МАТЕМАТИЧКА ГИМНАЗИЈА

У БЕОГРАДУ

МАТУРСКИ РАД

из математике

ТЕОРИЈА СКУПОВА

ментор: **Славко Моцоња**

ученик: **Матија Срећковић, IVБ**

Београд, јун 2015.

САДРЖАЈ

УВОД 2
УВОД У СКУПОВЕ 4
ЕЛЕМЕНТАРНЕ АКСИОМЕ 6
АКСИОМА БЕСКОНАЧНОСТИ; ИНДУКТИВНОСТ 11
АКСИОМА ЗАМЕНЕ 13
- УРЕЂЕНИ ПАРОВИ 13
- РЕЛАЦИЈЕ 14
- ФУНКЦИЈЕ 16
- ДОБРО УРЕЂЕНИ СКУПОВИ 17
- ОРДИНАЛНИ БРОЈЕВИ; АКСИОМА ЗАМЕНЕ 21

АКСИОМА РЕГУЛАРНОСТИ 26
АКСИОМА ИЗБОРА 29
ЗАКЉУЧАК 31
ЛИТЕРАТУРА 32

УВОД

Скуп је, без сумње, најелементарнији појам у математици, темељ на који заснивамо цело наше досадашње знање. Управо зато је од изузетне важности да се правилно дефинише и ограничи. Наизглед, скуп је једноставан концепт о коме није потребно много размишљати: било каква колекција било чега. Међутим, при овако наивном објашњењу настаје, између осталог, и филозофски проблем: скупови су творевина наших умова, а не предмети у стварном свету. Кеса кромпира није исто што и скуп тих кромпира. Скуп молекула у капљици воде није исто што и та капљица. Да ли можемо имати скуп нечега што не постоји, или нечега што математика не дозвољава? Да ли постоји скуп свих бројева дељивих нулом? Да ли постоји скуп који садржи све скупове? Одговоре на ова питања је могуће дати, али не без озбиљне и ригорозне дефиниције скупа.

Како би се избегла филозофска питања, повољније је дефинисати скупове као колекције математичких појмова, а проблеми у реалном свету се могу аналогијом свести на математичке. Тако су примери скупова: скуп свих простих делилаца броја 324; скуп свих бројева дељивих нулом; скуп свих непрекидних функција, итд. Примећујемо да су сви ови скупови задати неким условом. Сви чланови ових скупова имају неке заједничке особине. По том резоновању, логично је закључити да је сваки скуп могуће задати одређеном особином илити условом, колико год тај услов био једноставан или компликован.

До овог закључка је дошао Георг Кантор, немачки математичар који је основао теорију скупова, једну од фундаменталних теорија математике. У свом раду објављеном 1883. године под именом „Основи опште теорије скупова“, Кантор дефинише скуп као „било коју колекцију одређених и засебних објеката које наша интуиција или ум могу обухватити у целину.“ Ти објекти се називају „елементима“ скупа.

Наравно, његова теорија је била далеко од савршене, што су показали многи други бриљантни математичари у следећих неколико деценија (неке недостатке је и сам Кантор приметио), истичући многобројне парадоксе Канторове теорије. Најочигледнији парадокс је уочио Бертранд Расел 1903. године:

Уочимо скуп $S = \{x \mid x \notin x\}$. Да ли овај скуп садржи самог себе? Уколико да, тада, по дефиницији тог скупа S не припада себи. Са друге стране, уколико не припада себи, испуњава услов, па $S \in S$. Дакле, скуп S нити припада нити не припада самом себи, што доводи до контрадикције.

Тада је заиста почела да се развија ова област математике, у потрази за свеобухватајућим и непротивречним објашњењем за овај елементарни појам, и тада је означен крај Канторове *наивне теорије скупова*. Начин на који се постиже овај циљ јесте *аксиоматизација*, то јест утемељење основних правила која се наводе без доказа, а из којих се могу извести све истине које су нама познате.

Најпознатија оваква теорија јесте Зермело-Френкелова теорија скупа. Важно је напоменути да је ово теорија логике првог реда, тј. да се аксиоме дефинишу помоћу логичких оператора ($\Rightarrow$, $\Leftrightarrow$, $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$), знака једнакости = и бинарне релације $\in$, те се ове ознаке користе без објашњења. Сама теорија је настала 1908. године када је Ернст Зермело предложио своју аксиоматску теорију. Међутим, 1921. године је Абрахам Френкел уочио недостатак у Зермеловој теорији: није било могуће доказати постојање неких скупова за које су математичари знали да постоје (на пример, скуп $\{A_0, \wp(A_0), \wp(\wp(A_0)), ...\}$, где је A_0 бесконачан скуп). 1922. године су Френкел и Торалф Сколем формализовали Зермелову теорију као теорију првог реда са атомским формулама ограниченим на = и $\in$ и увели још неке измене самим аксиомама.

УВОД У СКУПОВЕ

Како бисмо избегли Раселов парадокс и друге нејасноће, морамо пажљиво дефинисати *особину* скупа. Ово није нимало лак задатак. На пример, скуп чији елементи имају особину „велики српски писци двадесетог века“ није јасно дефинисан, јер не постоји објективан критеријум којим се одређује квалитет писца. Као још један пример проблема са којим се можемо сусрести при дефинисању особине скупа је „скуп свих природних бројева који се могу записати у децималном запису оловком на папиру“. Математичка индукција налаже да ову особину има сваки природан број: 0 се може записати, а ако се n може записати, може и $n + 1$, с тим што би његов запис трајао коју секунду дуже. Међутим, да ли би ико током свог живота могао да напише број $10^{10^{10^{10}}}$, и да ли уопште постоји довољно папира на свету за то?

Управо због овога морају постојати јасно дефинисана правила за оно што сме да се назове *особином*. Оно што свакако прво мора постојати јесте особина ***припадања*** скупу, релација коју обележавамо симболом ∈ и пишемо $x \epsilon y$, што значи „x припада y“ или „x је елемент y“. Све остале особине се могу изразити помоћу ϵ, идентитета, квантификатора и логичких оператора.

За **идентитет** користимо знак једнакости = да искажемо да је један скуп исто што и други: $X = Y$. Без доказа, по интуицији, узимамо да важе следеће особине ове релације:

- Рефлексивност: $(\forall X)\ X = X$.
- Симетричност: $(\forall X)(\forall Y)\ X = Y \Rightarrow \mathrm{Y} = \mathrm{X}$.
- Транзитивност: $(\forall X)(\forall Y)(\forall Z)(X = Y\ \wedge Y = Z) \Rightarrow \mathrm{X} = \mathrm{Z}$.
- $(\forall X)(\forall Y)(\forall Z)(X = Y\ \wedge\ Y \epsilon Z) \Rightarrow X \epsilon Z$.
- $(\forall X)(\forall Y)(\forall Z)(X = Y\ \wedge\ Z \epsilon X) \Rightarrow Z \epsilon Y$.

Логички оператори и квантификатори, који су управо искоришћени при опису особина једнакости, јесу **конјукција** ∧ (и), **дисјункција** ∨ (или), **негација** ¬ (не, супротно од), **импликација** ⇒ (следи), **еквиваленција** ⇔ (је исто што), **за свако** ∀, **постоји** ∃.

Тако, на пример, следеће реченице записане логичким језиком значе:

- $X \in Y\ \vee Y \in X$ – X припада Y или Y припада X.
- $\neg(X \in Y) \wedge\ \neg(Y \in X)$ – X не припада Y и Y не припада X.
- $X = Y\ \Rightarrow (X \in Z\ \Leftrightarrow Y \in Z)$ – ако је X једнако Y, тада је „X припада Z“ исто што и „Y припада Z“.
- $\neg(X \in X)$ – X не припада X.

Све ове особине су особине скупова X и Y. Уколико укључимо квантификаторе у наше изразе, уводимо питање о *чијој* се особини ради. На пример, у изразу $(\exists Y)\ Y \in X$ је X

параметар, а Y није, јер се његово значење не би променило да смо рекли да „постоји *неки* елемент скупа X“. Особине скупова које *немају* параметре су заправо обични логички искази и имају своју тачносну вредност ($\top$ или $\bot$). На пример, исказ $(\forall X)(\exists Y)\ Y \in X$ је има вредност $\bot$, јер ниједан скуп не припада празном скупу $\emptyset$. Особине које имају параметре се обележавају са $P(X_1, X_2, X_3, \dots, X_n)$, где је P особина, а X_i су параметри.

Иако се све особине и својства скупова могу описати помоћу ових симбола, за често коришћене особине се обично уводи нова нотација због лакоће записа и практичности. На пример, подскуп се дефинише као

$$X \subseteq Y \ \Leftrightarrow (\forall \mathrm{A})\ \mathrm{A} \in X \Rightarrow \mathrm{A} \in Y,$$

што нам умногоме олакшава будуће коришћење овог појма.

ЕЛЕМЕНТАРНЕ АКСИОМЕ

Постоји више различитих формулација Зермело-Френкелове теорије, јер аксиоме нису међусобно независне. У овом раду ће бити изложена једна од њих, а од ових аксиома су спорне аксиома постојања и аксиома упаривања (које се могу доказати из осталих; а по неким критеријумима, област дискурса, то јест „свет о којем дискутујемо“ је непразан, те је аксиома постојања вишак). Такође, Френкел и Сколем су, независно један од другог, обојица предложили да се шема аксиома подскупа замени шемом аксиома замене. Рад ће садржати обе аксиоме, као и доказ њихове редундантности.

