

De Stelling van Minkowski

Hugo Zock

25 maart 2021

1 Inleiding

De stelling van Minkowski, ook wel de eerste stelling van Minkowski genoemd, is eind negentiende eeuw bewezen door Hermann Minkowski. Deze stelling wordt gezien als de basis voor het vakgebied genaamd de *meetkunde der getallen* [Min10]. Dit vakgebied is aanvankelijk ontwikkeld als hulpmiddel in de getaltheorie om onder andere vragen over diofantische approximatie en kwadratische vormen te kunnen beantwoorden. Vandaag de dag speelt deze stelling ook een rol in toegepaste gebieden, zoals de coderingstheorie en de cryptografie.

In dit artikel zullen eerst een aantal elementaire noties over *roosters* in $\mathbf{R}^n$ besproken worden. De stelling van Minkowski zal vervolgens aan de hand hiervan geformuleerd en bewezen worden. Tot slot, zal ter illustratie van de hoofdstelling een klassieke uitspraak uit de getaltheorie bewezen worden; te weten een stelling van Fermat over *sommen van twee kwadraten*.

2 Roosters in $\mathbf{R}^n$

In deze paragraaf worden de basisbegrippen over roosters in de euclidische ruimte besproken. Met het *volume* van een verzameling $A \subset \mathbf{R}^n$ wordt de Lebesgue-maat van deze verzameling bedoeld. Wanneer over het volume van een verzameling wordt gesproken, wordt impliciet aangenomen dat deze verzameling Lebesgue-meetbaar is.

Definitie 1. We noemen een ondergroep $L \subset \mathbf{R}^n$ van de vorm

$$L = \mathbf{Z}v_1 + \dots + \mathbf{Z}v_k, \quad (2.1)$$

met $v_1, \dots, v_k \in \mathbf{R}^n$ een collectie $\mathbf{R}$ -lineair onafhankelijke vectoren, een rooster. We noemen $v_1, \dots, v_k$ een basis voor L en k de rang van L . Indien $k = n$ geldt, spreken we van een volledig rooster.

Zij $L \subset \mathbf{R}^n$ een volledig rooster en $v_1, \dots, v_n$ een basis voor L . Definieer de verzameling $\Phi \subset \mathbf{R}^n$ door

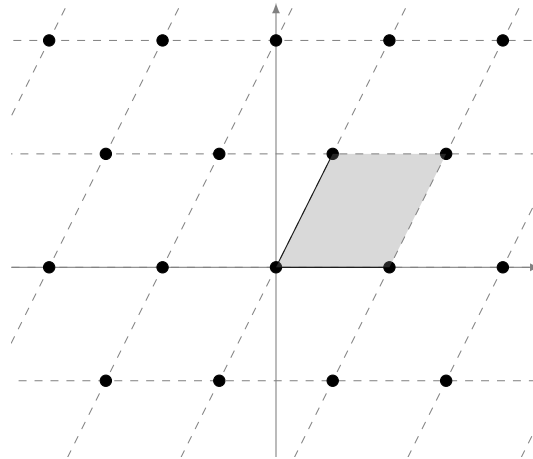
$$\Phi = \{\lambda_1 v_1 + \dots + \lambda_n v_n : 0 \leq \lambda_i < 1\}. \quad (2.2)$$

Φ wordt een *fundamenteel domein* voor L genoemd. Dit wil zeggen dat ieder element $v \in \mathbf{R}^n$ op unieke wijze te schrijven is als een som $v = x + \ell$, met $x \in \Phi$ en $\ell \in L$. Deze uitspraak volgt direct uit het feit dat $v_1, \dots, v_n$ een basis voor $\mathbf{R}^n$ vormt, en ieder reëel getal op unieke wijze te schrijven is als een som van een geheel getal en een element uit het interval $[0, 1)$. Dit leidt nu tot de observatie dat $\mathbf{R}^n$ “netjes” overdekt wordt door de translaties van Φ met elementen uit L :

$$\mathbf{R}^n = \bigcup_{\ell \in L} (\Phi + \ell), \quad (\Phi + \ell) \cap (\Phi + \ell') = \emptyset \text{ voor } \ell \neq \ell'. \quad (2.3)$$

Voorbeeld 1. (roosters en niet-roosters)

1. De ondergroepen $\mathbf{Z}(1, 2) + \mathbf{Z}(2, 0) \subset \mathbf{R}^2$ en $\mathbf{Z}\pi \subset \mathbf{R}$ zijn roosters van respectievelijk rang 2 en rang 1.
2. De ondergroep $\mathbf{Z} + \mathbf{Z}\sqrt{2} = \mathbf{Z}[\sqrt{2}] \subset \mathbf{R}$ is geen rooster in $\mathbf{R}$.



