РЕПУБЛИЧКИ ЗАВОД ЗА УНАПРЕДУВАЊЕ
НА ОБРАЗОВАНИЕТО И ВОСПИТУВАЊЕТО
НА СРМ

СМН

**СОВРЕМЕНА
МАТЕМАТИЧКА
НАСТАВА**

Ѓ. Чупона

АЛГЕБАРСКИ СТРУКТУРИ N РЕАЛНИ БРОЕВИ

„ПРОСВЕТНО ДЕЛО"
Скопје, 1976

СОДРЖИНА

ПРЕДГОВОР

1. Оваа книга е наменета, пред сè, за наставниците по математика во основните и средните училишта со цел да им овозможи активно повторување на материјалот по алгебра. Студентите од математичката група на Природно-математичкиот факултет во Скопје ќе можат да ја користат книгава при изучувањето на елементарната алгебра. Се надеваме дека книгава ќе најде свои читатели и меѓу студентите од другите факултети ,па дури и меѓу некои ученици на средните училишта.

2. Материјалот е поделен во пет глави. Првата глава претставува краток увод во теоријата на множествата. Голем дел од својствата се формулираат без докази. Овде се изнесуваат и почетни елементи на теоријата на природните броеви. Втората глава, всушност, е увод во теријата на алгебарските структури. Овде специјално внимание се посветува на собирањето и множењето на природните броеви. Во третата глава се конструираат целите броеви, при што како мотив се зема задачата — адитивната полугрупа на природните броеви што "поекономично" да се прошири до група; множењето се дефинира така, што да се запази множењето на природни броеви, како и да важат дистрибутивните закони. И испитувањето на деливоста на целите броеви е една од најважните задачи на оваа глава. Четвртата глава има две задачи. Првата е да се изврши натамошно проширување на поимите од теоријата на алгебарските структури, какви што се поимите за конгруенција, фактор-структура, изоморфизам, прстен, поле и изоморфно сместување. Втора задача е да се направи проширување (пак што "поекономично") на доменот на целите броеви до поле, така што полето **Q** на рационалните броеви се појавува како решение на оваа задача. Да истакнеме дека во оваа глава се покажува, како од дадено поле, во кое не постои $\sqrt{-1}$, може да се добие пошироко поле, во кое $\sqrt{-1}$ постои, така што, всушност, со тоа е извршена и конструкцијата на полето **C** на комплексните броеви, ако како појдовно се земе полето **R** на реалните броеви. Реалните броеви се основен мотив на последната, т.е. петтата глава. До нив се доаѓа преку анализа на поимот подредено поле. Имено, се докажува дека постои (до изоморфизам) само едно комплетно подредено поле **R**, за кое се вели дека е полето на реалните броеви. Освен тоа, се дефинираат и се анализираат поимите: корени со природни показатели, степени со реални експоненти и бескрајни десетични дропки.

Секоја глава е поделена на соодветен број делови, кои претставуваат интегрални целини. На крајот на секој дел се формулираат вежби. Во дел од вежбите се изнесуваат нови својства. Поголемиот дел од вежбите активниот читател ќе може да ги изработи сам. Оние, пак, коишто авторот ги смета како потешки, или за кои не е извршена соодветна доволна подготовка, се означени со "*".

Со цел да се истакне дека доказот на едно својство е комплетиран, се употребува знакот ∎. Овој знак доаѓа до израз и во случај кога доказот на соодветното својство му се предушта на читателот, како и кога се дава само скица на доказот.

3. Како што се гледа од изнесениот краток приказ на книгата, нејзина основна задача е постапна конструкција на множествата броеви **N**, **Z**, **Q**, **R**, како и на соодветните структури изградени на нив. Но, имајќи го предвид и тоа што читателот ги познава тие структури, истите се користат за илустрирање на соодветни апстрактни поими и пред да бидат предмет на конкретно изучување. Овие места во книгава се издвоени на следниов начин: "·"

4. Книгите [7], [8] и [9] ѝ претходат на оваа книга. Според тоа, авторот при пишувањето на книгава се наоѓаше под нивно влијание. Се разбира, со тоа не е исцрпен списокот на дела коишто, во помала или во поголема мера, нашле свој одраз во оваа книга. Дел од ваквата литература може да се најда во приложениот список, како и во списоците на книги приложени во [7], [8] и [9].

На читателот посебно му препорачуваме да ги консултира книгите [10] и [13], во кои авторите успеале на многу достапен начин да ги изнесат своите сфаќања за математиката, односно за современата настава по математика. На читателите што имаат желба (и време) да ги прошират и продлабочат знаењата од областа третирана во книгава, им препорачуваме да ја користат и книгата [6].

5. На крајот, еве неколку совети за читателот. При првото читање (веројатно) е најдобро да не се навлегува во сите детали на доказите. Ако по ова прво читање, читателот дојде до заклучок дека има желба (или потреба) да ја проучи подетално книгава или дел од неа, тогаш би било пожелно да се "чита со молив в раце" и да се работат самостојно што поголем број од вежбите.

Скопје, декември 1975 Авторот

Сметам дека е моја должност да дадам уште неколку информации. Иницијатива за издавањето на оваа книга потекнува од колегата Р. Ансаров. Колегите А. Самарџиски и Н. Целакоски ја прочитаа првата верзија на ракописот, и нивните сугестии овозможија да се извршат соодветни подобрувања. Студентите Д. Димовски и Ж. Попеска ја препишаа конечната верзија на ракописот, при што придонесоа да се намали бројот на грешките. На сите нив им благодарам за укажаната помош. На крајот, треба да се истакне и тоа дека книгава немаше да излезе од печат ако не најдеше соодветно разбирање кај колективите на Републичкиот завод за унапредување на образованието и воспитувањето, "Просветно дело" и Универзитетската печатница.

Скопје, август 1976 Авторот

1. ЕЛЕМЕНТИ ОД ТЕОРИЈАТА НА МНОЖЕСТВАТА

1.1. МНОЖЕСТВА

Со содржината на поимот множество е запознат, речиси секој човек, независно од степенот на неговото образование. Во секојдневниот живот се употребуваат други имиња, како што се: гарнитура, колекција и друго. Објектите што го формираат множеството се нарекуваат елементи на тоа множество. Секоја конкретна наука се карактеризира со природата на елементите од множествата што се предмет на нејзиното изучување. Теоријата на множествата (а и математиката, воопшто), обично, не навлегува во природата на множествата, т.е. изучува апстрактни множества.

Најчесто, множествата ќе ги означуваме со големите букви на латиницата, а елементите со малите букви од истата азбука. (Сепак, ќе употребуваме и други симболи, како и букви од други азбуки). Притоа, ќе избегнуваме едно конкретно множество, да го означиме со некоја од буквите X, Y, Z, X_1, Y_1, Z_1, ..., бидејќи со овие букви ќе означуваме "променливи" множества; во иста смисла, со x, y, z, x_1, y_1, z_1, ... ќе ги означуваме "променливите" елементи.

Множествата M и N ги сметаме за *еднакви*, ако и само ако тие се состојат од исти елементи, т.е. M и N се различни ознаки за едно исто множество; во овој случај пишуваме $M = N$. (Натаму, наместо "ако и само ако", ќе пишуваме "акко").

Ако множеството M се состои од елементите $a, b, c, d, e, \ldots$, ќе пишуваме: $M = \{a, b, c, d, e, \ldots\}$. Притоа, распоредот на елементите во $\{\ldots\}$ не го сметаме за битен, а допуштаме еден ист елемент да се јавува повеќе пати. Со други зборови, ги сметаме за точни, на пример, следниве равенства:

$$\{a, b, c\} = \{c, a, b\} = \{b, a, b, c, a, b\}.$$

Наместо "x е елемент на множеството X", ќе пишуваме "$x \in X$", а наместо "y не е елемент на множеството X", "$y \notin X$". Во оваа смисла, имаме: $a \in \{a, b, c\}$, $d \notin \{a, b, c\}$.

За множеството M велиме дека е *подмножество* на множеството N акко секој елемент на M е елемент и на N. Во тој случај пишуваме $M \subseteq N$. Велиме, исто така, дека N е надмножество на M. За M велиме дека е *вистинско подмножество* на N, акко $M \subseteq N$ и постои елемент во N што не е елемент на M во овој случај пишуваме: $M \subset N$.

Релациите $\subseteq$ и $\subset$ се викаат релации за *инклузија*. (Попрецизно, тие се ознаки на релациите за инклузија. За $\subset$ ќе велиме дека е стриктна инклузија).

Негациите на $=$, $\subseteq$, $\subset$ ќе ги означуваме, обично, со $\neq$, $\nsubseteq$, $\not\subset$ — соодветно.

Примерите на множества $\{1\}$, $\{1,2\}$, со еден односно со два елемента, кажуваат дека во едно множество не мора да има "многу" елементи. Се покажува како корисно да се допушти егзистенција на "множество" без елементи, т.е. на *празно множество*. Притоа се смета дека постои само едно празно множество. Празното множество ќе го означуваме со $\varnothing$ и ќе го сметаме како подмножество од секое множество, т.е. имаме $\varnothing \subseteq M$ за секое множество M, а $\varnothing \subset N$ за секое непразно множество N.

Ако M е множество, тогаш со $B(M)$ го означуваме множеството чиишто елементи се подмножествата на M, т.е.:

$$X \in B(M) \text{ акко } X \subseteq M.$$

За $B(M)$ велиме дека е *булеан* на M.[1)]

Еве неколку примери:

1) $B(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$.

2) $B(\{1\}) = \{\varnothing, \{1\}\}$.

3) $B(\varnothing) = \{\varnothing\}$. Овде треба да се има предвид дека постои битна разлика меѓу $\{\varnothing\}$ и $\varnothing$; имено, $\{\varnothing\}$ има еден елемент, додека $\varnothing$ е множество без елементи.

Сега ќе формулираме неколку својства, чијашто вистинитост е непосредно јасна од погоре дадените дефиниции.

1°. (i) $X = X$; (ii) $X \subseteq X$; (iii) $X \not\subset X$. ▒

2°. (i) Ако $X = Y$, тогаш $Y = X$;
(ii) Ако $X = Y$ и $Y = Z$, тогаш $X = Z$;
(iii) Ако $X \subseteq Y$ и $Y \subseteq Z$, тогаш $X \subseteq Z$. ▒

3°. $X = Y$ акко $X \subseteq Y$ и $Y \subseteq X$. ▒

При докажување еднаквоста на две множества многу често се користи својството **3°**. Според него, две множества се еднакви акко секое од нив е подмножество од другото.

Една од најважните задачи на книгава е да се даде постапна конструкција на множествата природни, цели, рационални, реални и комплексни броеви. За овие множества ќе употребуваме специјални ознаки. Имено, множеството на природните броеви го означуваме со $\mathbf{N}$ (притоа, сметаме дека $0 \in \mathbf{N}$), на целите со $\mathbf{Z}$, на рационалните со $\mathbf{Q}$, на реалните со $\mathbf{R}$ и на комплексните броеви со $\mathbf{C}$.

[1)] Да забележиме дека, обично, се употребува терминот *"партитивно множество на M"*, наместо овде употребениот термин *"булеан на M"*, а во таа смисла се пишува $P(M)$, наместо $B(M)$.

На овие множества броеви ќе им бидат посветени посебни делови на книгава, но сепак, раководејќи се од тоа што читателот е запознат со нив, тие често ќе бидат користени за илустрации, и пред да бидат предмет на изучување.

ВЕЖБИ. 1. Да се наведат неколку примери на множества што се предмет на изучување во: а) математиката, б) физиката, в) биологијата, г) економијата.

2. Да се определи булеанот на: а) $\{1, 2, 3\}$; б) $\{a, b, 1, 2\}$; в) $\{0, \square, \Delta\}$.

3. Да се покаже дека: а) ако $X = Y$ и $Y \subset Z$, тогаш $X \subset Z$; б) $X \subseteq Y$ и $Y \subset Z$ повлекува $X \subset Z$; в) $B(X) \subseteq B(Y)$ акко $X \subseteq Y$; г) $B(X) \subset B(Y)$ акко $X \subset Y$; д) $B(X) = B(Y)$ акко $X = Y$.

4. Нека $A = \{1, 2, 3\}$, $B = \{1, 2, 3, a, b, c\}$, $C = \{1, 2, a, b, d\}$. Да се определат сите множества M, такви што: а) $A \subset M$ и $M \subset B$; б) $A \subset M$ и $M \subset C$; в) $C \subset M$ и $M \subset A$.

1.2. ИСКАЗИ И ИСКАЗНИ ФУНКЦИИ

Во математиката се најважни реченицитe во кои се изнесуваат соодветни тврдења; таквите реченици ги нарекуваме искази. Попрецизно, за една реченица велиме дека е *исказ* ако таа е: (i) вистинита (т.е. точна), или (ii) невистинита (т.е. неточна), но (iii) не е и вистинита и невистинита. Така, $2 \in \{1, 2, 3\}$ е вистинит исказ, а $1 \notin \{1, 2, 3\}$ е невистинит исказ. Исказите ги означуваме со буквите: p, q, s, ... за кои велиме дека се исказни променливи. Ако p е вистинит исказ, тогаш пишуваме $\tau(p) = \top$ (читаме "тау од пе е те", односно дека "вредноста на вистинитост на p е $\top$"). Ако, пак, исказот q е невистинит, пишуваме $\tau(q) = \bot$ ("тау од ку е не те"). Поедноставно, пишуваме $p = \top$ и $q = \bot$, наместо $\tau(p) = \top$, $\tau(q) = \bot$.

Со помош на логичките операции: негација ($\neg$), конјункција ($\wedge$), дисјункција ($\vee$), импликација ($\Rightarrow$) и еквиваленција ($\Leftrightarrow$), од исказите p и q ги формираме посложените искази $\neg p$, $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$. Вистинитосните вредности на новите искази се дефинирани како што е покажано во приложените шеми:

¬:

p	¬p
T	⊥
⊥	T

∧:

p	q	p∧q
T	T	T
T	⊥	⊥
⊥	⊥	⊥
⊥	T	⊥

∨:

p	q	p∨q
T	T	T
T	⊥	T
⊥	T	T
⊥	⊥	⊥

⇒

p	q	p⇒q
T	T	T
T	⊥	⊥
⊥	T	T
⊥	⊥	T

⇔

p	q	p⇔q
T	T	T
T	⊥	⊥
⊥	T	⊥
⊥	⊥	T

Според тоа:

$\neg p$ е вистинит акко p е невистинит;
$p \wedge q$ е вистинит акко p и q се вистинити;
$p \vee q$ е невистинит акко p и q се невистинити;
$p \Rightarrow q$ е невистинит акко p е вистинит а q невистинит;
$p \Leftrightarrow q$ е вистинит акко $\tau(p) = \tau(q)$.

Со повеќекратна примена на логичките операции се добиваат *исказни формули*, какви што, покрај $\neg p$, $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$, се и следниве: $\neg(\neg p)$, $(p \wedge q) \Rightarrow (p \vee q)$, $(p \wedge (p \Rightarrow q)) \Rightarrow q)$ и др.[1)]

Исказните формули ги означуваме со: $\varphi, \psi, \ldots$ За исказната формула φ велиме дека е *логички закон* (односно *тавтологија*) акко при која било замена на исказните букви што фигурираат во φ со конкретни искази (односно со $\top$ и $\bot$) се добива вистинит исказ (т.е. исказ со вистинитосна вредност $\top$). Во тој случај пишуваме $\models \varphi$. Ќе приложиме список на неколку логички закони.

1°. $\models p \vee \neg p$ (закон за исклучување на третото).
2°. $\models \neg(p \wedge \neg p)$ (закон за контрадикција).
3°. $\models p \wedge (p \Rightarrow q) \Rightarrow q$ (закон за скратување).
4°. $\models (p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ (закон за силогизам).
5°. $\models \neg\neg p \Leftrightarrow p$ (закон за двојна негација).
6°. $\models (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ (закон за контрапозиција).

Една декларативна реченица (искажана со зборови или со соодветни симболи), во којашто фигурира една или повеќе променливи, се вика *исказна функција*, акко при секоја замена на променливите со конкретни објекти се добива конкретен исказ.

Да разгледаме неколку примери.

1) Со $x \in \{1, 2, 3\}$ е определена исказна функција. Од неа се добива вистинит исказ, ако наместо x се замени некој од елементите 1, 2, 3, а невистинит — во секој друг случај.

2) Од исказната функција $1 \in X$ се добива вистинит исказ ако X се замени со конкретно множество во кое се содржи 1 како елемент.

3) $x \in X$ е исказна функција со две променливи x и X. Заменувајќи го X со $\{1, 2, 3\}$ ја добиваме исказната функција од 1), а во иста смисла, ставајќи 1 наместо x, се добива исказната функција од 2).

За една исказна функција велиме дека е *вистинита* ако е вистинит секој конкретен исказ што може да се добие од таа функција.

Еве неколку примери на вистинити исказни функции.

7°. (i) $x \notin \varnothing$; (ii) $\varnothing \subseteq X$.
8°. (i) $X \subseteq Y \Leftrightarrow (x \in X \Rightarrow x \in Y)$; (ii) $X = Y \Leftrightarrow (x \in X \Leftrightarrow x \in Y)$.

[1)] Натаму, некои загради ќе бидат изоставувани; на пример, претпоследната формула ќе ја пишуваме во облик $p \wedge q \Rightarrow p \vee q$.

На крајот од претходниот дел се изнесени уште седум примери (**1.1.** $1° - 3°$) на вистинити исказни функции.

Нека M е дадено множество, а $\psi(x)$ дадена исказна функција. Ако M се состои од оние конкретни објекти кои, заменети во $\psi(x)$ наместо x, даваат точни искази, тогаш велиме дека M е дефинирано со $\psi(x)$ и пишуваме:

$$M = \{ x \mid \psi(x)\}. \tag{1}$$

Велиме, исто така, дека M е *решение на исказната функција* $\psi(x)$.

Така, на пример, имаме:

4) $\{1\} = \{x \mid x = 1\}$, $\{1, 2\} = \{x \mid x = 1 \vee x = 2\}$,
$\varnothing = \{x \mid x \neq x\}$.

Поопшто:

9°. Ако M е множество, тогаш:

(i) $M = \{x \mid x \in M\}$; (ii) $B(M) = \{X \mid X \subseteq M\}$. ∎

За исказната функција $\psi(x)$ велиме дека е *вистината на множеството* M акко:

$$\{x \mid x \in M \wedge \psi(x)\} = M, \tag{2}$$

т.е. акко $\psi(x)$ е вистинита за секој елемент од M. Во тој случај велиме дека е вистинит исказот:

$$(\forall x \in M)\, \psi(x). \tag{3}$$

Знакот $\forall$ се чита "за секој" и се вика *знак за универзален квантификатор*.

Исказот

$$(\exists x \in M)\ \psi(x) \tag{4}$$

го сметаме за вистинит акко:

$$\{x \mid x \in M \wedge \psi(x)\} \neq \varnothing, \tag{5}$$

т.е. акко $\psi(x)$ е вистинита барем на еден елемент од M. Знакот $\exists$ се чита "за некој" (или "постои некој") и се вика *знак за егзистенцијален квантификатор*.

Да претпоставиме дека $\psi(x, y)$ е исказна функција со две променливи во M[1]. Секој од следниве два израза:

$$(\forall x)\ \psi(x, y), \quad (\exists y)\ \psi(x, y),$$

[1]) Обично ќе претпоставуваме дека променливите $x, y, \ldots$ се менуваат во едно фиксно множество (во случајов M), за кое велиме дека е универзално; во овој случај, на место $(\forall x \in M)$, $(\exists x \in M)$, пишуваме $(\forall x)$, $(\exists x)$, соодветно.

определува по една исказна функција; да ги означиме со $\psi_1(y)$, $\psi_2(x)$, соодветно. Смислата на овие исказни функции следува од дефинициjата на квантификаторите. Имено, ако a е фиксен елемент од M, тогаш $\psi_1(a)$ е вистинит исказ ако за секој елемент $b \in M$ исказот $\psi(b, a)$ е вистинит, додека $\psi_2(a)$ е вистинит, акко постои елемент $c \in M$, таков што $\psi(a, c)$ е вистинит.

Можеме да ги формираме и следниве искази:

$$(\forall x)\ (\forall y)\ \psi(x, y), \quad (\forall y)\ (\forall x)\ \psi(x, y), \quad (\exists x)\ (\forall y)\ \psi(x, y),$$

$$(\forall y)\ (\exists x)\ \psi(x, y), \quad (\exists x)\ (\exists y)\ \psi(x, y), \quad (\exists y)\ (\exists x)\ \psi(x, y)$$

чија смисла се определува лесно ако се има предвид значењето на квантификаторите.

Ако множеството M го сметаме за универзално, тогаш исказната, функција $\varphi(x)$ сметаме дека е вистинита акко е вистинита на M. Значи, $\varphi(x)$ е вистинита акко е вистинит исказот $(\forall x \in M)\,\varphi(x)$. Поради ова, при формулирање на соодветни својства го изоставуваме "најлевиот" израз $(\forall x)$. Во иста смисла, наместо $(\forall x)\ (\forall y)\ (\exists z)\,\varphi(x, y, z)$, ќе пишуваме само $(\exists z)\,\varphi(x, y, z)$.

Да разгледаме уште два примера.

5) Ако M е множеството граѓани на Југославија, тогаш исказот "$(\forall x)\ (\exists y)$ x и y се родени во иста година" секако е вистинит, но исказот "$(\exists x)\ (\forall y)$ x и y се родени во иста година" е невистинит.

6) Исказот "$(\exists x)\ x^2 + 1 = 0$" е невистинит во $\mathbf{R}$, но истиот исказ е вистинит во $\mathbf{C}$. (Од ова се гледа дека универзалното множество е битно за вистинитоста на соодветни искази).

Да забележиме дека натаму, често пати, под *тврдење* ќе подразбираме вистинит исказ, односно вистинита исказна функција. Имајќи го предвид и фактот што во секое тврдење се изнесуваат соодветни својства на математички објекти, и терминот *својство* ќе го употребуваме во смисла на тврдење, т.е. вистинит исказ.

ВЕЖБИ. 1. Да се покаже дека:

а) ако p и $p \Rightarrow q$ се вистинити, тогаш и q е вистинит;

б) ако q е невистинит, а $\neg p \Rightarrow q$ вистинит, тогаш и p е вистинит;

в) ако $p \Rightarrow q$ и $q \Rightarrow r$ се вистинити, тогаш и $p \Rightarrow r$ е вистинит.

2. Да се докажат законите **1°—6°**.

3. Да се докажат законите:

а) $\models p \wedge p \Leftrightarrow p$; $\models p \vee p \Leftrightarrow p$; $\models p \wedge (p \vee q) \Leftrightarrow p$; $\models p \vee (p \wedge q) \Leftrightarrow p$;

б) $\models p \wedge q \Leftrightarrow q \wedge p$; $\models p \vee q \Leftrightarrow q \vee p$;
$\models p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$; $\models (p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$.

в) $\models p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$;
$\models p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$;

г) $\models p \Leftrightarrow \neg\neg p$; $\models \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$; $\models \neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$;

д) $\models (p \Rightarrow q) \Leftrightarrow \neg p \vee q$; $\models (p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$.

4. Операцијата исклучителна дисјункција $\veebar$ се дефинира со: $p \veebar q = \top$ ако ($p = \top$ $q = \bot$) или ($p = \bot$, $q = \top$). Да се докажат законите:

$$\models p \veebar q \Leftrightarrow q \veebar p; \quad \models p \veebar (q \veebar r) \Leftrightarrow (p \veebar q) \veebar r;$$
$$\models p \wedge (q \veebar r) \Leftrightarrow (p \wedge q) \veebar (p \wedge r).$$

5. Нека $A = \{1, 2, 3\}$, $B = \{1, 2, a\}$, $C = \{1, 2\}$. Дали е вистинит исказот: $A \subset B \wedge B \subset C \Rightarrow A \subset C$?

6. Нека $\varphi(x)$ и $\psi(x)$ се исказни функции дефинирани во универзалното множество M. Да се покаже дека:

а) $\varphi(x) \Rightarrow \psi(x)$ е вистинита акко $\{x \mid \varphi(x)\} \subseteq \{x \mid \psi(x)\}$;

б) $\varphi(x) \Leftrightarrow \psi(x)$ е вистинита акко $\{x \mid \varphi(x)\} = \{x \mid \psi(x)\}$.

(Во случајот а) велиме дека $\psi(x)$ е *последица* од $\varphi(x)$, а во б) дека $\varphi(x)$ и $\psi(x)$ се *еквивалентни* на M. Да го спомнеме и тоа дека $\{x \mid \varphi(x)\}$ се пишува наместо $\{x \mid \varphi(x) \wedge x \in M\}$, бидејќи по претпоставка $\varphi(x)$ е дефинирана само за елементите на M.)

7. Да се покаже дека се точни исказите:

а) $\neg(\forall x)\varphi(x) \Leftrightarrow (\exists x)\neg\varphi(x)$; $\quad \neg(\exists x)\varphi(x) \Leftrightarrow (\forall x)\neg\varphi(x)$.

б) $(\exists x)(\forall y)\varphi(x, y) \Rightarrow (\forall y)(\exists x)\varphi(x, y)$

в) $(\forall x)(\forall y)\varphi(x, y) \Leftrightarrow (\forall y)(\forall x)\varphi(x, y)$;
$(\exists x)(\exists y)\varphi(x, y) \Leftrightarrow (\exists y)(\exists x)\varphi(x, y)$.

(Натаму често ќе го изоставуваме изразот "исказите се точни".).

8. Ако M е дадено универзално множество, а $\varphi(x)$ исказна функција на M, тогаш за $\{x \mid \varphi(x) \wedge x \in M\} = \{x \mid \varphi(x)\}$ велиме дека е *решение* на $\varphi(x)$. Ако $M = \{1, 2, 3, 4, 5\}$, да се определат решенијата на следниве исказни функции:

а) $x=1 \vee x=2$; б) $x=1 \vee x=a$; в) $x=x$; г) $x \neq x$; д) $x \in \{1, 2\} \vee x \in \{1, 3\}$;
ѓ) $x \in \{1, 2\} \Rightarrow x \in \{1, 3\}$.

9. Нека **Z** е универзално множество. Да се решат исказните функции:

а) x е делител на 12; б) 12 е делител на x; в) x е заемно прост со 50 и $|x| < 50$.

Потоа, истото да се направи за случај кога универзално множество е **N**.

10. Да се реши секоја од приложените исказни функции (т.е. равенки).

а) $x^4 - 1 = 0$; б) $x^4 + 1 = 0$; в) $x^2 - 10x + 23 = 0$.

Да се разгледаат одвоено случаите кога универзално е некое од множествата **Q**, **R**, **C**.

1.3. ОПЕРАЦИИ СО МНОЖЕСТВА

Овде ќе ги разгледаме операциите: пресек, унија, разлика, комплемент и декартов (односно директен) производ на множества.

Ако M и N се произволни множества, тогаш нивниот *пресек* $M \cap N$ и *унија* $M \cup N$ се дефинираат со:

$$x \in M \cap N \Leftrightarrow x \in M \wedge x \in N, \tag{1}$$

$$x \in M \cup N \Leftrightarrow x \in M \vee x \in N. \tag{2}$$

Инаку напишано:

$$M \cap N = \{x \mid x \in M \wedge x \in N\}, \tag{1'}$$

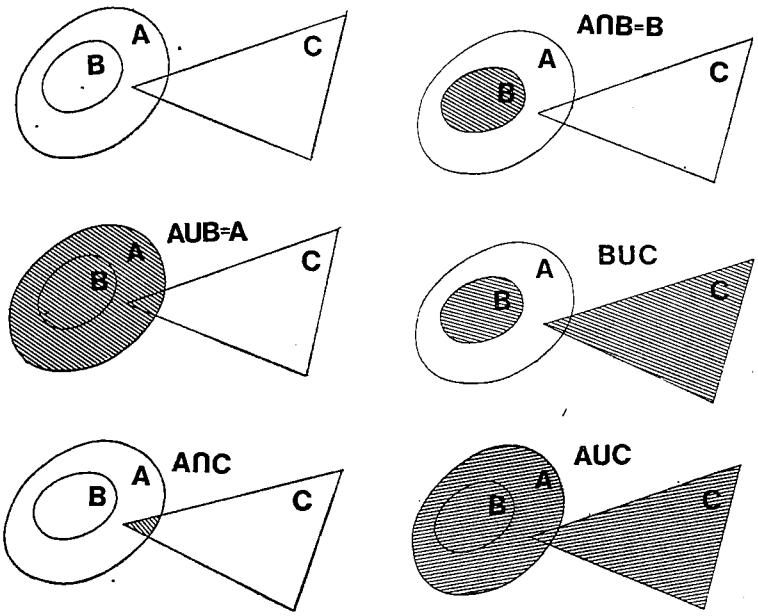
$$M \cup N = \{x \mid x \in M \vee x \in N\}. \tag{2'}$$

Да разгледаме два примера.

1) Ако $A = \{a, b, c, d, e\}$, $B = \{a, b, c, 1, 2, 3\}$, тогаш:

$A \cap B = \{a, b, c\}$, $A \cup B = \{a, b, c, d, e, 1, 2, 3\}$.

2) Ако A, B и C се множества точки од трите фигури расположени како на цртежот, тогаш множествата $A \cap C$, $A \cup C$, $A \cap B$ и $A \cup B$ се определени со исшрафираните делови од цртежите.



За две множества M и N велиме дека се *дисјунктни* акко немаат заеднички елементи, т.е. акко $M \cap N = \varnothing$. (Во примерот 2) дисјунктни се множествата B и C.).

Од дефинициите (1) и (2) непосредно е јасно дека се точни следниве својства:

1°. (i) $X \cap Y \subseteq X$; $X \cap Y \subseteq Y$;
(ii) $X \subseteq X \cup Y$; $Y \subseteq X \cup Y$. ∎

2°. (i) $X \cap Y = X \Leftrightarrow X \subseteq Y$.
(ii) $X \cup Y = X \Leftrightarrow Y \subseteq X$. ∎

3°. $X_1 \subseteq Y_1,\ X_2 \subseteq Y_2 \Rightarrow X_1 \cap X_2 \subseteq Y_1 \cap Y_2,\ X_1 \cup X_2 \subseteq Y_1 \cup Y_2$.[1] ∎

4°. (i) $X \cap \varnothing = \varnothing$; (ii) $X \cup \varnothing = X$. ∎

5°. (i) $X \cap X = X$; (закони за идемпотентност)
(ii) $X \cup X = X$. ∎

6°. (i) $X \cap Y = Y \cap X$; (закони за комутативност)
(ii) $X \cup Y = Y \cup X$. ∎

7°. (i) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$; (закони за асоцијативност)
(ii) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$. ∎

8°. (i) $x \notin X \cap Y \Leftrightarrow x \notin X \vee x \notin Y$;
(ii) $x \notin X \cup Y \Leftrightarrow x \notin X \wedge x \notin Y$. ∎

9°. (i) $X \cap (X \cup Y) = X$; (закони за апсорпција)
(ii) $X \cup (X \cap Y) = X$. ∎

Читателот треба да биде во состојба да ги докаже и следниве две својства:

10°. (i) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$; (закони за дистрибутив-
(ii) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. ∎ ност)

11°. $X \cap Y = X \cap Z,\ X \cup Y = X \cup Z \Rightarrow Y = Z$. ∎

Разликата $M \setminus N$ на множеството M со множеството N се дефинира со:

$$x \in M \setminus N \Leftrightarrow x \in M \wedge x \notin N, \tag{3}$$

т. е.

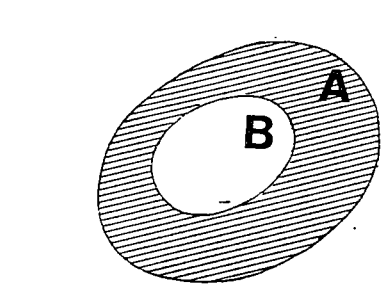
$$M \setminus N = \{x \mid x \in M \wedge x \notin N\}. \tag{3'}$$

Ако A и B се множествата од примерот 1), тогаш:

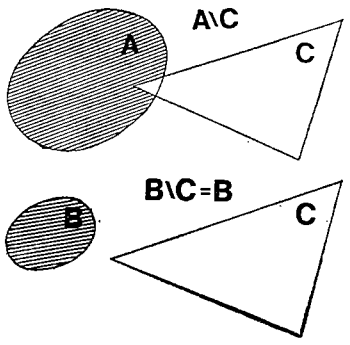
$$A \setminus B = \{d, e\},\quad B \setminus A = \{1, 2, 3\},\quad A \setminus A = \varnothing.$$

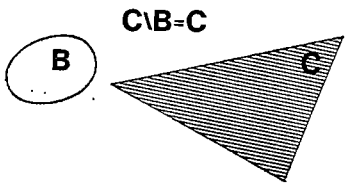
Ако, пак, A, B и C се множествата точки од примерот 2), тогаш $A \setminus B$, $A \setminus C$, $B \setminus C$, $C \setminus B$ и $C \setminus A$ се определени како што е обележано во приложените цртежи:

[1]) Овде запирката се употребува наместо знакот за конјункција. Во иста смисла пишуваме и $a, b \in M$, наместо $a \in M$ и $b \in M$, или $A, B \subseteq M$, наместо $A \subseteq M$ и $B \subseteq M$.

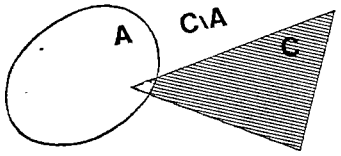


A\B





B\A=∅



Ќе формулираме неколку својства на операцијата разлика.

12°. (i) $X \setminus Y \subseteq X$; (ii) $(X \setminus Y) \cap Y = \emptyset$; (iii) $X \cup Y = X \cup (Y \setminus X)$. ▒

13°. (i) $X \setminus X = \emptyset$; (ii) $X \setminus \emptyset = X$; (iii) $\emptyset \setminus X = \emptyset$. ▒

14°. (i) $X \setminus Y = \emptyset \Leftrightarrow X \subseteq Y$; (ii) $X \setminus Y = X \Leftrightarrow X \cap Y = \emptyset$. ▒

15°. $x \notin X \setminus Y \Leftrightarrow x \notin X \vee x \in Y$. ▒

16°. $X \subseteq Y \Rightarrow X = Y \setminus (Y \setminus X)$. ▒

17°. (i) $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$;
(ii) $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$. ▒

Операцијата што ќе ја дефинираме сега е позната под името симетрична разлика. Имено, *симетрична разлика* $M \dot{-} N$ на множествата M и N се дефинира со:

$$M \dot{-} N = (M \cup N) \setminus (M \cap N). \tag{4}$$

Според тоа: ▬

18°. $M \dot{-} N$ се состои од елементите што припаѓаат на едно и само на едно од множествата M, N. ▒

Од (4) (или **18°**) се гледа дека:

19°. $X \dot{-} Y = Y \dot{-} X$. ▒

20°. (i) $X \dot{-} X = \varnothing$; (ii) $X \dot{-} \varnothing = X$. ▒

Ќе докажеме две својства во врска со операцијата $\dot{-}$, а, имено, дека таа е асоцијативна, како и дека $\cap$ е дистрибутивен спрема $\dot{-}$.

21°. $X \dot{-} (Y \dot{-} Z) = (X \dot{-} Y) \dot{-} Z$.

Доказ. Според **18°**, левата и десната страна се состојат од елементите што припаѓаат на сите три множества X, Y, Z или само на едно од нив. ▒

22°. $X \cap (Y \dot{-} Z) = (X \cap Y) \dot{-} (X \cap Z)$.

Доказ. И двете страни на равенството се состојат од елементите што припаѓаат на X и припаѓаат на едно и само на едно од множествата Y, Z. ▒

Ако $X \subset M$, тогаш множеството на елементи од M што не се содржани во X се вика *комплемент* на X во M и се означува со $\overset{C}{M}X$, или само со ${}^{C}X$, бидејќи M го сметаме за фиксно. Според тоа:

$$ {}^{C}X = M \setminus X. \text{ [1]} \tag{5}$$

Следните својства се познати како *Де Морганови теореми*:

23°. (i) ${}^{C}({}^{C}X) = X$;

(ii) ${}^{C}(Y \cup Z) = {}^{C}Y \cap {}^{C}Z$;

(iii) ${}^{C}(Y \cap Z) = {}^{C}Y \cup {}^{C}Z$;

(iv) $X \subset Y \Leftrightarrow {}^{C}Y \subset {}^{C}X$. ▒

Пред да дадеме дефиниција на операцијата декартов производ, ќе разгледаме уште еден пример.

3) Нека $A = \{a, b, c\}$, $B = \{a, b, 1, 2\}$ и нека формираме ново множество C со:

$$C = \{(a,a),\ (a, b),\ (a, 1),\ (a, 2),\ (b, a),\ (b, b),\ (b, 1),\ (b, 2)\ (c, a),\ (c, b),\ (c, 1),\ (c, 2)\}.$$

Притоа сметаме дека сите дванаесет елементи што го определуваат C се различни. Значи, C се состои од сите подредени двојки (x, y) каде што $x \in A$, а $y \in B$, и притоа $(x_1, y_1) = (x_2, y_2)$ акко $x_1 = x_2$, $y_1 = y_2$. За C велиме дека е декартов, односно директен, производ на A и B и пишуваме $C = A \times B$.

---

[1]) Почесто, комплементот на X во M се означува со X', но сепак овде ќе ја избегнуваме таа ознака за комплемент.

Ситуацијата е иста и во општиот случај. Имено, ако M и N се две произволни множества, тогаш *декартовиот производ* $M \times N$ е множество што се состои од сите подредени двојки (x, y), каде што $x \in M$ и $y \in N$. Притоа:

$$(x_1, y_1) = (x_2, y_2) \Leftrightarrow x_1 = x_2,\ y_1 = y_2. \tag{6}$$

Еве неколку својства на декартовиот производ.

24°. (i) $\varnothing \times Y = \varnothing$; (ii) $X \times \varnothing = \varnothing$. ▒

25°. $X_1 \subseteq X_2,\ Y_1 \subseteq Y_2 \Rightarrow X_1 \times Y_1 \subseteq X_2 \times Y_2$. ▒

26°. $X \times Y = Y \times X \Leftrightarrow X = Y$. ▒

ВЕЖБИ. **1.** Да се докажат "што повеќе" од својствата погоре формулирани без доказ. (Во врска со оваа вежба напоменуваме дека и во натамошното изнесување на материјалот првата вежба од секој оддел ќе се состои во дообјаснување на тврдењата за кои обично ќе велиме дека се "јасни" или "очигледни"; исто така, ќе треба да се докажуваат својствата што во текстот не се докажани. Затоа, овие вежби нема да ги формулираме експлицитно. Значи, оваа вежба има елементи на "повторување на материјалот", па затоа е пожелно таа да се работи во две етапи, пред решавањето на другите задачи и по нивното решавање.)

2. Да се верифицираат **16°**, **17°**, **21°** и **22°** на конкретен пример кога A, B и C се множества точки од еден триаголник, квадрат и круг што лежат во една рамнина.

3. Да се покаже дека:

а) $(X \cup Y) \cap (Y \cup Z) \cap (Z \cup X) = (X \cap Y) \cup (Y \cap Z) \cup (Z \cap X)$;

б) $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup Z$;

в) $X \cap ((X \cap Y) \cup Z) = (X \cap Y) \cup (X \cap Z)$;

г) $(X \times Y) \cap (Z \times T) = (X \cap Z) \times (Y \cap T)$;

д) $B(X \cap Y) = B(X) \cap B(Y)$; ѓ) $B(X) \cup B(Y) \subseteq B(X \cup Y)$, за кои било множества X, Y, Z, T.

4. Во кој случај се точни равенствата:

а) $A \cup (B \setminus C) = (A \cup B) \setminus C$; б) $B(A \cup B) = B(A) \cup B(B)$;

в) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$?

5. Ако A и B се подмножества од M, да се покаже дека:

а) $^c(A \setminus B) = {}^cA \cup B$; б) $A \setminus B = A \cap {}^cB$;

в) $^c(A \cup B) \cap {}^c({}^cA \cup {}^cB) = \varnothing$; г) $^c({}^c(A \cup B) \cup (A \cup {}^cB)) = B \setminus A$.

6. Да се даде пример на три множества A, B и C, така што:

а) $A \cap B = A \cap C,\ B \neq C$; б) $A \cup B = A \cup C,\ B \neq C$.

7. Да се покаже дека ако постои множество X такво што $A \cap X = B$, $A \cup X = C$, тогаш тоа е еднозначно определено. Да се изнесат нужните и доволните услови што треба да ги задоволуваат множествата A, B и C за да постои множество X со спомнатите својства.

8. Нека $\varphi(x)$ и $\psi(x)$ се исказни функции во едно универзално множество M. Да се покаже дека:

а) $\{x \mid \varphi(x)\} \cap \{x \mid \psi(x)\} = \{x \mid \varphi(x) \wedge \psi(x)\}$;

б) $\{x \mid \varphi(x)\} \cup \{x \mid \psi(x)\} = \{x \mid \varphi(x) \vee \psi(x)\}$;

в) $^c\{x \mid \varphi(x)\} = \{x \mid \neg \varphi(x)\}$;

г) $\{x \mid \varphi(x) \Rightarrow \psi(x)\} = {}^c\{x \mid \varphi(x)\} \cup \{x \mid \psi(x)\}$.

1.4. ПРЕСЛИКУВАЊА

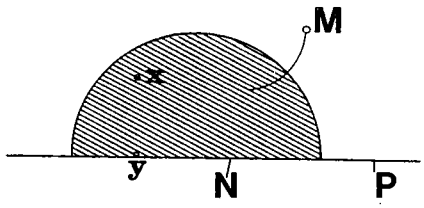
Нека M и N се две непразни множества и нека на секој елемент $x \in M$ му е придружен, по некаков пропис f, еднозначно определен елемент $y \in N$. Тогаш велиме дека f е *пресликување* од M во N и пишуваме $f: M \to N$; за y велиме дека е *слика* на x и пишуваме $y = f(x)$, $f: x \to y$, или $x \xrightarrow{f} y$. Множеството M го нарекуваме *домен*, а N *кодомен* на f и пишуваме $M = dm\, f$, $N = cdm\, f$. Значи, f е пресликување со домен M и кодомен N акко:

$$(\forall x \in M)\ (\exists!\ y \in N)\ \ y = f(x).^{1)} \tag{1}$$

За две пресликувања f_1 и f_2 сметаме дека се еднакви акко имаат еднакви домени, еднакви кодомени и $(\forall x \in M)\ f_1(x) = f_2(x)$. (2)

Да разгледаме еден пример.

1) Нека M е множеството точки од полукругот, N множеството точки на дијаметарот, а P множеството точки од правата на која се наоѓа дијаметарот, како на цртежот. Проектирајќи ја секоја точка ортогонално од M на дијаметарот добиваме две пресликувања $f: M \to N$ и $g: M \to P$. Притоа, имаме $f(x) = g(x)$ за секој $x \in M$, но сепак f и g се различни пресликувања, бидејќи кодомените им се различни.



Нека $f: L \to M$, $g: M \to N$ се две пресликувања. Ако ставиме:

$$(\forall x \in L)\ h(x) = g(f(x)) \tag{3}$$

добиваме пресликување $h: L \to N$, за кое велиме дека е *производ* (или *состав*) на f и g и пишуваме: $h = gf$. (Да се обрати внимание на редоследот!). Значи:

$$(\forall x \in L)\ \ gf(x) = g(f(x)). \tag{3'}$$

Да разгледаме уште еден пример.

2) Нека $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$, $C = \{a, b, c\}$ и нека $f: A \to B$, $g: B \to C$ се пресликувања определени со:

$f: 1 \to 3,\ 2 \to 4,\ 3 \to 6$; $g: 3 \to a,\ 4 \to a,\ 5 \to b,\ 6 \to c$. gf: $1 \to a,\ 2 \to a,\ 3 \to c$.

Често пати се покажува корисно едно пресликување f да се означува со: $f = \begin{pmatrix} \dots & x & \dots \\ \dots & f(x) & \dots \end{pmatrix}$. Така, на пример, ако f и g се горе определените пресликувања, тогаш:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 6 \end{pmatrix},\ g = \begin{pmatrix} 3 & 4 & 5 & 6 \\ a & a & b & c \end{pmatrix},\ \ gf = \begin{pmatrix} 3 & 4 & 5 & 6 \\ a & a & b & c \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ a & a & c \end{pmatrix}.$$

---

[1]) $(\exists!\dots)$ се пишува наместо „постои еден и само еден ...“

Множеството на сите пресликувања со домен M и кодомен N ќе го означуваме со N^M. Елементите на M^M се викаат *трансформации* на M. Еве еден пример:

3) Ако $A = \{1, 2, 3\}$, $B = \{a, b\}$, тогаш:

$$A^B = \left\{\begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} a & b \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} a & b \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} a & b \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} a & b \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} a & b \\ 3 & 3 \end{pmatrix}\right\},$$

$$B^B = \left\{\begin{pmatrix} a & b \\ a & a \end{pmatrix}, \begin{pmatrix} a & b \\ a & b \end{pmatrix}, \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & b \end{pmatrix}\right\},$$

$$B^A = \left\{\begin{pmatrix} 1 & 2 & 3 \\ a & a & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ a & a & b \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ a & b & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ b & a & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ a & b & b \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ b & a & b \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ b & b & a \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ b & b & b \end{pmatrix}\right\}.$$

За секое множество M со 1_M ќе ја означуваме трансформацијата на M дефинирана со:

$$(\forall x \in M)\ 1_M(x) = x. \tag{4}$$

За 1_M велиме дека е *идентичната трансформација* (т.е. пресликување) на M.

Ќе докажеме две тврдења во врска со поимот производ (т.е. состав) на пресликувања.

1°. Ако $f: M \to N$, тогаш: (i) $f 1_M = f$; (ii) $1_N f = f$.

Доказ. (i) Да го означиме со g пресликувањето $f 1_M$; според тоа, $g \in N^M$, т. е. g има ист домен, односно кодомен, како и f; потоа, ако $x \in M$, имаме: $g(x) = f 1_M(x) = f(1_M(x)) = f(x)$, од што конечно следува дека $g = f$. ▨

2°. Ако $f: K \to L$, $g: L \to M$, $h: M \to N$, тогаш: $h(gf) = (hg)f$.

Доказ. Да ставиме $k' = h(gf)$, $k'' = (hg)f$. Прво, уочуваме дека K е домен, а N кодомен за k' и k''. Потоа, ако $x \in L$ и ако ставиме: $f(x) = y$, $g(y) = z$, $h(z) = u$, добиваме $k'(x) = u = k''(x)$, од што го добиваме заклучокот дека $k' = k''$. ▨

Нека $f: M \to N$ и нека $A \subseteq M$. Со $f(A)$ го означуваме множеството што се состои од оние елементи на N што се слики на елементите од A, т.е.

$$f(A) = \{y \mid (\exists x \in A)\ y = f(x)\}. \tag{5}$$

Десната страна на (5), обично, ќе ја пишуваме во облик $\{f(x) \mid x \in A\}$, така што имаме:

$$f(A) = \{f(x) \mid x \in A\}. \tag{5'}$$

Сега да претпоставиме дека $B \subseteq N$. Тогаш со $f^{-1}(B)$ го означуваме множеството што се состои од оние елементи на M што се пресликуваат во B, т. е.

$$f^{-1}(B) = \{x \mid f(x) \in B\}. \tag{6}$$

Му препорачуваме на читателот да го докаже следново тврдење:

3°. Ако f е пресликување од M во N и ако $A_1, A_2 \subseteq M$, $B_1, B_2 \subseteq N$, тогаш:

(i) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$;
(i′) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$;
(ii) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;
(ii′) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;
(iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$;
(iii′) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$. ▒

Да разгледаме еден пример.

Ако g е определено како и во 2), тогаш имаме:

$$g(B) = C, \quad g(\{3, 4, 5\}) = \{a, b\} = g(\{3, 5\}),$$

$$g^{-1}(\{a, c\}) = \{3, 4, 6\}, \quad g(\{5\}) = \{b\} \subset g(\{3, 5\}) \cap g(\{4, 5\}) = \{a, b\}.$$

Од овој пример се гледа дека знакот $\subseteq$ не може во (i) да се замени со $\subset$, ниту во (ii) да се замени со $=$.

Од спроведената дискусија следува дека со помош на дадено пресликување $f: M \to N$ можат да се дефинираат две нови пресликувања, едно од $B(M)$ во $B(N)$ и едно од $B(N)$ во $B(M)$. Тоа се постигнува, имено, со:

$$f_* : A \to f(A), \quad f^* : C \to f^{-1}(C) \tag{7}$$

каде $A \in B(M)$, $C \in B(N)$. Според тоа, имаме

$$f_* : B(M) \to B(N), \quad f^* : B(N) \to B(M).$$

Нови пресликувања можат да се добијат и со стеснување на доменот, односно кодоменот на f. Имено, ако $f: M \to N$ и ако $K \subseteq M$, тогаш со f_K ќе го означуваме пресликувањето чиј домен е K, а кодомен N и притоа

$$(\forall x \in K) \quad f_K(x) = f(x). \tag{8}$$

Исто така, ако $L \subseteq N$ и ако $f(M) \subseteq L$, тогаш со f^L ќе го означуваме пресликувањето со домен M, кодомен L, а "има исто дејство како и f", т.е.

$$(\forall x \in M) \quad f^L(x) = f(x). \tag{9}$$

За пресликувањата f_K и f^L велиме дека се *рестрикции* на f, а во иста смисла и дека е *проширување* на f_K (односно на f^L).

Со цел да го илустрираме поимот за рестрикција ќе се вратиме на примерот 2). Ако $K=\{3,4,5\}$, тогаш $g_K=\begin{pmatrix}3&4&5\\a&a&b\end{pmatrix}$. Да го означиме gf со h и да ставиме $L=\{a,c\}$ тогаш $h^L=\begin{pmatrix}1&2&3\\a&a&c\end{pmatrix}$; овде имаме $h^L\neq h$, бидејќи h^L и h имаат различни кодомени.

Ќе разгледаме неколку специјални видови пресликувања.

За пресликувањето $f: M\to N$ велиме дека е *инјекција* акко:

$$f(x_1)=f(x_2)\Rightarrow x_1=x_2. \tag{10}$$

Директно, или со помош на 1.2.6° (т.е. законот за контрапозиција), се покажува дека:

4°. Пресликувањето $f: M\to N$ е инјекција акко различни елементи од M имаат различни слики во N. ■

Пресликувањето $f: M\to N$ се вика *сурјекција* акко:

$$(\forall y\in N)\ (\exists x\in M)\ y=f(x), \tag{11}$$

т.е. акко секој елемент од N е слика на барем еден елемент од M.

Од пресликувањата во 1), f е сурјекција, но не е инјекција, а g не е ни инјекција, ни сурјекција. Во 2), f е инјекција, но не е сурјекција, а g е сурјекција, но не е инјекција; производот gf не е ни инјекција, ни сурјекција.

Да покажеме дека својството да се биде инјекција, односно сурјекција, се пренесува и на производот од две пресликувања.

5°. Ако $f: L\to M$, $g: M\to N$ се: а) инјекции б) сурјекции, тогаш соодветното својство го има и нивниот прозивод gf.

Доказ. Да ставиме $gf=h$.

а) Нека f и g се инјекции и нека $x_1, x_2, \in L$ се такви што $h(x_1)=h(x_2)$, т. е. $g(f(x_1))=g(f(x))$; од последново равенство, ако се има предвид тоа што е g инјекција, се добива $f(x_1)=f(x_2)$, од што следува: $x_1=x_2$. Според тоа, и h е инјекција.

б) Нека f и g се сурјекции. Ако $z\in N$, тогаш постои $y\in M$, таков што $g(y)=z$; избирајќи еден таков елемент y, добиваме дека постои $x\in L$, таков што $f(x)=y$; и конечно, ако x е еден елемент од L што го задоволува равенството, ќе добиеме: $h(x)=g(f(x))=g(y)=z$. Според тоа, и h е сурјекција. ■

Пресликувањето $f: M\to N$ се вика *биекција* акко е и инјекција и сурјекција. Според тоа, f е биекција акко за секој елемент $y\in N$ постои точно еден елемент $x\in M$, таков што $y=f(x)$, т.е.:

$$(\forall y\in N)\ (\exists!\, x\in M)\ y=f(x). \tag{12}$$

Ниедно од пресликувањата спомнати во примерите 1) и 2) не е биекција, па затоа разгледуваме нов пример.

4) Ако $A = \{1, 2, 3\}$, $D = \{3, 4, 6\}$ и ако ставиме $h : 1 \to 3,\ 2 \to 4,\ 3 \to 6$, добиваме биекција $h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 6 \end{pmatrix}$ од A во D. Да забележиме дека пресликувањето h не е еднакво со f од 2), бидејќи кодомените им се различни.

Биекциите од M во M ги нарекуваме *пермутации* на M; множеството од сите пермутации на M ќе го означуваме со $S(M)$. Така, ако $A = \{1, 2, 3\}$, тогаш:

$$S\ A) = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}.$$

Притоа: $1_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ е идентичната трансформација, па затоа велиме дека таа е идентична пермутација. Да забележиме дека ова важи за секое множество M, т.е. дека:

6°. $1_M \in S(M)$. ∎

Од **5°**, исто така, следува и дека:

7°. Ако $f : L \to M$ и $g : M \to N$ се биекции, тогаш и $gf : L \to N$ е биекција. ∎

На секоја биекција $f : M \to N$ ќе ѝ се придружува инверзна биекција $f^{-1} : N \to M$ на следниов начин:

$$f(x) = y \Leftrightarrow f^{-1}(y) = x. \tag{13}$$

Од дадената дефиниција не е непосредно јасно дека f^{-1} е биекција. Сега ќе докажеме дека тоа е навистина точно.

8°. Ако f е биекција од M во N, тогаш со (13) е определена биекција f^{-1} од N во M. (Велиме дека f^{-1} е инверзна биекција на f).

