STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951 - 008

Voordracht in de serie Actualiteiten over de stelling van Minkowski-Hajos

door

C.G. Lekkerkerker

1951

MATHEMATISCH CENTRUM
2de Boerhaavestr. 49
A M S T E R D A M O.

Rapport ZW 1951- 008

Voordracht in de serie Actualiteiten over de stelling van Minkowski-Hajós,

door

C.G.Lekkerkerker.

1. De groepentheoretische stelling van Hajós.

Zij G een eindige Abelse groep met n elementen. Laat de groepoperatie multiplicatief geschreven worden. Als tegenhanger van de fundamentaalstelling, die zegt dat G te beschrijven is als direct product van enige cyclische ondergroepen, bewijzen we:

Zijn $g_1,\ldots,g_r$ elementen van G, zijn $q_1,\ldots,q_r$ natuurlijke getallen, en is elk element van de groep op één manier te schrijven als

$$g_1^{k_1} g_2^{k_2} \ldots g_r^{k_r},$$

waarin $k_1, k_2,\ldots,k_r$ gehele getallen zijn die voldoen aan $0 \leq k_i < q_i$ $(i=1,\ldots,r)$, dan is minstens één der deelverzamelingen van G:

$$(1, g_i, g_i^2, \ldots, g_i^{q_i-1})$$

een groep.

In deze stelling beschouwen we een aantal deelverzamelingen, die wel een speciale gedaante hebben, maar geen ondergroep van G behoeven te zijn. En er wordt ondersteld dat G op te vatten is als een soort direct product van deze deelverzamelingen; dat zoiets kan optreden wordt door de fundamentaalstelling op drastische wijze gegarandeerd: zelfs wanneer we eisen dat al die deelverzamelingen ondergroepen zijn, bestaat er zo 'n direct product. De stelling spreekt nu uit dat bij een splitsing met de beschouwde eigenschap minstens één factor een ondergroep van G is, of anders gezegd: voor minstens één waarde van de index i moet gelden: $g_i^{q_i}=1$. Het is duidelijk dat $q_1 \ldots q_r$ gelijk is aan de orde van G.

Bij het bewijs kunnen we ons beperken tot het geval, dat de q_i priemgetallen zijn. Want is b.v. $q_i=p_1 \ldots p_s$, waarin $p_1,\ldots,p_s$ priemgetallen (waaronder gelijke mogen voorkomen), dan kunnen we eeneenduidig schrijven:

$$k_i = \lambda_1 + \lambda_2 p_1 + \lambda_3 p_1 p_2 + \ldots \lambda_s p_1 \ldots p_{s-1},$$

dus

$$g_i^{k_i} = g_i^{\lambda_1} \cdot (g_i^{p_1})^{\lambda_2} \cdot (g_i^{p_1 p_2})^{\lambda_3} \ldots (g_i^{p_1 \ldots p_{s-1}})^{\lambda_s},$$

waarin λ_σ $(\sigma=1,\ldots,s)$ een geheel getal is met $0 \leq \lambda_\sigma < p_\sigma$. Door dit voor alle g_i te doen wordt men gevoerd op nieuwe deelverzamelingen met dezelfde eigenschappen, maar waarvoor nu steeds het aantal elementen een priem-

getal is. Hebben we bewezen dat er bij een bepaalde waarde van i een σ bestaat waarvoor geldt $(g_i^{p_1\cdots p_{\sigma}-1})^{p_{\sigma}}=1$, dan geldt ook $g_i^{q_i}=1$.

2. Bij het bewijs van de stelling van Hajós leiden we schattingen af voor het aantal priemfactoren in de orde van zekere ondergroepen van G. Verder is het nodig om naast ondergroepen en deelverzamelingen van G ook uitdrukkingen van de volgende gedaante in de beschouwing te betrekken:

$$c_1g_1+c_2g_2+\ldots+c_ng_n,$$

z.g. <u>complexen</u>. Hierbij zijn de c_i, de coëfficiënten van een complex, gehele getallen ≥ 0, en de g_i de verschillende elementen van G. Twee complexen heten alleen gelijk, als alle coëfficiënten gelijk zijn. Optelling van complexen geschiedt door optelling van de coëfficienten; vermenigvuldiging wordt vastgelegd door distributiviteit te eisen en twee elementen g_μ, g_ν te vermenigvuldigen, zoals in de groep gebeurt. De complexen vormen blijkbaar een <u>ring</u>. Een ondergroep H of een deelverzameling K van G zullen we wel eens opvatten als een complex, d.i. een element uit die ring, en daarbij een willekeurige coëfficiënt c_ν gelijk aan 1 of 0 te stellen, al naar gelang het overeenkomstige element g_ν in H resp. K voorkomt of niet.

Stellen we nog voor i=1,...,r de deelverzameling $(1,g_i,\ldots,g_i^{q_i-1})$ voor door S_i, dan kunnen we de te bewijzen stelling aldus uitspreken: Geldt $G=S_1S_2\ldots S_r$, dan is minstens één der S_i een groep.

Is B een complex $\neq S$, dan geven we met H(B) de ondergroep van G aan, die voortgebracht wordt door <u>die</u> elementen van B, waarvan de coëfficiënt van nul verschilt. Met d(B) geven we het aantal priemfactoren aan in het getal, dat de orde aangeeft van H(B); meervoudige priemfactoren worden hierbij meervoudig geteld. Zijn $B_i,\ldots,B_k$ complexen $\neq 0$, dan definieren we $H(B_1,\ldots,B_k)$ als de ondergroep, voortgebracht door de elementen die in minstens één van de complexen $B_1,\ldots,B_k$ met van nul verschillende coëfficiënt voorkomen, en $d(B_1,\ldots,B_k)$ als het aantal priemfactoren in de orde van die ondergroep. We wijzen er op, dat $H(B_1B_2\ldots B_k)$ niet hetzelfde hoeft te zijn als $H(B_1,B_2,\ldots,B_k)$, maar er een echt deel van kan zijn, en dat voorts geldt:

$$H(B_1,B_2,\ldots,B_k)=H(B_1).H(B_2)\ldots H(B_k).$$

3. Enige hulpstellingen.

a) $d(G)=r$

b) $H_1 \subset H_2 \rightarrow d(H_1) \leqq d(H_2)$ (H_1 en H_2 ondergroepen van G).

c) $d(B_1,B_2) \leqq d(B_1)+d(B_2)$, voor willekeurige complexen B_1 en B_2.
Immers, als $H_1=H(B_1)$, $H_2=H(B_2)$ is, dan is het concrete product van H_1 en H_2 te verkrijgen als homomorf beeld van het abstracte product, en is dus de orde van H_1H_2 een deler van het product van de orden van H_1 en H_2.

d) Zijn H_1,H_2,H_3 ondergroepen van G met $H_1 \subset H_2$, dan is
$d(H_2H_3)-d(H_2) \leqq d(H_1H_3)-d(H_1)$.

