Teoretická aritmetika

5. novembra 2015

1 Úvod

Teoretická aritmetika sa zaoberá štúdiom číselných oborov. Spoločnou vlastnosťou niektorých základných číselných oborov ako sú napríklad obor celých čísel, obor racionálnych čísel a obor reálnych čísel je skutočnosť, že sú to usporiadané okruhy. Preto pre štúdium vlastností a konštrukcií týchto číselných oborov je užitočné poznať pojem usporiadaného okruhu, usporiadaného poľa a základné vlastnosti týchto algebraických štruktúr.
Všade v nasledujúcom texte budeme používať tieto označenia:
$\mathbb{N}$ označuje množinu všetkých prirodzených čísel
$\mathbb{N}_0$ označuje množinu všetkých celých nezáporných čísel
$\mathbb{Z}$ označuje množinu všetkých celých čísel
$\mathbb{Q}$ označuje množinu všetkých racionálnych čísel
$\mathbb{R}$ označuje množinu všetkých reálnych čísel
$\mathbb{C}$ označuje množinu všetkých komplexných čísel

2 Usporiadané okruhy a polia

Najprv pripomeňme pojem (komutatívneho) okruhu, poľa a usporiadanej množiny.

Definícia 2.1. *a) Usporiadaná trojica $(A, +, .)$, kde A je množina, $+$ a $.$ sú binárne operácie na A (sčitovanie a násobenie), sa nazýva okruh, ak platí:*
(1) Operácia $+$ je komutatívna a asociatívna.
(2) Existuje prvok $0 \in A$ tak, že pre všetky $a \in A$ $a + 0 = 0 + a = a$ (nulový prvok okruhu).
(3) Pre každé $a \in A$ existuje $b \in A$ tak, že $a + b = b + a = 0$ (prvok b sa nazýva opačný prvok k prvku a a označuje sa $-a$.
(4) Operácia $.$ je asociatívna.
(5) Pre každé $a, b, c \in A$ platí $a.(b + c) = a.b + a.c$ a tiež $(a + b).c = a.c + b.c$ (distributívnosť operácie $.$ vzhľadom na operáciu $+$).
b) Okruh $(A, +, .)$ sa nazýva komutatívny, ak pre každé $a, b \in A$ platí $a.b = b.a$, t. j. operácia násobenia je komutatívna.

c) Okruh $(A,+,.)$ sa nazýva okruh s jednotkou (unitárny okruh), ak existuje prvok $\mathbf{1} \in A$, $\mathbf{1} \neq 0$ tak, že pre každé $a \in A$ platí $a.\mathbf{1} = \mathbf{1}.a = a$ (jednotkový prvok okruhu; pre jeho odlíšenie od prirodzeného čísla 1 ho označujeme tučne, t. j. $\mathbf{1}$).
d) Komutatívny okruh s jednotkou $(A,+,.)$ sa nazýva pole, ak pre každé $a \in A$, $a \neq 0$ existuje $c \in A$ tak, že $a.c = c.a = \mathbf{1}$ (inverzný prvok k a, ktorý sa označuje a^{-1}).

Príklady 2.1. *$(\mathbb{Z},+,.)$ (s obvyklým sčitovaním a násobením) je komutatívny okruh s jednotkou, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$ (s obvyklým sčitovaním a násobením) sú polia. $(\mathbb{N},+,.)$ ani $(\mathbb{N}_0,+,.)$ (s obvyklým sčitovaním a násobením) nie sú okruhy.*

Pripomeňme, že ak $(A,+,.)$ je okruh, $a \in A$, tak pre každé $z \in \mathbb{Z}$ je definovaný z -násobok za prvku a v okruhu $(A,+,.)$ nasledovne: $0a = 0$. Pre každé $n \in \mathbb{N}_0$ (n + 1)a = na + a. Pre každé $n \in N$ (-n)a = -(na) (= n(-a)). Teda napríklad $3a = a + a + a$, $(-3)a = -(a + a + a) = (-a) + (-a) + (-a)$.

Definícia 2.2. *a) Binárna relácia $<$ na množine A sa nazýva usporiadanie (množiny A),ak má nasledujúce vlastnosti:*
(u1) Pre všetky $a,b,c \in A$ platí: Ak $a < b$ a $b < c$, tak $a < c$ (tranzitívnosť).
(u2) Pre všetky $a,b \in A$ platí práve jeden z výrokov: $a < b$, $a = b$, $b < a$ (trichotómia).
b) Ak $<$ je usporiadanie množiny A, tak usporiadaná dvojica $(A,<)$ sa nazýva usporiadaná množina.

Príklady 2.2. *Množiny $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ spolu s obvyklým usporiadaním sú usporiadané množiny. $(\mathcal{P}(\mathbb{N}),\subseteq)$, kde $\mathcal{P}(\mathbb{N})$ je množina všetkých podmnožín množiny $\mathbb{N}$ a $\subseteq$ je množinová inklúzia, nie je usporiadaná množina, pretože neplatí $(u2)$.*

Poznámka 2.1. *Ak $(A,<)$ je usporiadaná množina, $B \subseteq A$ a na množine B definujeme binárnu reláciu $<_B$ tak, že pre každé $b,c \in B$, $b <_B c$ práve vtedy, keď $b < c$, tak $(B,<_B)$ je tiež usporiadaná množina. Usporiadanie $<_B$ sa nazýva usporiadanie podmnožiny B indukované usporiadaním $<$.*

Teraz už môžeme definovať pojem usporiadaného okruhu a usporiadaného poľa. Pretože v aritmetike sa stretávame len s komutatívnymi okruhmi, pri štúdiu usporiadaných okruhov sa obmedzíme na komutatívne okruhy s jednotkovým prvkom.

Definícia 2.3. *a) Systém $(A,+,.,<)$ sa nazýva usporiadaný okruh, ak $(A,+,.)$ je komutatívny okruh s jednotkou, $(A,<)$ je usporiadaná množina a pre všetky $a,b,c \in A$ platí:*
(uo1) Ak $a < b$, tak $a + c < b + c$.
(uo2) Ak $a < b$ a $0 < c$, tak $a.c < b.c$.
b)Prvok a usporiadaného okruhu $(A,+,.,<)$ sa nazýva kladný (záporný), ak $0 < a$ ($a < 0$).
c) Usporiadaný okruh $(A,+,.,<)$ sa nazýva usporiadané pole, ak $(A,+,.)$ je pole.

Príklady 2.3. $(\mathbb{Z},+,.,<)$ *je usporiadaný okruh,* $(\mathbb{Q},+,.,<)$, $(\mathbb{R},+,.,<)$ *sú usporiadané polia.* $(\mathbb{N},+,.,<)$ *nie je usporiadaný okruh. Systém* $(\mathbb{Z}_3,+,.,<)$, *kde* $(\mathbb{Z}_3,+,.)$ *je zvyškové pole modulo 3 a* $<$ *je obvyklé usporiadanie množiny* $\mathbb{Z}_3$ *nie je usporiadané pole, pretože platí* $1<2$ *a neplatí* $2=1+1<2+1=0$ *v* $(\mathbb{Z}_3,<)$.

Veta 2.1. *Ak* $(A,+,.,<)$ *je usporiadaný okruh,* B *je podokruh okruhu* $(A,+,.)$ *obsahujúci jednotku okruhu* $(A,+,.)$ *a* $<_B$ *je usporiadanie na* B *indukované usporiadaním* $<$, *tak* $(B,+,.,<_B)$ *je tiež usporiadaný okruh. Usporiadaný okruh* $(B,+,.,<_B)$ *sa potom nazýva usporiadaný podokruh usporiadaného okruhu* $(A,+,.,<)$.

Dôkaz. Je zrejmý. □

Veta 2.2. *Nech* $(A,+,.,<)$ *je usporiadaný okruh. Potom pre ľubovoľné* $a,b,c,\in A$ *platí:*
(1) Ak $a<b$, *tak* $-b<-a$.
(2) Ak $a<b$ *a* $c<0$, *tak* $b.c<a.c$.
(3) Ak $0<a$ *a* $0<b$, *tak* $0<a.b$.
(4) Ak $0<a$ *a* $b<0$, *tak* $a.b<0$.
(5) Ak $a<0$ *a* $0<b$, *tak* $a.b<0$.
(6) Ak $a<0$ *a* $b<0$, *tak* $0<a.b$.
(7) Ak $c\in A$ *a* $c\neq 0$, *tak* $c^2=c.c>0$.
(8) Ak $\mathbf{1}\in A$ *je jednotkový prvok okruhu* $(A,+,.,<)$, *tak* $0<\mathbf{1}$.
(9) Ak $a\neq 0$, $b\neq 0$, *tak* $a.b\neq 0$.
(10) Ak $0<a$, *tak pre každé* $n\in\mathbb{N}$, $na<(n+1)a$ *(ak* $a<0$, *tak* $(n+1)a<na$*).*
Ak $(A,+,.,<)$ *je usporiadané pole, tak pre každé* $a,b\in A$ *platí:*
(11) Ak $0<a$, *tak* $0<a^{-1}$.
(12) Ak $a<0$, *tak* $a^{-1}<0$.
(13) Ak $0<a<b$, *tak* $0<b^{-1}<a^{-1}$.

Dôkaz. (1) Ak $a<b$, tak $a+((-a)+(-b))<b+((-a)+(-b))$ a teda $-b<-a$.
(2) Nech $a<b$ a $c<0$. Potom $-c>0$ a preto $a.(-c)<b.(-c)$. Z toho dostávame, že $-a.c<-b.c$ a podľa (1) potom $-(-b.c)<-(-a.c)$. Teda $b.c<a.c$.
(3) Ak $0<a$ a $0<b$, tak $0.b<a.b$ a teda $0<a.b$.
(4) Ak $0<a$ a $b<0$, tak $b.a<0.a$ a teda $a.b<0$.
(5), (6) Podobne ako (4).
(7) Ak $c\neq 0$, tak $0<c$ alebo $c<0$. Potom, podľa (3), resp. (6) platí $0<c.c$.
(8) Pretože $\mathbf{1}\neq 0$, podľa (7) platí $0<\mathbf{1}.\mathbf{1}=\mathbf{1}$.
(9) Vyplýva z (3) - (6).
(10) Nech $n\in\mathbb{N}$. Potom $na\in A$ a pretože $0<a$, platí $0+na<a+na$. Teda $na<(n+1)a$.
(11) Nech $a^{-1}\leq 0$. Pretože $a^{-1}\neq 0$, platí $a^{-1}<0$. Pretože $0<a$, dostávame $a^{-1}.a<0.a$ a teda $\mathbf{1}<0$. Dostali sme spor s (8). Preto platí $0<a^{-1}$.
(12) Ak $a^{-1}\geq 0$, tak, pretože $a^{-1}\neq 0$, platí $a^{-1}>0$. Potom, podľa (11), $(a^{-1})^{-1}=a>0$ čo je spor. Teda $a^{-1}<0$.

(13)Ak $0 < a < b$, tak, podľa (11), (12) a (3) platí $0 < a^{-1}.b^{-1}$. Potom $0 < a.a^{-1}.b^{-1} < b.a^{-1}.b^{-1}$ a teda $0 < b^{-1} < a^{-1}$. □

Dôsledok 2.1. *Ak $(A, +, ., <)$ je usporiadaný okruh, tak $(A, +, .)$ je obor integrity, má charakteristiku ∞ a teda je nekonečný.*

Dôkaz. Z vlastnosti (9) predchádzajúcej vety vyplýva, že $(A, +, .)$ je obor integrity. Pretože $0 < \mathbf{1}$, pre každé pre každé $n \in \mathbb{N}$, $n\mathbf{1} < (n+1)\mathbf{1}$ (podľa (10)) a preto pre každé $n \in \mathbb{N}$ platí $0 < n\mathbf{1}$. Teda prvok $\mathbf{1}$ má v $(A, +, .)$ nekonečný rád a charakteristika tohoto okruhu je ∞. □

Príklady 2.4. *Žiadny konečný komutatívny okruh nie je možné usporiadať tak, aby sme dostali usporiadaný okruh. Pole $(\mathbb{C}, +, .)$ komplexných čísel s obvyklým sčitovaním a násobením tiež nie je možné usporiadať tak, aby sme dostali usporiadané pole. Skutočne, nech $<$ je usporiadanie množiny $\mathbb{C}$ také, že $(\mathbb{C}, +, ., <)$ je usporiadané pole. Potom pre prvok $i \in \mathbb{C}$ platí $i \neq 0$ a teda $i.i = -1 > 0$. Potom ale $1 = -(-1) < 0$, čo je spor s vlastnosťou (8) predchádzajúcej vety.*

Teraz ukážeme, že usporiadanie v usporiadanom okruhu je možné definovať pomocou tzv. normálnej množiny, ktorá zodpovedá množine všetkých kladných prvkov tohoto okruhu. Vyplýva to z toho, že pre ľubovoľné prvky a, b z usporiadaného okruhu platí: $a < b$ práve vtedy, keď $0 < b - a$.

Veta 2.3. *V každom usporiadanom okruhu $(A, +, ., <)$ má množina $A^+_< = \{a \in A : 0 < a\}$ (t. j. množina všetkých kladných prvkov) nasledujúce vlastnosti:*
(1) Ak $a, b \in A^+_<$, tak $a + b, a.b \in A^+_<$.
(2) Pre každé $a \in A$ platí práve jeden z výrokov: $a \in A^+_<$, $a = 0$, $-a \in A^+_<$.
(3) Pre každé $a, b \in A$ platí: $a < b$ práve vtedy, keď $0 < b - a$.
(4) Nech $<_1$, $<_2$ sú usporiadania množiny A také, že $(A, +, ., <_1)$ aj $(A, +, ., <_2)$ sú usporiadané okruhy. Potom platí:
a) $<_1 = <_2$ práve vtedy, keď $A^+_{<_1} = A^+_{<_2}$.
b) Ak $A^+_{<_1} \subseteq A^+_{<_2}$, tak $A^+_{<_1} = A^+_{<_2}$.

Dôkaz. (1) Nech $0 < a$, $0 < b$. Potom $0 < b = 0 + b < a + b$ a teda $0 < a + b$. Platí tiež $0 = 0.b < a.b$.
(2) Pretože $(A, <)$ je usporiadaná množina, pre každé $a \in A$ platí práve jeden z výrokov: $0 < a$, $a = 0$, $a < 0$. Z toho vyplýva, že platí práve jeden z výrokov: $0 < a$, $a = 0$, $0 < -a$.
(3) Nech $a < b$. Potom $a + (-a) < b + (-a)$ a teda $0 < b - a$. Obrátene, nech $0 < b - a$. Potom $0 + a < b - a + a$ a teda $a < b$.
(4) a) Nech $<_1 = <_2$ a $a \in A$. Potom $a \in A^+_{<_1} \Leftrightarrow 0 <_1 a \Leftrightarrow 0 <_2 a \Leftrightarrow a \in A^+_{<_2}$. Teda $A^+_{<_1} = A^+_{<_2}$.
Obrátene, nech $A^+_{<_1} = A^+_{<_2}$ a $a, b \in A$. Potom $a <_1 b \Leftrightarrow b - a \in A^+_{<_1} \Leftrightarrow b - a \in A^+_{<_2} \Leftrightarrow a <_2 b$. Teda $<_1 = <_2$.
b) Nech $A^+_{<_1} \neq A^+_{<_2}$. Potom existuje $a \in A$ tak, že $a \in A^+_{<_2} \setminus A^+_{<_1}$. Potom $a \notin A^+_{<_1}$, $a \neq 0$ a preto $-a \in A^+_{<_1}$. Pretože $A^+_{<_1} \subseteq A^+_{<_2}$, dostávame, že $-a \in A^+_{<_2}$. Potom a aj $-a$ patria do $A^+_{<_2}$ a dostali sme spor. Teda $A^+_{<_1} = A^+_{<_2}$. □

Príklady 2.5. *V okruhu* $(\mathbb{Z},+,.)$ *(*$(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$*) je obvyklé usporiadenie* $<$ *jediným usporiadaním, pre ktoré je* $(\mathbb{Z},+,.,<)$ *(*$(\mathbb{Q},+,.,<)$, $(\mathbb{R},+,.,<)$*) usporiadaný okruh.*
Nech $<'$ *je usporiadanie množiny* $\mathbb{Z}$*, pre ktoré* $(\mathbb{Z},+,.,<')$ *je usporiadaný okruh. Pretože* $0<'1$ *v* $(\mathbb{Z},+,.,<')$*, platí* $1\in\mathbb{Z}^+_{<'}$*. Ďalej, ak* $k\in\mathbb{Z}^+_{<'}$*, tak aj* $k+1\in\mathbb{Z}^+_{<'}$*. Preto* $\mathbb{N}=\mathbb{Z}^+_{<}\subseteq\mathbb{Z}^+_{<'}$ *a, podľa predchádzajúcej vety, potom* $\mathbb{Z}^+_{<}=\mathbb{Z}^+_{<'}$*. Z toho vylýva, že* $<'=<$*.*
Nech teraz $<'$ *je usporiadanie množiny* $\mathbb{Q}$*, pre ktoré* $(\mathbb{Q},+,.,<')$ *je usporiadaný okruh. Potom, podobne ako pre* $(\mathbb{Z},+,.,<')$ *sa ukáže, že* $\mathbb{N}\subseteq\mathbb{Q}^+_{<'}$*. Nech* $r\in\mathbb{Q}^+_{<}$*. Potom* $0<r$ *a existujú* $m,k\in\mathbb{N}$ *tak, že* $r=\frac{m}{k}$*. Pretože* $m,k\in\mathbb{Q}^+_{<'}$*, platí tiež, že* $\frac{1}{k}=k^{-1}$ *a aj* $r=m.\frac{1}{k}$ *patria do* $\mathbb{Q}^+_{<'}$*. Teda* $\mathbb{Q}^+_{<}\subseteq\mathbb{Q}^+_{<'}$ *a preto* $\mathbb{Q}^+_{<}=\mathbb{Q}^+_{<'}$*. Z toho už vyplýva, že* $<'=<$*.*
Nakoniec, nech $<'$ *je usporiadanie množiny* $\mathbb{R}$*, pre ktoré* $(\mathbb{R},+,.,<')$ *je usporiadaný okruh. Nech* $a\in\mathbb{R}^+_{<}$*, t. j.* $0<a$*. Potom existuje* $c\in\mathbb{R}$*,* $0<c$ *tak, že* $c^2=a$*. Pretože* $c\neq 0$*,* $c.c=c^2=a\in\mathbb{R}^+_{<'}$ *a preto* $\mathbb{R}^+_{<}\subseteq\mathbb{R}^+_{<'}$*. Potom ale* $\mathbb{R}^+_{<}=\mathbb{R}^+_{<'}$ *a teda* $<'=<$*.*

Teraz ukážeme, ako je možné definovať usporiadanie ukruhu pomocou množiny, ktorá zodpovedá množine kladných prvkov definovaného usporiadania.

