STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1958 - 012

Voordracht in de serie "Actualiteiten"

Dr. C.G. Lekkerkerker

31 mei 1958

Samengestelde convexe lichamen

1958

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

ZW 1958-012

Voordracht in de serie

"Actualiteiten"

door

Dr C.G. Lekkerkerker

31 mei 1958

Samengestelde convexe lichamen

1. De volgende overweging is het uitgangspunt van de meetkunde der getallen. Zij $f(x_1,\dots,x_n)$ een reële functie van n veranderlijken ($n \geq 2$) en μ een positief getal. Laat K de verzameling der punten $x=(x_1,\dots,x_n) \in R_n$ zijn, waarvoor $|f(x_1,\dots,x_n)| < \mu$. Dan kan de vraag of er gehele getallen $u_1,\dots,u_n$ zijn met $|f(u_1,\dots,u_n)|<\mu$ ook aldus geformuleerd worden: bevat K een roosterpunt $u=(u_1,\dots,u_n)$?

Veelal is f een homogene functie (van positieve graad). Dan is $O=(0,\dots,0)$ een triviale oplossing en vragen we uitsluitend naar roosterpunten $u \neq O$ in K.

We beperken ons in het volgende tot het geval dat K een convex lichaam is. We geven het volume van K aan met V(K) en noemen K O-symmetrisch, als het punt O middelpunt van K is. De fundamentele stelling is hier de bekende

Hoofdstelling van Minkowski. Als K begrensd, convex en O-symmetrisch is en $V(K) > 2^n$, dan bevat K een roosterpunt $u \neq O$.

In deze stelling kan de voorwaarde $V(K) > 2^n$ niet verzwakt worden, zoals blijkt, als we voor K de kubus: $|x_i| < 1$ ($i=1,\dots,n$) nemen. Toch heeft reeds Minkowski een essentiële verscherping van zijn hoofdstelling gegeven. Om deze te formuleren voeren we eerst enkele begrippen en notaties in. We behandelen daarbij de punten

$x \in R_n$ als vectoren en noemen b.v. x afhankelijk van een stelsel punten $x^{(1)},\dots,x^{(k)}$, als er reële getallen $\alpha_1,\dots,\alpha_k$ zijn met

$$(1) \qquad x = \alpha_1\, x^{(1)} + \dots + \alpha_k x^{(k)} .$$

De verzameling der punten x die afhankelijk zijn van k gegeven punten $x^{(1)},\dots,x^{(k)}$, d.i. in de vorm (1) te schrijven zijn, stellen we voor door $R(x^{(1)},\dots,x^{(k)})$ (voor $k=0$ alleen het punt O). Verder geven we, als K een (O-symmetrisch, convex) lichaam en $\lambda > 0$ is, met λK aan de verzameling der punten λx met $x \in K$; voor $\lambda' > \lambda$ is $\lambda' K \supset \lambda K$. We kiezen nu opvolgend positieve getallen $\lambda_1,\dots,\lambda_n$ en roosterpunten $u^{(1)},\dots,u^{(n)}$, en wel als volgt ($\overline{K}$ is de afsluiting van K):

$$(2)\begin{cases} \lambda_1 = \text{kleinste positieve getal, waarvoor } \lambda_1\overline{K} \text{ een rooster-} \\ \qquad \text{punt } u^{(1)} \neq 0 \text{ bevat; algemener} \\ \lambda_i = \text{kleinste positieve getal, waarvoor } \lambda_i\overline{K} \text{ een rooster-} \\ \qquad \text{punt } u^{(i)} \notin R(u^{(1)},\dots,u^{(i-1)}) \text{ bevat } (1 \leq i \leq n). \end{cases}$$

Dat er getallen λ_i en roosterpunten $u^{(i)}$ met de bovengenoemde eigenschap bestaan, volgt uit de overweging dat O middelpunt van het convexe lichaam K is en dat λK voor voldoend grote λ dus de kubus $|x_i| \leq 1$ $(i=1,\dots,n)$ bevat. Men merke op, dat $u^{(i)}$ juist op de rand van $\lambda_i K$ ligt. De punten $u^{(i)}$, of liever (met het oog op de O-symmetrie van K) de puntenparen $\pm u^{(i)}$ zijn door het bovenstaande voorschrift niet noodzakelijk eenduidig bepaald. Echter wel de getallen λ_i; want λ_i is niets anders dan het kleinste positieve getal, zodanig dat $\lambda_i\overline{K}$ tenminste i onafhankelijke roosterpunten bevat. We noemen de door (2) gedefinieerde getallen λ_i de <u>successieve minima</u> van K. Het is duidelijk dat

$$(3) \qquad \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n \quad .$$

De bedoelde verscherping van de hoofdstelling luidt nu:
<u>Tweede stelling van Minkowski.</u> Als K een begrensd, convex en O-symmetrisch lichaam is, en als de getallen λ_i $(1 \leq i \leq n)$ gedefinieerd zijn door (2), dan geldt