Најпре претпостављамо да област дискурса није „**ништа**“, те постулирамо постојање једног скупа, тачније **празног** скупа. Пре него што уведемо аксиому, уведимо важан симбол $\notin$, „не припада“, у нашу нотацију.

$$X \notin Y \ \Leftrightarrow \ \neg(\mathrm{X} \in Y)$$

Аксиома празног скупа: Постоји празан скуп.

$$(\exists X)(\forall Y)\ X \notin Y$$

Овај скуп се може описати на бесконачно начина: скуп свих људи који су били на Марсу, скуп свих краљева Србије пре 1000. године, скуп свих српских тенисера који су пре Новака Ђоковића освојили 5 грен слем турнира. Међутим, све ово је заправо један исти скуп, то јест очигледно постоји само један празан скуп. Ово и даље не можемо доказати, јер нам је за то потребна још једна аксиома.

Аксиома екстензионалности: Ако је сваки елемент скупа X елемент скупа Y и сваки елемент скупа Y елемент скупа X, скупови X и Y су једнаки, илити два скупа су једнака ако имају све исте елементе.

$$(\forall A)(A \in X \ \Leftrightarrow A \ \in Y) \Rightarrow X = Y$$

Сада можемо доказати наше тврђење.

Теорема: Постоји тачно један празан скуп.

Доказ: Претпоставимо супротно, да постоје празни скупови A и B. Тада они имају исте елементе (тачније, немају елементе), па је по аксиоми екстензионалности A = B. ■

Дакле, скуп који не садржи елементе је јединствен, зове се празан скуп и обележава се симболом $\varnothing$.

Сада, желимо да испунимо жељу наше интуиције да скупове дефинишемо помоћу одређених особина и својстава. Међутим, да бисмо избегли парадоксе, морамо бити пажљиви. На пример, особине $X \notin X$ и $(\forall A) A \in X$ не одређују скуп. Из свих парадоксалних примера смо могли да приметимо једну ствар: свака од ових особина при покушају дефиниције скупа користи **сам тај скуп**. Дакле, особина којом дефинишемо скуп сме да има као параметре све аргументе у изразу осим самог скупа који дефинишемо.

Аксиома подскупа: Нека је $P(X)$ особина са параметром X. За сваки скуп A постоји скуп B такав да скуп X припада B ако и само ако X припада A и важи $P(X)$.

$$(\forall A)(\exists B)(\forall X)(X \in B \iff [X \in A \land P(X)])$$

Да бисмо лакше разумели аксиому, посматрајмо скуп B као подскуп скупа A. Дакле, да би B, објекат описан особином $P(X)$, био скуп, најпре је потребно да буде подскуп неког скупа који постоји. Овиме је избегнут парадокс.

Уочимо такође да је ова аксиома другачија за сваку особину, и да самим тим има бесконачно много варијанти, по једну за сваку формулу у теорији. Зато се за аксиому подскупа каже да је **шема аксиома**.

Интересантно је да се помоћу досадашњих аксиома може доказати постојање подскупа одређена два скупа, а самим тим и њиховог пресека, као „највећег“ таквог скупа.

Теорема: Ако су A и B скупови, онда постоји скуп R такав да је $x \in R$ ако и само ако је $x \in A$ и $x \in B$, то јест постоји скуп који је подскуп два скупа.

Доказ: Нека је формула $P(x,B)=x \in B$. Тада по аксиоми подскупа важи:

$$x \in R \iff P(x,B) \land x \in A$$

$$x \in R \iff x \in B \land x \in A$$

што је и требало доказати.■

Како бисмо олакшали нотацију, уведимо нов начин дефинисања скупова.

Дефиниција: $\{x \epsilon A | P(x)\}$ је скуп свих $x \epsilon A$ са особином $P(x)$.

Дефиниција: Скуп P је **пресек** скупова A и B ако садржи свако x за које $x \in A$ и $x \in B$.

$$A \cap B = \{x \,\big|\, x \in A \land x \in B\}$$

Заиста, свака два скупа имају скуп који им обојици припада. А да ли постоји скуп којем дата два скупа припадају? Како проширити спектар скупова са којима радимо? Због овога нам је потребна следећа аксиома:

Аксиома упаривања: Ако су A и B скупови, тада постоји скуп који садржи тачно скупове *A* и *B* као елементе.

$$(\forall A)(\forall B)(\exists C)(\forall x)(x \in C \Leftrightarrow x \in A \vee x \in B)$$

Потребност ове аксиоме је дискутабилна, јер се може извести из аксиоме празног скупа и још две аксиоме које ћу касније навести. У суштини, с обзиром на то да смо до сада могли да „баратамо“ само са празним скупом, ова аксиома гарантује постојање скупа празног скупа, скупа празног скупа и скупа празног скупа, итд.

Пример: Ако ставимо *A*=*Ø*, *B*=*Ø*, тада постоји скуп *C*=$\{Ø\}$. Сада, ако применимо аксиому упаривања на *A* и *C* добијамо *D*=$\{Ø, \{Ø\}\}$. Међутим, не можемо конструисати скуп *E*=$\{Ø, \{Ø\}, \{Ø,\{Ø\}\}\}$, јер би нам за то били потребни *B*, *C* и *D*.

За конструкцију скупа *E* из примера нам је потребна још једна аксиома.

Аксиома уније: За сваки скуп *A* постоји скуп *B* такав да је *x*∈*B* ако и само ако постоји скуп *D* такав да важи *x*∈*D* и *D*∈*A*.

$$(\forall A)(\exists B)(\forall x)(x \in B \ \Leftrightarrow (\exists D)(x \in D \wedge \ D \in A))$$

Скуп *B* се зове **унија скупа** *A* и обележава се са $\bigcup A$.

Ова аксиома на први поглед не делује тривијално, али је то заправо иста унија која се учи у основној школи, с тим што је овде *A* заправо **скуп скупова**, то јест његови чланови се третирају као скупови. На пример, ако је $A = \{\{1,2,3\},\{4,5\}\}$, тада је $B = \bigcup A = \bigcup\{\{1,2,3\},\{4,5\}\} = \{1,2,3\} \bigcup \{4,5\} = \{1,2,3,4,5\}$. Овај пример је интуиционистички, јер је потребно још аксиома и ознака да би се увео скуп природних бројева.

Међутим, да ли ова аксиома заиста помаже у конструкцији скупа *E* из претходног примера? Пошто је пресек дефинисан, логично је било дефинисати и унију, која се није могла извести из претходних аксиома, па је за њу уведена нова. Али посматрајмо следећи пример:

Пример: A_1 =*Ø*, A_2 =*Ø*, A_3 =$\{Ø\}$, A_4 =$\{Ø, \{Ø\}\}$. Ако искористимо аксиому уније на скупове *A*, *B*, *C* и *D*, добијамо скуп $X = \bigcup_{i=1}^{4} A_i$ за кога важи

$$x \in X \ \Leftrightarrow (\exists F)(x \in F \ \wedge \ F \in X)$$

$$\Leftrightarrow x \in \emptyset \ \vee x \in \{\emptyset\} \ \vee x \in \{\emptyset, \{\emptyset\}\}$$

$$\Leftrightarrow x = \emptyset \ \Leftrightarrow X = \{\emptyset\}.$$

Дакле, аксиома уније ипак нема моћ да конструише скуп E. Ту могућност има следећа аксиома:

Аксиома партитивног скупа: За сваки скуп S постоји скуп P такав да је $X \in P$ ако и само ако је $X \subseteq S$, то јест за сваки скуп постоји скуп који садржи све његове подскупове.

$$(\forall S)(\exists P)(\forall X)\ X \in P \ \Leftrightarrow X \subseteq S$$

Ако се примени аксиома партитивног скупа на скуп A_4 из претходног примера, добија се скуп $E = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Важно је напоменути да партитивни скуп скупа X увек садржи бар празан скуп и сам скуп X.

За крај, дефинишимо још две елементарне операције над скуповима чије постојање следи из аксиоме подскупа. Подскуп, унија и пресек су већ дефинисани, а остају нам разлика и симетрична разлика.

Дефиниција: Разлика скупова A и B је скуп који садржи све елементе скупа A који уједно не припадају скупу B.

$$A \setminus B = \{x | x \in A \ \wedge x \in B\}$$

Дефиниција: Симетрична разлика скупова A и B је разлика њихове уније и пресека, то јест скуп који садржи све елементе који припадају тачно једном од скупова A и B.

$$A \,\Delta\, B = \ \{x | x \in A \ \veebar x \in B\}$$

Симбол $\veebar$ означава ексклузивну дисјункцију (или A или B), и исказ $A \ \veebar \ B$ је тачан ако и само ако су A и B различитих тачносних вредности.

