Björn de Rijk (brijk@math.leidenuniv.nl)

Het lokaal-globaalprincipe

Bachelorscriptie, 18 augustus 2010

Scriptiebegeleider: drs. P. Bruin

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

1.1 Kwadratische vormen

Het oplossen van polynomiale vergelijkingen over de gehele getallen is één van de oudste en meest bestudeerde wiskundige problemen. Behalve in het expliciet geven van oplossingen is men geïnteresseerd in de existentie van oplossingen. Al rond 2000 voor Christus slaagden Babyloniërs erin om vergelijkingen met twee onbekenden op te lossen. In de 17e, 18e en 19e eeuw werden kwadratische vergelijkingen in twee variabelen uitgebreid bestudeerd door onder achtereenvolgens Fermat, Wallis, Euler, Lagrange en Gauss. Hierin worden algemene methodes behandeld, waarbij kettingbreuken worden gebruikt. Gauss generaliseerde dit concept in zijn boek Disquisitiones Arithmeticae tot vergelijkingen in kwadratische vormen. Dit zijn homogene kwadratische polynomen in een willekeurig (maar eindig) aantal variabelen. Er bestaat een algemene methode om te bepalen of een vergelijking

$$\sum_{i,j} a_{ij} X_i X_j = b \tag{1}$$

met $a_{ij}, b \in \mathbb{Q}$ een niet-triviale oplossing in de rationale getallen heeft. Met een niet-triviale oplossing wordt een oplossing bedoeld waarbij niet alle variabelen gelijk aan 0 zijn. Dit resultaat staat bekend als de stelling van Hasse en Minkowski. Als we b gelijk aan 0 nemen, dan is het duidelijk dat er niet-triviale oplossingen in de gehele getallen bestaan dan en slechts dan als er niet-triviale oplossingen in de rationale getallen zijn. Voor $b \neq 0$ kan het bestaan van een rationale oplossing onder een zekere voorwaarde op de kwadratische vorm, gevonden door Davenport en Cassels, ook de existentie van een oplossing in de gehele getallen garanderen. Hiermee kan men bewijzen dat de diophantische vergelijking

$$X^2 + Y^2 + Z^2 + W^2 = N \tag{2}$$

een oplossing in de gehele getallen heeft voor alle $N \geq 0$. Met andere woorden: we kunnen ieder natuurlijk getal schrijven als een som van vier kwadraten.[1]

1.2 Het lokaal-globaalprincipe

Zij p een priemgetal. We definiëren de functie $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ door $v_p(0) = \infty$ en $v_p(x) = n$ als $x \in \mathbb{Q}^*$, waarbij n eenduidig gedefinieerd is door de identiteit $x = p^n \frac{c}{d}$ met $c, d \in \mathbb{Z}$ zodanig dat cd niet deelbaar is door p. De functie $d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$ gegeven door $d_p(x, y) = e^{-v_p(x-y)}$ voorziet het lichaam $\mathbb{Q}$ van een metriek. Het lichaam $\mathbb{Q}_p$ der p-adische getallen is de completering onder deze metriek. We noemen de lichamen $\mathbb{Q}_p$ voor priemgetallen p samen met het lichaam $\mathbb{Q}_\infty$ der reële getallen[2] de *lokale lichamen* van $\mathbb{Q}$. In deze context is $\mathbb{Q}$ het *globale lichaam* van de lichamen $\mathbb{Q}_p$ en $\mathbb{Q}_\infty$. Het globale lichaam $\mathbb{Q}$ is ingebed in alle lokale lichamen. Een polynomiale vergelijking over $\mathbb{Q}$ kunnen we daardoor beschouwen als een vergelijking over alle lokale lichamen.

Een familie polynomiale vergelijkingen over $\mathbb{Q}$ voldoet aan het lokaal-globaalprincipe wanneer het bestaan van niet-triviale oplossingen in de lokale lichamen, de existentie van een niet-triviale oplossing over $\mathbb{Q}$ garandeert.

Laten we de triviale oplossing (de nuloplossing) toe, dan zou meteen evident zijn dat alle homogene polynomiale vergelijkingen voldoen aan het lokaal-globaalprincipe. Men is echter geïnteresseerd in het lokaal-globaalprincipe om te bepalen of er een niet-triviale oplossing van een homogene vergelijking over $\mathbb{Q}$ bestaat. Het is om die reden dat we eisen dat de oplossingen niet-triviaal zijn in de definitie van het lokaal-globaalprincipe.

[1] Als men meer wil weten over de geschiedenis van Diophantische vergelijkingen en kwadratische vergelijkingen in het bijzonder kan men kijken op [VO].

[2] Afhankelijk van de context zullen we zowel de notatie $\mathbb{Q}_\infty$ als $\mathbb{R}$ gebruiken voor dit lichaam.

Stel V is een vergelijking uit een familie polynomiale vergelijkingen die voldoet aan het lokaal-globaalprincipe. Het is voldoende na te gaan of er oplossingen in $\mathbb{Q}_\infty$ en in $\mathbb{Q}_p$ bestaan voor alle priemgetallen p van V om aan te tonen dat er een oplossing in $\mathbb{Q}$ bestaat. Het bepalen van een oplossing in $\mathbb{Q}_\infty$ van V is geen lastig probleem als we bedenken dat we methodes uit de reële analyse tot onze beschikking hebben zoals de tussenwaardestelling. Om oplossingen van V in $\mathbb{Q}_p$ te bepalen gebruiken we het lemma van Hensel. Dit is een p-adische equivalent van de Newton-Raphson methode. Door eerst V te vermenigvuldigen met een geschikte factor bekijken we V in de ring $\mathbb{Z}/p^n\mathbb{Z}$. Met het lemma van Hensel kunnen we niet-triviale oplossingen voor V in $\mathbb{Z}/p^n\mathbb{Z}$ liften naar $\mathbb{Q}_p$ onder bepaalde voorwaarden. We reduceren zo het oplossen van vergelijkingen over een lichaam $\mathbb{Q}_p$ van oneindige kardinaliteit naar het oplossen van vergelijkingen over eindige ringen. Het vinden van een niet-triviale oplossing over $\mathbb{Q}_p$ is daarom eveneens in veel gevallen eenvoudiger dan over $\mathbb{Q}$.

In deze scriptie zullen we bewijzen dat vergelijkingen van de vorm (1) aan het lokaal-globaalprincipe voldoen. Dit is de eerdergenoemde stelling van Hasse en Minkowski. Het bewijs is grotendeels gebaseerd op het bewijs uit [SE]. Hiervoor is enige kennis over de p-adische getallen en kwadratische vormen noodzakelijk. Deze zullen we in hoofdstuk 2 en 3 uit de doeken doen. In het bijzonder besteden we in hoofdstuk 3 aandacht aan de familie van kwadratische vormen $Z^2 - aX^2 - bY^2$ over een lichaam K met $a, b \in K^*$. We definiëren het Hilbertsymbool (a, b) en nemen dit gelijk aan 1 als deze vorm een niet-triviaal nulpunt heeft over K en anders gelijk aan -1. Het blijkt dat het Hilbertsymbool over de lokale lichamen van $\mathbb{Q}$ bilineair is en voor $a, b \in \mathbb{Q}$ over slechts eindig veel lokale lichamen gelijk aan -1 is. Van deze structuur zullen we gebruik maken in het bewijs van het lokaal-globaalprincipe voor kwadratische vormen. Als toepassing van de stelling van Hasse en Minkowski laten we zien dat (2) oplossingen in de gehele getallen heeft voor alle $N \geq 0$. Hierbij zien we ook hoe het lemma van Hensel van pas komt om oplossingen in $\mathbb{Q}_p$ te bepalen voor priemgetallen p.

In het tweede deel van de scriptie zullen we laten zien dat, wanneer we de kwadratische vorm uit (1) vervangen door een homogeen kubisch polynoom, het lokaal-globaalprincipe niet op zal gaan voor de verkregen familie van kubische vergelijkingen. De vergelijking $3X^3 + 4Y^3 + 5Z^3 = 0$ gevonden door de Noorse wiskundige E.S. Selmer heeft slechts een triviale oplossing over $\mathbb{Q}$, maar heeft niet-triviale oplossingen over alle lokale lichamen. Om te bewijzen dat deze vergelijking een tegenvoorbeeld is, zullen we de grotendeels de methode uit [CA] volgen. We gebruiken hierbij het feit dat we elementen uniek in een product van priemelementen kunnen factoriseren in het hoofdideaaldomein $\mathbb{Z}[\sqrt[3]{6}]$ en we hebben enige kennis nodig over de eenhedengroep van $\mathbb{Z}[\sqrt[3]{6}]$. Om te laten zien dat $\mathbb{Z}[\sqrt[3]{6}]$ een hoofdideaaldomein is, maken we gebruik van methodes uit de algebraïsche getaltheorie. De lezer die geen inleiding algebraïsche getaltheorie heeft gevolgd zal desalniettemin de hoofdlijnen van het bewijs kunnen volgen. Een inleiding algebra en topologie wordt wel als voorkennis voor het lezen van deze scriptie verondersteld.

2 p-adische getallen

2.1 De ring $\mathbb{Z}_p$

Laat p een priemgetal zijn.

2.1 Definitie. *De verzameling der p-adische gehele getallen* is

$$\mathbb{Z}_p = \{(x_n)_n \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} : x_n \equiv x_m \bmod p^m \text{ voor alle } m \leq n\}.$$

De somrij $(1, 1+p, 1+p+p^2, 1+p+p^2+p^3, \ldots)$ is bijvoorbeeld een element van $\mathbb{Z}_p$ evenals de constante rij $(b, b, \ldots)$ waarbij we een getal $b \in \mathbb{Z}$ op een natuurlijke manier als element van $\mathbb{Z}/p^n\mathbb{Z}$ zien. Er bestaat dus een inbedding $\mathbb{Z} \to \mathbb{Z}_p$. We noteren de constante rij $(b, b, \ldots)$ als b, wanneer duidelijk is dat b een geheel getal is. Elementen $x, y \in \mathbb{Z}_p$ kunnen we coördinaatsgewijs optellen en vermenigvuldigen door gebruik te maken van de ringstructuur op $\mathbb{Z}/p^n\mathbb{Z}$. Men gaat direct na dat de som $x + y$ en het product xy tevens in $\mathbb{Z}_p$ liggen. Dit maakt $\mathbb{Z}_p$ tot een ring met als neutraal element voor de optelling de constante rij 0 en de constante rij 1 als eenheidselement voor de vermenigvuldiging. Gegeven het natuurlijke homomorfisme $\phi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ voor $n \in \mathbb{Z}$ (reductie modulo p^{n-1}) kan men nu inzien dat $\mathbb{Z}_p$ de projectieve limiet is van het systeem

$$\ldots \to \mathbb{Z}/p^n\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Uit het feit dat $\mathbb{Z}_p$ een ring is, merken we op dat de inbedding $\mathbb{Z} \to \mathbb{Z}_p$ een ringhomomorfisme is evenals de surjectieve *coördinaatafbeelding* $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, waarbij een rij $x \in \mathbb{Z}_p$ wordt afgebeeld op de n-de coördinaat $\varepsilon_n(x)$. Voor $x, y \in \mathbb{Z}_p$ geeft de afbeelding ε_n aanleiding tot de notatie $x \equiv y \bmod p^n$ voor $\varepsilon_n(x) = \varepsilon_n(y)$.

2.2 De eenhedengroep $\mathbb{Z}_p^*$

Uit de constructie van $\mathbb{Z}_p$ is duidelijk dat een p-adisch geheel getal x inverteerbaar is precies als $\varepsilon_n(x) \in (\mathbb{Z}/p^n\mathbb{Z})^*$ voor alle $n \geq 1$. Een element $a \in \mathbb{Z}/p^n\mathbb{Z}$ inverteerbaar is dan en slechts dan als het beeld onder het natuurlijke ringhomomorfisme $\phi : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{F}_p$ ongelijk aan 0 is. Men gaat dit na door te gebruiken dat als $\phi(a)$ een eenheid is in $\mathbb{F}_p$, er $b, c \in \mathbb{Z}/p^n\mathbb{Z}$ bestaan zodanig dat geldt $ab = 1 - pc$, oftewel $ab(1 + pc + \ldots + p^{n-1}c^{n-1}) = 1$. We vinden dus a in $(\mathbb{Z}/p^n\mathbb{Z})^*$ precies als a niet in het ideaal $(p) = \ker \phi$ bevat is, oftewel als $p \nmid a$. We concluderen:

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : p \nmid x\}.$$

Laat nu $x \in \mathbb{Z}_p$ met $x \neq 0$. Dan bestaat er een grootste n met $\varepsilon_n(x) = 0$. Door de eis $\varepsilon_m(x) \equiv \varepsilon_{n+1}(x) \bmod p^{n+1}$ voor $m > n$ en $\varepsilon_{n+1}(x) \neq 0$ vinden we $p^{n+1} \nmid \varepsilon_m(x) \neq 0$ voor $m > n$. Elk element $x \in \mathbb{Z}_p$ ongelijk aan 0 is dus te schrijven als $x = p^n u$ met $u \in \mathbb{Z}_p^*$ en $n \geq 0$. Deze schrijfwijze is uniek. Vermenigvuldigen van twee elementen in $\mathbb{Z}_p \setminus \{0\}$ geeft weer een element van de vorm $p^n u \neq 0$ met $u \in \mathbb{Z}_p^*$ en $n \geq 0$. Het is hieruit helder dat $\mathbb{Z}_p$ een domein is.

2.3 Het lichaam $\mathbb{Q}_p$

2.2 Definitie. *Het lichaam der p-adische getallen* $\mathbb{Q}_p$ is het quotiëntenlichaam $Q(\mathbb{Z}_p)$.

Uit het voorgaande is in te zien dat ieder p-adisch getal $x \in \mathbb{Q}_p^*$ uniek schrijven als $x = p^n u$ met $n \in \mathbb{Z}$ en $u \in \mathbb{Z}_p^*$. Als gevolg kan $\mathbb{Q}_p$ tevens uit $\mathbb{Z}_p$ verkregen worden door p^{-1} aan $\mathbb{Z}_p$ te adjungeren. De natuurlijke inbedding $\mathbb{Z} \to \mathbb{Z}_p$ geeft door het nemen van quotiëntenlichamen aanleiding tot een injectief ringhomomorfisme $\mathbb{Q} \to \mathbb{Q}_p$ waarbij een breuk $\frac{a}{b}$ wordt afgebeeld op het quotiënt $\frac{a}{b} \in \mathbb{Q}_p$ van de twee constante rijen a en b.

2.4 Een metriek op $\mathbb{Q}_p$

2.3 Definitie. De *p-adische valuatie* is de functie $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ voorgeschreven door $v_p(0) = \infty$ en $v_p(x) = n$, waarbij we $x \neq 0$ schrijven als $x = p^n u$ met $n \in \mathbb{Z}$ en $u \in \mathbb{Z}_p^*$. De functie $d_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$ gegeven door $d_p(x, y) = e^{-v_p(x-y)}$ heet de *p-adische afstand*.[3]

Omdat de schrijfwijze $x = p^n u$ uniek is, is v_p een welgedefinieerde functie, waarvoor geldt $v_p(xy) = v_p(x) + v_p(y)$ en $v_p(x + y) \geq \inf\{v_p(x), v_p(y)\}$. Men gaat eenvoudig na dat d_p het lichaam $\mathbb{Q}_p$ van een metriek voorziet en verifieert dat $\mathbb{Q}_p$ een topologisch lichaam is met de topologie geïnduceerd door d_p, zie propositie 1 uit paragraaf 1.3.7 in [RO]. Dat wil zeggen dat de optelling en vermenigvuldiging continue afbeeldingen van $\mathbb{Q}_p \times \mathbb{Q}_p$ naar $\mathbb{Q}_p$ zijn, evenals het nemen van de inverse op $\mathbb{Q}_p^*$. Aangezien x een element van $\mathbb{Z}_p$ is precies als $v_p(x) \geq 0$, oftewel $v_p(x) > -1$, is $\mathbb{Z}_p$ in $\mathbb{Q}_p$ bevat als de open bol met straal e om 0. Dus is $\mathbb{Z}_p$ een open deelring van $\mathbb{Q}_p$.