Доказ. Прво од (12), т.е. од дефиницијата на поимот биекција, следува дека f^{-1} е пресликување од N во M. Потоа, ако $f^{-1}(y_1) = x = f^{-1}(y_2)$, тогаш $y_1 = f(x) = y_2$, т.е. f^{-1} е инјекција. И на крајот, ако $x \in M$, тогаш $x = f^{-1}(y)$, каде $y = f(x)$, а со тоа покажавме дека f е и сурјекција. ∎

Лесно се докажува точноста и на следниве тврдења:

9°. За секое множество M, $1_M^{-1} = 1_M$. ∎

10°. Ако $f : L \to M$, $g : M \to N$ се биекции, тогаш:

(i) $(f^{-1})^{-1} = f$; (ii $ff^{-1} = 1_N$, $f^{-1}f = 1_M$;

(iii) $(gf)^{-1} = f^{-1}g^{-1}$. ∎

При дефиницијата на поимот пресликување претпоставивме дека и доменот и кодоменот се непразни. Но, земајќи го исказот (1) како дефинирачки и тоа претставен во следнава форма:

$$x \in M \Rightarrow (\exists!\, y \in N)\ y = f(x), \tag{1'}$$

можеме да го прошириме поимот за пресликување. Имено, допуштаме да постои точно едно пресликување $\varnothing^{(N)} : \varnothing \to N$ со домен $\varnothing$ и кодомен N; велиме дека $\varnothing^{(N)}$ е празното пресликување во N. Притоа имаме:

11°. (i) $\varnothing^{(N)}$ е инјекција за секое множество N;

(ii) $\varnothing^{(N)}$ е биекција акко $N = \varnothing$.

(iii) Ако f е пресликување од M во N, тогаш: $f\varnothing^{(M)} = \varnothing^{(N)}$.

Да спомнеме, исто така, дека сите порано докажани тврдења се точни и кога некое од соодветните пресликувања има облик $\varnothing^{(S)}$.

Со помош на биекциите се дефинира и поимот за еквивалентност меѓу множествата. Имено, велиме дека M и N се *еквивалентни множества* и пишуваме $M \sim N$, акко постои биекција f од M во N.

Од својствата **6°**, **7°** и **8°** следува дека:

12°. (i) $X \sim X$; (ii) $X \sim Y \Rightarrow Y \sim X$;
(iii) $X \sim Y,\ Y \sim Z \Rightarrow X \sim Z$.

Ќе докажеме уште две тврдења.

13°. Ако $M_1 \sim N_1,\ M_2 \sim N_2,\ M_1 \cap M_2 = N_1 \cap N_2 = \varnothing$, тогаш: $M_1 \cup M_2 \sim N_1 \cup N_2$.

Доказ. Нека $f_1 : M_1 \to N_1,\ f_2 : M_2 \to N_2$ се биекции и нека ставиме:

$$f(x) = \begin{cases} f_1(x) & \text{за } x \in M_1 \\ f_2(x) & \text{за } x \in M_2. \end{cases}$$

Од $M_1 \cap M_2 = \varnothing$, следува дека f е пресликување од $M_1 \cup M_2$ во $N_1 \cup N_2$. Потоа, од тоа што е $N_1 \cap N_2 = \varnothing$, а f_1 и f_2 се инјекции следува дека и f е инјекција. И на крај, ако се има предвид тоа што f_1 и f_2 се сурјекции, се добива дека и f е сурјекција.

14°. Ако $N \cap P = \varnothing$, тогаш: $M^{N \cup P} \sim M^N \times M^P$.

Доказ. Нека $f \in M^{N \cup P}$, и нека ставиме $\xi : f \to (f_N, f_P)$. Според тоа, ξ е пресликување од $M^{N \cup P}$ во $M^N \times M^P$. Ако се има предвид тоа што $N \cap P = \varnothing$, ќе се добие дека ξ е биекција.

ВЕЖБИ. 2. Нека M е множеството луѓе од Скопје, а N множеството на нивните имиња. Со изразот "y е име на x" е определено пресликување од M во N. Дали тоа пресликување е: а) инјекција; б) сурјекција?

3. Нека $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, a, b\}$, $C = \{\alpha, \beta, \gamma, \delta\}$ и нека $f : A \to A$, $g : A \to B$, $h : B \to C$ се определени со: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 1 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & a & 1 & a \end{pmatrix}$, $h = \begin{pmatrix} 1 & 2 & a & b \\ \beta & \delta & \alpha & \gamma \end{pmatrix}$.

а) Дали некое од пресликувањата f, g, h е биекција?

б) Кој од "производите" *ff, gf, gh, hg, fg* е пресликување? Во потврден случај да се определат соодветните пресликувања што се резултати на производите.

в) Да се определи $g(X)$ ако X е некое од множествата: B, $\{1, 2\}$, $\varnothing$, $\{1, 5\}$, $\{2, 3, 4\}$

4. Ако $f: M \to N$, да се објасни во кој случај е точно тврдењето:

$$\text{а) } f(M) = N, \quad \text{б) } f(M) \subset N.$$

5. Нека M и N се непразни множества и нека F е подмножество на $M \times N$ со следниве својства:

(i) $(\forall x \in M)\,(\exists y \in N)\,(x, y) \in F$;

(ii) $(\forall x \in M)\,(\forall y_1, y_2 \in N)\,[(x, y_1), (x, y_2) \in F \Rightarrow y_1 = y_2]$.

Потоа, да ставиме $y = f(x) \Leftrightarrow (x, y) \in F$. Да се покаже дека f е пресликување од M во N Какви својства треба да има множеството F за да биде f: а) инјекција; б) сурјекција?

.6. Нека $f, g, h \in \mathbf{R}^{\mathbf{R}}$ се определени со:

$f(x) = x^2$, $g(x) = 1/(x^2 + 1)$, $h(x) = 0$ за $-1 \leqslant x \leqslant 1$, $h(x) = 1$ за $x < -1 \vee x > 1$.

а) Да се определат сите можни девет производи: *ff, fg, fh, gf, gg, gh, hf, hg, hh.*

б) Ако $A = \{x \mid x \in \mathbf{R},\ x \leqslant 0\}$, $B = \left\{x \mid x \in \mathbf{R},\ x \geqslant \frac{1}{2}\right\}$, $C = \{x \mid \in \mathbf{R},\ g(x) \geqslant 1\}$, да се определат: $k(X)$ и $k^{-1}(X)$, каде k е кое било од пресликувањата f, g, h, а $X \in \{\mathbf{R}, A, B, C\}$.

7. Ако $f: M \to N$ и g: $N \to M$ се такви што $gf = 1_M$, тогаш f е инјекција, а g сурјекција.

8. Пресликувањето $f: M \to N$ е биекција акко постојат пресликувања g, $h: N \to M$, такви што $gf = 1_M$, $fh = 1_N$. Во тој случај, имаме $g = h = f^{-1}$.

9. Нека f е биекција од M во N. Ако $B \subseteq N$, тогаш имаме две дефиниции за множеството $f^{-1}(B)$, а имено:

$$f^{-1}(B) = \{x \mid f(x) \in B\} \text{ и } f^{-1}(B) = \{f^{-1}(y) \mid y \in B\}.$$

Да се покаже дека овие дефиниции се согласни, т.е. дека: $\{x \mid f(x) \in B\} = \{f^{-1}(y) \mid y \in B\}$.

10. Ако $f: M \to N$ е инјекција, тогаш:

(i) $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$,

(ii) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$,

каде A_1, $A_2 \subseteq M$.

11. Ако X, Y и Z се произволни множества, тогаш: (i) $X \times Y \sim Y \times X$;

(ii) $X \times (Y \times Z) \sim (X \times Y) \times Z$.

12. Ако $X_1 \sim Y_1$, $X_2 \sim Y_2$, тогаш $X_1 \times X_2 \sim Y_1 \times Y_2$.

13. За секое множество X и елемент $\{a\}$, имаме $X \sim X^{\{a\}}$.

.14. (i) $\mathbf{N} \sim \mathbf{Z}$; (ii) $\mathbf{N} \sim \mathbf{Q}$.

1.5. РЕЛАЦИИ

Ако M е множество, тогаш секое подмножество α од $M \times M$ се вика *релација* во M. Во тој случај, наместо $(x, y) \in \alpha$, често ќе пишуваме $x \alpha y$ и ќе читаме "x е во релација α со y",

За релацијата α велиме дека е:

рефлексивна акко: $(\forall x \in M)\ x \alpha x$;[1] (1)

симетрична акко: $x \alpha y \Rightarrow y \alpha x$; (2)

транзитивна акко: $x \alpha y \wedge y \alpha z \Rightarrow x \alpha z$. (3)

Ако сите три услови се исполнети, тогаш велиме дека α е *еквивалентност* во M.

1°. Во секое множество M, релациите $\alpha = M \times M$ и $\Delta_M = \{(x, x) \mid x \in M\}$ се еквивалентности. ▨

За Δ_M велиме дека е *дијагонала* во M, а $M \times M$ *универзална релација* во M; да уочиме дека дијагоналата, всушност, е релацијата за равенство во M.

Ќе разгледаме еден конкретен пример.

1) Нека $A = \{1, 2, 3, 4, 5, 6, 7\}$ и нека релациите α_1, α_2, α_3 и α_4 се дефинирани со:

$\alpha_1 = \{(1, 2), (1, 3), (2, 1), (3,1)\}$; $\alpha_2 = \{(1, 2), (1,3), (4,5)\}$;

$\alpha_3 = \Delta_A \cup \{(1,4), (4,1), (1,7), (7,1), (4,7), (7,4), 2,5), (5,2), (3,6), (6,3)\}$;

$\alpha_4 = \{(1, 1), (2,2), (1,3)\}$. Од дадените релации, еквивалентност е само α_3, а симетрична, освен α_3, е уште α_1.

Нека α е релација во M и нека $a \in M$. Со a^α ќе го означиме подмножеството на сите елементи од M со кои a е во релација α, т.е.

$$a^\alpha = \{x \mid x \in M \wedge a \alpha x\}. \tag{4}$$

Ќе ја искористим ознаката (4) за давање нова карактеристика на еквивалентностите.

2°. Релацијата α е еквивалентност во M акко:

$$x \in x^\alpha \wedge (x^\alpha \cap y^\alpha \neq \emptyset \Rightarrow x^\alpha = y^\alpha). \tag{5}$$

Доказ. Нека α е еквивалентност во M. Од рефлексивноста следува дека $x \in x^\alpha$, за секој $x \in M$. Нека $x^\alpha \cap y^\alpha \neq \emptyset$, т.е. постои $z \in M$, таков што $x \alpha z$ и $y \alpha z$. Ако $u \in x^\alpha$, тогаш $x \alpha u$, па ако се има предвид тоа што $y \alpha z$, $z \alpha x$, $x \alpha u$, се добива $y \alpha u$, т.е. $u \in y^\alpha$. Со тоа покажавме дека $x^\alpha \subseteq y^\alpha$, а од причини на симетрија ќе имаме и $y^\alpha \subseteq x^\alpha$, т.е. $x^\alpha = y^\alpha$. Според тоа, точно е тврдењето (5).

Да претпоставиме сега дека е точно (5), за секои $x, y \in M$. Од $x \in x^\alpha$ добиваме прво дека α е рефлексивна. Нека $x \alpha y$, т.е. $y \in x^\alpha$; тогаш имаме: $y \in x^\alpha \cap y^\alpha$, па значи $x^\alpha = y^\alpha$, од што следува дека $x \in y^\alpha$, т.е. $y \alpha x$; според ова,

[1] Според договорот направен во 1. 2, овде не е неопходен квантификатор $(\forall x \in M)$, па во таа смисла во (2) и (3) не употребуваме квантификатори.

α е симетрична. Нека $x\alpha y$, $y\alpha z$; тогаш $x\alpha y$, $z\alpha y$, т.е. $y \in x^\alpha \cap z^\alpha$, од што следува $x^\alpha = z^\alpha$, па и $z \in x^\alpha$, така што добиваме дека $x\alpha z$. Со тоа докажавме дека α е и транзитивна.

Во горниот пример имаме:

$$1^{\alpha_1} = \{2, 3\},\ 2^{\alpha_1} = \{1\} = 3^{\alpha_1},\ 4^{\alpha_1} = 5^{\alpha_1} = 6^{\alpha_1} = 7^{\alpha_1} = \emptyset;$$

$$1^{\alpha_2} = \{2, 3\},\ 2^{\alpha_2} = 3^{\alpha_2} = 5^{\alpha_2} = 6^{\alpha_2} = 7^{\alpha_2} = \emptyset,\ 4^{\alpha_2} = \{5\};$$

$$1^{\alpha_3} = \{1, 4, 7\} = 4^{\alpha_3} = 7^{\alpha_3},\ 2^{\alpha_3} = \{2, 5\} = 5^{\alpha_3},\ 3^{\alpha_3} = \{3, 6\} = 6^{\alpha_3};$$

$$1^{\alpha_4} = \{1, 3\},\ 2^{\alpha_4} = \{2\},\ 3^{\alpha_4} = 4^{\alpha_4} = 5^{\alpha_4} = 6^{\alpha_4} = 7^{\alpha_4} = \emptyset.$$

Веднаш се гледа дека условот (5) го задоволува само α_3, па, значи, само таа релација е еквивалентност.

Ако α е еквивалентност во M, тогаш за подмножеството a^α велиме дека е *класа на еквивалентноста* α *со претставник* a; ако $b \in a^\alpha$, тогаш $b \in a^\alpha \cap b^\alpha$, па, значи, $a^\alpha = b^\alpha$, од што следува дека и b е претставник на a^α. За множеството:

$$M_{/\alpha} = \{x^\alpha \mid x \in M\}, \tag{6}$$

велиме дека е *факторможество* на M во однос на α. Од горната дискусија следува дека:

$$A_{/\alpha} = \{\{1, 4, 7\}, \{2, 5\}, \{3, 6\}\},$$

каде α_3 е означено со α.

Како што спомнавме погоре, секој елемент на класата $\{1, 4, 7\}$, на пример, го сметаме за претставник на таа класа. Имајќи го тоа предвид, можеме да напишеме:

$A_{/\alpha} = \{1, 2, 3\} = \{1, 5, 3\} = \ldots = \{7, 5, 6\}$, при што секој елемент на A го сметаме како ознака на соодветната класа. Можеме да напишеме и:

$$A_{/\alpha} = \{1, 2, 3, 4, 5, 6, 7\},$$

но сега сметаме дека $1 = 4 = 7$, $2 = 5$, $3 = 6$. Оваа ознака нема да ја користиме, бидејќи тоа може да доведе до недоразбирање, а, имено, погрешно би било да се смета за точно равенството: $A = A_{/\alpha}$.

Сепак, елементите од едно множество M се користат како ознаки за елементите од соодветно фактормножество $M_{/\alpha}$ ако за нас е побитно фактормножеството. Еве еден таков пример:

.2) Ако $\mathbf{Q} = \left\{\frac{x}{y} \mid x, y \in \mathbf{Z}, y \neq 0\right\}$, тогаш ние, често премолчено, сметаме дека $\frac{x}{y} = \frac{u}{v}$ акко $xv = yu$; така, на пример, $\frac{1}{2} = \frac{2}{4} = \frac{6}{12} = \ldots$. Значи, во

овој случај еден ист рационален број се означува на различни (и тоа бесконечно многу) начини.

За една релација α велиме дека е *антисиметрична* акко:

$$x \alpha y \wedge y \alpha x \Rightarrow x = y. \tag{7}$$

Во примерот 1) антисиметрични се α_2 и α_4.

Подредување на M е секоја релација што е рефлексивна, антисиметрична и транзитивна.

3°. Дијагоналата Δ_M на M (т.е. равенството) е единствената релација во M што е и подредување и еквивалентност.

Да разгледаме уште два примера.

3) Нека $A = \{0, 1, 2, 3, 4\}$ и:

$$\alpha = \Delta_A \cup \{(0,1), (0,2), (0,3), (0,4), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}.$$

$$\beta = \Delta_A \cup \{(0,1), (0,2), (0,3), (0,4), (1,3), (2,4)\}.$$

И двете релации α, β се подредувања на A. Притоа, имаме

$$(\forall x, y)\ x \alpha y \vee y \alpha x, \tag{8}$$

но β ја нема таа особина, бидејќи, на пример, $(2,3) \notin \beta$ и $(3,2) \notin \beta$.

За една релација α велиме дека е *потполно подредување* акко е подредување со особината (8). Подредувањата што не ја задоволуваат особината (8) се викаат *делумни.*

Ако α е релација во едно множество M, тогаш комплементот $M \times M \setminus \alpha$ на α во $M \times M$ се вика *негација* на α, а се означува со $\neg \alpha$.

За релацијата α велиме дека е *нерефлексивна* акко:

$$(\forall x \in M)\ x \neg \alpha x \text{ (т.е. } (x, x) \notin \alpha). \tag{9}$$

Ќе докажеме неколку својства на подредувањата.

4°. Ако α е подредување на множеството M и ако релацијата α_* е определена со;

$$x \alpha_* y \Leftrightarrow x \alpha y \ \wedge \ x \neq y, \tag{10}$$

тогаш α_* е нерефлексивна и транзитивна релација во M.

Доказ. Од (10) е јасно дека α_* е нерефлексивна. Нека $x \alpha_* y$, $y \alpha_* z$, т.е. $x \alpha y$, $x \neq y$, $y \alpha z$, $y \neq z$. Од транзитивноста на α следува: $x \alpha z$; не може да биде $x = z$, бидејќи тогаш од $x \alpha y$, $y \alpha x$ би следувало $x = y$; според тоа, имаме $x \alpha z$ и $x \neq z$, т. е. $x \alpha_* z$.

5°. Ако β е нерефлексивна и транзитивна релација во M и ако β^* е определена со:

$$x\,\beta^*\,y \Leftrightarrow x\beta y \vee x = y, \tag{11}$$

тогаш β^* е подредување на M.

Доказ. Од (11) се гледа дека β^* е рефлексивна. Не може да биде $x\beta^* y$, $y\beta^* x$ и $x \neq y$, бидејќи тогаш би имале $x\beta y$, $y\beta x$ од што би следувало $x\beta x$; според тоа, β^* е антисиметрична. На читателот му препуштаме да покаже дека β^* е и транзитивна, т.е. подредување на M. ∎

Читателот би требало да биде во состојба да го докаже и следново тврдење:

6°. Ако α е подредување на M, а β нерефлексивна и транзитивна релација во M, тогаш:

$$\text{(i) } (\alpha_*)^* = \alpha; \text{ (ii) } (\beta^*)_* = \beta. \text{ ▒}$$

Ако во едно множество M е определено едно фиксно подредување α, тогаш за M велиме дека е подредено множество. Наместо $x\alpha y$, обично, се пишува $x \leqslant y$. Според тоа, имаме:

$$\begin{gathered}(\forall x, y, z \in M)\ x \leqslant x;\ x \leqslant y,\ y \leqslant x \Rightarrow x = y; \\ x \leqslant y,\ y \leqslant z \Rightarrow x \leqslant z.\end{gathered} \tag{12}$$

Во овој случај, соодветната нерефлексивна и транзитивна релација α_* ја означуваме со $<$, т.е.

$$x < y \Leftrightarrow x \leqslant y,\ x \neq y. \tag{13}$$

Натаму, под подредување ќе подразбираме потполно подредување,а во иста смисла за едно множество M ќе велиме дека е подредено ако соодветното подредување е потполно. Според тоа:

7°. Ако M е подредено множество и ако $x, y \in M$, тогаш еден и само еден од следните три услови е исполнет:

$$x < y;\ x = y;\ y < x. \text{ ▒} \tag{14}$$

Да спомнеме и дека често пати ќе пишуваме $x \geqslant y$ наместо $y \leqslant x$, како и $x > y$ наместо $y < x$. Исто така, наместо

$$x \leqslant y,\ \ y \leqslant z, \quad \text{ќе пишуваме} \quad x \leqslant y \leqslant z.$$

Во оваа смисла ќе ги употребуваме и ознаките:

$$x < y < z,\ \ x \leqslant y < z,\ \ x < y \leqslant z.$$

Уште неколку поими во врска со подредените множества ќе спомнеме во **1.6.**, а овој дел ќе го завршиме со поимот рестрикција на една релација.

Нека α е релација во M и $N \subseteq M$. Тогаш, за релацијата:

$$\alpha_N = \alpha \cap (N \times N) = \{(x, y) \mid (x, y) \in \alpha,\ x, y \in N\} \tag{15}$$

велиме дека е *рестрикција* од α на N, или дека α е *проширување* на α_N.

8°. Ако α е релација во M и ако α е: а) рефлексивна; б) нерефлексивна; в) симетрична; г) антисиметрична; д) транзитивна; ѓ) еквивалентност; е) подредување, тогаш соодветната особина ја има и секоја нејзина рестрикција. ▒

Пред да поминеме на вежбите, да забележиме дека веројатно би било поприродно релациите во едно множество M да се дефинираат како исказни функции со две променливи во M, наместо како подмножества од $M \times M$. Имено, ако $\varphi(x, y)$ е исказна функција, каде x и y се променливи во M, тогаш "решението на $\varphi(x, y)$", т.е. множеството:

$$\alpha_\varphi = \{(x, y) \mid \varphi(x, y)\} \tag{16}$$

е подмножество од $M \times M$, за кое велиме дека е *график* на $\varphi(x, y)$. И обратно, ако β е подмножество на $M \times M$, т.е. релација во M, тогаш можеме **да** определиме исказна функција $\psi(x, y)$ со:

$$\begin{aligned} \psi(x, y) &= \top \text{ акко } (x, y) \in \beta \\ \psi(x, y) &= \bot \text{ акко } (x, y) \notin \beta. \end{aligned} \tag{17}$$

Според тоа, ако исказната функција се смета за релација, тогаш нејзиниот график ја има смислата на поимот релација, дефиниран во почетокот на овој дел.

ВЕЖБИ: **1.** Во множеството $M = \{a, b, c, d\}$ се определени релациите α, β, γ и δ на следниов начин:

$\alpha = \{(a, b), (b, c), (b, a)\}$;
$\beta = \{(a, b), (b, c), (c, d), (a, c), (a, d), (b, d)\}$;
$\gamma = \{(a, b), (b, a)\}$;
$\delta = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}$.

Да се испитаат особините на дефинираните релации.

2. Нека S е множеството прави од една рамнина и нека $a \alpha b$ означува дека правите a и b немаат заеднички точки. Да се покаже дека α е нерефлексивна и симетрична релација, но дека таа релација не е транзитивна. Да се покаже дека релацијата β определена со $a \beta b \leftrightarrow a \alpha b \vee a = b$ е еквивалентност во S.

3. Имајќи предвид дека релациите во множеството M се подмножества на $M \times M$ меѓу релациите можеме да ги определиме операциите унија и пресек.

Да се покаже дека ако и двете релации α и β ја имаат некоја од особините: а) рефлексивност, б) симетричност, в) транзитивност, г) нерефлексивност, д) антисиметричност, тогаш истата особина ја има и нивниот пресек. Со конкретен пример да се покаже дека унија на две транзитивни релации не мора да биде транзитивна.

4. Нека α е рефлексивна и транзитивна релација во S и нека ставиме

$$x \beta y \Leftrightarrow x \alpha y \wedge y \alpha x.$$

Да се покаже дека β е еквивалентност.

5. Нека f е пресликување од множеството M во N и нека ставиме:

$$x_1 \alpha x_2 \Leftrightarrow f(x_1) = f(x_2).$$

Да се покаже дека α е еквивалентност во M. Да се определат класите на еквивалентноста α, ако $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = N$,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 1 & 2 & 4 & 5 & 1 & 3 & 4 \end{pmatrix}.$$

6. Ако M е непразно множество, тогаш: $x^{\Delta} = \{x\}$, $x^{M \times M} = M$ за секој $x \in M$, т.е.

$$M_{/\Delta} = \{\{x\} \mid x \in M\},\ M_{/M \times M} = \{M\},$$ каде што $\Delta = \Delta_M$.

7. Релацијата $\subset$ е подредување на булеанот $B(M)$; ако M има барем 2 елементи тогаш ова подредување е делумно.

8. Ако α и β се определени како во 3), тогаш α е потполно, а β делумно подредување. Да се определат релациите α_* и β_*.

9. Во множеството $\mathbf{N}$ на природните броеви дефинираме релација $\leqslant$ со:

$$x \leqslant y \Leftrightarrow (\exists z)\ y = xz.$$

Да се покаже дека $\leqslant$ е делумно подредување на $\mathbf{N}$.

10. Во множеството $\mathbf{C}$ на комплексните броеви дефинираме релација $\leqslant$ со:

$$x + iy \leqslant u + iv \Leftrightarrow x \leqslant u \vee (x = u \wedge y \leqslant v).$$

Да се покаже дека $\leqslant$ е подредување на $\mathbf{C}$.

11. Да дефинираме релација α во $\mathbf{Z}$ со: $x \alpha y \Leftrightarrow 4$ е делител на $x - y$. Да се покаже дека α е еквивалентност и дека $\mathbf{Z}_{/\alpha} = \{0^{\alpha}, 1^{\alpha}, 2^{\alpha}, 3^{\alpha}\}$ се состои точно од четири елементи. Што ќе се добие ако во горната дефиниција наместо 4 се стави: а) 1; б) 2; в) m, каде $m \in \mathbf{N}$ е позитивен природен број?

12. За секое множество M имаме $M_{/\Delta} \sim M$.

1.6. МНОЖЕСТВО НА ПРИРОДНИТЕ БРОЕВИ

Множеството броеви:

$$\mathbf{N} = \{0, 1, 2, 3, \ldots, n, n + 1, \ldots\} \tag{1}$$

се вика множество на *природните* броеви, бидејќи тие се првите броеви со кои се среќава човекот во својот развој. Потоа, со помош на $\mathbf{N}$ се конструираат пошироките множества броеви, какви што се $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$.

Ќе издвоиме неколку својства на $\mathbf{N}$, познати под името Пеанови аксиоми, а потоа ќе покажеме како со нивна помош се изградува теоријата на природните броеви, којашто им е позната, речиси, на сите читатели.

Пред сè, $\mathbf{N}$ е непразно и притоа:

(I) $0 \in \mathbf{N}$.

Потоа, ако x е природен број, тогаш и $x + 1$ е природен број. Овде ќе пишуваме x^+ наместо $x + 1$. Според тоа: $1 = 0 + 1 = 0^+$, $2 = 1 + 1 = 1^+ = 0^{++}$ итн. Користејќи ја новата ознака, добиваме:

$$\mathbf{N} = \{0, 0^+, 0^{++}, 0^{+++}, \ldots 0^{++\cdots+}, \ldots\}. \tag{1'}$$

За бројот x^+ велиме дека е *следбеник* на x, а во иста смисла x е *претходник* на x^+. Сега лесно доаѓаме и до наредните барани својства на $\mathbf{N}$.

(II) $x \in \mathbf{N} \Rightarrow x^+ \in \mathbf{N}$. (Секој природен број има свој следбеник што е, исто така, природен број).

(III) $x^+ = y^+ \Leftrightarrow x = y$. (Следбениците на два броја се еднакви акко тие броеви се еднакви).

(IV) $0 \neq x^+$. (Нулата нема претходник).

Исто така, уочуваме дека ако се тргне од нулата со едноподруго допишување на знакот $^+$ (т.е. "броење"), се доаѓа до секој природен број. Со други зборови:

(V) $S \subseteq \mathbf{N}$, $0 \in S$, $(x \in S \Rightarrow x^+ \in S) \Rightarrow S = \mathbf{N}$.

(Ако во едно подмножество S од $\mathbf{N}$ се содржи нулата и ако заедно со секој свој елемент S го содржи и неговиот следбеник, тогаш S го содржи секој природен број).

Формулираните својства (I)—(V) се познати како *Пеанови аксиоми* за природните броеви, бидејќи прв ги формулирал италијанскиот математичар Пеано, во 1895 година.

Својството (V) е познато како *аксиома на индукцијата*. Оваа аксиома се користи при докажувањето на, речиси, секое својство на природните броеви.

Од претходната дискусија следува дека множеството $\mathbf{N}$ ги задоволува Пеановите аксиоми, а сега ќе докажеме дека тоа е единственото множество со тие својства.

1°. Ако $\mathbf{N}'$ и $\mathbf{N}''$ се две множества што ги задоволуваат својствата, (I) — (V), тогаш $\mathbf{N}' = \mathbf{N}''$.

Доказ. Да ставиме $S = \mathbf{N}' \cap \mathbf{N}''$. Имаме $S \subseteq \mathbf{N}'$. Од $0 \in \mathbf{N}'$, $0 \in \mathbf{N}''$ следува $0 \in S$; ако $x \in S$, тогаш $x \in \mathbf{N}'$ и $x \in \mathbf{N}''$, од што следува дека $x^+ \in \mathbf{N}'$, $x^+ \in \mathbf{N}''$, т.е. $x^+ \in S$. Сега, според (V), ако наместо $\mathbf{N}$ се замени $\mathbf{N}'$, добиваме $S = \mathbf{N}'$. На ист начин се добива и $S = \mathbf{N}''$, т.е. $\mathbf{N}' = \mathbf{N}''$. ∎

Од (II), (III) и (IV) следува:

2°. Пресликувањето $^+$: $x \to x^+$ е инјекција од $\mathbf{N}$ во $\mathbf{N}$, но не е сурјекција. (Нулата не е слика на ниеден елемент.) ▨

Да докажеме уште две својства.

3°. Секој природен број е различен од својот следбеник.

Доказ. Да го означиме со S множеството на сите природни броеви што се различни од своите следбеници. Според (IV), $0 \in S$. Да претпоставиме дека $x \in \mathbf{N}$ и $x \in S$; тогаш $x \neq x^+$, бидејќи $x \in S$. Ќе докажеме дека $x^+ \neq (x^+)^+$, т.е. $x^+ \in S$, од што, според (V), ќе следува $S = \mathbf{N}$, т.е. точноста на својството. Навистина, од равенството $x^+ = (x^+)^+$, според (III), би следувало $x = x^+$, што противречи на претпоставката: $x \in S$. ∎

4°. Секој природен број, различен од нулата, има еднозначно определен претходник што е природен број.

Доказ. Прво, од (III) следува дека еден природен број не може да има различни претходници. Да го означиме со M множеството природни броеви што имаат претходници и да ставиме $S = \{0\} \cup M$. Тогаш имаме $0 \in S$ и $x^+ \in S$ (бидејќи $x^+ \in M$), па според аксиомата на индукцијата, добиваме $S = \mathbf{N}$, т. е. $M = \mathbf{N} \setminus \{0\}$. ∎

Ако $K \subseteq \mathbf{N}$, тогаш со K^+ се означува множеството следбеници на елементите од K, т.е.

$K^+ = \{x^+ \mid x \in K\}$. Според тоа:

$$\mathbf{N}^+ = \{0^+, 0^{++}, \ldots\} = \{1, 2, 3, \ldots, n, n+1, \ldots\} \tag{2}$$

Елементите од $\mathbf{N}^+$ ги нарекуваме *позитивни природни броеви*.

Ако е y претходник на x, ќе пишуваме $y = x^-$. Според тоа:

$$y = x^- \Leftrightarrow x = y^+. \tag{3}$$

Од **4°** следува и следново својство.

5°. Со $^-: x \to x^-$ е определена биекција од $\mathbf{N}^+$ во $\mathbf{N}$. ∎

Ако $n \in \mathbf{N}$, тогаш со $\mathbf{N}_n$ го означуваме множеството на оние природни броеви што "се конструирани пред n", т.е во (1) (односно (1′)) се "наоѓаат лево од n". Но, ние сакаме да ги користиме само Пеановите аксиоми, така што дадената дефиниција на $\mathbf{N}_n$ не е доволно прифатлива. Затоа, $\mathbf{N}_n$ се дефинира со:

$$\mathbf{N}_0 = \varnothing, \quad \mathbf{N}_{x^+} = \mathbf{N}_x \cup \{x\}. \tag{4}$$

Според тоа:

6°. $x \to \mathbf{N}_x$ е пресликување од $\mathbf{N}$ во $B(\mathbf{N})$. ∎

Точноста на тврдењето (поправо: тврдењата) што сега ќе го формулираме е очигледна ако се има предвид првобитната "механичка", односно "геометриска" дефиниција на $\mathbf{N}_n$. На читателот му препорачуваме да даде прецизни докази барем на неколку делови од тврдењето, а со цел да го овозможиме тоа, извршуваме погоден распоред на "подтврдењата".

7°. Нека $x, y \in \mathbf{N}$.

(i) $x \neq 0 \Rightarrow x^- \in \mathbf{N}_x$. (ii) $0 \in \mathbf{N}_{x^+}$. (iii) $x^+ \in \mathbf{N}_y \Rightarrow x \in \mathbf{N}_y$.
(iv) $x \notin \mathbf{N}_x$. (v) $x \in \mathbf{N}_y \Rightarrow x^+ \in \mathbf{N}_{y^+}$. (vi) $x \in \mathbf{N}_y \Rightarrow \mathbf{N}_x \subset \mathbf{N}_y$.
(vii) Еден и само еден од следниве услови е исполнет:

$$\mathbf{N}_x \subset \mathbf{N}_y; \quad x = y; \quad \mathbf{N}_y \subset \mathbf{N}_x. \tag{5}$$

(viii) $x \in \mathbf{N}_y \Leftrightarrow \mathbf{N}_x \subset \mathbf{N}_y$. (ix) $\mathbf{N}_x \sim \mathbf{N}_x^+$.

Ќе го докажеме само "подтврдењето" (vi).

Вршиме индукција по y. За $y = 0$, каков и да биде $x \in \mathbf{N}$, претпоставката $x \in \mathbf{N}_0$ не е точна, така што $x \in \mathbf{N}_0 \Rightarrow \mathbf{N}_x \subset \mathbf{N}_0$ е точна исказна функција. Да претпоставиме точност за $y = n$, т.е. дека:

$$x \in \mathbf{N}_n \Rightarrow \mathbf{N}_x \subset \mathbf{N}_n \tag{*}$$

е точно. Треба да покажеме дека и:

$$x \in \mathbf{N}_{n^+} \Rightarrow \mathbf{N}_x \subset \mathbf{N}_{n^+} \tag{**}$$

е точно. Нека $x \in \mathbf{N}_{n^+} = \mathbf{N}_n \cup \{n\}$; ако $x \neq n$, тогаш $x \in \mathbf{N}_n$, па според (*), имаме: $\mathbf{N}_x \subset \mathbf{N}_n \subset \mathbf{N}_{n^+}$; ако $x = n$, тогаш $\mathbf{N}_x = \mathbf{N}_n \subset \mathbf{N}_{n^+}$. ▒

При конструкцијата на $\mathbf{N}$ (во (1), односно (1′)), е извршено и *подредување* на $\mathbf{N}$. Имено, можеме да речеме дека природниот број m е помал од природниот број n акко m е "конструиран пред n", т.е. акко "m е налево од n." Прецизна дефиниција на релацијата за подредување се формулира на следниов начин:

$$x < y \Leftrightarrow \mathbf{N}_x \subset \mathbf{N}_y. \tag{6}$$

Лесно се покажува дека:

8°. (i) Релацијата $<$ е нерефлексивна и транзитивна.

(ii) Ако $x, y \in \mathbf{N}$, тогаш еден и само еден од следните услови е исполнет:

$$x < y; \quad x = y; \quad y < x \tag{7}$$

Доказ. (i) Ова е директна последица од (6) и соодветните својства на релацијата $\subset$.

(ii) Ова е последица од **7°** (vii). ▒

Од **8°**, ако се има предвид и **1.5.5°**, се добива дека е точно и следново својство.

9°. Ако релацијата $\leqslant$ се дефинира во $\mathbf{N}$ со:

$$x \leqslant y \Leftrightarrow \mathbf{N}_x \subset \mathbf{N}_y \vee x = y, \tag{6′}$$

тогаш се добива подредување на $\mathbf{N}$.▒

Со помош на соодветните својства спомнати во 7°, лесно се докажува и следново својство:

10°. Ако $x, y \in \mathbf{N}$, тогаш:

(i) $x < x^+$; (ii) $x < y \Leftrightarrow x \in \mathbf{N}_y$; (iii) $x < y \Rightarrow x^+ \leqslant y$;
(iv) $0 \leqslant x$; (v) $\mathbf{N}_x = \{u \mid u \in \mathbf{N},\ u < x\}$. ▒

Пред да го докажеме најважното својство на подредувањето на **N**, ќе воведеме уште еден поим во врска со подредените множества.

Нека M е подредено множество и A непразно подмножество на M. За елементот $a \in A$ велиме дека е *најмал* во A акко:

$$(\forall x \in A)\ a \leqslant x. \tag{8}$$

Според **10°** (iv), (v) добиваме дека:

11°. Нулата е најмалиот елемент во **N** и, поопшто, x е најмалиот елемент во $\mathbf{N} \setminus \mathbf{N}_x$. (Овде употребивме определен член, бидејќи, според (8), ако постои најмал елемент, тој е единствен.) ▒

За подреденото множество M велиме дека е *добро подредено* акко секое непразно подмножество од M има најмал елемент.

Дадените дефиниции и својството **11°** беа подготовка за формулирање и докажување на следново својство.

12°. **N** е добро подредено множество.

Доказ. Нека A е непразно подмножество од **N**; ако $0 \in A$, тогаш, според **11°**, $0 \leqslant x$ за секој $x \in A$, т.е. 0 е најмал елемент во A. Затоа ќе претпоставиме дека $0 \notin A$. Нека S е подмножество од **N** определено со:

$$S = \{x \mid x \in \mathbf{N} \wedge (\forall y \in A)\ x < y\}. \tag{*}$$

Множеството S не е празно, бидејќи поради $0 \notin A$, имаме $0 < y$ за секој $y \in A$, па, значи, $0 \in S$. Не може да биде точен исказот $(\forall x)\ [x \in S \Rightarrow x^+ \in S]$, бидејќи тогаш би имале $S = \mathbf{N}$, од што би следувало дека A е празно.

Според тоа, постои $s \in S$, таков што $s^+ \notin S$. Ќе покажеме дека $a = s^+$ е најмал елемент во A. Навистина, од $s \in S$, според (*), следува $s < y$ за секој $y \in A$, а од тоа, според **10°** (iii), и $s^+ \leqslant y$, исто така, за секој $y \in A$; ако $s^+ \notin A$, би имале $s^+ < y$ за секој $y \in A$, од што би следувало $s^+ \in S$; според тоа, $s^+ = a \in A$ и $(\forall y \in A)\ a \leqslant y$, т.е. a е најмал елемент во A. ▒

Ќе формулираме уште неколку дефиниции во врска со подредените множества.

Ако B е непразно подмножество од подреденото множество M и ако $b \in B$ е таков елемент од B што

$$(\forall y \in B)\ y \leqslant b, \tag{8'}$$

тогаш b се вика *најголем елемент* во B.

Нека C е непразно подмножество од подреденото множество M. За елементот $m \in M$ велиме дека е *мајорант* на C во M акко:

$$(\forall y \in C)\ y \leqslant m \tag{9}$$

Најмалиот мајорант на C во M (ако таков постои) се вика *супремум* на C во M и се означува со $sup_M C$, или само со $sup\ C$, ако M е однапред фиксирано.

Елементот $n \in M$ се вика *минорант* на C во M акко

$$(\forall x \in C)\ n \leqslant x \tag{9'}$$

Најголемиот минорант n_0 на C во M (ако таков постои) се означува со $inf_M C$ (односно $inf\ C$) и се вика *инфимум* на C во M.

C се вика *минорирано* (*мајорирано*) акко има барем еден минорант (мајорант) во M. C се вика *ограничено* во M акко е и мајорирано и минорирано во M.[1)]

Од **12°** следува дека:

13°. Секое непразно подмножество A од $\mathbf{N}$ има инфимум во $\mathbf{N}$. (Тоа е, имено, најмалиот елемент на A).■

Ако се има предвид тоа што $x < x^+$, добиваме дека:

14°. Во $\mathbf{N}$ нема најголем елемент.■

15°. Едно непразно подмножество A од $\mathbf{N}$ е мајорирано во $\mathbf{N}$ акко има најголем елемент m, и притоа $m = sup\ A$.

Доказ. Јасно е дека, ако m е најголем елемент на A, тогаш m е и супремум на A во $\mathbf{N}$.

Да претпоставиме дека A е мајорирано во $\mathbf{N}$. Тогаш множеството B од мајоранти на A е непразно, па според **12°**, постои најмал елемент m, т.е. $m = sup\ A$. Потоа, се покажува дека $m \in A$, од што ќе следува дека m е најголем елемент во A.■

16°. Ако M е непразно подмножество на $\mathbf{N}$ и ако во M нема најголем елемент, тогаш постои биекција $f: \mathbf{N} \to M$.

Доказ. Ќе дадеме само скица на доказот. Да го означиме најмалиот елемент на M со a_0; потоа, најмалиот елемент на $M \setminus \{a_0\}$ го означуваме со a_1. Да претпоставиме дека сме го формирале подмножеството $A_n = \{a_k \mid k \in \mathbf{N}_n\}$ на M, така што:

$$r, s \in \mathbf{N}_n,\ r < s \Rightarrow a_r < a_s. \tag{*}$$

Множеството $M \setminus A_n$ не е празно, бидејќи во спротивен случај a_{n-} би бил најголем елемент на M. Најмалиот елемент на $M \setminus A_n$ го означуваме со a_n.

[1)] Поимите за инфимум и супремум не се битни кај природните броеви, бидејќи се сведуваат на поимите за најмал, односно најголем елемент. Овие поими ќе ги сретнуваме повеќе кај реалните броеви.

Со горната дискусија добивме дека постои инјекција $f: n \to a_n$ од **N** во M. Потоа, претпоставката дека $M \setminus f(\mathbf{N}) = B$ е непразно би не довела до апсурд, од што и ќе следува дека f е биекција. ∎

ВЕЖБИ: **2.** Во секој од следните случаи да се испита кои од петте Пеанови аксиоми се задоволени.

а) $A = \{0, 1, 2\}$, $0^+ = 1$, $1^+ = 2$, $2^+ = 0$.

б) $B = \{0, 1\}$, $0^+ = 1^+ = 1$.

в) $\mathbf{N}^\omega = \mathbf{N} \cup \{\omega\}$, $\omega^+ = \omega$, а x^+ е определено на ист начин како и во **N**, за $x \in \mathbf{N}$.

3. Нека a е фиксен природен број и нека g е дадено пресликување од **N** во **N**. Да се покаже дека со равенствата:

$$h(0) = a, \quad h(x^+) = g(h(x))$$

е определено пресликување од **N** во **N**. (За h велиме дека е определено рекурзивно со помош на a и g.)

4. Нека f_1 и f_2 се дадени пресликувања од **N** во **N** и нека ставиме $h(x, 0) = f_1(x)$, $h(x, y^+) = f_2(h(x, y))$. Да се покаже дека h е пресликување од $\mathbf{N} \times \mathbf{N}$ во **N**.

5. Нека f е дадено пресликување од **N** во **N**, а g од $\mathbf{N} \times \mathbf{N}$ во **N**. Да се покаже дека со: $h(x, 0) = f(x)$, $h(x, y^+) = g(h(x, y), x)$ е определено пресликување од $\mathbf{N} \times \mathbf{N}$ во **N**. Дали резултатот од вежбата **4.** е специјален случај од овој резултат?

6. Да се покаже дека следнава исказна функција:

$$x \ll y \vee y \ll x^+$$

е вистинита во **N**.

7. Да се покаже дека, ако $\varphi(x)$ е исказна функција во **N**, таква што: $\varphi(0)$ и $(\forall x)[\varphi(x) \Rightarrow \varphi(x^+)]$ се вистинити искази, тогаш $\varphi(x)$ е вистинита исказна функција. (Принцип на математичка индукција.).

8. Да се покаже дека во Пеановиот систем на аксиоми, аксиомата за индукција може да се замени со принципот на математичка индукција.

9. Нека f е инјекција од **N** во **N**, таква што $x < y \Rightarrow f(x) < f(y)$. Да се покаже дека $(\forall x)\ x \leqslant f(x)$.

10. Нека A е непразно подмножество од подреденото множество M. Да се покаже дека A има најмал (најголем) елемент акко некој минорант (мајорант) на A припаѓа на A.

.11. Едно подмножество од **Z** има најмал (најголем) елемент акко е минорирано (мајорирано).

.12. Нека $A = \{x \mid x \in \mathbf{Q},\ x > 0,\ x^2 \leqslant 2\}$. Да се покаже дека:

(i) A нема најмал, ни најголем елемент.

(ii) $inf_{\mathbf{Q}} A = 0$, A е мајорирано во **Q**, но нема супремум во **Q**.

(iii) $sup_{\mathbf{R}} A = \sqrt{2}$.

1.7. КОНЕЧНИ И БЕСКОНЕЧНИ МНОЖЕСТВА

Поимот за конечност е толку близок до нас што реченицата "Едно множество е конечно акко има конечно многу елементи" не е толку без смисла како што на прв поглед изгледа. Прашањето "Што е конечно множество?" еден нематематичар не го интересира, бидејќи за него секое множество со кое се среќава во пракса е конечно, т.е. (за него) "конечно множество" значи исто

што и "множество". Но, и нематематичарот (а и математичарот) се интересира за "бројот на елементите во дадено множество M". До одговор се доаѓа често со "броење" на елементите од M ("еден, два, . . .") и ако во процесот на броењето се исцрпат елементите на M, последниот број m до кој ќе се дојде се вика број на елементи на M. При броењето, се конструира биекција $f: n \to a_n$ од $\mathbf{N}_m^+ = \{1, \ldots, m\}$ во M. Извршената дискусија ја сугерира дефиницијата што ќе ја дадеме подолу.

Нека $m \in \mathbf{N}^+$ е позитивен природен број. За множеството M велиме дека се состои од m елементи и пишуваме $|M| = m$ акко постои биекција f од $\mathbf{N}_m^+$ во M. Според тоа:

$$|M| = m \Leftrightarrow M \sim \mathbf{N}_m^+. \tag{1}$$

За празното множество $\varnothing$ ќе велиме дека има 0 елементи, т.е. $|\varnothing| = 0$. Имајќи го предвид тоа што $\mathbf{N}_0^+ = \varnothing$, заклучуваме дека (1) е точно и за $m = 0$.

Од дадената дефиниција, ако се имаат предвид и својствата **1.4.9°** и **1.6. 7°** (ix), се добива:

1°. (i) $|\mathbf{N}_m| = m$; (ii) $|\mathbf{N}_m^+| = m$;

(iii) $M \sim L, |M| = m \Rightarrow |L| = m$; (iv) $|M| = 0 \Leftrightarrow M = \varnothing$.

За едно множество M велиме дека е *конечно* акко постои природен број m, таков што $|M| = m$.

Пред да формулираме неколку својства за конечните множества, да уочиме дека:

2°. $|M| = m$, $m \neq 0$ акко M може да се претстави во облик:

$$M = \{a_1, a_2, \ldots, a_m\}, \tag{2}$$

каде што $a_i \neq a_j$ за $i \neq j$. (Се разбира, наместо буквата a може да се употреби која било друга буква).

Ќе формулираме неколку својства чија точност е "очигледна". Се препорачува читателот да се обиде да ги докаже овие својства).

3°. Ако $|M| = m$ и $K \subset M$, тогаш постои природен број k, таков што $k < m$ и $|K| = k$.

4°. Секое подмножество од едно конечно множество е конечно.

5°. Бројот на елементите од едно конечно множество е еднозначно определен.

Да го докажеме последново својство. Нека M е конечно множество и нека $|M| = m$, $|M| = n$. Тогаш, $|\mathbf{N}_m| = |\mathbf{N}_n|$. Да претпоставиме дека $n < m$ и дека n е најмалиот број со особината $|\mathbf{N}_m| = |\mathbf{N}_n|$; тогаш ќе имаме и $\mathbf{N}_n \subset \mathbf{N}_m$, од што, според **3°**, ќе следува дека $|\mathbf{N}_n| = k$ за некој $k < n$, т.е. $|\mathbf{N}_k| = |\mathbf{N}_n|$, а ова е во спротивност со претпоставката за минималност на n.

6°. Ако L и M се конечни множества, тогаш и множествата $L \cup M$, $L \times M$ се конечни.

Доказ. Ќе претпоставиме дека и двете множества L и M се непразни, бидејќи ако едно од нив е празно, тогаш $L\times M=\varnothing$ и $L\cup M=L$ или $L\cup M=M$.

Ако $L\subseteq M$, тогаш $M\cup L=M$. Затоа, да претпоставиме дека постои $a\in L\setminus M$. Тогаш, $M\cup L=(M\cup L\setminus\{a\})\cup\{a\}$. Множеството $K=M\cup(L\setminus\{a\})$ можеме да претпоставиме дека е конечно, па ако $|K|=k$, тогаш $|M\cup L|=k^+$.

Нека $L=\{a_1,\ldots,a_l\}$, $M=\{b_1,\ldots,b_{m+}\}$. Тогаш:

$L\times M=L\times\{b_1,\ldots,b_m\}\cup L\times\{b_{m+}\}$, од што следува дека $L\times M$ е конечно, бидејќи такви се $L\times\{b_1,\ldots,b_m\}$ и $L\times\{b_{m^+}\}$ $(\sim L)$.■

За едно множество M велиме дека е *бесконечно* ако не е конечно. Прво ќе докажеме дека постои бесконечно множество, а потоа и неколку карактеристични својства на бесконечните множества.

7°. Множеството $\mathbf{N}$ е бесконечно.

Доказ. Да претпоставиме дека е точно спротивното, т.е. дека $\mathbf{N}$ е конечно. Тогаш би имале $|\mathbf{N}|=|\mathbf{N}_m|$ за некој природен број m; ако се има предвид 3°, и тоа што $\mathbf{N}_m\subset\mathbf{N}$, се добива дека $|\mathbf{N}_m|=n$ за некој $n<m$, што не е можно според 5°.■

Ќе докажеме уште две карактеристики на бесконечните множества.

8°. Ако M е дадено множество, тогаш следните искази се еквивалентни:

(i) M е бесконечно; (ii) Постои подмножество на M што е еквивалентно со $\mathbf{N}$; (iii) M е еквивалентно со некое свое подможество.

Доказ. Прво ќе покажеме дека (i) $\Rightarrow$ (ii).

Нека M е бесконечно; тогаш $M\neq\varnothing$; да избереме еден елемент $a_0\in M$ произволно; да претпоставиме дека $A_n=\{a_0,a_1,\ldots,a_n\}$ е подмножество на M такво што $a_i\neq a_j$ за $i\neq j$; множеството $M\setminus A_n$ е непразно бидејќи, во спротивен случај, $M=A_n$ би било конечно; да означиме со a_{n+} произволен елемент од $M\setminus A_n$; со спроведената постапка покажавме дека постои инјекција $f:n\to a_n$ од $\mathbf{N}$ во M; ако ставиме $f(\mathbf{N})=A$ добиваме подмножество A од M, такво што $\mathbf{N}\sim A$.

Ќе покажеме сега дека (ii) $\Rightarrow$ (iii).

Нека $A=\{a_n\mid n\in\mathbf{N}\}$ е подмножество од M, при што $f:n\to a_n$ е биекција од $\mathbf{N}$ во A; да го означиме со K множеството $M\setminus\{a_0\}$; имаме $K\subset M$; да ставиме $g(a_n)=a_{n+}$ за $a_n\in A$ и $g(x)=x$, за $x\in M\setminus A$, така добивме биекција g од M во K, па, значи, $M\sim K$.

Преостанува да покажеме дека (iii) $\Rightarrow$ (i).

Нека $K\sim M$, каде што K е вистинско подмножество од M. Не може M да биде конечно, бидејќи тогаш, според 3°, би имале $|K|<|M|$ и $|K|=|M|$.■

Да ги окарактеризираме бесконечните (па ,според тоа, и конечните) подмножества на $\mathbf{N}$.

9°. Едно непразно подмножество M од $\mathbf{N}$ е бесконечно акко не е мајорирано во $\mathbf{N}$.

Доказ. Ако M е мајорирано, тогаш (според 1.6.**15**°) M има најголем елемент m, од што следува дека M е конечно, бидејќи $M \subseteq \mathbf{N}_{m+}$.

Обратно, ако M не е мајорирано, тогаш (според 1.6.**16**°) $\mathbf{N} \sim M$, од што следува дека M е бесконечно. ∎

За едно множество M велиме дека е *пребројво* акко е еквивалентно со $\mathbf{N}$, т.е. акко постои биекција f од $\mathbf{N}$ во M. Ако се имаат предвид некои од порано формулираните својства, се добива и следново својство:

10°. (i) Секое бесконечно подмножество на $\mathbf{N}$ е пребројво.

(ii) Секое пребројво множество е бесконечно.

(iii) M е бесконечно множество акко постои пребројво подмножество на M. ∎

Да покажеме дека постојат бесконечни непребројви множества.

11°. $\mathbf{B}(\mathbf{N})$ е бесконечно непребројво множество.

Доказ. Прво, $B(\mathbf{N})$ е бесконечно множество, бидејќи $\{\{x\} \mid x \in \mathbf{N}\}$ е пребројво подмножество од $B(\mathbf{N})$.

Нека $f: \mathbf{N} \to B(\mathbf{N})$ е пресликување од $\mathbf{N}$ во $B(\mathbf{N})$.

Според тоа, ако $m \in \mathbf{N}$, тогаш $f(m) \subseteq \mathbf{N}$. Да го означиме со K подмножеството на $\mathbf{N}$ определено со:

$$K = \{x \mid x \in \mathbf{N},\ x \notin f(x)\} \qquad (*)$$

Ќе покажеме дека $K \neq f(x)$ за секој $x \in \mathbf{N}$, од што ќе следува дека f не е сурјекција, па, значи, ни биекција; со тоа ќе покажеме дека $B(\mathbf{N})$ не е пребројво.

Да претпоставиме дека $f(a) = K$ за некој $a \in \mathbf{N}$. Се прашуваме дали $a \in K$ или $a \notin K$. Ако $a \in K$, тогаш $a \notin f(a) = K$, од што ќе следува дека $a \notin K$, ако, пак, $a \notin K$, тогаш $a \notin f(a) = K$ од што ќе следува $a \in K$. Според тоа, не е можно да биде $a \in K$, ниту $a \notin K$, што е апсурд. Од тоа заклучивме дека $f(x) \neq K$ за секој $x \in \mathbf{N}$. ∎

ВЕЖБИ: **2.** Нека M и K се конечни, а N кое било множество. Да се покаже дека и секое од приложените множества е конечно:

$$M \cap N,\ M \setminus N,\ M \dot{-} N,\ B(M),\ M^K,\ S(M).$$

3. Ако M е бесконечно, тогаш и $B(M)$, M^M, $S(M)$ се бесконечни.

