Vojtěch Jarník
Dvě poznámky ke geometrii čísel

Věstník Král. čes. spol. nauk 1941, XXIV, 12 p.

Persistent URL: http://dml.cz/dmlcz/500518

Zvláštní otisk z Věstn. Král. Spol. Nauk. Tř. matemat.-přírodověd. Ročník 1941.

Dvě poznámky ke geometrii čísel.

VOJTĚCH JARNÍK, Praha.

(Došlo dne 11. listopadu 1941.)

V n-rozměrném prostoru R_n, opatřeném pravoúhlými osami souřadnými, značme body tučnými písmeny, na př. $\mathfrak{x} = (x_1, \ldots, x_n)$, $\mathfrak{y} = (y_1, \ldots, y_n)$; při tom $\mathfrak{o}$ značí vždy bod $(0, 0, \ldots, 0)$ (počátek). Jsou-li a, b čísla, definujme $a\mathfrak{x} + b\mathfrak{y} = (ax_1 + by_1, \ldots, ax_n + by_n)$ a pod. Body $\mathfrak{x}^1, \ldots, \mathfrak{x}^k$ $(1 \leqq k \leqq n)$[1]) nazýváme nezávislými, neplatí-li žádná rovnice $t_1\mathfrak{x}^1 + \ldots + t_k\mathfrak{x}^k = \mathfrak{o}$, kde $\operatorname{Max}(|t_1|, \ldots, |t_k|) > 0$.[2]) Takové nezávislé body spolu s počátkem určují „k-rozměrnou rovinu" $\{\mathfrak{o}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$, což je množina všech bodů tvaru

$$t_1\mathfrak{x}^1 + \ldots + t_k\mathfrak{x}^k \tag{1}$$

($t_1, \ldots, t_k$ libovolná reálná čísla). n-rozměrná rovina je ovšem celý prostor R_n.

Body s celočíselnými souřadnicemi nazýváme mřížovými body. Jsou-li $\mathfrak{x}^1, \ldots, \mathfrak{x}^k$ $(1 \leqq k \leqq n)$ nezávislé *mřížové* body, lze ovšem všechny mřížové body k-rozměrné roviny $\{\mathfrak{o}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$ psáti ve tvaru (1) s reálnými $t_1, \ldots, t_k$; lze-li všechny *mřížové* body této roviny psáti dokonce ve tvaru (1) s *celistvými* $t_1, \ldots, t_k$, říkáme, že body $\mathfrak{x}^1, \ldots, \mathfrak{x}^k$ tvoří *mřížovou basi* roviny $\{\mathfrak{o}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$.

Je-li M bodová množina, λ nezáporné číslo, značíme znakem λM množinu všech bodů $\lambda\mathfrak{x}$, kde $\mathfrak{x} \in M$. Znakem $J(M)$ značme vnitřní Peano-Jordanův objem množiny M. Budiž nyní M uzavřená omezená množina, mající vnitřní bod. Budiž τ_1 nejmenší kladné číslo takové, že množina $\tau_1 M$ obsahuje nezávislý mřížový bod $\mathfrak{x}^1$ (t. j. různý od počátku); budiž τ_2 nejmenší kladné číslo takové, že množina $\tau_2 M$ obsahuje mřížový bod $\mathfrak{x}^2$ tak, že $\mathfrak{x}^1, \mathfrak{x}^2$ jsou nezávislé. Budiž τ_3 nejmenší kladné číslo takové, že množina $\tau_3 M$ obsahuje mřížový bod $\mathfrak{x}^3$ tak, že $\mathfrak{x}^1, \mathfrak{x}^2, \mathfrak{x}^3$ jsou nezávislé atd. Tak dostáváme celkem n čísel $\tau_1, \ldots, \tau_n$ $(0 < \tau_1 \leqq$

[1]) Čtenář jistě nezamění horní index s mocnitelem.

[2]) Pro $k = 1$ má tedy definice tento smysl: bod $\mathfrak{x}$ je „nezávislý" tehdy a jen tehdy, je-li $\mathfrak{x} \neq \mathfrak{o}$.

$\leqq \tau_2 \leqq \ldots \leqq \tau_n$) a n nezávislých mřížových bodů $\mathsf{x}^1, \ldots, \mathsf{x}^n$; čísla $\tau_1, \ldots, \tau_n$, jež jsou zřejmě jednoznačně určena množinou M, nazýváme *postupnými minimy*, příslušnými k množině M.[3])

Je-li N libovolná neprázdná bodová množina, označme znakem $\mathfrak{B}(N)$ množinu všech bodů $\mathsf{x} - \mathsf{y}$, kde $\mathsf{x} \in N$, $\mathsf{y} \in N$; množinu $\mathfrak{B}(N)$ nazýváme *vektorovou množinou* množiny N. Je zřejmo: je-li N uzavřená, omezená a má vnitřní bod, platí totéž o množině $\mathfrak{B}(N)$. Dále je zřejmě vždy $\mathfrak{B}(tN) = t\mathfrak{B}(N)$ pro $t \geqq 0$.

Neprázdná bodová množina M nazývá se konvexní, má-li tuto vlastnost: je-li $\mathsf{x} \in M$, $\mathsf{y} \in M$, $0 \leqq t \leqq 1$, je též $t\mathsf{x} + (1-t)\mathsf{y} \in M$. O bodové množině M říkáme, že je souměrná vzhledem k počátku, má-li tuto vlastnost: je-li $\mathsf{x} \in M$, je též $-\mathsf{x} \in M$. Zřejmá je tato vlastnost: je-li M konvexní množina, souměrná vzhledem k počátku, je $\mathfrak{B}(M) = 2M$. Vskutku, je-li $\mathsf{z} \in \mathfrak{B}(M)$, je $\mathsf{z} = \mathsf{x} - \mathsf{y}$, kde $\mathsf{x} \in M$, $\mathsf{y} \in M$, tedy $-\mathsf{y} \in M$, $\frac{1}{2}\mathsf{x} + \frac{1}{2}(-\mathsf{y}) \in M$, $\mathsf{z} = \mathsf{x} - \mathsf{y} \in 2M$; naopak, je-li $\mathsf{z} \in 2M$, je $\frac{1}{2}\mathsf{z} \in M$, $-\frac{1}{2}\mathsf{z} \in M$, $\mathsf{z} = \frac{1}{2}\mathsf{z} - (-\frac{1}{2}\mathsf{z}) \in \mathfrak{B}(M)$. Dále: je-li M konvexní množina, souměrná vzhledem k počátku a je-li $\mathsf{y}^i \in M$, $|t_i| \leqq \lambda_i$ pro $i = 1, \ldots, r$, je $t_1\mathsf{y}^1 + \ldots + t_r\mathsf{y}^r \in (\lambda_1 + \ldots + \lambda_r)M$.

