MATEMATICKÉ OBZORY 16/1980

NETRADIČNÁ KONŠTRUKCIA REÁLNYCH ČÍSEL III

LADISLAV MIŠÍK

V druhej časti sa opisuje systém Ad (X) všetkých aditívnych zobrazení na komutatívnej grupe X. Ukazujú sa niektoré vlastnosti aditívnych zobrazení (tvrdenia 8, 9, 10 a 11 a veta 4). Dokazuje sa tvrdenie o reprezentácii prvkov najmenšej podgrupy $G(a, \psi)$ generovanej prvkom a a aditívnym zobrazením ψ (tvrdenie 12). Zavádza sa pojem absolútne komutujúceho aditívneho zobrazenia na komutatívnej grupe X a vo vete 5 sa uvádza existencia jediného takého aditívneho zobrazenia χ_x z $G(a, \psi)$ do $G(a, \psi)$, ktoré v prvku a nadobúda hodnotu x. Pritom x je prvkom podgrupy $G(a, \psi)$.

Veta 5 nám v tretej časti umožní definovať súčin na $G(a, \psi)$. Veta 6 z druhej časti sa zas použije pri dôkaze vlastností definovaného súčinu. Veta 7 hovorí o možnosti jednoznačného rozšírenia násobenia na úplnú lineárne usporiadanú v sebe hustú komutatívnu grupu, ak na jej hustej podgrupe je definované násobenie spĺňajúce istú vlastnosť. Tvrdenie 17 ukazuje na existenciu takého aditívneho absolútne komutujúceho zobrazenia ψ na úplnej lineárne usporiadanej v sebe hustej komutatívnej grupe X, ktoré každému prvku x priraďuje taký prvok y, ktorého dvojnásobok je x, t.j. platí $x = 2y$. Pre ľubovoľný kladný prvok $a \in X$ je podgrupa $G(a, \psi)$ hustá v X a násobenie na $G(a, \psi)$ definované v zmysle vety 5 má vlastnosti, ktoré sa vyžadujú od násobenia vo vete 7. Tým je urobená príprava, aby sa dokázalo, že na každej úplnej lineárne usporiadanej v sebe hustej komutatívnej grupe možno definovať násobenie tak, že takto vzniknutá štruktúra je množinou všetkých reálnych čísel (veta 11). Tým je v prvých troch častiach článku skončená prvá úloha článku, totiž definovaním násobenia na úplnej lineárne usporiadanej v sebe hustej komutatívnej grupe vytvorenie množiny všetkých reálnych čísel.

Pretože v tejto časti článku sa budú veľmi často opakovať axiómy množiny všetkých reálnych čísel, ktoré boli uvedené v prvej časti článku, aby sa čitateľ nemusel stále vracať k prvej časti, uvedieme znova tieto axiómy tým, že zopakujeme definíciu množiny všetkých reálnych čísel.

Množinou všetkých reálnych čísel rozumieme nekonečnú množinu, v ktorej operácie súčtu a súčinu a usporiadanie spĺňajú tieto axiómy:

(+1) (asociatívny zákon pre súčet) Pre každé x, y a $z \in X$ platí: $(x+y)+z = x+(y+z)$;

(+2) (komutatívny zákon pre súčet) Pre každé x a $y \in X$ platí: $x+y = y+x$;

(+3) Pre každé x a $y \in X$ existuje také $z \in X$, že $x+z=y$;

($\cdot$1) (asociatívny zákon pre súčin) Pre každé x, y a $z \in X$ platí: $(xy)z = x(yz)$;

($\cdot$2) (komutatívny zákon pre súčin) Pre každé x a $y \in X$ platí: $xy = yx$;

($\cdot$3) (zákon delenia) Pre každé x a $y \in X$, pre ktoré $x \neq 0$, existuje také $z \in X$, že $xz = y$;

(+$\cdot$1) (distributívny zákon) Pre každé x, y a $z \in X$ platí: $(x+y)z = xz + yz$;

(<1) (tranzitívnosť usporiadania) Pre každé x, y a $z \in X$ platí: ak $x<y$ a $y<z$, tak aj $x<z$;

(<2) (lineárnosť usporiadania) Pre každé x, $y \in X$ platí práve jeden zo vzťahov: $x<y$, $x=y$ a $y<x$;

(+<1) Pre každé x, y a $z \in X$ platí: ak $x<y$, tak aj $x+z<y+z$;

($\cdot$<) Pre každé x a $y \in X$, pre ktoré $0<x$ a $0<y$, platí $0<xy$;

(<3) Pre každú neprázdnu podmnožinu A množiny X, ktorá je zhora ohraničená, t.j. existuje také $x \in X$, že $a<x$, pre každé $a \in A$, existuje také $z \in X$, že pre každé $a \in A$ platí $a \leqq z$ a $z \leqq y$ pre každé $y \in X$, pre ktoré $a \leqq y$ pre každé $a \in A$. Prvok z nazývame suprémom množiny A a označujeme ho sup A.

4. Násobenie v úplných lineárne usporiadaných komutatívnych grupách

Definícia. Lineárne usporiadaná komutatívna grupa X sa nazýva úplnou vtedy a len vtedy, keď pre usporiadanie platí aj (<3), t.j. pre každú neprázdnu zhora ohraničenú podmnožinu A grupy X existuje také $z \in X$, že pre každé $a \in A$ platí $a \leqq z$ a $z \leqq y$ pre každé $y \in X$, pre ktoré $a \leqq y$ pre každé $a \in A$.

Lema 3. Nech Y je lineárne usporiadaná komutatívna grupa. Potom

(1) Nech Y je úplná. Nech $x \in Y$, $x > 0$. Potom množina $\{n \cdot x : n \in N\}$ je zhora neohraničená.

Nech na Y je definované násobenie s vlastnosťami $(\cdot 1)$, $(\cdot 2)$, $(+\cdot 1)$ a $(\cdot < 1)$. Potom platí:

(2) Nech Y je hustá v sebe, t. j. obsahuje aspoň jeden nenulový prvok a ku každým dvom prvkom $x, y \in Y$, pre ktoré $x < y$, existuje také $z \in Y$, že $x < z < y$. Potom ku každému $x \in Y$, $x > 0$ a ku každému prirodzenému číslu n existuje taký prvok $t \in Y$, že $0 < n \cdot t < x$.

(3) Nech $x \in Y$, $x > 0$. Potom $xy > 0$ vtedy a len vtedy, keď $y > 0$ a $xy \geqq 0$ práve vtedy, keď $y \geqq 0$.

(4) Nech $x \in Y$, $x > 0$. Nech $y, z \in Y$. Potom $xy < xz$ vtedy a len vtedy, keď $y < z$ a $xy \leqq xz$ práve vtedy, keď $y \leqq z$.

Dôkaz. (1): Nech množina $\{n \cdot x : n \in N\}$ je zhora ohraničená. Pretože je neprázdna, existuje také z, že $z = \sup \{n \cdot x : n \in N\}$. Zrejme $z > 0$ (totiž $x > 0$ a $x \leqq z$). Pretože $x > 0$, je $z - x < z$. Teda existuje také prirodzené číslo n, že $z - x < n \cdot x$. Ale potom je $(n+1) \cdot x = n \cdot x + x > (z - x) + x = z$. To je však spor s definíciou supréma množiny $\{n \cdot x : n \in N\}$.