Definícia 2.4. *Podmnožina* P *množiny* A *prvkov komutatívneho okruhu s jednotkou* $(A,+,.,)$ *sa nazýva normálna, ak platí:*
(p1) Ak $a,b\in P$*, tak* $a+b,a.b\in P$*.*
(p2) Pre každé $a\in A$ *platí práve jeden z nasledujúcich výrokov:* $a\in P$*,* $a=0$*,* $-a\in P$*.*

Veta 2.4. *Nech* P *je normálna podmnožina v komutatívnom okruhu s jednotkou* $(A,+,.,)$*. Pre každé* $a,b\in A$ *definujme* $a<_P b\Leftrightarrow b-a\in P$*. Potom* $(A,+,.,<_P)$ *je usporiadaný okruh a* $A^+_{<_P}=P$*.*

Dôkaz. Najprv ukážeme, že $<_P$ je usporiadanie množiny A. Nech $a,b,c\in A$, $a<_P b$, $b<_P c$. Potom $b-a,c-b\in P$ a preto, podľa (p1), platí $(b-a)+(c-b)=c-a\in P$. Teda, $a<_P c$.
Nech teraz $a,b\in A$. Potom $b-a\in A$ a podľa (p2) platí práve jeden z výrokov: $b-a\in P$, $b-a=0$, $-(b-a)=a-b\in P$. To je ale ekvivalentné s tým, že platí práve jeden z výrokov: $a<_P b$, $a=b$, $b<_P a$.
Overme platnosť (uo1), (uo2). Nech $a,b,c\in A$. Ak $a<_P b$, tak $b-a=(b+c)-(a+c)\in P$ a preto $a+c<_P b+c$. Ak $a<_P b$ a $0<_P c$, tak $b-a,c-0=c\in P$ a potom aj $(b-a).c=b.a-c.a\in P$. Preto $a.c<_P b.c$.
Nakoniec, nech $a\in A$. Potom $a\in A^+_{<_P}\Leftrightarrow 0<_P a\Leftrightarrow a-0=a\in P$. Teda $A^+_{<_P}=P$. □

Príklady 2.6. *Nech* $\mathbb{Q}[\sqrt{2}]=\{a+b.\sqrt{2}:\ a,b\in\mathbb{Q}\}$ *je podmnožina množiny* $\mathbb{R}$*. Je známe, že táto množina určuje podpole poľa* $(\mathbb{R},+,.)$ *a teda* $(\mathbb{Q}[\sqrt{2}],+,.,<)$*, kde* $+,.$ *sú obvyklé operácie sčitovania a násobenia reálnych čísel (presnejšie ich zúženia na množinu* $\mathbb{Q}[\sqrt{2}]$*)* $a<$ *je usporiadenie na* $\mathbb{Q}[\sqrt{2}]$ *indukované obvyklým usporiadaním množiny* $\mathbb{R}$*, je usporiadané pole. Nech* $P=\{a+b.\sqrt{2}:$

$a - b.\sqrt{2} > 0\}$. *Ukážeme, že* P *je normálna podmnožina v poli* $(\mathbb{Q}[\sqrt{2}], +, .)$. *Skutočne, ak* $a + b.\sqrt{2}, c + d.\sqrt{2} \in P$, *tak* $a - b.\sqrt{2} > 0$, $c - d.\sqrt{2} > 0$. *Potom aj* $(a+c)-(b+d).\sqrt{2} > 0$ *a teda* $(a+b.\sqrt{2})+(c+d.\sqrt{2}) = (a+c)+(b+d).\sqrt{2} \in P$. *Súčasne platí* $0 < (a - b.\sqrt{2}).(c - d.\sqrt{2}) = (a.c + 2.b.d) - (a.d + b.c).\sqrt{2}$ *a teda* $(a + b.\sqrt{2}).(c + d.\sqrt{2}) = (a.c + 2.b.d) + (a.d + b.d).\sqrt{2} \in P$. *Nech teraz* $a + b.\sqrt{2}$ *je ľubovoľný prvok* $\mathbb{Q}[\sqrt{2}]$. *Potom pre číslo* $a - b.\sqrt{2}$ *platí práve jeden z výrokov:* $0 < a - b.\sqrt{2}$, $a - b.\sqrt{2} = 0$, $a - b.\sqrt{2} < 0$. *To je ale ekvivalentné s tým, že platí práve jeden z výrokov:* $a + b.\sqrt{2} \in P$, $a + b.\sqrt{2} = 0$, $-(a + b.\sqrt{2}) \in P$.
Teda P *je normálna podmnožina v poli* $(\mathbb{Q}[\sqrt{2}], +, .)$, *ktorá určuje usporiadanie* $<_P$ *množiny* $\mathbb{Q}[\sqrt{2}$ *definované predpisom* $a + b.\sqrt{2} <_P c + d.\sqrt{2} \Leftrightarrow (c + d.\sqrt{2}) - (a+b.\sqrt{2}) \in P$ *(t. j.* $(c-a)-(d-b).\sqrt{2} > 0$*) také, že* $(\mathbb{Q}[\sqrt{2}], +, ., <_P)$ *je usporiadané pole. Pre číslo* $-\sqrt{2} = 0 + (-1).\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ *platí* $0 - (-1).\sqrt{2} > 0$ *a preto* $-\sqrt{2} \in P$. *To znamená, že* $0 <_P -\sqrt{2}$ *v usporiadanom poli* $(\mathbb{Q}[\sqrt{2}], +, ., <_P)$ *a teda* $<_P \neq <$. *Vidíme, že na komutatívnom okruhu s jednotkou môžu existovať viaceré usporiadania, ktoré jeho štruktúru rozširujú na štruktúru usporiadaného okruhu.*

Na porovnávanie usporiadaných okruhov z hľadiska ich vlastností je užitočný pojem homomorfizmu usporiadaných okruhov. Je to zobrazenie medzi usporiadanými okruhmi, ktoré zachováva štruktúru usporiadaného okruhu.

Definícia 2.5. *Nech* $(A, +, ., <_A)$, $(B, +, ., <_B)$ *sú usporiadané okruhy. Zobrazenie* $f : A \longrightarrow B$ *sa nazýva homomorfizmus usporiadaných okruhov, ak pre každé* $a, b \in A$ *platí:*
a) $f(a + b) = f(a) + f(b)$, $f(a.b) = f(a).f(b)$.
b) Ak $a <_A b$, *tak* $f(a) <_B f(b)$.
Označenie: $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$
Homomorfizmus usporiadaných okruhov $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ *sa nazýva izomorfizmus usporiadaných okruhov, ak zobrazenie* $f : A \longrightarrow B$ *je bijektívne. Ak existuje izomorfizmus usporiadaných okruhov* $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$, *tak hovoríme, že usporiadaný okruh* $(B, +, ., <_B)$ *je izomorfný s usporiadaným okruhom* $(A, +, ., <_A)$.

Z definície je zrejmé, že ak $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ je homomorfizmus usporiadaných okruhov $(A, +, ., <_A)$, $(B, +, ., <_B)$, tak f je prosté zobrazenie. Ďalej je tiež zrejmé, že ak $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ je homomorfizmus usporiadaných okruhov $(A, +, ., <_A)$, $(B, +, ., <_B)$, tak $f : (A, +, .) \longrightarrow (B, +, .)$ je homomorfizmus okruhov $(A, +, .)$, $(B, +, .)$. Je známe (z algebry), že ak $f : (A, +, .) \longrightarrow (B, +, .)$ je homomorfizmus okruhov, tak množina $f[B]$ určuje podokruh okruhu $(B, +, .)$. Analogické tvrdenie platí aj pre homomorfizmus usporiadaných okruhov.

Veta 2.5. *Nech* $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ *je homomorfizmus usporiadaných okruhov. Potom platí:*
(a) $(f[A], +, ., <)$, *kde* $+, .$ *sú zúženia operácií usporiadaného okruhu* $(B, +, ., <_B$ *) na podmnožinu* $f[A]$ $a <$ *je zúženie usporiadania* $<_B$ *usporiadaného okruhu* $(B, +, ., <_B)$ *na podmnožinu* $f[A]$, *je usporiadaný podokruh usporiadaného okruhu*

$(B,+,.,<_B)$.
(b) Usporiadaný okruh $(f[A],+,.,<)$ *je izomorfný s usporiadaným okruhom* $(A,+,.,<_A)$.

Dôkaz. (a) Podľa vety 2.1 stačí ukázať, že podokruh $(f[A],+,.)$ okruhu $(B,+,.)$ obsahuje jednotku $\mathbf{1}$ okruhu $(B,+,.)$. Pretože $0 < \mathbf{1}$ v $(A,+,.,<_A)$, platí $0 = f(0) < f(1)$ a teda $f(1) \neq 0$ v $(B,+,.,<_B)$. Ďalej platí $f(\mathbf{1}).f(\mathbf{1}) = f(\mathbf{1}.\mathbf{1}) = f(\mathbf{1}) = f(\mathbf{1}).\mathbf{1}$ a pretože podľa vety 2.2.(9) $(B,+,.)$ je obor integrity, z rovnosti $f(\mathbf{1}).f(\mathbf{1}) = f(\mathbf{1}).\mathbf{1}$ vyplýva, že $f(\mathbf{1}) = \mathbf{1}$. Teda $\mathbf{1} \in f[A]$.
(b) Definujme zobrazenie $g : A \longrightarrow f[A]$ tak, že pre každé $a \in A$ $g(a) = f(a)$. Pretože f je prosté, g je bijektívne a pre všetky $a, b \in A$ platí: $g(a+b) = f(a+b) = f(a) + f(b) = g(a) + g(b)$, $g(a.b) = f(a.b) = f(a).f(b) = g(a).g(b)$ a ak $a <_A b$, tak $g(a) = f(a) <_B f(b) = g(b)$, t. j. $g(a) < g(b)$. Teda $g : (A,+,.,<_A) \longrightarrow (f[A],+,.,<)$ je izomorfizmus usporiadaných okruhov. □

Cvičenie 2.1. *(1) Na množine* $\mathbb{C}$ *komplexných čísel definujme relácie* $<_1$ *a* $<_2$ *takto:*
$a + b.i <_1 c + d.i$ *práve vtedy, keď* $a < c$ *v* $(\mathbb{R},<)$ *alebo* $a = c$ *a súčasne* $b < d$ *v* $(\mathbb{R},<)$,
$a + b.i <_2 c + d.i$ *práve vtedy, keď* $b < d$ *v* $(\mathbb{R},<)$ *alebo* $b = d$ *a súčasne* $a < c$ *v* $(\mathbb{R},<)$*).*
Dokážte, že $(\mathbb{C},<_1)$ *aj* $(\mathbb{C},<_2)$ *sú usporiadané množiny. Usporiadanie* $<_1$ *sa nazýva lexikografické a* $<_2$ *antilexikografické usporiadanie množiny* $\mathbb{C}$.
(2) Definujte usporiadanie na množine $\mathbb{C}$ *, ktoré je rôzne od* $<_1$ *aj* $<_2$.

Cvičenie 2.2. *Na množine* $\mathbb{Z}$ *definujme binárnu operáciu* $\circ$ *predpisom* $a \circ b = -a.b$ *a reláciu* $<_1$ *tak, že* $a <_1 b$ *práve vtedy, keď* $b < a$. *Dokážte, že* $(\mathbb{Z},+,\circ,<_1)$ *je usporiadaný okruh.*

Cvičenie 2.3. *Nech* $(A,+,.,<)$ *je usporiadaný okruh,* $a,b,c,d \in A$. *Dokážte, že platí:*
a) Ak $a < b$ *a* $c < d$, *tak* $a + c < b + d$.
b) Ak $0 \leq a < b$ *a* $0 \leq c < d$, *tak* $a.c < b.d$.
c) Ak $a + c < b + c$, *tak* $a < b$.
d) Ak $a.c < b.c$ *a* $0 < c$ $(c < 0)$, *tak* $a < b$ $(a > b)$.
e) $a^2 - a.b + b^2 \geq 0$.
f) Pre každé $n \in \mathbb{N}_0$ *definujme* a^n *takto:* $a^0 = \mathbf{1}$, $a^{n+1} = a^n.a$. *Potom pre každé* $a > \mathbf{1}$ $(0 < a < \mathbf{1})$ *a pre každé* $n \in \mathbb{N}_0$ *platí* $a^n < a^{n+1}$ $(a^n > a^{n+1})$.
g) $a.b + a.c + b.c \leq a^2 + b^2 + c^2$.
h) Ak $a + b > 0$, *tak* $a.b.(a+b) \leq a^3 + b^3$.
i) $(x^3 + y^3)^2 \leq (x^2 + y^2).(x^4 + y^4)$.

Cvičenie 2.4. *Nech* $(A,+,.,<)$, $(B,+,.,<)$ *sú usporiadané okruhy. Zistite či je možné definovať na množine* $A \times B$ *usporiadanie tak, aby priamy súčin* $(A,+,.) \times (B,+,.)$ *okruhov* $(A,+,.)$ *a* $(B,+,.)$ *spolu s týmto usporiadaním bol usporiadaný okruh.*

Cvičenie 2.5. *(1) Dokážte, že ak* $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ *je homomorfizmus usporiadaných okruhov, tak pre každé* $a, b \in A$ *platí* $a <_A b \Leftrightarrow f(a) <_B f(b)$.
(2) Dokážte, že ak $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ *je izomorfizmus usporiadaných okruhov, tak aj* $f^{-1} : (B, +, ., <_B) \longrightarrow (A, +, ., <_A)$ *je izomorfizmus usporiadaných okruhov.*
(3) Dokážte že zobrazenie $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$ *je homomorfizmus usporiadaných okruhov vtedy a len vtedy, keď platí:*
a) $f(a + b) = f(a) + f(b)$, $f(a.b) = f(a).f(b)$.
c) Ak $a \in A^+_{<_A}$, *tak* $f(a) \in B^+_{<_B}$.
(4) Dokážte, že ak $f : (A, +, ., <_A) \longrightarrow (B, +, ., <_B)$, $g : (B, +, ., <_B) \longrightarrow (C, +, ., <_C)$ *sú homomorfizmy usporiadaných okruhov, tak aj* $g \circ f : (A, +, ., <_A) \longrightarrow (C, +, ., <_C)$ *je homomorfizmus usporiadaných okruhov.*
(5) Nech $(A, +, ., <_A)$ *je usporiadaný okruh. Dokážte, že podmnožina* $\overline{\mathbb{Z}} = \{z\mathbf{1} : z \in \mathbb{Z}\}$ *okruhu* $(A, +, ., <_A)$ *určuje usporiadaný podokruh okruhu* $(A, +, ., <_A)$, *ktorý je izomorfný s usporiadaným okruhom* $(\mathbb{Z}, +, ., <)$.

Cvičenie 2.6. *V okruhu polynomov* $\mathbb{Z}[x]$ *nech* $P = \{f(x) = a_0 + a_1.x + ... + a_n.x^n \in \mathbb{Z}[x] : a_n > O\}$. *Dokážte, že* P *je normálna podmnožina okruhu* $\mathbb{Z}[x]$ *a popíšte usporiadanie* $<_P$ *na* $\mathbb{Z}[x]$ *určené množinou* P.

Cvičenie 2.7. *V okruhu polynomov* $\mathbb{Z}[x]$ *definujme podmnožinu* P_1 *takto:* $f(x) = a_0 + a_1.x + ... + a_n.x^n \in P_1$ *práve vtedy, keď* $f(x) \neq 0$ *a pre* $j = min\{i \in \{0, ..., n\} : a_i \neq 0\}$ *platí* $a_j > 0$. . *Zistite, či* P_1 *je normálna podmnožina okruhu* $\mathbb{Z}[x]$ *a ak áno, tak popíšte usporiadanie* $<_{P_1}$ *na* $\mathbb{Z}[x]$ *určené množinou* P_1.

3 Absolútna hodnota v usporiadaných okruhoch

Definícia 3.1. *Nech* $(A, +, ., <)$ *je usporiadaný okruh,* $a \in A$. *Absolútnou hodnotou prvku* a *v* $(A, +, ., <)$ *nazývame prvok* $|a| \in A$ *definovaný nasledovne: Ak* $0 \leq a$, *tak* $|a| = a$, *ak* $a < 0$, *tak* $|a| = -a$.

Je zrejmé, že $|0| = 0$ a ak $a \neq 0$, tak $|a| > 0$.

Veta 3.1. *Nech* $(A, +, ., <)$ *je usporiadaný okruh,* $a, b \in A$. *Potom platí:*
a) $|a| = |-a| \geq 0$
b) $|a| = 0 \Leftrightarrow a = 0$
c) $a \leq |a|$, $-a \leq |a|$
d) $|a.b| = |a|.|b|$
e) $|a| < b \Leftrightarrow -b < a < b$
f) $|a| \leq b \Leftrightarrow -b \leq a \leq b$
g) $|a + b| \leq |a| + |b|$
h) $|a| - |b| \leq ||a| - |b|| \leq |a - b|$.

Dôkaz. a) Ak $a > 0$, tak $|a| = a > 0$, $-a < 0$ a preto $|-a| = -(-a) = a = |a|$. Ak $a < 0$, tak $|a| = -a > 0$ a teda $|-a| = -a = |a|$.

b) Zrejmé.
c) Ak $a \geq 0$, tak $|a| = a \geq 0 \geq -a$. Ak $a < 0$, tak $|a| = -a > 0 > a$. Teda, v obidvoch prípadoch platí $|a| \geq a$ a súčasne $|a| \geq -a$.
d) Ak $a = 0$ alebo $b = 0$, tak $a.b = 0$ a platí $|a.b| = 0 = |a|.|b|$. Ak $a > 0$, $b > 0$, tak $a.b > 0$ a platí $|a.b| = a.b = |a|.|b|$. Nech $a < 0$, $b > 0$. Potom $a.b < 0$, $|a| = -a$, $|b| = b$, $|a.b| = -(a.b)$ a teda $|a.b| = -(a.b) = (-a).b = |a|.|b|$. Zostávajúce prípady podobne.
e) Nech $|a| < b$. Pretože $a \leq |a|$, $-a \leq |a|$, dostávame $a < b$, $-a < b$ a z toho aj $-b < -(-a) = a$. Teda platí $-b < a < b$.
Obrátene, nech $-b < a < b$. Potom $a < b$, $-a < b$ a teda $|a| < b$.
f) Podobne, ako e).
g)Pretože $a \leq |a|$, $b \leq |b|$, platí tiež $a + b \leq |a| + |b|$. Z nerovností $-a \leq |a|$,$-b \leq |b|$ dostávame $-(a + b) \leq |a| + |b|$ z toho $-(|a| + |b|) \leq a + b$. Teda $-(|a| + |b|) \leq a + b \leq |a| + |b|$.
h) Platí $|a| = |a - b + b| \leq |a - b| + |b|$ a preto $|a| - |b| \leq |a - b|$. Súčasne platí $|b| = |b - a + a| \leq |b - a| + |a|$ a preto aj $|b| - |a| \leq |a - b|$. Potom ale $-|a - b| \leq |a| - |b| \leq |a - b|$ a z toho dostávame $||a| - |b|| \leq |a - b|$. Druhá nerovnosť je zrejmá.