2.4 Propositie. *De ring $\mathbb{Z}_p$ is volledig onder d_p.*

Bewijs. Zij $(x_k)_k$ een Cauchyrij in $\mathbb{Z}_p$ en $n \in \mathbb{N}$, dan bestaat er een kleinste $M_n \in \mathbb{N}$ zodanig dat voor alle $k, l \geq M_n$ geldt $v_p(x_k - x_l) \geq n$. Er volgt dat x_k en x_l overeenstemmen op de eerste n coördinaten voor alle $k, l \geq M_n$. Noem $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ de n-de coördinaat van x_k voor $k \geq M_n$ en beschouw de rij $a = (a_n)_n \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$. Laat nu a_m, a_n twee termen met $m \leq n$. Er geldt logischerwijs $M_m \leq M_n$. Dus is de m-de coördinaat van x_k gelijk aan a_m en de n-de coördinaat van x_k gelijk aan a_n als $k \geq M_n \geq M_m$. Uit $x_k \in \mathbb{Z}_p$ volgt $a_n \equiv a_m \bmod p^m$ en dus geldt $a \in \mathbb{Z}_p$. Voor $n \in \mathbb{N}$ bestaat er $M_n \in \mathbb{N}$ zodanig dat $v_p(x_k - a) \geq n$ voor alle $k \geq M_n$ en er volgt $\lim_{k\to\infty} x_k = a$. □

Zoals in de inleiding is het ook mogelijk om de p-adische metriek d_p op $\mathbb{Q}$ te beschouwen; de completering zal dan het lichaam $\mathbb{Q}_p$ geven. Het lichaam der reële getallen $\mathbb{Q}_\infty$ is de completering van $\mathbb{Q}$ onder de metriek d_∞ geassocieerd met de reguliere absolute waarde $|\cdot|_\infty$.

2.5 Definitie. Zij V de verzameling van priemgetallen samen met het symbool ∞. De lichamen $\mathbb{Q}_v$ voor $v \in V$ worden *lokale lichamen* van het *globale lichaam* $\mathbb{Q}$ genoemd.[4]

Zij $m \in \mathbb{N}$. Als $x \in \mathbb{Z}_p$ een p-adisch geheel getal is, dan bestaat er een $b \in \mathbb{Z}$ zodanig dat $\varepsilon_m(b) = \varepsilon_m(x)$ in $\mathbb{Z}/p^m\mathbb{Z}$. Er volgt $d_p(x, b) \leq e^{-m}$ en we zien dat $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ ligt. Door nu op te merken dat een element $x \in \mathbb{Q}_p^*$ te schrijven is als $x = p^n u$ met $n \in \mathbb{Z}$ en $u \in \mathbb{Z}_p^*$, kunnen we weer $b \in \mathbb{Z}$ kiezen zodanig dat $\varepsilon_m(b) = \varepsilon_m(u)$ en voor $p^n b \in \mathbb{Q}$ volgt $d_p(x, p^n b) = e^{-n-m}$. Duidelijk is nu dat $\mathbb{Q}$ dicht in $\mathbb{Q}_p$ ligt en samen met het bekende resultaat dat $\mathbb{Q}$ dicht in $\mathbb{Q}_\infty$ ligt, concluderen we dat $\mathbb{Q}$ een dichte deelverzameling van $\mathbb{Q}_v$ is voor alle $v \in V$. We kunnen dit resultaat enigszins verbeteren.

2.6 Propositie (Approximatiestelling)**.** *Zij $S \subset V$ eindig. Het beeld van $\mathbb{Q}$ in $\prod_{v\in S} \mathbb{Q}_v$ ligt dicht in $\prod_{v\in S} \mathbb{Q}_v$.*

Bewijs. Zij $(x_v)_{v\in S} \in \prod_{v\in S} \mathbb{Q}_v$. We moeten bewijzen dat er voor elke $\epsilon > 0$ een $x \in \mathbb{Q}$ bestaat zodanig dat $d_v(x, x_v) < \epsilon$ voor alle $v \in S$. Noem $p_1, \ldots, p_m$ de verschillende priemen in S zodanig dat $x_i \in \mathbb{Q}_{p_i}$. Door $(x_v)_{v\in S}$ met een product van de priemen $p_1, \ldots, p_m$ te vermenigvuldigen, kunnen we aannemen $x_i \in \mathbb{Z}_p$, immers we kunnen de gevonden $x \in \mathbb{Q}$ later weer delen door dat product. Zij $N \in \mathbb{N}$ zodanig dat geldt $e^{-N} < \epsilon$. Aangezien $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ ligt, bestaan er $a_1, \ldots, a_m$ in $\mathbb{Z}$ met $v_p(a_i - x_i) \geq N$. Wegens de Chinese reststelling bestaat er een $a \in \mathbb{Z}$ zodanig dat $a \equiv a_i \bmod p_i^N$, oftewel $v_p(a - x_i) \geq N$ voor alle i. Als ∞ geen element van S is, zijn we klaar. Neem daarom aan $\infty \in S$. Kies een priemgetal q zodanig dat $q \notin S$. We kiezen nu $u \in \mathbb{Z}$ en $m \geq 0$ zodanig dat $|x_\infty - a - uq^{-m}p_1 \ldots p_n| < \epsilon$. Dit is mogelijk omdat getallen van de vorm u/q^m dicht in $\mathbb{Q}_\infty$ liggen. Het getal $x = a + uq^{-m}p_1 \ldots p_n$ voldoet aan de eisen. □

[3] We definiëren de conventionele rekenregels: $e^{-\infty} := 0$ en $\pm\infty + a := \pm\infty$ voor $a \in \mathbb{Z}$.

[4] Merk op dat men ook spreekt over lokaal en globaal als men $\mathbb{Q}$ vervangt door een willekeurig getallenlichaam. We zullen dit echter buiten beschouwing laten.

2.5 Twee hulpresultaten

Aangezien $\mathbb{Z}_p$ volledig is, hebben we een equivalent van bepaalde resultaten uit de reële analyse. Een p-adische equivalent van de Newton-Raphson iteratiemethode staat aan de basis van de p-adische analyse en is in vrijwel elk boek over p-adische getallen te vinden. Met deze methode is het mogelijk nulpunten van een polynoom te benaderen en onder zekere voorwaarden te liften naar nulpunten in $\mathbb{Z}_p$. Dit is de meest gebruikte manier om vergelijkingen in de p-adische getallen op te lossen en we zullen dit dan ook nog veelvuldig tegenkomen. Merk op dat de voorwaarde dat de afgeleide niet te klein moet zijn, sterk doet denken aan de Newton-Raphson iteratiemethode.

2.7 Lemma (Hensel)**.** *Laat $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x \in \mathbb{Z}_p^m$ en $n, k \in \mathbb{Z}$ met $0 \leq 2k < n$ zodanig dat:*

1. *$f(x) \equiv 0 \bmod p^n$;*
2. *Er bestaat een $1 \leq j \leq m$ zodanig dat $v_p(\frac{\partial f}{\partial X_j}(x)) = k$.*

Dan heeft f een nulpunt $y \in \mathbb{Z}_p^m$ zodanig dat $x_i \equiv y_i \bmod p^{n-k}$ voor $1 \leq i \leq m$.

Bewijs. Zie stelling 1 uit paragraaf II.2.2 in [SE]. □

Voor het bewijs van het lokaal-globaalprincipe voor kwadratische vormen is het nuttig meer te weten te komen over de kwadraten in $\mathbb{Z}_p$ en $\mathbb{Q}_p$. We zien meteen een eerste toepassing van het lemma van Hensel.

2.8 Gevolg. *Voor $p \neq 2$ is $x \in \mathbb{Z}_p^*$ een kwadraat dan en slechts dan als $\varepsilon(x) \in \mathbb{F}_p^{*2}$. Een element $x \in \mathbb{Z}_2^*$ is een kwadraat precies als $\varepsilon_3(x) \in (\mathbb{Z}/8\mathbb{Z})^{*2}$.*

Bewijs. Stel $p \neq 2$. Laat $a \in \mathbb{F}_p^{*2}$ en $x \in \mathbb{Z}_p$ zodanig dat geldt $\varepsilon(x) = a$. Er bestaat een $v \in \mathbb{F}_p^*$ met $v^2 = a$. Kies een $y \in \mathbb{Z}_p^*$ zodanig dat $\varepsilon(y) = v$. We beschouwen het polynoom $f = X^2 - x \in \mathbb{Z}_p[X]$. Er geldt $f(y) \equiv 0 \bmod p$ en $v_p(f'(y)) = v_p(2y) = 0$. Met 2.7 ($n = 1, k = 0$) volgt dat er een $z \in \mathbb{Z}_p$ bestaat met $z^2 = x$ en we concluderen $x \in \mathbb{Z}_p^{*2}$. Andersom impliceert $x \in \mathbb{Z}_p^{*2}$ op triviale wijze $\varepsilon(x) \in \mathbb{F}_p^{*2}$.

Stel $p = 2$. Merk op $(\mathbb{Z}/8\mathbb{Z})^{*2} = \{1\}$. Laat $x \in \mathbb{Z}_p$ zodanig dat $\varepsilon_3(x) = 1$ en beschouw het polynoom $f = X^2 - x \in \mathbb{Z}_p[X]$. Er geldt $f(1) \equiv 0 \bmod 8$ en $v_p(f'(1)) = v_p(2) = 1$. Met 2.7 ($n = 3, k = 1$) volgt nu dat er een $y \in \mathbb{Z}_p$ bestaat met $y^2 = x$ en daarmee is x een kwadraat in $\mathbb{Z}_p^*$. Als andersom geldt $x \in \mathbb{Z}_p^{*2}$, dan zien we meteen in $\varepsilon_3(x) \in (\mathbb{Z}/8\mathbb{Z})^{*2}$. □

2.9 Lemma. *De ondergroep $\mathbb{Q}_p^{*2}$ van $\mathbb{Q}_p^*$ is open in $\mathbb{Q}_p$.*

Bewijs. We geven $\mathbb{Z}/p^n\mathbb{Z}$ de discrete topologie. Voor $a \in \mathbb{Z}/p^n\mathbb{Z}$ en $b \in \mathbb{Z}_p$ zodanig dat $\varepsilon_n(b) = a$ volgt dat $\varepsilon_n^{-1}(a) = \{x \in \mathbb{Z}_p : \varepsilon_n(x) = a\} = \{x \in \mathbb{Z}_p : v_p(x - b) > n\} = B(b, e^{-n})$ open is. Aangezien de verzameling $\{\{a\} : a \in \mathbb{Z}/p^n\mathbb{Z}\}$ een basis vormt voor de discrete topologie, is ε_n continu. Dus $\varepsilon^{-1}(\mathbb{F}_p^{*2}) = \mathbb{Z}_p^{*2}$ is open in $\mathbb{Z}_p$ voor $p \neq 2$ en $\varepsilon_3^{-1}((\mathbb{Z}/8\mathbb{Z})^{*2}) = \mathbb{Z}_2^{*2}$ is open in $\mathbb{Z}_2$ wegens 2.8. Dus $\mathbb{Z}_p^{*2}$ is open in $\mathbb{Z}_p$ voor alle priemgetallen p en daarmee ook in $\mathbb{Q}_p$, aangezien $\mathbb{Z}_p$ open is in $\mathbb{Q}_p$. Stel $x \in \mathbb{Q}_p^{*2}$, dan volgt $x = p^{2n}u^2$ voor $n \in \mathbb{Z}$ en $u \in \mathbb{Z}_p^*$ en dus geldt $\mathbb{Q}_p^{*2} = \bigcup_{n \in \mathbb{Z}} p^{2n}\mathbb{Z}_p^{*2}$. Als vereniging van open verzamelingen is $\mathbb{Q}_p^{*2}$ open in $\mathbb{Q}_p$. □

2.10 Gevolg. *Zij $S \subset V$ eindig en $(a_s)_s \in \prod_{s \in S} \mathbb{Q}_s^*$. Stel er bestaat een rij $(\alpha_i)_i \in \mathbb{Q}^{\mathbb{N}}$ zodanig dat geldt $\lim_{i \to \infty} \alpha_i = a_s$ voor alle $s \in S$, dan bestaat er een i zodanig dat $\alpha_i / a_s \in \mathbb{Q}_s^{*2}$ voor alle $s \in S$.*

Bewijs. Uit 2.9 is $\mathbb{Q}_p^{*2}$ open in $\mathbb{Q}_p$ voor alle priemgetallen p. Tevens is $\mathbb{Q}_\infty^{*2} = (\mathbb{Q}_\infty)_{>0}$ open in $\mathbb{Q}_\infty$. Daar 1 een kwadraat is in $\mathbb{Q}_s^*$ voor alle $s \in S$ bestaat er een $\epsilon_s > 0$ zodanig dat $B(1, \epsilon_s) \subset \mathbb{Q}_s^{*2}$. Laat nu $\epsilon = \min\{\epsilon_s d_s(0, a_s) : s \in S\}$. Er bestaat een $i \in \mathbb{N}$ met $d_s(a_s, \alpha_i) < \epsilon$ voor alle $s \in S$. Er geldt

$$d_s(\alpha_i/a_s, 1) = e^{-v_s(\alpha_i/a_s - 1)} = e^{-v_s(\alpha_i - a_s)} e^{v_s(a_s)} < \epsilon_s \qquad \text{als } s \in S \setminus \{\infty\};$$
$$d_s(\alpha_i/a_s, 1) = |\alpha_i/a_s - 1| = |\alpha_i - a_s||a_s^{-1}| < \epsilon_s \qquad \text{als } s = \infty \in S.$$

Dus volgt dat α_i/a_s een kwadraat is in $\mathbb{Q}_s^*$ voor alle $s \in S$. □

3 Het lokaal-globaalprincipe voor kwadratische vormen

3.1 Kwadratische vormen

Zij K een lichaam van karakteristiek ongelijk aan 2.

3.1 Definitie. Zij $n \geq 1$. Een homogeen kwadratisch polynoom $f = \sum_{i,j} a_{ij} X_i X_j$ in $K[X_1, \ldots, X_n]$ heet een *kwadratische vorm*.

Merk op dat we kunnen schrijven $f = X^t A X$ waarbij X de vector $(X_1, \ldots, X_n)^t$ is en A de $n \times n$-matrix $(a_{ij})_{i,j}$. We kiezen A symmetrisch, wat mogelijk is omdat de karakteristiek van K niet 2 is. Nu kunnen we bij een kwadratische vorm de matrix A eenduidig vastleggen en noteren deze als A_f.

3.2 Definitie. We noemen een kwadratische vorm $f \in K[X_1, \ldots, X_n]$ *niet-ontaard* als $\det(A_f) \neq 0$.

3.3 Definitie. Twee kwadratische vormen $f, f' \in K[X_1, \ldots, X_n]$ zijn *equivalent* als er een matrix $Y \in \mathrm{GL}_n(K)$ bestaat met $A_{f'} = Y^t A_f Y$. We noteren $f \sim f'$.

Een voorbeeld van twee equivalente kwadratische vormen in $K[X_1, X_2]$ is $a_1 X_1^2 + a_2 X_2^2 \sim a_1 X_1^2 + b^2 a_2 X_2^2$ met $a_1, a_2, b \in K$, maar ook $X_1 X_2 \sim X_1^2 - X_2^2$. Hierbij kiezen we $Y = \mathrm{diag}(1, b)$ respectievelijk $Y = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. Stel $f, f' \in K[X_1, \ldots, X_n]$ zijn equivalent. Uit $\det(A'_f) = \det(A_f)\det(Y)^2$ volgt dat f niet-ontaard is dan en slechts dan als f' het is. Voor $x \in K^n$ geldt $f'(x) = x^t A_{f'} x = x^t Y^t A_f Y x = f(Yx)$. Dus volgt $f'[K^n] = f[K^n]$ en $f'[K^n \setminus \{0\}] = f[K^n \setminus \{0\}]$ daar Y een inverteerbare matrix is.

3.4 Definitie. We zeggen dat f een element $a \in K$ *representeert* als er een $x \in K^n$ bestaat met $x \neq 0$ zodanig dat $f(x) = a$.

Equivalente kwadratische vormen representeren uit voorgaande dezelfde elementen van K. In het bijzonder heeft f een niet-triviaal nulpunt precies als f' dit heeft. Het gevolg van de volgende propositie uit de lineaire algebra vereenvoudigt het werken met kwadratische vormen aanzienlijk.