Figuur 1: Het rooster $\mathbf{Z}(1, 2) + \mathbf{Z}(2, 0)$ en een van zijn fundamentele domeinen.

Een cruciale observatie is de volgende; de ondergroepen $\mathbf{Z}(1, 2) + \mathbf{Z}(2, 0) \subset \mathbf{R}^2$ en $\mathbf{Z}\pi \subset \mathbf{R}$ zijn *discreet*, terwijl $\mathbf{Z}[\sqrt{2}]$ dat niet is.

Definitie 2. we noemen een ondergroep $A \subset \mathbf{R}^n$ *discreet* als er voor ieder punt $x \in A$ een omgeving van x in $\mathbf{R}^n$ bestaat zonder andere punten van A .

Opmerking 1. Dit is equivalent aan de uitspraak dat iedere begrensde verzameling van $\mathbf{R}^n$ slechts eindig veel punten van A bevat.

Om in te zien dat $\mathbf{Z}[\sqrt{2}]$ niet discreet is, bekijken we het rijtje $((\sqrt{2} - 1)^n)_{n=0}^{\infty}$ van elementen uit $\mathbf{Z}[\sqrt{2}]$. Dit rijtje convergeert naar nul, waaruit volgt dat iedere omgeving van 0 in $\mathbf{R}^2$ punten van dit rijtje bevat.

Dit blijkt een karakterisering van roosters op te leveren die door de volgende propositie precies wordt gemaakt.

Propositie 1. Een ondergroep $L \subset \mathbf{R}^n$ is een rooster dan en slechts dan als L discreet is. ■

Deze propositie biedt een boel motivatie voor het bestuderen van roosters. Dit laat namelijk zien dat de klasse van roosters aanzienlijk groter is dan men wellicht aanvankelijk vermoedt. Voor het bewijs van propositie 1 verwijzen we de geïnteresseerde lezer door naar [Neu99], propositie 4.2.

Men kan dus over roosters nadenken als discrete punten in de ruimte met een bepaalde dichtheid. Dit geeft aanleiding tot het volgende begrip.

Propositie 2. Zij $L \subset \mathbf{R}^n$ een volledig rooster. Kies een basis $v_1, \dots, v_n$ van L . We noemen

$$d(L) := \text{vol } \Phi = |\det(v_1, \dots, v_n)|, \quad (2.4)$$

met Φ zoals in vergelijking 2.2, de determinant van L . Deze is onafhankelijk van de keuze van basis $v_1, \dots, v_n$.

Bewijs. Laat $w = (w_1, \dots, w_m)$ een tweede basis voor L zijn en schrijf $v = (v_1, \dots, v_n)$. Definieer het lineaire automorfisme $\varphi : \mathbf{R}^n \rightarrow \mathbf{R}^n$ door v_i naar w_i te sturen voor $i = 1, \dots, n$. Uit het feit dat geldt $w_i \in \mathbf{Z}v_1 + \dots + \mathbf{Z}v_n$, volgt dat de matrix van φ t.o.v de basis v , $(\varphi)_v$, gehele coëfficiënten heeft. Hieruit volgt $\det \varphi = \det(\varphi)_v \in \mathbf{Z}$. Met analoge argumentatie vinden we zo ook $(\det \varphi)^{-1} = \det \varphi^{-1} = \det(\varphi^{-1})_w \in \mathbf{Z}$. Nu moet gelden $\det \varphi \in \{\pm 1\}$, en dus

$$|\det(w_1, \dots, w_n)| = |\det \varphi| \cdot |\det(v_1, \dots, v_n)| = |\det(v_1, \dots, v_n)|.$$