Uzavřenou, omezenou konvexní množinu, jež je souměrná vzhledem k počátku a obsahuje aspoň jeden vnitřní bod, budeme nazývati souměrným konvexním tělesem. Z geometrie čísel je známa tato věta:

Věta 1. *Budiž $n > 0$ celé. Potom existuje číslo $c_n > 0$ s touto vlastností: je-li M souměrné konvexní těleso v R_n, a jsou-li $\tau_1, \ldots, \tau_n$ jeho postupná minima, je $\tau_1\tau_2 \ldots \tau_n J(M) \leqq c_n$.*

Platí dokonce, jak známo:[4])

Věta 2. *Ve větě 1. je dovoleno klásti $c_n = 2^n$.*

Číslo 2^n je již ostrá hranice: je-li M krychle $|x_i| \leqq 1$ $(i = 1, \ldots, n)$, je $\tau_1 = \ldots = \tau_n = 1$, $J(M) = 2^n$. Naším prvním cílem jest ukázati, že věta 1, a to s hodnotou $c_n = 2^{2n-1}$, je speciálním případem obecnější věty, platící pro libovolné uzavřené omezené množiny s vnitřním bodem. Platí totiž tato věta, kterou v dalším dokážeme:

Věta 3. *Budiž N uzavřená omezená množina, mající aspoň jeden vnitřní bod; buďte $\tau_1, \ldots, \tau_n$ postupná minima, příslušná k množině $\mathfrak{B}(N)$. Potom je $\tau_1\tau_2 \ldots \tau_n J(N) \leqq 2^{n-1}$.*

---

[3]) Body $\mathsf{x}^1, \ldots, \mathsf{x}^n$ nemusí býti množinou M jednoznačně určeny; leží-li na př. v množině $\tau_1 M$ několik mřížových bodů různých od počátku, mohu kterýkoliv z nich vzíti za x^1; existuje-li mezi nimi k nezávislých (ale nikoliv $k+1$ nezávislých) bodů, je $\tau_1 = \tau_2 = \ldots = \tau_k < \tau_{k+1}$.

[4]) Literaturu viz v knize J. F. Koksma, Diophantische Approximationen, Berlin 1936, str. 13—14 a v Zentralblatt für Mathematik und ihre Grenzgebiete 21, str. 296, poslední referát.

Věta 1. s hodnotou $c_n = 2^{2n-1}$ plyne bezprostředně z věty 3. Je-li totiž M souměrné konvexní těleso a jsou-li $\tau_1, \ldots, \tau_n$ jeho postupná minima, je $M = \mathfrak{B}(\frac{1}{2}M)$ a tedy podle věty 3.

$$\tau_1 \ldots \tau_n J(\tfrac{1}{2}M) = \tau_1 \ldots \tau_n 2^{-n} J(M) \leqq 2^{n-1}.$$

Zde se naskytá důležitá otázka, zda je možno ve větě 3. nahraditi číslo 2^{n-1} jedničkou;*) kdyby to bylo možno, plynula by odtud zřejmě nejenom věta 1, nýbrž i věta 3.

Budiž nyní M souměrné konvexní těleso s postupnými minimy $\tau_1, \ldots, \tau_n$. Budiž σ nejmenší kladné číslo, jež má tuto vlastnost: je-li $\mathfrak{x}$ libovolný bod, obsahuje množina[5]) $\mathfrak{x} + \sigma M$ aspoň jeden mřížový bod. Číslo σ řeší t. zv. nehomogenní problém, příslušný k tělesu M. Význam čísla τ_n pro tento nehomogenní problém je pak dán těmito nerovnostmi:

$$\tfrac{1}{2}\tau_n \leqq \sigma \leqq \tfrac{1}{2}(\tau_1 + \ldots + \tau_n) \leqq \tfrac{1}{2}n\tau_n. \qquad (0)$$

Nerovnosti (0) jsou ostré: je-li M krychle $|x_i| \leqq 1$ $(i = 1, \ldots, n)$, je $\tau_1 = \ldots = \tau_n = 1$, $\sigma = \frac{1}{2}$; je-li M těleso $|x_1| + \ldots + |x_n| \leqq 1$, je $\tau_1 = \ldots = \tau_n = 1$, $\sigma = \frac{1}{2}n$ (nerovnost $|x_1 - \frac{1}{2}| + \ldots + |x_n - \frac{1}{2}| \leqq \sigma$ nelze totiž řešiti celými čísly x_i, je-li $\sigma < \frac{1}{2}n$). Nerovnosti (0) nejsou nové; bylo již v literatuře zdůrazněno,[6]) že jsou obsaženy v úvahách páté kapitoly Geometrie der Zahlen; ježto však přímý důkaz lze provésti na několika řádcích, bude zde v dalším proveden.

Druhým naším cílem je důkaz této věty:

Věta 4. *Buďte* $L_i(\mathfrak{x}) = \gamma_{i1}x_1 + \ldots + \gamma_{in}x_n$ $(i = 1, 2, \ldots, n)$ *reálné lineární formy s determinantem 1; budiž* $\varepsilon > 0$. *Potom existuje mřížový bod* $\mathfrak{x} = (x_1, \ldots, x_n) \neq \mathfrak{o}$ *tak, že*

$$|L_1(\mathfrak{x}) \ldots L_n(\mathfrak{x})| < 2^{-\frac{n-1}{2}} + \varepsilon.$$

Důkaz této věty provedeme metodou, obdobnou metodě, které bylo užito při důkazu obdobné nehomogenní věty[7]): platí-li předpoklady věty 4, a jsou-li $b_1, \ldots, b_n$ libovolná reálná čísla, existuje mřížový bod $\mathfrak{x} = (x_1, \ldots, x_n)$ (zde smí býti $\mathfrak{x} = \mathfrak{o}$) tak, že $|(L_1(\mathfrak{x}) + b_1) \ldots (L_n(\mathfrak{x}) + b_n)| < 2^{-\frac{n}{2}} + \varepsilon$.

Důkaz věty 3. Buďte $\mathfrak{x}^1, \ldots, \mathfrak{x}^n$ nezávislé mřížové body, definované jako svrchu (ovšem pro množinu $M = \mathfrak{B}(N)$). Tedy: je-li $0 < \lambda < \tau_1$, leží v množině $\lambda\mathfrak{B}(N)$ jediný mřížový bod $\mathfrak{o}$; je-li $0 < \lambda < \tau_i$ $(2 \leqq i \leqq n)$, potom všechny mřížové body, ležící v $\lambda\mathfrak{B}(N)$, leží v rovině $\{\mathfrak{o}, \mathfrak{x}^1, \ldots$

*) Pan Vl. Knichal právě sestrojil příklad, který ukazuje, že to není možno.