Immers, daar G Abels is, zijn de genoemde ondergroepen tevens normaaldelers, en kunnen we de factorgroepen H_2/H_1 en H_2H_3/H_1H_3 vormen, als verzamelingen van nevenklassen. De eerste is homomorf af te beelden op de tweede, en dus is de orde van de tweede factorgroep een deler van die van de eerste, en dus

$$d(H_2H_3)-d(H_1H_3) \leqq d(H_2)-d(H_1).$$

4. We leveren nu het bewijs van onze stelling met volledige inductie en uit het ongerijmde. Voor r=1 spreekt de stelling voor zichzelf. We leiden een contradictie af uit de onderstelling dat de stelling geldt voor r=1,..., r-1 en dat G een splitsing $S_1S_2...S_r$ toelaat, waarbij geen enkele S_i een groep is.

Wegens de groepeigenschap is $Gg_r=G$, ofwel $G(g_r-1)=0$, of

(1) $$S_1...S_{r-1}D_r=0 \text{ met } D_r=g_r^{q_r}-1.$$

Krachtens onderstelling is $D_r \neq 0$. In het linkerlid van (1) laten we zoveel mogelijk factoren S_i weg (event. geen enkele), terwijl toch het product gelijk aan nul blijft. Door geschikte nummering van de S_i bereiken we: er is een natuurlijk getal k met $1 \leqq k \leqq r-1$, zodat geldt

(2) $$S_1...S_kD_r=0,$$

en zodat hierin geen factor meer weggelaten kan worden. Vanzelf mag de factor D_r niet weggelaten worden. We zullen nu aantonen:

I $d(S_1,...,S_k) > k$
II $d(S_1,...,S_k,D_r) \not> k.$

Wegens $d(S_1,...,S_k) \leqq d(S_1,...,S_k,D_r)$ houdt dit een contradictie in. Bewijs van I. Hiervoor is de minimaliteitseigenschap van (2) nog niet nodig. Zij $K=S_1...S_k$. Dan is K een complex $\neq 0$ met alleen niet-negatieve coëfficiënten; K is geen ondergroep - anders was een der $S_1,...,S_k$ wegens inductieveronderstelling een groep; $KS_{k+1}...S_r$ is wèl een groep, n.l. G. Zij H=H(K), q het aantal elementen van K en t dat van H. Er geldt

$$H.KS_{k+1}...S_r=H.G \text{ en } H.K=qH,\ H.G=tG,$$

dus

(3) $$qHS_{k+1}...S_r=tG.$$

Hier staat een gelijkheid tussen twee complexen. Rechts in (3) staat elk element van G t-maal. Dus is q een deler van t, en wel een echte deler, omdat K echt bevat is in H. We delen door q en tellen de priemfactoren in de aantallen elementen links en rechts:

$d(K)+1+...+1 > d(G)$, ofwel $d(K)+r-k > r$, dus $d(K) > k$.

En d(K) is hetzelfde als $d(S_1,...,S_k)$, omdat $H(S_1,...,S_k)$ voortgebracht wordt door $g_1,...,g_k$ en die laatste elementen tevens in K voorkomen met van nul verschillende coëfficiënt.

In plaats van II bewijzen we de volgende stelling:
Is het complex $B \neq 0$ en zijn de complexen $T_1,\ldots,T_m$ priemreeksen of differenties, d.w.z. is elke T_μ van de gedaante $1+g+\ldots+g^{p-1}$ of de gedaante $g-1$ ($\mu=1,\ldots,m$); en geldt verder

$$BT_1\ldots T_m=0, \tag{4}$$

terwijl het linkerlid van (4) $\neq 0$ is, als een factor T_μ weggelaten wordt, dan geldt:

$$d(B,T_1,\ldots,T_m)-d(B)<m.$$

Voor $m=k+1$, $B=1$, $T_m=D_r$, $T_\mu=S_\mu$ ($\mu=1,\ldots,k$) ontstaat II.

We handelen nu eerst het geval $m=1$ af. Is T_1 een differentie $g-1$, dan is dus $B(g-1)=0$, ofwel $Bg=B$, en dus g bevat in $H(B)$. Is T_1 een priemreeks $1+g+\ldots+g^{p-1}$, dan is enerzijds $BT(g-1)=B(g^p-1)=0$, dus $g^p\in H(B)$. Anderzijds is $B(g+\ldots+g^{p-1})=-B$; een element b_2 rechts komt ook links voor, neg als b_1g^i met $1\leq i\leq p-1$. Dan is $g^i\in H(B)$. Door combinatie volgt: $g\in H(B)$. Bijgevolg is altijd $H(B,T_1)=H(B)$, dus $d(B,T_1)-d(B)=0$ en de stelling voor $m=1$ bewezen.

Vervolgens beschouwen we het geval: $d(T_\mu)=1$ voor $\mu=1,\ldots,m$. Wegens het gegeven is het complex $BT_1\ldots T_{m-1}\neq 0$ en op grond van de vorige alinea toegepast met T_m i.p.v. T_1 en $BT_1\ldots T_{m-1}$ i.p.v. B, is dan:

$$d(BT_1\ldots T_{m-1},T_m)-d(BT_1\ldots T_{m-1})=0. \tag{5}$$

Verder is wegens 3 d) met $H_1=H(BT_1\ldots T_{m-1})$, $H_2=H(B,T_1,\ldots,T_{m-1})$, $H_3=H(T_m)$:

$$d(B,T_1,\ldots,T_{m-1},T_m)-d(B,T_1,\ldots,T_{m-1})\leq d(BT_1\ldots T_{m-1},T_m)-d(BT_1\ldots T_{m-1}). \tag{6}$$

en krachtens 3 c) hebben we de ongelijkheid:

$$d(B,T_1,\ldots,T_{m-1})-d(B)\leq d(T_1)+\ldots+d(T_{m-1})=m-1. \tag{7}$$

Door optellen van (5), (6), (7) krijgen we de stelling ook voor dit geval.

