доказали смо да је f „1–1".

Покажимо сада да не постоји функција $g\colon \bigcup_{i\in I} A_i \to \prod_{i\in I} B_i$, која је „на". Нека је g било која функција из $\bigcup_{i\in I} A_i$ у $\prod_{i\in I} B_i$. Означимо са π_j одговарајуће пројекције, $\pi_j : \prod_{i\in I} B_i \to B_j$, $\pi_j(b) = b_j$, где је

$b = (b_i) \in \prod_{i \in I} B_i$. За $i \in I$ посматрајмо функције $\pi_i \circ g_{|_{A_i}} : A_i \to B_i$. Како је $|A_i| < |B_i|$ то те функције не могу бити „на", па постоје елементи $c_i \in B_i \setminus (\pi_i \circ g_{|_{A_i}})[A_i]$. Покажимо да елемент $c = (c_i) \in \prod_{i \in I} B_i$ није у слици функције g, те g није „на". У супротном, нека је $c = g(x)$ за неко $x \in \bigcup_{i \in I} A_i$. Нека $x \in A_j$. Како је $c = g(x)$ то је и $c_j = g(x)_j$. Но, $g(x)_j = \pi_j(g_{|_{A_j}}(x))$. Елемент c_j је тако изабран да није у слици функције $\pi_j \circ g_{|_{A_j}}$. Ова контрадикција завршава доказ.

Напомена: Како се из 60. задатка може извести закључак да не постоји функција $g\colon \bigcup_{i \in I} A_i \to \prod_{i \in I} B_i$, која је „на"? Погледати и 49. задатак из претходне главе.

63. Пре свега уведимо (добро познату) ознаку $x + A = \{x + a : a \in A\}$. Нека $y \in (x + A) \cap A$. У том случају је $y \in A$ и $y = x + a$, за неко $a \in A$. Добијамо да је $x = y - a$ где и y и a припадају скупу A. Према томе, ако желимо да наведени пресек буде празан, то морамо наћи реалан број x који се *не може* представити у облику разлике два броја из A. Јасно је да је то могуће, јер је због пребројивости скупа A и скуп свих могућих разлика његових елемената пребројив. Наиме постоји једно „на" пресликавање скупа $A \times A$, који је пребројив, на скуп свих могућих разлика $A - A$. Пресликавање $f\colon A \times A \to A - A$ задато је са $f(a, b) = a - b$. Како је f „на", а $A \times A$ пребројив, то је и $A - A$ пребројив. Скуп $\mathbb{R}$ је непребројив и стога постоји $x \notin A - A$, што завршава задатак.

64. Изведимо најпре Хауздорфов принцип максималности из Цорнове леме. Нека је P било који посет и L ланац у њему. Посматрајмо следећи посет: $\mathcal{L} = \{C \subseteq P : L \subseteq C$ и C је ланац $\}$. У посету $\mathcal{L}$ уређење је наравно задато инклузијом. Применимо Цорнову лему на посет $\mathcal{L}$. Јасно је (остављамо читаоцу да се у то сам убеди) да је унија ланца ланаца такође ланац, те стога у $\mathcal{L}$ сваки ланац има мајоранту. Према Цорновој леми $\mathcal{L}$ има максимални елемент, а тај елемент није ништа друго до тражени максимални ланац који садржи L.

Докажимо сада Цорнову лему коришћењем Хауздорфовог принципа максималности. Нека је P било који посет у коме сваки ланац има мајоранту. Треба да докажемо да P садржи максимални елемент. Али, то је једноставно: узмимо било који *максимални* ланац у P. Он постоји због Хауздорфовог принципа — можемо узети било који елемент из P и њега посматрати као ланац, па је он садржан у максималном! Но, мајоранта за тај максимални ланац *мора* бити максимални елемент — у супротном тај ланац не би могао бити максималан: на њега би „надовезали" елемент који је већи од његове мајоранте.

65. Приметимо да су у свим случајевима елементи скупова о којима

је реч задати као подскупови неког скупа који задовољавају још неке додатне услове. Но, јасно је да за било које скупове X и Y важи: X је подскуп од Y акко сваки коначан подскуп од X је подскуп од Y. Стога ћемо се у свим случајевима концентрисати само на те додатне услове.

(а) Нека је $X \in \mathcal{F}$ и X' коначан подскуп од X. Ако су S и T елементи из X' онда су они и елементи из X и њихов пресек је празан, па према томе и $X' \in \mathcal{F}$. За доказ другог смера претпоставимо да је $X \subseteq \mathcal{P}(A)$ такав да је сваки његов коначан подскуп у $\mathcal{F}$. Ако су S и T произвољни различити елементи из X онда је скуп $\{S, T\}$ коначан подскуп од X и као такав у $\mathcal{F}$. Но, то значи да је $S \cap T = \emptyset$.

(б) Приметимо пре свега да не тврдимо да су то само функције са доменом A, него функције чији је домен подскуп од A (подсетите се дефиниције појма функције). Јасно је да је сваки коначан подскуп функције такође функција. Интересантна је друга импликација. У ту сврху, претпоставимо да је сваки коначан подскуп од f функција, а да само f није функција. То значи да постоје $a \in A$ и $b_1, b_2 \in B$ такви да $(a, b_1) \in f$ и $(a, b_2) \in f$. Но, скуп $\{(a, b_1), (a, b_2)\}$ је коначан подскуп од f, а очигледно није функција. Тако смо добили контрадикцију.

(в) Као и у претходном задатку разреши се питање да ли је дати подскуп функција. Ако то можда није „1–1“ функција, онда разматрањем скупа $\{(a_1, b), (a_2, b)\}$ добијамо контрадикцију.

66. (а) Нека је $\mathcal{F}$ скуп коначног карактера. Формирајмо посет $(\mathcal{F}, \subseteq)$ (елементи у $\mathcal{F}$ су скупови и можемо разматрати овај посет — уосталом тражени максимални елемент је баш максимални елемент у овом посету). Нека је $\mathcal{L}$ ланац у $\mathcal{F}$. Довољно је да покажемо да тај ланац има мајоранту — из Цорнове леме ће следити постојање максималног елемента. Посматрајмо $\cup\mathcal{L}$. Ако тај скуп припада $\mathcal{F}$, онда је он мајоранта за наведени ланац (сваки елемент из ланца је подскуп тог скупа). У супротном $\cup\mathcal{L} \notin \mathcal{F}$, па како је $\mathcal{F}$ скуп коначног карактера то постоји неки коначан подскуп $\{f_1, \ldots, f_n\}$ скупа $\cup\mathcal{L}$ који не припада $\mathcal{F}$. Но, за свако $i \in \{1, \ldots, n\}$ $f_i \in L_i$ за неки $L_i \in \mathcal{L}$. Но, $\mathcal{L}$ је ланац те међу скуповима $L_1, \ldots, L_n$ мора постојати највећи, означимо га са L'. Тада бисмо добили да је $\{f_1, \ldots, f_n\}$ коначан подскуп од L' па мора бити у $\mathcal{F}$ $(L' \in \mathcal{F})$. Тиме добијамо контрадикцију.

(б) Нека је $\mathcal{F}$ непразан скуп непразних скупова. Треба показати да постоји функција избора $f\colon \mathcal{F} \to \cup\mathcal{F}$ таква да је $f(X) \in X$ за сваки $X \in \mathcal{F}$. Нека је $A = \cup\mathcal{F}$. Посматрајмо скуп

$$K = \{f \subseteq \mathcal{F} \times A : f \text{ је функција и } (\forall X \in \mathrm{Dom}(f))(f(X) \in X)\}.$$

Остављамо читаоцима за вежбу да провере да је K скуп коначног карактера (дакле и непразан). Према Тјукијевој леми K садржи максимални елемент. Тај елемент мора бити функција дефинисана на сваком сваком скупу у $\mathcal{F}$. У супротном могли бисмо да је додефинишемо у тачки у којој није дефинисана, те не би могла бити максимални елемент. Наведена функција и јесте тражена функција избора.

67. Овај задатак се не разликује битно од задатка број 12 из друге главе. Пре свега, парабола је кардиналности $\mathfrak{c}$. То се може видети из чињенице да пројекција параболе на $x-$осу представља бијекцију. С друге стране, ако је x рационалан број и (x, y) на параболи, то је y јединствено одређен. Стога је скуп свих тачака на параболи чија је прва координата рационалан број пребројив. Ако је $y \in \mathbb{Q}$ и (x, y) на параболи, онда могу постојати највише две такве тачке. Према томе и скуп тачака параболе код којих је друга координата рационална јесте пребројив. Како је јасно да је скуп тачака параболе код којих су обе координате рационалне нужно пребројив, то закључујемо да је кардиналност скупа тачака параболе са обе ирационалне координате заправо $\mathfrak{c}$.

68. За фиксирано x добијамо алгебарску једначину петог степена по y, па решења има највише 5. За фиксирано y добијамо једначину трећег степена по x, те решења има највише 3. Погледајте решење претходног задатка.

69. Нека је ℓ *било која права* у равни. Пресек праве ℓ и *било које кружнице* је највише двочлан. Како кружница у скупу $\mathbb{K}$ има пребројиво много, то права ℓ има највише пребројиво много тачака са унијом $\cup\mathbb{K}$ свих кружница из тог скупа. Но, права је кардиналности $\mathfrak{c}$ и стога на њој мора бити $\mathfrak{c}$ тачака које не леже ни ни једној од датих кружница ($\aleph_0 + \kappa = \mathfrak{c} \Rightarrow \kappa = \mathfrak{c}$). Како у целој равни има $\mathfrak{c}$ тачака, то добијамо тражени закључак.

70. Уочимо било коју праву ℓ у равни и запитајмо се које је геометријско место тачака центара кружница са рационалним полупречником које додирују задату праву. Јасно је да је растојање од центра неке такве кружнице до праве ℓ рационалан број. Но, то је заправо и довољан услов. Према томе тражено геометријско место тачака чиниће све праве које су паралелне датој и налазе се на рационалном растојању од ње. Има их пребројиво много. Ако поступак поновимо за сваку праву из наведеног скупа добићемо пребројиво много правих (пребројива унија пребројивих скупова је пребројив скуп). Било која тачка ван тих правих јесте центар неке кружнице са рационалним полупречником која не додирује ни једну од правих из почетног скупа. Јасно је да таквих тачака, па тиме и кружница има непребројиво много, заправо је кардиналност тог скупа $\mathfrak{c}$. За доказ је довољно узети произвољну праву

у равни која није паралелна ни једној од правих из скупа Π (зашто таква права постоји?). На њој има $\mathfrak{c}$ тачака које не леже ни на једној од добијених правих. Тиме је задатак решен.

71. $\Rightarrow$: Претпоставимо да је f „на“. Стога је скуп $X_z = f^{-1}[\{h(z)\}]$ непразан за било који елемент $z \in Z$. Према Аксиоми избора, можемо изабрати по један елемент x_z из сваког од тих скупова. Ако функцију $g\colon Z \longrightarrow X$ дефинишемо са $g(z) := x_z$, то је испуњено $f \circ g = h$. Наиме $f(g(z)) = f(x_z) = h(z)$, према избору елемента x_z.

    $\Leftarrow$: Уколико за скуп Z узмемо баш скуп Y и за функцију h узмемо id_Y, то добијамо да постоји $g\colon Y \longrightarrow X$ тако да важи $f \circ g = \mathrm{id}_Y$, а одатле непосредно следи да је f „на“.

72. Означимо са $\mathbb{P}$ скуп свих простих природних бројева. Нека је $f\colon \mathbb{P} \to \mathbb{N}$ произвољна функција. Показаћемо да се она може продужити до мултипликативно периодичне функције. На тај начин показаћемо да мултипликативно периодичних функција има бар колико функција из $\mathbb{P}$ у $\mathbb{N}$. Како ових функција има $\mathfrak{c}$, а то је уједно и кардиналност скупа свих функција из $\mathbb{N}$ у $\mathbb{N}$, то закључујемо да и мултипликативно периодичних има $\mathfrak{c}$.

    Нека је $n \in \mathbb{N}$ произвољан. Ако је он облика $4^l p$ за неки прост број p, где је $l \in \mathbb{N}$, онда дефинишемо $\tilde{f}(n) := f(p)$. Уколико није овог облика, узимамо $\tilde{f}(n) = 1$. Овако дефинисана функција је мултипликативно периодична. Наиме, показаћемо да је њен „мултипликативни период“ 4, тј. да је $\tilde{f}(4m) = \tilde{f}(m)$ за све $m \in \mathbb{N}$. Нека је m произвољан природан број. Ако је он облика $4^l p$ за неки прост број p онда је и $4m$ такав и $\tilde{f}(m) = f(p) = \tilde{f}(4m)$. У супротном је $\tilde{f}(m) = 1$, но тада ни $4m$ не може бити облика $4^l p$ ($4m$ сигурно није прост, па ако би био тог облика, то би после скраћивања са 4 добили да је и m такав—приметимо да случај $l = 0$ *не* искључујемо), те је и $\tilde{f}(4m) = 1$. Овим је доказ завршен.

73. Бинарна релација на скупу A је подскуп од $A \times A$. Дакле, скуп свих бинарних релација на скупу $\mathcal{P}(\mathbb{R})$ је $\mathcal{P}(\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}))$. Дакле, кардиналност скупа свих бинарних релација на скупу $\mathcal{P}(\mathbb{R})$ је $2^{2^{\mathfrak{c}} \cdot 2^{\mathfrak{c}}} = 2^{2^{\mathfrak{c}}}$.

74. Подсетимо се да се n-арна релација на скупу $\mathbb{N}$ дефинише као подскуп од $\mathbb{N}^n$. Дакле, n-арних релација на скупу $\mathbb{N}$ има $2^{\aleph_0^n} = 2^{\aleph_0} = \mathfrak{c}$. Према томе *релација* на скупу $\mathbb{N}$ има $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$.

    Напомена: У формулацији задатка, тражи се да се одреди колико има свих релација на скупу $\mathbb{N}$. Дакле, унарних, бинарних, ...

75. Ознажимо са $\mathcal{E}$ скуп свих релација еквиваленције на $\mathbb{N}$. Јасно је да је $|\mathcal{E}| \leq \mathfrak{c}$ (погледајте решење претходног задатка). Означимо са $\mathcal{P}'(\mathbb{N})$ скуп свих подскупова од $\mathbb{N}$ који садрже 0. Јасно је да

постоји бијекција између овог скупа и скупа $\mathcal{P}(\mathbb{N}\setminus\{0\})$ (додавањем односно избацивањем нуле из датог скупа), те је $|\mathcal{P}'(\mathbb{N})| = \mathfrak{c}$. Дефинишимо функцију $\Phi\colon \mathcal{P}'(\mathbb{N})\setminus\{\mathbb{N}\} \to \mathcal{E}$ са $\Phi(A) = \rho_A$, где је релација ρ_A дефинисана са:

$$x\rho_A y \overset{\text{def}}{\iff} x, y \in A \text{ или } x, y \in A^c.$$

Ово наравно јесте релација еквиваленције и то таква да има само две класе еквиваленције — A и A^c (комплемент је у односу на скуп $\mathbb{N}$). Покажимо да је Φ „1–1“. Уколико је $\Phi(A) = \Phi(B)$, тј. $\rho_A = \rho_B$ то повлачи да су и скупови класа еквиваленције једнаки, тј. $\{A, A^c\} = \{B, B^c\}$. Закључујемо да је $A = B$ или $A = B^c$. Како B^c не садржи 0 (сада видимо зашто нам је то требало — наравно да смо могли да изаберемо и неки други елемент), то мора бити $A = B$ и добијамо да је Φ заиста „1–1“. Према томе, $|\mathcal{P}'(\mathbb{N})| = |\mathcal{P}'(\mathbb{N})\setminus\{\mathbb{N}\}| \leq |\mathcal{E}|$ и добијамо да је $|\mathcal{E}| = \mathfrak{c}$.

76. Искористићемо чињеницу да постоји бијекција између $2\mathbb{N}$ (скупа свих парних природних бројева) и скупа $\mathbb{N}$. Дефинишимо функцију $\Phi\colon \mathbb{N}^{2\mathbb{N}+1} \longrightarrow \mathcal{F}$ са $\Phi(g)(2n+1) = g(2n+1)$; $\Phi(g)(2n) = n$. Јасно је да је $\Phi(g)$ увек „на“, па $\Phi(g)$ заиста припада скупу $\mathcal{F}$. Како је $\Phi(g)$ заправо једно проширење функције g то је Φ „1–1“. Обратите пажњу на све ово: $\Phi(g)$ је функција из $\mathbb{N}$ у $\mathbb{N}$ и она је „на“; са друге стране Φ је функција из $\mathbb{N}^{2\mathbb{N}+1}$ у $\mathcal{F}$ и она је „1–1“. *Не тврдимо* да је Φ „на“! Φ и $\Phi(g)$ нису исти објекти! У сваком случају, добили смо да је Φ „1–1“, па је $|\mathcal{F}| \geq |\mathbb{N}^{2\mathbb{N}+1}| = {\aleph_0}^{\aleph_0} = \mathfrak{c}$. Како је и $|\mathcal{F}| \leq |\mathbb{N}^{\mathbb{N}}| = \mathfrak{c}$, то закључујемо да је $|\mathcal{F}| = \mathfrak{c}$.