(2) Nech Y je hustá v sebe, $x \in Y$ a $x > 0$. Označme znakom W množinu všetkých tých prirodzených čísel n, pre ktoré existuje také $t \in Y$, že $0 < n \cdot t < x$. Z hustoty v sebe množiny Y vyplýva, že existuje také $t \in Y$, že $0 < t < x$. Teda $0 < t = 1 \cdot t < x$, čiže $1 \in W$. Nech $n \in W$. Teda existuje také $t \in Y$, že $0 < n \cdot t < x$. Potom existuje také $u \in Y$, že $0 < u < x - n \cdot t$. Ak $t \leqq u$, tak $0 < (n+1) \cdot t = n \cdot t + t \leqq n \cdot t + u < n \cdot t + (x - n \cdot t) = x$; ak $u < t$, tak $0 < (n+1) \cdot u = n \cdot u + u < n \cdot t + u < n \cdot t + (x - n \cdot t) = x$, čiže $n + 1 \in W$. Tým je matematickou indukciou dokázané, že W je množina všetkých prirodzených čísel. Tvrdenie (2) je teda dokázané.

(3) Nech $x \in Y$, $x > 0$.

Ak $y > 0$, tak $xy > 0$ podľa $(\cdot < 1)$.

Nech $xy > 0$. Potom neplatí $y = 0$, pretože $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, a teda podľa tvrdenia 3 je $x \cdot 0 = 0$. Ale neplatí ani $y < 0$. Pretože, keby to platilo, platilo by $-y > 0$, a teda $x(-y) > 0$. Z toho by vyplývalo, že $0 = x \cdot 0 = x(y + (-y)) = xy + x(-y) > 0$, čo je spor. Teda musí platiť $y > 0$.

Pretože $x \cdot 0 = 0$, platí $xy \geqq 0$, ak $y \geqq 0$.

Nech $xy \geqq 0$. Potom ak platí $xy > 0$, tak podľa dokázaného je $y > 0$.

Nech $xy=0$. Potom $y=0$, pretože $xy>0$, ak $y>0$ a $xy<0$, ak $y<0$ (je totiž $xy+x(-y) = x(y+(-y)) = x\cdot 0=0$, čiže $xy=-(x(-y))$).

(4) Nech $x\in Y$ a $x>0$. Potom $xy<xz$ platí vtedy a len vtedy, keď $xz-xy>0$. Ale to platí vtedy a len vtedy, keď $x(z-y)>0$. Ale to podľa (3) platí vtedy a len vtedy, keď $z-y>0$. Ale vzťah $z-y>0$ platí vtedy a len vtedy, keď $z>y$, čiže $y<z$.

Nerovnosť $xy\leqq xz$ platí práve vtedy, keď $x(z-y)\geqq 0$. Podľa (3) posledná nerovnosť platí práve vtedy, keď $z-y\geqq 0$, čiže $y\leqq z$.

Lema 4. Nech na komutatívnej grupe Y je definované násobenie spĺňajúce $(\cdot 2)$ a $(+\cdot 1)$. Potom pre každé x, y a $z\in Y$ platí:

$0\cdot x=x\cdot 0=0$,

$x(y-z)=xy-xz$,

$x(-y)=(-x)y=-xy$.

Dôkaz. Nech x, y a $z\in Y$. Potom dostaneme: $x\cdot 0+x\cdot 0 = x(0+0) = x\cdot 0$ a z tvrdenia 3 vyplýva, že $x\cdot 0=0$. Pretože $0\cdot x=x\cdot 0$, je aj $0\cdot x=0$.

Pretože $xz+x(y-z)=x(z+(y-z))=xy$, je $x(y-z)=xy-xz$.

Pretože $xy+(-x)y=yx+y(-x)=y(x+(-x))=y\cdot 0=0$, je $(-x)y=-xy$. Ďalej dostaneme, že $x(-y) = (-y)x = -yx = -xy$.

Veta 7. Nech X je úplná lineárne usporiadaná grupa. Nech H je jej podgrupa, ktorá je v nej hustá, t. j. pre každé dva prvky $x, y\in X$, pre ktoré $x<y$, existujú také prvky a, b a $c\in H$, že $a<x<b<y<c$. Nech na podgrupe H definované násobenie spĺňa $(\cdot 1)$, $(\cdot 2)$, $(+\cdot 1)$ a $(\cdot <1)$ a vlastnosť

(A): Pre každé $x\in H$, $x>0$ a pre každé $e\in H$, $e>0$, existuje také $h\in H$, že $0<xh<e$.

Potom na X existuje jediné násobenie, ktoré je rozšírením násobenia na H a ktoré spĺňa $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$.

Dôkaz. Najprv ukážeme, že to násobenie na X, ktoré je rozšírením na X násobenia na H a spĺňa vlastnosti $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$ môže byť jediné. Ukážeme to tak, že dokážeme, že tými vlastnosťami to rozšírenie je jednoznačne definované.

V tejto úvahe označujme násobenie na H prvkov a, $b\in H$ znakom $(ab)_H$, kým násobenie na X, ktoré je rozšírením násobenia na H a spĺňa $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$ znakom xy, ak x a $y\in X$.

Nech $x, y\in X$ a $x\geqq 0$, $y\geqq 0$. Pretože $uy\leqq xy$ pre každé $u\in H$, pre ktoré $0\leqq u\leqq x$, platí $w=\sup\{uy\colon 0\leqq u\leqq x\,;\, u\in H\}\leqq xy$. Ukážeme, že $w=xy$.

Keby totiž platilo $w < xy$, existovalo by také $h \in H$, že $0 < h < xy - w$. Z hustoty H vyplýva, že existuje také $c \in H$, že $y < c$. Z vlastnosti (A) vyplýva, že existuje také $k \in H$, že $0 < (kc)_H < h$. Z toho dostaneme: $w < xy - h < xy - (kc)_H < xy - ky = (x-k)y$. Z hustoty H vyplýva, že existuje také $\bar{u} \in H$, že $x - k < \bar{u} < x$. Preto $w < (x-k)y < \bar{u}y \leqq \leqq \sup \{uy\colon 0 \leqq u \leqq x;\ u \in H\} = w$. To je spor. Preto $w = xy$.

Z dokázaného dostaneme: $xy = \sup \{uy\colon 0 \leqq u \leqq x;\ u \in H\} = \sup\{\sup \{(uv)_H\colon 0 \leqq v \leqq y;\ v \in H\}\colon 0 \leqq u \leqq x;\ u \in H\} = \sup \{(uv)_H\colon 0 \leqq u \leqq x, 0 \leqq v \leqq y;\ u, v \in H\}$.

Nech $x \geqq 0$ a $y < 0$. Podľa lemy 4 platí $xy = -(-xy) = -(x(-y))$. Ak $x < 0$, tak z lemy 4 zas dostaneme: $xy = -(-xy) = -((-x)y)$.

Z týchto úvah vidieť, že ak existuje také rozšírenie, potom násobenie na X musí byť definované takto: Nech $x, y \in X$.

Ak $x \geqq 0$ a $y \geqq 0$, tak $xy = \sup \{(uv)_H\colon 0 \leqq u \leqq x, 0 \leqq v \leqq y;\ u, v \in H\}$.

Ak $x \geqq 0$ a $y < 0$, tak definujeme $xy = -(x(-y))$.

