BANACH – TARSKIJEV “PARADOKS”

I ANALOGNI VON NEUMANNOVI REZULTATI U NIŽIM DIMENZIJAMA

VEDRAN ČAČIĆ

((Boljem razumijevanju posljedicâ Aksioma izbora))

SAŽETAK. U ovom radu dokazuje se Banach–Tarskijev teorem (u nekoliko varijanti, specijalnih slučajeva i generalizacijâ), te se razmatraju posljedice koje on ima na teoriju mjere.

Centralna tvrdnja je teorem 9, koji tvrdi da se jedinična kugla u $\mathbb{R}^3$ može rastaviti na konačno mnogo (konkretno, 5) dijelova, od kojih se primjenom izometrijâ mogu sastaviti *dvije* jedinične kugle. Koliko god paradoksalno izgledala, ta tvrdnja se može dokazati u standardnoj ZFC teoriji, koristeći sredstva koja su većini matematičarâ dobro poznata, na način koji će biti detaljno prikazan.

Jedan od naglasaka stavljen je na dobivanje (koliko je to moguće) analognih paradoksalnih rastavâ u nižim dimenzijama, dakle u ravnini i na pravcu.

((U radu se bitno koristi Aksiom izbora.))

Oni kojima se notacija učini previše egzotičnom za normalno praćenje, mogu prvo baciti pogled na odjeljak V, strana 43.

Date: 6. studenog 2015.
1991 *Mathematics Subject Classification.* Teorija skupova, osnove matematike, mjera.
Key words and phrases. Banach–Tarski, aksiom izbora, paradoks.
Mentor: **M. Vuković.**

Sadržaj

A. Uvod. Slobodni produkti

Cilj ovog rada je dokazati Banach–Tarskijev teorem, kao i mnoštvo rezultatâ posredno ili neposredno vezanih uz njega, te dati neke osnove opće teorije jednakosastavljivosti. U tu svrhu, koristit će se (u smislu smatrati se poznatima) uglavnom neki pojmovi i teorije s kojima bi trebali biti upoznati studenti viših godinâ dodiplomskog studija matematike. Međutim, kako nam na samom početku treba pojam slobodnog produkta grupâ, koji se u studiju matematike susreće relativno kasno, odlučio sam u ovom (i sljedećem) odjeljku dati neke osnovne informacije o tome, kako bi ovaj rad postao dostupan (nadam se) širem krugu studenata. Detalji o tome, kao i o mnogim drugim algebarskim pojmovima, idejama i rezultatima koje ćemo u ovom radu koristiti, mogu se potražiti u [3].

Teorija kategorijâ definira slobodni produkt grupâ jednostavno kao *koprodukt* (opći kategorološki pojam) u kategoriji grupâ. To jednostavno znači da je slobodni produkt dviju grupâ G_1 i G_2 neka grupa G (oznaka $G = G_1 \star G_2$), zajedno s homomorfizmima grupâ $\iota_1 : G_1 \to G$ i $\iota_2 : G_2 \to G$, koja je "univerzalna" u smislu da za svaku grupu H s homomorfizmima grupâ $\rho_1 : G_1 \to H$ i $\rho_2 : G_2 \to H$ postoji jedinstveni homomorfizam grupâ $\rho : G \to H$ takav da vrijedi $\rho \circ \iota_1 = \rho_1$ i $\rho \circ \iota_2 = \rho_2$. Može se (na općem, kategorološkom nivou) pokazati da su sve grupe, koje mogu stajati na mjestu grupe G gore, međusobno izomorfne, pa se može govoriti o slobodnom produktu kao o jedinstvenom objektu (ako postoji).

Sâmo postojanje slobodnog produkta u kategoriji svih grupâ dokazuje se konstruktivno: polazeći od grupâ-faktorâ, konstruira se skup, na njemu se uvede binarna operacija, i dokaže se da je na taj način dobivena grupa, te da ona ima traženo tzv. *univerzalno* svojstvo. Ovdje dajem pregled tog postupka: prvo promotrimo skup svih (konačnih) riječi nad abecedom koja je unija disjunktnih kopijâ svih grupâ-faktorâ. Dakle, jednostavno konstruiramo riječi od elemenata danih grupâ, pamteći pri tome iz koje je grupe pojedini element. Za takvu riječ kažemo da je *nereducirana* ako se u njoj pojavljuju kao susjedna slova dva elementa iz iste grupe-faktora, ili se u njoj javlja jedinica (neutralni element) neke grupe-faktora. Naravno, riječ je *reducirana* ako takvih pojava u njoj nema.

Redukcija (nereducirane riječi) se sastoji u zamjeni dvaju susjednih slovâ iz iste grupe njihovim produktom u odgovarajućoj grupi, i/ili brisanju svih neutralnih elemenata iz riječi. Budući da svaka redukcija strogo smanjuje duljinu riječi, nakon konačno mnogo redukcijâ bilo koje riječi moramo dobiti reduciranu riječ. Štoviše, zbog asocijativnosti i svojstva neutralnih elemenata, za svaku riječ je pripadna reducirana riječ jedinstvena (na riječ možemo primjenjivati redukcije na razne načine, ali konačan rezultat je jednoznačno određen). Na taj način, ako promotrimo relaciju ekvivalencije generiranu reduciranjem riječî, vidimo da u svakoj klasi ekvivalencije postoji jedinstvena reducirana riječ, pa umjesto s klasama možemo raditi s reduciranim riječima, što ćemo i činiti.

Dakle, skup-nosač slobodnog produkta bit će skup reduciranih riječî. Binarna operacija bit će konkatenacija, uz eventualno reduciranje (dakle, produkt dvije riječi w_1 i w_2 bit će jedinstvena pripadna reducirana riječ od w_1w_2). Na taj način, neutralni element je prazna riječ (koja se često, uz multiplikativnu notaciju, označava s 1 — do zabune ne može doći jer se neutralni elementi pojedinih grupâ-faktorâ ne pojavljuju u reduciranim riječima), a inverz riječi w je riječ w^{-1}, koja se dobiva tako da se riječ w pročita obrnutim redoslijedom, zamjenjujući pri tome svako slovo njegovim inverzom u pripadnoj grupi (dakle, inverz od $a_1b_2c_1$ bit će $c_1^{-1}b_2^{-1}a_1^{-1}$). Lako se vidi da je, za svaku reduciranu riječ w, riječ w^{-1} također reducirana, te da je njihov produkt u gornjem smislu zaista prazna riječ.

B. Slobodne grupe. Zadavanje grupâ generatorima i relacijama

Za primjer pogledajmo nešto što će nam također trebati kasnije, slobodnu grupu ranga[A] 2. Slobodna grupa ranga 2 je u gornjem kontekstu jednostavno "slobodni kvadrat" aditivne grupe cijelih brojeva, $\mathbb{Z}_\star^2 = \mathbb{Z} \star \mathbb{Z}$. Budući da moramo imati disjunktne kopije, označimo elemente prvog $\mathbb{Z}$ indeksom 1, a drugog indeksom 2. Grupa $\mathbb{Z}$ inače ima aditivnu notaciju, ali to ne smeta — svejedno možemo pisati "slova" (brojeve s indeksima) jedno do drugog. Jedna riječ je npr. $2_14_25_2$. Ta riječ nije reducirana, jer su 4_2 i 5_2 susjedni, iz iste grupe. Redukcijom dobivamo riječ 2_19_2, koja jest reducirana. Također, višestrukom redukcijom riječi $0_13_2(-2)_16_10_2(-4)_15_2(-8)_15_2$ dobivamo reduciranu riječ $8_2(-8)_15_2$. Produkt od 1_23_1 i $5_18_27_1$ je $1_28_18_27_1$, dok je inverz od $(-1)_14_29_1$ jednak $(-9)_1(-4)_21_1$.

Postoji i za nijansu drugačiji pogled na slobodne grupe. On dolazi do izražaja ako promotrimo ta dva faktora ("prvi" i "drugi" $\mathbb{Z}$) kao beskonačne cikličke grupe (što karakterizira $\mathbb{Z}$), ali s različitim (preciznije, nezavisnim) generatorima (kako bismo imali zahtijevanu disjunktnost). U gornjem slučaju, to su npr. 1_1 i 1_2. Ovdje ih označimo sa σ i τ tim redom, i prijeđimo potpuno na multiplikativnu notaciju. Dakle, $n_1 = \sigma^n$, a $n_2 = \tau^n$, za svaki $n \in \mathbb{Z}$. Jer se 0_1 i 0_2 ne pojavljuju u reduciranim riječima, slučaj $n = 0$ nam ne treba. U slučaju $n > 0$ možemo npr. σ^n zapisati kao n slovâ σ zaredom, dok ga u slučaju $n < 0$ možemo zapisati kao $-n$ "slovâ" σ^{-1}. Tako dobivamo da se svaka riječ u grupi (izomorfnoj sa) $\mathbb{Z}_\star^2$ može zapisati, i to na jedinstven način, kao riječ sastavljena od 4 "slova": σ, σ^{-1}, τ i τ^{-1}, takva da se nigdje u njoj ne pojavljuju podriječi $\sigma\sigma^{-1}$, $\sigma^{-1}\sigma$, $\tau\tau^{-1}$ niti $\tau^{-1}\tau$. Množenje u tom kontekstu je konkatenacija, uz "križanje" (brisanje iz novodobivene riječi) svih "zabranjenih" podriječî koje se pojave na mjestu spajanja, dok je invertiranje, kao i prije, čitanje riječi obrnutim redoslijedom, uz zamjene $\sigma \leftrightarrow \sigma^{-1}$ i $\tau \leftrightarrow \tau^{-1}$.

[A] Iako se pojam ranga (kao kardinaliteta proizvoljnog nezavisnog skupa generatorâ) uglavnom veže uz slobodne *Abelove* grupe, analogni pojam može se definirati i za slobodne (ne-Abelove) grupe. Naime, promatrajući komutatorske kvocijente u slobodnim grupama može se dokazati da su svaka dva nezavisna skupa generatorâ neke slobodne grupe G jednakobrojna (za detalje vidjeti [3, vježba 12 na str. 75]). Ovdje koristim pojam "rang" (slobodne grupe) upravo u tom smislu. Dakle, slobodna grupa ranga 2 je grupa koja je slobodna nad dvočlanim skupom, odnosno ima 2 nezavisna generatora.

Analogno, slobodna grupa ranga κ (gdje je κ bilo koji kardinal) je slobodni produkt κ faktorâ $\mathbb{Z}$, dakle $\mathbb{Z}_\star^\kappa$. Kao što smo prije imali skup generatorâ $\{\sigma, \tau\}$ kardinaliteta 2, sada možemo promatrati neki skup X, kardinaliteta κ, kao skup (nezavisnih) generatorâ za $\mathbb{Z}_\star^\kappa$. Da bismo to istakli, možemo tu grupu (instancijaciju općenite slobodne grupe ranga κ) označiti sa $\mathbb{Z}_\star^X$. Kažemo da je grupa $\mathbb{Z}_\star^X$ slobodna *nad* X.

Preslikavanje $\iota : X \to Z_\star^X$, koje slovu $x \in X$ pridružuje jednoslovnu riječ $x \in Z_\star^X$, je očito injekcija i zovemo ga *kanonska inkluzija*. Pokazuje se da su slobodne grupe općenito slobodni objekti (kategorološki pojam) u kategoriji grupâ, tj. da vrijedi sljedeći

Teorem 1. *((bez dokaza, može se naći u* [3, T. I.9.2]*)) Neka je $F = \mathbb{Z}_\star^X$ slobodna grupa nad skupom X, i $\iota : X \hookrightarrow F$ pripadna kanonska inkluzija. Tada za bilo koju grupu G i bilo koje preslikavanje $\theta : X \to G$, postoji jedinstveni homomorfizam grupâ $\Theta : F \to G$, takav da je $\Theta \circ \iota = \theta$.*

Neka je G bilo koja grupa. G je tada ujedno i skup, pa možemo u gornji teorem uvrstiti $X := G$, $F := \mathbb{Z}_\star^G$, i $\theta := 1_G$. Dobivamo homomorfizam $\Theta : \mathbb{Z}_\star^G \to G$, koji zapravo predstavlja "računanje" u G: riječi sastavljenoj od elemenata iz G pridruži njen "rezultat" (produkt svih njenih slova u tom redoslijedu). Budući da se već sve jednoslovne riječi u $\mathbb{Z}_\star^G$ na taj način preslikaju u sve elemente od G, Θ je surjekcija, dakle epimorfizam. No da bi Θ bio epimorfizam, nije potrebno uzeti za X cijeli G: iz definicije "računanja" vidimo da je dovoljno uzeti neki skup generatorâ za G, s čime ćemo i raditi.

Dakle, grupa G je generirana skupom X, i imamo epimorfizam grupâ $\Theta : F \twoheadrightarrow G$, gdje je $F := \mathbb{Z}_\star^X$ slobodna grupa nad skupom X. Po I. teoremu o izomorfizmu, G je izomorfna kvocijentnoj grupi $F/_N$, gdje je $N := \operatorname{Ker}\Theta$ jezgra "računanja" u G, odnosno skup svih reduciranih riječi čiji je rezultat u G jednak e (neutralni element). Dakle, to su dodatne relacije koje generatori moraju zadovoljavati da bi činili grupu G. Slično kao što gore nismo morali uzeti cijeli G za X, već samo skup generatorâ, tako ni ovdje ne moramo specificirati cijeli N, već samo neki skup generatorâ $Y \subseteq N$, dakle skup relacijâ koje generiraju sve ostale. Štoviše, Y možemo još "smanjiti" ako se sjetimo da je N, kao jezgra homomorfizma, sigurno normalna podgrupa od F, pa možemo staviti da N bude $\langle Y \rangle_{\trianglelefteq F}$, odnosno, normalna podgrupa od F generirana s Y (presjek svih normalnih podgrupâ od F koje sadrže Y).

Na taj način, svaku grupu možemo zadati s X i Y, i ona je jedinstvena do na izomorfizam, jer je izomorfna s $\mathbb{Z}_\star^X/_{\langle Y \rangle_{\trianglelefteq \mathbb{Z}_\star^X}}$. Takav način zadavanja zove se *zadavanje grupe pomoću generatorâ i relacijâ*, i kažemo da je grupa G zadana generatorima $\{x\}_x^X$ i relacijama $\{y = e\}_y^Y$. Često se umjesto relacije oblika $u^{-1}v = e$ piše njoj ekvivalentna $u = v$ (gdje su u i v riječi iz $\mathbb{Z}_\star^X$). Npr. Kleinova četvorna grupa, $\mathcal{G}r(2_\times^2)$, zadana je generatorima a i b, te relacijama $ab = ba$ i $a^2 = b^2 = e$.

C. Algebarska osnova paradoksa

Promotrimo slobodni produkt (cikličkih) grupâ redova 2 i 3:

$$\mathcal{G}r(G) := \mathcal{G}r(\{1, \varphi\}) \star \mathcal{G}r(\{1, \psi, \psi^{-1}\}),$$

ili, ekvivalentno, grupu generiranu generatorima φ i ψ, te relacijama $\varphi^2 = 1$ i $\psi^3 = 1$.

Zatim, definirajmo funkciju $f : G \to 3$ (lijevolinearno) rekurzivno na reduciranim riječima od G, sljedećim formulama:

$$\begin{aligned} f(1) &:= 0 \\ f(\varphi\,\alpha) &:= \delta_0(f(\alpha)) \\ f(\psi^k\,\alpha) &:= f(\alpha) +_3 k. \end{aligned}$$

(S δ_0 je označena Kroneckerova delta-nula funkcija; $0 \mapsto 1$ & $1 \mapsto 0$ & $2 \mapsto 0$.) Naravno, u zadnjoj relaciji, da bi riječ $\psi^k\alpha$ bila reducirana, nužno je da vrijedi $k \in \{-1, 1\}$, te da α ne počinje s ψ niti ψ^{-1}, no pokazuje se da vrijedi i više:

Lema 2. *Vrijedi:*

$$(\forall k \in \mathbb{Z})(\forall \alpha \in G)(f(\psi^k\,\alpha) = f(\alpha) +_3 k).$$

Dokaz:

Metodom "optimiziranog iscrpljivanja". Prvo, zbog

$$l +_3 (k \bmod 3) = l +_3 (k +_3 0) = (l +_3 k) +_3 0 = l +_3 k$$

$$\text{i} \quad \psi^k = \psi^{\lfloor \frac{k}{3} \rfloor \cdot 3 + k \bmod 3} = \underbrace{(\psi^3)}_{=1}{}^{\lfloor \frac{k}{3} \rfloor} \psi^{k \bmod 3} = \psi^{k \bmod 3},$$

možemo promatrati samo slučajeve $k \in \{-1, 0, 1\}$. Zatim, zbog simetrije G i f u odnosu na zamjenu $1 \leftrightarrow -1$ ($\Rightarrow \psi \leftrightarrow \psi^{-1}$ & $k +_3 1 \leftrightarrow k +_3 2$), slučaj $k = -1$ je analogan slučaju $k = 1$. Slučaj $k = 0$ je trivijalan:

$$f(\psi^0\,\alpha) = f(1\,\alpha) = f(\alpha) = f(\alpha) \bmod 3 = f(\alpha) +_3 0,$$

pa preostaje dokazati

$$(\forall \alpha \in G)(f(\psi\,\alpha) = f(\alpha) +_3 1).$$

Ako je $\alpha = 1$ ili (reducirani predstavnik od) α počinje s φ, tada je $\psi\,\alpha$ reducirana riječ, pa tvrdnja slijedi direktno iz definicije od f. Ako pak reducirani predstavnik od α počinje s ψ, tada je on jednak $\psi\,\beta$ ili $\psi^{-1}\,\beta$, gdje je β reducirana riječ od G. Tu imamo dva slučaja:

$1^{@}$) $\alpha = \psi\,\beta$. Tada je $f(\alpha) = f(\beta) +_3 1$, pa je

$$f(\psi\,\alpha) = f(\psi\,\psi\,\beta) = f(\psi^{-1}\,\beta) = f(\beta) +_3 (-1) =$$

$$= f(\beta) +_3 2 = f(\beta) +_3 1 +_3 1 = f(\alpha) +_3 1.$$

$2^{@}$) $\alpha = \psi^{-1}\,\beta$. Tada je $f(\alpha) = f(\beta) +_3 (-1)$, pa je

$$f(\psi\,\alpha) = f(\psi\,\psi^{-1}\beta) = f(\beta) = f(\beta) +_3 (-1) +_3 1 = f(\alpha) +_3 1.$$

Vidimo da je u oba slučaja tvrdnja leme istinita. $\square$

"Jezgra" preslikavanja f, definirana sa $\forall_k^3(A_k := f^{\langle}(\{k\}))$, je particija G u 3 skupa: $G = \biguplus_k^3 A_k$.

Teorem 3. *((Algebarska osnova)) Vrijede sljedeće jednakosti:*

$$\begin{aligned} A_1 &= \{\psi\}A_0 \\ A_2 &= \{\psi^{-1}\}A_0 \\ A_1 \uplus A_2 &= \{\varphi\}A_0. \end{aligned}$$

Dokaz:

((1.$\subseteq$)) Uzmimo $\alpha \in A_1$. To znači da je $f(\alpha) = 1$. No tada je po lemi 2 $f(\psi^{-1}\,\alpha) = 1 +_3 (-1) = 0$, pa je $\psi^{-1}\,\alpha \in A_0$, a očito je $\alpha = \psi\,\psi^{-1}\,\alpha$.

((1.$\supseteq$)) Uzmimo $\alpha \in \{\psi\}A_0$. Tada je $\alpha = \psi\,\beta$; $\beta \in A_0$, pa je po lemi 2 $f(\alpha) = f(\beta) +_3 1 = 0 +_3 1 = 1$, tj. $\alpha \in A_1$.

((2.)) Analogno kao ((1.)), koristeći simetriju kao u dokazu leme 2.

((3.)) Prvo uočimo da je $A_1 \uplus A_2 = G \dot{\setminus} A_0$, a iz toga da je (za $\alpha \in G$) $\alpha \in A_1 \uplus A_2 \Leftrightarrow f(\alpha) \neq 0 \Leftrightarrow \delta_0(f(\alpha)) = 0$.

((3.$\subseteq$)) Uzmimo takav α. Ako je $\alpha = 1$ ili (reducirani predstavnik od) α počinje s ψ (ili ψ^{-1}), tada je $\varphi\,\alpha$ reducirana riječ, pa je $f(\varphi\,\alpha) = \delta_0(f(\alpha)) = 0$. Ako je pak reducirani predstavnik od α jednak $\varphi\,\beta$, gdje je β reducirana riječ od G, tada je $f(\varphi\,\alpha) = f(\varphi\,\varphi\,\beta) = f(\beta)$, što mora biti 0 jer je $0 \neq f(\alpha) = f(\varphi\,\beta) = \delta_0(f(\beta))$. Dakle, u svakom slučaju je $f(\varphi\,\alpha) = 0$, odnosno $\varphi\,\alpha \in A_0$, što uz $\alpha = \varphi\,\varphi\,\alpha$ daje tvrdnju.

((3.$\supseteq$)) Uzmimo $\alpha \in A_0$, tj. takav da vrijedi $f(\alpha) = 0$. Ako je $\varphi\,\alpha$ reducirana riječ, tada je $f(\varphi\,\alpha) = \delta_0(f(\alpha)) = \delta_0(0) = 1 \neq 0$. Ako to nije slučaj (a α je reducirana riječ), tada je $\alpha = \varphi\,\beta$ (gdje je β reducirana riječ od G, konkretno, reducirani predstavnik od $\varphi\,\alpha$), pa je $0 = f(\alpha) = f(\varphi\,\beta) = \delta_0(f(\beta))$, iz čega zaključujemo da $f(\varphi\,\alpha) = f(\beta) \neq 0$. Vidimo da je u oba slučaja $\varphi\,\alpha \in A_1 \uplus A_2$, što smo i htjeli dokazati. □

Relacije u gornjem teoremu uspostavljaju prirodne bijekcije između A_0 s jedne strane i A_1, A_2 i $A_1 \uplus A_2$ s druge strane, pa vidimo da su svi oni istog kardinaliteta. To samo po sebi nije ništa čudno — svi moraju biti najviše prebrojivi jer je G prebrojiv, a očito su beskonačni — ali uskoro ćemo vidjeti da, gledano geometrijski, ta činjenica ima prilično zanimljivu interpretaciju.