In het algemene geval passen we volledige inductie toe naar de uitdrukking

$$F=d(T_1)+\ldots+d(T_m).$$

Het is na het voorafgaande voldoende de stelling aan te tonen voor een zekere waarde van F in de onderstelling dat hij al bewezen is voor de lagere waarden van F. Verder mogen we aannemen $d(T_m)\geq 2$. We gaan nu op geschikte manier een differentie D kiezen, die verkregen wordt door T_m met een zekere factor te vermenigvuldigen, terwijl $d(D)=d(T_m)-1$ is. En wel, als $T_m=g-1$ is en q de orde van het groepselement g (wegens $d(T_m)\geq 2$ is q geen priemgetal), kiezen we een priemfactor p van q; $D=g^p-1$ voldoet dan aan de vereisten. En als $T_m=1+g+\ldots+g^{p-1}$ is, vormen we eerst $D_1=T_m(g-1)=g^p-1$; dan is $d(D_1)=d(T_m)$ of $d(D_1)=d(T_m)-1$; in het laatste geval zijn we al klaar; in het eerste geval voldoet een zeker veelvoud $D=g^{pp_1}-1$ van D_1 aan de vereisten.

Conclusie: $BT_1\ldots T_{m-1}D=0$. Laat bij geschikte nummering van de T_μ gelden:

(8) $BT_1 \ldots T_k D = 0$,

terwijl het linkerlid van (8) niet meer nul is bij schrapping van een T_μ. Wegens het gegeven kan ook D niet geschrapt worden.

Hierbij is $0 \leqq k \leqq m-1$. Het geval k=0 moet apart behandeld worden. Daarbij is op grond van het voorgaande $d(B,D)-d(B)=0$ en verder op grond van 3 d): $d(B,T_m)-d(B,D) \leqq d(T_m)-d(D)=1$. Dus geldt:

(7') $d(B,T_m)-d(B) \leqq 1$.

Wegens inductieveronderstelling is

(5') $d(PT_m,T_1,\ldots,T_{m-1})-d(BT_m) < m-1$;

en uit 3 d) volgt:

(6') $d(B,T_1,\ldots,T_{m-1},T_m)-d(B,T_m) \leqq d(BT_m,T_1,\ldots,T_{m-1})-d(BT_m)$

In het geval $k>0$ leiden we uit de inductieveronderstelling af $d(B,T_1,\ldots,T_k,D)-d(B) < k+1$ (wegens $d(T_1)+\ldots+d(T_k)+d(D) \leqq d(T_1+\ldots+d(T_m)-1$), en dus

(7") $d(B,T_1,\ldots,T_k)-d(B) \leqq k$.

Ook kunnen we uit de inductieveronderstelling afleiden:

(5") $d(BT_1 \ldots T_k, T_{k+1},\ldots,T_m)-d(BT_1 \ldots T_k) < m-k$.

Op grond van 3 d) hebben we nog

(6") $d(B,T_1,\ldots,T_k, T_{k+1},\ldots,T_m)-d(B,T_1,\ldots,T_k) \leqq d(BT_1 \ldots T_k,T_{k+1},\ldots,T_m) - d(BT_1 \ldots T_k)$.

Door optelling van (5'), (6') (7'), resp. (5"), (6"), (7") ontstaat in beide gevallen de uitspraak van de stelling.

5. Wij willen nu overgaan op continue Abelse groepen. De groep G, waarvan in het vorige sprake was, wordt voortgebracht door de elerenten $g_1,\ldots,g_r$. We kunnen dit zo zien, dat aan elk stel van r gehele getallen $k_1,\ldots,k_r$ een element van de groep is toegevoegd. Componentsgewijze optellen van twee zulke stellen beantwoordt aan de groepoperatie. Het komt zeker voor, dat aan verschillende stellen hetzelfde groepselement is toegevoegd; de groep G was zelfs eindig. Er zijn dus identificaties; daarbij zijn er natuurlijke getallen $q_1,\ldots,q_r$ ($\geqq 2$), zodat de stellen met $0 \leqq k_i < q_i$ (i=1,...,r) alle elementen van G precies éénmaal leveren.

We beschouwen nu een groep G met de volgende eigenschappen: een willekeurig element g wordt beschreven door n <u>reele</u> parameters $y_1,\ldots,y_n$. Aan het optellen van twee stellen parameters beantwoordt de groepoperatie. Er zijn verder identificaties; en wel n positieve getallen $\tau_1,\ldots,\tau_n$, zodat de stellen met $0 \leqq y_i < \tau_i$ (i=1,...,n) alle elementen van G precies éénmaal leveren (vgl blz.10, laatste alinea).

Stellen we het element met parameters $y_1,\ldots,y_n$ voor door $g(y_1,\ldots,y_n)$. Blijkbaar is $g(0,0,\ldots,0)$ het eenheidselement, zeg 1,

van de groep. We zullen in 8. en 9. bewijzen dat voor minstens één waarde van i het element $g(0,\ldots,\tau_i,\ldots,0)$ het eenheidselement 1 is.

We mogen ons beperken tot het geval $\tau_i = 1 (i=1,\ldots,n)$. Want we kunnen als parameters even goed gebruiken $y_i^1 = \frac{y_i}{\tau_i}$.