Ak $x < 0$, tak definujeme $xy = -((-x)y)$.

Z toho vidieť, že násobenie xy je definované pre každé x a $y \in X$.

Ak ukážeme, že takto definované násobenie na X spĺňa $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$ a je rozšírením na X násobenia na H, t. j. pre $u, v \in H$ platí $uv = (uv)_H$, tak bude veta 7 dokázaná.

Skôr než prejdeme k tomuto dôkazu, dokážeme dve tvrdenia a jednu lemu.

Tvrdenie 15. Platí: $0 \cdot x = 0 = x \cdot 0$ pre každé $x \in X$.

Dôkaz. Nech $x \in X$. Potom pre $x \geqq 0$ platí: $0 \cdot x = \sup \{(ab)_H\colon 0 \leqq a \leqq 0, 0 \leqq b \leqq x;\ a, b \in H\} = \sup \{(0 \cdot b)_H\colon 0 \leqq b \leqq x;\ b \in H\} = = \sup \{0\} = 0 = \sup \{0\} = \sup \{(a \cdot 0)_H\colon 0 \leqq a \leqq x;\ a \in H\} = \sup \{(ab)_H\colon 0 \leqq a \leqq x, 0 \leqq b \leqq 0;\ a, b \in H\} = x \cdot 0$.

Pre $x < 0$ je $0 \cdot x = -(0 \cdot (-x)) = 0 = -((-x) \cdot 0) = x \cdot 0$.

Tvrdenie 16. Pre každé $x, y \in X$ platí: $(-x)y = -xy$.

Dôkaz. Nech $x, y \in X$. Potom pre $x > 0$ platí: $(-x)y = -((-(-x))y) = = -xy$. Pre $x = 0$ platí: $(-x)y = 0 = -xy$. Pre $x < 0$ platí: $(-x)y = = -(-((-x)y)) = -xy$.

Lema 5. Nech $u, v \in H$, $u > 0$, $v > 0$. Potom pre každé prirodzené číslo n platí: $u(n \cdot v) = n \cdot (uv)$.

Dôkaz. Označme $W = \{n \in N\colon \text{pre } n \text{ platí: } u(n \cdot v) = n \cdot (uv)\}$. Potom $1 \in W$, pretože $u(1 \cdot v) = uv = 1 \cdot (uv)$. Nech $j \in N$ je také, že $j \in W$, t. j.

$u(j\cdot v) = j\cdot(uv)$. Potom je aj $j+1\in W$, pretože $u((j+1)\cdot v) = u(j\cdot v+v) = u(j\cdot v)+uv = j\cdot(uv)+uv = (j+1)\cdot(uv)$. Teda W je množina všetkých prirodzených čísel a lema je dokázaná.

Teraz dokážeme, že násobenie na X je rozšírením násobenia na H. Potom $(xy)_H\in\{(ab)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\}$ a $(ab)_H \leqq (xy)_H$ pre každé a, b, x, $y\in H$, pre ktoré $0\leqq a\leqq x$, $0\leqq b\leqq y$. Preto $xy = \sup\{(ab)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a, b\in H\}=(xy)_H$ pre každé $x, y\in H$.

Najprv zrejme platí $(\cdot<1)$. Nech totiž x, $y\in X$, $x>0$ a $y>0$. Potom existujú také u, $v\in H$, že $0<u<x$, $0<v<y$. Zrejme $uv>0$. Z toho $xy=\sup\ \{(ab)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\} \geqq uv>0$.

Ďalej ukážeme, že platí $(\cdot 2)$. Nech x, $y\in X$.

Nech $x\geqq 0$, $y\geqq 0$. Pretože pre násobenie na H platí $(\cdot 2)$, platí: $\{(ab)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\}=\{(ba)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\}$. Teda $xy=\sup\ \{(ab)_H\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\} = \sup\ \{(ba)_H\colon 0\leqq b\leqq y,\ 0\leqq a\leqq x;\ a,\ b\in H\}=yx$.

Nech $x\geqq 0$, $y<0$. Potom $xy=-(x(-y)) = -((-y)x)=yx$.

Nech $x<0$. Potom $-x>0$. Teda $(-x)y=y(-x)$ a $xy=-((-x)y)= -(y(-x))=yx$, ak $y\geqq 0$ a $xy=-((-x)y)=-(y(-x))=(-y)(-x)= -((-y)x)=yx$, ak $y<0$.

Dôkaz vlastnosti $(\cdot 1)$: Nech x, y, $z\in X$. Potom dokážeme, že pre $x\geqq 0$, $y\geqq 0$ a $z\geqq 0$ platí $(xy)z = \sup\{(uv)w\colon 0\leqq u\leqq x, 0\leqq v\leqq y, 0\leqq w\leqq z;\ u,\ v,\ w\in H\}$. Označme to suprémum znakom d.

Pretože $uv\leqq xy$ pre každé u, $v\in H$, pre ktoré $0\leqq u\leqq x$, $0\leqq v\leqq y$, je $(uv)w\leqq(xy)z$ pre každé w, pre ktoré $w\in H$ a $0\leqq w\leqq z$. Z toho vyplýva, že $d\leqq(xy)z$. Keby platilo $d<(xy)z$, existovalo by také $h\in H$, že $d<h<(xy)z=\sup\ \{ab\colon 0\leqq a\leqq xy,\ 0\leqq b\leqq z;\ a,\ b\in H\}$. Teda existuje také p a $w\in H$, že $0\leqq p\leqq xy$, $0\leqq w\leqq z$ a $h<pw$.

Ak $p<xy$, tak existujú také u, $v\in H$, že $0\leqq u\leqq x$, $0\leqq v\leqq y$ a $p<uv$. Pretože $\{ab\colon 0\leqq a\leqq p,\ 0\leqq b\leqq w;\ a,\ b\in H\}\subset\{ab\colon 0\leqq a\leqq uv,\ 0\leqq b\leqq w;\ a,\ b\in H\}$, platí $pw\leqq(uv)w$. Teraz dostaneme: $h<pw\leqq (uv)w\leqq d<h$, čo je spor.

Nech $p=xy$. Vtedy $xy\in H$. Pretože $(xy)w-h>0$, existuje podľa (A) také $s\in H$, že $0<sw<(xy)w-h$, čiže $h<(xy)w-sw = (xy-s)w$. Keďže $xy-s<xy$, existujú také u, $v\in H$, že $0\leqq u\leqq x$, $0\leqq v\leqq y$ a $xy-s<uv$. Z toho vyplýva, že $h<(xy-s)w \leqq (uv)w\leqq d<h$, čo je spor.

Tým sme zistili, že $d<(xy)z$ vedie k sporu, a preto musí platiť $d=(xy)z$.

Z dokázaného pre $x\geqq 0$, $y\geqq 0$ a $z\geqq 0$ dostaneme:

$(xy)z=\sup\{(uv)w\colon 0\leqq u\leqq x,\ 0\leqq v\leqq y,\ 0\leqq w\leqq z;\ u,\ v,\ w\in H\}=$ $=\sup\{u(vw)\colon 0\leqq u\leqq x,\ 0\leqq v\leqq y,\ 0\leqq w\leqq z;\ u,\ v,\ w\in H\}=\sup$ $\{(vw)u\colon 0\leqq v\leqq y,\ 0\leqq w\leqq z,\ 0\leqq u\leqq x;\ u,\ v,\ w\in H\}=(yz)x=x(yz)$.