D. Geometrijska podloga

Neka je $U := \{x \in \mathbb{R}^3 : \|x\| \leq 1\}$ jedinična kugla, a $S := \mathrm{Fr}U$ jedinična sfera u $\mathbb{R}^3$. Za mnoge stvari koje ćemo ovdje raditi bit će nam svejedno da li ih radimo na U ili na S, pa neka nam P označava bilo koji od ta dva skupa (radimo paralelno na U i na S).

Neka su d_1 i d_2 dva pravca kroz 0_3. Interpretirajmo apstraktne generatore od G kao permutacije od P ovako: φ kao osnu simetriju s obzirom na d_1, restringiranu na P, koju nazovimo $\hat{\varphi}$, a ψ kao rotaciju oko d_2 za kut $\frac{2\pi}{3}$ u nekom (fiksnom) smjeru[B], restringiranu na P, koju nazovimo $\hat{\psi}$. Operaciju u G interpretirajmo kao kompoziciju preslikavanjâ. Algebarskim rječnikom, definirajmo da grupa G *djeluje* na skup P na gore opisani način.

S druge strane, ako grupu izometrijâ od P označimo s $\mathrm{Iso}(P)$, možemo na to gledati kao na konstruiranje homomorfizma grupâ $\Theta : G \to \mathrm{Iso}(P)$ koji preslikava generatore od G kao $\varphi \mapsto \hat{\varphi}$ & $\psi \mapsto \hat{\psi}$. Zbog univerzalnog svojstva slobodnog produkta (odnosno kvocijenta slobodne grupe), da bi Θ bio homomorfizam (zapravo i da bi uopće bio dobro definiran), dovoljno je provjeriti samo da je $\hat{\varphi}^2_\circ = \hat{\psi}^3_\circ = \mathit{1}_P$, što je očito točno.

Napomenimo da Θ ne može biti epimorfizam, iz jednostavnog razloga: G je (kao svaka slobodna grupa konačnog ranga) prebrojiva, ali $\mathrm{Iso}(P)$ to nije — primijetimo da sadrži npr. rotacije (restringirane na P) oko d_1 za sve kutove u intervalu $\langle 0, 2\pi\rangle$, kojih očito ima kontinuum.

Sljedeće pitanje koje si postavljamo jest: je li Θ monomorfizam? Naravno, općenito to neće biti — npr. ako uzmemo $d_1 = d_2$, tada $\hat{\varphi}$ i $\hat{\psi}$ komutiraju, pa Θ sigurno nije injekcija (jer je npr. $\Theta(\varphi\,\psi\,\varphi\,\psi^{-1}) = \mathit{1}_P = \Theta(1)$, a $\varphi\,\psi\,\varphi\,\psi^{-1} \neq 1$). Ili, ako je $d_1 \perp d_2$, tada je $\hat{\varphi} \circ \hat{\psi}$ involucija, u što se možemo uvjeriti jednostavnim matričnim računom (budući da se radi o restrikcijama na P linearnih operatorâ od $\mathbb{R}^3$):

$$\left(\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -\frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ 0 & 1 & 0 \\ -\frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} \end{bmatrix}\right)^2_{.} = \begin{bmatrix} \frac{1}{2} & 0 & -\frac{\sqrt{3}}{2} \\ 0 & -1 & 0 \\ -\frac{\sqrt{3}}{2} & 0 & -\frac{1}{2} \end{bmatrix}^2_{.} = \mathrm{I}_3.$$

Tada je dakle $\Theta(\varphi\,\psi\,\varphi\,\psi) = \mathit{1}_P = \Theta(1)$, a $\varphi\,\psi\,\varphi\,\psi \neq 1$, pa Θ opet nije injekcija.

No to su sve ipak posebni slučajevi. Postoji li neki "opći položaj" pravaca d_1 i d_2, takav da nema takvih anomalijâ? Dokazat ćemo (egzistencijalno, a zatim i dati ideju konstruktivnog dokaza) da postoji.

Prvo, primijetimo da struktura preslikavanja Θ (specijalno, njegova injektivnost) ovisi samo o kutu $q := \sphericalangle(d_1, d_2) \in [0, \frac{\pi}{2}]$, pa ubuduće to preslikavanje označimo s Θ_q. (Primjerice, dosad smo dokazali da Θ_0 i $\Theta_{\frac{\pi}{2}}$ nisu monomorfizmi.) Nadalje, znamo da je, da bismo dokazali da je neki Θ_q monomorfizam, dovoljno dokazati da mu je jezgra trivijalna: $\operatorname{Ker}\Theta_q = \{1\}$.

Lema 4. *Za svaku riječ $\alpha \in G$ različitu od 1, postoji samo konačno mnogo kutova q takvih da je odgovarajući Θ_q u α trivijalan, tj.*

$$(\forall \alpha \in G \setminus \{1\})(\overset{\infty}{\forall}\, q \in [0, \frac{\pi}{2}])(\Theta_q(\alpha) \neq \mathit{1}_P).$$

(($\overset{\infty}{\forall}$ znači "za skoro svaki", odnosno, "za svaki osim konačno mnogo".))

[B]Ako baš hoćemo biti "egzaktni", recimo da je d_2 orijentirani pravac, pa onda nazovimo s $\hat{\psi}$ rotaciju oko d_2 za $\frac{2\pi}{3}$ u pozitivnom smjeru.

Dokaz:

Postavimo koordinatni sustav u $\mathbb{R}^3$ tako da d_2 bude koordinatna os x, a d_1 leži u koordinatnoj ravnini $z^\perp$. Sada d_1 ima vektor smjera $(\cos q, \sin q, 0)$, a $\hat{\varphi}$, $\hat{\psi}$ i $\hat{\psi}^{-1}$, prošireni linearno na $\mathbb{R}^3$, imaju matrične zapise (tim redom)

$$\begin{bmatrix} \cos 2q & \sin 2q & 0 \\ \sin 2q & -\cos 2q & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \text{ i } \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}.$$

Uzmimo proizvoljnu reduciranu riječ $\alpha \in G\ ; \alpha \neq 1$. Tada je matrični zapis linearnog proširenja od $\Theta_q(\alpha)$ 3×3-matrica čiji su matrični elementi neki polinomi u varijablama $\cos 2q$ i $\sin 2q$. Uvjet da je ta matrica jednaka I_3 može se izraziti kao sustav algebarskih jednadžbî s nepoznanicama $\cos 2q$ i $\sin 2q$, od kojih je bar jedna netrivijalna (čak i nakon uvažavanja $\cos^2 2q + \sin^2 2q = 1$ — ovdje jest malo "mahanja rukama", ali egzaktan dokaz ovog detalja bio bi prilično dugačak i "tehnički"[C]) jer je α reducirana riječ, pa između svake dvije pojave od φ u α dolazi ψ ili ψ^{-1}. Tada ta jednadžba ima samo konačno mnogo rješenjâ (uzevši u obzir $\cos^2 2q + \sin^2 2q = 1$), pa sustav pogotovo ima konačno mnogo rješenjâ. □

Dobro. Sad možemo dokazati

Teorem 5. *Moguće je odabrati položaj pravaca d_1 i d_2 tako da je pripadni Θ_q monomorfizam, tj.*

$$(\exists q \in [0, \frac{\pi}{2}])(\mathit{Ker}\,\Theta_q = \{1\}).$$

Dokaz:

((Egzistencijalno)) Skup onih $q$ova koji "nisu dobri" je

$$\{q \in [0, \frac{\pi}{2}] : \mathrm{Ker}\,\Theta_q \neq \{1\}\} = \bigcup_{\alpha}^{G \setminus \{1\}} \{q \in [0, \frac{\pi}{2}] : \Theta_q(\alpha) = 1_P\},$$

što je prebrojivo zbog prethodne leme, činjenice da je G prebrojiva, te teorema[D] da je unija prebrojive familije konačnih skupova prebrojiv skup. Međutim, izborâ za q imamo $\mathrm{card}[0, \frac{\pi}{2}]$, odnosno kontinuum. Dakle, mora postojati q koji je "dobar".

((Konstruktivno — ideja)) Zapravo, konstruirati q takav da je odgovarajući Θ_q monomorfizam nije uopće teško — npr. $q = 1$ je sasvim u redu — no veći je problem to dokazati. Možemo, slično kao u dokazu prethodne leme, gledati matrične reprezentacije linearnih proširenjâ od $\hat{\varphi}$ i $\hat{\psi}$, i zaključiti da

---

[C] U odjeljku L prikazan je alternativni pristup, koji, zahvaljujući odmaku na višu razinu apstrakcije, svodi količinu tehničkih detalja na mnogo manju mjeru.

[D] Napomenimo samo da to nije teorem od ZF — već ovdje počinjemo koristiti Aksiom izbora. On se iz dokaza gornjeg teorema doduše može eliminirati — da smo preciznije dokazali prethodnu lemu, mogli bismo pokazati i kako — ali to nam ovdje nije cilj.

su rješenja odgovarajućih algebarskih jednadžbî u svakom slučaju algebarski brojevi, dok su $\sin 2$ i $\cos 2$, koji bi to tebali biti, transcendentni[E] (što je prilično teško elementarno dokazati). □

Ovim teoremom dali smo definicijama iz odjeljka C geometrijsku interpretaciju. Ubuduće fiksirajmo neki "dobar" q (npr. $q := 1$) i identificirajmo $\hat{\varphi}$ i $\hat{\psi}$ s φ i ψ, redom (samim time i grupu G s podgrupom od $\mathrm{Iso}(P)$ generiranom s $\hat{\varphi}$ i $\hat{\psi}$). Sva daljnja razmatranja iz odjeljka C (posebno, definicije od A_0, A_1 i A_2, te tvrdnje iz teorema 3) prirodno se prenose na novu situaciju. Apstraktni skupovi A_0, A_1 i A_2 sada su skupovi nekih izometrijâ od P.

E. Aksiom izbora

Kao što sam napomenuo na početku, ovaj rad koristi Aksiom izbora. Aksiom izbora i inače ima veliku ulogu u teoriji jednakosastavljivosti (kao i u s njom povezanoj teoriji mjere), kako direktno — za dokazivanje velikog broja teoremâ, tako i na meta-razini — što se uglavnom tiče razmišljanjâ o "konstruktivizaciji" dokazâ izbacivanjem korištenja Aksioma izbora iz njih (bilo nalaženjem novih metoda dokazivanja, dokazujući za nijansu slabije tvrdnje, ili pak modificirajući definicije nekih pojmova tako da se mogu konstruktivno upotrijebiti).

Uzmimo za primjer sljedeće tri tvrdnje:

(1) ⟨(u $\mathbb{R}^3$)⟩ *Svaka dva poliedra su konačno jednakosastavljiva.* (S. Banach & A. Tarski, 1924.)
(2) ⟨(u $\mathbb{R}^2$)⟩ *Nikoja dva poligona, od kojih je jedan pravi podskup drugoga, nisu konačno jednakosastavljiva.* (A. P. Morse, 1949.)
(3) ⟨(u $\mathbb{R}^1$)⟩ *Postoji Lebesgue-neizmjeriv podskup segmenta.* (G. Vitali, 1905.)

Uočimo kontrast prve i druge tvrdnje. Također, dokazat ćemo tvrdnju 1 i za više dimenzije od 3, čime ćemo pokazati da konačno-aditivne izometrijski invarijantne mjere na euklidskim prostorima mogu postojati samo u dimenzijama 1 i 2. No treća tvrdnja pokazuje da najpoznatija σ-aditivna[F] mjera ne može biti definirana totalno čak ni u slučaju dimenzije 1.

Sada pogledajmo ovisnost tih tvrdnji o Aksiomu izbora. Prva tvrdnja je jednostavna posljedica jakog Banach–Tarskijevog teorema, i za njen dokaz je potreban Aksiom izbora. Za dokaz treće tvrdnje također, i to znamo dokazati. Druga tvrdnja je zanimljiva. Banach i Tarski su je u svojim

[E] To pokazuje da, čim je $\cos 2q$ (a time i $\sin 2q$) transcendentan, Θ_q jest monomorfizam. Zanimljivo je da obrat ne vrijedi — $\Theta_{\frac{\pi}{4}}$ je monomorfizam (B. Osofsky & S. Adams: Problem 6102 and solution; *American Mathematical Monthly* **85** (1978), 504).

[F] Inače, i σ-aditivnost Lebesgueove mjere bitno ovisi o Aksiomu izbora — postoje modeli za $\mathbb{ZF}$ u kojima je čitav $\mathbb{R}$ prebrojiva unija prebrojivih skupovâ. ⟨(Naravno, "$\mathbb{R}$ u modelu" znači bilo koju strukturu koju dani model ne može razlikovati od $\mathbb{R}$ — je li to, u nekom ontološkom smislu, "onaj pravi $\mathbb{R}$ kakvim ga volimo zamišljati", je ovdje više filozofsko nego matematičko pitanje.)⟩

radovima dokazali, korištenjem Aksioma izbora. Zaključili su da, na taj način, Aksiom izbora jest odgovoran za paradoksalne rastave, ali je isto tako u nekim slučajevima odgovoran za njihovo nepostojanje. Nije se vidjelo kako bi se tvrdnja 2 dokazala bez Aksioma izbora, čak štoviše, na intuitivnoj razini, dokaz tvrdnje 2 koristi Aksiom izbora u još većoj mjeri nego dokaz tvrdnje 1 (korišten je izbor iz općenitijih familijâ skupovâ).

I zato je velikim iznenađenjem rezultiralo ono što se dogodilo 20ak godinâ kasnije: nađen je dokaz tvrdnje 2 u ZF. Nakon toga su se pojavile još neke ingeniozne eliminacije Aksioma izbora, i danas se njegova uloga u teoriji jednakosastavljivosti može otprilike izreći ovako: potreban je za dokazivanje nepostojanja određenih totalnih invarijantnih mjerâ na euklidskim prostorima, i prilikom "konstrukcije" takvih mjerâ ako postoje, no uglavnom nije potreban za dokazivanje nepostojanja paradoksalnih rastavâ.

Stvar je u tome da je prilikom "konstrukcije" mjere potrebna mnogo veća određenost, i definiranje funkcijâ na "velikim" skupovima bez neke eksplicitne strukture, dok kod opovrgavanja paradoksalnih rastavâ možemo pretpostaviti da takav rastav postoji, osloniti se na neka njegova svojstva, i dobiti kontradikciju "lokalno", bez odlaženja predaleko u skupove koji nas zapravo ne zanimaju.

Aksiom izbora (u onom obliku u kojem ćemo ga mi koristiti, i u kojem se navodi u standardnoj ZFC aksiomatici) glasi:

> *Za svaki kvocijentni skup (skup nepraznih, međusobno disjunktnih skupova) postoji skup reprezentanata (skup kojem je presjek sa svakim elementom početnog skupa jednočlan):*

$$(\forall Q : \emptyset \notin Q \mathbin{\&} \forall^{Q}_{a\neq b}(a\cap b=\emptyset))(\exists r\in\mathcal{P}(\biguplus Q))(\forall a\in Q)(\mathsf{card}(a\cap r)=1).$$

Posljedicâ Aksioma izbora — čak i njemu logički ekvivalentnih tvrdnji — ima vrlo raznolikih: od prihvatljivih i "očitih", poput nepraznosti produkta familije nepraznih skupova, preko čudnih, poput teorema o dobrom uređenju, i teško razumljivih, poput Zornove leme, do krajnje neintuitivnih, poput egzistencije neizmjerivih skupova i paradoksalnih rastavâ. Teoremi kojima se bavimo u ovom radu spadaju u posljednju skupinu.

Opremljeni Aksiomom izbora, krenimo dalje.

F. Hausdorffov teorem

((U ovom odjeljku radimo na S ($P := S$).))

Na S se može definirati relacija ekvivalencije po djelovanju grupe G na standardni način: $\sim_{G.}\colon S$—S; $x \sim_{G.} y :\Leftrightarrow (\exists g\in G)(x=g(y))$. No nama će trebati malo modificirana relacija. Definirajmo $Q := \bigcup_{\alpha}^{G\setminus\{1_S\}} \mathrm{Fix}(\alpha|_S)$ (gdje je $\mathrm{Fix} f := \{x\in \mathrm{Dom} f : f(x)=x\}$ skup fiksnih točaka funkcije f), te $\sim_{G.}$ gledajmo restringiranu samo na $S\setminus Q$ (G djeluje i na $S\setminus Q$) i ubuduće nju (restringiranu relaciju) označimo s $\sim_1$. Također, prirodno proširimo definiciju $\sim_1$ na skupove — za $C_1 \subseteq S \dot{\setminus} Q \supseteq C_2$ definirajmo $C_1 \sim C_2 :\Leftrightarrow (\exists g \in G)(C_1 = g^{\rangle}(C_2))$.

Budući da je $G \leq_{\mathcal{G}r} \textsc{Iso}(S)$, relacija $\sim$ profinjuje ($\subset$) običnu geometrijsku kongruentnost (na $S \dot{\setminus} Q$). Drugim riječima, $C_1 \sim C_2$ povlači da su C_1 i C_2 kongruentni.

Također, budući da su elementi od G kompozicije određenih rotacijâ (φ možemo shvatiti kao rotaciju za π) koje prirodno djeluju na $\mathbb{R}^3$, pripadni linearni operatori (osim $\mathit{1}_{\mathbb{R}^3}$) imaju točno jednu[G] svojstvenu vrijednost iznosa 1 (zbog $\mathsf{det} = 1$ mogu imati jednu ili tri, a tri znače identitetu), pa svaki element od G osim $\mathit{1}_S$ ima točno dvije fiksne točke: $(\forall g \in G \dot{\setminus} \{\mathit{1}_S\})(\mathsf{card}\mathrm{Fix}\, g = 2)$, što povlači da je Q najviše prebrojiv.

Jer je $\sim_1$ relacija ekvivalencije na $S \dot{\setminus} Q$, možemo promatrati kvocijentni skup $(S \dot{\setminus} Q)/_{\sim_1}$ (njegove klase, standardno, zovemo G-orbitama), te na njega primijeniti Aksiom izbora, koji nam daje egzistenciju skupa $M \subset S \dot{\setminus} Q$, koji siječe svaku G-orbitu u točno jednoj točki. Sada možemo definirati $\forall_k^3 (X_k := \biguplus_{\alpha}^{A_k} \alpha^{\rangle}(M))$ (da je unija disjunktna, vidi se direktno iz osnovnog svojstva od M — nikoja dva njegova elementa nisu u relaciji $\sim_1$), te dokazati sljedeću tvrdnju:

Lema 6. *Vrijedi*

$$X_0 \sim X_1 \uplus X_2 \sim X_1 \sim X_2,$$

preciznije, $\varphi^{\rangle}(X_0) = X_1 \uplus X_2$ & $\psi^{\rangle}(X_0) = X_1$ & $\psi^{\langle}(X_0) = X_2$.

Dokaz:

To je zapravo teorem 5, u novom (geometrijskom) ruhu. Radi ilustracije dajemo dokaz da je $\varphi^{\rangle}(X_0) \subseteq X_1 \uplus X_2$. Dakle, uzmimo proizvoljni $t \in X_0$. To znači $(\exists \alpha \in A_0)(\exists m \in M)(t = \alpha(m))$. Tada je, po teoremu 5, $\varphi \circ \alpha \in A_1 \uplus A_2$, pa je $\varphi(t) = (\varphi \circ \alpha)(m) \in (\varphi \circ \alpha)^{\rangle}(M) \subseteq X_1 \uplus X_2$. Iz ovog se vidi kako bi se dokazale sve ostale tvrdnje potrebne za dokaz leme. □

Sva razmatranja u ovom odjeljku mogu se sažeti u ovaj

Teorem 7. *((Hausdorff, 1914.)) Postoji particija jedinične sfere u $\mathbb{R}^3$ u 4 dijela: $S = X_0 \uplus X_1 \uplus X_2 \uplus Q$, pri čemu je $\mathsf{card} Q \leq \aleph_0$, a X_0, $X_1 \uplus X_2$, X_1 i X_2 su svi međusobno kongruentni.*

Sad vidimo na što se odnosi riječ "paradoks" iz naslova: do na prebrojiv skup, X_0 je ujedno i polovina i trećina od S. No, S je ipak dvodimenzionalan skup, i tako na neki način zanemariv[H] u $\mathbb{R}^3$. Trebalo bi ideju proširiti na neki skup neprazne unutrašnjosti (a ipak ograničen — npr. U), da bismo dobili nešto što potpuno proturječi intuiciji.

[G] Naravno, računajući kratnost.

[H] Na primjer, Lebesgueova mjera mu je 0.

G. Jednakosastavljivost i svojstva

Na $\mathcal{P}(\mathbb{R}^3)$ definiramo relaciju jednakosastavljivosti, $\approx$, kao zatvorenje od $\sim_{\mathrm{Iso}(\mathbb{R}^3).}$ s obzirom na konačne particije, tj.

$$X \approx Y :\Leftrightarrow (\exists n \in \mathbb{N})(\exists \{X_i\}_i^n \cup \{Y_i\}_i^n \in \mathcal{P}(\mathcal{P}(\mathbb{R}^3)))\cdot$$

$$\cdot(X = \biguplus_i^n X_i \;\&\; Y = \biguplus_i^n Y_i \;\&\; \forall_i^n (X_i \sim_{\mathrm{Iso}(\mathbb{R}^3).} Y_i)).$$

Uz "pravu", geometrijsku jednakosastavljivost (onu koja pazi na "ljepotu" od X_{ii}^n i Y_{ii}^n, i koja zanemaruje skupove niže dimenzije[I]) vezani su mnogi zanimljivi problemi i neintuitivne tvrdnje koje, iako nemaju direktne veze s Banach–Tarskijevim teoremom, dobro pokazuju kako princip "izreži, pomakni, eventualno zrcali i zalijepi", kad se strogo matematički objasni, postaje nešto poprilično složenije. Jedan od takvih problema je i geometrijska jednakosastavljivost kocke brida 1 i pravilnog tetraedra[J] brida $\sqrt{2}\sqrt[3]{3}$, na kojeg je i Hilbert potrošio mnogo vremena. No, nas će uglavnom zanimati samo gore definirana, "skupovna" jednakosastavljivost. Vidjet ćemo da će nas i to, zajedno s Hausdorffovim teoremom, dovesti do zanimljivih rezultatâ.

Naravno, najčešće izometrije koje ćemo uzimati za uspostavljanje jednakosastavljivosti bit će upravo elementi iz G (shvaćeni kao da djeluju na cijeli $\mathbb{R}^3$).

Prvo dokažimo nekoliko tehničkih stvarî o relaciji $\approx$.