We kunnen een meetkundige voorstelling van G ontwerpen in een euclidische ruimte R_n. We kiezen daarin een assenstelsel met oorsprong O en noemen de eenheidsvectoren in de coördinaatrichtingen $e_1,\ldots,e_n$. Aan het punt $x=y_1e_1+\ldots+y_ne_n$ $(-\infty < y_i < +\infty)$ voegen we het groepselement $x^*=g(y_1,\ldots,y_n)$ toe. De punten van de eenheidskubus $W: 0 \leqslant y_i < 1$ $(i=1,\ldots,n)$ representeren dan eeneenduidig de groepselementen. Letten we nu op de verzameling $\mathfrak{P}$ der punten $x=y_1e_1+\ldots+y_ne_n$, waaraan het eenheidselement van de groep is toegevoegd. Allereerst behoort O tot $\mathfrak{P}$. Als x_1 en x_2 er toe behoren, dan ook x_1+x_2. Want als $g(y_1,\ldots,y_n)= g(z_1,\ldots,z_n)=1$, dan is ook $g(y_1+z_1,\ldots,y_n+z_n)=g(y_1,\ldots,y_n).g(z_1,\ldots,z_n)= 1.1=1$. Met x behoort ook lx tot $\mathfrak{P}$ (l een geheel getal). We laten nu zien, dat er in $\mathfrak{P}$ n punten $p_1,\ldots,p_n$ zijn, die tezamen met O de ruimte R_n voortbrengen, terwijl elk punt van $\mathfrak{P}$ geschreven kan worden in de gedaante $l_1p_1+\ldots+l_np_n$, waarin $l_1,\ldots,l_n$ gehele getallen zijn.

We merken eerst op, dat de verzameling $\mathfrak{P}$ geen verdichtingspunten bezit. Stel n.l. eens, dat twee punten x_1 en x_2 van $\mathfrak{P}$ een afstand $< \frac{1}{2}$ hebben en zij / het punt $\frac{1}{2}e_1+\ldots+\frac{1}{2}e_n$, het middelpunt van de hierboven beschouwde kubus. Dan liggen de coördinaten van het punt / $-x_1+x_2$ zeker tussen O en 1 en ligt dat punt ook in die kubus. Maar $(-x_1+x_2)^* = t^*$, en dat is in strijd met de onderstelling, dat er geen twee punten van de kubus hetzelfde groepselement representeren. Zij nu $p_1 \neq 0$ een punt van $\mathfrak{P}$ met de eigenschap, dat op het verbindingslijnstuk van 0 en p_1 geen verdere punten van $\mathfrak{P}$ liggen. Dan kunnen de andere punten van $\mathfrak{P}$ op de rechte door O en p_1 geschreven worden als l_1p_1 (l_1 een geheel getal). Laten nu in $\mathfrak{P}$ reeds de punten $p_1,\ldots,p_k \neq 0$ gevonden zijn $(1 \leqslant k < n)$, die tezamen met O een k-dimensionale ruimte R_k voortbrengen, terwijl elk punt van $\mathfrak{P}$ in R_k m.b.v. gehele getallen $l_1,\ldots,l_k$ te schrijven is als $l_1p_1+\ldots+l_kp_k$. Er zijn punten van $\mathfrak{P}$ buiten R_k; neem maar een punt $x=y_1e_1+\ldots+y_ne_n$ op afstand $> n$ van de ruimte R_k; er is een punt x_1 in de beschouwde eenheidskubus dat hetzelfde groepselement representeert als x; het punt $x-x_1$ ligt buiten de ruimte R_k en behoort tot $\mathfrak{P}$. We beschouwen nu de k+1-dimensionale ruimte R_{k+1} voortgebracht door de ruimte R_k en zo 'n punt. De punten van $\mathfrak{P}$, die tot die R_{k+1} behoren, liggen in aan de ruimte R_k evenwijdige k-dimensionale ruimten, die zich niet verdichten en aequidistant zijn. Er is dus een punt p_{k+1}, dat tot $\mathfrak{P}$ en de ruimte R_{k+1} behoort en een minimale afstand tot de ruimte R_k heeft. Dan wordt de ruimte R_{k+1} voortgebracht door de punten $0,p_1,\ldots,p_{k+1}$ en kan elk punt van $\mathfrak{P}$ dat er toe behoort geschreven worden in de gedaante $l_1p_1+\ldots+l_{k+1}p_{k+1}$ met gehele getallen $l_1,\ldots,l_{k+1}$. Dpor volledige inductie zien we de juistheid in van de bewering in de vorige alinea. We noe-

men $\mathfrak{P}$ een rooster, en het stel vectoren $p_1,\ldots,p_n$ een basis van $\mathfrak{P}$.

We beschouwen nu R_n als groep, en wel optelgroep met de afspraak $x+x' = \sum y_i e_i + \sum y_i' e_i = \sum (y_i+y'_i) e_i$. Onder $p+W$ verstaan we de kubus die uit de eenheidskubus W ontstaat bij de translatie $O \to p$. De verzameling kubussen $p+W$, $p \in \mathfrak{P}$ geven we aan met $\mathfrak{P}+W$. Dan is R_n homomorf afgebeeld op G en $\mathfrak{P}$ de kern. Dus is $G \cong R_n/\mathfrak{P}$. Evenals W heeft ook elke kubus $p+W$ de eigenschap, dat de punten ervan eeneenduidig alle groepselementen representeren ($p \in \mathfrak{P}$); de punten die bij de translatie $O \to p$ in elkaar overgaan representeren hetzelfde groepselement. Elk punt x van R_n ligt in een kubus, omdat er wegens de onderstelling altijd een der punten $x-p$ ($p \in \mathfrak{P}$) tot W behoort. Ook kan een punt x niet in twee verschillende kubussen $p+W$, $q+W$ liggen ($p,q \in \mathfrak{P}$), omdat anders in strijd met de onderstelling zowel $x-p$ als $x-q$ in W gelegen was. De verzameling $\mathfrak{P}+W$ levert dus een enkelvoudige overdekking van R_n. Hebben we omgekeerd een rooster $\mathfrak{P}$ in R_n, d.w.z. een ondergroep van de optelgroep R_n met een basis bestaande uit n punten $p_1,\ldots,p_n$ welke tezamen met O de ruimte R_n voortbrengen, en levert de kubussenverzameling $\mathfrak{P}+W$ een enkelvoudige overdekking van R_n, dan is $R_n/\mathfrak{P}$ een groep G met de aan het begin van 5. opgesomde eigenschappen, en wel $\tau_1=\ldots=\tau_n=1$. Men laat dan x de nevenklasse $x+\mathfrak{P}$ representeren; van elke nevenklasse ligt één punt $x+p$ in W. We noemen W wel een fundamentaalgebied van de ondergroep $\mathfrak{P}$ in de groep R_n.