77. Означимо са $\mathcal{P}_{\inf}(\mathbb{Z})$ скуп свих бесконачних подскупова од $\mathbb{N}$. Дефинишимо $\Phi\colon \mathcal{F} \longrightarrow \mathcal{P}_{\inf}(\mathbb{Z})$ са $\Phi(f) = f[\mathbb{N}]$. Приметимо да у случају да је f „1–1“, скуп $f[\mathbb{N}]$ мора бити бесконачан, па је наше пресликавање добро дефинисано. Оно је и „на“: сваки бесконачан подскуп од $\mathbb{Z}$ је у бијекцији са $\mathbb{N}$, па је тиме и слика неке „1–1“ функције из $\mathbb{N}$ у $\mathbb{Z}$. Не тврдимо наравно да је Φ „1–1“! Но, како је „на“, то добијамо $|\mathcal{F}| \geq |\mathcal{P}_{\inf}(\mathbb{Z})|$. Сваки подскуп од $\mathbb{Z}$ је или коначан или бесконачан (као уосталом и подскуп било ког скупа — ако је тај скуп коначан онда нема бесконачних подскупова!), кардиналност скупа свих коначних подскупова је $\aleph_0$, а кардиналност скупа свих подскупова је $\mathfrak{c}$. Према томе $|\mathcal{P}_{\inf}(\mathbb{Z})| = \mathfrak{c}$ из чега добијамо $|\mathcal{F}| = \mathfrak{c}$. Наведимо да смо задатак могли решити и коришћењем стандардног „трика“ којим од било које функције можемо добити „1–1“ функцију, ако променимо кодомен. Наиме, ако $f\colon X \to Y$, онда је функција $\hat{f}\colon X \to X \times Y$ дефинисана са $\hat{f}(x) = (x, f(x))$ обавезно „1–1“. Искористите то да бисте нашли друго решење овог задатка.

78. Означимо, за ову прилику, са $\mathcal{I}$ скуп свих „1–1“ функција из $\mathbb{N}$ у

$\mathbb{N}$. Показаћемо да постоји „1–1“ функција $\Phi: \mathcal{I} \to \mathcal{F}$, што је довољно да, уз претходне резултате, закључимо да је $|\mathcal{F}| = \mathfrak{c}$. Нека је $f \in \mathcal{I}$ било која „1–1“ функција; дефинишемо $\Phi(f) : \mathbb{N} \to \mathbb{N}$ на следећи начин. $\Phi(f)(2n) = 2f(n)$; $\Phi(f)(2n+1) = \min(\mathbb{N} \setminus (2f[\mathbb{N}] \cup \Phi(f)[\{1, \ldots, 2n-1\}]))$ (за $n = 0$, $\Phi(f)(1) = \min(\mathbb{N} \setminus f[2\mathbb{N}])$). Дакле, $\Phi(f)$ парне бројеве слика „помоћу“ функције f, док све што је остало $\Phi(f)$ „прекрије“ коришћењем непарних бројева. Јасно је да је сама Φ „1–1“: ако је $f \neq g$, онда се оне разликују у некој тачки n, но тада је и $\Phi(f)(2n) \neq \Phi(g)(2n)$. Са друге стране, функција $\Phi(f)$ је увек бијекција за сваку „1–1“ функцију f. Наиме, различити парни бројеви се сликају у различите, јер је f „1–1“. А ниједан непаран број се не слика у исти број као и неки паран, или неки непаран који је мањи од њега — тако је дефинисана функција $\Phi(f)$. Осим тога, $\Phi(f)$ је „на“: $\Phi(f)$ редом слика непарне бројеве у оне природне који нису већ „погођени“, тако да је за сваки $m \in \mathbb{N}$ сигурно испуњено да $m \in \Phi(f)[2\mathbb{N} \cup \{1, \ldots, 2m+1\}]$.

79. Приметимо пре свега да је нерастући низ природних бројева обавезно константан почев од неког члана. Уколико не би био константан почев од неког члана то бисмо могли да издвојимо неки његов строго опадајући подниз, а то је немогуће. Са C_k означимо све оне низове који су константни почев од индекса k (не тражимо да су нерастући). Таквих низова има

$$\underbrace{\aleph_0 \cdots \aleph_0}_{k+1} \cdot 1 \cdot 1 \cdots = \aleph_0.$$

Наиме првих $k+1$ чланова тог низа су произвољни, а остали су потпуно одређени. Но, тада је и унија свих C_k пребројива. Закључујемо да низова природних бројева који су константни почев од неког члана има пребројиво много, па стога има пребројиво много и нерастућих низова природних бројева.

80. Подсетимо се да је $(\mathbb{N} \setminus \{0\}, |) \cong (P, \leq_P)$, где је са P означен скуп свих низова природних бројева који су 0 почев од неког индекса, а релација $\leq_P$ задата је по координатама (погледајте одговарајући задатак из друге главе). Свака бијекција $\sigma : \mathbb{N} \to \mathbb{N}$ индукује и бијекцију $\Sigma : P \to P$ ($\Sigma(\langle x_n \rangle) = \langle x_{\sigma(n)} \rangle$), која је заправо аутоморфизам стуктуре $(P, \leq_P)$ (уверите се у то!). Како је кардиналност скупа свих бијекција из $\mathbb{N}$ у $\mathbb{N}$ једнака $\mathfrak{c}$ и како тражених аутоморфизама не може бити више од $\mathfrak{c}$ (зашто?), то је $|\mathrm{Aut}(\mathbb{N} \setminus \{0\}, |)| = \mathfrak{c}$.

81. Нека је x било који реалан број. Од којих се елемената састоји његова класа еквиваленције $C(x)$? Није тешко видети, с обзиром на дефиницију наше релације еквиваленције да је $C(x) = x + \mathcal{A}$, где смо са $\mathcal{A}$ означили скуп свих алгебарских бројева (ознаку смо увели само за ову ситуацију). Но, доказано је у тексту да

алгебарских бројева има пребројиво много, па добијамо да је за сваки $x \in \mathbb{R}$ $|C(x)| = \aleph_0$. Ако са κ означимо тражени кардинал, добијамо да је $\kappa \cdot \aleph_0 = |\mathbb{R}|$. Одавде следи да је $\kappa = \mathfrak{c}$.

82. Одредимо, као и у претходном задатку, класу еквиваленције елемента x. Знамо да $y \in C(x)$ **акко** $\sin x = \sin y$. Користећи својства синусне функције добијамо да тада мора бити $y = x + 2k\pi$, за неки цео број k или $y = \pi - x + 2k\pi$ за неки цео број k. Краћи запис: $C(x) = (x + 2\pi\mathbb{Z}) \cup (\pi - x + 2\pi\mathbb{Z})$. Дакле, $|C(x)| = \aleph_0$ за све $x \in \mathbb{R}$. Као и претходном задатку, закључујемо да је $|\mathbb{R}/_\sim| = \mathfrak{c}$.

83. Посматрајмо функцију $\Phi: \mathcal{F} \longrightarrow \mathbb{R}^{\mathbb{N}}$ дефинисану са $\Phi(f) = f|_{\mathbb{N}}$. Да ли је Φ „1–1“? Претпоставимо да је $\Phi(f) = \Phi(g)$. То значи да је $f|_{\mathbb{N}} = g|_{\mathbb{N}}$. То наравно не значи да је $f = g$, *али значи* да је $f \sim g$ (према нашој дефиницији релације $\sim$). Дакле, Φ није „1–1“, али $\tilde{\Phi}: \mathcal{F}/_\sim \longrightarrow \mathbb{R}^{\mathbb{N}}$ дефинисана са $\tilde{\Phi}([f]) = f_{|\mathbb{N}}$ јесте добро дефинисана и „1–1“ ($[f]$ означава класу еквиваленције функције f). Заправо је $\tilde{\Phi}$ и „на“: ако је $h: \mathbb{N} \to \mathbb{R}$ било која функција онда се она може продужити до функције $\hat{h}: \mathbb{R} \to \mathbb{R}$, нпр. можемо дефинисати $\hat{h}(x) = 1$ за све $x \in \mathbb{R} \setminus \mathbb{N}$ (сва продужења су еквивалентна у смислу релације $\sim$). Тада је $\tilde{\Phi}([\hat{h}]) = h$. Дакле $|\mathcal{F}/_\sim| = |\mathbb{R}^{\mathbb{N}}| = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

84. Свака функција са доменом и кодоменом $[0, 1]$ или је непрекидна или је прекидна. Шта значи да је функција прекидна? Па то значи да она није непрекидна бар у једној тачки. Ако са κ означимо кардиналност тог скупа, онда, уз коришћење чињенице да је кардиналност скупа свих непрекидних функција $\mathfrak{c}$, добијамо једнакост $\mathfrak{c}^{\mathfrak{c}} = \mathfrak{c} + \kappa$. Како је је $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}} > \mathfrak{c}$, то добијамо да мора бити $\kappa = 2^{\mathfrak{c}} > \mathfrak{c}$.

85. Означимо са $\mathcal{P}_\omega(\mathbb{R})$ скуп свих највише пребројивих подскупова од $\mathbb{R}$. $f: \mathbb{R}^{\mathbb{N}} \longrightarrow \mathcal{P}_\omega(\mathbb{R})$, задата са $f(x_0, x_1, \ldots) = \{x_0, x_1, \ldots\}$ јесте „на“ (не тврдимо наравно да је и „1–1“). То значи да је $|\mathcal{P}_\omega(\mathbb{R})| \leq |\mathbb{R}^{\mathbb{N}}| = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$. Но, јасно је да је $\mathcal{P}_\omega(\mathbb{R}) \geq \mathfrak{c}$ (већ једночланих подскупова има толико!), па добијамо да је тражена кардиналност $\mathfrak{c}$.

Додатак I

Парадокс Банаха и Тарског

У овом додатку искључиво се посвећујемо разматрању чувеног парадокса Банаха[1] и Тарског[2] а који, у најкраћем, тврди да се сфера (односно кугла) у тродимензионом простору може разбити на подскупове, који се затим могу тако ротирати да се од њих саставе две сфере (односно кугле) истог полупречника као и полазна. Дакле, од једног објекта добијамо два иста таква! Видећемо како се до тога долази.

Пре свега, потребно је да обновимо (или научимо, у зависности од предзнања!) неке појмове из алгебре.

Под слободном групом ранга 2 подразумева се група F_2 за коју постоје елементи $x, y \in F_2$ такви да је сваки елемент у групи производ елемената из скупа $\{x, x^{-1}, y, y^{-1}\}$ при чему не важи ниједна нетривијална релација (дакле нека релација која није последица аксиома групе) међу тим елементима. На пример, важи релација $xxx^{-1}y = xy$, јер она следи из чињенице да је производ xx^{-1} једнак неутралу, док не сме важити релација попут ове $xxyyy = yx$, јер она не следи из аксиома групе. Заправо се сваки елемент групе може написати на јединствен начин у облику производа $g_1g_2\cdots g_n$, за неки природан број n (уколико је $n = 0$, тада је у питању неутрал групе), при чему су елементи g_i из горе наведеног скупа и $g_{i+1} \neq g_i^{-1}$ (наравно да овде подразумевамо да је $(x^{-1})^{-1} = x$).

Уколико вам појам слободне групе и није био познат, онда вам је из курса Алгебре 1 сигурно познат појам дејства групе на скупу. Подсетимо се укратко тог појма. Група G дејствује на скупу X, ако постоји пресликавање $\Theta : G \times X \to X$, тако да за све $x \in X$ важи: $\Theta(1, x) = x$ (са 1 смо означили неутрал у групи) и за све $x \in X$ и све $g, h \in G$ $\Theta(g, \Theta(h, x)) = \Theta(gh, x)$. Присетимо се још да уместо $\Theta(g, x)$ пишемо $g \cdot x$ и да се *орбита* елемента x дефинише као скуп $\{g \cdot x : g \in G\}$. Један

[1] Stefan Banach (1892–1945), пољски математичар.

[2] Alfred Tarski (1902–1983) (рођен као Alfred Teitelbaum, променио име 1923.), пољски (и амерички) логичар.

од најосновнијих примера дејства групе је дејство групе на самој себи множењем. Уведимо још и следећу ознаку. Нека је $A \subseteq X$ (G дејствује на X).

$$g \cdot A = \{g \cdot a : a \in A\}.$$

Пређимо сада на нове појмове и резултате који нас воде ка доказу резултата Банаха и Тарског.

Дефиниција I.1 Нека група G дејствује на скупу X. За $E \subseteq X$ кажемо да је $G-$*парадоксалан* уколико за неке природне бројеве m, n постоје дисјунктни подскупови $A_1, \ldots, A_m, B_1 \ldots, B_n$ скупа E и елементи $g_1, \ldots, g_m, h_1, \ldots, h_n$ групе G за које је

$$E = \bigcup_{i=1}^{m} g_i \cdot A_i \qquad \text{и} \qquad E = \bigcup_{j=1}^{n} h_j \cdot B_j.$$

Дакле, скуп је $G-$парадоксалан уколико је могуће изабрати неке његове дисјунктне подскупове, које затим поделимо у две групе, „завртимо“ скупове из било које од те две групе погодно изабраним елементима из G и добијемо цео скуп E. Тако заправо добијамо две копије скупа E полазећи од неких његових подскупова. Но, ниједан појам уведен неком дефиницијом није користан, ако не постоје добри примери. Следећи став је баш томе посвећен.

Став I.2 а) Слободна група F_2 ранга 2 је F_2-парадоксална;
б) Ако група G дејствује на X без фиксних тачака и ако је она $G-$парадоксална, онда је и сам скуп X један $G-$парадоксалан скуп.

Доказ. а) Нека су генератори наше групе елементи x и y. Видели смо како се сваки елемент те групе може представити. Означимо са $w(x)$ скуп свих елемената групе који „почињу“ са x у том представљању. Аналогно дефинишемо и скупове $w(x^{-1})$, $w(y)$ и $w(y^{-1})$. Јасно је да је

$$F_2 = \{1\} \cup w(x) \cup w(x^{-1}) \cup w(y) \cup w(y^{-1}),$$

при чему је ово унија дисјунктних скупова. Но, јасно је и да је

$$F_2 = 1 \cdot w(x) \cup x \cdot w(x^{-1}).$$

Наиме, ако $g \notin w(x)$, онда је $g = x \cdot (x^{-1}g)$, а елемент $x^{-1}g$ сигурно припада $w(x^{-1})$, јер g не почиње са x, па се то x^{-1} није могло „скратити“. Слично је и

$$F_2 = 1 \cdot w(y) \cup y \cdot w(y^{-1}),$$

па закључујемо да је F_2 заиста F_2-парадоксалан.
б) Појаснимо најпре шта подразумевамо под тврдњом да група дејствује на скупу X без фиксних тачака. То заправо значи да је за све $g \in G \setminus \{1\}$ и $x \in X$ испуњено $g \cdot x \neq x$. Наведимо да се такво дејство често назива и *слободно дејство*.

По претпоставци постоје дисјунктни скупови $A_1, \ldots, A_m, B_1 \ldots, B_n$ групе G и елементи $g_1 \ldots, g_m, h_1 \ldots, h_n$ те групе тако да важи

$$G = \bigcup_{i=1}^{m} g_i \cdot A_i \qquad \text{и} \qquad G = \bigcup_{j=1}^{n} h_j \cdot B_j.$$

Како су орбите при дејству групе G на скупу X дисјунктне, то према Аксиоми избора постоји скуп C који има тачно по један елемент из сваке орбите. Према избору скупа C важи једнакост

$$X = G \cdot C (= \{g \cdot c : c \in C\}),$$

јер је X унија свих орбита. Како је $G = \bigcup_{i=1}^{m} g_i \cdot A_i$, то добијамо да је

$$X = \bigcup_{i=1}^{m} g_i \cdot (A_i \cdot C).$$

Слично је и

$$X = \bigcup_{j=1}^{n} h_j \cdot (B_j \cdot C).$$

За завршетак доказа довољно је да покажемо да су скупови $A_1 \cdot C, \ldots, A_m \cdot C, B_1 \cdot C, \ldots, B_n \cdot C$ међусобно дисјунктни. Нека нпр. за неке i, j такве да је $i \neq j$ важи

$$(A_i \cdot C) \cap (A_j \cdot C) \neq \emptyset.$$

Дакле, постоје елементи $g \in A_i$, $c \in C$, $g' \in A_j$ и $c' \in C$, такви да је

$$g \cdot c = g' \cdot c'.$$

Но, одатле следи да је $c' = ((g')^{-1} g) \cdot c$ из чега би следило да су c и c' из исте орбите. Како скуп C има тачно по један елемент из сваке орбите, закључујемо да је $c = c'$. Но, тада добијамо да је $c = ((g')^{-1} g) \cdot c$, а како група дејствује без фиксних тачака добијамо да је $(g')^{-1} g) = 1$, односно $g' = g$, што није могуће, јер су скупови A_i и A_j дисјунктни за $i \neq j$. На исти начин показује се да су и преостали парови скупова дисјунктни што завршава доказ. $\square$

Подсетимо се неких ознака. Са $O(3)$ означава се група свих ортогоналних оператора простора $\mathbb{R}^3$, која се, избором стандардне базе тог простора може идентификовати са групом свих ортогоналних матрица реда 3. Дакле, ако је задата матрица $A \in M_3(\mathbb{R}^3)$ она одређује оператор $L_A : \mathbb{R}^3 \to \mathbb{R}^3$, са

$$L_A(X) = AX,$$

где је са X означен вектор из $\mathbb{R}^3$ записан у облику колоне. Ортогоналне матрице су оне матрице код којих колоне (или врсте) чине ортонормирани систем вектора. Оператор индукован ортогоналном матрицом је *изометрија*, тј. растојање између слика једнако је растојању између оригинала. Производ две ортогоналне матрице је ортогонална матрица, јединична матрица је ортогонална, а такође је и свака ортогонална матрица инвертибилна и њен инверз је такође ортогонална матрица. Стога ове матрице и чине групу. Геометријски посматрано, сваки елемент из те групе или одређује неку ротацију (дакле око неке праве и за неки угао), или је рефлексија . Нас ће интересовати искључиво ротације — то ће бити оне матрице чија је детерминанта једнака јединици и та се подгрупа означава са $SO(3)$ и зове специјална ортогонална група. За даљи рад потребна нам је следећа теорема.