[5]) Je-li $\mathfrak{b}$ bod, N bodová množina, značí $\mathfrak{b} + N$ množinu všech bodů tvaru $\mathfrak{b} + \mathfrak{y}$, kde $\mathfrak{y} \in N$.

[6]) Viz poslední dva referáty v Zentralblatt 21, str. 104.

[7]) Viz na př. práce, o nichž je referováno v Zentralblatt 23, str. 207.

..., $\mathbf{x}^{i-1}\}$.[8]) Sestrojme nyní mřížové body $\mathbf{y}^1, \ldots, \mathbf{y}^n$ takto: $\mathbf{y}^1$ budiž mřížovou basí přímky $\{\mathbf{0}, \mathbf{x}^1\}$ (stačí zvoliti za $\mathbf{y}^1$ mřížový bod na $\{\mathbf{0}, \mathbf{x}^1\}$, mající co nejmenší kladnou vzdálenost od počátku); $\mathbf{y}^2$ budiž takový mřížový bod v rovině $\{\mathbf{0}, \mathbf{x}^1, \mathbf{x}^2\} = \{\mathbf{0}, \mathbf{y}^1, \mathbf{x}^2\}$, že $\mathbf{y}^1, \mathbf{y}^2$ tvoří mřížovou basi této roviny (stačí zvoliti za $\mathbf{y}^2$ mřížový bod v této rovině, mající od přímky $\{\mathbf{0}, \mathbf{x}^1\} = \{\mathbf{0}, \mathbf{y}^1\}$ co nejmenší kladnou vzdálenost). Potom bude ovšem $\{\mathbf{0}, \mathbf{y}^1, \mathbf{y}^2\} = \{\mathbf{0}, \mathbf{y}^1, \mathbf{x}^2\} = \{\mathbf{0}, \mathbf{x}^1, \mathbf{x}^2\}$. Takto pokračujíce, dostaneme n nezávislých mřížových bodů $\mathbf{y}^1, \ldots, \mathbf{y}^n$ (kde $\mathbf{y}^k = (y_1^k, \ldots, y_n^k)$), jež tvoří basi mřížových bodů celého prostoru a při tom je $\{\mathbf{0}, \mathbf{x}^1, \ldots, \mathbf{x}^k\} = \{\mathbf{0}, \mathbf{y}^1, \ldots, \mathbf{y}^k\}$ pro $k = 1, \ldots, n$. Determinant čísel y_i^k $(i, k = 1, \ldots, n)$ je tedy (jak známo) ± 1 a tedy existuje lineární substituce $y_i = a_{i1}x_1 + \ldots + a_{in}x_n$ $(i = 1, \ldots, n)$ s celočíselnými koeficienty a_{il} a s determinantem ± 1, která převádí bod $\mathbf{y}^k$ $(k = 1, \ldots, n)$ v bod $(0, \ldots, 0, 1, 0, \ldots, 0)$ (na k-tém místě jednička). Tato substituce převádí množinu všech mřížových bodů samu v sebe a nemění vnitřní objem, tedy ani čísla $\tau_1, \ldots, \tau_n$. Můžeme tedy od počátku důkazu předpokládati, že tato substituce již byla provedena. Potom ovšem každý bod $\mathbf{u} = (u_1, \ldots, u_n)$ roviny $\{\mathbf{0}, \mathbf{x}^1, \ldots, \mathbf{x}^{i-1}\} = \{\mathbf{0}, \mathbf{y}^1, \ldots, \mathbf{y}^{i-1}\}$ bude splňovati rovnice $u_i = u_{i+1} = \ldots = u_n = 0$. Platí tedy:

(A) *Je-li* $0 < \lambda < \tau_i$ $(i = 1, \ldots, n)$ *a leží-li mřížový bod* $\mathbf{x} = (x_1, \ldots, x_n)$ *v množině* $\lambda\mathfrak{B}(N)$, *je* $\mathbf{x} \in \{\mathbf{0}, \mathbf{x}^1, \ldots, \mathbf{x}^{i-1}\}$ (resp. $\mathbf{x} = \mathbf{0}$ pro $i = 1$), *t. j.* $x_i = x_{i+1} = \ldots = x_n = 0$.

Předpokládejme, že $\tau_1 \ldots \tau_n J(N) > 2^{n-1}$. Potom lze voliti čísla $\lambda_1, \ldots, \lambda_n$ tak, že

$$0 < \lambda_i < \tau_i, \quad \lambda_1 \leqq \lambda_2 \leqq \ldots \leqq \lambda_n, \quad \lambda_1 \ldots \lambda_n J(N) > 2^{n-1}, \qquad J(N) > \frac{2^{n-1}}{\lambda_1 \ldots \lambda_n}. \tag{2}$$

Sestrojme nyní v prostoru krychlovou síť o straně $\dfrac{1}{\lambda_n m}$ (m celé kladné), jejíž vrcholy jsou všechny body $\mathbf{X}$ tvaru

$$\mathbf{X} = \frac{\mathbf{x}}{\lambda_n m}, \tag{3}$$

kde $\mathbf{x}$ probíhá všechny mřížové body; budiž $\mathfrak{B}$ množina oněch bodů (3), jež leží v N; budiž B počet prvků množiny $\mathfrak{B}$. Zvolím-li m dosti velké,

[8]) Je-li totiž $\mathbf{x}$ mřížový bod, ležící v $\lambda\mathfrak{B}(N)$, nemohou býti — podle definice čísla τ_i — body $\mathbf{x}^1, \ldots, \mathbf{x}^{i-1}, \mathbf{x}$ nezávislé, takže platí rovnice tvaru $t_1\mathbf{x}^1 + \ldots + t_{i-1}\mathbf{x}^{i-1} + t\mathbf{x} = \mathbf{0}$, kde $\operatorname{Max}(|t_1|, \ldots, |t_{i-1}|, |t|) > 0$; ježto $\mathbf{x}^1, \ldots, \mathbf{x}^{i-1}$ jsou nezávislé, nemůže býti $t = 0$, a tedy je $\mathbf{x} = -\frac{t_1}{t}\mathbf{x}^1 - \ldots - \frac{t_{i-1}}{t}\mathbf{x}^{i-1}$, t. j. $\mathbf{x} \in \{\mathbf{0}, \mathbf{x}^1, \ldots, \mathbf{x}^{i-1}\}$.

je podle (2)

$$B \cdot \left(\frac{1}{\lambda_n m}\right)^n > \frac{2^{n-1}}{\lambda_1 \dots \lambda_n}. \tag{4}$$

Sestrojme celá čísla $k_1, \dots, k_n$ tak, že $2^{k_i-1} < \frac{\lambda_n}{\lambda_i} \leqq 2^{k_i}$ a položme $T_i = \frac{2^{k_i}}{\lambda_n}$, takže

$$0 = k_n \leqq k_{n-1} \leqq \dots \leqq k_1, \; T_n = \frac{1}{\lambda_n}, \; \frac{1}{\lambda_i} \leqq T_i < \frac{2}{\lambda_i} \; (1 \leqq i \leqq n-1). \tag{5}$$