□

Cvičenie 3.1. *a) Nech $(F, +, ., <)$ je usporiadané pole a $a \in F \setminus \{0\}$. Dokážte, že $|a^{-1}| = |a|^{-1}$.*

b) Nech $(A, +, .)$ je usporiadaný okruh, $a, b \in A$. Dokážte, že ak $a^2 = b^2$, tak $|a| = |b|$.

c) Dokážte časti b), f) vety 3.1.

4 Archimedovsky usporiadané okruhy a polia

V obore reálnych čísel (rovnako ako v oboroch celých čísel a racionálnych čísel) je množina všetkých prirodzených čísel zhora neohraničená. Táto vlastnosť oboru reálnych čísel sa nazýva Archimedova vlastnosť reálnych čísel. Uvedené číselné obory sú príkladmi archimedovsky usporiadaných okruhov v zmysle nasledujúcej definície:

Definícia 4.1. *Usporiadaný okruh $(A, +, ., <)$ sa nazýva archimedovsky usporiadaný, ak pre každé $a, b \in A$ platí: Ak $0 < a < b$, tak existuje $n \in \mathbb{N}$, pre ktoré $b < na$.*

Príklady 4.1. *Usporiadané okruhy $(\mathbb{Z}, +, ., <)$, $\mathbb{Q}, +, ., <)$ sú archimedovsky usporiadané okruhy. Skutočne, ak $a, b \in \mathbb{Z}$ a $0 < a < b$, tak $a \geq 1$ a $(b + 1).a \geq b+1 > b$,t. j. za n stačí zvoliť $b+1$. Ak $0 < \frac{p}{q} < \frac{m}{k}$ v $(\mathbb{Q}, +, ., <)$, $(p, q, m, k \in \mathbb{N})$, tak $q.(m+1).\frac{p}{q} = (m+1).p \geq m+1 > m \geq \frac{m}{k}$, t. j. za n môžeme zvoliť $q.(m+1)$. Je známe a neskôr to aj dokážeme, že aj usporiadané pole $(\mathbb{R}, +, ., <)$ je archimedovsky usporiadané.*
Teraz uvedieme príklad usporiadaného okruhu, ktorý nie je archimedovsky usporiadaný. Nech $(\mathbb{Q}[x], +, .)$ je okruh polynomov nad poľom $(\mathbb{Q}, +, .)$. Je to komu-

tatívny okruh s jednotkou a na tomto okruhu budeme definovať usporiadanie pomocou normálnej podmnožiny. Nech $P = \{f(x) = a_0 + a_1.x + ... + a_n.x^n \in \mathbb{Q}[x] : a_n > 0\}$. *Je zrejmé, že ak* $f(x), g(x) \in P$, *tak aj* $f(x) + g(x), f(x).g(x) \in P$. *Ak* $f(x) \in \mathbb{Q}[x]$, *tak platí práve jeden z výrokov:* $f(x) = 0$, $f(x) = a_0 + a_1.x + ... + a_n.x^n$ *a* $a_n > 0$, $f(x) = a_0 + a_1.x + ... + a_n.x^n$ *a* $a_n < 0$. *To ale znamená, že platí práve jeden z výrokov:* $f(x) = 0$, $f(x) \in P$, $-f(x) \in P$. *Teda* P *je normálna podmnožina v* $(\mathbb{Q}[x], +, .)$, *pomocou ktorej je definované usporiadanie* $<_P$ *množiny* $\mathbb{Q}[x]$, *pre ktoré je* $(\mathbb{Q}[x], +, ., <_P)$ *usporiadaný okruh. V tomto okruhu platí, že* $0 <_P 1 <_P x$ *lebo* $x - 1 = -1 + 1.x \in P$. *Pre každé* $n \in \mathbb{N}$ *platí* $x - n = -n + 1.x \in P$ *a preto* $n = n1 <_P x$. *Teda usporiadaný okruh* $(\mathbb{Q}[x], +, ., <_P)$ *nie je archimedovsky usporiadaný.*

Veta 4.1. *Ak* $(B, +, ., <_B)$ *je usporiadaný podokruh archimdovsky usporiadaného okruhu* $(A, +, ., <)$, *tak* $(B, +, ., <_B)$ *je archimedovsky usporiadaný okruh.*

Dôkaz. Nech $a, b \in B$, $0 <_B a <_B b$. Potom $a, b \in A$ a $0 < a < b$ v $(A, +, ., <)$ a preto existuje $n \in \mathbb{N}$ tak, že $b < na$. Pretože $b, na \in B$, platí $b <_B na$ v $(B, +, ., <_B)$. □

Veta 4.2. *Usporiadané pole* $(F, +, ., <)$ *je archimedovsky usporiadané vtedy a len vtedy, keď pre každé* $b > 0$ *existuje* $n \in \mathbb{N}$ *tak, že* $b < n\mathbf{1}$.

Dôkaz. Nech $(F, +, ., <)$ je archimedovsky usporiadané, $b > 0$. Potom $b + \mathbf{1} > \mathbf{1} > 0$ a preto existuje $n \in \mathbb{N}$ tak, že $b + 1 < n\mathbf{1}$. Pretože $b < b + 1$, dostávame, že $b < n\mathbf{1}$.
Obrátene, nech pre každé $b > 0$ existuje $n \in \mathbb{N}$ tak, že $b < n\mathbf{1}$. Nech $0 < a < b$. Pretože $0 < a^{-1}$ platí $0 < b.a^{-1}$. Pretože $0 < b.a^{-1}$, podľa predpokladu existuje $n \in \mathbb{N}$ tak, že $b.a^{-1} < n\mathbf{1}$. Potom ale $b < (n\mathbf{1}).a = n(\mathbf{1}.a) = na$. □

Dôsledok 4.1. *Usporiadané pole* $(F, +, ., <)$ *je archimedovsky usporiadané vtedy a len vtedy, keď pre každé* $b > 0$ *existuje* $n \in \mathbb{N}$ *tak, že* $(n\mathbf{1})^{-1} < b$.

Dôkaz. Ak $b > 0$, tak aj $b^{-1} > 0$ a existuje $n \in \mathbb{N}$ tak, že $b^{-1} < n\mathbf{1}$. Potom $(n\mathbf{1})^{-1} < b$. Obrátene, nech $a > 0$. Potom $a^{-1} > 0$ a existuje $n \in \mathbb{N}$ tak, že $(n\mathbf{1})^{-1} < a^{-1}$. Potom $a < n\mathbf{1}$. □

Definícia 4.2. *Prvok* r *usporiadaného poľa* $(F, +, ., <)$ *sa nazýva racionálny, ak existuje* $z \in \mathbb{Z}$ *a* $n \in \mathbb{N}$ *tak, že* $r = (z\mathbf{1}).(n\mathbf{1})^{-1}$. *Množinu všetkých racionálnych prvkov usporiadaného poľa* $(F, +, ., <)$ *budeme označovať* $\mathbb{Q}_F$.

Veta 4.3. *Ak* $(F, +, ., <)$ *je archimedovsky usporiadané pole, tak pre každé* $a, b \in F$, $a < b$ *existuje racionálny prvok* $r \in \mathbb{Q}_F$ *tak, že platí* $a < r < b$.

Dôkaz. Nech $0 \leq a < b$. Potom $0 < b - a$ a podľa dôsledku 4.1 existuje $n \in \mathbb{N}$ tak, že $(n\mathbf{1})^{-1} < b - a$. Pretože $0 < (n\mathbf{1})$ a $0 \leq a$, platí $0 \leq a.(n\mathbf{1})$. Pole $(F, +, ., <)$ je archimedovsky usporiadané, preto existuje $m \in \mathbb{N}$ tak, že $a.(n\mathbf{1}) < m\mathbf{1}$. Potom, keďže $0 < (n\mathbf{1})^{-1}$, platí $a < (m\mathbf{1}).(n\mathbf{1})^{-1}$. Nech k je najmenšie prirodzené číslo, pre ktoré $a < (k\mathbf{1}).(n\mathbf{1})^{-1}$. Potom $((k-1)\mathbf{1}).(n\mathbf{1})^{-1} \leq a$ a $(k\mathbf{1}).(n\mathbf{1})^{-1} = ((k-1)\mathbf{1}+\mathbf{1}).(n\mathbf{1})^{-1} = ((k-1)\mathbf{1}).(n\mathbf{1})^{-1} + (n\mathbf{1})^{-1} \leq a + (n\mathbf{1})^{-1} < a + (b-a) = b$.

Teda $a < (k\mathbf{1}).(n\mathbf{1})^{-1} < b$, pričom $(k\mathbf{1}).(n\mathbf{1})^{-1} \in \mathbb{Q}_F$. Ak $a < 0 < b$, tak tvrdenie platí, lebo $0 \in \mathbb{Q}_F$. Nech $a < b \leq 0$. Potom $0 \leq -b < -a$ a podľa prvej časti tohoto dôkazu existuje $r \in \mathbb{Q}_F$ tak že $-b < r < -a$. Potom $a < -r < b$, pričom $-r \in \mathbb{Q}_F$. □

Cvičenie 4.1. *Zistite, či usporiadaný okruh z cvičenia* 2.5. *je archimedovsky usporiadaný.*

Cvičenie 4.2. *Nech $(A, +, ., <)$ je usporiadaný okruh. Dokážte:*
a) Ak množina $A^+_<$ má najmenší prvok a, tak $a = \mathbf{1}$.
b) Ak $(A, +, ., <)$ je archimedovsky usporiadaný a množina $A^+_<$ má najmenší prvok, tak $(A, +, ., <)$ je izomorfný s usporiadaným okruhom $(\mathbb{Z}, +, ., <)$.
c) Uveďte príklad usporiadaného okruhu, v ktorom má množina kladných prvkov najmenší prvok a tento okruh nie je archimedovsky usporiadaný.

Cvičenie 4.3. *Dokážte, že množina $\mathbb{Q}_F$ racionálnych prvkov usporiadaného poľa $(F, +, ., <)$ je podpoľom poľa $(F, +, .)$ a usporiadané podpole $(\mathbb{Q}_F, +, ., <)$ usporiadaného poľa $(F, +, ., <)$ je izomorfné s usporiadaným poľom $(\mathbb{Q}, +, ., <)$.*

Cvičenie 4.4. *Nech $(A, +, ., <)$ je usporiadaný okruh a $(\mathbb{Q}(A), +, .)$ je podielové pole okruhu $(A, +, .)$ (pripomeňme, že $(A, +, .)$ je komutatívny obor integrity s jednotkovým prvkom). Nech $P = \{\frac{a}{b} \in \mathbb{Q}(A) : \ a.b > 0 \ v \ (A, +, ., <)\}$. Dokážte, že P je normálna podmnožina v poli $(\mathbb{Q}(A), +, .)$, zobrazenie $h : (A, +, ., <) \longrightarrow (\mathbb{Q}(A), +, ., <_P)$ definované predpisom $h(a) = \frac{a}{\mathbf{1}}$ je homomorfizmus usporiadaných okruhov. Ďalej dokážte, že usporiadané pole $(\mathbb{Q}(A), +, ., <_P)$ je archimedovsky usporiadané vtedy a len vtedy,keď $(A, +, ., <)$ je archimedovsky usporiadaný okruh.*

5 Spojito usporiadané polia

Je známe, že v obore reálnych čísel má každá neprázdna, zhora ohraničená podmnožina suprémum. Obor reálnych čísel je teda príkladom spojito usporiadaného poľa v zmysle nasledujúcej definície:

Definícia 5.1. *Nech $(A, <)$ je usporiadaná množina, $M \subseteq A$.*
a) Prvok $a \in A$ sa nazýva horné (dolné) ohraničenie množiny M, ak pre každé $b \in M$ $b \leq a$ $(b \geq a)$.
b) Množina M sa nazýva zhora (zdola) ohraničená, ak existuje horné (dolné) ohraničenie M v $(A, <)$.
c) Prvok $c \in A$ sa nazýva suprémum (infimum) množiny M, ak c je najmenšie horné ohraničenie (najväčšie dolné ohraničenie) množiny M.
d) $(A, <)$ sa nazýva husto usporiadaná, ak A má aspoň dva rôzne prvky a pre každé $a, b \in A$, $a < b$ existuje $c \in A$ tak, že $a < c < b$.
e) $(A, <)$ sa nazýva spojito usporiadaná, ak pre každú neprázdnu zhora ohraničenú podmnožinu množiny A existuje suprémum tejto množiny.
f) Usporiadané pole $(F, +, ., <)$ sa nazýva spojito (husto) usporiadané, ak usporiadaná množina $(F, <)$ je spojito (husto) usporiadaná.

Príklady 5.1. *a) Každé usporiadané pole $(F,+,.,<)$ je husto usporiadané. Skutočne, nech $a,b \in F$, $a<b$. Nech $\mathbf{1}$ je jednotka poľa $(F,+,.,<)$ a $\mathbf{2}$ označuje prvok $\mathbf{1}+\mathbf{1} \in F$. Potom, zrejme, $\mathbf{2}.a = (\mathbf{1}+\mathbf{1}).a = a+a < a+b < b+b = \mathbf{2}.b$ a pretože $\mathbf{2}^{-1} > 0$, platí tiež $a < (a+b).\mathbf{2}^{-1} < b$.*
b) Usporiadané pole $(\mathbb{Q},+,.,<)$ nie je spojito usporiadané. Skutočne, nech $M = \{a \in \mathbb{Q} : \ 0 < a, \ a^2 < 2\}$. Ukážeme, že M je neprázdna, zhora ohraničená podmnožina usporiadanej množiny $(\mathbb{Q},<)$, ktorá nemá supremum. Pretože $1 \in M$, $M \neq \emptyset$. Ak $0 < a$ a $a^2 < 2$, tak $a^2 < 4$ a teda $a = |a| < 2$. Ukázali sme, že 2 je horné ohraničenie množiny M. Ďalej budeme postupovať sporom. Nech existuje $c = supM$. Zrejme $c \geq 1 > 0$. Potom pre každé $a \in M$ $a \leq c$ a potom aj $a^2 \leq c^2$. Pretože $c \in \mathbb{Q}$, máme $c^2 \neq 2$ a preto $c^2 > 2$ alebo $c^2 < 2$. Predpokladajme, že $c^2 > 2$. Ukážeme, že existuje $r \in \mathbb{Q}$, $r > 0$, tak, že $c - r$ je horné ohraničenie M. Ak $r \in \mathbb{Q}$ a $r > 0$, tak $(c-r)^2 = c^2 - 2.c.r + r^2 > c^2 - 2.c.r$. Súčasne platí $c^2 - 2.c.r > 2 \Leftrightarrow c^2 - 2 > 2.c.r \Leftrightarrow r < \frac{c^2-2}{2.c}$. Pretože $0 < \frac{c^2-2}{2.c}$ a $0 < c$, existuje $r \in \mathbb{Q}$ tak, že $0 < r < \frac{c^2-2}{2.c}$ a súčasne $r < c$ a pre toto r platí $(c-r)^2 > c^2 - 2.c.r > 2$. Potom pre každé $a \in M$ platí $a^2 < 2 < (c-r)^2$ a preto $a = |a| < |c-r| = c - r$. Teda $c - r$ je horné ohraničenie M a súčasne $c - r < c = supM$ a to je spor. Teraz predpokladajme, že $c^2 < 2$. Ukážeme, že v tomto prípade existuje $r \in \mathbb{Q}$, $0 < r < 1$ tak, že $c + r$ je prvkom množiny M. Ak $r \in \mathbb{Q}$ a $0 < r < 1$, tak platí $(c+r)^2 = c^2 + 2.c.r + r^2 < c^2 + 2.c.r + r$ (lebo $r^2 < r$). Súčasne platí $c^2 + 2.c.r + r < 2 \Leftrightarrow 2.c.r + r < 2 - c^2 \Leftrightarrow r < \frac{2-c^2}{2.c+1}$. Pretože $0 < \frac{2-c^2}{2.c+1}$, existuje $r \in \mathbb{Q}$, $r < 1$ tak, že $0 < r < \frac{2-c^2}{2.c+1}$. Pre takéto r potom $(c+r)^2 < c^2 + 2.c.r + r < 2$ a pretože súčasne $0 < c + r$, dostávame, že $c + r \in M$. Potom $c = supM < c + r \in M$ a to je spor. Teda predpoklad, že existuje $supM$ vedie k sporu.

Veta 5.1. *Ak usporiadané pole $(F,+,.,<)$ je spojito usporiadané, tak je aj archimedovsky usporiadané.*

Dôkaz. Nech $(F,+,.,<)$ nie je archimedovsky usporiadané. Potom existuje $a \in F$ tak, že pre každé $n \in \mathbb{N}$ $n\mathbf{1} \leq a$. Nech $M = \{n\mathbf{1} : \ n \in \mathbb{N}\}$. Potom $M \subseteq F$, $M \neq \emptyset$ a M je zhora ohraničená podmnožina v $(F,<)$. Preto existuje $supM = c \in F$. Pretože $-\mathbf{1} < 0$, platí $c - \mathbf{1} < c$ a teda prvok $c - \mathbf{1}$ nie je horné ohraničenie množiny M. Preto existuje $k \in \mathbb{N}$ tak, že $c - \mathbf{1} < k\mathbf{1}$. Potom ale $supM = c = (c - \mathbf{1}) + \mathbf{1} < k\mathbf{1} + \mathbf{1} = (k+1)\mathbf{1} \in M$, čo je spor. Teda $(F,+,.,<)$ je archimedovsky usporiadané pole. □

Veta 5.2. *Usporiadané pole $(F,+,.,<)$ je spojito usporiadané vtedy a len vtedy, keď každá neprázdna zdola ohraničená podmnožina poľa $(F,+,.,<)$ má infimum.*

Dôkaz. Nech $(F,+,.,<)$ je spojito usporiadané, M je neprázdna, zdola ohraničená podmnožina poľa $(F,+,.,<)$ a $d \in F$ je dolné ohraničenie M. Nech $-M = \{-a : \ a \in M\}$. Potom $-M$ je neprázdna, zhora ohraničená podmnožina poľa $(F,+,.,<)$ (zrejme prvok $-d$ je horné ohraničenie $-M$,lebo $a \geq d \Leftrightarrow -a \leq -d$). Potom ale existuje $c \in F$ tak, že $c = sup(-M)$. Ľahko sa overí, že $-c = infM$. Obrátená implikácia sa dokáže analogicky. □

Cvičenie 5.1. *Dokážte podrobne vetu 5.2.*

Cvičenie 5.2. *Dokážte, že v usporiadanom okruhu $(\mathbb{Z}, +, ., <)$ má každá neprázdna zhora ohraničená množina najväčší prvok a každá neprázdna zdola ohraničená množina najmenší prvok (prvok $a \in M$ sa nazýva najväčší (najmenší) prvok množiny M, ak pre všetky $b \in M$ platí $b \leq a$ $(b \geq a)$).*

Cvičenie 5.3. *Dokážte, že ak $(F, +, ., <_F)$ je usporiadané podpole usporiadaného poľa $(\mathbb{R}, +, ., <)$ a $F \neq \mathbb{R}$, tak $(F, +, ., <_F)$ nie je spojito usporiadané.*

6 Úplné usporiadané polia

Pojem úplného usporiadaného poľa súvisí s konvergenciou postupností a s fundamentálnymi postupnosťami v usporiadaných poliach.