■

3 De stelling van Minkowski

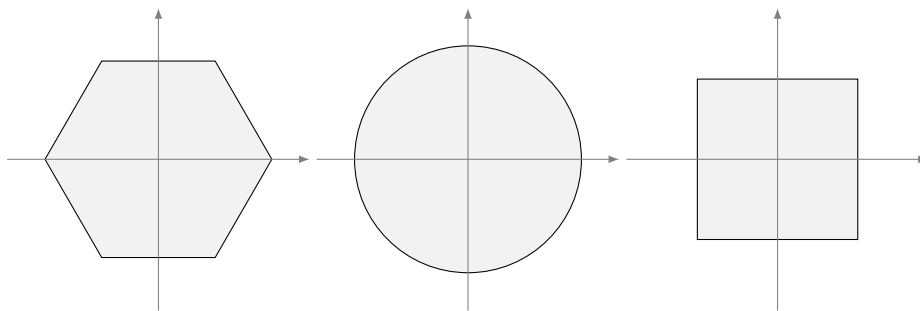
Enigszins onzorgvuldig gezegd vertelt de stelling van Minkowski ons iets over de connectie tussen meetkundige eigenschappen van deelverzamelingen van de Euclidische ruimte, en discrete eigenschappen: het bevatten van roosterpunten. Gegeven een rooster, kan men zich afvragen onder welke voorwaarden een deelverzameling van $\mathbf{R}^n$ roosterpunten moet bevatten. De stelling van Minkowski geeft hiervoor voldoende voorwaarden.

Ter herinnering herhalen we hier de begrippen convexiteit en symmetrie voor deelverzamelingen van de euclidische n -ruimte. Zij $X \subset \mathbf{R}^n$ een deelverzameling. X heet *convex*, als voor alle $x, y \in X$ en $\lambda \in [0, 1]$ geldt $\lambda x + (1 - \lambda)y \in X$. X heet *symmetrisch*, als voor alle $x \in X$ geldt $-x \in X$.

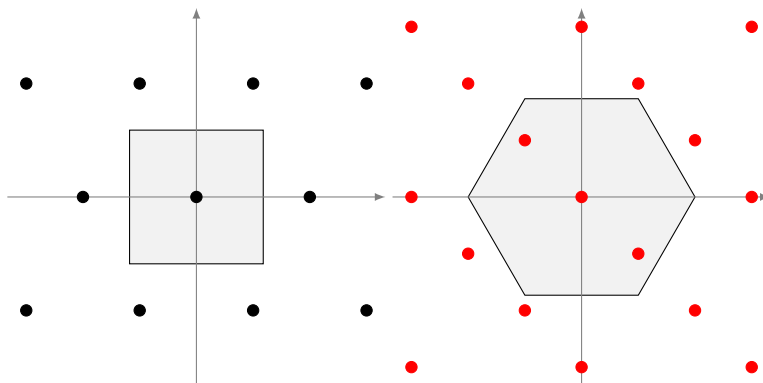
Stelling 1 (Minkowski). Zij $L \subset \mathbf{R}^n$ een volledig rooster, en zij $X \subset \mathbf{R}^n$ een symmetrische, convexe verzameling met

$$\text{vol } X > 2^n d(L). \quad (3.1)$$

Dan bevat X een punt van $L \setminus \{0\}$.



Figuur 2: Symmetrische, convexe verzamelingen.



Figuur 3: Een symmetrische, convexe verzameling die geen niet-nul roosterpunten bevat (links), en een symmetrische, convexe verzameling die dat wel doet (rechts).

Opmerking 2. Iedere symmetrische, convexe verzameling bevat 0, en dus sluiten we dit roosterpunt uit in stelling 1.

Ons bewijs van deze stelling berust grotendeels op het volgende lemma dat aan de Deens-Amerikaanse wiskundige Blichfeldt wordt toegekend.

Lemma 1. Zij L een volledig rooster, en zij $X \subset \mathbf{R}^n$ een (Lebesgue-meetbare) verzameling met

$$\text{vol } X > d(L). \quad (3.2)$$

Dan bestaan er $x, y \in X$ zodanig dat geldt $x - y \in L \setminus \{0\}$.