Podle (4), (5) je $B > \lambda_n^n m^n T_1 \dots T_n = m^n 2^{k_1+\dots+k_n}$. Dva body

$$\mathsf{X} = \frac{\mathsf{x}}{\lambda_n m}, \; \mathsf{Y} = \frac{\mathsf{y}}{\lambda_n m} \; (\mathsf{x} = (x_1, \dots, x_n), \; \mathsf{y} = (y_1, \dots, y_n)) \tag{6}$$

množiny $\mathfrak{B}$ počítáme do téže třídy, je-li

$$x_1 \equiv y_1 \pmod{2^{k_1} m}, \dots, x_n \equiv y_n \pmod{2^{k_n} m}. \tag{7}$$

Počet těchto tříd je $2^{k_1+\dots+k_n} m^n < B$; v $\mathfrak{B}$ a tedy v N existují dva různé body (6), pro něž platí (7). Položíme-li $\mathsf{X} - \mathsf{Y} = \mathsf{z} = (z_1, \dots, z_n)$, je

$$\mathsf{z} \neq \mathsf{0}, \; \mathsf{z} \in \mathfrak{B}(N), \; \lambda_n z_i \equiv 0 \pmod{2^{k_i}} \; (i = 1, \dots, n). \tag{8}$$

Tedy předně (viz stále (5), (8), (A))

$$\lambda_n z_i \equiv 0 \pmod 1 \; (i = 1, \dots, n), \tag{9}$$

t. j. $\lambda_n \mathsf{z}$ je mřížový bod, ležící v $\lambda_n \mathfrak{B}(N)$; ježto $\lambda_n < \tau_n$, je $z_n = 0$. Tedy je za druhé

$$\lambda_n z_i \equiv 0 \pmod{2^{k_n-1}} \; (i = 1, \dots, n), \tag{10}$$

t. j. $\frac{\lambda_n \mathsf{z}}{2^{k_n-1}}$ je mřížový bod, ležící v $\frac{\lambda_n}{2^{k_n-1}} \mathfrak{B}(N)$; ježto

$$\frac{\lambda_n}{2^{k_n-1}} = \frac{1}{T_{n-1}} \leqq \lambda_{n-1} < \tau_{n-1}, \tag{11}$$

je $z_{n-1} = 0$. Tedy je dále

$$\lambda_n z_i \equiv 0 \pmod{2^{k_n-2}} \; (i = 1, \dots, n), \tag{12}$$

takže $\frac{\lambda_n \mathsf{z}}{2^{k_n-2}}$ je mřížový bod, ležící v $\frac{\lambda_n}{2^{k_n-2}} \mathfrak{B}(N)$; ježto

$$\frac{\lambda_n}{2^{k_n-2}} = \frac{1}{T_{n-2}} \leqq \lambda_{n-2} < \tau_{n-2}, \tag{13}$$

je $z_{n-2} = 0$. Tak pokračujíce, obdržíme $z_n = z_{n-1} = \dots = z_1 = 0$, t. j. $\mathsf{z} = \mathsf{0}$, což je ve sporu s (8).

Důkaz nerovností (0). Buďte $\tau_1, \ldots, \tau_n$ postupná minima souměrného konvexního tělesa M; buďte $\mathfrak{x}^1, \ldots, \mathfrak{x}^n$ nezávislé mřížové body, definované jako v úvodu, takže platí na př.: je-li $0 < \lambda < \tau_n$, a je-li $\mathfrak{x}$ mřížový bod, ležící v tělese λM, je $\mathfrak{x} \in \{\mathfrak{0}, \mathfrak{x}^1, \ldots, \mathfrak{x}^{n-1}\}$. Podobně jako v důkazu věty 3. smíme předpokládati, že tato rovina je množina všech bodů, jejichž n-tá souřadnice je rovna nule.

I. Předpokládejme, že $\sigma < \frac{1}{2}\tau_n$. Budiž $\mathfrak{b} = (b_1, \ldots, b_n)$ takový bod tělesa M, jenž má co největší n-tou souřadnici (tedy ovšem $b_n > 0$), takže pro $\mathfrak{x} = (x_1, \ldots, x_n) \in M$ je vždy $x_n \leqq b_n$. Podle definice čísla σ existuje k bodu $-\frac{1}{2}\tau_n\mathfrak{b}$ mřížový bod $\mathfrak{g} = (g_1, \ldots, g_n)$ tak, že $\mathfrak{g} \in -\frac{1}{2}\tau_n\mathfrak{b} + \sigma M$, takže existuje bod $\mathfrak{z} = (z_1, \ldots, z_n)$ tak, že $\mathfrak{z} \in M$, $\mathfrak{g} = -\frac{1}{2}\tau_n\mathfrak{b} + \sigma\mathfrak{z}$. Je tedy $\mathfrak{g} \in (\frac{1}{2}\tau_n + \sigma) M$; ježto $0 < \frac{1}{2}\tau_n + \sigma < \tau_n$, je (podle definice čísla τ_n) $g_n = 0$, tedy $\frac{1}{2}\tau_n b_n = \sigma z_n$; ježto $0 < \sigma < \frac{1}{2}\tau_n$, plyne odtud $z_n > b_n$, což je spor.

II. Ježto body $\mathfrak{x}^1, \ldots, \mathfrak{x}^n$ jsou nezávislé, existují ke každému bodu $\mathfrak{x} \in R_n$ reálná čísla $m_1, \ldots, m_n$ tak, že $\mathfrak{x} = m_1\mathfrak{x}^1 + \ldots + m_n\mathfrak{x}^n$. Zvolme celá čísla $g_1, \ldots, g_n$ tak, že $m_i = g_i - t_i$, $|t_i| \leqq \frac{1}{2}$ $(i = 1, \ldots, n)$. Potom je $\mathfrak{a} = g_1\mathfrak{x}^1 + \ldots + g_n\mathfrak{x}^n$ mřížový bod a je $\mathfrak{a} = \mathfrak{x} + t_1\mathfrak{x}^1 + \ldots + t_n\mathfrak{x}^n$; ježto $\mathfrak{x}^i \in \tau_i M$, je $t_1\mathfrak{x}^1 + \ldots + t_n\mathfrak{x}^n \in \frac{1}{2}(\tau_1 + \ldots + \tau_n) M$, tedy $\mathfrak{a} \in \mathfrak{x} + \frac{1}{2}(\tau_1 + \ldots + \tau_n) M$, takže $\sigma \leqq \frac{1}{2}(\tau_1 + \ldots + \tau_n)$.