Теорема I.3 Група $SO(3)$ садржи као своју подгрупу слободну групу ранга 2.

Доказ. Дакле, потребно је наћи две ротације Φ, Ψ такве да међу њима не важе никакве релације које нису последице аксиома групе. Подгрупа $F = \langle \Phi, \Psi \rangle$ групе $SO(3)$ генерисана тим елементима биће тражена подгрупа. Ротација Φ биће ротација у позитивном смеру око $z-$осе за угао $\arccos \frac{1}{3}$, док је ротација Ψ ротација у позитивном смеру око $x-$осе за исти угао. Матрице (и одговарајуће инверзне матрице) које репрезентују ове ротације, такође ћемо означавати истим словима и оне су дате са

$$\Phi^{\pm 1} = \begin{bmatrix} \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \Psi^{\pm 1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{bmatrix}.$$

Наиме, матрица која одговара ротацији за угао θ у равни xOy је матрица

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

С обзиром да при ротирању око $z-$осе, та оса остаје фиксирана, то је ротација око те осе задата матрицом

$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Но, $\cos(\arccos \frac{1}{3}) = \frac{1}{3}$, док је $\sin(\arccos \frac{1}{3}) = \frac{2\sqrt{2}}{3}$ те добијамо наведене форме.

Да бисмо показали да је подгрупа генерисана ротацијама Φ и Ψ слободна, довољно је да покажемо да ниједан производ облика $\mathrm{P}_1\mathrm{P}_2\cdots\mathrm{P}_n$ где је за свако $i \in \{1, \ldots, n\}$ $\mathrm{P}_i \in \{\Phi, \Phi^{-1}, \Psi, \Psi^{-1}\}$ при чему два узастопна члана у производу нису облика $\mathrm{P}\mathrm{P}^{-1}$, није једнак јединичној матрици. Уколико би он био једнак јединичној матрици, а не би се завршавао са $\Phi^{\pm 1}$, то бисмо га могли коњуговати са Φ, тј. уместо производа Π имали бисмо производ $\Phi\Pi\Phi^{-1}$, који би био једнак јединичној матрици акко би Π био такав, а завршавао би се са Φ^{-1}. Дакле, можемо претпоставити да се тај производ завршава са Φ или Φ^{-1}.

Да бисмо показали да такав производ Π никада није једнак јединици показаћемо да важи следеће:

$$\Pi \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{3^n} \begin{bmatrix} a \\ b\sqrt{2} \\ c \end{bmatrix},$$

где је n број чинилаца у производу, a, b, c цели бројеви при чему b <u>није</u> дељиво са 3. Будући да је 0 <u>дељиво</u> са 3, то закључујемо да Π никада није јединична матрица. Доказ горње једнакости извешћемо индукцијом по броју чиниоца у производу.

Претпоставимо да се производ Π састоји само од једног елемента. По облику производа закључујемо да је $\Pi = \Phi^{\pm 1}$. Но, директна провера даје

$$\Phi^{\pm 1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 \\ \pm 2\sqrt{2} \\ 0 \end{bmatrix}.$$

Нека је број чинилаца у производу n и нека је наведена једнакост тачна за сваки производ у наведеном облику са мање од n чинилаца. Покажимо најпре да су бројеви a, b, c који се појављују у наведеној једнакости заиста цели. Овде се ради о простој провери. Наш производ Π је облика $\Pi = \Phi^{\pm 1}\Pi'$, или $\Pi = \Psi^{\pm 1}\Pi'$. По претпоставци је

$$\Pi' \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{3^{n-1}} \begin{bmatrix} a' \\ b'\sqrt{2} \\ c' \end{bmatrix}.$$

Но,

$$\Phi^{\pm 1} \frac{1}{3^{n-1}} \begin{bmatrix} a' \\ b'\sqrt{2} \\ c' \end{bmatrix} = \frac{1}{3^n} \begin{bmatrix} a' \mp 4b' \\ (b' \pm 2a')\sqrt{2} \\ 3c' \end{bmatrix};$$

$$\Psi^{\pm 1} \frac{1}{3^{n-1}} \begin{bmatrix} a' \\ b'\sqrt{2} \\ c' \end{bmatrix} = \frac{1}{3^n} \begin{bmatrix} 3a' \\ (b' \mp 2c')\sqrt{2} \\ c' \pm 4b' \end{bmatrix}.$$

Дакле, заиста се ради о целим бројевима. Да бисмо се уверили да 3 не дели b, морамо се вратити за још један корак тј. размотрити случајеве.

1. $\Pi = \Phi^{\pm 1}\Psi^{\pm 1}\Pi''$

2. $\Pi = \Psi^{\pm 1}\Phi^{\pm 1}\Pi''$

3. $\Pi = (\Phi\Phi)^{\pm 1}\Pi''$

4. $\Pi = (\Psi\Psi)^{\pm 1}\Pi''$

Наравно да овде нећемо проверавати све могућности. За пример наведимо шта се дешава у трећем случају. Користећи раније добијене резултате видимо да добијамо следеће везе

$$a = a' \mp 4b' \qquad a' = a'' \mp 4b''$$

$$b = b' \pm 2a' \qquad b' = b'' \pm 2a''$$

Одавде добијамо да је

$$\begin{aligned} b &= b' \pm 2a' \\ &= b' \pm 2(a'' \mp 4b'') \\ &= b' \pm 2a'' - 8b'' \\ &= b' + b'' \pm 2a'' - 9b'' \\ &= 2b' - 9b'', \end{aligned}$$

а како, по претпоставци, $3 \not| \, b'$, то добијамо да $3 \not| \, b$. Читаоцима остављамо да провере остале случајеве. □

Мада група $SO(3)$, која садржи као своју подгрупу слободну групу ранга 2, дејствује на јединичној сфери S^2, Став **I**.2 не можемо непосредно применити, јер то дејство има фиксних тачака. Наиме, свака ротација не помера тачке са осе ротације, те су стога тачке продора осе ротације и сфере фиксиране при овом дејству. Но,ових тачака има пребројиво много (група F_2 је пребројива), па њиховим избацивањем добијамо следећу теорему.

Теорема I.4 (Хауздорфов[3] парадокс) Постоји пребројив подскуп Ω на сфери S^2 такав да је скуп $S^2 \setminus \Omega$ један $F-$парадоксалан скуп.

Доказ. Нека је Ω скуп свих фиксних тачака ротација из F. Довољно је показати да F дејствује на скупу $S^2 \setminus \Omega$, тј. да је $g \cdot x \notin \Omega$ за сваку ротацију $g \in F$ и све $x \notin \Omega$. Но, то није тешко доказати.

Претпоставимо супротно, тј. нека постоје $g \in F$ и $x \notin \Omega$ тако да важи: $g \cdot x \in \Omega$. То значи да постоји $f \in F$ тако да је $f \cdot (g \cdot x) = g \cdot x$. Одавде добијамо $g^{-1} \cdot (f \cdot (g \cdot x)) = g^{-1} \cdot (g \cdot x)$, из чега применом особина дејства групе добијамо $(g^{-1} f g) \cdot x = x$, а како $g^{-1} f g \in F$, то закључујемо да $x \in \Omega$ што је супротно претпоставци. □

Преостаје да некако са скупа $S^2 \setminus \Omega$ пређемо на S^2. У ту сврху увешћемо појам $G-$*подједнаке раставаљивости*.

[3] Felix Hausdorff (1868–1942), немачки математичар.

Дефиниција I.5 Нека група G дејствује на скупу X. За подскупове A, B скупа X кажемо да су $G-$*подједнако растављиви* уколико постоје подскупови $A_1, \ldots, A_n$ скупа A, $B_1, \ldots, B_n$ скупа B и елементи $g_1, \ldots, g_n \in G$ тако да важи

$$A = A_1 \sqcup \ldots \sqcup A_n, \quad B = B_1 \sqcup \ldots \sqcup B_n, \quad g_i \cdot A_i = B_i, \text{ за } i = \overline{1, n}.$$

Ознака $\sqcup$ наравно означава унију дисјунктних скупова. Ако су скупови A и B $G-$подједнако растављиви користићемо ознаку $A \sim_G B$. Није тешко видети да је овако уведена релација $\sim_G$ релација еквиваленције. Једино што није потпуно тривијално за доказивање је транзитивност те релације. У ту сврху, претпоставимо да је $A \sim_G B$ и $B \sim_G C$. То значи да постоје подскупови $A_1, \ldots, A_m \subseteq A$, $B_1 \ldots, B_m \subseteq B$ и елементи $g_1, \ldots, g_m \in G$ такви да је за све $i = \overline{1, m}$: $g_i \cdot A_i = B_i$, а такође и подскупови $B'_1, \ldots, B'_n \subseteq B$, $C_1, \ldots, C_n \subseteq C$, односно елементи $h_1, \ldots, h_n \in G$, такви да је за све $j = \overline{1, n}$: $h_j \cdot B'_j = C_j$. Формирајмо скупове $B_{ij} = B_i \cap B'_j$ за све могуће вредности индекса i и j. Тада, ако са A_{ij} означимо скупове $g_i^{-1} \cdot B_{ij}$ и са C_{ij} скупове $h_j \cdot B_{ij}$ видимо да важи $A \sim_G C$ ($(h_j g_i) \cdot A_{ij} = C_{ij}$).

Докажимо најпре следећу техничку лему.

Лема I.6 Скуп E је $G-$парадоксалан ако и само ако постоје дисјунктни скупови $A, B \subseteq E$ такви да је $E \sim_G A$ и $E \sim_G B$.

Доказ. $\Longrightarrow$: Како је, по претпоставци, скуп E један $G-$парадоксалан скуп, то постоје дисјунктни подскупови $A_1, \ldots, A_m, B_1 \ldots, B_n$ скупа E и елементи $g_1, \ldots, g_m, h_1, \ldots, h_n$ групе G за које је

$$E = \bigcup_{i=1}^{m} g_i \cdot A_i \qquad \text{и} \qquad E = \bigcup_{j=1}^{n} h_j \cdot B_j.$$

Нама је потребно да скупови $g_i \cdot A_i$ буду дисјунктни (такође и скупови $h_j \cdot B_j$). У ту сврху, задржимо скуп A_1 и посматрајмо скуп $g_2 \cdot A_2$. Ако је $g_2 \cdot A_2 \cap g_1 \cdot A_1 \neq \emptyset$, то из скупа A_2 избацимо све елементе које елемент g_2 пребацује у неки елемент из $g_1 \cdot A_1$. Ако на исти начин поступимо са елементима из $A_3, \ldots, A_m$, то добијамо тражене подскупове. Њихова унија је тражени скуп A. На исти начин добијамо и скуп B.
$\Longleftarrow$: Овај смер је једноставан и остављамо га читаоцима за вежбу. $\square$

Наведимо сада још једну лему чији је доказ сличан доказу транзитивности релације $\sim_G$ и стога ћемо га изоставити.

Лема I.7 Нека група G дејствује на скупу X. Ако су $E, E' \subseteq X$ такви да је $E \sim_G E'$ и E је $G-$парадоксалан, тада је E' такође $G-$парадоксалан.

За доказ парадокса Банаха и Тарског за случај јединичне сфере S^2 потребна нам је само још следећа лема.

Лема I.8 Нека је D пребројив подскуп од S^2. Тада постоји ротација $\Sigma \in SO(3)$ таква, да ако са F' означимо подгрупу $\langle\Sigma\rangle$ групе $SO(3)$ генерисану са Σ, то је $S^2 \sim_{F'} S^2 \setminus D$.

Доказ. Како је скуп D пребројив, а S^2 непребројив, то постоји права ℓ која пролази кроз координатни почетак и не садржи ниједну тачку из D. Посматрајмо скуп U, свих могућих углова θ таквих да ротација око осе ℓ за неки целобројни умножак $n\theta$ тог угла преводи неку тачку из D у неку тачку из D. Није тешко уверити се да је скуп U пребројив (доказ те чињенице остављамо читаоцу). Изаберимо неки угао из $(0, \pi)$ који не припада том скупу и означимо са Σ ротацију око праве ℓ за тај угао у неком смеру (свеједно је који смер бирамо). Тада, према избору осе и угла ротације важи:

$$\text{за све } n \in \mathbb{Z} : (\Sigma^n \cdot D) \cap D = \emptyset.$$

Из ове чињенице следи и да је $(\Sigma^m \cdot D) \cap (\Sigma^n \cdot D) = \emptyset$ за све $m, n \in \mathbb{Z}$, за које је $m \neq n$. Нека је скуп $\overline{D}$ дат са

$$\overline{D} = \bigcup_{n \in \mathbb{N}} \Sigma^n \cdot D.$$

Због горе наведених особина јасно је да је $\Sigma \cdot \overline{D} = \overline{D} \setminus D$. Дакле

$$S^2 = \overline{D} \cup (S^2 \setminus \overline{D}) \sim_{F'} \Sigma \cdot \overline{D} \cup (S^2 \setminus \overline{D}) = S^2 \setminus D.$$

□

Нека је $F'' = \langle\Phi, \Psi, \Sigma\rangle$ подгрупа групе $SO(3)$ генерисана наведеним ротацијама. Формулишимо напокон парадокс Банаха и Тарског у облику следеће теореме.

Теорема I.9 Сфера S^2 је $F''-$парадоксална.

Доказ. Показали смо да је $S^2 \setminus \Omega$ један $F-$парадоксалан скуп (тиме је наравно и $F''-$парадоксалан — погледајте дефиницију $G-$парадоксалности). Но, претходна лема даје (уколико за скуп D узмемо баш Ω) $S^2 \sim_{F'} S^2 \setminus \Omega$, па је тада и $S^2 \sim_{F''} S^2 \setminus \Omega$. Лема **I**.7 завршава доказ. □

Може се сличан резултат доказати и за јединичну куглу у тродимензионалном простору, али тај доказ нећемо наводити.

Додатак II

Почеци теорије скупова

У овом невеликом историјском осврту покушаћемо да прикажемо како се развио савремени поглед на бесконачне скупове и како су скупови постали основа на којој градимо савремену математику.

Наше излагање започињемо кратким освртом на рад Бернарда Болцана[1].

Сигурно најпознатије дело овог математичара је његов рад из 1817. године у којем је доказао теорему да свака непрекидна функција узима све међувредности и која је сигурно свим студентима позната из курса математичке анализе (сличан доказ је касније дао и Коши[2] у свом *Курсу анализе*, те је зато та теорема и позната као Болцано-Кошијева теорема).

Но, ми се нећемо задржавати на овом раду, но на његовој постхумно објављеној расправи *Парадокси бесконачног* (1851). До овог рада, чак и велики математичари попут Даламбера и Гауса[3], су избегавали да прихвате стварно постојање бесконачног, но су о појму бесконачности писали као о *начину изражавања*, у контексту променљивих величина које могу узимати произвољно велике вредности и слично. Болцано у овој својој расправи истиче да бесконачни објекти заиста постоје. На пример, он овде наводи да је реална права бесконачна, а није променљива. Такође наводи и следећи пример (скоро идентичан пример је касније навео и Дедекинд у својој дискусији о бесконачним скуповима, а о којој ће касније бити више речи): скуп свих истина је бесконачан. Наиме, узмимо било које истинито тврђење A. Онда можемо формирати ново тврђење B, које није идентично старом: „A је истинито". Дакле, на тај начин добијамо ново истинито тврђење B и потом C итд. Он указује да тако добијамо бесконачно много тврђења, а и истиче сличност формирања ових тврђења формирању скупа свих (природних) бројева.

[1] Bernard Bolzano (1781–1848), чешки филозоф и математичар .
[2] Augustin-Louis Cauchy (1789–1857), француски математичар .
[3] Johann Carl Friedrich Gauss (1777–1855), немачки математичар.

Најзанимљивији део за ову нашу причу је вероватно следећи пример, који Болцано наводи. Он разматра два скупа: све реалне бројеве (за њега, све *величине*) између 0 и 5 и све реалне бројеве између 0 и 12 и истиче да постоји бијекција (овде користимо савремену терминологију, Болцано није то тако исказао) између ова два скупа задата једначином $5y = 12x$. Но, он нажалост пропушта могућност да препозна појам кардиналности бесконачних скупова, него истиче да ипак не можемо те скупове сматрати једнаким у односу на бројност својих чланова, пошто, тако каже Болцано, елементима 3 и 4 одговарају елементи $7\frac{1}{5}$ и $9\frac{3}{5}$ и док су елементи 3 и 4 на растојању 1, дотле су елементи који њима одговарају на растојању $2\frac{2}{5}$. И стога те скупове он не сматра истобројним. Очигледно је да код њега још увек превелики значај имају метричка својства. Из других примера које наводи види се да и Еуклидово „цело је веће од свог дела“ има велики утицај на њега, чак и у разматрањима која се тичу бесконачних скупова (и сума). Занимљиво је да он чак понегде истиче да скупови могу имати исте елементе, а да су ипак различити! Наводи као пример крчаг и разбијени крчаг. Очигледно је да апстрактан појам скупа није још присутан код њега.

На крају треба још истаћи да Болцанови радови нису били довољно познати у своје време, па чак ни доста касније те да стога нису имали значајан утицај на развој математике тога времена.

Први велики математичар (Болцано је као математичар имао одређени значај, али сигурно се не би могло рећи да је био велики математичар), који је имао значајан утицај на развој теорије скупова био је свакако Риман[4].

