KATHOLIEKE UNIVERSITEIT
LEUVEN

FACULTEIT WETENSCHAPPEN
Departement Wiskunde
Afdeling Algebra

Hilberts Tiende Probleem en aanverwante kwesties

door

Frank FEYS

Promotor: prof. dr. J. Denef

Proefschrift ingediend tot het
behalen van de graad van
Master in de wiskunde

Academiejaar 2010-2011

Dankwoord

Mijn bijzondere dank gaat uit naar professor Denef voor zijn raad tijdens het tot stand komen van deze thesis. Niet alleen vestigde hij mijn aandacht op het werk van Poonen en Königsmann, maar ik kon ook steeds op zijn hulp rekenen indien ik ergens vast zat. Het enthousiasme waarmee professor Denef over wiskunde praat werkte voor mij in elk geval aanstekelijk. Met interesse en vooral veel plezier heb ik aan deze scriptie gewerkt.

Eveneens veel dank aan mijn lezers professor Cluckers en dr. Delvaux.

Tot slot wil ik ook aan mijn medestudenten een woord van dank richten voor hun soms waardevolle input.

Frank Feys

Leuven, 10 juni 2011

Inhoudsopgave

Deel I

Voorbereidend werk

HOOFDSTUK 1

INLEIDING

In deze thesis zullen we verschillende problemen beschouwen die voortkomen uit de studie van Hilberts Tiende Probleem. Op het Internationaal Wiskundecongres van 1900 te Parijs stelde de Duitse wiskundige David Hilbert (1862-1943) een lijst van drieëntwintig wiskundige problemen voor waarvan hij vond dat ze behoorden tot de belangrijkste op te lossen problemen voor de twintigste eeuw. Hilbert daagde de gehele wiskundige gemeenschap uit om ze voor het jaar 2000 allemaal op te lossen. Er zijn tot nog toe elf problemen volledig opgelost.

1.1 Het originele probleem

Het Tiende Probleem van Hilbert werd door Hilbert in letterlijke bewoordingen als volgt geformuleerd.

10. ENTSCHEIDUNG DER LÖSBARKEIT EINER DIOPHANTISCHEN GLEICHUNG. *Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Dit wil zeggen: Hilberts Tiende Probleem vraagt om een algoritme dat, indien een willekeurige polynoom $f \in \mathbb{Z}[x_1, \ldots, x_n]$ als input ingevoerd wordt, als output JA of NEE geeft al naargelang er al dan niet $a_1, \ldots, a_n \in \mathbb{Z}$ bestaan zodat $f(a_1, \ldots, a_n) = 0$.

Hilbert spreekt hier van een *eindig aantal operaties*. Tegenwoordig zou men hiervoor het woord *algoritme* gebruiken. Echter, ten tijde van Hilbert was er nog helemaal geen wiskundige notie van algoritme; deze werd pas in de jaren dertig van de negentiende eeuw wiskundig geformaliseerd door onder andere Alan Turing (1912-1954), Alonzo Church (1903-1995) en Kurt Gödel (1906-1978). Verschillende theoretische modellen voor een computer werden in deze periode in een wiskundig kader gegoten. De *Turingmachine* is hiervan allicht de bekendste. Men heeft kunnen aantonen dat deze verschillende modellen in feite equivalent zijn; immers, de *Hypothese van Church* stelt dat elke mechanische procedure op een Turing machine geïmplementeerd kan worden. In feite mogen we het begrip algoritme dus als synoniem zien voor Turingmachine. We zullen in deze thesis als input voor een Turingmachine meestal met natuurlijke getallen werken. Maar door voor wiskundige objecten op voorhand een codering in natuurlijke getallen af te spreken, kunnen Turingmachines veel algemenere objecten als input nemen. Bijvoorbeeld, een polynoom $\sum_{i=0}^{n} a_i x^i \in \mathbb{N}[x]$ kunnen we coderen als $\prod_{i=1} p_i^{a_i}$ met p_i het i-de priemgetal.

In 1970 bewees de Russische wiskundige Yuri Matiyasevich (1947) de onoplosbaarheid van Hilberts Tiende Probleem. Met andere woorden het is niet mogelijk een algoritme te construeren dat aan de gegeven voorwaarden voldoet. In feite werd er zelfs heel wat meer bewezen, en was de negatieve oplossing van Hilberts Tiende Probleem slechts een nogal triviale implicatie van een veel sterkere stelling, de zogenaamde *Davis-Putnam-Robinson-Matiyasevich stelling*. Meestal wordt echter de afkorting DPRM-stelling gebruikt. Matiyasevich steunde in zijn bewijs op eerder werk van Martin Davis (1928), Hilary Putnam (1926) en Julia Robinson (1919-1985), vandaar de naam. In feite is de DPRM-stelling het hart van de onoplosbaarheid van Hilberts Tiende Probleem over $\mathbb{Z}$. We tonen ze aan in Deel 2.

1.2 Gerelateerde problemen

Hoewel Hilberts Tiende Probleem als dusdanig al lange tijd opgelost is, heeft dit probleem in de loop van jaren aanleiding gegeven tot andere interessante problemen.