Definícia 6.1. *Nech $\{a_n\}_{n=1}^{\infty}$ je postupnosť prvkov usporiadaného poľa $(F, +, ., <)$. Potom*
a) Postupnosť $\{a_n\}_{n=1}^{\infty}$ sa nazýva ohraničená v usporiadanom poli $(F, +, ., <)$, ak existuje $c \in F$ tak, že pre každé $n \in \mathbb{N}$ platí $|a_n| \leq c$.
b) Hovoríme, že postupnosť $\{a_n\}_{n=1}^{\infty}$ konverguje k prvku $c \in F$, ak pre každé $\varepsilon \in F$, $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ tak, že pre každé $n \in \mathbb{N}$, $n \geq n_0$ platí $|a_n - c| < \varepsilon$. Označenie: $\lim_{n\to\infty} a_n = c$, alebo $a_n \longrightarrow c$.
c) Postupnosť $\{a_n\}_{n=1}^{\infty}$ sa nazýva fundamentálna v $(F, +, ., <)$, ak pre každé $\varepsilon \in F$, $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ tak, že pre každé $n, k \in \mathbb{N}$, $n, k \geq n_0$ platí $|a_n - a_k| < \varepsilon$.
d) Postupnosť $\{a_n\}_{n=1}^{\infty}$ sa nazýva neklesajúca (rastúca, nerastúca, klesajúca), ak pre každé $n \in \mathbb{N}$ platí $a_n \leq a_{n+1}$ $(a_n < a_{n+1}$, $a_n \geq a_{n+1}$, $a_n > a_{n+1})$.

Poznámka 6.1. *Ľahko sa overí, že ak $\lim_{n\to\infty} a_n = c$ a súčasne $\lim_{n\to\infty} a_n = d$, tak $c = d$ (ak napríklad $c < d$, tak zvolíme $\varepsilon = (d - c).\mathbf{2}^{-1} > 0$ a z daného predpokladu dostaneme spor. Podobne pre $d < c$).*

Odteraz budeme v usporiadaných poliach $(F, +, ., <)$ používať nasledujúce označenia: Pre každé $z \in \mathbb{Z}$ budeme z-násobok jednotkového prvku $z\mathbf{1}$ označovať $\mathbf{z}$ (t. j. napríklad $\mathbf{1} + \mathbf{1} = \mathbf{2}$, $\mathbf{1} + \mathbf{1} + \mathbf{1} = \mathbf{2} + \mathbf{1} = \mathbf{3}$, a pod.). Inverzný prvok b^{-1} k prvku b budeme označovať aj $\frac{1}{b}$ a súčin $a.b^{-1}$ budeme označovať aj $\frac{a}{b}$. Racionálny prvok $(z\mathbf{1}).(n\mathbf{1})^{-1}$ môžeme potom zapísať aj $\frac{\mathbf{z}}{\mathbf{n}}$.

Veta 6.1. *Nech $\{a_n\}_{n=1}^{\infty}$ je postupnosť v usporiadanom poli $(F, +, ., <)$. Potom platí:*
a) Ak $\{a_n\}_{n=1}^{\infty}$ je konvergentná, tak $\{a_n\}_{n=1}^{\infty}$ je fundamentálna.
b) Ak $\{a_n\}_{n=1}^{\infty}$ je fundamentálna, tak $\{a_n\}_{n=1}^{\infty}$ je ohraničená.

Dôkaz. a) Nech $\lim_{n\to\infty} a_n = c$ a $\varepsilon \in F$, $\varepsilon > 0$. Potom aj $\frac{\varepsilon}{\mathbf{2}} > 0$ a existuje $n_0 \in \mathbb{N}$ tak, že pre každé $n \in \mathbb{N}$, $n \geq n_0$ platí $|a_n - c| < \frac{\varepsilon}{\mathbf{2}}$. Potom, pre každé $n, k \in \mathbb{N}$, $n, k \geq n_0$, platí $|a_n - a_k| = |a_n - c + c - a_k| \leq |a_n - c| + |c - a_k| < \frac{\varepsilon}{\mathbf{2}} + \frac{\varepsilon}{\mathbf{2}} = \varepsilon$. Teda $\{a_n\}_{n=1}^{\infty}$ je fundamentálna.
b) Nech $\{a_n\}_{n=1}^{\infty}$ je fundamentálna. Zvoľme prvok $\mathbf{1} \in F$. Pretože $\mathbf{1} > 0$ existuje

$n_0 \in \mathbb{N}$ tak, že pre všetky $n, k \in \mathbb{N}$, $n, k \geq n_0$ platí $|a_n - a_k| < \mathbf{1}$ a teda pre každé $n \geq n_0$ platí $|a_n - a_{n_0}| < \mathbf{1}$, čo je ekvivalenné s tým, že $-\mathbf{1} < a_n - a_{n_0} < \mathbf{1}$. Potom pre každé $n \geq n_0$ platí $-\mathbf{1} - |a_{n_0}| \leq -\mathbf{1} + a_{n_0} < a_n < \mathbf{1} + a_{n_0} \leq \mathbf{1} + |a_{n_0}|$. Teda pre každé $n \geq n_0$ platí $|a_n| < \mathbf{1} + |a_{n_0}|$. Nech c je najväčší prvok množiny $\{|a_1|, ...|a_{n_0-1}|, \mathbf{1} + |a_{n_0}|\}$. Potom pre každé $n \in \mathbb{N}$ platí $|a_n| \leq c$. □

Dôsledok 6.1. *Každá konvergentná postupnosť v usporiadanom poli je ohraničená.*

Definícia 6.2. *Usporiadané pole $(F, +, ., <)$ sa nazýva úplné, ak každá fundamentálna postupnosť v poli $(F, +, ., <)$ je konvergentná.*

Príklady 6.1. *a) Je známe (napríklad z matematickej analýzy), že usporiadané pole $(\mathbb{R}, +, ., <)$ je úplné.*
b) Usporiadané pole $(\mathbb{Q}, +, ., <)$ nie je úplné.
Nech pre každé $n \in \mathbb{N}$ $a_n = 1 + \frac{1}{1!} + ... + \frac{1}{n!}$. Ukážeme, že postupnosť $\{a_n\}_{n=1}^{\infty}$ je fundamentálna a nie je konvergentná v $(\mathbb{Q}, +, ., <)$. Zrejme, pre každé $n \in \mathbb{N}$ platí $a_{n+1} = a_n + \frac{1}{(n+1)!} > a_n$, t. j. $\{a_n\}_{n=1}^{\infty}$ je rastúca postupnosť. Pripomeňme, že pre $n \geq 4$ platí $n! = 1.2.3.4...n > 2^n$ a teda $\frac{1}{n!} < \frac{1}{2^n}$. Nech $3 \leq k < n$. Potom $0 < a_n - a_k = \frac{1}{(k+1)!} + ... + \frac{1}{n!} < \frac{1}{2^{k+1}} + ... + \frac{1}{2^n} \leq \frac{1}{2^k}.(\frac{1}{2} + ... + \frac{1}{2^{n-k}}) \leq \frac{1}{2^k}.(\frac{1}{2} + ... + \frac{1}{2^{n-k}} + ...) = \frac{1}{2^k}$.
Nech $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$. Potom existuje $k_0 \geq 3$ tak, že $\frac{1}{2^{k_0}} < \varepsilon$. Pre ľubovoľné $k, n \in \mathbb{N}$ také, že $k_0 \leq k < n$ platí $a_n - a_k = |a_n - a_k| < \frac{1}{2^k} \leq \frac{1}{2^{k_0}} < \varepsilon$. Teda $\{a_n\}_{n=1}^{\infty}$ je fundamentálna.
Ukážeme, že $\{a_n\}_{n=1}^{\infty}$ nekonverguje v usporiadanom poli $(\mathbb{Q}, +, ., <)$. Sporom. Nech existuje $\lim_{n\to\infty} a_n = c \in \mathbb{Q}$. Zrejme $c > 0$ a preto existujú $p, q \in \mathbb{N}$ tak, že $c = \frac{p}{q}$, pričom môžeme predpokladať, že $q \geq 3$ ($\frac{p}{q} = \frac{3.p}{3.q}$). Pretože postupnosť $\{a_n\}_{n=1}^{\infty}$ je rastúca, pre každé $n \in \mathbb{N}$ platí $a_n < \frac{p}{q}$, a teda $|a_n - \frac{p}{q}| = \frac{p}{q} - a_n$. Zvoľme $\varepsilon = \frac{1}{2.(q!)} > 0$. Potom existuje $n_0 \in \mathbb{N}$ tak, že pre každé $n \in \mathbb{N}$, $n \geq n_0$ platí $|a_n - \frac{p}{q}| = \frac{p}{q} - a_n < \frac{1}{2.(q!)}$. Zvoľme $n \in \mathbb{N}$ tak, že $n \geq n_0$ a súčasne $n > q$. Potom $0 < \frac{p}{q} - a_n = \frac{p}{q} - (1 + \frac{1}{1!} + ... + \frac{1}{q!} + ... + \frac{1}{n!}) = \frac{p}{q} - a_q - \frac{1}{(q+1)!} - ... - \frac{1}{n!} < \frac{1}{2.(q!)}$. Potom $0 < \frac{p}{q} - a_q < \frac{1}{(q+1)!} + ... + \frac{1}{n!} + \frac{1}{2.(q!)}$ a po vynásobení tejto nerovnosti číslom $q!$ dostaneme, že platí $0 < p.((q-1)!) - (q!).a_q < \frac{1}{q+1} + \frac{1}{(q+1).(q+2)} + ... + \frac{1}{(q+1).....n} + \frac{1}{2} < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^{n-q+1}} < 1$. Číslo $d = p.(q-1)!) - (q!).a_q = p.((q-1)!) - (q!).(1 + \frac{p1}{1!} + ... + \frac{1}{q!})$ je celé číslo, pre ktoré platí $O < d < 1$, čo je spor. Teda postupnosť $\{a_n\}_{n=1}^{\infty}$ nekonverguje v $(\mathbb{Q}, +, ., <)$.

Veta 6.2. *Ak usporiadané pole $(F, +, ., <)$ je spojito usporiadané, tak je úplné.*

Dôkaz. Nech $\{a_n\}_{n=1}^{\infty}$ je fundamentálna postupnosť v poli $(F, +, ., <)$. Potom $\{a_n\}_{n=1}^{\infty}$ je ohraničená v $(F, +, ., <)$ a teda existuje $b \in F$ tak, že pre každé $n \in \mathbb{N}$ platí $-b \leq a_n \leq b$. Definujme množinu $M \subseteq F$ takto: $M = \{x \in F : \{n \in \mathbb{N} : \ a_n < x\}$ je konečná$\}$. Zrejme $-b \in M$, lebo $\{n \in \mathbb{N} : \ a_n < -b\} = \emptyset$ je konečná. Teda $M \neq \emptyset$. Ak $t \in F$ a $b < t$, tak $\{n \in \mathbb{N} : \ a_n < t\} = \mathbb{N}$ je nekonečná a preto $t \notin M$. Teda pre každé $x \in M$ platí $x \leq b$ a preto M je zhora

ohraničená v $(F,<)$. Pretože pole $(F,+,.,<)$ je spojito usporiadané, existuje $supM = c \in F$. Ukážeme, že $\lim_{n\to\infty} a_n = c$.
Nech $\varepsilon \in F$, $\varepsilon > 0$. Potom aj $\frac{\varepsilon}{\mathbf{2}} > 0$ a $c + \frac{\varepsilon}{\mathbf{2}} > c$. Preto $c + \frac{\varepsilon}{\mathbf{2}} \notin M$ a množina $K = \{n \in \mathbb{N} : \ a_n < c + \frac{\varepsilon}{\mathbf{2}}\}$ je nekonečná. Pretože $c - \frac{\varepsilon}{\mathbf{2}} < c$, existuje $y \in M$ tak, že $c - \frac{\varepsilon}{\mathbf{2}} < y \leq c$. Množina $L = \{n \in \mathbb{N} : \ a_n < y\}$ je konečná a preto množina $K \setminus L$ je nekonečná. Nech $K \setminus L = \{n_1 < n_2 < ... < n_k < ...\}$. Pre každé $k \in \mathbb{N}$ platí $c - \frac{\varepsilon}{\mathbf{2}} < y \leq a_{n_k} < c + \frac{\varepsilon}{\mathbf{2}}$ a teda $|a_{n_k} - c| < \frac{\varepsilon}{\mathbf{2}}$. Pretože postupnosť $\{a_n\}_{n=1}^{\infty}$ je fundamentálna a $\frac{\varepsilon}{\mathbf{2}} > 0$, existuje $n_0 \in \mathbb{N}$ tak, že pre všetky $m, n \geq n_0$ platí $|a_m - a_n| < \frac{\varepsilon}{\mathbf{2}}$. Pretože množina $K \setminus L$ je nekonečná, môžeme vybrať $k \in \mathbb{N}$, pre ktoré $n_k \geq n_0$. Potom pre každé $n \geq n_0$ platí $|a_n - c| \leq |a_n - a_{n_k}| + |a_{n_k} - c| < \frac{\varepsilon}{\mathbf{2}} + \frac{\varepsilon}{\mathbf{2}} = \varepsilon$. Teda $\lim_{n\to\infty} a_n = c$. □

Lema 6.1. *Nech $(F,+,.,<)$ je usporiadané pole. Potom platí:*
a) Ak $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ sú postupnosti prvkov poľa $(F,+,.,<)$, $r \in F$, $\lim_{n\to\infty} a_n = c$, $\lim_{n\to\infty} b_n = d$, tak $lim_{n\to\infty}(a_n+b_n) = c+d$, $lim_{n\to\infty} r.a_n = r.c$ a $lim_{n\to\infty}(a_n.b_n) = c.d$.
b) Ak $\lim_{n\to\infty} a_n = c$, $t \in F$ a pre každé $n \in \mathbb{N}$ platí $a_n \leq t$ $(a_n \geq t)$, tak $c \leq t$ $(c \geq t)$.
c) Ak $(F,+,.,<)$ je archimedovsky usporiadané a $r \in F$, $r > 0$, tak $\lim_{n\to\infty} \frac{r}{\mathbf{2}^n} = 0$.

Dôkaz. Je rovnaký ako pre analogické tvrdenia o postupnostiach reálnych čísel v matematickej analýze. Na ukážku uvedieme dôkaz časti a) pre súčin postupností. Nech $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ sú konvergentné postupnosti. Potom tieto postupnosti sú ohraničené a existuje $r \in F$, $r > 0$ tak, že pre každé $n \in \mathbb{N}$ platí $|a_n| \leq r$. Nech $\varepsilon \in F$, $\varepsilon > 0$. Potom aj $\frac{\varepsilon}{\mathbf{2}.r} > 0$ a existuje $n_1 \in \mathbb{N}$ tak, že pre všetky $n \in \mathbb{N}$, $n \geq n_1$ platí $|b_n - d| < \frac{\varepsilon}{\mathbf{2}.r}$. Zrejme $|d| + \mathbf{1} > 0$ a preto aj $\frac{\varepsilon}{\mathbf{2}.(|d|+\mathbf{1})} > 0$. Potom existuje $n_2 \in \mathbb{N}$ tak, že pre všetky $n \in \mathbb{N}$, $n \geq n_2$ platí $|a_n - c| < \frac{\varepsilon}{\mathbf{2}.(|d|+\mathbf{1})}$. Nech $n_0 = n_1 + n_2$. Potom pre každé $n \in \mathbb{N}$, $n \geq n_0$ platí $|a_n.b_n - c.d| = |a_n.b_n - a_n.d + a_n.d - c.d| \leq |a_n|.|b_n - d| + |a_n - c|.|d| \leq r.|b_n - d| + |a_n - c|.(|d| + \mathbf{1}) < r.\frac{\varepsilon}{\mathbf{2}.r} + \frac{\varepsilon}{\mathbf{2}.(|d|+\mathbf{1})}.(|d| + \mathbf{1}) = \varepsilon$. Teda $lim_{n\to\infty}(a_n.b_n) = c.d$. □

Veta 6.3. *Ak usporiadané pole $(F,+,.,<)$ je úplné a archimedovsky usporiadané, tak $(F,+,.,<)$ je spojito usporiadané.*

Dôkaz. Nech $M \subseteq F$, $M \neq \emptyset$ a M je zhora ohraničená v $(F,+,.,<)$. Vyberme prvok $t \in M$ a prvok $b_1 \in F$ tak, že b_1 je horné ohraničenie množiny M. Potom $t \leq b_1$ a pre prvok $a_1 = t - \mathbf{1} \in F$ platí $a_1 < t \leq b_1$. Teda a_1 nie je horné ohraničenie M a $a_1 < b_1$. Utvorme prvok $\frac{a_1+b_1}{\mathbf{2}}$. Pretože $a_1 < b_1$, platí $a_1 + a_1 < a_1 + b_1 < b_1 + b_1$ a tiež $a_1 < \frac{a_1+b_1}{\mathbf{2}} < b_1$ (lebo $\frac{\mathbf{1}}{\mathbf{2}} > 0$). Ak prvok $\frac{a_1+b_1}{\mathbf{2}}$ nie je horné ohraničenie M, tak zvolíme $a_2 = \frac{a_1+b_1}{\mathbf{2}}$ a $b_2 = b_1$. Ak prvok $\frac{a_1+b_1}{\mathbf{2}}$ je horné ohraničenie M, tak zvolíme $a_2 = a_1$ a $b_2 = \frac{a_1+b_1}{\mathbf{2}}$. V obidvoch prípadoch platí $a_1 \leq a_2 < b_2 \leq b_1$, $b_2 - a_2 = \frac{b_1-a_1}{\mathbf{2}}$, a_1, a_2 nie sú horné ohraničenia M a b_1, b_2 sú horné ohraničenia M. Predpokladajme, že $n \in \mathbb{N}$ a sú dané prvky $a_n < b_n$ poľa $(F,+,.,<)$ tak, že a_n nie je horné ohraničenie M a b_n je horné ohraničenie M. Potom, v prípade, že $\frac{a_n+b_n}{\mathbf{2}}$ nie je

horné ohraničenie M, zvolíme $a_{n+1} = \frac{a_n+b_n}{\mathbf{2}}$, $b_{n+1} = b_n$, v opačnom prípade (ak $\frac{a_n+b_n}{\mathbf{2}}$ je horné ohraničenie M) zvolíme $a_{n+1} = a_n$ a $b_{n+1} = \frac{a_n+b_n}{\mathbf{2}}$. Je zrejmé, že $a_n \leq a_{n+1} < b_{n+1} \leq b_n$, a_{n+1} nie je, b_{n+1} je horné ohraničenie M a $b_{n+1} - a_{n+1} = \frac{b_n-a_n}{\mathbf{2}}$. Týmto spôsobom sú matematickou indukciou definované postupnosti $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ v poli $(F, +, ., <)$, pre ktoré platí: $a_1 \leq a_2 \leq ... \leq a_n \leq ..... \leq b_n \leq ... \leq b_2 \leq b_1$, pre každé $n \in \mathbb{N}$ platí, že a_n nie je a b_n je horné ohraničenie množiny M, $a_n < b_n$ a $b_{n+1} - a_{n+1} = \frac{b_n-a_n}{\mathbf{2}} = ... = \frac{b_1-a_1}{\mathbf{2}^n}$. Pretože pole $(F, +, ., <)$ je archimedovsky usporiadané a $\mathbf{2}.(b_1 - a_1) > 0$, podľa Lemy 6.1 platí, že $lim_{n\to\infty}(b_n - a_n) = lim_{n\to\infty}\frac{\mathbf{2}.(b_1-a_1)}{\mathbf{2}^n} = 0$. Ukážeme, že postupnosť $\{a_n\}_{n=1}^{\infty}$ je fundamentálna. Nech $\varepsilon > 0$. Potom existuje $n_0 \in \mathbb{N}$ tak, že $|(b_{n_0} - a_{n_0}) - 0| = b_{n_0} - a_{n_0} < \varepsilon$. Pre všetky $m, k \in \mathbb{N}$, $m, k \geq n_0$ platí $a_{n_0} \leq a_n, a_k \leq b_{n_0}$ ($a_n < b_n \leq b_{n_0}$, $a_k < b_k \leq b_{n_0}$) a preto $|a_n - a_k| \leq b_{n_0} - a_{n_0} < \varepsilon$. Pretože $\{a_n\}_{n=1}^{\infty}$ je fundamentálna a $(F, +, ., <)$ je úplné, existuje $\lim_{n\to\infty} a_n = c$. Potom $lim_{n\to\infty}b_n = lim_{n\to\infty}(a_n + (b_n - a_n)) = c + 0 = c$. Ukážeme, že $c = supM$. Nech $r \in M$. Pretože pre každé $n \in \mathbb{N}$ platí $r \leq b_n$ a podľa Lemy 6.1.b) potom $r \leq c$. Teda c je horné ohraničenie M. Nech $s \in F$ je ľubovoľné horné ohraničenie M. Pretože pre každé $n \in \mathbb{N}$ a_n nie je horné ohraničenie M, platí $a_n < s$ a preto, podľa Lemy 6.1.b) $c \leq s$. Teda c je najmenšie horné ohraničenie (t. j. supremum) množiny M. Dokázali sme, že pole $(F, +, ., <)$ je spojito usporiadané. □