3.5 Propositie. *Als $A \in \mathrm{Mat}_n(K)$ een symmetrische matrix is, kunnen we A diagonaliseren, oftewel er bestaat een $Y \in \mathrm{GL}_n(K)$ zodanig dat $Y^t A Y$ een diagonaalmatrix is.*

Bewijs. We bewijzen met inductie naar n. Voor $n = 1$ valt er niets te bewijzen. Zij $n \in \mathbb{N}$ en stel de propositie is waar voor alle symmetrische matrices $A \in \mathrm{Mat}_k(K)$ voor $k < n$. Zij $A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(K)$ symmetrisch. Als A de nulmatrix is, volgt het resultaat meteen, dus neem aan $A \neq 0$. We onderscheiden twee gevallen:

1. Er bestaat een element a_{ii} op de diagonaal van A ongelijk aan 0. Laat Z de inverteerbare matrix verkregen uit de $n \times n$-identiteitsmatrix door de i-de rij te vervangen door

   $$a_{ii}^{-1}(-a_{i1}, -a_{i2}, \ldots, -a_{i(i-1)}, a_{ii}, -a_{i(i+1)}, \ldots, -a_{in}).$$

   Het is duidelijk dat de elementen van de i-de rij en kolom van de symmetrische matrix $C = Z^t A Z$ op het diagonaalelement a_{ii} na gelijk aan 0 zijn.

2. Alle elementen op de diagonaal van A zijn gelijk aan 0. Aangezien A niet de nulmatrix en symmetrisch is, bestaat er een element $a_{ij} \in K^*$ met $i < j$. Laat W de inverteerbare matrix verkregen uit de $n \times n$-identiteitsmatrix door de 0 op de (j, i)-de coördinaat in 1 te veranderen. Men ziet direct in dat de coördinaat (i, i)-de coördinaat van de matrix $B = W^t A W$ gelijk is aan $2a_{ij} \in K^*$. Net zoals in geval 1 kunnen we nu een inverteerbare matrix Z vinden zodanig dat de i-de rij en kolom van de symmetrische matrix $C = Z^t B Z$ op het diagonaalelement $2a_{ij}$ na gelijk aan 0 zijn.

Verwijder nu de i-de rij en kolom van de symmetrische matrix C en noem de verkregen symmetrische $(n-1)\times(n-1)$-matrix C'. Met de inductiehypothese volgt dat er een inverteerbare matrix Y' bestaat, zodanig dat ${Y'}^t C' Y'$ een diagonaalmatrix is. Zij tot slot Y de inverteerbare $n \times n$-matrix verkregen uit Y' door een i-de rij en kolom in te voegen met op de i-de plek een 1 en op de andere plekken 0. Uit de eigenschappen van C met betrekking tot de i-de rij en kolom volgt dat $Y^t C Y$ een diagonaalmatrix is. We kunnen A dus diagonaliseren. □

3.6 Gevolg. *Zij $f \in K[X_1, \ldots, X_n]$ een kwadratische vorm, dan bestaan er $a_1, \ldots, a_n \in K$ zodanig dat $f \sim a_1 X_1^2 + \ldots + a_n X_n^2$. Er geldt $a_1, \ldots, a_n \neq 0$ dan en slechts dan als f niet-ontaard is.* □

We kunnen nu inzien dat het representeren van nul equivalent is aan het representeren van alle elementen van K.

3.7 Lemma. *Als een niet-ontaarde kwadratische vorm $f \in K[X_1, \ldots, X_n]$ het element $0 \in K$ representeert, worden alle elementen van K gerepresenteerd door f.*

Bewijs. Uit 3.6 volgt $f \sim a_1 X_1^2 + \ldots + a_n X_n^2$ voor $a_1, \ldots, a_n \in K^*$ en aangezien f en $a_1 X_1^2 + \ldots + a_n X_n^2$ dezelfde elementen van K representeren, kunnen we aannemen $f = a_1 X_1^2 + \ldots + a_n X_n^2$. Laat nu $x = (x_1, \ldots, x_n) \in K^n \setminus \{0\}$ een element dat 0 representeert. Kies $y_i = \frac{1}{a_i x_i}$ als i minimaal is met $x_i \neq 0$ en $y_i = 0$ anders. Noem $y = (y_1, \ldots, y_n) \in K^n \setminus \{0\}$. Er geldt

$$\sum_{i=1}^{n} 2 a_i x_i y_i = 2.$$

Laat nu $z = 2y - f(y)x$. Invullen in f geeft:

$$f(z) = \sum_{i=1}^{n} a_i (2y_i - f(y)x_i)^2 = \sum_{i=1}^{n} (f(y)^2 a_i x_i^2 + 4 a_i y_i^2 - 4 f(y) a_i x_i y_i)$$
$$= f(y)^2 f(x) + 4f(y) - 4f(y) = 0.$$

Neem nu $\alpha \in K$, er geldt $f(\alpha z) = \alpha^2 f(z) = 0$ en dus volgt

$$f(x + \alpha z) = f(x + \alpha z) - f(x) - f(\alpha z) = 2\alpha \sum_{i=1}^{n} a_i x_i z_i = 2\alpha \sum_{i=1}^{n} a_i x_i (2y_i - f(y)x_i)$$
$$= 2\alpha(2 - f(y)f(x)) = 4\alpha.$$

Neem nu $\beta \in K$ willekeurig. Door in bovenstaande $\alpha = \beta/4$ te kiezen volgt $f(x + \alpha z) = \beta$. Dus β wordt gerepresenteerd door f. □

3.8 Gevolg. *Zij $g \in K[X_1, \ldots, X_n]$ een niet-ontaarde kwadratische vorm. De vorm g representeert $a \in K^*$ dan en slechts dan als de kwadratische vorm $f = g - aZ^2 \in K[X_1, \ldots, X_n, Z]$ nul representeert.*

Bewijs. Het is meteen duidelijk dat f nul representeert als g het element $a \in K^*$ representeert. Stel andersom dat $(x_1, \ldots, x_n, z)$ een niet-triviaal nulpunt van f is. Stel $z \neq 0$ dan volgt $g(x_1/z, \ldots, x_n/z) = a$. Stel $z = 0$, dan wordt 0 gerepresenteerd door g en dus ook het element $a \in K^*$. □

Bij het bewijs van het lokaal-globaalprincipe is het belangrijk te weten wanneer een kwadratische vorm over $\mathbb{Q}_p$ met coëfficiënten in $\mathbb{Z}_p$ nul representeert. Dit blijkt voor $p \neq 2$ al het geval te zijn als de vorm meer dan 2 variabelen bevat en de determinant een eenheid is. Dit resultaat is een gevolg van het lemma van Hensel en de volgende bekende stelling:

3.9 Stelling (Chevalley-Warning)**.** *Zij K een eindig lichaam van karakteristiek p en f een polynoom in $K[X_1, \ldots, X_n]$ met $\deg(f) < n$. Er geldt $\#\{x \in K^n : f(x) = 0\} \equiv 0 \bmod p$.*

Bewijs. Zie stelling 3 uit paragraaf I.2.2 in [SE]. □

3.10 Gevolg. *Zij $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ voor $n \geq 3$ en $p \neq 2$ priem een kwadratische vorm over $\mathbb{Q}_p$ met $\det(A_f) \in \mathbb{Z}_p^*$. Dan representeert f nul.*

Bewijs. Via de coördinaatafbeelding $\varepsilon : \mathbb{Z}_p \to \mathbb{F}_p$, kunnen we f als kwadratische vorm over het eindige lichaam $\mathbb{F}_p$ beschouwen. Ook de geassocieerde matrix A_f kunnen we over $\mathbb{F}_p$ beschouwen en er volgt $\det(A_f) \not\equiv 0 \bmod p$, omdat geldt $\det(A_f) \in \mathbb{Z}_p^*$. De graad van f is kleiner dan n en dus is het aantal nulpunten van f deelbaar door p. Aangezien $0 \in \mathbb{F}_p^n$ een nulpunt van f is, moet er een tweede nulpunt $a \in \mathbb{F}_p^n \setminus \{0\}$ zijn. Kies nu $x \in \mathbb{Z}_p^n \setminus \{0\}$ zodanig dat $\varepsilon(x_i) = a_i$ voor $1 \leq i \leq n$. Er geldt $\frac{\partial f}{\partial X_i}(x) = 2(A_f)_i x$ voor $1 \leq i \leq n$. Stel $\frac{\partial f}{\partial X_i}(x) \equiv 0 \bmod p$ voor alle i, dan geldt $A_f a = 0$ in $\mathbb{F}_p^n$. Dit is in tegenspraak met $\det(A_f) \neq 0 \bmod p$ en $a \neq 0$. Dus bestaat er een i met $v_p(\frac{\partial f}{\partial X_i}(x)) = 0$. Uit 2.7 $(k = 0, n = 1)$ volgt dat er een $y \in \mathbb{Z}_p^n \setminus \{0\}$ (immers $a_i = \varepsilon(x_i) = \varepsilon(y_i)$ voor $1 \leq i \leq n$) bestaat met $f(y) = 0$. □

3.2 Het Hilbertsymbool

Zij K een lichaam van karakteristiek 0. Een bijzondere plek heeft de kwadratische vorm $Z^2 - aX^2 - bY^2$ met $a, b \in K^*$ in het bewijs van het lokaal-globaalprincipe voor kwadratische vormen.

3.11 Definitie. De afbeelding[5] $K^* \times K^* \to \{\pm 1\}$ gegeven door $(a, b) = 1$ als de kwadratische vorm $Z^2 - aX^2 - bY^2 \in K[X, Y, Z]$ nul representeert en $(a, b) = -1$ in andere gevallen wordt het *Hilbertsymbool* met betrekking tot K genoemd.

Voor $a, b, c, d \in K^*$ is duidelijk dat geldt $Z^2 - aX^2 - bY^2 \sim Z^2 - ac^2X^2 - bd^2Y^2$. Tevens vinden we $(1, 1, 0), (1, 0, 1), (1, 1, 1)$ als niet-triviale nulpunten van $Z^2 - aX^2 + aY^2, Z^2 - X^2 - aY^2$ respectievelijk $Z^2 - bX^2 - (1 - b)Y^2$ voor $a, b \in K^*$ met $b \neq 1$. We concluderen:

3.12 Propositie. *Voor $a, b, c, d \in K^*$ geldt:*

1. $(a, b) = (b, a)$;
2. $(a, b) = (ac^2, bd^2)$;
3. $(1, a) = (a, -a) = 1$ *en als* $a \neq 1$: $(a, 1 - a) = 1$. □

Met behulp van de norm N weten we precies wanneer een Hilbertsymbool de waarde 1 aanneemt. Als $K \subset K(\sqrt{b})$ voor $b \in K^*$ geen kwadraat een kwadratische uitbreiding van graad 2 is, is de norm voor een element $c + d\sqrt{b} \in K(\sqrt{b})$ met $c, d \in K$ gedefinieerd als $N(c + d\sqrt{b}) = c^2 - bd^2$. Als $b \in K^*$ wel een kwadraat is, dan geldt $K = K(\sqrt{b})$ en is de norm de identiteit op K.[6]

3.13 Propositie. *Zijn $a, b \in K^*$. Er geldt $(a, b) = 1$ dan en slechts dan als a de norm is van een element uit $K(\sqrt{b})^*$.*

Bewijs. Als b een kwadraat is, volgt $K = K(\sqrt{b})$ en is a de norm van het element $a \in K$. Wegens 3.12 geldt tevens $(a, b) = (a, 1) = 1$, daar b een kwadraat is. Dus volgt de propositie in dit geval. Neem nu aan dat b geen kwadraat is. Stel a is gelijk aan de norm van een element $c + d\sqrt{b} \in K(\sqrt{b})^*$ voor $c, d \in K$, dan volgt $a = c^2 - bd^2$ en is $(1, d, c)$ een oplossing. We vinden $(a, b) = 1$. Stel omgekeerd dat geldt $(a, b) = 1$. Dan bestaat er een niet-triviaal nulpunt (z, x, y). We hebben $x \neq 0$, omdat anders moet gelden $y \neq 0$ en b gelijk is aan het kwadraat $(z/y)^2$. Er volgt dat a de norm is van het element $(z + y\sqrt{b})/x \in K(\sqrt{b})$. □

3.14 Gevolg. *Er geldt $(ac, b) = (a, b)(c, b)$ voor $a, b, c \in K^*$ als $(ac, b) = 1$, $(a, b) = 1$ of $(c, b) = 1$.*

[5] Merk op dat de lege notatie gebruikt wordt voor de afbeelding.

[6] Voor de definitie van de norm voor willekeurige eindige uitbreidingen verwijzen we naar paragraaf 4.1.

Bewijs. Stel $(a,b)=1$, dan is a de norm $N(x)$ van een element $x \in K(\sqrt{b})^*$. Er geldt $(c,b)=1$ precies dan als c een norm $N(y)$ is van een element $y \in k(\sqrt{b})^*$ en evenzo geldt $(ac,b)=1$ dan en slechts dan als $ac=N(z)$ voor $z \in K(\sqrt{b})^*$. Uit de eigenschappen van de norm $N(xy)=N(x)N(y)=ac$ en $N(\frac{z}{N(x)})=c$ volgt dat c een norm is van een element dan en slechts dan als ac dat is. Er geldt dus $(ac,b)=(c,b)$ en de conclusie volgt. Het geval $(c,b)=1$ gaat analoog. Als $(ac,b)=1$ merken we op dat voorgaande en 3.12 impliceren $(ac,b)(a,b)=(a^2c,b)=(c,b)$. Aangezien (a,b) zijn eigen inverse is, volgt het resultaat. □

Merk op dat de bilineaire eigenschap uit 3.14 ook geldt in de tweede coördinaat als één van de termen uit het product $(a,bc)=(a,b)(a,c)$ gelijk aan 1 is. Dit volgt uit de symmetrische eigenschap $(a,b)=(b,a)$ van het Hilbertsymbool.

3.15 Gevolg. *Er geldt* $(a,b)=(a,-ab)$ *voor* $a,b \in K^*$.

Bewijs. We weten $(a,-a)=1$ uit 3.12 en dus schrijven we met 3.12 en 3.14:

$$(a,-ab)=(a,-ab)(a,-a)=(a,a^2b)=(a,b). \square$$

Het volgende lemma hebben we nodig bij het bewijs van het lokaal-globaalprincipe voor kwadratische vormen en laat goed zien hoe men met behulp van 3.12–3.15 kan rekenen met het Hilbertsymbool.

3.16 Lemma. *Als de kwadratische vorm* $f=a_1X^2+a_2Y^2 \in K[X,Y]$ *met* $a_1,a_2 \in K^*$ *een element* $a \in K^*$ *representeert, dan geldt* $(a,-a_1a_2)=(a_1,a_2)$.

Bewijs. Merk op dat 0 gerepresenteerd wordt door de vorm $g=-af+Z^2=Z^2-a_1aX^2-a_2aY^2$ in $\mathbb{Q}_p[X,Y,Z]$, want f representeert a. Dus geldt $(a_1a,a_2a)=1$ en volgt met behulp van 3.12 en 3.15

$$1=(a_1a,a_2a)=(a_1a,-a_1a_2a^2)=(a_1a,-a_1a_2).$$

Aangezien geldt $(a_1a,-a_1a_2)=1$, mogen we schrijven $1=(a_1a,-a_1a_2)=(a_1,-a_1a_2)(a,-a_1a_2)$ uit 3.14. Tot slot schrijven we nogmaals $(a_1,-a_1a_2)=(a_1,a_2)$ met 3.15. Dit geeft $(a,-a_1a_2)(a_1,a_2)=1$, oftewel $(a,-a_1a_2)=(a_1,a_2)$. □

3.3 Het Hilbertsymbool over $\mathbb{Q}$ en $\mathbb{Q}_v$

Als we nu K gelijk aan $\mathbb{Q}_v$ nemen voor $v \in V$, vinden we een sterker resultaat dan 3.14. Het valt buiten het bereik van deze scriptie om het hier te bewijzen en we hebben het alleen nodig voor het geval $n \geq 4$ van het bewijs van het lokaal-globaalprincipe.

3.17 Stelling. *Zij* $K=\mathbb{Q}_v$ *voor* $v \in V$*, dan is het Hilbertsymbool bilineair, dat wil zeggen er geldt* $(ac,b)=(a,b)(c,b)$ *voor alle* $a,b,c \in K^*$.

