Vladimir Ćepulić

Darko Žubrinić

1.

Matematička logika
Realni i kompleksni brojevi

Što je matematika? Čime se bavi? Sama riječ dolazi od grčke riječi $\mu\alpha\vartheta\eta\mu\alpha$ (mathema) — znanje, u množini $\mu\alpha\vartheta\eta\mu\alpha\tau\alpha$ (mathémata) — znanja, znanost, posebice matematika. Od svojih početaka matematika se bavila količinskim i položajnim odnošajima, što ne iscrpljuje sav njezin sadržaj. Moglo bi se reći, da matematika proučava sve što se može istraživati "matematičkom metodom", to jest polazeći od nekih temeljnih činjenica, postavaka *logičkim zaključivanjem* dolaziti do novih. Polazne činjenice sažimlju se u sustavu *aksioma* (grč. $\alpha\xi\iota o\varsigma$, áksios — dostojan, a iz njih se logičkim zaključivanjem — *dokazima* dolazi do novih činjenica, koje se izriču u obliku *stavaka* (teorema). Stavak se redovito sastoji od pretpostavaka i tvrdnja. Radi lakšeg izražavanja, za nove se pojmove uvode kratki nazivi u *definicijama*. Zavisno o objektima koji se proučavaju, matematika se dijeli na pojedine teorije — teoriju skupova, brojeva, funkcija i t.d. Sadržaj pojedine teorije tvore pripadni aksiomi, definicije, te stavci s dokazima.

Temeljne oznake

Podsjetimo se na neke važne skupove, koje znamo iz srednje škole, a koji će nam stalno biti potrebni:

1. $\mathbf{N} = \{1, 2, 3, ...\}$ — skup prirodnih brojeva
2. $\mathbf{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ — skup cijelih brojeva
3. $\mathbf{Q} = \{\frac{a}{b} \mid a, b \in \mathbf{Z},\ b \neq 0\}$ — skup racionalnih brojeva, cjelobrojnih razlomaka
4. $\mathbf{R}$ — skup realnih brojeva koji možemo predočiti brojnim pravcem. Svakoj njegovoj točki pridružen je neki realni broj i obratno, svakom broju neka točka

Za zbroj i umnožak brojeva imamo oznake:

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + ... + a_n, \quad \prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot ... \cdot a_n.$$

Znakom $:=$ iskazuje se, da je izraz sa strane dvotočja oznaka za izraz s druge strane jednakosti.

1.1. Sudovi

Temeljni pojam matematičke logike je *sud* — izricanje neke tvrdnje o nekim objektima. Sudove obično označujemo slovima, na pr.

$$a : "5 > 3", \quad b : "2 > 7".$$

Sud a je *istinit*, a sud b je *lažan*. Svakom je sudu pridijeljena jedna i samo jedna od tih dviju *vrijednosti istinitosti*: T (engl. true-istinit) ili F (engl. false-lažan). Za sud x označujemo njegovu vrijednost istinitosti s $v(x)$. Dakle je $v(a) = T$, $v(b) = F$.

Sudovima se bavi *algebra sudova*. Ona ih promatra samo s obzirom na njihovu istinitost, a ne i sadržaj. Stoga kraće pišemo $a = T$, $b = F$. Uz T i F rabe se i druge oznake, na pr. $\top$ ("te") i $\perp$ ("ne te"), 1 i 0 i t.d.

Logičke operacije

Iz sudova tvorimo nove sudove logičkim operacijama:

Definicija 1. Neka su x i y sudovi. Logičkim operacijama:
1. $\neg$ ("non", nije) — negacija,
2. $\wedge$ ("et", i) — konjunkcija,
3. $\vee$ ("vel", ili) — disjunkcija,
4. $\Rightarrow$ ("implicat", ima za posljedicu) — implikacija,
5. $\Leftrightarrow$ ("aequivalet", jednakovrijedno je s) — ekvivalencija

dobivamo iz njih nove oznake: $\neg x$, $x \wedge y$, $x \vee y$, $x \Rightarrow y$, $x \Leftrightarrow y$.

Istinitosti tih sudova definiraju se u ovisnosti o istinitosti sastavnica x, y ovako:

x	$\neg x$
T	F
F	T

x	y	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \Leftrightarrow y$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Time su definirane i same logičke operacije.

Primjedba 1. 1) Konjunkcija $x \wedge y$ je istinita jedino ako su oba suda x, y istinita.

2) U disjunkciji $x \vee y$ je " $\vee$ " t.zv. *uključni ili* sa značenjem: ili x ili y ili oba. Stoga je disjunkcija lažna jedino kad su oba suda x i y lažna.

3) Implikacija $x \Rightarrow y$ čita se "iz x slijedi y", "ako je x, onda je y", te se x zove *pretpostavka*, y *tvrdnja*. Smatra se u matematici lažnom jedino ako je pretpostavka x istinita, a tvrdnja y lažna. Sve drugo je "u redu", jer se za slučaj da x nije (istinit) ništa nije tvrdilo. Ako iz x slijedi y kažemo još da je x *dostatan uvjet za* y, jer čim je x onda je i y, a da je y *nuždan uvjet za* x, jer ne može biti x, a da nije y, ako $x \Rightarrow y$. Implikacija $x \Rightarrow y$ zove se još i zaključak.

4) Ekvivalenciju $x \Leftrightarrow y$ čitamo "x je onda i samo onda, ako je y", "x je točno onda kad je y", "x je nuždan i dostatan uvjet za y". Ekvivalencija je istinita točno onda kad su x i y jednake istinitosti, t.j. oba istinita ili oba lažna.

Primjer 1. *a*) $x^2 > 1$ je nuždan uvjet za $x > 1$

b) $x < -2$ je dostatan uvjet za $x^2 > 4$

c) $|x| > 2$ je nuždan i dostatan uvjet za $x^2 > 4$.

S pomoću logičkih operacija i zagrada tvorimo složene sudove — *formule algebre sudova*, na pr. $\neg(x \wedge \neg y)$, $(x \Rightarrow y) \vee (y \Rightarrow x)$.

Za svaki *slog* (izbor) *istinitosti* sudova sastavnica neke formule jednoznačno je određena istinitost formule. To se pridruživanje zove *Booleova* ili *logička funkcija*, a prikazujemo ju t.zv. *tablicom istinitosti*.

Primjer 2. Naći Booleovu fukciju za $\neg(x \wedge \neg y)$

x	y	$\neg y$	$x \wedge \neg y$	$\neg(x \wedge \neg y)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

Vidimo da $\neg(x \wedge \neg y)$ i $x \Rightarrow y$ imaju iste Booleove funkcije.