За унију и пресек важе закони комутативности, асоцијативности и дистрибутивности, који се лако доказују из њихове дефиниције и комутативност, асоцијативности и дистрибутивности конјукције и дисјункције:

Комутативност: $A \cup B = B \cup A$

$$A \ \cap B = B \cap A$$

Асоцијативност: $(A \cup B) \cup C = A \cup (B \cup C)$

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

Дистрибутивност: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

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

Такође за разлику и пресек, односно разлику и унију важе Деморганови закони:

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

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

Доказ: Доказ за прво тврђење:

$$C \setminus (A \cap B) = \{x | x \in C \ \land x \notin (A \cap B)\} =$$

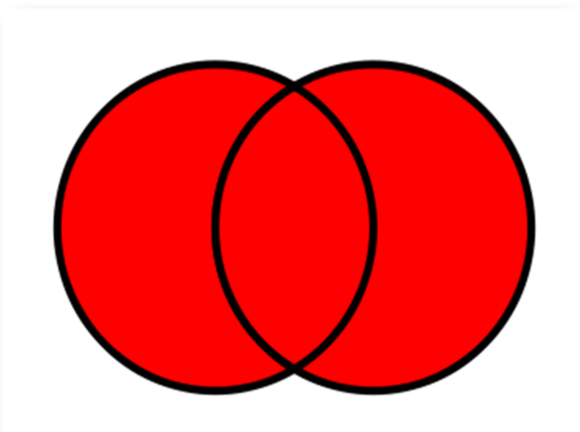
$$\{x | x \in C \land (x \notin A \lor x \notin B)\} =$$

$$\{x | (x \in C \land x \notin A) \lor (x \in C \ \lor x \notin B)\} =$$

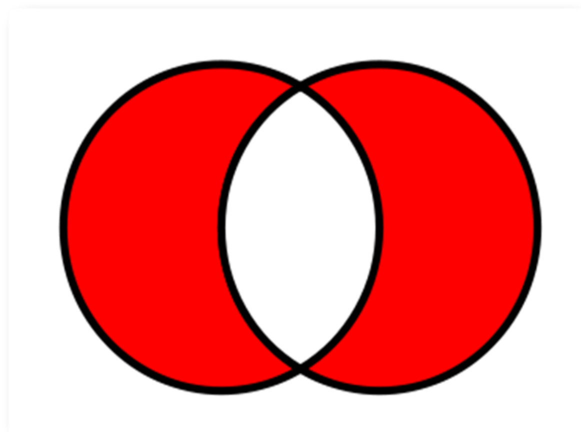
$$(C \setminus A) \cup (C \setminus B).$$

Доказ другог тврђења се ради аналогно. ■

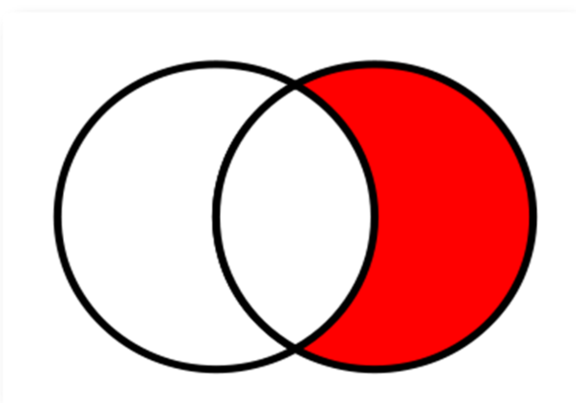
За визуелизацију, али не и строге доказе својстава ових операција су од велике помоћи **Венови дијаграми**. То су репрезентације скупова као „кругова“ и на једноставан начин показују све односе коначних скупова. Обојени делови представљају тражени резултат примене назначених операција над скуповима.



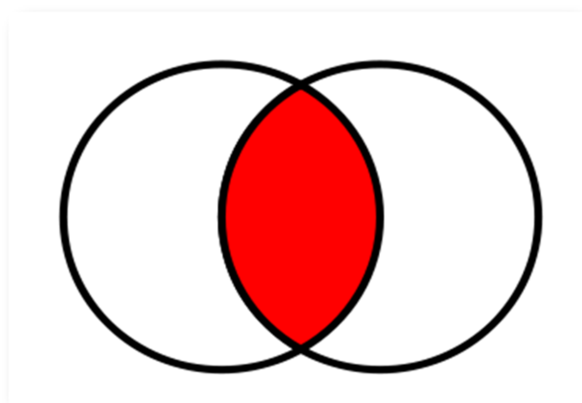
Унија два скупа



Симетрична разлика



Разлика



Пресек

АКСИОМА БЕСКОНАЧНОСТИ; ИНДУКТИВНОСТ

У овој глави ће бити објашњено заснивање скупа природних бројева помоћу теорије скупова и биће дата мотивација за додавање још једне важне аксиоме. Како дефинисати **број** помоћу до сада уведених појмова? Једине структуре чије је постојање познато јесу $\emptyset$ (празан скуп) и скупови који се дефинишу помоћу њега. Тај скуп има 0 елемената. Његов партитивни скуп, $\{\emptyset\}$ садржи 1 елемент. Користећи аксиому упаривања, добијамо скуп $\{\emptyset, \{\emptyset\}\}$ који има 2 елемента, и тако даље. По овој логици, могуће је **увести ознаку** (заправо је 0 само „назив“ за скуп $\emptyset$): 0=$\emptyset$.

Помоћу дефиниције „броја“ 0 (заправо скупа), могу се дефинисати остали бројеви:

$$1 = \{0\} = \{\emptyset\}$$

$$2 = \{0,1\} = \big\{\emptyset, \{\emptyset\}\big\}$$

$$3 = \{0,1,2\} = \Big\{\emptyset, \{\emptyset\}, \big\{\emptyset, \{\emptyset\}\big\}\Big\}, \text{ и тако даље.}$$

Идеја је једноставна: n је **природан број** ако се може записати у облику $\{0,1,2,\ldots,n\text{-}1\}$, то јест ако садржи све претходне природне бројеве. Међутим, ова дефиниција има фундаметалан недостатак: позива саму себе, а управо ова грешка у логици је одговорна за скоро све парадоксе у теорији скупова. Међутим, уз малу промену форме је могуће исправити ову грешку; на пример:

$$2 = \{0,1\} = \{0\} \cup \{1\} = 1 \cup \{1\}.$$

$$\text{Слично, } 3 = \{0,1,2\} = \{0,1\} \cup \{2\} = 2 \cup \{2\}.$$

Ово је много успешнији запис дефиниције природног броја, јер се користи само **претходни** природни број, а када се скуп који садржи тачно њега дода том броју, добија се следећи.

Дефиниција: Следбеник скупа X је скуп $S(X)=X \cup \{X\}$.

Ова дефиниција се може интуитивно изразити и као: следбеник броја $n \in \mathbb{N}$ је број $n+1 \in \mathbb{N}$. Важно је напоменути да је овде $n+1$ само ознака, јер операција + није дефинисана. Одавде је лако дефинисати индуктиван скуп.

Дефиниција: Скуп S је индуктиван ако важи:

I. $0 \in S$
II. $n \in S \Rightarrow (n+1) \in S$.

Дефиниција: Ако је I индуктиван скуп, скуп природних бројева је скуп

$$\mathbb{N} = \{x | (\forall I) x \ \in \ I\}.$$

Индуктиван скуп није исто што и скуп природних бројева, јер је заправо скуп природних бројева подскуп сваког индуктивног скупа (ово не значи да скуп природних бројева припада самом себи, што је и нетачно, већ да је једнак самом себи, а припада сваком другом индуктивном скупу који му није једнак).

Проблем са досадашњим дефиницијама је што не гарантују постојање индуктивног скупа. То не гарантују ни досадашње аксиоме. Зато је потребно увести нову аксиому.

Аксиома бесконачности: Постоји индуктиван скуп.

$$(\exists \boldsymbol{I})\big(\emptyset \ \in \boldsymbol{I} \ \wedge (\forall x)(x \in \boldsymbol{I} \Rightarrow x \cup \{x\} \in \boldsymbol{I})\big)$$

Остаје да се покаже да је $\mathbb{N}$ индуктиван скуп.[1]

Теорема: $\mathbb{N}$ је индуктиван скуп. Ако је $\boldsymbol{I}$ индуктиван скуп, тада важи $\mathbb{N} \subseteq \boldsymbol{I}$.

Доказ: Други део тврђења следи директно из дефиниције скупа $\mathbb{N}$. Остаје да се докаже први део тврђења. Како 0 припада сваком индуктивном скупу по дефиницији индуктивног скупа, следи $0 \epsilon \mathbb{N}$. Затим, ако је $n \epsilon \mathbb{N}$, онда је и $n \ \in \ \boldsymbol{I}$**,** па је и $n + 1 \ \in \ \boldsymbol{I}$, за сваки индуктивни скуп $\boldsymbol{I}$. Из $n + 1 \ \in \ \boldsymbol{I}$ сада следи $n + 1 \ \in \ \mathbb{N}$, па је задовољен услов

$$n \ \in \ \mathbb{N} \Rightarrow \ n + 1 \ \in \ \mathbb{N},$$

те је скуп $\mathbb{N}$ индуктиван.■

[1] Из дефиниције скупа $\mathbb{N}$ као теорема следе принципи математичке индукције и трансфинитне индукције, као и појам низа, које нећу доказивати, али ћу се њима користити у неким доказима.

АКСИОМА ЗАМЕНЕ

Да би се објаснила мотивација за следећу аксиому, потребно је увести поприлично много нових појмова; неки од ових су елементарни (релације и функције), а неки су мало мање интуитивни (ординални бројеви).

Најпре се дошло до идеје да се генерализује процес бројања на нешто више од скупа природних бројева. Замислимо, тако, да постоји неки број ω који долази „после“ свих природних бројева. После њега иде $\omega + 1$, $(\omega + 1) + 1$, и тако даље. Како дефинисати ове бројеве? Да бисмо уопште дискутовали о постојању $\omega + 1$, морамо увести релације и функције.