Bewijs (schets)**.** In het bewijs wordt gebruikt gemaakt van expliciete formules voor het Hilbertsymbool, waarmee men bij gegeven $a,b \in \mathbb{Q}_v^*$ voor $v \in V$ het Hilbertsymbool kan uitrekenen als men weet wat de kwadraten in $\mathbb{Q}_v$ zijn. Hiervoor is kennis van de kwadraten in $\mathbb{Z}/p^n\mathbb{Z}$ nodig voor p een priemgetal, zoals al bleek in het bewijs van 2.9. Doordat deze formules bilineair zijn, volgt het resultaat. Zie stelling 1 in paragraaf III.1.2 uit [SE] voor de formules. □

De kwadratische vorm $Z^2-aX^2-bY^2 \in \mathbb{Q}[X,Y,Z]$ voor $a,b \in \mathbb{Q}^*$ kunnen we via de inbeddingen $\mathbb{Q} \to \mathbb{Q}_v$ bekijken over $\mathbb{Q}_v$ voor $v \in V$. Om verwarring te voorkomen noteren we $(a,b)_v$ voor het Hilbertsymbool van $a,b \in \mathbb{Q}_v^*$ en $(a,b)_{\mathbb{Q}}$ voor het Hilbertsymbool van $a,b \in \mathbb{Q}^*$. Het nut van het Hilbertsymbool wordt duidelijk uit de sterke relatie die de niet-triviale nulpunten van $Z^2-aX^2-bY^2$ in $\mathbb{Q}_v$ voor verschillende $v \in V$ ten opzichte van elkaar hebben.

3.18 Stelling. *Laat $a, b \in \mathbb{Q}^*$. Er geldt $(a,b)_v = 1$ voor bijna alle $v \in V$ en*

$$\prod_{v \in V} (a,b)_v = 1.$$

Bewijs (schets)**.** Aangezien het Hilbertsymbool bilineair is, voldoet het om de stelling te bewijzen als elk van a en b gelijk is aan -1 of een priemgetal. Gebruik van de eerder genoemde expliciete formules voor het Hilbertsymbool $(a,b)_v$ voor $v \in V$ geeft weer het resultaat, waarbij manipulatie met de kwadratische reciprociteitsstelling nodig is. Zie uit [SE] stelling 6 in paragraaf I.3.3 voor de reciprociteitsstelling, stelling 1 in paragraaf III.1.2 voor de formules en stelling 3 in paragraaf III.2.1 het bewijs van de stelling. □

Een gevolg van stelling 3.18 is dat de verzameling van $v \in V$ waarvoor $Z^2 - aX^2 - bY^2$ slechts een triviaal nulpunt heeft, eindig is en van even kardinaliteit. Het is omgekeerd mogelijk om een element $x \in \mathbb{Q}^*$ te construeren dat past in een rij Hilbertsymbolen. We gebruiken hierbij de stelling van Dirichlet over priemen in rekenkundige rijen.

3.19 Lemma (Dirichlet)**.** *Als $a, m \in \mathbb{Z}_{\geq 1}$ onderling ondeelbaar zijn, dan bestaan er oneindig veel priemen p zodanig dat $p \equiv a \bmod m$.*

Bewijs. Zie stelling 2 in paragraaf VI.4.1 uit [SE]. □

3.20 Lemma. *Als $p \neq 2$ een priemgetal is, dan geldt $(a,b)_p = 1$ voor $a, b \in \mathbb{Z}_p^*$.*

Bewijs. Er geldt $\det(Z^2 - aX^2 - bY^2) = ab \in \mathbb{Z}_p^*$. Het resultaat volgt met 3.10. □.

3.21 Stelling. *Zij $(a_i)_{i \in I}$ een eindige familie elementen in $\mathbb{Q}^*$ en $(\epsilon_{i,v})_{i \in I, v \in V}$ een familie uit $\{\pm 1\}$. Er bestaat een $x \in \mathbb{Q}^*$ zodanig dat $(a_i, x)_v = \epsilon_{i,v}$ voor $i \in I$ en $v \in V$ dan en slechts dan als:*

1. *Bijna alle $\epsilon_{i,v}$ zijn gelijk aan 1.*
2. *Voor alle $i \in I$ geldt $\prod_{v \in V} \epsilon_{i,v} = 1$.*
3. *Voor alle $v \in V$ bestaat een $x_v \in \mathbb{Q}_v^*$ zodanig dat $(a_i, x_v)_v = \epsilon_{i,v}$ voor alle $i \in I$.*

Bewijs. Uit 3.18 is duidelijk dat als een dergelijke $x \in \mathbb{Q}^*$ bestaat, 1. en 2. moeten gelden. Eis 3. is triviaal, we kunnen $x_v = x$ nemen voor alle $v \in V$. Neem nu aan dat eisen 1–3 gelden; we bewijzen dat een dergelijke $x \in \mathbb{Q}^*$ bestaat. We kunnen aannemen $a_i \in \mathbb{Z} \setminus \{0\}$, omdat het Hilbertsymbool invariant is onder vermenigvuldiging met kwadraten uit 3.12.

Beschouw de eindige deelverzameling $S \subset V$ bestaande uit $2, \infty$ en de priemfactoren van a_i voor alle $i \in I$. Met 2.6 volgt dat er een rij $(\alpha_n)_n$ in $\mathbb{Q}$ bestaat met $\lim_{n \to \infty} \alpha_n = x_v$ voor alle $v \in S$. Toepassen van 2.10 geeft dat er een $x' \in \mathbb{Q}^*$ bestaat zodanig dat x'/x_v een kwadraat is voor alle $v \in S$. Er geldt $(a_i, x')_v = (a_i, x_v)_v = \epsilon_{i,v}$ voor alle $v \in S$ en $i \in I$ wegens 3.12. Laat nu $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v$ voor alle $v \in V$ en $i \in I$. Er volgt dat bijna alle $\eta_{i,v}$ gelijk zijn aan 1, aangezien bijna alle $\epsilon_{i,v}$ gelijk zijn aan 1 en bijna alle $(a_i, x')_v$ gelijk zijn aan 1 wegens 3.18. Met 3.18 volgt tevens voor $i \in I$

$$\prod_{v \in V} \eta_{i,v} = \prod_{v \in V} \epsilon_{i,v} \prod_{v \in V} (a_i, x')_v = 1.$$

Verder bestaat er voor alle $v \in V$ een element $y_v = x_v x' \in \mathbb{Q}_v^*$ zodanig dat $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v = (a_i, x_v)_v (a_i, x')_v = (a_i, y_v)_v$ met 3.17. Het is dus duidelijk dat de familie $(\eta_{i,v})_{i \in I, v \in V}$ aan de eisen 1–3 voldoet. Tevens geldt $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v = \epsilon_{i,v}^2 = 1$ voor alle $v \in S$ en $i \in I$.

Zij $T \subset V$ de eindige deelverzameling bestaande uit de $v \in V$ zodanig dat $\eta_{i,v} = -1$ voor een $i \in I$. De verzamelingen S en T zijn dus disjunct. De natuurlijke getallen

$$a = \prod_{\substack{l \in T \\ l \neq \infty}} l \quad \text{en} \quad m = 8 \prod_{\substack{l \in S \\ l \neq 2, \infty}} l$$

zijn daarmee copriem en met 3.19 bestaat er een priemgetal p, zodanig dat $p \equiv a \bmod m$ met $p \notin S \cup T$. We laten zien dat $y = ap$ voldoet aan $(a_i, y)_v = \eta_{i,v}$ voor alle $v \in V$ en $i \in I$.

Stel $v \in S$, dan geldt $\eta_{i,v} = 1$ voor alle $i \in I$ uit $S \cap T = \emptyset$. Als $v = \infty$ ziet men meteen in $(a_i, y)_v = 1 = \eta_{i,v}$ voor alle $i \in I$, omdat geldt $y > 0$. Als $v \in S$ een priemgetal is, volgt uit $y \equiv a^2 \bmod m$ dat geldt $y \equiv a^2 \bmod 8$ als $v = 2$ en $y \equiv a^2 \bmod v$ als $v \neq 2$. Aangezien geldt $v \in S$, $S \cap T = \emptyset$ en $p \notin S$, is v geen deler van p en a. De elementen a en y zijn dus eenheden in $\mathbb{Z}_v$. Met 2.8 zien we in dat $y = z^2$ een kwadraat is met $z \in \mathbb{Z}_v^*$ en er volgt $(a_i, y)_v = (a_i, z^2)_v = (a_i, 1)_v = 1 = \eta_{i,v}$ voor alle $i \in I$ uit 3.12.

Stel $v \notin S$, dan is v een priemgetal ongelijk aan 2 en a_i is een eenheid in $\mathbb{Z}_v^*$ voor alle $i \in I$. Als $v \notin T \cup \{p\}$ dan geldt ook $y \in \mathbb{Z}_v^*$ en dus volgt $(a_i, y)_v = 1$ voor alle $i \in I$ uit 3.20. Als $v \in T$ volgt $y = vu$ voor een $u \in \mathbb{Z}_v^*$. Tevens geldt $(a_j, y_v)_v = \eta_{j,v} = -1$ voor een zekere $j \in I$. Schrijf $y_v = v^n w$ met $w \in \mathbb{Z}_v^*$. Stel n is even, dan zien we $(a_j, v^n)_v = (a_j, 1)_v = 1$ uit 3.12 en $(a_j, w)_v = 1$ met 3.20. Wegens 3.14 geldt $(a_j, y_v)_v = (a_j, v^n)(a_j, w) = 1$, wat duidt op een tegenspraak. Dus is n oneven en met 3.14, 3.20 en 3.12 volgt

$$(a_i, y)_v = (a_i, v)_v (a_i, u)_v = (a_i, v)_v = (a_i, v)_v (a_i, v^{n-1})_v (a_i, w)_v = (a_i, v^n w)_v = (a_i, y_v)_v = \eta_{i,v}$$

voor alle $i \in I$. Tot slot bekijken we het geval dat $v = p$. Met behulp van de productformule 3.18 geldt voor alle $i \in I$

$$(a_i, y)_p = \prod_{v \in V \setminus \{p\}} (a_i, y)_v = \prod_{v \in V \setminus \{p\}} \eta_{i,v} = \eta_{i,p}.$$

Er geldt dus $(a_i, y)_v = \eta_{i,v}$ voor alle $i \in I$ en $v \in V$. Neem nu $x = yx' \in \mathbb{Q}^*$. Er volgt $(a_i, x)_v = (a_i, y)_v (a_i, x')_v = \eta_{i,v}(a_i, x')_v = \epsilon_{i,v}(a_i, x')_v^2 = \epsilon_{i,v}$ voor alle $i \in I$ en $v \in V$ met 3.17. Dus $x \in \mathbb{Q}^*$ voldoet. $\square$

3.4 Bewijs van het lokaal-globaalprincipe voor kwadratische vormen

Laat $f \in \mathbb{Q}[X_1, \ldots, X_n]$ een kwadratische vorm zijn. Via de inbeddingen $\mathbb{Q} \to \mathbb{Q}_v$ voor alle $v \in V$ kunnen we f als kwadratische vorm f_v over $\mathbb{Q}_v$ beschouwen. We bewijzen ons hoofdresultaat.

3.22 Stelling (Hasse-Minkowski)**.** *Zij $f \in \mathbb{Q}[X_1, \ldots, X_n]$ een kwadratische vorm. De vorm f representeert nul dan en slechts dan als $f_v \in \mathbb{Q}_v[X_1, \ldots, X_n]$ voor alle $v \in V$ nul representeert.*

Bewijs. Als f een niet-triviaal nulpunt $x \in \mathbb{Q}^n$ heeft, is duidelijk dat $x \in \mathbb{Q}_v^n$ een niet-triviaal nulpunt van f_v is voor elke $v \in V$. Voor de omgekeerde implicatie nemen we aan dat f_v nul representeert voor alle $v \in V$. Merk op

$$f \sim a_1 X_1^2 + \ldots + a_n X_n^2$$

met $a_1, \ldots, a_n \in \mathbb{Q}$ wegens 3.6. Wanneer alle coëfficiënten van f gelijk zijn aan 0, is meteen helder dat f nul representeert. Laat daarom $f \neq 0$. We kunnen aannemen dat $a_1, \ldots, a_n \neq 0$ en anders overgaan op een vorm in minder variabelen, totdat aan deze eis is voldaan. Het is duidelijk dat nul wordt gerepresenteerd door een kwadratische vorm g precies als de vorm αg ook nul representeert voor $\alpha \in \mathbb{Q}^*$. We nemen dus aan dat f van de vorm $a_1 X_1^2 + \ldots + a_n X_n^2$ met $a_1 = 1$ is. Aangezien $X_1^2 + a_2 X_2^2 + \ldots a_n X_n^2$ equivalent is met $X_1^2 + a_2 b_2^2 X_2^2 + \ldots a_n b_n^2 X_n^2$ voor $b_2, \ldots, b_n \in \mathbb{Q}^*$, maken we tot slot de aanname $a_2, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. We beschouwen achtereenvolgens de gevallen $n = 2, 3, 4$ en ≥ 5. Voor $n = 1$ is meteen in te zien dat f_v nul representeert voor geen enkele $v \in V$.

• $n = 2$
We kunnen schrijven $f = X_1^2 - aX_2^2$ voor $a \in \mathbb{Z} \setminus \{0\}$. Nul wordt gepresenteerd door f_∞; dus is a positief. Als $(x_p, y_p) \in \mathbb{Q}_p^2$ een niet-triviale oplossing is, volgt $x_p, y_p \neq 0$ en $a = (x_p/y_p)^2$. Schrijven we $x_p/y_p = p^m u$ voor $u \in \mathbb{Z}_p^*$ en $m \in \mathbb{Z}$, dan geldt $a = p^{2m} u^2$ en dus $v_p(a) = 2m$. Factorisatie geeft:

$$a = \prod_{p \text{ priem}} p^{n_p}$$

met $n_p \geq 0$. Er geldt dat $v_p(a) = n_p$ even is en dus volgt dat a een kwadraat is in $\mathbb{Q}$ en dus wordt 0 gepresenteerd door f.

• $n = 3$ (Legendre)
Merk op dat f van de vorm $X_1^2 - aX_2^2 - bX_3^2$ is voor $a, b \in \mathbb{Z}^*$. Aangezien geldt $(a, b)_{\mathbb{Q}} = (ac^2, bd^2)_{\mathbb{Q}}$ voor $b, d \in \mathbb{Q}^*$ uit 3.12, kunnen we dus aannemen dat $a, b \in \mathbb{Z} \setminus \{0\}$ kwadraatvrij zijn. Ook kunnen we uit symmetrieoverwegingen aannemen $|a| \leq |b|$. We bewijzen met inductie naar $m = |a| + |b|$.

Stel $m = 2$, dan volgt

$$f = X_1^2 \pm X_2^2 \pm X_3^2.$$

Merk op dat het geval $X_1^2 + X_2^2 + X_3^2$ niet voor kan komen, omdat f_∞ anders 0 niet representeert. Uit 3.12 volgt $(1, -1)_{\mathbb{Q}} = (-1, 1)_{\mathbb{Q}} = (1, 1)_{\mathbb{Q}} = 1$, dus in alle andere gevallen representeert f nul.

Laat nu $m > 2$, dan volgt $|b| \geq 2$ en we ontbinden $b = \pm p_1 \dots p_k$ in een product van verschillende priemen. Zij p een priemgetal uit de factorisatie van b. We beweren dat a een kwadraat is modulo p. Als $a \equiv 0 \bmod p$ volgt dat a een kwadraat is in $\mathbb{F}_p$. Stel $a \not\equiv 0 \bmod p$, oftewel $a \in \mathbb{Z}_p^*$. Neem $(x', y', z') \in \mathbb{Q}_p^3$ een niet-triviaal nulpunt van f_v. Er volgt dat $c(x', y', z')$ voor $c \in \mathbb{Q}_p$ ook een nulpunt is. Neem nu $h = \min\{v_p(x'), v_p(y'), v_p(z')\}$, dan is $(x, y, z) = p^{-h}(x', y', z')$ een nulpunt in $\mathbb{Z}_p^3$, zodanig dat x, y of z een eenheid is in $\mathbb{Z}_p$. Dit is in te zien doordat elk element in $\mathbb{Q}_p^*$ te schrijven is als $p^k u$ met $k \in \mathbb{Z}$ en $u \in \mathbb{Z}_p^*$ en x', y' of z' een element is van $\mathbb{Q}_p^*$. Uit $p \mid b$ volgt $x^2 - az^2 \equiv 0 \bmod p$. Stel nu $z \notin \mathbb{Z}_p^*$, dan deelt p het element z en daarmee is x deelbaar door p, oftewel $x \notin \mathbb{Z}_p^*$. Er geldt $by^2 = x^2 - az^2 \equiv 0 \bmod p^2$. Daar b kwadraatvrij is, concluderen we $y \equiv 0 \bmod p$ en daarmee $y \notin \mathbb{Z}_p^*$. Echter dit is in tegenspraak met het feit dat x, y of z een eenheid is in $\mathbb{Z}_p$. Dus kunnen we vaststellen $z \in \mathbb{Z}_p^*$ en er volgt $a \equiv (x/z)^2 \bmod p$. Dus a is een kwadraat modulo p voor alle verschillende priemgetallen p uit de factorisatie van b.