Za formule koje imaju iste Booleove funkcije kažemo da su *istovrijedne* ili *logički ekvivalentne*, oznakom $\equiv$.

Na pr. $x \Rightarrow y \equiv \neg(x \wedge \neg y) \equiv \neg x \vee y$ (provjeriti!)

Navest ćemo još neke važnije istovrijedne formule.

Stavak 1. *Vrijedi:*
1. $\neg(\neg x) \equiv x$ — *pravilo dvostruke negacije*
2. $x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$, $x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$ — *distributivnost*
3. $\neg(x \wedge y) \equiv \neg x \vee \neg y$, $\neg(x \vee y) \equiv \neg x \wedge \neg y$ — *De Morganove formule*
4. $x \Leftrightarrow y \equiv (x \Rightarrow y) \wedge (y \Rightarrow x)$
5. $x \Rightarrow y \equiv \neg y \Rightarrow \neg x$ — *obrat po kontrapoziciji*
6. $\neg(x \Rightarrow y) \equiv x \wedge \neg y$.

Dokaz. S pomoću tablica istinitosti.

Zamjenom formule ili njezinog dijela s istovrijednim izrazom dobivamo novu formulu istovrijednu s prvotnom.

Primjer 3. $\neg(x \Rightarrow y) \equiv \neg(\neg(x \wedge \neg y)) \equiv_{1.} x \wedge \neg y$.

Primjer 4. Naći Booleovu funkciju za $(x \Rightarrow y) \vee (y \Rightarrow x)$.

x	y	$x \Rightarrow y$	$y \Rightarrow x$	$(x \Rightarrow y) \vee (y \Rightarrow x)$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

Ova formula istinita je za sve slogove istinitosti.

Ako je neka formula istinita za sve slogove istinitosti, kažemo da je *identički istinita* ili *tautologija* ($\equiv T$). Ako je pak lažna za sve slogove istinitosti kažemo da je *identički lažna* ($\equiv F$).
Identički istinite formule temelj su logičkoga zaključivanja.
Navodimo neke važnije tautologije:

Stavak 2. *Sljedeće formule su identički istinite:*
1. $(x \wedge (x \Rightarrow y)) \Rightarrow y$ *(modus ponens)*
2. $((x \Rightarrow y) \wedge \neg y) \Rightarrow \neg x$ *(modus tollens)*
3. $((\neg x \Rightarrow y) \wedge \neg y) \Rightarrow x$ *(dokaz iz protuslovlja)*
4. $((x \Rightarrow y) \wedge (y \Rightarrow z)) \Rightarrow (x \Rightarrow z)$ *(zakon silogizma)*

Dokaz. S pomoću tablica istinitosti ili zamjenama po istovrijednosti.

1.2. Predikati

Jednostavni sudovi obično izriču neka *svojstva objekata*, koji se promatraju ili *odnošaje*, relacije *među njima*. Skup svih promatranih objekata neke teorije zvat ćemo *univerzalnim skupom* i označavat ćemo s U, a za objekte iz U kažemo da su njegovi elementi.

Primjer 5. Neka je $U = \mathbf{N}$. Rečenice kao $P(x)$: "$x^2 < 5$", $Q(x_1, x_2, x_3)$: "$x_1 + x_2 = x_3$" nisu ni istinite ni lažne, dakle nisu sudovi, ali uvrštenjem konkretnih x, x_1, x_2, x_3 iz U postaju sudovi. Na pr. $P(2)$: "$2^2 < 5$" je istinit, $P(3) = F$, $Q(1,4,5) = T$ $(1+4=5)$, a $Q(5,1,4) = F$ $(5+1 \neq 4)$.

Takve rečenice, "sudne forme", zovu se *predikati*.

Definicija 2. Sudna forma $P(x_1, x_2, ..., x_n)$ koja za svaki slog (izbor) elemenata $x_1, x_2, ..., x_n$ univerzalnog skupa U postaje sud zove se *n-mjesni predikat na U*. Skup C_P svih slogova $(x_1, x_2, ..., x_n)$ elemenata iz U za koje je $P(x_1, x_2, ..., x_n)$ istinit zove se *karakterističan skup* predikata P. On potpuno određuje P u logičkom smislu, t.j. s obzirom na istinitost.

Primjer 6. Neka je $U = \mathbf{N}$. Za predikat $P(x,y)$: "$x + y = 5$" je $C_P = \{(1,4),(2,3),(3,2),(4,1)\}$.

Iz predikata možemo tvoriti nove predikate logičkim operacijama.

Primjer 7. Neka je $P(x)$: "$x \geq 2$", $Q(x)$: "$x \leq 5$". Definiramo novi predikat $R(x) = P(x) \wedge Q(x)$: "$x \geq 2$" $\wedge$ "$x \leq 5$", t.j. "$2 \leq x \leq 5$". Sada je na pr. $R(3) = P(3) \wedge Q(3)$ ="$3 \geq 2$" $\wedge$ "$3 \leq 5$"$= T \wedge T = T$, $R(7) = P(7) \wedge Q(7) = T \wedge F = F$. Očevidno je $C_R = \{2,3,4,5\}$.

Definicija 3. Kažemo da je predikat $P(x_1, ..., x_n)$ *identički istinit* ($\equiv T$), ako je istinit za sve slogove elemenata od U, a da je *identički lažan*, ako je lažan za sve slogove elemenata od U.

Primjer 8. Za $U = \mathbf{N}$ je predikat $P(x,y,z)$: "$x^2 + y^2 + z^2 < 3$" identički lažan, jer niti najmanja vrijednost lijeve strane $1^2 + 1^2 + 1^2 = 3$ nije manja od 3. Dakle je $P(x,y,z) \equiv F$.

Primjer 9. Za $U = \mathbf{R}$ je $Q(x,y)$: "$x^2 + y^2 \geq 0$" uvijek istinit, t.j. identički istinit, $Q(x,y) \equiv T$.

U logici važnu ulogu imaju "kvantifikatori" $\forall$ i $\exists$. Oni iz 1-mjesnih predikata tvore sudove.