4. Во кои случаи M^N е конечно?

5. Нека $A = \{x \mid m \leqslant x \leqslant n\}$, каде m и n се дадени елементи од $\mathbf{N}$. Да се покаже дека A е конечно.

6. Нека M е конечно множество и нека f е сурјекција од M во N. Да се покаже дека N е конечно и дека $|N| \leqslant |M|$.

7. Нека M и N се две конечни множества со ист број на елементи и нека f е пресликување од M во N. Да се покаже дека следниве искази се еквивалентни:

(i) f е инјекција; (ii) f е сурјекција; (iii) f е биекција.

8. Нека M е подредено множество. Да се покаже дека M е конечно акко секое непразно подмножество од M има и најголем и најмал елемент.

9. Ако M е пребројво, а N конечно или пребројво, тогаш и $M \cup N$ е пребројво.

10. Ако M е пребројво, тогаш секое бесконечно подмножество на M е пребројво.

***11.** Ако M е пребројво, а N непразно конечно или пребројво множество, тогаш и, $M \times N$ е пребројво.

.12. (i) Едно непразно подмножество A на $\mathbf{Z}$ е конечно акко A е минорирано и мајорирано во $\mathbf{Z}$.

(ii) Ако $a, b \in \mathbf{Z}$, тогаш $\{x \mid x \in \mathbf{Z},\ a \leqslant x \leqslant b\}$ е конечно.

(iii) Ако $a, b \in \mathbf{Q}$ и $a < b$, тогаш $\{x \mid x \in \mathbf{Q},\ a < x < b\}$ е бесконечно.

*(iv) $\mathbf{Z}$ и $\mathbf{Q}$ се пребројви, а $\mathbf{R}$ и $\mathbf{C}$ се бесконечни непребројви множества.

1. 8. СИСТЕМИ И НИЗИ

Ако J и M се две множества, тогаш секој елемент $f \in M^J$, т.е. пресликување од J во M се вика *J-систем* во M и се означува со:

$$(f_i \mid i \in J), \tag{1}$$

каде што $f_i = f(i)$. За J велиме дека е множество индекси. Значи, J-систем во M е друг термин за пресликување од J во M, при што се сака „да се истакнат сликите". Специјално, треба да се има предвид тоа што:

$$(f_i \mid i \in J) \neq \{f_i \mid i \in J\}. \tag{2}$$

Имено, десната страна на (2) е подмножеството $f(J)$ од M, додека левата е самото пресликување.

Меѓу системите елементи и пресликувањата, сепак, правиме извесна разлика со тоа што допуштаме две различни пресликувања да определуваат еднакви системи елементи. Имено, ако $f \in M^J$, $g \in N^J$, тогаш:

$$(f_i \mid i \in J) = (g_i \mid i \in J) \Leftrightarrow (\forall\, i \in J) f_i = g_i \tag{3}$$

Секој $\mathbf{N}^+$ - систем се вика *бесконечна низа*. Ако ставиме $f(n) = a_n$, тогаш една бесконечна низа може да се претстави во облик

$$(a_1,\ a_2, \ldots,\ a_n, \ldots). \tag{1'}$$

(и $\mathbf{N}$ - системите се викаат бесконечни низи.) Ако, пак, $J = \mathbf{N}_n^+$, тогаш J-системите се викаат *n-низи*, односно *подредени n-ки*. Еден n-систем се означува со:

$$(a_1,\ a_2, \ldots,\ a_n). \tag{1''}$$

Ако се има предвид тоа што $\mathbf{N}_0^+ = \varnothing$, добиваме дека 0-систем во M е празното пресликување $\varnothing^{(M)}$, а него го идентификуваме со празното множесто $\varnothing$, во согласност со договорот (3) за еднаквоста на системи.

Множеството од сите подредени n-ки во M ќе го означуваме со M^n; се покажува за корисно да се смета дека $M^1 = M$.

Нека $\sum$ е множество чии елементи се множества. Ако $(f_i \mid i \in J)$ е J-систем во $\sum$, тогаш велиме дека тоа е J-систем множества. За да истакнеме дека f_i е множество, ќе пишуваме M_i наместо f_i, т.е. системот ќе го претставуваме во облик:

$$(M_i \mid i \in J) \tag{4}$$

Ќе дефинираме поими за пресек и унија на систем множества.

Имено, ако е даден системот множества од облик (4), тогаш:

$$\bigcap_{i\in J} M_i = \{x \mid (\forall i \in J)\, x \in M_i\}, \tag{5}$$

$$\bigcup_{i\in J} M_i = \{x \mid (\exists i \in J)\, x \in M_i\}. \tag{6}$$

Велиме дека $\bigcap_{i\in J} M_i$ е *пресек*, а $\bigcup_{i\in J} M_i$ *унија* на *системот множества* (4).

Поимите за пресек и унија, воведени во 1.3., се специјални случаи од новите поими. Навистина, ако $J = \mathbf{N}_2^+ = \{1,2\}$, тогаш

$$\begin{aligned} \bigcap_{i\in I} M_i &= \{x \mid (\forall\, i \in J)\, x \in M_i\} \\ &= \{x \mid x \in M_1 \wedge x \in M_2\} \\ &= M_1 \cap M_2 \end{aligned} \tag{5'}$$

$$\begin{aligned} \bigcup_{i\in I} M_i &= \{x \mid (\exists\, i \in J)\, x \in M_i\} \\ &= \{x \mid x \in M_1 \vee x \in M_2\} \\ &= M_1 \cup M_2 \end{aligned} \tag{6'}$$

Ако $J = \{1\}$ се состои само од еден елемент, тогаш:

$$\bigcap_{i\in J} M_i = M_1 = \bigcup_{i\in J} M_i.$$

Поопшто, ако $(M_k \mid k \in \mathbf{N}_n^+)$ е n-низа множества, тогаш пишуваме:

$$\bigcap_{\kappa} M_k = M_1 \cap M_2 \cap \ldots \cap M_n, \tag{5''}$$

$$\bigcup_{\kappa} M_k = M_1 \cup M_2 \cup \ldots \cup M_n. \tag{6''}$$

Ќе го обопштиме и поимот декартов (или директен) производ на множества. Нека е даден системот множества (4) и нека M е унијата на тој систем, т.е.

$$M = \bigcup_{i\in J} M_i.$$

Множеството што се состои од сите J-системи $(x_i \mid i \in J)$ во M, такви што $x_i \in M_i$ за секој $i \in J$, се вика *декартов* (или *директен*) *производ* на даденият систем множества (4) и ќе го означуваме со $\prod_{i \in J} M_i$. Според тоа:

$$\prod_{i \in J} M_i = \{(x_i \mid i \in J) \mid (\forall\, i \in J)\, x_i \in M_i\}. \tag{7}$$

Во специјалниот случај, кога $J = \mathbf{N}_n^+$, ќе пишуваме

$$\prod_{i} M_i = M_1 \times M_2 \times \ldots . \times M_n. \tag{7'}$$

Според тоа:

$$M_1 \times \ldots . \times M_n = \{(x_1, \ldots . , x_n) \mid x_1 \in M_1, \ldots , x_n \in M_n\}. \tag{7''}$$

Специјално за $n = 2$ се добива дека дефиницијата дадена во 1.3. е специјален случај од овде воведениот поопшт поим.

ВЕЖБИ. 2. Ако $M = \{a, b\}$, да се определат множествата: M^2, M^3, M^4.

3. Ако сите множества од системот $(M_k \mid k \in \mathbf{N}_n^+)$ се конечни, тогаш множествата:

$$M_1 \cap \ldots \cap M_n;\ M_1 \cup \ldots \cup M_n;\ M_1 \times \ldots \times M_n$$

се конечни.

4. Множествата $M_1 \times M_2 \times M_3$, $(M_1 \times M_2) \times M_3$, и $M_1 \times (M_2 \times M_3)$ се еквивалентни.

5. Едно множество M е конечно акко M^n е конечно за некој $n \in$.

1.9. НЕКОЛКУ ЗАБЕЛЕШКИ ЗА ТЕОРИЈАТА НА МНОЖЕСТВАТА

Теоријата на множествата е млада математичка дисциплина. За нејзин основач со право може да се смета германскиот математичар Г. Кантор кој (кон крајот на минатиот век) прв ги третирал множествата како објекти на самостојна математичка дисциплина. Канторовата теорија на множествата не е аксиоматски изградена, туку се базира само на интуитивната претстава за овој поим ,а така, впрочем, се работи и во оваа книга. Но, не долго по почетокот на оваа теорија се покажало дека сосема слободното оперирање со поимот множество доведува до "несакани" резултати, познати како парадокси на теријата на множествата. Еден од најпознатите парадокси прв пат е формулиран од англискиот филозоф и математичар Расел во 1901 год., па затоа и се вика *Раселов парадокс.*

До овој парадокс се доаѓа ако се разгледа "множеството" чии елементи се сите множества X, такви што $X \notin X$. Ако ова "множество" го означиме со M, тогаш, според договорот од 1.2., ќе имаме:

$$M = \{X \mid X \text{ е множество и } X \notin X\}. \tag{1}.$$

На пример, множеството S од сите студенти не е студент, т.е. $S \notin S$, па, значи, $S \in M$. Исто така, $\emptyset \in M$, бидејќи $\emptyset \notin \emptyset$. Уште повеќе, сите примери на множества изнесени досега се елементи на M.

Се прашуваме: кој од следните искази $M \in M$, $M \notin M$ е вистинит? Дека еден и само еден од нив треба да е вистинит следува од тоа што вториот е негација на првиот. Ако $M \in M$, тогаш според (1), M е множество, такво што $M \notin M$. Обратно, ако $M \notin M$, тогаш пак, според (1), добиваме $M \in M$. Така, добивме дека:

$$M \in M \Rightarrow M \notin M \text{ и } M \notin M \Rightarrow M \in M \tag{2}$$

што е апсурд. Според ова, не може да биде точен ни еден од исказите $M \in M$, $M \notin M$.

Значи, добивме исказ $M \in M$ што не е ни вистинит ни невистинит, а тоа е во спротивност со нашето сфаќање за поимот исказ. Да се обидеме да го објасниме добиениот апсурден резултат, т.е. парадоксот на Расел.

За да добиеме конкретен исказ од исказната функција "X е множество такво што $X \notin X$" треба во неа X да се замени со множество. Апсурдниот резултат што е добиен по замената на X со M ни сугерира да заклучиме дека постои исказна функција $\psi(x)$, таква што $\{x \mid \psi(x)\}$ не е множество. Во тој случај се вели дека $\psi(x)$ не е *колективирачка исказна функција.*

Појавата на парадоксите беше една од причините за аксиоматизирањето на теоријата на множествата. На аксиоматското градење на оваа теорија овде нема да се задржиме, а ќе ги изнесеме само принципите на тој пристап. Имено, поимите: множество и припадност се земаат како основни, т.е. недефинирани. Потоа, се формулираат соодветни аксиоми и се докажуваат теореми како последици на аксиомите, без притоа да се користи интуитивната претстава за множества. Една од аксиомите е *аксиомата за обемност*, според која: *ако две множества се состојат од исти елементи, тогаш тие се еднакви.* Поголемиот дел од другите аксиоми, всушност, се тврдења за тоа дека соодветни исказни функции се колективирачки. Ќе ја спомнеме класата *аксиоми за спецификација*, според која: *ако* $\Phi(X)$ *е исказна функција, тогаш за секое множество* M, *исказната функција* $\Phi(X) \wedge X \in M$ *е колективирачка т.е. со*

$$\{X \mid \Phi(X) \wedge X \in M\} \tag{3}$$

е определено множество. Како последица се добива дека; не постои множество M, такво што секое множество е елемент на M. Навистина, кога такво множество M би постоело, тогаш ако во (3) наместо $\Phi(X)$ ставиме $X \notin X \wedge X$ е множество, би добиле дека

$$\{X \mid X \notin X \wedge X \text{ е множество}\} \tag{4}$$

е множество, т.е. би го добиле апсурдниот резултат од парадоксот на Расел.

На крајот, да забележиме дека теоријата на множествата изградена во оваа глава може да се аксиоматизира (така се работи, на пример, во [11]) со помош на следниов систем аксиоми.

(I) *Аксиомата за обемност.*

(II) *Фамилијата аксиоми за спецификација.*

(III) *Аксиома за егзистенција на празно множество*: Постои множество $\emptyset$, такво што $(\forall X)\, X \notin \emptyset$.

(IV) *Аксиома за неподредена двојка*: Ако M и N се множества, тогаш постои множество S, такво што $S = \{M, N\}$, т.е. $(\forall X)\,[X \in S \Leftrightarrow X = M \vee X = N]$.

(V) *Аксиома за егзистенција на булеан*: Ако M е множество, тогаш постои множество N што е булеан на M, т.е.

$$(\forall X)\ [X \in N \Leftrightarrow (\forall Y)\ (Y \in X \Rightarrow Y \in M)].$$

(VI) *Аксиома за унија на фамилија множества*: Ако M е множество, тогаш постои множество N што е унија на елементите од M, т.е.

$$(\forall X)\ [X \in N \Leftrightarrow (\exists Y)\ (X \in Y \wedge Y \in M].$$

(VII) *Аксиома за егзистенција на бесконечно множество*: Постои множеството $\mathbf{N}$ на природните броеви.

(VIII) *Аксиома на изборот*: Ако M е непразно множество чии елементи се, исто така, непразни множества, тогаш постои множество N што има, точно по еден заеднички елемент со секој елемент на M.

На читателот којшто има желба да добие увид во аксиоматиката на теоријата на множествата, му ги препорачуваме книгите [3] и [11], каде што ќе сретне и многу резултати од теоријата на множествата, што (од разбирливи причини) не ги спомнавме во погоре направениот преглед.

ВЕЖБИ. **2.** Нека M е множеството членови на едно семејство во кое важи правилото: "секое утро треба да биде измиен секој член на семејството". Притоа е определен еден член на семејството, да го означиме со a, кој има задача "да ги мие членовите на семејството што не се мијат самите и тоа само нив". Да го означиме со A подмножеството на M што се состои од сите елементи на M што ги мие a. Се наложува задача да се одговори на прашањето: "Дали $a \in A$"? Да се објасни добиениот апсурден резултат.

3. Само од аксиомата за обемност следува дека, ако една исказна функција $\varphi(x)$ е колективирачка, тогаш множеството $\{x \mid \varphi(x)\}$ е еднозначно определено.

4. Од аксиомите за обемност и спецификација следува дека, ако M и N се множества, тогаш $M \cap N$ и $M \setminus N$ се еднозначно определени множества.

5. Од аксиомата за обемност следува дека:

(i) постои најмногу едно празно множество.

(ii) ако M е множество, тогаш постои најмногу едно множество што е булеан на M.

(iii) ако M и N се множества, тогаш постои најмногу едно множество P што е нивна унија и најмногу едно множество S што се состои од M и N, т.е. $S = \{M, N\}$.

2. ГРУПОИДИ. ОПЕРАЦИИ СО ПРИРОДНИ БРОЕВИ

2.1. ОПЕРАЦИИ

Пред да ја дадеме општата дефиниција на поимот операција, ќе се задржиме на операциите пресек, унија, разлика и симетрична разлика на подмножества од едно множество.

1) Нека $G = B(M)$ е булеанот на едно множество M. Ако $A, B \in G$, т.е. $A, B \subseteq M$, тогаш имаме $A \cap B$, $A \cup B$, $A \setminus B$, $A \dot{-} B \subseteq M$, т.е. $A \cap B$, $A \cup B$, $A \setminus B$, $A \dot{-} B \in G$. Поради ова, велиме дека $\cap$, $\cup$, $\setminus$, $\dot{-}$ се операции на G. Заедничка особина на сите овие операции е таа што ако $\square$ е која било од нив, тогаш на секоја подредена двојка $(A, B) \in G \times G$ со $\square$ ѝ се придружува елемент $C = A \square B \in G$. Според тоа, $\square$ може да се смета за пресликување од $G \times G$ во G.

Поопшто, ако G е множество, тогаш секое пресликување $f: G \times G \to G$ се вика *операција на* G. Според тоа, на секоја подредена двојка (x, y) елементи x и y од G ѝ се придружува еднозначно определен елемент z од G. За да го истакнеме тоа, пишуваме $z = xfy$. Значи:

$$z = xfy \Leftrightarrow f : (x, y) \to z. \tag{1}$$

Наместо f, ќе употребуваме некој од следниве знаци: $*$, $\cdot$, $+$, $-$, $:$, $\circ$, $\cup$, $\cap$, $\setminus$, ... Во оваа смисла, наместо $z = xfy$, ќе пишуваме: $z = x * y$, $z = x \cdot y$, $z = x + y$, ...

Да дадеме уште неколку примери.

2) Множењето (т.е. составувањето) на пресликувања е операција на множеството M^M од сите трансформации на M, т.е. пресликувања од M во M.

3) Нека $*$ е операција на конечното множество $G = \{a_1, a_2, a_3, \ldots, a_n\}$ и нека производот $a_i * a_j$ го означиме со a_{ij}. Така ја добиваме следнава шема:

$*$	a_1	a_2 .... a_j .... a_n
a_1	a_{11}	a_{12} .... a_{1j} .... a_{1n}
a_2	a_{21}	a_{22} .... a_{2j} .... a_{2n}
.	.	. . . .
.	.	. . . .
.	.	. . . .
a_i	a_{i1}	a_{i2} .... a_{ij} .... a_{in}
.	.	. . . .
.	.	. . . .
.	.	. . . .
a_n	a_{n1}	a_{n2} .... a_{nj} .... a_{nn}

нарачена *келиева шема* за дадената операција. При тоа ќе велиме дека $a_{i1}\, a_{i2} \ldots a_{in}$ е редицата што одговара на a_i, додека $a_{1j}\, a_{2j} \ldots a_{nj}$ е колоната што одговара на a_j. (Низата над цртата се вика главна редица, а низата лево од цртата — главна колона. Да уочиме дека главната редица и колоната се определени со една и иста низа.).

Да забележиме дека на секоја шема од горниот облик ѝ одговара соодветна операција.

4) Така, ако $G = \{a, b, c\}$, тогаш со шемата:

$*$	a	b	c
a	b	a	a
b	b	c	b
c	b	a	a

е определена следнава операција: $b * b = c$, $a * b = a * c = c * b = c * c = a$, $a * a = b * a = b * c = c * a = b$.

ВЕЖБИ. 1. Да се определат сите операции на множеството $G = \{a, b\}$.

2. Да се определат келиевите шеми на операциите од примерите 1) и 2) ако $M = \{1,2\}$.

3. Нека $M \neq \emptyset$. Унијата е операција на $H = B(M) \setminus \{\emptyset\}$, но разликата и симетричната разлика не се. Ако M има барем два различни елементи тогаш и пресекот не е операција на H.

Да се изврши слична дискусија и за случајот кога $H = B(M) \setminus \{M\}$.

4. Нека M е бесконечно множество и нека K е фамилијата од сите конечни подмножества, а H фамилијата од сите бесконечни подмножества на M.

Дали: унијата, пресекот, симетричната разлика, разликата е операција на: а) K; б) H?

5. Множеството од сите операции на едно конечно множество G е конечно.

2.2. ГРУПОИДИ

Ако $*$ е операција на множеството G, тогаш велиме дека $G(*)$ е *групоид*; притоа, G се вика *носител*, а $*$ *операција* на групоидот.

Во 2.1.1) имаме примери на четири групоиди: $G(\cup)$, $G(\cap)$, $G(\setminus)$, $G(\dot{-})$. Сите тие имаат ист носител, но различни операции, па, според тоа, тие се различни групоиди. Во 2.1.2) имаме пример уште на еден групоид $M^M(\cdot)$. Секоја келиева шема определува групоид. Во 2.1.4) е определен групоид со носител $\{a, b, c\}$.

Да дадеме уште неколку примери.

1) а)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

б)

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

в)

	e	a	b	c
e	e	a	b	c
a	e	a	b	c
b	a	a	a	a
c	b	b	c	a

(Во сите три примери имаме ист носител, но различни операции).

2) Ако се има предвид тоа што производ на пермутации е пермутација, добиваме дека $S(M)$ $(\cdot)$ е групоид. (Притоа $S(M)$ е множеството од сите пермутации на M, т.е. биекции од M во M, а операцијата множење на пермутации).

Специјално, ако $M = \{1, 2, 3\}$, тогаш пишуваме S_3, наместо $S(\{1, 2, 3\})$.

Според тоа, имаме: $S_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$.

Заради поекономично пишување, наместо $\begin{pmatrix}1&2&3\\i&j&k\end{pmatrix}$ ќе пишуваме (ijk), така што сега S_3 го добива следниов облик:

$S_3 = \{(1\ 2\ 3),\ (2\ 3\ 1),\ (3\ 1\ 2),\ (1\ 3\ 2),\ (2\ 1\ 3),\ (3\ 2\ 1)\}$, а келиевата шема на $S_3(\cdot)$ ќе гласи:

	(1 2 3)	(2 3 1)	(3 1 2)	(1 3 2)	(2 1 3)	(3 2 1)
(1 2 3)	(1 2 3)	(2 3 1)	(3 1 2)	(1 3 2)	(2 1 3)	(3 2 1)
(2 3 1)	(2 3 1)	(3 1 2)	(1 2 3)	(2 1 3)	(3 2 1)	(1 3 2)
(3 1 2)	(3 1 2)	(1 2 3)	(2 3 1)	(3 2 1)	(1 3 2)	(2 1 3)
(1 3 2)	(1 3 2)	(3 2 1)	(2 1 3)	(1 2 3)	(3 1 2)	(2 3 1)
(2 1 3)	(2 1 3)	(1 3 2)	(3 2 1)	(2 3 1)	(1 2 3)	(3 1 2)
(3 2 1)	(3 2 1)	(2 1 3)	(1 3 2)	(3 1 2)	(2 3 1)	(1 2 3).

3) Предмет на натамошни изучувања ќе бидат следниве групоиди: $\mathbf{N}(+)$, $\mathbf{N}(\cdot)$, $\mathbf{Z}(+)$, $\mathbf{Z}(\cdot)$, $\mathbf{Q}(+)$, $\mathbf{Q}(\cdot)$, $\mathbf{R}(+)$, $\mathbf{R}(\cdot)$.

Во натамошните општи дискусии, обично, ќе го изоставуваме знакот за операција. Имено, ако се работи за групоид $G(*)$, тогаш самиот носител G ќе го викаме групоид, а наместо $x * y$, ќе пишуваме xy. (Во вакви случаи се вели дека се работи за *мултипликативна ознака*).

Нека G е (мултипликативно означен) групоид.

За еден елемент $e' \in G$ се вели дека е *лева единица* на групоидот G акко:

$$(\forall x)^{1)} \quad e'x = x \tag{1}$$

Во иста смисла, $e'' \in G$ се вика *десна единица* на G акко:

$$(\forall x) \quad xe'' = x. \tag{1'}$$

За e велиме дека е *единица* ако е и лева и десна единица, т.е. акко:

$$xe = x = ex. \tag{1''}$$

---

[1]) Според договорот направен во 1.2., можевме овде да го изоставиме изразот "$(\forall x)$", а така и натаму ќе работиме.

Во примерот 2.1.1) $\varnothing$ е единица на групоидот $G(\cup)$ и на $G(\dot{-})$, а M на $G(\cap)$; групоидот $G(\setminus)$ има десна единица $\varnothing$, но нема лева единица. Во 2.1.2) единица е идентичното пресликување. Во 2.1.4) не постои ни лева ни десна единица. Во 1) а), б) e е единица, а во 1) b) e е лева единица, но не е единица.

Ќе докажеме две својства.

1°. Ако e' е лева, а e'' десна единица на групоидот G, тогаш $e' = e''$.

Доказ. Имаме $e'\,e'' = e''$, бидејќи e' е лева единица, но и $e'\,e'' = e'$, бидејќи e'' е десна единица, од што следува $e' = e''$. ▒

2°. Во еден групоид G има најмногу една единица.

Доказ. Ако e_1 и e_2 се единици на G, тогаш, според **1°**, имаме $e_1 = e_2$. ▒

Покрај мултипликативната ознака ќе ја користиме и *адитивната*, т.е. ќе пишуваме $x + y$. наместо $x*y$ Во овој случај единицата се вика нула на групоидот и се означува со o. Значи, o е нула на групоидот $G(+)$ акко:

$$x + o = x = o + x \quad \text{за секој} \quad x \in G.$$

Сега ќе разгледаме уште два вида групоиди.

За групоидот G велиме дека е *комутативен* акко:

$$xy = yx \tag{2}$$

а *асоцијативен* (или *полугрупа*) акко:

$$x(yz) = (xy)z. \tag{3}$$

Да ги илустрираме и овие поими со примерите разгледани во **2.1**.

Во 2.1.1) групоидите $G(\cap)$, $G(\cup)$ и $G(\dot{-})$ се и комутативни и асоцијативни, но $G(\setminus)$ нема ни една од овие особини. Во 2.1.2) групоидот е полугрупа (т.е. асоцијативен), а истото важи и за $S(M)$ од примерот 2). Што се однесува за комутативноста на овие полугрупи, точни се следните две тврдења.

3°. Ако M има барем два различни елементи, тогаш полугрупата M^M е некомутативна.

Доказ. Нека a и b се различни елементи од M. Ако ставиме $(\forall x \in M)$ $f(x) = a$, $g(x) = b$, добиваме две различни трансформации на M. Притоа, имаме $f = fg \neq gf = g$. ▒

4°. Ако M има барем три различни елементи, тогаш полугрупата $S(M)$ е некомутативна.

Доказ. Нека a, b, и c се различни елементи од M. Со: $f(a) = c$, $f(c) = a$, $f(x) = x$ за $x \neq a$, c и $g(b) = c$, $g(c) = b$, $g(x) = x$ за $x \neq b$, c се определени две различни пермутации на M, т.е. $f, g \in S(M)$. Притоа, $gf \neq fg$, бидејќи $gf(c) = a \neq b = fg(c)$. ▒

Да се задржиме на случајот кога G е конечен групоид определен со својата шема како што е наведено во 2.1.3). G ќе биде комутативен акко

$$a_{ij} = a_i a_j = a_j a_i = a_{ji}$$

за секои $i, j = 1, \ldots, n$. Елементот a_r ќе биде лева (десна) единица акко

$$a_{rj} = a_r a_j = a_j \quad (a_{ir} = a_i a_r = a_i)$$

за секој $j = 1, \ldots, n$ ($i = 1, \ldots, n$). Според ова, точно е следново тврдење:

5°. Нека G е определен со својата шема. Тогаш:

(i) G е комутативен акко неговата шема е симетрична (т.е. секоја редица се совпаѓа со соодветната колона).

(ii) Еден елемент на G е лева (десна) единица акко неговата редица (колона) се совпаѓа со главната редица (колона).▒

Како примена на ова тврдење добиваме дека групоидите од 1) а), б) се комутативни со единица e, како и дека групоидот од 1) в) е некомутативен, во кој e и a се леви единици. (Слична анализа може да се изврши и на другите примери).

Да забележиме и дека:

6.° Ако $G = \{a\}$ е едноелементен групоид, тогаш тој е комутативна полугрупа со единица a.▒

Да се задржиме сега на прашањето како се утврдува дали еден групоид што е определен со својата шема е полугрупа. Во принцип, одговорот на ова прашање е едноставен. Имено, треба да се формираат сите подредени тројки (a_i, a_j, a_k) и да се провери дали за секоја таква тројка е точно равенството

$$(a_i a_j) a_k = a_i (a_j a_k). \tag{4}$$

Ако барем во еден случај тоа равенство не е точно, тогаш групоидот не е полугрупа.

Така, групоидот од 2.1.4) не е полугрупа, бидејќи на пример,

$$(aa)\, b = bb = c, \quad \text{но} \quad a\,(ab) = aa = b.$$

4) Да покажеме дека групоидот:

$*$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

($*$ е операцијата еквивалентост $\Leftrightarrow$ определена во 1.2.)

е полугрупа. Навистина, од шемата, добиваме:

$$(\top * \top) * \top = \top * \top = \top, \quad \top * (\top * \top) = \top * \top = \top;$$
$$(\top * \top) * \bot = \top * \bot = \bot, \quad \top * (\top * \bot) = \top * \bot = \bot;$$
$$(\top * \bot) * \top = \bot * \top = \bot, \quad \top * (\bot * \top) = \top * \bot = \bot;$$

$$(\bot * \top) * \top = \bot * \top = \bot, \quad \bot * (\top * \top) = \bot * \top = \bot;$$
$$(\top * \bot) * \bot = \bot * \bot = \top, \quad \top * (\bot * \bot) = \top * \top = \top;$$
$$(\bot * \top) * \bot = \bot * \bot = \top, \quad \bot * (\top * \bot) = \bot * \bot = \top;$$
$$(\bot * \bot) * \top = \top * \top = \top, \quad \bot * (\bot * \top) = \bot * \bot = \top;$$
$$(\bot * \bot) * \bot = \top * \bot = \bot, \quad \bot * (\bot * \bot) = \bot * \top = \bot.$$

Како што гледаме, потребна ни беше прилично обемна работа за да покажеме дека е полугрупа еден групоид што се состои само од два елемента. Ќе докажеме неколку тврдења кои во некои случаи овозможуваат полесно да се покаже дека даден групоид е полугрупа.

7°. Ако G е групоид со единица e, тогаш:

$$x = e \vee y = e \vee z = e \Rightarrow x(yz) = (xy)z.$$

Доказ. За $x = e$ имаме $e(yz) = yz = (ey)z$, а слично се добива равенство и во другите случаи. ▨

8°. Ако G е комутативен групоид, тогаш:

(i) $x(xx) = (xx)x$;

(ii) $x(yx) = (xy)x$;

(iii) $x(yz) = (xy)z \Rightarrow z(yx) = (zy)x$.

Доказ. (i) е специјален случај од (ii).

(ii) Ако се искористи комутативноста на G, добиваме:

$$x(yx) = (yx)x = (xy)x.$$

(iii) $x(yz) = (xy)z \Rightarrow$

$$z(yx) = (yx)z = (xy)z = x(yz) = (yz)x = (zy)x.$$ ▨

Да видиме сега како се применуваат докажаните тврдења. **7°** ни дозволува, во случај ако постои единица, да вршиме проверка само за оние тројки (a_i, a_j, a_k), за кои a_i, a_j и a_k се различни од единицата. Ако групоидот е комутативен, тогаш според **8°**(ii), равенството (4) е точно за $i = k$, а според **8°**(iii), ако е точно равенството (4), тогаш е точно и равенството:

$$(a_k\, a_j)\, a_i = a_k\, (a_j\, a_i).$$

Да се вратиме на групоидот $\{\top, \bot\}(*)$. Од неговата шема се гледа дека тој е комутативен групоид со единица $\top$. Од ова, според **7°** и **8°** (i), веднаш се добива дека овој групоид е и полугрупа.

Да го разгледаме уште групоидот од примерот 1) а) и да покажеме дека тој е полугрупа. Како што спомнавме и порано, овој групоид е комутативен и има единица e. Кога не би ги користеле тврдењата **7°** и **8°**, би тре-

бало да го провериме равенството (4) за сите можни тројки (такви има 64), а овие две тврдења ни дозволуваат да се задржиме само на следните тројки: (a, a, b), (a, b, b), (a, b, c), (a, c, b), (c, a, b). Ако се искористи шемата на групоидот ќе се добие:

$$a(ab) = b = (aa)b; \quad a(bb) = a = (ab)b;$$
$$a(bc) = e = (ab)c; \quad a(cb) = e = (ac)b; \quad c(ab) = e = (ca)b.$$

Од сето тоа следува дека даденият групоид е полугрупа.

Да напоменеме дека дискусијата би можела да се скрати ако претходно се уочеше дека:

$$x \neq e,\ y \neq e,\ z \neq e,\ x \neq y,\ x \neq z,\ y \neq z \Rightarrow xx = e,\ xy = z. \tag{5}$$

На сосема ист начин се покажува дека и групоидот од 1) б) е полугрупа.

Во овој дел ќе го дефинираме уште поимот за групоид со кратење. Имено, за G велиме дека е *групоид со кратење* акко:

$$xz = yz \vee zx = zy \Rightarrow x = y, \tag{6}$$

т.е.

$$(xz = yz \Rightarrow x = y) \wedge (zx = zy \Rightarrow x = y). \tag{6'}$$

Да видиме како може од шемата на еден групоид да се заклучи дали се работи за групоид со кратење. Прво, да уочиме дека $(a_i a_1, a_i a_2, \ldots, a_i a_n)$ е редицата што одговара на елементот a_i, а $(a_1 a_i, a_2 a_i, \ldots, a_n a_i)$ е колоната што одговара на истиот елемент. Имајќи го ова предвид, од (6′) добиваме дека:

9°. Нека G е определен со својата келиева шема. Тогаш: G е групоид со кратење акко еден ист елемент не се појавува два пати ни во една редица, ни во една колона.

Користејќи го формулираното тврдење, добиваме дека групоидите од 2.1.4) и 1) в) не го задоволуваат условот за кратење, додека во 1) а) и б) имаме групоиди со кратење.

Да го разгледаме случајот кога носителот G на еден групоид $G(\cdot)$ е празното множество. Во тој случај, $G \times G = \varnothing = G$, па, значи, празното пресликување $\varnothing^{(\varnothing)}$ (да се види 1.4.) е единственото пресликување од $G \times G$ во G. Затоа, велиме дека $\varnothing$ е празниот групоид. Ако се има предвид и тоа што (2), (3) и (6) може да се сметаат за точни при $G = \varnothing$[1], добиваме дека:

10°. Празниот групоид е комутативна полугрупа со кратење.

[1]) Условот за комутативност, на пример, може да се претстави во облик: $x, y \in \varnothing \Rightarrow xy = yx$, а тоа е точно, бидејќи претпоставката е невистинита.

ВЕЖБИ. 2. Ако $A = \{1,2\}$, $B = \{a, b, c\}$ да се определат келиевите шеми на групоидите A^A, $S(B)$.

3. Ако е можно, да се пополни секоја од приложените шеми, така што соодветниот групоид да биде: а) комутативен; б) групоид со единица; в) групоид со кратење; г) полугрупа

	a	b
a	a	
b		

;

	a	b	c
a			
b	a	b	c
c			

Ако постојат повеќе решенија, да се најдат сите.

4. Нека a е фиксен елемент од G и нека операцијата $\circ$ е определена на G со: $x \circ y = a$, за секои $x, y \in G$. Добиениот групоид $G(\circ)$ е комутативна полугрупа; $G(\circ)$ има единица акко $G = \{a\}$.

5. Ако во множеството G дефинираме операција $*$ со: $x * y = y$ за секои $x, y \in G$, добиваме полугрупа $G(*)$ во која секој елемент е лева единица; $G(*)$ е комутативна акко G нема повеќе од еден елемент.

6. Нека $G(*)$ е групоид и нека групоидот $G(\circ)$ е определен со: $x \circ y = y * x$ за секои $x, y \in G$; велиме дека $G(\circ)$ е *спротивен групоид* на $G(*)$.

Еден групоид е: а) комутативен; б) полугрупа; в) групоид со единица; г) групоид со кратење, акко соодветната особина ја има нему спротивниот групоид.

7. Ако G е групоид и a фиксен елемент од G, тогаш пресликувањето $\gamma_a : x \to ax$ се вика *лева транслација*, а $\delta_a : x \to xa$ *десна транслација* на G.

(i) $\gamma_a = 1_G \Leftrightarrow a$ е лева единица.

(ii) $\gamma_a = \delta_a = 1_G \Leftrightarrow a$ е единица.

(iii) $(\forall y)\ \gamma_y = \delta_y \Leftrightarrow G$ е комутативен.

(iv) $(\forall x, y)\ \gamma_{xy} = \gamma_x \gamma_y \Leftrightarrow G$ е полугрупа.

(v) $(\forall x)\ \gamma_x$ и δ_x се инјекции $\Leftrightarrow G$ е групоид со кратење.

8. Нека G_1 и G_2 се групоиди и нека на $G = G_1 \times G_2$ е дефинирана операција со: $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2, y_2)$. Добиениот групоид G е: а) комутативен; б) полугрупа; в) групоид со единица; г) групоид со кратење, акко соодветните особини ги имаат и двата групоида G_1, G_2.

9. Нека $G = \{1, -1, i, -i, j, -j, k, -k\}$ и нека за $a = 1, i, j, k$ пишуваме: $-(-a) = a$. Во G е определена операција $*$ со: $1 * x = x * 1 = x$ за секој $x \in G$; $i * j = k$; $j * k = i$; $k * i = j$; $(-x) * y = -(x * y) = x * (-y)$; $x * y = -(y * x)$ за $x, y \neq 1, -1$. Да се определи келиевата шема на $G(*)$ и да се покаже дека $G(*)$ е некомутативна полугрупа со единица.

10. Да се испитаат особините на групоидите $\mathbf{R}(\circ)$, $\mathbf{R}(*)$, $\mathbf{R}(\square)$, каде: $x \circ y = 2xy$, $x * y = \sqrt{x^2 + y^2}$, $x \square y = \sqrt[3]{x^3 + y^3}$.

2.3. СОБИРАЊЕ НА ПРИРОДНИ БРОЕВИ

Природниот број c се вика *збир* на природните броеви a, b акко постојат множества A и B, такви што:

$$A \cap B = \varnothing,\ |A| = a,\ |B| = b,\ |A \cup B| = c. \tag{1}$$

Во тој случај, пишуваме:

$$c = a + b. \tag{1'}$$

Ќе покажеме дека:

1°. $\mathbf{N}(+)$ е комутативна полугрупа со нула 0.

Доказ. Прво, ако a и b се дадени природни броеви, тогаш имаме:

$$|\mathbf{N}_a| = a,\ |\mathbf{N}_b \times \{0\}| = b,\ \mathbf{N}_a \cap (\mathbf{N}_b \times \{0\}) = \emptyset,$$

а според 1. 7. **6°** $\mathbf{N}_a \cup (\mathbf{N}_b \times \{0\})$ е конечно множество, па ако $c = |\mathbf{N}_a \cup (\mathbf{N}_b \times \{0\}|)$, тогаш добиваме $c = a + b$. Да претпоставиме сега дека A и B се произволни конечни множества, такви што:

$$|A| = a,\ |B| = b,\ A \cap B = \emptyset,\ c' = |A \cup B|.$$

Тогаш, според 1. 4. **13°** имаме $A \cup B \sim \mathbf{N}_a \cup (\mathbf{N}_b \times \{0\})$, од што според 1. 7. **5°**, следува $c = c'$.

Со тоа покажавме дека $\mathbf{N}(+)$ е групоид. Ако се има предвид тоа што:

$$A \cup B = B \cup A,\ A \cup (B \cup C) = (A \cup B) \cup C,\ \emptyset \cup A = A$$

за кои било множества A, B, C, добиваме дека $\mathbf{N}(+)$ е комутативна полугрупа и дека 0 е нула на оваа полугрупа.

Ќе докажеме уште неколку својства на собирањето.

2°. Точни се равенствата:

$$x^+ = x + 1,\ (x + y)^+ = x + y^+$$

за секои $x,\ y \in \mathbf{N}$.

Доказ. Првото равенство следува од тоа што $\mathbf{N}_{x^+} = \mathbf{N}_x \cup \{x\}$, $|\mathbf{N}_x| = x$, $|\{x\}| = 1$, $\mathbf{N}_x \cap \{x\} = \emptyset$. Потоа добиваме:

$$(x + y)^+ = (x + y) + 1 = x + (y + 1) = x + y^+.$$

3.° $\mathbf{N}(+)$ е полугрупа со кратење.

Доказ. Треба да покажеме дека

$$x + z = y + z \Rightarrow x = y. \qquad (*)$$

За $z = 0$, $(*)$ има облик: $x = y \Rightarrow x = y$. Да претпоставиме дека $(*)$ е точно за $z = m$ и нека $x + m^+ = y + m^+$. Тогаш, според **2°**, $(x + m)^+ = (y + m)^+$, т. е. $x + m = y + m$, од што, според направената претпоставка, добиваме $x = y$.

Непосредно од дефиницијата на собирањето се добива дека:

4°. $x + y = 0 \Leftrightarrow x = y = 0$.

5.° $x < y \Leftrightarrow (\exists z)\ z \neq 0 \wedge y = x + z$.

Доказ. Нека $x < y$; тогаш имаме $\mathbf{N}_x \subset \mathbf{N}_y$, од што следува $\mathbf{N}_y \setminus \mathbf{N}_x \neq \emptyset$, $\mathbf{N}_y = \mathbf{N}_x \cup (\mathbf{N}_y \setminus \mathbf{N}_x)$ и $\mathbf{N}_x \cap (\mathbf{N}_y \setminus \mathbf{N}_x) = \emptyset$. Според тоа:

$$y = x + z, \text{ каде што } z = |\mathbf{N}_y \setminus \mathbf{N}_x| \neq |\emptyset|.$$

Сега да претпоставиме дека $y = x + z$, каде $z \neq 0$. Не е можно да биде $y = x$, според **4°**. Ако $y < x$, тогаш, според погоре покажаното, би постоел $u \in \mathbf{N}^+$ таков што $x = y + u$, така што би добиле $y = y + (u + z)$ што не е можно. Според тоа, мора да биде $x < y$. ∎

Од **5°** следуваат и следниве тврдења:

6°. $x \leqslant y \Leftrightarrow (\exists z)\ y = x + z$. ∎

7°. Ако $x, y \in \mathbf{N}$, тогаш е исполнет еден и само еден од следниве три услови:

$$(\exists u)\ x = y + u,\ u \neq 0;\quad x = y;\quad (\exists v)\ y = x + v,\ v \neq 0. \blacksquare$$

Да забележиме дека е можно да се дефинира собирањето на $\mathbf{N}$, без да се користи поимот за конечно множество, а имено со:

$$x + 0 = x,\quad x + y^+ = (x + y)^+. \tag{2}$$

Овој пристап би бил и поекономичен, бидејќи, од порано изнесената теорија на природните броеви, доволни би ни биле Пеановите аксиоми. Потоа, собирањето може да се искористи за дефинирање на подредувањето, а, имено, тоа може да се направи со својството **5°**. Сепак, ние избравме инаков пат, бидејќи сметаме дека тој е "поприроден".

ВЕЖБИ. **2.** Нека f е дадено пресликување од $\mathbf{N}$ во $\mathbf{N}$, а $\circ$ дадена операција на $\mathbf{N}$. Постои една и само една операција $*$ на $\mathbf{N}$ што ги задоволува равенствата:

$$\begin{aligned} x * 0 &= f(x) \\ x * y^+ &= (x * y) \circ x \end{aligned} \tag{3}$$

за секои $x, y \in \mathbf{N}$.

3. Ако во (3) ставиме $f(x) = x$ и $x \circ y = x^+$, се добива дека $*$ е операцијата собирање.

4. Земајќи ги равенствата (2) како дефинирачки за собирањето, да се докажат својствата **1°**, **3°** и **4°**. Потоа, земајќи го **5°** како дефиниција на $<$, да се покаже дека $<$ е нерефлексивна и транзитивна релација, како и својствата **1.6.8°**, **10°**: (i), (iii), (iv).

5. Дефинирајќи ја низата множества $(\mathbf{N}_x \mid x \in \mathbf{N})$ со **1.6.10°** (v), да се докаже тврдењето **1.6.7°**.

6. Да се определат множествата: $\{x \mid x + x = x\}$, $\{x \mid x + 1 = x\}$, $\{(x, y) \mid x + y = 3\}$.

7. Ако M и N се конечни множества, тогаш: $|M \cup N| + |M \cap N| = |M| + |N|$.

8. Ако $x, y, z, u \in \mathbf{N}$, тогаш:
(i) $x < y \Leftrightarrow x + z < y + z$; (ii) $x < y,\ z < u \Rightarrow x + z < y + u$.

2.4. СЛОЖЕНИ ПРОИЗВОДИ. СТЕПЕНИ

Нека (a, b, c, d) е четиричлена низа елементи од групоидот $G(*)$. Применувајќи ја операцијата на групоидот три пати на членовите од дадената низа, можеме да ги формираме следниве производи:

$$((a * b) * c) * d; \quad (a * (b * c)) * d; \quad (a * b) * (c * d);$$

$$a * ((b * c) * d); \quad a * (b * (c * d)).$$

Уочуваме дека овие пет производи се разликуваат само во распоредот на заградите, а сите тие имаат иста низа фактори. Во иста смисла, од низата (a, b, c) можат да се формираат два производа: $a * (b * c)$ и $(a * b) * c$, а од низата (a, b) само еден: $a * b$.

Со цел да го дефинираме поимот за производ попрецизно, прво ќе го воведеме поимот за форма на производ.

За една двојка загради од облик ( ) велиме дека е *елементарна форма*, односно *форма со должина* 1. Потоа, ако Π' е форма со должина m, а Π'' форма со должина n, тогаш за $(\Pi'\ \Pi'')$ велиме дека е *форма со должина* $m + n$.

Според тоа, постои една форма со должина 2: (( ) ( )); две форми со должина 3: ((( ) ( )) ( )), (( ) (( ) ( ))) и пет форми со должина 4: ((( ) ( )) ( )) ( )), ((( ) (( ) ( ))) ( )), ((( ) ( )) (( ) ( ))), (( ) (( ) (( ) ( )))), (( ) ((( ) ( )) ( ))).

Ако должината на формата Π е поголема од 1, тогаш најлевата загради (и најдесната) не ги пишуваме, т. е. наместо $(\Pi'\ \Pi'')$ пишуваме $\Pi'\ \Pi''$. Така, ( ) ( ) е формата со должина 2; (( ) ( )) ( ), ( ) (( ) ( )) се формите со должина 3.

Да се вратиме на случајот кога $G(*)$ е даден групоид. Секоја форма Π со должина n ја интерпретираме како пресликување од G^n [1] во G. Тоа го правиме на следниот начин.

Ако $\Pi = (\ )$ е елементарната форма, тогаш ѝ го придружуваме единичното пресликување 1_G, т.е.:

$$(\ )(x) = x \tag{1}$$

за секој $x \in G$. Да претпоставиме дека $\Pi = \Pi'\ \Pi''$, каде што Π' има должина m, а Π'' должина n и дека се определени пресликувањата:

$$\Pi' : (x_1, \ldots, x_m) \to \Pi'(x_1, \ldots, x_m)$$

$$\Pi'' : (x_1, \ldots, x_n) \to \Pi''(x_1, \ldots, x_n)$$

Тогаш, $\Pi(x_1, \ldots, x_{m+n})$ се дефинира со:

$$\Pi(x_1, \ldots, x_{m+n}) = \Pi'(x_1, \ldots, x_m) * \Pi''(x_{m+1}, \ldots, x_{m+n}) \tag{2}$$

[1] Секое такво пресликување се вика *n-арна операција* на G.

Според тоа, ако П е ( ) ( ), тогаш

$$\Pi(x, y) = x * y, \tag{2'}$$

т.е. на ( ) ( ) и се придружува операцијата $*$ што го определува групоидот.

Ако П е форма со должина n, а $(x_1, \ldots, x_n)$ низа променливи елементи во G, тогаш велиме дека $\Pi(x_1, \ldots, x_n)$ е *производ со должина n*.

Ако $G(*)$ е полугрупа, тогаш двата производа $\Pi'(x, y, z) = x*(y*z)$, $\Pi''(x, y, z) = (x*y)*z$ се еднакви. Ќе покажеме дека кај полугрупите важи и поопшто својство, познато како *општ асоцијативен закон*.

1°. Нека $G(*)$ е полугрупа. Ако Π' и Π'' се две форми со иста должина n, тогаш

$$\Pi'(x_1, \ldots, x_n) = \Pi''(x_1, \ldots, x_n) \tag{3}$$

за секои $x_1, x_2, \ldots, x_n \in G$.

Доказ. Определуваме прво еден специјален вид форми $\Pi^{(n)}$ со:

$$\Pi^{(n)} = \begin{cases} (\ ) \text{ за } n = 1 \\ \Pi^{(n-1)} \ (\ ) \text{ за } n > 1 . \end{cases} \tag{4}$$

Според тоа:

$$\Pi^{(n)}(x_1, \ldots, x_n) = \Pi^{(n-1)}(x_1, \ldots, x_{n-1}) * x_n \tag{4'}$$

за $n > 1$.

За да покажеме дека е точно равенството (3), доволно е да покажеме дека:

$$\Pi(x_1, \ldots, x_n) = \Pi^{(n)}(x_1, \ldots, x_n) \tag{3'}$$

за секоја форма П со должина n.

Доказот ќе го спроведеме со индукција по n. За $n = 1$ и $n = 2$, (3') следува од тоа што постои само една форма со должина 1 и само една, со должина 2. Да претпоставиме дека $m > 2$ и дека (3') е точно за сите форми П што имаат должина $n < m$.

Нека П има должина m; тогаш П е $\Pi_1 \Pi_2$ каде Π_1 има должина r, а Π_2 должина s; при тоа $r + s = m$, па, значи, $r > 1$ или $s > 1$, бидејќи $m > 2$. Од индуктивната претпоставка следува:

$$\begin{aligned} \Pi(x_1, \ldots, x_m) &= \Pi_1(x_1, \ldots, x_r) * \Pi_2(x_{r+1}, \ldots, x_m) \\ &= \Pi^{(r)}(x_1, \ldots, x_r) * \Pi^{(s)}(x_{r+1}, \ldots, x_m). \end{aligned} \tag{3''}$$

Ако $s = 1$, тогаш десната страна на (3'') е, според (4'), $\Pi^{(m)}(x_1, \ldots, x_m)$. Ако $s > 1$, тогаш десната страна од (3'') е:

$$\Pi^{(r)}(x_1, \ldots, x_r) * [\Pi^{(s-1)}(x_{r+1}, \ldots, x_{m-1}) * x_m],$$

па, ако се искористи тоа што е $G(*)$ полугрупа, се добива:

$$[\Pi^{(r)}(x_1, \ldots, x_r) * \Pi^{(s-1)}(x_{r+1}, \ldots, x_{m-1})] * x_m =$$
$$\Pi^{(m-1)}(x_1, \ldots, x_{m-1}) * x_m = \Pi^{(m)}(x_1, \ldots, x_m).$$

Со тоа доказот е комплетиран.■

Поради резултатот на тукушто докажаното својство, производот $\Pi(x_1, \ldots, x_n)$ ќе го претставуваме во облик $x_1 * x_2 * \ldots * x_n$, односно: $x_1 x_2 \ldots x_n$, ако не го пишуваме знакот на операцијата, т.е. ако употребуваме мултипликативна ознака. Значи, кај полугрупи не е неопходна употребата на загради, при производи со повеќе фактори. Ако се работи за комутативна полугрупа, ќе покажеме дека тогаш не е битен ни распоредот на факторите.

2°. Нека $G(*)$ е комутативна полугрупа, $n \in \mathbf{N}^+$ и $f: \nu \to i_\nu$ пермутација на множеството $\mathbf{N}_n^+ = \{1, \ldots, n\}$. Тогаш:

$$x_1 * x_2 * \ldots * x_n = x_{i1} * x_{i2} * \ldots * x_{in} \tag{5}$$

за секоја низа елементи $x_1, \ldots, x_n$ од G.

Доказ. За $n = 1$, (5) се сведува на: $x_1 = x_1$. Да претпоставиме точност на (5) за секој $n < m$, и да го разгледаме производот $x_{i1} * \ldots * x_{im}$;

Нека $i_k = m$; ако $k = m$, тогаш:

$$x_{i1} * \ldots * x_{im} = (x_{i1} * \ldots * x_{im-1}) * x_m = x_1 * x_2 * \ldots * x_{m-1} * x_m,$$

според индуктивната претпоставка; ако $k < m$, тогаш со едноподруга примена на **1°** и комутативноста на $*$, добиваме:

$$x_{i1} * \ldots * x_m * \ldots * x_{im} = x_{i1} * \ldots * x_{ik-1} * \ldots * x_{im} * x_m = x_1 * \ldots * x_m.$$■

Да спомнеме дека, во случај на адитивно означена комутативна полугрупа $G(+)$, се пишува и:

$$x_1 + \ldots + x_n = \sum_1^n x_i. \tag{6}$$

Во секоја полугрупа со единица може да се дефинира поимот *степен со природни експоненти*. Имено, ако G е (мултипликативно означена) полугрупа со единица e, тогаш се дефинира пресликување $(n, x) \to x^n$ од $\mathbf{N} \times G$ во G со:

$$n \geqslant 1 \Rightarrow x^n = \underbrace{x\, x \ldots x}_{n};\ x^0 = e. \tag{7}$$

Велиме дека x е *основа*, а n *експонент* (или показател) на степенот x^n.

Да покажеме дека поголемиот дел од добро познатите својства на степени се точни кај секоја полугрупа со единица.

3°. Ако $x \in G$, $m, n \in \mathbf{N}$, тогаш:

$$\text{(i) } x^1 = x; \quad \text{(ii) } x^m * x^n = x^{m+n}.$$

Доказ. (i) Ова е специјален случај од (7) за $n = 1$.

(ii) За $m = 0 \vee n = 0$, равенството е последица на (1) и фактот дека e е единица на G. Ако $m, n \in \mathbf{N}^+$, равенството е последица од (7) и **1°**. ∎

4°. Ако полугрупата G е комутативна, тогаш:

$$(x\,y)^n = x^n\,y^n \tag{*}$$

за секои $x, y \in G$ и $n \in \mathbf{N}$.

Доказ. Ова тврдење е последαца од **2°** и (7). ∎

Да забележиме дека равенството (*) не мора да важи ако G не е комутативна. Таков е случајот, на пример, кај полугрупата $S(M)$, ако $M=\{a, b, c\}$ се состои од три елементи. Имено, ако $f = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$, $g = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$, тогаш:

$$f^2 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = 1_M = g^2, \quad fg = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad (fg)^2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \neq 1_M,$$

од што следува: $(fg)^2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \neq 1_M = f^2 g^2$.

Ќе докажеме овде уште две тврдења во врска со собирањето на природни броеви.