$$(4) \qquad \lambda_1 \lambda_2 \dots \lambda_n V(K) \leq 2^n .$$

Gebruiken we (3), dan leidt (4) tot $\lambda_1^n\ V(K)=V(\lambda_1 K)\leq 2^n$, wat aequivalent is met de bewering van de hoofdstelling. Het bewijs van de tweede stelling van Minkowski (zie [1,2]) ligt veel dieper dan dat van de hoofdstelling en maakt op essentiële punten gebruik van de convexiteit. Veel gemakkelijker is het een ondergrens voor het linkerlid van (4) te vinden. Daartoe merken we op dat de punten $\lambda_1^{-1}u^{(1)},\ldots,\lambda_n^{-1}u^{(n)}$ alle tot $\overline{K}$ behoren. Dan bevat $\overline{K}$ het 2^n-eder met hoekpunten $\pm\lambda_i^{-1}u^{(i)}$ en is dus

$$V(K) \geq 2^n\ (n!\lambda_1\lambda_2\ldots\lambda_n)^{-1}.\ |\det(u^{(1)},\ldots,u^{(n)})|\ .$$

Verder is $\det(u^{(1)},\ldots,u^{(n)})$ een van nul verschillend geheel getal. We vinden dus

$$\lambda_1\lambda_2\ldots\lambda_n\ V(K)\geq 2^n/n! \tag{5}$$

2. We gaan thans over tot de bespreking van een door Mahler [3] aangegeven methode om aan een gegeven convex lichaam, of ook een gegeven stelsel convexe lichamen, een nieuw convex lichaam, het z.g. samengestelde (compound) convexe lichaam toe te voegen. Daarbij gaat het er vooral om ongelijkheden af te leiden voor de diverse daarbij optredende successieve minima. Zoals Mahler aangeeft, kan men uit zijn resultaten door specialisatie een nieuw bewijs halen van het transferprincipe van Chintsjin (Uebertragungsprinzip van Khintchine). In het algemeen is het samengestelde convexe lichaam van hogere dimensie.

Zij p een natuurlijk getal $< n$. Laten $x^{(i)}=(x_{1i},\ldots,x_{ni})$ $(i=1,\ldots,p)$ p punten in R_n zijn. Aan elk stelsel $\{\nu\}$ van p indices $\nu_1,\nu_2,\ldots,\nu_p$ met $1\leq\nu_1<\nu_2<\ldots<\nu_p\leq n$ voegen we toe de determinant $x_{\{\nu\}}=x_{\nu_1\nu_2\ldots\nu_p}$, gegeven door

$$x_{\{\nu\}} = \det(x_{\nu_i i}) = \begin{vmatrix} x_{\nu_1 1}\ldots x_{\nu_p 1} \\ \vdots \qquad \vdots \\ x_{\nu_1 p}\ldots x_{\nu_p p}\end{vmatrix}\ . \tag{6}$$

In totaal zijn er $N=\binom{n}{p}$ stelsels $\{\nu\}$ en determinanten $x_{\{\nu\}}$. We rangschikken ze in de een of andere volgorde en geven ze in die volgorde aan door $\xi_1,\ldots,\xi_N$. Met de p punten

$x^{(1)},\dots,x^{(p)}$ laten we nu corresponderen het punt $\xi=(\xi_1,\dots,\xi_N)$ in R_N. We noemen ξ het samengestelde punt der punten $x^{(i)}$ en geven het aan met $\xi=[x^{(1)},\dots,x^{(p)}]$.

Als $2\leq p\leq n-2$, dan voldoen de determinanten $x_{\{\nu\}}$ aan zekere homogene algebraïsche vergelijkingen. Het punt ξ ligt daarom op een zekere algebraïsche variëteit $\Omega(n,p)\subset R_N$, die een kegel is met top in O. Deze variëteit zal in het volgende geen rol spelen.

Belangrijk is dat met een affiene transformatie van R_n, werkend op de punten $x^{(i)}$, een affiene transformatie van het samengestelde punt ξ in R_N correspondeert. Zij eens $A=(a_{ij})$ een affiene transformatie van R_n. Men verifieert gemakkelijk dat voor willekeurige punten $x^{(i)}$ de coördinaten van het samengestelde punt $\bar{\xi}=[Ax^{(1)},\dots,Ax^{(p)}]$ gegeven worden door

$$\bar{x}_{\{\nu\}}=\sum_{\{\nu\}}\pm\det\,(a_{\nu_i\mu_j})\,x_{\{\mu\}}\;. \tag{7}$$