1.2.1 Veralgemening van Hilberts Tiende Probleem

Men kan in plaats van de ring van gehele getallen te nemen, een analoog probleem formuleren voor een andere ring. Zij R een ring. De formulering luidt dan: geef, indien mogelijk, een algoritme dat bij input van een willekeurige polynoom $f \in R[x_1,\ldots,x_n]$, als output JA of NEE geeft al naargelang f al dan niet een oplossing heeft in R^n.

Omdat er in feite naar een Turingmachine gevraagd wordt moeten we, technisch gezien, een codering vastleggen voor de elementen van R. Dit is echter niet altijd mogelijk, bijvoorbeeld indien R niet aftelbaar is. Om dit probleem te omzeilen zullen we in dat soort gevallen de polynomen die we als input toelaten beperken tot degene met coëfficiënten in een aftelbare deelring $S \subset R$, in plaats van polynomen in $R[x_1,\ldots,x_n]$ zelf. In het geval dat $R = \mathbb{R}$ kunnen we bijvoorbeeld $S = \mathbb{Q}$ nemen, of $S = \mathbb{Z}$; dit zijn equivalente problemen. De vraag is dan of er een Turing machine bestaat zodanig dat, gegeven als input een polynoom $f \in \mathbb{Q}[x_1,\ldots,x_n]$, de machine als output JA of NEE geeft al naargelang er al dan niet een oplossing $(a_1,\ldots,a_n) \in \mathbb{R}^n$ bestaat met $f(a_1,\ldots,a_n) = 0$. Of Hilberts Tiende Probleem oplosbaar is of niet hangt in het algemeen af van de ring R en de deelring $S \subset R$ die we vastgelegd hebben. We noemen dit Hilberts Tiende Probleem *over R met coëfficiënten in S*. Tenzij anders vermeld zullen we steeds $S = \mathbb{Z}$ veronderstellen. We noemen dit Hilberts Tiende Probleem *over R*. Eigenlijk zullen we het in deze thesis enkel hebben over Hilberts Tiende Probleem over $\mathbb{Z}$ en Hilberts Tiende Probleem over $\mathbb{N}$. Merk op dat $\mathbb{N}$ natuurlijk geen ring is, zodat bovenstaande constructie niet opgaat, maar we zullen zien dat we dit probleem toch kunnen beschouwen.

We beschouwen nu een aantal concrete ringen, en vermelden of Hilberts Tiende Probleem over deze ring al dan niet oplosbaar is.

- $R = \mathbb{C}$ oplosbaar

- $R = \mathbb{R}$ oplosbaar
- $R = \mathbb{F}_q$ oplosbaar
- $R = p$-adisch veld oplosbaar
- $R = \mathbb{F}_q((t))$ **niet geweten**
- $R =$ getallenveld **niet geweten**
- $R = \mathbb{Q}$ **niet geweten**
- $R =$ globaal functieveld onoplosbaar
- $R = \mathbb{F}_q(t)$ onoplosbaar
- $R = \mathbb{C}(t)$ **niet geweten**
- $R = \mathbb{C}(t_1, t_2)$ onoplosbaar
- $R = \mathbb{R}(t)$ onoplosbaar
- $R = \mathscr{O}_K$ met K een veld **niet geweten**
- $R = \mathscr{O}_K$ met K een getallenveld onoplosbaar
- $R = K$ met K een totaal reëel veld onoplosbaar

Merk op dat de gevallen $R = \mathbb{C}$ en $R = \mathbb{F}_q$ triviaal zijn; immers, het veld van de complexe getallen $\mathbb{C}$ is algebraïsch gesloten, zodat er steeds een oplossing bestaat. En $\mathbb{F}_q$ is een eindig veld zodat we simpelweg alle mogelijkheden achtereenvolgens kunnen nagaan.

1.2.2 Eerste-orde theorieën

In volgend hoofdstuk voeren we eerste-orde talen in. In het bijzonder zullen we de *taal van ringen*, genoteerd als $\mathscr{L}_r$, definiëren. Het idee is dan dat we zinnen en formules uit deze taal kunnen interpreteren in een particuliere ring R. De taal $\mathscr{L}_r$ zullen we doorheen de thesis intensief gebruiken.

Ten eerste vermelden we dat, nu we deze terminologie voor handen hebben, we voor veel ringen een equivalente formulering van de onoplosbaarheid van Hilberts Tiende Probleem over een ring R kunnen geven; dikwijls betekent dit immers niets anders dan dat *de positieve existentiële eerste-orde theorie van R in de taal van ringen $\mathscr{L}_r$ onbeslisbaar is*. In volgend hoofdstuk definiëren we wat we hiermee precies bedoelen en zullen we deze bewering aantonen.

Ten tweede, nu we onze horizon hebben verruimd door deze equivalente interpretatie van Hilberts Tiende Probleem in termen van de taal der ringen te geven, ligt de volgende analoge vraag voor de hand. Namelijk, is de verzameling van *alle* zinnen van

$\mathscr{L}_r$ die waar zijn indien we ze in R interpreteren, de zogenaamde *eerste-orde theorie van R in de taal van ringen $\mathscr{L}_r$*, al dan niet beslisbaar? In dit verband herinneren we de onbelisbaarheid van $\mathbb{N}$: er bestaat geen algoritme om na te gaan of een zin van $\mathscr{L}_r$ al dan niet waar is in $\mathbb{N}$. Hiervoor verwijzen we bijvoorbeeld naar [8]. In deze thesis echter ligt de focus anders en zullen we ons verder niet met de beslisbaarheid van eerste-orde theorieën bezighouden.