Lema 8. *Vrijede sljedeće tvrdnje:*

(1) *$\approx$ je relacija ekvivalencije na $\mathcal{P}(\mathbb{R}^3)$.*
(2) *Ako je $n \in \mathbb{N}$, te X_{ii}^n, kao i Y_{ii}^n, međusobno disjunktni podskupovi od $\mathbb{R}^3$, u parovima G-jednakosastavljivi (tj. $\forall_i^n (X_i \approx Y_i)$), tada je i $\biguplus_i^n X_i$ G-jednakosastavljiv s $\biguplus_i^n Y_i$.*
(3) *((o sendviču)) Ako je $Z \subseteq Y \subseteq X \subseteq \mathbb{R}^3$ i $X \approx Z$, tada je i $Y \approx X$.*

Dokaz:

((1 – Refleksivnost i simetričnost)) To su direktne posljedice refleksivnosti i simetričnosti relacije $\sim_{\mathrm{Iso}(\mathbb{R}^3).}$.

[I] To je nužno npr. u elementarnoj geometriji, jer tamo gotovo uvijek kad dijelimo neki lik ili tijelo na dva dijela, to činimo duž neke granice, za koju ne specificiramo pripada li prvom ili drugom dijelu - zapravo, najčešće uzimamo da pripada oboma. Tako npr. kad podijelimo kvadrat dijagonalom na dva (pravokutna) trokuta, htjeli bismo da oba imaju hipotenuzu, iako tada, strogo govoreći, to više nije particija kvadrata. Nama takva razmišljanja neće biti potrebna, jer će dijelovi u rastavu biti toliko neintuitivno definirani da nam pozivanje na zor i tako ne bi pomoglo.

[J] Naravno, to je 3. Hilbertov problem, kojeg je riješio Dehn, 1900. Detalji se mogu potražiti u knjizi D. Veljana "Elementarna matematika II", kao i u M. Aigner & G. M. Ziegler, Proofs from The Book, 7.

⦅1 – Tranzitivnost⦆ Neka je $A \approx X \approx B$. To znači da se A može napisati u obliku $\biguplus_i^n A_i$, B kao $\biguplus_j^m B_j$, a $X = \biguplus_i^n C_i = \biguplus_j^m D_j$, za neke prirodne (ili 0) m i n, tako da vrijedi $\forall_i^n(A_i \sim_{\mathrm{Iso}(\mathbb{R}^3).} C_i)$ & $\forall_j^m(D_j \sim_{\mathrm{Iso}(\mathbb{R}^3).} B_j)$. To znači da postoje $\alpha_i{}_i^n$ i $\beta_j{}_j^m$ iz $\mathrm{Iso}(\mathbb{R}^3)$, takvi da je $\forall_i^n(\alpha_i{}^{\rangle}(A_i) = C_i)$ & $\forall_j^m(\beta_j{}^{\rangle}(D_j) = B_j)$. Ako sada definiramo

$$\forall_i^n\forall_j^m(E_{ij} := C_i \cap D_j \;\&\; F_{ij} := \alpha_i{}^{\langle}(E_{ij}) \;\&\; H_{ij} := \beta_j{}^{\rangle}(E_{ij}) \;\&$$
$$\& \; \gamma_{ij} := \beta_j \circ \alpha_i \in \mathrm{Iso}(\mathbb{R}^3)),$$

vidi se da su $F_{ij}{}_{ij}^{nm}$, kao i $H_{ij}{}_{ij}^{nm}$, svi međusobno disjunktni, te da vrijedi

$$\biguplus_{ij}^{nm} F_{ij} = \biguplus_i^n \biguplus_j^m F_{ij} = \biguplus_i^n \biguplus_j^m \alpha_i{}^{\langle}(E_{ij}) = \biguplus_i^n \alpha_i{}^{\langle}(\biguplus_j^m E_{ij}) =$$
$$= \biguplus_i^n \alpha_i{}^{\langle}(\biguplus_j^m (C_i \cap D_j)) = \biguplus_i^n \alpha_i{}^{\langle}(C_i \cap \biguplus_j^m D_j) = \biguplus_i^n \alpha_i{}^{\langle}(C_i \cap X) =$$
$$= \biguplus_i^n \alpha_i{}^{\langle}(C_i) = \biguplus_i^n \alpha_i{}^{\langle}(\alpha_i{}^{\rangle}(A_i)) = \biguplus_i^n A_i = A,$$

i analogno[K]

$$\biguplus_{ij}^{nm} H_{ij} = B.$$

Osim toga, jer su svi $\gamma_{ij}{}_{ij}^{nm}$ izometrije, a

$$\forall_i^n\forall_j^m(\gamma_{ij}{}^{\rangle}(F_{ij}) = (\beta_j \circ \alpha_i)^{\rangle}(\underbrace{F_{ij}}_{=\alpha_i{}^{\langle}(E_{ij})}) = \beta_j{}^{\rangle}(\alpha_i{}^{\rangle}(\alpha_i{}^{\langle}(E_{ij}))) = \beta_j{}^{\rangle}(E_{ij}) = H_{ij}),$$

vidimo da je $\forall_i^n\forall_j^m(F_{ij} \sim_{\mathrm{Iso}(\mathbb{R}^3).} H_{ij})$. No to znači da je i $A \approx B$.

⦅2⦆ To je direktna posljedica tvrdnje da je $\approx$ zatvorenje relacije $\sim_{\mathrm{Iso}(\mathbb{R}^3).}$ s obzirom na konačne particije (kad se ponovo zatvori, ne dobije se ništa novo), no trebalo bi dokazati da ta tvrdnja slijedi iz definicije od $\approx$.
Dakle, neka su za neki $n \in \mathbb{N}$ dani međusobno disjunktni skupovi $X_i{}_i^n$, te $Y_i{}_i^n$, takvi da vrijedi $\forall_i^n(X_i \approx Y_i)$. To znači da se ti skupovi mogu zapisati kao

$$\forall_i^n(X_i = \biguplus_j^{m_i} A_{ij} \;\&\; Y_i = \biguplus_j^{m_i} B_{ij};\; \forall_j^{m_i}(A_{ij} \sim_{\mathrm{Iso}(\mathbb{R}^3).} B_{ij})).$$

No, uzevši u obzir da je tada $\biguplus_i^n X_i = \biguplus_{ij}^{nm_i} A_{ij}$ & $\biguplus_i^n Y_i = \biguplus_{ij}^{nm_i} B_{ij}$, to direktno daje $\biguplus_i^n X_i \approx \biguplus_i^n Y_i$.

⦅3⦆ Tvrdnja nalikuje na Cantor–Schröder–Bernsteinovu lemu (antisimetričnost standardnog uređaja na kardinalima), a i dokaz je sličan. $X \approx Z$ povlači da postoji f, po dijelovima izometrija od $\mathbb{R}^3$, bijekcija skupova X i Z (lako se vidi da je to alternativna definicija jednakosastavljivosti: ako je $X = \biguplus_i^n X_i$ & $Z = \biguplus_i^n Z_i$ & $\forall_i^n(Z_i = f_i{}^{\rangle}(X_i);\; f_i \in \mathrm{Iso}(\mathbb{R}^3))$, stavimo $f := \biguplus_i^n(f_i|_{X_i})$). Definirajmo $\forall_i^{\mathbb{N}}(W_i := f_\circ^{i\rangle}(X \setminus Y))$. Dokažimo da su svi

[K] Stvar nije simetrična s obzirom na zamjenu $\alpha \leftrightarrow \beta$, ali jest s obzirom na $\alpha \leftrightarrow \beta_\circ^{-1}$ ($\beta_j{}_j^m$ su, kao i sve izometrije od $\mathbb{R}^3$, bijekcije).

$W_{i\,i}^{\mathbb{N}}$ u parovima disjunktni. Neka su i i j prirodni brojevi (ili 0), različiti. BSOMP da je $i < j$. Tada je $j - i - 1 \in \mathbb{N}$, pa je

$$W_i \cap W_j = f_\circ^{i\rangle}(X \setminus Y) \cap f_\circ^{i\rangle}(X \setminus Y) =$$

$$= f_\circ^{i\rangle}((X \setminus Y) \cap \underbrace{f^{\rangle}(f_\circ^{j-i-1\rangle}(X \setminus Y))}_{\subseteq \mathsf{im} f = Z \subseteq Y}) \subseteq f_\circ^{i\rangle}((X \setminus Y) \cap Y) = \emptyset.$$

Sada definirajmo $W := \biguplus_i^{\mathbb{N}} W_i$. Po alternativnoj definiciji vrijedi $W \approx f^{\rangle}(W)$, a vrijedi i

$$f^{\rangle}(W) = f^{\rangle}(\biguplus_i^{\mathbb{N}} W_i) = \biguplus_i^{\mathbb{N}} f^{\rangle}(W_i) = \biguplus_i^{\mathbb{N}} W_{i+1} =$$

$$= \biguplus_i^{\mathbb{N}^*} W_i = W \setminus W_0 = W \setminus (X \setminus Y) = W \cap Y \subseteq W.$$

Očito je $X = W \uplus (X \setminus W)$, a zbog gornjeg je $f^{\rangle}(W)$ disjunktan s $X \setminus W$, te je $f^{\rangle}(W) \uplus (X \setminus W) = (W \setminus (X \setminus Y)) \uplus (X \setminus W) = Y$ (što se npr. lako vidi metodom karakterističnih funkcijâ:

$$\chi_{(W \setminus (X \setminus Y)) \uplus (X \setminus W)} = (\chi_W - (\chi_X - \chi_Y)) + (\chi_X - \chi_W) =$$

$$= \chi_W - \chi_X + \chi_Y + \chi_X - \chi_W = \chi_Y).$$

Sada iz refleksivnosti i (2) slijedi tvrdnja. □

H. Kugla do kugle — kugla?

((U ovom odjeljku radimo na U ($P := U$).))

Očito, pojam jednakosastavljivosti nam je trebao da bismo elegantnije mogli iskazati centralnu tvrdnju ovog rada,

Teorem 9. *((Banach–Tarski)) Jedinična kugla u $\mathbb{R}^3$ može se rastaviti u dva dijela, od kojih je svaki jednakosastavljiv s njom, tj.*

$$(\exists X \in \mathcal{P}(U))(\exists Y \in \mathcal{P}(U))(U = X \uplus Y \;\&\; X \approx U \approx Y).$$

Dokaz:

Ako bolje pogledamo Hausdorffov teorem, vidimo da još treba proširiti paradoksalni rastav na unutrašnjost kugle, te riješiti se skupa Q (i ishodišta, koje će nam se prirodno pojaviti kao poseban slučaj). Idemo redom:

Za $D \subseteq S$, označimo s $\hat{D}$ 0_3-deprojekciju od D u $U \setminus \{0_3\}$ (skup svih točaka iz U čija je projekcija iz 0_3 na S u D, odnosno $(\mathsf{sgn}|_U)^{\langle}(D)$). Koristit ćemo oznake iz Hausdorffovog teorema za dijelove u particiji od S: $S = Q \uplus X_1 \uplus X_2 \uplus X_3$. Dakle, $U = \hat{S} \uplus \{0_3\} = \hat{X}_0 \uplus \hat{X}_1 \uplus \hat{X}_2 \uplus \hat{Q} \uplus \{0_3\}$. Iz $X_0 \sim X_1 \sim X_2 \sim X_1 \uplus X_2$ slijedi $\hat{X}_0 \approx \hat{X}_1 \approx \hat{X}_2 \approx \hat{X}_1 \uplus \hat{X}_2$ ($\hat{X}_{i\,i}^{\,3}$ su također međusobno disjunktni). Iz toga pak po lemi o svojstvima jednakosastavljivosti slijedi $\hat{X}_0 \approx \hat{X}_2 \approx \underbrace{\hat{X}_1}_{\approx \hat{X}_0} \uplus \underbrace{\hat{X}_2}_{\approx \hat{X}_1 \uplus \hat{X}_2} \approx \biguplus_i^3 \hat{X}_i$, što povlači

$$X := \hat{X}_0 \uplus \hat{Q} \uplus \{0_3\} \approx \hat{X}_2 \uplus \hat{Q} \uplus \{0_3\} \approx \biguplus_i^3 \hat{X}_i \uplus \hat{Q} \uplus \{0_3\} = U.$$

Primijetimo da X već imamo, pa za Y nema puno izbora: $Y := U \setminus X = \hat{X}_1 \uplus \hat{X}_2$. Treba još samo dokazati $Y \approx S$. Za to nam treba

Lema 10. *Postoji β, rotacija oko neke osi od U, takva da je $\beta^{\rangle}(Q)$ disjunktan s Q i $\beta \notin G$.*

<u>Dokaz:</u>

Kardinalnim argumentom. Prvo, fiksirajmo os koja ne prolazi kroz nijednu točku od Q (takva postoji jer U ima kontinuum osi, a samo prebrojivo mnogo njih prolazi nekom točkom iz Q). Oko te osi ima kontinuum rotacijâ, dok parova točaka iz Q ima prebrojivo mnogo (a svaki par točaka iz Q eliminira najviše jednu rotaciju), pa postoji još uvijek kontinuum rotacijâ koje Q preslikaju disjunktno s Q. Budući da je G prebrojiva, postoji takva rotacija koja nije u G. □

To što je $\beta^{\rangle}(Q)$ disjunktan s Q zapravo znači $\beta^{\rangle}(Q) \subseteq \biguplus_i^3 X_i$. Jer je $X_2 \approx \biguplus_i^3 X_i$, slijedi da postoji $T \subseteq X_2$ takav da je $T \approx \beta^{\rangle}(Q) \approx Q$ ($T := (f \circ \beta)^{\rangle}(Q)$, gdje je f po dijelovima izometrija koja uspostavlja jednakosastavljivost $\biguplus_i^3 X_i$ i X_2). f i β su bijekcije, pa je $\mathsf{card} T = \mathsf{card} Q = \aleph_0$. X_2 je očito neprebrojiv (kad bi bio prebrojiv, to bi isto bili i X_1 i X_0, pa i S, što je kontradikcija), pa postoji točka $p \in X_2 \setminus T$. To znači da je $T \uplus \{p\} \subset X_2$, pa dakle i $\hat{T} \uplus \{p\} \subset \hat{X}_2$ ($p \notin \hat{T}$ zbog $p \in X_2 \subset S$, a $\hat{T} \cap S = T$).

Naravno, pomoću p se želimo riješiti 0_3, a pomoću T skupa Q. To napravimo ovako: $\hat{X}_0 \approx \hat{X}_1$ (znamo otprije), $\hat{Q} \approx \hat{T}$ (funkcija $(f \circ \beta)|_{\hat{Q}}$) i $\{0_3\} \approx \{p\}$ (jednočlana funkcija $0_3 \mapsto p$) povlače

$$U \approx X = \hat{X}_0 \uplus \hat{Q} \uplus \{0_3\} \approx \hat{X}_1 \uplus \underbrace{\hat{T} \uplus \{p\}}_{\subset \hat{X}_2} \subseteq \hat{X}_1 \uplus \hat{X}_2 = Y \subseteq U,$$

iz čega po sendvič-svojstvu jednakosastavljivosti slijedi $Y \approx U$. □

To je to. Intuitivan ili ne, teorem je dokazan. Pogledajmo kako se to odražava na teoriju mjere.

I. Vrijedi li u ZFC zakon očuvanja volumena?

Promotrimo sljedeće zaključivanje:

> U ima volumen $\frac{4}{3}\pi$. Rastavljen je kao $X \uplus Y$ (čak bez "šavova"), dakle zbroj volumenâ od X i od Y iznosi $\frac{4}{3}\pi$. $X \approx Y$,

pa X i Y imaju jednake volumene — dakle, svaki po $\frac{2}{3}\pi$. No, $X \approx U$, a $\frac{2}{3}\pi \neq \frac{4}{3}\pi$. Kontradikcija.

Gdje je greška? Na prvi pogled, koristili smo samo stvari u koje nismo navikli sumnjati: formulu za volumen kugle (ako pažljivije promotrimo gornje razmišljanje, vidimo da je korištena samo činjenica da je dotični volumen različit od 0), svojstva volumena: 2-aditivnost i invarijantnost na izometrije, te rješavanje (prilično trivijalnih i bez sumnje regularnih) linearnih jednadžbî i 2×2-sustavâ.

Na drugi pogled, koristili smo i činjenicu da skupovi X i Y uopće imaju volumen, iako su definirani, blago rečeno, vrlo čudno. To mora da je pogrešna pretpostavka. Dakle, dokazali smo, metodom kontradikcije, da u $\mathbb{R}^3$ (a množenjem s $[0, 1]$ i izgradnjom ograničenih cilindara i u višim dimenzijama — detaljnije u odjeljku `J`), postoje neizmjerivi skupovi, ako za mjeru zahtijevamo invarijantnost na izometrije. Je li nam zato trebao Aksiom izbora? Ukratko, da. Opća egzistencija neizmjerivih skupova zahtijeva, zapravo *ekvivalentna je* Aksiomu izbora.

Naravno, sve uobičajene "konstrukcije" Vitalijevih, Bernsteinovih i ostalih takvih skupova oslanjaju se na Aksiom izbora. Npr. standardni Vitalijev skup V je skup reprezentanata za kvocijentni skup $[0, 1\rangle/_{\sim_{\mathbb{Q}}}$, gdje je $x \sim_{\mathbb{Q}} y :\Leftrightarrow x - y \in \mathbb{Q}$.

U vezi s izgradnjom Vitalijevog skupa primijetimo još nešto: iako je i taj skup prilično paradoksalan, ipak se u dokazu da je neizmjeriv koristi σ-aditivnost mjere, odnosno, pojavljuje se beskonačno mnogo kopijâ od V. Nitko ne kaže postoji li možda izometrijski (translatorno i centralnosimetrički) invarijantna totalna *konačno aditivna* mjera na $\mathcal{P}(\mathbb{R})$. Zapravo, takva mjera *postoji*, što je (vrlo netrivijalna) posljedica činjenice da je grupa izometrijâ realnog pravca rješiva.

Zahvaljujući Banach–Tarskijevom teoremu, znamo da u $\mathbb{R}^3$ takvo nešto ne postoji. Dakle, vrijedi

Teorem 11. *Za prirodan $n \geq 3$, na $\mathcal{P}(\mathbb{R}^n)$ ne postoji totalna konačno aditivna mjera koja je sačuvana pri izometrijama, te koja U preslikava u pozitivan realan broj.*

<u>*Dokaz:*</u>

S obzirom na gore provedeno zaključivanje, kad bi takva mjera μ postojala, bilo bi

$$\mu(U) = \mu(X \uplus Y) = \mu(X) + \mu(Y) = \mu(U) + \mu(U) = 2\mu(U),$$

što je nemoguće za $\mu(U) \in \mathbb{R}^+$. $\square$

Naravno, ovo se može generalizirati. U odjeljku `K` dana je opća definicija G-paradoksalnosti (definicija 16), za djelovanje grupe G na skup X. Ovdje dajemo na neki način "dualnu" definiciju njoj, sa stanovišta teorije mjere.

Definicija 12. *Neka grupa G djeluje na neki skup X, te neka je $E \subseteq X$. Kažemo da je E G-zanemariv ako ne postoji G-invarijantna (g-invarijantna za svaki $g \in G$) totalna konačno-aditivna mjera na X (s domenom $\mathcal{P}(X)$), koja E preslikava u pozitivan realan broj.*

Dakle, ovdje smo pokazali da je U $\mathrm{Iso}(\mathbb{R}^3)$-zanemariv. Laka generalizacija (uz korištenje definicije 16) pokazuje da općenito vrijedi:

Ako je E G-paradoksalan, tada je E G-zanemariv.

J. Jaka verzija Banach–Tarskijevog teorema

Ovdje ćemo dokazati još nekoliko zanimljivih posljedicâ prethodnih rezultatâ, što će kulminirati "jakim Banach–Tarskijevim teoremom", koji, kao što ćemo vidjeti, potpuno poražava našu intuiciju jednakosastavljivosti. Naime, kugle su ipak vrlo posebni skupovi, i može nam se činiti na prvi pogled da od ostalih skupova nešto možemo spasiti (drugim riječima, da je ono što se događa u Banach–Tarskijevom teoremu više izuzetak nego pravilo). Naravno, to nije točno. Kugla jest dobro poslužila da se na njoj dokaže glavni teorem, no usput smo naučili dovoljno da dokažemo jednakosastavljivost i mnogo općenitijih skupova. Kao i obično, treba nam nekoliko tehničkih stvarî, koje ćemo dokazivati tijekom izlaganja.

Za početak, primijetimo da "konstrukciju" u Banach–Tarskijevom teoremu možemo iterirati: budući da je $X \uplus Y \approx X$, X (a analogno i Y, zbog simetrije tvrdnje Banach–Tarskijevog teorema $X \leftrightarrow Y$) se može rastaviti na dva dijela, $X = XX \uplus XY$, tako da je $XX \approx X \approx U$ & $XY \approx Y \approx U$. Ukupno, dobivamo particiju $U = XX \uplus XY \uplus YX \uplus YY$ od U u 4 s njom jednakosastavljiva dijela. To možemo još jednom učiniti na isti način, pa dobijemo particiju od U u 8 s njom jednakosastavljivih dijelova: XXX do YYY. Da su svi oni jednakosastavljivi s U, vidi se po tranzitivnosti, $T_0T_1T_2 \approx T_0T_1 \approx T_0 \approx U$, za $\{T_i\}_i^3 \subseteq \{X, Y\}$.

Osim toga, primijetimo da su sve sfere istog polumjera međusobno kongruentne (jedna translacija koja preslikava središte jedne u središte druge je dovoljna), dakle i jednakosastavljive. Drugim riječima, našu jediničnu kuglu možemo pomicati po $\mathbb{R}^3$. Štoviše, kugla ne mora biti jedinična — primjenom homotetije sa središtem u ishodištu i koeficijentom r (označimo je s $\hbar_r$) možemo lako dokazati Banach–Tarskijev teorem za kuglu centriranu u 0_3, bilo kojeg polumjera $r \in \mathbb{R}^+$: $\hbar_r^{\rangle}(U) = \hbar_r^{\rangle}(X) \uplus \hbar_r^{\rangle}(Y) \approx \hbar_r^{\rangle}(X) \approx \hbar_r^{\rangle}(Y)$. To nam govori da je bilo kugla polumjera r jednakosastavljiva s (disjunktnom unijom) bilo koje dvije takve kugle (polumjera r). No još uvijek ne možemo prelaziti između različitih polumjerâ — kao što ćemo vidjeti, ne zadugo.