Definicija 4. Neka je $P(x)$ predikat na U. Sud $\forall x P(x)$ ("za svaki x je $P(x)$") je istinit, ako je $P(x) \equiv T$, t.j. ako je $P(x)$ identički istinit. Sud $\exists x P(x)$ ("za neki x je $P(x)$") je istinit, ako nije $P(x) \equiv F$, t.j. ako sud $P(x)$ nije identički lažan, dakle ako opstoji $a \in U$ za koji je $P(a)$ istinit. Možemo to zapisati i ovako: $\forall x P(x) := (P(x) \equiv T)$, $\exists x P(x) := \neg(P(x) \equiv F)$.

Primjer 10. *a*) Za $U = \mathbf{R}$ je $\forall x(x^2 \geq 0) = T$; $\exists x(x^2 = 2) = T$ - za $x = \sqrt{2}$ ili $x = -\sqrt{2}$ je $x^2 = 2$.

b) Za $U = \mathbf{Q}$ je $\exists x(x^2 = 2) = F$, jer $\sqrt{2}$ i $-\sqrt{2}$ nisu racionalni brojevi.

Stavak 3. *Neka je $P(x)$ bilo koji jednomjesni predikat. Onda vrijedi:*

1. $\neg\forall x P(x) \equiv \exists x \neg P(x)$
2. $\neg\exists x P(x) \equiv \forall x \neg P(x)$
3. $\forall x P(x) \Rightarrow \exists x P(x)$

Dokaz. 1. Ako nešto nije za svaki x, onda za neki x nije.

2. Slijedi iz 1. zamjenjujući $P(x)$ s $\neg P(x)$, a zatim negirajući obje strane.

3. Očevidno.

Tvrdnje 1. i 2. zovu se De Morganove formule za predikate. Veoma su važne pri negaciji formula s kvantifikatorima. Negacija preskače kvantifikator tako da ga mijenja u onaj drugi.

Primjer 11. Neka je $U = \{2,3,4\}$, $P(x,y)$: "$x \geq y$". Vidimo da je $C_P = \{(2,2),(3,2),(3,3),(4,2),(4,3),(4,4)\}$. Sada je izraz $\forall x P(x,y)$ jednomjesni predikat $\forall x P(x,y) = P_1(y)$, jer za svaki konkretni y postaje sud. Naime:

za $y = 2$ je $P_1(2) = \forall x(x \geq 2) = T$,

za $y = 3$ je $P_1(3) = \forall x(x \geq 3) = F$ (uzimljući $x = 2$),

za $y = 4$ je $P_1(4) = \forall x(x \geq 4) = F$ (uzimljući $x = 2$ ili $x = 3$).

Vidimo da je $\forall y P_1(y) = F$, $\exists y P_1(y) = T$, jer je $P_1(3) = F, P_1(2) = T$. To možemo zapisati i u obliku $\forall y \forall x P(x,y) = F$, $\exists y \forall x P(x,y) = T$.

Vrijedi i općenito: Opetovanom primjenom po jednog kvantifikatora za svako mjesto x_i predikata $P(x_1,\ldots,x_n)$ dobivamo iz n-mjesnog predikata sud.

Primjer 12. $U = \mathbf{R}$;

1. $\forall x \exists y(x + y = y) = F$, jer ovdje x mora biti 0,
2. $\forall x\, \exists y\, (x + y = 0) = T$, ovdje je $y = -x$,
3. $\exists x\, \forall y\, (x + y = y) = T$, takav je $x = 0$.

1.3. Skupovi i preslikavanja

Neka je U univerzalni skup, ukupnost promatranih objekata. Kažemo, da je na U definiran *skup* S, ako se za svaki objekt x iz U znade *pripada* li skupu S, oznakom $x \in S$, ili mu *ne pripada*, oznakom $x \notin S$. Svakom dakle skupu S možemo pridružiti njegov *predikat pripadanja* $S(x)$, koji je istinit za one x koji pripadaju S, a lažan za ostale. S je dakle karakterističan skup svoga predikata, $S = C_{S(x)}$. Često pišemo $S = \{x \mid S(x)\}$, što čitamo: "S je skup svih x (iz U), za koje je (istinit) $S(x)$".

Primjer 13. Neka je $U = \mathbf{N}$, $S = \{1,2,3\} = \{x \mid x < 4\} = \{x \mid x^2 < 12\}$. Vidimo, da različiti predikati mogu definirati isti skup.

Primjer 14. Za $U = \mathbf{R}$ označujemo $\mathbf{R}^+ = \{x \mid x > 0\}$, ${\mathbf{R}_0}^+ = \{x \mid x \geq 0\}$.

Definicija 5. Neka su S, S_1, S_2 skupovi definirani na U. Definiramo operacije na skupovima:

a) $\overline{S} := \{x \mid x \notin S\} = \{x \mid \neg(x \in S)\}$ — *komplement* ili dopunak skupa S,
b) $S_1 \cap S_2 := \{x \mid x \in S_1 \wedge x \in S_2\}$ — *presjek* skupova S_1 i S_2,
c) $S_1 \cup S_2 := \{x \mid x \in S_1 \vee x \in S_2\}$ — *unija* ili spoj skupova S_1 i S_2,
d) $S_1 \setminus S_2 := \{x \mid x \in S_1 \wedge x \notin S_2\}$ — *razlika* skupova S_1 i S_2,

i relacije među skupovima:

e) $S_1 \subseteq S_2 \equiv \forall x(x \in S_1 \Rightarrow x \in S_2)$ — S_1 je podskup od S_2,
f) $S_1 = S_2 \equiv \forall x(x \in S_1 \Leftrightarrow x \in S_2)$ — skup S_1 je jednak skupu S_2.

Primjedba 2. Za svaki skup S je $\emptyset \subseteq S$ — prazan skup je podskup svakoga skupa.

Slično kao u slučaju dvaju skupova definiramo presjek i uniju više skupova $S_1, S_2, \ldots, S_n$:

1. presjek

$$\bigcap_{i=1}^{n} S_i := S_1 \cap S_2 \cap \ldots \cap S_n = \{x \mid x \in S_1 \wedge x \in S_2 \wedge \ldots \wedge x \in S_n\},$$

2. unija

$$\bigcup_{i=1}^{n} S_i := S_1 \cup S_2 \cup \ldots \cup S_n = \{x \mid x \in S_1 \vee x \in S_2 \vee \ldots \vee x \in S_n\}.$$

Opisat ćemo još jednu konstrukciju koja se često pojavljuje u matematici:

Definicija 6. Neka su $S_1, S_2, ..., S_n$ skupovi na U.
Skup *poredanih n-teraca* (slogova)

$$S_1 \times S_2 \times ... \times S_n := \{(x_1, x_2, ..., x_n) \mid x_1 \in S_1 \wedge x_2 \in S_2 \wedge ... \wedge x_n \in S_n\}$$
$$= \{(x_1, x_2, ..., x_n) \mid \forall i\, x_i \in S_i\}$$

zove se *Kartezijev umnožak* (produkt) skupova $S_1, S_2, ..., S_n$.