Hilberts Tiende Probleem heeft dus als het ware een hele nieuwe waaier van problemen geïnduceerd; inderdaad, voor elke ring R kan men zich nu ook vragen of de eerste-orde theorie van R beslisbaar is of niet. We merken hierbij nog op dat de beslisbaarheid van de theorie van R de oplosbaarheid van Hilberts Tiende Probleem op triviale wijze impliceert.

1.2.3 Definieerbaarheid

Een ander substantieel deel van de thesis, dat gerelateerd is aan Hilberts Tiende Probleem, gaat over *definieerbaarheid*, een begrip dat we later formeel invoeren. Meer specifiek gaan we het hebben over de *definieerbaarheid van $\mathbb{Z}$ in $\mathbb{Q}$*. Informeel gezegd: kunnen we "spreken" over de gehele getallen in de (taal der) rationale getallen? Dit probleem blijkt een affirmatief antwoord te hebben: Robinson vond reeds vijftig jaar geleden zulk een definitie.

Echter, kunnen we beter doen dan Robinson? Robinsons resultaat geeft namelijk aanleiding naar de vraag tot verscherping; met andere woorden, kan men $\mathbb{Z}$ in $\mathbb{Q}$ definiëren op een meer eenvoudige manier, dat wil zeggen met een kleiner aantal veranderingen van kwantoren? Meer specifiek kan men zich afvragen of dit gaat met behulp van diophantische formules of, iets algemener, met existentiële formules. In dat geval spreken we van *existentiële definieerbaarheid*.

Indien $\mathbb{Z}$ existentieel definieerbaar in $\mathbb{Q}$ zou zijn, dan volgt uit de onoplosbaarheid van Hilberts Tiende Probleem over $\mathbb{Z}$, de onoplosbaarheid van Hilberts Tiende Probleem over $\mathbb{Q}$. Dit is eenvoudig in te zien. Nu is het echter zo dat er een aantal wiskundige standaardconjecturen bestaan die impliceren dat $\mathbb{Z}$ *niet* existentieel definieerbaar is $\mathbb{Q}$. De bekendst zulke conjectuur is die van Barry Mazur (1937), die handelt over de topologie van een variëteit over de rationale getallen.

1.3 Overzicht van de thesis

De thesis bestaat essentieel uit drie delen.

- In Deel 1 leggen we de grondvesten van de thesis: we voeren alle belangrijke begrippen in die doorheen de thesis een essentiële rol spelen. Het concept van definieerbaarheid wordt ingevoerd. Ook gaan we onder andere wat dieper in op de notie van Turingmachine en leggen we de link met recursietheorie. Het gaat hier essentieel over de vraag wat berekenbaarheid is.

- Deel 2 gaat over het eerste stuk van de titel van deze thesis: Hilberts Tiende Probleem over $\mathbb{Z}$. Om de onoplosbaarheid hiervan aan te tonen hebben we heel wat basis nodig, die voor een stuk al in Deel 1 gelegd werd. Het doel van dit deel van de thesis is om de DPRM-stelling aan te tonen; daaruit is de onoplosbaarheid van Hilberts Tiende Probleem makkelijk af te leiden, zoals zal blijken.

- Deel 3 gaat over een aanverwante kwestie, namelijk over de definieerbaarheid van $\mathbb{Z}$ in $\mathbb{Q}$. We werken een artikel van Poonen (1968) uit waarin een elegantere definitie dan die van Robinson wordt gegeven. Daarna bekijken we ook nog een recent artikel van Königsmann. De tot nu toe mooiste definitie van $\mathbb{Z}$ in $\mathbb{Q}$ wordt hierin gegeven. We zullen echter maar een stuk van dit artikel uitwerken. De essentie van beide definities ligt in het samenspel van de theorie van quaternionenalgebra's samen met kwadratische vormen, en het Hasse-Minkowski principe.

HOOFDSTUK 2

LOGICA

In dit hoofdstuk zullen we Hilberts Tiende Probleem en aanverwante problemen in een formeel wiskundig kader gieten. We definiëren de meest essentiële begrippen die we verderop in de thesis steeds opnieuw nodig zullen hebben.

2.1 Eerste-orde talen

We definiëren eerst wat we bedoelen met een eerste-orde taal.

Definitie 2.1

> Een *eerste-orde taal*, of kortweg *taal*, $\mathscr{L}$ bestaat uit eindige verzamelingen van respectievelijk constantesymbolen, functiesymbolen en relatiesymbolen. (Met een *symbool* bedoelen we een string van lengte één over het ASCII-alfabet.) Een *term* in $\mathscr{L}$ wordt recursief gedefinieerd als een constantesymbool of een variabele $(x, y, z, \ldots)$, of als een functiesymbool toegepast op een term. Een *formule* in $\mathscr{L}$ is een relatiesymbool toegepast op termen van $\mathscr{L}$, een uitdrukking zoals $t_1 = t_2$ waarbij t_1 en t_2 termen in $\mathscr{L}$ zijn, en recursief ook iets van de vorm $(A \vee B), (A \wedge B), (A \to B), (A \leftrightarrow B), \neg A, (\exists x)A$ of $(\forall x)A$, waarbij A en B formules in $\mathscr{L}$ zijn en x eender welke variabele is.

