Karel Koutský; Milan Sekanina

Rozklad přímky na shodné trojbodové množiny

Časopis pro pěstování matematiky, Vol. 83 (1958), No. 3, 317–326

Persistent URL: http://dml.cz/dmlcz/108293

Časopis pro pěstování matematiky, roč. 83 (1958), Praha

ROZKLAD PŘÍMKY NA SHODNÉ TROJBODOVÉ MNOŽINY

KAREL KOUTSKÝ a MILAN SEKANINA (Brno)

Došlo dne 10. července 1957

DT: 513.832
519.52

V článku je ukázáno, že každá trojbodová podmnožina přímky je její rozkladovou množinou.

I

Přímou shodnost podmnožin z eukleidovského prostoru E_n (zprostředkovanou eukleidovským pohybem 1. druhu) značíme symbolem $\dot{\cong}$, shodnost $\cong$.

1.1. (definice). *Budiž E_n n-rozměrný eukleidovský prostor a množina $M \subset E_n$. Řekneme, že M je rozkladová množina prostoru E_n, když existuje rozklad $\boldsymbol{R}$ na E_n*[1]*) takový, že*

$$A \in \boldsymbol{R} \Rightarrow A \cong M .$$

Rozklad $\boldsymbol{R}$ budeme značit podrobněji $\boldsymbol{R}$ $(M, \cong)$. Je-li dokonce pro jisté $\boldsymbol{R}$

$$A \in \boldsymbol{R} \Rightarrow A \dot{\cong} M ,$$

potom M nazýváme přímou rozkladovou množinou prostoru E_n a příslušný rozklad značíme podrobněji $\boldsymbol{R}(M, \dot{\cong})$.

1.2. (definice). *Budiž $\mathfrak{G}$ grupa eukleidovských pohybů v E_n. Budiž $M \subset E_n$ s těmito vlastnostmi:*

1. $x, y \in M, \quad \sigma \in \mathfrak{G}, \ \sigma(x) = y \Rightarrow x = y.$
2. $y \in E_n \Rightarrow$ *existuje* $x \in M$ *a* $\sigma \in \mathfrak{G}$ *tak, že* $\sigma(x) = y$.

Potom M nazýváme fundamentální množinou grupy $\mathfrak{G}$.

1.3. (definice). *Nechť $\mathfrak{E}_n$ značí grupu všech eukleidovských pohybů v E_n. Nechť je dán na E_n rozklad $\boldsymbol{R}(M, \cong)$, kde $M \subset E_n$. Nechť $\sigma \in \mathfrak{E}_n$. Řekneme, že σ je zákrytovým pohybem na $\boldsymbol{R}(M, \cong)$, když*

$$A \in \boldsymbol{R} \Rightarrow \sigma(A) \in \boldsymbol{R} .$$

1.4. (lemma). *Budiž $\boldsymbol{R}(M, \cong)$ rozklad na E_n, $M \subset E_n$. Potom množina všech zákrytových pohybů na $\boldsymbol{R}(M, \cong)$ tvoří grupu (grupovou operací je skládání zobrazení).*

[1]) Definici rozkladu na množině viz např. v [1], str. 14.

Důkaz je zřejmý.

1.5. (definice). *Budiž* $\boldsymbol{R}(M, \cong)$ *rozklad na* E_n, $M \subset E_n$. *Grupu všech zákrytových pohybů na* $\boldsymbol{R}(M, \cong)$ *nazveme totální zákrytovou grupou na* $\boldsymbol{R}(M, \cong)$ *a budeme ji značit* $\mathfrak{G}_R$.

1.6. (definice). *Budiž* $\boldsymbol{R}(M, \cong)$ *rozklad na* E_n, $M \subset E_n$, $\mathfrak{G}$ *podgrupa v* $\mathfrak{G}_R$. *Je-li každá množina* $A \in \boldsymbol{R}$ *fundamentální množinou grupy* $\mathfrak{G}$, *nazveme* $\mathfrak{G}$ *fundamentální zákrytovou grupou na* $\boldsymbol{R}(M, \cong)$.

V dalším se zabýváme prostorem E_1, který považujeme za číselnou osu. Připomeňme, že na E_1 přímou shodností je translace, shodnost je buďto translací nebo symetrií.

II

Bezprostředně se nahlédne, že každá dvoubodová podmnožina přímky je její přímou rozkladovou množinou. Budiž nyní $M = \{x, y, z\} \subset E_1$, $x < y < z$. Bez újmy na obecnosti můžeme položit $x = 0$. Dále rozlišme dva případy:

a) y a z jsou racionálně závislé, tj. existují celá čísla m, n, $m \neq 0 \neq n$, tak, že $n \,.\, y = m \,.\, z$.

b) y a z nejsou racionálně závislá čísla.