Риманов живот је био нажалост кратак, али изузетно плодотворан са математичке тачке гледишта. Он је започео студије на универзитету у Гетингену 1846. године да би године од 1847 до 1849 провео у Берлину где је имао прилику да учи од Јакобија и Дирихлеа. По повратку у Гетинген започела је једна од сигурно најуспешнијих деценија у историји математике. Риман је одбранио докторат 1851. године из области комплексне анализе и у том докторату је увео појам Риманове површи. Године 1853, предао је своју тезу за хабилитацију на тему Фуријеових[5] редова, у оквиру које је прецизирао појам интеграла. Наредне године је одржао своју лекцију за хабилитацију о нееуклидској геометрији у којој је увео појам многострукости и са којом се може рећи да започиње модерни развој диференцијалне геометрије. Значајан рад о Абеловим функцијама објавио је 1857. године, а рад о зета функцији 1859. године. Читаоцу је сигурно јасно да би за приказ свих ових радова и њиховог значаја, била сигурно потребна не једна, но више *књига*, али ми ћемо се у нашем историјском осврту задржати само на на најважнијим елементима који се тичу теорије скупова.

[4] Georg Friedrich Bernhard Riemann (1826–1866), немачки математичар.
[5] Jean Baptiste Joseph Fourier (1768–1830), француски математичар.

Први Риманов утицај на развој теорије скупова је садржан у његовој лекцији за хабилитацију, коју је имао обавезу да одржи да би добио одобрење да предаје у Гетингену. У ту сврху он је понудио три теме и Гаус је, што је било неуобичајено, одабрао да Риман одржи лекцију на трећу тему. И Римана је то изненадило (у писму свом брату је писао да је припремио прве две теме добро и да се надао да ће Гаус изабрати неку од њих, али да сада мора да припреми и предавање за ту трећу тему). Ово предавање је одржано 10. јуна 1854. године и наслов је био: *О хипотезама које леже у основи геометрије.* Сам Гаус, који је предложио тему, био је веома импресиониран Римановим излагањем.

Како је предавање било замишљено за ширу публику, у њему није било техничких резултата, као што би се популарно рекло „није било много формула“, но било је богато дубоким и новим идејама. У њему је Риман увео појам *многострукости*, на немачком *Mannigfaltigskeit*, као *n-тоструко проширене величине.* Ту је практично дата савремена дефиниција многострукости — (тополошки) простор, који је локално еуклидски простор од n димензија. Дискутовано је о појму растојања, дужине кривих и уопште о рачуну у таквим просторима. Треба истаћи да је Риман ту успутно навео и могућност разматрања, тј. постојања и бесконачно димензионалних многострукости (многострукости чије су тачке функције, за које је потребно задавање бесконачно много *величина*, другим речима вредности функција). Но, за нашу причу је значајно то што Риман разликује *непрекидне* многострукости и *дискретне* многострукости. Он каже да су *индивидуалне специјализације* непрекидних многострукости тачке, а дискретних, елементи многострукости. Заправо, може се рећи да је он овим својим радом желео да учини и више од онога што је садржано у самом наслову. Док би се за непрекидне многострукости могло рећи да представљају истинску расправу о геометријском простору, дотле дискретне многострукости заправо представљају први почетак заснивања свих појмова математике на појму скупа. Наиме, дискретна многострукост није ништа друго него скуп (Кантор, под очигледним утицајем Риманових идеја, у својим првим радовима посвећеним скуповима *није* користио за скупове термин *Menge*, но Риманов термин *Mannigfaltigskeit*). Ово Риманово предавање није било одмах доступно широј публици. Заправо, оно је објављено тек 1868. године, две године после Риманове смрти и имало је изванредан утицај на развој математичара те и будућих генерација.

Док се у овом Римановом предавању о геометрији налази клица каснијег заснивања математике на појму скупа и оно као такво представља методолошко-филозофску основу за почетак развоја теорије скупова, дотле његова хабилитациона теза, која је посвећена разматрању Фуријеових редова, представља конкретну основу на којој су започела истраживања која су довела до развоја апстрактне теорије скупова, основних тополошких појмова, као и теорије мере. Стога ћемо посветити пажње и тој тези.

Да бисмо боље схватили проблеме који су се истраживали, морамо да се вратимо мало уназад у времену, до Ојлера[6].

У свом *Уводу у анализу бесконачности* из 1748. године, он је дефинисао функцију променљиве величине као „аналитички израз“, који је на произвољан начин направљен од те променљиве и разних константи. Дакле, за функцију је неопходно да има запис у облику формуле. Но, он је у свом ранијем раду из 1734. у области парцијалних диференцијалних једначина допуштао и могућност да функција буде „прекидна“, тј. да нема јединствен аналитички запис у целој области, него да *криве* које представљају график функције буду састављене од више делова са потенцијално различитим аналитичким записом. То је истакао и у расправи са Д'Аламбером[7], који је 1747. показао да једначина струне која осцилује има решење $F(x,t) = \frac{1}{2}(f(x+t)+f(x-t))$. Даламбер је истицао да f мора бити „непрекидна“, тј. да има јединствен аналитички запис, док је Ојлер сматрао да може да буде и прекидна у горе наведеном смислу те речи. У ту дискусију се укључио и Данијел Бернули[8], који је на основу физичког разматрања о струни која осцилује, навео да функција f мора бити представљива у облику реда

$$f(x) = a_1 \sin(\pi x/L) + a_2 \sin(2\pi x/L) + \cdots,$$

где је L дужина струне. Са математичке тачке гледишта, Бернулијево тврђење се своди на то да се свака функција може представити тригонометријским редом. То тврђење је већина водећих математичара одбацила.

Но, Фурије, најпре у свом раду о провођењу топлоте из 1807, који није објављен, а потом у свом значајном делу *Аналитичка теорија топлоте* из 1822, враћа се на ту идеју. Заправо, он тврди да се свака ограничена функција f на $(-\pi, \pi)$ може представити у облику

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} \left(a_n \cos(nx) + b_n \sin(nx)\right), \qquad (*)$$

где су коефицијенти задати са

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)dx, \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)dx.$$

Наравно, ово су сада свима добро познате формуле из теорије Фуријеових редова.

Фурије говори о произвољној функцији, али се из његовог излагања види да ипак размишља на начин својих претходника. На пример, њему је функција задата са e^{-x} за ненегативне x , а са e^{x} за негативне

[6]Leonhard Euler (1707–1783), швајцарски математичар.
[7]Jean le Rond d'Alembert (1717–1783), француски математичар.
[8]Daniel Bernoulli (1700–1782), швајцарски математичар.

x (другим речима, функција $e^{-|x|}$) „прекидна“ пошто је задата помоћу два аналитичка израза.

Он је заправо дао два доказа свог тврђења о развоју произвољне функције у тригонометријски ред. У првом доказу је претпоставио да се функција може развити у степени ред и затим решавајући систем од бесконачно много једначина са бесконачно много непознатих, дошао до траженог развоја. У другом доказу он разматра „произвољну“ функцију (претпоставља се да је ограничена) и полази од једначине $(*)$. Множењем те једначине са $\cos(nx)$ и $\sin(nx)$ и интеграцијом (при чему интеграл пролази кроз суму) он добија коефицијенте у наведеном облику и тиме тврди да је функција f заиста представљена тим тригонометријским редом. Много се примедби може навести у вези таквог „доказа“. Пре свега, није јасно зашто се ред може интегралити члан по члан, зашто чак и када се интеграли члан по члан, наведени интеграли постоје и напокон, зашто тако одређени коефицијенти заиста дају тригонометријски ред чија је сума једнака датој функцији. Дакле, много је примедби, а Фурије је покушао да оправда постојање интеграла о којима је реч. Наиме, он је објаснио да је функција $f(x)\sin x$ која се добија множењем произвољне функције функцијом синус сличног понашања као и синусна функција, она само представља синус који је „увећан“ за одговарајући фактор (као да имамо осцилацију тако да величина амплитуде варира у свакој тачки) и да онда интеграл јесте задат површином. Но, није дао објашњење зашто та површина постоји.

Дакле, модерни концепт непрекидне функције се сигурно не може наћи код Фуријеа и заправо се први пут појављује код Кошија. У свом *Курсу анализе*, он уводи појам непрекидности на следећи начин. функција f, која је дефинисана и ограничена на одсечку $[a, b]$ је непрекидна унутар тих граница уколико за x из тог одсечка „нумеричка вредност разлике $f(x+\alpha) - f(x)$ бесконачно опада како то чини α“. Дакле, Коши дефинише не појам непрекидности у тачки, него непрекидности на одсечку. Заправо се појам непрекидности и појам равномерне непрекидности код њега не разликују. Године 1823, Коши дефинише одређени интеграл непрекидне функције помоћу интегралних сума. Он наиме разматра поделу одсечка $a = x_0 < x_1 < x_2 < \cdots < x_{n-1} < x_n = b$ и суму $S = \sum_{i=1}^{n}(x_i - x_{i-1})f(x_i)$. Уз коришћење равномерне непрекидности функције f (као што је горе напоменуто), он показује да су за поделе чија је норма довољно мала (норма поделе је наравно максимална дужина интервала поделе) и одговарајуће суме произвољно близу и закључује да постоји јединствени лимес и тај лимес је заправо одређени интеграл. Он у даљем, за непрекидну функцију f, разматра и функцију $F(x) = \int_0^x f$ и количник $\frac{F(x+h)-F(x)}{h}$ и показује да је F једна примитивна функција за f, тј. $F' = f$, као и да се свака друга примитивна функција за f од F разликује за константу.

Као што видимо, резултати које је Коши добио су сасвим савремени и у модерном духу. Но, и поред тога, Коши ипак није разматрао опште функције, тј. за Кошија функција ипак није била произвољно придруживање, но се и код њега у основи крила концепција да функција мора бити задата аналитичким изразом. То се најбоље може видети у чињеници да је Коши у доказима који се тичу конвергенције Фуријеових редова, у функцији $f(x)$ реалну променљиву x замењивао комплексном променљивом $z = x + iy$, што заиста нема много смисла, сем уколико се подразумева да је f ипак задата неким аналитичким записом.

И поред дефиниције појма непрекидности, Коши није у пуној мери разматрао могућности постојања произвољних прекидних функција. „Најнеправилније“ функције у том смислу које је он разматрао су заправо биле функције облика (наравно у модерној нотацији)

$$\chi_{I_1} g_1 + \cdots + \chi_{I_n} g_n,$$

где су са χ_{I_j} означене карактеристичне функције одсечака I_j, а g_j су непрекидне функције у његовом смислу. Дакле, прекидне функције које је Коши разматрао су биле искључиво оне које су имале највише коначно много тачака прекида. Први математичар који је озбиљно разматрао функције са бесконачно много тачака прекида био је Дирихле[9].

Дирихле је лично познавао Фуријеа, пошто је од 1822. до 1825. године боравио у Паризу. Он је 1829. године дао први строг доказ о конвергенцији Фуријевог реда дате функције f (наравно под одређеним условима). Наиме, он је разматрао парцијалну суму Фуријеовог реда $S_n(x) = \frac{1}{2}a_0 + \sum_{k=1}^{n}(a_k \cos(kx) + b_k \sin(kx))$ и приказао је ту суму у облику

$$S_n(x) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\frac{\sin\frac{(2n+1)(t-x)}{2}}{sin\frac{t-x}{2}}dt,$$

коју су сигурно видели (или ће видети) сви студенти на курсу анализе у којем се изучавају Фуријеови редови. Саму формулу наравно није тешко извести (присетимо се дефиниције коефицијената Фуријевог реда—одатле се добија интеграл). Дирихле је претпоставио да функција има или највећу или најмању вредност и да није непрекидна у највише коначно много тачака. Заправо тај услов му је требао да би се доказала егзистенција интеграла помоћу којих се одређују Фуријеови коефицијенти. Доказао је да парцијална сума конвергира ка $\frac{1}{2}(f(x-0) + f(x+0))$ за $x \in (-\pi, \pi)$, а ка $\frac{1}{2}(f(-\pi+0) + f(\pi-0))$ за $x \in \{-\pi, \pi\}$. У доказу је ипак користио и претпоставку да је функција f монотона у довољно малом интервалу сваке тачке $x \in [-\pi, \pi]$.

Он је сматрао да се случај функција које имају бесконачно много екстремних вредности, или бесконачно много тачака прекида, могу свести на случај који је разматрао. Заправо је сматрао да је једини

[9] Johann Peter Gustav Lejeune Dirichlet (1805–1859), немачки математичар.

услов да функција има интеграл. Као довољан услов за постојање интеграла, он је навео (користимо модерну терминологију) да функција мора бити таква да је скуп D, тачака прекида те функције, нигде густ (подсетимо читаоца да је нигде густ скуп онај скуп чије затворење не садржи ниједан интервал). Дирихле то тврђење није доказао и навео је да ће доказ бити презентиран у неком наредном раду, али... Тај доказ никада није објавио.

Године 1864, у својој докторској дисертацији, Рудолф Липшиц[10] покушао је да прошири Дирихлеове резултате о конвергенцији Фуријеових редова. Интересантно је да је упркос чињеници да је његова теза рађена чак 10 година после Риманових основних резултата о којима ћемо ускоро говорити, ти резултати нису утицали на Липшицов рад и по свему судећи, он их и није био свестан. Као што смо већ написали, многи Риманови главни резултати су постали опште познати тек после његове смрти. Липшиц је пажљиво анализирао Дирихлеов доказ и разматрао је могућности под којима Дирихлеов доказ „не би прошао“ за дату функцију. Установио је да проблем настаје у случају ограничене и део-по-део монотоне функције (као што смо већ навели, те претпоставке јесу стајале у основи Дирихлеовог доказа), која има бесконачно много тачака прекида између $-\pi$ и π. Заправо закључио је да би Дирихлеов доказ и прошао под условом да та функција има интеграл (дакле уколико се појам интеграла може проширити и на ту класу функција). Закључио је да уколико функција задовољава услов који је Дирихле навео (да је скуп D тачака прекида нигде густ), то може бити изведено. Грешка коју је направио била је у томе што је сматрао да се тада може добити да је скуп D', тачака нагомилавања скупа D, коначан. Проблем је заправо био и у томе што у то време није било занимљивих, другим речима нетривијалних, примера скупова који су нигде густи и онда није било неочекивано да се дође то таквог закључка.

Но, Липшиц је ипак у својој тези дошао и до значајних резултата. Наиме, он се потрудио да замени Дирихлеов услов о монотоности неким другим условом и успео је да га замени другом претпоставком из које је успео да докаже Дирихлеов резултат. Услов који је дао данас је добро познат свим математичарима као Липшицов услов: $|f(x+h) - f(x)| \leq C|h|^\alpha$ за позитивне бројеве C и α.

Пре него што најзад пређемо на Риманов допринос у овој области, а који је био и основа за почетак Канторовог истраживања, а како ћемо видети и почетак озбиљног разматрања бесконачних скупова, наведимо ипак две значајне последице Дирихлеовог рада у овој области. Са његовим радом је први пут почела да се разматра разлика између појма непрекидних и појма интеграбилних функција. Такође је Дирихле био први значајни математичар који је заиста разматрао општи појам функције реалне променљиве, као придруживање $x \mapsto f(x)$ независно

[10] Rudolf Otto Sigismund Lipschitz (1832–1903), немачки математичар .

од цртежа и формула. Уосталом добро нам је позната Дирихлеова функција која је на један начин задата на рационалним, а на други начин на ирационалним бројевима и коју је свакако немогуће нацртати, а и задати формулом на начин како је то рађено до тада (поделом датог одсечка на мање одсечке и задавањем формулама на тим деловима). Дирихле је увео ту функцију као пример функције за коју појам интеграла нема смисла. Тек је са појавом Лебеговог[11] појма интеграла показано да то није тако, али то није већ није део наше приче.

Значајан помак у разумевању појма интеграла и у питањима конвергенције Фуријеових редова дао је Риман. Он је имао прилику да у Берлину прати Дирихлеова предавања из теорија бројева, интеграла, као и парцијалних диференцијалних једначина. Веома је ценио Дирихлеа и сматрао га је, уз Гауса, за највећег живог математичара.

Интересантно је да је Риман имао различит приступ комплексним и реалним функцијама. Наиме, у случају функција $f(z)$ комплексне променљиве, он је захтевао обавезно постојање извода $f'(z)$ док је у случају функција реалне променљиве допуштао, по угледу на Дирихлеа, произвољно придруживање. Но, треба имати у виду да је Риман као и Дирихле и Гаус сматрао да се свака реална функција на одсечку $[-\pi, \pi]$ може представити Фуријеовим редом. Заправо је Ди Боа Рејмон[12] био први математичар који је дао пример да то у општем случају није тачно.

У проблему представљања функција тригонометријским редовима, Риман је најпре истакао да је значајно установити под којим условима интеграл постоји. Као и Коши, он је разматрао интегралне суме и поставио је питање под којим условима те суме имају граничну вредност. Коши јесте показао да је то тачно за (униформно) непрекидне функције, но Римана су занимали општи услови. Он је истакао да је то тачно ако и само ако сума $\sum_{i=1}^{n} D_i(x_i - x_{i-1})$ тежи нули када параметар поделе (максимална дужина интервала у подели) тежи нули, где је са D_i означена осцилација функције f на одсечку $[x_{i-1}, x_i]$. Осим овог услова разматрао је и следеће. Уколико је σ неки позитиван број, са $s(P, \sigma)$ означимо збир дужина интервала на којима је осцилација већа од σ. Природно се поставља питање да ли можда $s(P, \sigma)$ тежи нули када параметар поделе и σ теже нули. Риман је показао да је тај услов еквивалентан претходно наведеном. То су дакле били услови које је он добио као потребне и довољне услове за постојање граничне вредности интегралних сума, тј. за постојање интеграла.