Primjer 15. $S_1 = \{1, 4\}$, $S_2 = \{2, 3, 5\}$,
$S_1 \times S_2 = \{(1, 2), (1, 3), (1, 5), (4, 2), (4, 3), (4, 5)\}$.

Primjer 16. Skup $\mathbf{R}^2 := \mathbf{R} \times \mathbf{R} = \{(x, y) \mid x \in \mathbf{R} \wedge y \in \mathbf{R}\}$ možemo predočiti kao skup točaka ravnine XOY.

Preslikavanja

Jedan od najvažnijih pojmova u matematici je pojam preslikavanja.

Definicija 7. Neka su S_1 i S_2 skupovi na U. Kažemo da je f *preslikavanje skupa S_1 u skup S_2*, oznakom $f : S_1 \to S_2$, ako je svakom $x \in S_1$ pridružen nekim propisom f jedincati $y \in S_2$, oznakom $f : x \mapsto y$ ili kraće $y = f(x)$.

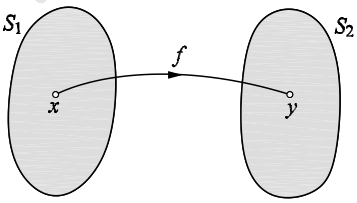
Pri tom se y zove *f-slika originala x*. S_1 i S_2 zovu se još i polazni dotično dolazni skup preslikavanja f. Dva preslikavanja $f : S_1 \to S_2$ i $g : T_1 \to T_2$ su jednaka, $f = g$, onda i samo onda, ako je $S_1 = T_1$, $S_2 = T_2$, te za sve $x \in S_1$ vrijedi $f(x) = g(x)$.

Neka je $f : S_1 \to S_2$. Skup S_1 zove se *područje definicije* ili original preslikavanja f, a skup $f(S_1) := \{f(x) \mid x \in S_1\} \subseteq S_2$ je *područje vrijednosti* ili *slika od f*. Drugi su nazivi područje i protupodručje, domena i kodomena. Ta područja označujemo i oznakama:

$$D(f) = S_1,\ f(D) = f(D(f)) = f(S_1).$$

Preslikavanja kod kojih je $S_1 \subseteq \mathbf{R}, S_2 = \mathbf{R}$ zovu se realne funkcije realne varijable. Ukoliko je realna funkcija zadana nekim matematičkim izrazom, zovemo njezinim (prirodnim) područjem definicije skup realnih brojeva na kojem je taj izraz definiran.

Primjer 17. Neka je $U = \mathbf{R}$.
a) Za $f(x) = \sqrt{x}$ je $D(f) = \mathbf{R}_0{}^+$, a također $f(D) = \mathbf{R}_0{}^+$ (razlikujemo funkcije $\sqrt{x}$ i $-\sqrt{x}$),
b) $f(x) = x^2 + 1$, $D(f) = \mathbf{R}$, $f(D) = [1, +\infty\rangle$,
c) $f(x) = \sin x$, $D(f) = \mathbf{R}$, $f(D) = [-1, 1]$.



Sl. 1.1.

U daljnem ćemo iz praktičnih razloga uz kvantifikatore i pripadajuće elemente pisati skupove iz kojih su ti elementi, ukoliko se kvantifikator odnosi samo na podskup od U. U tom smislu je

$$(\forall x \in S)P(x) \equiv \forall x(x \in S \Rightarrow P(x))$$
$$(\exists x \in S)P(x) \equiv \exists x(x \in S \wedge P(x)).$$

Definicija 8. Neka je $f : S_1 \to S_2$, t.j. $D(f) = S_1$, $f(D) \subseteq S_2$.

$a)$ Preslikavanje $f : S_1 \to S_2$ je *surjektivno* (surjekcija) ili preslikavanje S_1 *na* S_2, ako je $f(D) = S_2$, t.j. ako je svaki $y \in S_2$ slika nekoga $x \in S_1$, dakle:

$$\forall y \in S_2\ \exists x \in S_1\ f(x) = y.$$

$b)$ Preslikavanje $f : S_1 \to S_2$ je *injektivno* (injekcija), ako različiti originali imaju uvijek različite slike, t.j. ako

$$\forall x_1, x_2 \in S_1 \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2). \qquad (*)$$

Poradi $a \Rightarrow b \equiv \neg b \Rightarrow \neg a$ $(*)$ je ekvivalentno s

$$\forall x_1, x_2 \in S_1\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2. \qquad (**)$$

$c)$ Kažemo da je $f : S_1 \to S_2$ *bijektivno* preslikavanje (bijekcija), ako je injektivno i surjektivno, t.j. ako vrijedi:

1. $S_2 = \{f(x) \mid x \in S_1\}$ t.j. $\forall y \in S_2\ \exists x \in S_1\ y = f(x)$,
2. $\forall x_1 \in S_1\ \forall x_2 \in S_1\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Primjer 18. $a)$ x^n za neparne n, e^x, $\ln x$ su injektivne funkcije na prirodnom području definicije

$b)$ x^n za parne n, $\sin x$, $\cos x$, $\operatorname{tg} x$, $\operatorname{ctg} x$ nisu injektivne

$c)$ $f : \mathbf{R} \to \mathbf{R}$, $f(x) = e^x$ nije surjektivna. Naime, $f(D) = \{e^x \mid x \in \mathbf{R}\} = \langle 0, +\infty \rangle = \mathbf{R}^+ \neq \mathbf{R}$.

$d)$ $g : \mathbf{R}^+ \to \mathbf{R}$, $g(x) = \ln x$ je surjektivna, $g(D) = \{\ln x \mid x \in \mathbf{R}^+\} = \mathbf{R}$ i injektivna, dakle je g bijekcija.

Definicija 9. Neka je $f : S_1 \to S_2$, $X \subseteq S_1$. Onda je

$$f(X) := \{f(x) \mid x \in X\} \ \ f\text{-slika podskupa } X.$$

Očevidno je $f(X) \subseteq S_2$.

Ograničimo li se u djelovanju f na podskup X, dobivamo novo preslikavanje — *restrikciju* ili *suženje preslikavanja* f *na* X, oznakom $f|_X$. Dakle je:

$$f|_X : X \to S_2, \text{ pri čemu je } (f|_X)(x) = f(x) \text{ za svaki } x \in X.$$

Za $g = f|_X$ je dakle $D(g) = X$, $g(D) = f(X)$.