Důkaz věty 4. Případ $n = 1$ je triviální; budiž tedy $n > 1$. Buďte dány reálné formy $L_i(\mathfrak{x})$ $(i = 1, \ldots, n)$ s determinantem 1; budiž g dolní hranice součinu $|L_1(\mathfrak{x}) \ldots L_n(\mathfrak{x})|$ pro všechny mřížové body $\mathfrak{x} = (x_1, \ldots, x_n) \neq \mathfrak{0}$. Předpokládejme $g > 2^{\frac{n-1}{2}}$; odtud odvodíme spor. Definujme $a > 0$ rovnicí $a^{n(n-1)} = g$, takže

$$a^{2n} > \tfrac{1}{2}. \tag{14}$$

Zvolme $\eta > 0$ tak malé, že

$$1 - \frac{(1+\eta)^2}{4a^{2n}} < \frac{1}{(1+\eta)^2}, \quad \frac{1}{a^{2n}} < \frac{1}{(1+\eta)^2} + \frac{1}{(1+\eta)^4}, \quad a^{2n} > \frac{1}{2}(1+\eta)^2 \tag{15}$$

(to lze podle (14)) a potom zvolme $\varepsilon > 0$ tak, že

$$\frac{g+\varepsilon}{g} < 1 + \eta. \tag{16}$$

Zvolme mřížový bod $\mathfrak{x} \neq \mathfrak{0}$ tak, že

$$g \leqq \left|\prod L_i(\mathfrak{x})\right| < g + \varepsilon \tag{17}$$

(index i v součinech probíhá vždy hodnoty $1, 2, \ldots, n$). Pro každý mřížový bod $\mathfrak{y} \neq \pm\mathfrak{x}$ je pak

$$|\prod(L_i(\mathbf{x}) + L_i(\mathbf{y}))| = |\prod L_i(\mathbf{x}+\mathbf{y})| \geqq g, \tag{18}$$

$$|\prod(L_i(\mathbf{x}) - L_i(\mathbf{y}))| = |\prod L_i(\mathbf{x}-\mathbf{y})| \geqq g. \tag{19}$$

Znásobme nerovnosti (18), (19) a dělme čtvercem nerovnosti (17); položíme-li $L_i(\mathbf{x}) = X_i$, obdržíme podle (16) nerovnost

$$\left|\prod\left(1 - \frac{L_i^2(\mathbf{y})}{X_i^2}\right)\right| > \left(\frac{g}{g+\varepsilon}\right)^2 > \frac{1}{(1+\eta)^2}, \tag{20}$$

jež platí, když $\mathbf{y}$ je jakýkoliv mřížový bod, různý od $\mathbf{x}$ a od $-\mathbf{x}$.

Bod $\mathbf{y}$ nyní vhodně zvolíme. Budiž M rovnoběžnostěn

$$|L_i(\mathbf{y})| \leqq \frac{|X_i|}{a^{n-1}} \quad (i = 1, \ldots, n); \tag{21}$$

jeho objem je (podle (17)) $2^n \frac{|X_1 \ldots X_n|}{a^{n(n-1)}} \geqq 2^n \frac{g}{g} = 2^n$, takže jeho postupná minima $\tau_1, \ldots, \tau_n$ vyhovují podle věty 2. nerovnosti $\tau_1\tau_2 \ldots$ $\ldots \tau_n \leqq 1$, tedy $\tau_1\tau_2^{n-1} \leqq 1$, $\tau_2 \leqq \tau_1^{-\frac{1}{n-1}}$. Existují dva nezávislé mřížové body $\mathbf{u}$, $\mathbf{v}$ tak, že

$$|L_i(\mathbf{u})| \leqq \tau_1 \frac{|X_i|}{a^{n-1}}, \quad |L_i(\mathbf{v})| \leqq \tau_2 \frac{|X_i|}{a^{n-1}} \quad (i = 1, \ldots, n). \tag{22}$$

Podle (22), (17), (16) jest

$$g \leqq |\prod L_i(\mathbf{u})| \leqq \tau_1^n \frac{|\prod X_i|}{a^{n(n-1)}} < \tau_1^n \frac{g+\varepsilon}{g} < \tau_1^n (1+\eta), \tag{23}$$

takže $\tau_1 > \frac{a^{n-1}}{1+\eta}$, $\tau_2 < \frac{1+\eta}{a}$. Aspoň jeden z bodů $\mathbf{u}$, $\mathbf{v}$ je nezávislý na $\mathbf{x}$; označme jej $\mathbf{w}$; jest pak podle (22)

$$|L_i(\mathbf{w})| < \frac{1+\eta}{a^n} |X_i| \quad (i = 1, \ldots, n). \tag{24}$$

Uvažujme body $\mathbf{w}$, $2\mathbf{w}$, $4\mathbf{w}$, $8\mathbf{w}$, ...; mezi nimi existuje bod $\mathbf{z}$ takový, že platí

$$|L_i(\mathbf{z})| < \frac{1+\eta}{a^n} |X_i| \quad (i = 1, \ldots, n), \tag{25}$$

že však bod $2\mathbf{z}$ již tyto nerovnosti aspoň pro jednu hodnotu i nesplňuje, na př. pro $i = 1$, takže je

$$|L_1(\mathbf{z})| \geqq \frac{1+\eta}{2a^n} |X_1|; \tag{26}$$

mimo to je ovšem $\mathbf{z} \neq \mathbf{x}$, $\mathbf{z} \neq -\mathbf{x}$. Položme $\left|\frac{L_i(\mathbf{z})}{X_i}\right| = \alpha_i$, takže podle

(25), (26), (20) je

$$0 \leqq \alpha_i < \frac{1+\eta}{a^n} (i = 1, \ldots, n), \quad \alpha_1 \geqq \frac{1+\eta}{2a^n}, \quad \prod | 1 - \alpha_i^2 | > \frac{1}{(1+\eta)^2}; \tag{27}$$

tedy podle (27), (15) postupně

$$\alpha_i^2 < 2, \quad -1 < 1 - \alpha_i^2 \leqq 1, \quad | 1 - \alpha_i^2 | \leqq 1 \quad (i = 2, \ldots, n),$$

$$| 1 - \alpha_1^2 | > \frac{1}{(1+\eta)^2}. \tag{28}$$

Je-li $1 - \alpha_1^2 \geqq 0$, je podle (27), (28)

$$1 - \frac{(1+\eta)^2}{4a^{2n}} \geqq 1 - \alpha_1^2 = | 1 - \alpha_1^2 | > \frac{1}{(1+\eta)^2}, \tag{29}$$

což je ve sporu s (15). Je-li však $1 - \alpha_1^2 < 0$, je podle (27), (28)

$$\frac{(1+\eta)^2}{a^{2n}} - 1 > \alpha_1^2 - 1 = | 1 - \alpha_1^2 | > \frac{1}{(1+\eta)^2}, \tag{30}$$

což je opět ve sporu s (15).