УРЕЂЕНИ ПАРОВИ

Редослед елемената у скупу је небитан: $\{a, b\} = \{b, a\}$. Међутим, многи проблеми у животу захтевају поштовање одређених редоследа. Поставља се питање: како дефинисати редослед у теорији скупова, ако је у скуповима неважан редослед? Једноставно, могуће је конструисати скуп који садржи скуп са траженим елементима, као и скуп који назначује редослед елемената.

По конвенцији се уводи:

Дефиниција: Уређени пар (a, b) се дефинише као

$$(a, b) = \big\{\{a\}, \{a, b\}\big\}.$$

У дефиницији први скуп означава да је a први елемент. Ово је само конвенција, јер је исто тако могуће дефинисати уређени пар као $\big\{\{b\}, \{a, b\}\big\}$. Такође, важно је напоменути да је уређена двојка (a, a) заправо скуп $\big\{\{a\}, \{a, a\}\big\} = \big\{\{a\}\big\}$.

Одавде је лако дефинисати уређене тројке, четворке итд. као

$$(a, b, c) = \big((a, b), c\big),$$

$$(a, b, c, d) = \big((a, b, c), d\big).$$

Теорема: $(a, b) = (a', b') \Leftrightarrow a = a' \wedge b = b'$.

Доказ: Ако важи $a = a' \wedge b = b'$, тада $\big\{\{a\}, \{a, b\}\big\} = \big\{\{a\}, \{a', b'\}\big\} \Rightarrow (a', b')$. С друге стране, ако је $(a, b) = (a', b')$, тада важи $\big\{\{a\}, \{a, b\}\big\} = \big\{\{a'\}, \{a', b'\}\big\}$. Како су $\{a\}$ и $\{a'\}$ једини једночлано подскупови оба скупа, $a = a'$. Користећи ово добијамо $\{a, b\} = \{a, b'\}$, одакле следи $b = b'$.■

Са дефинисаним појмом уређеног пара можемо дефинисати релацију.

РЕЛАЦИЈЕ

Релације су неизоставни део математике и један од њених најважнијих појмова. Описују одређену везу између објеката. На пример, релација ρ_1 је релација између праве p и равни π где су они у релацији ако права p припада равни π. Нека је, сада, исто тако, релација ρ_1' релација између равни и праве, где су они у релацији ако раван садржи праву. Релације ρ_1 и ρ_1' су уско повезане, само су им елементи „обрнути". Ово говори да је при дефиницији релације битан уређени пар.

Дефиниција: Скуп ρ је бинарна релација ако су сви његови елементи уређени парови.

$$z \in \rho \Leftrightarrow (\exists x)(\exists y)\, z = (x, y)$$

Обично се пише $x\rho y$ уместо $(x, y) \in \rho$.

Везано за скупове којима припадају координате уређених парова, уводи се још једна дефиниција.

Дефиниција:

I. Скуп свих x који су у релацији ρ са y се зове **домен** релације ρ и обележава се са $dom\rho$.
$$dom\rho = \{x | (\exists y) x\rho y\}$$
II. Скуп свих y таквих да је за неко x важи $x\rho y$ се зове **кодомен** релације ρ и обележава се са $cod\rho$.
$$cod\rho = \{y | (\exists x) x\rho y\}$$

Постоји још много важних особина релација, али је за увођење појма који желимо потребно још само неколико.

Дефиниција: Нека су A и B скупови. Скуп свих уређених парова чији је први члан елемент скупа A, а други члан елемент скупа B се зове Декартов производ скупова A и B и означава се са $A \times B$.

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

Дефиниција:

I. Бинарна релација ρ је рефлексивна у скупу A ако је сваки елемент у релацији са самим собом, то јест ако важи:
$$(\forall x \in A)\, x\rho x.$$
II. Бинарна релација ρ је симетрична у скупу A ако важи
$$(\forall x \in A)(\forall y \in A)\, x\rho y \Rightarrow y\rho x.$$
III. Бинарна релација ρ је антисиметрична у скупу A ако важи
$$(\forall x \in A)(\forall y \in A)\, x\rho y \wedge y\rho x \Rightarrow x = y.$$

IV. Бинарна релација ρ је транзитивна у скупу A ако важи
$$(\forall x \in A)(\forall y \in A)(\forall z \in A)\ x\rho y \wedge y\rho z \Rightarrow x\rho z.$$
V. Коначно, бинарна релација ρ чији су домен и кодомен подскупови скупа A која је рефлексивна, антисиметрична и транзитивна је релација поретка на скупу A. Пар (A,ρ) се зове *уређен скуп.*

На пример, $\leq$ је релација поретка на скуповима $\mathbb{N}, \mathbb{Q}$ и $\mathbb{R}$. Ако x и y припадају истом скупу A, релације $\subseteq$ и $\supseteq$ су релације поретка на скупу A. Мало другачији пример релације поретка је релација $n|m$ (n дели m). Ако смо дефинисали $\leq$, логично је и дефинисати релацију $<$. Она није релација поретка, али има друго важно место.

Дефиниција: Релација ρ у скупу A је асиметрична ако важи
$$(\forall x \in A)(\forall y \in A)\ x\rho y \Rightarrow\ \neg(y\rho x).$$
Управо ову особину има релација $<$ која се сматра елементарном у математици.

Дефиниција: Релација ρ је релација строгог поретка на скупу A ако је асиметрична и транзитивна.

Релације поретка и релације строгог поретка су уско повезане, чему сведочи следећа теорема.

Теорема:

I. Нека је ρ релација поретка на скупу A; тада је релација σ за коју важи
$$a\sigma b\ \Leftrightarrow a\rho b\ \wedge a \neq b$$
релација строгог поретка скупа A.

II. Нека је σ релација строгог поретка на скупу A; тада је релација ρ за коју важи
$$a\rho b\ \Leftrightarrow a\sigma b\ \wedge a = b$$
релација поретка на скупу A.

Доказ:

I. Најпре треба доказати асиметричност: претпоставимо супортно, да је релација σ симетрична. Важи
$$a\sigma b \Rightarrow b\sigma a\ \Leftrightarrow$$
$$a\rho b\ \wedge a \neq b \Rightarrow b\rho a\ \wedge a \neq b\ \Leftrightarrow$$
$$a = b\ \wedge a \neq b,$$
јер је релација ρ антисиметрична. Дакле, из контрадикције следи да је релација σ асиметрична.

За транзитивност важи:
$$a\sigma b \wedge b\sigma c \Rightarrow a\sigma c \Leftrightarrow$$
$$a \neq b \neq c \wedge (a\rho b \wedge b\rho c \Rightarrow a\rho c),$$

што је очигледно тачно.

II. Доказ је сличан као I. само уместо асиметричности доказати рефлескивност и антисиметричност.■

Вратимо се сада на пример дељивости као релације поретка. Интересантно је да $2\nmid 3$ и $3\nmid 2$. Иако је дељивост релација поретка на скупу природних бројева, за разлику од $\leq$, где је један број свакако мањи или једнак другом, није тачно да су свака два природна броја у релацији дељивости, то јест релација дељивости **не упоређује** свака два природна броја.

Дефиниција: Нека је релација $\leq$ $(<)$ релација (строгог) поретка на скупу А. Два елемента a и b скупа А су упоредиви ако важи $a \leq b$ или $b \leq a$ (за строги поредак ако важи $a \neq b$ и $a < b$ или $b < a$).

Упоредивост води до једног врло важног појма: релације линеарног поретка.

Дефиниција: Релација поретка или релација строгог поретка $\leq$ $(<)$ на скупу A је релација линеарног поретка ако су свака два елемента скупа A упоредива. Уређен скуп $(A, \leq)$ се зове **линеарно уређен скуп**.

ФУНКЦИЈЕ

У математичкој анализи и многим другим областима, функција је најважнији и најосновнији појам, заправо и предмет изучавања. У теорији скупова, функција је само обична релација, са једним специјалним својством: један елемент из домена може бити у релацији са највише једним елементом из кодомена. За мотивацију за дефинисање аксиоме замене није потребно екстензивно дефинисати својства функција, већ је довољно дефинисати инјективност (1-1 пресликавање).

Дефиниција: Бинарна релација f се зове **функција** ако из afb_1 и afb_2 следи $b_1 = b_2$.

Другим речима, f је функција ако и само ако за свако $a \in domf$ постоји тачно b за које је afb. Ово b се зове вредност функције f у тачки a и обележава се са $f(a)$. $f(a)$ није дефинисано ако a не припада домену функције. Такође, уобичајено је да се при дефиницији функције назначе домен и кодомен на следећи начин: $f{:}A\to B$.

Дефиниција: Функција f је 1-1 или инјективна ако важи

$$(\forall x_1 \in domf)(\forall x_2 \in domf)x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Дефиниција: Функција $f{:}A\to A$ дефинисана на линеарно уређеном скупу $(A,<)$ је растућа ако важи

$$(\forall x_1 \in A)(\forall x_2 \in A)x_1 < x_2 \Rightarrow f(x_1) < f(x_2).$$

Још два неизоставна појма везана за функције су појам композиције функција и појам инверзне функције.