Риман је наравно истакао да такве услове испуњавају и поједине функције које имају бесконачно много тачака прекида на коначном одсечку и дао је следећи пример. Са (x) означимо функцију која реалном броју x придружује растојање до најближег целог броја, ако такав

[11] Henri Léon Lebesgue (1875–1941), француски математичар .
[12] Paul David Gustav du Bois-Reymond (1831–1889), немачки математичар.

постоји и придружује 0 уколико је x полуцео број (тј. број облика $n/2$, где је n непаран број), пошто у том случају не постоји јединствени цео број који је најближи броју x. Јасно је да је функција (x) прекидна у свим полуцелим тачкама и непрекидна у осталим тачкама. Риман затим разматра ред $\sum_{n=1}^{\infty} \frac{(nx)}{n^2}$. Тај ред задаје функцију која је прекидна у свим тачкама облика $\frac{m}{2n}$, где су m и $2n$ узајамно прости. Дакле, функција је прекидна у свуда густом скупу тачака. И поред тога, како је у тачкама $x = \frac{m}{2n}$, $f(x+0) = f(x) + \frac{\pi^2}{16n^2}$ и $f(x-0) = f(x) - \frac{\pi^2}{16n^2}$ то је функција f интеграбилна пошто је „скок“ у свакој таквој тачки једнак $\frac{\pi^2}{8n^2}$, а очигледно да за свако $\sigma > 0$ и сваки ограничени интервал реалне праве, постоји само коначно много тачака у којима је тај скок већи од σ. Стога је други наведени услов испуњен и функција је интеграбилна.

Да би установио потребне и довољне услове да би нека функција била представљена тригонометријским редом

$$\Omega(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx),$$

он је урадио следеће. Претпоставио је да низ функција $A_n(x)$ задат са: $A_0(x) = \frac{1}{2}a_0$, $A_n(x) = a_n \cos(nx) + b_n \sin(nx)$, равномерно конвергира ка нули када $n \to \infty$ и формално је интегрирао тај ред члан по члан те добио функцију F:

$$F(x) = C + C'x + A_0\frac{x^2}{2} - \sum_{n=1}^{\infty}\frac{A_n(x)}{n^2}.$$

Овај ред конвергира за све вредности x и представља непрекидну функцију. Риман је показао да та функција задовољава два важна услова:

$$\mathcal{D}^2F(x) = \lim_{a,b\to 0}\frac{F(x+a+b) - F(x-a+b) - F(x+a-b) + F(x-a-b)}{4ab} = 0,$$

$$\lim_{a\to 0}\frac{F(x+a) - 2F(x) + F(x-a)}{a} = 0.$$

Коришћењем ових резултата, Риман је добио потребне и довољне услове за представљање дате функције тригонометријским редом у датој тачки. Важно је истаћи да коефицијенти a_n и b_n нису добијени интеграцијом, но су то произвољни низови бројева, који морају да задовољавају горе наведени услов, који се тиче равномерне конвергенције низа функција $A_n(x)$.

Дакле, Риман је проширио појам интеграла на ширу класу функција, а дао је и метод за испитивање могућности представљања функција тригонометријским редом. Као што смо већ рекли, ови Риманови резултати су објављени тек 1867. године и тек тада је шири круг математичара имао прилику да настави та истраживања.

Георг Кантор је 14. децембра 1866. године званично завршио своје студије у Берлину. Он је највећи део својих студија провео управо у Берлину учећи од водећих математичара тог времена који су се тамо налазили — Кумера[13], Кронекера[14] и Вајерштраса[15]. Његов примарни интерес је у почетку био везан за теорију бројева, из те области је и његова дисертација, као и каснија хабилитација. Пошто је неко време предавао у локалној школи за девојке и положио пруски државни испит, Кантор је прихватио позицију приватдоцента на универзитету у Халеу. Посао приватдоцента је специфичан за немачки образовни систем и занимљиво је напоменути да приватдоцент нема плату од универзитета, но његов приход зависи од тога колико се студената пријави на његов курс. Звање му само омогућава да предаје на универзитету, но не гарантује приход. Но, Кантор није имао финансијских проблема и та чињеница није утицала на њега.

Како је у раније наведеним радовима других математичара било доста речи о могућности представљања функције Фуријеовим редом, то се природно поставило питање о јединствености тог приказа. Дакле, ако функцију f прикажемо помоћу два тригонометријска реда, да ли они морају бити једнаки, тј. да ли су сви одговарајући коефицијенти једнаки. Јасно је да се то своди на следеће питање. Ако је $\frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx) = 0$, за све $x \in [-\pi, \pi]$, да ли нужно следи да је $a_0 = a_n = b_n = 0$ за све $n \geq 1$?

Као што смо већ раније наводили, ако би било допуштена интеграција реда члан по члан, онда би доказ био једноставан. Помножили бисмо дату једнакост са $\cos(mx)$, извршили интеграцију члан по члан на одсечку $[-\pi, \pi]$ и добили да је $a_m = 0$. На сличан начин би се могло показати да су и остали коефицијенти једнаки нули. Но, интеграција на овај начин није увек могућа. Студенти који су учили о појму униформне конвергенције редова знају да она омогућава поступак интеграције члан по члан. У то време је на значај униформне конвергенције стално указивао Вајерштрас. Инспирисан таквим идејама, Хајне[16], за кога су студенти најпре чули због дефиниције граничне вредности функције преко низова, а који је у ово време већ био професор у Халеу, доказао је јединственост Фуријеовог развоја функције под слабијом претпоставком од униформне конвергенције. Наиме, он је доказао јединственост под претпоставком да постоји коначно много тачака у одсечку $[-\pi, \pi]$ тако да је конвергенција униформна на сваком интервалу који не садржи ове тачке.

Јасно је да овакав резултат подстиче на генерализацију и то у два смера. Најпре се поставља питање да ли се може ослабити услов за униформну конвергенцију, а потом и да ли се може искључити и више тачака од њих коначно много. На тај начин је размишљао и Кантор.

[13] Ernst Eduard Kummer (1810–1893), немачки математичар.
[14] Leopold Kronecker (1823–1891), немачки математичар.
[15] Karl Theodor Wilhelm Weierstrass (1815–1897), немачки математичар.
[16] Heinrich Eduard Heine (1821–1881), немачки математичар.

Кантор је 1870. доказао следећи резултат: ако $a_n \cos(nx) + b_n \sin(nx)$ тежи нули када n тежи бесконачности за све вредности x из неког отвореног интервала, онда и низови (a_n), (b_n) конвергирају ка 0. Да би доказао јединственост приказа нула функције тригонометријским редом, Кантор је искористио Риманов метод. Наиме, он је посматрао раније наведени ред (функцију) F која се добија двоструком формалном интеграцијом датог тригонометријског реда члан по члан. Да би показао оно што је желео, било му је битно да добије да је та функција заправо линеарна. Заправо је баш то у писму од 17. фебруара питао свог колегу Шварца[17]. Шварц му је написао да је то заиста тако и послао му је доказ тог тврђења. Одавде је следило да важи следећа једнакост:

$$a_0 \frac{x^2}{2} - Cx - C' = \sum_{n=1}^{\infty} \frac{a_n \cos nx + b_n \sin nx}{n^2},$$

где је наравно претпостављено да је $0 = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx)$. Како је функција са десне стране добијене једнакости периодична са периодом 2π, то мора бити и полином са десне стране периодичан, а то је могуће једино у случају да је тај полином константан, тј. $a_0 = C = 0$. Ово је омогућило Кантору да покаже да остатак горе добијеном реда равномерно тежи нули, те је могао даље да примени идеју о интеграцији реда члан по члан (не можемо наводити све детаље у доказу) и напокон је добио да су сви коефицијенти једнаки 0. Дакле, на тај начин је доказао јединственост приказа у облику Фуријеовог реда под претпоставком да Фуријеов ред конвергира у *свакој тачки* и да се у *свакој тачки* поклапа са вредношћу функције, али *без претпоставке о униформној конвергенцији* Фуријеовог реда.

Следећи корак који је Кантор предузео је да, пошто се већ „ослободио" претпоставке о униформној конвергенцији Фуријеовог реда, покуша да ослаби и претпоставку о конвергенцији Фуријеовог реда у свакој тачки. То је и успео следеће године. У „ноти" (тако математичари често називају кратке радове) објављеној 1871. године, он наводи појендостављење претходног доказа који му је послао Шварц, али и показује да тврђење важи под слабијом претпоставком да ред не конвергира ка вредности функције у свим тачкама из $[-\pi, \pi]$, но да постоји коначно много тачака $x_0 < x_1 < \cdots < x_n$, у којима се то не дешава. Идеја доказа састоји се у томе да се најпре примети да, према ранијем, функција F је линеарна на сваком интервалу (x_i, x_{i+1}), тј. да је линеарна функција облика $k_i x + l_i$ на том интервалу, а потом да се покаже да се заправо ради о истој линеарној функцији на свим интервалима и тако се све сведе на претходно доказано. Следећи корак је наравно да се покуша са даљим слабљењем претпоставки, тј. да постоји *бесконачно много* тачака у којима ред не конвергира почетној функцији. Овај корак заправо представља први корак у изградњи теорије бесконачних

[17] Hermann Amandus Schwarz (1843–1921), немачки математичар.

скупова.

Дакле, претпоставимо да је скуп *изузетих* тачака, тј. оних тачака у којима не ред не конвергира ка 0, бесконачан. Према Болцано-Вајерштрасовом ставу тај скуп има тачку нагомилавања. Размотримо најпре случај да има само једну тачку нагомилавања x' и концентришимо се на конвергенцију тригонометријског реда на ограниченом интервалу (a,b) (свеједно је наравно на ком). Посматрајмо интервале (a,x') и (x',b). Ако је (s,t) било који прави подинтервал од (a,x'), онда у њему има само коначно много изузетих тачака (иначе би у њему постојала тачка нагомилавања скупа свих изузетих тачака, а по претпоставци је то само тачка x'). Но, случај коначно много изузетих тачака је већ обрађен и онда знамо да је Риманова функција F линеарна на (s,t). Но, то је непрекидна функција која је линеарна на сваком правом подинтервалу од (a,x'), па проширивањем тог произвољног подинтервала до целог (a,x') добијамо да је F заправо линеарна на (a,x'). Слично се добија да је F линеарна и на (x',b), а потом, као и раније, да је то заправо линеарна функција на (a,b).

Аналогни доказ пролази и у случају да имамо коначно много тачака нагомилавања скупа изузетих тачака (на коначно много подинтервала је F свуда линеарна, а онда се као и раније покаже да је то једна те иста линеарна функција). Шта се дешава у случају у коме скуп изузетих тачака има бесконачно много тачака нагомилавања? Поступа се као у претходном. Претпостави се најпре да тај скуп тачака нагомилавања има само тачно једну тачку нагомилавања x''. Разматрањем интервала (a,x'') и (x'',b), односно њихових правих подинтервала (s,t) добија се да у њима има само коначно много тачака нагомилавања скупа свих изузетих тачака. Но, то је већ урађено и на таквим подинтервалима је F линеарна. Даље се поступа као и у претходном.

Можемо да закључимо да постоји јасна идеја како се резултат генералише и то је било јасно и Кантору. Но, једно је идеја, а друго је реализација. Да би успешно доказао то што се наслућује као резултат, он је морао да се пре свега мало позабави прецизирањем основних резултата који се тичу теорије реалних бројева. Ма колико то било изненађујуће читаоцу, у то време та теорија није била још добро заснована.

Стога Кантор у свом раду из 1872. године почиње баш са тим. Он полази од скупа A, свих рационалних бројева, као датих и циљ му је да заснује теорију ирационалних бројева. У ту сврху посматра фундаменталне низове рационалних бројева (студентима је сигурно познатији термин Кошијеви низови, при чему треба имати на уму да се претпоставља да је ε, које се појављује у дефиницији Кошијевог низа обавезно рационалан број) и каже да је сваком таквом низу придружен један симбол. Потом дефинише уређење на тим симболима, као и аритметичке операције (рационалне бројеве види као константне низове) и пошто све то уведе у даљем те новодобијене објекте назива бројевима. Тако је добио скуп бројева B. Следећи корак савременом читаоцу делује збуњујуће. Наиме, Кантор сада посматра фундаменталне низове бројева из B и формира нови домен C (sic!). Он је потпуно свестан да тиме не добија ништа ново, као што и наши читаоци знају, али истиче концептуалну разлику B и C (подсетимо се да је ово ипак рад о јединствености тригонометријског реда и да Кантор има на уму претходно наведене идеје). После λ таквих конструкција долази до домена L. Дакле, у L су фундаментални низови фундаменталних низова ... Наравно да сваком елементу из L одговара број из B, али као што је већ наведено, Кантору је та дистинкција важна.

Следећи корак је успостављање бијекције између тако добијених реалних бројева и геометријског (једнодимензионог) континуума, тј. праве. Јасно је да избором координатног почетка и основне јединице мерења на датој правој имамо у потпуности одређене *рационалне тачке*, тј. тачке са рационалним координатама. Ако се узме нека друга тачка на правој, онда се њој може „прићи“ фундаменталним низом рационалних тачака $a_1, a_2, \ldots, a_n, \ldots$. Кантор каже да је растојање b те тачке од координатног почетка онај број у B који одговара том фундаменталном низу. Јасно је да Кантор не може да докаже да обратно, сваком ирационалном броју одговара јединствена тачка на правој и стога он то поставља као аксиому, тј. сваком броју из B јединствено одговара тачка на правој чија је координата управо тај број. Коришћењем ове аксиоме, Кантор успоставља обострано једнозначну кореспонденцију између (аритметички) добијених скупова бројева и геометријских тачака на правој.

Долазимо до фундаменталног појма *скупа тачака прве врсте* (Кантор истиче да кад год користи термин „тачка“, он заправо има у виду број који одговара тачки на правој). Најпре Кантор дефинише појам изводног скупа: ако је дат неки скуп тачака P, онда је нека тачка тачка нагомилавања тог скупа уколико се у сваком интервалу око ње налази бесконачно много тачака тог скупа. Наравно, тачка нагомилавања може, а не мора припадати почетном скупу P. Скуп свих тачка нагомилавања Кантор је назвао „први изводни скуп скупа тачака P“ и означио са P'. Овде је важно истаћи да је скуп P' на тачно одређен начин придружен скупу P. Наиме за сваку тачку је јасно да она или јесте тачка нагомилавања скупа P, или то није. Дакле, скупу P придружујемо скуп P'. Такво „баратање“ са скуповима није било уобичајено у то време и представљало је новост и омогућавало дубљи продор у проблематику, која се истраживала.

Ако је скуп P бесконачан скуп у неком ограниченом интервалу, онда он има тачке нагомилавања, тј. скуп P' није празан (заправо се у то време празан скуп помало избегавао, па се говорило да P *има* изводни скуп). Уколико је скуп P скуп свих рационалних тачака, онда се наравно добија скуп свих тачака праве. Но, као што се из B конструише $C, \ldots, L$, тако се формирају и виши изведени скупови $P'', \ldots, P^{\lambda}$. Наравно P'' формирамо у случају бесконачности скупа P'

на коначном интервалу итд. Скуп P је *скуп тачака прве врсте* уколико је $P^{(\nu)}$ коначан скуп за неки природан број ν.

Када је ове појмове јасно дефинисао и прецизирао, Кантору није било тешко да докаже генерализацију теореме о јединствености тригонометријског реда. Наиме, доказао је да је тригонометријски ред јединствено одређен под условом да је скуп изузетих тачака скуп тачака прве врсте. Доказ се заснива на раније наведеним својствима Риманове функције F. Ево како се он изводи. Како је почетни скуп P такав да је за неки природан број ν одговарајући изводни скуп коначан, то у нашем интервалу (a, b) има само коначно много тачака из $P^{(\nu)}$. Те тачке деле интервал на коначно много подинтервала. Ако посматрамо било који интервал (a_1, b_1), који је прави подинтервал од неког од њих, онда у њему има само коначно много тачака из $P^{(\nu-1)}$. У супротном, у том подинтервалу се налази тачка из $P^{(\nu)}$, а то није могуће, јер су те тачке ван тог скупа као деоне тачке почетног интервала (a, b). Поступак понављамо са свим таквим подинтервалима у којима има само коначно много тачака из $P^{(\nu-1)}$. После коначно много корака добићемо коначан број подпод...интервала у којима је само коначно много тачака из P. На њима је Риманова функција линеарна и онда постепеним повећавањем тих интервала и њиховим „лепљењем“, као што је већ наведено, добијамо да је та функција линеарна на целом почетном интервалу. Тиме је доказ сведен на основни случај.