Jedna od posljedicâ sendvič-svojstva jednakosastavljivosti jest i

Lema 13. *"Biti jednakosastavljiv s nekim podskupom od" (označimo tu relaciju s $\approx\!\subseteq$) je parcijalni uređaj na skupu klasâ jednakosastavljivosti (definiran preko reprezentanata), tj. vrijedi refleksivnost, tranzitivnost i $X \approx W \subseteq$*

$Y \approx Z \subseteq X$ povlači $X \approx Y$. ((Primijetimo da vrijedi alternativna definicija slična onoj za jednakosastavljivost, samo se od po dijelovima izometrije između skupova zahtijeva samo da bude injekcija (ne mora biti surjekcija).))

Dokaz:

- Trebamo prvo vidjeti da je dana relacija dobro definirana na klasama pomoću reprezentanata. Ako je $[X]_\approx = [Y]_\approx \precsim [Z]_\approx$, to znači zapravo $X \approx Y \approx W$, za neki $W \subseteq Z$. No to povlači $X \approx W \subseteq Z$, odnosno $[X]_\approx \precsim [Z]_\approx$. S druge strane, ako je $X \approx Y \subseteq Z \approx W$, tada zbog $Z \approx W$ postoji bijekcija $f : Z \longleftrightarrow W$ koja je po dijelovima izometrija. Ako označimo $V := f^{\rangle}(Y)$, vidimo da je $X \approx ((Y \approx))V \subseteq W$, odnosno $[X]_\approx \precsim [W]_\approx$.
- Refleksivnost je očita: $X \approx X \subseteq X$.
- Tranzitivnost: neka je $X \approx W \subseteq Y \approx V \subseteq Z$. Zbog $Y \approx V$ imamo po dijelovima izometriju $f : Y \longleftrightarrow V$. No tada je $X \approx W \approx f^{\rangle}(W) \subseteq \mathsf{im} f = V \subseteq Z$, odnosno $[X]_\approx \precsim [Z]_\approx$.
- Antisimetričnost: Neka je $X \approx W \subseteq Y \approx Z \subseteq X$. To kao i prije znači da postoji po dijelovima izometrija $f : Y \longleftrightarrow Z$. No tada je kao i gore $X \approx f^{\rangle}(W) \subseteq Z \subseteq X$, pa je po sendvič-svojstvu $X \approx Z$, što s $Y \approx Z$ daje $X \approx Y$. □

Dobro. Sada nam treba

Lema 14. *Ako je za neki $m \in \mathbb{N}$ $A = \biguplus_i^m B_i \;\&\; \forall_i^m (A \approx B_i \approx C_i)$, tada je i $A \approx \bigcup_i^m C_i$ (primijetimo da ta unija ne mora biti disjunktna). Dakle, ako za A imamo particiju na s njim jednakosastavljive podskupove, pa od svakog od tih podskupova sastavimo nešto drugo (posebno, kopiju od A), tada će A biti jednakosastavljiv s unijom tako dobivenih skupova (koji se mogu preklapati).*

Dokaz:

Matematičkom indukcijom po m.

- $((m = 0))$ Tada mora biti $A = \biguplus_i^0 B_i = \bigcup_i^0 C_i = \emptyset$, pa tvrdnja vrijedi.
- $((m = 1))$ $A = \biguplus_i^1 B_i = B_1 \approx C_1 = \bigcup_i^1 C_i$, pa tvrdnja također vrijedi.
- $((m = 2))$ Imamo $A = B_0 \uplus B_1 \;\&\; B_0 \approx C_0 \;\&\; B_1 \approx C_1$. Iz $C_1 \setminus C_0 \subseteq C_1 \approx B_1$ slijedi da postoji $D \subseteq B_1$ takav da je $C_1 \setminus C_0 \approx D$. Sada imamo ove relacije:

$$A \approx B_1 \approx C_1 \subseteq C_0 \cup C_1 = \underbrace{C_0}_{\approx B_0} \uplus \underbrace{(C_1 \setminus C_0)}_{\approx D} \approx B_0 \uplus \underbrace{D}_{\subseteq B_1} \subseteq B_0 \uplus B_1 = A,$$

  iz čega po prethodnoj lemi slijedi $A \approx C_0 \cup C_1$.
- $((m = k))$ Pretpostavimo da tvrdnja leme vrijedi za $m = k$, tj. $A = \biguplus_i^k B_i \;\&\; \forall_i^k (A \approx B_i \approx C_i)$ povlači $A \approx \bigcup_i^k C_i$. Naravno, $k \geq 2$, i tvrdnja leme vrijedi i za $m = 2$ (dokazano gore).
- $((m = k + 1))$ Neka je $A = \biguplus_i^{k+1} B_i \;\&\; \forall_i^{k+1} (A \approx B_i \approx C_i)$. Po pretpostavci indukcije je $\biguplus_i^k B_i \approx \bigcup_i^k C_i$, a u uvjetima imamo $B_k \approx C_k$. Sada raspisivanje $A = (\biguplus_i^k B_i) \uplus B_k$ i primjena slučaja $((m = 2))$ daje tvrdnju. □

Sad kad sve to znamo, napravimo sljedeće: kuglu polumjera $r := \frac{2}{\sqrt{3}}$, sa središtem u ishodištu, stavimo u kocku stranice $2r$ ($U_1 := \hbar_r^{\rangle}(U) \subseteq [-r,r]^3_\times$). Tu kocku podijelimo na 8 jednakih kocaka stranice r (ovaj put nas nije briga za granice duž kojih se te kocke dodiruju), oblika $\times_i^3 I_i$, za $\{I_i\}_i^3 \subseteq \{[-r,0],[0,r]\}$. Svakoj od tih kocaka *opišimo* po sferu. Budući da su prostorne dijagonale tih kocaka dugačke po $\sqrt{3}r = 2$, time dobivamo osam kugala polumjerâ 1, čija je unija "jastučasto" tijelo koje nazovimo J. Jer je svaka od malih kocaka sadržana u "svojoj" kugli, velika kocka (a time i U) je sadržana u J. Sada se sjetimo triplicirane primjene Banach–Tarskijevog teorema s početka ovog odjeljka, gdje smo dobili skupove XXX do YYY. Ako ih označimo s $B_i{}_i^8$, a kugle opisane našim kockicama označimo s $C_i{}_i^8$, pa to uvrstimo u lemu 14, dobit ćemo $U \approx J$. S druge strane, jer je $r > 1$, očito je $U \subset U_1$. Ukupno imamo $U \subseteq U_1 \subseteq J \approx U$, što po sendvič-svojstvu povlači $U \approx U_1$.

Nema razloga da se zaustavimo na U_1. Definirajmo $\forall_k^{\mathbb{Z}}(U_k := \hbar_{r^k}^{\rangle}(U))$. Sada se lako vidi da su sve kugle $U_k{}_k^{\mathbb{Z}}$ međusobno jednakosastavljive — svaka od njih je jednakosastavljiva s $U = U_0$, što za pozitivne k ide indukcijom i tranzitivnošću, a za negativne također, krenuvši na obrnut način (jediničnu kuglu ubacimo u uniju 8 kugala polumjera $\frac{1}{r} = \frac{\sqrt{3}}{2}$).

Također, jer je $r > 1$, vrijedi $\mathsf{lim}_k\, r^k = +\infty$ & $\mathsf{lim}_k\, r^{-k} = 0$. To povlači da za svaki $s \in \mathbb{R}^+$ postoje cijeli brojevi $k_i{}_i^2$, takvi da je $r^{k_0} \leq s \leq r^{k_1}$, odnosno, $U_{k_0} \subseteq \{x \in \mathbb{R}^3 : \|x\| \leq s\} \subseteq U_{k_1}$. Kao što smo vidjeli, $U_{k_0} \approx U_{k_1}$, što po sendvič-svojstvu daje $\{x \in \mathbb{R}^3 : \|x\| \leq s\} \approx U_{k_1} \approx U$: svaka kugla (sa središtem u ishodištu, ali pokazali smo da je možemo i pomicati) jednakosastavljiva je s U. Direktna posljedica toga i tranzitivnosti jednakosastavljivosti je činjenica da su svake dvije kugle u $\mathbb{R}^3$ jednakosastavljive.

Sad nas još samo malo dijeli do konačnog rezultata. *Pun* skup (u $\mathbb{R}^n$) definirajmo kao skup kojem je interior neprazan.

Teorem 15. *((Banach–Tarskijev teorem, jaka verzija)) Neka je $n \geq 3$ prirodan broj, i neka su A i B puni i ograničeni skupovi u $\mathbb{R}^n$. Tada je $A \approx B$ (uz prirodno proširenje od $\approx$ na više dimenzije).*

<u>*Dokaz:*</u>

Matematičkom indukcijom po n.

- $((n = 3))$[L] Neka su A i B dva puna, ograničena podskupa od $\mathbb{R}^3$. Da je A pun, znači da postoji točka $a \in \mathrm{INT}A$. $\mathrm{INT}A$ je po definiciji otvoren, pa oko a postoji kugla K_A koja je sadržana u $\mathrm{INT}A \subseteq A$. Da je B ograničen pak znači da se B može smjestiti u neku kuglu L_B. Naravno, po prethodno dokazanom, $K_A \approx L_B$. Sada iz $B \subseteq L_B \approx K_A \subseteq A$ slijedi po lemi 13 $[B]_\approx \approx\!\subseteq [A]_\approx$. Analogno (zamjenom

[L]Naravno, ovaj slučaj je najzanimljiviji za "interpretaciju u stvarnom svijetu", jer je ovaj dio Svemira po njegovim "geometrijskim" svojstvima najbliži euklidskom prostoru $\mathbb{R}^3$.

$A \leftrightarrow B$) dobijemo $[A]_{\approx} \approx\subseteq [B]_{\approx}$, što s prethodnim opet po lemi 13 daje $A \approx B$.

- $((n = k))$ Pretpostavimo da su svaka dva puna, ograničena podskupa od $\mathbb{R}^k$ jednakosastavljiva. Specijalno, paralelepipedne okoline (otvoreni paralelotopi kojima su bridovi paralelni koordinatnim osima) su takve, pa to i za njih vrijedi.
- $((n = k+1))$ Iz pretpostavke indukcije direktno Kartezijevim množenjem s proizvoljnim segmentom (i proširujući naše po dijelovima izometrije tako da novu dimenziju ostavljaju na miru) i translacijama duž nove koordinatne osi dobivamo da su paralelepipedne okoline s jednakom posljednjom dimenzijom ("visinom", ako smjer nove koordinatne osi nazovemo "gore") jednakosastavljive. Rotacijom možemo postići da to ne bude visina, već bilo koja od preostalih dimenzijâ (imamo ih dovoljno) — nazovimo je "širinom". Sad uzmimo dvije bilo kakve $(k+1)$-dimenzionalne paralelepipedne okoline P_0 i P_1. Ako su im širine jednake, vidjeli smo da su jednakosastavljive. Ako nisu, jedna je šira od druge, pa BSOMP da je P_0 šira od P_1. S jedne strane time imamo da je P_1 jednakosastavljiva s podskupom od P_0 (paralelepipedne okoline u P_0 koja sve dimenzije ima kao P_0, osim širine, koju ima kao P_1). S druge strane, po "Arhimedovom aksiomu" možemo naslagati u smjeru širine konačno mnogo kopijâ od P_1, čija je unija (nazovimo je P_2) takva da je P_0 jednakosastavljiva s nekim njenim podskupom. Jer je $\mathsf{lim}_k\, 2^k = +\infty$, BSOMP da je broj kopijâ od P_1 u P_2 oblika 2^k. Sada k-strukom primjenom analogne "konstrukcije" kao u početku ovog odjeljka (tamo smo je učinili 3 puta), te primjenom leme 14 dobivamo $P_1 \approx P_2$, što nam s prethodnim daje $P_0 \approx P_1$. To nam je dovoljno za nastaviti indukciju.
- Sada imamo jednakosastavljivost paralelepipednih okolinâ u svakom euklidskom prostoru dimenzije ≥ 3. Budući da se u svaku paralelepipednu okolinu može smjestiti kugla i obrnuto, imamo i jednakosastavljivost kugala iste dimenzije. To znači da možemo dokazati bilo koji slučaj $n > 3$ kao slučaj $n = 3$ (jer nam je trebala samo jednakosastavljivost kugala). $\square$

K. Općenitije o paradoksalnim rastavima

U ovom odjeljku pogledat ćemo neke apstraktnije rezultate teorije jednakosastavljivosti, koji će nam omogućiti da u sljedećem odjeljku dokažemo Hausdorffov teorem "egzaktno", bez suvišnih tehničkih detaljâ poput onih u dokazu leme 4.

Pristup će se zasnivati na činjenici da je, za paradoksalni rastav kakav nama treba, u našoj situaciji (dovoljno malo fiksnih točaka djelovanja) dovoljna činjenica da grupa preslikavanjâ koja su nam na raspolaganju (u ovom slučaju npr. SO_3, shvaćena kao grupa rotacijâ od P) ima slobodnu podgrupu ranga 2 (dakle, dva nezavisna elementa beskonačnog reda).

Kad jednom imamo slobodnu podgrupu ranga 2 (tj. imamo $\mathbb{Z}_\star^2$ uloženu u našu grupu), do paradoksalnog rastava je (u principu) lako doći, na jedan opći način, kojeg ćemo sada prikazati. Za to nam treba generalnija definicija paradoksalnog rastava.

Definicija 16. *Neka grupa G djeluje na neki skup X, te neka je $E \subseteq X$. Kažemo da je E G-paradoksalan ako postoje prirodni brojevi m i n, te međusobno disjunktni (svaka 2 od njih) podskupovi ${A_i}_i^n, {B_j}_j^m$ od E i elementi ${g_i}_i^n, {h_j}_j^m$ od G, takvi da vrijedi $E = \bigcup_i^n g_i^\rangle(A_i) = \bigcup_j^m h_j^\rangle(B_j)$.*

Ako je G grupa, G djeluje na samu sebe npr. lijevim množenjem, pa možemo u definiciji postaviti u specijalnom slučaju $E := X := G$, tj. prirodno se zapitati kada je G G-paradoksalna. Takve grupe zvat ćemo samoparadoksalnima. Pronalaženje nužnih i dovoljnih uvjeta na strukturu grupe da bi ona bila samoparadoksalna je vrlo težak problem, no nas će zanimati (uz neke jednostavne posljedice) samo sljedeći

Teorem 17. *Grupa $\mathbb{Z}_\star^2$ je samoparadoksalna.*

Dokaz:

Označimo s 1_1 i 1_2 (nezavisne) generatore od $\mathbb{Z}_\star^2$. Također, za riječ $v \in \mathbb{Z}_\star^2$, označimo s $B(v)$ skup svih riječi iz $\mathbb{Z}_\star^2$ koje počinju s v. Npr. kako svaka netrivijalna riječ u $\mathbb{Z}_\star^2$ počinje s 1_1, -1_1, 1_2 ili (ekskluzivno) -1_2, vrijedi $\mathbb{Z}_\star^2 = \{1\} \uplus B(1_1) \uplus B(-1_1) \uplus B(1_2) \uplus B(-1_2)$. Također, ako riječ $w \in \mathbb{Z}_\star^2$ ne počinje s 1_1, tada je $(-1_1)w$ (reducirana riječ) iz $B(-1_1)$, pa je $w = 1_1(-1_1)w \in 1_1B(-1_1)$. Dakle, $\mathbb{Z}_\star^2 \setminus B(1_1) \subseteq 1_1B(-1_1)$ (i analogno za 1_2), odnosno

$$\mathbb{Z}_\star^2 = B(1_1) \cup 1_1B(-1_1) = B(1_2) \cup 1_2B(-1_2),$$

što je upravo po definiciji paradoksalni rastav. $\square$

Sada pogledajmo jedan jednostavan slučaj kada se samoparadoksalnost grupe može prebaciti na skup na koji ona djeluje. ((Dok nam za prethodni dokaz nije trebao Aksiom izbora, njegovo korištenje se općenito ne može izbjeći u sljedećem slučaju.))

Lema 18. *Ako samoparadoksalna grupa G nefiksno (netrivijalni elementi od G nemaju fiksnih točaka) djeluje na X, tada je i X G-paradoksalan. Specijalno, svaka grupa H sa slobodnom podgrupom ranga 2 je samoparadoksalna.*

Dokaz:

Dokaz prve tvrdnje je sličan onome što smo napravili prilikom dokaza Hausdorffovog teorema (zapravo još lakši, jer se ne moramo brinuti o fiksnim točkama). Dakle, uzmimo po jednu točku iz svake G-orbite. Po Aksiomu izbora, to možemo učiniti tako da one tvore skup, nazovimo ga M. Sada je glavno dokazati da je $\mathcal{M} = \{g^\rangle(M)\}_g^G$ particija od X. Uzmimo bilo koju točku x od X. Njena G-orbita ima jedinstvenog predstavnika u M, neka je to m. Budući da su x i m u istoj G-orbiti, postoji $g \in G$ takav da je $x = g(m) \in g^\rangle(M)$, pa je $\mathcal{M}$ pokrivač za X. Sada pretpostavimo da se neki

$m \in X$ nalazi i u $g^{\rangle}(M)$ i u $h^{\rangle}(M)$, gdje su g i h dva različita elementa od G. Dakle, $m = g(m_1) = h(m_2)$, gdje su m_1i m_2 iz M, iz čega dobivamo $m_1 = (g^{-1}h)(m_2)$, pa su m_1 i m_2 u istoj G-orbiti. Budući da M ima samo po jednu točku iz svake G-orbite, to je moguće jedino tako da su m_1 i m_2 jedan te isti element, no tada je on fiksna točka od $g^{-1}h$ (uz $g^{-1}h \neq 1$ zbog $g \neq h$), što je kontradikcija s nefiksnim djelovanjem G na X. Dakle, $\mathcal{M}$ je zaista particija od X.

Budući da je G paradoksalna, postoje prirodni brojevi m i n, u parovima disjunktni podskupovi ${A_i}_i^m$, ${B_j}_j^n$, te elementi ${g_i}_i^m$ i ${h_j}_j^n$ od G, takvi da je $G = \bigcup_i^m g_i A_i = \bigcup_j^n h_j B_j$. To zajedno s činjenicom da je $\mathcal{M}$ particija od X daje da su s $\forall_i^m (A_i^* := \biguplus_g^{A_i} g^{\rangle}(M))$ & $\forall_j^n (B_j^* := \biguplus_g^{B_j} g^{\rangle}(M))$ dani u parovima disjunktni podskupovi od X koji, pomoću ${g_i}_i^m$ i ${h_j}_j^n$, tvore paradoksalni rastav od X.

Za dokaz druge tvrdnje, neka je H grupa i G (neka) njena slobodna podgrupa ranga 2. G je dakle izomorfna sa $\mathbb{Z}_\star^2$, pa je samoparadoksalna, a kako G očito nefiksno djeluje na H (jer u grupi možemo kratiti), slijedi da je H G-paradoksalna, pa i samoparadoksalna. $\square$

Dakle, opći dokaz teoremâ Banach–Tarskijevog tipa je sljedeći: prvo u nekoj grupi G (koja predstavlja ono što imamo na raspolaganju od preslikavanjâ, npr. izometrije) pronađemo dva nezavisna elementa beskonačnog reda (dakle, slobodnu podgrupu $H \leq_{\mathcal{G}r} G$ ranga 2). Tako dobivamo samoparadoksalnost od H. Nakon toga pronađemo način da G djeluje na X, po mogućnosti nefiksno, a ako to nije moguće postići, sa što manje (netrivijalnih) fiksnih točaka[M] (u našem slučaju prebrojivo mnogo je bilo dovoljno malo). Tako dobivamo H-paradoksalnost od $X \setminus Q$, gdje je Q skup netrivijalnih fiksnih točaka djelovanja G na X. Tada još treba eliminirati elemente od Q, za što postoje razni trikovi, no naš slučaj (lema 10) može dobro poslužiti kao univerzalna metoda u slučaju prebrojivog Q, ako imamo kontinuum (ili više) preslikavanjâ na raspolaganju.

L. Alternativni dokaz Hausdorffovog teorema

U odjeljku F dokazan je Hausdorffov teorem, koristeći dvije rotacije od P. Dokaz se oslanjao na činjenicu da su te dvije rotacije nezavisne, što znači da nijedna njihova netrivijalna kompozicija nije identiteta na P (odnosno, da je njima zaista razapet slobodni produkt (izomorfan s) $2 \star 3$). Za dokaz toga bila je bitna lema 4, čija je tvrdnja bila da se to može postići samo biranjem odgovarajućeg kuta između osî tih rotacijâ. U njenom dokazu, međutim, postoji jedan detalj kojeg nisam znao dokazati ni na koji drugi način osim "grube sile", a i to dosta dugačko i s mnogo slučajeva koje treba provjeriti, te dokaz nije ovdje naveden.

[M]Često se u takvim prilikama gledaju lokalno komutativna djelovanja — djelovanja grupâ koja imaju svojstvo da svaka dva elementa koja imaju zajedničku fiksnu točku, komutiraju. Naravno, to je trivijalno ispunjeno kod nefiksnog djelovanja, kao i kod djelovanja komutativnih grupâ.