We geven met $A^{(p)}$ aan de $N\times N$-matrix met elementen $a_{\{\nu\}\{\mu\}}=\pm\det(a_{\nu_i\mu_j})$ en noemen $A^{(p)}$ de p^{de} samengestelde matrix van A. Uit de determinantenleer is bekend dat

$$\det A^{(p)}=(\det A)^P\;,\qquad P=\frac{Np}{n}=\binom{n-1}{p-1}\;. \tag{8}$$

Laten nu gegeven zijn p begrensde, gesloten, convexe, O-symmetrische lichamen $K_1,\dots,K_p$ in R_n. Zij Σ de verzameling der punten $[x^{(1)},\dots,x^{(p)}]$ in R_N met $x^{(i)}\in K_i$ $(i=1,\dots,p)$. Dan heet het convex omhulsel van Σ (i.e. de kleinste gesloten convexe verzameling die Σ bevat) in R_N het samengestelde convexe lichaam van de lichamen K_i, aangegeven met $K=[K_1,\dots,K_p]$. Ingeval de p convexe lichamen K_i identiek zijn, stel $K_i=K$, schrijven we $\mathcal{K}=K^{(p)}$, en noemen we $\mathcal{K}$ het p^{de} samengestelde convexe lichaam van K.

We laten zien dat $\mathcal{K}$ een begrensd, gesloten, convex, O-symmetrisch lichaam in R_N is. Het is duidelijk dat $\mathcal{K}$ begrensd, gesloten en convex is. Omdat bijv. K_1 O-symmetrisch is en $[-x^{(1)},x^{(2)},\dots,x^{(p)}]=-[x^{(1)},x^{(2)},\dots,x^{(p)}]$, is Σ, en dus $\mathcal{K}$, ook O-symmetrisch. Als verder $e^{(1)},\dots,e^{(n)}$ de eenheidspunten (i^{de} coördinaat 1 en overige 0) in R_n zijn en elk der lichamen K_i de punten $\pm\delta e^{(1)},\dots,\pm\delta e^{(n)}$ bevat ($\delta > 0$), dan bevat $\mathcal{K}$ de 2N punten $\pm\delta^p \mathcal{E}^{\{\nu\}} = \pm\delta^p[e^{(\nu_1)},\dots,e^{(\nu_p)}]$. Immers voor elk stelsel $\{\nu\}$ is $\delta e^{(\nu_i)}$ een punt van K_i ($i=1,\dots,p$). Nu heeft $\mathcal{E}^{\{\nu\}}$ één coördinaat 1, terwijl de overige 0 zijn, m.a.w. de punten $\mathcal{E}^{\{\nu\}}$ zijn de eenheidspunten in R_N. Uit een en ander volgt dat $\mathcal{K}$ een omgeving van 0 bevat. Dus is $\mathcal{K}$ een lichaam.

3. We leiden nu enige stellingen over het volume en de successieve minima van $\mathcal{K}$ af, <u>in geval de lichamen K_i identiek zijn</u>. We hebben daarbij nodig de eigenschap dat een willekeurig begrensd, convex, 0-symmetrisch lichaam K in R_n in te sluiten is tussen twee ellipsoïden E en λE om 0, waarbij λ een constante is die alleen van n afhangt. Men kan deze eigenschap als volgt inzien: als E de ellipsoïde in K is met maximaal volume en λ voldoende groot is, dan bevat het convex omhulsel van E en een willekeurig randpunt van λE een ellipsoïde met volume $> V(E)$, zodat de randpunten van λE buiten K liggen. Men kan bewijzen dat men kan nemen $\lambda = \sqrt{n}$.

Voor de volumina $V(K)$ en $V(\mathcal{K})$ in R_n resp. R_N geldt nu:

<u>Stelling 1</u>. Er zijn twee positieve constanten c_1 en c_2, die alleen van n en p afhangen, zodanig dat

$$(9) \qquad c_1 \leq V(\mathcal{K})\,V(K)^{-P} \leq c_2 \qquad \left(P=\binom{n-1}{p-1}\right).$$

<u>Bewijs</u>. Zij G_n de eenheidsbol in R_n. Zij verder E een ellipsoïde om 0 met $E \subseteq K \subseteq \sqrt{n}E$, en zij A een affiene transformatie van R_n met $E=AG_n$. Zij tenslotte $\Gamma_n^{(p)} = [G_n]^{(p)}$ en $\mathcal{E} = [E]^{(p)}$. Dan is $\mathcal{E} = A^{(p)}\Gamma_n^{(p)}$, wegens (8) dus

$$V(\mathcal{E})\,V(E)^{-P} = V(\Gamma_n^{(p)})\,V(G_n)^{-P} ,$$

waarbij het rechterlid alleen van n en p afhangt. Verder ligt $V(K)$ in tussen $V(E)$ en $n^{\frac{1}{2}n}V(E)$, en is $\mathcal{E} \subseteq \mathcal{K} \subseteq n^{\frac{1}{2}p}\mathcal{E}$, zodat $V(\mathcal{K})$ inligt tussen $V(\mathcal{E})$ en $n^{\frac{1}{2}pN}\,V(\mathcal{E})$. Daaruit volgt de stelling.