Nech $x\geqq 0$, $y\geqq 0$ a $z<0$. Potom $(xy)z=-((xy)(-z))=-(x(y(-z)))=$ $=-((y(-z)x)=(-(y(-z)))x=(yz)x=x(yz)$.

Nech $x\geqq 0$ a $y<0$. Potom $-y>0$, a teda podľa dokázaného $(x(-y))z=x((-y)z)$. Z toho: $(xy)z=(-x(-y))z=-((x(-y))z)=$ $=-(x((-y)z))=-(((-y)z)x)=(-((-y)z))x=(yz)x=x(yz)$.

Tým sme zistili, že pre x, y a $z\in X$, pre ktoré $x\geqq 0$, platí: $(xy)z=x(yz)$.

Nech $x<0$. Potom $(xy)z=(-(-x)y)z=-(((-x)y)z)=$ $=-((-x)(yz))=(-(-x))(yz)=x(yz)$.

Dôkaz vlastnosti: $(+\cdot 1)$: Nech $x,\ y,\ z\in X$.

Nech $x\geqq 0$, $y\geqq 0$ a $z\geqq 0$. Pre $z=0$ platí: $x(y+z)=xy=xy+0$ $=xy+x\cdot 0=xy+xz$. V ďalšom budeme preto predpokladať, že $z>0$. Najprv dokážeme, že platí: $\sup\{a(b+c)\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y,\ 0\leqq c\leqq z;$ $a,\ b,\ c\in H\}=xy+xz$. Označme to suprémum znakom d.

Zrejme platí $d=\sup\{ab+ac\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y,\ 0\leqq c\leqq z;\ a,\ b,$ $c\in H\}\leqq\sup\{ab\colon 0\leqq a\leqq x,\ 0\leqq b\leqq y;\ a,\ b\in H\}+\sup\{ac\colon 0\leqq a\leqq x,$ $0\leqq c\leqq z;\ a,\ c\in H\}=xy+xz$.

Nech $d<xy+xz$. Potom $d-xz<xy$, a teda existujú také $u,\ v\in H$, že $0\leqq u\leqq x$, $0\leqq v\leqq y$ a $d-xz<uv$. Potom $d-uv<xz$, a teda existujú také $s,\ w\in H$, že $0\leqq s\leqq x$, $0\leqq w\leqq z$ a $d-uv<sw$. Nech $t=\max(u,s)$. Zrejme $t\in H$, $0\leqq t\leqq x$, $uv\leqq tv$ a $sw\leqq tw$. Potom $d<uv+sw\leqq tv+$ $+tw=t(v+w)\leqq d$, čo je spor. Preto $d=xy+xz$.

Pretože pre každé $a,\ b,\ c\in H$, pre ktoré $0\leqq a\leqq x$, $0\leqq b\leqq y$, $0\leqq c\leqq z$ platí $a(b+c)\leqq x(y+z)$, platí $d\leqq x(y+z)$. Keby platilo, že $d<x(y+z)$, existovali by také $u,\ \bar{v}\in H$, že $0\leqq u\leqq x$, $0\leqq\bar{v}\leqq y+z$ a $d<u\bar{v}$. Z hustoty H v X a z vlastnosti $(\cdot<1)$ násobenia na H môžeme $\bar{v}\in H$ voliť tak, že $y<\bar{v}<y+z$. Potom $\bar{v}-y<z$. Z hustoty H v X vyplýva, že existuje také $w\in H$, že $0<\bar{v}-y<w<z$. Potom $\bar{v}-w<y$. Z hustoty H v X vyplýva, že existuje také $v\in H$, že $0<v$ a $\bar{v}-w<v<y$. Potom $0<u<x$, $0<v<y$ a $0<\bar{v}<v+w<y+z$. Teda $d<u\bar{v}<u(v+w)$. Z toho dostaneme, že $d<u(v+w)\leqq d$, čo je spor. Preto platí $x(y+z)=d=xy+xz$.

Nech $x \geqq 0$. Ak $y \geqq 0$, $z < 0$ a $y + z \geqq 0$, tak $xy = x(y + z + (-z)) = x(y + z) + x(-z) = x(y + z) - (-(x(-z))) = x(y + z) - xz$, čiže $xy + xz = x(y + z)$. Ak $y \geqq 0$, $z < 0$ a $y + z < 0$, tak $-y \leqq 0$, $-z > 0$ a $(-z) + (-y) > 0$. Preto $x(y + z) = -(x(-(y + z))) = -(x((-y) + (-z))) = -(x((-z) + (-y))) = -(x(-z) + x(-y)) = -(x(-z)) + (-(x(-y)) = xz + (-((-y)x)) = xz + (-((-y)x)) = xz + (-(-y))x = xz + yx = xy + xz$. Ak $y < 0$, tak $-y > 0$ a podľa dokázaného $x((-y) + (-z)) = x(-y) + x(-z)$. Z toho dostaneme: $xy + xz = -(x(-y)) + (-(-zx)) = -(x(-y) + ((-z)x)) = -(x(-y) + x(-z)) = -(x((-y) + (-z))) = -((-(y + z))x) = (-(-(y + z)))x = (y + z)x = x(y + z)$. Tým sme dokázali, že $x(y + z) = xy + xz$ pre každé x, y a $z \in X$, pre ktoré $x \geqq 0$.

Nech $x < 0$. Potom $(-x)(y + z) = (-x)y + (-x)z$, a teda $x(y + z) = -((-x)(y + z)) = -((-x)y + (-x)z) = -(-x)y + (-(-x)z) = xy + xz$.

Tým sme dokázali, že násobenie na X má vlastnosť $(+\cdot 1)$.

Dôkaz vlastnosti $(\cdot 3)$: Nech $x, y \in X$.

Najprv predpokladajme, že $x > 0$.

Nech $y > 0$. Uvažujme o množine $A = \{u \in X\colon xu < y,\ u > 0\}$. Najprv ukážeme, že A je neprázdna a zhora ohraničená. Z hustoty množiny H v X vyplýva, že existujú také $a, b \in H$, že $x < a$ a $0 < b < y$. Z vlastnosti (A) vyplýva, že existuje také $h \in H$, že $0 < ah < b$. Zrejme $h > 0$ a $0 < xh < ah < b < y$. Teda $h \in A$. Tým sme dokázali, že A je neprázdna. Z hustoty H v X vyplýva, že existujú také $a, b \in H$, že $0 < a < x$, $y < b$. Podľa lemy 3 (1) je množina $\{n \cdot (a \cdot a)\colon n \in N\}$ zhora neohraničená, teda existuje $n \in N$ tak, že neplatí $n \cdot (a \cdot a) \leqq b$. Teda podľa (<2) a lemy 5 platí: $y < b < n \cdot (a \cdot a) = a(n \cdot a) < x(n \cdot a)$. Nech $u \in A$. Potom $u \leqq n \cdot a$. Keby totiž platilo, že $n \cdot a < u$, platilo by $y < x(n \cdot a) < xu < y$, čo je spor. Podľa (<3) existuje suprémum množiny A. Označme ho z.