No, u prošlom odjeljku vidjeli smo da je dovoljno u grupi $\mathcal{SO}_3$ naći slobodnu podgrupu ranga 2. Prvo pokažimo (više kao napomenu), *koristeći* rezultate iz odjeljka `F`, da je to zaista općenitiji rezultat, tj. da se slobodna podgrupa ranga 2 nalazi već u G (reprezentaciji od $2 \star 3$ u $\mathrm{Iso}(P)$):

Lema 19. *Riječi $a := \psi\varphi\psi$ i $b := \varphi\psi\varphi\psi\varphi$ generiraju slobodnu podgrupu od G, ranga 2.*

<u>*Dokaz:*</u>

Lako je dokazati (matematičkom indukcijom) da je, za sve prirodne n, $a^n = \psi(\varphi\psi^{-1})^{n-1}\varphi\psi$, $a^{-n} = \psi^{-1}(\varphi\psi)^{n-1}\varphi\psi^{-1}$, te $b^n = \varphi a^n \varphi$ i $b^{-n} = \varphi a^{-n}\varphi$. Iz toga se vidi da, za svaki $n \in \mathbb{Z}^*$, a^n počinje i završava s ψ ili s ψ^{-1}, a b^n počinje i završava s φ. Budući da se svaka netrivijalna riječ u $\langle\{a, b\}\rangle_{\mathcal{G}r}$ može zapisati kao produkt gornjih riječi (s bar jednim faktorom), te da se kombinacije $\varphi\psi$, $\varphi\psi^{-1}$, $\psi\varphi$ i $\psi^{-1}\varphi$ ne reduciraju, tvrdnja je dokazana. $\square$

Sada vidimo da nam je, za dokaz Hausdorffovog teorema, dovoljno naći dva nezavisna elementa u $\mathcal{SO}_3$, beskonačnog reda. (Q će i dalje biti prebrojiv, jer je slobodna grupa ranga 2 prebrojiva, a svaka rotacija oko neke osi od S ima samo dvije fiksne točke na S.) Na taj način smo izbjegli lemu 4, i dobili mogućnost izbora "spretnijih" rotacijâ od naših φ i ψ s početka. To nam daje

Lema 20. *Neka su ϕ i ρ rotacije oko z- i x-osi, tim redom, za kut $-\mathsf{arccos}\,\frac{1}{3}$ ($\mathsf{arccos}\,\frac{1}{3}$ u negativnom smjeru). Tada su ϕ i ρ nezavisni generatori slobodne podgrupe od $\mathcal{SO}_3$.*

<u>*Dokaz:*</u>

Matrične reprezentacije od $\phi^{\pm 1}$ i $\rho^{\pm 1}$ dane su s

$$\phi^{\pm 1} \cong \begin{bmatrix} \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{bmatrix} \ \& \ \rho^{\pm 1} \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{bmatrix}.$$

Pretpostavimo da neka netrivijalna riječ w nad $\{\phi, \phi^{-1}, \rho, \rho^{-1}\}$ predstavlja identitetu u $\mathcal{SO}_3$. Dokažimo da se, za svaki netrivijalan w, shvaćen kao element od $\mathcal{SO}_3$, we_1 (prvi stupac matrične reprezentacije od w) može napisati u obliku $\frac{(a,b\sqrt{2},c)}{3^k}$, gdje je $\{a, b, c, k\} \subset \mathbb{Z}$ & $3\nmid b$. Specijalno, $we_1 \neq e_1$ (jer bi inače bilo $b = 0$, što je djeljivo s 3), pa je to kontradikcija s pretpostavkom da w djeluje kao identiteta.

Dokaz tvrdnje o netrivijalnom prvom stupcu je matematičkom indukcijom po duljini od (reducirane riječi) w. Prije toga još primijetimo da je tvrdnja, kao i pretpostavke, simetrična s obzirom na zamjenu $a \leftrightarrow c$ (općenito, obrtanje koordinatâ vektora), te $\phi \leftrightarrow \rho$. Dakle, BSOMP da je prvo slovo u w $\phi^{\pm 1}$. Baza je (uz gornju pretpostavku) $w = \phi^{\pm 1}$, pa je $(a_0, b_0, c_0, k_0) = (1, -2, 0, 1)$, te je tvrdnja ispunjena. Za korak je, za dokaz da su parametri cijeli brojevi, dovoljno vidjeti da je

$$\phi^{\pm 1}\big(\frac{(a, b\sqrt{2}, c)}{3^k}\big) = \frac{(\pm a \pm 4b, (\mp 2a \pm b)\sqrt{2}, 3c)}{3^{k+1}}.$$

Za dokaz da b nije djeljivo s 3 imamo dva slučaja, ovisno o drugom slovu u w (w sad ima duljinu bar 2). Ako je to $\phi^{\pm 1}$, vidimo da ono mora biti jednako prvom slovu u w (ne smije biti njegov inverz jer tada w ne bi bila reducirana), pa w ima oblik $w = \phi^{\pm 2}v$, gdje je v neka riječ (može biti i trivijalna). Ako sad označimo $u := \phi^{\pm 1}v$ (s istim predznakom eksponenta, dakle w bez prvog slova), te s b_1, b_2 i b_3 označimo pripadne b iz zapisa djelovanja w, u i v na $e_1 = (1, 0, 0)$, tim redom (b_3 može biti i 0, ako je $v = 1$, ali po pretpostavci indukcije znamo da $3 \nmid b_2$), imamo $b_1 = 2b_2 - 9b_3$, odnosno $b_1 \equiv 2b_2$ $(\cdot 3)$, iz čega zbog $\mathtt{gcd}(2, 3) = 1$ po pretpostavci indukcije slijedi tvrdnja. Ako je pak drugo slovo u w jednako $\rho^{\pm 1}$, tada je, uz oznake analogne onima gore, $b_1 = \pm 3c_3 \pm 4b_2$ (c_3 je c iz zapisa od ve_1, gdje je v "rep" od w od trećeg slova dalje — može biti i trivijalan), odnosno $b_1 \equiv \pm 4b_2 \equiv \pm b_2$ $(\cdot 3)$, iz čega zbog $\mathtt{gcd}(\pm 4, 3) = 1$ opet slijedi tvrdnja (b_1 je djeljiv s 3 akko je b_2 takav, što znamo da nije po pretpostavci indukcije). □

M. Izmjerive grupe

Dosad smo se uglavnom bavili "pozitivnim" rezultatima iz perspektive paradoksalnih rastavâ, odnosno teoremima koji su davali njihovu egzistenciju. Kao što je pokazano u odjeljku `I`, ti rezultati su negativni iz perspektive određenih invarijantnih (konačno-aditivnih) mjerâ, odnosno, znače da one, u situacijama koje smo razmatrali, ne postoje. Preciznije, vidjeli smo da, ako grupa G djeluje na skup X, tada (uz $E := X$) tvrdnja "X je G-paradoksalan" povlači tvrdnju "X je G-zanemariv". Mogli bismo se zapitati vrijedi li obrat toga, odnosno: jesu li paradoksalni rastavi jedini razlog za nepostojanje G-invarijantne totalne netrivijalne konačno-aditivne mjere na X? Pokazuje se da je odgovor potvrdan, no do toga je prilično netrivijalno doći (Tarskijev teorem). Nama to neće biti cilj, već ćemo se koncentrirati na to da pokažemo kako se mogu provesti razmatranja slična onima u odjeljku `K`, na dualnoj razini. Prisjetimo se, tamo smo imali samoparadoksalne grupe ($\mathbb{Z}_\star^2$ je bila prototip), te smo u određenim slučajevima (nefiksno djelovanje, npr.) mogli prenijeti tu paradoksalnost s grupe na skup na koji ona djeluje. Ovdje ćemo slično imati *izmjerive* grupe, koje će moći prenositi odgovarajuće na njima definirane mjere na skupove na koje djeluju. Prvo precizno definirajmo pojmove:

Definicija 21. *Neka je G grupa. Konačno aditivno preslikavanje*

$$\mu : \mathcal{P}(G) \to [0, 1],$$

takvo da vrijedi

(1) $\mu(G) = 1$ *((normiranost)), i*
(2) $(\forall g \in G)(\forall A \in \mathcal{P}(G))(\mu(gA) = \mu(A))$ *((lijeva invarijantnost))*

zovemo grupna mjera. *Grupu na kojoj postoji grupna mjera zovemo* izmjeriva grupa.

Prvo pokažimo da se izmjerivost može preko (bilo kakvog) djelovanja prenijeti s grupe na skup, u smislu da tada taj skup nije G-zanemariv.

Teorem 22. *Neka izmjeriva grupa G djeluje na skup X. Tada postoji konačno aditivna mjera na X, koja je G-invarijantna, totalna i normirana. Specijalno, X nije G-zanemariv, pa nije ni G-paradoksalan.*

<u>*Dokaz:*</u>

Neka je μ grupna mjera na G, i odaberimo neki $x \in X$. Definirajmo ν na $\mathcal{P}(X)$ s

$$\nu(A) := \mu(\{g \in G : g(x) \in A\}).$$

Tada:

- ⦅konačna aditivnost⦆ Naravno, dovoljno je provjeriti aditivnost za dva skupa. Dakle, neka su A i B dva disjunktna podskupa od X. To znači da, za svaki $g \in G$, $g(x)$ može biti u najviše jednom od skupova A i B, odnosno da su skupovi $\{g \in G : g(x) \in A\}$ i $\{g \in G : g(x) \in B\}$ disjunktni, iz čega uz konačnu aditivnost funkcije μ slijedi
$$\nu(A \uplus B) = \mu(\{g \in G : g(x) \in A \uplus B\}) =$$
$$= \mu(\{g \in G : g(x) \in A\} \uplus \{g \in G : g(x) \in B\}) =$$
$$= \mu(\{g \in G : g(x) \in A\}) + \mu(\{g \in G : g(x) \in B\}) = \nu(A) + \nu(B).$$
- Totalnost i nenegativnost su trivijalne po definiciji.
- ⦅G-invarijantnost⦆ Neka je $A \subseteq X$ i $h \in G$. Tada je
$$\nu(hA) = \mu(\{g \in G : g(x) \in hA\}) = \mu(\{g \in G : (\exists a \in A)(g(x) = h(a))\}) =$$
$$= \mu(\{g \in G : h^{-1}(g(x)) \in A\}) = \mu(h^{-1}\{g \in G : (h^{-1}g)(x) \in A\}) =$$
$$= \mu(\{f \in G : f(x) \in A\}) = \nu(A).$$
- ⦅normiranost⦆ $\nu(X) = \mu(\{g \in G : g(x) \in X\}) = \mu(G) = 1$. Štoviše, ν daje vrijednost 1 već na G-orbiti od x, dok je izvan tog skupa svuda nula ($\nu(X \mathbin{\dot\setminus} G(x)) = 0$).

Budući da je $\nu(X) = 1 \in \mathbb{R}^+$, vidimo da X nije G-zanemariv, pa, po principu iskazanom na kraju odjeljka `I`, nije ni G-paradoksalan. □

Sada nas zanima koje grupe su izmjerive. Pokazuje se da je klasa izmjerivih grupa dosta široka (npr. sve tzv. *elementarne* grupe[N] su izmjerive), no za neke važne klase grupâ (npr. Abelove) je to teško dokazati. Nas će zanimati svojstva koja se mogu dobiti iz sljedeća dva teorema (lakši ćemo dokazati, a teži ostaviti bez dokaza, jer je težište ovog rada ipak na egzistenciji paradoksalnih rastavâ):

Teorem 23. *Klasa izmjerivih grupâ ima ova svojstva:*

[N]Elementarne grupe su grupe koje se mogu dobiti konačnom primjenom uzimanja podgrupâ, kvocijenata po normalnim podgrupama, de-kvocijenata (ako je H normalna podgrupa od G, te su H i $G/_H$ elementarne, tada je i G elementarna) i direktnih limesâ (unijâ direktnih sustavâ podgrupâ), počevši od Abelovih i konačnih grupâ.

(1) *Sve konačne grupe su izmjerive.*
(2) *Podgrupa izmjerive grupe je izmjeriva.*
(3) *Kvocijentna grupa izmjerive grupe po njenoj normalnoj podgrupi je izmjeriva.*

<u>Dokaz:</u>

⦅(1)⦆ Možemo (zapravo, to je jedini način) iskoristiti Laplaceov model i definirati $\mu(A) := \frac{\mathsf{card} A}{\mathsf{card} G}$. Totalnost, nenegativnost i normiranost su očite, konačna aditivnost slijedi iz konačne aditivnosti funkcije card (što je zapravo definicija zbrajanja kardinalnih brojeva), dok G-invarijantnost slijedi iz činjenice da je množenje s fiksnim elementom grupe zapravo neka permutacija članova grupe, odnosno bijekcija, pa čuva kardinalitet.

⦅(2)⦆ ⦅Zanimljivo je da se u dokazu ove tvrdnje koristi Aksiom izbora, iako se ne radi o proširenju mjere, već naprotiv, o "suženju" na podgrupu.⦆ Neka je μ grupna mjera na G, i $H \leq_{\mathcal{G}r} G$. Promotrimo relaciju ekvivalencije $\sim_{H\cdot}$, definiranu s $x \sim_{H\cdot} y :\Leftrightarrow xy^{-1} \in H$. Naravno, kvocijentni skup je $G/_{H\cdot} = \{Hg\}_g^G$. Neka je M odgovarajući skup reprezentanata, tj. skup za kojeg vrijedi $(\forall g \in G)(\exists! m \in M)(m \in Hg)$. Definirajmo ν na $\mathcal{P}(H)$, s $\nu(A) := \mu(AM)$.

Totalnost i nenegativnost su očite.

Za normiranost, dokažimo prvo da je $HM = G$. Neka je $g \in G$. Tada je $Hg \in G/_{H\cdot}$, pa postoji (jedinstveni) $m \in M$ takav da je $m \in Hg$, odnosno, $h := mg^{-1} \in H$. Budući da je H (pod)grupa, $h^{-1} = gm^{-1}$ je također u H, pa je $g = h^{-1}m \in HM$. Dakle, $G \subseteq HM$. S druge strane, jer je G zatvorena s obzirom na množenje, a H i M su podskupovi od G, vrijedi $HM \subseteq G$. To zajedno daje $HM = G$. Sada vidimo da je $\nu(H) = \mu(HM) = \mu(G) = 1$, odnosno, normiranost je ispunjena.

Za konačnu aditivnost, uzmimo A i B, disjunktne podskupove od H. Naravno, $(A \uplus B)M = AM \cup BM$, još treba vidjeti da je unija ostala disjunktna. Pretpostavimo da nije, i uzmimo neki $x \in AM \cap BM$. Dakle, $x = am = bn$, gdje su $a \in A$, $b \in B$ i $m \in M \ni n$. Množenjem relacije $am = bn$ slijeva s b^{-1} i zdesna s m^{-1}, dobivamo $b^{-1}a = nm^{-1}$. No, A i B su podskupovi od H, pa su i a i b iz H. H je (pod)grupa, pa je $b^{-1}a$ također u H. No, to je jednako nm^{-1}, pa je $nm^{-1} \in H$, odnosno, $n \sim_{H\cdot} m$. Dakle, m i n su u istoj klasi $\sim_{H\cdot}$-ekvivalencije, pa je $Hm = Hn$. Naravno, $e \in H$, pa je $m = em \in Hm = Hn$ i $n = en \in Hn$. No, M sadrži samo po jednog predstavnika svakog desnog H-razreda, pa tako i Hn, iz čega zaključujemo $m = n$. Ako to uvrstimo gore (prikaz od x) i skratimo s n, dobivamo $a = b$, što je nemoguće jer se a i b nalaze u disjunktnim skupovima A i B. Dakle, kontradikcijom, unija jest disjunktna, odnosno, $(A \uplus B)M = AM \uplus BM$. Sada se lako dobije

$$\nu(A \uplus B) = \mu((A \uplus B)M) = \mu(AM \uplus BM) =$$

$$= \mu(AM) + \mu(BM) = \nu(A) + \nu(B).$$

G-invarijantnost od ν je jednostavna: neka su $g \in G$ i $A \subseteq G$. Tada je $\nu(gA) = \mu((gA)M) = \mu(g(AM)) = \mu(AM) = \nu(A)$.

((3)) Neka je μ grupna mjera na G, i neka je $H \trianglelefteq_{\mathcal{G}r} G$. Definirajmo ν na $\mathcal{P}(G/_H)$ s $\nu(A) := \mu(\biguplus A)$ (unija jest disjunktna jer su elementi od A — H-razredi — klase ekvivalencije, dakle međusobno disjunktni). Provjerimo svojstva (totalnost i nenegativnost su očite):

Normiranost: H-razredi kao klase ekvivalencije čine particiju od G, pa je $\biguplus(G/_H) = G$, te je $\nu(G/_H) = \mu(\biguplus(G/_H)) = \mu(G) = 1$.

Konačna aditivnost slijedi iz činjenice da je unija u definiciji od ν disjunktna. Naime,

$$\nu(A \uplus B) = \mu(\biguplus(A \uplus B)) = \mu(\biguplus A \uplus \biguplus B) =$$
$$= \mu(\biguplus A) + \mu(\biguplus B) = \nu(A) + \nu(B).$$

G-invarijantnost: neka je $\mathcal{A} \subseteq G/_H$, dakle $\mathcal{A} = \{aH\}_a^A$ (A uzmimo takav da $a \mapsto aH$ bude injekcija — zapravo, takav A je skup reprezentanata za $\mathcal{A}$, iako se ovdje korištenje Aksioma izbora može izbjeći), te neka je $gH \in G/_H$ bilo koji H-razred. Tada, jer je množenje s g permutacija u G, je

$$\nu((gH)\mathcal{A}) = \mu(\biguplus((gH)\mathcal{A})) = \mu(\biguplus_a^A gHaH) = \mu(\biguplus_a^A gaH) =$$
$$= \mu(g\biguplus_a^A aH) = \mu(g\biguplus \mathcal{A}) = \mu(\biguplus \mathcal{A}) = \nu(\mathcal{A}). \square$$

Teorem 24. *((bez dokaza — dokaz se može naći u* [2, T.10.4]*)) Klasa izmjerivih grupâ ima i ova svojstva:*

(1) *Sve Abelove grupe su izmjerive.*
(2) *Svaki de-kvocijentna grupa izmjerivih grupâ je izmjeriva, tj. ako je H normalna podgrupa od G, i pritom su H i $G/_H$ izmjerive, tada je i G izmjeriva.*

N. Zašto u $\mathbb{R}^1$ i $\mathbb{R}^2$ nema Banach–Tarskijevog paradoksa?

Za odgovor na to pitanje, prisjetimo se prvo što su rješive grupe. Dat ćemo kao definiciju tvrdnju koja se obično navodi kao karakterizacija, no za naše svrhe je operativnija. ((Standardna definicija, kao i dokaz da je ekvivalentna navedenoj, može se pronaći u [3, II.7,8])).

Definicija 25. *Za grupu G kažemo da je* rješiva *ako postoji $n \in \mathbb{N}$ i grupe ${G_i}_i^{n+1}$, takve da je $G_0 = \{e\}$, $G_n = G$, te za svaki $k \in n$ vrijedi: G_k je normalna podgrupa u G_{k+1}, i odgovarajuća kvocijentna grupa, $G_{k+1}/_{G_k}$, je Abelova.*

Npr., sve Abelove grupe su rješive, jer možemo staviti $n = 1$. Također, diedralna grupa D_n, grupa transformacijâ pravilnog n-terokuta ($3 \le n \in \mathbb{N}$)

(zadana generatorima a i b, te relacijama $a^n = b^2 = abab = e$) je rješiva, što pokazuje tzv. *rješivi niz* $\{e\} \triangleleft \langle\{a\}\rangle_{\leq D_n} \triangleleft D_n$, s pripadnim kvocijentnim grupama (izomorfnima s) n i 2, redom. S druge strane, proste ne-Abelove grupe (npr. A_n, alternirajuća grupa stupnja n — grupa parnih permutacijâ od n elemenata — za $5 \leq n \in \mathbb{N}$) nisu rješive (jer ne možemo ništa staviti na pretposljednje mjesto u najkraćem rješivom nizu).

Ono što je bitno zaključiti je da su, po teoremu na kraju prethodnog odjeljka, sve rješive grupe izmjerive. Zaista, jer su sve kvocijentne međugrupe Abelove, one su i izmjerive po svojstvu ⟮1⟯, pa se u rješivom nizu možemo popeti do grupe od koje smo krenuli, u svakom koraku primjenjujući svojstvo ⟮2⟯ na ono što smo dobili u prethodnom koraku i po jednu kvocijentnu među-grupu (početak je trivijalan: $\{e\}$ je konačna, dakle izmjeriva).

Sada se već vidi djelomičan odgovor na pitanje iz naslova: grupe izometrijâ u $\mathbb{R}$ i $\mathbb{R}^2$ su rješive. Prvo, uvedimo oznaku $Tran_n$ za grupu translacijâ u $\mathbb{R}^n$. Zatim, znamo da se svaka izometrija u $\mathbb{R}^n$ može na jedinstven način zapisati kao kompozicija linearnog operatora i translacije. Preciznije, za svaku izometriju $f \in \mathrm{Iso}(\mathbb{R}^n)$, s $\ell_f(x) := f(x) - f(0_n)$ dan je linearan operator, za kojeg se lako provjeri da je ortogonalan. Štoviše, kompoziciji izometrijâ odgovara kompozicija pripadnih linearnih operatorâ, odnosno $f \mapsto \ell_f$ je homomorfizam. Budući da je svaki ortogonalni operator ujedno i izometrija, to je i epimorfizam.

S obzirom na to da je prikaz jedinstven, možemo proširiti definiciju determinante i definirati $\mathsf{det}\ f := \mathsf{det}\ \ell_f$. Naravno, u našem slučaju, zbog ortogonalnosti, taj broj će biti 1 ili -1 (ovisno o tome čuva li f orijentaciju ili ne). Zbog $\ell_{f \circ g} = \ell_f \circ \ell_g$, Binet–Cauchyjev teorem i dalje vrijedi:

$$\mathsf{det}\ (f \circ g) = \mathsf{det}\ \ell_{f \circ g} = \mathsf{det}\ (\ell_f \circ \ell_g) = \mathsf{det}\ \ell_f \cdot \mathsf{det}\ \ell_g = \mathsf{det}\ f \cdot \mathsf{det}\ g.$$

Još sa SI_2 označimo grupu svih izometrijâ od $\mathbb{R}^2$ koje čuvaju orijentaciju. Sada možemo dokazati

Teorem 26. *Grupe* $\mathrm{Iso}(\mathbb{R})$ *i* $\mathrm{Iso}(\mathbb{R}^2)$ *su rješive.*

$$\{1_{\mathbb{R}}\} \triangleleft Tran_1 \triangleleft \mathrm{Iso}(\mathbb{R}) \quad i \quad \{1_{\mathbb{R}^2}\} \triangleleft Tran_2 \triangleleft SI_2 \triangleleft \mathrm{Iso}(\mathbb{R}^2)$$

su pripadni rješivi nizovi.

<u>*Dokaz:*</u>

Vidimo da moramo dokazati nekoliko tvrdnjî oblika: H je normalna podgrupa od G, i njihov kvocijent je izomorfan s K, što je Abelova grupa. U tu svrhu možemo iskoristiti I. teorem o izomorfizmu grupâ, tako da konstruiramo neki epimorfizam sa G na Abelovu grupu K, takav da mu je H upravo jezgra.

⟮$\{1_{\mathbb{R}}\} \triangleleft Tran_1$⟯ Pridružimo svakoj translaciji broj za koji ona translatira ($f \mapsto f(0)$). Po definiciji translacijâ, to je epimorfizam na aditivnu grupu realnih brojeva, čija je jezgra trivijalna.