5°. Ако $M_1, M_2, \ldots, M_n$ се конечни множества две по две дисјунктни, т.е. $M_i \cap M_j = \varnothing$ за $i \neq j$, тогаш:

$$|M_1 \cup M_2 \cup \ldots \cup M_n| = |M_1| + |M_2| + \ldots + |M_n|. \tag{8}$$

Доказ. За $n = 1$, во (8) имаме $|M_1| = |M_1|$, а за $n = 2$, (8) е последица од дефиницијата на собирањето. Да претпоставиме дека (8) е точно за $n = k$. За $n = k + 1$, добиваме:

$$\begin{aligned} |M_1 \cup \ldots \cup M_n| &= |(M_1 \cup \ldots \cup M_k) \cup M_{k+1}| = |M_1 \cup \ldots \cup M_k| + |M_{k+1}| \\ &= |M_1| + \ldots + |M_k| + |M_{k+1}| \\ &= |M_1| + \ldots + |M_n|. \end{aligned}$$

∎

6°. За секој природен број x, $x \neq 0$, точно е равенството:

$$x = \underbrace{1 + 1 + \ldots + 1}_{x}. \tag{9}$$

Доказ. Од **5°** следува:

$$x = |\mathbf{N}_x^+| = |\{1\} \cup \ldots \cup \{x\}| = |\{1\}| + \ldots + |\{x\}| = \underbrace{1 + 1 + \ldots + 1}_{x}.$$ ■

ВЕЖБИ: 2. Да се определат сите форми со должина пет.

3. Нека $G = S(A)$, каде што $A = \{1, 2\}$. Да се определат сите можни степени на елементите од G.

4. Исто како и во претходната вежба за групоидите од вежбите 2.2. **4, 5.**

5. Ако A, B и C се три конечни множества, тогаш: $|A| + |B| + |C| + |A \cap B \cap C| = |A \cup B \cup C| + |A \cap B| + |A \cap C| + |B \cap C|$.

2.5. МНОЖЕЊЕ НА ПРИРОДНИ БРОЕВИ

Во претходниот дел го дефинираме поимот степен, за секоја мултипликативно означена полугрупа со единица. Во случај на комутативна полугрупа $G(+)$ со нула o, наместо x^n, ќе пишуваме nx. Во овој случај 2.4.(7) го добива следниов облик:

$$0x = o, \quad nx = \underbrace{x + x + \ldots + x}_{n}, \quad n \geqslant 1. \tag{1}$$

(При тоа, во равенството $0x = o$, 0 е природниот број нула, а o нулата на полугрупата $G(+)$; натаму нема да употребуваме различни ознаки.)

Од својствата 2.4. **3°** и **4°** следува дека:

1°. Ако $G(+)$ е адитивно означена полугрупа со нула 0, тогаш:

(i) $n0 = 0x = 0$; (ii) $1x = x$;

(iii) $mx + nx = (m + n)x$; (iv) $n(x + y) = nx + ny$, за секои $x, y \in G$, $m, n \in \mathbf{N}$. ■

Имајќи го предвид тоа што $\mathbf{N}(+)$ е комутативна полугрупа со нула 0, заклучуваме дека со (1) е определено пресликување од $\mathbf{N} \times \mathbf{N}$ во $\mathbf{N}$, т.е. операција на $\mathbf{N}$. За оваа операција велиме дека е *множење* на природни броеви.

Ако во **1°** улогата на $G(+)$ ја преземе полугрупата $\mathbf{N}(+)$, добиваме неколку својства на операцијата множење на природни броеви, а имено:

1.′ За секои $x, y, z \in \mathbf{N}$ се точни равенствата:

(i) $x0 = 0x = 0$; (ii) $1x = x1 = x$;

(iii) $xz + yz = (x + y)z$; (iv) $x(y + z) = xy + xz$.

Равенството $x1 = x$ следува од (1) и 2.4. **6°**). ■

Пред да докажеме уште неколку својства на множењето, ќе го докажеме својството за "степенување на степен".

2°. Ако G е мултипликативно означена полугрупа со единица e, тогаш

$$(x^m)^n = x^{mn} \tag{2}$$

за секои $x \in G$, $m, n \in \mathbf{N}$.

Доказ. Вршиме индукција по n. За $n = 0$ и двете страни се e; претпоставуваме точност за $n = k$; за $n = k + 1$, добиваме:

$$(x^m)^n = (x^m)^{k+1} = (x^m)^k \cdot (x^m)^1 = x^{mk} \cdot x^m$$
$$= x^{mk+m} = x^{mn}.\blacksquare$$

Ако е $G(+)$ адитивно означена полугрупа, тогаш (2) го добива следниов облик:

$$n(mx) = (nm)x \tag{2'}$$

Сега ќе покажеме дека:

3°. $\mathbf{N}(\cdot)$ е комутативна полугрупа со единица 1.

Доказ. 1 е единица, според **1'** (ii). Асоцијативноста следува од (2'), ако при тоа $G(+)$ се замени со $\mathbf{N}(+)$. Потоа, според **1'** (i), имаме $x0 = 0x$; нека $xk = kx$; имајќи ги предвид **1'** (iii), (iv), добиваме:

$$xk^+ = x(k + 1) = xk + x = kx + 1 \cdot x = (k + 1)\ x = k^+ x.\blacksquare$$

Значи, на $\mathbf{N}$ имаме, изградено две полугрупи $\mathbf{N}(+)$ и $\mathbf{N}(\cdot)$. Првата ќе ја викаме *адитивна*, а втората — *мултипликативна полугрупа* на природните броеви.

Имајќи го предвид тоа што $\mathbf{N}(\cdot)$ е комутативна полугрупа со единица, добиваме дека е осмислен поимот за степен x^y каде што $x, y \in \mathbf{N}$. Притоа, точни се својствата **2°** и 2.4. **4°**, со тоа што G се заменува со $\mathbf{N}(\cdot)$. Да забележиме и дека:

4°. $0^0 = 1$, $0^x = 0$ за $x \neq 0$.

Ќе докажеме уште две тврдења.

5°. $xy = 0 \Leftrightarrow x = 0 \vee y = 0$.

Доказ. Ако $y \neq 0$, тогаш $y = u + 1$, каде што u е претходникот на y, така што добиваме:

$xy = 0 \Leftrightarrow xu + x = 0 \Leftrightarrow xu = x = 0$. (Овде е користено својството 2.3. **4°**.)

6°. $x \neq 0 \Rightarrow (xy = xz \Leftrightarrow y = z)$.

Доказ. Нека $x \neq 0$ и $xy = xz$. Според 2.3. **7°**, постои $u \in \mathbf{N}$, таков што $y = z + u \vee z = y + u$; нека $z = y + u$; тогаш: $xy = xy + xu$, т.е. $xu = 0$, односно $u = 0$.

Пред да докажеме неколку тврдења во врска со конечните множества, ќе дефинираме пресликување од **N** во **N**, $x \to x!$ со:

$$0! = 1,\ x! = 1 \cdot 2 \cdot \ldots \cdot x \text{ за } x \neq 0. \tag{3}$$

7°. Ако M и N се конечни множества, тогаш:

(i) $|M \times N| = |M| \cdot |N|$; (ii) $|M^N| = |M|^{|N|}$;

(iii) $|B(M)| = 2^{|M|}$; (iv) $|S(M)| = |M|!$.

Доказ. Нека $M = \{a_1, \ldots, a_m\}$, $N = \{b_1, \ldots, b_n\}$, $|M| = m$, $|N| = n$. Сметајќи дека спомнатите својства се очигледно точни за $M = \varnothing$ или $N = \varnothing$, ќе претпоставуваме дека $m \neq 0$, $n \neq 0$.

(i) Ако се има предвид тоа што $M \times N = \{a_1\} \times N \cup \ldots \cup \{a_m\} \times N$, $\{a_i\} \times N \cap \{a_j\} \times N = \varnothing$ за $i \neq j$ и $|\{a_i\} \times N| = |N| = n$, според 2.4. **5°** добиваме:

$$|M \times N| = \underbrace{n + n + \ldots + n}_{m} = mn = |M| \cdot |N|.$$

(ii) За $n = 1$, имаме $|M^N| = |M| = |M|^{|N|}$. Да претпоставиме точност за $n = k$ и да го разгледаме случајот $n = k + 1$, т.е. $N = \{b_1, \ldots, b_k, b\} = N' \cup \{b\}$ каде што $N' = \{b_1, \ldots, b_k\}$, $b \notin N'$. Тогаш имаме: $M^N \sim M^{N'} \times M^{\{b\}}$ (овде е користено својството 1.4. **14°**), така што, според (i) добиваме:

$$|M^N| = |M^{N'}| \cdot |M^{\{b\}}| = m^k \cdot m = m^{k+1} = |M|^{|N|}.$$

(iii) Да претпоставиме точност за $m = k$ и да го разгледаме случајот кога $M = M' \cup \{a\}$, каде што $M' = \{a_1, \ldots, a_k\}$, $a \notin M'$. Тогаш, ако ставиме $\mathcal{G} = B(M) \setminus B(M')$, добиваме дека $B(M) = B(M') \cup \mathcal{G}$, каде $\mathcal{G}$ се состои од оние подмножества A на M, во кои се содржи a. Јасно е дека: $A \to A \setminus \{a\}$ е биекција од $\mathcal{G}$ во $B(M')$ и дека $\mathcal{G} \cap B(M') = \varnothing$. Имајќи го сето тоа предвид, добиваме:

$$|B(M)| = |B(M')| + |\mathcal{G}| = |B(M')| + |B(M')|$$
$$= 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} = 2^{|M|}.$$

(iv) За поедноставно работење ќе претпоставиме дека $M = \{1, 2, \ldots, k, k+1\}$. Потоа, $S(M)$ ќе го претставиме во облик $A_1 \cup A_2 \cup \ldots \cup A_{k+1}$, каде што

$$f \in A_i \Leftrightarrow f \in S(M),\ f(i) = k + 1.$$

Да покажеме дека $A_i \sim S(\mathbf{N}_k^+)$. Нека $f \in A_i$ каде што $i \leqslant k$; го определуваме $f' \in S(\mathbf{N}_k^+)$ со: $f'(j) = f(j)$ за $j \neq i$, $f'(i) = f(k+1)$; јасно е дека $f \to f'$ е биекција од A_i во $S(\mathbf{N}_k^+)$. Ако $f \in A_{k+1}$, тогаш $f' \in S(\mathbf{N}_k^+)$ се определува со $f'(j) = f(j)$ за $j \neq k + 1$. Сега добиваме:

$$|S(M)| = |A_1| + \ldots + |A_{k+1}| = \underbrace{k! + \ldots + k!}_{k+1} = (k+1)\,k! =$$

$$= (k+1)! = |M|!. \quad \blacksquare$$

Со $\binom{n}{k}$ ќе го означуваме бројот од подмножествата на $\mathbf{N}_n$ со по k елементи. Според тоа, имаме:

8°. (i) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$, за секој $n \in \mathbf{N}$.

(ii) $n < k \Rightarrow \binom{n}{k} = 0$. $\blacksquare$

Ќе покажеме уште дека:

9°. $k, n \in \mathbf{N} \Rightarrow \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

Доказ. За $n \leqslant k$ точноста следува од **8°**. Затоа ќе претпоставиме дека $k < n$. Ако $A = \{a_1, a_2, \ldots, a_{k+1}\}$ е подмножество на $\mathbf{N}_{n+1}$, $|A| = k+1$, тогаш имаме $n \notin A$ или $n \in A$. Ако првото е точно, тогаш $A \in B(\mathbf{N}_n)$, така што постојат $\binom{n}{k+1}$ множества од тој облик; ако $n \in A$, ставајќи $A' = A \setminus \{n\}$, добиваме пак $A' \in B(\mathbf{N}_n)$, но сега $|A'| = k$; според тоа, постојат $\binom{n}{k}$ множества од вториот облик. На читателот, веројатно, нема да му биде многу тешко да го комплетира доказот. $\blacksquare$

На крајот, да направиме две забелешки во врска со дефиницијата на операцијата множење. Прво, множењето би можело да се дефинира и директно, а не преку собирањето, со тоа што за дефиниција би се прифатило својството **7°** (i). Друг начин да се дефинира множењето со помош на собирањето е следниов:

$$x \cdot 0 = 0, \quad x \cdot y^+ = x \cdot y + x. \tag{4}$$

На читателот му се препорачува да се обиде да докаже некои од својствата на множењето, ако тоа се дефинира со помош на некој од овде спомнатите два нови начини.

ВЕЖБИ. **2.** Ако $*$ е операцијата степенување, т.е. ако за секои $x, y \in \mathbf{N}$ ставиме $x * y = x^y$, тогаш $\mathbf{N}(*)$ е групоид со десна единица 1, но не е комутативен, ниту полугрупа и нема единица.

3. Ако $x, y, z \in \mathbf{N}$, тогаш: (i) $xy = 1 \Leftrightarrow x = y = 1$; (ii) $x^y = 0 \Leftrightarrow x = 0,\ y \neq 0$; (iii) $x^y = 1 \Leftrightarrow x = 1 \vee y = 0$; (iv) $x \neq 0,1 \Rightarrow (x^y = x^z \Leftrightarrow y = z)$; (v) $x \neq 0 \Rightarrow (y < z \Leftrightarrow xy < xz)$; (vi) $y \leqslant z,\ u \leqslant v \Rightarrow yu \leqslant zv$; (vii) $z \neq 0 \Rightarrow (x^z = y^z \Leftrightarrow x = y)$.

4. Ако операцијата $\circ$ се дефинира на $\mathbf{N}$ со: $x \circ y = \binom{x}{y}$, тогаш добиваме групоид $\mathbf{N}(\circ)$. Дали овој групоид: а) има (лева, десна) единица, б) е комутативен, в) е полугрупа?

5. Ако $x, y \in \mathbf{N}$, тогаш $\binom{x+y}{x} = \binom{x+y}{y}$.

6. Ако a е фиксен елемент од $\mathbf{N}$ и ако операцијата $\square$ е дефинирана со $x \square y = axy$, тогаш е точно равенството:

$$(x+y) \square (u+v) = (x \square u) + (x \square v) + (y \square u) + (y \square v), \qquad (*)$$

за секои $x, y, u, v \in \mathbf{N}$. И обратно, ако е точен "идентитетот" $(*)$, тогаш постои $a \in \mathbf{N}$, таков што $x \square y = axy$.

7. Да го формираме "триаголникот" наречен *Паскалов триаголник*, како на приложената шема. Да се уочи правилото по кое е формиран овој триаголник и да се покаже дека k-тиот член на n-тата низа е $\binom{n}{k}$.

```
     1
   1   1
 1   2   1
1   3   3   1
1   4   6   4   1
```

Користејќи го Паскаловиот триаголник да се пресметаат $\binom{7}{4}$, $\binom{8}{3}$.

8. Ако $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{a, b, c, d\}$, $D = \{1, 2, b, c, d\}$ да се определи бројот на:

а) инјекциите од A во B и од A во D.

б) сурјекциите од A во B и од A во D.

в) биекциите од A во B и од A во C.

9. Да се решат p-ките:
а) $2x = 3$; б) $2x = 6$; б) $xy = 6$; г) $x^y = 6$; д) $x^y = 16$.

10. Ако $x \in \mathbf{N}_+$, тогаш $2^x = \binom{x}{0} + \binom{x}{1} + \ldots + \binom{x}{x}$.

2.6. ИНВЕРЗНИ ОПЕРАЦИИ

Прво ќе го дефинираме поимот делумна операција. Нека $D \subseteq G \times G$. Секое пресликување $* : (x, y) \to x * y$ од D во G се вика *делумна операција* на G. Во тој случај велиме дека $G(*)$ е *делумен групоид* со домен D. Од ова следува дека:

1°. $G(*)$ е групоид акко $G(*)$ е делумен прупоид со домен $G \times G$.

Ако $G(*)$ е делумен групоид, тогаш, при $a, b, c \in G$ ќе сметаме дека исказот $a * b = c$ е точен акко (a, b) припаѓа на доменот од G и притоа $* : (a, b) \to c$. Во тој случај ќе велиме и дека $a * b$ постои во G, и пишуваме $a * b \in G$.

Сега да претпоставиме дека $G(+)$ е адитивно означен комутативен групоид со кратење и да ставиме:

$$x - y = z \Leftrightarrow x = z + y. \qquad (1)$$

Ако е (1) точно, тогаш велиме дека z е *разлика* на x со y.

Од (1) се добива дека:

$$(z + y) - y = z \tag{2}$$

за секои $y, z \in G$. Потоа, ако $x - y = z_1$ и $x - y = z_2$, добиваме $z_1 + y = x = z_2 + y$, од што следува $z_1 = z_2$.

Со тоа го докажавме следново тврдење:

2°. Ако $G(+)$ е комутативен групоид со кратење, тогаш со (1) е определен делумен групоид $G(-)$. Притоа, точно е равенството (2), за секои $y, z \in G$.

Делумниот групоид $G(-)$ се вика *инверзен на* $G(+)$, а во иста смисла — е *инверзна операција* на $+$, која се вика одземање. (Да забележиме дека условот за комутативност не е користен.).

Да го разгледаме случајот кога $G(+)$ е и полугрупа.

3°. Нека $G(+)$ е комутативна полугрупа со кратење.

(i) Точни се следниве равенства:

$$x + (y - z) = (x + y) - z, \tag{3}$$

$$x - (z - y) = (x + y) - z, \tag{4}$$

$$x - (y + z) = (x - y) - z, \tag{5}$$

$$(x - y) + (u - v) = (x + u) - (y + v), \tag{6}$$

во таа смисла што од егзистенцијата на левата страна на некое од тие равенства следува егзистенцијата и на десната страна, како и еднаквост на двете страни.

(ii) Ако $x - y,\ u - v \in G$, тогаш:

$$x - y = u - v \Leftrightarrow x + v = u + y. \tag{7}$$

(iii) Ако $x - y \in G$, тогаш:

$$(x + z) - (y + z) = x - y \tag{8}$$

за секој $z \in G$.

(iv) Ако G има нула 0, тогаш:

$$x - x = 0,\quad x - 0 = x. \tag{9}$$

Доказ. (i) Нека $x + (y - z) = m \in G$, тогаш: $y - z = k \in G$, т.е. $y = k + z$; од тоа следува: $x + y = x + (k + z) = (x + k) + z$, т.е. $(x + y) - z = x + k = m$. Според тоа, точно е равенството (3). Слично се докажуваат и другите равенства.

(ii) Нека $x - y = u - v = m$, т.е. $x = m + y,\ u = v + m$.

Тогаш: $x + v = (m + y) + v = (v + m) + y = u + y$. Обратно, од $x + v = u + y$, следува: $(x - y) + v = (x + v) - y = (u + y) - y = u$, а потоа и $x - y = u - v$.

(iii) е директна последица од (1) и асоцијативноста, а јасно е и дека равенствата (9) се последици од (2).■

Во случај на мултипликативно означен групоид, инверзната операција се вика *делење* и се означува со /. Според тоа:

$$x/y = z \Leftrightarrow x = zy. \tag{1'}$$

Во смисла на оваа ознака, имаме:

$$(zy) / y = z; \tag{2'}$$

$$x \cdot (y / z) = (x \cdot y) / z; \tag{3'}$$

$$x / (z / y) = (x \cdot y) / z; \tag{4'}$$

$$x / (y \cdot z) = (x / y) / z; \tag{5'}$$

$$(x / y) \cdot (u / v) = (xu) / (yv); \tag{6'}$$

$$x / y = u/v \Leftrightarrow xv = uy; \tag{7'}$$

$$(xz) / (yz) = x / y; \tag{8'}$$

$$x / x = e, \quad x/e = x. \tag{9'}$$

Притоа, во (9′) се претпоставува дека e е единица во $G(\cdot)$.

Според 2.3. **1°**, **3°**, $\mathbf{N}(+)$ е комутативна полугрупа со кратење, од што следува дека се точни тврдењата **2°** и **3°**. Потоа, ако се имаат предвид и својствата 2.3. **5°**, **6°** и **7°**, се добива и следново својство.

4°. Ако $x, y \in \mathbf{N}$, тогаш:

(i) $x - y \in \mathbf{N} \Leftrightarrow y \leqslant x$;

(ii) $x - y \in \mathbf{N}^+ \Leftrightarrow y < x$;

(iii) $x - y \in \mathbf{N} \vee y - x \in \mathbf{N}$.■

Следните две тврдења укажуваат на соодветни врски меѓу одземањето и множењето на природни броеви.

5°. Множењето е дистрибутивно спрема одземањето, т.е. ако $y - z \in \mathbf{N}$, тогаш $xy - xz \in \mathbf{N}$ и притоа:

$$x(y - z) = xy - xz.$$

Доказ. Ако $y - z = k$, тогаш: $y = k + z$, $xy = xk + xz$,

од што следува: $x(y - z) = xk = xy - xz$.■

6°. Ако $x - y$, $u - v \in \mathbf{N}$, тогаш:

$$(x - y)(u - v) = (xu + yv) - (xv + yu)$$

Доказ. Ги користиме 3° и 5°.

$$\begin{aligned}(x - y)\,(u - v) &= (x - y)\,u - (x - y)\,v \\ &= (xu - yu) - (xv - yv) \\ &= [(xu - yu) + yv] - xv \\ &= [(xu + yv) - yu] - xv \\ &= (xu + yv) - (xv + yu).\end{aligned}$$

Имајќи го предвид тоа што $\mathbf{N}^+$ $(\cdot)$ е комутативна полугрупа со кратење и единица 1, добиваме дека делењето е делумна операција на $\mathbf{N}^+$, т.е. $\mathbf{N}^+(/)$ е делумен групоид. Притоа точни се тврдењата (1′) — (9′), при што во (9′) треба да се стави 1 наместо e.

Да докажеме уште едно тврдење.

7°. (i) $x/z,\ y/z \in \mathbf{N}^+ \Rightarrow x/z + y/z = (x + y)/z;$ (10)

(ii) $x/y,\ u/v \in \mathbf{N}^+ \Rightarrow x/y + u/v = (xv + uy)/(yv).$ (11)

Доказ. (i) Ако $x/z = m$, $y/z = n$, тогаш $x = mz$, $y = nz$, т.е. $x + y = (m + n)\,z$, од што следува (10).

(ii) Со помош на (8′) и (10), добиваме:

$$x/y + u/v = (xv)/(yv) + (uy)/yv) = (xv + uy)/(yv).$$

Операцијата делење може да се прошири на $\mathbf{N}$ на следниов начин:

$$\begin{gathered}x/y = z \text{ во } \mathbf{N}^+ \Rightarrow x/y = z \text{ во } \mathbf{N} \\ 0/y = 0 \text{ за секој } y \in \mathbf{N}^+.\end{gathered} \tag{12}$$

Лесно се проверува дека сите порано спомнати својства на делењето ќе бидат точни и при ова проширување, со тоа што треба да се претпостави дека сите "именители" што фигурираат во својствата се различни од нула.

ВЕЖБИ: **2.** Ако K и L се конечни множества, тогаш:

(i) $K \subseteq L \Rightarrow |\,L \setminus K\,| = |\,L\,| - |\,K\,|$;

(ii) $|\,K \cup L\,| = |\,K\,| + |\,L\,| - |\,K \cap L\,|$.

3. Нека K и L се конечни множества, такви што $K \subseteq L$. Да се определи бројот на подмножествата на L што имаат m заеднички елементи со K, каде што $m \leqslant |\,K\,|$.

4. Да се определи бројот на пресликувањата f од $\mathbf{N}_m$ во $\mathbf{N}_n$, такви што:
а) $f(\mathbf{N}_p) \subseteq \mathbf{N}_q$; б) $f(\mathbf{N}_p) \cap \mathbf{N}_q = \varnothing$. $(p \leqslant m,\ q < n)$.

5. Ако $x, y, z \in \mathbf{N}$, $x \neq 0$, $z \leqslant y$, тогаш: $x^y/x^z = x^{y-z}$.

6. Ако $x, y \in \mathbf{N}$, тогаш:

(i) $\binom{x+y}{y} = (x + y)!/(y!\,x!)$;

(ii) Бројот на сите инјекции од $\mathbf{N}_y$ во $\mathbf{N}_{x+y}$ е $(x+y)!/y!$.

7. За групоидот $G(\circ)$ велиме дека е *слабо проширување* на делумниот групоид $G(*)$ акко: $x \circ y = z$ во $G(\circ) \Rightarrow x * y = z$ во $G(*)$. За секој делумен групоид постои слабо проширување.

8. Да се определат неколку слаби проширувања на делумните групоиди определени со шемите:

а)
	a	b	c
a	b	a	a
b	c	a	
c	b	b	

б)
	a	b
a		a
b		

в)
	a	b	c	d
a	a	b	a	b
b		b	c	a
c			c	b
d				a.

9. Да се определи едно слабо проширување на:

а) $\mathbf{N}(-)$; б) $\mathbf{N}(/)$.

2.7. ГРУПИ

Нека G е полугрупа со единица e. Ако $a, b \in G$ и $ab = e$, тогаш велиме дека a е *лева инверзија* на b, а b е *десна инверзија* за a.

Да претпоставиме дека a' е лева, а a'' десна инверзија за ист елемент a. Тогаш имаме:

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

Точно е, значи, следново тврдење:

1°. Ако елементот a од полугрупата G со единица има и лева инверзија a' и десна инверзија a'', тогаш $a' = a''$.

Во овој случај елементот $a' = a''$ го означуваме со a^{-1} и го нарекуваме *инверзија* на a, а за a велиме дека е *инверзибилен елемент* во G. Според тоа, имаме:

$$aa^{-1} = a^{-1}a = e, \tag{1}$$

а од ова непосредно следува дека:

2°. Ако a е инверзибилен елемент во G, тогаш и a^{-1} е инверзибилен во G и притоа имаме:

$$(a^{-1})^{-1} = a. \tag{2}$$

Да претпоставиме дека a и b се инверзибилни елементи во G. Тогаш имаме:

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e.$$

Со тоа го докажавме следново тврдење:

3°. Ако a и b се инверзибилни елементи во полугрупата G со единица, тогаш и ab е инверзибилен во G и притоа:

$$(ab)^{-1} = b^{-1}a^{-1}. \quad \blacksquare \tag{3}$$

Изнесените поими ни беа потребни, пред сè, за да го дефинираме поимот група. Имено, за ~ден групоид G велиме дека е *група* акко е полугрупа со единица, во која секој елемент е инверзибилен.

Поради важноста на поимот група, дефиницијата на овој поим ќе ја изнесеме во порасчленета форма.

4°. Групоидот $G(\cdot)$ е група акко се исполнети следниве три услови.

(i) G е полугрупа, т.е.

$$(xy)z = x(yz),$$

за секои $x, y, z \in G$.

(ii) G содржи единица, т.е. таков елемент e, што

$$xe = ex = x$$

за секој $x \in G$.

(iii) Секој елемент од G е инвезибилен во G, т.е. за секој елемент $x \in G$ постои (еднозначно определен) елемент $x^{-1} \in G$, таков што:

$$xx^{-1} = e = x^{-1}\, x.$$

Притоа: $e^{-1} = e$ и

$$(x^{-1})^{-1} = x, \quad (xy)^{-1} = y^{-1}x^{-1}$$

за секои $x, y \in G$. $\blacksquare$

Ако $M \neq \emptyset$, ниеден од групоидите $G(\cap)$, $G(\cup)$, $G(\setminus)$ од примерот 2.1.1) не е група. Имено, $G(\setminus)$ нема единица, ниту е полугрупа, а $G(\cup)$ и $G(\cap)$ се комутативни полугрупи со единица, во кои ниеден неединичен елемент не е инверзибилен. Групоидот $G(\dot{-})$ е група; имено, ако $A \in G$, т.е. $A \subseteq M$, тогаш $A \dot{-} A = (A \cup A) \setminus (A \cap A) = \emptyset$, од што следува дека секој елемент на $G(\dot{-})$ е своја инверзија, а спомнавме во 2.2. дека $G(\dot{-})$ е комутативна полугрупа со единица $\emptyset$.

Групоидот во 2.1.4) не е полугрупа, па, според тоа, не е ни група. Групоидот 2.2.1) а) е група и притоа имаме $x^{-1} = x$ за секој $x \in G$. И групоидот 2.2.1) б) е група: $e^{-1} = e$, $a^{-1} = c$, $b^{-1} = b$, $c^{-1} = a$. Ако се има предвид тоа што за секоја пермутација $f \in S(M)$ имаме $f^{-1} \in S(M)$ и $ff^{-1} = f^{-1}f = 1_M$. добиваме дека:

5°. Групоидот $S(M)$ е група. (За оваа група велиме дека е *симетричната група пермутации* на M.) $\blacksquare$

Да видиме кои елементи од M^M се инверзибилни. За да биде f инверзибилна трансформација треба да постои $g \in M^M$, таква што $gf = fg = 1_M$, а од тоа, според 1.4.8°, следува дека f е инјекција и сурјекција, т.е. f е биекција. Ако M има барем два различни елемента a, b и ако $(\forall x \in M) f(x) = a$ добиваме трансформација на M што не е биекција, па, значи, f не е инверзибилна во M^M. Со тоа го докажавме следново тврдење:

6°. (i) Множеството инверзибилни елементи на полугрупата M^M се совпаѓа со $S(M)$.

(ii) Ако M има барем два различни елемента, тогаш M^M не е група.

Ќе докажеме уште две својства.

7°. Секоја група е групоид со кратење.

Доказ. Ако $xz = yz$, тогаш:

$$x = xe = x(zz^{-1}) = (xz)z^{-1} = (yz)z^{-1} = y(zz^{-1}) = ye = y.$$

(Притоа e е единицата.) На ист начин се покажува дека $zx = zy \Rightarrow x = y$.

8°. Ако a и b се дадени елементи од групата G, тогаш постои една и само една двојка елементи x, $y \in G$, така што $ax = b$, $ya = b$.

Доказ. Да претпоставиме дека $ax = b$. "Множејќи" одлево со a^{-1}, добиваме $x = a^{-1}b$. Според тоа, постои најмногу еден елемент x што го задоволува равенството $ax = b$. Со проверка лесно се установува дека $a(a^{-1}b) = b$, од што следува дека, навистина, постои еден и само еден таков елемент x.

Слично се покажува дека $y = ba^{-1}$ е единствениот елемент $y \in G$ што го задоволува равенството $ya = b$.

За групата G велиме дека е *комутативна* (или *абелова*) акко е комутативна како групоид. Операцијата на една комутативна група, обично, се означува адитивно, т.е. се пишува $x + y$, наместо xy. Во овој случај, како што спомнавме и во 2.2., единицата се означува со o и се вика *нула* на групата. Инверзниот елемент на x се означува со $-x$ и се вика *спротивен елемент* на x.

Во една (адитивно означена) комутативна група $G(+)$ (како и кај секоја комутативна полугрупа) се дефинира операција *одземање* со 2.6. (1). Но, за разлика од општиот случај, сега одземањето е наполно дефинирано. Имено:

9°. Ако $G(+)$ е адитивно означена комутативна група, тогаш $G(-)$ е групоид и притоа:

$$x - y = x + (-y). \tag{4}$$

Имајќи ги предвид својствата **4°** и **9°**, како и направените договори, добиваме дека е точно следново тврдење.

10°. Ако $G(+)$ е комутативна група, тогаш:

$$x + o = x = o + x,\ x + y = y + x,\ x + (y + z) = (x + y) + z,$$
$$x - x = -x + x = o,\ -(-x) = x,\ -(x + y) = -x - y,$$
$$-(x - y) = -x + y = y - x,\ -(-x - y) = x + y,$$

за секои $x, y, z \in G$.

На крајот, да забележиме и дека:

11°. Ниедна од полугрупите $\mathbf{N}(+)$, $\mathbf{N}(\cdot)$ не е група. (Имено, 1 е единствениот инверзибилен елемент во $\mathbf{N}(\cdot)$, а 0 во $\mathbf{N}(+)$.) ▨

ВЕЖБИ. **2.** Да се провери дали групоидот од 2.2. 1) б) е група.

3. Да се определат келиевите шеми на сите групи со носител:

а) $\{a, b\}$; б) $\{a, b, c\}$. (Единицата не мора да биде означена со e.).

4. Еден групоид е група акко соодветниот спротивен групоид е група.

5. Полугрупата $G(*)$ од вежбата 2.2. **9.** е група.

.6. Кои од групоидите во вежбата 2.2.**10.** се групи?

7. Ако $G(*)$ е група и ако $\circ$ е определана со: $x \circ y = x * a * y$, каде што a е фиксен елемент на G, тогаш и $G(\circ)$ е група.

8. На $\mathbf{N}$ определуваме операција $*$ со:

$$x * y = \begin{cases} x - y \text{ за } y \leqslant x \\ y - x \text{ за } x < y. \end{cases}$$

Добиваме комутативен групоид со единица, но овој групоид не е група.

.9. Кои од групоидите: $\mathbf{Z}(+)$, $\mathbf{Z}(\cdot)$, $\mathbf{Q}(+)$, $\mathbf{Q}(\cdot)$, $\mathbf{Q}^+(+)$, $\mathbf{Q}^+(\cdot)$ се групи? (Притоа $\mathbf{Q}^+$ е множеството од позитивните рационални броеви).

10. Директно од шемата на секој од приложените групоиди да се заклучи дека ниеден од нив не е полугрупа.

а)

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	e

;

б)

	a	b	c
a	a	a	b
b	a	b	c
c	b	c	c

;

б)

	e	a	b	c
e	e	a	b	c
a	a	e	a	b
b	b	b	e	a
c	c	c	b	e

.

11. Да се пополнат приложените шеми, така што добиените групоиди да бидат групи.

а)

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

;

б)

	e	a	b	c
e	e	a	b	c
a	a	b	c	
b	b			
c	c			

;

в)

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	c
b	b				
c	c				
d	d				

.

12. Нека G е група, а S непразно множество. На G^S определуваме операција $*$ со:

$$f * g = h \Leftrightarrow (\forall x \in S)\ h(x) = f(x)\ g(x).$$

Добиениот групоид, исто така, е група.

13. Нека G е група. Следниве искази се еквивалентни:

(i) G е комутативна;

(ii) $(\forall x, y \in G)\ (xy)^{-1} = x^{-1} y^{-1}$;

(iii) $(\forall x, y \in G)\ (xy)^2 = x^2 y^2$.

14. Ако во групата G имаме $(\forall x \in G)\ x = x^{-1}$, тогаш таа група е комутативна.

*** 15.** Секоја конечна (непразна) полугрупа со кратење е група.

2.8. ПОДГРУПОИДИ

Групоидот $H(\circ)$ се вика *подгрупоид* на групоидот $G(*)$ акко:

$$H \subseteq G \wedge (x,\ y \in H \Rightarrow x \circ y = x * y). \tag{1}$$

Во овој случај ќе велиме и дека $G(*)$ е *надгрупоид* на $H(\circ)$.

Да разгледаме неколку примери:

1) Ако $G = B(M)$ и ако H е множеството од сите непразни подмножества на M, тогаш H е подгрупоид на $G(\cup)$.

2) $S(M)$ е подгрупоид на M^M.

3) $\mathbf{N}^+(+)$ е подгрупоид на $\mathbf{N}(+)$, а $\mathbf{N}^+(\cdot)$ на $\mathbf{N}(\cdot)$.

Речиси, очигледно е следново тврдење:

1°. Нека $H(\circ)$ е подгрупоид на $G(*)$. Ако $G(*)$ е: (а) комутативен (б) полугрупа, (в) групоид со кратење, тогаш соодветната особина ја има и $H(\circ)$.

Доказ. (а) Ако $G(*)$ е комутативен групоид, тогаш:

$$x,\ y \in H \Rightarrow x \circ y = x * y = y * x = y \circ x,$$

т.е. и $H(\circ)$ е комутативен.

(б) На ист начин како и (а).

(в) Ако $G(*)$ е групоид со кратење и ако $x, y, z \in H$ и $x \circ z = y \circ z \vee z \circ x = z \circ y$, тогаш $x,\ y,\ z \in G$ и $x * z = y * z \vee z * x = z * y$ од што следува $x = y$, па, значи, и $H(\circ)$ е групоид со кратење. ▒

Еден подгрупоид на групоид со единица може и да нема единица; таков случај имаме кај погоре спомнатите групоиди $H(\cup)$ и $G(\cup)$.

За подгрупоидот $H(\circ)$ од групоидот $G(*)$ се вели дека е: а) потполугрупа, б) подгрупа акко $H(\circ)$ е: а) полугрупа, б) група.

Од **1°** следува дека:

2°. Секој подгрупоид од една полугрупа е и потполугрупа. ▒

Соодветното својство за подгрупите не важи. (· На пример, $\mathbf{N}(+)$ е подгрупоид од групата $\mathbf{Z}(+)$, но не е подгрупа.).

Во претходните делови носителот G на еден групоид $G(*)$ го идентификувавме со самиот групоид. Во таа смисла, ако $H(\circ)$ е подгрупоид на $G(*)$, за подмножеството H велиме дека е подгрупоид на G. Но, не е подгрупоид секое подмножесто од G. Имајќи ја предвид дефиницијата (1), добиваме дека:

3°. Подмножеството H од групоидот G е подгрупоид акко:

$$x,\ y \in H \Rightarrow xy \in H. \text{ ▒} \tag{2}$$

Исто така, јасно е дека:

4°. $\varnothing$ и G се подгрупоиди на групоидот G. ▒

Да видиме какви услови треба да задоволува едно подмножество H од една група G за да биде подгрупа. Пред сè, H треба да биде подгрупоид, од што следува дека условот (2) треба да биде исполнет. Потоа, во H треба да постои единица, да ја означиме со e^*; ако e е единицата на G, ќе имаме $e^*e = e^* = e^*e^*$, од што, според 2.7.7°, следува $e^* = e$. Така, покажавме дека треба да биде исполнет и следниов услов:

$$e \in H. \tag{3}$$

Нека $x \in H$ и нека со x^* ја означиме инверзијата на x во H; тогаш имаме $xx^* = e = xx^{-1}$, од што следува $x^* = x^{-1}$. Според тоа, добиваме дека:

$$x \in H \Rightarrow x^{-1} \in H. \tag{4}$$

Да претпоставиме дека H е подмножество од групата G, при што се исполнети условите (2), (3) и (4). Од (2) следува дека H е подгрупоид, па според **2°**, H како групоид е полугрупа. Од (3) и (4) потоа добиваме дека H е полугрупа со единица, во која секој елемент е инверзибилен, т.е. дека H е група

Со спроведената дискусија, го докажавме следново тврдење:

5°. Едно подмножество H од групата G е подгрупа акко се исполнети условите (2), (3) и (4). ▒

Ќе докажеме уште едно својство.

6°. Нека G е полугрупа со единица. Ако H се состои од сите инверзибилни елементи на G, тогаш H е подгрупа на G.

Доказ. Според 2.7.**3°**, H е подгрупоид, па, значи, (според **1°**) и потполугрупа. Потоа, единицата e на G е инверзибилна ($e^{-1} = e$), од што следува дека $e \in H$. Секој елемент $a \in H$ има инверзија во H, бидејќи $a^{-1} \in H$. Од сето тоа следува дека H (како групоид) е група, т.е. дека е подгрупа на G. ▒

ВЕЖБИ. **2.** Да се определат сите подгрупоиди на групоидот определен со шемата:

а)

	a	b
a	a	b
b	b	a

;

б)

	a	b	c
a	b	a	c
b	b	a	c
c	a	b	a

;

б)

	a	b	c	d
a	a	b	a	b
b	a	b	c	c
c	b	c	c	c
a	a	b	c	c

.

3. Нека G $(*)$ е групоид и a објект што не е елемент на G. На множеството $G^a = G \cup \{a\}$ определуваме операција $\circ$ со:

$$x, y \in G \Rightarrow x \circ y = x * y,\ x \in G^a \Rightarrow x \circ a = a \circ x = x.$$

Добиваме групоид G^a $(\circ)$ со единица a, и притоа G $(*)$ е подгрупоид на G^a $(\circ)$.

4. Дали може групоидот G^a од претходната вежба да биде група?

5. Ако K и H се подгрупи на групата G, тогаш и $K \cap H$ е подгрупа; $K \cup H$ е подгрупа акко $K \subseteq H \vee H \subseteq K$.

6. Ако G е група, тогаш

$$L(G) = \{\gamma_x | x \in G\} \text{ е подгрупа на } S(G).$$

(γ_x се определува како во вежбата 2.2. 7.).

***7.** Секој непразен подгрупоид на една конечна група е подгрупа.

8. Нека $k \in \mathbf{N}$ и нека $A_k = \{x \mid x \in \mathbf{N},\ x \geqslant k\}$. A_k е потполугрупа и од $\mathbf{N}(+)$ и од $\mathbf{N}(\cdot)$.

9. Во кој случај $\mathbf{N}_n$ е потполугрупа: а) на $\mathbf{N}(+)$, б) на $\mathbf{N}(\cdot)$?

3. ЦЕЛИ БРОЕВИ

3.1. АДИТИВНА ГРУПА НА ЦЕЛИТЕ БРОЕВИ

Како што спомнавме во 2.7., $\mathbf{N}(+)$ е комутативна полугрупа со нула, но не е група, бидејќи ниеден ненулти елемент од $\mathbf{N}$ нема спротивен елемент. Ја поставуваме задачата да определиме надгрупоид $\mathbf{Z}(+)$ на $\mathbf{N}(+)$, така што добиениот групоид да биде комутативна група, а множеството $\mathbf{Z} \setminus \mathbf{N}$ да има "што помалку" елементи. Оваа задача наложува на секој ненулти природен број n да му придружиме елемент $-n$ кој сакаме да биде спротивен на n. Да го означиме со $-\mathbf{N}^+$ множеството од сите такви елементи, т.е.

$$-\mathbf{N}^+ = \{-x \mid x \in \mathbf{N}^+\}. \tag{1}$$

Притоа сметаме дека $\mathbf{N} \cap (-\mathbf{N}^+) = \varnothing$ и:

$$-x = -y \Leftrightarrow x = y. \tag{2}$$

Бараното множество $\mathbf{Z}$ се определува со:

$$\mathbf{Z} = \mathbf{N} \cup (-\mathbf{N}^+). \tag{3}$$

Елементите на множеството $\mathbf{Z}$ ги нарекуваме *цели* броеви; притоа елементите од $\mathbf{N}^+$ се викаат *позитивни*, а оние од $-\mathbf{N}^+$ *негативни цели броеви.*

Поставената задача ја наложува следната дефиниција на операцијата *собирање* $(+')$ во $\mathbf{Z}$.

$$x,\ y \in \mathbf{N} \Rightarrow x +' y = x + y. \tag{4.1}$$

Ако x и y се позитивни цели броеви, т.е. ако $x, y \in \mathbf{N}^+$, тогаш:

$$(-x) +' (-y) = -(x + y), \tag{4.2}$$

$$(-x) +' 0 = -x = 0 +' (-x), \tag{4.3}$$

$$x +' (-y) = \begin{cases} x - y & \text{ако } x \geqslant y \\ -(y - x) & \text{ако } y > x \end{cases} \tag{4.4}$$

$$= (-y) +' x.$$

(Операцијата собирање во $\mathbf{Z}$ ја означуваме со $+'$ бидејќи $+$ е знак за собирање во $\mathbf{N}$. Оваа ознака е само привремена).

Од тврдењето што ќе го докажеме подолу, се гледа дека поставената задача е успешно извршена. (Да се види и 4.5.8°.).

1°. $\mathbf{Z}(+')$ е комутативна група за која $\mathbf{N}(+)$ е потполугрупа.

Доказ. (i) Да покажеме прво дека $\mathbf{Z}(+')$ е групоид. Нека $u, v \in \mathbf{Z}$; ако $u, v \in \mathbf{N}$, тогаш $u +' v$ е дефиниран со (4.1), а со (4. 2), ако $u, v \in -\mathbf{N}^+$; ако еден од броевите u, v е нула, а другиот негативен, тогаш $u +' v$ е определен со (4.3); и на крајот, ако еден од броевите u, v е позитивен, а другиот негативен, тогаш збирот $u +' v$ се дефинира со (4.4).

(ii) Во (4.3) и (4.4) комутативноста се претпоставува по дефиниција, а во (4.1) и (4.2) следува од комутативноста на собирањето во $\mathbf{N}$.

(iii) Од (4.1) следува дека $\mathbf{N}(+)$ е потполугрупа на $\mathbf{Z}(+')$. Ова ни дозволува да го употребуваме знакот $+$ и за собирањето во $\mathbf{Z}$.

(iv) Ако се има предвид (4.3) и тоа што 0 е нула во $\mathbf{N}(+)$, добиваме дека 0 е нула и во $\mathbf{Z}(+)$.

(v) Преостанува да покажеме дека $\mathbf{Z}(+)$ е полугрупа, т.е. дека е точно равенството:

$$u + (v + w) = (u + v) + w, \tag{5}$$

за секои $u, v, w \in \mathbf{Z}$.

Дека е точно равенството (5), ќе покажеме во неколку етапи.

(v.1) Ако некој од u, v, w е 0, (5) е точно според (iv) и 2.2. 7°. Ако $u, v, w \in \mathbf{N}$, гогаш точноста на (5) следува од (iii). Нека $u, v, w \in -\mathbf{N}^+$, т.е. $u = -x$, $v = -y$, $w = -z$, каде $x, y, z \in \mathbf{N}^+$. Тогаш, според (4.2), добиваме:

$$u + (v + w) = -[x + (y + z)] = -[(x + y) + z] = (u + v) + w.$$

(v.2) Да претпоставиме дека $u = x$, $v = -y$, $w = -z$, каде $x, y, z \in \mathbf{N}^+$. (Во текот на натамошниот доказ, секогаш ќе претпоставуваме дека $x, y, z \in \mathbf{N}^+$.) Можни се сега следниве случаи:

(v.2.1) $x < y$;

(v.2.2) $y \leqslant x \leqslant y + z$;

(v.2.3) $y + z < x$.

Користејќи ги соодветните својства на делумната операција одземање спомната во 2.6., лесно се добива дека во првите два случаја, левата и десната страна на (5) се еднакви со $-[(y + z) - x]$, а со $x - (y + z)$ во третиот случај.

(v.3) $u = x$, $v = y$, $w = -z$.

Сега ги разликуваме следните случаи:

(v.3.1) $z < y$;

(v.3.2.) $y \leqslant z \leqslant x + y$;

(v.3.3) $x + y < z$.

Во првите два случаја, двете страни на (5) се еднакви со $(x + y) - z$, а во третиот, со $-[z - (x + y)]$.

(v.4) $u = x, \quad v = -y, \quad w = z.$

Ако $y < z$ или $z \leqslant y \leqslant x + z$, тогаш и двете страни на (5) се еднакви со $(x + z) - y$, а со $-[y - (x + z)]$ ако $y \geqslant x + z$.

(v.5) $u = -x, \quad v = y, \quad w = z.$

Точноста на (5) сега следува од (v.3), според 2.2.**8**° (iii).

(v.6) $u = -x, \quad v = y, \quad w = -z.$

Ако $y \geqslant x + z$,тогаш и двете страни на (5) се еднакви со $y - (x + z)$, а со $-[(x + z) - y]$ ако $z \leqslant y < x + z$, или $y < z$.

(v.7 $u = -x, \quad v = -y, \quad w = z.$

Ако $z \geqslant x + y$, тогаш и двете страни на (5) се еднакви со $z - (x + y)$, а со $-[(x + y) - z]$, ако $y \leqslant z < x + y$ или $z < y$.

Со тоа го комплетиравме доказот. ▒

Во иднина, обично, множеството позитивни цели броеви ќе го означуваме со $\mathbf{Z}^+$, а со $\mathbf{Z}^-$, множеството негативни цели броеви. Множеството ненултри цели броеви ќе го изначуваме со $\mathbf{Z}^*$; поопшто, ако M е множество броеви, тогаш со M^* го означуваме множеството броеви, $M \setminus \{0\}$. Според тоа, имаме:

2°. (i) $\mathbf{Z} = \mathbf{Z}^- \cup \{0\} \cup \mathbf{Z}^+$; (ii) $\mathbf{Z}^* = \mathbf{Z}^- \cup \mathbf{Z}^+$;

(iii) $\mathbf{Z}^- \cap \mathbf{Z}^+ = \varnothing$; (iv) $\mathbf{Z}^+ = \mathbf{N}^+ = \mathbf{N}^*$; (v)$\mathbf{Z}^- = -\mathbf{N}^+$. ▒

ВЕЖБИ. **2.** Да се направи обид за скратување доказот на равенството (5), со тоа што претходно ќе се докаже дека $-[x + (-y)] = y + (-x)$, при што:

$-0 = 0$ и $-(-x) = x$ за секој $x \in \mathbf{N}^+$.

3. $\mathbf{Z}^-$ е потполугрупа на групата $\mathbf{Z}(+)$.

4. Нека $A = \{a_n \mid n \in \mathbf{Z}\}$, $B = \{b_n \mid n \in \mathbf{Z}\}$ и $G = A \cup B$. На G определуваме операција $*$ со:

$$a_m * a_n = a_{m+n}, \quad a_m * b_n = b_{m+n},$$
$$b_m * b_n = a_{m-n}, \quad b_m * a_n = b_{m-n}.$$

Добиениот групоид $G(*)$ е некомутативна група. (Притоа, се претпоставува дека $A \cap B = \varnothing$ и $a_m = a_n \vee b_m = b_n \Rightarrow m = n$.).

5. $\mathbf{Z}$ е пребројво множество.

6. Ако H е подгрупа на $\mathbf{Z}(+)$, таква што $\mathbf{N} \subseteq H$, тогаш $H = \mathbf{Z}$.

7. Нека $P(+)$ е полугрупа со кратење и нула 0, таква што: за секои $x, y \in P$, $x \neq y$ еден и само еден од исказите $x - y \in P$, $y - x \in P$ е точен. Тогаш, со: $x \leqslant y \Leftrightarrow y - x \in P$ е дефинирано потполно подредување на P со најмал елемент 0.

8. Ако P е како во претходната вежба, тогаш со P^+ го означуваме множеството ненулти елементи. На секој елемент $a \in P^+$ му придружуваме елемент $-a$, така што (2) е точно и $P \cap \{-x \mid x \in P^+\} = \varnothing$. Да го означиме со R множеството $P \cup P^-$, каде што $P^- = \{-x \mid x \in P^+\}$. Во P дефинираме собирање $+'$ со (4.1) — (4.4), при што $\mathbf{N}$ се заменува со P. Добиениот групоид $R(+')$ е комутативна група, за која $P(+)$ е потполугрупа.

3.2. МНОЖЕЊЕ НА ЦЕЛИ БРОЕВИ

Овде сакаме да дефинираме операција $*$ во $\mathbf{Z}$, така што $\mathbf{N}(\cdot)$ да биде подгрупоид на $\mathbf{Z}(*)$, а некои од својствата на групоидите $\mathbf{N}(+)$ и $\mathbf{N}(\cdot)$ да важат и за групоидите $\mathbf{Z}(+)$, $\mathbf{Z}(*)$. Имено, сакаме $\mathbf{Z}(*)$ да е комутативна полугрупа, а множењето $(*)$ да е дистрибутивно спрема собирањето $(+)$, т.е да биде точно равенството:

$$x * (y + z) = (x * y) + (x * z) \tag{1}$$

за секои цели броеви x, y, z.

Да претпоставиме дека таква операција $*$ е определена во $\mathbf{Z}$.

Ако $x, y \in \mathbf{N}$, тогаш ќе имаме:

$$x * y = x \cdot y, \tag{2.1}$$

бидејќи $\mathbf{N}(\cdot)$ е подгрупоид на $\mathbf{Z}(*)$.

Нека $x, y \in \mathbf{N}^+ (= \mathbf{N}^* = \mathbf{Z}^+)$. Ако се користи (1) и фактот што $\mathbf{Z}(+)$ е група, добиваме:

$$(-x) * 0 + 0 = (-x) * 0 = (-x) * (0 + 0) = [(-x) * 0] + [(-x) * 0].$$

т.е. $(-x) * 0 = 0$. Од тоа (ако се има предвид и комутативноста на $\mathbf{Z}(*)$) се добива:

$$(-x) * 0 = 0 = 0 * (-x). \tag{2.2}$$

Потоа, ако се користи и (2.2) се добива:

$$0 = x * 0 = x * [y + (-y)] = (x * y) + [x * (-y)],$$

т.е. $x * (-y) = -(x * y)$. Според тоа, имаме:

$$x * (-y) = -(x \cdot y) = (-x) * y. \tag{2.3}$$

И на крајот:

$$0 = (-x) * 0 = (-x) * [y + (-y)] = [(-x) * y] + [(-x) * (-y)],$$

од што следува $(-x) * (-y) = -[(-x) * y)$, т.е.

$$(-x) * (-y) = x \cdot y. \tag{2.4}$$

Со извршената дискусија покажавме дека, ако операцијата $(*)$ ги има бараните својства, тогаш се точни равенствата (2.1) — (2.4), но од тоа уште не следува дека постои таква операција. Сепак, ако се погледнат спомнатите равенства, ќе се уочи дека со нив може да се дефинира операција $*$, но сега се поставува прашање дали таа е дистрибутивна спрема собирањето; во следново тврдење, покрај другото, се покажува дека и тоа е точно.

1°. Нека во $\mathbf{Z}$ е определена операција $(*)$ со (2.1) — (2.4), при што во (2.1) $x, y \in \mathbf{N}$, а во (2.2) — (2.4) $x, y \in \mathbf{N}^+$. Точни се следниве искази:

(i) $\mathbf{N}(\cdot)$ е потполугрупа на $\mathbf{Z}(*)$.

(ii) За секои $x, y \in \mathbf{Z}$, точни се равенствата:

$$x * 0 = 0 * x = 0, \tag{2.2'}$$

$$x * (-y) = (-x) * y = -(x * y), \tag{2.3'}$$

$$(-x) * (-y) = x * y. \tag{2.4'}$$

(iii) $\mathbf{Z}$ $(*)$ е комутативна полугрупа.

(iv) За секои $x, y, z \in \mathbf{Z}$, точно е равенството (1), како и равенството

$$(x + y) * z = (x * z) + (y * z). \tag{1'}$$

Доказ. (i) Ова е последица од (2.1) и фактот што $\mathbf{N}(\cdot)$ е полугрупа.

(ii) Ако $x \in \mathbf{N}$, равенството (2.2') е точно според (i), а за $x \in \mathbf{Z}^-$, тоа равенство е точно според (2.2). Ако $x = 0 \vee y = 0$, тогаш е јасно дека се точни и (2.3') и (2.4'); за $x, y \in \mathbf{N}^+$, тие равенства се точни според (2.1) и (2.3), односно (2.4). Користејќи ги (2.1), (2.3) и (2.4), лесно се докажуваат (2.3') и (2.4'), во секој од следниве случаи: $x, y \in \mathbf{Z}^-$; $x \in \mathbf{Z}^+$, $y \in \mathbf{Z}^-$; $x \in \mathbf{Z}^-$, $y \in \mathbf{Z}^+$.