Een formule van een taal is dus per definitie een eindige string van symbolen over een alfabet die voldoet aan bovenstaande regels; dit alfabet wordt impliciet gegeven door de verzamelingen van constantesymbolen, functiesymbolen en relatiesymbolen. In deze thesis zullen we, zoals eerder al opgemerkt werd, vooral werken met één specifieke taal, die we hieronder invoeren.

Definitie 2.2

> Neem als verzamelingen van constantesymbolen, functiesymbolen en relatiesymbolen respectievelijk $\{0,1\}$, $\{+,\cdot\}$ en $\emptyset$. De op deze manier bekomen taal noemen we de *taal van ringen*, genoteerd als $\mathscr{L}_r$. We noteren kortweg ook wel $\mathscr{L}_r = \{0,1,+,\cdot\}$.

Voorbeelden van formules in deze taal zijn

$$(\forall x)(x = 0 \vee x \cdot x = 1)$$
$$(x = z) \wedge (1 = z)$$
$$(\exists y)\, y + 1 + 1 = 0.$$

De string $(\exists y)\, y+2=0$ behoort strikt genomen niet tot $\mathscr{L}_r$. Maar we spreken vanaf nu af dat we zulk een uitdrukking als afkorting voor $(\exists y)\, y+1+1=0$ zien. Deze misbruik van notatie laat ons bijvoorbeeld ook toe te zeggen dat de string $y^2-4x=3$ tot onze taal behoort; inderdaad, hier staat in feite de string $y\cdot y=1+1+1+x+x+x+x$, dewelke duidelijk tot $\mathscr{L}_r$ behoort.

Merk op dat in het eerste voorbeeld hierboven de variabele x in zijn dubbele voorkomen in de formule in het *bereik* zit van de kwantor $(\forall x)$. Inderdaad, herinner dat het *bereik* van een kwantor $(\exists x)$ (of $(\forall x)$), met x een variabele, de kleinste deelformule van een gegeven formule is die zelf een formule is. In het tweede voorbeeld van hierboven is dat niet het geval: zowel x als z op beide plaatsen komen niet voor in een kwantor of in het bereik daarvan, we noemen ze daarom *vrij*.

Definitie 2.3

> Een *zin* van een taal $\mathscr{L}$ is een formule van $\mathscr{L}$ zonder vrije variabelen.

Zo zijn in de gegeven voorbeelden hierboven zowel de eerste als de derde zinnen van $\mathscr{L}_r$, maar de tweede dus niet. Ook is bijvoorbeeld $(\forall x)\,(\exists y)\, x^2-4y=3$ een zin, daar hier inderdaad, ter afkorting, eigenlijk staat $(\forall x)\,(\exists y)\, x\cdot x=1+1+1+y+y+y+y$, hetgeen duidelijk een formule van $\mathscr{L}_r$ is zonder vrije variabelen. We zullen in het vervolg ten behoeve van een makkelijke notatie vaak de $\cdot$ niet schrijven, indien het duidelijk is wat we bedoelen.

We spitsen ons nu even toe op de taal der ringen $\mathscr{L}_r$.

Definitie 2.4

> Een *positief existentiële formule* in de taal $\mathscr{L}_r$ is een formule in die taal van de vorm
>
> $$(\exists x_1)(\exists x_2)\ldots(\exists x_n)\, S$$
>
> waarbij S een formule van $\mathscr{L}_r$ is waarin geen kwantoren, geen negaties en geen implicaties of equivalenties voorkomen, en met $x_1,\ldots,x_n$ variabelen. Ook het geval $n=0$ is toelaten: we bedoelen daar dan mee dat er *geen* existentiële kwantoren voor de formule S staan.

Voor een positief existentiële formule zijn de enige toegelaten logische operatoren in de constructie van de formule S dus $\vee$ en $\wedge$. De formules

$$(\exists x)(\exists y)(\exists z)(x^2=y\vee y^2=z\vee z^2=x)$$
$$(\exists x)\, x^2=y+1$$
$$(\exists x)(\exists y)\, x^3+x^2y=1$$

zijn voorbeelden van positief existentiële formules in $\mathscr{L}_r$. Op informele wijze zouden we dus kunnen zeggen dat de formule S uit de definitie opgebouwd is door herhaaldelijke conjuncties en disjuncties van gelijkheden tussen veeltermvergelijkingen.

Merk op dat de formules in het eerste en het derde voorbeeld zelfs zinnen zijn; we spreken in dat geval dan ook van positief existentiële *zinnen*.

Definitie 2.5

> Een *diophantische formule* in de taal $\mathscr{L}_r$ is een positief existentiële formule in de taal $\mathscr{L}_r$ waarvoor bovendien geldt dat de formule S uit vorige definitie bekomen werd zonder logische operatoren te gebruiken.