(($Tran_1 \lhd \textsc{Iso}(\mathbb{R})$)) Lako se vidi da je svaka izometrija na $\mathbb{R}$ ili translacija ili centralna simetrija. Ako translacijama pridružimo 0, a centralnim simetrijama 1, dobivamo epimorfizam na Abelovu grupu 2, čija je jezgra $Tran_1$ po definiciji.

(($\{1_{\mathbb{R}}\} \lhd Tran_1$)) Kao gore, pridružimo $f \mapsto f(0_2)$. To je izomorfizam $Tran_2$ s kvadratom aditivne grupe realnih brojeva.

(($Tran_2 \lhd SI_2$)) Ovdje je epimorfizam $f \mapsto \ell_f$. Jezgru mu čine upravo translacije: Ako je $\ell_f = 1_{\mathbb{R}^2}$, to znači, za svaki $x \in \mathbb{R}^2$, $x = \ell_f(x) = f(x) - f(0_n)$, odnosno $f(x) = x + f(0_n)$, dakle f je translacija. Obrnuto, ako je $f(x) = x + c$ za neki $c \in \mathbb{R}^2$, tada je $f(0_n) = 0_n + c = c$, pa je $\ell_f(x) = (x+c) - c = x$. Slika tog epimorfizma je grupa svih specijalnih ($\det = 1$) ortogonalnih operatorâ u ravnini, dakle grupa svih rotacijâ oko ishodišta, za koju je ključno vidjeti da je izomorfna s $\mathbb{R}/_{2\pi\mathbb{Z}}$, dakle komutativna.
((Tu je upravo skok kojeg nema u višim dimenzijama, odnosno detalj koji razdvaja pravac i ravninu od ostalih euklidskih prostorâ: SO_n **nije** komutativna za $n \geq 3$.))

(($SI_2 \lhd \textsc{Iso}(\mathbb{R}^2)$)) Epimorfizam je naravno $\det$, čija je slika multiplikativna grupa nad $\{-1, 1\}$, dakle Abelova. □

Gornji teorem, zajedno s rezultatima iz prethodnog odjeljka, daje da $\mathbb{R}^n$ nije $\textsc{Iso}(\mathbb{R}^n)$-paradoksalan za $n \in \{1, 2\}$. Štoviše, tada imamo totalnu, izometrički-invarijantnu normiranu konačno aditivnu mjeru na $\mathbb{R}^n$. Međutim, to nije dovoljno za obaranje Banach–Tarskijevog paradoksa — takva mjera, s obzirom na to da je ograničena na $\mathbb{R}^n$, sigurno iščezava na svim omeđenim skupovima. Nama treba činjenica da segment, odnosno krug, nisu paradoksalni s obzirom na izometrije.

To je posljedica općeg teorema iz teorije mjere, odnosno njegove varijante koja je relevantna za teoriju jednakosastavljivosti, koju ovdje navodimo bez dokaza.

Teorem 27. *((o invarijantnom proširenju mjere)) ((bez dokaza — može se naći u* [2, T.10.7,8]*)) Neka je $\mathcal{A}$ Booleova algebra, $G \leq_{\mathcal{G}r} \textsc{Aut}\mathcal{A}$ neka izmjeriva grupa njenih automorfizama, $\mathcal{A}_0$ G-invarijantan potprsten od $\mathcal{A}$, a μ G-invarijantna mjera na $\mathcal{A}_0$. Tada postoji G-invarijantna mjera $\tilde{\mu}$ na $\mathcal{A}$, koja proširuje μ.*

Naravno, u našem slučaju, za $n \in \{1, 2\}$, $\mathcal{A} = \mathcal{P}(\mathbb{R}^n)$, $\mathcal{A}_0$ je skup svih Lebesgue-izmjerivih skupova u $\mathbb{R}^n$, $G = \textsc{Iso}(\mathbb{R}^n)$, a μ je Lebesgueova mjera. Jedini uvjet za ograničenje na n je izmjerivost od G. Iz toga dobivamo da ovo sve možemo provesti i u višim dimenzijama, samo ako se ograničimo na neku izmjerivu podgrupu grupe izometrijâ. Također, možemo ići i u suprotnom smjeru: paradoks bi mogao postojati i u nižim dimenzijama, ako samo proširimo grupu izometrijâ tako da više ne bude izmjeriva. Kako to učiniti, pokazat ćemo u sljedećim odjeljcima.

0. Neizmjerivo proširenje grupe izometrijâ ravnine

U prethodna dva odjeljka vidjeli smo (otprilike) kako rješivost grupe izometrijâ pravca i ravnine utječe na to da Banach–Tarskijev paradoks ne postoji u dimenzijama 1 i 2. Pitanje je koju širu grupu pogledati, tako da s obzirom na nju segment, odnosno krug (ili kvadrat) budu paradoksalni. U ovom odjeljku koncentrirat ćemo se na preslikavanja ravnine $\mathbb{R}^2$.

Naravno, ne zanimaju nas proizvoljna proširenja grupe izometrijâ: ako uzmemo grupu svih bijekcijâ ravnine, lako se vidi (korištenjem Aksioma izbora) da su svi beskonačni skupovi paradoksalni, što uopće ne zvuči kontraintuitivno — čak štoviše, vrlo slična tvrdnja često se uzima za definiciju beskonačnosti.

Jedino što proizvoljne bijekcije čuvaju je kardinalitet. Nas više zanima *mjera* (u slučaju ravnine površina) kao ono što se udvostručuje, a intuitivno bi trebalo ostati sačuvano. Izometrije čuvaju više od površine — one čuvaju udaljenost (može se vidjeti da je u $\mathbb{R}^n$ to zaista jači uvjet). Ta činjenica ima i zanimljivu matričnu reprezentaciju. Izometrije u $\mathbb{R}^n$ su afina preslikavanja (afino preslikavanje je kompozicija linearnog operatora i translacije), takva da je pripadni linearni operator ortogonalan. Budući da je apsolutna vrijednost determinante operatora upravo faktor kojim on povećava površinu, čuvanje površine je ekvivalentno sa zahtjevom $\mathsf{det} = \pm 1$.

Ortogonalnost operatora po Binet–Cauchyjevom teoremu povlači da mu je determinanta jednaka 1 ili -1:

$$(\mathsf{det}\ A)^2 = \mathsf{det}\ A \cdot \mathsf{det}\ A = \mathsf{det}\ A \cdot \mathsf{det}\ A^\tau = \mathsf{det}\ AA^\tau = \mathsf{det}\ \mathrm{I}_n = 1.$$

Naravno, obrat ne vrijedi. U ortogonalnoj (2×2) matrici svi matrični elementi moraju biti po apsolutnoj vrijednosti manji od 1, dok npr. matrica $A := \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ ima determinantu $1 \cdot 1 - 0 \cdot 2 = 1$. Dakle, linearni operator na $\mathbb{R}^2$, zadan matricom A, čuva površinu, iako nije izometrija. (Geometrijski, možemo ga interpretirati kao "naginjanje" ravnine za po dvije horizontalne jedinice za svaku vertikalnu.) Prirodno se postavlja pitanje: možemo li promatrati sva afina preslikavanja determinante ± 1, u nadi da ćemo među njima dobiti slobodnu podgrupu ranga 2? Pokazuje se da možemo uzeti i puno manje. Naime, možemo se (promatrajući linearne dijelove afinih preslikavanjâ) ograničiti samo na matrice s cjelobrojnim koeficijentima (čiju ćemo specijalnu grupu[0] označiti sa $SL_2(\mathbb{Z})$).

Lema 28. *Matrice* $A := \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ *i* $B := A^\tau = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ *generiraju slobodnu podgrupu od* $SL_2(\mathbb{Z})$*, ranga* 2.

Dokaz:

[0] To zaista jest grupa, jer je zbog uvjeta $\mathsf{det}\ A = 1$ inverz od $A \in SL_2(\mathbb{Z})$ ponovo matrica s cjelobrojnim elementima: $ad - bc = 1 \Rightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Prvo pogledajmo kako izgledaju cjelobrojne potencije od A i od B. U tu svrhu izmnožimo općenito

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

iz čega slijedi da je s

$$r : \mathcal{G}r(\mathbb{Z}, +) \to \mathcal{G}r(SL_2(\mathbb{Z}), \cdot);\ a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

zadan homomorfizam (zapravo monomorfizam) grupâ, takav da je $A = r(2)$. No tada je

$$A^n_{\cdot} = (r(2))^n_{\cdot} = r(n \cdot 2) = r(2n) = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix} \ \&$$

$$\& \ B^n_{\cdot} = (A^\tau)^n_{\cdot} = (A^n_{\cdot})^\tau = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}^\tau = \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix},$$

iz čega slijedi $A^n_{\cdot} = \mathrm{I}_2 \Rightarrow n = 0$, i analogno za B. Dakle, nijedna netrivijalna cjelobrojna potencija od A (niti od B) nije jednaka jediničnoj matrici.

Sada pretpostavimo da su A i B zavisne, pa neka je w' neka netrivijalna (BSOMP reducirana) riječ u grupi generiranoj s A i B, koja se uz gornje interpretacije od A i B izračuna u jediničnu matricu. Zbog gore dokazanog, w' se ne sastoji samo od jednog slova, dakle, ima u sebi bar jedno A i bar jedno B. Neka w' počinje s A^{l_1} (ako w' počinje s B, stavimo $l_1 := 0$), a završava s A^{l_2} (uz analognu napomenu). Ako sad označimo $l_3 := \mathsf{max}\{l_1, -l_2\} + 1$, te $w := A^{-l_3} w' A^{l_3}$ (preciznije, pripadna reducirana riječ), vidimo da se i w izračuna u I_2, s tom razlikom da w zaista počinje i završava s A (preciznije, w počinje s $A^{l_1 - l_3}$, a završava s $A^{l_2 + l_3}$, što su zbog odabira od l_3 netrivijalne potencije od A). Dakle, w je oblika (reducirano) $\prod_i^s (A^{n_i} B^{m_i}) \cdot A^{n_s}$, gdje je $s \in \mathbb{N}^*$, i svi ${n_i}_i^{s+1}$ i ${m_j}_j^s$ su iz $\mathbb{Z}^*$ (iz čega slijedi da su im apsolutne vrijednosti bar 1, što će nam trebati poslije).

Matrično, $w = \mathrm{I}_2$, pa je

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathrm{I}_2 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = w \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \prod_i^s (A^{n_i} B^{m_i}) \cdot A^{n_s} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$= \prod_i^s \left(\begin{bmatrix} 1 & 2n_i \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2m_i & 1 \end{bmatrix} \right) \cdot \left(\begin{bmatrix} 1 & 2n_s \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right),$$

odnosno, prvi vektor kanonske baze u $\mathbb{R}^2$ jednak je samom sebi nakon množenja sa svim gornjim matricama. Pogledajmo u kakvom su odnosu njegove komponente u svakom međukoraku. U tu svrhu označimo (u sljedećim formulama $i \in s \ \& \ j := s - 1 - i$):

$$\begin{bmatrix} a_0 \\ b_0 \end{bmatrix} := A^{n_s} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 2n_s \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} c_i \\ d_i \end{bmatrix} := B^{m_j} \cdot \begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2m_j & 1 \end{bmatrix} \cdot \begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} a_i \\ 2m_j a_i + b_i \end{bmatrix}, \text{ te}$$

$$\begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} := A^{n_j} \cdot \begin{bmatrix} c_i \\ d_i \end{bmatrix} = \begin{bmatrix} 1 & 2n_j \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} c_i \\ d_i \end{bmatrix} = \begin{bmatrix} 2n_j d_i + c_i \\ d_i \end{bmatrix}.$$

Po gornjem, trebalo bi biti $(a_s, b_s) = (1, 0)$. Pokazat ćemo da to ne može biti slučaj. Promotrimo sljedeći lanac implikacijâ:

$$\underline{|a_i| > |b_i|} \Rightarrow |d_i| = |2m_j a_i + b_i| \geq |2m_j a_i| - |b_i| > 2\,|m_j|\,|a_i| - |a_i| \geq$$

$$\geq 2\,|a_i| - |a_i| = |a_i| = |c_i| \Rightarrow \underline{|d_i| > |c_i|} \Rightarrow |a_{i+1}| = |2n_j d_i + c_i| \geq |2n_j d_i| -$$

$$- |c_i| > 2\,|n_j|\,|d_i| - |d_i| \geq 2\,|d_i| - |d_i| = |d_i| = |b_{i+1}| \Rightarrow \underline{|a_{i+1}| > |b_{i+1}|}\ .$$

Budući da je na početku zaista $|a_0| = |1| = 1 > 0 = |0| = |b_0|$, vidimo da općenito vrijedi $|a_{i+1}| > |b_{i+1}|\ \&\ |d_i| > |c_i|$. No tada je

$$|a_{i+1}| > |b_{i+1}| = |d_i| > |c_i| = |a_i|\,,$$

pa funkcija $i \mapsto |a_i|$ strogo raste, dakle je injekcija. Specijalno je $i \mapsto a_i$ injekcija, pa, jer je $s \neq 0$, ne može biti $a_0 = 1 = a_s$. Kontradikcija, dakle A i B su nezavisne. □

Dakle, grupa $SL_2(\mathbb{Z})$ ima slobodnu podgrupu ranga 2, pa je po rezultatima iz odjeljka K samoparadoksalna. Zanimljivo je vidjeti da se gornja slobodna podgrupa može dobiti dodajući grupi linearnih izometrijâ ravnine (čak samo onih čije matrice imaju samo cjelobrojne elemente, čiju ćemo grupu označiti sa $SO_2(\mathbb{Z})$[P]) samo jedno "naginjanje" (i grupno zatvarajući), zadano sa $\sigma(x, y) := (x + y, y)$. Tada je matrica od σ jednaka $C_1 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = r(1)$, pa odmah vidimo da je $A = C_1^{\cdot 2}$. Također, ako sa $C_2 := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in SO_2(\mathbb{Z})$ označimo matricu rotacije za $\frac{\pi}{2}$ (oko 0_2), tada je $B = C_2 \cdot C_1^{\cdot -2} \cdot C_2^{\cdot -1}$, pa su i A i B u grupi generiranoj sa $SO_2(\mathbb{Z})$ i C_1.

P. Geometrijska priprema — u 2 dimenzije

Budući da je grupa $SL_2(\mathbb{Z})$ samoparadoksalna, prirodno je zapitati se može li se to iskoristiti za dobivanje paradoksalnih rastava u ravnini, slično kao kod Hausdorffovog teorema. Nažalost, ne direktno — ulogu koju je tamo imala jedinična sfera ovdje bi trebala preuzeti jedinična kružnica, no naša proširena grupa ne djeluje na kružnicu. Štoviše, ne djeluje ni na koji ograničen skup koji sadrži neku točku osim 0_2. Naime, neka je (x, y) neka točka u ravnini koja nije na x-osi ($y \neq 0$). Sa σ_1 i σ_2 označimo linearne operatore zadane matricama A i B, redom, a s F označimo (slobodnu) grupu generiranu njima. Tada je $\sigma_1{}_\circ^n(x, y) = (x + 2ny, y)$, pa, zbog $\mathsf{lim}_n(x + 2ny) = \infty$, F-orbita točke (x, y) nije ograničena. Analogno je za točku kojoj je $x \neq 0$, uzevši σ_2 umjesto σ_1.

Dakle F, iako je samoparadoksalna, nije dovoljna za dokazivanje egzistencije paradoksalnih rastava ograničenih podskupova ravnine. Da bismo to postigli, moramo nekako ograničiti djelovanje od F, tako da točke pri tom novom djelovanju ostanu unutar nekog ograničenog područja. Treba primijetiti da je F grupa linearnih operatorâ — jednostavna preslikavanja

[P] To je zapravo ciklička grupa reda 4, generirana sa C_2.

koja čuvaju površinu, a koja nismo uzeli u obzir, su translacije. Njih treba iskoristiti.

Sa SA_2^* označimo grupu svih afinih preslikavanjâ oblika $\tau \circ l$, gdje je $l \in SL_2(\mathbb{Z})$, a $\tau \in Tran_2$ bilo koja translacija. Neka je J poluotvoreni jedinični kvadrat, $J := [0,1\rangle_\times^2$. Neka je $\sim_{\mathbb{Z}^2}$ relacija (ekvivalencije) na $\mathbb{R}^2$, dana s $P \sim_{\mathbb{Z}^2} Q :\Leftrightarrow P - Q \in \mathbb{Z}^2$. Uvedimo oznaku $\hat{\ }$, koju ćemo koristiti na više razinâ:

- Za $x \in \mathbb{R}$, $\hat{x} := x - \lfloor x \rfloor$ (razlomljeni dio broja x).
- Za točku $P = (x, y) \in \mathbb{R}^2$, $\hat{P} := (\hat{x}, \hat{y}) \in J$.
- Za preslikavanje $\sigma \in SA_2^*$, $\hat{\sigma} : J \to J;\ P \mapsto \widehat{\sigma(P)}$.
- Za podgrupu $H \leq_{\mathcal{G}r} SA_2^*$, $\hat{H} := \{\hat{\sigma}\}_\sigma^H$.

Naravno, J je skup reprezentanata za $\mathbb{R}^2/_{\sim_{\mathbb{Z}^2}}$, a $\hat{\ } : \mathbb{R}^2 \to J$ je upravo kvocijentno preslikavanje. Lako se vidi da je preslikavanje $\hat{\ }$, u svim gornjim kontekstima, idempotentno, dakle dvostruka njegova primjena daje isto što i jednostruka. Također, vrijedi sljedeća

Lema 29. *Preslikavanje $\sigma \mapsto \hat{\sigma}$ je homomorfizam s grupe SA_2^* u grupu (po dijelovima afinih) permutacijâ od J koje čuvaju površinu. Restrikcija tog preslikavanja na $SL_2(\mathbb{Z})$ je monomorfizam.*

Dokaz:

Prvo pokažimo da preslikavanja iz SA_2^* čuvaju relaciju $\sim_{\mathbb{Z}^2}$. Neka je $\sigma \in SA_2^*$, dakle, $\sigma(x, y) = \ell_\sigma(x, y) + \sigma(0_2)$, gdje je $\ell_\sigma \in SL_2(\mathbb{Z})$ pripadni linearni operator. On je zadan matricom s cjelobrojnim elementima, pa vrijedi $\ell_\sigma{}^\rangle(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$. Tada iz $P \sim_{\mathbb{Z}^2} Q$ slijedi

$$\sigma(P) - \sigma(Q) = (\ell_\sigma(P) + \sigma(0_2)) - (\ell_\sigma(Q) + \sigma(0_2)) = \ell_\sigma(P) - \ell_\sigma(Q) =$$
$$= \ell_\sigma(P - Q) \in \ell_\sigma{}^\rangle(\mathbb{Z}^2) \subseteq \mathbb{Z}^2,$$

dakle $\sigma(P) \sim_{\mathbb{Z}^2} \sigma(Q)$.

Budući da je SA_2 grupa, djelujući sa σ^{-1} dobivamo i obrat: $P \sim_{\mathbb{Z}^2} Q \Leftrightarrow \sigma(P) \sim_{\mathbb{Z}^2} \sigma(Q)$. Iz toga, uz činjenicu da je J skup reprezentanata za $\mathbb{R}^2/_{\sim_{\mathbb{Z}^2}}$, lako dobivamo da je $\hat{\sigma}$ injekcija na J. Također, za $P \in J$, $\hat{\sigma}(\sigma_\circ^{-1}(P)) = \hat{P} = P$, odnosno, $\hat{\sigma}$ je i surjekcija na J, dakle permutacija od J.

Zbog konačnodimenzionalnosti, linearni operator ℓ_σ je neprekidan, pa je $\ell_\sigma{}^\rangle(J)$ ograničen skup. Dakle je i njegov translat $\sigma^\rangle(J)$ ograničen, pa siječe samo konačno mnogo poluotvorenih kvadratâ oblika $\tau_P{}^\rangle(J)$, gdje je τ_P translacija za $P \in \mathbb{Z}^2$. Na svakom od tih kvadratâ $\hat{\sigma}$ djeluje kao σ komponiran slijeva s nekom fiksnom translacijom (za $\sigma(0_2) - P$), dakle afino preslikavanje. To nam daje da je $\hat{\sigma}$ po dijelovima afina permutacija (koja je svuda determinante 1), iz čega slijedi da čuva površinu.

Da je preslikavanje homomorfizam, dobije se ovako: prvo iz $Q \sim_{\mathbb{Z}^2} \hat{Q}$ dobijemo $\sigma(Q) \sim_{\mathbb{Z}^2} \sigma(\hat{Q})$, odnosno (djelujući na to s $\hat{\ }$) $\hat{\sigma}(Q) = \hat{\sigma}(\hat{Q})$. Iz toga je (uz $Q := \sigma_2(P)$ & $\sigma := \sigma_1$)

$$(\hat{\sigma_1} \circ \hat{\sigma_2})(P) = \hat{\sigma_1}(\hat{\sigma_2}(P)) = \hat{\sigma_1}(\sigma_2(P)) = (\sigma_1 \mathbin{\hat{\circ}} \sigma_2)(P),$$

pa je $\hat{\sigma_1} \circ \hat{\sigma_2} = \sigma_1 \mathbin{\hat{\circ}} \sigma_2$.

Još treba vidjeti da je dano preslikavanje restringirano na grupu $SL_2(\mathbb{Z})$ monomorfizam, odnosno da mu se u jezgri od linearnih operatora nalazi samo identiteta. Pretpostavimo da je $l \in SL_2(\mathbb{Z})$ takav da je $\hat{l} = \mathit{1}_J$. Gore smo vidjeli da je $\hat{l}$ po dijelovima jednak $\tau \circ l$, gdje je τ translacija. Budući da kvadrat nije unija konačno mnogo dužinâ, vidimo da bar jedan od gornjih dijelova mora sadržavati 3 geometrijski nezavisne (nekolinearne) točke. No tada su $\tau \circ l$ i $\mathit{1}_{\mathbb{R}^2}$ dva afina preslikavanja ravnine koja se podudaraju u 3 nekolinearne točke, pa su jednaka: $\tau \circ l = \mathit{1}_{\mathbb{R}^2}$, iz čega $l = \tau_\circ^{-1} \in Tran_2$. No jedina linearna translacija je identiteta. □

Glavna posljedica (posljednje tvrdnje) gornje leme je da, ako je F slobodna podgrupa od $SL_2(\mathbb{Z})$ (npr. ona čije postojanje smo utvrdili u prethodnom odjeljku), tada je $\hat{F}$ slobodna grupa istog ranga, koja djeluje na J.