Met de Chinese reststelling geldt dat a een kwadraat is modulo b. Er bestaan dus $t, b \in \mathbb{Z}$, zodanig dat

$$t^2 = a + bb'.$$

Omdat t slechts op equivalentie modulo b vastligt, kunnen we eisen dat t zich bevindt in een interval in $\mathbb{Z}$ van lengte minstens b. We kunnen dus t kiezen zodanig dat geldt $|t| \leq |b|/2$. Stel er geldt $b' = 0$, dan is a een kwadraat in $\mathbb{Q}^*$ en volgt $(a, b)_{\mathbb{Q}} = (t^2, b)_{\mathbb{Q}} = (1, b)_{\mathbb{Q}} = 1$ met 3.12 en zijn we klaar. Neem nu verder aan $b' \in \mathbb{Q}^*$. De identiteit $bb' = (t + \sqrt{a})(t - \sqrt{a})$ laat zien dat bb' een norm is in de uitbreiding $K \subset K(\sqrt{a})$ voor $K = \mathbb{Q}_v, \mathbb{Q}$. Met 3.13 volgt nu $(bb', a) = 1$ over K. Toepassen van 3.12 geeft vervolgens $1 = (bb', a) = (b, a)(b', a) = (a, b)(a, b')$. Er geldt dus $(a, b) = (a, b')$ gezien over $K = \mathbb{Q}_v, \mathbb{Q}$. We weten $(a, b')_v = (a, b)_v = 1$ voor alle $v \in V$, omdat f_v nul representeert. Schrijven we nu $b' = b''u^2$ met $b'', u \in \mathbb{Z} \setminus \{0\}$ en b'' kwadraatvrij, volgt $1 = (a, b')_v = (a, b''u^2)_v = (a, b'')_v$ met 3.12 voor alle $v \in V$. Dus de vorm $f' = X_1^2 - aX_2^2 - b''X_3^2$ representeert 0 in $\mathbb{Q}_v$ voor alle $v \in V$. Er geldt

$$|b''| = \left|\frac{b'}{u^2}\right| \leq |b'| = \left|\frac{t^2 - a}{b}\right| \leq \left|\frac{t^2}{b}\right| + \left|\frac{a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|.$$

Uit de inductiehypothese volgt nu dat de vorm f' nul representeert in $\mathbb{Q}$, omdat b'' kwadraatvrij is. Er geldt dus $1 = (a, b'')_{\mathbb{Q}} = (a, b''u^2)_{\mathbb{Q}} = (a, b')_{\mathbb{Q}} = (a, b)_{\mathbb{Q}}$ uit 3.12 en f representeert 0. Inductie geeft het resultaat.

• $n = 4$
We schrijven $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$ met $a, b, c, d \in \mathbb{Z} \setminus \{0\}$. Zij $v \in V$. Omdat f_v nul representeert in $\mathbb{Q}_v$, bestaat er een $x_v \in \mathbb{Q}_v$ die zowel gerepresenteerd wordt door $aX_1^2 + bX_2^2$ als door $cX_3^2 + dX_4^2$. Als geldt $x_v = 0$, representeren $aX_1^2 + bX_2^2$ en $cX_3^2 + dX_4^2$ alle elementen uit $\mathbb{Q}_v$ wegens 3.7. We kunnen dus aannemen $x_v \in \mathbb{Q}_v^*$. Toepassen van 3.16 geeft de identiteiten $(x_v, -ab)_v = (a, b)_v$ en $(x_v, -cd)_v = (c, d)_v$ voor $v \in V$. Met 3.18 volgt

$$\prod_{v \in V} (a, b)_v = 1 \quad \text{en} \quad \prod_{v \in V} (c, d)_v = 1.$$

Uit 3.21 bestaat er een $x \in \mathbb{Q}^*$ met $(x,-ab)_v = (a,b)_v$ en $(x,-cd)_v = (c,d)_v$ voor alle $v \in V$. We schrijven met behulp van 3.15 en 3.17 voor $v \in V$:

$$1 = (x,-ab)_v(a,b)_v = (x,-ab)_v(a,-ab)_v = (xa,-ab)_v = (xa,a^2xb)_v = (xa,xb)_v.$$

Er volgt dat de vorm $Z^2 - xaX_1^2 - xbX_2^2$ nul representeert, oftewel dat de vorm $xZ^2 - x^2aX_1^2 - x^2bX_2^2 \sim xZ^2 - aX_1^2 - bX_2^2$ het element 0 representeert over $\mathbb{Q}_v$ voor alle $v \in V$ en daarom ook in $\mathbb{Q}$ uit het geval $n = 3$. Dus wordt $x \in \mathbb{Q}^*$ gerepresenteerd door $aX_1^2 + bX_2^2$ met 3.8. Geheel analoog volgt dat $cX_3^2 + dX_4^2$ het element $x \in \mathbb{Q}^*$ representeert en dus heeft f een niet-triviaal nulpunt.

• $n \geq 5$
We bewijzen met inductie naar n. Voor $n \leq 4$ weten we dat de stelling waar is uit voorgaande. Dus laat $n \geq 5$ en neem aan dat de stelling waar is voor kwadratische vormen in minder dan n variabelen. Schrijf $f = h - g$ met h, g de kwadratische vormen $h = a_1X_1^2 + a_2X_2^2$ en $g = a_3X_3^2 + \ldots + a_nX_n^2$. Laat $S \subset V$ de deelverzameling bestaande uit $\infty, 2$ en de priemen die a_i delen voor $3 \leq i \leq n$. Het is duidelijk dat S eindig is. Zij $s \in S$. Er bestaat een $b_s \in \mathbb{Q}_s$, die wordt gerepresenteerd door h_s en g_s, want f_s representeert 0. Stel $b_s = 0$, dan representeren h_s en g_s alle elementen uit $\mathbb{Q}_s$ wegens 3.7. We concluderen dat we mogen aannemen $b_s \in \mathbb{Q}_s^*$.

Laat nu $(x_1^s, x_2^s) \in \mathbb{Q}_s^2 \setminus \{0\}$ zodanig dat $h(x_1^s, x_2^s) = b_s$. Uit 2.6 volgt dat er rijtjes $(x_{1,i})_i$ en $(x_{2,i})_i$ in $\mathbb{Q}$ bestaan zodanig dat geldt $\lim_{i\to\infty} x_{1,i} = x_1^s$ en $\lim_{i\to\infty} x_{2,i} = x_2^s$ voor alle $s \in S$. Laat nu $\alpha_i = h(x_{1,i}, x_{2,i}) \in \mathbb{Q}$, er volgt uit de continuïteit van de functie $x \mapsto x^2$ in $\mathbb{Q}_s$ ($\mathbb{Q}_s$ is een topologisch lichaam) voor $s \in S$

$$b_s = a_1(x_1^s)^2 + a_2(x_2^s)^2 = \lim_{i\to\infty} a_1x_{1,i}^2 + a_2x_{2,i}^2 = \lim_{i\to\infty} \alpha_i.$$

Gevolg 2.10 geeft nu dat er een $i \in \mathbb{N}$ bestaat zodanig dat voor $\beta = \alpha_i \in \mathbb{Q}^*$ geldt dat β/b_s een kwadraat is in $\mathbb{Q}_s^*$ voor alle $s \in S$. Laat nu $\gamma_s \in \mathbb{Q}_s^*$ zodanig dat $\gamma_s^2 = \beta/b_s$. Als geldt $s \in S$, representeert g_s het element $b_s \in \mathbb{Q}_s^*$. Er bestaat dus een $y_s \in \mathbb{Q}_s^{n-2} \setminus \{0\}$ zodanig dat $g_s(y_s) = b_s$. Er geldt $g_s(\gamma_s y_s) = \gamma_s^2 g_s(y_s) = \beta$. Dus g_s representeert ook het element β in $\mathbb{Q}_s^*$ voor alle $s \in S$.

Stel nu $v \in V \setminus S$, dan is $v \neq 2$ een priemgetal en geldt $\det(A_g) = a_3 \ldots a_n \in \mathbb{Z}_v^*$. In het bijzonder representeert de vorm g_v in $n - 2 \geq 3$ variabelen het element 0 uit 3.10 en daarmee alle elementen in $\mathbb{Q}_v$ wegens 3.7. Ook voor $v \notin S$ wordt β in $\mathbb{Q}_v$ gerepresenteerd door g_v. We vinden dat β voor alle $v \in V$ wordt gerepresenteerd door g_v.

Beschouw de kwadratische vorm $k = g - \beta Z^2 \in \mathbb{Q}[X_3, \ldots, X_n, Z]$. Nul wordt dus gerepresenteerd door k_v voor alle $v \in V$. Het aantal variabelen van k is gelijk aan $n - 1$ en dus volgt uit de inductiehypothese dat k nul representeert in $\mathbb{Q}$. Wegens 3.8 representeert g nu $\beta \in \mathbb{Q}^*$. Het is duidelijk dat $\beta = \alpha_i = h(x_{1,i}, x_{2,i})$ en dus representeert h het element $\beta \in \mathbb{Q}^*$. We concluderen dat f nul representeert en het resultaat volgt met inductie. □

3.23 Gevolg. *Een kwadratische vorm $f \in \mathbb{Q}[X_1, \ldots, X_n]$ representeert $a \in \mathbb{Q}^*$ precies dan als $f_v \in \mathbb{Q}_v[X_1, \ldots, X_n]$ het element a representeert voor alle $v \in V$.*

Bewijs. Het is meteen helder dat als f het element a representeert, dat a wordt gerepresenteerd door f_v voor alle $v \in V$. Neem nu andersom aan dat f_v het element a representeert voor alle $v \in V$. Beschouw de vorm $g = f - aZ^2 \in \mathbb{Q}[X_1, \ldots, X_n, Z]$. Dan volgt dat g_v nul representeert in $\mathbb{Q}_v$ voor alle $v \in V$. Er volgt dus dat g een niet-triviaal nulpunt in $\mathbb{Q}$ heeft en met 3.8 volgt dat f het element $a \in \mathbb{Q}^*$ representeert. □

3.24 Lemma (Davenport-Cassels)**.** *Zij $f \in \mathbb{Q}[X_1, \ldots, X_n]$ een kwadratische vorm zodanig dat A_f coëfficiënten in $\mathbb{Z}$ heeft en er voor alle $x \in \mathbb{Q}^n$ een element $y \in \mathbb{Z}^n$ bestaat zodanig dat $f(x - y) < 1$. Als $a \in \mathbb{Z}$ wordt gerepresenteerd door $f \in \mathbb{Q}$ dan bestaat er een $z \in \mathbb{Z}^n \setminus \{0\}$ zodanig dat $f(z) = a$.*

Bewijs. Het bewijs van dit technische lemma maakt slechts gebruik van algebraïsche manipulatie met de kwadratische vorm f. We verwijzen naar lemma B uit de appendix van hoofdstuk IV uit [SE]. □

3.25 Gevolg (Lagrange)**.** *De vergelijking $X^2+Y^2+Z^2+W^2=n$ heeft een oplossing over $\mathbb{Z}$ voor elke $n \geq 0$, oftewel ieder natuurlijk getal kan geschreven worden als een som van vier kwadraten.*

Bewijs. Schrijf $n = 4^a m$ voor $a, m \in \mathbb{Z}$ zodanig dat 4 niet m deelt. Beschouw de kwadratische vorm $f = X^2+Y^2+Z^2 \in \mathbb{Q}[X,Y,Z]$. We laten zien dat als geldt $m \equiv 1,2,5,6 \bmod 8$ de vorm f het element m representeert in $\mathbb{Q}$. Uit $f_\infty(\sqrt{m},0,0) = m$ volgt dat m wordt gerepresenteerd door f_∞. Zij p een priemgetal ongelijk aan 2. Met behulp van 3.20 volgt $(-1,-1)_p = 1$. Dus representeert de kwadratische vorm f_p nul in $\mathbb{Q}_p$ en daarmee alle elementen uit $\mathbb{Q}_p$ wegens 3.7, dus in het bijzonder m.

Laat nu $p = 2$. Beschouw het polynoom $g = f_p - m \in \mathbb{Z}_p[X,Y,Z]$. Kies nu $x = (1,0,0)$ als $m \equiv 1 \bmod 8$, $x = (1,1,0)$ als $x \equiv 2 \bmod 8$, $x = (1,2,0)$ als $x \equiv 5 \bmod 8$ en tot slot $x = (1,1,2)$ als $m \equiv 6 \bmod 8$. Er geldt $g(x) \equiv 0 \bmod 8$ en $v_p(\frac{\partial g}{\partial X}(x)) = v_p(2) = 1$. Nu geeft 2.7 ($n = 3, k = 1$) dat er een $y \in \mathbb{Z}_p^3$ bestaat zodanig dat $f_p(y) = m$ en $y_i \equiv x_i \bmod 2$. Er geldt dus $y \neq 0$ en de vorm f_2 representeert m.

Dus de vorm f representeert $m \in \mathbb{Q}$ wegens 3.23. Neem $u \in \mathbb{Q}^3$, er bestaat een $v \in \mathbb{Z}^3$ zodanig dat $|u_i - v_i| \leq \frac{1}{2}$ voor $i = 1,2,3$. Er volgt $f(u-v) = \sum_{i=1}^3 (u_i - v_i)^2 \leq \frac{3}{4} < 1$. Met 3.24 bestaat er een $z \in \mathbb{Z}^3 \setminus \{0\}$ zodanig dat $f(z) = m$. We kunnen m dus schrijven als een som van drie kwadraten als $m \equiv 1,2,5,6 \bmod 8$. Als $m \equiv 3,7 \bmod 8$ volgt dat we $m-1$ kunnen schrijven als som van drie kwadraten en dus m als som van vier kwadraten. Door elk van de vier kwadraten uit de som van m met een factor 2^a te vermenigvuldigen ziet men in dat $X^2+Y^2+Z^2+W^2 = n$ een oplossing over $\mathbb{Z}$ heeft voor elke $n \geq 0$. $\square$

4 Tegenvoorbeeld lokaal-globaalprincipe voor kubische vormen

4.1 Definitie. Zij K een lichaam en $n \geq 1$. Een homogeen kubisch polynoom $f = \sum_{i,j,k} a_{ijk} X_i X_j X_k$ in $K[X_1, \ldots, X_n]$ heet een *kubische vorm*.

We bewijzen in deze paragraaf dat het lokaal-globaalprincipe niet opgaat voor kubische vormen. We beschouwen hiervoor de kubische vorm $f = 3X^3 + 4Y^3 + 5Z^3 \in \mathbb{Q}[X, Y, Z]$. Eerst zullen we bewijzen dat f slechts een triviaal nulpunt heeft over $\mathbb{Q}$ en vervolgens laten we zien dat f_v nul representeert over $\mathbb{Q}_v$ voor alle $v \in V$. Uit het laatste volgt dat f gezien over $\mathbb{Z}/p^n\mathbb{Z}$ een niet-triviaal nulpunt heeft voor elke priemmacht p^n. Als $(x, y, z) \in \mathbb{Q}_p$ immers een niet-triviale oplossing is en we nemen $h = \min\{v_p(x'), v_p(y'), v_p(z')\}$, dan is $(x, y, z) = p^{-h}(x', y', z')$ een oplossing in $\mathbb{Z}_p^3$, zodanig dat x, y of z een eenheid is in $\mathbb{Z}_p$. Om aan te tonen dat de vergelijking $3X^3 + 4Y^3 + 5Z^3 = 0$ slechts een triviale rationale oplossing heeft, is het dus niet mogelijk te reduceren modulo k voor een geheel getal k en aan te tonen dat de vergelijking modulo k geen niet-triviale oplossing heeft, waarbij we gebruiken dat voor een oplossing $(u, v, w) \in \mathbb{Q}^3 \setminus \{0\}$ moet gelden dat u, v, w paarsgewijs copriem zijn (zie 4.16). We blijken methodes uit de algebraïsche getaltheorie nodig te hebben. We werken hierbij over de ring $\mathbb{Z}[\sqrt[3]{6}]$ en zullen ervan gebruik maken dat elementen van deze ring op unieke wijze factoriseren in priemelementen. Het is hiervoor nuttig de norm van de uitbreiding $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{6})$ te beperken tot de ring $\mathbb{Z}[\sqrt[3]{6}]$.