Ad a) Nechť $n \,.\, y = m \,.\, z$, n, m celá čísla, $n \neq 0 \neq m$. Můžeme zřejmě předpokládat, že m a n jsou nesoudělná. Zaveďme na E_1 souřadnicový systém tak, aby $\frac{y}{m}$ byl jednotkový bod. Trojice M v tomto novém systému má tvar $\{0, m, n\}$. Odsud plyne, že se v tomto případě stačí omezit na množiny tvaru $\{0, m, n\}$, kde m, n jsou celá nesoudělná čísla, $0 < m < n$.

Ad b) Nechť y a z nejsou racionálně závislá čísla. Podobnou úvahou jako v odstavci ad a) zjistíme, že se stačí omezit na množiny tvaru $\{0, 1, \alpha\}$, $1 < \alpha$, α iracionální.

2.1. (věta). *Nechť* $M = \{0, m, n\}$, $0 < m < n$, m, n *reálná čísla. Nechť existuje* $\boldsymbol{R}(M, \dot{\cong})$. *Potom translace*

$$\varrho(x) = x + m + n, \ x \in E_1, \ \sigma(x) = x + m - 2n, \ x \in E_1,$$

jsou zákrytovými pohyby na $\boldsymbol{R}(M, \dot{\cong})$.

Důkaz. Nechť $M' \in \boldsymbol{R}(M, \dot{\cong})$. Potom existuje $z \in E_1$ tak, že $M' = \{z, z + m, z + n\}$.

a) Uvažujme o bodu $z + m + n$. Existuje $Z \in \boldsymbol{R}(M, \dot{\cong})$ a translace ϱ' tak, že $z + m + n \in Z$, $\varrho'(M') = Z$.

Protože

$\varrho'(z + m) = z + m + n \Rightarrow M' \neq Z$, $\varrho'(z) = z + n \Rightarrow Z \cap M' \neq \emptyset$, což je spor,
$\varrho'(z + n) = z + m + n \Rightarrow M' \neq Z$, $\varrho'(z) = z + m \Rightarrow Z \cap M' \neq \emptyset$, což je spor,
jest $\varrho'(z) = z + m + n$ a tedy $\varrho' = \varrho$.

b) Uvažujme o bodu $z + m - n$. Existuje $X \in \boldsymbol{R}(M, \doteqdot)$ a translace σ' tak, že $z + m - n \in X$, $\sigma'(M') = X$. Obdobně jako v části a) se ukáže, že $\sigma'(z + n) = z + m - n$, tedy $\sigma' = \sigma$. Tím je věta dokázána.

2.2. (věta). *Budiž $M = \{0, m, n\}$, kde m, n jsou celá nesoudělná čísla, $0 < m < n$. Potom M je přímou rozkladovou množinou prostoru E_1 právě tehdy, když $0, m, n$ jsou vzájemně nekongruentní* mod 3.[2])

Důkaz. Předpokládejme, že $0, m, n$ jsou vzájemně nekongruentní mod 3. Definujme relaci ϱ_1 na E_1 takto: $x, y \in E_1$, $x \varrho_1 y \Leftrightarrow x - y$ je celé číslo. Relace ϱ_1 je zřejmě ekvivalence. Nechť N je množina representantů z jednotlivých tříd ekvivalence ϱ_1[3]) Definujme systém P takto:

$$M' \in P \Leftrightarrow M' = \{x, x + m, x + n\},\ x \in E_1,\ x - z_x \equiv 0 \pmod 3\,,$$

kde $z_x \in N$, $z_x \varrho_1 x$.

Ukážeme, že P je rozklad na E_1 v množiny přímo shodné s M.

1. $M' \in P \Rightarrow M' \doteqdot M$, plyne ihned z definice P,
2. $M', M'' \in P$, $M' \neq M'' \Rightarrow M' \cap M'' = \emptyset$.

Toto tvrzení dokážeme takto: Nechť

$$M' = \{x, x + m, x + n\}\,, \quad M'' = \{y, y + m, y + n\}\,,$$

kde $x, y \in E_1$, $M' \neq M''$.