Primjer 19. *a)* Što znači da $f : S_1 \to S_2$ nije surjekcija?
De Morganove formule za predikate daju nam:

$$\neg(\forall y \in S_2)(\exists x \in S_1)(y = f(x)) \equiv (\exists y \in S_2)(\forall x \in S_1)(y \neq f(x)),$$

t.j. ima neki $y \in S_2$ koji nije slika nijednoga $x \in S_1$.

b) Što znači da $f : S_1 \to S_2$ nije injekcija?
Uzimljući u obzir $\neg(a \Rightarrow b) \equiv a \wedge \neg b$ imamo:

$$\neg(\forall x_1 \in S_1)(\forall x_2 \in S_1)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)) \equiv$$
$$\equiv (\exists x_1 \in S_1)(\exists x_2 \in S_1)(x_1 \neq x_2 \wedge f(x_1) = f(x_2)),$$

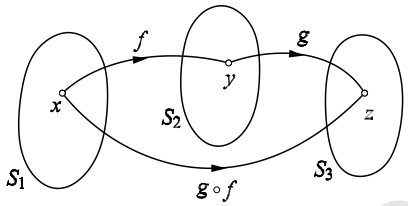
t.j. postoje (barem) dva različita elementa u S_1, koja f preslikava u isti element iz S_2.

Kompozicija funkcija

Uz neke uvjete iz preslikavanja se izvode nova t.zv. kompozicijom.

Definicija 10. Neka su S_1, S_2 i S_3 skupovi, te $f : S_1 \to S_2, g : S_2 \to S_3$. *Kompozicija* ili *sastavak* $g \circ f$ tih preslikavanja je preslikavanje: $g \circ f : S_1 \to S_3$, definirano ovako:

$$\forall x \in S_1 \ (g \circ f)(x) = g[f(x)].$$



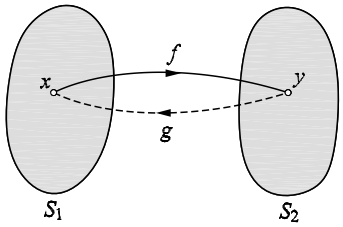
Sl. 1.2.

Primjedba 3. 1) Kompozicija bijekcija je opet bijekcija. (pokazati!)

2) Kompozicija preslikavanja je asocijativna, t.j. za $f : S_1 \to S_2, g : S_2 \to S_3, h : S_3 \to S_4$ vrijedi: $h \circ (g \circ f) = (h \circ g) \circ f : S_1 \to S_4$. (pokazati!)

3) Bijektivno preslikavanje $f : S \to S$ zove se *permutacija* ili *premjestba skupa* S ili kratko: bijekcija na S. Permutacija $id_S : S \to S$, $\forall x \in S \ id_S(x) = x$, koja svaki x iz S preslikava u njega samoga zove se *identičko preslikavanje* ili *identitet* na S. Očevidno za svaki $f : S_1 \to S_2$ vrijedi $f \circ id_{S_1} = id_{S_2} \circ f = f$.

Definicija 11. Neka je $f : S_1 \to S_2$. Preslikavanje $g : S_2 \to S_1$ zove se *inverzno preslikavanje od* f, ako je: $\forall x \in S_1 \quad g[f(x)] = x$, $\forall y \in S_2 \quad f[g(y)] = y$, t.j. ako je $g \circ f = id_{S_1}, f \circ g = id_{S_2}$ (vidi sliku):



Sl. 1.3.

Važne su činjenice:

Stavak 4. *Za preslikavanje $f : S_1 \to S_2$ opstoji inverzno preslikavanje $g : S_2 \to S_1$ onda i samo onda, ako je f bijekcija. U tom slučaju je i g bijekcija. Inverzno preslikavanje je jedincato i označujemo ga $f^{(-1)}$.*

Dokaz. 1) Pretpostavimo, da je g inverzno preslikavanje od f. Za $y \in S_2$ je $y = (f \circ g)(y) = f(g(y)) = f(x)$, uz $x = g(y)$. Dakle je f surjekcija. Ako su $x_1, x_2 \in S_1$ i $f(x_1) = f(x_2)$, onda je $g[f(x_1)] = g[f(x_2)]$, pa je $x_1 = x_2$, jer je $g \circ f = id_{S_1}$. Stoga je f injekcija. Dokazali smo da je f bijekcija. Kada bi i $h : S_2 \to S_1$ bilo inverzno preslikavanje za f, bilo bi za svaki $y \in S_2$, te x za koji je $f(x) = y$ (surjektivnost od f !): $h(y) = h[f(x)] = x = g[f(x)] = g(y)$, pa je $h = g$. Stoga je inverzno preslikavanje jedincato.

2) Pretpostavimo, da je f bijekcija. Za svaki $y \in S_2$ opstoji $x \in S_1$ takav da je $f(x) = y$ (surjektivnost od f !) i takav je x samo jedan, jer iz $f(x') = f(x)$ slijedi $x' = x$ (injektivnost). Definiramo $g(y) = x$, za koji je $f(x) = y$. Sad je $g(y) = g[f(x)] = x$ i $f(x) = f[g(y)] = y$, te je $g \circ f = id_{S_1}, f \circ g = id_{S_2}$, dakle je g inverzno preslikavanje od f. Očevidno su g i f međusobno inverzni, pa je po dokazanom i g bijekcija, jer ima inverzno preslikavanje f.

Stavak 5. *Ako su $f : S_1 \to S_2$ i $g : S_2 \to S_3$ bijekcije, onda je*

$$(g \circ f)^{(-1)} = f^{(-1)} \circ g^{(-1)}.$$

Dokaz. Poradi asocijativnosti kompozicije je $(g \circ f) \circ (f^{(-1)} \circ g^{(-1)}) = g \circ (f \circ f^{(-1)}) \circ g^{(-1)} = (g \circ id_{S_2}) \circ g^{(-1)} = g \circ g^{(-1)} = id_{S_2}$ i slično $(f^{(-1)} \circ g^{(-1)}) \circ (g \circ f) = id_{S_1}$. Dakle je $(g \circ f)^{(-1)} = f^{(-1)} \circ g^{(-1)}$.