4.1 De norm

4.2 Definitie. Zij $K \subset L$ een eindige separabele lichaamsuitbreiding en kies een algebraïsch afgesloten lichaam Ω dat K bevat. Noteer $X(L/K) = \mathrm{Hom}_K(L, \Omega)$ voor de fundamentele verzameling van de uitbreiding. De *norm* van een element $x \in L$ is gedefinieerd als:

$$N_{L/K}(x) = \prod_{\sigma \in X(L/K)} \sigma(x).$$

Aangezien $K \subset L$ eindig en separabel is, vinden we $\#X(L/K) = [L : K]$ eindig en dus is de norm goed gedefinieerd als element van Ω. Men ziet meteen in dat de norm multiplicatief is, dat wil zeggen voor $x, y \in L$ geldt $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$. Zij nu $x \in L$ een primitief element, waarvan het bestaan wordt gegarandeerd doordat $K \subset L$ eindig en separabel is. Zij $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ het minimumpolynoom van x. De nulpunten van f zijn precies de n verschillende $\sigma(x)$ met $\sigma \in X(L/K)$. Er geldt dus $N_{L/K}(x) = (-1)^n a_0 \in K$. Neem nu $y \in L$ en beschouw de toren $K \subset K(y) \subset L$. Iedere inbedding $L \to \Omega$ kan verkregen worden door voor iedere inbedding $K(y) \to \Omega$ de $[L : K(y)]$ voortzettingen te beschouwen. Hieruit vinden we

$$N_{L/K}(y) = N_{K(y)/K}(y)^{[L:K(y)]} \in K$$

omdat we eerder zagen $N_{K(y)/K}(y) \in K$, daar y een primitief element voor de uitbreiding $K \subset K(y)$ is. De norm is dus een multiplicatief groepshomomorfisme $N_{L/K} : L^* \to K^*$.

4.2 De ring $\mathbb{Z}[\alpha]$ met α algebraïsch geheel

4.3 Definitie. Een element $\alpha \in \overline{\mathbb{Q}}$ heet *algebraïsch geheel* als het minimumpolynoom van α over $\mathbb{Q}$ coëfficiënten in $\mathbb{Z}$ heeft.

Voor de rest van deze paragraaf beschouwen we de uitbreiding $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ van graad n, waarbij α algebraïsch geheel is. Daar $\mathbb{Q}$ een perfect lichaam is, is de uitbreiding eindig en separabel. Het is duidelijk dat $\mathbb{Z}[\alpha] = \{\sum_{i=0}^{n-1} b_i \alpha^i : b_i \in \mathbb{Z}\}$ een deelring van $\mathbb{Q}(\alpha)$ is. In dit geval blijkt dat de beperking van de norm tot $\mathbb{Z}[\alpha]$ als beeld $\mathbb{Z}$ heeft.

4.4 Lemma. *Zij $x \in \mathbb{Z}[\alpha]$ en g het minimumpolynoom van x over $\mathbb{Q}$. Er geldt $g \in \mathbb{Z}[X]$.*

Bewijs. Er geldt $x\alpha^i \in \mathbb{Z}[\alpha]$ met $0 \leq i < n-1$, omdat $\mathbb{Z}[\alpha]$ een ring is. We kunnen schrijven $x\alpha^i = \sum_{j=0}^{n-1} b_{ij}\alpha^j$. Laat z de vector $(\alpha^i)_{0\leq i<n} \in \mathbb{Z}[\alpha]^n$ en B de matrix $(b_{ij})_{0\leq i,j<n}$ in $\mathrm{Mat}_n(\mathbb{Z})$. Er geldt $xz = Bz$ met $z \neq 0$. Als gevolg is de determinant van de matrix $xI - B$ nul, omdat $\mathbb{Z}[\alpha]$ een domein is als deelring van een lichaam. Het monische polynoom $\det(XI - B) \in \mathbb{Z}[X]$ heeft dus x als nulpunt en dus heeft het minimumpolynoom g van x over $\mathbb{Q}$ gehele coëfficiënten wegens het lemma van Gauss. □

4.5 Gevolg. *De beperking van de norm tot $\mathbb{Z}[\alpha]$ is een multiplicatieve afbeelding $\mathbb{Z}[\alpha] \to \mathbb{Z}$.*

Bewijs. Als $x \in \mathbb{Z}[\alpha]$ volgt dat de constante term c_0 van het minimumpolynoom g van x over $\mathbb{Q}$ geheel is. Er volgt dat $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x) = N_{\mathbb{Q}(x)/\mathbb{Q}}(x)^{[\mathbb{Q}(\alpha):\mathbb{Q}(x)]}$ geheel is uit $N_{\mathbb{Q}(x)/\mathbb{Q}}(x) = (-1)^{\deg(g)}c_0 \in \mathbb{Z}$. □

Aangezien de lichaamsuitbreiding $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ duidelijk is, zullen we de norm simpelweg noteren als N. We gaan de eenhedengroep van $\mathbb{Z}[\alpha]$ nader bekijken. We kiezen $\mathbb{C}$ als algebraïsch afgesloten lichaam Ω dat $\mathbb{Q}$ bevat. De norm stelt ons in staat vast te stellen welke elementen in $\mathbb{Z}[\alpha]$ eenheden zijn.

4.6 Propositie. *Er geldt $a \in \mathbb{Z}[\alpha]^*$ dan en slechts dan als $N(a) \in \mathbb{Z}^* = \{\pm 1\}$.*

Bewijs. Stel $a \in \mathbb{Z}[\alpha]^*$, dan geldt $1 = N(1) = N(aa^{-1}) = N(a)N(a^{-1})$ en dus is $N(a)$ een eenheid in $\mathbb{Z}$. Als andersom geldt $N(a) \in \mathbb{Z}^*$, volgt $N(a)N(a)^{-1} = 1$. Daar de identiteit een inbedding in $X(\mathbb{Q}(\alpha)/\mathbb{Q})$ is, vinden we de factor a in het product $N(a)$. Dus is a een eenheid in $\mathbb{Z}[\alpha]$. □

4.7 Definitie. We noemen een inbedding $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ een *reële inbedding* als $\sigma[\mathbb{Q}(\alpha)] \subset \mathbb{R}$ en anders een *complexe inbedding.*

Het beeld van $\mathbb{Q}(\alpha)$ onder $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ ligt volledig vast door het beeld $\sigma(\alpha)$, want de elementen van $\mathbb{Q}(\alpha)$ zijn $\mathbb{Q}$-polynomiale expressies in α. Dus is $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ een reële inbedding dan en slechts dan als $\sigma(\alpha) \in \mathbb{R}$. Als $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ een complexe inbedding is, is de samenstelling van σ met de complexe conjugatie een andere complexe inbedding. De complexe inbeddingen kunnen we dus indelen in geconjugeerde tweetallen. Er geldt daarmee $r_1 + 2r_2 = n$, voor r_1 het aantal reële inbeddingen en r_2 het aantal paren complexe inbeddingen. Nummer de inbeddingen in $X(\mathbb{Q}(\alpha)/\mathbb{Q})$, zodanig dat $\sigma_1, \ldots, \sigma_{r_1}$ de reële inbeddingen zijn en $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ representanten van de paren complexe inbeddingen. Beschouw nu de afbeelding $\lambda : \mathbb{Z}[\alpha]^* \to \mathbb{R}^{r_1+r_2}$ gegeven door

$$\lambda(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|)$$

waarbij $|\cdot|$ de absolute waarde is over het complexe vlak. Het is duidelijk dat λ een homomorfisme is van de multiplicatieve eenhedengroep $\mathbb{Z}[\alpha]^*$ naar de optelgroep $\mathbb{R}^{r_1+r_2}$. De vector $\lambda(x)$ voor $x \in \mathbb{Z}[\alpha]^*$ bevat de waardes van de logaritmen van $|\sigma(x)|$ voor *alle* $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$, aangezien de paren complexe inbeddingen dezelfde absolute waarde hebben ($|\sigma(x)| = |\overline{\sigma(x)}|$). Via λ bepalen we de structuur van de eenhedengroep $\mathbb{Z}[\alpha]^*$.

4.8 Lemma. *Laat $C \subset \mathbb{R}^{r_1+r_2}$ een begrensde deelverzameling, dan is $B = \{x \in \mathbb{Z}[\alpha]^* : \lambda(x) \in C\}$ eindig.*

Bewijs. Voor alle $x \in B$ en $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ geldt $|\sigma(x)| \in [0, a]$ met $a > 1$, immers C is begrensd. Alle elementaire symmetrische polynomen in $\sigma(x)$ voor $x \in B$ en $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ bevinden zich dus ook in een interval $[0, b]$ voor zekere $b > 1$.

Voor $x \in \mathbb{Z}[\alpha]$ weten we dat alle nulpunten van het minimumpolynoom f van x van de vorm $\sigma(x)$ zijn met $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$. De coëfficiënten van f zijn op teken na elementaire symmetrische polynomen in $\sigma(x)$ met $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$ en bevinden zich wegens 4.4 in $\mathbb{Z}$. Deze coëfficiënten van het minimumpolynoom van een element $x \in B$ bevinden zich dus in $[-b, b] \cap \mathbb{Z}$ en er zijn dus eindig veel keuzes hiervoor. Er zijn dus eindig veel mogelijke minimumpolynomen voor elementen $x \in B$ en daarmee is B eindig. □

4.9 Gevolg. *De ondergroep* $\ker\lambda$ *van* $\mathbb{Z}[\alpha]^*$ *is eindig en cyclisch en bestaat precies uit de eenheidswortels in* $\mathbb{Z}[\alpha]^*$.

Bewijs. Toepassen van voorgaand lemma op $C = \{0\}$ geeft dat $\ker\lambda$ eindig is en als eindige ondergroep van de eenhedengroep van het domein $\mathbb{Z}[\alpha]$ is $\ker\lambda$ cyclisch. Omdat $\ker\lambda$ eindig is volgt voor $x \in \ker\lambda$ dus $x^m = 1$ voor zekere m, dus bestaat $\ker\lambda$ volledig uit eenheidswortels. Als andersom $x \in \mathbb{Z}[\alpha]^*$ een eenheidswortel is, dan geldt $x^m = 1$ voor zekere m. We zien $|\sigma(x)|^m = |\sigma(x^m)| = 1$ en dus geldt $|\sigma(x)| = 1$ voor alle $\sigma \in X(\mathbb{Q}(\alpha)/\mathbb{Q})$. Er volgt $x \in \ker\lambda$. Dus bestaat $\ker\lambda$ precies uit de eenheidswortels in $\mathbb{Z}[\alpha]^*$. □

4.10 Stelling (zwakke eenhedenstelling van Dirichlet)**.** *De eenhedengroep* $\mathbb{Z}[\alpha]^*$ *is isomorf met* $G\times\mathbb{Z}^s$ *waarbij* $s \leq r_1+r_2-1$ *met* G *een eindige en cyclische groep, die precies bestaat uit de eenheidswortels in* $\mathbb{Z}[\alpha]^*$.

Bewijs. Merk op dat het beeld $\lambda[\mathbb{Z}[\alpha]^*]$ een discrete ondergroep van $\mathbb{R}^{r_1+r_2}$ is uit 4.8. Wegens een bekend resultaat uit de algebra (zie stelling 9.10 uit [SH]) is $\lambda[\mathbb{Z}[\alpha]^*]$ een vrij $\mathbb{Z}$-moduul van rang $s \leq r_1 + r_2$. Als $x \in \mathbb{Z}[\alpha]^*$ volgt uit 4.6

$$1 = |N(x)| = \left|\prod_{i=1}^{n}\sigma_i(x)\right| = \prod_{i=1}^{r_1}|\sigma_i(x)| \cdot \prod_{i=r_1+1}^{r_1+r_2}|\sigma_i(x)\overline{\sigma_i(x)}|.$$

Noteer nu $\lambda(x) = (y_1, \ldots, y_{r_1+r_2})$. Nemen we nu de logaritme van bovenstaande vergelijking, volgt

$$0 = \sum_{i=1}^{r_1} y_i + 2\sum_{i=r_1+1}^{r_1+r_2} y_i.$$

Dus ligt $\lambda(x)$ in een hypervlak met dimensie r_1+r_2-1. Het beeld $\lambda[\mathbb{Z}[\alpha]^*]$ is vrij van rang $s \leq r_1+r_2-1$. Noteer nu $G = \ker\lambda$, er volgt $\mathbb{Z}^s \cong \lambda[\mathbb{Z}[\alpha]^*] \cong \mathbb{Z}[\alpha]^*/G$ met de isomorfiestelling. Aangezien G eindig is en $\mathbb{Z}^s$ torsievrij, volgt uit $\mathbb{Z}^s \cong \mathbb{Z}[\alpha]^*/G$ dat $\mathbb{Z}[\alpha]^*$ isomorf is met $G \times \mathbb{Z}^s$. De gewenste eigenschappen voor G volgen uit 4.9. □

Tot slot speelt factorisatie in $\mathbb{Z}[\sqrt[3]{6}]$ een belangrijke rol in het bewijs van het tegenvoorbeeld. Hiervoor is het nuttig te weten welke priemidealen in een ideaal $(p) \subset \mathbb{Z}[\alpha]$ bevat zijn voor een priemgetal $p \in \mathbb{Z}$.

4.11 Propositie. *Zij* $p \in \mathbb{Z}$ *een priemgetal en* $g = g_1^{e_1}\ldots g_d^{e_d}$ *de factorisatie van het minimumpolynoom van* α *in* $\mathbb{F}_p$. *De idealen* $(p, g_1(\alpha))$ *zijn maximaal en er geldt*[7]

$$(p, g_1(\alpha))^{e_1}\ldots(p, g_d(\alpha))^{e_d} \subset (p).$$

Bewijs. We laten eerst zien dat idealen van de vorm $(p, g_i(\alpha))$ maximaal zijn. Het polynoom g_i is irreducibel in $\mathbb{F}_p[X]$. Het ideaal (g_i) is dus een priemideaal en daarmee maximaal, aangezien $\mathbb{F}_p[X]$ een hoofdideaaldomein is. Het is duidelijk dat $\mathbb{F}_p[X]/(g_i) \cong \mathbb{Z}[X]/(p, g_i)$ een lichaam is. Omdat gezien over $\mathbb{Z}[X]$ geldt $g = g_1^{e_1}\ldots g_d^{e_d} + ph$ voor een polynoom $h \in \mathbb{Z}[X]$ volgt $g \in (p, g_i)$ en $(p, g_i) = (g, p, g_i)$. Er geldt $\mathbb{Z}[X]/(g, p, g_i) \cong (\mathbb{Z}[X]/(g))/(p, g_i) \cong \mathbb{Z}[\alpha]/(p, g_i(\alpha))$. Omdat g het minimumpolynoom is van α, zijn $\mathbb{Z}[\alpha]$ en $\mathbb{Z}[X]/(g)$ immers isomorf. Dus is $\mathbb{Z}[\alpha]/(p, g_i(\alpha)) \cong \mathbb{F}_p[X]/(g_i)$ een lichaam en $(p, g_i(\alpha))$ een maximaal ideaal.