Nechť x non $\varrho_1 y$. Potom z definice ϱ_1 plyne, že $M' \cap M'' = \emptyset$. Nechť $x \varrho_1 y$. Protože podle předpokladu je $M' \neq M''$, je třeba uvažovat pouze o rovnostech $x = y + m$, $x + m = y + n$, $x = y + n$ a o rovnostech, které vzniknou

---

[2]) Otázky, týkající se rozkladu přímky na množiny přímo shodné, lze formulovati v pojmech faktorisace grupy reálných čísel R. Nechť totiž $\{M_0, M_1, \ldots, M_j, \ldots\}$ je rozklad přímky, kterou považujeme za číselnou osu, na množiny přímo shodné, tedy $M_j \doteqdot M_0$. Nechť t_j je libovolně, ale pevně zvolené číslo takové, že $\underset{x}{\mathrm{E}}[x = y + t_j,\ y \in M_0] = M_j$.
Označme $S_1 = M_0$, $S_2 = \{t_0, t_1, \ldots, t_j, \ldots\}$. Každé reálné číslo se dá psát právě jedním způsobem jako $a + b$, $a \in S_1$, $b \in S_2$. Píšeme $R = S_1 + S_2$. Obdobná poznámka platí pro množinu C všech celých čísel. V článku [5] na str. 240 je vyslovena tato domněnka:
Nechť C značí množinu všech celých čísel, p nechť je prvočíslo. Nechť S_1 je množina p celých čísel, $0 \in S_1$ a čísla z S_1 mají za největšího společného dělitele 1. Nechť $C = S_1 + S_2$, $0 \in S_2$. Potom S_2 je množinou všech násobků p a S_1 je úplný systém zbytků mod p.
V témže článku je pomocí jistých vlastností polynomů dokázána druhá část této domněnky. Ve větě 2.2 je podán elementární důkaz druhé části domněnky pro $p = 3$. Zároveň z rovnic (2.1), (2.4), (2.5) vyplývá platnost i prvého tvrzení v tomto případě. Je totiž největší společný dělitel čísel $m - 2n$ a $m + n$ roven 3. Rozkladem množiny celých čísel na přímo shodné množiny o r číslech se bude zabývat článek prof. K. Koutského. (Pozn.: Během recense vyšel článek [6], ve kterém je uvedená domněnka dokázána.)

[3]) Např. $N = \langle 0, 1)$.

z nich záměnou x za y. Každá z těchto rovností je však ve sporu s předpokladem, že $0, m, n$ jsou čísla nekongruentní mod 3. Tedy $M' \cap M'' = \emptyset$.

3. $x \in E_1 \Rightarrow$ existuje $M' \in P$ tak, že $x \in M'$.

Tvrzení toto plyne z následujících implikací:

a) $x - z_a \equiv 0 \pmod 3 \Rightarrow \{x, x + m, x + n\} \in P$.

b) $x - z_x \equiv m \pmod 3 \Rightarrow \{x - m, x, x + n - m\} \in P$.

c) $x - z_x \equiv n \pmod 3 \Rightarrow \{x - n, x - n + m, x\} \in P$.

Tvrzení 1 až 3 ukazují, že P je žádaný rozklad na E_1. Tím je dostatečnost podmínky z věty 2.2 dokázána.

Nechť nyní $M = \{0, m, n\}$, $(m, n) = 1$, je trojice, v níž $0, m, n$ nejsou vzájemně nekongruentní mod 3. Pak je to trojice jednoho z následujících typů

$$\{0, 3m', 3n' + 2\}, \tag{I}$$

$$\{0, 3m' + 2, 3n' + 2\}, \tag{II}$$

$$\{0, 3m', 3n' + 1\}, \tag{III}$$

$$\{0, 3m' + 1, 3n' + 1\}, \tag{IV}$$

$$\{0, 3m' + 1, 3n'\}, \tag{V}$$

$$\{0, 3m' + 2, 3n'\}, \tag{VI}$$

kde m', n' jsou vhodná nezáporná celá čísla. Potom rovnice

$$k_1(m - 2n) + k_2(m + n) = k \tag{2.1}$$

má řešení v celých číslech k_1 a k_2 pro každé celé k. K důkazu tohoto tvrzení stačí ukázat, že největší společný dělitel l čísel $m - 2n$ a $m + n$ je 1. Nechť

$$m - 2n = l \, . \, d_1 \,, \tag{2.2}$$

$$n + m = l \, . \, d_2 \,. \tag{2.3}$$

kde d_1 a d_2 jsou nesoudělná čísla.

Z (2.2) a (2.3) plyne

$$-3n = l \, . \, (d_1 - d_2) \,, \tag{2.4}$$

$$3m = l \, . \, (d_1 + 2d_2) \,. \tag{2.5}$$

Počtem se snadno zjistí, že pro dvojice m, n z typů (I)—(IV) je největší společný dělitel $(l, 3) = 1$. Tedy $l \mid (m, n)$, odkud $l = 1$.