Dokážeme, že platí $xz \leqq y$. Keby totiž platilo $xz > y$, existovali by také $u, v \in H$, že $0 \leqq u \leqq x$, $0 \leqq v \leqq z$ a $y < uv$. Podľa (A) existuje také $h \in H$, že $0 < uh < uv - y$. Z toho $y < u(v - h)$. Potom pre každé $w \in X$, pre ktoré $v - h \leqq w$, platí $\{ab\colon 0 \leqq a \leqq x,\ 0 \leqq b \leqq v - h;\ a, b \in H\} \subset \{ab\colon 0 \leqq a \leqq x,\ 0 \leqq b \leqq w;\ a, b \in H\}$, teda $x(v - h) \leqq xw$ a $y < u(v - h) \leqq x(v - h) \leqq xw$, čiže $w \notin A$. Teda pre $t \in A$ platí $t < v - h$. Preto $z = \sup A \leqq v - h$. Z toho $z \leqq v - h < v \leqq z$, čo je spor.

Ale musí platiť, že $xz = y$. Keby totiž platilo, že $xz < y$, tak by existovali také a, $b \in H$, že $x < a$ a $0 < b < y - xz$. Z vlastnosti (A) vyplýva, že existuje také $h \in H$, že $0 < ah < b$. Z toho $0 < xh < ah < b < y - xz$. Teda $xz + xh < y$, čiže $x(z + h) < y$. Z toho vyplýva, že $z + h \in A$ a $z = \sup A \geqq z + h > z$, čo je spor. Tým sme dokázali, že $xz = y$.

Nech $y = 0$. Potom $x \cdot 0 = y$.

Nech $y < 0$. Potom $-y > 0$. Existuje také $z \in X$, že $xz = -y$. Z toho dostaneme, že $x(-z) = -xz = -(-y) = y$.

Nech $x < 0$. Potom $-x > 0$. Podľa dokázaného existuje také $z \in X$, že $(-x)z = y$. Z toho dostaneme, že $x(-z) = (-x)z = y$.

Tým je dokázaná vlastnosť $(\cdot 3)$.

Význam vety 7 spočíva v tom, že násobenie na úplnej lineárne usporiadanej v sebe hustej komutatívnej grupe s vlastnosťami $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot < 1)$ možno definovať, ak možno definovať na jej vhodnej podgrupe násobenie s vlastnosťami $(\cdot 1)$, $(\cdot 2)$, $(+\cdot 1)$ a $(\cdot < 1)$.

Napokon ukážeme, že netriviálna úplná lineárne usporiadaná komutatívna grupa môže predstavovať len alebo grupu všetkých celých čísel (ak nie je grupa v sebe hustá), alebo grupu všetkých reálnych čísel (ak je v sebe hustá). V tejto časti X bude vždy znamenať úplnú lineárne usporiadanú komutatívnu grupu.

Veta 8. Nech X je úplná lineárne usporiadaná komutatívna grupa, ktorá nie je v sebe hustá a triviálna. Potom existuje taký prvok $e \in X$, že $e > 0$, $X = \{n \cdot e\colon n \in Z\}$, $n \cdot e + m \cdot e = (n + m) \cdot e$ pre každé n, $m \in Z$ a $n \cdot e \neq m \cdot e$ pre každé n, $m \in Z$, pre ktoré $n \neq m$.

Dôkaz. Pretože X nie je triviálna a nie je v sebe hustá, existujú také dva prvky x, $y \in X$, že $x < y$ a $\{z \in X\colon x < z < y\}$ je prázdna. Položme $e = y - x$. Zrejme $e \in X$, $e > 0$ a $\{n \cdot e\colon n \in Z\} \subset X$.

Nech $u \in X$. Podľa lemy 3 (1) je množina $\{n \cdot e\colon n \in N\}$ zhora neohraničená. Teda pre $-u \in X$ existuje také prirodzené číslo n, že $-u < n \cdot e$. Z toho dostaneme, že $(-n) \cdot e = -(n \cdot e) < u$. Definujme $A = \{k \in Z\colon k \cdot e < u\}$. Pretože $-n \in A$, je A neprázdna. Pretože $\{n \cdot e\colon n \in N\}$ je zhora neohraničená, existuje také prirodzené číslo m, že $u < m \cdot e$. Nech $k \in A$. Potom musí platiť $k < m$. Keby totiž platilo $m \leqq k$, tak by platilo aj $u < m \cdot e \leqq k \cdot e < u$, čo je spor. Teda $k < m$. Preto A je zhora ohraničená. Podľa vlastnosti (Z) množiny všetkých celých čísel má množina A

maximum. Označme ho i. Teda platí: $i \cdot e < u$ a $u \leqq (i+1) \cdot e$. Ukážeme, že nemôže platiť $u < (i+1) \cdot e$.

Keby totiž platilo, že $u < (i+1) \cdot e$, bolo by $v = (i+1) \cdot e - u > 0$ a $v = (i+1) \cdot e - u < (i+1) \cdot e - i \cdot e = i \cdot e + e - i \cdot e = e$. Potom by platilo: $x < x + v < x + e = x + (y - x) = y$, a teda $x + v \in \{z \in X \colon x < z < y\}$. To je však spor.

Teda je $u = (i+1) \cdot e \in \{n \cdot e \colon n \in Z\}$. Pretože u bol ľubovoľný prvok z X a $u \in \{n \cdot e \colon n \in Z\}$, je $X \subset \{n \cdot e \colon n \in Z\}$. Teda $X = \{n \cdot e \colon n \in Z\}$.

Nech $n, m \in Z$. Potom $n \cdot e + m \cdot e = (n + m) \cdot e$ je práve tvrdenie (d1) z vety 1.

Nech n, $m \in Z$ a $n \neq m$. Potom $n - m \in Z$ a $n - m \neq 0$. Z tvrdenia 6 vyplýva, že $(n - m) \cdot e \neq 0$. Preto $n \cdot e = ((m + (n - m)) \cdot e = m \cdot e + (n - m) \cdot e \neq m \cdot e$.

Tým je veta 8 dokázaná.

Tvrdenie 17. Nech X je úplná v sebe hustá lineárne usporiadaná komutatívna grupa. Potom ku každému prvku $x \in X$ existuje jediný taký prvok $y \in X$, že $2y = x$.

Ak $x \in X$ a $x > 0$, tak je aj $y > 0$.

Dôkaz. Nech $x \in X$. Najprv dokážeme, že existuje aspoň jeden taký prvok $y \in X$, že $2y = x$. Nech $x > 0$. Nech $A = \{z \in X \colon z > 0,\ 2z < x\}$. Pretože $0 < x$ a X je hustá v sebe, existuje také $t \in X$, že $0 < t < x$. Teda $\min(t, x - t) > 0$. Pretože X je hustá v sebe, existuje také $u \in X$, že $0 < u < \min(t, x - t)$. Potom je $u \in A$, pretože $u > 0$ a $2u = u + u < t + (x - t) = x$. Tým sme zistili, že množina A je neprázdna pre každé $x \in X$, pre ktoré $x > 0$.

Ukážeme teraz, že pre každé $z \in A$, je $z < x$, čiže množina A je zhora ohraničená. Nech $z \in A$. Potom podľa (<2) je alebo $z < x$, alebo $x \leqq z$. Keby platilo $x \leqq z$, bolo by $x = x + 0 < z + z = 2z < x$, čo je spor. Teda $z < x$.

Pretože X je úplná, existuje podľa (<3) suprémum množiny A. Označme ho y. Podľa (<2) platí alebo $2y < x$, alebo $2y = x$, alebo $x < 2y$.