Zwei Bemerkungen zur Geometrie der Zahlen.

(Zusammenfassung.)

(Eingegangen am 11. November 1941.)

Bezeichnungen. $\mathfrak{x} = (x_1, \ldots, x_n)$, $\mathfrak{y} = (y_1, \ldots, y_n)$ usw. bedeuten stets Punkte des n-dimensionalen Raumes R_n $(n \geqq 1)$; stets ist $\mathfrak{o} = (0, \ldots, 0)$. Sind a, b reelle Zahlen, so schreiben wir $a\mathfrak{x} + b\mathfrak{y} = (ax_1 + by_1, \ldots, ax_n + by_n)$ usw. Ist M eine Punktmenge, $\mathfrak{a}$ ein Punkt, $\lambda \geqq 0$, so bedeute $\mathfrak{a} + M$ die Menge aller Punkte $\mathfrak{a} + \mathfrak{x}$ mit $\mathfrak{x} \in M$ und λM die Menge aller Punkte $\lambda\mathfrak{x}$ mit $\mathfrak{x} \in M$. Ist N eine nichtleere Punktmenge, so sei $\mathfrak{B}(N)$ die Menge aller Punkte $\mathfrak{x} - \mathfrak{y}$ mit $\mathfrak{x} \in N$, $\mathfrak{y} \in N$. Offenbar ist $\mathfrak{B}(tN) = t\mathfrak{B}(N)$ für $t \geqq 0$; ist N beschränkt, abgeschlossen und besitzt N einen inneren Punkt, so hat offenbar auch $\mathfrak{B}(N)$ diese Eigenschaften. $J(N)$ sei der innere Peano-Jordansche Inhalt von N. Eine Punktmenge M heiße ein „symmetrischer konvexer Körper", wenn sie folgende Eigenschaften besitzt: M ist beschränkt, abgeschlossen und besitzt einen inneren Punkt; aus $\mathfrak{x} \in M$ folgt $-\mathfrak{x} \in M$; aus $\mathfrak{x} \in M$, $\mathfrak{y} \in M$, $0 \leqq t \leqq 1$ folgt $t\mathfrak{x} + (1-t)\mathfrak{y} \in M$. Für symmetrische konvexe Körper M gilt offenbar: I. $M = \mathfrak{B}(\frac{1}{2}M)$. II. ist $| t_i | \leqq \lambda_i$, $\mathfrak{x}^i \in M$ für $i = 1, \ldots, r$, so ist $t_1\mathfrak{x}^1 + \ldots + t_r\mathfrak{x}^r \in (\lambda_1 + \ldots + \lambda_r) M$.

k Punkte $\mathfrak{x}^1, \ldots, \mathfrak{x}^k$ heißen unabhängig, wenn aus $t_1\mathfrak{x}^1 + \ldots + t_k\mathfrak{x}^k = \mathfrak{0}$ (wo $t_1, \ldots, t_k$ Zahlen sind) $t_1 = \ldots = t_k = 0$ folgt. Solche k Punkte zusammen mit dem Punkt $\mathfrak{0}$ erzeugen die k-dimensionale Ebene $\{\mathfrak{0}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$ d. h. die Menge aller Punkte (1) mit reellen t_i.[9]) Es sei M eine abgeschlossene beschränkte Punktmenge, die einen inneren Punkt besitzt. Es sei τ_1 die kleinste positive Zahl, für welche $\tau_1 M$ einen Gitterpunkt $\mathfrak{x}^1 \neq \mathfrak{0}$ enthält; es sei τ_2 die kleinste positive Zahl, für welche $\tau_2 M$ einen Gitterpunkt $\mathfrak{x}^2$ enthält, sodaß $\mathfrak{x}^1, \mathfrak{x}^2$ unabhängig sind; es sei τ_3 die kleinste positive Zahl, für welche $\tau_3 M$ einen Gitterpunkt $\mathfrak{x}^3$ enthält, sodaß $\mathfrak{x}^1, \mathfrak{x}^2, \mathfrak{x}^3$ unabhängig sind u. s. w. So bekommt man n Zahlen τ_i $(0 < \tau_1 \leqq \tau_2 \leqq \ldots \leqq \tau_n)$, die *sukzessiven Minima* von M, und n unabhängige Gitterpunkte $\mathfrak{x}^1, \ldots, \mathfrak{x}^n$; offenbar sind die τ_i, nicht aber immer die $\mathfrak{x}^i$, durch M eindeutig bestimmt. Aus der Geometrie der Zahlen kennt man folgenden

Satz 1. *Zu jedem ganzen $n > 0$ gibt es ein $c_n > 0$ mit folgender Eigenschaft: Ist M ein symmetrischer konvexer Körper in R_n und sind $\tau_1, \ldots, \tau_n$ seine sukzessiven Minima, so ist $\tau_1\tau_2 \ldots \tau_n J(M) \leqq c_n$.*

Und noch schärfer:

Satz 2. *Im Satz 1 darf man $c_n = 2^n$ setzen.*[10])

Wir wollen nun zeigen, daß Satz 1 als Spezialfall eines wesentlich allgemeineren Satzes angesehen werden kann; dieser Satz lautet:

Satz 3. *Es sei N beschränkt, abgeschlossen und besitze einen inneren Punkt. Es seien $\tau_1, \ldots, \tau_n$ die sukzessiven Minima von $\mathfrak{B}(N)$. Dann ist*

$$\tau_1\tau_2 \ldots \tau_n J(N) \leqq 2^{n-1}.$$

In der Tat, sind die Voraussetzungen von Satz 1 erfüllt, so ist $M = \mathfrak{B}(\frac{1}{2}M)$, also nach Satz 3: $\tau_1 \ldots \tau_n J(\frac{1}{2}M) = \tau_1 \ldots \tau_n 2^{-n} J(M) \leqq \leqq 2^{n-1}$, woraus Satz 1 mit $c_n = 2^{2n-1}$ folgt. Satz 1 ist zwar schwächer als Satz 2, leistet aber auch oft gute Dienste. **Problem:** kann man 2^{n-1} im Satz 3 durch 1 ersetzen?*) Dann wäre nicht nur der Satz 1, sondern auch der Satz 2 ein Spezialfall dieses verschärften Satzes 3.

Beweis des Satzes 3. Es seien unabhängige Gitterpunkte $\mathfrak{x}^1, \ldots, \mathfrak{x}^n$ wie oben eingeführt (und zwar für die Menge $M = \mathfrak{B}(N)$); $\mathfrak{x}^i = (x_1^i, \ldots, x_n^i)$. Dann gibt es n unabhängige Gitterpunkte $\mathfrak{y}^1, \ldots, \mathfrak{y}^n$, welche eine Basis aller Gitterpunkte bilden, sodaß $\{\mathfrak{0}, \mathfrak{y}^1, \ldots, \mathfrak{y}^k\} = \{\mathfrak{0}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$ für

[9]) Die Formeln findet man im tschechischen Text.