(iii) Ако $x = 0 \vee y = 0$, тогаш имаме $x * y = y * x = 0$, според (2.2'); ако $x, y \in \mathbf{Z}^+ = \mathbf{N}^+$, тогаш: $x * y = xy = yx = y * x$, според (2.1); ако $x, y \in \mathbf{Z}^-$ тогаш $-x, -y \in \mathbf{Z}^+$, па имаме: $x * y = (-x) * (-y) = (-y) * (-x) = y * x$; ако $x \in \mathbf{Z}^+$, $y \in \mathbf{Z}^-$, тогаш $-y \in \mathbf{Z}^+$, па $x * y = -[x * (-y)] = -[(-y) * x] = -[-(-y)] * x = y * x$. Со тоа покажавме дека $\mathbf{Z}(*)$ е комутативен групоид.

Користејќи го тоа што е $\mathbf{N}(\cdot)$ полугрупа, како и (2.2′) — (2.4′), лесно се покажува дека и $\mathbf{Z}(*)$ е полугрупа.

(iv) Ако $x = 0 \vee y = 0 \vee z = 0$, тогаш (1) е точно според (2.2′). За $x, y, z \in \mathbf{N}$, точноста на (1) следува од (2.1) и фактот што множењето на природни броеви е дистрибутивно спрема собирањето (својство: 2.5.**1**°). Ако $x, y \in \mathbf{N}^+ = \mathbf{Z}^+$, $z = -u \in \mathbf{Z}^-$, $u \in \mathbf{Z}^+$, $y - z \in \mathbf{Z}^+$, тогаш:

$$x * (y + z) = x \cdot (y - u) = (xy) - (xu)$$

$$= (x * y) + [-(x * u)] = (x * y) + x * (-u)$$

$$= (x * y) + (x * z).$$

Разгледувајќи ги сите можни случаи, ќе добиеме дека (1) е точно за секоја тројка цели броеви x, y, z.

Доказот на (1) може да се комплетира и на друг начин. Имено, може прво да се докаже дека, ако целите броеви m, n, p го задоволуваат равенството:

$$m * (n + p) = (m * n) + (m * p),$$

тогаш се точни и равенствата:

$$m * (p + n) = (m * p) + (m * n)$$

$$m * [(-n) + (-p)] = [m * (-n)] + [m * (-p)]$$

$$(-m) * (n + p) = [(-m) * n] + [(-m) * p].$$

Потоа, се добива дека точноста на (1), за секој случај кога $x, y, z \in \mathbf{Z}^*$, е последица од точноста за разгледаните случаи: $x, y, z \in \mathbf{N}^+$; $x, y \in \mathbf{N}^+$, $z \in \mathbf{Z}^-$, $y - z \in \mathbf{Z}^+$.

Равенството (1′) е последица на (1) и комутативноста на $*$. ▒

Натаму ќе ја употребуваме мултипликативната ознака и за операцијата $*$, т.е. ќе пишуваме xy, наместо $x * y$. Исто така, сметајќи "множењето да сврзува повеќе од собирањето", некои загради нема да ги пишуваме. На пример, десната страна на (1) ќе ја пишуваме во облик: $xy + xz$; наместо $-(xy)$, односно $(-x)y$, ќе пишуваме $-xy$.

Полугрупата $\mathbf{Z}(\cdot)$ ќе ја викаме *мултипликативна полугрупа* на целите броеви. На читателот му препуштаме да ги докаже следните тврдења.

2°. Мултипликативната полугрупа на целите броеви има единица 1, а -1 е единствениот неединичен инверзибилен елемент во оваа полугрупа. ▒

3°. $xy = 0 \Leftrightarrow x = 0 \vee y = 0$. ▒

4°. $x \neq 0 \wedge xy = xz \Rightarrow y = z$. ▒

5°. За секоја тројка цели броеви x, y, z, точни се равенствата:

$$x(y - z) = xy - xz, \tag{1''}$$

$$(x - y)z = xz - yz. \tag{1'''}$$

(На десните страни од (1'') и (1''') се изоставени соодветни загради.)

ВЕЖБИ. 2. Операцијата $\circ$ на $\mathbf{Z}$ е таква што:

$$(x + y) \circ (u + v) = x \circ u + x \circ v + y \circ u + y \circ v$$

за секои $x, y, u, v \in \mathbf{Z}$ акко постои $a \in \mathbf{Z}$, таков што $x \circ y = axy$. Тогаш, $\mathbf{Z}(\circ)$ е комутативна полугрупа.

3. Ако $a, b, a', b' \in \mathbf{Z}$ се такви што $ab' - a'b \neq 0$, тогаш:

$$(ax + by = c) \wedge (a'x + b'y = c') \Leftrightarrow [(ab' - ba')\, x = b'c - c'b] \wedge [(ab' - ba')\; y = ac' - ca'].$$

4. (i) Ако во $\mathbf{Z}$ дефинираме релација α со: $x\alpha y \Leftrightarrow (\exists z)\ y = xz$, тогаш, α е рефлексивна и транзитивна, но α не е ни симетрична, ни антисиметрична.

(ii) Релацијата β определена со: $x\beta y \Leftrightarrow x\alpha y \wedge y\alpha x$ е еквивалентност во $\mathbf{Z}$ и притоа: $\mathbf{Z}_{/\beta} = \{\{0\}, \{-1,1\}, \{-2,2\}, \ldots, \{-n, n\}, \ldots\}$.

5. $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$ е потполугрупа на $\mathbf{Z}(\cdot)$, и притоа $\mathbf{Z}^*$ е полугрупа со кратење и единица 1. Според тоа, во $\mathbf{Z}^*$ е определена делумна операција делење $/$. Оваа операција се проширува на $\mathbf{Z}$ со: $0/x = 0$ за $x \neq 0$. Во делумниот групоид $\mathbf{Z}(/)$ се точни равенствата (1') — (9') од 2.6., како и тврдењата 2.6. 7°.

3.3. СТЕПЕНИ СО ЦЕЛИ ЕКСПОНЕНТИ

При дефиницијата на поимот за инверзибилен елемент во полугрупа со единица, всушност, го воведовме поимот за степен со експонент -1, и покрај тоа што таму "-1" беше само еден симбол без определена содржина на цел број. Овде ќе го дефинираме поимот за *степен со произволен цел експонент* (т.е. *показател*).

Нека $G(*)$ е полугрупа со единица e. Ако $a \in G$ е инверзибилен елемент во G и ако $n \in \mathbf{N}^+$, тогаш a^{-n} се дефинира со:

$$a^{-n} = (a^{-1})^n. \tag{1}$$

Според тоа, ако a е инверзибилен елемент во G ,тогаш, за секој цел број k, определен е степенот a^k. Специјално, ако G е група, тогаш секој елемент е инверзибилен, па, според тоа, за секој цел број m и елемент $x \in G$, степенот x^m е елемент од G. На читателот му препуштаме да го докаже следново својство:

1°. Ако $G(*)$ е група, тогаш:

(i) $x^m * x^n = x^{m+n}$;

(ii) $(x^m)^n = x^{mn}$;

(iii) $xy = yx \Rightarrow (xy)^m = x^m y^m$,

за секои $m, n \in \mathbf{Z}$, $x, y \in G$.

Во случај на адитивно означена комутативна група $G(+)$, пишуваме mx, наместо x^m. Според тоа, во овој случај, имаме:

2°. (i) $mx + nx = (m + n)x$;

(ii) $m(nx) = (mn)x$;

(iii) $m(x + y) = mx + my$;

(iv) $mx - my = m(x - y)$, $(m - n)x = mx - nx$;

(v) $1x = x$, $(-1)x = -x$, $0x = 0$;

за секои $x, y \in G$, $m, n \in \mathbf{Z}$.

Во адитивната група $\mathbf{Z}(+)$ на целите броеви е определен "степенот" m^n за секои $m \in \mathbf{Z}$, $n \in \mathbf{Z}$, а, од друга страна, и производот $m \cdot n$ во $\mathbf{Z}(\cdot)$. Ако се има предвид дефиницијата на множењето, како и **2°**, се добива дека и двата производа се еднакви.

ВЕЖБИ. **2.** Ако $G(*)$ е групата од вежбата 3.1.**4**, тогаш $a_n = a_1^n$, $b_n^m = a_0 \vee b_n^m = b_n$.

3. Ако $a, b \in \mathbf{Z}$, $n \in \mathbf{Z}^+$, тогаш:

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n.$$

3.4. ПОДРЕДУВАЊЕ НА ЦЕЛИТЕ БРОЕВИ

Ако се искористи својството 2.3.**6°**, се доаѓа до поимот за *подредување во множеството* $\mathbf{Z}$. Имено, релацијата $\leqslant^*$ се дефинира со:

$$x, y \in \mathbf{Z} \Rightarrow (x \leqslant^* y \Leftrightarrow y - x \in \mathbf{N}). \tag{1}$$

Од ова, ако се има предвид спомнатото својство, се добива дека:

1°. Релацијата $\leqslant$ е рестрикција од $\leqslant^*$ на $\mathbf{N}$, т.е.

$$x, y \in \mathbf{N} \Rightarrow (x \leqslant y \Leftrightarrow x \leqslant^* y). \tag{2}$$

Поради (2), нема потреба да ги означуваме различно релациите $\leqslant$ и $\leqslant^*$, па затоа ќе ја употребуваме само првата ознака. Ако се има предвид тоа што: $0 \in \mathbf{N}$; $x \in \mathbf{N} \wedge -x \in \mathbf{N} \Leftrightarrow x = 0$; $\mathbf{N}(+)$ е полугрупа, добиваме:

2°. Релацијата $\leqslant$ е подредување на $\mathbf{Z}$.

Како и кај секое подредување, *стриктното подредување* се дефинира со:

$$x, y \in \mathbf{Z} \Rightarrow (x < y \Leftrightarrow x \leqslant y \wedge x \neq y). \tag{3}$$

На читателот му препуштаме да ги докаже следните тврдења.

3°. $x, y \in \mathbf{Z} \Rightarrow (x < y \Leftrightarrow y - x \in Z^{+})$.

4°. $x, y \in \mathbf{Z} \Rightarrow (x < y \vee x = y \vee y < x)$.

5°. Во $\mathbf{Z}$ нема најмал, ниту најголем елемент.

Да го дефинираме уште поимот за *апсолутна вредност*. Имено, ако $x \in \mathbf{Z}$, тогаш бројот $|x|$, определен со:

$$|x| = \begin{cases} x \text{ за } x \geqslant 0 \\ -x \text{ за } x < 0 \end{cases} \tag{4}$$

се вика апсолутна вредност на x.

6°. Ако $x, y \in \mathbf{Z}$, тогаш:

(i) $|x| = |-x| \in \mathbf{N}$;

(ii) $|xy| = |x|\,|y|$;

(iii) $|x + y| \leqslant |x| + |y|$.

ВЕЖБИ. **2.** Ако $x, y, z \in \mathbf{Z}$, тогаш:

(i) $x < y \Leftrightarrow x + z < y + z$; (ii) $x > 0 \Rightarrow (y < z \Leftrightarrow xy < xz)$;
(iii) $x < 0 \Rightarrow (y < z \Leftrightarrow xy > xz)$;
(iv) $|x + y + z| \leqslant |x| + |y| + |z|$;
(v) $|x| < y \Leftrightarrow -y < x,\ x < y$;
(vi) $||x| - |y|| \leqslant |x + y|$; (vii) $||x| - |y|| \leqslant |x - y|$;
(viii) $(x + y)^2 \geqslant 4xy$.

3. Непразното подмножество A на $\mathbf{Z}$ е конечно акко е ограничено во $\mathbf{Z}$; притоа ако $A = \{x \mid x \in \mathbf{Z},\ a \leqslant x \leqslant b\}$, каде што a и b се дадени цели броеви $(a \leqslant b)$, тогаш $|A| = b - a + 1$.

4. Непразното подмножество A на $\mathbf{Z}$ има најголем (најмал) елемент акко е мајорирано (минорирано) во $\mathbf{Z}$.

5. Да се определат сите цели броеви x, y, такви што:

а) $|x| + |y| = 3$; б) $|x - 3| + |y - 5| = 4$.

3.5. ДЕЛИВОСТ

Множеството $\mathbf{Z}^*$, на целите броеви различни од нула, е комутативна полугрупа со кратење во однос на операцијата множење на цели броеви. Според тоа, во $\mathbf{Z}^*$ е определена делумна операција делење $/$. Оваа операција се проширува и на $\mathbf{Z}$ со тоа што се става:

$$0/y = 0$$

за секој $y \in \mathbf{Z}$, $y \neq 0$. Овде нас нè интересира релацијата за деливост $|$ определена со:

$$x \mid y \Leftrightarrow (\exists z)\, y = xz. \tag{1}$$

(Треба веднаш да се уочи разликата меѓу "$|$" и "$/$", бидејќи во првиот случај имаме знак за релација, а во вториот знак, за делумна операција).
Ако $a, b \in \mathbf{Z}$ и ако е точен исказот $b \mid a$, тогаш велиме дека b *е делител на* a.

Од (1) следува дека:

1°. За секој цел број x:

(i) $1 \mid x$, $-1 \mid x$; (ii) $x \mid x$, $x \mid -x$;

(iii) $x \mid 0$; (iv) $0 \mid x \Leftrightarrow x = 0$.

Пред да дефинираме неколку нови поими ќе докажеме уште три тврдења.

2°. Релацијата $|$ е рефлексивна и транзитивна, но не е симетрична ни антисиметрична.

Доказ. Дека $|$ е рефлексивна, но не е ни симетрична ни антисиметрична следува од **1°**. Ако $a \mid b$, $b \mid c$, тогаш $b = am$, $c = bn$ за некои $m, n \in \mathbf{Z}$, па значи $c = (am)n = a(mn)$, т.е. $a \mid c$.

3°. $a \neq 0 \wedge b \mid a \Rightarrow |b| \leqslant |a|$.

Доказ. Од $b \mid a$ следува $a = bc$, каде што c е цел број. Во тој случај имаме $|a| = |bc| = |b|\,|c|$, од што, поради $|a| \geqslant 1$, добиваме $|b| \leqslant |a|$.

4°. Ако $a, b \in \mathbf{Z}$, тогаш следниве искази се еквивалентни:

(i) $b \mid a$; (ii) $-b \mid a$; (iii) $b \mid -a$; (iv) $-b \mid -a$.

Доказ.. Нека $b \mid a$, т.е. $a = bc$ за некој $c \in \mathbf{Z}$. Тогаш имаме

$$a = (-b)(-c), \quad -a = b(-c) = (-b)c$$

т.е. добиваме $-b \mid a$, $b \mid -a$, $-b \mid -a$. Од тоа, имајќи предвид дека $-(-x) = x$, следува точноста на својството.

Од својствата **1°** и **4°** следува дека при испитувањето на релацијата $\cdot \mid$ можеме да се ограничиме на рестрикцијата од оваа релација на $\mathbf{N}$, па дури и на $\mathbf{N}^+$. Да уочиме притоа дека:

5°. $a, b \in \mathbf{N} \Rightarrow (a \mid b \wedge b \mid a \Leftrightarrow a = b)$.

Поради примената што ја наоѓа, следното тврдење се вика *основна теорема за делење.*

6°. Нека a и b се природни броеви, при што $b \neq 0$. Постојат природни броеви q, r такви што:

$$a = qb + r, \quad r < b. \tag{1}$$

Притоа, q и r се однозначно определени; q се вика *количник*, а r *остаток* при делењето на a со b.

Доказ. Нека r е најмалиот природен број во множеството $A = \{a - kb \mid k \in \mathbf{N}\}$. Според тоа, постои $q \in \mathbf{N}$, таков што $r = a - qb$, т.е. $a = qb + r$. Притоа, имаме $r < b$, бидејќи за $r \geqslant b$, бројот $r - b = a - (q + 1)b$ би бил помал природен број отколку r.

Преостанува да покажеме дека q и r се еднозначно определени. Навистина, ако:

$$\begin{aligned} a &= q'b + r' \\ &= q''b + r'', \end{aligned} \qquad r' \leqslant r'' < b$$

тогаш:

$$r'' - r' = (q' - q'')\, b,$$

што, поради $0 \leqslant r'' - r' < b$, е можно само за $r'' - r' = 0$, т.е. $r'' = r'$ и $q' - q'' = 0$, т.е. $q' = q''$.

Директно, или со помош на **6°**, лесно се докажува и следново тврдење:

6′. Нека $a, b \in \mathbf{Z}$, $b \neq 0$. Постојат еднозначно определени цели броеви q и r такви што:

$$a = bq + r, \quad 0 \leqslant r < |b|. \tag{1′}$$

Јасно е и дека:

7°. Нека $b \neq 0$. Остатокот при делењето на a со b е нула акко b е делител на a.

ВЕЖБИ **2.** Ако $x, y \in \mathbf{Z}$ тогаш:

(i) $3 \mid xy\,(x + y)\,(x - y)$;

(ii) $5 \mid xy\,(x^2 + y^2)\,(x^2 - y^2)$; (iii) $6 \mid x\,(x^2 + 5)$.

3. Ако $x \in \mathbf{Z}$, $x \neq 0$, тогаш множеството од сите делители на x е конечно.

4. Ако $x, y \in \mathbf{N}$, тогаш $x! \cdot y! \mid (x+y)!$.

5. Ако $x, y \in \mathbf{N}$, $x \neq 0$, тогаш $x \mid y(y+1)\ldots(y+x)$.

6. Да се определат целите броеви x, y така што:

а) $xy = x + y$; б) $2xy + 3y^2 = 24$.

3.6. БРОЈНИ СИСТЕМИ

Ќе го образложиме добро познатиот начин за означување на природните броеви во *десетичниот систем* и ќе покажеме дека како основа на системот може да се земе кој било позитивен природен број различен од еден. За таа цел ќе ни послужи следново тврдење:

1°. Нека b е фиксен позитивен природен број различен од еден. Секој природен број a може да се претстави во облик

$$a = b^n b_n + b^{n-1} b_{n-1} + \ldots + b\, b_1 + b_0, \tag{1}$$

каде што $0 \leqslant b_i < b$ за секое i: $0 \leqslant i \leqslant n$. Ако $b_n \neq 0$, тогаш низата $b_0, b_1, \ldots, b_n$ е еднозначно определена.

Доказ. Тврдењето е очигледно точно за $a \leqslant b$. Да претпоставиме точност за сите природни броеви a: $a < c$. При делењето на c со b нека се добие количник d и остаток b_0. Според тоа, имаме $c = db + b_0$, каде што $0 < d < c$ и $0 \leqslant b_0 < b$. Од индуктивната претпоставка следува дека d може да се претстави во облик

$$d = b^{n-1} b_n + b^{n-2} b_{n-1} + \ldots + b\, b_2 + b\ ,$$

каде што $0 \leqslant b_i < b$. Од последното равенство, ако се има предвид и равенството $c = db + b_0$, се добива дека е точно равенството (1) и за $a = c$.

Ако $a = b^m c_m + b^{m-1} c_{m-1} + \ldots + bc_1 + c_0$ е друго претставување на бројот a, јасно е дека b_0 и c_0 се остатоци што се добиваат при делењето на a со b, па, според тоа, имаме $c_0 = b_0$. Потоа, кратејќи со b, добиваме $c_1 = b_1$, итн., ќе добиеме $m = n$, $c_m = b_n$. ▒

Од докажаното тврдење следува дека ако $b > 1$, тогаш, избирајќи b знаци (нив ќе ги наречеме *цифри*) за првите b природни броеви, можеме секој природен број a да го претставиме во облик (1), или пократко

$$a = b_n\, b_{n-1} \ldots b_1\, b_0.$$

Притоа, на десната страна имаме само нанижување на цифри, а не множење, т.е. $b_n\, b_{n-1} \ldots b_1\, b_0$ се пишува наместо десната страна од равенството (1). Во тој случај велиме дека работиме во *позиционен броен систем со основа* b. За $b = 10$ имаме *десетичен систем*, а *бинарен* за $b = 2$.

Да разгледаме неколку примери.

1) Ако основата е два, тогаш нулата и единицата се означуваат, како досега, со 0 и 1, а сите други природни броеви се изразуваат со нивна помош. Така, бројот 1010111 е бројот $2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 87$.

Се разбира, не би смееле да пишуваме $1010111 = 87$, бидејќи левата страна е претставена во бинарен, а десната во десетичен систем. Горното равенство би можеле да го напишеме во облик: $1010111_2 = 87$, при што отсуството на индекс на десната страна кажува дека се работи за десетичен систем.

2) Во систем со основа три, имаме три цифри 0, 1, 2 кои го имаат обичното значење. Во овој случај би имале, на пример, $2101_3 = 64$.

3) Во обичниот, т.е. десетичниот, систем имаме десет цифри: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, но ако сакаме основата на системот да е поголема од десет, на пример, $b =$ дванаесет, тогаш е потребно за десет и единаесет да избереме специјални знаци; на пример, десет $=$ **L**, единаесет $=$ Λ.

Да истакнеме дека за која било основа b (> 1) имаме: $b = 10$ и

$$b^n = 1 \cdot b^n + 0 \cdot b^{n-1} + \ldots + 0 \cdot b + 0 = \underbrace{1000\ldots0}_{n}. \tag{2}$$

Затоа, до крајот на овој дел, со 10 ќе ја означуваме основата b на систем, што не значи дека мора да биде $b =$ десет.

Правилата за собирање, одземање, множење и делење на броеви во десетичен систем му се познати на секој ученик од основно училиште. Истите правила важат за систем при која било основа, како што ќе покажеме подолу.

Нека броевите x и y се определени со:

$$x = x_n\, x_{n-1} \ldots . x_1 x_0,\quad y = y_m\, y_{m-1} \ldots . y_1\, y_0, \tag{3}$$

каде што $0 \leqslant x_i,\ y_j < 10$. Ако притоа, на пример, $n > m$, можеме да ставиме $y_{m+1} = \ldots = y_n = 0$, па затоа можеме да сметаме дека $m = n$. Тогаш имаме:

$$x + y = 10^n\,(x_n + y_n) + \ldots + 10\,(x_1 + y_1) + x_0 + y_0. \tag{4}$$

Да ставиме:

$$z_0 = 0,\ x_i + y_i + z_i = 10\, z_{i+1} + u_i,\ u_{n+1} = z_{n+1}. \tag{5}$$

Добиваме:

$$x + y = 10^{n+1}\, u_{n+1} + 10^n\, u_n + \ldots + 10\, u_1 + u_0, \tag{6}$$

каде што $0 \leqslant u_i < 10$, $u_{n+1} = 0$ или 1. Со тоа го докажавме следново „*правило за собирање*“:

2°.
$$\begin{array}{r} z_n\ z_{n-1} \quad\ldots\quad z_1\ z_0 \\ x_n\ x_{n-1} \ldots x_1\ x_0 \\ +\ y_n\ y_{n-1} \ldots y_1\ y_0 \\ \hline u_{n+1}\ u_n\ u_{n-1} \ldots u_1\ u_0 \end{array},$$

каде што z_i, u_j се определени со (5).

(Да забележиме дека во пракса z_i, u_j ги определуваме усно.)

4) Еве еден пример:

$$\begin{array}{r} 23415_6 \\ +\ 4512_6 \\ \hline 32331_6 \end{array}$$

Правилото за одземање се сведува на докажаното правило за собирање, со тоа што постапката се спроведува во обратен редослед. И тоа да го илустрираме со еден пример.

5) $$\begin{array}{r} 648123_9 \\ -\ 233457_9 \\ \hline 414555_9. \end{array}$$

Ако бројот

$$x = x_n\, x_{n-1} \ldots x_1 x_0 = 10^n\, x_n + \ldots + 10\, x_1 + x_0,$$

го помножиме со $b^m = 10^m$ добиваме:

$$10^m \times x = 10^{m+n}\, x_n + \ldots + 10^m\, x_0 + 10^{m-1}\, 0 + \ldots + 10 \cdot 0 + 0$$

$$= x_n \ldots x_1\, x_0 \underbrace{0\,0 \ldots 0}_{m}.$$

Во овој дел, понатаму, множењето ќе го означуваме со "$\times$", бидејќи точката ќе има улога на "нанижување" цифри.

Според тоа:

3°. Еден број x се множи со 10^m на тој начин, што "оддесно" му се допишува низа од m нули.

Лесно се покажува и следново правило за множење со едноцифрен број.

4°. Ако $x = x_n \ldots x_1\, x_0$, $0 < y < 10$, тогаш:

$$x \times y = u_{n+1} \ldots u_1\, u_0,$$

каде што:

$$z_0 = 0,\ x_i\, y + z_i = 10\, z_{i+1} + u_i,\ 0 \leqslant u_i < 10.$$

6) $237_8 \times 5 = 1433_8$,

бидејќи: $5 \times 7 = 4 \times 10 + 3$, $5 \times 3 + 4 = 2 \times 10 + 3$, $5 \times 2 + 2 = 1 \times 10 + 4$.

Со комбинација на својствата **2°**, **3°** и **4°** се добива соодветното правило за множење на повеќецифрени броеви, но тоа правило нема да го формулираме, а само ќе го илустрираме со еден пример.

7) $237_8 \times 45_8 = 237_8 \times (10 \cdot 4 + 5)$
$= 2370_8 \times 4 + 237_8 \times 5$
$= 11740_8 + 1433_8$
$= 13373_8$

Пократко:

$$\begin{array}{r} 237_8 \times 45_8 = 1433 \\ + \quad 1174 \\ \hline 13373_8 \end{array}$$

Пред да го формулираме правилото за определувањето на остатокот и количникот што се добиваат при делење на еден број со друг, да одговориме на прашањето како се споредуваат два броја.

5°. Нека $x = x_n \ldots x_1 x_0$, $y = y_m y_{m-1} \ldots y_1 y_0$, каде $x_n \neq 0$, $y_m \neq 0$. Тогаш: $x < y$ акко е исполнет некој од следниве услови:

(i) $n < m$;

(ii) $n = m$, $x_n < y_m$;

(iii) $n = m$, $x_n = y_n, \ldots, x_{k+1} = y_{k+1}$, $x_k < y_k$, за некој k: $0 \leqslant k < n$.

Доказот на основната теорема за делење со остаток го дава и правилото за определување на остатокот и количникот што се добиваат при делење на еден број со друг.

6°. Нека q е количникот, а r остатокот што се добиваат при делењето на бројот x со y. Тогаш:

(i) Ако $x < y$, имаме $q = 0$ и $r = x$.

(ii) Ако $x \geqslant y$, q е најмалиот природен број со својството $x < (q+1)y$, а r е $x - qy$.

8) Така, ако $x = 437_8$, $y = 56_8$, тогаш: $y < x$; $2 \cdot y = 134_8$, $3 \cdot y = 212_8$, $4 \cdot y = 270_8$, $5 \cdot y = 346_8$, $6 \cdot y = 424_8$, $7 \cdot y = 502_8$. Според тоа, $q = 6$, и $r = x - 6 \cdot y = 437_8 - 424_8 = 13_8$.

Изнесеното правило не е практично и тоа се користи многу ретко. Почесто се користи друго правило, познато уште од основното училиште, а е последица на тврдењето што ќе го докажеме сега.

7°. Нека x и y се два природни броја, и нека:

(i) $x = 10u + x_0$, $0 \leqslant x_0 < 10$, т.е. x_0 е последна цифра на x, а u е бројот што се добива од x кога ќе се изостави последната цифра x_0.

(ii) $u = q_1 y + r_1$, $0 \leqslant r_1 < y$.

(iii) $10r_1 + x_0 = q_2 y + r_2$, $0 \leqslant r_2 < y$.

Тогаш, количникот q и остатокот r што се добиваат при делењето на x со y се определени со:

$$q = 10q_1 + q_2, \quad r = r_2, \tag{*}$$

и притоа q_2 е последна цифра на q.

Доказ. Од (i), (ii), и (iii) веднаш се добива:

$$\begin{aligned} x = 10u + x_0 &= 10(q_1 y + r_1) + x_0 \\ &= 10q_1 y + 10r_1 + x_0 = 10q_1 y + q_2 y + r_2 \\ &= (10q_1 + q_2)y + r_2, \end{aligned}$$

од каде следуваат равенствата (*). За да се докаже дека q_2 е последна цифра на q треба уште да се покаже дека $q_2 < 10$. Навистина, од $r_1 < y$, следува $10r_1 \leqslant 10(y - 1) = 10y - 10$, па и $10r_1 + x_0 < 10y$. ∎

Докажаното тврдење укажува како, наместо со x, може да се работи со бројот u кој има една цифра помалку од x. Потоа, истата постапка би требало да се спроведе и за u. Правилото за кое стана збор погоре, практично, изгледа вака: ако бројот x има облик

$$x = b_n\, b_{n-1} \ldots b_1\, b_0,$$

и ако k е најголемиот број за кој е точна релацијата

$$y \leqslant b_n b_{n-1} \ldots b_k = t,$$

тогаш се определува прво количникот што се добива при делењето на t со y, при што се добива и остатокот. Потоа, се повторува истата постапка на бројот $b_n \ldots b_k\, b_{k-1}$ и, по конечно многу такви постапки, се доаѓа до бараниот резултат.

Да разгледаме еден пример.

9) $x = 4372_8$, $y = 27_8$.

Имаме: $43_8 = 1\times27_8 + 14_8$; $147_8 = 4\times27_8 + 13_8$; $132_8 = 3\times27_8 + 25_8$. Од сето тоа следува:

$$4372_8 = 143_8\times27_8 + 25_8.$$

Тоа шематски може да се изведе на следниов начин:

4372_8	$27_8 = 143_8$
147	
132	
25	

Во целиот овој дел работевме со природни броеви. Ако a е негативен, тогаш $c = -a$ е позитивен, па ако $c = c_n \ldots c_1c_0$, тогаш $a = -c_n \ldots c_1c_0$

ВЕЖБИ. 2. При декадниот (т.е. десетичниот) систем операциите ги изведуваме многу полесно, бидејќи ние и мислиме во тој систем. При тоа, многу ни помогнува фактот што ги знаеме резултатите што се добиваат при собирање и множење на едноцифрени броеви, т.е. ги знаеме *"малиште таблици"* за собирање и множење кај десетичниот систем. Да се состават аналогни таблици за собирање и множење на едноцифрени броеви во системи со основа: два, четири, девет и дванаесет.

3. Да се извршат означените операции:

а) $1001_2 + 1011_2$; б) $1001_2 \times 10101_2$;

б) $100111_2 - 111101_2$; г) $3421_5 \times 2412_5$;

д) $2381_9 + 312_8$.

4. Бројот 1296 (даден во десетичен систем) да се претстави во системи со основа: два, четири, пет; дванаесет.

5. Користејќи го идентитетот

$$(ab + c)^2 = a^2b^2 + c(2ab + c)$$

да се формулира правилото за квадрирање на повеќецифрени броеви. Користејќи го добиеното правило, да се извршат следниве квадрирања: 11011_2^2; 246_8^2; 24126_7^2.

6. Да се даде правило за множење на броеви кои имаат последни цифри чиј збир е десет, а сите други цифри им се исти. Овој резултат да се искористи за да се извршат "усно" следниве множења: $26\cdot24$; $46\cdot44$; $98\cdot92$; $101\cdot109$; $123\cdot127$; $146\cdot144$; $85\cdot85$; $115\cdot115$.

Дали е битно тоа што се работи во десетичен систем?

7. Да се определи во каков броен систем е точно равенството:

а) $4\times13 = 100$; б) $3\times25 = 141$;

в) $5\times36 = 114$; г) $12! - 11! = 100^2 + 10^2$.

8. Да се определи основата на системот ако $722_b - 554_b = 133$, каде што 133 е во десетичен систем.

9. Еден број претставен во десетичен систем се дели со: а) 2; б) 3; в) 4; г) 5; д) 6; ѓ) 8; е) 9; ж) 10, акко:

а) неговата последна цифра се дели со 2;

б) збирот на неговите цифри се дели со 3;

в) бројот формиран од неговите последни две цифри се дели со 4;
г) неговата последна цифра е 0 или 5;
д) тој се дели и со 2 и со 3;
ѓ) бројот формиран од неговите последни три цифри се дели со 8;
е) збирот на неговите цифри се дели со 9;
ж) неговата последна цифра е 0.

3.7. НАЈГОЛЕМ ЗАЕДНИЧКИ ДЕЛИТЕЛ И НАЈМАЛ ЗАЕДНИЧКИ СОДРЖАТЕЛ

Нека $a, b \in \mathbf{Z}^+$. Множествата делители на дадените броеви не се дисјунктни, бидејќи 1 е делител и на a и на b. Најголемиот број што е делител и на a и на b го означуваме со $(a;b)$ и велиме дека тоа е *најголемиот заеднички делител* на a и b. Со $[a;b]$ ќе го означуваме најмалиот позитивен природен број што се дели и со a и со b; велиме дека $[a;b]$ е *најмал заеднички содржател* на a и b. Од дадените дефиниции е јасно дека се точни следните тврдења.

1°. (i) $(a;b) = (b;a)$, $[a;b] = [b;a]$;

(ii) $(a;b) = a \Leftrightarrow a \mid b$

$\Leftrightarrow [a;b] = b$;

(iii) $(a;b) \leqslant a$, $[a;b] \leqslant ab$.

Ќе докажеме неколку својства во врска со поимот најголем заеднички делител.

2°. Нека a и b се природни броеви и нека $d = ua + vb$ е најмалиот позитивен природен број од обликот $xa + yb$, каде што x и y се цели броеви. Тогаш имаме $d = (a;b)$, а секој заеднички делител на a и b е делител и на d.

Доказ. Ако x и y се природни броеви, тогаш таков е и бројот $xa + yb$, па значи постојат позитивни природни броеви од овој облик, од што следува дека меѓу нив има и најмал број $d = ua + vb$. Нека при делењето на a со d се добие количник q и остаток r, т.е. $a = qd + r$, каде што $0 \leqslant r < d$. Притоа имаме $r = (1 - uq)a + (-vq)b$, од што следува дека $r = 0$, бидејќи во спротивност r би бил позитивен природен број помал од d, а од обликот $xa + yb$. Слично се докажува дека d е делител и на b.

Нека $a = a_1 d_1$, $b = b_1 d_1$, т.е. d_1 е некој заеднички делител на a и b. Тогаш имаме $d = d_1(ua_1 + vb_1)$. т.е. d_1 е делител и на d. Од тоа следува дека d се дели со секој заеднички делител на a и b, па, според тоа, d е најголемиот заеднички делител на a и b.

За броевите a и b велиме дека се *заемно прости* акко $(a;b) = 1$, т.е. акко бројот 1 е единствениот заеднички природен делител на a и b.

3°. Нека $(a;b) = 1$. Од $a \mid bc$ следува $a \mid c$.

Доказ. Според својството **2°**, постојат цели броеви u и v, така што $1 = au + bv$. Тогаш имаме $c = auc + bcv = a(uc + kv)$, каде што $bc = ka$. Од сето тоа следува $a \mid c$. ∎

4°. Ако $(a;b) = d$, $a = a_1 d$, $b = b_1 d$, тогаш $(a_1;b_1) = 1$.

Доказ. Ако $(a_1;b_1) = d_1$, тогаш dd_1 е заеднички делител на a и b, од што следува дека dd_1 е делител и на d, но тоа е можно само за $d_1 = 1$. ∎

5°. $(a;b) \cdot [a;b] = a \cdot b$

Доказ. Нека $(a;b) = d$, $a = a_1 d$, $b = b_1 d$. Јасно е дека a и b се делители на $a_1 b_1 d = a_1 b = a b_1 = c$. Од тоа следува дека $[a;b] \leqslant c$; ќе покажеме дека важи равенството, од што ќе следува точноста на тврдењето. Нека $[a;b] = ax = by$. Тогаш: $a_1 d \mid d b_1 y$, т.е. $a_1 \mid b_1 y$, од што, според **3°** и **4°**, следува $a_1 \mid y$, така што, $y = a_1 z$. Со тоа покажавме дека $[a;b] = b a_1 z = cz$, т.е. $c \leqslant [a;b]$, од што следува $[a;b] = c$

6°. Ако r е остатокот што се добива при делењето на бројот a со бројот b $(b \neq 0)$, тогаш имаме $(a;b) = (b;r)$.

Доказ. Од $a = qb + r$ е јасно дека секој заеднички делител на b и r е делител и на a, а, исто така, и дека секој заеднички делител на a и b е делител и на r. Според тоа, имаме $(a;b) = (b;r)$. ∎

7°. Нека a и b се позитивни природни броеви такви што $b < a$, и нека ставиме $c_0 = a$, $c_1 = b$. Потоа, ако $0 < c_i < c_{i-1}$, со c_{i+1} го означуваме остатокот што се добива при делењето на c_{i-1} со c_i. Тогаш, постои k таков што $c_{k+1} = 0$, $c_k > 0$ и во тој случај имаме:

$$c_k = (a;b).$$

Доказ. Од тоа што: $c_0 > c_1 > \ldots > c_{i-1} > c_i > \ldots$ следува дека постои $k \in \mathbf{N}^+$, таков што $c_k > 0$, $c_{k+1} = 0$. Тогаш:

$$(a;b) = (c_0;c_1) = (c_1;c_2) = \ldots = (c_{k-1};c_k) = c_k.$$ ∎

Последното тврдење е познато под името *Евклидов алгоритам* за наоѓање најголем заеднички делител на два броја. Инаку под *алгоритам* се подразбира правило според кое со помош на конечно многу постапки се решава "секоја задача од едно множество задачи". Во оваа смисла во **3.6.2° — 3.6.7°** се формулирани соодветни алгоритми.

Да разгледаме еден конкретен пример.

1) Нека $a = 1280$, $b = 520$. Имаме:

$$1280 = 2 \cdot 520 + 240$$
$$520 = 2 \cdot 240 + 40$$
$$240 = 6 \cdot 40 + 0.$$

Според тоа, $(1280;\ 520) = 40$.

Поимите најголем заеднички делител, односно најмал заеднички содржател, можат да се дефинираат и за случај на негативни броеви и тоа на следниов начин:

$$(-a;b) = (-a;-b) = (a;-b) = (a;b)$$

$$[-a;b] = [-a;-b] = [a;-b] = [a;b],$$

каде што $a, b \in \mathbf{Z}^+$. Ако $a \in \mathbf{Z}^+$, тогаш е природно да се стави

$$(a;0) = (-a;0) = (0;a) = (0;-a) = a,$$

но (0;0) не се дефинира. Исто така, не се дефинира ни $[a;b]$ ако $a = 0 \vee b = 0$.

ВЕЖБИ. **2.** Да се определат $(a; b)$ и $[a; b]$ ако: а) $a = 240$, $b = 192$; б) $a = 1000$, $b = 450$. Потоа, да се определат цели броеви x и y, така што $(a; b) = ax + by$.

3. Да се определат броевите x и y ако се знае дека:

а) $(x; y) = 15$, $[x; y] = 150$; б) $(x; y) = 120$, $[x; y] = 1320$; в) $(x; y) = 100$, $[x; y] = 990$.

4. Ако $a, b, c \in \mathbf{Z}$, $(a \neq 0 \vee b \neq 0)$, тогаш $[(\exists x, y)\ ax + by = c] \Leftrightarrow (a; b) \mid c$.

5. Ако $(a; b) = 1$, $c \in \mathbf{Z}$, $ax_0 + by_0 = c$, тогаш:

$$ax + by = c \Leftrightarrow (\exists t)\ (x = x_0 - bt,\ y = y_0 + at).$$

6. Да се решат, во цели броеви, равенките:

а) $8x - 13y = 63$; б) $39x - 22y = 10$;

в) $122x + 129y = 2$; г) $258x - 172y = 56$;

д) $x^2 - y^2 = 2xyz$.

7. За превоз на жито има вреќи од 60 и 80 кг. По колку вреќи од едниот и од другиот вид треба да се наполнат за да се превезе 440 кг. жито?

8. Колку марки по 30 и 50 пари можат да се купат со 14 динари и 90 пари?

9. Ако a е позитивен цел број, тогаш да го означиме со D_a множеството од сите позитивни цели, броеви што се делители на a, а со F_a множеството од сите позитивни цели броеви за кои a е делител. Тогаш, имаме:

(i) $D_a \cap D_b = D_{(a; b)}$;

(ii) $F_a \cap F_b = F_{[a; b]}$.

10. Со помош на резултатите од претходната вежба (или директно) да се докаже дека: ако a, b, c се позитивни природни броеви, тогаш:

(i) $(a; (b; c)) = ((a; b); c)$,
$[a; [b; c]] = [[a; b]; c]$;

(ii) $(a; [b; c]) = [(a; b); (a; c)]$, $[a; (b; c)] = ([a; b]; [a; c])$;

(iii) $(ab; ac) = a(b; c)$, $(c; b) = (a; b + ac) = (a + kb; b)$;

(iv) $(a; b) = 1 \wedge (a; c) = 1 \Rightarrow (a; bc) = 1$;

(v) $(a; b) = 1 \Rightarrow (a^n; b^n) = 1$.

3.8. ПРОСТИ БРОЕВИ

Ако $n \in \mathbf{N}^+ = \mathbf{Z}^+$, тогаш множеството позитивни делители на n е конечно, бидејќи е подмножество од $\mathbf{N}_n^+$. Да го означиме со $\tau(n)$ бројот на сите (различни) позитивни делители на n. Ако се има предвид тоа што 1 и n се делители на n, добиваме дека:

1°. (i) $\tau(1) = 1$. (ii) $n \geqslant 2 \Rightarrow \tau(n) \geqslant 2$.■

За природниот број n велиме дека е *прост* акко $\tau(n) = 2$, а *сложен* акко $\tau(n) \geqslant 3$. Од ова следува дека бројот 1 не е ни прост, ни сложен и дека секој природен број поголем од 1 е или прост или сложен, но не и едно и друго.

Да забележиме дека бројот два е најмалиот прост број, а четири најмалиот сложен број.

Како и во претходните делови, ќе работиме само со позитивни природни броеви, па затоа, тоа нема и да го спомнуваме специјално.

Ќе докажеме неколку својства на простите броеви.

2°. Секој број различен од 1 има барем еден прост делител.

Доказ. Нека $n \neq 1$ и нека p е најмалиот природен број што е делител на n и е различен од 1. Ќе покажеме дека p е прост. Навистина, ако p не би бил прост, би постоел број q, таков што $q|p$ и $1 < q < p$, но тоа не е можно, бидејќи тогаш q би бил делител на n и тоа помал од p.■

3°. Постојат бесконечно многу прости броеви и бесконечно многу сложени броеви.

Доказ. Нека P е множеството прости броеви. P не е празно, бидејќи, на пример, $2, 3 \in P$. (Да забележиме дека егзистенција на прости броеви следува индиректно и од **2°**). Ќе покажеме дека P е неограничено множество од што (според 1.7.**9°**) ќе следува дека е бесконечно.

Нека $p \in P$ и нека $\{p_0, p_1, \ldots, p_k (= p)\}$ е множеството од сите прости броеви што не се поголеми од p. Бројот $a = p_0 p_1 \ldots p_k + 1$, според **2°**, има барем еден прост делител q. Не може да биде $q = p_i$ за некое $i = 0, \ldots, k$, бидејќи тогаш би имале $1 = p_i (b - p_0 \ldots p_{i-1} p_{i+1} \ldots p_k)$, каде $a = qb$. Според тоа, имаме $p < q$. Со тоа докажавме дека P е неограничено, па, значи, и бесконечно.

На читателот му препуштаме да докаже и дека множеството сложени броеви е бесконечно.■

4°. Ако p е прост број и ако p не е делител на a, тогаш a и p се заемно прости.

Доказ. Нека $(a;p) = d$. Тогаш $d|p$ од што следува: $d = 1 \vee d = p$; не може да биде $d = p$, бидејќи p би бил делител на a.■

Нека простиот број p е делител на производот ab. Ако p не е делител на a, тогаш, според својството **4°**, имаме $(p;a) = 1$, а од тоа, според својството 3.7.3°, следува дека p е делител на b. Значи, точно е следново својство:

5°. Простиот број p е делител на производот ab акко е делител барем на еден од броевите a, b.

Нека $p, p_1, p_2, \ldots, p_k$ се прости броеви, и нека p е делител од производот $p_1p_2 \ldots p_k$. Од својството **5°** следува дека p е делител на p_1 или на $p_2p_3 \ldots p_k$. Ако $p \mid p_1$, тогаш имаме $p = p_1$. Ако тоа не биде исполнето, ќе имаме $p \mid p_2p_3 \ldots p_k$ и, по конечно многу повторувања на оваа постапка, ќе добиеме дека $p = p_i$ за некој $i : 1 \leqslant i \leqslant k$. Со тоа ја докажавме точноста на следново својство.

6°. Простиот број p е делител на производот $p_1p_2 \ldots p_k$, од простите броеви $p_1, p_2, \ldots, p_k$, акко $p = p_i$ за некој $i : 1 \leqslant i \leqslant k$.

Наредното својство, поради својата важност, добило име: *основна теорема на аритметиката*.

7°. Секој сложен природен број n може, на единствен начин, да се претстави како производ $n = p_1p_2 \ldots p_k$, каде што $p_1, p_2, \ldots, p_k$ се прости броеви, такви што $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$.

Доказ. Бројот 4 е најмалиот сложен природен број, а за него точноста на тврдењето е јасна. Да претпоставиме дека својството е точно за сите сложени броеви помали од сложениот број n, и да го означиме со p најмалиот делител на n, различен од 1. Според доказот на **2°**, p е прост број. Нека: $n_1 = n/p_1$, т.е. $n = n_1p_1$, каде што $p_1 = p$. Ако $n_1 = p_2$ е прост број, тогаш $n = p_1p_2$. Ако n_1 е сложен, тогаш од индуктивната претпоставка следува дека n_1 може да се претстави во облик $n_1 = p_2p_3 \ldots p_k$, каде што $p_2, p_3, \ldots, p_k$ е еднозначно определена низа прости броеви, таква што $p_2 \leqslant p_3 \leqslant \ldots \leqslant p_k$. Според тоа, имаме $n = p_1p_2 \ldots p_k$, каде што $p_1 \leqslant p_2$, бидејќи p_1 е најмалиот прост делител на n. Да претпоставиме дека n може да се претстави и во облик $n = q_1q_2 \ldots q_s$, каде што q_i се прости броеви, при што $q_i \leqslant q_{i+1}$. Тогаш p_1 е делител на производот $q_1q_2 \ldots q_s$, а од тоа, според својството **6°**, следува дека $p_1 = q_i$ за некој i, а со оглед на тоа што p_1 е најмалиот делител на n различен од 1 и претпоставката $q_i \leqslant q_{i+1}$, добиваме $p_1 = q_1$. Според тоа, имаме

$$n_1 = p_2p_3 \ldots p_k = q_2q_3 \ldots q_s,$$

од каде што, пак, според направената индуктивна претпоставка, следува $k = s$ и $p_i = q_i$.

Да напомнеме дека некои од факторите $p_1, p_2, \ldots, p_k$ на сложениот број n можат да бидат и еднакви. Ако таквите фактори ги групираме, бројот n ќе можеме да го претставиме во форма

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \tag{1}$$

каде што $p_i \neq p_j$ за $i \neq j$. За равенството (1) велиме дека е *канонично претставување* на бројот n.

ВЕЖБИ. **2.** Ако a, b, c се различни прости броеви поголеми од 3 и ако $a + c = 2b$, тогаш $6 \mid b - a$. Дали сите претпоставки се битни?

3. Ако $a, b \in \mathbf{N}^+$ и ако $2^a + 1$ и $2^b - 1$ се прости, тогаш a има облик $a = 2^k$, а b е прост.

4. Да се определи простиот број p, така што и $8p^2 + 1$ да биде прост.

5. Нека p, q, r и s се различни прости броеви. Да се определат броевите m и n, така што:

а) $(m; n) = pq$, $[m; n] = p^2 qs$;

б) $(m; n) = pq$, $[m; n] = qrs^2$.

6. Ако a е сложен природен број, тогаш постои прост делител p на a, таков што: $p^2 \leqslant a$.

7. Да ги напишеме сите природни броеви од 2 до n (во случајов е земено $n = 69$). 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69.

Тргнувајќи од 2, го прецртуваме секој втор број, оставајќи го 2 непрецртан; потоа, тргнувајќи од 3 (т.е. првиот непрецртан број), го прецртуваме секој трет број; потоа, оставајќи го бројот 5, го прецртуваме секој петти број итн., сé додека не дојдеме до положба кога ќе дојдеме до непрецртан број m таков што $m^2 \geqslant n$. Тогаш, еден природен број $p : p \leqslant n$ е прост акко не е прецртан. (Ова правило е познато под името: *Ератостеново сито*.) Според тоа, меѓу броевите помали од 70, прости се следниве: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67.

8. Да се определат сите прости броеви помали од 200.

9. Нека m и n се ненулти природни броеви и нека $p_1, p_2, \ldots, p_k$ е низата од првите k прости броеви, при што k е избран така, што во таа низа се наоѓаат сите прости делители на m и n. Тогаш m и n можат да се претстават во облици:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \quad \alpha_i, \beta_i \in \mathbf{N}.$$

Тогаш:

$$(m; n) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k},$$
$$[m; n] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}.$$

каде што γ_i е помалиот од броевите α_i, β_i, а δ_i е поголемиот од нив.

4. КОНГРУЕНЦИИ И ИЗОМОРФИЗМИ. ПРСТЕНИ. РАЦИОНАЛНИ БРОЕВИ

4.1. КОНГРУЕНЦИИ НА ГРУПОИДИ

Нека G е (мултипликативно означен) групоид, а α еквивалентност во G, т.е. во носителот на групоидот. Тогаш, според 1.5.(6), со:

$$G/\alpha = \{x^\alpha \mid x \in G\}$$

е определено фактормножеството на G по α, при што: $x \in x^\alpha$ и $(x^\alpha = y^\alpha \vee x^\alpha \cap y^\alpha = \emptyset)$. Природно е да се постави задача G/α да се претвори во групоид, со помош на операцијата на G. Се наложува следнава дефиниција на бараната операција:

$$(x^\alpha)(y^\alpha) = (xy)^\alpha \tag{1}$$

за секои $x, y \in G$.

Ќе покажеме дека:

1°. Со (1) е определена операција на G/α акко е исполнет следниов услов:

$$x \equiv u(\alpha),\ y \equiv v(\alpha) \Rightarrow xy \equiv uv(\alpha).^{1)} \tag{2}$$

Доказ. Да претпоставиме прво дека (2) е точно. Тогаш, ако $x^\alpha = u^\alpha$, $y^\alpha = v^\alpha$, имаме $x \equiv u(\alpha)$ и $y \equiv v(\alpha)$, од што, според (2), следува $xy \equiv uv(\alpha)$, т.е. $(xy)^\alpha = (uv)^\alpha$. Со тоа покажавме дека десната страна од (1) зависи само од класите x^α, y^α, а не и од нивните претставници x, y, т.е. дека со (1) е дефинирана операција на G/α.

Да претпоставиме сега дека со (1) е определена операција на G/α. Тогаш, ако

$$x \equiv u(\alpha) \text{ и } y \equiv v(\alpha), \text{ имаме } x^\alpha = u^\alpha,\ y^\alpha = v^\alpha,$$

па и $(xy)^\alpha = x^\alpha y^\alpha = u^\alpha v^\alpha = (uv)^\alpha$, од што следува:

$xy \equiv yv(\alpha)$, т.е. дека е исполнет условот (2). ∎

---

[1]) $a \equiv b\ (\alpha)$ се пишува наместо $a \alpha b$.

Секоја еквивалентност α што го има својството (2) се вика *конгруенција* на групоидот G. Тогаш, добиениот групоид G/α се вика *факторгрупоид* на G во однос на α.

Да разгледаме неколку примери.

1) Нека $G = \{e, a, b, c\}$ и нека групоидот е определен со шемата:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(Видовме во 2.7. дека G е комутативна група.)

Со $G/\alpha = \{\{e, a\}, \{b, c\}\}$, $G/\beta = \{\{e, a\}, \{b\}, \{c\}\}$ се определени две еквивалентности α и β во G. Притоа, β не е конгруенција, бидејќи, на пример, $e \equiv a(\beta)$, $b \equiv b(\beta)$, но $e \cdot b \not\equiv ab(\beta)$. Еквивалентноста α е конгруенција, и соодветниот факторгрупоид е определен со шемата:

	e^α	b^α
e^α	e^α	b^α
b^α	b^α	e^α.

2) Ако во $\mathbf{N}^+$ е определена релација α со: $x \equiv y\,(\alpha) \Leftrightarrow (x = 1,\ y = 1) \vee (x \neq 1,\ y \neq 1)$, добиваме конгруенција на полугрупата $\mathbf{N}^+(\cdot)$, а соодветниот факторгрупоид е определен со шемата:

	1	**2**
1	**1**	**2**
2	**2**	**2**

Притоа: $\mathbf{1} = \{1\}$, $\mathbf{2} = \{2, 3, 4, \ldots\} = \mathbf{N}^+ \setminus \{1\}$.

3) За секој групоид G, дијагоналата Δ и универзалната релација $G \times G = \rho$ се конгруенции и притоа:

$$G/\Delta = \{\{x\} \mid x \in G\},\ \{x\}\{y\} = \{xy\};$$

$$G/\rho = \{G\},\ GG = G.$$

Ќе видиме сега како некои својства на еден групоид G се пренесуваат и на неговите факторгрупоиди.

2°. Ако групоидот G е: а) комутативен, б) полугрупа, в) групоид со единица, г) група, тогаш соодветното својство го има и секој факторгрупоид на G.

Доказ. Нека α е конгруенција на G.

а) Ако G е комутативен, тогаш $(\forall x, y \in G)\ x^\alpha y^\alpha = (xy)^\alpha = (yx)^\alpha = y^\alpha x^\alpha$, т.е. и G/α е комутативен групоид.

б) Ако G е полугрупа, тогаш и G/α е полугрупа, бидејќи $(\forall x, y, z \in G)$.

$$x^\alpha (y^\alpha z^\alpha) = x^\alpha (yz)^\alpha = [x(yz)]^\alpha = [(xy)z]^\alpha = (x^\alpha y^\alpha) z^\alpha.$$

в) Ако e е единица во G, тогаш

$$(\forall x \in G)\ e^\alpha x^\alpha = (ex)^\alpha = x^\alpha,\ x^\alpha e^\alpha = (xe)^\alpha = x^\alpha,$$

т.е. e^α е единица на G/α.