Dat wil zeggen, de formule S uit bovenstaande definitie is van de vorm $t_1 = t_2$, met t_1 en t_2 termen. Typische voorbeelden van voorgaande definitie zijn

$$(\exists x)(\exists y)\, 3x^2y + xy - 3 = 0$$
$$(\exists x)\, x^2 + xz + z^2 = 1.$$

Meer informeel kunnen we dus zeggen dat een diophantische formule in de taal $\mathscr{L}_r$ een uitdrukking is van de vorm $(\exists \vec{x})\, P(\vec{x},\vec{y}) = 0$, waarbij $P(\vec{x},\vec{y}) \in \mathbb{Z}[\vec{x},\vec{y}]$ een veelterm over de gehele getallen is en $\vec{x} = (x_1,\ldots,x_n)$ en $\vec{y} = (y_1,\ldots,y_m)$ een aantal variabelen zijn. Vaak is het notationeel handiger deze informele schrijfwijze te gebruiken. Merk op dat $n = 0$ toegelaten is; er zijn dan geen existentiële kwantoren. Zie Definitie 2.4.

Duidelijk is de formule in het eerste voorbeeld zelfs een zin in de taal der ringen is; in dat geval spreken we van een diophantische *zin*.

Tot hier toe zijn we enkel bezig geweest met het invoeren van formele talen. We kunnen echter formules en zinnen van een taal gaan *interpreteren in een structuur $\mathscr{D}$ met overeenkomstige signatuur*. Essentieel betekent dit dat we een niet-lege verzameling D hebben, *het universum* van $\mathscr{D}$ genaamd, tesamen met een eindig aantal particuliere elementen van D, *constanten* genaamd, een eindig aantal afbeeldingen $F_j : D^{i_j} \to D$ en tot slot een eindig aantal relaties R_i op D, waarvoor bovendien het volgende geldt: met elk relatiesymbool van de taal $\mathscr{L}$ moet er precies één relatie D_i van $\mathscr{D}$ overeenkomen; analoog moet er met ieder functiesymbool van $\mathscr{L}$ precies één functie F_j overeenkomen die ook nog hetzelfde aantal argumenten heeft; tenslotte moeten er in de structuur precies evenveel constanten zitten als we in de taal hadden.

Beschouw opnieuw een taal $\mathscr{L}$ en een structuur $\mathscr{D}$ met overeenkomstige signatuur.

- Zij A een zin van $\mathscr{L}$. We kunnen A dan *interpreteren* in D door elk relatiesymbool, functiesymbool en constantesymbool te interpreteren door respectievelijk zijn uniek geassocieerde relatie, functie en constante in de structuur $\mathscr{D}$; bovendien interpreteren we $=$ door de gelijkheidsrelatie, en de connectieven $\vee, \wedge, \to, \leftrightarrow, \neg$ door 'en', 'of', 'implicatie', 'asa', 'niet' respectievelijk, en $(\exists x)$ door 'er bestaat een x in het universum D zodanig dat' en $(\forall x)$ door 'voor alle x in het universum D geldt'. Op deze wijze bekomen we een bewering aangaande de structuur $\mathscr{D}$ die ofwel waar is, we zeggen dan dat A waar is in $\mathscr{D}$ en noteren dit als $\mathscr{D} \models A$, ofwel vals is.

- Zij $\phi(x_1,\ldots,x_n)$ een formule van $\mathscr{L}$ met vrije variabelen $x_1,\ldots,x_n$. Merk dan op dat we slechts de waarheidswaarde van deze formule kunnen beschouwen *nadat* we de vrije variabelen vervangen door concrete elementen $a_1,\ldots,a_n \in D$.

We zullen hier echter geen nauwkeurige definitie van bovenstaande intuïtief duidelijke begrippen geven, en verwijzen voor de exacte definitie en een bovendien meer gedetailleerde uiteenzetting naar [8].

2.2 Eerste-orde- en positief existentiële theorieën

Beschouw opnieuw de taal van ringen $\mathscr{L}_r$. We gaan ons nu toespitsen op het geval dat de door ons beschouwde structuur een ring is. Zij daarom R een ring. We nemen dus aan dat R commutatief is en een eenheidselement 1 heeft. We construeren dan een structuur $\mathscr{D}_R$ met dezelfde signatuur als $\mathscr{L}_r$ als volgt.

- Neem als niet-lege verzameling $D = R$.
- Definieer geen enkele relatie op R.
- Neem als functies $F_1 = +$ en $F_2 = \cdot$, dat wil zeggen

$$+ : R^2 \to R : (x,y) \mapsto x+y$$
$$\cdot : R^2 \to R : (x,y) \mapsto x \cdot y.$$

- Neem twee particuliere elementen uit R, namelijk 0 en 1.

Merk op dat $\mathscr{D}_R$ wel degelijk precies dezelfde signatuur heeft als $\mathscr{L}_r$. Zoals in vorige paragraaf werd uitgelegd, kunnen we zinnen van $\mathscr{L}_r$ dan interpreteren in de structuur $\mathscr{D}_R$. Alzo krijgt iedere zin een waarheidswaarde, dat wil zeggen, kan waar of onwaar zijn in die structuur. In plaats van te zeggen dat een zin van de taal der ringen waar is in $\mathscr{D}_R$, zullen we ter afkorting ook wel zeggen dat de zin waar is *in* R.