[10]) Literatur in J. F. Koksma, Diophantische Approximationen, Berlin 1936, S. 13—14 und Zentralblatt für Mathematik und ihre Grenzgebiete 21, S. 296, letztes Referat.

*) Herr Vl. Knichal hat soeben durch ein Gegenbeispiel gezeigt, dass dies nicht der Fall ist.

$1 \leqq k \leqq n$.[11]) Denkt man sich die Modulsubstitution durchgeführt, die den Punkt $\mathfrak{y}^k$ in den Punkt $(0, \ldots, 0, 1, 0, \ldots, 0)$ überführt (1 an der k-ten Stelle), so ist $x_i^i \neq 0$, $x_{i+1}^i = \ldots = x_n^i = 0$. Dann gilt nach der Definition von τ_i:

$$\text{(A)} \quad \begin{cases} \textit{Ist } 0 < \lambda < \tau_i \ (1 \leqq i \leqq n) \textit{ und liegt der Gitterpunkt } \mathfrak{x} = (x_1, \ldots, x_n) \\ \textit{in } \lambda\mathfrak{B}(N), \textit{ so ist } \mathfrak{x} \in \{\mathfrak{0}, \mathfrak{x}^1, \ldots, \mathfrak{x}^{i-1}\} \text{ (bzw. } \mathfrak{x} = \mathfrak{0} \text{ für } i = 1), \textit{ also} \\ x_i = x_{i+1} = \ldots = x_n = 0. \end{cases}$$

Man setze nun voraus, daß $\tau_1 \ldots \tau_n J(N) > 2^{n-1}$; man wähle $\lambda_1, \ldots, \lambda_n$ so, daß (2) gilt. Man konstruiere ein Würfelnetz mit der Kante $(\lambda_n m)^{-1}$ ($m > 0$ ganz), dessen Eckpunkte alle Punkte (3) sind, wo $\mathfrak{x}$ alle Gitterpunkte durchläuft. Es sei $\mathfrak{B}$ die Menge, B die Anzahl derjenigen Punkte (3), die in N liegen. Ist m hinreichend groß, so gilt (4). Man konstruiere ganze Zahlen $k_1, \ldots, k_n$ mit $2^{k_i - 1} < \frac{\lambda_n}{\lambda_i} \leqq 2^{k_i}$ und setze $T_i = \frac{2^{k_i}}{\lambda_n}$; dann gilt (5). Nach (4), (5) ist $B > \lambda_n^n m^n T_1 \ldots T_n = m^n 2^{k_1 + \ldots + k_n}$; zwei Punkte (6) aus $\mathfrak{B}$ rechne man in dieselbe Klasse, wenn (7) gilt. Da die Anzahl der Klassen $< B$ ist, so gibt es in $\mathfrak{B}$, also in N, zwei verschiedene Punkte (6) mit (7). Setzt man $\mathfrak{X} - \mathfrak{Y} = \mathfrak{z} = (z_1, \ldots, z_n)$, so gilt (8). Also (vgl. stets (5), (8), (A)) gilt (9), d. h. $\lambda_n \mathfrak{z}$ ist ein Gitterpunkt aus $\lambda_n \mathfrak{B}(N)$; wegen $\lambda_n < \tau_n$ ist $z_n = 0$. Also gilt zweitens (10); d. h. $\frac{\lambda_n \mathfrak{z}}{2^{k_n - 1}}$ ist ein Gitterpunkt aus $\frac{\lambda_n}{2^{k_n - 1}} \mathfrak{B}(N)$; wegen (11) ist $z_{n-1} = 0$. Also gilt weiter (12), sodaß $\frac{\lambda_n \mathfrak{z}}{2^{k_n - 2}}$ ein Gitterpunkt aus $\frac{\lambda_n}{2^{k_n - 2}} \mathfrak{B}(N)$ ist; wegen (13) ist also $z_{n-2} = 0$. So fortfahrend, bekommt man $z_n = z_{n-1} = \ldots = \ldots = z_1 = 0$, im Widerspruch gegen (8).

Bemerkung. Es sei nun M ein symmetrischer konvexer Körper, $\tau_1, \ldots, \tau_n$ seien seine sukzessiven Minima; σ sei die kleinste positive Zahl, welche folgende Eigenschaft besitzt: ist $\mathfrak{x}$ ein beliebiger Punkt, so enthält die Punktmenge $\mathfrak{x} + \sigma M$ mindestens einen Gitterpunkt. Kennt man also σ, so hat man das dem Körper M zugehörige „inhomogene Problem" gelöst. Die Bedeutung von τ_n für dieses Problem folgt aus den folgenden Ungleichungen:

$$\tfrac{1}{2}\tau_n \leqq \sigma \leqq \tfrac{1}{2}(\tau_1 + \ldots + \tau_n) \leqq \tfrac{1}{2} n \tau_n. \qquad (0)$$

[11]) Anleitung: Sind $\mathfrak{y}^1, \ldots, \mathfrak{y}^k$ bereits so gewählt, daß sie eine Basis für die in der Ebene $\{\mathfrak{0}, \mathfrak{y}^1, \ldots, \mathfrak{y}^k\} = \{\mathfrak{0}, \mathfrak{x}^1, \ldots, \mathfrak{x}^k\}$ liegenden Gitterpunkte bilden, so wähle man für $\mathfrak{y}^{k+1}$ einen Gitterpunkt der Ebene $\{\mathfrak{0}, \mathfrak{y}^1, \ldots, \mathfrak{y}^k, \mathfrak{x}^{k+1}\}$, der einen möglichst kleinen positiven Abstand von der Ebene $\{\mathfrak{0}, \mathfrak{y}^1, \ldots, \mathfrak{y}^k\}$ hat.

Diese Schranken sind scharf (man betrachte den Würfel $|x_i| \leqq 1$ $(i = 1, \ldots, n)$ mit $\tau_n = 1$, $\sigma = \frac{1}{2}$ und das „Oktaeder" $|x_1| + \ldots + |x_n| \leqq 1$ mit $\tau_1 = \ldots = \tau_n = 1$, $\sigma = \frac{1}{2}n$. Die Ungleichungen (0) sind nicht neu; es ist schon in der Literatur hervorgehoben worden, daß (0) aus den Betrachtungen des fünften Kapitels der „Geometrie der Zahlen" folgt[12]); jedoch möge hier ein kurzer Beweis gegeben werden.

$\mathfrak{x}^1, \ldots, \mathfrak{x}^n$ seien wie am Anfang dieser Note eingeführt. Wie im Beweis des Satzes 3 darf man voraussetzen, daß die n-te Koordinate aller Punkte der Ebene $\{\mathfrak{o}, \mathfrak{x}^1, \ldots, \mathfrak{x}^{n-1}\}$ gleich Null ist.