Дефиниција: Композиција две фунцкије $f: A \rightarrow B$ и $g: B \rightarrow C$ је функција

$$g \circ f = \{(a, c) \big| (\exists b \in B)\big((a, b) \in f \ \wedge (b, c) \in g\big)\}$$

Дефиниција: Инверзна функција функције $f: A \rightarrow B$ је функција $f^{-1}: B \rightarrow A$ за коју важи

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

за свако $x \in A$.

Теорема: Функција f је инверзибилна ако и само ако је 1-1.[2]

Доказ: Нека је најпре f инверзибилна. Тада је f^{-1} функција и по дефиницији је за свако $a \in domf \ \ f^{-1}\big(f(a)\big) = a$. Сада, ако су $a_1, a_2 \in domf$ и важи $f(a_1) = f(a_2)$, тада је $f^{-1}\big(f(a_1)\big) = f^{-1}\big(f(a_2)\big)$, што значи да је $a_1 = a_2$. Из овога следи да је f 1-1.

Сада, нека је f 1-1, а f^{-1} релација за коју треба доказати да је функција. За $af^{-1}b_1$ и $af^{-1}b_2$ имамо b_1fa и b_2fa. Управо због овога и претпоставке да је f 1-1 следи да је $b_1 = b_2$, па је по дефиниција f^{-1} функција.■

Сада су уведени сви појмови који су потребни за дефиницију **изоморфизма**, који је кључан за „повезивање“ уређених скупова.

Дефиниција: Изоморфизам између два уређена скупа $(\mathcal{F}, <)$ и $(\mathcal{M}, \prec)$ је 1-1 функција h са доменом $\mathcal{F}$ и кодоменом $\mathcal{M}$ таква да за свака два $p_1, p_2 \epsilon\ \mathcal{F}$ важи

$$p_1 < p_2 \Leftrightarrow h(p_1) \prec h(p_2).$$

ДОБРО УРЕЂЕНИ СКУПОВИ

Наставимо сада са питањем „Шта следи после природних бројева?“ Увели смо скуп $\omega = \mathbb{N}$, а исто као и природне бројеве следбенике скупа ω:

$$S(\omega) = \omega \cup \{\omega\} = \{0,1,2, \dots, \omega\}$$

[2] У зависности од литературе је некада довољно да функција буде 1-1 да би била инверзибилна, а негде мора бити и „на“ (сурјективна) (функција је „на“ ако је скуп других координата уређених парова функције исто што и кодомен те функције). У овом раду је довољан услов 1-1, с тим што није гарантовано да је функција f^{-1}у свим тачкама свог домена дефинисана.

$$S(S(\omega)) = S(\omega) \cup \{S(\omega)\} = \{0,1,2, \dots, \omega, S(\omega)\}.$$

Ради олакшања нотације се уводи ознака $S(\omega) = \omega + 1$, $S(\omega + n) = \omega + (n + 1)$ за $n \epsilon \mathbb{N}\backslash\{0\}$.

Овако се могу дефинисати и скупови као:

$$\omega \cdot 2 + 1 = \{0,1,2, \dots, \omega, \dots, \omega \cdot 2\},$$

$$\omega \cdot 3 + 1 = \{0,1,2, \dots \omega, \omega + 1, \dots, \omega + \omega, \omega + \omega + 1, \dots, \omega + \omega + \omega\},$$

чак и

$$\omega \cdot \omega = \{0,1,2, \dots \omega, \dots, \omega \cdot 2, \dots, \omega \cdot 3, \dots, \}.$$

Скуп свих следбеника скупа ω (овај скуп заправо не постоји; у следећих неколико потпоглавља ће то бити објашњено; зато, рецимо уместо тога да се овај скуп завршава са $\omega \cdot \omega$ као последњим елементом) заједно са скупом природних бројева формира линеарно уређен скуп уз релацију ∈, уз својство да имамо „почетак“, тј. скуп $\emptyset$, и да који год подскуп овог скупа изабрали, и даље имамо „почетак“, тј. елемент који је подскуп свих осталих елемената.

Дефиниција: Скуп W је **добро уређен** релацијом < ако важи

I. $(W, <)$ је линеарно уређен скуп.
II. Сваки непразан подскуп скупа W има најмањи елемент, тј. елемент који припада сваком другом елементу тог подскупа.

Фундаментално својство добро уређених скупова јесте то да се могу поредити по „величини“ (која, иако интуитиван појам, се мора добро дефинисати). Да би се увела та дефиниција, најпре је потребно објаснити иницијални сегмент, скуп који садржи „највећи“ елемент и све „мање“ елементе, тј. скуп који садржи неки елемент и све остале елементе који му припадају.

Дефиниција: Нека је $(W,<)$ линеарно уређен скуп. Скуп $S \subseteq W$ је иницијални сегмент скупа W ако важи $S \neq W$ и ако за свако $a \epsilon S$ сви $x<a$ такође припадају скупу S.

Ово је подскуп скупа W ограничен одозго неким његовим елементом, а како је W добро уређен, и S је добро уређен. Чињеница да је сваки иницијални сегмент добро уређеног скупа и сам добро уређен је важна за доказ следеће леме.

Лема: Ако је $(W,<)$ добро уређен скуп и S неки његов иницијални сегмент, постоји $a \in W$ такав да $S = \{x \in W | x < a\}$.

Доказ: Дефинишимо скуп X као разлику скупа W и скупа S. Због $S \neq W$ скуп X не може бити празан. Како су S и W добро уређени, X мора имати неки најмањи [3]елемент a. Разматрајмо сада однос неког $x \in S$ са a:

$$x < a \Rightarrow x \notin X,$$

јер је a најмањи елемент скупа X. С друге стране,

$$x \geq a \Rightarrow x \notin S,$$

јер би иначе $x \in S$ повукло $a \in S$.■

Пошто важи $X \cup S = W$, сви елементи који не припадају скупу X припадају скупу S, па важи $S = \{x \in W | x < a\}$.

Овај скуп се означава са $W[a]$.

Са дефинисаним иницијалним сегментима, могуће је увести теорему која у практичном смислу омогућује поређење скупова.

Теорема*: Ако су два добро уређена скупа $(W_1, <_1)$ и $(W_2, <_2)$, важи тачно једно од следећа три тврђења:

I. Постоји изоморфизам између скупова W_1 и W_2.
II. Постоји изоморфизам између скупа W_1 и неког иницијалног сегмента скупа W_2.
III. Постоји изоморфизам између скупа W_2 и неког иницијалног сегмента скупа W_1.

За доказ ове теореме су најпре потребне две леме.

Лема: Ако је $(W, <)$ добро уређен скуп и $f: W \to W$ растућа функција, онда важи

$$f(x) \geq x$$

за свако $x \in W$.

Доказ: Претпоставимо супротно, да је скуп $X = \{x \in W | f(x) < x\}$ непразан. Тада, као добро уређен скуп, има најмањи елемент a. Тада важи $f(a) < a$, а како растућа функција f чува редослед, важи и $f(f(a)) < f(a)$. Међутим, тада по услову скупа X важи $f(a) \in X$, што је контрадикција, јер је a најмањи елемент скупа X, а $f(a) < a$.■

Лема:

I. Не постоји изоморфизам између добро уређеног скупа и било којег његовог иницијалног сегмента.
II. Сваки добро уређен скуп има само један аутоморфизам[4], и то идентитет.

[3] За најмањи елемент се овде сматра елемент који припада сваком другом елементу скупа.

III. Ако су W_1 и W_2 изоморфни добро уређени скупови, изоморфизам између њих је јединствен.

Доказ:

I. Претпоставимо да такав изоморфизам постоји: $f: W \to W[a]$, за неко $a \in W$. Тада следи $f(a) \in W[a]$ као елемент кодомена, те $f(a) < a$, што се противи претходној леми.
II. Нека је f аутоморфизам на скупу W. Тада су f и f^{-1} растуће функције, па за $x \in W$ важи $f(x) \geq x$ и $f^{-1}(x) \geq x$ по претходној леми. Из друге неједнакости и чињенице да је f растућа функција добијамо $f\left(f^{-1}(x)\right) \geq f(x)$, тј. $x \geq f(x)$. Из претходне леме и антисиметричности $\geq$ следи $f(x) = x$.
III. Претпоставимо супротно, да постоје два изоморфизма f и g за W_1 и W_2. Тада је $f \circ g^{-1}$ аутоморфизам и по претходном делу ове леме идентитет. Дакле, $f = g$. ■

Уз ове две леме је могуће извести доказ претходне теореме.

Доказ теореме*: Нека су W_1 и W_2 добро уређени скупови. Прва лема налаже да су три случаја у теореми узајамно искључива: нпр. када би постојала два изоморфизма са доменима и кодоменима $W_1 \to W_2[a_2]$ и $W_2 \to W_1[a_1]$, њихова композиција би био изоморфизам који пресликава добро уређен скуп на његов иницијални сегмент, што је немогуће.

Јединственост изоморфизма у сваком од три случаја следи директно из друге леме.

Сада остаје само да се докаже да изоморфизам задовољава један од три задата услова. Дефинишимо функцију $f \subseteq W_1 \times W_2$ као

$$f = \{(x, y) \in W_1 \times W_2 | \text{ постоји изоморфизам између } W_1[x] \text{ и } W_2[y]\}.$$

Прво, ова функција је 1-1, јер, када би се два различита x_1 и x_2 сликала у y, постојао би изоморфизам између $W_1[x_1]$ и $W_1[x_2]$, што је немогуће, јер је један сигурно иницијални сегмент другог, а између скупа и његовог иницијалног сегмента не сме постојати изоморфизам.