Indien nu het element $g(0,0,\ldots,1,\ldots,0)$ uit G met alle parameters 0, behalve de i^{de} die gelijk aan 1 is, gelijk is aan het eenheidselement $g(0,0,\ldots,0)$ van G, dan betekent dit dat het rooster $\mathfrak{P}$ de eenheidsvector e_i bevat. Betreffende de verzameling $\mathfrak{P}+W$ kan men zeggen: daarin komt voor W, e_i+W, algemeen le_i+W (l een geheel getal). Omdat nu de vector e_i als ribbe van W optreedt, vormen die kubussen een zuil, waarbij steeds twee opeenvolgende een geheel zijvlak met elkaar gemeen hebben. Hetzelfde geldt, als p een willekeurig punt van $\mathfrak{P}$ is, voor de kubussen $p+le_i+W$. De verzameling $\mathfrak{P}+W$ is dus in zuilen gerangschikt.

Het resultaat is, dat we de te bewijzen bewering zo kunnen uitspreken:
(I) Is $\mathfrak{P}$ een rooster in R_n, W de eenheidskubus en geeft de verzameling $\mathfrak{P}+W$ een enkelvoudige overdekking van R_n, dan bevat $\mathfrak{P}$ een eenheidsvector, anders gezegd, is de kubussenverzameling $\mathfrak{P}+W$ gezuild.

Een voorbeeld van een groep met de aan 't begin van 5. vooropgestelde eigenschappen krijgt men door in R_n, als optelgroep beschouwd, het fundamentaalrooster $\mathfrak{N}$ te nemen van de punten, waarvan alle coördinaten gehele getallen zijn en de factorgroep $Rn/\mathfrak{N}$ te vormen, bestaande uit de restklassen $x^* = x+\mathfrak{N}$, $x \in R_n$.

6. We bespreken nu een probleem betreffende diophantische approximaties en sporen de samenhang daarvan op met de bewering (I). Vervolgens wordt de bewering (I) teruggevoerd op de groepentheoretische stelling van Hajós.

We houden ons bezig met een stelsel van n homogene reele lineaire vormen in n variabelen $x_1,\ldots,x_n$, en wel

$$\begin{cases} L_1(x_1,\ldots,x_n)=\alpha_{11}x_1+\ldots+\alpha_{1n}x_n \\ \hline L_n(x_1,\ldots,x_n)=\alpha_{n1}x_1+\ldots+\alpha_{nn}x_n \end{cases} \qquad A=(\alpha_{ij}),\ |A|=\det(\alpha_{ij})\neq 0.$$

Zijn $\tau_1,\ldots,\tau_n$ positieve getallen en vatten we $x_1,\ldots,x_n$ als de coördinaten van een punt in R_n op, dan wordt door de ongelijkheden

$$(1) \qquad |L_i(x_1,\ldots,x_n)|\leq \tau_i \quad (i=1,\ldots,n)$$

een parallelotoop in R_n gedefinieerd, begrensd door n paren van evenwijdige n-1-dimensionale ruimten. De vraag of (1) door een stel gehele waarden van $x_1,\ldots,x_n$ bevredigd wordt is aequivalent met de vraag of dat parallelotoop een punt van het fundamentaalrooster $\mathfrak{R}$ bevat, roosterpunt geheten. We sluiten hierbij het stel $x_1=\ldots=x_n=0$ en daarmee corresponderend de oorsprong in R_n uit, omdat het triviaal is dat die aan de vraag voldoen.

Een algemene stelling zegt: is een gebied K in R_n symmetrisch t.o.v. de oorsprong, begrensd en convex, d.w.z. behoort $\theta x+(1-\theta)y$ er toe $(0\leq\theta\leq 1)$, als x en y er toe behoren, en heeft K een volume groter dan 2^n, dan bevat K behalve 0 nog een punt van $\mathfrak{R}$ in zijn inwendige. Om dit te bewijzen vorme men uit K het lichaam $\frac{1}{2}K$ door vanuit 0 met de factor $\frac{1}{2}$ te vermenigvuldigen; het volume V van $\frac{1}{2}K$ is groter dan 1. Evenals in 5. kunnen we, R_n als optelgroep opvattende, de verzameling $\mathfrak{R}+\frac{1}{2}K$ van de gebieden $n+\frac{1}{2}K$, $n\in\mathfrak{R}$ beschouwen, die uit K ontstaan door de translatie $0\to n$.

Men heeft zo een roostervormige opstelling van lichamen, allen met hetzelfde volume, groter dan 1, terwijl het fundamentaalgebied van het rooster $\mathfrak{R}$, b.v. de eenheidskubus, het volume 1 heeft. Men bewijst nu, wat we niet verder uitvoeren, dat elk lichaam uit de verzameling met een of meer andere gemeenschappelijke inwendige punten heeft. Men bewijst ook: is het volume van K gelijk aan 2^n, dus dat van $\frac{1}{2}K$ gelijk aan 1 en is geen enkel punt van R_n inwendig punt van twee verschillende lichamen uit de verzameling, dan is elk punt van R_n inwendig- of randpunt van een der lichamen. Is nu x inwendig punt van $n_1+\frac{1}{2}K$ en ook van $n_2+\frac{1}{2}K$, dan zijn in $\frac{1}{2}K$ bevat de beide punten $x-n_1$ en $x-n_2$. Wegens de symmetrie is ook n_2-x, en dan ook $\frac{1}{2}(x-n_1+n_2-x)=\frac{n_2-n_1}{2}$ in $\frac{1}{2}K$ bevat. Maar dan is n_2-n_1, wat een roosterpunt $\neq 0$ is, bevat in K, en wel als inwendig punt.