Bewijs. Zij Φ een fundamenteel domein voor L zoals in vergelijking 2.2. Voor alle $\ell \in L$ definiëren we $X_\ell = X \cap (\Phi + \ell)$. Uit 2.3 volgt dan dat geldt $X_\ell \cap X_{\ell'} = \emptyset$ voor $\ell \neq \ell'$ en

$$\bigcup_{\ell \in L} X_\ell = X \cap \bigcup_{\ell \in L} (\Phi + \ell) = X.$$

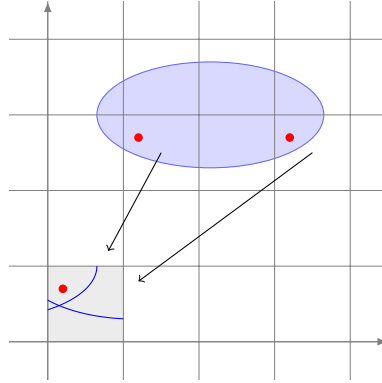
We vinden nu

$$\sum_{\ell \in L} \text{vol } X_\ell = \text{vol } \bigcup_{\ell \in L} X_\ell = \text{vol } X > d(L).$$

Definieer nu voor alle $\ell \in L$ de verzameling $\tilde{X}_\ell = X_\ell - \ell = (X - \ell) \cap \Phi \subset \Phi$. De Lebesgue-maat is invariant onder translatie, waaruit volgt $\text{vol } \tilde{X}_\ell = \text{vol } X_\ell$, en dus $\sum_{\ell \in L} \text{vol } \tilde{X}_\ell > d(L)$. Er moeten nu $\ell, \ell' \in L$ bestaan, met $\ell \neq \ell'$, en zodanig dat $\tilde{X}_\ell \cap \tilde{X}_{\ell'}$ niet leeg is. Anders vinden we namelijk

$$\sum_{\ell \in L} \text{vol } \tilde{X}_\ell = \text{vol } \bigcup_{\ell \in L} \tilde{X}_\ell \leq \text{vol } \Phi = d(L),$$

hetgeen in tegenspraak is met de eerder gevonden ongelijkheid. Laat $x, y \in X$ zodanig dat $x - \ell = y - \ell'$. Dan geldt $x - y = \ell - \ell' \in L \setminus \{0\}$. ■



Figuur 4: In het bewijs van lemma 1 wordt X (de blauwe ellips in dit plaatje) in stukjes, X_ℓ , opgesneden door de translaties van Φ (het grijze vierkant). De stukjes worden in Φ gelegd, waar naar overlap wordt gezocht.

Bewijs van stelling 1. We vinden $\text{vol } \frac{1}{2}X = 2^{-n} \text{vol } X > d(L)$. Met lemma 1 bestaan er nu $x, y \in X$ zodanig dat $\frac{1}{2}x - \frac{1}{2}y \in L \setminus \{0\}$. Uit symmetrie en convexiteit volgt $\frac{1}{2}x - \frac{1}{2}y \in X$. ■

Onder bepaalde voorwaarden kan men de eisen in stelling 1 iets verzwakken en dezelfde conclusie bereiken.

Gevolg 1. *Mits X ook gesloten en begrensd is in stelling 1, is de gelijkheid $\text{vol } X = 2^n d(L)$ voldoende om de gestelde conclusie te trekken.*

Bewijs. Voor alle $k \geq 1$ heeft $(1 + k^{-1})X$ een volume strikt groter dan $2^n d(L)$. Met stelling 1 bestaat er dan een $\ell_k \in (1 + k^{-1})X \cap L \setminus \{0\}$. De verzameling $2X \cap L$ is eindig wegens opmerking 1, en dus bestaat er een ℓ in het rijtje $\ell_1, \ell_2, \dots$ die oneindig vaak voorkomt.

Dan geldt $\ell \in \bigcap_{k \geq 1} (1 + k^{-1})X$. Voor alle $k \geq 1$ geldt nu $\frac{1}{1+k^{-1}}\ell \in X$. Uit de geslotenheid van X volgt $\lim_{k \rightarrow \infty} \frac{1}{1+k^{-1}}\ell = \ell \in X$. ■

Opmerking 3. De grens $2^n d(L)$ in de stelling van Minkowski kan echter niet scherper gemaakt worden. Bekijk bijvoorbeeld de open kubus

$$K = \{(x_1, \dots, x_n) \in \mathbf{R}^n : |x_i| < 1\} \quad (3.3)$$

van volume 2^n . K bevat geen niet-nul roosterpunten van het rooster $\mathbf{Z}^n$ met determinant 1.