Připusťme, že existuje $\boldsymbol{R}(M, \doteq)$ na E_1. Podle 2.1 jsou translace $\varrho(x) = x + m + n$, $\sigma(x) = x + m - 2n$, $x \in E_1$, zákrytovými pohyby na $\boldsymbol{R}(M, \doteq)$. Nechť $M' = \{z, z + m, z + n\} \in \boldsymbol{R}(M, \doteq)$. Existují celá čísla m_1 a m_2 tak, že

$$m_1(m - 2n) + m_2(n + m) = m \,.$$

Potom je $M'' = \sigma^{m_1}\varrho^{m_2}(M') \in \boldsymbol{R}(M, \doteq)$, $M'' \neq M'$, $\sigma^{m_1}\varrho^{m_2}(z) = z + m$, odkud plyne $M'' \cap M' \neq \emptyset$, což je spor. Tím je dokázána nutnost uvedené podmínky.

Podobně jako prvá část věty 2.2 se dokáže

2.3. (věta). *Budiž M množina n celých čísel, které patří do různých zbytkových tříd* mod n. *Potom M je přímou rozkladovou množinou prostoru E_1.*

2.4. (věta). *Budiž $M = \{0, m, n\}$, m, n celá nesoudělná čísla, $0 < m < n$. Potom M je rozkladovou množinou prostoru E_1.*

Důkaz. Jsou-li čísla $0, m, n$ navzájem nekongruentní mod 3, platí věta podle 2.2. Dále se stačí omezit na typy II, IV, V, VI z důkazu věty 2.2, neboť případ typu I (resp. III) se převede na typ II (resp. IV) úvahou o množině $M' = \{0, n - m, n\}$ místo o množině M. Je $M \cong M'$.

a) Nechť v $M = \{0, m, n\}$ je $0 \equiv n \pmod{2^l . 3}$, $0 \not\equiv n \pmod{2^{l+1} . 3}$, l celé nezáporné číslo.

Položme $k_j = \left(j + \left[\frac{j+1}{2}\right]\right) m$ pro $j = 0, 1, \ldots, 2^{l+1} - 1$. Pro j sudé nechť

$$M_j = \{k_j, k_j + m, k_j + n\} .$$

Pro j liché nechť

$$M_j = \{k_j, k_j + n - m, k_j + n\} .$$

Ukážeme, že čísla obsažená v $\bigcup_{j=0}^{2^{l+1}-1} M_j$ jsou navzájem nekongruentní mod $2^{l+1} . 3$ a že je jich právě $2^{l+1} . 3$. Snadno se vidí, že při zkoumání nekongruentnosti se stačí omezit na dvojice čísel, incidentní s dvěma různými množinami M_j. Kvůli stručnosti označme $2^{l+1} . 3 = L$, $2^l . 3 = I$.

Z podmínky $(m, n) = 1$ a z předpokladu $0 \equiv n \pmod{I}$ plyne, že $(m, I) = 1$ a tedy čísla $0, m, 2m, \ldots, (I - 1) m$ jsou vzájemně nekongruentní mod I. Nyní pro $j = 0, 1, \ldots, 2^{l+1} - 1$ je

$$j + \left[\frac{j+1}{2}\right] \leqq 2^{l+1} - 1 + 2^l < 2^l . 3 = I .$$

Odtud plyne, že $k_h \not\equiv k_g \pmod{I}$ pro $h \neq g$.

1. Nechť g a h jsou sudá čísla, $g \neq h$. Připusťme, že pro $x \in M_g$, $y \in M_h$ je $x \equiv y \pmod{L}$. Platí pak jeden z následujících vztahů nebo ze vztahů z těchto vzniklých záměnou g za h: $k_g \equiv k_h \pmod{L} \Rightarrow k_g \equiv k_h \pmod{I}$; $k_g \equiv k_h + m \pmod{L} \Rightarrow K . m \equiv 0 \pmod{I}$, $0 < K < I$; $k_g \equiv k_h + n \pmod{L} \Rightarrow k_g \equiv k_h \pmod{I}$; $k_g + m \equiv k_h + n \pmod{L} \Rightarrow K . m \equiv 0 \pmod{I}$, $0 < K < I$. Ve všech případech jsme dospěli ke sporu se shora uvedenou vlastností čísel k_h, resp. se vztahem $K . m \not\equiv 0 \pmod{I}$ pro $K = 1, \ldots, I - 1$.

2. Případ, že g a h jsou lichá čísla, $g \neq h$, je naprosto analogický případu 1.

3. Nechť h je sudé, g liché číslo, $M_h = \{k_h, k_h + m, k_h + n\}$, $M_g = \{k_g, k_g + n - m, k_g + n\}$. Připusťme, že pro $x \in M_g$, $y \in M_h$ platí $x \equiv y \pmod{L}$.