Voor de te bewijzen inclusie van idealen nemen we een element in $x \in (p, g_1(\alpha))^{e_1}\ldots(p, g_d(\alpha))^{e_d}$. We merken op dat x een som is van producten $y = \prod_{j=1}^{e_1+\ldots+e_d} y_j$ waarbij $y_j = p$ of $y_j = g_i(\alpha)$ voor zekere i. Als $y_j = p$ voor een zekere j volgt $p \mid y$. Als y_j van de vorm $g_i(\alpha)$ is voor alle j wordt y gedeeld door het product $g_1(\alpha)^{e_1}\ldots g_d(\alpha)^{e_d}$. Er geldt dus $x \in (p, g_1(\alpha)^{e_1}\ldots g_d(\alpha)^{e_d})$. Door nu het beeld van $g_1^{e_1}\ldots g_d^{e_d} - g \in p\mathbb{Z}[X]$ onder de evaluatieafbeelding in α te bekijken, vinden we $g_1(\alpha)^{e_1}\ldots g_d(\alpha)^{e_d} \in p\mathbb{Z}[\alpha] = (p)$. Dit geeft de gelijkheid $(p, g_1(\alpha)^{e_1}\ldots g_d(\alpha)^{e_d}) = (p)$ en er geldt $x \in (p)$. De te bewijzen ideaalinclusie volgt. □

[7] In feite geldt voor alle priemgetallen op eindige veel na gelijkheid, zie pagina 199–201 uit [CH]

4.3 Het hoofdideaaldomein $\mathbb{Z}[\sqrt[3]{6}]$

Beschouw de deelring $\mathbb{Z} \subset \mathbb{Q}$ en de eindige en separabele uitbreiding $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{6})$ van graad 3. Aangezien het minimumpolynoom $g = X^3-6$ van $\sqrt[3]{6}$ over $\mathbb{Q}$ coëfficiënten in $\mathbb{Z}$ heeft, is $\sqrt[3]{6}$ algebraïsch geheel en kunnen we de norm N beperken tot de ring $\mathbb{Z}[\sqrt[3]{6}] = \{a + b\sqrt[3]{6} + c\sqrt[3]{36} : a, b, c \in \mathbb{Z}\}$, waarbij we $\sqrt[3]{36}$ definiëren als $(\sqrt[3]{6})^2$. De nulpunten van g zijn precies de 3 verschillende $\sigma(\sqrt[3]{6})$ met $\sigma \in X(\mathbb{Q}(\sqrt[3]{6})/\mathbb{Q})$. Er volgt dus $\sigma_1(\sqrt[3]{6}) = \sqrt[3]{6}, \sigma_2(\sqrt[3]{6}) = \zeta_3\sqrt[3]{6}$ en $\sigma_3(\sqrt[3]{6}) = \zeta_3^2\sqrt[3]{6}$ waarbij ζ_3 een primitieve 3-de eenheidswortel is in $\overline{\mathbb{Q}}$ en $X(\mathbb{Q}(\sqrt[3]{6})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3\}$. Laat nu $a+b\sqrt[3]{6}+c\sqrt[3]{36} \in \mathbb{Z}[\sqrt[3]{6}]$, er geldt

$$N(a+b\sqrt[3]{6}+c\sqrt[3]{36}) = \prod_{i=1}^{3} \sigma_i(a+b\sqrt[3]{6}+c\sqrt[3]{36}) = \prod_{i=1}^{3} a+b\sigma_i(\sqrt[3]{6})+c(\sigma_i(\sqrt[3]{6}))^2 = -18abc+a^3+6b^3+36c^3$$

waarbij we in de laatste stap het product uitwerken en de expressies voor $\sigma_i(\sqrt[3]{6})$ substitueren. Merk op dat geldt $\sigma_i(\sqrt[3]{6}) \in \mathbb{R}$ dan en slechts dan als $i = 1$. Er bestaan dus één reële inbedding en twee complexe inbeddingen in $X(\mathbb{Q}(\sqrt[3]{6})/\mathbb{Q})$. We beschouwen de eenhedengroep nader.

4.12 Lemma. *De eenhedengroep $\mathbb{Z}[\sqrt[3]{6}]^*$ is gelijk aan $\langle \pm u \rangle$ met $u \in \mathbb{Z}[\sqrt[3]{6}]$.*

Bewijs. Er zijn één reële inbedding en twee complexe inbeddingen van $\mathbb{Z}[\sqrt[3]{6}]$ in $\mathbb{C}$. Uit 4.10 volgt $\mathbb{Z}[\sqrt[3]{6}] \cong G \times \mathbb{Z}$ of $\mathbb{Z}[\sqrt[3]{6}] \cong G$ waarbij G de groep is bestaande uit de eenheidswortels in $\mathbb{Z}[\sqrt[3]{6}]^*$. Omdat $\mathbb{Z}[\sqrt[3]{6}]$ ingebed kan worden in $\mathbb{R}$ bevat $\mathbb{Z}[\sqrt[3]{6}]$ slechts de eenheidswortels ± 1. Er geldt dus $G = \{\pm 1\}$. Aangezien voor $v = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36} \neq \pm 1$ geldt $N(v) = 1$, zijn er meer eenheden dan $\{\pm 1\}$ in $\mathbb{Z}[\sqrt[3]{6}]$. Er volgt $\mathbb{Z}[\sqrt[3]{6}]^* \cong \{\pm 1\} \times \mathbb{Z}$. Er bestaat dus een eenheid $u \in \mathbb{Z}[\sqrt[3]{6}]$ van oneindige orde zodanig dat $\mathbb{Z}[\sqrt[3]{6}]^* \cong \langle \pm u \rangle$. □

Om aan te tonen dat de rationale kubische vorm $3X^3 + 4Y^3 + 5Z^3$ een tegenvoorbeeld is van het lokaal-globaalprincipe, is het belangrijk meer te weten te komen over de factorisatie van elementen in $\mathbb{Z}[\sqrt[3]{6}]$. We gebruiken hierbij methodes uit de algebraïsche getaltheorie, welke we omwille van de lengte van de scriptie hier niet verder toe zullen lichten.

4.13 Lemma. *Elk niet-nul ideaal in $\mathbb{Z}[\sqrt[3]{6}]$ ontbindt op unieke wijze in een product van maximale idealen.*

Bewijs (schets)**.** Beschouw een kubische uitbreiding $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{m})$ met $m = m_1m_2^2$, $\gcd(m_1, m_2) = 1$ en $m_1, m_2 \in \mathbb{Z}$ kwadraatvrij. Uit een propositie van Dedekind uit 1900 (zie pagina 132 uit [KA]) weten we dat als $m_1 \not\equiv \pm m_2 \bmod 9$, de discriminant van $\mathbb{Q}(\sqrt[3]{m})$ gelijk aan $-27m_1^2m_2^2$ is en 1, $\sqrt[3]{m_1m_2}$, $\sqrt[3]{m_1^2m_2}$ een basis van gehelen vormt. Nemen we $m = 6$, vinden we $m_1 = 6$ en $m_2 = 1$ en $m_1 \not\equiv \pm m_2 \bmod 9$. Dus de ring van gehelen van het lichaam $\mathbb{Q}(\sqrt[3]{6})$ heeft een basis van gehelen bestaande uit 1, $\sqrt[3]{6}$, $\sqrt[3]{36}$. Het is duidelijk dat $\mathbb{Z}[\sqrt[3]{6}]$ de ring van gehelen van het lichaam $\mathbb{Q}(\sqrt[3]{6})$ is. Een bekend feit (zie propositie 12.2.8 in [IR]) uit de algebraïsche getaltheorie is dat in een ring van algebraïsche gehelen elk ideaal in een uniek product van maximale idealen ontbindt. □

Om te bewijzen dat $\mathbb{Z}[\sqrt[3]{6}]$ een hoofdideaaldomein is, is het nuttig om de hoofdidealen $(2), (3), (5), (7)$ en $(\sqrt[3]{6})$ te ontbinden in een product van maximale idealen. We ontbinden hiervoor het minimumpolynoom $g = X^3 - 6$ van $\sqrt[3]{6}$ in irreducibele factoren in $\mathbb{F}_p$ voor $p = 2, 3, 5$ en 7. We vinden $X^3, X^3, (X^2 + X + 1)(X - 1)$ respectievelijk $(X + 1)(X + 2)(X - 3)$ als ontbinding. Er volgt

$$(2, \sqrt[3]{6})^3 = (2), \quad (3, \sqrt[3]{6})^3 = (3), \quad (5, -1+\sqrt[3]{6})(5, 1 + \sqrt[3]{6} + \sqrt[3]{36}) = (5),$$
$$(7, 1 + \sqrt[3]{6})(7, 2 + \sqrt[3]{6})(7, -3 + \sqrt[3]{6}) = (7).$$

waarbij de inclusie $\subset$ volgt uit 4.11 en de inclusie $\supset$ met behulp van de identiteiten

$$2 = 2^3 - (\sqrt[3]{6})^3, \quad 3 = 3^3 - 4(\sqrt[3]{6})^3, \quad 5 =(-1 + \sqrt[3]{6})(1 + \sqrt[3]{6} + \sqrt[3]{36}),$$
$$7 = 7^3 + 8\sqrt[3]{36}(1 + \sqrt[3]{6})(2 + \sqrt[3]{6})(-3 + \sqrt[3]{6}).$$

Aanschouw nu de volgende elementen en hun norm:

$$\begin{aligned} p_2 &= 2 - \sqrt[3]{6} & N(p_2) &= 2; \\ p_3 &= 3 + 2\sqrt[3]{6} + \sqrt[3]{36} & N(p_3) &= 3; \\ p_5 &= -1 + \sqrt[3]{6} & N(p_5) &= 5; \\ p_{25} &= 1 + \sqrt[3]{6} + \sqrt[3]{36} & N(p_{25}) &= 25; \\ p_{7,1} &= 1 + \sqrt[3]{6} & N(p_{7,1}) &= 7; \\ p_{7,2} &= 7 + 4\sqrt[3]{6} + 2\sqrt[3]{36} & N(p_{7,2}) &= 7; \\ p_{7,3} &= -5 + \sqrt[3]{6} + \sqrt[3]{36} & N(p_{7,3}) &= 7. \end{aligned}$$

Daar een element $q \in \mathbb{Z}[\sqrt[3]{6}]$ zelf een factor is in de norm $N(q)$, volgt $q \mid N(q)$. Voor $i = 2, 3$ concluderen we uit $p_i \mid N(p_i) = i$ en de identiteit

$$\sqrt[3]{6} = p_2 p_3$$

dat geldt $(i, \sqrt[3]{6}) \subset (p_i)$. Wegens 4.11 is $(i, \sqrt[3]{6})$ een maximaal ideaal. Omdat p_i uit 4.6 geen eenheid is, volgt dus $(i, \sqrt[3]{6}) = (p_i)$ voor $i = 2, 3$. Er geldt $p_5 \mid N(p_5) = 5$ en dus volgt $(p_5) = (5, p_5)$. Berekenen van het quotiënt $5/p_5$ geeft de identiteit $p_5 p_{25} = 5$. Dus p_{25} deelt 5 en er volgt $(p_{25}) = (5, p_{25})$. Merk op dat $(p_5) = (5, p_{25})$ en $(p_{25}) = (5, p_{25})$ maximale idealen zijn uit 4.11. Tot slot wordt 7 gedeeld door $p_{7,i}$ voor $i = 1, 2, 3$ en dus is $(p_{7,1})$ gelijk aan het ideaal $(7, p_{7,1})$, welke maximaal is met 4.11. Er geldt $7 \in (p_{7,2}), (p_{7,3})$ en uit voorgaande is duidelijk dat $2 + \sqrt[3]{6}$ en $-3 + \sqrt[3]{6}$ deelbaar zijn door p_2 respectievelijk p_3. Berekenen van de quotiënten $(2 + \sqrt[3]{6})/p_2$ en $(-3 + \sqrt[3]{6})/p_3$ geeft $2 + \sqrt[3]{6} = p_2 p_{7,2}$ en $-3 + \sqrt[3]{6} = -p_3 p_{7,3}$. Dus geldt $(7, 2 + \sqrt[3]{6}) = (p_{7,2})$ en $(7, -3 + \sqrt[3]{6}) = (p_{7,3})$, waarbij de inclusie $\subset$ volgt uit voorgaande en de inclusie $\supset$ uit het feit dat $p_{7,2}$ en $p_{7,3}$ geen eenheden zijn uit 4.6 en $(7, 2 + \sqrt[3]{6}), (7, -3 + \sqrt[3]{6})$ maximale idealen zijn uit 4.11. Met 4.13 is duidelijk dat de idealen $(2), (3), (5)$ en (7) eenduidig ontbinden in een product van maximale hoofdidealen als

$$2 = (p_2)^3, \quad 3 = (p_3)^3, \quad 5 = (p_5)(p_{25}), \quad 7 = (p_{7,1})(p_{7,2})(p_{7,3}).$$

Met methodes uit de algebraïsche getaltheorie weten we nu voldoende om te concluderen:

4.14 Lemma. *Het domein $\mathbb{Z}[\sqrt[3]{6}]$ is een hoofdideaaldomein en een ontbindingsring, oftewel een element $x \in \mathbb{Z}[\sqrt[3]{6}]$ met $x \neq 0$ kunnen we op volgorde en vermenigvuldiging met eenheden na eenduidig schrijven als een product*

$$x = u p_1 \dots p_t$$

met $u \in \mathbb{Z}[\sqrt[3]{6}]^*$ en $p_i \in \mathbb{Z}[\sqrt[3]{6}]$ irreducibel.

Bewijs (schets)**.** Men laat met methodes uit de algebraïsche getaltheorie zien dat $\mathbb{Z}[\sqrt[3]{6}]$ klassengetal 1 heeft. Hierbij maken we gebruik van de Minkowskigrens, welke in ons geval gelijk is aan

$$\frac{4n!}{\pi n^n} \sqrt{|\mathrm{disc}(\mathbb{Q}[\sqrt[3]{6}])|} = \frac{16\sqrt{3}}{\pi} \approx 8.82.$$

We moeten dus nog de priemidealen boven de idealen $(2), (3), (5), (7)$ bekijken. Aangezien deze idealen hoofdidealen blijken te zijn uit bovenstaande tekst, geeft dit dat $\mathbb{Z}[\sqrt[3]{6}]$ een hoofdideaaldomein is. Zie het voorbeeld uit paragraaf 7 van hoofdstuk 10 uit [CA] voor het volledige bewijs. □

Aangezien $\mathbb{Z}[\sqrt[3]{6}]$ een hoofdideaaldomein is, zijn de priemelementen precies de irreducibele elementen in $\mathbb{Z}[\sqrt[3]{6}]$. We zullen de beide termen door elkaar gebruiken. Uit voorgaande trekken we de conclusie:

4.15 Lemma. *De elementen*

$$p_2 = 2 - \sqrt[3]{6}, \quad p_3 = 3 + 2\sqrt[3]{6} + \sqrt[3]{36}, \quad p_5 = -1 + \sqrt[3]{6} \quad \text{en} \quad p_{25} = 1 + \sqrt[3]{6} + \sqrt[3]{36}$$

zijn priem in $\mathbb{Z}[\sqrt[3]{6}]$. De eenduidige ontbinding van $\sqrt[3]{6}, 2, 3, 5 \in \mathbb{Z}[\sqrt[3]{6}]$ in irreducibele factoren wordt gegeven door:

$$2 = p_2^3 u_2, \quad 3 = p_3^3 u_3, \quad 5 = p_5 p_{25}, \quad \sqrt[3]{6} = p_2 p_3$$

waarbij $u_2 = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$ en $u_3 = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{6}$ eenheden zijn in $\mathbb{Z}[\sqrt[3]{6}]$. □

4.4 Het lokaal-globaalprincipe gaat voor de kubische vorm $3X^3+4Y^3+5Z^3$ niet op

4.16 Stelling. *Nul wordt niet gerepresenteerd door de kubische vorm* $f = 3X^3 + 4Y^3 + 5Z^3 \in \mathbb{Q}[X, Y, Z]$.

Bewijs. Stel er bestaat een oplossing $w = (x, y, z) \in \mathbb{Q}^3 \setminus \{0\}$ zodanig dat $f(w) = 0$. Er geldt $(x, y, z) \neq 0$. Dus er zijn hoogstens 2 coördinaten van w gelijk aan 0. Als er 2 coördinaten van w nul zijn, geeft dit geen oplossing. Als er 1 coördinaat van w gelijk is aan 0, merken we op dat $3/4, 3/5$ of $4/5$ derde machten zijn in $\mathbb{Q}$. Echter de polynomen $4X^3 - 3, 5X^3 - 3$ en $5X^3 - 4$ zijn Eisenstein bij 3 respectievelijk 2 en dus bevinden de derde machtswortels van $3/4, 3/5$ en $4/5$ zich niet in $\mathbb{Q}$. We vinden dus dat alle coördinaten van w ongelijk zijn aan 0.