We beschouwen vervolgens de successieve minima van $\mathcal{K}$, stel $\mu_1,\dots,\mu_N$. Dus μ_k is het kleinste positieve getal, waarvoor $\mu_k\mathcal{K}$ tenminste k onafhankelijke roosterpunten in R_N bevat

($k=1,\dots,N$). We beschouwen ook de successieve minima $\lambda_1,\dots,\lambda_n$ van K en voeren in de producten

$$M_{\{\nu\}} = \lambda_{\nu_1}\lambda_{\nu_2}\dots\lambda_{\nu_p} .$$

We rangschikken de grootheden $M_{\{\nu\}}$ naar opklimmende grootte en geven ze in die volgorde aan door $M_1,\dots,M_n$. Er geldt

Stelling 2. Er is een positieve constante c_3, die alleen van n en p afhangt, zodanig dat

(10) $\qquad c_3 M_k \leq \mu_k \leq M_k \quad (k=1,\dots,N).$

Bewijs. Krachtens de definitie van successieve minima is er een stelsel van n onafhankelijke roosterpunten $u^{(1)},\dots,u^{(n)} \in R_n$, zodanig dat $u^{(i)}$ op de rand van $\lambda_i K$ ligt. De samengestelde punten $U^{\{\nu\}} = [u^{(\nu_1)},\dots,u^{(\nu_p)}]$ zijn roosterpunten in R_N. Daarbij geldt $U^{\{\nu\}} = A^{(p)} \mathcal{E}^{\{\nu\}}$ voor alle systemen $\{\nu\}$, als A een affiene transformatie in R_n is met $u^{(i)} = Ae^{(i)}$ ($i=1,\dots,n$). Dus zijn de punten $U^{\{\nu\}}$ onafhankelijk (zie punt 2, eind).

Wegens $u^{(i)} \in \lambda_i K$ ($i=1,\dots,n$) is voor alle systemen $\{\nu\}$

$$U^{\{\nu\}} \in [\lambda_{\nu_1}K,\dots,\lambda_{\nu_p}K] = \lambda_{\nu_1}\dots\lambda_{\nu_p}[K]^{(p)} = M_{\{\nu\}}\mathcal{K} .$$

Als nu $M_{\{\nu\}}$ bij de hierboven ingevoerde rangschikking de index k gekregen heeft, dan liggen tenminste k punten $U^{\{\nu\}}$ in $M_{\{\nu\}}\mathcal{K}$. Dit wil juist zeggen dat $\mu_k \leq M_k$ ($k=1,\dots,N$).

Hieruit kunnen we het eerste deel van (10) als volgt afleiden. Uit (4) en (5), toegepast op K resp. $\mathcal{K}$, volgt dat

$$\frac{\mu_1\mu_2\cdots\mu_N V(\mathcal{K})}{\{\lambda_1\lambda_2\dots\lambda_n V(K)\}^P} \geq \frac{2^{N-nP}}{N!} .$$

We hebben $(\lambda_1\lambda_2\dots\lambda_n)^P = M_1M_2\dots M_N$. Passen we stelling 1 toe, dan vinden we dus dat

$$\frac{\mu_1\mu_2\dots\mu_N}{M_1M_2\dots M_N} \geq c_3 = \frac{2^{N-nP}}{N!c_1}$$

Wegens $\mu_k \leq M_k$ ($k=1,\dots,N$) volgt hieruit $\mu_k \geq c_3 M_k$ ($k=1,\dots,N$). Daarmee is de stelling bewezen.

4. We geven thans de toepassing op het transferprincipe van Chintsjin. We beschouwen eerst een willekeurige $n \times n$-matrix $A=(a_{ij})$ met determinant 1 en de p^{de} samengestelde matrix $A^{(p)} = a_{hk}^{(p)}$. Zij K het parallelotoop in R_n en Q het parallelotoop in R_N, bepaald door

$$(11) \qquad K: \left| \sum_{i=1}^{n} a_{ij} x_j \right| \leq 1 \; (i=1,\ldots,n) \; ,$$

$$Q: \left| \sum_{k=1}^{N} a_{hk}^{(p)} \xi_k \right| \leq 1 \; (h=1,\ldots,N).$$

Zij $\mathcal{K} = [K]^{(p)}$. Er zijn twee vaste positieve constanten c', c'' met $c'Q \subseteq \mathcal{K} \subseteq c''Q$. Want dit geldt als A de eenheidsmatrix is, en de ongelijkheden blijven gelden bij affiene transformatie. Laten nu $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_n$ de successieve minima van K zijn, en $\mu_1, \ldots, \mu_N$ die van $\mathcal{K}$. En zij μ het eerste successieve minimum van Q.