У доказу теореме о јединствености тригонометријског реда, Кантор се концентрисао на скупове тачака прве врсте, дакле на скупове код којих је $P^{(n)}$ празан скуп за неки природан број n. Но, већ је у том раду имплицитно споменуто да се поступак налажења изводних скупова може продужити и *иза коначног* подручја. Кантор пише: „концепт броја, у смислу у коме је уведен овде, носи у себи клицу неопходне и апсолутно бесконачне екстензије“. Скупови тачака друге врсте, тј. они код којих $P^{(n)}$ није празан скуп ни за један природан број n експилицитно се помињу тек у Канторовим каснијим радовима. Но, он у напомени уз свој рад из 1880. наводи да је он низ скупова

$$P^{(\infty)}, P^{(n\infty^{\infty})}, P^{(\infty^{\infty+1})}, P^{(\infty^{\infty+n})}, P^{(\infty)n^{\infty}}, P^{(\infty^{\infty^{n}})}, P^{(\infty^{\infty^{\infty}})},$$

где је са ∞ означен најмањи бесконачни број већи од свих природних бројева, открио још пре десет година. Скуп $P^{(\infty)}$ се природно дефинише као пресек свих $P^{(n)}$ за коначне n, а онда се поставља питање постојања његовог изводног скупа (уколико он има бесконачно много тачака) $(P^{(\infty)})'$ који Кантор означава са $P^{(\infty+1)}$. Сигурно да пажљив читалац не може пропустити да уочи сличност са раније виђеним $(\omega' = \omega + 1)$, но концепт трансфинитних бројева (оних које долазе „иза коначних“) није одмах формулисан и било је потребно време да ти појмови буду усвојени, но јасно је да је клица садржана у овим почетним радовима.

Видљиво је да код генерализације теореме о јединствености тригонометријског реда, сам тригонометријски ред има секундарну улогу. Главна је била манипулација реалним бројевима и потпуно је природно да се Кантор у свом даљем истраживању концентрише управо на својства скупа реалних бројева, тј. на реалну праву. Но, пре него што изложимо Канторове почетне резултате, а с њима у вези и улогу, коју је Дедекинд имао у тим првим испитивањима, као и о утицају Дедекинда на увођење скупа као централног појма у математици, одговорићемо на непостављено питање пажљивог читаоца.

Наиме, ми причамо о изведеним скуповима прве и друге врсте, али да ли постоје такви примери? Не само то, него да ли су такви примери били познати у време о којем говоримо. Одговор је потврдан.

Позабавимо се најпре питањем скупова прве врсте. Хенкел[18] је навео један такав пример. То је скуп свих бројева облика $\frac{1}{2^n}$. Јасно је да тај скуп има једну једину тачку нагомилавања 0, те он јесте скуп прве врсте. Наравно, ово је веома једноставан пример, али то је уз пример скупа свих рационалних бројева (који је наравно скуп друге врсте) био у почетку једини познат пример. Знатно боље примере дао је извесни Смит[19] (sic!) из Велике Британије. Он се првенствено бавио теоријом бројева, али је боравио и у Француској те је био упознат са проблемима којима се баве математичари на континенту (као што би рекли прави Британци). Нажалост његови резултати нису били познати (на континенту), а да јесу сигурно би то убрзало разрешавање неких проблематичних питања, која се тичу својстава скупова реалних бројева. Смит је посматрао генерализацију Хенкеловог примера. Наиме, уочимо скуп

$$P_2 = \left\{ \frac{1}{n_1} + \frac{1}{n_2} : n_1, n_2 \geq 1 \right\}.$$

Јасно је да је $P_2^{'} = \{0\} \cup \{1/n_1 : n_1 \geq 1\}$ и $P_2^{''} = \{0\}$. Сада се види шта треба радити. Скуп

$$P_k = \left\{ \frac{1}{n_1} + \cdots + \frac{1}{n_k} : n_1, \ldots, n_k \geq 1 \right\}$$

задовољава услов $P_k^{(k)} = \{0\}$. Дакле, тако добијамо скупове прве врсте (типа n, тј. такве да је n-ти изводни скуп коначан). Како добити пример скупа друге врсте . Први такав пример дао је Ди Боа Рејмон.

Нека је p било који реалан број. Посматрамо два низа тачака (a_n) и (b_n), за које је $a_n < b_n$, а осим тога оба низа конвергирају ка p. На сваком интервалу (a_n, b_n) изаберимо скуп P_n типа n (можемо да узмемо транслацију горе наведеног скупа). Нека је $P = \cup_{n \geq 1} P_n$. Није тешко уверити се да је $P^{(\infty)} = \cap_{n \geq 1} P^{(n)} = \{p\}$.

[18]Hermann Hankel (1839–1873), немачки математичар.

[19]Henry John Stephen Smith (1826–1883), британски математичар.

Вратимо се сада главном току нашег излагања. Оно што следи је можда и најинтересантнији део овог историјског осврта. Наиме, појаснићемо како је Кантор дошао до доказа непребројивости реалних бројева. Овај доказ нам сада не представља проблем, али не смемо заборавити какво је стање са основама анализе тада било (читалац се у то, надамо се, могао до сада уверити). И не, први доказ није био базиран на дијагоналном поступку (дијагонални поступак је тек доста касније откривен). Ево како се то све десило (след догађаја су историчари реконструисали на основу писама и скица писама, које су размењивали Кантор и Дедекинд).

Године 1873, прецизније, 29. новембра те године, Кантор је упутио следеће питање Дедекинду. Да ли постоји узајамно једнозначна кореспонденција (или, како би ми то краће данас рекли, бијекција) између скупа свих позитивних целих бројева и свих позитивних нумеричких величина (то јест позитивних реалних бројева)? Кантор наводи да би неко могао да укаже да је то немогуће пошто су цели бројеви дискретни, а реални нису, али он истиче да се том напоменом ништа не добија и мада он мисли да таква кореспонденција не може постојати, он ипак нема доказ те чињенице.

Дедекинд је одмах одговорио на то писмо и навео да ни он не може да докаже да таква кореспонденција не постоји, али да сматра да тај проблем није од посебног интереса. Но, он је успео да докаже да постоји бијекција између скупа свих алгебарских бројева и скупа позитивних целих бројева и тај доказ је приложио. Овде треба напоменути да су Дедекиндова писма изгубљена, али да су скице тих писама сачуване, као и то да је Дедекинд био изузетно методичан и организован научник, који је водио веома уредне записе (чак је записивао и дневне температуре!).

Кантор је у писму од 2. децембра потврдио да је Дедекинд заиста послао доказ тог резултата. Ево како је Дедекинд доказао ту чињеницу. Сваки алгебарски број је нула неког нерастављивог полинома са рационалним коефицијентима. Но, множењем са одговарајућом константом можемо претпоставити да се ради о полиному са целобројним коефицијентима код кога је најстарији коефицијент позитиван. Дакле, ако је ω неки алгебарски број, онда постоји полином $p(x)$ (користимо ознаке које су ови математичари користили) такав да је

$$p(\omega) = a_0\omega^n + a_1\omega^{n-1} + \cdots + a_n = 0.$$

Број $N = n - 1 + |a_0| + |a_1| + \cdots + |a_n|$ називамо *висином* полинома $p(x)$ (да, могли смо да не пишемо апсолутну вредност уз a_0, пошто смо претпоставили да је то позитиван број). Можемо да приметимо да за сваки позитиван број N постоји највише коначно много полинома са целобројним коефицијентима, који имају висину баш N (обратите пажњу на значај чињенице да се степен полинома n појављује у дефиницији висине полинома). Но, сваки од тих полинома има највише коначно много нула. Дакле, за фиксирано N, постоји коначно много нула полинома са целобројним коефицијентима који имају висину n. Те нуле можемо да уредимо на произвољан начин и тако добијамо да има пребројиво много алгебарских бројева (најпре узимамо бројеве висине 1, па висине 2, итд.).

Кантор је претходно разматрао постојање бијекције између скупа позитивних целих бројева и скупа ν-торки таквих бројева. Идеја му је била да свакој ν-торци $(n_1, \ldots, n_\nu)$ придружи број $n_1^2 + \cdots + n_\nu^2 = \mathfrak{N}$. Идеја је онда слична Дедекиндовој—за сваки $\mathfrak{N}$, уредити све n-торке чији је збир квадрата $\mathfrak{N}$ на произвољан начин и тако показати да n-торки има колико и позитивних целих бројева. Кантору се чинило да је то практично исти доказ као и Дедекиднов, но то није баш тако. Наиме, ако би се у случају полинома поступило по овој идеји, онда бисмо имали проблема са чињеницом да се нигде не појављује степен полинома и да, наравно, неки од коефицијената полинома буду једнаки нули, те бисмо добили бесконачно много полинома за које је збир квадрата коефицијената једнак фиксираном броју. Дакле, без додатка степена, овакав доказ не би могао да „прође“. Но, када је видео Дедекиндов доказ, Кантор је сматрао да он у суштини има сличан доказ и није имао проблема да Дедекиндов доказ у потпуности касније наведе у раду без спомињања да је доказ заправо Дедекиндов (иначе Кантор до тада нигде није писао о томе да има доказ пребројивости алгебарских бројева, нити да је тај проблем уопште разматрао). Но, више о томе касније.

Кантор се у писму од 7. децембра поново враћа питању пребројивости реалних бројева и наводи да је успео да докаже непребројивости. Ево како је изгледао тај први доказ.

Претпоставимо да се сви реални бројеви могу поређати у низ

$$\omega_1, \omega_2, \ldots, \omega_n \ldots .$$

Пођимо од ω_1 и потражимо први следећи члан низа ω_α, који је већи од ω_1. Нека је затим ω_β први следећи члан који је већи од ω_α $(\beta > \alpha)$ итд. На тај начин добијамо растући подниз $\omega_1^1, \omega_1^2, \ldots, \omega_1^n \ldots$ (после преозначавања) почетног низа. Понављањем поступка добијамо нови подниз итд. Дакле, на овај начин Кантор добија бесконачну матрицу

$$\begin{array}{ccccccc}
(1) & \omega_1^1, & \omega_1^2, & \ldots, & \omega_1^n & \ldots \\
(2) & \omega_2^1, & \omega_2^2, & \ldots, & \omega_2^n & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(k) & \omega_k^1, & \omega_k^2, & \ldots, & \omega_k^n & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

Свака врста ове бесконачне матрице је растући низ. Сада посматрамо одсечак $[p, q]$ у коме нема елемената из прве врсте (нпр. било који одсечак садржан у интервалу (ω_1^1, ω_1^2)). Уколико у овом одсечку нема елемената из преосталих врста, доказ је готов (било који елемент из тог одсечка је тражени реални број који није набројен у почетном низу). У супротном, нека је k најмањи број такав да у том одсечку има чланова низа из k-те врсте. Тада тај одсечак сигурно садржи пододсечак $[p^{(1)}, q^{(1)}]$ у коме нема елемената k-те врсте (k-та врста представља растући низ и довољно је узети пододсечак садржан у интервалу који дефинишу узастопни чланови низа који су у $[p, q]$, а ако је само један члан k-те врсте у $[p, q]$ то је још лакше). Поступак настављамо и добијамо опадајући низ одсечака $[p^{(\nu)}, q^{(\nu)}]$, који, као што добро знамо, мора да има непразан пресек. Ма који елемент тог пресека је тражени реалан број пошто се он не може налазити у почетном набрајању — тада би онда био у некој врсти l, а пододсечак $[p^{(\nu)}, q^{(\nu)}]$ за довољно велико ν не садржи елементе врсте l.

Као што видимо, доказ није баш једноставан и Дедекинд је у писму од 8. децембра навео поједностављење овог доказа, а такође је то одмах урадио и Кантор. Доказ који је објављен доказује да се за сваки низ реалних бројева и сваки интервал (α, β) може наћи елемент η из тог интервала, који није у том низу.

Нека је дат низ $x_1, x_2, x_3, \ldots$. Означимо са α', β' прва два члана тог низа који се налазе у интервалу (α, β) и за које је $\alpha' < \beta'$. Са α'', β'' означавамо прва два члана наведеног низа у интервалу (α', β') за које је $\alpha'' < \beta''$. Настављамо овај процес и добијамо низ уметнутих одсечака $[\alpha^n, \beta^n]$. Сада се разликују два случаја. Може се десити да је овај низ коначан и уколико је $[\alpha^n, \beta^n]$ последњи одсечак у том низу онда било који елемент у (α^n, β^n) није у датом низу (сем можда једног—може се десити да је у том интервалу један члан низа, али не и два, па зато не можемо наставити процес). Уколико смо добили бесконачан низ уметнутих одсечака, онда заправо имамо два низа бројева — растући и одозго ограничени низ (α^n) и опадајући одоздо ограничени низ (β^n). Дедекинд је у својој верзији доказа навео да сада на основу принципа непрекидности (Дедекинд је сматрао да чињеница да сваки растући одозго ограничени низ има граничну вредност, представља суштину појма непрекидности за реалне бројеве) добијамо да први низ има граничну вредност α^∞, а други β^∞. Кантор у публикованој верзији избацује спомињање принципа непрекидности и само наводи да ове граничне вредности постоје (касније ћемо продискутовати зашто је то урадио). Сада постоје два случаја: у првом је $\alpha^\infty = \beta^\infty$ и тада за η узимамо ту граничну вредност, а у другом је $\alpha^\infty < \beta^\infty$ и за η можемо узети ма коју вредност из интервала $(\alpha^\infty, \beta^\infty)$. Овим је доказ завршен.

Дакле, видели смо како је Кантор дошао до важног резултата (и какву је улогу ту имао Дедекинд) у коме се показује да не постоји бијекција између скупа природних бројева и скупа реалних бројева, тј. да постоје два бесконачна скупа између којих се не може успоставити бијекција. Тај резултат заправо представља почетак развоја теорије бесконачних скупова. Но, погледајмо како је тај резултат Кантор представио. Видећемо да је он то урадио на помало необичан начин.

Кантор је 25. децембра 1873. године писао Дедекинду да је написао и послао у *Journal für die Reine und Angewandte Mathematik* рад под насловом „О једном својству колекције свих реалних алгебарских бројева“. Написао је да у почетку није имао намеру да објављује ове резултате, али је у Берлину разговарао са Вајерштрасом и он му је рекао да треба да објави резултате док год су у вези са алгебарским бројевима. Кантор је Дедекинду написао да је искористио његове коментаре и начин изражавања. Дедекинд му је сугерисао да избаци реч „реалних“ из наслова, пошто резултат о пребројивости важи за све алгебарске бројеве, но Кантор је ипак задржао првобитни наслов. Интересантно је да је Вајерштрас сматрао да је резултат о пребројивости алгебарских бројева посебно занимљив и да је то заправо главни резултат тог рада (те је стога Кантор рад тако и назвао), а не чињеница да не постоји бијекција између реалних и природних (самим тим и алгебарских бројева). Наиме, Вајерштрас је резултат о пребројивости алгебарских бројева касније искористио да да пример непрекидне функције која има извод у свакој трансцендентној тачки, а ни у једној алгебарској. Осим тога, у то време, Вајерштрас је имао изузетно негативан став по питању поређења бесконачних скупова. Он је у лето 1874. држао курс у коме је навео да две бесконачно велике величине нису упоредиве и да примена појма једнакости на бесконачне величине не даје нове резултате (sic!). Касније се његов став променио, али је у то време био управо такав.

Кантор је рад организовао на следећи начин. У првом делу рада наведен је доказ (како га је дао Дедекинд) пребројивости скупа алгебарских бројева, а у другом је показано да не постоји бијекција између скупа реалних и природних бројева и затим су ови резултати примењени на нови доказ Лиувиловог[20] резултата о постојању трансцендентних бројева. Дедекиндов допринос нигде није наведен.

Видели смо да је под утицајем Вајерштраса истакнута пребројивост алгебарских бројева, док је напомена о непостојању бијекције између скупа природних бројева и скупа реалних бројева само укратко наведена и то при исправљању рада у припреми за штампу (навели смо негативан Вајерштрасов став по питању поређења бесконачних скупова). Разлог за искључивање спомињања Дедекинда, па и не истицање принципа непрекидности у доказу, састоји се у следећем. Кантор је био ученик веома утицајне берлинске школе и знао је да водећи професори у Берлину Кумер и Кронекер имају помало негативан став према Дедекинду због његове алгебарске теорије бројева. Наиме, Кронекер је тврдио да је исту ту теорију он имао још 1858. године, али да је није објавио и они никада нису признали Дедекиндов приоритет у тој области. Кантор је касније, развијајући даље своју теорију бесконачних скупова дошао у сукоб са Кронекером, но у времену о коме говоримо, он је био у добрим односима са берлинском школом и рачунао

[20] Joseph Liouville (1809–1882), француски математичар.

је да су му они потребни за даљу каријеру (но, испоставило се да он никада прешао из Халеа на неко престижније место). Дедекинд је изразио своје чуђење што је Кантор навео његове доказе без помињања извора и од тада су њихови односи помало захладнели и на писма која му је Кантор упућивао често није одговарао.

Због ограничености (по обиму) овог историјског прегледа, нећемо се бавити Канторовим даљим радом. Тај рад је изузетно значајан и било би потребно доста простора да би се описао.

Ради комплетније слике почетака теорије скупова и то посебно увођења терминологије скупова и функција у све математичке области посветићемо се мало Дедекиндовом доприносу.

Дедекинд је своју хабилитацију одбранио 1854, само неколико дана после Римана, такође у Гетингену. Наслов теме био је: „О увођењу нових функција у математику“. У оквиру те теме он је говорио о тригонометријским функцијама, интеграцији и елементарној аритметици. Дедекинд је тиме започео један програм, који је заправо следио током целе своје каријере. Наиме, идеја грађења бројева почев од природних бројева је нешто о чему је он писао у више објављених и необјављених радова. На самом почетку је централну улогу дао операцијама (дакле функцијама), тј. идеја конструкције све шире класе бројева била је условљена операцијама које вршимо у постојећој класи, прецизније могућности, односно немогућности извођења инверзних операција. У својим каснијим радовима, саме скупове је поставио у центар интересовања.