Даље, функција је растућа, тј. важи $x < x' \Rightarrow f(x) < f(x')$, јер ако је h изоморфизам између $W_1[x']$ и $W_2[f(x')]$, а његова рестрикција[5] $h \upharpoonright W_1[x]$ изоморфизам између $W_1[x]$ и $W_2[h(x)]$, те је $h(x) = f(x)$ и самим тим $f(x) < f(x')$.

---

[4] Аутоморфизам је заправо изоморфизам који пресликава неки скуп S у самог себе.
[5] Рестрикција функције f на скуп X се добија када се домен функције ограничи на одређени подскуп њеног домена. Функција на новом домену задржава исте вредности које је имала са старим, већим доменом. Рестрикција функције f на скуп X се обележава са $f \upharpoonright X$.

Због тога што је функција f 1-1 и растућа следи да је изоморфизам између домена, подскупа W_1 и кодомена, подскупа W_2. Ако су домен и кодомен цели скупови W_1 и W_2, услов I. је задовољен. Иначе је или домен или кодомен цео скуп.

На пример, нека је домен $W_1[x]$, подскуп скупа W_1 који је различит од њега. Кодомен може бити цео скуп W_2, што се слаже са теоремом, или неки његов иницијални сегмент $W_2[y]$, што је супротно теореми. Претпоставимо да је то случај, то јест да постоји изоморфизам између $W_1[x]$ и $W_2[y]$. Тада, по дефиницији функције f важи $(x, y) \in f$, $x \in domf = W_1[x]$, што значи $x < x$, што је немогуће. Аналогно се доказује да смо претпоставили да је кодомен иницијални сегмент. ■

Сада, са способношћу да упоређујемо величине скупова можемо увести ординалне бројеве.

ОРДИНАЛНИ БРОЈЕВИ; АКСИОМА ЗАМЕНЕ

У претходних неколико потпоглавља смо као мотив изразили наставак бројања после скупа природних бројева и увели скуп ω и његове следбенике. Приметили смо да је $(\omega, \in)$, као и скуп било ког следбеника скупа ω заједно са $\in$ добро уређен скуп, као и да сваки следбеник скупа ω садржи скуп $\mathbb{N}$ као свој иницијални сегмент. Међутим, најважније од свега је да су ординални бројеви представници свих добро уређених скупова. Да бисмо то показали, морамо увести мноштво нових појмова у овом потпоглављу, као и једну аксиому.

Дефиниција: Скуп **T** је транзитиван ако је сваки његов елемент уједно и његов подскуп, тј.

$$(\forall x \in \mathbf{T}) x \subseteq \mathbf{T}.$$

Скуп природних бројева као и ординални бројеви су очигледно транзитивни. Као пример се могу навести и скуп свих правих у еуклидској равни, или скуп свих равни у еуклидском простору $\mathbb{E}^3$.

Транзитиван скуп се, баш као својство транзитивности неке релације, може другим речима описати и као

$$x \in y \wedge y \in \mathbf{T} \Rightarrow x \in \mathbf{T}.$$

Дефиниција: Скуп α је **ординални број (ординал)** ако важи:

I. α је транзитиван.
II. Уређени скуп $(\alpha, \in)$ је добро уређен скуп.

Теорема: Сваки природан број је ординалан.
Доказ: Природан број је транзитиван јер је $n + 1 = n \cup \{n\}$, па је његов највећи[6] елемент n његов подскуп у виду $\{n\}$, а сви мањи елементи су елементи скупа n, који је подскуп скупа $n + 1$, те је по транзитивности $\subseteq$ сваки његов елемент његов подскуп. Што се добре уређености тиче, природни бројеви су по дефиницији индуктивности добро уређени.■

Теорема: Ако је α ординалан број, онда је и $\alpha + 1 = \alpha \cup \{\alpha\}$ ординал.

Доказ: Аналогно доказу претходне теореме. ■

За ординале α и β важи $\alpha < \beta$ ако и само ако важи $\alpha \in \beta$, што помаже уређењу ординалних бројева заједно са природним. Ова релација је изузетно битна јер и она, као и $\in$, добро уређује ординалне бројеве.

Такође, треба напоменути да нема сваки ординални број свог претходника. Два таква броја су 0 и ω. 0 је најмањи ординални број, а претходник ω би био „највећи природан број“, што није дозвољен нити постојан израз у математици, јер би и он имао следбеника који је такође природан број. Такви бројеви се зову **гранични ординали**, а бројеви који су следбеници неких су **следбенички ординали**.

Теорема:** Ако су, α, β и γ ординални бројеви, важи:

I. $\alpha < \beta \wedge \beta < \gamma \Rightarrow \alpha < \gamma$.
II. Не могу истовремено важити $\alpha < \beta$ и $\beta < \alpha$.
III. Важи или $\alpha < \beta$ или $\alpha = \beta$ или $\beta < \alpha$.
IV. Сваки непразан скуп ординалних бројева има најмањи елемент по релацији $<$.
V. За сваки скуп ординала X постоји ординал α који не припада скупу X. ■

За доказ ове теореме су претходно потребне три леме.

Лема: Ако је α ординал, $\alpha \notin \alpha$.

Доказ: Ако би важила $\alpha \in \alpha$, добро уређен скуп $(\alpha, \in)$ би имао члан $x = \alpha$ за кога важи $x \in x$, што крши асиметричност релације $\in$.■

Заправо, ниједан скуп у математици не припада самом себи.

Лема: Сваки елемент ординалног броја је ординалан број.

Доказ: Нека је α ординалан број и $x \in \alpha$.

[6] Као и најмањи, највећи елемент у скупу у овом случају се дефинише као елемент који припада сваком другом елементу тог скуа.

I. Транзитивност: Нека је $u \in v$ и $v \in x$. Пошто је α транзитиван, $v \in \alpha$ и $u \in \alpha$. Дакле, u, v и x су елементи α, а пошто је $\in$ релација линеарног поретка на скупу α, што значи да су свака два његова елемента упоредива, мора бити $u \in x$.
II. $(x, \in)$ је добро уређен скуп: Због транзитивности скупа α имамо $x \subseteq \alpha$, па је релација $\in$ са кодоменом x заправо само рестрикција релације $\in$ са кодоменом α, што значи да је $(x, \in)$ добро уређен скуп. ■

Лема: Ако су α и β ординали и $\alpha \subset \beta$, онда је $\alpha \in \beta$.

Доказ: Због $\alpha \subset \beta$ је скуп $\beta \backslash \alpha$ непразан подскуп скупа β, па има најмањи елемент γ, јер је добро уређен. Приметимо да важи $\gamma \subseteq \alpha$: уколико не би важило, свако $\delta \in \gamma \backslash \alpha$ би било елемент $\beta \backslash \alpha$ и било би мање од најмањег елемента тог скупа, γ.

Докажимо сада и да је $\alpha \subseteq \gamma$: нека је $\delta \in \alpha$; тада мора бити $\delta \in \gamma$, јер би у супротном важило $\gamma \in \delta$ или $\gamma = \delta$, а затим и $\gamma \in \alpha$, што је немогуће јер $\gamma \in \beta \backslash \alpha$.

Дакле, из $\alpha \subseteq \gamma$ и $\gamma \subseteq \alpha$ следи $\alpha = \gamma$, то јест $\alpha \in \beta$. ■

Доказ теореме:**

I. Следи директно из транзитивности ординала, јер је $\alpha < \beta \iff \alpha \in \beta$ за ординале.
II. Претпоставимо супротно: $\alpha \in \beta$ и $\beta \in \alpha$. Тада би по транзитивности ординала важило $\alpha \in \alpha$, што је контрадикторно са првом лемом.
III. Ако су α и β ординали, $\alpha \cap \beta$ такође мора бити ординал јер важи $\alpha \cap \beta \subseteq \alpha$ и $\alpha \cap \beta \subseteq \beta$. Разликујемо 3 случаја:
    i. $\alpha \cap \beta = \alpha$, и тада је $\alpha \subseteq \beta$, што значи да важи или $\alpha \in \beta$ или $\beta = \alpha$.
    ii. $\alpha \cap \beta = \beta$, и тада је или $\beta \in \alpha$ или $\beta = \alpha$.
    iii. $\alpha \cap \beta \subset \alpha$ и $\alpha \cap \beta \subset \beta$, што по трећој леми значи да важи $\alpha \cap \beta \in \alpha$ и $\alpha \cap \beta \in \beta$, што значи да $\alpha \cap \beta \in \alpha \cap \beta$, што је немогуће, поново због прве леме.
IV. Нека је A непразан скуп ординала. Узмимо неко $\alpha \in A$ и посматрајмо скуп $\alpha \cap A$ (интуитивно је да је ово скуп α, међутим, то нам није потребно за доказ овог тврђења). Ако $\alpha \cap A = \emptyset$, α је најмањи елемент A. У супротном важи $\alpha \cap A \subseteq \alpha$, па као добро уређен скуп $\alpha \cap A$ има најмањи елемент β, који је уједно и најмањи елемент добро уређеног скупа $(A,<)$.
V. Нека је X скуп ординала. Пошто су сви елементи скупа X транзитивни, и $\bigcup X$ је транзитиван. Пошто $\in$ добро уређује $\bigcup X$ (због транзитивности релације и претходног тврђења IV.), $\bigcup X$ је ординал. Сада, нека је $\alpha = S(\bigcup X)$. α је ординал и важи $\alpha \notin X$. ■

Као закључак, сваки ординал је добро уређен скуп са релацијом $\in$, и ниједна два различита ординала нису изоморфна, јер је један увек иницијални сегмент другог.