Primjer 20. Promatramo realne funkcije $f : \mathbf{R} \to \mathbf{R}_0{}^+$, $f(x) = x^2$ i $g = f|_{\mathbf{R}_0{}^+}$. Funkcija f nije injektivna, $f(-x) = f(x) = x^2$, pa nema inverzne funkcije. Funkcija $g = f|_{\mathbf{R}_0{}^+}$ je surjektivna i injektivna, dakle bijektivna, pa ima inverznu funkciju $g^{(-1)} = \sqrt{x}$, $g^{(-1)} : \mathbf{R}_0{}^+ \to \mathbf{R}_0{}^+$.

Stavak 6. *Neka je S neprazan skup. Za sve bijekcije skupa S na sama sebe i njihove kompozicije vrijedi:*

1. *Ako su f i g bijekcije na S, onda je i $f \circ g$ bijekcija na S.*
2. *Ako su f, g, h bijekcije na S, onda je $f \circ (g \circ h) = (f \circ g) \circ h$ -asocijativnost.*
3. *Opstoji "jedinična" bijekcija id_S, takva da je za svaku bijekciju f na S $id_S \circ f = f \circ id_S = f$.*
4. *Za svaku bijekciju $f : S \to S$ opstoji bijekcija $f^{(-1)} : S \to S$ takva da je $f^{(-1)} \circ f = f \circ f^{(-1)} = id_S$.*

Dokaz. Tvrdnje slijede neposredno iz prethodnih rezultata.

1.4. Algebarske strukture — grupa, prsten, polje

Posve slične okolnosti kao navedene u skupu bijekcija skupa S na sama sebe, uz kompoziciju kao operaciju vrijede i u mnogim drugim primjerima skupova s operacijama, te su povod definiranju temeljne algebarske strukture — grupe.

Definicija 12. Neka je na skupu G definirano preslikavanje $\circ : G \times G \to G$, koje svakom poredanom paru (a, b) elemenata iz G pridružuje jednoznačno određeni element $a \circ b$ iz G. Kažemo, da je na G definirana *binarna operacija* $\circ$ ("kružić").

Definicija 13. Kažemo da je neprazan skup G na kojem je definirana binarna operacija $\circ$, *grupa* s obzirom na tu operaciju, ako vrijedi:

1. za sve $a, b, c \in G$ vrijedi $a \circ (b \circ c) = (a \circ b) \circ c$ — asocijativnost
2. opstoji element $e \in G$ takav da za sve $a \in G$ vrijedi $a \circ e = e \circ a = a$. Element e zove se *neutralni element*.
3. za svaki $a \in G$ opstoji $a' \in G$ takav da je $a \circ a' = a' \circ a = e$. Element a' zove se *inverzni element* elementa a.

Ako još vrijedi i

4. za svaki $a \in G$ i $b \in G$ je $a \circ b = b \circ a$
   kažemo da je grupa G *komutativna* ili *abelova*.

Grupu G s operacijom $\circ$ bilježimo $(G, \circ)$.

Lako se pokaže, da su neutralni element i inverzni element za svaki pojedini a jedincati.

Primjedba 4. U slučaju zbrojidbenog zapiska binarne operacije, t.j. za "$\circ$" $\equiv$ "$+$" neutralni element se bilježi kao 0 (ništica, nula), a inverzni element od a kao $-a$ (suprotni element). U slučaju množidbenog zapiska "$\circ$" $\equiv$ "$\cdot$" neutralni element se bilježi kao 1 (jedinica), a inverzni kao a^{-1}.

Primjer 21. Primjeri komutativnih grupa su $(\mathbf{R}, +)$, $(\mathbf{R} \setminus \{0\}, \cdot)$, $(\{1, -1, i, -i\}, \cdot)$ i td. Primjer najmanje nekomutativne grupe je skup bijekcija skupa $S = \{1, 2, 3\}$ na S s obzirom na kompoziciju.

Primjer 22. Skup svih bijekcija na nepraznom skupu S s obzirom na kompoziciju kao binarnu operaciju je, kako smo pokazali, grupa.

Stavak 7. *U grupi $(G, \circ)$ vrijedi:*

1. *Iz $a \circ x = a \circ y$ slijedi $x = y$.*
2. *Iz $x \circ a = y \circ a$ slijedi $x = y$.*
3. *Jednadžba $a \circ x = b$ ima jedincato rješenje $x = a' \circ b$.*
4. *Jednadžba $x \circ a = b$ ima jedincato rješenje $x = b \circ a'$.*
5. $(a \circ b)' = b' \circ a'$.

Dokaz. Na pr. 1. $a \circ x = a \circ y \Rightarrow a' \circ a \circ x = a' \circ a \circ y \Rightarrow e \circ x = e \circ y \Rightarrow x = y$
3. $a \circ x = b \Rightarrow a' \circ a \circ x = a' \circ b \Rightarrow e \circ x = x = a' \circ b$
5. analogno kao kod bijekcije.

Definicija 14. Neprazan skup R na kojem su definirane dvije binarne operacije $+$ i $\cdot$ je *prsten*, oznakom $(R,+,\cdot)$, ako je:

1. $(R,+)$ komutativna grupa
2. Za $a,b \in R$ je $a\cdot(b\cdot c) = (a\cdot b)\cdot c$.
3. Za $a,b,c \in R$ je $(a+b)\cdot c = ac+bc,\ c(a+b) = ca+cb$-distributivnost.

$(R,+,\cdot)$ je *prsten s jedinicom*, ako još vrijedi:

4. U R opstoji element 1 takav da je $a\cdot 1 = 1\cdot a = a$ za svaki $a \in R$.

Primjer 23. Skup cijelih brojeva je prsten $(\mathbf{Z},+,\cdot)$ za operacije zbroja i umnoška i to je prsten s jedinicom.

Definicija 15. Neprazan skup $(R,+,\cdot)$ je polje, ako je

1. $(R,+)$ je komutativna grupa
2. $(R\setminus\{0\},\cdot)$ je komutativna grupa
3. Vrijede zakoni distribucije — za $a,b,c \in R$ je $(a+b)\cdot c = ac+bc,\ c(a+b) = ca+cb$.

Primjer 24. $(\mathbf{Q},+,\cdot)$, $(\mathbf{R},+,\cdot)$, $(\mathbf{C},+,\cdot)$ su polja.

1.5. Relacije na skupu

Definicija 16. Kažemo, da je na skupu S definirana relacija ρ, ako je $\rho \subseteq S\times S$. Za svaki $(x,y) \in S\times S$ je dakle $(x,y)\in\rho$ ("x i y su u relaciji ρ") ili $(x,y)\notin\rho$ ("x i y nisu u relaciji ρ"). Često umjesto $(x,y)\in\rho$ pišemo kraće $x\rho y$ ("x je u relaciji ρ s y").