Definitie 2.6

> De *eerste-orde theorie* van een ring R in de taal der ringen $\mathscr{L}_r$ is de verzameling van alle eerste-orde zinnen die waar zijn in $\mathscr{D}_R$.

Bijvoorbeeld behoren de zinnen

$$(\forall x)((\exists y)\, x = 2y \vee (\exists y)\, x = 2y+1)$$
$$(\forall x)(\forall y)\, xy = yx$$
$$(0 = 1 \to (\forall x)\, x = 0)$$

tot de eerste-orde theorie van de ring $\mathbb{Z}$. De tweede zin is per definitie zelfs waar in eender welke ring. Ook de laatste zin is steeds waar, hetgeen een triviaal gevolg is van de ringaxioma's.

We doen nu het analogon voor positief existentiële zinnen in $\mathscr{L}_r$.

Definitie 2.7

De *positief existentiële theorie* van een ring R in de taal der ringen $\mathscr{L}_r$ is de verzameling van alle positief existentiële zinnen die waar zijn in $\mathscr{D}_R$.

Merk op dat de positief existentiële theorie van een ring een deelverzameling is van de eerste-orde theorie van diezelfde ring. Een paar triviale voorbeelden van elementen van de positief existentiële theorie van $\mathbb{Z}$ zijn

$$(\exists x)\, x = 0$$
$$(\exists x)(\exists y)\, 3x^2 + y = 1.$$

We voeren nu het concept van *beslisbaarheid* in, voor zowel de eerste-orde theorie als de positief existentiële theorie.

Definitie 2.8

We noemen de eerste-orde theorie van een ring R in de taal der ringen $\mathscr{L}_r$ *beslisbaar* indien er een Turingmachine bestaat die als input een eerste-orde zin neemt en beslist of die zin al dan niet tot de theorie behoort.

Definitie 2.9

We noemen de positief existentiële theorie van een ring R in de taal der ringen $\mathscr{L}_r$ *beslisbaar* indien er een Turingmachine bestaat die als input een positief existentiële zin neemt en beslist of die zin al dan niet tot de positief existentiële theorie behoort.

Opmerking. In bovenstaande definities komt het concept van een Turingmachine ter sprake, en ook verder in deze sectie zal er voortdurend gebruik van gemaakt worden. We verwijzen hiervoor naar sectie 3.1, waar we dit begrip formeel invoeren.

2.3 Definieerbaarheid: positief existentiële en diophantische verzamelingen

We expanderen nu het idee uit de vorige sectie maar beschouwen nu formules uit de taal $\mathscr{L}_r$ die *geen* zinnen zijn; dat wil zeggen dat ze nog een aantal vrije variabelen bevatten. Zij $\phi(x_1,\ldots,x_n)$ een formule in $\mathscr{L}_r$ met vrije variabelen $x_1,\ldots,x_n$. We kunnen dan de elementen $(a_1,\ldots,a_n) \in R^n$ beschouwen waarvoor geldt dat $\phi(a_1,\ldots,a_n)$ waar is in $\mathscr{D}_R$. Dit geeft aanleiding tot een deelverzameling van R^n.

Definitie 2.10

Zij R een ring. Een deelverzameling $A \subset R^n$ noemen we *definieerbaar in R* indien

$$A = \{(a_1,\ldots,a_n) \in R^n \mid \phi(a_1,\ldots,a_n) \text{ is waar in } \mathscr{D}_R\}$$

voor een zekere formule $\phi(x_1,\ldots,x_n)$ in $\mathscr{L}_r$ met vrije variabelen $x_1,\ldots,x_n$.

Verderop in de thesis, meer bepaald in Deel 3, zullen we het over de definieerbaarheid van $\mathbb{Z}$ in $\mathbb{Q}$ hebben.

Definitie 2.11

Zij R een ring. Een deelverzameling $A \subset R^n$ noemen we *positief existentieel in R* indien

$$A = \{(a_1,\ldots,a_n) \in R^n \mid \phi(a_1,\ldots,a_n) \text{ is waar in } \mathscr{D}_R\}$$

voor een zekere positief existentiële formule $\phi(x_1,\ldots,x_n)$ in $\mathscr{L}_r$ met vrije variabelen $x_1,\ldots,x_n$.

Definitie 2.12

Zij R een ring. Een deelverzameling $A \subset R^n$ noemen we *diophantisch in R* indien

$$A = \{(a_1,\ldots,a_n) \in R^n \mid \phi(a_1,\ldots,a_n) \text{ is waar in } \mathscr{D}_R\}$$

voor een zekere diophantische formule $\phi(x_1,\ldots,x_n)$ in $\mathscr{L}_r$ met vrije variabelen $x_1,\ldots,x_n$.

Met betrekking tot vorige twee definities spreken we ook wel over *positief existentiële definieerbaarheid in R* en *diophantische definieerbaarheid in R*, respectievelijk.