Nech $2y < x$. Potom podľa dokázaného je množina $\{h \in X \colon h > 0,\ 2h < x - 2y\}$ neprázdna, pretože $x - 2y > 0$. Nech teda $v \in \{h \in X \colon h > 0,\ 2h < x - 2y\}$. Potom platí $v > 0$ a $2v < x - 2y$, čiže $2 \cdot (y + v) = 2 \cdot y + 2 \cdot v < x$. Teda $y + v \in A$. Preto $y < y + v \leqq \sup A = y$. To je spor. Teda nemôže platiť $2y < x$.

Nech $x<2y$. Potom $2y-x>0$ a podľa dokázaného je množina $\{h\in X\colon h>0,\ 2h<2\cdot y-x\}$ neprázdna. Nech $v\in\{h\in X\colon h>0,\ 2\cdot h<2\cdot y-x\}$. Teda $v>0$, $2\cdot v<2\cdot y-x$, čiže $x<2\cdot y-2\cdot v\ =\ 2\cdot(y-v)$. Nech $u\in A$. Potom nemôže platiť $u\geqq y-v$. Keby totiž platilo $y-v\leqq u$, bolo by $x<2\cdot(y-v)\leqq 2\cdot u<x$, čo je spor. Teda pre každé $u\in A$ platí $u<y-v$. Z definície supréma množiny A vyplýva, že $y=\sup A\ \leqq\ y-v<y$. To je spor. Teda nemôže platiť ani $x<2\cdot y$.

Tým sme dokázali, že $2\cdot y=x$, a teda pre $x>0$ je zaručená existencia takéhoto prvku $y\in X$, že $2\cdot y=x$. Súčasne je zrejmé, že $y>0$, pretože je suprémom množiny prvkov väčších ako 0.

Pre $x=0$, je $2\cdot 0=0=x$.

Pre $x<0$, je $-x>0$. Teda existuje také $y\in X$, že $2\cdot y=-x$. Potom $-y\in X$ a $2\cdot(-y)\ =\ -2\cdot y\ =\ -(-x)=x$.

Zostáva už len dokázať, že taký prvok existuje jediný. Nech $x\in X$ a nech $u,\ v\in X$ sú také, že $2\cdot u=x$ a $2\cdot v=x$. Potom podľa (<2) platí alebo $u<v$, alebo $u=v$, alebo $v<u$. Nech $u<v$. Potom $x=2\cdot u=$ $=u+u\ <\ v+v=2\cdot v=x$ dáva spor. Podobne pre $v<u$ dostaneme: $x=2\cdot v=v+v\ <\ u+u=2\cdot u=x$, čo je spor. Preto $u=v$. Tým je dokázaná jednoznačnosť.

Tvrdenie 17 nám umožňuje nasledovnú definíciu:

Definícia. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa. Zobrazenie $\psi\colon X\to X$ definované tak, že $2\cdot\psi(x)=x$ pre každé $x\in X$, nazývame pôlením.

Tvrdenie 18. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa. Potom pôlenie je kladné aditívne absolútne komutujúce zobrazenie.

Dôkaz. ψ je kladné: Nech $x\in X$, $x>0$. Potom podľa tvrdenia 17 je $\psi(x)>0$.

ψ je aditívne zobrazenie: Nech $x,\ y\in X$. Potom platí: $2\cdot\psi(x)=x$ a $2\cdot\psi(y)=y$. Z toho: $2\cdot(\psi(x)+\psi(y))=2\cdot\psi(x)+2\cdot\psi(y)=x+y$. Pretože aj $2\cdot\psi(x+y)=x+y$, musí podľa tvrdenia 17 byť $\psi(x)+$ $+\ \psi(y)=\psi(x+y)$ (využili sme pritom jednoznačnosť).

ψ je absolútne komutujúce: Nech H je komutatívna podgrupa grupy X, pre ktorú $\psi(H)\subset H$. Nech $\chi\in\mathrm{Ad}\ (H)$. Ukážeme, že platí: $\psi_{\circ}\chi=\chi_{\circ}(\psi/H)$. Nech $x\in H$. Potom použitím tvrdenia 9 dostaneme, že $2\chi(\psi(x))\ =\ \chi(2\cdot\psi(x))\ =\ \chi(x)$. Pretože aj $2\cdot\psi(\chi(x))\ =\ \chi(x)$, musí byť podľa tvrdenia 17 $\chi(\psi(x)) = \psi(\chi(x))$ pre každé $x \in H$ (využili sme zas jednoznačnosť). Z toho vidieť, že $\chi_0(\psi/H) = \psi_0 \chi$.

Definícia. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa, nech ψ je pôlenie na X a nech $a \in X$, $a > 0$. Nech $G(a, \psi)$ je komutatívna podgrupa grupy X vytvorená prvkom a a zobrazením ψ. Nech $x, y \in G(a, \psi)$, nech χ_x a χ_y sú jediné (pozri vetu 5 (ii)) aditívne zobrazenia na $G(a, \psi)$, pre ktoré $\chi_x(a) = x$ a $\chi_y(a) = y$. Potom súčinom xy prvkov x a y rozumieme prvok $(\chi_y \circ \chi_x)(a)$.

Lema 6. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa, nech ψ je pôlenie na X, nech $a \in X$, $a > 0$ a nech $G(a, \psi)$ je podgrupa grupy X vytvorená prvkom a a zobrazením ψ. Potom platí:

(1) $\chi_{xy} = \chi_y \circ \chi_x$ a $\chi_{x+y} = \chi_x + \chi_y$ pre každé $x, y \in G(a, \psi)$, pričom χ_{xy}, χ_{x+y}, χ_x a χ_y sú aditívne zobrazenia na $G(a, \psi)$, pre ktoré platí: $\chi_{xy}(a) = xy$, $\chi_{x+y}(a) = x + y$, $\chi_x(a) = x$, $\chi_y(a) = y$.

(2) Pre každé nezáporné celé číslo k platí $\psi^k(a) > 0$.

(3) Pre každý prvok $x \in G(a, \psi)$ existuje také celé číslo p, a také nezáporné celé číslo k, že $x = p\psi^k(a)$. Ak je ešte $x > 0$, je $p > 0$.

(4) Pre každé prirodzené číslo n platí $2^n \cdot \psi^n(u) = u$ pre každé $u \in X$.

Dôkaz. (1): Podľa vety 4 (iii) je $\chi_y \circ \chi_x \in \mathrm{Ad}\,(G(a, \psi))$. Pretože $\chi_{xy}(a) = xy = (\chi_y \circ \chi_x)(a)$, musí podľa vety 5 (ii) platiť $\chi_{xy} = \chi_y \circ \chi_x$.

Pretože χ_x, $\chi_y \in \mathrm{Ad}\,(G(a, \psi))$, je tiež podľa tvrdenia 13 $\chi_x + \chi_y \in \mathrm{Ad}(G(a, \psi))$. Pretože $\chi_{x+y}(a) = x + y = \chi_x(a) + \chi_y(a) = (\chi_x + \chi_y)(a)$, podľa vety 5 (ii) platí $\chi_{x+y} = \chi_x + \chi_y$.