Keren we terug tot onze lineaire vormen. Voeren we de niet-singuliere affiene transformatie

$$\begin{cases} \xi_1=\alpha_{11}x_1+\ldots+\alpha_{1n}x_n \\ \hline \xi_n=\alpha_{n1}x_1+\ldots+\alpha_{nn}x_n \end{cases}$$

uit, dan gaat het door (1) bepaalde gebied over in het parallelotoop $|\xi_i| \leq \tau_i$ $(i=1,\ldots,n)$ met volume $2\tau_1 \ldots 2\tau_n = 2^n \prod_{i=1}^{n} \tau_i$. Het heeft dus zelf als volume $\frac{1}{|A|} 2^n \prod_{i=1}^{n} \tau_i$. Indien nu de getallen τ_i voldoen aan $\prod_{i=1}^{n} \tau_i \geq |A|$, dan is gemakkelijk na te gaan dat alle voorwaarden van de stelling vervuld zijn. Er is dan dus een roosterpunt $(x_1,\ldots,x_n) \neq 0$, zodat voldaan is aan

$$(2) \qquad |L_i(x_1,\ldots,x_n)| < \tau_i \quad (i=1,\ldots,n).$$

We kunnen ook bewijzen: zijn $\tau_1,\ldots,\tau_n$ positieve getallen en is $\prod_{i=1}^{n} \tau_i = |A|$, dan is er een roosterpunt $(x_1,\ldots,x_n) \neq 0$, zodat (1) geldt. Om dit in te zien, merken we op, dat voor elke positieve waarde van ε te voldoen is aan $|L_i(x_1,\ldots,x_n)| < \tau_i'$, als we kiezen $\tau_1' = \tau_1(1+\varepsilon)$, $\tau_i' = \tau_i$ $(i=2,\ldots,n)$. Laten we nu ε tot nul naderen, dan is er steeds een roosterpunt $\neq 0$, dat aan de vraag voldoet; eventueel moet men, als ε beneden een bepaalde waarde daalt, op een ander roosterpunt overgaan, doordat het oorspronkelijke erbuiten komt te liggen. Maar zo 'n verandering is slechts eindig veel malen nodig, omdat er slechts eindig veel roosterpunten in het (begrensde) lichaam liggen. Dus is er zelfs een roosterpunt, dat voldoet aan,

$$(3) \qquad |L_1(x_1,\ldots,x_n)| \leq \tau_1, |L_i(x_1,\ldots,x_n)| < \tau_i \quad (i=2,\ldots,n).$$

Hier rijst nu het volgende probleem, behandeld door Minkowski en Hajós: Kan in (3) in de eerste ongelijkheid het gelijkteken worden weggelaten? Wanneer we de n vormen opvolgend door $\pm\tau_1, \tau_2, \ldots, \tau_n$ delen, zodat de determinant van het vormenstelsel, die eerst evnt. op teken na gelijk was aan $\prod_{i=1}^{n} \tau_i$, gelijk wordt aan 1, dan luidt het probleem:

Als $L_1(x_1,\ldots,x_n),\ldots,L_n(x_1,\ldots,x_n)$ n reële, homogene, lineaire vormen zijn met determinant 1, is er dan een roosterpunt $(x_1,\ldots,x_n) \neq 0$, zodat geldt $|L_i(x_1,\ldots,x_n)| < 1$ voor $i=1,\ldots,n$. We zullen voortaan het probleem alleen in deze gedaante bekijken.

Van vormenstelsels, waarvoor er niet zo 'n roosterpunt is, zullen we zeggen dat ze in het grensgeval verkeren.

7. Zij x de vector met componenten $x_1,\ldots,x_n$. Dan is Ax de vector met componenten $L_1(x_1,\ldots,x_n),\ldots,L_n(x_1,\ldots,x_n)$. Er geldt nu de stelling: (II) Kan men de vormen in een zodanige volgorde plaatsen, dat de coefficientenmatrix A te schrijven is als DU, waarin D een triangulaire matrix is met in de hoofddiagonaal louter enen en daarboven nullen, en U een matrix met gehele getallen als coefficienten en determinantwaarde ± 1, terwijl DU het gewone matrixproduct is, dan verkeert het stelsel vormen in het grensgeval. En omgekeerd: verkeert het stelsel vormen in het grensgeval, dan heeft het de genoemde eigenschap.

Het eerste deel van deze stelling is bijna triviaal. In het geval A=D heeft het vormenstelsel n.l. de gedaante:

$$\begin{cases} L_1(x_1,\ldots,x_n)=x_1 \\ L_2(x_1,\ldots,x_n)=\alpha_{21}x_1+x_2 \\ \hline L_n(x_1,\ldots,x_n)=\alpha_{n1}x_1+\ldots+\alpha_{n,n-1}x_{n-1}+x_n \end{cases}$$

Is nu voor een roosterpunt $|L_i|<1$ voor $i=1,\ldots,n$, dan is op grond van de eerste ongelijkheid, n.l. $|x_1|<1$, alvast $x_1=0$; maar dan is evenzo op grond van de tweede $x_2=0$, en evenzo is $x_3=\ldots=x_n=0$. Door een transformatie $x=Ux'$ wordt een roosterpunt x overgevoerd in een roosterpunt x', en omgekeerd, omdat de inverse van U een matrix is met dezelfde eigenschappen als U; verder gaat 0 in 0 over. Bovenstaand stelsel gaat bij de substitutie $x=Ux'$ over in een nieuw stelsel met als coefficientenmatrix DU; er was eerst geen roosterpunt $\neq 0$ dat aan de ongelijkheden $|L_i|<1$ voldeed, dus ook na de substitutie niet. Volgordeverandering verandert natuurlijk niets aan de situatie.

Het bewijs van het tweede deel is lastig. We geven eerst een andere karakterisering van het grensgeval (zie blz. 8): de verzameling $\mathfrak{M}+\frac{1}{2}K$, waarin $\mathfrak{M}$ het fundamentaalrooster is en K het lichaam $|L_i|<1$, levert een overdekking van R_n, die voorts, afgezien van de randpunten van de lichamen in die verzameling, enkelvoudig is. Verder passen we de substitutie $z=Ax$ toe, z een vector met componenten $z_1=L_1(x_1,\ldots,x_n),\ldots,z_n=L_n(x_1,\ldots,x_n)$. Daarbij gaat $\frac{1}{2}K$ over in het lichaam, bepaald door $|z_i|<\frac{1}{2}$ $(i=1,\ldots,n)$, dat is een eenheidskubus, zeg W, $\mathfrak{M}$ in een of ander scheef rooster $\mathfrak{P}$, en de verzameling $\mathfrak{M}+\frac{1}{2}K$ in een roostervormig opgestelde verzameling $\mathfrak{P}+W$ van kubussen. Als we hierin voor W de eenheidskubus nemen, bepaald door $0\leqslant z_i\leqslant 1$, dan betekent dat voor de verzameling $\mathfrak{P}+W$ een translatie, en blijft de enkelvoudige overdekking van R_n gehandhaafd. Tenslotte kunnen we schrijven: $\mathfrak{P}=A\mathfrak{M}$. Voor het tweede deel van de stelling (II) kunnen we nu de volgende aequivalente formulering (II*) geven: Is W de eenheidskubus, $\mathfrak{P}$ een rooster, en levert de verzameling $\mathfrak{P}+W$ een enkelvoudige overdekking van R_n, dan is $\mathfrak{P}$ bij geschikte nummering der coördinaten van de gedaante $DU\mathfrak{M}$. We merken op dat $U\mathfrak{M}$ hetzelfde is als $\mathfrak{M}$, en dus $DU\mathfrak{M}=D\mathfrak{M}$ is, wegens de eigenschappen van de matrix U.