Године 1857, Дедекинд је прочитао Хамилтоново[21] дело *Лекције о кватернионима.* Као што се комплексни бројеви добијају као уређени парови реалних бројева са одговарајуће дефинисаним операцијама, на сличан начин се кватерниони добијају из комплексних. Множење кватерниона није комутативно, али сва остала су задржана. Дедекинд је евидентно закључио да су те конструкције (комплексних бројева и кватерниона) добро изведене и никада се у својим радовима није бавио питањем конструкције нпр. комплексних бројева. Но, бавио се конструкцијом целих и рационалних бројева, као и реалних бројева. Целе и рационалне бројеве је конструисао попут конструкције коју ми данас користимо — помоћу уређених парова са одговарућим идентификација, а што се тиче конструкције реалних бројева, присетимо се Дедекидновог реза из Анализе 1. Нас ће овде највише занимати Дедекиндов поглед на природне бројеве.

Главно Дедекиндово дело, које се бави заснивањем математике је *Was sind und was sollen die Zahlen*, објављено 1888. Најчешћи превод овог наслова је *Шта су и чему служе бројеви*, али, имајући у виду садржај дела, превод могао да буде и *Шта су и чему би <u>требало</u> да служе бројеви.* Ми ћемо се позабавити овим делом, као и рукописима, који су му претходили.

[21]Sir William Rowan Hamilton (1805–1865), британски математичар.

Као што смо већ навели, Дедекинд је био темељан математичар, који није журио са објављивањем радова пре него што би они достигли онај ниво свеобухватности и целовитости који је он желео. Дакле, он је следио Гаусову максиму: *мало, али зрело.* Било је случајева када се то лоше одразило на његову каријеру (недовољан број објављених радова), али он се тог принципа држао целог живота.

У рукописима насталим између 1854. и 1872. године можемо наћи да је Дедекинд природне бројеве градио почевши од броја 1 и формирајући *следбенике* бројева додавањем јединице. Сабирање је дефинисао формулом $a+(b+1) = (a+b)+1$ (не делује ли ово некако познато?). Занимљиво је да је Дедекинд многе идеје на основу којих су базирани резултати из тог главног његовог рада о заснивању бројева, наводио у писму извесном гимназијском професору Кеферштајну, а пропустио да их наведе у самом раду и тиме тај рад учинио неразумљивијим и мање схваћеним од стране професионалних математичара. Касније је операцију сабирања дефинисао апстрактније, као функцију φ, која има својства $\varphi(a, d(b)) = d\varphi(a, b)$ и $\varphi(a, 1) = d(a)$, где је $d : \mathbb{N} \to \mathbb{N}$ функција која представља „додавање јединице“.

Пређимо сада на само дело. На самом почетку, Дедекинд уводи основну скуповну терминологију: *систем* (скуп), *ствар* (елемент скупа), *део* (подскуп), *прави део* (прави подскуп), *комбинован систем* (унија скупова), *заједница система* (пресек скупова). Читаоци који су упознати са Хилбертовим[22] делом *Основи геометрије*, сигурно су ову терминологију препознали пошто на почетку овог дела Хилберт наводи: „*Разматраћемо три система ствари. Ствари првог система зваћемо тачке.*“ Хилберт је тада користио Дедекиндову терминологију.

Поред појма скупа навео је и појам пресликавања и то практично у смислу у коме се у модерној математици оно и уводи — пресликавање система S је *закон* по коме сваком елементу s из S одговара ствар $\varphi(s)$, која се зове слика од s. Дефинисао је и композицију пресликавања. Дедекинд је навео да је овим дао *дефиницију* појма пресликавања, мада са логичке тачке гледишта то се не може назвати дефиницијом (јер, шта је то *закон*?), но само појашњењем.

Као главне недостатке Дедекиндове презентације скупова, истакнути логичар Фреге[23] је навео:

1) Нејасно разликовање релације припадности и подскупа.

2) Често неразликовање једночланог скупа и његовог елемента.

3) Избацивање празног скупа.

Наравно, чињеница да постоје овакви проблеми код Дедекинда, не оправдава садашње студенте математике да праве такве грешке! Подсетимо се да је Пеано (баш у вези са оваквим примедбама) увео посебну ознаку, коју и данас користимо, за припадност елемента скупу, док је Дедекинд ипак раније имао појам празног скупа, али га је ипак

[22]David Hilbert (1862–1943), немачки математичар.
[23]Friedrich Ludwig Gottlob Frege (1848–1925), немачки математичар.

из публикованог рада избацио.

Велики недостатак Дедекиндовог погледа на скупове је и у прихватању постојања универзалног скупа, тј. скупа свих скупова, а знамо да се на тај начин парадокси појављују у теорији скупова, но у тренутку објављивања, то још није било видљиво.

Посветимо се за крај најзанимљивијем појму, са аспекта теорије скупова, који је Дедекинд увео у овом раду, а то је појам *ланца*. Упозоримо одмах да се не ради о појму ланца у вези парцијалног уређења.

Идеја ланца је добијена из идеје математичке индукције, тј. разматрањем доказа помоћу индукције. Ако је дато пресликавање $\varphi : S \to S$, онда подскуп K од S зовемо *ланац* уколико је $\varphi[K] \subseteq K$ (користимо ознаке које смо користили у овој књизи). Дедекинд уводи појам *ланца система* (сетимо се да је тако Дедекинд називао скуп). Наиме, ако је $A \subseteq S$ и $\varphi : S \to S$, онда је *ланац система* A по дефиницији пресек свих ланаца (дакле свих подскупова K скупа S за које је $\varphi[K] \subseteq K$), чији је A подскуп. Ознака коју Дедекинд користи да означи ланац скупа A је A_0 (а понекад користи и ознаку $\varphi_0(A)$). Видећемо ускоро како је ова идеја повезана са аксиоматиком природних бројева, као и са Кантор-Бернштајновом теоремом.

Дедекинд је имао оригиналну идеју — да заснује коначно (природне бројеве) на бесконачном. Стога му је био потребан појам бесконачног скупа. Ту дефиницију је он формулисао још 1872. године. Наиме, скуп S је бесконачан ако постоји бијекција (користимо савремену терминологију) између S и неког његовог правог подскупа. У супротном је коначан. Наравно да нам и ова дефиниција „звучи“ познато. Оригиналност ове идеје је наравно у чињеници да се овде нешто што уопште није спорно, попут природних бројева заснива на нечем што су многи математичари као што смо видели, избегавали да користе, тј. на појму стварне бесконачности.

Ево како је Дедекинд увео природне бројеве. Основни појам је појам *просто бесконачног* скупа. Скуп N је просто бесконачан уколико постоји „1–1“ пресликавање $\varphi : N \to N$ (Дедекинд је „1–1“ пресликавања називао *слична* или *истакнута*), тако да је N ланац једног елемента који не припада $\varphi[N]$. Овај истакнути елемент зове се базни елемент и означава са 1. Овде поново имамо проблем са Дедекидновом терминологијом, пошто заправо N не може бити ланац неког елемента, но ланац једночланог скупа са тим елементом као јединим својим чланом, али се то како видимо лако исправља. Дакле имамо четири важна услова:

$$(\alpha)\ \varphi[N] \subseteq N;\ (\beta)\ N = \{1\}_0;\ (\gamma)\ 1 \notin \varphi[N];\ (\delta)\ \varphi \text{ је „1–1“.}$$

Да ли је неко споменуо Пеанове аксиоме? Пеано је своје аксиоме објавио 1899. године и навео је да јесте консултовао овај Дедекиднов рад, но сам је пре тога дошао до њих. Но, ево их и овде код Дедекинда.

За крај излагања о Дедекиндовом доприносу теорији скупова, наведимо и горе споменуту везу ланаца и Кантор-Бернштајнове теореме.

Кантор и Дедекинд су се у септембру 1882. године срели у Харцбургу и наравно разговарали о математици. Кантор је тада информисао Дедекинда (а то се види и из писма из новембра те године) да има проблема са доказом следећег тврђења:

Ако је $M'' \subseteq M' \subseteq M$ и ако постоји бијекција између M и M'' онда постоји бијекција између M и M'.

Јасно је да је ово тврђење еквивалентно Кантор-Бернштајновој теореми.

Ево које се тврђење може наћи у наведеном Дедекиндовом раду о бројевима.

Нека је φ дато пресликавање и уведимо ознаку $K' = \varphi[K]$. Претпоставимо да је $K' \subseteq L \subseteq K$. Дакле и K и L су ланци. Дедекинд пише да се при овим условима увек може извршити следећа декомпозиција L и K. Нека је $U = K \setminus L$ и $V = K \setminus U_0$. Тада је

$$K = U_0 \cup V \text{ и } L = U'_0 \cup V.$$

Овај доказ Дедекинд оставља читаоцима (а то ћемо и ми урадити!) и даље га уопште не коментарише. Но, није тешко видети да се у случају да је φ „1–1“ добија тражено Канторово тврђење (сугеришемо читаоцу да то сам уради). Подсетимо се да је Дедекинд био врло систематична особа, тако да није могуће да се он није присетио питања које му је поставио Кантор. Пре ће бити да је Дедекинд решио да се мало, да се тако изразимо, нашали са Кантором (а треба имати у виду и ранија искуства која је имао у преписци са њим) и да провери да ли ће он успети да препозна тражено тврђење. Тешко је поверовати, али Кантор не само да је чак и 1895. године сматрао да теорема још није доказана, него се и негативно изразио о овом Дедекиндовом раду, који је описао као вештачки систем од 172 тврђења, који се баве најелементарнијим и понекад најтривијалнијим својствима бројева и који уместо да појасне, само још више замагљују природу бројева! Као поука ове приче може се закључити да треба пажљиво читати дела истакнутих аутора—можда су они доказали баш оно што нам треба, а нису то желели да истакну!

Овим завршавамо историјски осврт на почетке теорије скупова. Уколико је читаоца заинтересовала ова прича и желео би да више сазна о даљем развоју, препоручујемо му да консултује наведену литературу.

Додатак III

Борелови скупови и континуум хипотеза

Истраживања подскупова реалне праве, која је Кантор започео мотивисан проблемом у вези Фуријеових редова, а о коме је било речи у претходном прилогу, довела су га до формулисања, сада добро познате, *контиуум хипотезе*.

Сваки непребројив подскуп од $\mathbb{R}$ у бијекцији је са $\mathbb{R}$.

Другим речима, ако је $A \subseteq \mathbb{R}$, онда $|A| \leq \aleph_0$ или $|A| = \mathfrak{c}$. Кантор је покушавао да докаже ову хипотезу и најављивао је публиковање овог доказа, али то се никада није десило. Испоставило се да је то питање много дубље и теже него што се очекивало. Но, колекција скупова за коју се ова хипотеза може доказати проширивана је и тако је и започела тзв. *Дескриптивна теорија скупова* У овом прилогу показаћемо како се може доказати континуум хипотеза за фамилију Борелових[1] скупова, тј. показаћемо да је сваки непребројив Борелов скуп кардиналности $\mathfrak{c}$.

Подсетимо се најпре неколико неопходних појмова.

Дефиниција III.1 Нека је X непразан скуп. Колекција $\mathcal{F}$ подскупова од X је σ-алгебра уколико су испуњени следећи услови:
1) $X \in \mathcal{F}$;
2) Ако за све $n \in \mathbb{N}$ $A_n \in \mathcal{F}$, онда и $\cup_{n\in\mathbb{N}} A_n \in \mathcal{F}$;
3) Ако $A \in \mathcal{F}$ онда и $A^c \in \mathcal{F}$.

Јасно је да тада и пресек пребројиво много скупова из σ-алгебре припада тој σ-алгебри.

Дефиниција III.2 Нека је X било који тополошки простор. Најмања σ-алгебра која садржи фамилију свих отворених скупова назива се σ-алгебра Борелових скупова.

[1] Félix Edouard Justine Emile Borel (1871–1956), француски математичар.

Како ће сви простори које ћемо разматрати бити метрички простори, то није неопходно познавање топологије за даље читање овог додатка.

Наш задатак ће бити да докажемо да је сваки непребројив Борелов подскуп од $\mathbb{R}^n$ кардиналности $\mathfrak{c}$. Доказаћемо најпре једну техничку лему, која нам је корисна за даљи рад.

Лема III.3 Нека је $\mathcal{A}$ колекција подскупова скупа X, која има својство да је комплемент сваког скупа из $\mathcal{A}$ једнак пресеку пребројиво много скупова из $\mathcal{A}$. Тада се најмања σ-алгебра која садржи $\mathcal{A}$ поклапа са најмањом фамилијом скупова која садржи $\mathcal{A}$ и затворена је у односу на највише пребројиве пресеке и највише пребројиве дисјунктне уније.

Доказ. Означимо са Σ најмању σ-алгебру која садржи $\mathcal{A}$, са $\mathcal{S}$ фамилију из услова леме и нека је

$$\mathcal{B} = \{A \in \mathcal{S} : X \setminus A \in \mathcal{S}\}.$$

Доказаћемо да је $\mathcal{B} = \mathcal{S} = \Sigma$. Ако је $A \in \mathcal{A}$, онда је по претпоставци $X \setminus A = \cap_{n \in \mathbb{N}} A_n$ при чему $A_n \in \mathcal{A}$. Како је Σ једна σ-алгебра која садржи $\mathcal{A}$, то наведени пресек припада Σ и закључујемо да $A \in \mathcal{B}$, те следи да је $\mathcal{A} \subseteq \mathcal{B}$. Такође је јасно да мора бити $\mathcal{S} \subseteq \Sigma$. Дакле, за сада знамо да је

$$\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{S} \subseteq \Sigma.$$

Довољно је, дакле, доказати да је $\mathcal{B}$ једна σ-алгебра (тада мора бити $\Sigma \subseteq \mathcal{B}$, по дефиницији Σ).

Докажимо најпре да је $\mathcal{B}$ затворена у односу на разлику скупова и коначне уније. Наравно да је довољно то доказати за унију два скупа.

Нека $A, B \in \mathcal{B}$. Пре свега, $X \setminus (A \setminus B) = (X \setminus A) \cup (A \cap B) \in \mathcal{S}$, пошто су скупови $X \setminus A$ и $A \cap B$ дисјунктни, $\mathcal{B} \subseteq \mathcal{S}$ и $\mathcal{S}$ је затворена у односу на коначне пресеке и коначне дисјунктне уније. Дакле, $A \setminus B \in \mathcal{B}$. Тада је $A \cup B = (A \setminus B) \cup B \in \mathcal{S}$, пошто је $\mathcal{B} \subseteq \mathcal{S}$ и $\mathcal{S}$ затворена у односу на дисјунктне уније. Но, $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \in \mathcal{S}$ и добијамо да је $A \cup B \in \mathcal{B}$.

Ако $A_n \in \mathcal{B}$, онда је

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} \left(A_n \setminus \bigcup_{j<n} A_j \right),$$

а према претходним резултатима $A_n \setminus \bigcup_{j<n} A_j \in \mathcal{B}$ и како су ти скупови дисјунктни, добијамо да наведена унија припада $\mathcal{S}$. Осим тога,

$$X \setminus \left(\bigcup_{n \in \mathbb{N}} A_n \right) = \bigcap_{n \in \mathbb{N}} (X \setminus A_n) \in \mathcal{S},$$

пошто је $\mathcal{S}$ затворена у односу на пребројиве пресеке. Закључујемо да је $\mathcal{B}$ затворена у односу на пребројиве уније, а како је очигледно затворена у односу на комплемент (тако смо је и изабрали), добијамо да је $\mathcal{B}$ једна σ-алгебра, што и завршава доказ. $\square$

Напомена: Када у претходном доказу, а и касније, говоримо о пребројивим пресецима, односно унијама, наравно да не мислимо да су ти пресеци (уније) сами по себи пребројиви скупови, него су то пресеци (уније) *пребројиве* фамилије скупова.

Колекција отворених скупова метричког простора испуњава наведено својство. Наиме, ако је U отворен скуп у метричком простору X, онда је његов комплемент $F = X \setminus U$ затворен скуп. За сваки $A \subseteq X$ и елемент $x \in X$ дефинише се растојање тачке x од подскупа A, у ознаци $d(x, A)$ са:

$$d(x, A) := \inf\{d(x, a) : a \in A\}.$$

Тада је $d(x, A) = 0$ ако и само је $x \in \overline{A}$. Дакле, у случају затвореног скупа F добијамо: $x \in F$ ако и само ако је $d(x, F) = 0$. Није тешко проверити да је за свако $\varepsilon > 0$, скуп $\{x \in X : d(x, F) < \varepsilon\}$ један отворени скуп који садржи F. Тада је

$$F = \bigcap_{n \geq 1} \left\{x \in X : d(x, F) < \frac{1}{n}\right\},$$

те је комплемент отвореног скупа једнак пресеку пребројиво много отворених скупова и то је управо услов о коме смо говорили.

Наведимо идеју доказа тврђења да је сваки непребројив Борелов скуп у $\mathbb{R}^n$ кардиналности $\mathfrak{c}$.

Доказаћемо следеће теореме.

Теорема III.4 Сваки затворени подскуп сепарабилног метричког простора може се приказати као унија једног савршеног скупа и једног највише пребројивог скупа.

Овај резултат је познат и као Кантор-Бендиксонова[2] теорема.

Теорема III.5 Сваки непразан савршен скуп у комплетном метричком простору је кардиналности бар $\mathfrak{c}$.

Теорема III.6 Сваки Борелов скуп у $\mathbb{R}^n$ је слика при неком „1–1“ пресликавању неког затвореног подскупа једног комплетног сепарабилног метричког простора.

Из ових теореме тражено тврђење следи — непребројив Борелов скуп у $\mathbb{R}^n$ је у бијекцији са неким затвореним подскупом комплетног сепарабилног метричког простора. Тај затворени скуп садржи у себи непразан савршен подскуп, који мора имати кардиналност бар $\mathfrak{c}$. Дакле,

[2] Ivar Otto Bendixson (1861–1935), шведски математичар.