г) Ако G е група, тогаш, според б) и в), G/α е полугрупа со единица e^α, каде што e е единица на G. Потоа: $(\forall x \in G)\ x^\alpha (x^{-1})^\alpha = (xx^{-1})^\alpha = e^\alpha$, од што следува дека секој елемент од G/α е инверзибилен, со што и покажуваме дека G/α е група. ∎

Од примерот 2) се гледа дека факторгрупоид на еден групоид со кратење не мора да е групоид со кратење.

ВЕЖБИ. 2. Ако $(\forall x, y \in G)\ xy = x$, тогаш секоја еквивалентност во G е конгруенција на групоидот.

3. Да се определат сите конгруенции на групата од примерот 1).

4. Ако α е конгруенција на полугрупата $\mathbf{N}(+)$, тогаш α е конгруенција и на $\mathbf{N}(\cdot)$.

5. Нека релацијата α во $\mathbf{N}$ е определена со: $x \equiv y\ (\alpha) \Leftrightarrow [x = y \vee (x \geqslant 3, y \geqslant 3, 4 \mid y - x)]$. Да се покаже дека α е конгруенција на $\mathbf{N}(+)$ и да се определат факторполугрупите $\mathbf{N}/\alpha\ (+)$, $\mathbf{N}/\alpha\ (\cdot)$.

6. Ако α е конгруенција на групата G, тогаш $x \equiv y\ (\alpha) \Leftrightarrow x^{-1} \equiv y^{-1}\ (\alpha)$.

7. Еквивалентноста α е конгруенција на групоидот G акко:

$$x \equiv y\ (\alpha) \Rightarrow xz \equiv yz\ (\alpha) \wedge zx \equiv zy\ (\alpha). \tag{3}$$

4.2. КОНГРУЕНЦИИ НА Z

За релацијата α велиме дека е *конгруенција на* $\mathbf{Z}$ акко е конгруенција и на двете полугрупи $\mathbf{Z}(+)$, $\mathbf{Z}(\cdot)$. Подолу ќе дадеме комплетен опис на фамилијата конгруенции на $\mathbf{Z}$, како и на соодветните факторгрупоиди.

Нека m е природен број. Ја определуваме релацијата α_m во $\mathbf{Z}$ со:

$$x\alpha_m y \Leftrightarrow m \text{ е делител на } x - y. \tag{1}$$

Ќе докажеме дека:

1°. За секој природен број m, α_m е конгруенција на $\mathbf{Z}$.

Доказ. Рефлексивноста на α_m следува од тоа што $m \mid 0$, за секој $m \in \mathbf{N}$. Потоа, ако $x\alpha_m y$, имаме $m \mid x - y$, па $m \mid y - x$, т.е. $y\alpha_m x$, од што следува дека α_m е и симетрична. Ако $x\alpha_m y$ и $y\alpha_m z$, тогаш $m \mid x - y$ и $m \mid y - z$, од што следува дека m е делител и на $(x - y) + (y - z) = x - z$, т.е. дека $x\alpha_m z$. Со тоа покажавме дека α_m е еквивалентност.

Нека $x\alpha_m u$ и $y\alpha_m v$. Тогаш постојат цели броеви s и t, такви што $x - u = sm$, $y - v = tm$. Од последниве равенства следува:

$(x + y) - (u + v) = (s + t)\, m$, т.е. $(x + y)\, \alpha_m\, (u + v)$ и $xy - uv = (sv + tu + tsm)\, m$, т. е. $(xy)\, \alpha_m\, (uv)$. Со тоа покажавме дека α_m е и конгруенција.■

Понатаму, ќе пишуваме

$$x \equiv y\ (mod\ m), \tag{2}$$

наместо $x\alpha_m y$, односно $x \equiv y\ (\alpha_m)$. Соодветното фактормножество $\mathbf{Z}/\alpha_m$ ќе го означуваме со $\mathbf{Z}_m$.

Имајќи го предвид тоа што 1 е делител на секој цел број, како и: $0 \mid x \Leftrightarrow x = 0$, добиваме дека: $\alpha_0 = \Delta_{\mathbf{Z}}$, $\alpha_1 = \mathbf{Z} \times \mathbf{Z}$ од што следува:

2°. (i) $\mathbf{Z}_0 = \{\{x\} \mid x \in \mathbf{Z}\}$, $\{x\} + \{y\} = \{x + y\}$, $\{x\} \cdot \{y\} = \{x \cdot y\}$

(ii) $\mathbf{Z}_1 = \{\mathbf{Z}\}$, $\mathbf{Z} \cdot \mathbf{Z} = \mathbf{Z} = \mathbf{Z} + \mathbf{Z}$.■

Ќе покажеме дека:

3°. Ако $m \geqslant 1$, тогаш $x \equiv y\ (mod\ m)$ акко остатоците што се добиваат при делењето на x и y со m се еднакви.

Доказ. Нека $x = q_1 m + r_1$, $y = q_2 m + r_2$, каде што $0 \leqslant r_1,\ r_2 < m$. Ако $r_1 = r_2$, тогаш имаме: $x - y = (q_1 - q_2)\, m$, т.е. $x \equiv y\ (mod\ m)$. Обратно, ако $x \equiv y\ (mod\ m)$, тогаш, $x - y = km$ за некој $k \in \mathbf{Z}$, така што $r_1 - r_2 = x - y + (q_2 - q_1)\, m = m\,(k + q_2 - q_1)$, од што следува $r_1 = r_2$.■

Сега лесно ќе го определиме обликот на множеството $\mathbf{Z}_m$. Ако $i \in \{0,1,\ldots, m-1\}$, ќе ја означиме со i_m класата на еквивалентоста α_m, таква што $i \in i_m$. Ако $x \in \mathbf{Z}$ и ако при делењето на x со m се добива остаток r, тогаш, според **3°**, имаме $x \equiv r(m)$, т.е. $x \in r_m$. Според тоа:

4°. (i) $\mathbf{Z}_m = \{0_m, 1_m, \ldots, (m-1)_m\}$

(ii) Ако при делењето на $i + j$ со m се добива остаток r, а при делењето на $i \cdot j$ со m се добива остаток s, тогаш:

$$i_m + j_m = r_m,\ i_m \cdot j_m = s_m.$$■

Ако m е фиксен број, тогаш ќе пишуваме i, наместо i_m. Според тоа:

$$\mathbf{Z}_m = \{0,1,\ldots, m-1\}. \tag{3}$$

Да ги напишеме шемите на операциите собирање и множење за $\mathbf{Z}_3$ и $\mathbf{Z}_4$.

$\mathbf{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbf{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Од тврдењето што сега ќе го докажеме следува дека со $\{\alpha_m \mid m \in \mathbf{N}\}$ се исцрпува множеството конгруенции на $\mathbf{Z}$.

4°. ρ е конгруенција на $\mathbf{Z}$ акко $\rho = \alpha_m$, за некој $m \in \mathbf{N}$.

Доказ. Ако $\rho = \alpha_m$, за некој $m \in \mathbf{N}$, тогаш ρ е конгруенција според **1°**.

Нека ρ е конгруенција на $\mathbf{Z}$. Ако $\rho = \Delta$, тогаш $\rho = \alpha_0$, според **2°**. Затоа, ќе претпоставуваме дека $\rho \neq \Delta$. Тогаш, постојат a, $b \in \mathbf{Z}$, такви што $a \neq b$ и $a \equiv b(\rho)$. Имајќи го предвид тоа што $-a \equiv -a(\rho)$ и $-b \equiv -b(\rho)$, добиваме $0 \equiv (b-a)(\rho)$ и $a - b \equiv 0(\rho)$, па, според тоа, постои природен број m, таков што $m \equiv 0(\rho)$, $m \neq 0$; да го означиме со m најмалиот природен број со овие својства.

Нека $x \equiv y(\rho)$, тогаш $x - y \equiv 0(\rho)$; ако $x - y = qm + r$, $0 \leqslant r < m$, тогаш $qm \equiv 0(\rho)$, па, значи, $x - y \equiv r(\rho)$, т.е. $r \equiv 0(\rho)$, од што следува $r = 0$. Според тоа: $x \equiv y(\rho)$ повлекува $x \equiv y(mod\ m)$.

Обратно, ако $x \equiv y(mod\ m)$, тогаш според **3°**: $x = q_1 m + r$, $y = q_2 m + r$, па, ако се има предвид тоа што $m \equiv 0(\rho)$, добиваме $x \equiv r(\rho)$, $y \equiv r(\rho)$, од што конечно следува $x \equiv y(\rho)$. ∎

Од својството 4.1.**2°** (имајќи предвид дека $\mathbf{Z}(+)$ е комутативна група, а $\mathbf{Z}(\cdot)$ комутативна полугрупа со единица 1), следува дека:

5°. За секој природен број $m \geqslant 2$, $\mathbf{Z}_m(+)$ е комутативна група, а $\mathbf{Z}_m(\cdot)$ комутативна полугрупа со единица $1(= 1_m)$. ∎

Конгруенциите на $\mathbf{Z}$ наоѓаат примена и кај испитување деливоста на целите броеви, како што се гледа од следните примери.

1) Нека $x = 98302416$. Да го определиме остатокот што се добива при делењето на x со 11. Имаме:

$$\begin{aligned} x &= 9 \cdot 10^7 + 8 \cdot 10^6 + 3 \cdot 10^5 + 2 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10 + 6 \\ &\equiv 9 \cdot (-1)^7 + 8(-1)^6 + 3(-1)^5 + 2(-1)^3 + 4(-1)^2 + 1 \cdot (-1) + 6 \\ &\equiv -9 + 8 - 3 - 2 + 4 - 1 + 6 \\ &\equiv 3(mod\ 11) \end{aligned}$$

$x \equiv 3 \pmod{11}$

Според тоа, при делењето на x со 11 се добива остаток 3.

2) Да ја разгледаме задачата за определување на остатокот што се добива при делењето на $y = 17^{99}$ со 13.

Од $17 \equiv 4 (mod\ 13)$, прво добиваме:

$y \equiv 4^{99}$. Потоа: $4^3 \equiv -1 \Rightarrow (4^3)^{33} \equiv (-1)^{33}$ т.е. $4^{99} \equiv -1$.

Според тоа: $y \equiv 12$,т.е. при делењето на y со 13 се добива остаток 12.

3) Ќе дадеме и критериум за деливост на бројот $x = a_n a_{n-1} \ldots a_1 a_0$ со 7, при што $a_0, \ldots, a_n$ се цифрите на x. Имаме: $10 \equiv 3 (mod\ 7)$, $10^2 \equiv 2$

$10^3 \equiv -1$, $10^4 \equiv -3$, $10^5 \equiv -2$, $10^6 \equiv 1$, $10^7 \equiv 3$, $10^8 \equiv 2$, $10^9 \equiv -1$

од што следува:

$$x \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \\ - (a_9 + 3a_{10} + 2a_{11}) + \ldots \ (mod\ 7) \qquad (*)$$

Според тоа: x се дели со 7 акко десната страна од (*) се дели со 7.

Така, ако x е бројот од 1), тогаш:

$$x \equiv (6 + 3 \cdot 1 + 2 \cdot 4) - (2 + 3 \cdot 0 + 2 \cdot 3) + (8 + 3 \cdot 9) \\ \equiv -1 + 3 + 1 - 2 + 1 + 1 + 6 \\ \equiv 2 (mod\ 7)$$

па, значи, x не се дели со 7.

ВЕЖБИ. **2.** Да се определат келиевите шеми на $\mathbf{Z}_2(+)$, $\mathbf{Z}_2(\cdot)$, $\mathbf{Z}_5(+)$, $\mathbf{Z}_5(\cdot)$, $\mathbf{Z}_{10}(+)$, $\mathbf{Z}_{10}(\cdot)$.

3. Да се определи остатокот што се добива при делењето на x со y, ако:

а) $x = 10^{1024}$, $y = 5$; б) $x = 2^{87}$, $y = 223$; в) $x = 3^{36}$, $y = 77$.

4. Да се провери дали 7 е делител на:

а) 670012345302; б) 99901230542.

5. Бројот $x = a_n a_{n-1} \ldots a_2 a_1 a_0$ се дели со 11 акко $a_0 - a_1 + a_2 - \ldots + (-1)^n a_n$ се дели со 11.

6. Ако се искористи тоа што, за даден прост број p, имаме $p \mid \binom{p}{i}$ за $i \in \{1, 2, \ldots, p-1\}$, се добива дека $a^{p-1} \equiv 1 (mod\ p)$, за секој цел број a што не се дели со p. (Теорема на Ферма).

7. Секоја конгруенција на $\mathbf{Z}(+)$ е конгруенција и на $\mathbf{Z}(\cdot)$.

8. Да се решат равенките:

$$x^{100} = 0, \ x^2 + 3x + 1 = 0, \ x^3 + x^2 - 4x + 3 = 0,$$

како и системот равенки: $2x + 3y = 1$, $4x - 5y = 2$ во: а) $\mathbf{Z}_4$; б) $\mathbf{Z}_5$; б) $\mathbf{Z}_{15}$. (Притоа, треба да се има предвид тоа, што $m = 0$, $-i = m - i$ во $\mathbf{Z}_m$).

9. За секој позитивен природен број m постои група со m елементи.

10. α е конгруенција на $\mathbf{Z}(-)$ акко е конгруенција на $\mathbf{Z}(+)$.

4.3. ПРСТЕНИ

Нека на множеството A е определена низа операции: $(*, \circ, \square, \ldots.)$. Тогаш велиме дека $A(*, \circ, \square, \ldots.)$ е *алгебарска структура* со носител A. Досега се сретнавме со неколку такви алгебарски структури, кави што се, на пример, $\mathbf{N}(+, \cdot)$, $\mathbf{Z}(+, \cdot)$, $\mathbf{Z}(+, -, \cdot)$; ако $A = B(M)$ е булеанот на едно множество M, тогаш $A(\cap, \cup, \setminus, -)$ е алгебарска структура.

Овде ќе разгледаме специјална класа алгебарски структури со две операции, а тоа се прстените. Имено, алгебарската структура $R(+, \cdot)$ се вика *прстен* акко се исполнети следниве услови:

(I) $R(+)$ е комутативна група

(II) За секоја тројка $x, y, z \in R$ се точни равенствата:

$$x(y + z) = xy + xz, (x + y) z = x z + y z. \tag{1}$$

Операцијата $+$ се вика *собирање*, а $\cdot$ *мно ење*. Во оваа смисла, $R(+)$ се вика *адитивна група*, а $R(\cdot)$ *мултипликативен групоид* на прстенот. Десните страни на (1) би требало да се напишат во облик $(xy) + (xz)$, $(xz) + (yz)$, но заградите ги изоставуваме, бидејќи се договараме "множењето да сврзува повеќе од собирањето". Равенствата (1) се викаат *дистрибутивни закони*.

Како и кај групоидите, носителот R на прстенот $R(+, \cdot)$ ќе го викаме прстен.

Да разгледаме неколку примери.

1) $\mathbf{Z}(+, \cdot)$ е прстен. $\mathbf{N}(+, \cdot)$ не е прстен, бидејќи $\mathbf{N}(+)$ не е група.

2) Множеството R (тридимензионални) вектори е прстен во однос на обичните операции: собирање $(+)$ и векторско множење $(\times)$ на вектори.

3) Нека $G(+)$ е адитивно означена комутативна група и нека во G дефинираме множење со: $x \cdot y = 0$ за секои $x, y \in G$, каде што 0 е нулата на G. Добиената структура е прстен, бидејќи:

$$x(y + z) = 0 = xy + xz, \quad (x + y)\ z = 0 = xz + yz.$$

Овој прстен се вика *нулти прстен*.

Ако R е прстен, тогаш за нулата 0 на адитивната група $R(+)$ велиме дека е *нула* и на прстенот; во иста смисла, $-a$ е *спротивен* елемент на a, а разликата, $a - b$ се дефинира со: $a + (-b)$. Со други зборови, се што порано се договоривме за адитивно означени комутативни групи, важи и за адитивната група на еден прстен. (Да се види 2.7.).

Ќе докажеме неколку општи својства на прстените:

1°. Ако R е прстен, тогаш:

(i) $x0 = 0x = 0$; (ii) $x(-y) = (-x) y = -(xy)$;

(iii) $(-x)(-y) = xy$; (iv) $x(y - z) = xy - xz$, $(x - y)\ z = xz - yz$, за секои $x, y, z \in R$.

Исто така, точен е и следниов таканаречен *обопштен дистрибутивен закон*:

$$(x_1+\ldots+x_m)(y_1+\ldots+y_n)=x_1y_1+\ldots+x_1y_n+\ldots+x_my_1+\ldots+x_my_n \quad (1')$$

за секои $x_i,\ y_j \in R$.

Доказ. (i) Ако се има предвид тоа што 0 е нула за собирање и дистрибутивноста на множењето спрема собирањето, добиваме:

$$x0 + 0 = x0 = x(0 + 0) = x0 + x0,$$

од што, по кратењето со $x0$, се добива $x0 = 0$. На ист начин се докажува и дека $0x = 0$.

(ii) Користејќи го докажаното равенство, добиваме:

$$0 = x0 = x[y + (-y)] = xy + x(-y),$$

од што следува: $x(-y) = -(xy)$. Ако се искористи равенството $0y = 0$, на ист начин, се добива: $(-x)y = -(xy)$.

(iii) Според (ii), имаме:

$$(-x)(-y) = -[x(-y)] = -[-(xy)] = xy.$$

(iv) $x(y-z) = x[y + (-z)] = xy + x(-z) = xy + (-(xz)) =$
$= xy - xz.$

Обопштениот дистрибутивен закон (1′) се докажува со помош на дистрибутивните закони (1), како и асоцијативноста на собирањето. ∎

Равенствата (ii) дозволуваат да пишуваме $-xy$, наместо $-(xy)$, односно $(-x)y$.

Ако R е прстен и ако $n \in \mathbf{Z}$, $x \in R$, тогаш nx е еднозначно определен елемент од R. (Овој елемент, имено, е определен во адитивно означената комутативна група $R(+)$.) Попрецизно би било да употребиме различни ознаки за производот xy на два елемента од прстенот и "производот" nx на целиот број n и елементот x од прстенот, но, сепак, и двата вида производи ги означуваме на ист начин, бидејќи не постои опасност од недоразбирања. Ќе го докажеме следново тврдење:

2°. $n(xy) = (nx)y = x(ny)$,

за секои $n \in \mathbf{Z}$, $x,\ y \in R$.

Доказ. Поради $1x = x$, $(-1)x = -x$, $0x = 0$, горните равенства се точни за $n \in \{1, 0, -1\}$. Да претпоставиме точност за $n = k \in \mathbf{N}^+$. За $n = k + 1$ ќе имаме:

$$(nx)\,y = ((k+1)\,x)\,y = (kx + x)\,y = (kx)\,y + xy$$
$$= k\,(xy) + xy = (k+1)\,(xy) = n\,(xy),$$
$$x\,(ny) = x\,((k+1)\,y) = x\,(ky + y) = x\,(ky) + xy$$
$$= k\,(xy) + xy = n\,(xy),$$

т.е. добиваме точност за секој $n \in \mathbf{N}^+$.

Ако n е негативен цел број, тогаш $-n \in \mathbf{N}^+$, па

$$n\,(xy) = -((-n)\,(xy)) = -(((-n)\,x)\,y) =$$
$$= (-(-n)\,x)\,y = (nx)\,y,$$

а слично се добива и: $n\,(xy) = x\,(ny)$. ∎

Нека $R\,(+, \cdot)$ е алгебарска структура со две операции. За α велиме дека е *конгруенција* на $R\,(+, \cdot)$ акко е конгруенција на $R\,(+)$ и $R\,(\cdot)$, т.е. акко α е еквивалентност во R, таква што:

$$x \equiv u\,(\alpha),\ y \equiv v\,(\alpha) \Rightarrow x + y \equiv u + v\,(\alpha),\quad x \cdot y \equiv u \cdot v\,(\alpha). \tag{2}$$

Во тој случај, операциите собирање и множење на фактормножеството R/α се определуваат со:

$$x^\alpha + y^\alpha = (x + y)^\alpha,\ x^\alpha \cdot y^\alpha = (xy)^\alpha. \tag{3}$$

3°. Ако α е конгруенција на прстенот $R(+, \cdot)$, тогаш и факторструктурата $R/\alpha\,(+, \cdot)$ е прстен.

Доказ. Според 4.1.**2°**, $R/\alpha\ (+)$ е комутативна група. Потоа, имаме:

$$(\forall x, y, z \in R)\ x^\alpha\,(y^\alpha + z^\alpha) = x^\alpha\,(y + z)^\alpha = [x\,(y + z)]^\alpha$$
$$= (xy + xz)^\alpha = (xy)^\alpha + (xz)^\alpha$$
$$= x^\alpha\,y^\alpha + x^\alpha\,z^\alpha$$

т.е. го докажавме едниот од дистрибутивните закони, а на наполно ист начин се покажува и другиот дистрибутивен закон. ∎

Како последица се добива и дека:

4°. За секој природен број n, $\mathbf{Z}_n$ е прстен. (За $\mathbf{Z}_n$ велиме дека е *прстен од класи на остатоци.*) ∎

Како аналогија на поимот подгрупоид се добива поимот потпрстен. Имено, ако R е прстен и $P \subseteq R$, за P велиме дека е *потпрстен* на R акко P е прстен во однос на операциите собирање и множење, дефинирани во R. Поимот потпрстен може да се окарактеризира и на следниов начин:

5°. Подмножеството P од прстенот R е потпрстен акко се исполнети следниве услови:

(i) $0 \in P$; (ii) $x, y \in P \Rightarrow -x,\ x+y,\ x \cdot y \in P$.

Доказ. Ако P е потпрстен на R, тогаш $P(+)$ е подгрупа на $R(+)$, а $P(\cdot)$ подгрупоид на $R(\cdot)$, од што следува дека се исполнети условите (i) и (ii).

Обратно, ако се исполнети (i) и (ii) тогаш $P(+)$ е подгрупа на $R(+)$, а $P(\cdot)$ е подгрупоид на $R(\cdot)$. Групата $P(+)$ е комутативна, бидејќи таква е $R(+)$. Преостанува да се покаже дека се точни дистрибутивните закони. Но, од тоа што тие се точни за сите елементи од R, следува дека се точни и во P, бидејќи $P \subseteq R$. ∎

Да забележиме дека:

6°. За секој прстен R, $\{0\} = O$ и R се потпрстени. ∎

ВЕЖБИ. **2.** Нека $R = B(M)$ е булеанот на едно множество M. Ако ставиме:

$$XY = X \cap Y,\ X + Y = X \dot{-} Y,$$

за секои $X, Y \in R$, тогаш се добива прстен $R(+, \cdot)$ за кој велиме дека е *булов прстен* над M. (Да забележиме дека не е неопходно да употребуваме мултипликативна, односно адитивна ознака за операциите на еден прстен).

3. Имајќи ја предвид забелешката од претходната вежба, да се формулираат аксиомите што треба да ги задоволува алгебарската структура $A(*, \square)$ за таа да биде прстен. Да се уочи дека при тоа е важен редоследот по кој се напишани операциите во $(*, \square)$, т.е. дека се работи за подредена двојка операции.

4. (i) Ниедна од структурите $\mathbf{Z}(\cdot, +)$ $\mathbf{Z}(+, -)$, $\mathbf{Z}(-, \cdot)$, $\mathbf{Z}(\cdot, -)$ не е прстен.

(ii) Ако M е непразно и ако $R = B(M)$, тогаш ниедна од структурите: $R(\cup, \cap)$ $R(\cap, \cup)$, $R(\cap, \setminus)$, $R(\setminus, \cap)$, $R(\cup, \setminus)$, $R(\setminus, \cup)$, $R(\cup, \dot{-})$, $R(\dot{-}, \cup)$, $R(\cap, \dot{-})$, $R(\dot{-}, \setminus)$, $R(\setminus, \dot{-})$ не е прстен.

5. Ако $G(+, \cdot)$ е прстенот од примерот 3), тогаш:

(i) Секоја конгруенција на $G(+)$ е конгруенција на прстенот.

(ii) Секоја подгрупа на $G(+)$ е потпрстен.

6. Да се покаже дека $R(+, \cdot)$ е прстен. каде што:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$R = \{0, 1, a, b\}$.

7. Да се определат сите потпрстени на: *а)* $\mathbf{Z}_6$; б) $\mathbf{Z}_{12}$; *b)* $\mathbf{Z}_{13}$.

8. Едно подмножество P на $\mathbf{Z}$ е потпрстен акко постои природен број k, таков што $P = \{kx \mid x \in \mathbf{Z}\}$.

9. Пресек на потпрстени е потпрстен.

10. Во кој случај, унија на два потпрстени е потпрстен?

4.4. ВИДОВИ ПРСТЕНИ

Својствата на еден прстен зависат од својствата на неговата адитивна група, како и од неговиот мултипликативен групоид. Овде ќе ги класифицираме прстените според својствата на нивните мултипликативни групоиди. Така, за прстенот R се вели дека е: а) *комутативен*, б) *асоцијативен*, в) *прстен со единица* — акко соодветното својство го има неговиот мултипликативен групоид. Од прстените со кои се сретнавме во претходниот дел, сите три својства ги имаат $\mathbf{Z}$, $\mathbf{Z}_n$ (за секој природен број n), како и прстените од вежбите 4.3.2. и 4.3.6. Прстенот $G(+, \cdot)$ од 4.3.3) е комутативен и асоцијативен, но ако G има барем два различни елемента, овој прстен нема единица. Прстенот од примерот 4.3.2), т.е. прстенот од тридимензионални вектори, нема, ниедно од спомнатите својства.

Пред да се запознаеме со нови видови прстени, ќе докажеме две тврдења.

1°. Ако R е прстен со единица e и ако R има барем два различни елемента, тогаш $e \neq 0$.

Доказ. Да претпоставиме дека $e = 0$. Тогаш, за секој $x \in R$ имаме:

$$x = xe = x0 = 0,$$

т.е. $R = \{0\}$ е едноелементно множество. ∎

(Понатаму, секогаш кога ќе се работи за прстен R, ќе претпоставуваме дека R има и ненулти елементи, така што ако R има единица, тогаш таа е различна од нула.)

2°. Нека R е комутативен и асоцијативен прстен со единица. За секој позитивен природен број n и елементи $x, y \in R$ е точно равенството:

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + \ldots + \binom{n}{n-1} x y^{n-1} + y^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i, \tag{1}$$

познато како *биномна формула*.

Доказ. За $n = 1$, равенството (1) има облик $(x+y)^1 = x^1 + y^1$, па е очигледно, точно. Да претпоставиме точност за $n = k$. За $n = k+1$ имаме

$$
\begin{aligned}
(x+y)^n &= (x+y)^k\,(x+y)\\
&= (x^k + \binom{k}{1} x^{k-1}y + \ldots + \binom{k}{k-1} xy^{k-1} + y^k)\,(x+y)\\
&= x^{k+1} + \binom{k}{1} x^k y + \ldots + \binom{k}{k-1} x^2 y^{k-1} + xy^k + x^k y +\\
&\qquad \ldots + \binom{k}{k-2} x^2 y^{k-1} + \binom{k}{k-1} xy^k + y^{k+1}\\
&= x^{k+1} + \left[\binom{k}{1} + \binom{k}{0}\right] x^k y + \ldots + \left[\binom{k}{k-1} +\right.\\
&\left. + \binom{k}{k-2}\right] x^2 y^{k-1} + \left[\binom{k}{k-1} + \binom{k}{k}\right] xy^k + y^{k+1}\\
&= x^{k+1} + \binom{k+1}{1} x^k y + \ldots + \binom{k+1}{k-1} x^2 y^{k-1} +\\
&+ \binom{k+1}{k} xy^k + y^{k+1}\\
&= x^n + \binom{n}{1} x^{n-1}y + \ldots + \binom{n}{n-2} x^2 y^{n-1} +\\
&\qquad + \binom{n}{n-1} xy^{n-1} + y^n.
\end{aligned}
$$

(Да уочиме дека овде е искористено равенството $\binom{k}{i-1} + \binom{k}{i} = \binom{k+1}{i}$ докажано во 2.5. **9°**.)■

Како последица од 4.1.**2°**, се добива и следново тврдење:

3°. Ако прстенот R е: а) комутативен, б) асоцијативен, в) прстен со единица, тогаш соодветното својство го има и секој факторпрстен на R.■

Исто така, јасно е дека:

4°. Секој потпрстен од еден: а) комутативен, б) асоцијативен прстен, е прстен со истото својство.■

Но, еден потпрстен на прстен со единица не мора да има единица. На пример, $P = \{2x \mid x \in \mathbf{Z}\}$ е потпрстен на $\mathbf{Z}$, притоа $\mathbf{Z}$ има единица, додека P нема единица.

За еден прстен R велиме дека е *интегрален домен* акко R е комутативен и асоцијативен прстен со единица $e\,(\neq 0)$, таков што:

$$x \neq 0,\quad y \neq 0 \Rightarrow xy \neq 0. \tag{2}$$

[illegible] на R.

9. Ако R е поле, тогаш $\mathbf{Q}' = \{(xe)\,(ye)^{-1} \mid x, y \in \mathbf{Z},\ ye \neq 0\}$ е потполе на R и притоа, ако P е потполе на R, тогаш $\mathbf{Q}' \subseteq P$.

10. Ако p е прост број, тогаш $\mathbf{Z}_p$ е единственото потполе на $\mathbf{Z}_p$.

11. Пресек од потполиња на едно поле [illegible]

4.5. ИЗОМОРФИЗМИ

Нека G $(*)$ и $G'(\circ)$ се групоиди и f биекција од G во G'. За f велиме дека е *изоморфизам* од G $(*)$ во G' $(\circ)$ акко "слика од производ е производ на слики", т.е. акко:

$$f(x * y) = f(x) \circ f(y) \tag{1}$$

за секои $x, y \in G$. По обичај, и кај двата групоида нема да го пишуваме знакот на операцијата, така што (1) го добива следниов облик:

$$f(xy) = f(x)\, f(y). \tag{1'}$$

1°. Идентичното пресликување е изоморфизам од G во G.

Доказ. Ако $x, y \in G$, тогаш $1_G(xy) = xy = 1_G(x)\, 1_G(y)$, а 1_G е и биекција. ∎

2°. Ако $f : G \to G'$ е изоморфизам, тогаш и $f^{-1}: G' \to G$ е изоморфизам.

Доказ. Според 1.4.**8°**, f^{-1} е биекција. Нека $x', y' \in G'$ и $f^{-1}(x') = x$, $f^{-1}(y') = y$, т.е. $f(x) = x'$, $f(y) = y'$. Тогаш имаме:

$$f^{-1}(x')\, f^{-1}(y') = xy = f^{-1} f(xy) = f^{-1}(f(xy)) = \\ = f^{-1}(f(x)\, f(y)) = f^{-1}(x'\, y'). \text{∎}$$

3°. Ако $f : G \to G'$ и $g : G' \to G''$ се изоморфизми, тогаш и $h = gf$ е изоморфизам.

Доказ. h е биекција според 1.4. **7°**. Ако $x, y \in G$, тогаш:

$$h(xy) = gf(xy) = g[f(xy)] = g[f(x)\, f(y)] = \\ = g(f(x))\; g(f(y)) = h(x)\, h(y). \text{∎}$$

Велиме дека групоидот G е *изоморфен* со групоидот G' и пишуваме $G \cong G'$ акко постои изоморфизам f од G во G'.

Како последица од **1°**, **2°** и **3°**, добиваме:

4°. Ако G, G' и G'' се групоиди, тогаш: (i) $G \cong G$; (ii) $G \cong G' \Rightarrow G' \cong G$; (iii) $G \cong G'$, $G' \cong G'' \Rightarrow G \cong G''$. ∎

Изоморфизмите ги запазуваат сите алгебарски својства на групоидите. Овде нема да дадеме прецизна дефиниција на терминот *алгебарско својство*, но ќе се задоволиме само да кажеме дека тоа е *секое својство што се формулира со помош на операциите*. Следново својство е една илустрација на изнесениот став дека изоморфните групоиди имаат исти алгебарски својства.

5°. Ако групоидот G е: а) комутативен, б) полугрупа, в) групоид со единица, г) група, д) групоид со кратење, тогаш соодветното својство го има и секој групоид G' изоморфен со G.

Доказ. Нека f е изоморфизам од G во G'. Ако $x', y', z' \in G'$, тогаш постојат $x, y, z \in G$, такви што: $x' = f(x)$, $y' = f(y)$, $z' = f(z)$, бидејќи f, по претпоставка, е биекција.

а) Нека G е комутативен; тогаш имаме:

$x' y' = f(x) f(y) = f(xy) = f(yx) = f(y) f(x) = y' x'$, т.е. G' е комутативен.

б) Ако G е полугрупа, тогаш имаме:

$$\begin{aligned} x' (y' z') &= f(x) [f(y) f(z)] = f(x) f(yz) \\ &= f[x (yz)] = f[(xy) z] = f(xy) f(z) \\ &= [f(x) f(y)] f(z) = \\ &= (x' y') z', \end{aligned}$$

па, значи, и G' е полугрупа.

в) Ако e е единица на G и ако $e' = f(e)$, тогаш:

$x' e' = f(x) f(e) = f(xe) = f(x) = x'$,

$e' x' = f(e) f(x) = f(ex) = f(x) = x'$,

од што следува дека e' е единица на G'.

г) Ако G е група, тогаш според в) и б), G' е полугрупа со единица $e' = f(e)$, каде што e е единицата на G. Значи, треба да покажеме дека секој елемент $x' \in G$ е инверзибилен во G'. Навистина, ако $x' = f(x)$, тогаш имаме:

$$x' f(x^{-1}) = f(x) f(x^{-1}) = f(xx^{-1}) = f(e) = e'.$$

Од што следува дека $f(x^{-1})$ е инверзија за $f(x)$ во G'. Според тоа, и G' е група.

д) Нека G е групоид со кратење. Ако $a' b' = a' c'$ и ако $a' = f(a)$, $b' = f(b)$, $c' = f(c)$, тогаш $f(ab) = f(ac)$, па и $ab = ac$, од што следува дека $b = c$, па и $b' = c'$. Слично, од $b' a' = c' a'$ следува $b' = c'$. Значи, и G' е групоид со кратење. ∎

Да забележиме дека според **4°** (ii), до исти резултати би дошле и при претпоставка дека G' ги има соодветните својства.

Да претпоставиме сега дека $R(+, \cdot)$ и $R'(+, \cdot)$ се алгебарски структури. За $f: R \to R'$ велиме дека е *изоморфизам* од $R(+, \cdot)$ во $R'(+, \cdot)$ акко е изоморфизам од $R(+)$ во $R'(+)$ и од $R(\cdot)$ во $R'(\cdot)$, т.е. акко f е биекција, таква што:

$$f(x + y) = f(x) + f(y), \quad f(x \cdot y) = f(x) f(y), \tag{1''}$$

за секои $x, y \in R$. Велиме дека $R(+, \cdot)$ и $R'(+, \cdot)$ се *изоморфни* и пишуваме $R \cong R'$ акко постои изоморфизам од $R(+, \cdot)$ во $R'(+, \cdot)$.

Како последица од дадените дефиниции и својствата **1°**, **2°** и **3°** се добива и следното својство.

6°. Ако $R(+, \cdot)$ и $R'(+, \cdot)$ се две алгебарски структури, тогаш:

(i) $R \cong R$; (ii) $R \cong R' \Rightarrow R' \cong R$; (iii) $R \cong R'$, $R' \cong R'' \Rightarrow R \cong R''$. ∎

Ќе докажеме и својство аналогно на **5°**.

7°. Нека $R(+, \cdot)$ и $R'(+, \cdot)$ се две изоморфни структури. Ако едната од нив е: а) прстен, б) интегрален домен, в) поле, тогаш соодветното својство го има и другата.

Доказ. Поради **6°** (ii), можеме да претпоставиме дека соодветното својство го има R. Нека f е изоморфизам од R во R' и нека $x', y', z' \in R'$, $x, y, z \in R$, $f(x) = x'$, $f(y) = y$, $f(z) = z'$.

а) Ако $R(+, \cdot)$ е прстен, тогаш $R(+)$ е комутативна група, од што следува, според **5°**: а) и г), дека и $R'(+)$ е комутативна група.

Преостанува да се докажат дистрибутивните закони.

$$\begin{aligned} x'(y' + z') &= f(x)\,(f(y) + f(z)) = f(x)\,f(y + z) \\ &= f(x\,(y + z)) = f(xy + xz) = \\ &= f(xy) + f(xz) = f(x)f(y) + f(x)f(z) \\ &= x'\,y' + x'\,z'. \end{aligned}$$

На ист начин се покажува и другиот дистрибутивен закон.

б) Нека $R(+, \cdot)$ е интегрален домен. Според **5°** : а), б), в), $R'(+, \cdot)$ е комутативен и асоцијативен прстен со единица. Притоа, имаме и $f(0) = 0'$, $f(e) = e'$, каде што 0 и e се нулата и единицата во R, а $0'$ и e' нулата и единицата во R'.

Ако $x'\,y' = 0'$, тогаш имаме:

$$f(xy) = f(x)\,f(y) = x'\,y' = 0' = f(0),$$

т.е. $xy = 0$, па значи $x' = 0'$ или $y' = 0'$. Со тоа покажавме дека и $R'(+, \cdot)$ е интегрален домен.

в) Нека $R(+, \cdot)$ е поле. Тогаш, според б), $R'(+, \cdot)$ е интегрален домен, бидејќи $R(+, \cdot)$, (како и секое поле), е и интегрален домен. Ако $x' \neq 0'$, тогаш имаме и $x \neq 0$, од што следува:

$$x'\,f(x^{-1}) = f(x\,x^{-1}) = f(e) = e',$$

т.е. $f(x^{-1}) = x'^{-1}$ во $R'(+, \cdot)$. Со тоа покажавме дека и $R'(+, \cdot)$ е поле. ∎

При конструкцијата на адитивната група $\mathbf{Z}(+)$ на целите броеви, што е направена во 3.1., се раководевме од задачата да се прошири $\mathbf{N}(+)$ до група, со додавање на "што помалку" елементи. Од следново тврдење следува дека таму е извршена и втората задача.

8°. Ако во адитивно означената комутативна група $G(+)$ постои потполугрупа N', изоморфна со полугрупата $\mathbf{N}(+)$, тогаш постои и подгрупа Z', изоморфна со групата $\mathbf{Z}(+)$.

Доказ. Нека f е изоморфизам од $\mathbf{N}$ во N'. Го формираме множеството $Z' = N' \cup \{-y \mid y \in N'\}$. Лесно се покажува дека Z' е подгрупа на G, и дека пресликувањето g од $\mathbf{Z}$ во Z' дефинирано со:

$$g(x) = f(x) \text{ за } x \in \mathbf{N},\ g(-x) = -f(x) \text{ за } x \in \mathbf{Z}^-$$

е изоморфизам од $\mathbf{Z}(+)$ во Z'. ∎

ВЕЖБИ. **2.** Ако на $\mathbf{Z}$ дефинираме операција $*$ со: $x * y = x + y + 1$ добиваме група $\mathbf{Z}(*)$ изоморфна со $\mathbf{Z}(+)$.

3. Ако $a \in \mathbf{Z}$, $a \neq 1$ и ако $x \circ y = axy$, тогаш групоидот $\mathbf{Z}(\circ)$ не е изоморфен со $\mathbf{Z}(+)$ ни со $\mathbf{Z}(\cdot)$.

4. Изоморфизам од групоидот $G(*)$ во $G(*)$ се вика *автоморфизам на групоидот*. Множеството *Aut* G од сите автоморфизми на G е подгрупа на $S(G)$.

5. $1_{\mathbf{Z}}$ и $f: x \to -x$ се единствените автоморфизми на $\mathbf{Z}(+)$, како и на $\mathbf{Z}(+, \cdot)$, (При тоа, g се вика *автоморфизам* на структурата $A(\circ, *, \square, \ldots)$ акко е *автоморфизам* на секој од групоидите: $A(\circ)$, $A(*)$, $A(\square)$, $\ldots$).

6. Нека f е биекција од R во R и нека $R(+, \cdot)$ е прстен. Ако на R се дефинираат операции $+', \cdot'$ со:

$x +' y = f^{-1}(f(x) + f(y))$, $x \cdot' y = f^{-1}(f(x) f(y))$ се добива прстен изоморфен со даденият.

7. (i) Пресликувањето $f: x \to 2^x$ е изоморфизам од $\mathbf{R}(+)$ во $\mathbf{R}^+(\cdot)$, каде што $\mathbf{R}$ е множеството од сите реални броеви, а $\mathbf{R}^+$ од сите позитивни реални броеви.

(ii) Пресликувањата $f: x \to -x$, $g: x \to \bar{x}$ се автоморфизми на полето на комплексните броеви.

4.6. ИЗОМОРФНО СМЕСТУВАЊЕ НА ПРСТЕН ВО ПРСТЕН

Поимот за изоморфно сместување може да се дефинира за групоиди, како и за какви било алгебарски структури, но ние ќе се задржиме само на прстените, бидејќи тоа ќе ни треба при конструкцијата на рационалните броеви.

Нека $R(+, \cdot)$ и $R'(+, \cdot)$ се два прстена. Ако f е инјекција од R во R', таква што:

$$f(x + y) = f(x) + f(y),\ f(x \cdot y) = f(x) \cdot f(y), \tag{1}$$

тогаш велиме дека f е *изоморфно сместување* (или само: *сместување*) од R во R'.

Ќе докажеме две својства.

1°. Ако f е сместување од прстенот R во R', тогаш $R_1=f(R)$ е потпрстен од R' и притоа, $R\cong R_1$.

Доказ. Нека $x_1, y_1 \in R_1$. Тогаш $x_1=f(x)$, $y_1=f(y)$ за некои $x, y \in R$. Имајќи го предвид (1) добиваме:

$$x_1 y_1 = f(x)\, f(y) = f(xy) \in R_1$$

$$x_1 + y_1 = f(x) + f(y) = f(x+y) \in R_1$$

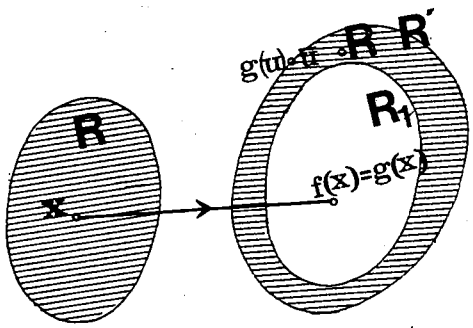
$$-x_1 = f(-x) \in R_1$$

од што следува дека R_1 е потпрстен на R'.

Потоа, ако определиме пресликување $f_1 : R \to R_1$ со: $(\forall x \in R) f_1(x)=f(x)$, добиваме дека f_1 е изоморфизам од R во R_1.

2°. Нека f е сместување од прстенот R во прстенот R', при што $R' \cap R = \varnothing$. Постои прстен R'', таков што:

(i) $R'' \sim R'$; (ii) R е потпрстен на R''.



Доказ. Ако f е биекција, тогаш прстенот R ги има бараните својства на R''. Затоа, ќе претпоставиме дека f не е биекција, т.е. $f(R)=R_1 \subset R'$. Го формираме множеството $R''=R' \cup (R' \setminus R_1)$. (Исшрафираниот дел од сликата!). Да дефинираме пресликување $g : R'' \to R'$ со:

$$g(x) = \begin{cases} f(x) & \text{за } x \in R \\ x & \text{за } x \in R' \setminus R_1. \end{cases} \tag{2}$$

Имаме:

$$g(R'') = g(R \cup (R' \setminus R_1)) = g(R) \cup g(R' \setminus R_1)$$

$$= f(R) \cup (R' \setminus R_1) = R_1 \cup (R' \setminus R_1) = R',$$

т.е. g е сурјекција. Ако се има предвид тоа што f е инјекција, од (2) се гледа дека g е инјекција, т.е. биекција.

Во R'' дефинираме две операции: собирање $(+'')$ и множење $(*'')$ со:

$$\begin{aligned} x +'' y &= g^{-1}(g(x) + g(y)) \\ x *'' y &= g^{-1}(g(x) \cdot g(y)). \end{aligned} \tag{3}$$

Од (3) следува:

$$\begin{aligned} g(x +'' y) &= g(x) + g(y) \\ g(x *'' y) &= g(x)\ g(y). \end{aligned} \tag{3'}$$

така што g е изоморфизам од R'' во R', па, значи, $R'' \cong R'$. Според 4.5. 7°: (а), $R''(+'', *'')$, исто така, е прстен.

Преостанува да покажеме дека $R(+, \cdot)$ е потпрстен на $R''(+'', *'')$. Нека $x, y \in R$. Од (3') следува:

$$\begin{aligned} g(x +'' y) &= f(x) + f(y) = f(x + y), \\ g(x *'' y) &= f(x)\, f(y) = f(x \cdot y), \end{aligned} \tag{4}$$

па, според тоа, $x +'' y,\ x *'' y \in R$, така што

$$g(x +'' y) = f(x +'' y),\ g(x *'' y) = f(x *'' y).$$

Заменувајќи во (4) добиваме:

$$f(x +'' y) = f(x + y),\ f(x *'' y) = f(xy),$$

т. е. $x +'' y = x + y,\ \ x *'' y = xy.$ (5)

Од (5) следува дека $R(+, \cdot)$ е потпрстен на $R''(+'', *'')$.

(Од (5) се гледа и дека операциите на R'' можеме да ги означуваме на обичниот начин, т.е. на (3) можеме да му го дадеме следниов облик:

$$\begin{aligned} x + y &= g^{-1}(g(x) + g(y)) \\ x \cdot y &= g^{-1}(g(x)\ g(y)). \end{aligned} \tag{3''}$$

Во текот на натамошното работење, неколкупати ќе се сретнеме со задачата да проширме даден прстен R до прстен R'', така што R да биде потпрстен на R'', а R'' да задоволува соодветни апстрактни својства, т.е. својства што се запазуваат при изоморфизми. Со соодветни конструкции, ќе формираме прстен R' што ги има бараните својства, но R и R' ќе бидат дисјунктни. Според тоа, R' се уште не ќе можеме да го сметаме за задоволително

решение на проблемот. Но, ако успееме да определиме сместување f од R во R',тогаш ќе бидеме сигурни дека сме го решиле проблемот, бидејќи прстенот R'', конструиран во доказот на **2°**, ќе биде бараниот прстен. Инаку, обично, прстенот R' ќе го сметаме за задоволително решение, со тоа што ќе се договориме за $x \in R$ да биде точно равенството $x = f(x)$, т.е. ќе сметаме $f(x)$ да биде друга ознака за x.

Со цел да го илустрираме кажаното, подолу ќе ја образложиме добро познатата конструкција на комплексните броеви. При конструкцијата на комплексните броеви се тргнува од реалните броеви и се поставува задача полето на реалните броеви да се прошири до поле во кое ќе постои елемент j, таков што $j^2 = -1$.

Со оглед на тоа што полето на реалните броеви сè уште не го имаме конструирано, ќе претпоставиме дека R е кое било поле во кое $x^2 \neq -e$, за секој $x \in R$; овде (како и обично) со e е означена единицата на R. Да претпоставиме дека F е поле со следниве својства:

(а) R е потполе на F,

(б) Постои елемент $j \in F$, таков што $j^2 = -e$.

Потоа да ставиме:

$$K = \{x + jy \mid x, y \in R\}. \tag{6}$$

Ќе покажеме дека:

3°. K е потполе на F и притоа:

(i) $R \cup \{j\} \subset K$; (ii) ако M е потполе на R, такво што $R \cup \{j\} \subseteq M$, тогаш $K \subseteq M$; (iii) ако $x, y, u, v \in R$, тогаш:

$$x + jy = u + jv \Leftrightarrow x = u, \quad y = v; \tag{7}$$

$$(x + jy) + (u + jv) = (x + u) + j\,(y + v); \tag{8}$$

$$(x + jy) \cdot (u + jv) = (xu - yv) + j\,(xu + yv). \tag{9}$$

Доказ. Прво ќе го покажеме третиот дел. Нека $x + jy = u + jv$; тогаш $x - u = j(v - y)$; не може да биде $v - y \neq 0$, бидејќи тогаш би имале: $j = (x - u)\,(v - y)^{-1} \in R$, што би противречело на претпоставката дека $t^2 \neq -e$ за секој $t \in R$; според тоа, $v = y$, а од тоа следува и $x = u$. Равенствата (8) и (9) следуваат од тоа што F е поле и $j^2 = -e$.

Сега ќе покажеме дека K е потполе на F такво што $R \cup \{j\} \subset K$. Прво, $j = 0 + j \cdot e \in K$; ако $x \in R$, тогаш $x = x + j0 \in K$; ако се има предвид и тоа што, на пример, $e + j \in K$, но $e + j \notin R \cup \{j\}$ добиваме дека $R \cup \{j\} \subset K$. Ако $x + jy \in K$, тогаш $-(x + jy) = (-x) + j(-y) \in K$. Имајќи ги предвид равенствата (8) и (9), добиваме дека K е потпрстен на F.

Нека $z = x + iy \in K$, $z \neq 0$. Тогаш, $x \neq 0 \vee y \neq 0$. Не може да биде $x^2 + y^2 = 0$, бидејќи од тоа би следувало дека $u^2 = -e$, каде $u = xy^{-1}$ за $y \neq 0$, односно $u = yx^{-1}$ за $x \neq 0$. Со директна примена на (8) и (9) се добива дека

$$z\,[x\,(x^2+y^2)^{-1}+j\,(-y)\,(x^2+y^2)^{-1}]=e,\ \text{т. е.}$$

$$z^{-1}=(x^2+y^2)^{-1}\,x+j\,(-y)\,(x^2+y^2)^{-1}.$$

Со тоа покажавме дека K е потполе на F. Точноста на (ii) е јасна.■

Сега да ја разгледаме ситуацијата кога е дадено поле R во кое $x^2\neq -e$ за секој $x\in R$. Сакаме да најдеме поле F во кое ќе постои елемент j, таков што $j^2=-e$ и за кое даденото поле R ќе биде потполе.

Својството 3° ни сугерира да дефинираме операции собирање (+) и множење (·) на $C=R\times R$ со:

$$(x,y)+(u,v)=(x+u,\ y+v) \tag{8'}$$

$$(x,y)\cdot(u,v)=(xu-yv,\ xv+yu); \tag{9'}$$

имено, сакаме (x,y) да ја има улогата на $x+jy$.

Од својството што ќе го докажеме ќе следува дека сме го решиле поставениот проблем.

4°. (i) $C(+,\cdot)$ е поле. Притоа, $(0,0)$ е нулата, а $(e,0)$ единицата на C, и:

$$-(x,y)=(-x,-y),\ (0,e)^2=-(e,0);$$

(ii) Пресликувањето $f: x\to(x,0)$ е изоморфно сместување од R во C.

Доказ. (i) Користејќи го само фактот што R е комутативен прстен со единица e, се добива дека C е комутативен прстен со нула $(0,0)$, единица $(e,0)$, $-(x,y)=(-x,-y)$ и притоа

$$(0,e)^2=(0,e)\,(0,e)=(0-e,\ 0)=-(e,0).$$

Потоа, со директна примена на (9') се добива дека:

$$(x,y)\neq(0,0)\Rightarrow(x,y)^{-1}=(x\,(x^2+y^2)^{-1},\ -y\,(x^2+y^2)^{-1}) \tag{10}$$

од што ќе следува дека C е поле.

(ii) Прво, $C\cap R=\varnothing$; јасно е дека f е инјекција. Притоа:

$$f(x+y)=(x+y,0)=(x,0)+(y,0)=f(x)+f(y)$$

$$f(xy)=(xy,0)=(x,0)\ (y,0)=f(x)\cdot f(y),$$

т.е. f е сместување од R во C.■

Согласно погоре наведениот договор, ако ставиме:

$$x=(x,0),\quad j=(0,e), \tag{11}$$

добиваме:

$$(x,y)=(x,0)+(0,y)=(x,0)+(0,e)\,(y,0)$$

$$=x+jy, \tag{12}$$

така што сега добиваме дека C ја има улогата на полето K, дискутирано во својството 3°.

Како што спомнавме и во почетокот на дискусијата, ако $\mathbf{R}$ е полето на реалните броеви, тогаш добиеното поле $\mathbf{C}$ го викаме поле на комплексните броеви.

(На читателот му е добро познато дека "имагинарната единица" се означува со "i", а не со "j", како што тоа ние погоре го направивме. Буквата "i" ја избегнавме, бидејќи неа често ја користиме за нумерација. Од слични причини, таа буква се избегнува и во електротехниката.)

Да разгледаме два примера.

1) $\mathbf{Z}_3 = \{0, 1, 2\}$ е поле во кое $x^2 + 1 \neq 0$. Според тоа:

$$C = \{0, 1, 2, j, 2j, 1 + j, 1 + 2j, 2 + j, 2 + 2j\}$$

е поле со 9 елементи. Притоа, операциите собирање и множење се определени во C со (8) и (9), при што треба да се има предвид дека $-1 = 2$.

2) Во $\mathbf{Z}_5$ имаме $2^2 = -1$, така што овде не е можно проширување на $\mathbf{Z}_5$ во поле со 25 елементи. Имено, ако се дефинира C со $\{x + yj \mid x, y \in \mathbf{Z}_5\} = C$ и во C се определат собирање и множење со (8) и (9), ќе се добие комутативен и асоцијативен прстен со единица, што не е поле.

ВЕЖБИ. 2. Постои поле со: а) 49; б) 121 елементи.

3. Да се формулира поим за изоморфно сместување на еден групоид во друг и да се докаже својството аналогно на 2°.

4. Нека $G(*)$ е комутативна полугрупа со кратење и нека на $S = G \times G$ определиме операција $*$ со: $(x, y) * (u, v) = (x * u,\ y * v)$ и релација α со:

$$(x, y)\ \alpha\ (u, v) \Leftrightarrow x * v = y * u.$$

(i) $S(*)$ е комутативна полугрупа со кратење, но не е група.

(ii) α е конгруенција на $S(*)$ и притоа фактор групоидот S/α $(*)$ е комутативна група

(iii) Пресликувањето $x \to (xa, a)^\alpha$, каде што a е фиксен елемент на G, е сместување од G во S/α.