Verder elimineren we de moeilijkheid, dat de enkelvoudige overdekking niet opgaat voor sommige punten van R_n, n.l. de randpunten van de kubussen, op de volgende wijze. Neem voor W de half-open kubus, gedefinieerd door $0\leqslant z_i<1$ $(i=1,\ldots,n)$; in 5. gingen we daar al van uit. Zij $\mathfrak{A}$ het punt, waarvan alle componenten gelijk aan 1 zijn, en ε een positief getal. Zij x een willekeurig punt van R_n. Omdat de punten van het rooster $\mathfrak{P}$ zich niet verdichten, is er een ε, zodat het lijnstuk dat x verbindt met het punt $x+\varepsilon\mathfrak{A}$, geheel tot één kubus, zeg $p+W$, behoort. Is daarbij x randpunt, dan is $x-p$ weliswaar randpunt van de kubus W, maar het maakt zeker deel uit van het voor de half-open kubus toegelaten gedeelte van de rand, omdat $x+\varepsilon\mathfrak{A}-p$ ook tot W behoort en de coördinaten

van $\mathcal{EA}$ allen positief zijn. Uit dit alles volgt, dat bij de nieuwe definitie van W elk punt van R_n zonder uitzondering tot één en slechts één kubus behoort.

We tonen de aequivalentie aan van (II*) met (I) (zie 5.). In de ene richting is dat gemakkelijk: $D\mathcal{A}$ bevat de eenheidsvector e_1. In de andere richting gaat het als volgt. Voor n=1 spreekt II* voor zichzelf. Is I bewezen en geldt II* voor de ruimten $R_1,\ldots,R_{n-1}$, dan volgt de geldigheid voor R_n aldus. Laat, bij geschikte nummering der coördinaten, e_1 een in $\mathcal{F}$ bevatte eenheidsvector zijn. Voer in R_n de loodrechte projectie uit op de n-1-dimensionale ruimte $x_1=0$. Dan gaat W over in een n-1-dimensionale eenheidskubus W' en $\mathcal{P}$ in een n-1-dimensionaal rooster $\mathcal{P}'$. I.v.m. het gezuild zijn van de verzameling $\mathcal{P}+W$ levert ook de verzameling $\mathcal{P}'+W'$ een enkelvoudige overdekking van de ruimte $x_1=0$ van dimensie n-1. Dan heeft $\mathcal{P}'$ een basis van de vorm

$$q_1'=(0,1,0,\ldots,0)$$
$$q_2'=(0,*,1,0,\ldots,0)$$
$$\text{---------------------}$$
$$q_{n-1}'=(0,*,\ldots,*,1).$$

Elke q_i' is beeld van een q_i, die met q_i' alleen in de 1^e coördinaat verschilt. Het rooster $\mathcal{Q}$ met basis $e_1,q_1,\ldots,q_{n-1}$ is van de vorm $D\mathcal{A}$ en er geldt voor: $\mathcal{Q}\subset\mathcal{P}$, terwijl de basisvectoren van $\mathcal{Q}$, evenals die van $\mathcal{P}$ een parallelotoop van volume 1 opspannen. Dus $\mathcal{Q}=\mathcal{P}$.

Voor het bewijs van II is nu nog nodig het bewijs van I. Dit wordt gegeven in 8. en 9. door I terug te voeren op de groepentheoretische stelling uit 1. In 8. behandelen we het geval, dat van alle punten die tot $\mathcal{P}$ behoren alle coördinaten rationale getallen zijn; we noemen het rooster dan rationaal. In 9. wordt het geval besproken, dat $\mathcal{P}$ geen rationaal rooster is.

8. Laat dus het rooster $\mathcal{P}$ een basis $u_1=(a_{11},\ldots,a_{1n}),\ldots u_n=(a_{n1},\ldots,a_{nn})$ bezitten met a_{ij} rationaal (i,j=1,...,n). Zij q_i een gemeen veelvoud ≥ 2 van de noemers van $a_{1i},\ldots,a_{ni}$ en zij $\mathcal{Q}$ het rooster met als basis de n vectoren $t_i=\frac{1}{q_i}e_i$ (i=1,...,n). Dan is $\mathcal{P}$ bevat in $\mathcal{Q}$. Beschouwen we $\mathcal{P}$ en $\mathcal{Q}$ als optelgroepen, dan is $\mathcal{P}$ een ondergroep van $\mathcal{Q}$. We richten onze aandacht nu op de factorgroep $G=\mathcal{Q}/\mathcal{P}$, bestaande uit de nevenklassen $q+\mathcal{P}$ $(q\in\mathcal{Q})$.

Voeren we het parallelotoop Z in, gedefinieerd door $0\leq z_i<\frac{1}{q_i}$, dan vormt de verzameling $\mathcal{Q}+Z$ een enkelvoudige overdekking van R_n; is elk parallelotoop uit die verzameling bevat in één der kubussen uit $\mathcal{P}+W$, en geven de verzamelingen $q+\mathcal{P}+Z$ een meetkundige beschrijving van de factorgroep $\mathcal{Q}/\mathcal{P}$. Speciaal zien we aan de hand daarvan de eindigheid van G in: G bevat zoveel elementen als er parallelotopen q+Z in W bevat zijn, en wel $\prod_{i=1}^{n} q_i$. Stellen we $t_i+\mathcal{P}$ voor door g_i, dan zijn $g_1,\ldots,g_n$ elementen van G met de eigenschap, dat de sommen $k_1g_1+\ldots+k_ng_n$

met k_i geheel en $0 \leq k_i < q_i$ $(i=1,\ldots,n)$ eeneenduidig de groepselementen representeren. Maar dan is er wegens 1. -4. (daar werd de groepoperatie multiplicatief geschreven, hier additief) een index i, waarvoor $q_i g_i = 0$ is, d.w.z. $q_i t_i = e_i \in \mathfrak{P}$. Dit moesten we bewijzen.