Nejprve se zabývejme případem, kdy $x = k_g + n - m$, $y = k_h + m$. Je-li $h \neq g - 1$, potom z kongruence $k_g + n - m \equiv k_h + m \pmod{L}$ plyne $K \cdot m \equiv 0 \pmod{I}$, $0 < K < I$, což je spor. Je-li $h = g - 1$, potom uvedená kongruence podle definice čísel k_g a k_h vede na vztah $n \equiv 0 \pmod{L}$, což je spor s předpokladem o čísle n.

V ostatních případech dospějeme ke sporu jako v odstavci 1.

b) Nechť v $M = \{0, m, n\}$ je $m \equiv n \pmod{3}$, $m \not\equiv n \pmod{6}$. Odsud plyne, že čísla m a n jsou různé parity. Zvolme k celé tak, že $0 \not\equiv k \not\equiv m \pmod{3}$ a k je téže parity jako m. Potom ukážeme, že čísla

$$0, m, n\,, \tag{2.6}$$

$$k, k + n - m,\ k + n \tag{2.7}$$

jsou navzájem nekongruentní mod 6. Z předpokladu o n a m se ihned vidí, že čísla v (2.6), resp. v (2.7) jsou vzájemně nekongruentní mod 6. Stačí tedy vyšetřovat, zda jsou kongruentní dvojice incidentní s (2.6) i (2.7).

Připusťme, že existují čísla x a y, při čemž x je z množiny (2.6), y z množiny (2.7), taková, že $x \equiv y \pmod{6}$. Vyšetříme nejdříve případ $x = 0$, $y = k + n$. Potom z kongruence $0 \equiv k + n \pmod{6}$ plyne, že $2 \mid k + n$, což je spor s volbou čísla k. V ostatních případech dojdeme ze vztahu $x \equiv y \pmod{6}$ ihned ke sporu s předpokladem, že čísla $0, m, k$ jsou nekongruentní mod 3.

c) Nechť v $M = \{0, m, n\}$ je $m \equiv n \pmod{2^l \cdot 3}$, $m \not\equiv n \pmod{2^{l+1} \cdot 3}$, $l \geqq 1$ celé. Položme

$$k_j = \left(j + \left[\frac{j+1}{2}\right]\right) m \text{ pro } j = 0, 1, \ldots, 2^{l+1} - 2\,,$$

$$k_j = \left(j + \left[\frac{j+1}{2}\right]\right) n \text{ pro } j = 2^{l+1} - 1\,.$$

Položme jako dříve $2^{l+1} \cdot 3 = L$, $2^l \cdot 3 = I$. Sestrojme jako v odstavci a) množiny M_j pro $j = 0, 1, \ldots, 2^{l+1} - 1$. Ukážeme, že čísla z $\bigcup_{j=0}^{2^{l+1}-1} M_j$ jsou navzájem nekongruentní mod L. Opět je $(m, I) = 1$ a $k_h \not\equiv k_g \pmod{I}$ pro $g \neq h$. Nechť $0 \leqq g \neq h \leqq 2^{l+1} - 1$. Připusťme, že existují čísla $x \in M_g$ a $y \in M_h$ tak, že $x \equiv y \pmod{L}$. Jsou-li g i h téže parity, je situace naprosto analogická jako v odstavci a). Je-li g liché číslo a h sudé číslo, potom případy různé od případu, kdy $x = k_h$, $y = k_g + n$, vedou na úvahu jako v odstavci a) 1. Nechť tedy $x = k_h$, $y = k_g + n$. α) Nechť $h = g + 1$. Potom z kongruence $k_h \equiv k_g + n \pmod{L}$ plyne $m \equiv n \pmod{L}$, což je spor s předpokladem o číslech m a n. β) Nechť $g = 2^{l+1} - 1$, $h = 0$. Potom je $0 \equiv I \cdot n \pmod{L}$, odkud $2 \mid n$, což je spor, neboť n je liché číslo, jak plyne z kongruence $m \equiv n \pmod{I}$, $(m, n) = 1$. γ) V ostatních případech z kongruence $k_h \equiv k_g + n \pmod{L}$ plyne $K \cdot m \equiv 0 \pmod{I}$, $0 < K < I$, což je spor s tím, že čísla $0, m, \ldots$ $\ldots, (I - 1)\, m$ jsou nekongruentní $\pmod{I}$.

Je tedy podle věty 2.3 v případě a) i c) množina $\bigcup_{j=0}^{2^{l+1}-1} M_j$ přímou rozkladovou množinou prostoru E_1 a rovněž sjednocení množin (2.6) a (2.7) je přímou rozkladovou množinou E_1. Poněvadž M je zřejmě rozkladovou množinou množiny $\bigcup_{j=0}^{2^{l+1}-1} M_j$ resp. sjednocení (2.6) a (2.7), je M rozkladovou množinou přímky ve všech třech případech. Poněvadž případ a) zahrnuje typy V a VI, případy b) a c) typy II a IV, je tím důkaz dokončen.