5. Со помош на резултатите о претходната вежба, да се даде нова конструкција на адитивната група $\mathbf{Z}(+)$ на целите броеви, поточно, на група изоморфна со неа.

6. Нека R е поле и a фиксен елемент на R, таков што равенката $x^2 = a$ нема решение во R. Да се покаже дека постои поле F во кое таа равенка има решение и притоа R е потполе на F.

7. Да се определи поле F за кое $\mathbf{Z}_5$ е потполе и во кое постои елемент α, таков што $\alpha^2 = 2$.

4.7. ПОЛЕ НА РАЦИОНАЛНИТЕ БРОЕВИ

Овде ќе покажеме како се врши сместување на интегралниот домен $\mathbf{Z}$ на целите броеви во поле. Ќе докажеме прво едно помошно тврдење.

1°. Нека $\mathbf{Z}$ е потпрстен на полето F и нека Q е подмножество на F дефинирано со:

$$Q = \{xy^{-1} \mid x, y \in \mathbf{Z},\ y \neq 0\}. \tag{1}$$

Тогаш:

(i) Q е потполе на F такво што $\mathbf{Z} \subset Q$.

(ii) Ако е P потполе на F, тогаш $Q \subseteq P$. (Затоа, Q се вика *минимално потполе* на F.)

Доказ. (i) $\mathbf{Z} \subseteq Q$, бидејќи: $x \in \mathbf{Z} \Rightarrow x = x \cdot 1 = x \cdot 1^{-1} \in Q$. Нека $x, y, z, u, v \in \mathbf{Z}$, $y, v \neq 0$. Тогаш:

$$-(xy^{-1}) = (-x)\ y^{-1} \in Q$$

$$(xy^{-1})\ (uv^{-1}) = (xu)\ (yv)^{-1} \in Q \tag{2}$$

$$(xy^{-1}) + (uv^{-1}) = (xv)\ (yv)^{-1} + (uy)\ (yv)^{-1} \tag{3}$$

$$= (xv + yu)\ (yv)^{-1} \in Q.$$

Потоа, ако $xy^{-1} \neq 0$, имаме $x \neq 0$, па и $(xy^{-1})^{-1} = yx^{-1} \in Q$. Од сето тоа следува дека Q е потполе на F. Како последица од ова следува и дека $\mathbf{Z}$ е вистинско подмножество на Q, бидејќи $\mathbf{Z}$ не е потполе.

Да забележиме и дека:

$$xy^{-1} = uv^{-1} \Leftrightarrow xv = yu \tag{4}$$

(ii) Прво, да уочиме дека единицата 1 на $\mathbf{Z}$ е единица и на F, бидејќи ако e е единица на F ќе имаме: $1 \cdot e = 1 = 1 \cdot 1$, т.е. $e = 1$. Според тоа, ако P е потполе на F, имаме: $0, 1, -1 \in P$, од што следува и дека $\mathbf{Z} \subseteq P$, бидејќи $x \in \mathbf{Z}^+ \Rightarrow x = \underbrace{1 + \ldots + 1}_{x} \in P$; $x \in \mathbf{Z}^- \Rightarrow x = \underbrace{(-1) + \ldots + (-1)}_{-x} \in P$. Ако $y \in \mathbf{Z}$, $y \neq 0$, тогаш $y \in P$, така што $y^{-1} \in P$. И, на крајот, ако $x, y \in \mathbf{Z}$, $y \neq 0$, имаме $x, y^{-1} \in P$, т.е. $xy^{-1} \in P$. Со тоа докажавме дека $Q \subseteq P$. ∎

Да покажеме дека постои поле за кое $\mathbf{Z}$ е потпрстен. Конструкцијата на едно такво поле е сугерирана од доказот на **1°** (i). Имено, точно е следново тврдење:

2°. Нека $S = \{(x, y) \mid x, y \in \mathbf{Z},\ y \neq 0\}$ и нека во S дефинираме операции собирање $(+)$ и множење $(\cdot)$ со:

$$(x, y) + (u, v) = (xv + yu,\ yv) \tag{3'}$$

$$(x, y) \cdot (u, v) = (xu,\ yv) \tag{2'}$$

и релација ρ со:

$$(x, y)\ \rho\ (u, v) \Leftrightarrow xv = yu. \tag{4'}$$

Тогаш:

(i) $S(+)$ и $S(\cdot)$ се комутативни полугрупи; (0,1) е нула на $S(+)$, а (1,1) единица на $S(\cdot)$.

(ii) ρ е конгруенција на $S(+, \cdot)$ и притоа $S/\rho(+, \cdot)$ е поле.

(iii) Ако F е поле во кое $\mathbf{Z}$ е потпрстен, тогаш минималното потполе Q на F е изоморфно со полето S/ρ.

(iv) Пресликувањето

$$f: x \to (x, 1)^\rho \tag{5}$$

е изоморфно сместување од $\mathbf{Z}$ во S/ρ.

Доказ. (i) Точноста се докажува со директна проверка, ако се има предвид тоа што $\mathbf{Z}$ е интегрален домен.

(ii) Непосредно од комутативноста на множењето на целите броеви следува дека ρ е рефлексивна и симетрична релација. Да покажеме дека е ρ и транзитивна.

Ако $(x, y)\ \rho\ (u, v)$, $(u, v)\ \rho\ (z, t)$, тогаш $xv = yu$, $ut = vz$, од што следува $xvt = yut = yvz$, т.е. $xt = yz$, од што следува дека ρ е и транзитивна.

Нека $(x_1, y_1)\ \rho\ (u_1, v_1)$ и $(x_2, y_2)\ \rho\ (u_2, v_2)$, т.е.

$$x_1 v_1 = y_1 u_1, \text{ и } x_2 v_2 = y_2 u_2. \tag{*}$$

Од (*) се добива $(x_1, x_2)(v_1, v_2) = (y_1, y_2)(u_1, u_2)$, т.е.

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)\ \rho\ (u_1 u_2, v_1 v_2) = (u_1, v_1)(u_2, v_2).$$

Ако го помножиме првото равенство од (*) со $y_2 v_2$, а второто со $y_1 v_1$ и извршиме собирање, ќе добиеме:

$$(x_1 y_2 + y_1 x_2)(v_1 v_2) = (y_1 y_2)(u_1 v_2 + v_1 u_2), \text{ од што следува:}$$

$$(x_1 y_2 + y_1 x_2, y_1 y_2)\ \rho\ (u_1 v_2 + v_1 u_2, v_1 v_2) \text{ т. е.}$$

$$(x_1, y_1) + (x_2 y_2)\ \rho\ (u_1, v_1) + (u_2, v_2).$$

Со сето тоа покажавме дека ρ е конгруенција на $S(+, \cdot)$.

Од (i), ако се има предвид својството 4.1.**2**°, се добива дека $S/\rho(+)$ и $S/\rho(\cdot)$ се комутативни полугрупи, при што $(0, 1)^\rho$ е нула на првата, а $(1,1)^\rho$ единица на втората полугрупа.

Пред да го комплетираме доказот на (ii) да уочиме дека, ако $u \neq 0$, тогаш:

$$(x, y)\ \rho\ (xu, yu), \text{ т.е. } (x, y)^\rho = (xu, yu)^\rho, \tag{5}$$

од што следува дека:

$$(x, y)^\rho + (u, y)^\rho = (xy + yu, yy)^\rho = (x + u, y)^\rho. \tag{6}$$

Сега добиваме:

$$(x, y)\rho + (-x, y)\rho = (0, y)\rho = (0, 1)\rho,$$

т.е.

$$-(x, y)\rho = (-x, y)\rho. \tag{7}$$

Според тоа, $S/\rho\,(+)$ е комутативна група.

Ако (x, y), (u, y), $(v, y) \in S$, тогаш, според (6),

$$\begin{aligned}(x, y)\rho\,[(u, y)\rho + (v, y)\rho] &= (x, y)\rho\,(u + v, y)\rho = (xu + xv, yy)\rho \\ &= (xu, yy)\rho + (xv, yy)\rho \\ &= (x, y)\rho\,(u, y)\rho + (x, y)\rho\,(v, y)\rho.\end{aligned}$$

Со тоа покажавме дека $S/\rho\,(+, \cdot)$ е комутативен прстен. (Ако имавме (x_1, y_1), (x_2, y_2), $(x_3, y_3) \in S$, тогаш $(x_1, y_1)\,\rho\,(x_1 y_2 y_3, y_1 y_2 y_3)$, $(x_2, y_2)\,\rho\,(x_2 y_1 y_3, y_1 y_2 y_3)$, $(x_3, y_3)\,\rho\,(x_3 y_1 y_2, y_1 y_2 y_3)$, така што пак добиваме тројка од облик (x, y), (u, y), $(v, y) \in S$.).

На крајот, ако $(x, y)\rho \neq (0, 1)\rho$, т. е.

ако $x \neq 0$, тогаш

$$(x, y)\rho \cdot (y, x)\rho = (xy, yx)\rho = (1, 1)\rho,$$

од што следува:

$$[(x, y)\rho]^{-1} = (y, x)\rho. \tag{8}$$

Со тоа го комплетиравме доказот дека $S/\rho\,(+, \cdot)$ е поле.

(iii) Нека $\mathbf{Z}$ е потпрстен на полето F. Тогаш, минималното потполе Q на F е определено со (1). Ако $x, y \in \mathbf{Z}$, $y \neq 0$, тогаш ќе ставиме:

$$g(x y^{-1}) = (x, y)\rho. \tag{9}$$

Да покажеме дека g е пресликување од Q во S/ρ. Ако $xy^{-1} = uv^{-1}$, тогаш според (4), $xv = yu$, од што следува $(x, y)\ \rho\ (u, v)$, т.е. $(x, y)\rho = (u, v)\rho$. Од (9) и дефиницијата на S е јасно дека g е сурјекција. Ако $g(x y^{-1}) = g(u v^{-1})$, т.е. $(x, y)\rho = (u, v)\rho$, тогаш $(x, y)\ \rho\ (u, v)$, од што следува $xv = yu$ и, конечно, $xy^{-1} = uv^{-1}$; со тоа покажавме дека g е инјекција. Од (2), (3), (2′) и (3′) следува и дека g е изоморфно сместување.

(iv) Ако $(x, 1)\rho = (y, 1)\rho$, т.е. $(x, 1)\ \rho\ (y, 1)$ тогаш $x \cdot 1 = 1 \cdot y$. Според тоа, f е инјекција. Потоа:

$$\begin{aligned}f(xy, 1) &= (xy, 1)\rho = (x, 1)\rho\,(y, 1)\rho = f(x)\,f(y) \\ f(x + y, 1) &= (x + y, 1)\rho = (x, 1)\rho + (y, 1)\rho = f(x) + f(y),\end{aligned} \tag{10}$$

т.е. f е изоморфно сместување од $\mathbf{Z}$ во S/ρ.

Добиеното поле S/ϱ ќе го означуваме со $\mathbf{Q}$ и ќе велиме дека тоа е *полето на рационалните броеви*. Ако $(x, y) \in S$, тогаш ќе пишуваме $\frac{x}{y}$ наместо $(x, y)\varrho$, т.е. ќе ја употребуваме обичната ознака за рационалните броеви. Според тоа, имаме:

$$\frac{x}{y} = \frac{u}{v} \Leftrightarrow xv = yu; \quad -\left(\frac{x}{y}\right) = \frac{-x}{y} = \frac{x}{-y};$$

$$\left(\frac{x}{y}\right)^{-1} = \frac{y}{x} \text{ за } x, y \neq 0; \tag{11}$$

$$\frac{x}{y} \cdot \frac{u}{v} = \frac{xu}{yv}; \quad \frac{x}{y} + \frac{u}{v} = \frac{xv + yu}{yv}, \quad \frac{x}{y} + \frac{u}{y} = \frac{x+u}{y}.$$

Според договорот што го направивме во претходниот дел, ќе сметаме дека:

$$x \in \mathbf{Z} \Rightarrow x = \frac{x}{1}, \tag{12}$$

па, според тоа, ако $\mathbf{Z}$ е потпрстен од полето F и ако $x, y \in \mathbf{Z}$, $y \neq 0$, тогаш:

$$x y^{-1} = \frac{x}{1} \cdot \frac{1}{y} = \frac{x}{y}. \tag{13}$$

Со други зборови, сметаме дека:

3°. Полето $\mathbf{Q}$ на рационалните броеви се совпаѓа со простото потполе Q на секое поле R во кое $\mathbf{Z}$ е потпрстен. ∎

ВЕЖБИ. 2. Ако $a, b \in \mathbf{Q}$, $b \neq 0$, тогаш $a \cdot b^{-1}$ се означува често со $\frac{a}{b}$. (Оваа ознака се користи во секое поле). Сите својства наведени во (11) (а и, поопшто, сите познати својства за работата со дропки) се точни акко $x, y, u, v \in \mathbf{Q}$, со тоа што соодветните именители се различни од нула.

3. Секој ненулти рационален број x може на единствен начин да се претстави во облик: $x = \frac{m}{n}$, каде што $n \in \mathbf{Z}^+$, $m \in \mathbf{Z}$ и $(m; n) = 1$.

4. Ако $a \in \mathbf{Q}$, $m, n \in \mathbf{N}^+$ се такви, што $a^m = n$, тогаш $a \in \mathbf{N}$.

5. Не постои рационален број a, таков што: а) $a^2 = 2$; б) $a^3 = 2$; в) $a^2 = 7$.

6. Рационалниот број x се вика *конечна десетична дропка* акко може да се претстави во облик: $x = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}$, каде што $a_i \in \mathbf{N}$, $0 \leqslant a_j < 10$, за $j = 1, \ldots, n$. Тогаш се пишува: $x = a_0, a_1 a_2 \ldots a_n$.

(i) Ако $x = \frac{r}{s}$, $r, s \in \mathbf{N}+$, $(r; s) = 1$, тогаш x е конечна десетична дропка акко s има облик: $s = 2^k \cdot 5^m$, каде што $k, m \in \mathbf{N}$.

(ii) Да се докажат познатите правила за: собирање, ваденье, множење, квадрирање на конечни дропки.

7. Какви треба да бидат бревите $a, b, c \in \mathbf{Q}$ за да биде точно равенството:

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{1}{a+b+c}?$$

8. Да се определи поле R за кое $\mathbf{Q}$ е потполе и во кое постои елемент α, таков што:

а) $\alpha^2 = 2$; б) $\alpha^3 = 3$; в) $\alpha^3 = 2$.

9. $\mathbf{Q}$ е единственото потполе на $\mathbf{Q}$.

* **10.** Множеството $\mathbf{Q}$ е пребројво.

11. Ако во 2°, наместо со $\mathbf{Z}$ се работи со произволен интегрален домен, ќе се добие дека: Секој интегрален домен може да се смести во поле.

5. ПОДРЕДЕНИ ПОЛИЊА. РЕАЛНИ БРОЕВИ

5.1. ПОДРЕДЕНИ ИНТЕГРАЛНИ ДОМЕНИ

Во 3.4., користејќи го подредувањето на **N**, дефинираме подредување и на **Z**. Слично би можело да се подреди и полето **Q**, како што ќе видиме во следниот дел. Претходно ќе воведеме поопшт поим, а тоа е, имено, поимот за подреден интегрален домен. До овој нов поим доаѓаме раководејќи се од следните својства на множеството $\mathbf{Z}^+$ од позитивни цели броеви:

(i) $\mathbf{Z}^+$ е потполугрупа и од двете полугрупи $\mathbf{Z}(+)$ и $\mathbf{Z}(\cdot)$;

(ii) $0 \notin \mathbf{Z}^+$;

(iii) ако $x \in \mathbf{Z}$ и $x \neq 0$, тогаш $x \in \mathbf{Z}^+$ или $-x \in \mathbf{Z}^+$.

Поопшто, за интегралниот домен R велиме дека е *подреден* акко е дадено непразно подмножество R^+ на R со следниве особини:

$$x, y \in R^+ \Rightarrow x + y, x \cdot y \in R^+; \tag{1}$$

$$0 \notin R^+; \tag{2}$$

$$x \neq 0 \Rightarrow x \in R^+ \vee -x \in R^+. \tag{3}$$

Ако сето тоа е исполнето, велиме дека R^+ е множеството од *позитивни елементи* на R. За множеството:

$$R^- = \{x \mid -x \in R^+\} \tag{4}$$

велиме дека е множеството *негативни елементи* на R.

Имајќи ја предвид дискусијата што ја направивме пред дефиницијата на подреден домен, добиваме дека:

1°. **Z** е подреден интегрален домен, каде поимите за позитивни, односно негативни елементи го имаат обичното значење.

Ќе докажеме неколку својства на подредените интегрални домени. Притоа ќе претпоставуваме дека R е подреден интегрален домен, со множество позитивни елементи R^+ и единица e.

2°. $R = R^- \cup \{0\} \cup R^+$, при што $0 \notin R^-$, $R^- \cap R^+ = \varnothing$.

Доказ. Нека $x \in R$ и $x \notin \{0\} \cup R^+$; тогаш, според (3), $-x \in R^+$, од што, според (4), следува дека $x \in R^-$; со тоа покажавме дека $R = R^- \cup \{0\} \cup R^+$. Според (2), 0 не е во R^+, од што, ако се има предвид дека $-0 = 0$, следува и $0 \notin R^-$. Ако $a \in R^+ \cap R^-$, тогаш, според (4), би имале: $a, -a \in R^+$, од што би следувало: $0 = a + (-a) \in R^+$, а тоа противречи на (2). Со тоа докажавме дека $R^+ \cap R^- = \emptyset$.

3°. (i) $x \neq 0 \Rightarrow x^2 \in R^+$; (ii) $e \in R^+$, $-e \in R^-$;

(iii) $xy \in R^+ \Leftrightarrow (x \in R^+, y \in R^+) \vee (x \in R^-, y \in R^-)$;

(iv) $xy \in R^- \Leftrightarrow (x \in R^+, y \in R^-) \vee (x \in R^-, y \in R^+)$.

Доказ. (i) Ако $x \neq 0$, имаме $x \in R^+$ или $-x \in R^+$, од што ќе следува $x^2 = xx \in R^+$ или $x^2 = (-x)(-x) \in R^+$, па, значи, $x^2 \in R^+$. (ii). Ова е последица од (i), ако притоа се има предвид дека $e^2 = e$.

(iii) и (iv). Ако $x \in R^+$, $y \in R^+$, тогаш $xy \in R^+$, според (1); ако $x, y \in R^-$, тогаш $-x, -y \in R^+$, па: $xy = (-x)(-y) \in R^+$. Ако $x \in R^+$, $y \in R^-$, тогаш $x \in R^+$, $-y \in R^+$, така што $-(xy) \in R^+$, т.е. $xy \in R^-$.

4°. Ако $n \in \mathbf{Z}$ тогаш:

(i) $ne \in R^+ \Leftrightarrow n \in \mathbf{Z}^+$; (ii) $ne \in R^- \Leftrightarrow n \in \mathbf{Z}^-$;

(iii) $nx \in R^+ \Leftrightarrow (n \in \mathbf{Z}^+, x \in R^+) \vee (n \in \mathbf{Z}^-, x \in R^-)$.

Доказ. (i) и (ii). Ако $n \in \mathbf{Z}^+$, тогаш, според (1) и **3°** (ii), добиваме: $ne = e + e + \ldots + e \in R^+$, $-(ne) \in R^-$, т.е. $(-n)e \in R^-$.

(iii) Да се искористат **3°** (iii) и (iv) и тоа што $nx = (ne)x$.

5°. Ако P е поддомен на подредениот домен R и ако ставиме $P^+ = R^+ \cap P$, добиваме подреден домен P, за кој велиме дека е подреден поддомен на R.

6°. Ако f е изоморфизам од подредениот домен R во доменот R' и ако ставиме $f(R^+) = R'^+$, добиваме подреден домен R'. (Ќе велиме дека R и R' се *изоморфни подредени домени.*)

Нека R и R' се два подредени домени и нека f е сместување на R во R', во смисла на договорот направен во 4.6. Ако, освен тоа, имаме и:

$$f(R^+) \subseteq R'^+, \tag{5}$$

тогаш велиме дека f е *сместување согласно со подредувањето*. Да спомнеме дека тврдењето **4.6.2°** важи и за подредените интегрални домени, кое сега ја добива следнава форма:

7°. Ако f е сместување на подредениот домен R во подредениот домен R' и ако f е согласно со подредувањето, тогаш постои подреден домен R'' изоморфно подреден со R', и притоа R е подреден поддомен на R''.

Ако се има предвид **4°** (i), се добива дека:

8°. За секој подреден домен R, пресликувањето $f: n \to ne$ е сместување на $\mathbf{Z}$ во R согласно со подредувањето.

Имајќи ги предвид својствата **7°** и **8°**, како и договорот направен во 4.6., добиваме дека:

9°. Доменот $\mathbf{Z}$ е подреден поддомен од секој подреден домен R. (Според ова, понатаму ќе претпоставуваме дека $\mathbf{Z} \subseteq R$, а специјално и $e = 1$.)

Во секој подреден интегрален домен R се дефинира релација за подредување на ист начин како и кај целите броеви. Имено, ако $x, y \in R$, тогаш:

$$x \leqslant y \Leftrightarrow y - x \in R^+ \vee x = y, \tag{6}$$

т. е.

$$x < y \Leftrightarrow y - x \in R^+. \tag{7}$$

10°. Ако R е подреден домен, тогаш релацијата $\leqslant$ е подредување на R и притоа:

$$x \in R^+ \Leftrightarrow 0 < x; \quad x \in R^- \Leftrightarrow x < 0. \tag{8}$$

Доказ. Релацијата $<$ е нерефлексивна според (2), и транзитивна, бидејќи ако $x < y$, $y < z$, тогаш $y - x, z - y \in R^+$, па и $z - x = (z - y) + (y - x) \in R^+$, т.е. $x < z$. Потоа, ако $x \neq y$, имаме: $x - y \in R^+$ или $y - x \in R^+$, т.е. $y < x$ или $x < y$. Со тоа докажавме дека $\leqslant$ е подредување на R. Точноста на (8) е директна последица од (2) и (4).

11°. Ако $m, n \in \mathbf{N}$ и ако x, y, z се елементи на подредениот домен R, тогаш:

(i) $x + z < y + z \Leftrightarrow x < y$;

(ii) $0 < z \Rightarrow \{xz < yz \Leftrightarrow x < y\}$;

(iii) $z < 0 \Rightarrow \{yz < xz \Leftrightarrow x < y\}$;

(iv) $x \neq 0 \Rightarrow 0 < x^{2m}$;

(v) $m > 0,\ x > 0,\ y > 0 \Rightarrow \{x < y \Leftrightarrow x^m < y^m\}$;

(vi) $x < y \Leftrightarrow x^{2m+1} < y^{2m+1}$;

(vii) $x \geqslant -1 \Rightarrow (1 + x)^m \geqslant 1 + mx$;

(viii) $1 < x \Rightarrow \{m < n \Leftrightarrow x^m < x^n\}$;

(ix) $0 < x < 1 \Rightarrow \{m < n \Leftrightarrow x^n < x^m\}$.

Доказ. (i) $y - x \in R^+ \Leftrightarrow (y + z) - (x + z) \in R^+$.

(ii) Нека $0 < z$, т.е. $z \in R^+$; тогаш, според **3°**, имаме $y - x \in R^+ \Leftrightarrow yz - xz = (y - x)\, z \in R^+$.

(iii) Ако $z < 0$, тогаш $-z \in R^+$, така што: $y - x \in R^+ \Leftrightarrow xz - yz = (y - x)(-z) \in R^+$.

(iv) Прво, од **3°** (i) следува дека $x^2 > 0$, а, потоа, и $x^{2m} = (x^2)^m > 0$.

(v) Нека $0 < x$ и $0 < y$. Ако $x < y$, тогаш со примена на (ii) добиваме: $x < y \Rightarrow x^2 < xy$, $xy < y^2$, т.е. $x < y \Rightarrow x^2 < y^2$; нека $x^k < y^k$; тогаш: $x^{k+1} < y^k x$, но $x < y \Rightarrow xy^k < y^{k+1}$, така што конечно добиваме: $x^{k+1} < y^{k+1}$. Со тоа докажавме дека $x < y \Rightarrow x^m < y^m$. Обратно, ако $x^m < y^m$, тогаш не е можно да биде $x = y$, ниту $y < x$, така што преостанува $x < y$.

(vi) Ако $0 \leqslant x$, ова е последица од (v). За $x < 0$, $0 \leqslant y$ точноста е јасна, па затоа преостанува случајот $x < 0$, $y < 0$. Тогаш, имаме $0 < -x$, $0 < -y$, така што, според (v) добиваме:

$$\begin{aligned} x < y &\Leftrightarrow -y < -x \Leftrightarrow (-y)^{2m+1} < (-x)^{2m+1} \\ &\Leftrightarrow -y^{2m+1} < -x^{2m+1} \\ &\Leftrightarrow x^{2m+1} < y^{2m+1}. \end{aligned}$$

(vii) Со индукција по m.

(viii) и (ix) Со примена на (ii). ∎

Поимот за *апсолутна вредност* се дефинира кај секој подреден домен на ист начин како што ние тоа го направивме кај целите броеви (3.4.(4)), т.е. со:

$$|x| = \begin{cases} x \text{ за } x \geqslant 0 \\ -x \text{ за } x < 0. \end{cases} \tag{9}$$

12°. Ако $x, y \in R$, $a \in R^+$, тогаш:

(i) $|0| = 0$, $x \neq 0 \Rightarrow |x| > 0$;

(ii) $|x| = x \vee |x| = -x$; $x \leqslant |x|$, $-x \leqslant |x|$;

(iii) $|-x| = |x|$;

(iv) $|x| < a \Leftrightarrow -a < x < a$;

(v) $|xy| = |x||y|$;

(vi) $|x + y| \leqslant |x| + |y|$.

Доказ. (i), (ii) и (iii) се непосредни последици од (9).

(iv) е последица од тоа што

$$-a < x < a \Leftrightarrow -a < -x < a.$$

(v) е последица од (9) и (iii).

(vi) Според (iii) $|x + y| = |-x - y|$, а според (ii), $|x + y| = x + y \vee |x + y| = -x - y$; пак според (ii), имаме $x \leqslant |x|$, $-x \leqslant |x|$, $-y \leqslant |y|$, $y \leqslant |y|$, од што следува $x + y \leqslant |x| + |y|$ и $-x - y \leqslant |x| + |y|$, т.е. $|x + y| \leqslant |x| + |y|$. ∎

ВЕЖБИ 2. Ниеден конечен домен не е подреден.

3. Ако R е подреден домен, тогаш во R нема најмал, ниту најголем елемент.

* **4.** Ако во секое непразно подмножество од R^+ има најмал елемент (т.е. ако R^+ е добро подредено), тогаш R е подреден домен изоморфен со $\mathbf{Z}$, односно, според **9°**, $R = \mathbf{Z}$.

5. Интегралниот домен $\mathbf{C}$ на комплексните броеви не може да се подреди. Поопшто, ако R е интегрален домен со својството $(\exists x)\ x^2 + 1 = 0$, тогаш R не може да се подреди.

6. Интегралниот домен на целите броеви може да се подреди само на еден начин

7. Нека $R = \mathbf{Z}[x] = \{a_0 + a_1 x + \cdots + a_n x^n | a_0, \ldots, a_n \in \mathbf{Z}\}$ е доменот на полиноми со цели коефициенти, при што полиномите се собираат и се множат на обичниот начин. Да ставиме:

$$R_1^+ = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_0 > 0 \vee (\exists k)\ a_0 = \ldots = a_{k-1} = 0,\ a_k > 0\}$$

$$R_2^+ = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_n > 0\}.$$

Добиваме дека R_1^+, R_2^+ ги задоволуваат (1), (2) и (3) и покрај тоа што $R_1^+ \neq R_2^+$.

(На пример, $1 - x \in R_1^+$, $1 - x \in R_2^+$).

5.2. ПОДРЕДЕНИ ПОЛИЊА

За едно поле R велиме дека е *подредено* акко е подредено како интегрален домен. Сите својства, што се докажани во претходниот дел, се точни и за подредените полиња, а овде ќе докажеме уште неколку својства. Притоа, секаде (ако не биде инаку речено) ќе претпоставуваме дека R е подредено поле.

1°. Ако $x, y \in R$, тогаш:

(i) $0 < x \Leftrightarrow 0 < x^{-1}$; (ii) $x < 0 \Leftrightarrow x^{-1} < 0$;

(iii) $1 < x \Leftrightarrow 0 < x^{-1} < 1$;

(iv) $0 < x,\ 0 < y \Rightarrow (x < y \Leftrightarrow y^{-1} < x^{-1})$;

(v) $x < 0,\ y < 0 \Rightarrow (x < y \Leftrightarrow y^{-1} < x^{-1})$;

(vi) $x \neq 0 \Rightarrow |x^{-1}| = |x|^{-1}$.

Доказот му го препуштаме на читателот. Читателот би требало успешно да формулира (и да докаже) својства аналогни на 5.1. **11°.** (iv), (v), (vi), (viii) и (ix), за случаите кога соодветните експоненти се негативни.

Ако се имаат предвид својствата 5.1. **9°** и 4.7. **3°**, се добива дека:

2°. Полето $\mathbf{Q}$ на рационалните броеви е потполе од секое подредено поле R.

Да покажеме дека:

3° Ако $\mathbf{Q}^+$ се дефинира со:

$$\mathbf{Q}^+ = \left\{\frac{m}{n} \mid m \cdot n \in \mathbf{Z}^+,\ m, n \in \mathbf{Z}\right\} \tag{1}$$

тогаш $\mathbf{Q}$ станува подредено поле, уште повеќе, тоа е единственото подредување на $\mathbf{Q}$.

Доказ. Прво, да уочиме дека $\frac{m}{n} \in \mathbf{Q}^+$ акко $\frac{mk}{nk} \in \mathbf{Q}^+$, за кој било $k \in \mathbf{Z} \setminus \{0\}$. Од тоа следува дека $\mathbf{Q}^+$ е добро дефинирано подмножество од $\mathbf{Q}$, т.е. дека "еден рационален број е позитивен акко е позитивен секој рационален број еднаков со него". Од изнесеното следува дека можеме да претпоставиме соодветните именители да се позитивни, а тоа, пак, веднаш повлекува дека $\mathbf{Q}^+$ ги задоволува условите (1), (2) и (3) од 5.1. Со тоа покажавме дека $\mathbf{Q}$ е подредено поле.

Обратно, да претпоставиме дека $\mathbf{Q}$ е подредено, при што R^+ е множеството позитивни елементи. Тогаш, ако $m, n \in \mathbf{Z}^+$, имаме: $m, 1/n \in R^+$, па и $m/n \in R^+$, од што следува: $\mathbf{Q}^+ \subseteq R^+$, и $\mathbf{Q}^- \subseteq R^-$, што е можно само ако $\mathbf{Q}^+ = R^+$.

Од **2°** и **3°** следува и:

4°. $\mathbf{Q}$ е подредено потполе на секое подредено поле R. (Со други зборови: $\mathbf{Q}^+ = \mathbf{Q} \cap R^+$.)

Ако се искористи фактот дека не постои природен број m меѓу нула и еден, се добива дека, каков и да биде целиот број n, не постои цел број s, таков што $n < s < n + 1$. Ќе покажеме дека кај подредените полиња ситуацијата е поинаква.

5°. Ако $a, b \in R$ и ако $a < b$, тогаш постои $c \in R$, таков што $a < c < b$.

Доказ. Ако се искористи тоа што $\frac{1}{2} > 0$, добиваме дека $\frac{1}{2}a < \frac{1}{2}b$, така што

$$a = \frac{1}{2}a + \frac{1}{2}a < \frac{1}{2}a + \frac{1}{2}b < \frac{1}{2}b + \frac{1}{2}b = b.$$

Според тоа, ако ставиме $c = \frac{1}{2}(a + b)$, добиваме дека $a < c < b$.

Докажаното тврдење е познато и како својство за *густа подреденост* на подредените полиња.

Подреденото поле R се вика *архимедово* акко за секоја двојка позитивни елементи $a, b \in R^+$ постои природен број n, таков што $na > b$.

6°. $\mathbf{Q}$ е архимедово поле.

Доказ. Ако $a = \frac{m}{k}$, $b = \frac{s}{k}$, каде што $m, k, s \in \mathbf{Z}^+$, тогаш:

$(sk + 1)\ a > ska = sm \geqslant b$.

7°. Ако R е архимедово поле и ако $a, b, c \in R^+$, $a < 1$, $b > 1$, тогаш постојат природни броеви m и n, такви што:

$$a^m < c, \quad b^n > c.$$

Доказ. Нека $b = 1 + u$. Според 5.1. **11°.** (Vii), имаме: $b^k = (1+u)^k \geqslant 1 + ku$ за секој $k \in \mathbf{N}$. Имајќи предвид тоа што $u > 0$, добиваме дека постои $n \in \mathbf{Z}^+$, таков што $nu > c$, од што ќе следува: $b^n \geqslant 1 + nu > c$.

Поради $0 < a < 1$, имаме $a^{-1} > 1$, па, според тоа, $(a^{-1})^m > c^{-1}$ за некој $m \in \mathbf{Z}^+$, т.е. $a^m < c$. ∎

Содржината на поимите: најмал (најголем) елемент, минорант (мајорант), инфимум (супремум) кај едно подредено множество е објаснета во 1.6. Овде ќе докажеме неколку тврдења, при претпоставка дека R е подредено поле, напомнувајќи дека дел од тврдењата важат и за кој било подреден домен.

8°. (i) Во R нема најмал, ниту најголем елемент.

(ii) Ако $a \in R$ и ако $_R(a) = \{x \mid x \in R,\ x < a\}$, $(a)_R = \{x \mid x \in R,\ a < x\}$, тогаш ниедно од множествата $(a)_R$, $_R(a)$ нема најмал, ниту најголем елемент.

Доказ. (i) Ако $b \in R$, тогаш $b - 1 < b < b + 1$.

(ii) Ако $b \in (a)_R$, $c \in {}_R(a)$, тогаш $b + 1 \in (a)_R$, $c - 1 \in {}_R(a)$, а според, **5°**, постојат $r, s \in R$, такви што: $a < r < b$, $c < s < a$. ∎

Нека A и B се подмножества на R. Подмножествата $-A$, $A + B$ и $A \cdot B$ се дефинираат со:

$$\begin{aligned} -A &= \{-x \mid x \in A\} \\ A + B &= \{x + y \mid x \in A,\ y \in B\} \\ AB &= \{xy \mid x \in A,\ y \in B\}. \end{aligned} \tag{2}$$

На пример, ако $A = \{-1, 0, 1, 2\}$, $B = \{-2, 0, -1, 3\}$, тогаш:

$$-A = \{-2, -1, 0, 1\},\quad -B = \{-3, 0, 1, 2\},$$

$$A + B = \{-3, -2, -1, 0, 1, 2, 3, 4, 5\},\quad AB = \{-4, -3, -2, -1, 0, 1, 2, 3, 6\}.$$

9°. (i) $-\inf(A) = \sup(-A)$;

(ii) $\sup A + \sup B = \sup(A + B)$;

(iii) $\inf A + \inf B = \inf(A + B)$.

(Притоа во (ii) и (iii) се претпоставува егзистенција на соодветната лева страна, од што следува егзистенција и на десната страна, како и соодветното, равенство.)

Доказ. (i) Нека $\inf A = b$; ако $x \in -A$, тогаш $-x \in A$, така што $b \leqslant -x$, т.е. $x \leqslant -b$; според тоа, $-b$ е мајорант за $-A$; ако $c < -b$, тогаш $b < -c$, така што $a < -c$, за некој $a \in A$, т.е. $c < -a$, од што следува дека c не е мајорант на $-A$.

(ii) Нека $\sup A = c$, $\sup B = d$; ако $x \in A + B$, тогаш $x = a + b$, $a \in A$, $b \in B$, па, значи, $c + d \geqslant a + b = x$, т.е. $c + d$ е мајорант на $A + B$. Нека $u < c + d$, и $c + d = u + 2h$, $h > 0$, т.е. $u = (c - h) + (d - h)$; постојат $a \in A$, $b \in B$, такви што $c - h < a$, $d - h < b$, така што ќе имаме: $u < a + b \in A + B$, па, значи, u не е мајорант на $A + B$. Со тоа докажавме дека $c + d = \sup(A + B)$.

(iii) Слично како и (ii), или, пак, да се добие како последица од (i) и (ii).■

10°. Ако R е архимедово поле и ако $A, B \subseteq R^+$, тогаш:

(i) $(inf\ A) \cdot (inf\ B) = inf\ (AB)$;

(ii) $(sup\ A)\ (sup\ B) = sup\ (AB)$.

Доказ. (i) Ако $c = inf\ A$, $d = inf\ B$, тогаш лесно се добива дека $u = cd$ е минорант на AB. Нека $u < z$, т.е. $zu^{-1} = h > 1$. Ќе определиме природен број n, таков што: $h > \left(\frac{n+1}{n}\right)^2 = 1 + \frac{2}{n} + \frac{1}{n^2}$. Имајќи го предвид тоа што $\frac{1}{n^2} \leqslant \frac{1}{n}$, доволно е да најдеме природен број n таков што $h > 1 + \frac{3}{n}$, т.е. $n(h-1) > 3$. Таков природен број n постои поради $h > 1$ и архимедовоста на R. Според тоа, имаме: $z = uh > cd \left(\frac{n+1}{n}\right)^2 = c\left(\frac{n+1}{n}\right) \cdot d\left(\frac{n+1}{n}\right)$. Од $c = inf\ A$, $d = inf\ B$ следува дека постојат $a \in A$, $b \in B$, такви што: $a < c\left(\frac{n+1}{n}\right)$, $b < d\left(\frac{n+1}{n}\right)$. Тогаш, ќе имаме: $ab \in AB$ и $ab < z$, така што заклучуваме дека u е најголемиот минорант на AB, т.е. $u = inf AB$.

(ii) Слично како и (i).■

11°. Ако R е архимедово поле и ако $a, b \in R$, $a < b$, тогаш постои рационален број r, таков што $a < r < b$.

Доказ. Нека $c = b - a$. Од $c > 0$ и архимедовоста на R следува дека постои $n \in \mathbf{Z}^+$, таков што $nc > 1$, т.е. $\frac{1}{n} < c$; да избереме еден таков број n, на пример, најмалиот. Постои $m \in \mathbf{Z}^+$, таков што $m = m \cdot 1 > na$; да го избереме најмалиот број m со таа особина; според тоа, ќе имаме $m - 1 \leqslant na$, т.е. $\frac{m-1}{n} \leqslant a$. Од сето тоа следува дека:

$$a < \frac{m}{n}\ ,\quad \frac{m}{n} = \frac{1}{n} + \frac{m-1}{n} < (b-a) + a = b,\quad \text{т.е.}\quad a < \frac{m}{n} < b.$$■

ВЕЖБИ: **2.** Ако $a, b \in \mathbf{Q}$, $a < b$, тогаш множеството $\{x \mid x \in \mathbf{Q},\ a < x < b\}$ е бесконечно. Притоа, наместо $\mathbf{Q}$, може да се земе кое било подредено поле.

3. Не постои рационален број a, таков што:

а) $a^2 + a + 1 = 0$; б) $1 + \frac{1}{a} = \frac{1}{a+1}$.

И овој заклучок важи за секое подредено поле.

4. Ако $n \in \mathbf{N}^+$, тогаш:

(i) $\frac{1}{2} \leqslant \frac{1}{n+1} + \ldots + \frac{1}{2n} < 1$; (ii) $\left(\frac{n+2}{n+1}\right)^{n+1} > 2$.

5. Ако R е подредено поле, тогаш:

(i) $\left(\frac{a+b}{2}\right)^2 \geqslant ab$; (ii) $\frac{1}{a} + \frac{1}{b} > \frac{1}{a+b}$; (iii) $a^4 + b^4 \geqslant a^3 b + ab^3$ за секои $a, b \in R^+$.

6. Ако $n \in \mathbf{N}^+$, тогаш множеството $A = \{x \mid x \in \mathbf{Q}^+, x^n \leqslant 2\}$ е мајорирано во $\mathbf{Q}$, но нема супремум во $\mathbf{Q}$.

7. Поимот за архимедовост може да се воведе и за подредени домени на наполно ист начин како и за подредени полиња.

(i) $\mathbf{Z}$ е архимедов домен.

(ii) Ако $\mathbf{Z}[x]$ е доменот од вежбата 5.1.7, и ако за позитивни ги сметаме сите полиноми $a_0 + a_1 x + \ldots + a_n x^n$, такви што $a_n > 0$, тогаш $\mathbf{Z}[x]$ станува неархимедов подреден домен.

(iii) Нека $R = \mathbf{Q}(x) = \left\{ \frac{a_0 + a_1 x + \ldots + a_m x^m}{b_0 + b_1 x + \ldots + b_n x^n} \;\middle|\; a_\nu, b_\lambda \in \mathbf{Q} \right\}$ е множеството од сите дробно рационални функции со рационални коефициенти. Ако се дефинира равенство во R како равенство на дропки, а собирање и множење како собирање на дропки, се добива дека R е поле. Ако, освен тоа, ставиме:

$$\frac{a_0 + a_1 x + \ldots + a_m x^m}{b_0 + b_1 x + \ldots + b_n x^n} \in R^+ \Leftrightarrow a_m b_n \in \mathbf{Q}^+$$

го претвораме R во неархимедово подредено поле.

5.3. КОМПЛЕТНИ ПОЛИЊА

За подреденото поле R велиме дека е *комплетно* акко секое минорирано непразно подмножество на R има инфимум во R. Имајќи го предвид својството 5.2. **9°**, добиваме дека:

1°. R е комплетно акко секое непразно мајорирано подмножество од R има супремум во R.

Натаму, не спомнувајќи го тоа посебно, ќе претпоставуваме дека R е комплетно (подредено) поле.

2°. R е архимедово поле.

Доказ. Да претпоставиме дека R не е архимедово. Тогаш, постојат $a, b \in R^+$, такви што $na \leqslant b$ за секој $n \in \mathbf{Z}^+$. Множеството $\{na \mid n \in \mathbf{Z}^+\} = A$ е мајорирано, бидејќи b е еден мајорант на A. Според **1°**, постои $c = \sup A$. Ако $n \in \mathbf{Z}^+$, тогаш $(n+1)a \in A$, така што $(n+1)a \leqslant c$, т.е. $na \leqslant c - a$, од што би следувало дека и $c - a$ е мајорант на A, што противречи на $c = \sup A$. Според тоа, не може да биде $na \leqslant b$ за секој $n \in \mathbf{Z}^+$, т.е. постои $m \in \mathbf{Z}^+$, таков што $ma > b$.

Ако $a \in R$, тогаш со $(a)_Q$ ќе го означуваме множеството од сите рационални броеви што се поголеми од a, т.е.

$$(a)_Q = \{x \mid x \in \mathbf{Q},\ x > a\}. \tag{1}$$

Натаму, ќе пишуваме (a), наместо $(a)_Q$.

3°. Ако $a, b \in R$, $c, d \in R^+$, тогаш:

(i) (a) е непразно множество без најмал елемент;

(ii) $(a) = (b) \Leftrightarrow a = b$;

(iii) $inf_R\,(a) = a$;

(iv) $(a) + (b) = (a + b)$;

(v) $(c)\,(d) = (cd)$.

Доказ. (i) Од $a < a + 1$, и 5.2. **11°**, следува дека $(a) \neq \varnothing$; дека (a) нема најмал елемент е јасно, исто така, од 5.2. **11°**.

(ii) Ако $a < b$, тогаш постои $r \in \mathbf{Q}$, таков што $a < r < b$, па би имале $r \in (a)$, но $r \notin (b)$.

(iii) Од (1) е јасно дека a е минорант на (a), а од 5.2. **11°** и дека тоа е најголемиот минорант на (a).

(iv) Прво, од (iii) и 5.2. **9°** следува дека $a + b$ е инфимум на $(a) + (b)$. Нека $r > a + b$, $r \in \mathbf{Q}$; ако $r = a + b + h$, постои $r_1 \in \mathbf{Q}$: $a < r_1 < a + \frac{h}{2}$; ако $r = r_1 + r_2$, тогаш:

$$r_2 = a + b + h - r_1 = b + \left(a + \frac{h}{2} - r_1\right) + \frac{h}{2} > b,$$

од што следува дека $r_1 \in (a)$, $r_2 \in (b)$, т.е. $r \in (a) + (b)$. Со тоа докажавме дека $(a) + (b) = (a + b)$.

(v) Како и во (iv), прво добиваме дека $(c)\,(d) \subseteq (cd)$. Нека $r \in (cd)$, т.е. $r \in \mathbf{Q}$ и $r = cdk$, каде што $k > 1$. Од архимедовоста на R следува дека може да се избере природен број n, таков што:

$$\left(1 + \frac{1}{n}\right)^2 \leqslant 1 + \frac{3}{n} < k.$$

Тогаш: $r > c\left(1 + \frac{1}{n}\right) \cdot d\left(1 + \frac{1}{n}\right)$. Нека $r_1 \in (c)$ е таков што $c < r_1 < c\left(1 + \frac{1}{n}\right)$; ако ставиме $r_2 = r \cdot r_1^{-1}$, добиваме

$r_2 = cdkr_1^{-1} > cd\left(1 + \frac{1}{n}\right)^2 r_1^{-1} > d\left(1 + \frac{1}{n}\right)$, т.е. $r_2 \in (d)$, од што конечно следува $r \in (c)\,(d)$. Со тоа докажавме: $(c)\,(d) = (cd)$. ∎

4°. Нека $S \subseteq \mathbf{Q}$. Постои елемент $a \in R$, таков што $(a) = S$ акко се исполнети следниве услови.

$$\varnothing \subset S \subset \mathbf{Q}; \tag{2}$$

S нема најмал елемент; (3)

$$s \in S,\ x \in \mathbf{Q},\ s \leqslant x \Rightarrow x \in S. \tag{4}$$

Доказ. Да потсетиме прво дека $(a) = \{x \mid x \in \mathbf{Q},\ a < x\}$. Нека S е подмножество на $\mathbf{Q}$ што ги задоволува условите (2), (3) и (4). Од (2) следува дека постои $t \in \mathbf{Q} \setminus S$, а од (4) добиваме дека t е минорант на S. Потоа, од комплетноста на R следува дека постои $a = inf_R\, S$. Ќе покажеме дека $(a) = S$. Нека $r \in (a)$, т.е. $r \in \mathbf{Q}$ и $a < r$; тогаш постои $s \in S$, таков што $s < r$, од што, според (4), ќе следува дека $r \in S$; според тоа, $(a) \subseteq S$. Нека $s \in S$; од (3) следува дека s не е најмал елемент на S, т.е. дека $s > a$ па значи, $s \in (a)$. Со тоа покажавме дека $(a) = S$. ∎

За едно подмножество S на $\mathbf{Q}$ велиме дека е *завршен интервал* во $\mathbf{Q}$ акко ги задоволува условите (2), (3) и (4). Множеството од сите такви подмножества на $\mathbf{Q}$ ќе го означуваме со $\mathbf{R}$.

Од **4°** следува дека:

5°. Со $f : a \to (a)$ е определена биекција од комплетното поле R во $\mathbf{R}$. ∎

Претходните својства беа подготовка за докажување на следново тврдење.

6°. Ако R и R' се комплетни полиња, тогаш тие се изоморфно подредени полиња.

Доказ. Нека $a \in R$. Според **5°**, $(a) = S$ е завршен интервал во $\mathbf{Q}$, од што' според **3°**, следува дека постои $a' \in R'$ (a' е еднозначно определен!), таков што $S = (a')$. Ако ставиме $g(a) = a'$, добиваме биекција од R во R'. Јасно е дека $a \in R^+ \Leftrightarrow a' = g(a) \in R^+$. Според **3°**, имаме $g(a + b) = g(a) + g(b)$ за секои $a, b \in R$ и $g(cd) = g(c) \cdot g(d)$ за секои $c, d \in R^+$. Според тоа, g е изоморфизам од $R(+)$ во $R'(+)$, од што следува $g(0) = 0$ и $g(-c) = -g(c)$, така што конечно добиваме и:

$$g((-c)\, d) = g(-(cd)) = -g(cd) = -[g(c)\ g(d)] = g(-c)\ g(d).$$

$$g((-c)\ (-d)) = g(cd) = g(c)\ g(d) = g(-c)\ g(-d).$$

Според, тоа g е изоморфизам и од $R(\cdot)$ во $R'(\cdot)$. ∎

Ако се има предвид тоа што не правиме разлика меѓу изоморфните алгебарски структури, од тукушто докажаното тврдење следува дека:

6′. Постои (до изоморфизам) најмногу едно комплетно поле. ∎

Се наметнува прашањето: Дали постои комплетно поле? Полето $\mathbf{Q}$ е единственото подредено поле со кое досега се сретнавме, па е природно да провериме дали тоа поле е комплетно. Имено, ќе покажеме, дека:

7°. **Q** не е комплетно поле.

Доказ. Нека $A = \{x \mid x \in \mathbf{Q}^+ \wedge x^2 \geqslant 2\}$. A е минорирано, бидејќи на пример, 1 е минорант на A. Да покажеме дека A нема инфимум во **Q**.

Прво, ќе покажеме дека не постои рационален број r, таков што $r^2=2$. Да претпоставиме дека $\left(\frac{m}{n}\right)^2 = 2$, каде $m, n \in \mathbf{Z}^+$ и притоа m и n се заемно прости; тогаш ќе имаме $m^2 = 2n^2$, од што следува дека $m = 2m_1$ е парен, а потоа, $2m_1^2 = n^2$ и дека $n = 2n_1$ е парен, што не е можно, бидејќи m и n, по претпоставка, се заемно прости.

Од докажаното следува дека: $A = \{x \mid x \in \mathbf{Q}^+,\ x^2 > 2\}$. Нека $a \in A$; тогаш $a^2 = 2 + h$, $h > 0$. Сакаме да покажеме дека постои $n \in \mathbf{Z}^+$, таков што $b = a - \frac{1}{n} \in A$, т.е. $a^2 - \frac{2}{n} \cdot a + \frac{1}{n^2} > 2$. Ако $2 + h = a^2 > 2 + \frac{2}{n} a$, т. е. $h > \frac{2}{n} a$, секако, ќе имаме $b^2 > 2$, т.е. $b \in A$; од архимедовоста на **Q** следува дека постои $n \in \mathbf{Z}^+$, таков што $nh > 2a$, т.е. $h > \frac{2}{n} a$. Со тоа докажавме дека A нема најмал елемент, од што следува дека позитивниот рационален број c е минорант на A акко $c^2 < 2$. Нека c е еден таков минорант; и нека $2 = c^2 + s$, $s > 0$; поради:

$$\left(c + \frac{1}{n}\right)^2 = c^2 + \frac{2}{n} + \frac{1}{n^2} \leqslant c^2 + \frac{3}{n} = 2 - s + \frac{3}{n},$$

ако n го избереме, така што $\frac{3}{n} < s$, т.е. $ns > 3$, ќе добиеме дека $c + \frac{1}{n}$ е минорант A, т.е. дека не постои најголем минорант на A. ∎

Својствата **3°**, **4°** и **5°** можат да се искористат како појдовни за конструкција на едно комплетно поле. Имено, според **5°**, ако R е комплетно поле, тогаш постои биекција f од R во множеството **R** на сите завршни интервали од **Q**, т.е. подмножества S на **Q** со својствата (2), (3) и (4). Ова ни сугерира да се обидеме да дефинираме операции на **R**, така што **R** да стане комплетно поле. Прво, собирањето на **R** се определува на обичен начин, т.е. со:

$$S_1, S_2 \in \mathbf{R} \Rightarrow S_1 + S_2 = \{x_1 + x_2 \mid x_1 \in S_1,\ x_2 \in S_2\}, \tag{5}$$

а, имено, оваа дефиниција произлегува од **3°** (iv).

Да покажеме дека:

8°. R $(+)$ е комутативна група.

Доказ [1]. Прво, се покажува дека збир на завршни интервали е завршен интервал, т.е. дека **R** $(+)$ е групоид.

[1]) До крајот на овој дел, ќе даваме само скици на соодветните докази.

Ако се има предвид тоа што $\mathbf{Q}(+)$ е комутативна полугрупа, се добива дека и $\mathbf{R}(+)$ е комутативна полугрупа.

Ако ставиме:

$$O = \{x \mid x \in \mathbf{Q},\ x > 0\} \tag{6}$$

добиваме дека O е нула на $\mathbf{R}(+)$.

И на крајот; ако за $S \in \mathbf{R}$, ^{-}S го дефинираме со:

$$^{-}S = \{-x \mid x \in \mathbf{Q} \setminus S,\ x \text{ не е најголем елемент во } \mathbf{Q} \setminus S\}, \tag{7}$$

добиваме $S + (^{-}S) = O$, т.е. дека ^{-}S е спротивен елемент на S во $\mathbf{R}(+)$, од што, конечно, следува дека $\mathbf{R}(+)$ е комутативна група.■

Читателот, веројатно, ќе се праша зошто во (7) е напишано ^{-}S, а не $-S$. Тоа се должи на фактот што, според 5.2. (2), би имале

$$-S = \{-x \mid x \in S\},$$

а ова не е исто со десната страна на (7). На пример, ако $S_1 = \{x \mid x > 1,\ x \in \mathbf{Q}\}$, тогаш:

$$-S_1 = \{y \mid y < -1,\ y \in \mathbf{Q}\},\ ^{-}S_1 = \{y \mid y > -1,\ y \in \mathbf{Q}\}.$$

За еден интервал $S \in \mathbf{R}$ велиме дека е *позитивен* акко во $\mathbf{Q} \setminus S$ има позитивни елементи. Множеството на сите позитивни интервали го означуваме со $\mathbf{R}^+$. Ако во S има и негативни елементи, тогаш велиме дека S е негативен, а множеството негативни интервали го изначуваме со $\mathbf{R}^-$. Нултиот интервал O не е ни позитивен, ни негативен. Според тоа:

9°. $\mathbf{R} = \mathbf{R}^- \cup \{O\} \cup \mathbf{R}^+$, при што унијата е дисјунктна.■

Освен тоа:

10°. (i) $\mathbf{R}^+$ и $\mathbf{R}^-$ се потполугрупи на $\mathbf{R}(+)$.