9. We bewijzen nu I uit het ongerijmde voor het geval van een niet-rationaal rooster door aan te tonen: is I onjuist voor een niet-rationaal rooster, dan is er ook een rationaal rooster, waarvoor I onjuist is.

We letten op de 1ste coördinaat van de punten van $\mathfrak{P}$. Zij $\mathfrak{P}_0$ de verzameling der tot $\mathfrak{P}$ behorende punten, waarvan de eerste coördinaat een rationaal getal is. Beschouwen we $\mathfrak{P}$ als optelgroep, dan is blijkbaar $\mathfrak{P}_0$ een ondergroep. De nevenklassen van $\mathfrak{P}_0$ in $\mathfrak{P}$ hebben de eigenschap: twee punten van $\mathfrak{P}$ behoren dan en slechts dan tot dezelfde nevenklasse als hun eerste coördinaten een rationaal getal verschillen; twee nevenklassen ontstaan uit elkaar door een translatie. $\mathfrak{P}_0$ brengt een zekere deelruimte R_m voort $(1 \leq m \leq n)$. Evenals in 5. voor $\mathfrak{P}$ in R_n kunnen we hier voor $\mathfrak{P}_0$ in R_m een basis vinden, bestaande uit m vectoren $v_1,\ldots,v_m$.

In R_m liggen geen andere punten van $\mathfrak{P}$ dan zulke, die tot $\mathfrak{P}_0$ behoren. Stel eens $p \in \mathfrak{P}$, $p \in R_m$, $p \notin \mathfrak{P}_0$. Dan is de 1ste coördinaat van p irrationaal. Tevens behoren alle veelvouden lp tot R_m, en ook de verzamelingen $lp+\mathfrak{P}$, allen uit punten van $\mathfrak{P}$ bestaande. Is nu R het parallelotoop, opgespannen door $v_1,\ldots,v_m$, dan ligt van elk van de oneindig vele verschillende verzamelingen $lp+\mathfrak{P}_0$ een punt in R; maar dan moeten de punten van $\mathfrak{P}$ een verdichtingspunt hebben, in strijd met de eigenschappen van het rooster $\mathfrak{P}$.

De punten van $\mathfrak{P}$ die tot R_m behoren vormen dus $\mathfrak{P}_0$. Met de methode van 5. kunnen we nu $v_1,\ldots,v_m$ aanvullen met $v_{m+1},\ldots,v_n$ tot een basis van $\mathfrak{P}$. De 1ste coördinaten van $v_{m+1},\ldots,v_n$ zijn beslist irrationaal.

Zij s een rechte evenwijdig aan de x_1-as. Die rechte snijdt elke (half-open) kubus uit de verzameling $\mathfrak{P}+W$ volgens een half-open lijnstuk ter lengte 1. Omdat elk punt van s tot precies één kubus behoort, is er een klasse van kubussen, die door s gesneden worden, volgens aan elkaar aansluitende lijnstukken te lengte 1; voor twee kubussen p+W, q+W uit die klasse verschillen de 1ste coördinaten van p en q een geheel, dus een rationaal getal. Is dus $\mathfrak{P}_\nu$ een nevenklasse van $\mathfrak{P}_0$ en $\mathfrak{P}_\nu+W$ de verzameling kubussen p+W met $p \in \mathfrak{P}_\nu$, dan wordt s door de verzameling $\mathfrak{P}_\nu+W$ óf helemaal óf in 't geheel niet overdekt. Onderwerpen we nu de verzamelingen $\mathfrak{P}_\nu+W$, onafhankelijk van elkaar, aan translaties van x_1-richting, dan blijft voor elke rechte evenwijdig aan de x_1-as, en dus voor de gehele ruimte R_n, de enkelvoudige overdekking door de verzameling van alle kubussen gehandhaafd.

We passen het laatste toe op de volgende verandering: vervanging van $\mathfrak{P}$ door het rooster $\mathfrak{P}^*$, opgebouwd op n vectoren $v_1,\ldots,v_m$, $v^*_{m+1},\ldots,v^*_n$, waarbij de 1e coördinaat van v^*_i rationaal is, terwijl v^*_i en v_i alleen in de 1ste coördinaat verschillen, en wel in absolute

waarde minder dan een nader te bepalen bedrag $\varepsilon < 1$. (i=m+1,...,n). Beschouw de vectoren $p=l_1v_1+\ldots+l_nv_n$ uit $\mathcal{P}$, waarvan alle coördinaten in absolute waarde hoogstens gelijk aan 2 zijn. Laten N en η positieve getallen zijn, zodat voor die vectoren $|l_i| < N$ is en de lengte van de vectoren $p-e_i$ groter dan η (i=1,...,n). Bij bovengenoemde verandering kiezen we nu $\varepsilon = \eta/N$. Dan gelden de voorwaarden van stelling I ook voor het rooster $\mathcal{P}^*$, dat geen eenheidsvector bevat en waarvan alle punten een rationale 1ste coördinaat bezitten.

Op de andere coördinaten passen we zonodig eenzelfde procédé toe. Zo komen we op een rationaal rooster, waarvoor I niet geldt.

10. Litteratuur:

H.Minkowski,	Geometrie der Zahlen (1896)
J.F.Koksma	Diophantische Approximationen, Ergebn. d. Math. IV, 4 (1936).
G.Hajós	Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, Math.Zeitschr. 47 (1942), 427-467.
L.Rédei	Vereinfachter Beweis des Satzes von Minkowski-Hajós, Acta Scient.Math.13 (Szeged) (1949) 21-35
L.Rédei	Kurzer Beweis des Gruppentheoretischen Satzes von Hajós, Commentarii Math.Helv. 23 (1949), 272-282.
I.Fáry	Die Aequivalente des Minkowski-Hajósschen Satzes in der Theorie der topologischen Gruppen, Commentarii Math. Helv. 23 (1949), 283-287.