Z viet 5.1, 6.2 a 6.3 dostávame:

Veta 6.4. *Usporiadané pole $(F, +, ., <)$ je spojito usporiadané vtedy a len vtedy, keď je archimedovsky usporiadané a úplné.*

7 Konštrukcia oboru celých čísel

Obor celých čísel zostrojíme z oboru celých nezáporných čísel $(\mathbb{N}_0, +, ., <)$, ktorý bol vytvorený v rámci teórie množín. V obore celých nezáporných čísel platí:

Lema 7.1. *Nech $m, k \in \mathbb{N}_0$. Potom $k \leq m$ vtedy a len vtedy, keď existuje $q \in \mathbb{N}_0$ tak, že $k + q = m$.*

Dôkaz. Najprv dokážeme, že ak $k \leq m$, potom existuje $q \in \mathbb{N}_0$ tak, že $k+q = m$. Dôkaz urobíme matematickou indukciou vzhľadom na m. Ak $m = 0$ a $k \leq m$, tak $k = 0$ a pre $q = 0$ výrok platí. Nech výrok platí pre $m \in \mathbb{N}_0$ a $k \leq m + 1$. Potom $k = m + 1$ v tomto prípade zvolíme $q = 0$ alebo $k < m + 1$ a potom $k \leq m$. Podľa indukčného predpokladu existuje $p \in \mathbb{N}_0$ tak, že $k+p = m$. Potom $k + (p + 1) = (k + p) + 1 = m + 1$. Teda pre $q = p + 1 \in \mathbb{N}_0$ platí $k + q = m + 1$. Obrátene, nech existuje $q \in \mathbb{N}_0$ tak, že $k+q = m$. Pretože $0 \leq q$, platí $0+k \leq q+k$ a teda $k \leq m$. □

Číslo q v leme 7.1 je jednoznačne určené. Ak totiž pre $p \in \mathbb{N}$ platí $k+p = m$, tak $k + p = k + q$ a z toho vyplýva, že $p = q$. Ak v obore celých nezáporných čísel platí $k + q = m$, tak číslo q sa nazýva rozdielom čísel m, k a označuje sa

$q = m - k$. Z lemy 6.1 vyplýva, že v obore $(\mathbb{N}_0, +, ., <)$ je rozdiel $m - k$ definovaný len pre také dvojice m, k, pre ktoré $m \geq k$.

Z algebraického hľadiska je obor celých čísel $(\mathbb{Z}, +, ., <)$ najmenším rozšírením oboru $(\mathbb{N}_0, +, ., <)$, ktoré je usporiadaným okruhom. Je zrejmé, že $(\mathbb{N}_0, +, ., <)$ nie je usporiadaný okruh (lebo k nenulovým prvkom v $\mathbb{N}_0$ neexistujú opačné prvky). Podstata konštrukcie oboru celých čísel spočíva v tom, že každé celé číslo sa dá vyjadriť ako rozdiel dvoch celých nezáporných čísel a je teda určené usporiadanou dvojicou celých nezáporných čísel. Napríklad $-2 = 0 - 2 = 1 - 3 = 2 - 4 = ...$ je určené usporiadanými dvojicami $(0, 2), (1, 3), (2, 4), ...$. Vidíme, že toto vyjadrenie nie je jednoznačné a z toho, že $n - k = m - q$ vtedy a len vtedy, keď $n + q = m + k$ možno v rámci $(\mathbb{N}_0, +, ., <)$ charakterizovať, ktoré usporiadané dvojice celých nezáporných čísel určujú to isté celé číslo nasledovne: $(n, k), (m, q) \in \mathbb{N}_0 \times \mathbb{N}_0$ určujú to isté celé číslo vtedy a len vtedy, keď $n + q = m + k$.

Definujeme množinu $\mathbb{Z}$ všetkých celých čísel takto: Nech $\mathbb{N}_0 \times \mathbb{N}_0$ je množina všetkých usporiadaných dvojíc celých nezáporných čísel. Definujme na $\mathbb{N}_0 \times \mathbb{N}_0$ reláciu ekvivalencie $\sim$ predpisom $(n, k) \sim (m, q) \Leftrightarrow n+q = m+k$. Táto relácia je naozaj reflexívna ($(n, k) \sim (n, k) \Leftrightarrow n + k = n + k$), symetrická ($(n, k) \sim (m, q) \Leftrightarrow n + q = m + k \Leftrightarrow m + k = n + q \Leftrightarrow (m, q) \sim (n, k)$) a tranzitívna (ak $(n, k) \sim (m, q)$ a $(m, q) \sim (r, p)$, tak $n + q = m + k$, $m + p = r + q$. Potom $n + q + p = m + k + p$, $m + p + k = r + q + k$ a z toho vyplýva, že $n + q + p = r + q + k$. Z poslednej rovnosti dostávame, že $n + p = r + k$ a teda $(n, k) \sim (r, p)$). Pre každé $(n, k) \in \mathbb{N}_0 \times \mathbb{N}_0$ označme $c(n, k)$ triedu ekvivalencie $\sim$ určenú dvojicou (n, k), t. j. $c(n, k) = \{(m, q) \in \mathbb{N}_0 \times \mathbb{N}_0 : \ (m, q) \sim (n, k)\} = \{(m, q) \in \mathbb{N}_0 \times \mathbb{N}_0 : \ m + k = n + q\}$.

Množinu $\mathbb{Z}$ všetkých celých čísel definujme ako množinu všetkých tried ekvivalencie $\sim$, t. j. $\mathbb{Z} = \{c(n, k) : \ (n, k) \in \mathbb{N}_0 \times \mathbb{N}_0\}$. Teda celé čísla pri tejto konštrukcii sú triedy ekvivalencie $c(n, k)$ (sú to podmnožiny množiny množiny $\mathbb{N}_0 \times \mathbb{N}_0$), napríklad $c(3, 1) = c(2, 0)$ je celé číslo, ktoré zodpovedá číslu $2 \in \mathbb{N}$, celé číslo $c(1, 3) = c(0, 2)$ bude číslo,ktoré obvykle označujeme -2. Pripomeňme, že pre triedy ekvivalencie všeobecne a preto aj pre triedy ekvivalencie $\sim$ platí:
a) $c(n, k) = c(m, q)$ práve vtedy, keď $(n, k) \sim (m, q)$, t. j. práve vtedy,keď $n + q = m + k$
b) Ak $(n, k) \not\sim (m, q)$, tak $c(n, k) \neq c(m, q)$ a naviac $c(n, k) \cap c(m, q) = \emptyset$.
Okrem toho, pre každé $(n, k) \in \mathbb{N}_0 \times \mathbb{N}_0$ platí: Ak $n \geq k$, tak pre číslo $p = n - k \in \mathbb{N}_0$ platí $c(n, k) = c(p, 0)$. Okrem toho $c(p, 0) = c(q, 0) \Leftrightarrow p = q$. Ak $n \leq k$, tak pre číslo $q = k - n \in \mathbb{N}_0$ platí $c(n, k) = c(0, q)$. Tiež platí $c(0, q) = c(0, m) \Leftrightarrow q = m$. Predchádzajúce pozorovania môžeme zhrnúť v nasledujúcom pomocnom výsledku:

Lema 7.2. *Pre každé celé číslo $c(n, k) \in \mathbb{Z}$ platí: Ak $n \geq k$ tak existuje práve jedno $q \in \mathbb{N}_0$ ($q = n - k$), pre ktoré $c(n, k) = c(q, 0)$, ak $n < k$, tak existuje práve jedno $p \in \mathbb{N}_0$ ($p = k - n$), pre ktoré $c(n, k) = c(0, p)$.*

Teraz budeme definovať operácie sčitovania a násobenia na množine $\mathbb{Z}$. Nech $c(n,k), c(m,q) \in \mathbb{Z}$. Potom operácia sčitovania $+$ je definovaná predpisom $c(n,k)+c(m,q) = c(n+m, k+q)$ a operácia násobenia . je definovaná predpisom $c(n,k).c(m,q) = c(n.m + k.q, n.q + m.k)$ (vychádzajúc z toho, že $(n-k)+(m-q) = (n+m)-(k+q)$ a $(n-k).(m-q) = (n.m+k.q)-(n.q+m.k)$). Ak $(n,k),(m,q) \in \mathbb{N}_0 \times \mathbb{N}_0$, tak aj $(n+m, k+q), (n.m+k.q, n.q+m.k) \in \mathbb{N}_0 \times \mathbb{N}_0$ a teda $c(n+m,k+q), c(n.m+k.q, n.q+m.k) \in \mathbb{Z}$. Treba ešte overiť, že výsledky týchto operácií nezávisia na výbere usporiadaných dvojíc celých nezáporných čísel, ktorými sú dané celé čísla určené.
Nech teda $c(n,k) = c(n_1,k_1)$ a $c(m,q) = c(m_1,q_1)$ Potom $n+k_1 = n_1+k$ a $m+q_1 = m_1+q$ a potom, zrejme $(n+m)+(k_1+q_1) = (n_1+m_1)+(k+q)$. Teda $c(n,k)+c(m,q) = c(n+m,k+q) = c(n_1+m_1, k_1+q_1 = c(n_1,k_1)+c(m_1,q_1)$. Pre operáciu násobenia treba ukázať, že platí $c(n,k).c(m,q) = c(n_1,k_1).c(m_1,q_1)$. Najprv dokážeme, že $c(n,k).c(m,q) = c(n_1,k_1).c(m,q)$ a to je ekvivalentné s rovnosťou $c(n.m+k.q, n.q+m.k) = c(n_1.m+k_1.q, n_1.q+m.k_1)$. Teda stačí ukázať, že $n.m+k.q+n_1.q+m.k_1 = n_1.m+k_1.q+n.q+m.k$. Vieme, že platí $n+k_1 = n_1+k$ a preto tiež $n_1+k = n+k_1$. Ak prvú z týchto rovností vynásobíme číslo m, druhú číslom q a takto získané rovnosti sšítame, dostaneme žiadanú rovnosť $n.m+k.q+n_1.q+m.k_1 = n_1.m+k_1.q+n.q+m.k$. Podobne sa ukáže, že $c(n_1,k_1).c(m,q) = c(n_1,k_1).c(m_1,q_1)$. Teda operácie sčitovania a násobenia na množine $\mathbb{Z}$ sú definované korektne a platí:

Veta 7.1. $(\mathbb{Z}, +, .)$ *je komutatívny okruh s jednotkou.*

Dôkaz. Nech $c(n,k), c(m,q), c(p,r) \in \mathbb{Z}$. Potom $(c(n,k)+c(m,q))+c(p,r) = c(n+m,k+q)+c(p,r) = c((n+m)+p,(k+q)+r) = c(n+(m+p),k+(q+r)) = c(n,k)+c(m+p,q+r) = c(n,k)+(c(m,q)+c(p,r))$ (využili sme asociatívnosť operácie sčitovania v $(\mathbb{N}_0,+,.)$). Podobne sa dokáže komutatívnosť operácie $+$ v $\mathbb{Z}$. Je zrejmé, že prvok $c(0,0) \in \mathbb{Z}$ je nulový prvok v $(\mathbb{Z},+,.)$ a $c(k,n) \in \mathbb{Z}$ je opačný prvok k prvku $c(n,k)$, lebo $c(n,k)+c(k,n) = c(n+k,k+n) = c(0,0)$ (teda $-c(n.k) = c(k,n)$).
Ďalej, $(c(n,k).c(m,q)).c(p,r) = c(n.m+k.q, n.q+m.k).c(p,r) = c((n.m+k.q).p+(n.q+m.k).r, (n.m+k.q).r+r.(n.q+m.k))$ a
$c(n,k).(c(m,q)).c(p,r)) = c(n,k).c(m.p+q.r, m.r+p.q) = c(n.(m.p+q.r)+k.(m.r+p.q, n.(m.r+p.q)+(m.p+q.r).k)$. Pretože v $(\mathbb{N}_0,+,.)$ platí rovnosť $(n.m+k.q).p+(n.q+m.k).r+n.(m.r+p.q)+(m.p+q.r).k = n.(m.p+q.r)+k.(m.r+p.q+(n.m+k.q).r+r.(n.q+m.k)$, platí $(c(n,k).c(m,q)).c(p,r) = c(n,k).(c(m,q)).c(p,r))$.
Komutatívnosť operácie násobenia sa ukáže analogicky. Overme teraz distributívnosť násobenia vzhľadom na sčitovanie.
$c(n,k).(c(m,q)+c(p,r)) = c(n,k).c(m+p,q+r) = c(n.(m+p)+k.(q+r), n.(q+r)+(m+p).k) = c((n.m+k.q)+(n.p+k.r),(n.q+m.k)+(n.r+p.k)) = c(n.m+k.q, n.q+m.k)+c(n.p+k.r, n.r+p.k) = c(n,k).c(m,q)+c(n,k).c(p,r)$.
Nakoniec, je zrejmé, že prvok $c(1,0)$ je jednotkou okruhu $(\mathbb{Z},+,.)$. □

Teraz budeme definovať usporiadanie okruhu $(\mathbb{Z},+,.)$ pomocou normálnej podmnožiny. Nech $P = \{c(n,k) \in \mathbb{Z} : \ n > k \ v \ (\mathbb{N},<)\}$. Najprv ukážeme, že

definícia nezávisí na výbere reprezentácie celého čísla usporiadanou dvojicou $(n,k) \in \mathbb{N}_0 \times \mathbb{N}_0$, t. j., že ak $c(n,k) = c(m,q)$ a $n > k$, tak aj $m > q$. Vieme, že platí $n + q = m + k$. Potom $m + n > m + k = n + q$. Teda $m + n > q + n$ a z toho vyplýva (v $(\mathbb{N}_0, +, ., <)$), že $m > q$.

Lema 7.3. *Množina* $P = \{c(n,k) \in \mathbb{Z} : \ n > k\}$ *je normálna podmnožina okruhu* $(\mathbb{Z}, +, .)$.

Dôkaz. Nech $c(n,k), c(m,q) \in P$. Potom $n > k$, $m > q$ a preto existujú $p, r \in \mathbb{N}_0$ tak, že $n = p+k$, $m = r+q$ a $p, r > 0$. Potom $p+r > 0$, $p.r > 0$, $c(n,k)+c(m,q) = c(p,0)+c(r,0) = c(p+r,0) \in P$ a $c(n,k).c(m,q) = c(p,0).c(r,0) = c(p.r,0) \in P$. Pre každé $c(n,k) \in \mathbb{Z}$ platí práve jeden z výrokov: $n > k$, $n = k$, $k > n$. Z toho ale vyplýva, že platí práve jeden z výrokov: $c(n,k) \in P$, $c(n,k) = c(n,n) = c(0,0)$, $-c(n,k) = c(k,n) \in P$. Teda P je normálna podmnožina okruhu $(\mathbb{Z}, +, .)$. □

Ak teraz označíme $<$ usporiadanie okruhu $(\mathbb{Z}, +, .)$ dané normálnou podmnožinou P, ktoré je definované pre každé $c(n,k), c(m,q) \in \mathbb{Z}$ predpisom $c(n,k) < c(m,q)$ vtedy a len vtedy, keď $c(m,q) - c(n,k) \in P$, tak platí:

Veta 7.2. $(\mathbb{Z}, +, ., <)$ *je usporiadaný okruh, v ktorom* $c(n,k) > c(0,0) \Leftrightarrow n > k$ *v* $(\mathbb{N}_0, <)$.

Usporiadaný okruh $(\mathbb{Z}, +, ., <)$ nazveme usporiadaným okruhom celých čísel (oborom celých čísel), prvky množiny $\mathbb{Z}$ nazveme celými číslami.