Voeren we de grootheden M_k in zoals hierboven, dan geldt $M_1 = \lambda_1 \lambda_2 \ldots \lambda_p \geq \lambda_1^p = \lambda^p$ (zie (3)). Verder is $V(K)=2^n$; wegens (4), (3) en (5) hebben we dus

$$M_1 \leq \frac{1}{\lambda_{p+1} \ldots \lambda_n} \leq (\lambda_2 \lambda_3 \ldots \lambda_n)^{-\frac{n-p}{n-1}} \leq (n!\lambda)^{\frac{n-p}{n-1}} \; .$$

Vervolgens is, op grond van (10), $c_3 M_1 \leq \mu_1 \leq M_1$. Tenslotte volgt uit $c'Q \subseteq \mathcal{K} \subseteq c''Q$ dat $\frac{1}{c'}\mu \geq \mu_1 \geq \frac{1}{c''}\mu$. Dit voert ons tot de volgende

<u>Stelling 3</u>. Zijn de parallelotopen K en Q gedefinieerd door (11) en heeft $A=(a_{ij})$ determinant 1, dan zijn de eerste successieve minima λ en μ van K resp. Q verbonden door de ongelijkheden

$$(12) \qquad \lambda \leq c_4 \mu^{\frac{1}{p}} \; , \; \mu \leq c_5 \lambda^{\frac{n-p}{n-1}} \; ,$$

waarbij de constanten c_4 en c_5 alleen van n en p afhangen.

Om nu tot het transferprincipe van Chintsjin te komen, nemen we $p=n-1$ en beschouwen we een getal $t > 0$ en een stelsel van $p=n-1$ reële getallen $\alpha_1, \ldots, \alpha_p$, die onafhankelijk zijn over de ring van de gehele getallen. De volgende matrices horen dan bij elkaar:

$$A = \begin{pmatrix} t^p & t^p\alpha_1 & - - - - & t^p\alpha_p \\ & t & & \\ & & \ddots & \\ & & & t \end{pmatrix}, \quad B = \begin{pmatrix} t^{-p} & & & \\ -t\alpha_1 & t & & \\ \vdots & & \ddots & \\ -t\alpha_p & & & t \end{pmatrix},$$

waarbij alleen in de hoofddiagonaal en in de eerste rij, resp. kolom elementen $\neq 0$ staan. Dan is B de p^{de} samengestelde matrix van A en omgekeerd. We beschouwen getallen $\beta \geq 0$ met de eigenschap dat aan het stelsel ongelijkheden

$$\text{(I)} \quad |u_1\alpha_1 + \ldots + u_p\alpha_p + u_o| \leq \xi^{-(p+\beta)}, \quad |u_i| \leq \xi \quad (i=1,\ldots,p)$$

bij onbepaald toenemende ξ voldaan is voor oneindig veel verschillende stellen gehele getallen $u_o, u_1, \ldots, u_p$, en daarnaast getallen $\gamma \geq 0$ zodanig dat aan

$$\text{(II)} \quad |v_o\alpha_i - v_i| \leq \eta^{-\frac{1+\gamma}{p}} \quad (i=1,\ldots,p) \; ; \quad |v_o| \leq \eta$$

voor $\eta \to \infty$ voldaan is voor oneindig veel stellen gehele getallen $v_o, v_1, \ldots, v_p$.

Uit de hoofdstelling van Minkowski, toegepast op een parallelotoop in R_n, valt af te leiden dat zeker de getallen $\beta=0$, resp. $\gamma=0$ de genoemde eigenschappen bezitten. Maar voor bepaalde stellen $\{\alpha_i\}$ is het mogelijk dat de genoemde eigenschappen voor grotere waarden van β en γ gelden. Daarbij geldt (zie [4]):

<u>Stelling 4</u>. Als het stelsel (II) oneindig veel oplossingen toelaat voor een zekere waarde van $\gamma \geq 0$, dan laat (I) oneindig veel oplossingen toe, als $\beta < \gamma$. Als omgekeerd (I) oneindig veel oplossingen toelaat voor een $\beta \geq 0$, dan (II) voor $\gamma < \dfrac{\beta}{p^2+(p-1)\beta}$.