Primjer 25. Relacija "biti dijete istih roditelja" je relacija na skupu ljudi.

Relacija može imati neka važna svojstva.

Definicija 17. Kažemo da je relacija ρ na skupu S

1. refleksivna, ako je $\forall x\, x\rho x$, t.j. svaki je element u relaciji sam sa sobom
2. simetrična, ako $\forall x\forall y\quad x\rho y \Rightarrow y\rho x$, t.j. ako iz činjenice da su x i y u relaciji slijedi da su i y i x u relaciji — općenito je za relaciju bitan poredak u paru (x,y)
3. antisimetrična, ako $\forall x\forall y\ (x\rho y \wedge y\rho x \Rightarrow y = x)$, t.j. za različite elemente x i y ne može istodobno biti i $x\rho y$ i $y\rho x$
4. tranzitivna, ako $\forall x\forall y\forall z\ (x\rho y \wedge y\rho z \Rightarrow x\rho z)$, t.j. ako iz činjenice da su x i y u relaciji, te y i z u relaciji slijedi da su i x i z u relaciji.

Definicija 18. Relacija koja je refleksivna, simetrična i tranzitivna zove se *relacija ekvivalencije*.

Relacija koja je refleksivna, antisimetrična i tranzitivna zove se *relacija poretka*.

Primjer 26. Relacija "$=$" na $\mathbf{R}$ je relacija ekvivalencije:
1) $\forall a \in \mathbf{R}\ a = a$
2) $a, b \in \mathbf{R}\ a = b \Rightarrow b = a$
3) $a, b, c \in \mathbf{R}\ a = b \wedge b = c \Rightarrow a = c$

Neki drugi primjeri su sličnost trokuta, usporednost pravaca, "biti dijete istih roditelja".

Primjer 27. Na skupu $P(S)$ podskupova skupa S, t.zv. partitivnom skupu skupa S, $P(S) = \{X \mid X \subseteq S\}$ je "$\subseteq$" relacija poretka:
1) $\forall X \subseteq S$ je $X \subseteq X$
2) Ako su $X, Y \subseteq S$ iz $X \subseteq Y$ i $Y \subseteq X$ slijedi $Y = X$
3) Ako su $X, Y, Z \subseteq S$ iz $X \subseteq Y$ i $Y \subseteq Z$ slijedi $X \subseteq Z$.

1.6. Prirodni brojevi. Matematička indukcija. Binomna formula

Skup prirodnih brojeva $\mathbf{N} = \{1, 2, 3, \ldots\}$ čini se jednostavnim, međutim on je neizmjerno složen, pun otvorenih problema.

U matematici se do rezultata često dolazi eksperimentiranjem. Na pr. neka slutnja $A(n)$ koja ovisi o prirodnom broju n pokaže se da je istinita za neke početne prirodne brojeve, na pr. za $n = 1, 2, 3$. Važan problem je može li se istinitost te slutnje dokazati za sve n. O tome govori načelo matematičke indukcije.

Načelo matematičke indukcije se najjednostavnije vidi u dječjoj igri domina. Pretpostavimo da su na čvrstoj podlozi postavljena domina okomito na najmanjoj strani, u slijedu jedno iza drugog, s lijeva na desno, označena redom prirodnim brojevima. Pretpostavimo da su ispunjena ova dva uvjeta:
1) prvo domino palo je na desnu stranu;
2) ako je za bilo koji $n \in \mathbf{N}$ na desno palo n-to domino, onda će na desno pasti i $n+1$-vo domino.

Tvrdnja je da će onda pasti sva domina.

U skupu prirodnih brojeva vrijedi:

Načelo matematičke indukcije

Ako je neka tvrdnja koja ovisi o prirodnom broju n istinita za neki prirodan broj n_0, i ako iz istinitosti te tvrdnje za $n \in \mathbf{N}$ ($n \geqslant n_0$) slijedi da je istinita i za $n+1$, onda je ona istinita i za sve $n \in \mathbf{N}$ koji su veći od n_0.

RAZMIŠLJAMO OVAKO. Označimo tvrdnju s $A(n)$. Pretpostavke su dakle:
1) $A(n_0) = T$, *baza indukcije*;
2) vrijedi $A(n) = T \Rightarrow A(n+1) = T$, *korak indukcije*.

Rabeći 1) i 2) dobivamo da vrijedi $A(n_0) = T \Rightarrow A(n_0+1) = T \Rightarrow A((n_0+1)+1) = A(n_0+2) = T \Rightarrow \ldots \Rightarrow A(n_0+3) = T \Rightarrow \ldots$. Tvrdnja će biti dakle istinita za sve prirodne brojeve veće od n_0.

Primjer 28. Za sve prirodne brojeve n vrijedi

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

Dokažimo to matematičkom indukcijom.

1) Za $n_0=1$ tvrdnja vrijedi, jer je $1=\dfrac{1\cdot 2}{2}$.

2) Pretpostavimo da tvrdnja vrijedi za neki n, tj. $A(n)\equiv T$, dakle da je

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

Onda je

$$\begin{aligned}1+2+\ldots+n+(n+1)&=\frac{n(n+1)}{2}+(n+1)\\&=\frac{n+1}{2}(n+2)=\frac{(n+1)((n+1)+1)}{2},\end{aligned}$$

pa tvrdnja vrijedi i za $n+1$, $A(n+1)\equiv T$.

Time je prema načelu matematičke indukcije tvrdnja dokazana za sve n.

Primjer 29. Dokažimo matematičkom indukcijom da za sve prirodne brojeve n vrijedi

$$1^2+2^2+\ldots+n^2=\frac{1}{6}n(n+1)(2n+1).$$

1) za $n_0=1$ tvrdnja vrijedi, jer je $1^2=\frac{1}{6}\cdot 1\cdot 2\cdot 3$.

2) Pretpostavimo da je $A(n)=T$, tj. da za neki prirodan broj n vrijedi $1^2+2^2+\ldots+n^2=\frac{1}{6}n(n+1)(2n+1)$. Onda je

$$\begin{aligned}1^2+2^2+\ldots+(n+1)^2&=(1^2+2^2+\ldots+n^2)+(n+1)^2\\&=\frac{1}{6}n(n+1)(2n+1)+(n+1)^2\\&=\frac{1}{6}(n+1)[n(2n+1)+6(n+1)]\\&=\frac{1}{6}(n+1)(n+2)(2n+3)\\&=\frac{1}{6}(n+1)((n+1)+1)(2(n+1)+1).\end{aligned}$$

Dakle, $A(n+1)=T$.