III

Nechť je dána množina $\{0, 1, \alpha\}$, $1 < \alpha$, α irracionální. Nechť $x \in E_1$ a nechť $\mathfrak{T}(x)$ značí systém všech trojic tvaru

$$\{r(\alpha + 1) + 3s + x,\ r(\alpha + 1) + 3s + x + 1,\ r(\alpha + 1) + 3s + x + \alpha\},$$

kde r, s jsou celá čísla.

3.1. (lemma). a) *Čísla obsažená v každé trojici systému $\mathfrak{T}(x)$ jsou vesměs různá.*

b) *Každé dvě různé trojice z $\mathfrak{T}(x)$ jsou disjunktní.*

Důkaz. Tvrzení a) je zřejmé, tvrzení b) se dokáže snadno porovnáním prvků z jednotlivých trojic z toho, že α je iracionální.

Označme nyní $\mathfrak{M}(x) = \bigcup_{M' \in \mathfrak{T}(x)} M'$.

3.2. (lemma). $y, x \in E_1$, $y \in \mathfrak{M}(x) \Rightarrow \mathfrak{M}(x) = \mathfrak{M}(y)$.

Důkaz. Nechť $y \in \mathfrak{M}(x)$. Pak y má jeden z následujících tvarů:

$$y = r(\alpha + 1) + 3s + x\,,\quad y = r(\alpha + 1) + 3s + x + 1\,,$$
$$y = r(\alpha + 1) + 3s + x + \alpha\,.$$

Ukážeme, že $x \in \mathfrak{M}(y)$. Je

$$y = r(\alpha + 1) + 3s + x \Rightarrow y - r(\alpha + 1) - 3s = x \in \mathfrak{M}(y)\,,$$
$$y = r(\alpha + 1) + 3s + x + 1 \Rightarrow y - r(\alpha + 1) - 3s - 1 = x \Rightarrow (-r - 1)\,.$$
$$.\,(\alpha + 1) + \alpha + 1 - 3s - 1 + y = x \in \mathfrak{M}(y)\,,$$
$$y = r(\alpha + 1) + 3s + \alpha + x \Rightarrow y - r(\alpha + 1) - 3s - \alpha = y - (r + 1)\,.$$
$$.\,(\alpha + 1) + \alpha + 1 - 3s - \alpha = x \in \mathfrak{M}(y)\,.$$

Tedy $x \in \mathfrak{M}(y)$.

Buď nyní $z \in \mathfrak{M}(y)$. Potom z má jeden z následujících tvarů:

$$z = r'(\alpha + 1) + 3s' + y\,,\quad z = r'(\alpha + 1) + 3s' + y + 1\,,$$
$$z = r'(\alpha + 1) + 3s' + y + \alpha\,.$$

Je

$$z = r'(\alpha + 1) + 3s' + r(\alpha + 1) + 3s + x \in \mathfrak{M}(x)\,,$$
$$z = r'(\alpha + 1) + 3s' + r(\alpha + 1) + 3s + x + 1 \in \mathfrak{M}(x)\,,$$
$$z = r'(\alpha + 1) + 3s' + r(\alpha + 1) + 3s + x + \alpha \in \mathfrak{M}(x)\,,$$
$$z = r'(\alpha + 1) + 3s' + 1 + r(\alpha + 1) + 3s + x \in \mathfrak{M}(x)\,,$$

$$z = r'(\alpha + 1) + 3s' + 1 + r(\alpha + 1) + 3s + x + 1 = (r' + r - 1)(\alpha + 1) + \\ + \alpha + 3(s' + s + 1) + x \in \mathfrak{M}(x),$$
$$z = r'(\alpha + 1) + 3s' + 1 + r(\alpha + 1) + 3s + x + \alpha = (r' + r + 1)(\alpha + 1) + \\ + 3(s + s') + x \in \mathfrak{M}(x),$$
$$z = r'(\alpha + 1) + 3s' + \alpha + r(\alpha + 1) + 3s + x \in \mathfrak{M}(x),$$
$$z = r'(\alpha + 1) + 3s' + \alpha + r(\alpha + 1) + 3s + x + 1 \in \mathfrak{M}(x),$$
$$z = r'(\alpha + 1) + 3s' + \alpha + r(\alpha + 1) + 3s + x + \alpha = (r' + r + 2)(\alpha + 1) + \\ + 3(s + s' - 1) + 1 + x \in \mathfrak{M}(x).$$

Tedy $z \in \mathfrak{M}(y) \Rightarrow z \in \mathfrak{M}(x)$. Obdobně se dokáže $z \in \mathfrak{M}(x) \Rightarrow z \in \mathfrak{M}(y)$, takže $\mathfrak{M}(x) = \mathfrak{M}(y)$, c. b. d.