(2): Tvrdenie dokážeme matematickou indukciou. Nech $W = \{k \in Z^+ : \psi^k(a) > 0\}$. Zrejme $0 \in W$, pretože $\psi^0(a) = Id_{G(a,\psi)}(a) = a > 0$. Nech $j \in W$, t.j. $\psi^j(a) > 0$. Potom podľa tvrdenia 17 je $\psi(\psi^j(a)) > 0$. Teda $\psi^{j+1}(a) > 0$. Preto $j + 1 \in W$. Z toho matematickou indukciou dostaneme, že $W = Z^+$, a teda (2) je dokázaná.

(3): Nech $x \in G(a, \psi)$. Pretože podľa tvrdenia 12 platí $G(a, \psi) = G_0(a, \psi)$, je $x \in G_0(a, \psi)$. Teda existuje také nezáporné celé číslo k a také celé čísla $p_0, \ldots, p_k$, že $x = \sum_{i=0}^{k} p_i \cdot \psi^i(a)$. Matematickou indukciou v konečnu dokážeme, že pre každé $i = 0, 1, \ldots, k-1$ platí $\psi^i(a) = 2^{k-i} \cdot \psi^k(a)$. Pre $i = k - 1$ platí: $2^{k-(k-1)} \cdot \psi^k(a) = 2 \cdot \psi^k(a) = 2 \cdot \psi(\psi^{k-1}(a)) = \psi^{k-1}(a)$. Nech pre i splňujúce $0 < i \leqq k - 1$ platí $\psi^i(a) = 2^{k-i} \cdot \psi^k(a)$. Potom platí aj $2^{k-(i-1)} \cdot \psi^k(a) = 2^{(k-i)+1} \cdot \psi^k(a) =$

$= 2 \cdot 2^{k-i} \cdot \psi^k(a) = 2 \cdot \psi^i(a) = 2 \cdot \psi(\psi^{i-1}(a)) = \psi^{i-1}(a)$. Tým je dokázané, že $\psi^i(a) = 2^{k-i} \cdot \psi^k(a)$ pre $i = 0, 1, \ldots, k-1$.

Na základe tejto rovnosti môžeme písať: $x = \sum_{i=0}^{k} p_i \cdot \psi^i(a) = \sum_{i=0}^{k} p_i \cdot 2^{k-i} \cdot \psi^k(a) = \left(\sum_{i=0}^{k} 2^{k-i} p_i\right) \cdot \psi^k(a) = p \cdot \psi^k(a)$, kde $p = \sum_{i=0}^{k} 2^{k-i} \cdot p_i$ je celé číslo.

Nech $x > 0$ a $x = p \cdot \psi^k(a)$. Pretože podľa (2) je $\psi^k(a) > 0$, je podľa tvrdenia 6 $p > 0$.

(4): Nech $u \in X$ a $W = \{n \in N\colon 2^n \cdot \psi^n(u) = u\}$. Matematickou indukciou dokážeme, že $W = N$.

$1 \in W$: Pretože $2^1 \cdot \psi(u) = 2 \cdot \psi(u) = u$, je $1 \in W$.

Krok z $j \in W$ vyplýva $j+1 \in W$: Nech $j \in W$, t.j. $2^j \cdot \psi^j(u) = u$. Potom $2^{j+1} \cdot \psi^{j+1}(u) = 2^j(2 \cdot \psi(\psi^j(u))) = 2^j \cdot \psi^j(u) = u$. Teda $j+1 \in W$.

Preto $W = N$ a tvrdenie (4) je dokázané.

Tým je lema 6 dokázaná.

Veta 9. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa, nech ψ je pôlenie na X, nech $a \in X$ a $a > 0$. Nech $G(a, \psi)$ je podgrupa grupy X vytvorená prvkom a a zobrazením ψ. Potom násobenie, ako sme definovali na $G(a, \psi)$, má vlastnosti $(\cdot 1)$, $(\cdot 2)$, $(+\cdot 1)$ a $(\cdot < 1)$.

Dôkaz. Vlastnosť $(\cdot 1)$: Podľa lemy 6 (1) a vety 6 (2) platí $(xy)z = (\chi_z \circ \chi_{xy})(a) = (\chi_z \circ (\chi_y \circ \chi_x))(a) = ((\chi_z \circ \chi_y) \circ \chi_x)(a) = (\chi_{yz} \circ \chi_x)(a) = x(yz)$ pre každé x, y a $z \in G(a, \psi)$.

Vlastnosť $(\cdot 2)$: Podľa vety 6 (1) platí: $xy = (\chi_y \circ \chi_x)(a) = (\chi_x \circ \chi_y)(a) = yx$ pre každé x, $y \in G(a, \psi)$.

Vlastnosť $(+\cdot 1)$: Pre každé x, y a $z \in G(a, \psi)$ platí: $x(y+z) = (y+z) = (\chi_x \circ \chi_{y+z})(a)(\chi_x \circ (\chi_y + \chi_z))(a) = ((\chi_x \circ \chi_y) + (\chi_x \circ \chi_z))(a) = (\chi_x \circ \chi_y)(a) + (\chi_x \circ \chi_z)(a) = yx + zx = xy + xz$. Pritom sme použili lemu 6 (1), vetu 6 (3) a vlastnosť $(\cdot 2)$.

Vlastnosť $(\cdot < 1)$: Nech x, $y \in G(a, \psi)$ a $x > 0$, $y > 0$. Platí: $xy = (\chi_y \circ \chi_x)(a) = \chi_y(\chi_x(a)) = \chi_y(x)$. Keďže $\chi_y(u) = \sum_{i=0}^{n} p_i \cdot \psi^i(y)$, ak $u = \sum_{i=0}^{n} p_i \cdot \psi^i(a)$ a keďže podľa lemy 6 (3) existujú také k a p, že k je nezáporné celé číslo, p je prirodzené číslo a $x = p \cdot \psi^k(a)$, je $xy =$

$=\chi_y(x)=p\cdot\psi^k(y)>0$, pretože $y>0$, a teda aj $\psi^k(y)>0$ a p je prirodzené číslo.

Veta 10. Nech X je úplná lineárne usporiadaná v sebe hustá komutatívna grupa. Potom existuje násobenie na X splňujúce $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$.

Dôkaz. Pretože X je v sebe hustá, existuje aspoň jeden nenulový prvok v X. Nech $u\in X$, $u\neq 0$. Potom podľa (<2) je buď $u<0$, alebo $u>0$. V prvom prípade je $-u>0$. Teda existuje v X kladný prvok.

Nech $a\in X$, $a>0$. Nech ψ je pôlenie na X a nech $G(a,\psi)$ je podgrupa vytvorená prvkom a a zobrazením ψ. Teraz ukážeme, že $G(a,\psi)$ je hustá v X a že násobenie na $G(a,\psi)$, ako sme ho definovali, má vlastnosť (A), t.j. pre každé $x, e\in G(a,\psi)$, $x>0$ a $e>0$ existuje také $h\in G(a,\psi)$, že $0<xh<e$.

$G(a,\psi)$ je hustá v X: Nech $x, y\in X$ a $x<y$. Potom $y-x>0$. Pretože množina $\{n\cdot(y-x)\colon n\in N\}$ je zhora neohraničená, existuje také prirodzené číslo n, že $a<n\cdot(y-x)\ <\ 2^n\cdot(y-x)$. Tvrdím, že $\psi^n(a)<y-x$. Keby totiž $y-x\leqq\psi^n(a)$, platilo by podľa lemy 6 (4), že $a<2^n\cdot(y-x)\leqq$ $\leqq 2^n\cdot\psi^n(a)=a$. To je spor.