I. Es sei $\mathfrak{b} = (b_1, \ldots, b_n)$ ein Punkt von M mit maximaler n-ter Koordinate; aus $\mathfrak{x} = (x_1, \ldots, x_n) \in M$ folgt also $x_n \leqq b_n$; also ist $b_n > 0$. Es gibt einen Gitterpunkt $\mathfrak{g} = (g_1, \ldots, g_n)$ mit $\mathfrak{g} \in -\frac{1}{2}\tau_n\mathfrak{b} + \sigma M$; zu $\mathfrak{g}$ gibt es also einen Punkt $\mathfrak{z} = (z_1, \ldots, z_n) \in M$ mit $\mathfrak{g} = -\frac{1}{2}\tau_n\mathfrak{b} + \sigma\mathfrak{z}$. Also ist $\mathfrak{g} \in (\frac{1}{2}\tau_n + \sigma) M$. Wäre $\sigma < \frac{1}{2}\tau_n$, so wäre $0 < \sigma + \frac{1}{2}\tau_n < \tau_n$, also $g_n = 0$, $\frac{1}{2}\tau_n b_n = \sigma z_n$, also $z_n = \dfrac{\tau_n b_n}{2\sigma} > b_n$ — Widerspruch.

II. Jeder Punkt $\mathfrak{x}$ läßt sich in der Gestalt $\mathfrak{x} = m_1\mathfrak{x}^1 + \ldots + m_n\mathfrak{x}^n$ schreiben; man finde ganze g_i mit $m_i = g_i - t_i$, $|t_i| \leqq \frac{1}{2}$; also ist $\mathfrak{a} = g_1\mathfrak{x}^1 + \ldots + g_n\mathfrak{x}^n$ ein Gitterpunkt, $\mathfrak{a} = \mathfrak{x} + t_1\mathfrak{x}^1 + \ldots + t_n\mathfrak{x}^n$, $t_1\mathfrak{x}^1 + \ldots + t_n\mathfrak{x}^n \in \frac{1}{2}(\tau_1 + \ldots + \tau_n) M$ (denn $\mathfrak{x}^i \in \tau_i M$), also $\sigma \leqq \frac{1}{2}(\tau_1 + \ldots + \tau_n)$.

* * *

Unser zweites Ziel ist der Beweis des folgenden Satzes:

Satz 4. *Es seien* $L_i(\mathfrak{x}) = \gamma_{i1}x_1 + \ldots + \gamma_{in}x_n$ $(i = 1, \ldots, n)$ *reelle Linearformen mit der Determinante 1; es sei* $\varepsilon > 0$. *Dann gibt es einen Gitterpunkt* $\mathfrak{x} = (x_1, \ldots, x_n) \neq \mathfrak{o}$ *mit* $|L_1(\mathfrak{x}) \ldots L_n(\mathfrak{x})| < 2^{-\frac{n-1}{2}} + \varepsilon$.

Der Beweis dieses Satzes ist der Beweismethode nachgebildet, mit welcher man einen analogen „inhomogenen" Satz bewiesen hat.[13])

Beweis des Satzes 4. Es sei $n > 1$ (der Fall $n = 1$ ist trivial). Es seien n reelle Linearformen $L_i(\mathfrak{x})$ $(i = 1, \ldots, n)$ mit der Determinante 1 gegeben; es sei g die untere Grenze von $|L_1(\mathfrak{x}) \ldots L_n(\mathfrak{x})|$ für alle Gitterpunkte $\mathfrak{x} = (x_1, \ldots, x_n) \neq \mathfrak{o}$. Man setze $g > 2^{-\frac{n-1}{2}}$ voraus; daraus wird sich ein Widerspruch ergeben. Man definiere a durch $a > 0$, $a^{n(n-1)} = g$, sodaß (14) gilt. Man wähle $\eta > 0$ und nachher $\varepsilon > 0$ so klein, daß (15), (16) gilt; das geht wegen (14). Man wähle dann einen Gitterpunkt $\mathfrak{x} \neq \mathfrak{o}$ mit (17) (der Index i in Produkten läuft stets über

[12]) Vgl. die beiden letzten Referate im Zentralblatt 21, S. 104.

[13]) Vgl. z. B. die im Zentralblatt 23, S. 207 besprochenen Arbeiten.

die Zahlen $1, 2, \ldots, n$). Für jeden Gitterpunkt $\mathfrak{y} \neq \pm \mathfrak{x}$ gilt dann (18), (19). Multipliziert man (18), (19), dividiert dann durch das Quadrat von (17) und setzt man $L_i(\mathfrak{x}) = X_i$, so bekommt man (20). Wir werden nun den Gitterpunkt $\mathfrak{y}$ geeignet wählen. Es sei M das Parallelepiped (21) mit dem Inhalt $2^n \frac{|X_1 \ldots X_n|}{a^{n(n-1)}} \geqq 2^n$ (vgl. (17) und die Definition von a); für die sukzessiven Minima $\tau_1, \ldots, \tau_n$ von M gilt also (nach Satz 2) $\tau_1 \tau_2 \ldots \tau_n \leqq 1$, $\tau_1 \tau_2^{n-1} \leqq 1$, $\tau_2 \leqq \tau_1^{-\frac{1}{n-1}}$. Es gibt also zwei unabhängige Gitterpunkte $\mathfrak{u}, \mathfrak{v}$ mit (22). Nach (22), (17), (16) gilt (23), also $\tau_1 > \frac{a^{n-1}}{1+\eta}$, $\tau_2 < \frac{1+\eta}{a}$. Mindestens einer der beiden Gitterpunkte $\mathfrak{u}, \mathfrak{v}$ ist von $\mathfrak{x}$ unabhängig; er heiße $\mathfrak{w}$; wegen (22) gilt dann (24). Unter den Punkten $\mathfrak{w}, 2\mathfrak{w}, 4\mathfrak{w}, 8\mathfrak{w}, \ldots$ gibt es einen Punkt $\mathfrak{z}$ mit folgenden Eigenschaften: es gilt (25); für den Punkt $2\mathfrak{z}$ ist aber mindestens eine dieser Ungleichungen — z. B. die erste — nicht mehr erfüllt, so daß (26) gilt; außerdem ist freilich $\mathfrak{z} \neq \mathfrak{x}, \mathfrak{z} \neq -\mathfrak{x}$. Setzt man $\left|\frac{L_i(\mathfrak{z})}{X_i}\right| = \alpha_i$ und benutzt (25), (26), (20), so kommt (27) heraus; aus (27), (15) folgt (28). Ist $1 - \alpha_1^2 \geqq 0$, so gilt (29) — Widerspruch gegen (15). Ist aber $1 - \alpha_1^2 < 0$, so bekommt man (30) — ebenso Widerspruch gegen (15).