Řekněme, že $x \in E_1$ je v relaci ϱ_2 s $y \in E_1$, právě když $\mathfrak{M}(x) = \mathfrak{M}(y)$. Relace ϱ_2 je zřejmě ekvivalence; nechť N je množina representantů tříd příslušných k relaci ϱ_2.[4]) Potom platí

3.3. (věta). *Systém trojic* $\bigcup_{x \in N} \mathfrak{T}(x)$ *je rozkladem na* E_1 *na trojice přímo shodné s* $M = \{0, 1, \alpha\}$.

Důkaz. Nechť $M' \in \bigcup_{x \in N} \mathfrak{T}(x)$. Potom zřejmě $M' \doteq M$. Nechť $y \in E_1$. Potom existuje $x \in N$ tak, že $y \varrho_2 x$ a tedy $y \in \mathfrak{M}(x)$. Nechť $M_1, M_2 \in \bigcup_{x \in N} \mathfrak{T}(x)$, $M_1 \neq M_2$. Existují $x_1, x_2 \in N$ tak, že $M_1 \in \mathfrak{T}(x_1)$, $M_2 \in \mathfrak{T}(x_2)$.

1. $x_1 = x_2 \Rightarrow M_1 \cap M_2 = \emptyset$ podle 3.1,
2. $x_1 \neq x_2 \Rightarrow x_1$ non $\varrho_2 x_2 \Rightarrow \mathfrak{M}(x_1) \Rightarrow \mathfrak{M}(x_2) = \emptyset$ (podle 3.2).

Proto i $M_1 \cap M_2 = \emptyset$. Tím je 3.3 dokázáno.

Spojením výsledků 2.4 a 3.4 dostáváme následující tvrzení:

Každá trojbodová množina $M \subset E$ *je rozkladovou množinou na* E_1.

Poznamenejme, že věta neplatí již pro čtyřbodové množiny, jak je vidět na množině $\{0, 1, 3, 4\}$.

IV

4.1. (věta). *Budiž* $\mathfrak{G}$ *podgrupa v* $\mathfrak{E}_1$. *Nechť* $N \subset E_1$ *je fundamentální množina grupy* $\mathfrak{G}$. *Potom buď* $\overline{\overline{N}} = 1$ *nebo* $N \geqq \aleph_0$.[5])

Důkaz. E_1 považujeme za číselnou osu. Nechť nejprve $\mathfrak{G}$ obsahuje jen translace. Grupa všech translací na přímce je isomorfní s additivní grupou všech reálných čísel. Additivní grupa všech reálných čísel je úplná, její vlastní podgrupy mají index větší nebo roven $\aleph_0$ (definici a základní vlastnosti úplných grup viz např. v [2], str. 147). Nechť $\mathfrak{G}'$ je množina délek translací

[4]) Poněvadž, jak se snadno ukáže, množina $\mathfrak{M}(x)$ je hustá v E_1, není možno obejít zde axiom výběru způsobem, jak bylo poznamenáno v pozn. 3).

[5]) Za zkrácení důkazu děkují autoři dr. F. Šikovi.

z $\mathfrak{G}$; $\mathfrak{G}'$ tvoří additivní grupu isomorfní s $\mathfrak{G}$. Z definice fundamentální množiny plyne, že $\bigcup_{a \in N} \{\mathfrak{G}' + a\} = E_1$, $\{\mathfrak{G}' + a\} \cap \{\mathfrak{G}' + b\} = \emptyset$ pro a, $b \in N$, $a \neq b$, $\{\mathfrak{G}' + a\} = \underset{x}{\mathrm{E}}[x = g + a, g \in \mathfrak{G}']$. Tedy index grupy $\mathfrak{G}$ v grupě všech translací je roven právě $\overline{\overline{N}}$, tedy $\overline{\overline{N}} = 1$ nebo $\overline{\overline{N}} \geqq \aleph_0$.