<u>Bewijs</u>. Onderstel dat (II), voor zekere waarden van η en γ, een oplossing heeft. We bepalen t zodanig dat $t^{-p}\eta = t\,\eta^{-\frac{1+\gamma}{p}}$. Dus $t^{p+1} = \eta^{1+\frac{1+\gamma}{p}}$. Dan heeft het lichaam

$$(13) \quad |t(\alpha_i y_o - y_i)| \leq 1 \; (i=1,\ldots,p) , \quad |t^{-p} y_o| \leq 1$$

eerste minimum $\lambda \leq t^{-p}\eta$. Wegens stelling 3 heeft dan het lichaam

(14) $\quad |t^p(\alpha_1x_1+\ldots+\alpha_px_p+x_0)| \leqslant 1, \ |t^{-1}x_i| \leqslant 1 \quad (i=1,\ldots,p)$

eerste minimum $\mu \leqslant c_4(t^{-p}\eta)^{\frac{1}{p}}$. Dan heeft (I), bij weglating van factoren c_4, een oplossing met

$$\xi = t\mu \sim \eta^{\frac{1}{p}}, \quad \xi^{-(p+\beta)} = t^{-p}\mu \sim t^{-(p+1)}\eta^{\frac{1}{p}} = \eta^{-1-\frac{\gamma}{p}}.$$

Dus kunnen we nemen $\beta \sim \gamma$. Laten we η onbepaald toenemen, dan vinden we het eerste deel van de stelling.

Laat nu omgekeerd (I) een oplossing hebben voor zekere ξ en β . We bepalen t zó dat $t^{-1}\xi = t^p\xi^{-(p+\beta)}$. Dan is $t^{p+1} = \xi^{p+1+\beta}$ en heeft het lichaam (14) eerste minimum $\lambda \leq t^{-1}\xi$. Dus heeft het lichaam (13) eerste minimum $\mu \leq c_4(t^{-1}\xi)^{\frac{1}{p}}$. We vinden dat (II) een oplossing heeft met

$$\eta = t^p\mu \sim t^{\frac{p^2-1}{p}}\xi^{\frac{1}{p}} = \xi^{p+\frac{p-1}{p}\beta},$$

$$\eta^{-\frac{1+\gamma}{p}} = t^{-1}\mu \sim t^{-\frac{p+1}{p}}\xi^{\frac{1}{p}} = \xi^{-(1+\frac{\beta}{p})}.$$

We moeten dus γ zo kiezen dat $(1+\gamma)(p+\beta-\frac{\beta}{p}) < p+\beta$, ofwel $\gamma < \dfrac{\beta}{p^2+(p-1)\beta}$. Daaruit vinden we het tweede deel van de stelling.

5. De vraag doet zich voor of er analoga bestaan van de stellingen 1 en 2, ingeval de lichamen K_i niet identiek zijn. In plaats van het middelste lid van (9) moeten we dan beschouwen de uitdrukking

(15) $\quad T = V(\mathcal{K}) \prod_{i=1}^{p} V(K_i)^{-P/p}$.

Mahler [5] laat aan de hand van het stelsel lichamen

$$K_i : \sum_{j=1}^{n}|x_j| \leq 1 \quad (i=1,\ldots,p-1), \quad K_p: \frac{1}{a}\sum_{j=1}^{n-1}|x_j| + a^{n-1}|x_n| \leq 1$$

$(a > 0)$ gemakkelijk zien dat er geen bovengrens voor T bestaat.

Wèl kan men aantonen [6] dat er algemeen een positieve ondergrens voor de uitdrukking T is, en evenzo dat het tweede deel van de ongelijkheid (10) algemeen geldt. Dit berust op een generalisatie van de in punt 2 afgeleide eigenschap dat de N samengestelde punten die gevormd kunnen worden uit n onafhankelijke punten $u^{(i)}$ onafhankelijk zijn. Als $\{\mu\} = \{\mu_1, \ldots, \mu_p\}$ en $\{\nu\} = \{\nu_1, \ldots, \nu_p\}$ twee indicessystemen zijn (met $1 \leq \nu_1 < \nu_2 \ldots < \nu_p \leq n$), dan zullen we schrijven

$$\{\mu\} \prec \{\nu\}$$

als $\mu_i \leq \nu_i$ voor $i=1,\ldots,p$. De N indicessystemen $\{\nu\}$ zullen we, in een of andere volgorde, aangeven met $\{\nu^{(1)}\}, \ldots, \{\nu^{(N)}\}$. Er geldt nu de volgende

<u>Hulpstelling.</u> Laten gegeven zijn p systemen van n onafhankelijke punten $x^{(i,1)}, \ldots, x^{(i,n)}$ in R_n $(i=1,\ldots,p)$. Dan zijn er N indicessystemen $\{\mu^{(k)}\} = \{\mu_{1k}, \ldots, \mu_{pk}\}$ $(1 \leq \mu_{ik} \leq n$ voor alle i en k; $k=1,\ldots,N)$, zodanig dat

1. de N samengestelde punten $\mathfrak{z}^{\{\mu^{(k)}\}} = [x^{(\mu_{1k})}, \ldots, x^{(\mu_{pk})}]$ in R_N zijn onafhankelijk.
2. $\{\mu^{(k)}\} \prec \{\nu^{(k)}\}$ voor $k=1,\ldots,N$.

Voor het bewijs van deze hulpstelling, door volledige inductie naar p, zij verwezen naar [6].