Q. von Neumannov paradoks u ravnini

Sada imamo slobodnu grupu ranga 2, koja djeluje na jedinični kvadrat J. Još je samo preostalo eliminirati fiksne točke danog djelovanja. Ovdje će to biti nešto kompliciranije nego u Banach–Tarskijevom slučaju, jer sada fiksnih točaka djelovanja ima kontinuum: npr., sve točke od J na x-osi su fiksne za operator σ_1 (zadan matricom A).

To se može zaobići ako umjesto izoliranih fiksnih točaka gledamo točke i dužine (eventualno s isključenim krajevima): naime, za svako preslikavanje iz SA_2 osim identitete, skup njegovih fiksnih točaka je (pravi) afini potprostor od $\mathbb{R}^2$, dakle prazan skup, singleton ili pravac. Kad to pogledamo reducirano na J, dobivamo da se D, skup fiksnih točaka djelovanja grupe $\hat{F}$ na J može napisati kao $D = D_1 \cup \bigcup D_2$, gdje je D_1 najviše prebrojiv podskup od J, a D_2 je najviše prebrojiv skup "dužinâ" (eventualno s isključenim krajevima) — podskupova od J.

Eliminacija od D će se sastojati od 2 koraka: prvo ćemo pokazati kako eliminirati najviše prebrojiv skup točaka (koji može biti i pravi nadskup od D_1, označimo ga sa C) — preciznije, dokazat ćemo da vrijedi $J \dot{\setminus} C \approx_{Tran_2} J$, gdje je $C \subset J$ najviše prebrojiv, a $\approx_{Tran_2}$ relacija jdnakosastavljivosti generirana translacijama ($X \approx_{Tran_2} Y$ akko postoji bijekcija između X i Y koja je po dijelovima translacija). Zatim ćemo dokazati da se eliminacija dužinâ može svesti na eliminaciju točaka — preciznije, dokazat ćemo egzistenciju najviše prebrojivog skupa C takvog da vrijedi $J \dot{\setminus} D \approx_{Tran_2} J \dot{\setminus} C$, što će s gornjim po tranzitivnosti od $\approx_{Tran_2}$ povlačiti $J \dot{\setminus} D \approx_{Tran_2} J$, odnosno SA_2^*-paradoksalnost od J.

Za prvi korak, slično lemi 10, dovoljno je vidjeti da postoji translacija τ takva da je C disjunktan s $\hat{\tau}_\circ^{n\rangle}(C)$ za sve $n \in \mathbb{N}^*$. Naime, tada su svi

$C_i := \hat{\tau}_\circ^{i\rangle}(C)$ međusobno disjunktni, pa je $\biguplus_i^{\mathbb{N}^*} C_i \approx_{Tran_2} \biguplus_i^{\mathbb{N}} C_i$, odnosno $J \dot{\setminus} C \approx_{Tran_2} J$.

Enumerirajmo C kao $C = \{P_i\}_i^{\mathbb{N}}$. Za svaki $i \in \mathbb{N}$, translacijâ takvih da vrijedi $\tau_\circ^n(P_i) \sim_{\mathbb{Z}^2} P_j$ za neke $j \in i$ & $n \in \mathbb{Z}^*$, ima samo prebrojivo mnogo. Jer svih translacijâ ima kontinuum, mora postojati $\tau \in Tran_2$ koji nema gornje svojstvo ni za koji i, te je "dobar".

Za drugi korak, analogno, tvrdimo da postoji translacija τ' takva da je skup $D \cap \hat{\tau'}_\circ^{n\rangle}(D)$ najviše prebrojiv za svaki $n \in \mathbb{Z}^*$. U tu svrhu, enumerirajmo D_2 kao $D_2 = \{S_i\}_i^{\mathbb{N}}$.

Neka su $n \in \mathbb{Z}^*$ i $i \in \mathbb{N} \ni j \neq i$ zadani. Ako S_i i S_j nisu paralelne, tada svaki translat od S_i siječe S_j u samo jednoj točki. Ako je pak $S_i \| S_j$, tada odaberimo točku $P \in S_j$ i odbacimo sve translacije τ takve da, za neki $Q \in \mathbb{Z}^2$, $\tau_\circ^n(P)$ leži na pravcu koji sadrži S_i pomaknut za Q. Na taj način odbacili smo mnogo (kontinuum) translacijâ, ali krajevi njihovih pripadnih vektorâ leže na samo prebrojivo mnogo pravaca (sve translacije koje odbacimo za fiksne n, i, j, P i Q su "kolinearne"). Opet, jer se kvadrat ne može prekriti s prebrojivo mnogo pravaca (pravci su Lebesgueove mjere 0), postoji τ'.

Po svemu dokazanom, imamo paradoksalnost jediničnog kvadrata. Dakle, J se može rastaviti na 2 (pa dakle i 4) dijela, od kojih je svaki jednakosastavljiv s njim. Od tih 4 jediničnih poluotvorenih kvadratâ možemo upravo sastaviti poluotvoreni kvadrat stranice 2. Također, koristeći homotetiju s koeficijentom $\frac{1}{2}$, J je SA_2^*-jednakosastavljiv s poluotvorenim kvadratom stranice $\frac{1}{2}$. Sada, potpuno analogno kao u odjeljku J, možemo dobiti jednakosastavljivost (s obzirom na SA_2^*) bilo kojih punih (kvadrat se može upisati u njih) i ograničenih (mogu se upisati u kvadrat) skupova u ravnini.

Dakle, dokazali smo

Teorem 30. *((von Neumann, za ravninu)) Jedinični kvadrat u ravnini je SA_2^*-paradoksalan. Štoviše, svaka dva puna i ograničena skupa u ravnini su SA_2^*-jednakosastavljiva.*

Vidimo da je bilo dovoljno proširiti grupu izometrijâ na afina preslikavanja koja čuvaju mjeru. Na taj način, sačuvana je paradoksalnost rastava, jer smo skup površine 1, preslikavanjima koja čuvaju površinu, "presložili" u skup površine 2.

R. Jedna dimenzija — premalo za paradoks?

Sada se okrećemo realnom pravcu. Tu nam ideja o proširenju afinim preslikavanjima ne može pomoći, jer su u jednoj dimenziji za afina preslikavanja pojmovi "čuvati udaljenost" i "čuvati mjeru (duljinu)" jedno te isto (jezikom matricâ, postoje samo dvije 1×1-matrice s determinantom apsolutne vrijednosti 1 — $\begin{bmatrix} 1 \end{bmatrix}$ i $\begin{bmatrix} -1 \end{bmatrix}$ — i obje su ortogonalne).

Ipak je moguće gledati grupu *svih* permutacijâ od $\mathbb{R}$ koje u oba smjera čuvaju Lebesgueovu mjeru, i pokazati da je jedinični poluotvoreni interval $[0,1\rangle$ paradoksalan s obzirom na tu grupu, ali to uključuje dublje rezultate iz teorije mjere kojima se ovdje nećemo baviti. Ukratko, postoji bijekcija između $[0,1\rangle$ i S, jedinične sfere u $\mathbb{R}^3$, koja čuva Lebesgueovu mjeru u oba smjera[Q]. Pomoću te bijekcije može se Hausdorffov teorem prebaciti na $[0,1\rangle$.

Krenut ćemo drugim putem, koji omogućuje da se djelovanje matricâ tipa 2×2 upotrijebi i na pravcu. Pravac je jednodimenzionalan, pa najprirodnije djelovanje — kao linearni operatori — ne možemo iskoristiti. Međutim, postoji jedno manje poznato djelovanje, djelovanje regularnih 2×2-matricâ na pravcu upotpunjenom jednom točkom ($\dot{\mathbb{R}} := \mathbb{R}\uplus\{\infty\}$), preko *razlomljenih linearnih* preslikavanja, koje se definira ovako (djelovanje neke matrice A zapisujemo kao permutaciju od $\dot{\mathbb{R}}$, koju označavamo s f_A):

$$f_{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}}(x) := \begin{cases} \frac{ax+b}{d}, & x \in \mathbb{R} \\ \infty, & x = \infty \end{cases},$$

te, za $c \neq 0$,

$$f_{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}(x) := \begin{cases} \frac{ax+b}{cx+d}, & x \in \mathbb{R} \mathbin{\dot\setminus} \{-\frac{d}{c}\} \\ \infty, & x = -\frac{d}{c} \\ \frac{a}{c}, & x = \infty \end{cases}.$$

Lako se vidi (doduše, ispitivanjem brojnih slučajeva) da je na gornji način zaista zadano djelovanje grupe GL_2 na $\dot{\mathbb{R}}$, tj. da je $A \mapsto f_A$ homomorfizam grupâ GL_2 i $\mathcal{G}r(\dot{\mathbb{R}}!)$. Nas će zanimati restrikcija tog preslikavanja na grupu SL_2, te restrikcija samih f_A na neki interval u $\mathbb{R}$ koji ne sadrži "opasne" točke (one koje bi uvele ∞ u račun).

Jedno od svojstava koje gubimo gornjim nelinearnim djelovanjem je općenito čuvanje mjere (duljine, odnosno udaljenosti[R]). Zaista, jedina preslikavanja f_A koja čuvaju mjeru su ona za koja je $cx+d$ konstanta, odnosno, kao kod afinih preslikavanjâ, samo translacije i centralne simetrije.

Kako onda dobiti paradoks? Ideja je da se odustane od *čuvanja* udaljenosti, i da se traži njeno *sažimanje* (po dijelovima), s nekim koeficijentom koji se može mijenjati od mjesta do mjesta, ali je ograničen pozitivnom konstantom ε. U tu svrhu služi nam

Definicija 31. *Neka je* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2$, $\varepsilon \in \mathbb{R}^+$, *te* $I \subset \mathbb{R}$ *ograničen interval (ako je* $c \neq 0$*, dodatni uvjet na* I *je da ne sadrži točku* $-\frac{d}{c}$*). Tada se* f_A *zove* ε-kontrakcija (s obzirom) na I, *akko vrijedi*

$$\forall_{x,y}^{I}(|f_A(x) - f_A(y)| \leq \varepsilon\, |x-y|).$$

[Q]Taj rezultat može se naći u H. L. Royden, *Real Analysis*, 2nd ed., New York: Macmillan, 1968.; str. 327, T. 9

[R]Lak račun pokazuje $f_A{}'(x) = \frac{\det A}{(cx+d)^2}$ za $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ & $cx+d \neq 0$, što je za $A \in SL_2$ strogo pozitivno, pa u gornjem kontekstu f_A preslikava intervale u intervale, te je čuvanje udaljenosti laka posljedica čuvanja duljine (intervalâ).

Koristeći Teorem o srednjoj vrijednosti iz analize (funkcije f_A su glatke), vidi se da je za to svojstvo dovoljno provjeriti da vrijedi ${f_A}' \leq \varepsilon$ na cijelom intervalu I.

Prva jednostavna posljedica gornje definicije je da ε-kontrakcije (za $\varepsilon < 1$) sažimaju mjeru izmjerivih skupova, preciznije, vrijedi

Lema 32. *Neka je σ ε-kontrakcija s obzirom na $[a, b]$, te $A \subseteq [a, b]$ Lebesgue-izmjeriv. Tada je $\lambda(\sigma^{\rangle}(A)) \leq \varepsilon\lambda(A)$.*

<u>*Dokaz:*</u>

Budući da je σ bijekcija (praslika konačnog skupa je konačan skup), a konačni skupovi (specijalno $\{a, b\}$) su Lebesgueove mjere 0, BSOMP $A \subseteq \langle a, b\rangle$. Tada, jer je A izmjeriv, $\lambda(A) = \lambda^*(A)$ (vanjska Lebesgueova mjera). No ako je $A \subseteq \bigcup_i^{\mathbb{N}} \langle a_i, b_i\rangle \subseteq \langle a, b\rangle$, tada je (vidjeti fusnotu `R`)

$$\sigma^{\rangle}(A) \subseteq \bigcup_i^{\mathbb{N}} \langle \sigma(a_i), \sigma(b_i)\rangle,$$

s tim da je, za svaki $i \in \mathbb{N}$, $\sigma(b_i) - \sigma(a_i) \leq \varepsilon(b_i - a_i)$. Sumirajući i gledajući infimum, dobivamo $\lambda^*(\sigma^{\rangle}(A)) \leq \varepsilon\lambda(A)$. Kako je $\sigma_\circ^{-1}$ također razlomljena linearna funkcija, ona je izmjeriva, pa je $\sigma^{\rangle}(A) = (\sigma_\circ^{-1})^{\langle}(A)$ izmjeriv skup, te je $\lambda^*(\sigma^{\rangle}(A))$ upravo njegova Lebesgueova mjera, koja je po gornjem najviše $\varepsilon\lambda(A)$. □

S. Djelovanje grupe $\mathbb{Z}_\star^2$ na poluotvorenom intervalu

Nakon što smo vidjeli da i na $\mathbb{R}$ možemo iskoristiti 2×2-matrice, sljedeći korak je naći dva nezavisna (po dijelovima) linearna razlomljena preslikavanja, kako bismo dobili instancijaciju samoparadoksalne grupe $\mathbb{Z}_\star^2$. Naravno, za specijalne 2×2-matrice imamo lemu 28, no nju nećemo direktno iskoristiti (iz više razloga, jedan od kojih je sličan onome spomenutom na početku odjeljka `P` — djelovanje tako dobivene grupe nije ograničeno na segment, jer je već f_A translacija $x \mapsto x + 2$, za matricu A iz leme 28).

Put kojim ćemo krenuti bit će općenitije uočavanje slobodne podgrupe ranga 2 među razlomljenim linearnim preslikavanjima, koja će biti "umjetno" svedena na poluotvoreni interval — jedan generator namještanjem parametara, a drugi modularnom aritmetikom, poput preslikavanja ˆ u odjeljku `P`. Krenimo redom.

Prvo, generalizirajmo pojam transcendentnog broja. Za konačno mnogo brojeva ${\alpha_i}_i^n$ kažemo da su *algebarski nezavisni* (jer u tom slučaju moraju biti različiti, i redoslijed nije važan, još možemo reći da je skup $\{\alpha_i\}_i^n$ algebarski nezavisan) ako za svaki ne-nul polinom p u n varijabli s racionalnim (ekvivalentno, cjelobrojnim) koeficijentima ($p(x_i)_i^n \in \mathbb{Q}[x_i]_i^n \setminus \{0\}$) vrijedi $p(\alpha_i)_i^n \neq 0$. Naravno, jednočlan skup $\{\alpha\}$ je algebarski nezavisan akko je α transcendentan. Lako se vidi (matematičkom indukcijom, i koristeći algebarske činjenice poput $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$, te prebrojivost skupa $\mathbb{Q}$) da za svaki konačan[S] n postoji n algebarski nezavisnih brojeva. Štoviše, jer je svaki interval u $\mathbb{R}$ ekvipotentan sa cijelim $\mathbb{R}$, možemo dobiti algebarski nezavisne brojeve u bilo kojem intervalu. Nama će trebati samo 2 takva, i to u intervalu $\langle 0,1\rangle$. Manji označimo s α, a veći s β.

Neposredna posljedica algebarske nezavisnosti α i β je: ako je R racionalna funkcija u 2 varijable, s racionalnim koeficijentima, takva da je $R(\alpha,\beta)=a\in\mathbb{Q}$, tada je funkcija R zapravo konstanta a — samo prebacimo a na lijevu stranu, pomnožimo s nazivnikom i iskoristimo definiciju algebarske nezavisnosti. Ta činjenica će nam trebati.

Lema 33. *Neka su α i β algebarski nezavisni realni brojevi, takvi da vrijedi $0<\alpha<\beta<1$. Ako definiramo*

$$\gamma := \frac{\beta(2+\beta)}{(1+\beta)(2-\beta)},$$

$$\hat\sigma(x) := \frac{(1+\beta)x}{(2-\beta)x+\frac{1}{1+\beta}}\ \textit{(odnosno, } \hat\sigma = f_{\left[\begin{smallmatrix}1+\beta & 0\\ 2-\beta & \frac{1}{1+\beta}\end{smallmatrix}\right]}\textit{), te}$$

$$\hat\tau(x) := x +_{\cdot\gamma} \alpha\ \textit{(pomak za } \alpha \textit{ modulo } \gamma\textit{)},$$

tada su $\hat\sigma$ i $\hat\tau$ nezavisne permutacije poluotvorenog intervala $[0,\gamma\rangle$.

Dokaz:

$\hat\tau$ je očito permutacija od $[0,\gamma\rangle$, dok za $\hat\sigma$ (vidjeti fusnotu R) treba samo provjeriti rubove ($\hat\sigma(0)=0$ & $\hat\sigma(\gamma)=\gamma$) i vidjeti da "opasna" točka $-\frac{1}{(1+\beta)(2-\beta)}$ nije u intervalu $[0,\gamma\rangle$ (što je očito, jer je to strogo negativan broj).

Za nezavisnost, prvo uočimo da je $\hat\tau$ po dijelovima translacija, odnosno da djeluje kao f_A, gdje je $A=\begin{bmatrix}1&\alpha\\0&1\end{bmatrix}$ na intervalu $[0,\gamma-\alpha\rangle$, te $A=\begin{bmatrix}1&\alpha-\gamma\\0&1\end{bmatrix}$ na intervalu $[\gamma-\alpha,\gamma\rangle$ (jer se γ može zapisati kao $\beta\cdot\frac{2+\beta}{2+\beta-\beta^2}$, vidimo da je $\gamma>\beta>\alpha$, pa je $0<\gamma-\alpha<\gamma$, odnosno, intervali su netrivijalni). Dakle, pretpostavka da je w neka reducirana riječ nad $\{\hat\sigma,\hat\sigma^{-1},\hat\tau,\hat\tau^{-1}\}$ koja se izračuna u $\mathit{1}_{[0,\gamma\rangle}$ vodi na to da postoji W, reducirana riječ nad cjelobrojnim potencijama matricâ $A(\alpha):=\begin{bmatrix}1&\alpha\\0&1\end{bmatrix}$, $A(\alpha-\gamma)$ i $B(\beta):=\begin{bmatrix}1+\beta&0\\2-\beta&\frac{1}{1+\beta}\end{bmatrix}$, koja se izračuna u $\pm\mathrm{I}_2$. Budući da je γ racionalna funkcija od β, matrični elementi od W su racionalne funkcije u varijablama α i β, s racionalnim koeficijentima, koje poprimaju vrijednosti 0 odnosno ±1. Zbog algebarske nezavisnosti *brojeva* α i β, te racionalne funkcije poprimaju vrijednosti 0 odnosno ±1 za sve vrijednosti *varijabli* α i β, pa specijalno i za $\alpha:=2$ & $\beta:=0$. No tada je $\gamma=0$, pa je $A(\alpha)=A(\alpha-\gamma)=A(2)=A$, a $B(\beta)=B(0)=B$ iz leme 28. Dakle, W tada predstavlja reduciranu riječ u grupi F, koja se

[S] Zapravo, ako standardno definiramo da je neki (beskonačan) skup realnih brojeva algebarski nezavisan akko mu je svaki konačan podskup algebarski nezavisan, tada postoje algebarski nezavisni skupovi čak ekvipotentni s $\mathbb{R}$ (von Neumannovi brojevi).

ne može izračunati u I_2 po lemi 28, a lako se vidi iz dokaza te leme da se ne može izračunati niti u $-\mathrm{I}_2$. Budući da su I_2 i $-\mathrm{I}_2$ jedine matrice $A \in SL_2$ za koje je f_A identiteta na nekom intervalu, dobivamo kontradikciju, odnosno nezavisnost $\hat{\sigma}$ i $\hat{\tau}$. □

T. von Neumannov paradoks na pravcu

Napokon imamo sve potrebno za dokazati

Teorem 34. *((von Neumann, za pravac)) Za svaki $\varepsilon \in \mathbb{R}^+$, postoji paradoksalni rastav segmenta $[0,1]$, koji koristi samo ε-kontrakcije s obzirom na $[0,1]$, i translacije.*

((Jaka verzija)) Za svaki $\varepsilon \in \mathbb{R}^+$, te za svaka dva puna i ograničena podskupa od $\mathbb{R}$, U i V, postoji particija $U = \biguplus_i^n U_i$, takva da je $V = \biguplus_i^n f_{A_i}{}^{\rangle}(U_i)$, za neke ${A_i}_i^n$ iz SL_2, takve da su sva preslikavanja $f_{{A_i}_i}{}^n$ ε-kontrakcije s obzirom na neki interval koji sadrži U.

<u>*Dokaz:*</u>

Neka je $\varepsilon > 0$ zadan. Dovoljno je dokazati egzistenciju po dijelovima ε-kontrakcije sa $[0,1\rangle$ na neki nadskup od $[0,2]$, jer tada, rastavivši $[0,2]$ kao $[0,1\rangle \uplus [1,2]$, restringirajući preslikavanja na praslike odgovarajućih intervalâ i komponirajući preslikavanja čije su slike u drugom intervalu s translacijom za -1, dobivamo traženo dvostruko pokrivanje od $[0,1\rangle$.

Da bismo to izveli, prvo se koncentrirajmo na interval $[0,\gamma\rangle$. Budući da svaka linearna razlomljena funkcija koja nije identiteta, a odgovara specijalnoj 2×2-matrici (determinante 1), ima najviše 2 fiksne točke na intervalu bez "opasnih" točaka (dobivamo netrivijalnu algebarsku jednadžbu stupnja najviše 2), skup D fiksnih točaka djelovanja grupe $F_{\alpha,\beta} := \langle\{\hat{\sigma},\hat{\tau}\}\rangle_{\mathcal{G}r}$ na $[0,\gamma\rangle$ je prebrojiv, pa ga je moguće apsorbirati na standardni način, koristeći translacije modulo γ (njih ima kontinuum, a svaki par (d_1,d_2) točaka iz D eliminira najviše jednu uvjetom preslikavanja $d_1 \mapsto d_2$).

To nam daje da je $[0,\gamma\rangle$ paradoksalan pomoću translacijâ i preslikavanja $\hat{\sigma}$. Translacije su 1-kontrakcije, treba još vidjeti faktor kontrakcije od $\hat{\sigma}$. Po onome što je rečeno odmah iza definicije kontrakcijâ, to se lako vidi promatrajući derivaciju: za $x \in [0,\gamma\rangle$, $\hat{\sigma}'(x) = \frac{1}{N^2(x)}$, gdje je $N(x) := (2-\beta)x + \frac{1}{1+\beta}$ nazivnik od $\hat{\sigma}(x)$. Jer je $N(x) > 0$, maksimizacija od $\hat{\sigma}'(x)$ odgovara minimizaciji od $N(x)$. N je rastuća funkcija, pa joj je minimum $N(0) = \frac{1}{1+\beta}$, što daje maksimum derivacije $\hat{\sigma}'(0) = (1+\beta)^2$. Dakle, $\hat{\sigma}$ je $(1+\beta)^2$-kontrakcija. Naravno, $1 < (1+\beta)^2$, pa dobivamo da je $[0,\gamma\rangle$ paradoksalan pomoću $(1+\beta)^2$-kontrakcijâ.