Time je dokazano da je formula istinita za sve $n\in\mathbf{N}$.

Binomni koeficijenti

Veliku važnost u matematici, osobito u kombinatorici, imaju *binomni koeficijenti*. Za zadani prirodan broj n i bilo koji $k \in \{0, 1, 2, \ldots, n\}$ definiramo

$$\binom{n}{k} := \frac{n(n-1)\ldots(n-k+1)}{k!}, \quad k = 1, 2, \ldots, n,$$

$$\binom{n}{0} := 1.$$

Ovdje je $k!$ (k faktorijela) broj definiran sa $k! := 1 \cdot 2 \cdot 3 \ldots k$, $0! := 1$. Primijetite da u definiciji binomnog koeficijenta u brojniku imamo padajući umnožak točno k uzastopnih prirodnih brojeva počevši od n, a u nazivniku rastući umnožak k brojeva počevši od 1. Na pr.

$$\binom{n}{1} = \frac{n}{1} = n, \qquad \binom{n}{2} = \frac{n(n-1)}{1 \cdot 2}, \qquad \binom{n}{3} = \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}.$$

Vrlo lako je provjeriti da je

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

odakle odmah slijedi svojstvo simetrije $\binom{n}{k} = \binom{n}{n-k}$. Na pr.

$$\binom{n}{n} = \binom{n}{0} = 1, \qquad \binom{7}{4} = \binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 35.$$

Vrijedi također

$$\boxed{\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}, \quad k = 1, 2, \ldots, n.}$$

Doista,

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n(n-1)\ldots(n-k+1)}{k!} + \frac{n(n-1)\ldots(n-(k-1)+1)}{(k-1)!} \\
&= \frac{n(n-1)\ldots(n-k+2)[(n-k+1)+k]}{k!} \\
&= \frac{(n+1)n(n-1)\ldots((n+1)-k+1)}{k!} = \binom{n+1}{k}.
\end{aligned}$$

Ta relacija nam daje i poznati "Pascalov trokut" binomnih koeficijenta:

$$\boxed{\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
 & \ldots & & \ldots & & \ldots & & \ldots &
\end{array}}
\qquad
\boxed{\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & \ldots & & \ldots & & \ldots & & \ldots &
\end{array}}$$

Po lijevom i desnom rubu "trokuta" su jedinice, a svaki unutarnji broj je zbroj svoga lijevog i desnog susjeda iz prethodnog retka. Iz Pascalova trokuta možemo očitati potencije binoma $1+x$:

$$\begin{array}{rc}
(1+x)^0 = & 1 \\
(1+x)^1 = & 1+x \\
(1+x)^2 = & 1+2x+x^2 \\
(1+x)^3 = & 1+3x+3x^2+x^3 \\
(1+x)^4 = & 1+4x+6x^2+4x^3+x^4 \\
\dots & \dots
\end{array}$$

Evo zašto.

Binomna formula

Stavak 8. *Neka su a i b bilo koja dva realna broja, i n bilo koji prirodan broj. Onda vrijedi binomna formula:*

$$\begin{aligned}
(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.
\end{aligned}$$

Često se binomna formula zapisuje i u ovom jednostavnijem obliku, gdje je x bilo koji realan broj:

$$\begin{aligned}
(1+x)^n &= 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{n-1}x^{n-1} + x^n \\
&= \sum_{k=0}^{n}\binom{n}{k}x^k
\end{aligned}$$

DOKAZ. Dokazat ćemo najprije jednostavniji oblik binomne formule, i to indukcijom po n.

1) Za $n=1$ tvrdnja vrijedi, jer je $(1+x)^1 = 1+x = 1+\binom{1}{1}x$.

2) Pretpostavimo da je sud $A(n)$: $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$ istinit za neki n, tj. $A(n)=T$. Izračunajmo

$$\begin{aligned}
(1+x)^{n+1} = (1+x)^n(1+x) &= \left[\sum_{k=0}^{n}\binom{n}{k}x^k\right](1+x) \\
&= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=0}^{n}\binom{n}{k}x^{k+1} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^k
\end{aligned}$$

$$
\begin{aligned}
&= \binom{n}{0}x^0 + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]x^k + \binom{n}{n}x^{n+1} \\
&= \binom{n+1}{0}x^0 + \sum_{k=1}^{n}\binom{n+1}{k}x^k + \binom{n+1}{n+1}x^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k.
\end{aligned}
$$

Dakle $A(n+1) = T$. Time je binomna formula za $(1+x)^n$ dokazana.

Općenitija formula slijedi odmah iz netom dokazane formule:

$$(a+b)^n = a^n(1+a^{-1}b)^n = a^n\sum_{k=0}^{n}\binom{n}{k}(a^{-1}b)^k = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k. \blacksquare$$

Iz binomne formule zbog $\binom{n}{1} = n$ odmah slijedi:

Korolar 1. (Bernoullijeva nejednakost) *Za svaki $x > 0$ i za svaki prirodan broj n vrijedi*

$$(1+x)^n \geqslant 1 + nx.$$

Iz korolara zaključujemo da čak i za vrlo mali $x > 0$ broj $(1+x)^n$ može biti vrlo velik, pod uvjetom da je n dovoljno velik. Drugim riječima, za svaki $a > 1$ (koliko god blizu 1) i koliko god veliki broj $M > 0$ postoji n takav da je $a^n > M$. Na pr. $1.001^n > 200$ za dovoljno veliki n, na pr. za $n = 200\,000$ jer je $200\,000 \cdot 0.001 = 200$.

Primjer 30. Bernoullijevu nejednakost možemo vrlo lako dokazati i matematičkom indukcijom. Neka je $x > 0$.

1) Za $n = 1$ tvrdnja je jasna: $(1+x)^1 \geqslant 1 + x$.

2) Pretpostavimo da tvrdnja vrijedi za neki prirodni broj n, tj. $(1+x)^n \geqslant 1 + nx$. Računamo

$$
\begin{aligned}
(1+x)^{n+1} &= (1+x)^n(1+x) \geqslant (1+nx)(1+x) \\
&= 1 + (n+1)x + nx^2 \geqslant 1 + (n+1)x,
\end{aligned}
$$

pa tvrdnja vrijedi i za $n+1$.

Time je Bernoullijeva nejednakost dokazana matematičkom indukcijom.