(ii) $S \in \mathbf{R}^+ \Leftrightarrow {}^{-}S \in \mathbf{R}^-$.■

Својството 3° (v) сугерира и множењето да се дефинира во $\mathbf{R}^+$ на обичниот начин, т.е. со:

$$S_1, S_2 \in \mathbf{R}^+ \Rightarrow S_1 S_2 = \{x_1 x_2 \mid x_1 \in S_1,\ x_2 \in S_2\}. \tag{8}$$

11°. $\mathbf{R}^+(\cdot)$ е комутативна група.

Доказ. Како и во **8°**, прво треба да се покаже дека производ на два позитивни интервали е позитивен интервал, т.е. дека $\mathbf{R}(\cdot)$ е групоид. Потоа, ако се има предвид комутативноста и асоцијативноста на множењето во $\mathbf{Q}^+$ се добива дека $\mathbf{R}^+(\cdot)$ е комутативна полугрупа.

Ако ставиме:

$$\mathbf{1} = \{x \mid x \in \mathbf{Q},\ x > 1\} \tag{9}$$

добиваме дека $\mathbf{1}$ е единица на $\mathbf{R}^+(\cdot)$. Исто така, ако $S \in \mathbf{R}^+$, тогаш:

$$S^{-1} = \{x \mid x^{-1} \in \mathbf{Q}^+ \setminus S,\ x^{-1} \text{ не е најголем во } \mathbf{Q}^+ \setminus S\} \tag{10}$$

е инверзен за S во $\mathbf{R}^+(\cdot)$.

Ако $S \in \mathbf{R}$; $S_1, S_2 \in \mathbf{R}^+$, тогаш ќе ги дефинираме производите $(^-S_1)S_2$, $S_1(^-S_2)$, $(^-S_1)(^-S_2)$, SO, OS, така што сакаме $\mathbf{R}(+,\cdot)$ да биде прстен. Ова ги наложува следниве дефиниции:

$$\begin{gathered}(^-S_1)\,S_2 = {}^-(S_1S_2),\ S_1(^-S_2) = {}^-(S_1S_2),\\ (^-S_1)(^-S_2) = S_1S_2,\ OS = O,\ SO = O.\end{gathered} \tag{11}$$

Конечно добиваме:

12°. $\mathbf{R}(+,\cdot)$ е комплетно подредено поле.

Доказ. (i) Според **8°**, $\mathbf{R}(+)$ е комутативна група.

(ii) Од **11°** и (11) следува дека $\mathbf{R}(\cdot)$ е комутативна полугрупа со единица, во која секој елемент S, различен од O, е инверзибилен.

(iii) Нека $S_1, S_2, S_3 \in \mathbf{R}^+$. Ако $x = x_1(x_2 + x_3)$, каде што $x_i \in S_i$, односно $x \in S_1(S_2 + S_3)$, тогаш $x = x_1x_2 + x_1x_3$, т.е. $x \in S_1S_2 + S_1S_3$. Според тоа: $S_1(S_2 + S_3) \subseteq S_1S_2 + S_1S_3$. Обратно, ако $y \in S_1S_2 + S_1S_3$, тогаш $y = y_1y_2 + y_1'y_3$, каде што $y_i, y_i' \in S_i$; ако, на пример, $y_1 \leqslant y_1'$, тогаш $y \geqslant y_1y_2 + y_1y_3 = y_1(y_2 + y_3)$, а $y_1(y_2 + y_3) \in S_1(S_2 + S_3)$, од што ќе следува дека $y \in S_1(S_2 + S_3)$. Со тоа докажавме дека

$$S_1(S_2 + S_3) = S_1S_2 + S_1S_3 \tag{12}$$

за секои $S_i \in \mathbf{R}^+$. Потоа, слично како и доказот на соодветното својство кај $\mathbf{Z}$ (3.2. **1°**), се добива дека (12) е точно за секои $S_i \in \mathbf{R}$.

(iv) Од (i), (ii) и (iii) следува дека $\mathbf{R}(+,\cdot)$ е поле. Потоа, ако се имаат предвид **9°** и **10°**, се добива дека $\mathbf{R}(+,\cdot)$ е подредено поле, при што $\mathbf{R}^+$ е множеството позитивни елементи. Како и кај секое подредено поле во $\mathbf{R}$ се дефинира подредување $<$. Притоа ќе имаме:

$$S_1, S_2 \in \mathbf{R} \Rightarrow (S_1 < S_2 \Leftrightarrow S_2 \subset S_1). \tag{13}$$

(v) Да претпоставиме дека A е минорирано подмножество на $\mathbf{R}$. Според тоа, постои $S_0 \in \mathbf{R}$, таков што $S_0 \leqslant S$, т.е. $S \subseteq S_0$, за секој $S \in A$. Ако ја означиме со S_1 унијата на сите интервали од A, тогаш се добива дека $S_1 = \inf A$. Според тоа, $\mathbf{R}(+,\cdot)$ е комплетно подредено поле.

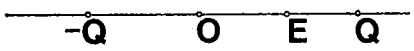
Од својствата **6°** и **12°** следува дека:

13°. Секое комплетно поле е изоморфно со полето **R**.

Натаму, елементите на **R** ќе ги викаме *реални броеви.* Притоа, ќе го користиме само фактот што $\mathbf{R}(+, \cdot)$ е комплетно поле, а не и тоа што елементите на **R** се завршни интервали во **Q**. Во оваа смисла, според 5.2. **4°**, ќе сметаме и дека **Q** е потполе на **R**, така што рационалните броеви се реални. Последното се постигнува на тој начин, што рационалниот број a се смета за еднаков со интервалот $S_a = \{x \mid x \in \mathbf{Q},\ x > a\}$. Да напомнеме дека овде се користи својството 4.6. **2°** односно се раководиме од спроведената дискусија по докажувањето на тоа својство.

За еден реален број велиме дека е *ирационален број* ако не е рационален. Според ова, интервалот $S \in \mathbf{R}$ е ирационален број акко не постои инфимум на S во **Q**.

Да забележиме дека постојат и други конструкции на комплетно подредено поле. За учениците, веројатно, е најблизок геометрискиот пристап, според кој, реални броеви се точките од една ориентирана права. Ориентирањето на правата се врши на тој начин, што се избираат две точки: нулта (0) и единична (E). Точките што се на иста страна од 0 како и E се викаат *позитивни*, а оние на спротивната страна — *негативни*. Операциите собирање



и множење се дефинираат со помош на собирање, односно множење, на отсечки. Но, оваа конструкција на реалните броеви бара претходна аксиоматска изградба на геометријата. (И покрај тоа што во наставата по математика во основно и средно училиште се прави очигледна логичка грешка со тоа што реалните броеви се дефинираат геометриски, а од друга страна, тие се користат во геометријата, сметаме дека треба и натаму свесно да се прави оваа грешка. Сепак, неопходно е да му се објасни на ученикот дека се работи само за илустрација и дека тоа не е строга градба на математичката теорија.).

ВЕЖБИ. **2.** Да се даде пример на подреден интегрален домен R што не е поле, но секое мајорирано подмножество од R да има супремум во R.

3. Нека $a = sup\ A$, каде $A = \{x \mid x \in \mathbf{Q}^+,\ x^2 \leqslant 2\}$. Да се покаже дека a е ирационален број.

4. Ако a е ирационален број, тогаш: $x \to x + a$ е инјекција од **Q** во множеството ирационални броеви **J**.

5. Ако r и s се рационални броеви $r < s$ и ако a е ирационален број, таков што $a > 1$ (таков е, на пример, бројот од вежбата **3**), тогаш $b = r + (s - r)\, a^{-1}$ е ирационален број, таков што: $r < b < s$.

6. Ако c и d се реални броеви, тогаш постои ирационален број b, таков што: $c < b < d$.

7. Низата реални броеви $(a_n \mid n \in \mathbf{N})$ се наречува *конвергентна* акко постои реален број a, таков што: за секој позитивен реален број h постои природен број m, таков што: $n \geqslant m \Rightarrow |a - a_n| < h$. Тогаш, велиме дека a е граница на низата и пишуваме $a = lim\ a_n$. Границата на една конвергентна низа е еднозначно определена.

8. За низата $(a_n \mid n \in \mathbf{N})$ велиме дека е *Кошиева* акко: за секој реален позитивен број h постои природен број m, таков што:

$$k, n \in \mathbf{N},\ n \geqslant m \Rightarrow |\, a_n - a_{n+k} \,| < h.$$

Една низа е конвергентна во $\mathbf{R}$ акко е Кошиева.

9. Поимот за конвергентна, односно Кошиева низа е осмислен кај секое подредено поле R. Ако низите $(a_n \mid n \in \mathbf{N})$, $(b_n \mid n \in \mathbf{N})$ се Кошиеви, тогаш такви се и $(a_n + b_n \mid n \in \mathbf{N})$ $(a_n\, b_n \mid n \in \mathbf{N})$.

* **10.** Нека K е множеството од сите Кошиеви низи во $\mathbf{Q}$.

(i) Ако ставиме

$$(a_n \mid n \in \mathbf{N}) + (b_n \mid n \in \mathbf{N}) = (a_n + b_n \mid n \in \mathbf{N})$$

$$(a_n \mid n \in \mathbf{N}) \cdot (b_n \mid n \in \mathbf{N}) = (a_n\, b_n \mid n \in \mathbf{N}),$$

тогаш добиваме комутативен прстен $K(+, \cdot)$. со нула $(0 \mid n \in \mathbf{N})$ и единица $(1 \mid n \in \mathbf{N})$.

(ii) Ако во K дефинираме релација $\approx$ со:

$$(a_n \mid n \in \mathbf{N}) \approx (b_n \mid n \in \mathbf{N}) \Leftrightarrow lim\ (a_n - b_n) = 0,$$

добиваме релација $\approx$ што е конгруенција на $K(+, \cdot)$ и притоа фактор прстенот $R = K/\!\approx$ е поле.

(iii) Една низа $(a_n \mid n \in \mathbf{N}) \in K$ се вика позитивна акко постои позитивен рационален број h, таков што $h < a_n$ за секој $n \in \mathbf{N}$. Нека $(a_n \mid n \in \mathbf{N}) \approx (b_n \mid n \in \mathbf{N})$. Тогаш: $(a_n \mid n \in \mathbf{N})$ е позитивна акко $(b_n \mid n \in \mathbf{N})$ е позитивна.

(iv) Нека R^+ се состои од сите позитивни класи од $R = K/\!\approx$. Тогаш R^+ е множеството позитивни елементи на R, така што R е подредено поле.

(v) R е комплетно подредено поле. Поради ова, ако се има предвид својството **6′**, можеме да речеме дека R е полето на реалните броеви.

5.4. КОРЕНИ

Нека $a, b \in \mathbf{R}$, $n \in \mathbf{N}^+$. Ако $b^n = a$, тогаш велиме дека b е *n-ти корен* на a и пишуваме $b = \sqrt[n]{a}$. Според тоа:

$$\boxed{b = \sqrt[n]{a} \Leftrightarrow b^n = a.} \tag{1}$$

Од дадената дефиниција следува дека:

1°. $\sqrt[n]{0} = 0$, $\sqrt[1]{a} = a$ за секои $a \in \mathbf{R}$, $n \in \mathbf{N}^+$. ■

Пред да докажеме егзистенција на корени, ќе докажеме неколку својства.

2°. Нека $n = 2k$ е парен број $(k \geqslant 1)$ и нека $a \in \mathbf{R}$.

(i) Ако $a < 0$, тогаш $\sqrt[n]{a}$ не постои.

(ii) Ако $a > 0$, и ако постои $\sqrt[n]{a} = b$, тогаш имаме и $-b = \sqrt[n]{a}$, и притоа b и $-b$ се единствените вредности на $\sqrt[n]{a}$.

Доказ. (i) Според 5.1. **11°**, имаме $x^n \geqslant 0$ за секој $x \in \mathbf{R}$, од што следува заклучокот.

(ii) Ако $b^n = a$, тогаш $(-b)^n = b^n = a$. Ако $0 < b < c$, тогаш, според 5.1. **11°**, $b^n < c^n$.

3°. Ако $n = 2k + 1$ $(k \geqslant 0)$ е непарен број и $a \in R$, тогаш постои најмногу една вредност на $\sqrt[n]{a}$ и притоа: $\sqrt[n]{a} = b \Leftrightarrow \sqrt[n]{-a} = -b$.

Доказ. Ако $b < c$, тогаш $b^n < c^n$. Исто така: $b^n = a \Leftrightarrow (-b)^n = -a$.

Ќе го решиме прашањето за егзистенција на корени.

4°. Нека $a > 0$, $n \in \mathbf{N}^+$. Постои еден и само еден позитивен реален број b, таков што $b^n = a$, т.е. $b = \sqrt[n]{a}$.

Доказ. Да го разгледаме множеството $\{x \mid x \in \mathbf{R}^+,\ x^n \geqslant a\} = A$. Множеството A е минорирано, бидејќи, на пример, 0 е еден минорант, па, според тоа, постои $\inf A = b$. Ќе покажеме дека $b^n = a$.

Да претпоставиме дека $b^n > a$, т.е. $b^n = a + h$, $h > 0$. Ако природниот број m го избереме така што $mb > 1$, тогаш, според 5.1. **11°**, ќе имаме:

$$\left(b - \frac{1}{m}\right)^n = b^n \left(1 - \frac{1}{bm}\right)^n \geqslant b^n \left(1 - \frac{n}{bm}\right) = b^n - \frac{nb^{n-1}}{m}.$$

Потоа, ако претпоставиме и дека $mh > nb^{n-1}$ ќе добиеме:

$$\left(b - \frac{1}{m}\right)^n \geqslant a + h - \frac{nb^{n-1}}{m} > a,$$

т.е. $b - \frac{1}{m} \in A$, што не е можно бидејќи b е инфимум на A.

Нека $b^n < a$. Ќе покажеме дека постои природен број m, таков што $\left(b + \frac{1}{m}\right)^n < a$, од што би следувало дека $b + \frac{1}{m}$ е минорант на A и тоа по голем од инфимумот b што не е можно. Прво да го избереме m така што $mb > 1$. Тогаш имаме:

$$\left(b + \frac{1}{m}\right)^n = b^n + \binom{n}{1} b^{n-1}\left(\frac{1}{m}\right) + \binom{n}{2} b^{n-2}\left(\frac{1}{m}\right)^2 + \ldots + \binom{n}{n} \cdot \left(\frac{1}{m}\right)^n$$

$$< b^n + \left[\binom{n}{1} + \ldots + \binom{n}{n}\right] b^{n-1} \cdot \frac{1}{m} = b^n + (2^n - 1)\, b^{n-1} \cdot \frac{1}{m}.$$

Ако $a = b^n + q$, и ако m го избереме така што (покрај од b^{-1}) да биде поголем од $(2^n - 1)\, b^{n-1} \cdot q^{-1}$, ќе добиеме $\left(b + \frac{1}{m}\right)^n < a$.

Од сето тоа следува дека мора да биде $b^n = a$. Потоа, до изнесениот заклучок се доаѓа со помош на **2°** и **3°**.

Од **2°** и **4°** следува дека за $a > 0$ и $n = 2k$ ($k \geqslant 1$) парен, постојат точно две вредности на коренот $\sqrt[2k]{a}$, едната од кои е позитивна b, а другата е $-b$. Со цел да биде запазена еднозначноста на $\sqrt[n]{a}$, натаму (при $a > 0$) со $\sqrt[2k]{a}$ ќе ја означуваме само позитивната вредност на коренот, додека со $-\sqrt[2k]{a}$ ќе ја означуваме соодветната негативна вредност. Велиме дека $\sqrt[2k]{a}$ е *аритметичка вредност* на коренот.

Според тоа, имаме.

5° (i) Ако $a > 0$, тогаш $\sqrt[n]{a}$ е еднозначно определен реален број за секој природен број n ($\geqslant 1$) и притоа $\sqrt[n]{a} > 0$.

(ii) Ако $a < 0$, тогаш $\sqrt[n]{a}$ постои акко n е непарен; притоа $\sqrt[n]{a} < 0$, и $\sqrt[n]{-a} = -\sqrt[n]{a}$.

Користејќи го својството на степени со природни експоненти, како и дефиницијата на корените, лесно се докажува точноста на следното својство.

6° Точни се равенствата:

$$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab},\quad \sqrt[n]{a} / \sqrt[n]{b} = \sqrt[n]{a/b},\quad (\sqrt[n]{a})^m = \sqrt[n]{a^m},\quad \sqrt[n]{a} = \sqrt[nm]{a^m},\quad \sqrt[n]{\sqrt[m]{a}} = \sqrt[nm]{a}.$$

Притоа, се претпоставува дека секој од корените постои.

Да напомнеме дека претпоставката за егзистенција на корените е битна. На пример, $\sqrt{(-2)(-3)} = \sqrt{6}$ постои, но производот $\sqrt{-2} \cdot \sqrt{-3}$ не постои, па, значи, не може да го сметаме за точно равенството $\sqrt{-2} \cdot \sqrt{-3} = \sqrt{6}$.

Ако n е непарен број, јасна е точноста на равенството $\sqrt[n]{a^n} = a$, но не е ист случајот и кога $n = 2m$ е парен број. На пример, имаме $\sqrt[4]{(-2)^4} = 2$, а не -2, бидејќи веќе се договоривме под $\sqrt[2k]{b}$ да ја подразбираме позитивната вредност на коренот. Значи, точно е следново својство.

7° $\sqrt[2m]{a^{2m}} = |a|$, $\sqrt[2m+1]{a^{2m+1}} = a$.

Ако се имаат предвид својствата 7° и 5.1. **11**°, се добива:

8°. Нека a и b се позитивни реални броеви, а m и n позитивни цели броеви. Тогаш:

(i) $a < b \Leftrightarrow \sqrt[n]{a} < \sqrt[n]{b}$;

(ii) $a > 1 \Rightarrow (m < n \Leftrightarrow \sqrt[n]{a} < \sqrt[m]{a})$;

(iii) $a < 1 \Rightarrow (m < n \Leftrightarrow \sqrt[m]{a} < \sqrt[n]{a})$;

(iv) $\sqrt[n]{1+a} \leqslant 1 + \frac{a}{n}$.

Доказ. Ќе го докажеме само својството (iv). Ако ставиме $\sqrt[n]{1+a} = 1+h$, добиваме $1 + a = (1+h)^n \geqslant 1 + nh$, т.е. $h \leqslant \frac{a}{n}$. ∎

9°. Нека $a > 1$, $0 < b < 1$. За секој позитивен реален број c постојат природни броеви $m, n \in \mathbf{N}^+$, такви што:

(i) $\sqrt[m]{a} < 1 + c$; (ii) $\sqrt[n]{b} > 1 - c$.

Доказ. (i) Имаме $(1+c)^m \geqslant 1 + cm$; ако m го избереме, така што $m > \frac{a-1}{c}$, ќе добиеме $a < (1+c)^m$, т.е. $\sqrt[m]{a} < 1 + c$.

(ii) Ако $c \geqslant 1$, неравенството е точно за секој позитивен број n. За $c < 1$, имаме $1 - c < 1$, $(1-c)^{-1} = 1 + d$, $d > 0$. Тогаш, според (i), постои $n \in \mathbf{Z}^+$, таков што

$$\left(\sqrt[n]{b}\right)^{-1} = \sqrt[n]{b^{-1}} < 1 + d = (1-c)^{-1}, \text{ т.е. } 1 - c < \sqrt[n]{b}.$$ ∎

ВЕЖБИ. **2.** Да се упростат изразите:

а) $\sqrt{(1-\sqrt{2})^2}$;

б) $\sqrt{4-2\sqrt{3}}$;

в) $\sqrt{75-12\sqrt{21}}$;

г) $\sqrt{17+4\sqrt{9-4\sqrt{5}}}$;

д) $\sqrt{\sqrt{5}-\sqrt{3-\sqrt{29-12\sqrt{5}}}}$.

3. Да се рационализираат именителите во изразите:

а) $\frac{6}{(3+\sqrt{2})-\sqrt{3}}$; б) $\frac{1}{\sqrt[4]{3}+\sqrt[4]{9}+\sqrt[4]{27}+3}$; в) $\frac{1}{\sqrt[8]{3}+\sqrt[8]{2}}$.

4. Нека $\mathcal{Q}(\sqrt{2})$ е множеството на сите реални броеви од облик $a + b\sqrt{2}$, каде што a и b се рационални. Да се покаже дека $\mathcal{Q}(\sqrt{2})$ е поле.

5. Дали бројот $\sqrt[3]{4}$ може да се напише во облик $\sqrt[3]{4} = a + b\sqrt[3]{2}$, каде што a и b се рационални?

6. Да се покаже дека за секој позитивен природен број n се точни неравенствата:

а) $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} \geqslant \sqrt{n}$;

б) $\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{2n+1}}$.

7. Да се покаже дека за секој позитивен природен број n и секоја n-ка позитивни реални броеви $a_1, a_2, \ldots, a_n$ е точно неравенството

$$a_1 + a_2 + \cdots + a_n \geqslant n\sqrt[n]{a_1 a_2 \ldots a_n}.$$

Упатство. Да се покаже прво дека тоа неравенство е точно за секој n од облик $n = 2^k$. Потоа, претпоставувајќи дека тоа неравенство е точно за $n = m$, и определувајќи го бројот x од равенството

$$\sqrt[m]{a_1 a_2 \ldots a_{m-1} x} = \sqrt[m-1]{a_1 a_2 \ldots a_{m-1}},$$

да се покаже точноста на неравенството и за $n = m - 1$.

8. Користејќи го резултатот од претходната вежба (или директно), да се докаже точноста на следниве неравенства:

а) $a + b \geqslant \sqrt{a^2 + b^2}$;

б) $(a + b)\sqrt{ab} \geqslant 2ab$;

в) $a + nb \geqslant (n + 1)\sqrt[n+1]{ab^n}$;

г) $a + b + \alpha + \beta \geqslant 2\sqrt{(a + \alpha)(b + \beta)}$;

д) $\sqrt{(a + \alpha)(b + \beta)} \geqslant \sqrt{ab} + \sqrt{\alpha\beta}$;

ѓ) $a + b + c \geqslant \sqrt{ab} + \sqrt{bc} + \sqrt{ab}$,

каде што a, b, c, α, β се позитивни реални броеви.

5.5. СТЕПЕНИ СО РЕАЛНИ ЕКСПОНЕНТИ

Како и кај секое поле, во $\mathbf{R}$ е осмислен поимот за степен со цели експоненти. Имено, ако $a \neq 0$, степенот a^n има смисла за секој $n \in \mathbf{Z}$, додека $0^n = 0$ за секој $n \in \mathbf{N}^+$. Поимот за степен a^r со каков било рационален експонент r се дефинира акко $a > 0$ и тоа со:

$$a^{\frac{m}{n}} = \sqrt[n]{a^m} \tag{1}$$

каде што $n \in \mathbf{Z}^+$.

Поради $\frac{m}{n} = \frac{mk}{nk}$, се наложува прашањето дали е точно и равенството

$$a^{\frac{m}{n}} = a^{\frac{mk}{nk}}.$$

Дека тоа равенство е точно, се гледа од равенството

$$\sqrt[nk]{a^{mk}} = \sqrt[n]{a^m}.$$

Ако $\frac{m}{n} = k$ е цел број, т.е. $m = nk$, тогаш

$$a^{\frac{m}{n}} = \sqrt[n]{a^{nk}} = a^k,$$

така што поимот за степен со цели експоненти е специјален случај од поимот за степен со рационални експоненти.

Според тоа, за секој рационален број r и позитивен реален број a, степенот a^r е еднозначно определен број. Претпоставката, основата a да биде позитивен број, се прави за да постои степенот a^r за секој рационален број r. Ако $r > 0$, природно е да се стави $0^r = 0$. За $a<0$, ако m и n се заемно прости и притоа n е непарен природен број, можеме $a^{\frac{m}{n}}$ да сметаме дека е определен со $\sqrt[n]{a^m}$. Дека претпоставката за непарност на n е потребна, лесно се уочува од следниов пример: поради $\sqrt[8]{(-2)^6} = \sqrt[4]{8}$ би требало да имаме $(-2)^{\frac{6}{8}} = \sqrt[4]{8}$, но од друга страна, поради $\frac{6}{8} = \frac{3}{4}$, $(-2)^{\frac{3}{4}} = \sqrt[4]{-8}$ не постои.

Користејќи ги својствата на корените и степените со цели експоненти лесно се докажуваат наредните две својства.

1°. Ако a и b се позитивни реални броеви, а r и s рационални, тогаш се точни равенствата:

$$a^r a^s = a^{r+s},\ (ab)^r = a^r b^r,\ (a/b)^r = a^r/b^r,\ (a^r)^s = a^{rs}.$$

2°. (i) $a > 1,\ r > s \Rightarrow a^r > a^s.$

(ii) $0 < a < 1,\ r > s \Rightarrow a^s > a^r.$

Својствата што сега ќе ги докажеме ќе нè доведат до поимот за степен со произволен реален експонент.

3°. Ако $a \in \mathbf{R}^+$, $a > 1$, тогаш:

$$\inf\{a^x \mid x \in \mathbf{Q}^+\} = 1.$$

Доказ. Пред сè, 1 е минорант на $\{a^x \mid x \in \mathbf{Q}^+\}$. Ако $c > 0$, тогаш, според 5.4.**9**°, постои $n \in \mathbf{Z}^+$, таков што $a^{1/n} = \sqrt[n]{a} < 1 + c$, од што и следува заклучокот. ∎

4°. Нека $a \in \mathbf{R}^+$, $a > 1$ и нека r е даден рационален број. Точно е равенството:

$$inf\{a^x \mid x \in \mathbf{Q},\ x > r\} = a^r. \tag{2}$$

Доказ. Се користи равенството

$$\{a^x \mid x \in \mathbf{Q},\ x > r\} = \{a^y \mid y \in \mathbf{Q}^+\} \cdot \{a^r\},$$

и својствата **3°** и 5.2.**10°**. ∎

Да претпоставиме сега дека a и b се дадени реални броеви, при што $a \geqslant 1$. Тогаш a^b се дефинира со:

$$a^b = inf\{a^x \mid x \in \mathbf{Q},\ x > b\}. \tag{3}$$

За $0 < a < 1$, a^b се определува со:

$$a^b = ((a^{-1})^b)^{-1}. \tag{3'}$$

Така добиваме дека при $a > 0$, за секој реален број b, a^b е еднозначно определен реален број. Притоа, ако b е рационален, според **4°**, новиот поим за степен се совпаѓа со порано дадената дефиниција за степени со рационални експоненти.

Својствата **1°** и **2°** се пренесуваат и на степени со реални експоненти.

1′. Нека a и b се позитивни реални броеви, а c и d какви било реални броеви. Точни се следниве равенства:

(i) $a^c \cdot a^d = a^{c+d}$; (ii) $(ab)^c = a^c \cdot b^c$; (iii) $(a^c)^d = a^{c \cdot d}$.

Доказ. (i) Нека $a > 1$. Тогаш:

$$\begin{aligned} a^c \cdot a^d &= inf\{a^x \mid x \in \mathbf{Q},\ x > c\} \cdot inf\{a^y \mid y \in \mathbf{Q},\ y > d\} \\ &= inf(\{a^x \mid x \in \mathbf{Q},\ x > c\} \cdot \{a^y \mid y \in \mathbf{Q},\ y > d\}) \\ &= inf\{a^{x+y} \mid x, y \in \mathbf{Q},\ x + y > c + d\} \\ &= inf\{a^z \mid z \in \mathbf{Q},\ z > c + d\} \\ &= a^{c+d}. \end{aligned}$$

За $0 < a < 1$ имаме:

$$a^c \cdot a^d = [(a^{-1})^c]^{-1}\,[(a^{-1})^d]^{-1} = [(a^{-1})^c \cdot (a^{-1})^d]^{-1}$$
$$= (a^{-1})^{c+d}]^{-1} = a^{c+d}.$$

За $a = 1$, точноста е јасна.

(ii) На сосема ист начин како и во (i).

Доказот на равенството (iii) бара малку пообемна работа, па затоа ќе се задоволиме со тоа што ќе го посоветуваме читателот да консултира соодветна литература, како, на пример, [7]. И докажите на следниве особини (или упатства) можат да се најдат во спомнатата книга.

2′. (i) $a > 1 \Rightarrow (b > c \Leftrightarrow a^b > a^c)$;
(ii) $0 < a < 1 \Rightarrow (b < c \Leftrightarrow a^b > a^c)$.

5°. Ако $a, b \in \mathbf{R}^+$, $a \neq 1$, тогаш постои еднозначно определен реален број c, таков што $a^c = b$. Овој број c се вика *логаритам* од b при основа a и се означува со $\log_a b$, т.е.

$$\log_a b = c \Leftrightarrow a^c = b. \tag{4}$$

6°. Ако $a, b, c \in \mathbf{R}^+$, $a \neq 1$, тогаш:

(i) $\log_a bc = \log_a b + \log_a c$;

(ii) $\log_a \dfrac{b}{c} = \log_a b - \log_a c$;

(iii) $\log_a b^c = c \cdot \log_a b$;

(iv) $a > 1 \Rightarrow (b < c \Leftrightarrow \log_a b < \log_a c)$;

(v) $a > 1 \Rightarrow (\log_a b > 0 \Leftrightarrow b > 1)$.

ВЕЖБИ. **1.** Да се докаже својството 6°, претпоставувајќи точност на претходните својства.

2. Во кој случај се еквивалентни равенките: $log\, f^2(x) = 0$, $log\, f(x) = 0$?

5.6 ДЕСЕТИЧНИ ДРОПКИ

Ако $a_0, \ldots, a_k \in \mathbf{N}$, $a_i < 10$ за $i \geqslant 1$, тогаш бројот

$$a = a_0 + a_1 \cdot 10^{-1} + \ldots + a_k \cdot 10^{-k} \tag{1}$$

се вика *конечна десетична дропка* и се означува со

$$a_0, a_1 \ldots a_k. \tag{1′}$$

Притоа, a_0 се вика *цел дел* на a и се означува со $[a]$, а $a_1, \ldots, a_k$ се *децимали* на a; запирката "," се вика *десетична запирка*.

Со следново тврдење се дава карактеристика на конечните десетични дропки.

1°. (i) Секоја конечна десетична дропка е ненегативен рационален број.

(ii) Нека $a = \frac{c}{d} \in \mathbf{Q}^+$, $c, d \in \mathbf{N}^+$, $(c; d) = 1$. Бројот a е конечна дестична дропка акко d може да се претстави во облик $d = 2^\alpha 5^\beta$, каде што $\alpha, \beta \in \mathbf{N}$.

Доказ. (i) Ова е јасно од (1).

(ii) Нека $d = 2^\alpha 5^\beta$ и нека $\gamma = max\{\alpha, \beta\}$. Тогаш

$$a = 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta} c \cdot 10^{-\gamma}.$$

Претставувајќи го бројот $c_1 = 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta} c$ во десетичен систем и множејќи со $10^{-\gamma}$, ќе добиме дека a има облик (1), т.е. дека е конечна десетична дропка.

Да претпоставиме сега дека $a = \frac{c}{d}$ е конечна десетична дропка, т.е.

$$\frac{c}{d} = a_0 + a_1 10^{-1} + \ldots + a_k 10^{-k} = \frac{10^k a_0 + 10^{k-1} a_1 + \ldots + a_k}{10^k}.$$

Тогаш: d е делител на $10^k c$ што, поради $(c; d) = 1$ е можно само ако $d \mid 10^k$, а од тоа следува дека d има облик $d = 2^\alpha 5^\beta$, каде што $\alpha \leqslant k$, $\beta \leqslant k$. ∎

И покрај тоа што само еден "мал дел" од множеството на рационалните броеви е претставено со множеството конечни дропки, сепак (што, впрочем, на читателот му е добро познато) во практичното оперирање со броеви до израз доѓаат само конечните десетични дропки. Својството што сега ќе го докажеме претставува едно образложение на оваа пракса.

2°. Нека $a \in \mathbf{R}^+$. Постои еднозначно определена низа од природни броеви $(a_n \mid n \in \mathbf{N})$ што ги задоволува следниве својства:

(i) $n \geqslant 1 \Rightarrow a_n \leqslant 9$

(ii) $a_0, a_1 \ldots a_n \leqslant a < a_0, a_1 \ldots a_n + 10^{-n}$, за секој $n \geqslant 1$.

Доказ. Од архимедовоста на $\mathbf{R}$ следува дека постои природен број m, таков што $a < m + 1$; ако a_0 е најмалиот природен број со тоа својство, тогаш имаме:

$a_0 \leqslant a < a_0 + 1$; од друга страна, јасно е дека a_0 е единствениот природен број со ова совјство. Потоа, постои еднозначно определен природен број a_1, таков што $a_1 \leqslant 9$ и:

$$a_0, a_1 \leqslant a < a_0, a_1 + 10^{-1}.$$

Претпоставувајќи дека е определена низата природни броеви $(a_0, a_1, \ldots, a_n)$, таква што (i) и (ii) се точни, добиваме дека постои еднозначно определен природен број a_{n+1}, таков што $a_{n+1} \leqslant 9$ и:

$$a_0, a_1 a_2 \ldots a_{n+1} \leqslant a < a_0, a_1 \ldots a_{n+1} + 10^{-n-1}.$$

Ако низата $(a_0, a_1, \ldots, a_n, \ldots)$ е определена како и погоре, тогаш пишуваме:

$$a = a_0, a_1 \ldots a_n \ldots \tag{2}$$

и велиме дека a е претставен како *бесконечна десетична дропка*. Притоа, конечната дропка $a_0, a_1 \ldots a_n$ ја означуваме со $[a]_n$, специјално, $[a]_0 = a = a_0$, (и во овој случај) се вика *цел дел* на a.

3°. Ако е точно равенството (2), тогаш:

(iii) за секој $n \in \mathbf{N}$ постои $k \in \mathbf{N}$, таков што $a_{n+k} \neq 9$.

Доказ. Да претпоставиме дека постои $m \in \mathbf{N}$, таков што $a_{m+k} = 9$ за секој $k \in \mathbf{N}^+$. Нека m е најмалиот број со таа особина. Тогаш, $a_m \neq 9$, $a_{m+1} = a_{m+2} = \ldots = 9$. Да ставиме $b = a_0, a_1 \ldots a_m + 10^{-m}$. Според **2°** (ii), имаме

$$a_0, a_1 \ldots a_m\, 9 \leqslant a < a_0, a_1 \ldots a_m\, 9 + 10^{-m-1} = b$$

$$a_0, a_1 \ldots a_m\, 99 \leqslant a < a_0, a_1 \ldots a_m\, 99 + 10^{-m-2} = b$$

и, поопшто:

$$a_0, a_1 \ldots a_m \underbrace{9 \ldots 9}_{n} \leqslant a < b$$

Нека: $b - a = h > 0$. Ако се има предвид тоа што:

$$a_0, a_1 \ldots a_m \underbrace{9 \ldots 9}_{n} = b - 10^{-m} + 9 \cdot 10^{-m-1} + \ldots + 9 \cdot 10^{-m-n}$$

$$= b - 10^{-m} + \frac{9 \cdot 10^{-m-1}(10^{-n} - 1)}{10^{-1} - 1}$$

$$= b - 10^{-m} + 10^{-m}(1 - 10^{-n})$$

$$= b - 10^{-m} \cdot 10^{-n}$$

добиваме дека

$$h \leqslant b - a_0, a_1 \ldots a_m\, 9 \ldots 9 = 10^{-m}\, 10^{-n},$$

за секој n, но тоа не е можно, бидејќи ако n го избереме така што $10^n > 10^{-m} h^{-1}$, ќе добиеме $h > 10^{-m} \cdot 10^{-n}$.

4°. Нека $(a_0, a_1, \ldots, a_n, \ldots)$ е низа природни броеви, таква што условите **2°** (i) и **3°** (iii) се задоволени. Тогаш постои еднозначно определен ненегати-

вен реален број a, таков што условот **2°** (ii) (односно равенството (2)) е исполнет.

Доказ. Прво, да уочиме дека условот **2°** (ii) не може да биде задоволен од два различни броја a', a'', бидејќи ако $a' < a''$, би имале:

$$0 < a'' - a' < 10^{-n} \text{ за секој } n.$$

Множеството:

$$A = \{a_0, a_1 \ldots a_n \mid n \in \mathbf{N}\} \tag{3}$$

е мајорирано, бидејќи $a_0, a_1 \ldots a_n < a_0 + 1$. Да ставиме

$$a = sup\, A. \tag{4}$$

Тогаш, имаме

$$a_0, a_1 \ldots a_n \leqslant a$$

за секој $n \in \mathbf{N}$. Да покажеме дека

$$a < a_0, a_1 \ldots a_n + 10^{-n}.$$

Прво, лесно се покажува дека секој број $a_0, a_1 \ldots a_n + 10^{-n}$ е мајорант на A, така што

$$a \leqslant a_0, a_1 \ldots a_n + 10^{-n}.$$

Ако претпоставиме дека

$$a = a_0, a_1 \ldots a_m + 10^{-m}$$

За некој m, слично како и при доказот на **3°**, би добиле $a_{m+1} = \ldots = a_{m+k} = \ldots = 9$, што противречи со **3°** (iii). ∎

Од **2°** и **4°** се гледа дека постои биекција меѓу позитивните реални броеви и бесконечните десетични дропки. Според тоа, постои можност да се дефинира $\mathbf{R}^+$ со помош на низи природни броеви со својствата **2°** (i), **3°** (iii). Ако се прифати овој пат, тогаш рационалните броеви "се прескокнуваат", т.е. нема потреба од нивна специјална конструкција.

Природно е да го поставиме прашањето: каков облик имаат бесконечните дропки што одговараат на рационалните броеви. Одговор даваат следните две тврдења.

5°. Ако рационалниот број a е претставен како бесконечна десетична дропка в облик (2), тогаш постојат броеви k и p, такви што:

$$a_{k+i+1} = a_{k+p+i+1}$$

за секој $i \in \mathbf{N}$.

(Во овој случај велиме дека десетичната дропка е *периодична*, а (2) го добива следниов облик:

$$a = a_0, a_1 \ldots a_k (a_{k+1} \ldots a_{k+p}); \tag{2'}$$

за $a_1 \ldots a_k$ велиме дека е *нејериодичен*, а $a_{k+1} \ldots a_{k+p}$ *јериодичен дел* на дропката.)

Доказ. Нека $a = \frac{c}{d}$. Го делиме c со d:

$$c = a_0 d + r_0, \quad a = a_0 + \frac{r_0}{d}.$$

Потоа, го делиме $10\, r_0$ со d:

$$10\, r_0 = a_1 d + r_1, \quad a = a_0 + \frac{a_1}{10} + \frac{r_1}{10\, d}.$$

Притоа, поради $r_0 < d$, имаме $a_1 \leqslant 9$. Да претпоставиме дека:

$$a = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n} + \frac{r_n}{10^n\, d},$$

каде што $a_k \leqslant 9$ за $k \geqslant 1$, $r_n < d$. Тогаш a_{n+1} е количникот што се добива при делењето на $10 r_n$ со d; од $r_n < d$ следува $a_{n+1} \leqslant 9$. Од сето тоа следува дека:

$$a_0, a_1 \ldots a_n \leqslant a < a_0, a_1 \ldots a_n + 10^{-n}$$

т.е. добиваме дека е точно равенството (2).

Патем, добивме алгоритам за претворање на позитивен рационален број во бесконечна дропка. (Читателот, веројатно, уочил дека тоа е добро познатата постапка за претворање на "обична дропка" во "десетична".).

Преостанува да ја докажеме периодичноста. За таа цел ќе ја разгледаме низата $r_0, r_1, \ldots, r_n, \ldots$ што се добива при горната постапка. Ако се има предвид тоа што $r_n < d$, добиваме дека $r_k = r_{k+p}$ за некои k, p $(p > 0)$. Да ги избереме најмалите броеви k и p со овие особини. Од равенствата

$$10\, r_k = a_{k+1}\, b + r_{k+1}, \; 10\, r_{k+p} = a_{k+p+1}\, b + r_{k+p+1},$$

добиваме:

$$a_{k+p+1} = a_{k+1} \text{ и } r_{k+p+1} = r_{k+1},$$

а од исти причини и:

$$a_{k+p+2} = a_{k+2}, \quad r_{k+p+2} = r_{k+2}$$

итн., ќе добиеме:

$$a_{k+p+n} = a_{k+n} \text{ за секој } n \in \mathbf{N}.$$

Од следново својство, чиј доказ му го препуштаме на читателот, се гледа дека периодичноста е карактеристична за рационалните броеви.

6°. Ако реалниот број a е претставен со бесконечна периодична дропка како во (2'), тогаш a е рационален број, а имено:

$$a = \frac{\alpha - \beta}{\gamma} \tag{2''}$$

каде што:

(i) α се добива кога на a_0 му се допишат (од десно) цифрите $a_1 \ldots a_k$ $a_{k+1} \ldots a_{k+p}$.

(ii) β се добива кога на a_0 му се допишат цифрите $a_1 \ldots a_k$.

(iii) $\gamma = 10^k (10^p - 1) = \underbrace{9 \ldots 9}_{p} \underbrace{0 \ldots 0}_{k}$.

Да разгледаме два примера.

1) $3{,}2\,(13) = \dfrac{3213 - 32}{990} = \dfrac{3181}{990}$.

2) Една конечна дропка $a_0, a_1 \ldots a_n$, може да се смета за периодична дропка од облик $a_0, a_1 \ldots a_n\,(0)$, т.е. тоа е бесконечна дропка во која периодично се повторува нулата.

Користејќи ги бесконечните десетични дропки, ќе покажеме дека:

7°. Множеството **R** е непребројиво бесконечно множество.

Доказ. Ќе докажеме дека тврдењето е точно за множеството $\{x \mid x \in \mathbf{R}, 0 < x < 1\} = K$ позитивни реални броеви помали од 1. Нека $A = \{a_1, a_2, \ldots, a_n, \ldots\}$ е пребројиво подмножество на K; такво постои бидејќи можеме да ставиме, на пример, $a_n = \dfrac{1}{n}$. Ќе покажеме дека A е вистинско подмножество на K, од што и ќе следува заклучокот.

Прво, елементите од A ќе ги претставиме како бесконечни десетични дропки:

$$\begin{aligned} a_1 &= 0,\ a_{11}\ a_{12} \ldots a_{1n} \ldots \\ a_2 &= 0,\ a_{21}\ a_{22} \ldots a_{2n} \ldots \\ &\vdots \\ a_n &= 0,\ a_{n1}\ a_{n2} \ldots a_{nn} \ldots \end{aligned} \tag{5}$$

Формираме нов број a со:

$$a = 0,\ a_1\, a_2 \ldots a_n \ldots \tag{6}$$

каде што $a_n = a_{nn} - 1$ за $a_{nn} \geqslant 1$, $a_n = 1$ за $a_{nn} = 0$. Јасно е дека $a \in K$, како и дека $a \notin A$.

(Од Кантор потекнува следнава хипотеза, позната како *хипотеза на континуумот*:

Ако B е бесконечно непребројво подмножество на $\mathbf{R}$, тогаш B е еквивалентно со $\mathbf{R}$.

Пред околу 40 години, Гедел докажал дека оваа хипотеза не е во спротивност со другите аксиоми на соодветен систем аксиоми на множествата, а пред десетина години Коен покажал дека таа е и независна од другите аксиоми.).

ВЕЖБИ. **2.** Ако $a = a_0, a_1 a_2 \ldots a_n$ е конечна десетична дропка, тогаш:

(i) $a = a_0, a_1, a_2 \ldots a_n \underbrace{00\ldots0}_{m}$; (ii) $10^k a$ се добива на тој начин,што десетичната запирка ќе се помести за k места надесно; притоа, ако $k \geqslant n$, претходно се допишуваат $k - n$ нули од десно и се добива дека $10^k a$ е природен број.

3. Користејќи ги резултатите од претходната вежба, да се докажат познатите правила за оперирање со конечни десетични дропки.

4. Нека S е множеството позитивни рационални броеви од облик m, a, каде што $m \geqslant 0$, $0 \leqslant a \leqslant 9$. Операцијата множење $*$ се определува на обичен начин, со тоа што ако се добие резултат s, $a\,b$ за $b < 5$, децималата b се изоставува, т.е. се зема бројот s, a, а за $b \geqslant 5$, наместо s, ab, се зема бројот $s, a + 0{,}1$. Да се испитаат својствата на операцијата $*$.

5. Дропките $\frac{329}{15}, \frac{1}{7}, \frac{3}{40}, \frac{27}{32}, \frac{83}{111}$ да се претворат во периодични десетични дропки.

6. Десетичните дропки 8, (24); 0,23 (45); 3, 110 (23) да се претворат во обични дропки, т.е. во облик $\frac{a}{b}$.

7. Да се покаже дека при претворувањето на дропката $\frac{a}{c}$ во десетична не е потребно да се извршат повеќе од c постапки.

8. За една бескрајна десетична дропка велиме дека е *чисто периодична* ако сите децимали се повторуваат периодично; таквите дропки имаат облик:

$$m, (a_1 a_2 \ldots a_k).$$

Периодичните дропки, кај кои некои децимали не се повторуваат, се нарекуваат *нечисто периодични*. Ако c и d се релативно прости природни броеви, тогаш:

а) $\frac{c}{d}$ е чисто периодична бесконечна дропка акко $d > 1$ и $(10; d) = 1$.

б) $\frac{c}{d}$ е нечисто периодична бесконечна дропка акко $d > 1$, $(10; d) > 1$ и постои прост делител на d што е различен од 2 и 5.

9. Сите докажани резултати во овој дел се точни и за систем со каква било основа b. Дури и доказите се исти, со тоа што, каде што дошол до израз бројот 9, би требало тој да се замени со $b - 1$, т.е. $10 - 1$.

10. Да се формулираат резултати што се обопштувања на резултатите од вежбата **8**, со тоа што сега да се работи во произволен броен систем со основа b. Во иста смисла, да се формулира и обопштување на **1°**.

11. Дропките $\frac{1}{3}, \frac{1}{5}, \frac{2}{7}, \frac{5}{14}$ да се изразат во бинарен систем, а потоа и како бескрајни периодични бинарни дропки, Бесконечните бинарни дропки 0,1101 (101); 0,101 (1001); 0,(011) да се претворат во обични.

12. На читателот му е добро познато дека се сметаат за точни, на пример, равенствата:

$$0{,}99\ldots9\ldots = 0,(9) = 1;\quad 2{,}349\ldots9\ldots = 2{,}34\,(9) = 2{,}35.$$

Да се даде образложение на тие равенства и да се разгледа поопштиот случај. Дали овие резултати се во спротивност со својството 3°?

5.7. ПРИБЛИЖНИ ВРЕДНОСТИ

Во практиката ирационалните (па и рационалните) реални броеви се заменуваат со соодветни конечни десетични дропки, што многу не се разликуваат од дадените броеви. Имено, ако реалниот број a е изразен со бескрајна десетична дропка

$$m, a_1 a_2 \ldots a_n \ldots,$$

тој број се смета за приближно еднаков со конечната десетична дропка.

$$a^* = m, a_1 a_2 \ldots a_n.$$

Притоа, разликата $a - a^*$ е помала од 10^{-n}, па, значи, таа дотолку е помала, доколку е поголем бројот n. Поопшто, ако $c \leqslant a \leqslant d$, тогаш секој број a^* : $c \leqslant a^* \leqslant d$ сметаме дека е "приближно" еднаков со a и пишуваме $a \approx a^*$. Притоа бројот $|a - a^*|$ се нарекува *апсолутна грешка на приближноста*. Обично, апсолутната грешка не ја знаеме, бидејќи во спротивен случај, немаме потреба од приближно сметање. Затоа, добро е да се знае максималната можна вредност на апсолутната грешка. Така, знаејќи дека $c \leqslant a \leqslant d$ и $c \leqslant a^* \leqslant d$, сигурни сме дека апсолутната грешка не е поголема од $d - c$. На пример, од $0{,}66 < \frac{2}{3} < 0{,}67$ следува дека за секој број a : $0{,}66 \leqslant a \leqslant 0{,}67$, ставајќи $a \approx \frac{2}{3}$ правиме апсолутна грешка помала од 0,01.

При конкретна работа со приближни вредности, оперираме со броеви кои се приближно точни. На крајот, се поставува задача да се оцени максималната можна вредност на апсолутната грешка. Според тоа, добро е да се знае како се менува апсолутната грешка при собирање, вадење, множење и делење на приближни вредности. Одговор на ова прашање (донекаде) дава следново својство.

1°. Нека

$$|x - x^*| < \varepsilon,\ |y - y^*| < \delta \text{ и } 0 < a < |y| < b,$$

тогаш, ставајќи

$$x + y \approx x^* + y^*,\ x - y \approx x^* - y^*,\ xy \approx x^* y^*,\ \frac{x}{y} \approx \frac{x^*}{y^*}$$

правиме апсолутни грешки што не се поголеми од:

$$\varepsilon + \delta,\ \varepsilon + \delta,\ b\varepsilon + |x^*|\,\delta,\ \frac{\varepsilon}{a} + \frac{|x^*|}{a|y^*|}\,\delta,$$

респективно.

Доказ. Од својствата на апсолутните вредности добиваме:

$$|(x \pm y) - (x^* \pm y^*)| \leqslant |x - x^*| + |y - y^*| < \varepsilon + \delta;$$

$$|xy - x^* y^*| = |y(x - x^*) + x^*(y - y^*)| \leqslant$$

$$\leqslant |y||x - x^*| + |x^*||y - y^*| < \varepsilon b + |x^*|\delta;$$

$$\left|\frac{x}{y} - \frac{x^*}{y^*}\right| = \frac{|y^*(x - x^*) + x^*(y^* - y)|}{|y||y^*|} < \frac{|y^*|\varepsilon + |x^*|\delta}{a|y^*|}.$$ ∎

Да разгледаме еден пример:

1) Нека страните на еден правоаголник се измерени приближно $a \approx 50$cm. $b \approx 100$ cm, при што се знае дека не е направена апсолутна грешка поголема од 1 mm. Приближната вредност на површината на правоаголникот е 5.000 cm², а, притоа, апсолутната грешка не е поголема од $(50{,}1 \cdot 0{,}1 + 100 \cdot 0{,}1)$ cm² = 15,01 cm².

Апсолутната грешка не е доволна за да се окарактеризира степенот на приближноста. Тоа може да се уочи и од следниов пример.

2) Нека при мерење на 1 m должина се направи апсолутна грешка од 1 mm, а при мерење на 10 km должина се направи апсолутна грешка од 1m. И покрај тоа што во вториот случај е направена многу поголема апсолутна грешка, јасно е дека тој резултат треба да го сметаме за попрецизен.

До оваа констатација ќе дојдеме полесно ако претходно воведеме поим за релативна грешка. Имено, ако $x \approx x^*$, тогаш количникот

$$\left|\frac{x - x^*}{x^*}\right|$$

се нарекува *релативна грешка*. Така, при првото мерење е направена релативна грешка $\frac{1}{10^3}$, а при второто $\frac{1}{10^4}$.

Теоријата на приближни пресметувања има едно од најважните места во математиката, но, сепак, ќе се задоволиме само со кажаното.

ВЕЖБИ. **1.** Да се оценат апсолутните и релативните грешки во секој од следните случаи:

а) $10 \approx 12$; б) $\frac{1}{3} \approx 1$; в) $\frac{1}{3} \approx 0{,}33$; г) $\sqrt{2} \approx 1{,}41$. д) $\sqrt[4]{80} \approx 3$.

2. Страните на правоаголникот се еднакви со $a = 2{,}5$ см $\pm$ 0,01 см. $b = 4{,}6$ см $\pm$ 0,02 см. Во кои граници се наоѓа површината на правоаголникот?

3. Да се определи приближноста на броевите: $2a + b - 3c$, $\frac{a^2 b}{c}$ ако: $a \approx 347{,}4$ ($\pm$ 0,1), $b \approx 4{,}45$ ($\pm$ 0,02), $c \approx 362$ ($\pm$ 0,2).

ЛИТЕРАТУРА

[1] Р. Ансаров и М. Трајковски, Елементи од математичката логика и од теоријата на множествата, Скопје, 1973.
[2] В. Девиде, Увод во математичката логика, Скопје, 1973.
[3] К. Куратовский, А. Мостовский, Теория множеств, Москва, 1970 (превод од англиски).
[4] С. Прешиќ, Елементи од математичката логика, Скопје, 1973.
[5] А. Самарџиски и Н. Целакоски, Решени задачи по алгебра I, Скопје, 1968.
[6] С. Феферман, Числовые системы, Москва, 1971 (превод од англиски).
[7] Ѓ. Чупона, Предавања по алгебра, кн. I, Скопје, 1968.
[8] Ѓ. Чупона, Краток преглед на елементарната алгебра, Билтен на Реп. Завод за унапредување на школ. на СРМ, бр. 3—4 (1970), 1—74.
[9] Ѓ. Чупона и Б. Трпеновски, Предавања по алгебра кн. II, Скопје, 1973.
[10] V. Devide, "Stara" i "nova" matematika, Zagreb, 1975.
[11] P. Halmos, Naive Set Theory, New York, 1963.
[12] S. Prešić, Savremeni pristup nastavi matematike, Beograd, 1975.
[13] A. Tarski, Uvod u matematičku logiku i metodologiju matematike, Beograd, 1973 (превод од англиски).

РОЗТ ЗА УЧЕБНИЦИ „ПРОСВЕТНО ДЕЛО“ — СКОПЈЕ
ул. „Иво Рибар Лола“ бб Градски ѕид блок 4

*

За издавачот
Михаило Ќорвезироски

*

ЃОРЃИ ЧУПОНА
АЛГЕБАРСКИ СТРУКТУРИ И РЕАЛНИ БРОЕВИ

*

Уредник
КИРИЛ МИЛЧЕВ

*

Јазична редакција
МИРА НИКОЛОВА

*

Илустрации
ПЕТАР ТАНЧЕВСКИ

*

Корицата ја илустрира
АЛЕКСАНДАР НИКОЛОВСКИ

*

Коректор
ДОНЧО ДИМОВСКИ

*

Ракописот е предаден во печат 31. III. 1976 година. Печатењето е завршено на 20. IX. 1976 год. Обем: страни 160 Формат: 17×24 Тираж: 2000 примероци. Книгата е отпечатена во Универзитетска печатница „Кирил и Методиј“ — Скопје