Zoals uitgelegd na Definitie 2.5 kunnen we op informele wijze zeggen dat

$$A = \{(a_1,\ldots,a_n) \in R^n \mid (\exists \vec{x})\, P(a_1,\ldots,a_n,\vec{x}) = 0\}$$

voor een zekere gehele veelterm P. We noemen dit een *diophantische representatie van de diophantische verzameling A aan de hand van de veelterm P*. Merk op dat zulk een representatie aan de hand van een veelterm hoegenaamd niet uniek is; inderdaad, veronderstel dat $P(a_1,\ldots,a_n,\vec{x})$ een diophantische representatie van een zekere diophantische verzameling is, dan is de veelterm $-P(a_1,\ldots,a_n,\vec{x})$ dit ook. Een iets minder triviaal voorbeeld is het volgende. Beschouw de verzameling $A := \{a \in \mathbb{Z} \mid a \text{ is even}\}$. Duidelijk is A diophantisch, daar

$$A = \{a \in \mathbb{Z} \mid (\exists x)\, a - 2x = 0\}.$$

Bijgevolg is de gehele veelterm $P_1(a,x) := a - 2x$ een diophantische representatie van A. Echter, omdat in de gehele getallen kwadraten strikt positief zijn, hebben we ook dat

$$A = \{a \in \mathbb{Z} \mid (\exists x_1)(\exists x_2)\, 2x_1^2 x_2 - a x_1^2 + 2x_2 - a = 0\}.$$

Dus is de gehele veelterm $P_2(a,x_1,x_2) := 2x_1^2 x_2 - a x_1^2 + 2x_2 - a$ eveneens een diophantische representatie van A.

Daar een relatie met n argumenten op R niets anders is dan een deelverzameling van R^n is, kunnen we in het algemeen ook zeggen dat een relatie op R *diophantisch in* R is. En dus kunnen we ook zeggen dat een functie diophantisch in R is. In het geval dat $R = \mathbb{Z}$ zeggen we dikwijls kortweg dat een verzameling $A \subset \mathbb{Z}^n$ *diophantisch* is. Merk op dat, hoewel $\mathbb{N}$ geen ring is, niets in de constructie ons verbiedt om $R = \mathbb{N}$ te nemen. Meer nog, in Deel 2, waarin we de onoplosbaarheid van Hilberts Tiende Probleem over $\mathbb{Z}$ aantonen, zal $R = \mathbb{N}$ *steeds* verondersteld zijn.

Voorbeelden.

- De verzameling van kwadraten in $\mathbb{Z}$ is diophantisch in $\mathbb{Z}$, want

$$a \text{ is een kwadraat} \Leftrightarrow (\exists x)\, x^2 - a = 0 \text{ is waar in } \mathbb{Z}.$$

- De verzameling van natuurlijke getallen $\mathbb{N} \subset \mathbb{Z}$ is diophantisch in $\mathbb{Z}$; inderdaad, de Vier-kwadratenstelling van Lagrange zegt precies dat

$$a \in \mathbb{N} \Leftrightarrow (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)\, x_1^2 + x_2^2 + x_3^2 + x_4^2 - a = 0 \text{ is waar in } \mathbb{Z}.$$

  In sectie 4.1 tonen we deze stelling in detail aan.

- De natuurlijke orderelatie $\geq$ op $\mathbb{N}^2$ is diophantisch in $\mathbb{N}$, want

$$a \geq b \Leftrightarrow (\exists x)\, a - b = x \text{ is waar in } \mathbb{N}.$$

- De verzameling van samengestelde getallen is diophantisch in $\mathbb{N}$, want

$$a \in \mathbb{N} \text{ is samengesteld} \Leftrightarrow (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)$$

$$0 = (x_1 x_2 - a)^2 + (x_1 - 2 - x_3)^2 + (x_2 - 2 - x_4)^2 \text{ is waar in } \mathbb{N}.$$

- De verzameling van positieve samengestelde getallen is diophantisch in $\mathbb{Z}$, want

$$a \text{ is samengesteld} \Leftrightarrow$$

$$(\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(\exists x_5)(\exists x_6)(\exists x_7)(\exists x_8)(\exists x_9)(\exists x_{10})$$

$$0 = (x_1 x_2 - a)^2$$

$$+(x_3^2 + x_4^2 + x_5^2 + x_6^2 - (x_1 - 2))^2 + (x_7^2 + x_8^2 + x_9^2 + x_{10}^2 - (x_2 - 2))^2 \text{ is waar in } \mathbb{Z}.$$

- Eindige unies en doorsnedes van diophantische verzamelingen in $\mathbb{Z}$ zijn opnieuw diophantisch in $\mathbb{Z}$. Merk op dat hetzelfde resultaat voor $\mathbb{N}$ geldt. Dit is heel makkelijk zo in te zien, maar we tonen dit verderop aan in Propositie 4.6. Merk op dat sommige van de vorige voorbeelden dit resultaat reeds illustreren. Bovendien is, in dezelfde setting, een Cartesisch product van diophantische verzamelingen opnieuw diophantisch.

Tot slot een aantal belangrijke opmerkingen.

Opmerking.