Všimnime si teraz vzťah oborov $(\mathbb{N}_0, +, ., <)$ a $(\mathbb{Z}, +, ., <)$. Nech $\overline{\mathbb{N}_0} = \{c(n,0) : n \in \mathbb{N}_0\} = \{c(m,q) : \ m \geq q\}$. Potom $\overline{\mathbb{N}_0} \subseteq \mathbb{Z}$ a pre každé $c(m,q) \in \mathbb{Z} \setminus \overline{\mathbb{N}_0}$ platí $q > m$ a teda $c(m,q) = c(0,n) = -c(n,0)$, kde $n = q - m \in \mathbb{N}_0$. Teda $\mathbb{Z} = \{c(n,0) : \ n \in \mathbb{N}_0\} \cup \{-c(n,0) : \ n \in \mathbb{N}_0 \setminus \{0\}\}$. Okrem toho, pre každé $n, p \in \mathbb{N}_0$ platí: $c(n,0) + c(p,0) = c(n+p,0)$, $c(n,0).c(p,0) = c(n.p,0)$ a $c(n,0) < c(p,0)$ $\Leftrightarrow c(p,0) - c(n,0) = c(p,0) + (-c(n,0)) = c(p,0) + c(0,n) = c(p,n) \in P \Leftrightarrow$ $n < p$. Teda ak stotožníme prvky množiny $\mathbb{N}_0$ s prvkami množiny $\overline{\mathbb{N}_0}$ tak, že každý prvok $n \in \mathbb{N}_0$ stotožníme s prvkom $c(n,0) \in \overline{\mathbb{N}_0}$, tak súčty a súčiny v obore $(\mathbb{N}_0, +, ., <)$ sa stotožnia so súčtami a súčinami odpovedajúcich čísel v $\overline{\mathbb{N}_0}$ a usporiadanie na $\mathbb{N}_0$ sa ztotožní s usporiadaním na $\overline{\mathbb{N}_0}$ indukovaným na tejto množine usporiadaním množiny $\mathbb{Z}$. Po takomto stotožnení je potom usporiadaný okruh $(\mathbb{Z}, +, ., <)$ rozšírením oboru $(\mathbb{N}_0, +, ., <)$ a platí $\mathbb{Z} = \mathbb{N}_0 \cup \{-n : \ n \in \mathbb{N}_0\}$.

8 Konštrukcia oboru racionálnych čísel

Pri konštrukcii oboru racionálnych čísel, ktorý tvorí usporiadané pole, budeme vychádzať z usporiadaného okruhu $(\mathbb{Z}, +, ., <)$ celých čísel. Z matematického hľadiska ide o konštrukciu podielového poľa pre obor integrity $(\mathbb{Z}, +, .)$ dobre známu z algebry, doplnenú o rozšírenie usporiadania z okruhu $(\mathbb{Z}, +, ., <)$ na usporiadanie vytvoreného podielového poľa. Vieme, že pre racionálne číslo $\frac{2}{3}$ platí, že $\frac{2}{3} = \frac{6}{9} = \frac{-2}{-3} = ...$, t. j. toto číslo môžeme vyjadriť (reprezentovať) hociktorou z usporiadaných dvojíc celých čísel $(2,3), (6,9), (-2,-3), ...$ Vo všeobecnosti vieme, že usporiadané dvojice celých čísel $(a,b), (c,d)$, $b \neq 0$, $d \neq 0$

reprezentujú to isté racionálne číslo, ak $a.d = b.c$ (t. j. $\frac{a}{b} = \frac{c}{d}$). Na tejto úvahe je založená konštrukcia poľa racionálnych čísel (vo všeobecnosti konštrukcia podielového poľa oboru integrity).

Utvorme množinu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \ b \neq 0\}$. Na tejto množine definujme reláciu $\sim$ nasledovne: Pre ľubovoľné $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, $(a, b) \sim (c, d) \Leftrightarrow a.d = b.c$. Táto relácia je reflexívna ($(a, b) \sim (a, b)$ pretože $a.b = b.a$), symetrická (ak $(a, b) \sim (c, d)$, tak $a.d = b.c$, potom $c.b = d.a$ a teda $(c, d) \sim (a, b)$) aj tranzitívna (Nech $(a, b) \sim (c, d)$ a $(c, d) \sim (u, v)$. Potom $a.d = b.c$, $c.v = d.u$ a preto aj $a.d.v = b.c.v$, $b.c.v = b.d.u$. Potom $a.d.v = b.d.u$ a pretože $d \neq 0$ platí $a.v = b.u$. Preto $(a, b) \sim (u, v)$.). Relácia $\sim$ je teda relácia ekvivalencie na množine $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Pre každé $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ nech $\frac{a}{b} = \{(c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) : \ (a, b) \sim (c, d)\}$ je trieda ekvivalencie $\sim$ určená dvojicou (a, b). Potom $\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a, b) \sim (c, d) \Leftrightarrow a.d = b.c$. Množina $\mathbb{Q} = \{\frac{a}{b} : \ (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}$ všetkých tried ekvivalencie relácie $\sim$ (t. j. faktorová množina množiny $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ podľa relácie ekvivalencie $\sim$) sa bude nazývať množinou racionálnych čísel a jej prvky sa budú nazývať racionálne čísla.

Definujme na množine $\mathbb{Q}$ operácie $+$ (sčitovanie) a $.$ (násobenie) takto:
Pre ľubovoľné $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $\frac{a}{b} + \frac{c}{d} = \frac{a.d+b.c}{b.d}$, $\frac{a}{b} . \frac{c}{d} = \frac{a.c}{b.d}$. Pretože $(a.d+b.c, b.d), (a.c, b.d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, uvedené definície majú zmysel. Treba ale overiť, že sú nezávislé od voľby reprezentácie príslušných racionálnych čísel.

Nech $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$. Potom $a.b' = b.a'$ a $c.d' = d.c'$. Ak prvú rovnosť vynásobíme číslom $d.d'$ a druhú číslom $b.b'$, dostaneme rovnosti $a.d.b'.d' = b.d.a'.d'$ a $b.c.b'.d' = b.d.b'.c'$. Potom (sčítaním posledných rovností) dostaneme $a.d.b'.d' + b.c.b'.d' = b.d.a'.d' + b.d.b'.c'$ a po úprave $(a.d + b.c).b'.d' = b.d.(a'.d' + b'.c')$. Z poslednej rovnosti vylýva, že $\frac{a}{b} + \frac{c}{d} = \frac{a.d+b.c}{b.d} = \frac{a'.d'+b'.c'}{b'.d'} = \frac{a'}{b'} + \frac{c'}{d'}$.
Z rovností $a.b' = b.a'$, $c.d' = d.c'$ tiež vyplýva rovnosť $a.c.b'.d' = b.d.a'.c'$ a teda platí $\frac{a}{b} . \frac{c}{d} = \frac{a.c}{b.d} = \frac{a'.c'}{b'.d'} = \frac{a'}{b'} . \frac{c'}{d'}$.

Veta 8.1. *$(\mathbb{Q}, +, .)$ je pole.*

Dôkaz. Dôkaz je analogický ako bol pre podielové pole v algebre. Na ilustráciu overme asociatívnosť operácie $+$. Nech $\frac{a}{b}, \frac{c}{d}, \frac{u}{v} \in \mathbb{Q}$. Potom $(\frac{a}{b} + \frac{c}{d}) + \frac{u}{v} = \frac{a.d+b.c}{b.d} + \frac{u}{v} = \frac{(a.d+b.c).v+(b.d).u}{(b.d)v} = \frac{a.(d.v)+b.(c.v+d.u)}{b.(d.v)} = \frac{a}{b} + \frac{b.v+d.u}{d.v} = \frac{a}{b} + (\frac{c}{d} + \frac{u}{v})$.
Pripomeňme tiež, že číslo $\frac{0}{1} \in \mathbb{Q}$ je nulový prvok, číslo $\frac{1}{1} \in \mathbb{Q}$ je jednotkový prvok poľa $(\mathbb{Q}, +, .)$, opačný prvok k číslu $\frac{a}{b} \in \mathbb{Q}$ je číslo $\frac{-a}{b}$, t. j. $-\frac{a}{b} = \frac{-a}{b}$ a ak $\frac{a}{b} \neq \frac{0}{1}$, tak $a \neq 0$ a $\frac{b}{a} = (\frac{a}{b})^{-1}$ v poli $(\mathbb{Q}, +, .)$. □

Usporiadanie v poli $(\mathbb{Q}, +, .)$ budeme definovať pomocou normálnej podmnožiny poľa $(\mathbb{Q}, +, .)$. Nech $P = \{\frac{a}{b} \in \mathbb{Q} : \ a.b > 0 \ \ v \ (\mathbb{Z}, +, ., <)\}$. Overme, že definícia množiny P je korektná, t. j. že nezávisí od výberu vyjadrenia čísla $\frac{a}{b}$. Nech $\frac{a}{b} = \frac{c}{d}$ a $a.b > 0$ v $(\mathbb{Z}, +, ., <)$. Nech $c.d \leq 0$. Potom $a.b.c.d \leq 0$ a pretože $a.d = b.c$, dostávame $a.b.c.d = (a.d)^2 \leq 0$. Potom ale $a.d = 0$ a pretože $d \neq 0$ dostávame, že $a = 0$ a preto aj $a.b = 0$, čo je spor. Teda platí $c.d > 0$.

Lema 8.1. *Množina $P = \{\frac{a}{b} \in \mathbb{Q} : \ a.b > 0 \ \ v \ (\mathbb{Z}, +, ., <)\}$ je normálna pomnožina v poli $(\mathbb{Q}, +, .)$.*

Dôkaz. Nech $\frac{a}{b}, \frac{c}{d} \in P$. Potom $a.b > 0$, $c.d > 0$ a pretože $b \neq 0$, $d \neq 0$ platí $b.b > 0$ aj $d.d > 0$. Potom $a.b.d.d + c.d.b.b = (a.d + b.c).b.d > 0$ a preto $\frac{a}{b} + \frac{c}{d} = \frac{a.d+b.c}{b.d} \in P$. Zrejme tiež $a.b.c.d = a.c.b.d > 0$ a preto $\frac{a}{b} \cdot \frac{c}{d} = \frac{a.c}{b.d} \in P$.

Nech teraz $\frac{a}{b} \in \mathbb{Q}$. Potom (pre celé číslo $a.b$ v $(\mathbb{Z}, +, ., <)$) nastane práve jedna z množností:
(1) $a.b > 0$ a teda $\frac{a}{b} \in P$,
(2) $a.b = 0$ z čoho vyplýva $a = 0$ a teda $\frac{a}{b} = \frac{0}{1}$,
(3) $a.b < 0$ z čoho vyplýva $-(a.b) = (-a).b > 0$ a teda $-\frac{a}{b} = \frac{-a}{b} \in P$. □

Ak teraz označíme $<$ usporiadanie množiny $\mathbb{Q}$ určené množinou P, ktoré je dané predpisom $\frac{a}{b} < \frac{c}{d} \Leftrightarrow \frac{c}{d} - \frac{a}{b} \in P$, tak dostávame:

Veta 8.2. $(\mathbb{Q}, +, ., <)$ *je usporiadané pole.*

Usporiadané pole racionálnych čísel nazývame tiež obor racionálnych čísel.

Nech $\overline{\mathbb{Z}} = \{\frac{a}{1} : \ a \in \mathbb{Z}\}$. Pre každé $a, b \in \mathbb{Z}$ platí: $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$, $\frac{a.b}{1} = \frac{a}{1} \cdot \frac{b}{1}$ a $\frac{a}{1} < \frac{b}{1}$ v $(\mathbb{Q}, +, ., <) \Leftrightarrow \frac{b}{1} + (-\frac{a}{1}) = \frac{b}{1} + \frac{-a}{1} = \frac{b+(-a)}{1} \in P \Leftrightarrow b + (-a) > 0 \Leftrightarrow a < b$ v $(\mathbb{Z}.+, ., <)$.
Je zrejmé, že podmnožina $\overline{\mathbb{Z}}$ je podokruh poľa racionálnych čísel a spolu s usporiadaním indukovaným na $\overline{\mathbb{Z}}$ usporiadaním poľa $(\mathbb{Q}, +, ., <)$ je to usporiadaný okruh, ktorý je usporiadaným podokruhom usporiadaného poľa $(\mathbb{Q}, +, ., <)$. Ak teraz stotožníme prvky množiny $\mathbb{Z}$ s prvkami množiny $\overline{\mathbb{Z}}$ tak, že každý prvok $a \in \mathbb{Z}$ stotožníme s prvkom $\frac{a}{1} \in \overline{\mathbb{Z}}$, tak operácie sčitovania, resp. násobenia v $(\mathbb{Z}, +, ., <)$ sa stotožnia s operáciami sčitovania, resp. násobenia v podokruhu $(\overline{\mathbb{Z}}, +, .)$ a usporiadanie v $(\mathbb{Z}, +, ., <)$ sa stotožní s usporiadaním v usporiadanom podokruhu $(\overline{\mathbb{Z}}, +, ., <)$. Usporiadaný okruh $(\mathbb{Z}, +, ., <)$ môžeme takto stotožniť s usporiadaným okruhom $(\overline{\mathbb{Z}}, +, ., <)$ a považovať ho za usporiadaný podokruh usporiadaného poľa $(\mathbb{Q}, +, ., <)$, resp. usporiadané pole $(\mathbb{Q}, +, ., <)$ môžeme považovať za rozšírenie usporiadaného okruhu $(\mathbb{Z}, +, ., <)$.

Pripomeňme ešte (pozri Príklady 4.1), že $(\mathbb{Q}, +, ., <)$ je archimedovsky usporiadané pole.

9 Konštrukcia oboru reálnych čísel

Existujú viaceré konštrukcie oboru (usporiadaného poľa) reálnych čísel z oboru (usporiadaného poľa) racionálnych čísel. My použijeme Cantorovu konštrukciu, ktorá je založená na nasledujúcich vlastnostiach oboru reálnych čísel: Usporiadané pole reálnych čísel je archimedovsky usporiadané a úplné. Ku každému reálnemu číslu α existuje postupnosť racionálnych čísel $\{r_n\}_{n=1}^{\infty}$, ktorá konverguje k α (je to dôsledok archimedovského usporiadania poľa reálnych čísel). Táto postupnosť, ako postupnosť v usporiadanom poli racionálnych čísel je fundamentálna. Obrátene, ak postupnosť racionálnych čísel je fundamentálna v poli $(\mathbb{Q}, +, ., <)$, tak je fundamentálna aj v usporiadanom poli reálnych čísel (lebo toto pole je archimedovsky usporiadané) a preto konverguje k nejakému reálnemu číslu (lebo usporiadané pole reálnych čísel je úplné). Teda každé reálne číslo možno reprezentovať množinou postupností racionálych čisel, ktoré k nemu

konvergujú a preto sú fundamentálne v poli $(\mathbb{Q}, +, ., <)$. Treba si ešte uvedomiť, že postupnosti $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ racionálnych čísel konvergujú k tomu istému reálnemu číslu práve vtedy, keď $\lim_{n\to\infty}(a_n - b_n) = 0$ v usporiadanom poli $(\mathbb{Q}, +, ., <)$.

Lema 9.1. *Nech* $\mathbf{u} = \{u_n\}_{n=1}^{\infty}$, $\mathbf{v} = \{v_n\}_{n=1}^{\infty}$, $\mathbf{w} = \{w_n\}_{n=1}^{\infty}$ *sú fundamentálne postupnosti v usporiadanom poli* $(\mathbb{Q}, +, ., <)$. *Nech* $\mathbf{u} + \mathbf{v} = \{(u_n + v_n)\}_{n=1}^{\infty}$, $-\mathbf{u} = \{-u_n\}_{n=1}^{\infty}$, $\mathbf{u}.\mathbf{v} = \{(u_n.n_n)\}_{n=1}^{\infty}$ *a* $\frac{\mathbf{1}}{\mathbf{v}} = \{\frac{1}{v_n}\}_{n=1}^{\infty}$. *Potom platí:*
a) Postupnosti $\mathbf{u} + \mathbf{v}$, $-\mathbf{u}$, $\mathbf{u}.\mathbf{v}$ *sú fundamentálne postupnosti (v* $(\mathbb{Q}, +, ., <)$*).*
b) Ak $\mathbf{v}$ *nekonverguje k* 0 *v* $(\mathbb{Q}, +, ., <)$ *tak existuje* $s \in \mathbb{Q}^+$ *a* $n_0 \in \mathbb{N}$ *také, že pre všetky* $n \geq n_0$ *platí* $|v_n| \geq s$.
c) Ak $\mathbf{v}$ *konverguje k* 0 *v* $(\mathbb{Q}, +, ., <)$, *tak aj* $\mathbf{u}.\mathbf{v}$ *konverguje k* 0 *v* $(\mathbb{Q}, +, ., <)$.
d) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$, $\mathbf{u}.\mathbf{v} = \mathbf{v}.\mathbf{u}$, $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$, $(\mathbf{u}.\mathbf{v}).\mathbf{w} = \mathbf{u}.(\mathbf{v}.\mathbf{w})$, $\mathbf{u}.(\mathbf{v} + \mathbf{w}) = \mathbf{u}.\mathbf{v} + \mathbf{u}.\mathbf{w}$, $\mathbf{u} + \overline{0} = \mathbf{u}$, $\mathbf{u} + (-\mathbf{u}) = \overline{0}$ *a* $\mathbf{u}.\overline{1} = \mathbf{u}$, *pričom* $\overline{0} = \{0\}_{n=1}^{\infty}$ *je nulová postupnosť v poli racionálnych čísel a* $\overline{1} = \{1\}_{n=1}^{\infty}$ *je postupnosť, ktorej všetky členy majú hodnotu* 1.

Dôkaz. a) Ukážeme pre $\mathbf{u}.\mathbf{v}$. Pretože $\mathbf{u}$, $\mathbf{v}$ sú fundamentálne, sú aj ohraničené, t. j. existujú $r, s \in \mathbb{Q}^+$ také, že pre každé $n \in \mathbb{N}$ platí $|u_n| \leq r$, $|v_n| \leq s$. Nech $\varepsilon \in \mathbb{Q}^+$. Potom aj $\frac{\varepsilon}{2s} > 0$ a existuje $n_1 \in \mathbb{N}$ tak, že pre všetky $n, k \geq n_1$ platí $|u_n - u_k| < \frac{\varepsilon}{2s}$. Rovnako aj $\frac{\varepsilon}{2r} > 0$ a preto existuje $n_2 \in \mathbb{N}$ tak, že pre všetky $n, k \geq n_2$ platí $|v_n - v_k| \leq \frac{\varepsilon}{2r}$. Potom pre všetky $n, k \geq n_0 = max\{n_1, n_2\}$ dostávame: $|u_n.v_n - u_k.v_k| = |u_n.v_n - u_n.v_k + u_n.v_k - u_k.v_k| \leq |u_n|.|v_n - v_k| + |v_k|.|u_n - u_k| < r.\frac{\varepsilon}{2r} + s.\frac{\varepsilon}{2s} = \varepsilon$.
b) Pretože $\mathbf{v}$ nekonverguje k 0, existuje $r \in \mathbb{Q}^+$ tak, že pre každé $n \in \mathbb{N}$ existuje $k > n$, pre ktoré $|v_k| \geq r$. Pretože $\mathbf{v}$ je fundamentálna a $\frac{r}{2} > 0$, existuje $n_0 \in \mathbb{N}$ také, že pre všetky $n, k \geq n_0$ platí $|v_n - v_k| < \frac{r}{2}$. Vyberme $k > n_0$ tak, že $|v_k| \geq r$. Potom pre každé $n \geq n_0$ platí $|v_n| = |v_k - (v_k - v_n)| \geq |v_k| - |v_k - v_n| \geq r - \frac{r}{2} = \frac{r}{2}$ $(-|v_k - v_n| > -\frac{r}{2})$. Teda pre každé $n \geq n_0$ platí $|v_n| \geq \frac{r}{2}$ $(\frac{r}{2} \in \mathbb{Q}^+)$.
c) Prenechávame čitateľovi ako cvičenie.
d) Overíme distributívnosť. Zrejme $\mathbf{u}.(\mathbf{v}+\mathbf{w}) = \{u_n.(v_n+w_n)\}_{n=1}^{\infty}$ a $\mathbf{u}.\mathbf{v}+\mathbf{u}.\mathbf{w} = \{u_n.v_n+u_n.w_n\}_{n=1}^{\infty}$. Pretože pre každé $n \in \mathbb{N}$ platí $u_n.(v_n+w_n) = u_n.v_n+u_n.w_n$ (ide o prvky poľa racionálnych čísel) dostávame rovnosť $\mathbf{u}.(\mathbf{v}+\mathbf{w}) = \mathbf{u}.\mathbf{v}+\mathbf{u}.\mathbf{w}$. Ostatné rovnosti sa overia podobne.