Sada bismo htjeli iterirati tu "konstrukciju" da dobijemo dovoljno kopijâ od $[0,\gamma\rangle$ za pokriti $[0,2]$. No ovdje to neće biti tako jednostavno, jer relacija jednakosastavljivosti u ovom kontekstu nije tranzitivna — kompozicija dviju ε-kontrakcijâ na odgovarajućim intervalima je ε^2-kontrakcija, što nije

ε-kontrakcija za $\varepsilon > 1$ (konkretno, u ovom slučaju, $(1+\beta)^2 > 1$). Ipak je moguće, namještanjem parametara, postići željeni faktor kontrakcije ε. Da to postignemo, treba pažljivije promatrati što se događa s faktorima.

Pretpostavimo da smo dobili dovoljan broj kopijâ od $[0,\gamma\rangle$, iterirajući m puta gornje udvostručavanje. Tada je broj kopijâ jednak 2^m, pa, da bismo mogli pokriti $[0,2]$, mora biti $2^m\gamma > 2$, odnosno $m > 1 - \mathrm{ld}\gamma$ (s ld je označen logaritam po bazi 2). Najmanji prirodni broj za koji to vrijedi je $m := 2 - \lceil \mathrm{ld}\gamma \rceil$. No, s m iteracijâ postigli smo da su nam preslikavanja po dijelovima $((1+\beta)^2)^m$-kontrakcije. S druge strane, da bismo dobili interval $[0,\gamma\rangle$ od početnog $[0,1\rangle$, moramo ga prvo podvrgnuti γ-kontrakciji $x \mapsto \gamma x$, tako da je ukupan faktor kontrakcije $\gamma \cdot (1+\beta)^{2m}$.

Sada se vidi, koristeći jednostavnu analizu, da se γ asimptotski ponaša kao β za $\beta \to 0$ (preciznije, $\mathsf{lim}_{\beta\to 0}\frac{\gamma}{\beta} = 1$), pa se tako m ponaša kao $-\mathrm{ld}\beta$. Dakle, limes faktora kontrakcije za $\beta \to 0$ jednak je $\mathsf{lim}_{\beta\to 0}\frac{\beta}{(1+\beta)^{2\mathrm{ld}\beta}}$. Nazivnik izraza pod limesom može se zapisati kao izraz $((1+\beta)^{\frac{1}{\beta}})^{2\beta\mathrm{ld}\beta}$, kojem baza teži k e, a eksponent (npr. po L'Hospitalovom pravilu) k 0. Dakle, nazivnik teži k 1, pa faktor kontrakcije teži k 0 za $\beta \to 0$. Po definiciji limesa, tada možemo odabrati $\beta > 0$ dovoljno malen da potrebna preslikavanja budu ε-kontrakcije. Time smo dokazali prvu tvrdnju teorema. Primijetimo da, kako smo pokrili $[0,2]$, možemo pokriti i bilo koji drugi ograničen interval.

Za dokaz jake verzije, neka je $[a_U, b_U] \subseteq U \subseteq [c_U, d_U]$ & $[a_V, b_V] \subseteq V \subseteq [c_V, d_V]$. Ponovo, dovoljno je naći jednu po dijelovima ε-kontrakciju sa $[c_U, d_U]$ u $[a_V, b_V]$, te drugu sa $[a_U, b_U\rangle$ na neki nadskup od V.

Za prvu upotrijebimo $x \mapsto \mathsf{min}\{\varepsilon, \frac{d_U - c_U}{b_V - a_V}\} \cdot (x - c_U) + a_V$. Za drugu, definirajmo $\eta := \mathsf{min}\{\frac{1}{2}, (b_U - a_U)\varepsilon\}$ i upotrijebimo gornji dokaz za pokrivanje $[c_V, d_V]$ dovoljnim brojem kopijâ od $[0,1\rangle$, pomoću η-kontrakcijâ. Ako sad prije svih tako dobivenih preslikavanjâ primijenimo $\frac{1}{b_U - a_U}$-kontrakciju $x \mapsto \frac{x - a_U}{b_U - a_U}$, koja $[a_U, b_U\rangle$ preslikava na $[0,1\rangle$, dobivamo upravo traženu ε-kontrakciju. □

U. Sierpiński–Mazurkiewiczev paradoks

U ovom odjeljku pokazat ćemo da se "geometrijski" paradoksi (u ravnini) mogu dobiti i bez korištenja Aksioma izbora. Prvo je na redu za dokazivanje

Lema 35. *Neka grupa G, koja djeluje na X, sadrži dva elementa τ i ρ, tako da postoji $x \in X$, takav da se svake dvije netrivijalne riječi nad alfabetom $\{\tau, \rho\}$ s različitim početnim slovom (dakle, jedna počinje s τ, a druga s ρ) na x razlikuju. Tada postoji neprazan G-paradoksalan podskup $E \subseteq X$.*

<u>*Dokaz:*</u>

Označimo sa S monoid generiran s τ i ρ, a s E S-orbitu od x. E je po definiciji τ- i ρ-invarijantan, odnosno $\tau(E) \uplus \rho(E) \subseteq E$. Da je unija disjunktna, kaže nam svojstvo od x spomenuto u izreci leme — $\tau(E)$ (i analogno za

ρ) je upravo sve što se dobije kad riječi s početkom τ djeluju na x. Budući da još očito vrijedi $E = \tau^{-1}(\tau(E)) = \rho^{-1}(\rho(E))$ (nema reduciranja jer ne gledamo inverze, samo monoid), te $S \subset G$, vidimo da je E G-paradoksalan. □

Kakve to veze ima s ravninom $\mathbb{R}^2$? Pa, u grupi $\mathrm{Iso}(\mathbb{C})$ postoje takvi elementi. (Identificiramo $\mathbb{R}^2$ sa $\mathbb{C}$ na prirodan način.) S τ označimo translaciju $z \mapsto z+1$, a s ρ rotaciju $z \mapsto u \cdot z$, gdje je $u = e^{i\theta}$ neki transcendentan jedinični kompleksan broj (takav postoji[T], jer na jediničnoj kružnici ima kontinuum točaka, dok je $\mathsf{card}\mathbb{A}_{\mathbb{C}} = \aleph_0$ — s $\mathbb{A}_{\mathbb{C}}$ je označen skup svih nad $\mathbb{Q}$ algebarskih kompleksnih brojeva). Za x uzmimo 0.

Komponiranje τ i ρ na 0 odgovara, po Hornerovoj shemi, računanju nekog polinoma s prirodnim (ili 0) koeficijentima u točki u. Npr. riječi $\tau^3\rho^2\tau$ odgovara polinom z^2+3, u smislu $\tau^3\rho^2\tau(0) = u^2+3$. Iako to pridruživanje (riječ $\mapsto$ polinom) nije injektivno (dodavanjem ili brisanjem ρ na kraju riječi polinom se ne mijenja), vidi se da riječima koje počinju s ρ (i imaju u sebi bar jedno τ) odgovaraju polinomi sa slobodnim članom 0 (osim nulpolinoma), dok riječima koje počinju s τ odgovaraju polinomi sa strogo pozitivnim slobodnim članom. Riječima koje se sastoje samo od ρ odgovara nulpolinom.

S druge strane, kad bi dvije takve riječi (jedna koja počinje s τ i jedna koja počinje s ρ) jednako djelovale na 0, dobili bismo da u poništava neki polinom (s cjelobrojnim koeficijentima), konkretno, razliku polinomâ koji odgovaraju tim dvjema riječima. Budući da je u transcendentan, ta razlika mora biti nulpolinom, pa ti polinomi moraju biti jednaki, dakle specijalno imati jednake slobodne članove, što je po gornjem nemoguće.

Dakle, po gornjoj lemi, dokazali smo

Teorem 36. *((Sierpiński–Mazurkiewicz)) U $\mathbb{C}$ postoji neprazan,* $\mathrm{Iso}(\mathbb{C})$*-paradoksalan podskup E.*

Primijetimo da je dokaz potpuno konstruktivan (uz pretpostavku da znamo npr. da je e^i transcendentan): $E = \{p(e^i)\}_{p(z)}^{\mathbb{N}[z]}$. To je gust, ali prebrojiv podskup od $\mathbb{C}$, dakle Lebesgueove mjere 0, pa nije od koristi prilikom dokazivanja postojanja neizmjerivih skupova. No, danas znamo da tako i mora biti, jer smo njegovo postojanje dokazali bez Aksioma izbora, dakle u ZF, a sa ZF[U] je konzistentno da su svi podskupovi od (svih konačnodimenzionalnih) $\mathbb{R}^n$ Lebesgue-izmjerivi (Solovay, 1964.).

[T]Zapravo, $\theta = 1$ je dobar, no to je prilično teško dokazati.

[U]Preciznije, trebalo bi pisati $\mathsf{ZF} + {:}\mathsf{IC}$ (IC je tvrdnja da postoji neprebrojiv nedostiživ kardinal). Konzistentnost te teorije je strogo jača od same konzistentnosti ZF, no u nju se također "općenito vjeruje". Također, za imalo smislenije raspravljanje o Lebesgueovoj mjeri (npr. za njenu σ-aditivnost) potrebna je određena doza izbora (vidjeti i fusnotu `F`) — ovdje je uobičajeno uzeti DC, tzv. *Aksiom zavisnog izbora*, koji, intuitivno, daje postojanje prebrojivog skupa reprezentanata $\{a_n\}_n^{\mathbb{N}}$, u kojem a_{n+1} ovisi (samo) o a_n.

V. Nekoliko napomenâ o notaciji

U radu poput ovog, gdje se isprepliću razne grane matematike, svaka sa svojim specijaliziranim sustavom prikladnih oznakâ, prilično je teško sve to pomiriti. Ovdje sam koristio sustav koji inače upotrebljavam za bilježenje matematičkih idejâ i postupaka, odnosno onaj njegov dio za kojeg sam smatrao da neće izazvati previše zabunâ prilikom interpretacije. U ovom odjeljku pokušat ću istaknuti neke ideje na kojima se taj sustav oznakâ bazira.

Osnova na kojoj se gradi je standardni $\mathbb{ZF}$. Jedna od stvari naslijeđenih iz te teorije, a koja ponekad izaziva zabunu kod matematičarâ koji preferiraju specifikaciju pred implementacijom, je: prirodni brojevi su konačni ordinali, shvaćeni u von Neumannovom smislu. Dakle, $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$ itd. Na taj način, prirodni broj n služi kao kanonski skup od n elemenata.

Po uzoru na npr. sume ($\sum_i^S f_i = \sum_{i \in S} f_i$) i produkte ($\prod_i^S f_i$), pišu se i skupovi: $\{f_i\}_i^S = \{f_i;\, i \in S\}$; slogovi: $(f_i)_i^S = (f_i)_{i \in S}$; općenito kolekcije objekata: "${f_i}_i^S$" za "$f_i,\ i \in S$"; i mnogi drugi u osnovi analogni pojmovi, pa i kvantificirane izjave: $\forall_i^S P(i)$ za $(\forall i \in S)P(i)$. To omogućuje puno uniformniji rad s operacijama na indeksiranim familijama.

Jedna od posljedicâ gornjih dogovorâ je da ${A_i}_i^n$ služi kao kompaktna oznaka za n objekata neke zajedničke karakteristike, za što je uobičajen mnogo dulji zapis "$A_1, A_2, \ldots, A_n$" ili "$A_i,\ i = 1, 2, \ldots, n$", s jedinom razlikom što su gore A_i indeksirani brojevima od 0 do $n - 1$, no to i nije bitno dok se operira s ${A_i}_i^n$ kao sa cjelinom. Ako baš želimo imati indekse od 1 do n, možemo napisati ${A_{i+1}}_i^n$.

Još jedna od posljedicâ je potreba za notacijskim razlikovanjem vrijednosti funkcije f u skupu S kao točki, i slike funkcije f restringirane na S. Npr. ako je f definirana na $\mathbb{N}$, tada je $f(3) = f(\{0, 1, 2\})$ općenito različito od $\{f(0), f(1), f(2)\}$. Za prvo je oznaka naravno $f(S)$, a drugo se može zapisati u gornjem stilu kao $\{f(x)\}_x^S$. Bez uvođenja varijable x, možemo to zapisati kao $f^{\rangle}(S)$. Također, praslika nekog skupa T po funkciji f može se zapisati kao $f^{\langle}(T)$. Primijetimo da taj pojam nema veze s tim je li f bijekcija ili ne, što uobičajenija oznaka $f^{-1}(T)$ može lažno sugerirati.

Postoje još neke dosjetke za jednostavno zapisivanje činjenicâ o funkcijama, ako se sjetimo notacije $f : A \rightharpoonup B$ za parcijalne funkcije. Naime, $f : A \to B$ je injekcija akko je pripadna dualna relacija (zamjenom A i B) zapravo parcijalna funkcija. U tom svjetlu, prirodna oznaka za injekciju je $f : A \hookrightarrow B$. Također, ono što nedostaje parcijalnoj funkciji ($\rightharpoonup$)da bi bila funkcija ($\to$) je totalnost. Ako to apstrahiramo u oznaku $\rightharpoondown$, te se sjetimo da je $f : A \to B$ surjekcija akko joj je dualna relacija totalna, za surjekciju se nameće oznaka $f : A \leftharpoondown\!\!\rightarrow B$. Naravno, tada je oznaka za bijekciju $f : A \leftrightarrow B$; dualna relacija joj je (inverzna) funkcija. ((Ovo se može učiniti još simetričnijim: $R : A \rightharpoonup B$ je relacija između A i B čija svaka klasa ima *najviše* jedan element, dok je $R : A \rightharpoondown B$ relacija između A i B čija svaka klasa ima *najmanje* jedan element. I analogno, obrnuvši strelice i zamijenivši uloge skupova A i B.))

Neka je f funkcija. Za što je oznaka f^3 — $f \cdot f \cdot f$, $f \circ f \circ f$, ili nešto treće? Ako je A skup, je li A^2 Kartezijev produkt skupa A sa samim sobom, ili kvadrat "po točkama"? Ili možda skup svih 2-produkata elemenata od A? Da bi se izbjegli takvi nesporazumi, kod potenciranja u poziciju ispod eksponenta (kao indeks) možemo pisati oznaku operacije u odnosu na koju je ta potencija. Tako ne možemo slučajno zamijeniti $f^3_\circ$ s $f^3_\cdot$. Također, Kartezijev kvadrat grupe cijelih brojeva $\mathbb{Z}^2_\times$ se vidljivo razlikuje od njenog slobodnog kvadrata $\mathbb{Z}^2_\star$.

$\uplus$ je oznaka za disjunktnu uniju — uniju za čije se operande želi naglasiti da su disjunktni. $A = B \uplus C$ znači $A = B \cup C$ & $B \cap C = \emptyset$. Analogno, $\dot\setminus$ je oznaka za potpunu razliku — skupovnu razliku čiji je drugi operand podskup prvog. $A = B \dot\setminus C$ znači $A = B \setminus C$ & $C \subseteq B$ (što je ekvivalentno s $B = A \uplus C$).

Gdje se domena funkcije podrazumijeva, često se funkcija f piše kao $x \mapsto f(x)$. Tako je općeniti zapis za funkciju $f : A \to B; x \mapsto f(x)$. Identiteta $(x \mapsto x)$ na skupu S označava se s 1_S, dok se karakteristična funkcija skupa S označava s χ_S. Domena funkcije f označava se s $\mathsf{Dom} f$, a slika s $\mathsf{im} f$. Polinomi se shvaćaju kao posebni izrazi s nekim istaknutim varijablama. Oznaka za polinom je oblika $p(x)$, dok je p polinomska funkcija $x \mapsto p(x)$. Skup svih polinomâ u varijabli x, s koeficijentima iz skupa S, označava se sa $S[x]$.

Neke skraćenice u tekstu su "akko" za logičku ekvivalenciju ("ako i samo ako"), te "BSOMP" za frazu "bez smanjenja općenitosti možemo pretpostaviti" (nastavak zaključivanja je pod danom pretpostavkom, dakle specijalni slučaj, dok se ostali slučajevi očitom ili navedenom supstitucijom svode na taj). "$\square$" je oznaka za kraj dokaza. Riječ "permutacija" se koristi za bijekciju skupa na samog sebe.

Grupa svih permutacijâ skupa S označava se s $\mathcal{G}r(S!)$. Općenito, $\mathcal{G}r(S)$ označava skup S, organiziran u grupu na prirodan način (npr. za $n \in \mathbb{N}$, $\mathcal{G}r(n)$ označava cikličku grupu reda n, u kojoj se operacija — zbrajanje modulo n — označava s $+_n$). $\mathcal{G}r$ se ponekad ispušta, ako je iz konteksta jasno da se radi o grupi. Slično, $\langle S \rangle_{\mathcal{G}r}$ označava grupu generiranu skupom S, unutar neke podrazumijevane grupe. Ako želimo naglasiti u kojoj se grupi G radi, možemo pisati $\langle S \rangle_{\leq G}$.

$\mathbb{N}$ je oznaka za skup svih konačnih ordinalâ, dakle $0 \in \mathbb{N}$ ($\mathbb{N}$ je ω s aritmetikom). Za skup prirodnih brojeva bez 0, oznaka je $\mathbb{N}^*$. Općenito, za $A \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, $A^* := A \dot\setminus \{0\}$. $\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\}$.

W. Zaključak

· *Grci:* Kako da se riješimo kuge?
· *Proročište u Delfima:* Sagradite novi oltar,
dvostruko veći od sadašnjeg.

· *Banach i Tarski:* Smijemo li koristiti Aksiom izbora?[V]

Literatura

[1] Discovering Modern Set Theory . I, 9.4; W. Just & M. Weese; AMS 1996.
[2] The Banach-Tarski Paradox; Stan Wagon; Cambridge University Press 1985., 1993., 1999.
[3] Algebra, I & II; Thomas W. Hungerford; Springer-Verlag 1974., 1996.

Poznavatelj onoga što je u današnjoj matematici napravljeno u vezi i oko Banach–Tarskijevog paradoksa vjerojatno će primijetiti da su neke stvari dokazane zaobilazno, neke s previše tehničkih detaljâ koji su se mogli izbjeći, a neke i nisu bile strogo potrebne za glavni cilj — dokaz jakih verzijâ Banach–Tarskijevog i von Neumannovih teorema. Glavni razlog za to je nedostatak odgovarajuće literature. Naime, za vrijeme pisanja prvog dijela rada (sâm Banach–Tarskijev teorem) imao sam na raspolaganju samo [1] — kasnije sam dobio [2], i tada odlučio proširiti opseg rada na niže dimenzije i razne druge generalizacije.

[1] je sjajna knjiga, no u njoj je Banach–Tarskijev teorem (i to samo slaba verzija, za kugle) samo ilustracija posljedice Aksioma izbora, dakle usputni rezultat, kojem je posvećeno nekoliko stranicâ i, naravno, mnogi detalji u dokazu su preskočeni. Posljedica toga je da sam mnoge rezultate morao sam dokazati, i pri tome nisam svaki put odabrao najelegantniji pristup. No logički je dokaz u redu i potpun, osim jednog detalja u lemi 4, što se može riješiti i na alternativni način, kako je pokazano u odjeljku `L`. Također, u [2] sam našao nekoliko sitnih previdâ, koje sam (nadam se, uspješno) "zakrpao" ovdje.

Usprkos tome, mislim da je [2] vrlo dobra knjiga, i preporučio bih je svakom tko želi steći potpunije znanje o Banach–Tarskijevom i ostalim sličnim teoremima. Ono što su bili nepovezani (ili slabo povezani) rezultati iz raznih granâ matematike, u toj knjizi je složeno u prilično potpunu i koherentnu sliku. Oko jednog "čisto-matematičkog" teorema izgrađena je čitava teorija, koja povezuje geometriju, algebru i teoriju mjere, i koja je već počela nalaziti svoje primjene kako u ostalim područjima matematike (osnove matematike, optimizacija, složenost,. . .), tako i u kvantnoj fizici[W]. Ima mnogo neriješenih (čak vrlo elementarno zadanih) problemâ, mnogo prostora za generalizaciju i unifikaciju, te za upotrebu i razvoj modernih tehnika dokazivanja, kako "čisto" matematičkih, tako i kompjuterskih.

[V] Aluzija na klasični nerješivi problem (duplikacija kocke ravnalom i šestarom u euklidskom smislu) je dublja nego što na prvi pogled može izgledati: u teoriji jednakosastavljivosti postoji, još uvijek neriješen i smatran vrlo teškim, problem popularno zvan "kvadratura kruga", koji postavlja pitanje je li jedinični krug jednakosastavljiv, koristeći izometrije ravnine, s kvadratom stranice $\sqrt{\pi}$. Zanimljivo je da je za geometrijsku jednakosastavljivost (vidjeti fusnotu `I`) problem riješen — negativno.

[W] Iako (još) ne možemo očekivati konkretnu tehničku izvedbu "replikatora" na makro-razini, neki rezultati teorije jednakosastavljivosti nam mogu pomoći u razumijevanju nekih pojavâ koje na to podsjećaju u kvantnom mikro-svijetu, gdje ne vrijede uobičajeni "klasični" zakoni o očuvanju mase ili volumena.

Iako su kroz povijest mnogi vidjeli ulogu Banach–Tarskijevog “paradoksa” samo kao ilustraciju koliko kontraintuitivne neke posljedice Aksioma izbora mogu biti, danas je ta uloga mnogo šira i obuhvaća dobivanje mnogih dubokih rezultata, prvenstveno u teoriji grupâ i teoriji mjere. Teorija jednakosastavljivosti je jedna od onih mladih teorijâ u kojima se praktički svaka matematička ideja može korisno upotrijebiti. Zato predstavlja vrlo dobar primjer unutarnje matematičke povezanosti, i pokazuje da čak i danas, s mnogim vrlo specijaliziranim granama matematike, postoje rezultati koji zahtijevaju “poprečne presjeke” velike širine i dubine.

K r a j

Vedran Čačić

PMF-MO, Bijenička 30, Zagreb

E-mail address: veky@student.math.hr