Nechť nyní $\sigma \in \mathfrak{G}$ je symetrie. Nechť $\mathfrak{G}_1$ je množina všech translací z $\mathfrak{G}$. Ukážeme, že $E_1 = \bigcup_{\gamma \in \mathfrak{G}_1} \gamma[N \cup \sigma(N)]$ ($\gamma[N \cup \sigma(N)]$ je obraz množiny $N \cup \sigma(N)$ v zobrazení γ). Ke každému reálnému číslu c existuje $c_1 \in N$, $\tau \in \mathfrak{G}$ tak, že $\tau(c_1) = c$. Je-li τ nepřímý pohyb, je $\tau = \tau_1\sigma$, kde $\tau_1 \in \mathfrak{G}_1$, tedy $\tau(c_1) = \tau_1[\sigma(c_1)] = c$. Existuje tedy $N_1 \subset N \cup \sigma(N)$ tak, že N_1 je fundamentální množinou grupy $\mathfrak{G}_1$. Podle prvé části důkazu je $\overline{\overline{N}}_1 = 1$ nebo $\overline{\overline{N}}_1 \geqq \aleph_0$. Je-li $\overline{\overline{N}}_1 = 1$, je $\mathfrak{G}_1$ transitivní grupa, tedy i $\mathfrak{G}$ a odtud $\overline{\overline{N}} = 1$. Je-li $\overline{\overline{N}}_1 \geqq \aleph_0$, plyne z $N_1 \subset N \cup \sigma(N)$, že též $\overline{\overline{N}} \geqq \aleph_0$. Tím je 4.1 dokázáno.

4.2. Poznámka. Ze shora uvedené věty 4.1 plyne, že pro $\boldsymbol{R}(M, \cong)$ prostoru E_1, kde $1 < \overline{\overline{M}} < \aleph_0$, neexistuje fundamentální zákrytová grupa.

Úvahy o rozkladových množinách a jejich zákrytových grupách se vyskytují např. v teorii automorfních funkcí. Problémy z tohoto okruhu otázek shrnul D. HILBERT v XVIII. kapitole své přednášky „Problèmes mathématiques“ přednesené na kongresu v Paříži v roce 1900.

Jeden z těchto problémů byl tento:

Existuje polyedr P, který není fundamentální oblastí žádné grupy pohybů a který má tu vlastnost, že E_n lze rozložit ve smyslu elementární geometrie v polyedry shodné s P?

Přitom systém $\mathfrak{S}$ podmnožin z E_n se nazývá rozkladem prostoru E_n ve smyslu elementární geometrie, když a) $\bigcup_{M \in \gamma} M = E_n$ a b) $x \in E_n \Rightarrow x$ je vnitřním bodem nejvýše jedné množiny $M \in \mathfrak{S}$. Tento problém řešil pro $n \geqq 3$ kladně K. REINHARDT v [3], pro $n = 2$ H. HEESCH v [4]. Pro $n = 1$ jest jediným polyedrem úsečka, problém je zřejmě řešen záporně. Zaměníme-li však pojem „polyedr“ pojmem „množina“ a „fundamentální oblast“ pojmem „fundamentální množina“, je z věty 4.1 vidět, že příkladem takové množiny, o níž se v problému jedná, je každá konečná rozkladová množina přímky mající více než jeden bod.

LITERATURA

[1] *O. Borůvka:* Theorie rozkladů v množině. Spisy vyd. přír. fak. MU, Brno *278*, 1946, 1—37.

[2] А. Курош: Теория групп. 1953.

[3] *K. Reinhardt:* Zur Zerlegung der euklidischen Räume in kongruente Polytope. Sitzungsber. d. preuss. Akad. d. Wiss. 1928, 150—155.

[4] *H. Heesch:* Aufbau der Ebene aus deckungsgleichen Bereichen. Göttingen Nachrichten *2*, *I*, 1935, 115—117.

[5] *N. G. De Bruijn:* On bases for the set of integers. Publicationes mathematicae, Debrecen *1*, 1950, 232—242.
[6] *A. D. Sands:* On the factorisation of finite abelian groups. Acta math. acad. sc. hung. *VIII*, 1957, 65—86.

Резюме

РАЗЛОЖЕНИЕ ПРЯМОЙ В КОНГРУЭНТНЫЕ ТРЕХТОЧЕЧНЫЕ МНОЖЕСТВА

КАРЕЛ КОУТСКЫ и МИЛАН СЕКАНИНА (Karel Koutský a Milan Sekanina), Брно

(Поступило в редакцию 10/VI 1957 г.)

В работе доказывается, что для каждого трехточечного подмножества М прямой существует такое разложение R прямой, что для каждого $X \in R$ имеет место соотношение $X \cong M$ ($\cong$ — знак конгруэнтности множества).

Summary

ON THE DECOMPOSITION OF THE STRAIGHT LINE IN THE CONGRUENT THREE-POINT SETS

KAREL KOUTSKÝ and MILAN SEKANINA, Brno

(Received July 10, 1957)

It is proved, that for every three-point subset M of the straight line there exists a decomposition $\boldsymbol{R}$ of the straight line in such a way, that for each $X \in \boldsymbol{R}$ is $X \cong M$ (where $\cong$ means a sign of the congruence of sets).