□

Nech teraz $\mathcal{F}(\mathbb{Q})$ je je množina všetkých fundamentálnych postupností racionálnych čísel. Podľa predchádzajúcej lemy, ak $\mathbf{u}, \mathbf{v} \in \mathcal{F}(\mathbb{Q})$, tak aj $\mathbf{u} + \mathbf{v}, -\mathbf{u}, \mathbf{u}.\mathbf{v} \in \mathcal{F}(\mathbb{Q})$. Pre každé $r \in \mathbb{Q}$, $\overline{r}$ bude označovať konštantnú postupnosť $\{r\}_{n=1}^{\infty}$. Zrejme, $\overline{r} \in \mathcal{F}(\mathbb{Q})$.

Definujme na $\mathcal{F}(\mathbb{Q})$ reláciu $\sim$ nasledovne:Ak $\mathbf{u} = \{u_n\}_{n=1}^{\infty}$, $\mathbf{v} = \{v_n\}_{n=1}^{\infty} \in \mathcal{F}(\mathbb{Q})$, tak $\mathbf{u} \sim \mathbf{v}$ práve vtedy, keď $\lim_{n\to\infty}(u_n - v_n) = 0$ (v usporiadanom poli racionálnych čísel). Je zrejmé, že pre každé $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{F}(\mathbb{Q})$ platí: (1) $\mathbf{u} \sim \mathbf{u}$ (lebo $\lim_{n\to\infty}(u_n - u_n) = 0$), (2) ak $\mathbf{u} \sim \mathbf{v}$, tak $\mathbf{v} \sim \mathbf{u}$ (lebo ak $\lim_{n\to\infty}(u_n - v_n) = 0$, tak aj $\lim_{n\to\infty}(v_n - u_n) = 0$, (3) ak $\mathbf{u} \sim \mathbf{v}$ a $\mathbf{v} \sim \mathbf{w}$, tak $\mathbf{u} \sim \mathbf{w}$ (lebo ak $\lim_{n\to\infty}(u_n - v_n) = 0$ a $\lim_{n\to\infty}(v_n - w_n) = 0$, tak aj $\lim_{n\to\infty}(u_n - w_n) =$

$\lim_{n\to\infty}((u_n - v_n) + (v_n - w_n)) = \lim_{n\to\infty}(u_n - v_n) + \lim_{n\to\infty}(v_n - w_n) = 0 + 0 = 0$. Teda $\sim$ je relácia ekvivalencie na $\mathcal{F}(\mathbb{Q})$.

Pre každé $\mathbf{u} \in \mathcal{F}(\mathbb{Q})$ označme $\alpha(\mathbf{u})$ triedu ekvivalencie obsahujúcu prvok $\mathbf{u}$, t. j. $\alpha(u) = \{\mathbf{v} \in \mathcal{F}(\mathbb{Q}) : \ \mathbf{u} \sim \mathbf{v}\}$. Potom pre každé $\mathbf{u}, \mathbf{v} \in \mathcal{F}(\mathbb{Q})$ platí $\alpha(\mathbf{u}) = \alpha(\mathbf{v}) \Leftrightarrow \mathbf{u} \sim \mathbf{v}$. Označme $\mathbb{R}$ roklad množiny $\mathcal{F}(\mathbb{Q})$ prislúchajúci relácii ekvivalencie $\sim$, t. j. $\mathbb{R} = \{\alpha(\mathbf{u}) : \ \mathbf{u} \in \mathcal{F}(\mathbb{Q})\}$.

Množinu $\mathbb{R}$ budeme nazývať množina reálnych čísel, jej prvky nazveme reálne čísla (reálne čísla sú teda (v tomto modeli) triedy ekvivelencie $\sim$ fundamentálnych postupností). Je zrejmé, že $\mathbf{u} \in \alpha(\overline{0})$ práve vtedy,keď $\mathbf{u}$ konverguje k 0 v $(\mathbb{Q}, +, ., <)$.

Na množine $\mathbb{R}$ definujme binárne operácie $+, .$ nasledovne: Ak $\alpha(\mathbf{u}),\ \alpha(\mathbf{v}) \in \mathbb{R}$, tak $\alpha(\mathbf{u}) + \alpha(\mathbf{v}) = \alpha(\mathbf{u} + \mathbf{v})$ a $\alpha(\mathbf{u}).\alpha(\mathbf{v}) = \alpha(\mathbf{u}.\mathbf{v})$. Z predchádzajúcej lemy vyplýva, že táto definícia má zmysel, treba ešte overiť, že nezávisí od vyjadrenia daných reálnych čísel.
Nech $\alpha(\mathbf{u}) = \alpha(\mathbf{t})$, $\alpha(\mathbf{v}) = \alpha(\mathbf{w})$. Potom $\mathbf{u} \sim \mathbf{t}$, $\mathbf{v} \sim \mathbf{w}$ a teda $\lim_{n\to\infty}(u_n - t_n) = 0$, $\lim_{n\to\infty}(v_n - w_n) = 0$. Potom $\lim_{n\to\infty}((u_n + v_n) - (t_n + w_n)) = \lim_{n\to\infty}((u_n - t_n) + (v_n - w_n)) = 0 + 0 = 0$ a z toho vyplýva, že $\mathbf{u} + \mathbf{v} \sim \mathbf{t} + \mathbf{w}$ a preto $\alpha(\mathbf{u}) + \alpha(\mathbf{v}) = \alpha(\mathbf{u} + \mathbf{v}) = \alpha(\mathbf{t} + \mathbf{w}) = \alpha(\mathbf{t}) + \alpha(\mathbf{w})$. Platí tiež $\lim_{n\to\infty}(u_n.v_n - t_n.w_n) = \lim_{n\to\infty}(u_n.v_n - u_n.w_n + u_n.w_n - t_n.w_n) = \lim_{n\to\infty} u_n.(v_n - w_n) + \lim_{n\to\infty} w_n.(u_n - t_n) = 0 + 0 = 0$ (použili sme c) z predchádzajúcej lemy). Z toho dostávame, že $\mathbf{u}.\mathbf{v} \sim \mathbf{t}.\mathbf{w}$ a preto $\alpha(\mathbf{u}).\alpha(\mathbf{v}) = \alpha(\mathbf{u}.\mathbf{v}) = \alpha(\mathbf{t}.\mathbf{w}) = \alpha(\mathbf{t}).\alpha(\mathbf{w})$. Teda binárne operácie $+$ a $.$ na $\mathbb{R}$ sú dobre definované.

Veta 9.1. $(\mathbb{R}, +, .)$ *je pole.*

Dôkaz. V dôkaze použijeme Lemu 9.1.a), b), d). Nech $\alpha(\mathbf{u}), \alpha(\mathbf{v}), \alpha(\mathbf{w}) \in \mathbb{R}$. Potom $\alpha(\mathbf{u}).(\alpha(\mathbf{v}) + \alpha(\mathbf{w})) = \alpha(\mathbf{u}).\alpha(\mathbf{v} + \mathbf{w}) = \alpha(\mathbf{u}.(\mathbf{v} + \mathbf{w})) = \alpha(\mathbf{u}.\mathbf{v} + \mathbf{u}.\mathbf{w}) = \alpha(\mathbf{u}.\mathbf{v}) + \alpha(\mathbf{u}.\mathbf{w}) = \alpha(\mathbf{u}).\alpha(\mathbf{v}) + \alpha(\mathbf{u}).\alpha(\mathbf{w})$. Komutatívnosť a asociatívnosť pre operácie $+$ aj $.$ na $\mathbb{R}$ sa dokážu podobne. Je zrejmé, že $\alpha(\overline{0})$ je neutrálny prvok vzhľadom na $+$, t.j. nulový prvok v $(\mathbb{R}, +, .)$, opačný prvok k číslu $\alpha(\mathbf{u})$ je číslo $\alpha(-\mathbf{u})$ a $\alpha(\overline{1})$ je jednotkový prvok v $(\mathbb{R}, +, .)$. Nech teraz $\alpha(\mathbf{u}) \in \mathbb{R}$, $\alpha(\mathbf{u}) \neq \alpha(\overline{0})$. Potom $\mathbf{u}$ nekonverguje k 0 v usporiadanom poli racionálnych čísel a existuje $r \in \mathbb{Q}^+$ a $n_1 \in \mathbb{N}$ tak, že pre všetky $n \geq n_1$ platí $|u_n| \geq r$ (a teda tiež $u_n \neq 0$). Definujme postupnosť $\mathbf{v} = \{v_n\}_{n=1}^{\infty}$ takto: Pre všetky $k < n_1$ $v_k = r$ a pre všetky $k \geq n_1$ $v_k = u_k$. Zrejme $\mathbf{v}$ je fundamentálna postupnosť v $(\mathbb{Q}, +, ., <)$, $\lim_{n\to\infty}(u_n - v_n) = 0$ a preto $\alpha(\mathbf{v}) = \alpha(\mathbf{u})$. Pre všetky $n \in \mathbb{N}$ $|v_n| \geq r$ a preto aj $\frac{1}{|v_n|} \leq \frac{1}{r}$. Uvažujme o postupnosti $\frac{1}{\mathbf{v}} = \{\frac{1}{v_n}\}_{n=1}^{\infty}$. Je to postupnosť racionálnych čísel a ukážeme, že je fundamentálna. Nech $\varepsilon \in \mathbb{Q}^+$. Potom aj $r^2.\varepsilon \in \mathbb{Q}^+$ a pretože $\mathbf{v}$ je fundamentálna existuje $n_0 \in \mathbb{N}$ tak, že pre všetky $n, k \geq n_0$ platí $|v_n - v_k| < r^2.\varepsilon$. Potom pre všetky $n, k \geq n_0$ platí $|\frac{1}{v_n} - \frac{1}{v_k}| = \frac{1}{|v_n|.|v_k|}.|v_k - v_n| \leq \frac{1}{r^2}.|v_k - v_n| < \frac{1}{r^2}.r^2.\varepsilon = \varepsilon$. Pre reálne číslo $\alpha(\frac{1}{\mathbf{v}})$ platí $\alpha(\mathbf{u}).\alpha(\frac{1}{\mathbf{v}}) = \alpha(\mathbf{v}).\alpha(\frac{1}{\mathbf{v}}) = \alpha(\mathbf{v}.\frac{1}{\mathbf{v}}) = \alpha(\overline{1})$. Teda $\alpha(\frac{1}{\mathbf{v}})$ je inverzný prvok k $\alpha(\mathbf{u})$ v $(\mathbb{R}, +, .)$. □

Teraz budeme definovať usporiadanie poľa $(\mathbb{R}, +, .)$ pomocou normálnej podmnožiny P. Nech $P = \{\alpha(\mathbf{u}) \in \mathbb{R} : \ \exists_{r\in\mathbb{Q}^+}\ \exists_{n_0\in\mathbb{N}}\ \forall_{n\geq n_0}\ u_n \geq r\}$. Najprv

overíme, či táto definícia je nezávislá od vyjadrenia čísla $\alpha(\mathbf{u})$, t. j. či platí: Ak $\alpha(\mathbf{u}) = \alpha(\mathbf{v})$ a $\alpha(\mathbf{u}) \in P$, tak aj $\alpha(\mathbf{v}) \in P$. Nech teda $\alpha(\mathbf{u}) = \alpha(\mathbf{v})$. Potom $\mathbf{u} \sim \mathbf{v}$ a teda $\lim_{n\to\infty}(u_n - v_n) = 0$. Pretože $\alpha(\mathbf{u}) \in P$ platí $\exists_{r\in\mathbb{Q}^+}\ \exists_{n_0\in\mathbb{N}}\ \forall_{n\geq n_0}\ u_n \geq r$. Zrejme $\frac{r}{2} > 0$ a keďže $\lim_{n\to\infty}(u_n - v_n) = 0$, existuje $n_1 \in \mathbb{N}$ tak, že pre všetky $n \geq n_1$ platí $|u_n - v_n| < \frac{r}{2}$. Nech $n_2 = max\{n_0, n_1\}$. Potom pre všetky $n \geq n_2$ platí $v_n = u_n - (u_n - v_n) \geq u_n - |u_n - v_n| \geq r - \frac{r}{2} = \frac{r}{2}$. Teda existuje $\frac{r}{2} > 0$ a $n_2 \in \mathbb{N}$ tak, že pre každé $n \geq n_2$ $v_n \geq \frac{r}{2}$. Z toho dostávame, že $\alpha(\mathbf{v}) \in P$.

Lema 9.2. *Množina P je normálna podmnožina v poli $(\mathbb{R}, +, .)$.*

Dôkaz. Nech $\alpha(\mathbf{u}), \alpha(\mathbf{v}) \in P$. Potom existujú $r, s \in \mathbb{Q}^+$ a $n_1, n_2 \in \mathbb{N}$ tak, že pre všetky $n \geq n_1$ platí $u_n \geq r$ a pre všetky $n \geq n_2$ platí $v_n \geq s$. Pre všetky $n \geq n_0 = max\{n_1, n_2\}$ dostávame $u_n + v_n \geq r + s > 0$ a $u_n.v_n > r.s > 0$. To ale znamená, že $\alpha(\mathbf{u} + \mathbf{v}) = \alpha(\mathbf{u}) + \alpha(\mathbf{v}) \in P$ a tiež $\alpha(\mathbf{u}.\mathbf{v}) = \alpha(\mathbf{u}).\alpha(\mathbf{v}) \in P$. Ďalej, nech $\alpha(\mathbf{u}) \in \mathbb{R}$, $\alpha(\mathbf{u}) \neq \alpha(\overline{0})$. Chceme ukázať, že potom nastane práve jedna z možností: $\alpha(\mathbf{u}) \in P$ alebo $-\alpha(\mathbf{u}) = \alpha(-\mathbf{u}) \in P$. Pretože $\alpha(\mathbf{u}) \neq \alpha(\overline{0})$, postupnosť $\mathbf{u}$ nekonverguje k 0 v usporiadanom poli racionálnych čísel a teda (podľa Lemy 9.1.b)) existuje $r \in \mathbb{Q}^+$ a $n_0 \in \mathbb{N}$ tak, že pr všetky $n \geq n_0$ platí $|u_n| \geq r$. Pretože $\mathbf{u}$ je fundamenálna a $\frac{r}{2} > 0$, existuje $n_1 \in \mathbb{N}$ tak, že pre všetky $n, k \geq n_1$ platí $|u_n - u_k| < \frac{r}{2}$. Nech $n_2 = max\{n_0, n_1\}$. Pretože $n_2 \geq n_0$, $|u_{n_2}| \geq r$. Môže nastať práve jeden z prípadov:
a) $u_{n_2} \geq r$. Potom pre všetky $n \geq n_2$ platí $|u_n - u_{n_2}| < \frac{r}{2}$ a teda $u_n = u_{n_2} - (u_{n_2} - u_n) \geq u_{n_2} - |u_{n_2} - u_n| \geq r - \frac{r}{2} = \frac{r}{2} > 0$. Potom, ale, $\alpha(\mathbf{u}) \in P$.
b) $u_{n_2} \leq -r$. Potom pre všetky $n \geq n_2$ platí $u_n = u_{n_2} + (u_n - u_{n_2}) \leq u_{n_2} + |u_n - u_{n_2}| \leq -r + \frac{r}{2} = -\frac{r}{2}$, teda $-u_n \geq \frac{r}{2} > 0$ a preto $\alpha(-\mathbf{u}) = -\alpha(\mathbf{u}) \in P$.
Dokázali sme, že nastáva práve jedna z možností: $\alpha(\mathbf{u}) = \alpha(\overline{0})$, $\alpha(\mathbf{u}) \in P$, $-\alpha(\mathbf{u}) \in P$. □

Nech teraz $< = <_P$ je usporiadanie poľa $(\mathbb{R}, +, .)$ dané normálnou podmnožinou P, t. j. pre každé $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$ práve vtedy, keď $\beta - \alpha \in P$. Potom platí:

Veta 9.2. *$(\mathbb{R}, +, ., <)$ je usporiadané pole.*

Pripomeňme ešte, že v usporiadanom poli $(\mathbb{R}, +, ., <)$ je vyššie definovaná množina P množinou všetkých kladných prvkov v $(\mathbb{R}, +, ., <)$, t. j. $P = \{\alpha \in \mathbb{R} :\ \alpha > \alpha(\overline{0})\} = \mathbb{R}^+$.

Teraz ešte ukážeme, že pole $(\mathbb{R}, +, ., <)$ je archimedovsky usporiadané a úplné a preto aj spojito usporiadané.

Predtým ešte overme, že pre každé $z \in \mathbb{Z}$ platí $z\alpha(\overline{1}) = \alpha(\overline{z})$. Najprv to dokážeme pre všetky $n \in \mathbb{N}_0$. Pre $n = 0$ platí $0\alpha(\overline{1}) = \alpha(\overline{0})$ (podľa definície z-násobku). Nech teraz $n \in \mathbb{N}_0$ a platí $n\alpha(\overline{1}) = \alpha(\overline{n})$. Potom $(n+1)\alpha(\overline{1}) = n\alpha(\overline{1}) + \alpha(\overline{1}) = \alpha(\overline{n}) + \alpha(\overline{1}) = \alpha(\overline{n} + \overline{1}) = \alpha(\overline{n+1})$. Nakoniec, pre každé $n \in \mathbb{N}$ platí $(-n)\alpha(\overline{1}) = -(n\alpha(\overline{1})) = -\alpha(\overline{n}) = \alpha(-(\overline{n})) = \alpha(\overline{-n})$. Teda pre každé $z \in \mathbb{Z}$ platí $z\alpha(\overline{1}) = \alpha(\overline{z})$.