Напоменимо за крај да је последица друге леме да се сваки ординал A може записати као

$$A = \{B | B \text{ је ординал и } B \in A\}.$$

Добро уређени скупови се могу јединствено представити као ординали, чему сведочи следећа теорема. Иако изгледа сасвим разумно, доказ ове теореме је само демонстративан у смислу да открива недостатак у досадашњем аксиоматском систему и захтева увођење нове аксиоме.

Теорема: Сваки добро уређени скуп је изоморфан јединственом ординалу.

Доказ: Нека је $(W, <)$ добро уређен скуп. Нека је

$$A = \{a \in W | W[a] \text{је изоморфан неком ординалу}\}.$$

Како ниједна два ординала нису изоморфна, овај ординал је јединствен; означимо га са α_a. Сада, **претпоставимо** да постоји скуп S=$\{\alpha_a | a \in A\}$. (S,∈) је добро уређен јер је скуп ординала. Такође је транзитиван: докажимо то тако што узмемо неко $\gamma \in \alpha_a \in S$. Затим, нека је φ изоморфизам између $W[a]$ и α_a и нека је $c = \varphi^{-1}(\gamma)$. Функција $\varphi \restriction c$ је изоморфизам између $W[c]$ и γ, па је $\gamma \in S$. Дакле, S је ординал. Назовимо тај ординал $S = \alpha$.

Покажимо да ако важи $b < a$ и $a \in A$, важи и $b \in A$. Нека је φ изоморфизам између $W[b]$ и неког иницијалног сегмента α_b, који мора припадати скупу S. Тада је $b \in A$ и $\alpha_b < \alpha_a$. Дакле, важи или $A = W$ или $A = W[d]$ за неко $d \in W$.

Сада, дефинишимо функцију $g: A \to S$ као $f(a) = \alpha_a$. Из дефиниције скупа S и чињенице да је функција g растућа следи да је она изоморфизам између A и S. Када би важило $A = W[d]$, важило би и $d \in A$, што је контрадикција. Дакле, $A = W$, а g је изоморфизам између добро уређеног скупа W и ординала S. ■

Нажалост, ниједна до сада уведена аксиома не гарантује постојање скупа S.

Посматрајмо још један пример који нам даје мотивацију за увођење аксиоме замене: аксиомом бесконачности се постулира постојање скупа ω. Одатле, лако је доказати постојање скупова $\omega + 1 = \omega \cup \{\omega\}$ и $\omega + 2 = \omega \cup \{\omega\} \cup \{\omega \cup \{\omega\}\}$ применом аксиома упаривања и уније коначан број пута. Међутим, како применити ове аксиоме **бесконачан број пута**, да би се доказало постојање скупа $\omega + \omega$? Зато је потребна аксиома замене.

Аксиома замене: Нека је $P(x, y)$ особина таква да за свако x постоји јединствено y за које она важи. За сваки скуп A постоји скуп B такав да за свако $x \in A$ постоји $y \in B$ за које важи $P(x, y)$.

$$(\forall A)((\forall x \in A)(\exists!\, y)P(x, y) \Rightarrow (\exists B)(\forall x \in A)(\exists y \in B)P(x, y).$$

Као и аксиома подскупа, аксиома замене је шема аксиома, што значи да за сваку особину постоји по једна аксиома.

Додатну интуитивну мотивацију за увођење ове аксиоме налазимо ако је упоредимо са аксиомом подскупа. Ако нам аксиома подскупа дозвољава да пролазимо кроз скуп A, проверавамо да ли његови елементи задовољавају особину $P(x)$ и оне који имају скупимо у скуп, аксиома замене нам дозвољава да пролазимо кроз скуп A и за сваки његов елемент x узмемо из скупа B одговарајуће y тако да важи $P(x, y)$.

Из ове аксиоме је могуће доказати да су аксиома упаривања и аксиома празног скупа вишак у Зермело-Френкеловој теорији. Аксиома празног скупа следи директно из аксиоме подскупа са формулом $P(X) = X \in X \wedge X \notin X$. Тада, примењујући аксиому подскупа добијамо $(\forall A)(\exists B)(\forall X)(X \in B \Leftrightarrow [X \in A \wedge X \in X \wedge X \notin X])$, што је еквивалентно са

$$(\exists B)(\forall X)\neg(X \in B).$$

Скупу B не припада ниједан скуп, па је B празан скуп.

Што се доказа аксиоме упаривања тиче, ако имамо скупове x и y, треба да докажемо постојање скупа $\{x, y\}$. Из аксиоме подскупа смо добили празан скуп: $\emptyset$. Користећи аксиому партитивног скупа добијамо $\mathcal{P}(\emptyset) = \{\emptyset\}, \mathcal{P}\big(\mathcal{P}(\emptyset)\big) = \big\{\emptyset, \{\emptyset\}\big\}$. Затим, дефинишимо особину $P(x, y, u, v) = (u = \emptyset \wedge v = x) \vee (u = \{\emptyset\} \wedge v = y)$.

Сада, користећи аксиому замене на ту особину добијамо да постоји скуп

$$\left\{v \middle| \Big(\exists u \in \mathcal{P}\big(\mathcal{P}(\emptyset)\big)\Big) P(x, y, u, v)\right\}.$$

Овај скуп је управо скуп $\{x, y\}$.

Са ових 8 аксиома је могуће дефинисати скоро све познате теореме у математици. Међутим, постоје још две аксиоме, од којих једна припада Зермело-Френкеловој теорији, а друга је потпуно независна од ње (постоји и верзија са њом и верзија без ње).

АКСИОМА РЕГУЛАРНОСТИ

Појам добро уређеног скупа је један од најважнијих појмова у теорији скупова, јер омогућује да поредимо његове елементе. Испоставља се да је могуће направити још корисних генерализација везаних за овај појам. У многим случајевима у математици је небитна „уређеност" скупа, већ је потребно да је „добар", да сваки његов подскуп има најмањи елемент. То доводи до следеће дефиниције:

Дефиниција: Ако је ρ бинарна релација у скупу A и нека је $X \subseteq A$. $a \in X$ је ρ-минимални елемент скупа X ако ни за једно $x \in X$ не важи $x\rho a$. ρ је **добро заснована релација** на скупу A ако његов сваки непразан подскуп има ρ-минимални елемент.

На пример, релација $\rho = \emptyset$ је добро заснована на сваком скупу, чак и празном. Такође, свака релација која добро уређује скуп A је и добро заснована на њему.

На којим скуповима је добро зансована релација $\in$? Иако можда не делује тако, ово питање је уско повезано са питањем постојања скупа који је елемент самог себе. С обзиром на то да такав скуп не можемо замислити, логичан одговор је да тај скуп не постоји. Међутим, на то питање не можемо одговорити са до сада уведеним аксиомама. Потребно је увести још алата за дискусију о таквом скупу.

Дефиниција: Транзитиван скуп X је **добро заснован скуп** ако и само ако је релација $\in_X$ добро заснована на скупу X, то јест ако за сваки његов непразан подскуп A постоји $a \in A$ за који важи $a \cap A = \emptyset$.

Лема: Сваки скуп X има најмањи транзитиван надскуп. Тај скуп се зове транзитивно затварање скупа X и пише се TC(X).

Доказ: Дефинишемо везу $X_0 = X, X_{n+1} = \bigcup X_n$ и скуп TC(X)= $\bigcup\{X_n | n \in \mathbb{N}\}$. Очигледно је да $X \subseteq$ TC(X) и да је TC(X) транзитиван. Ако би постојао неки транзитиван скуп T за који важи који садржи X, индукцијом се лако доказује и да X_n припада скупу T за сваки природан број n, па зато и $X_n \in$ T. ■

Уз овај појам, аналогна дефиниција добро заснованог скупа је:

Дефиниција: Скуп X је добро заснован скуп ако је TC(X) транзитиван и добро заснован.

Значај добро заснованог скупа је, између осталог, што ни за један добро заснован скуп не постоји низ чији је први члан тај скуп, а сваки следећи члан низа му припада, то јест не постоји низ скупова $X_1 \ni X_2 \ni X_3 \dots \ni X_n \dots$

Теорема: Ако је X добро заснован скуп, не постоји низ $X_0 = X, X_{n+1} \in X_n, n \in \mathbb{N}$.

Доказ: Пре доказа, важно је напоменути да, ако узмемо $X_n = X$, из ове теореме следи да не постоји скуп који припада самом себи.

Најпре претпоставимо да је X добро заснован скуп и претпоставимо да постоји наведени низ. Тада важи $X_0 \subseteq \mathrm{TC}(X)$ и по индукцији важи $X_n \subseteq \mathrm{TC}(X)$. Међутим, скуп $\{X_n | n \geq 1\}$, који је подскуп скупа $\mathrm{TC}(X)$ нема $\in$-најмањи елемент, што је контрадикција, јер је скуп $\mathrm{TC}(X)$ добро заснован. ■

Сада, да би било јасно зашто је потребна још једна аксиома, размотримо поново нашу идеју о скупу. Сетимо се Канторове интуитивне дефиниције: скуп је било која колекција одређених и засебних објеката које наша интуиција или ум могу обухватити у целину. Логично је да ови објекти морају најпре *постојати* (бар у уму) пре него што их обухватимо у целину. Први скуп за који знамо да *постоји* је $\emptyset$. Од њега даље можемо направити скуп који га садржи, $\{\emptyset\}$. Даље, од ова два скупа можемо конструисати четири: $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ и $\{\emptyset, \{\emptyset\}\}$. Од ова четири скупа можемо конструисати осам, и тако даље.