4 Sommen van twee kwadraten

In deze paragraaf zal een getaltheoretische uitspraak worden bewezen middels de stelling van Minkowski. Het is op het eerste gezicht niet duidelijk dat er in deze stelling sprake is van een structuur waarop de stelling van Minkowski van toepassing is. De kunst zit dan ook voornamelijk in het aanbrengen van deze structuur: geschikte roosters en symmetrische, convexe verzamelingen construeren.

Stelling 2. *Zij p een priemgetal en stel $p \equiv 1 \pmod{4}$. Dan bestaan er gehele getallen a en b zodanig dat*

$$p = a^2 + b^2. \quad (4.1)$$

Fermat was rond 1640 al op de hoogte van deze uitspraak. Het eerste bewijs wordt echter pas in 1752 gepubliceerd door Euler. Met behulp van de stelling van Minkowski geven we hier een eenvoudig en elegant bewijs.

Lemma 2. *Zij $p \equiv 1 \pmod{4}$ priem. Dan bestaat er een geheel getal r met $r^2 \equiv -1 \pmod{p}$.*

Bewijs. Zij $(\mathbf{Z}/p\mathbf{Z})^\times$ de eenhedengroep van $\mathbf{Z}/p\mathbf{Z}$. $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclisch van orde $p-1$. Laat α een voortbrenger van $(\mathbf{Z}/p\mathbf{Z})^\times$ zijn. Er geldt

$$\left(\alpha^{\frac{p-1}{4}}\right)^2 = \alpha^{\frac{p-1}{2}} = -1.$$

Immers, $\alpha^{\frac{p-1}{2}}$ is een nulpunt van $X^2 - 1$ en ongelijk 1, omdat α orde $p-1$ heeft. ■

Bewijs van stelling 2. Met lemma 2 vinden we een $r \in \mathbf{Z}$ met $r^2 + 1 \equiv 0 \pmod{p}$. Definieer $v_1 = (1, r)$ en $v_2 = (0, p) \in \mathbf{R}^2$. Beschouw het rooster

$$L = \mathbf{Z}v_1 + \mathbf{Z}v_2.$$

Voor $w = av_1 + bv_2 \in L$ geldt

$$\begin{aligned} \|w\|^2 &\equiv a^2 + (ar + bp)^2 \\ &\equiv a^2 + a^2r^2 \\ &\equiv a^2(1 + r^2) \equiv 0 \pmod{p}. \end{aligned}$$

Er geldt $d(L) = |\det(v_1, v_2)| = p$. Definieer de verzameling

$$X = \{x \in \mathbf{R}^2 : \|x\|^2 < 2p\},$$

met volume $\text{vol } X = 2\pi p > 4p = 2^2 d(L)$. Het is verder duidelijk dat X voldoet aan de eisen van stelling 1. We vinden zo een element $\ell \in (L \setminus \{0\}) \cap X$. Er geldt $0 < \|\ell\|^2 < 2p$, en $p \mid \|\ell\|^2$, waaruit volgt $\|\ell\|^2 = p$. Door de coëfficiënten van ℓ uit te schrijven, levert dit nu de gewenste schrijfwijze van p als som van twee kwadraten. ■

Een andere uitspraak die op vergelijkbare wijze bewezen kan worden, is de *vier-kwadratenstelling* van Lagrange. Deze stelt dat ieder geheel getal $n \geq 0$ een som is van vier kwadraten. Voor de details, zie [Mat02], pagina 28.

Referenties

- [Eve17] Jan-Hendrik Evertse. *Diophantine Approximation*. Leiden, 2017. URL: <http://www.math.leidenuniv.nl/~evertse/dio17-2.pdf>.
- [Mat02] Jiří Matoušek. *Lectures on Discrete Geometry*. Graduate Texts in Mathematics, No. 212. New York: Springer-Verlag, 2002.
- [Min10] Hermann Minkowski. *Geometrie der Zahlen*. Leipzig: B.G. Teubner Verlag, 1910.
- [Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften, No. 322. Berlin: Springer-Verlag, 1999.
- [Ste19] Peter Stevenhagen. *Number Rings*. Leiden, 2019. URL: <http://websites.math.leidenuniv.nl/algebra/ant.pdf>.