We bewijzen nu

<u>Stelling 5</u>. De uitdrukking T, gegeven door (15), heeft een positieve ondergrens.

<u>Bewijs</u>. Laten $\lambda_{i1}, \ldots, \lambda_{in}$ de successieve minima van K_i zijn en laten $x^{(i,1)}, \ldots, x^{(i,n)}$ n onafhankelijke roosterpunten in R_n zijn, zodanig dat $x^{(i,j)}$ op de rand van $\lambda_{i,j}K_i$ ligt $(j=1,\ldots,n;\ i=1,\ldots,p)$. Voor een willekeurig indicessysteem $\{\mu\}$ stellen we $L_{\{\mu\}} = \lambda_{1\mu_1}\lambda_{2\mu_2}\cdots\lambda_{p\mu_p}$. We mogen zonder beperking aannemen dat de volgorde van de lichamen K_i zó gekozen is dat het product

$$L = \prod_{\{\nu\}} L_{\{\nu\}}$$

over alle systemen $\{\nu\} = \{\nu^{(k)}\}$ ten hoogste gelijk is aan het geometrisch gemiddelde:

$$L \leq \Big(\prod_{j=1}^{n} L_{\{j,j,\ldots,j\}}\Big)^{N/n} = \Big(\prod_{i=1}^{p}\prod_{j=1}^{n}\lambda_{i,j}\Big)^{N/n} .$$

We nemen nu N indicessystemen $\{\mu^{(k)}\}$ met de in de hulpstelling genoemde eigenschappen. Dan zijn de N punten $\mathfrak{z}^{\{\mu^{(k)}\}}$ onafhankelijk. Bovendien zijn het roosterpunten. De punten

$\pm\,\xi\{\mu^{(k)}\}$ spannen dus een 2^N-eder op met volume $\geq 2^N/N!$ (vgl. bewijs van (5)).

Verder is $\{\mu^{(k)}\} \prec \{\nu^{(k)}\}$, dus $L_{\{\mu^{(k)}\}} \leq L_{\{\nu^{(k)}\}}$ $(k=1,\dots,N)$. En uit de definitie van de getallen $\lambda_{i,j}$ volgt dat de punten $(L_{\{\mu^{(k)}\}})^{-1}\xi\{\mu^{(k)}\}$ alle tot $\mathcal{K}$ behoren. We hebben dus

$$V(\mathcal{K}) \geq \frac{2^N}{N!}\left(\prod_k L_{\{\mu^{(k)}\}}\right)^{-1} \geq \frac{2^N}{N!}\left(\prod_k L_{\{\nu^{(k)}\}}\right)^{-1} = \frac{2^N}{N!L}.$$

Toepassing van (4) op de lichamen K_i geeft dus, wegens $N/n=P/p$,

$$T \geq \frac{2^N}{N!}\cdot\prod_{i=1}^{p}\left(\lambda_{i1}\lambda_{i2}\cdots\lambda_{in}V(K_i)\right)^{-P/p} \geq 2^{N-pN}/N!$$

Daarmee is de stelling bewezen.

<u>Stelling 6.</u> Laten de systemen $\{\nu\}$ zó gerangschikt zijn, dat de rij der producten $L_{\{\nu^{(k)}\}}$ niet-dalend is, en schrijf $L_{\{\nu^{(k)}\}} = M_k$ $(k=1,\dots,N)$. Laten $\mu_1,\dots,\mu_N$ de successieve minima van $\mathcal{K}$ zijn. Dan geldt

$$(16) \qquad \mu_k \leq M_k \quad (k=1,\dots,N).$$

<u>Bewijs</u>. Kies weer de indicessystemen $\{\mu^{(k)}\}$ zoals hierboven. Voor de punten $\xi\{\mu^{(k)}\}$, geleverd door de hulpstelling, geldt dan

$$\xi\{\mu^{(k)}\} \in L_{\{\mu^{(k)}\}}\,\mathcal{K} \subset L_{\{\nu^{(k)}\}}\,\mathcal{K} = M_k\,\mathcal{K} \quad (k=1,\dots,N).$$

Verder zijn deze punten roosterpunten en onafhankelijk. Daaruit volgt de stelling.

Uit de beschouwingen van deze paragraaf volgt ook dat er geen analogon is van het eerste deel van de ongelijkheid (10).

Zwakkere resultaten werden verkregen door <u>Rogers</u> [7].