Voor $a \in \mathbb{Q}^*$ volgt dat aw ook een niet-triviaal nulpunt is. Door a groot genoeg te nemen, kunnen we dus aannemen $w \in \mathbb{Z}^3 \setminus \{0\}$. Stel dat 2 coördinaten van w een gemeenschappelijke priemfactor p hebben, dan volgt uit $3x^3+4y^3+5z^3 = 0$ en het feit dat $3, 4$ en 5 geen derde machten in hun priemontbinding bevatten dat de derde coördinaat van w ook deelbaar is door p. Aangezien $\text{ggd}(x, y, z)^{-1}w$ ook een oplossing is, kunnen we aannemen dat x, y en z paarsgewijs copriem zijn. Er volgt dat $3x^3, 4y^3$ en $5z^3$ tevens paarsgewijs copriem zijn. Als er immers een priemdeler p bestaat van twee van de termen, volgt uit de vergelijking dat de derde term ook deelbaar is door p. Dit is echter in tegenspraak met het feit dat $3, 4, 5$ respectievelijk x, y, z paarsgewijs copriem zijn. We kunnen dus aannemen dat x, z oneven zijn, y, z niet deelbaar door 3 en x, y niet deelbaar door 5. Vermenigvuldigen met 2 geeft dat (x, y, z) voldoet aan de vergelijking

$$8y^3 + 6x^3 = -10z^3. \tag{3}$$

We bekijken de vergelijking in $\mathbb{Z}[\sqrt[3]{6}]$:

$$(2y + x\sqrt[3]{6})(4y^2 - 2xy\sqrt[3]{6} + x^2\sqrt[3]{36}) = -10z^3.$$

We gaan $a = 2y+x\sqrt[3]{6}$ en $b = 4y^2-2xy\sqrt[3]{6}+x^2\sqrt[3]{36}$ factoriseren. Hierbij maken we gebruik van lemma 4.15 en de notatie uit het lemma. Er geldt $p_2 \mid a, b$ en we gaan laten zien $p_2 = \text{ggd}(a, b)$. Merk hierbij op dat de grootste gemene deler gedefinieerd is op eenheden na, aangezien $\mathbb{Z}[\sqrt[3]{6}]$ een ontbindingsring is uit 4.14. Stel dat $p \in \mathbb{Z}[\sqrt[3]{6}]$ een gemeenschappelijke irreducibele factor van a en b is, dan geldt

$$p \mid b + (4y - x\sqrt[3]{6})a = 12y^2 \quad \text{en} \quad p \mid b - (2y - 2x\sqrt[3]{6})a = 3x^2\sqrt[3]{36}.$$

Uit 4.15 volgt $12y^2 = y^2u_2^2u_3p_2^6p_3^3$ en $3x^2\sqrt[3]{36} = x^2u_3p_2^2p_3^5$. Stel $p \neq p_2, p_3$, dan volgt $p \mid x$ en $p \mid y$. Er geldt $N(p) \mid N(x) = x^3$ en $N(p) \mid N(y) = y^3$ met $N(p) \neq 1$ uit 4.6. Maar dit is niet mogelijk, omdat x en y onderling ondeelbaar zijn. Dus is p gelijk aan p_2 of p_3. Stel nu dat het laatste waar is. Aangezien geldt $p_3 \mid \sqrt[3]{6}$, volgt $p_3 \mid a - x\sqrt[3]{6} = 2y$ en daarmee ook $3 = N(p_3) \mid N(2y) = 8y^3$ uit de multiplicatieve eigenschap van de norm. Echter y was niet deelbaar door 3. Dus dit duidt op een tegenspraak en er geldt $p = p_2$. We weten nu dat $\text{ggd}(a, b)$ een macht van p_2 is op eenheden na. Stel $p_2^2 \mid a$ dan volgt $4 = N(p_2^2) \mid N(a) = 8y^3 + 6x^3 = -10z^2$. Dit is in tegenspraak met het feit dat z oneven is, dus is $\text{ggd}(a, b)$ gelijk aan p_2 op eenheden na.

Met 4.15 ontbinden we $ab = -10z^3 = -u_2p_2^3p_5p_{25}z^3$ in $\mathbb{Z}[\sqrt[3]{6}]$. Bekijken we vergelijking (3) modulo 5 vinden we $(2y)^3 \equiv (-x)^3 \bmod 5$. Dit geeft $2y \equiv -x \bmod 5$ als we aan beide kanten een derde macht nemen. Immers voor $g \in \mathbb{F}_5^*$ geldt $(g^3)^3 = g^9 = g$. Dus 5 deelt $2y + x$ en er volgt $p_5 \mid xp_5 + 2y + x = a$. Stel nu dat a tevens wordt gedeeld door p_{25}, dan volgt $5 = p_5p_{25} \mid a = 2y + x\sqrt[3]{6}$. Echter $(2y)/5$ is geen element van $\mathbb{Z}$, omdat y niet deelbaar is door 5. We vinden meteen $a/5 \notin \mathbb{Z}[\sqrt[3]{6}]$, omdat $1, \sqrt[3]{6}$ en $\sqrt[3]{36}$ een basis van gehelen van $\mathbb{Z}[\sqrt[3]{6}]$ is uit het bewijs van 4.11. Dus p_{25} deelt a niet. Eerder zagen we al $p_2^2 \nmid a$ en $p_2 = \text{ggd}(a, b)$. De ontbinding van a en b wordt daarmee gegeven door:

$$a = u_ap_2p_5\alpha, \quad b = u_bp_2^2p_{25}\beta$$

met $\alpha\beta = z^3$ en u_a, u_b eenheden. Aangezien geldt $\text{ggd}(a, b) = p_2$, zijn α en β copriem. Eenheden van α en β kunnen we in u_a en u_b meenemen. Dus volgt dat α en β derde machten zijn. We concluderen:

$$2y + x\sqrt[3]{6} = \upsilon(2 - \sqrt[3]{6})(-1 + \sqrt[3]{6})\gamma^3$$

waarbij v een eenheid is die op derde machten na vastligt en γ het element in $\mathbb{Z}[\sqrt[3]{6}]$ is met $\gamma^3 = \alpha$. Uit 4.12 weten we dat $\mathbb{Z}[\sqrt[3]{6}]^*$ isomorf is met $\langle \pm u \rangle$ voor een $u \in \mathbb{Z}[\sqrt[3]{6}]$. Daar $(-1)^3 = -1$ volgt nu $\mathbb{Z}[\sqrt[3]{6}]^{*3} = \langle \pm u^3 \rangle$ en daarmee is $\mathbb{Z}[\sqrt[3]{6}]^*/\mathbb{Z}[\sqrt[3]{6}]^{*3}$ de cyclisch groep van orde 3. Aanschouw nu de afbeelding $\psi : \mathbb{Z}[\sqrt[3]{6}] \to \mathbb{F}_7$ gegeven door $a + b\sqrt[3]{6} + c\sqrt[3]{36} \to a + c - b \bmod 7$. Men gaat eenvoudig na dat ψ een ringhomomorfisme is door op te merken dat men door uitdelen naar het maximale ideaal $(p_{7,1}) = \ker \psi$ het lichaam $\mathbb{F}_7$ verkrijgt. Er geldt $\psi(u_3) = 3$. De derde machten modulo 7 zijn 0,1 en 6. Er volgt dat u_3 geen derde macht kan zijn in $\mathbb{Z}[\sqrt[3]{6}]$. Dus is de representant van u_3 een voortbrenger van de groep $\mathbb{Z}[\sqrt[3]{6}]^*/\mathbb{Z}[\sqrt[3]{6}]^{*3}$. We kunnen dus $v = u_3^j$ nemen met $j = 0, 1, 2$. Merk op dat uit $\sqrt[3]{6} = p_2 p_3$ volgt $u_2 u_3 p_2^3 p_3^3 = 6 = (\sqrt[3]{6})^3 = p_2^3 p_3^3$. Dus is u_2 de inverse van u_3. Vermenigvuldigen we de verkregen vergelijking uit de ontbinding van $2y + x\sqrt[3]{6}$ aan beide kanten met $2^j = u_2^j p_2^{3j}$, geeft dit:

$$2^j(2y + x\sqrt[3]{6}) = (2 - \sqrt[3]{6})(-1 + \sqrt[3]{6})(p_2^j\gamma)^3.$$

Schrijf nu $p_2^j\gamma = u + v\sqrt[3]{6} + w\sqrt[3]{36}$ voor $(u, v, w) \in \mathbb{Z}^3$. We stellen de coëfficiënten van $\sqrt[3]{36}$ aan beide kanten aan elkaar gelijk, er volgt

$$0 = u^3 + 6v^3 + 36w^3 + 36uvw - 3(3u^2v + 18uw^2 + 18v^2w) + 2(3uv^2 + 3u^2w + 18vw^2).$$

We beschouwen (u, v, w) in $\mathbb{Z}_3^3$. Zij $v_3(u) = \eta_u, v_3(v) = \eta_v$ en $v_3(w) = \eta_w$. Stel $\eta_u \leq \eta_v, \eta_w$, dan volgt uit de vergelijking $u^3 \equiv 0 \bmod 3^{3\eta_u+1}$, maar dan geldt $3\eta_u = v_3(u^3) \geq 3\eta_u + 1$. Stel $\eta_v < \eta_u$ en $\eta_v \leq \eta_w$, dan geldt met het oog op bovenstaande vergelijking $6v^3 \equiv 0 \bmod 3^{3\eta_v+2}$, maar dan volgt $3\eta_v + 1 = v_3(6v^3) \geq 3\eta_v + 2$. Stel $\eta_w < \eta_u, \eta_w$, dan zien we $36w^3 \equiv 0 \bmod 3^{3\eta_w+3}$, maar dan volgt $3\eta_w + 2 = v_3(36w^3) \geq 3\eta_w + 3$. De enige mogelijkheid is dat geldt $\eta_u, \eta_v, \eta_w = \infty$, dit betekent $(u, v, w) = 0$. Echter dan volgt $2^j(2y + x\sqrt[3]{6}) = (2 - \sqrt[3]{6})(-1 + \sqrt[3]{6})(u + v\sqrt[3]{6} + w\sqrt[3]{36})^3 = 0$ en daarmee $x, y = 0$, maar x, y, z waren ongelijk aan 0. We hebben dus een tegenspraak en de kubische vorm $3X^3 + 4Y^3 + 5Z^3 \in \mathbb{Q}[X, Y, Z]$ representeert nul niet. □

4.17 Stelling. *De kubische vorm $f_v = 3X^3 + 4Y^3 + 5Z^3$ representeert 0 in $\mathbb{Q}_v$ voor alle $v \in V$.*

Bewijs. We beschouwen eerst de gevallen $\mathbb{Q}_3, \mathbb{Q}_5$ en $\mathbb{Q}_\infty$ apart. In $\mathbb{Q}_\infty$ is $(\sqrt[3]{5}, -\sqrt[3]{5}, 1)$ een niet-triviaal nulpunt van f_∞. Beschouw het polynoom $g = 5X^3 + 4 \in \mathbb{Z}_3[X]$. We vinden $g(4) = 324 \equiv 0 \bmod 81$ en $v_3(g'(4)) = v_3(240) = 1$. Met 2.7 $(n = 4, k = 1)$ volgt nu dat er een $z \in \mathbb{Z}_3$ bestaat met $5z^3 = -4$. Het is duidelijk dat $(0, 1, z)$ een niet-triviaal nulpunt van f_3 is. Beschouw het polynoom $g_5 = 4X^3 + 3 \in \mathbb{Z}_5[X]$. We vinden $g_5(2) = 35 \equiv 0 \bmod 5$ en $v_5(g_5'(2)) = v_5(48) = 0$. Met 2.7 $(n = 1, k = 0)$ volgt nu dat er een $y \in \mathbb{Z}_5$ bestaat met $4y^3 = -3$. Het is duidelijk dat $(1, y, 0)$ een niet-triviaal nulpunt van f_5 is.

Laat nu p priem met $p \neq 3, 5$ en beschouw $f_p \in \mathbb{Z}_p[X, Y, Z]$. Stel er bestaat een $u \in \mathbb{Z}_p^3 \setminus \{0\}$ zodanig dat $f_p(u) \equiv 0 \bmod p$ en $v_p(\frac{\partial f_p}{\partial X}(u)) = 0$, dan volgt uit 2.7 $(n = 1, k = 0)$ dat er een nulpunt $v \in \mathbb{Z}_p^3$ van f_p bestaat met $v_i \equiv u_i \bmod p$ voor $i = 1, 2, 3$. Er geldt dus $v \neq 0$ en de vorm f_p representeert 0 in $\mathbb{Q}_p$. We zijn dus klaar als we zo'n $u \in \mathbb{Z}_p^3 \setminus \{0\}$ kunnen vinden.

Laat β een voortbrenger van $\mathbb{F}_p^*$. Omdat $p \neq 3, 5$ zijn 3 en 5 eenheden in $\mathbb{F}_p$. Schrijf $3 = \beta^i$ en $5 = \beta^j$, dan geldt $15 = \beta^{i+j} \in \mathbb{F}_p^*$. Stel nu dat $3, 5, 15 \notin \mathbb{F}_p^{*3}$, dan volgt $i, j, i + j \not\equiv 0 \bmod 3$. Afgaan van de mogelijkheden geeft $i \equiv j \bmod 3$ en dus is $2i+j$ deelbaar door 3. We vinden dat $\beta^{2i+j} = 45 \in \mathbb{F}_p^*$ dan een derde macht is. Dus is $3, 5, 15$ of 45 een derde macht in $\mathbb{F}_p^*$.

Stel er bestaat een element $v \in \mathbb{F}_p^*$ met $v^3 = 3$. Laat $u \in \mathbb{Z}_p^*$ zodanig dat geldt $\varepsilon(u) = v$. Er volgt $f_p(u, -1, -1) \equiv 0 \bmod p$ en $v_p(\frac{\partial f_p}{\partial X}(u, -1, -1)) = v_p(3u^2) = 0$, aangezien geldt $p \neq 3$ en $u \in \mathbb{Z}_p^*$. Stel er bestaat een element $v \in \mathbb{F}_p^*$ met $v^3 = 5$. Neem $u \in \mathbb{Z}_p^*$ met $\varepsilon(u) = v$. We krijgen $f_p(u, -u, 1) \equiv 0 \bmod p$ en $v_p(\frac{\partial f_p}{\partial X}(u, -u, 1)) = v_p(3u^2) = 0$. Stel $v \in \mathbb{F}_p^*$ met $v^3 = 15$. Laat $u \in \mathbb{Z}_p^*$ zodanig dat geldt $\varepsilon(u) = v$. Er geldt $f_p(3u, 5, -7) \equiv 0 \bmod p$ en $v_p(\frac{\partial f_p}{\partial X}(3u, 5, -7)) = v_p(3^3u^2) = 0$. Stel tot slot dat er een element $v \in \mathbb{F}_p^*$ bestaat met $v^3 = 45$. Kies $u \in \mathbb{Z}_p^*$ met $\varepsilon(u) = v$. Er geldt $f_p(u, 0, -3) \equiv 0 \bmod p$ en $v_p(\frac{\partial f_p}{\partial X}(u, 0, -3)) = v_p(3u^2) = 0$. We kunnen dus voor elke priem $p \neq 3, 5$ een dergelijke $u \in \mathbb{Z}_p^* \setminus \{0\}$ vinden. Samengevoegd met bovenstaande concluderen we dat f_v nul representeert voor alle $v \in V$. □

5 Referenties

[CA] J.W.S. Cassels, *Local Fields*, Cambridge University Press, 1983

[CH] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993

[IR] K.F. Ireland & M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990

[KA] G. Karpilovsky, *Classical Foundations and Multiplicative Groups: Vol. 120: Field Theory*, Taylor & Francis, 1988

[RO] A. Robert, *A course in p-adic analysis*, Springer, 2000

[SE] J.P. Serre, *A Course in Arithmetic*, Springer, 1973

[SH] P. Stevenhagen, *Algebra 1*, dictaat eerstejaarsvak wiskunde Universiteit Leiden, 2007

[VO] S.M. Voronin, *Encyclopaedia of Mathematics: Diophantine Equations*, Springer, 1988, http://eom.springer.de/d/d032610.htm