и почетни Борелов скуп је кардиналности бар $\mathfrak{c}$, а како је његова кардиналност највише $\mathfrak{c}$, то је кардиналност заиста $\mathfrak{c}$.

Пређимо на доказе наведених теорема.

За доказ Теореме **III**.4 потребно је да се подсетимо појма савршеног скупа, а увешћемо и појам, са којим се читаоц највероватније до сада није срео.

Скуп P је савршен уколико је $P = P'$. Дакле, савршен скуп је онај затворени скуп чија је свака тачка његова тачка нагомилавања. Скуп тачака *кондензације* скупа $A \subseteq X$, у ознаци A_γ, је скуп свих тачака из X у чијој се свакој отвореној околини налази *непребројиво* много тачака из A.

Веома важно својство сепарабилног метричког простора, које ћемо у даљем користити, је следеће: постоји пребројива колекција отворених скупова таква да је сваки отворени скуп у том простору унија чланова те колекције (другим речима, сваки сепарабилан метрички простор има пребројиву базу топологије). Наиме, како је простор сепарабилан, то у њему постоји неки пребројив, свуда густ скуп $D = \{x_n : n \in \mathbb{N}\}$. Тада је

$$\{K(x_n; 1/m) : n \geq 0, m \geq 1\}$$

тражена колекција, где са $K(x; r)$ означавамо отворену куглу са центром у x полупречника r.

Доказ Теореме III.4. Нека је X сепарабилан метрички простор и F затворени подскуп од X. Приметимо најпре да за сваки непребројив подскуп $A \subseteq X$ важи: $A \cap A_\gamma$ је непребројив. Наиме, за сваку тачку $a \in A \setminus A_\gamma$ постоји базни отворени скуп у коме има највише пребројиво много тачака из A. Како базних отворених скупова има пребројиво много, то би скуп $A \setminus A_\gamma$ био унија највише пребројиво много највише пребројивих скупова, па тиме и сам највише пребројив. Уколико је и $A \cap A_\gamma$ пребројив добили бисмо да је и скуп $A = (A \setminus A_\gamma) \cup (A \cap A_\gamma)$ пребројив.

Уколико је F највише пребројив, то немамо шта да доказујемо. Претпоставимо стога да је F непребројив. У том случају је $F_\gamma \neq \emptyset$, а како је скуп затворен, то мора бити $F_\gamma \subseteq F$ (свака тачка кондензације је наравно и тачка нагомилавања, а како је скуп F затворен, он садржи све своје тачке нагомилавања). Доказаћемо:

(1) $F \setminus F_\gamma$ је највише пребројив;

(2) F_γ је савршен скуп.

Из ове две чињенице тврђење следи.

Доказ за (1): Ово је заправо већ доказано. Погледајте горе.

Доказ за (2): Претпоставимо да F_γ није савршен скуп и нека $x \in F_\gamma \setminus F'_\gamma$. Тада постоји отворена околина U тачке x тако да је $U \cap F_\gamma = \{x\}$. Но, како $x \in F_\gamma$, скуп $U \cap F$ је непребројив. Према претходном он садржи непребројиво много својих тачака кондензације, но $(U \cap F) \cap (U \cap F)_\gamma \subseteq (U \cap F) \cap F_\gamma = \{x\}$. $\square$

Доказ Теореме III.5. Нека је P непразан савршен скуп у комплетном метричком простору X. Како је он нужно бесконачан (коначни скупови немају тачке нагомилавања), изаберимо две тачке $a_0 \neq a_1$ из P. Уочимо две дисјунктне затворене кугле $\overline{K}_0$ и $\overline{K}_1$ око тих тачака. Одговарајуће отворене кугле садрже бесконачно много тачака из P пошто су изабране тачке, тачке нагомилавања од P ($P = P'$). У кугли K_0 изаберимо тачке $a_{00} \neq a_{01}$, а у кугли K_1 тачке $a_{10} \neq a_{11}$. Тачке a_{00} и a_{01} садржане су у неким дисјунктним затвореним куглама $\overline{K}_{00}$ и $\overline{K}_{01}$ које у садржане у кугли $\overline{K}_0$. Осим тога, претпоставимо да су полупречници тих кугли мањи од половине полупречника кугле $\overline{K}_0$. Урадимо то исто са тачкама a_{10} и a_{11}. Поновимо поступак са сваком од четири новодобијене отворене кугле K_{ij}. Свака од њих садржи бесконачно много тачака из P, те можемо изабрати две тачке a_{ij0} и a_{ij1} из P, а потом и одговарајуће кугле при чему их бирамо тако да је полупречник нових кугли мањи од половине полупречника претходних кугли.

Понављањем поступка добијамо за сваки низ $(i_0, i_1, i_2, \ldots)$ нула и јединица, опадајући низ затворених скупова

$$\overline{K}_{i_0} \cap P \supseteq \overline{K}_{i_0 i_1} \cap P \supseteq \cdots \supseteq \overline{K}_{i_0 i_1 i_2 \cdots i_n} \cap P \supseteq \cdots$$

чији дијаметри теже нули (сетимо се како смо бирали полупречнике кугли). Како је простор комплетан, то је пресек сваког од ових низова затворених скупова непразан и представља елемент из P. Но, за различите низове добијамо различите елементе (одговарајуће кугле су дисјунктне). Како је кардиналност скупа свих низова нула и јединица једнака $\mathfrak{c}$, то имамо бар толико различитих тачака у P, тј. $|P| \geq \mathfrak{c}$. $\square$

Комплетан сепарабилан метрички простор, који се наводи у Теореми **III**.6 је следећи простор. На скупу $\mathbb{R}^{\mathbb{N}}$ дефинишемо метрику на следећи начин.

$$d((a_k), (b_k)) := \sum_{k=0}^{\infty} \frac{1}{2^k} \frac{|a_k - b_k|}{1 + |a_k - b_k|}.$$

Није тешко проверити да су сва својства метрике испуњена. Како су елементи у простору $\mathbb{R}^{\mathbb{N}}$ низови реалних бројева, то ћемо за низове у том простору користити горње индексе. Ако је (x^m) низ у простору $\mathbb{R}^{\mathbb{N}}$, онда $x^m \to x^0$ ако и само ако за све $k \in \mathbb{N}$ важи: $x_k^m \to x_k^0$. Ово није тешко доказати. Користећи овај резултат, на стандардан начин се показује да је овај простор комплетан. Он јесте сепарабилан, јер се може показати да је скуп свих низова рационалних бројева који су почев од неког индекса једнаки 0, један пребројив свуда густ скуп.

Доказ Теореме III.6. Да бисмо доказали да за сваки Борелов скуп B у $\mathbb{R}^n$ постоји затворен скуп F у $\mathbb{R}^{\mathbb{N}}$ и непрекидна „1–1" функција $f\colon \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^n$ таква да је $f[F] = B$, довољно је на основу Леме **III**.3 доказати три чињенице:

1. То је тачно за сваки отворени подскуп од $\mathbb{R}^n$;
2. Ако је тачно за $B_0, B_1, \ldots$, онда је тачно и за $\cap_{k\in\mathbb{N}} B_k$;
3. Ако је тачно за $B_0, B_1, \ldots$ и ако су ови скупови дисјунктни, онда је тачно и за $\cup_{k\in\mathbb{N}} B_k$.

Доказ за 1: Нека је $U \subseteq \mathbb{R}^n$. Јасно је да је тврђење тачно у случају $U = \mathbb{R}^n$ (зашто?). Претпоставимо стога да је $U \neq \mathbb{R}^n$. Формирајмо скуп

$$F = \left\{ \left(x_0, \ldots, x_{n-1}, \frac{1}{d(x, \partial U)}, 0, 0, \ldots \right) : x \in U \right\},$$

где је $x = (x_0, \ldots, x_{n-1})$, а ∂U граница скупа U. Како је U отворен скуп то је $\partial U = \overline{U} \setminus U$. Јасно је да је рестрикција пројекције на првих n координата $((x_0, x_1, \ldots) \mapsto (x_0, \ldots, x_{n-1}))$ непрекидна, „1–1" функција која F слика на U. Једино треба доказати да је F затворен скуп у $\mathbb{R}^{\mathbb{N}}$.

Нека $y \in \overline{F}$. То значи да постоји низ (y^k), $y^k \in F$, такав да $y^k \to y$. Како је $y^k_j = 0$ за $j \geq n+1$, то је и $y_j = 0$ за $j \geq n+1$. Из $y^k \to y$ следи да $(y^k_0, \ldots, y^k_{n-1}) \to (y_0, \ldots, y_{n-1})$. Стога $(y_0, \ldots, y_{n-1}) \in \overline{U}$. Ми желимо да покажемо да заправо $(y_0, \ldots, y_{n-1}) \in U$. Како

$$\frac{1}{d((y^k_0, \ldots, y^k_{n-1}), \partial U)} \to y,$$

закључујемо да је низ $\left(\frac{1}{d((y^k_0,\ldots,y^k_{n-1}),\partial U)} \right)$ ограничен и стога добијамо да $d((y^k_0, \ldots, y^k_{n-1}), \partial U) \not\to 0$. Но, уколико $(y_0, \ldots, y_{n-1}) \in \overline{U} \setminus U = \partial U$, узимајући у обзир чињеницу да $(y^k_0, \ldots, y^k_{n-1}) \to (y_0, \ldots, y_{n-1})$ и непрекидност метрике, добијамо да $d((y^k_0, \ldots, y^k_{n-1}), \partial U) \to 0$. Закључујемо да $(y_0, \ldots, y_{n-1}) \in U$, а осим тога и да је

$$y_n = \frac{1}{d((y_0, \ldots, y_{n-1}), \partial U)}.$$

Дакле, $y \in F$ те је скуп F затворен.

Доказ за 2: Нека су B_i Борелови скупови за које постоје затворени скупови F_i у $\mathbb{R}^{\mathbb{N}}$ и бијекције $f_i : F_i \to B_i$. Желимо да покажемо да постоји затворени скуп F у $\mathbb{R}^{\mathbb{N}}$ и бијекција $f\colon F \to \bigcap_{i\in\mathbb{N}} B_i$. Искористићемо чињеницу да у простору $\mathbb{R}^{\mathbb{N}}$ „има доста места" и „сместићемо" скупове F_i на погодан начин у $\mathbb{R}^{\mathbb{N}}$. Наравно, наиван покушај да за F узмемо пресек свих F_i не може бити успешан пошто се чак може десити да је тај пресек празан.

Урадићемо то пажљивије. Пре свега, скуп природних бројева $\mathbb{N}$ можемо приказати у облику бесконачне дисјунктне уније бесконачних скупова: $\mathbb{N} = \cup_{i\in N} N_i$. То можемо урадити, нпр. на следећи начин. Поређајмо све просте бројеве у растући низ: $p_o < p_1 < p_2 < \cdots$. У N_0 „ставимо" све парне природне бројеве. У N_1 „стављамо" све непарне природне бројеве дељиве са 3. У N_k се налазе сви природни бројеви дељиви са p_k, који нису ни у једном од претходних N_i, за $i < k$. Јасно је да су тако добијени скупови бесконачни, дисјунктни и да је сваки природан број у неком од њих. Јасно је да је $\mathbb{R}^{\mathbb{N}}$ хомеоморфан са $\mathbb{R}^{N_i}$ за све i (сваки N_i је у бијекцији са $\mathbb{N}$). Нека су $f_i : F_i \to B_i$ бијекције за које знамо да постоје, где су F_i затворени скупови у $\mathbb{R}^{N_i}$. Сада ћемо све те скупове „поставити" на њихова места у $\mathbb{R}^{\mathbb{N}}$. Формирамо скуп

$$F^* = \{x \in \mathbb{R}^{\mathbb{N}} : (\forall i \in \mathbb{N}) x_{|N_i} \in F_i\}.$$

Присетимо се да је елемент $x \in \mathbb{R}^{\mathbb{N}}$, заправо функција $x : \mathbb{N} \to \mathbb{R}$ и да онда има смисла тражити рестрикцију функције на неки подскуп. Овај скуп јесте затворен (он је пресек инверзних слика затворених скупова F_i при пројекцијама на просторе $\mathbb{R}^{N_i}$), али је још увек „превелики" за оно што нам треба (нисмо узели у обзир функције f_i при формирању овог скупа). Тражени скуп је

$$F = \{x \in F^* : (\forall i \in \mathbb{N})(\forall k \in \mathbb{N}) f_i(x_{|N_i}) = f_k(x_{|N_k})\},$$

а тражена непрекидна функција $f\colon F \to \cap_{i\in\mathbb{N}} B_i$ задата је са $f(x) = f_0(x_{|N_0})$. Наравно, нема ништа специјално у вези индекса 0, могли смо да узмемо и било који други индекс (погледајте како је скуп F задат). Скуп F је задат одговарајућим једнакостима и стога је затворен. Само треба проверити да је f бијекција. Како су функције f_i „1–1" функције, то је и f „1–1". Наиме, нека је $f(x) = f(y)$. То значи да је за свако $i \in \mathbb{N}$, $f_i(x_{|N_i}) = f_i(y_{|N_i})$ (погледајте како је дефинисана функција f и како је задат скуп F). Како је f_i „1–1", добијамо да за свако $i \in \mathbb{N}$ важи: $x_{|N_i} = y_{|N_i}$. Но, унија скупова N_i је цео скуп природних бројева и добијамо да је $x = y$.

Доказ за 3: По претпоставци постоји затворени подскупови F_i у $\mathbb{R}^{\mathbb{N}}$ који су у бијекцији са B_i, при чему су скупови B_i међусобно дисјунктни. Наравно, скупови F_i не морају бити дисјунктни, а осим тога унија затворених скупова не мора бити затворен скуп. Но, ево шта ћемо урадити. Јасно је да је простор $\mathbb{R}^{\mathbb{N}\setminus\{0\}}$ хомеоморфан простору $\mathbb{R}^{\mathbb{N}}$. Сваки од скупова F_i „сместићемо" на одговарајући ниво. Другим речима, посматрамо скупове $F_i^* \subseteq \mathbb{R}^{\mathbb{N}}$ задате са:

$$F_i^* = \{(i, x_0, x_1, \ldots) : (x_0, x_1, \ldots) \in F_i\}.$$

Дакле, сваки од скупова F_i смо поставили на „висину" i (замислите паралелне равни на нивоима 0, 1, итд. и у свакој од њих по један затворен скуп). Јасно је да постоји непрекидна бијекција између скупа $F = \cup_{i\in\mathbb{N}} F_i$ и скупа $\cup_{i\in\mathbb{N}} B_i$, која је задата коришћењем функција f_i. Једино што треба проверити је да је скуп F затворен. Покажимо да у сваком метричком простору важи следећи резултат: ако су F_i, за $i \in \mathbb{N}$ затворени скупови и ако је $d(F_i, F_j) \geq \frac{1}{2}$, за $i \neq j$, онда је скуп $F = \cup_{i\in\mathbb{N}} F_i$ затворен. Овде је растојање скупова $d(A, B)$ задато са:

$$d(A, B) := \inf\{d(a, b) : a \in A, b \in B\}.$$

Ово није тешко доказати. Претпоставимо да $x \in \overline{F}$. То значи да постоји низ (x_n) тачака из F који конвергира ка x. Дакле, постоји $n_0 \in \mathbb{N}$ тако да за све $n \geq n_0$ важи $d(x, x_n) < 1/4$. Тада за $m, n \geq n_0$ добијамо: $d(x_m, x_n) \leq d(x_m, x) + d(x, x_n) < 1/4 + 1/4 = 1/2$. Закључујемо да за $n \geq n_0$, сви чланови низа морају бити у истом скупу F_i за неко i. Како је тај скуп затворен, то и x, као гранична вредност тог низа, мора бити у F_i, те закључујемо да је скуп F затворен.

Наши скупови F_i задовољавају услове овог тврђења (нулте координате се разликују бар за 1 — проверите дефиницију метрике на $\mathbb{R}^{\mathbb{N}}$), те је скуп F затворен. Овим је завршен доказ Теореме **III**.6. $\square$

Литература

[1] P. J. Cameron, *Sets, Logic, and Categories*, Springer-Verlag London Ltd, 2nd printing 2000.

[2] K. Ciesielski, *Set Theory for the Working Mathematician*, London Math Society Student Texts 39, Cambridge University Press, 1997.

[3] J. W. Dauben, *Georg Cantor, His Mathematics and Philosophy of the Infinite*, Princeton University Press, Princeton, New Jersey, 1979.

[4] K. Devlin, *The Joy of Sets, Fundamentals of Contemporary Set Theory, Second Edition*, Springer-Verlag New York Inc. Corrected fourth printing, 1997.

[5] J. Ferreirós, *Labyrinth of Thought, A history of Set Theory and its Role in Modern Mathematics, Second Revised Edition*, Birkhäuser Verlag AG, Basel - Boston - Berlin, 2007.

[6] I. Grattan-Guinness, *The Search for Mathematical Roots 1870–1940*, Princeton University Press, Princeton, New Jersey, 2000.

[7] T. Hawkins, *Lebesgue's Theory of Integration, Its Origins and Development*, AMS Chelsea Publishing, American Mathematical Society, Providence, Rhode Island, 2002.

[8] M. Hallett, *Cantorian Set Theory and Limitation of Size*, Clarendon Press, Oxford, 1984.

[9] P. Komjáth, V. Totik, *Problems and Theorems in Classical Set Theory*, Springer Science+Business Media, LLC, New York, 2006.

[10] S. M. Srivastava, *A Course on Borel Sets*, Springer-Verlag New York, Inc. 1998.

[11] S. Wagon, *The Banach-Tarski Paradox*, Cambridge University Press, New York, 1994.

Индекс