Veta 9.3. *Usporiadané pole $(\mathbb{R}, +, ., <)$ je archimedovsky usporiadané.*

Dôkaz. Stačí ukázať, že pre každé $\alpha(\mathbf{u}) > \alpha(\overline{0})$ (t. j. $\alpha(\mathbf{u}) \in P$) existuje $m \in \mathbb{N}$ tak, že pre m-násobok jednotkového prvku platí $m\alpha(\overline{1}) > \alpha(\mathbf{u})$.
Nech teda $\alpha(\mathbf{u}) > \alpha(\overline{0})$. Postupnosť $\mathbf{u}$ je fundamentálna a preto ohraničená v $(\mathbb{Q}, +, ., <)$ a teda existuje $r \in \mathbb{Q}^+$ tak, že pre všetky $n \in \mathbb{N}$ platí $|u_n| \leq r$. V usporiadanom poli $(\mathbb{Q}, +, ., <)$ existuje $k \in \mathbb{N}$ tak, že $r < k$ (lebo $(\mathbb{Q}, +, ., <)$ je archimedovsky usporiadané). Potom pre každé $n \in \mathbb{N}$ platí $k - u_n > r - u_n \geq 0$. Zvoľme $m = k + 1$. Potom pre každé $n \in \mathbb{N}$ platí $m - u_n = m + (-u_n) \geq 1 > 0$ a preto $\alpha(\overline{m} + (-\mathbf{u})) = \alpha(\overline{m}) + (-\alpha(\mathbf{u})) \in P = \mathbb{R}^+$, t. j. $\alpha(\mathbf{u}) < \alpha(\overline{m}) = m\alpha(\overline{1})$. □

Teraz si všimnime ako vyzerá množina $\mathbb{Q}_\mathbb{R}$ racionálnych prvkov poľa $(\mathbb{R}, +, .)$. Podľa definície racionálneho prvku $\mathbb{Q}_\mathbb{R} = \{\frac{z\alpha(\overline{1})}{n\alpha(\overline{1})} : \ z \in \mathbb{Z}, \ n \in \mathbb{N}\}$. Ukázali sme, že pre každé $n \in \mathbb{N}$ a každé $z \in \mathbb{Z}$ platí $n\alpha(\overline{1}) = \alpha(\overline{n})$, $z\alpha(\overline{1}) = \alpha(\overline{z})$ a zrejme tiež platí $\frac{1}{\alpha(\overline{n})} = \alpha(\overline{(\frac{1}{n})})$ $(\alpha(\overline{n}).\alpha(\overline{(\frac{1}{n})}) = \alpha(\overline{n}.\overline{(\frac{1}{n})}) = \alpha(\overline{1}))$. Preto $\frac{z\alpha(\overline{1})}{n\alpha(\overline{1})} = \alpha(\overline{z}).\alpha(\overline{(\frac{1}{n})}) = \alpha(\overline{(\frac{z}{n})}) = \alpha(\overline{r})$, kde $r = \frac{z}{n} \in \mathbb{Q}$. Platí teda, že $\mathbb{Q}_\mathbb{R} = \{\alpha(\overline{r}) : \ r \in \mathbb{Q}\}$. Z vety 4.3 vyplýva, že $\mathbb{Q}_\mathbb{R}$ je hustá v $(\mathbb{R}, +, ., <)$, t.j. ak $\alpha, \beta \in \mathbb{R}$ a $\alpha < \beta$, tak existuje $r \in \mathbb{Q}$ tak, že $\alpha < \alpha(\overline{r}) < \beta$.

Lema 9.3. *Nech $\alpha(\mathbf{u}) \in \mathbb{R}$, $\mathbf{u} = \{u_n\}_{n=1}^\infty$ a pre každé $n \in \mathbb{N}$ $\overline{u_n}$ je konštantná postupnosť racionálnych čísel, ktorej všetky členy majú hodnotu u_n (t. j. $\overline{u_n}$ je postupnosť $(u_n, u_n, u_n, ..., u_n, ...)$). Potom $\lim_{n\to\infty} \alpha(\overline{u_n}) = \alpha(\mathbf{u})$.*

Dôkaz. Nech $\varepsilon \in \mathbb{R}$, $\varepsilon > \alpha(\overline{0})$. Potom existuje $r \in \mathbb{Q}$ tak, že $\alpha(\overline{0}) < \alpha(\overline{r}) < \varepsilon$. Zrejme $\alpha(\overline{r}) \in \mathbb{R}^+ = P$ a preto $r > 0$ v $(\mathbb{Q}, +, ., <)$. Pretože $\frac{r}{2} > 0$ a $\mathbf{u}$ je fundamentálna v $(\mathbb{Q}, +, ., <)$ existuje $n_0 \in \mathbb{N}$ tak, že pre všetky $k, l \geq n_0$ platí $|u_k - u_l| < \frac{r}{2}$. Nech teraz n je pevne zvolené prirodzené číslo, $n \geq n_0$. Potom pre každé $k \geq n_0$ platí $-\frac{r}{2} < u_k - u_n < \frac{r}{2}$.
Ak k obidvom stanám nerovnosti $-\frac{r}{2} < u_k - u_n$ pripočítame r, dostaneme nerovnosť $\frac{r}{2} < u_k - u_n + r$, ktorá platí pre každé $k \geq n_0$. Nech pre každé $k \in \mathbb{N}$ $v_k = u_k - u_n + r$, a $\mathbf{v} = \{v_k\}_{k=1}^\infty$. Pretože pre každé $p, q \in \mathbb{N}$ platí $v_p - v_q = u_p - u_q$, postupnosť $\mathbf{v}$ je fundamentálna a z definície $\mathbf{v}$ je zrejmé, že $\mathbf{v} = \mathbf{u} - \overline{u_n} + \overline{r}$. Pretože pre $k \geq n_0$ platí $v_k \geq \frac{r}{2} > 0$, $\alpha(\mathbf{v}) \in P = \mathbb{R}^+$ a teda platí $\alpha(\overline{0}) < \alpha(\mathbf{v}) = \alpha(\mathbf{u}) - \alpha(\overline{u_n}) + \alpha(\overline{r})$ a z toho dostávame
$-\alpha(\overline{r}) < \alpha(\mathbf{u}) - \alpha(\overline{u_n})$.
Ak teraz k obom stranám nerovnosti $u_k - u_n < \frac{r}{2}$ pripočítame $-r$, tak dostaneme nerovnosť $u_k - u_n - r < -\frac{r}{2}$, ktorá platí pre každé $k \geq n_0$. Nech pre každé $k \in \mathbb{N}$ $w_k = u_k - u_n - r$ a $\mathbf{w} = \{w_k\}_{k=1}^\infty$. Potom $\mathbf{w}$ je fundamentálna postupnosť v $(\mathbb{Q}, +, ., <)$ $(w_p - w_q = u_p - u_q)$, $\mathbf{w} = \mathbf{u} - \overline{u_n} - \overline{r}$, pre každé $k \geq n_0$ platí $-w_k > \frac{r}{2} > 0$ a preto $\alpha(-\mathbf{w}) = -\alpha(\mathbf{w}) > \alpha(\overline{0})$. Teda, $\alpha(\overline{0}) > \alpha(\mathbf{w}) = \alpha(\mathbf{u}) - \alpha(\overline{u_n}) - \alpha(\overline{r})$. Z toho potom dostávame, že platí
$\alpha(\mathbf{u}) - \alpha(\overline{u_n}) < \alpha(\overline{r})$.
Teda pre všetky $n \geq n_0$ platí $-\alpha(\overline{r}) < \alpha(\mathbf{u}) - \alpha(\overline{u_n}) < \alpha(\overline{r})$ a preto $|\alpha(\mathbf{u}) - \alpha(\overline{u_n})| < \alpha(\overline{r}) < \varepsilon$. Z toho vyplýva, že $\lim_{n\to\infty} \alpha(\overline{u_n}) = \alpha(\mathbf{u})$.
□

Všimnime si, že pre každé $r, s \in \mathbb{Q}$ platí $\alpha(\overline{r}) + \alpha(\overline{s}) = \alpha(\overline{r} + \overline{s}) = \alpha(\overline{r + s})$,

$\alpha(\overline{r}).\alpha(\overline{s}) = \alpha(\overline{r}.\overline{s}) = \alpha(\overline{r.s})$ a $r < s$ v $(\mathbb{Q}, +, ., <) \Leftrightarrow s+(-r) > 0 \Leftrightarrow \alpha(\overline{r + (-s)}) > \alpha(\overline{0}) \Leftrightarrow \alpha(\overline{s}) + \alpha(\overline{-r}) > \alpha(\overline{0}) \Leftrightarrow \alpha(\overline{s}) + (-\alpha(\overline{r}) > \alpha(\overline{0}) \Leftrightarrow \alpha(\overline{r}) < \alpha(\overline{s})$ v $(\mathbb{R}, +, ., <)$. (Inými slovami povedané, zobrazenie $f : (\mathbb{Q}, +, ., <) \longrightarrow (\mathbb{R}, +, ., <)$ definované predpisom $f(r) = \alpha(\overline{r})$ je homomorfizmus usporiadaných okruhov a preto usporiadaný podokruh $(f(\mathbb{Q}), +, ., <)$ usporiadaného okruhu $(\mathbb{R}, +, ., <)$ je izomorfný s usporiadaným okruhom $(\mathbb{Q}, +, ., <)$). Je zrejmé, že ak každé racionálne číslo r stotožníme s reálnym číslom $\alpha(\overline{r})$ tak usporiadané pole $(\mathbb{Q}, +, ., <)$ sa stotožní s usporiadaným podpoľom racionálnych prvkov poľa $(\mathbb{R}, +, ., <)$ a teda usporiadané pole $(\mathbb{Q}, +, ., <)$ môžeme považovať za usporiadané podpole poľa $(\mathbb{R}, +, ., <)$. V dôkaze nasledujúcej vety už využijeme túto skutočnosť.

Veta 9.4. *Pole $(\mathbb{R}, +, ., <)$ je úplné.*

Dôkaz. Pripomeňme, že racionálne prvky $\alpha(\overline{r})$, $r \in \mathbb{Q}$ poľa $(\mathbb{R}, +, ., <)$ označujeme len r, t. j. stotožňujeme r s $\alpha(\overline{r})$, (napríklad $\alpha(\overline{0}) = 0$).
Nech $\{\alpha_n\}_{n=1}^{\infty}$ je fundamentálne postupnosť v $(\mathbb{R}, +, ., <)$. Ukážeme, že je konvergentná. Pre každé $n \in \mathbb{N}$ je $\frac{1}{n} > 0$ v $(\mathbb{R}, +, ., <)$ a preto $\alpha_n + \frac{1}{n} > \alpha_n$. Potom existuje $r_n \in \mathbb{Q}$ tak, že $\alpha_n < r_n < \alpha_n + \frac{1}{n}$ (lebo $(\mathbb{R}, +, ., <)$ je archimedovsky usporiadané). Ukážeme, že $\mathbf{r} = \{r_n\}_{n=1}^{\infty}$ je fundamentálna postupnosť v $(\mathbb{Q}, +, ., <)$. Nech $a \in \mathbb{Q}^+$. Potom $a \in \mathbb{R}$ a $a > 0$ v $(\mathbb{R}, +, ., <)$ ($a = \alpha(\overline{a})$ a postupnosť $\overline{a}$ je zdola ohraničená číslom $a \in \mathbb{Q}^+$). Potom aj $\frac{a}{3} > 0$ v $(\mathbb{R}, +, ., <)$ a teda existuje $n_0 \in \mathbb{N}$ tak, že pre všetky $n, k \geq n_0$ platí $|\alpha_n - \alpha_k| < \frac{a}{3}$. Ďalej, existuje $n_1 \in \mathbb{N}$ tak, že pre všetky $n \geq n_1$ platí $\frac{1}{n} < \frac{a}{3}$. Pre všetky $n, k \geq n_2 = max\{n_0, n_1\}$ máme $|r_n - r_k| = |r_n - \alpha_n + \alpha_n - \alpha_k + \alpha_k - r_k| \leq |r_n - \alpha_n| + |\alpha_n - \alpha_k| + |\alpha_k - r_k| < \frac{1}{n} + \frac{a}{3} + \frac{1}{k} < a$. Podľa predchádzajúcej lemy potom $\lim_{n\to\infty} r_n = \alpha(\mathbf{r})$ v $(\mathbb{R}, +, ., <)$ (pripomeňme dohovor, že $r_n = \alpha(\overline{r_n})$). Pretože pre všetky $n \in \mathbb{N}$ platí $|r_n - \alpha_n| < \frac{1}{n}$, dostávame, že $\lim_{n\to\infty}(\alpha_n - r_n) = 0$. Potom $\lim_{n\to\infty} \alpha_n = \lim_{n\to\infty}(r_n + (\alpha_n - r_n)) = \lim_{n\to\infty} r_n + \lim_{n\to\infty}(\alpha_n - r_n) = \alpha(\mathbf{r}) + 0 = \alpha(\mathbf{r})$. Teda $(\mathbb{R}, +, ., <)$ je úplné. □

Dôsledom viet 9.3 a 9.4 je:

Veta 9.5. *Pole $(\mathbb{R}, +, ., <)$ je spojito usporiadané.*

10 Konštrukcia oboru komplexných čísel

Obor komplexných čísel, ktorý spolu s operáciami sčitovania a násobenia komplexných čísel je pole, je rozšírením oboru (poľa) reálnych čísel. Je známe, že pole kompexných čísel je algebraicky uzavreté, t. j. každá algebraická rovnica (polynom) stupňa $n \geq 1$, ktorej (ktorého) koeficienty sú komplexné čísla (a teda to platí aj v prípade reálnych koeficientov) má v poli komplexných čísel riešenie (koreň). Pole reálnych čísel takúto vlastnosť nemá, napríklad kvadratická rovnica (s reálnymi koeficientami) $x^2 = -1$ nemá v poli reálnych čísel riešenie.

Komplexné číslo $a + b.i$ vyjadrené v algebraickom tvare ($a, b \in \mathbb{R}$, i je imaginárna jednotla, pre ktorú platí $i.i = -1$) je jednoznačne určené usporiadanou dvojicou $(a, b) \in \mathbb{R} \times \mathbb{R}$, pretože pre komplexné čísla $a + b.i$, $c + d.i$ platí: $a + b.i = c + d.i$ vtedy a len vtedy, keď $a = c$ a $b = d$. Pre operácie súčtu

a súčinu komplexných čísel platí: Ak $a + b.i$ a $c + d.i$ sú komplexné čísla, tak $(a+b.i)+(c+d.i) = (a+c)+(b+d).i$, $(a+b.i).(c+d.i) = (a.c-b.d)+(a.d+b.c).i$. Na týchto poznatkoch je založená nasledujúca konštrukcia (jedného modelu) poľa komplexných čísel (v ktorej komplexné číslo $a+b.i$ je reprezentované (stotožnené s) usporiadanou dvojicou $(a, b) \in \mathbb{R} \times \mathbb{R}$).

Množinou všetkých komplexných čísel je množina $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Operácie $+$ sčitovania a $.$ násobenia komplexných čísel sú definované nasledovne: Ak $(a, b), (c.d) \in \mathbb{C}$, tak $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (a.c - b.d, a.d + b.c)$.

Veta 10.1. $(\mathbb{C}, +, .)$ *je pole.*

Dôkaz. Skutočnosť, že $(\mathbb{C}, +)$ je komutatívna grupa s nulovým prvkom $(0, 0)$, v ktorej opačný prvok k prvku (a, b) je prvok $(-a, -b)$ je známa napríklad aj z lineárnej algebry. Stačí teda ukázať, že operácia násobenia $.$ je asociatívna, komutatívna, má jednotkový prvok a pre každý prvok $(a, b) \in \mathbb{C}$, $(a, b) \neq (0, 0)$ existuje inverzný prvok vzhľadom na násobenie.
Nech $(a, b), (c, d), (u, v) \in \mathbb{C}$. Potom $((a, b).(c, d)).(u, v) = (a.c-b.d, a.d+b.c).(u, v) = ((a.c - b.d).u - (a.d + b.c).v, (a.c - b.d).v + (a.d + b.c).u) = (a.c.u - b.d.u - a.d.v - b.c.v, a.c.v - b.d.v + a.d.u + b.c.u) = (a.(c.u - d.v) - b.(c.v + d.u), a.(c.v + d.u) + b.(c.u - d.v)) = (a, b).(c.u - d.v, c.v + d.u) = (a, b).((c, d).(u, v))$. Ďalej, $(a, b).(c, d) = (a.c - b.d, a.d + b.c) = (c.a - d.b, c.b + d.a) = (c, d).(a, b)$, $(a, b).(1, 0) = (a.1 - b.0, a.0 + b.1) = (a, b)$. Teda operácia násobenia je asociatívna, komutatívna a má jednotkový prvok $(1, 0)$. Nech teraz $(a, b) \neq (0, 0)$. Potom $a^2+b^2 \neq 0$ a $(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}) \in \mathbb{C}$. Ľahko sa overí, že $(a, b).(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}) = (1, 0)$ a teda prvok $(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2})$ je inverzný k prvku (a, b) vzhľadom na násobenie. □

Nech $f : (\mathbb{R}, +, .) \longrightarrow (\mathbb{C}, +, .)$ je zobrazenie definované predpisom $f(a) = (a, 0)$. Potom toto zobrazenie je prosté a je to homomorfizmus okruhov. Skutočne, pre každé $a, c \in \mathbb{R}$ platí $f(a+c) = (a+c, 0) = (a, 0)+(c, 0) = f(a)+f(c)$ a $f(a.c) = (a.c, 0) = (a, 0).(c, 0) = f(a).f(c)$. Preto množina $\overline{\mathbb{R}} = f[\mathbb{R}]$ určuje podpole poľa $(\mathbb{C}, +, .)$, ktoré je izomorfné s poľom $(\mathbb{R}, +, .)$. Ak stotožníme každé reálne číslo a s komplexným číslom $(a, 0)$, tak môžeme pole reálnych čísel považovať za podpole poľa komplexných čísel a pole komplexných čísel za rozšírenie poľa reálnych čísel. Pre každé komplexné číslo (a, b) platí $(a, b) = (a, 0) + (b, 0).(0, 1)$. Ak označíme číslo $(0, 1)$ písmenom i a čísla $(a, 0)$, $(b, 0)$ stotožníme s reálnymi číslami a, resp. b, tak dostávame rovnosť $(a, b) = a + b.i$, pričom vyjadrenie komplexného čísla (a, b) v tvare $a + b.i$ je známe ako vyjadrenie komplexného čísla v algebraickom tvare.

Na množine $\mathbb{C}$ komplexných čísel existuje nekonečne veľa usporiadaní, napríklad lexikografické usporiadanie ($(a, b) < (c, d)$ práve vtedy, keď $a < b$ v $(\mathbb{R}, <)$ alebo $a = b$ a $c < d$ v $(\mathbb{R}, <)$). V odseku Príklady 2.4 sme ukázali že na množine komplexných čísel neexistuje také usporiadanie $<$, pre,ktoré by platilo, že $(\mathbb{C}, +, ., <)$ je usporiadané pole.

Literatúra

[1] Birkhoff, G a Mac Lane, S.: Prehľad modernej algebry, ALFA, 1979

[2] Katriňák, T. a kol.: Algebra a teoretická aritmetika (1), 1985, 1995, 1999, 2002

[3] Mac Lane, S. a Birkhoff, G.: Algebra, ALFA, 1973

[4] Šalát, T. a kol.: Algebra a teoretická aritmetika (2), ALFA, 1986

[5] Kolektív: Učebné texty z matematiky pre postgraduálne štúdium, SPN, 1970