6. Tot slot vermelden we een vergaande generalisatie die <u>Mahler</u> [8] gegeven heeft van de beschouwingen onder 2 en 3. Laten p,n en N natuurlijke getallen zijn. Mahler beschouwt nu een afbeelding, die aan elk stelsel van p punten $x^{(1)},\dots,x^{(p)}$ in R_n een punt $\xi = [x^{(1)},\dots,x^{(p)}]$ in R_N toevoegt en die aan

de volgende eisen voldoet:

1. het beeldpunt $[x^{(1)},\ldots,x^{(p)}]$ is lineair in elk der punten $x^{(i)}$ afzonderlijk.
2. onder de beeldpunten $[x^{(1)},\ldots,x^{(p)}]$ $(x^{(1)},\ldots,x^{(p)} \in R_n)$ komen N onafhankelijke punten in R_N voor.
3. aan elke niet-singuliere lineaire transformatie A van R_n beantwoordt een lineaire transformatie A^* van R_N zodanig dat
$$[Ax^{(1)},\ldots,Ax^{(p)}] = A^*[x^{(1)},\ldots,x^{(p)}] .$$
4. er is een constante P met $|\det A^*| = |\det A|^P$.
5. als de punten $x^{(i)}$ $(i=1,\ldots,p)$ rationale coördinaten hebben, dan ook het toegevoegde punt $[x^{(1)},\ldots,x^{(p)}]$ in R_N.

Bij deze eisen kan het volgende aangetekend worden. Zij f een afbeelding die aan de eisen 1 en 2 voldoet, anders gezegd een multilineaire afbeelding van het cartesisch product $R_n^{\,p}=R_n\times R_n\times\ldots\times R_n$ in R_N, zodanig dat R_N voortgebracht wordt door het volledige beeld $f(R_n^{\,p})$. Men kan $R_n^{\,p}$ op natuurlijke wijze inbedden in het tensorproduct $R_n^{[p]}= R_n\otimes R_n\otimes\ldots\otimes R_n$ -- te beschrijven als een euclidische ruimte met basis $\{e^{(i_1)}\otimes e^{(i_2)}\otimes\ldots\otimes e^{(i_p)}\}$ $(1\leq i_1\leq n,\ldots,1\leq i_p\leq n)$ -- met de volgende eigenschap: elke afbeelding f die aan 1 en 2 voldoet, is uit te breiden tot een lineaire afbeelding f^* van $R_n^{[p]}$ op R_N. Ook bepaalt elke niet-singuliere transformatie A van R_n een lineaire transformatie $A^{[p]}$ van $R_n^{[p]}$. Daarbij is, zoals men gemakkelijk inziet, de afbeelding $A\rightarrow A^{[p]}$ een <u>geheel rationale representatie</u> van de transformatiegroep van R_n in $R_n^{[p]}$ van de graad p.

Laat ξ een willekeurig punt van $R_n^{[p]}$ zijn. De eis 3 impliceert dat, voor alle A, de beelden van de punten ξ en $A^{[p]}\xi$ $(\xi\in R_n^{[p]})$ bij de afbeelding f verbonden zijn door een <u>eenduidige</u> (en dan vanzelf lineaire) transformatie A^* ; daarbij moet voor A^* dus gelden
$$f^*A^{[p]}\xi = A^*f^*\xi .$$

Dit is dan en slechts dan het geval als de nulruimte van f^* in $R_n^{[p]}$ invariant is voor alle (z.g. bisymmetrische) transformaties $A^{[p]}$. Daarbij is R_N isomorf met de factorgroep van $R_n^{[p]}$ naar een invariante deelruimte.

De elementen van de matrix A^* hangen linear af van die van $A^{[p]}$. Uit het voorgaande volgt nu dat $A \to A^*$ een geheel rationale representatie van de graad p van de transformatiegroep van R_n in R_N is. Daaruit valt 4 af te leiden, met $P=pN/n$.

De eis 5 houdt in dat de roosterpunten in R_n afgebeeld worden in een deelrooster van eindige index van het rooster der punten in R_N met als coördinaten veelvouden van een vast rationaal getal.

Mahler kan uit de eisen 1-5 gemakkelijk generalisaties van de stellingen 1 en 2 afleiden. We besluiten met het stellen van het volgende

Probleem. Is het mogelijk de stellingen 5 en 6 te generaliseren voor het hier beschouwde geval?

[1] H. Weyl, On geometry of numbers, Proc.London Math.Soc.47, 268-289 (1942).

[2] T. Estermann, Note on a theorem of Minkowski, Journal London Math.Soc.21, 179-182 (1946).

[3] K. Mahler, On compound convex bodies I, Proc.London Math. Soc.(3), 5, 358-379 (1955).

[4] J.F. Koksma, Diophantische Approximationen, Springer Berlin 1936, Kap.V.

[5] K. Mahler, On compound convex bodies II, Proc.London Math. Soc.(3), 5, 380-384 (1955).

[6] C.G. Lekkerkerker, On the volume of compound convex bodies, Proc.Kon.Ned.Akad.Wet.A60, 284-289 (1957).

[7] C.A. Rogers, The compound of convex bodies, Journal London Math.Soc.32, 312-318 (1957).

[8] K. Mahler, Invariant matrices and the geometry of numbers, Proc.Royal Soc. Edinburgh A64, 223-238 (1956).