Označme znakom $A=\{p\in Z\colon p\cdot\psi^n(a)\leqq x\}$. Množina A je neprázdna. Je totiž množina $\{k\cdot\psi^n(a)\colon k\in N\}$ zhora neohraničená, teda existuje také prirodzené číslo k, že $-x<k\cdot\psi^n(a)$. Ale potom $(-k)\cdot\psi^n(a)<x$, a teda $-k\in A$. Množina A je však aj zhora ohraničená. Totiž existuje také prirodzené číslo r, že $x<r\cdot\psi^n(a)$. Nech $p\in A$. Potom nemôže platiť $r\leqq p$. Pretože v prípade $r\leqq p$ platí $x<r\cdot\psi^n(a)\ \leqq\ p\cdot\psi^n(a)\leqq x$, čo je spor. Teda $p<r$. Keďže p bol ľubovoľný prvok z A, je množina A zhora ohraničená.

Podľa vlastnosti (Z) množiny všetkých celých čísel má množina A maximum. Označme ho q. Potom $q\cdot\psi^n(a)\leqq x$ a $x<(q+1)\cdot\psi^n(a)$. Teda platí $x<(q+1)\cdot\psi^n(a)\ =\ q\cdot\psi^n(a)+\psi^n(a)\ <\ x+(y-x)=y$. Keďže $(q+1)\cdot\psi^n(a)\in G(a,\psi)$, existuje také $z\in G(a,\psi)$, že $x<z<y$ (napr. $z=(q+1)\cdot\psi^n(a)$).

Keďže množina $\{n\cdot a\colon n\in N\}$ je zhora neohraničená, existujú také prirodzené čísla m a p, že $y<m\cdot a$ a $-x<p\cdot a$. Z toho dostaneme, že $m\cdot a$, $(-p)\cdot a\in G(a,\psi)$ a $(-p)\cdot a<x<y<m\cdot a$.

Tým sme dokázali, že $G(a,\psi)$ je hustá v X.

Násobenie na $G(a,\psi)$ má vlastnosť (A): Nech $x, e\in G(a,\psi)$, $x>0$,

$e>0$. Pretože množina $\{n \cdot e: n \in N\}$ je zhora neohraničená, existuje také prirodzené číslo k, že $x<k \cdot e<2^k \cdot e$. Potom musí platiť $\psi^k(x)<e$. Keby totiž bolo $e \leqq \psi^k(x)$, platilo by $2^k \cdot e \leqq 2^k \cdot \psi^k(x) = x<2^k \cdot e$, čo je spor. Voľme $h=\psi^k(a)$. Potom podľa lemy 6 (2) je $h>0$. Teda $0<xh = hx = (\chi_x \circ \chi_h)(a) = \chi_x(\chi_h(a)) = \chi_x(h) = \psi^k(x)<e$.

Pretože násobenie na $G(a, \psi)$ podľa vety 9 splňuje $(\cdot 1)$, $(\cdot 2)$, $(+\cdot 1)$ a $(\cdot <1)$ a má vlastnosť (A) a pretože $G(a, \psi)$ je hustá v X, existuje podľa vety 7 na X násobenie, ktoré splňuje $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$.

Veta 11. Úplná lineárne usporiadaná v sebe hustá komutatívna grupa X je pri násobení z vety 10 množinou všetkých reálnych čísel.

Dôkaz. Pretože súčet a usporiadanie na X splňujú axiómy $(+1)$, $(+2)$, $(+3)$, (<1), (<2), $(+<1)$ a (<3), a pretože násobenie z vety 10 splňuje axiómy $(\cdot 1)$, $(\cdot 2)$, $(\cdot 3)$, $(+\cdot 1)$ a $(\cdot <1)$ sú všetky axiómy množiny všetkých reálnych čísel splnené. Ak ukážeme, že každá úplná lineárne usporiadaná v sebe hustá komutatívna grupa je nekonečná, bude veta 11 dokázaná.

Na začiatku dôkazu vety 10 sme ukázali, že v úplnej lineárne usporiadanej v sebe hustej komutatívnej grupe X existuje aspoň jeden prvok väčší ako 0. Nech $a \in X$, $a>0$. Podľa lemy 3 (1) je množina $\{n \cdot a: n \in N\}$ zhora neohraničená, a preto musí byť nekonečná. Keďže $\{n \cdot a: n \in N\} \subset X$, je X nekonečná.

Túto tretiu časť skončíme jednou poznámkou. Vlastnosť (<3) sa často nahradzuje inými ekvivalentnými vlastnosťami. Spomenieme jednu z nich formulovanú v pojmoch Dedekindových rezov.

Lineárne usporiadanou množinou rozumieme množinu, na ktorej je definované usporiadanie, ktoré splňuje (<1) a (<2). Dvojicu (A, B) podmnožín množiny X nazývame rezom lineárne usporiadanej množiny X, ak pre ňu platí: $A \neq \emptyset$, $B \neq \emptyset$, $X=A \cup B$ a pre každé $a \in A$ a každé $b \in B$ platí $a<b$.

Nech C je podmnožina lineárne usporiadanej množiny X, potom hovoríme, že C má maximum, resp. minimum, ak existuje taký prvok $c \in C$, že $x \leqq c$, resp. $c \leqq x$ pre každé $x \in C$.

Rez (A, B) lineárne usporiadanej množiny X nazývame skokom, ak A má maximum a B má minimum; rez (A, B) nazývame medzerou, ak A nemá maximum a B nemá minimum. Rez (A, B) lineárne usporiadanej množiny X nazývame Dedekindovým rezom, ak buď A má maximum a B

nemá minimum, alebo A nemá maximum a B má minimum. Ľahko sa vidí, že každý rez lineárne usporiadanej množiny môže byť len alebo skokom, alebo medzerou príp. Dedekindovým rezom.

Dá sa pomerne ľahko dokázať, že množina všetkých reálnych čísel, ako sme ju definovali, má nasledovnú vlastnosť vyjadrenú pomocou rezov:

($<3^*$) Každý rez množiny všetkých reálnych čísel je Dedekindovým rezom.

Ak máme nekonečnú množinu X, v ktorej sú definované operácie súčtu a súčinu a relácia usporiadania, pričom sú splnené všetky axiómy množiny všetkých reálnych čísel až na vlastnosť (<3), namiesto ktorej je splnená vlastnosť ($<3^*$), dá sa dokázať, že v tomto prípade usporiadanie splňuje aj vlastnosť (<3).

Preto čitateľ sa môže stretnúť s takou definíciou množiny všetkých reálnych čísel, v ktorej namiesto axiómy (<3) je uvedená axióma ($<3^*$), ktorá je formulovaná pomocou rezov.

Literatúra

1. Bruijn, N. G. de: Defining reals without the use of rationals, Proc. of the Koninklijke Nederl. Akad. Wettensch. S. A. Math. Sc. 79 (1976), 100—108.
2. Legéň, A.: O grupách a okruhoch, I., II., Matematické obzory, zväzok 4 (1973), 27—46 a zväzok 5 (1974), 21—38. Bratislava, Alfa 1973, 1974.
3. Mišík, L.: Netradičná konštrukcia reálnych čísel, I., II., zväzok 14 (1979) a zväzok 15 (1980). Bratislava, Alfa 1979 a 1980.