Дефиниција: Хијерархија добро заснованих скупова је:

$$V_0 = \emptyset,$$

$$V_{\alpha+1} = \mathcal{P}(V_\alpha) \text{ за сваки следбенички ординал } \alpha,$$

$$V_\alpha = \bigcup_{\beta<\alpha} V_\beta \text{ за сваки гранични ординал } \alpha.$$

Ови скупови су очигледно добро засновани и транзитивни.

Овакво заснивање скупова, које је сасвим природно, би требало да обухвати сваки скуп који можемо да замислимо. Како су сви ови скупови добро засновани, логичан закључак је следећа теорема:

Теорема: Скуп X је добро заснован ако и само ако $X \in V_\alpha$ за неки ординал α.

Доказ: Прво, претпоставимо да је X добро заснован скуп. Тада је очигледно и скуп $\mathrm{TC}(X) \cup \{\mathrm{X}\} = \mathrm{TC}(\{\mathrm{X}\})$ транзитиван и добро заснован скуп. Сада, нека је Y пресек скупова $\mathrm{TC}(\{\mathrm{X}\})$ и V_α, где је α прозивољни ординал. Докажимо $\mathrm{TC}(\{\mathrm{X}\}) = Y$. Претпоставимо супротно: да ова два скупа имају неку непразну разлику, која мора бити добро заснована, и нека је њен најмањи елемент $a \notin Y$. Сада, за свако $y \in a$ важи $y \in Y$: нека је ε најмањи ординал за који је $y \in V_\varepsilon$ и нека је σ најмањи ординал за који важи $\varepsilon[a] \in \sigma$.[7] Тада за свако $y \in a$ важи $y \in V_\varepsilon \subseteq V_\sigma$, те $a \subseteq V_\sigma$ и $a \subseteq V_{\sigma+1}$, што је контрадикторно са $a \notin Y$.

[7] $\varepsilon[a]$ је иницијални сегмент ординала ε.

Друго, претпоставимо $X \in V_\alpha$. Тада је и $X \subseteq V_\alpha$ по транзитивности, што значи да важи и TC$(X) \subseteq V_\alpha$. Због овога је и TC(X) добро заснован, па је по дефиницији и X добро заснован. ■

Одавде видимо да је, због тога што наведена хијерархија скупова представља „све скупове које можемо да замислимо" сваки скуп добро заснован. У супротном, имали бисмо скуп који захтева постојање очигледне контрадикције, бесконачног низа самопозивања. Како је немогућ формалан доказ оваквог резона, потребно је увести аксиому која то гарантује.

Аксиома регуларности: Сваки скуп је добро заснован.

Важно је на крају напоменути да ова аксиома не утиче на развијање и заснивање многих грана математике. Природне, рационалне и реалне бројеве је могуће дефинисати без ове аксиоме. Формални систем који се ослања на претходних осам аксиома се назива ZF^- теорија. Уколико њима додамо и аксиому регуларности, добијамо ZF теорију, а са аксиомом избора (која ће бити објашњена у следећој глави), ове аксиоме чине стандардну ZFC теорију скупова.

АКСИОМА ИЗБОРА

Мотивација за ову аксиому ће бити јаснија после дефинисања индексираног система скупова.

Дефиниција: Индексиран систем $F = \{F_i | i \in I\}$ **скупова** индексиран скупом I је функција F са доменом I, тако да је $F(i) = F_i$.

Ова нотација се користи када је нагласак на набрајању елемената из скупова F_i, а не на самом скупу I. Приметимо да је сваки скуп A кодомен неког индексираног система, система $\{a | a \in A\}$. Ако је $\{A_i | i \in I\}$ неки систем скупова, онда је

$$\prod_{i \in I} A_i$$

заправо Декартов производ система A_i. Важно је напоменути да скуп I не мора нужно бити скуп бројева; међутим, у већини случајева, па и у овом, I представља неки подскуп скупа природних бројева $\{0,1,2, \dots, n\}$.

Нека је $\{K_i | i \in I\}$ систем непразних скупова. Да ли је онда и Декартов производ $K = \prod_{i \in I} K_i$ непразан? Ако је I подскуп скупа природних бројева $\{0,1,2, \dots, n\}$, бирањем по једног елемента из скупова $K_0, K_1, \dots, K_n$ следи да уређена $(n+1)$-торка $(k_0, k_1, \dots, k_n)$ припада скупу K. Међутим, шта ако је I цео скуп природних бројева? Да ли је могуће истовремено изабрати по један елемент из свих K_i?

Могуће је поставити и следеће питање: Ако је X скуп међусобно дисјунктних непразних скупова, да ли постоји скуп S (**изборни скуп**) који садржи тачно по један елемент из тих непразних скупова? Кантор је тврдио да је ово очигледна истина.

Слично томе, f је **изборна функција** система скупова S ако и само ако важи $f \subseteq \prod_{i \in S} S_i$.

Пре него што продискутујемо о могућности одговора на ово питање, уочимо следећу теорему:

Теорема: Скуп A се може добро уредити неком релацијом ако и само ако скуп $\mathcal{P}(A)$ има изборну функцију.

Доказ: [8] Подсетимо се најпре да, да бисмо добро уредили скуп A, довољно је конструисати изоморфизам између скупа A и неког ординала λ.

[8] Доказ, који је извео Кантор, није комплетан ни формалан, али је интуитиван и добро илуструје значај теореме. За комплетан доказ је потребно увести рекурзивну теорему и кардиналне бројеве, које нисам изабрао да укључим у рад.

Претпоставимо прво да се скуп A може добро уредити релацијом $<$. Дефинишемо изборну функцију g за скуп $\mathcal{P}(A)$ као

$$g(x) = \begin{cases} \text{најмањи елемент x по } <, & x \neq \emptyset \\ \emptyset, & x = \emptyset \end{cases}$$

Са друге стране, претпоставимо да скуп $\mathcal{P}(A)$ има изборну функцију. Дефинишимо онда изоморфизам између скупова A и неког ординала λ. Уочимо прво функцију

$$f(0) = \begin{cases} x_0 \in A, & A \neq \emptyset \\ a, & A = \emptyset \end{cases}$$

$$f(1) = \begin{cases} x_1 \in A \setminus \{f(0)\}, & A \neq \emptyset \\ a, & A = \emptyset \end{cases}$$

и тако даље. Приметимо да ће за неко x функција f „исцрпети“ све чланове скупа A. Нека је λ најмањи ординални број за који је $f(\lambda) = a$. Тада је функција $f \restriction \lambda$ тражени изоморфизам са доменом λ и кодоменом A. ■

У примеру смо показали да сваки коначан систем скупова има изборну функцију и да се самим тим може добро уредити, јер је и партитивни скуп коначног скупа коначан. Међутим, теже је наћи изборну функцију за $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathbb{Q})$, а још теже за $\mathcal{P}(\mathbb{R})$.

Први који је приметио да није тривијално претпоставити да је *сваки* скуп могуће добро уредити је био Ернст Зермело, који је 1904. поставио аксиому избора као **теорему о добром уређењу** (тврдио је да се сваки скуп може добро уредити и претпоставио као елементарну истину аксиому избора).

Аксиома избора: Постоји изборна функција за сваки систем скупова.

До аксиоме избора је дошло још неколико математичара (Расел, Зорн) са мало другачијом формулацијом, али је тек Пол Коен 1963. године показао да је аксиому избора немогуће доказати из осталих аксиома Зермело-Френкелове теорије, а Курт Гедел је доказао да се из осталих аксиома не може ни оповргнути њена истинитост.

Примене аксиоме избора у математици су евидентне: у математичкој анализи се при дефиницији лимеса и непрекидности функције претпоставља да важи аксиома избора, а многобројне су и њене примене у доказивању својстава векторских простора, као и у теорији мера.

ЗАКЉУЧАК

„Нико нас не може истерати из раја који је Кантор створио за нас“, рекао је Давид Хилберт, један од ретких математичара који су подржавали Кантора од самог почетка теорије скупова. Од тада је прошло више од сто година, а теорија скупова и даље стоји као темељ, као мост између логике и математике и показује да о свему треба размишљати, јер ништа није елементарно као што изгледа. Од формализације Зермело-Френкелове теорије 1922. године, многи други математичари су се бавили овом облашћу (фон Нојман, Гедел, Бернејс су продубили Зермело-Френкелову теорију својом тзв. НБГ теоријом, а позната је и Морс-Кели теорија скупова), али је Зермело-Френкелова теорија и даље најкоришћенији стандард.

ЛИТЕРАТУРА

[1] K. Hrbacek, T. Jech: Introduction to Set Theory, Third Edition, Revised and Expanded, 1999

[2] А. Перовић, А. Јовановић, Б. Величковић: Теорија скупова, Математички факултет, Београд, 2007

[3] G. Tourlakis: Lectures in Logic and Set Theory, Volume II: Set Theory, 2005

[4] sr.wikipedia.org

[5] en.wikipedia.org