- We hebben de hele theorie tot nu toe consequent opgebouwd voor een arbitraire ring R. Niets weerhoudt ons echter om niet enkel ringen te beschouwen maar om ook bijvoorbeeld $R = \mathbb{N}$ te nemen. Inderdaad gaat de hele constructie ook in dit geval helemaal op.
- Voor sommige ringen is het noodzakelijk dat we de taal $\mathscr{L}_r = \{0, 1, +, \cdot\}$ uitbreiden met één of meer constantesymbolen, die verwijzen naar particuliere elementen van de ring die we beschouwen. Bijvoorbeeld als $R = \mathbb{Z}[i]$ dan zullen we dikwijls genoodzaakt zijn aan de taal der ringen een symbool toe te voegen dat naar $i \in R$ verwijst, om over dit element te kunnen spreken. We zullen zulk een taal benoemen met *uitgebreide taal der ringen*. Merk op dat we de structuur $\mathscr{D}_R$ dan uiteraard ook moeten aanpassen. Ook alle definities eerder in dit hoofdstuk gegeven moeten dan op voor de hand liggende wijze veralgemeend worden. In het geval dat we een ring beschouwen waarbij deze procedure nodig is, bijvoorbeeld in de stellingen in sectie 2.4 verderop, zullen we dit expliciet vermelden. Indien $R = \mathbb{R}(t)$ dan is het bijvoorbeeld vaak handig een extra symbool T in te voeren dat naar t verwijst. In dat geval kunnen we de evidente notatie $\mathscr{L}_r \cup \{T\}$ gebruiken, waarbij nog steeds $\mathscr{L}_r = \{0, 1, +, \cdot\}$.

2.4 Formulering Hilberts Tiende Probleem

We hebben volgende proposities.

Propositie 2.13

> *Zij R een ring waarvoor geldt dat er polynomen $f(x,y), g(x,y) \in R[x,y]$ bestaan zodat we voor alle $a, b \in R$ hebben dat*
>
> $$f(a,b) = 0 \Longleftrightarrow a = 0 \text{ en } b = 0$$
>
> $$g(a,b) = 0 \Longleftrightarrow a = 0 \text{ of } b = 0.$$
>
> *Veronderstel dat we $\mathscr{L}_r$ uitbreiden met een voldoende aantal constantesymbolen zodat de coëfficiënten van f en g kunnen uitgedrukt worden in deze nieuw bekomen taal. Dan is de collectie van positief existentiële verzamelingen in R, in deze nieuw bekomen taal, gelijk aan de collectie van diophantische verzamelingen in R.*

Bewijs. Daar per definitie een diophantische formule in het bijzonder een positief existentiële formule is, is het voldoende aan te tonen dat elke positief existentiële verzameling ook diophantisch is. Beschouw dus een positief existentiële verzameling A. Dan bestaat er een positief existentiële formule $\phi(x_1, \ldots, x_n)$ in $\mathscr{L}_r$ met vrije variabelen $x_1, \ldots, x_n$ zodat

$$A = \{(a_1, \ldots, a_n) \in R^n \mid \phi(a_1, \ldots, a_n) \text{ is waar in } \mathscr{D}_R\}.$$

We hebben dus dat $\phi(x_1,\ldots,x_n)$ gelijk is aan

$$(\exists x_1)(\exists x_2)\ldots(\exists x_n)\,S$$

waarbij S een formule van $\mathscr{L}_r$ is die is opgebouwd uit conjuncties en disjuncties van gelijkheden tussen veeltermvergelijkingen (zie Definitie 2.4). We voeren nu volgende constructie uit.

- Transformeer om te beginnen elke veeltermvergelijking $p = q$ uit de constructie van S naar $p - q = 0$.
- Transformeer dan elke conjunctie $(p = 0) \wedge (q = 0)$ naar $f(p,q) = 0$.
- Transformeer tot slot elke disjunctie $(p = 0) \vee (q = 0)$ naar $g(p,q) = 0$.

Op deze wijze hebben we elk gebruik van een logische operator uit de constructie van S weggewerkt. We bekomen aldus een diophantische formule $\phi'(x_1,\ldots,x_n)$ in $\mathscr{L}_r$, met vrije variabelen $x_1,\ldots,x_n$, zodat

$$A = \{(a_1,\ldots,a_n) \in R^n \mid \phi'(a_1,\ldots,a_n) \text{ is waar in } \mathscr{D}_R\}.$$

Merk op dat deze gelijkheid volgt door het gegeven te gebruiken. Dus in het bijzonder is A diophantisch. Dit beëindigt het bewijs van Propositie 2.13. ■

Opmerking.

- Het aantal aan $\mathscr{L}_r$ toe te voegen symbolen in Propositie 2.13 zal meestal eindig, en zelfs bijna altijd slechts één of hooguit twee, zijn.
- Aangaande de formulering van vorige stelling spreekt het voor zich dat we het aantal toe te voegen symbolen aan $\mathscr{L}_r$ tot een minimum beperken; dat wil zeggen we voegen *genoeg* symbolen toe, maar zeker niet meer dan nodig.

Uit voorgaande propositie halen we volgend resultaat.

Propositie 2.14

> *Zij R een integriteitsdomein waarvoor geldt dat het breukenveld K van R niet algebraïsch gesloten is. Indien er een voldoende aantal constantesymbolen aan $\mathscr{L}_r$ toegevoegd worden, dan is in deze nieuw bekomen taal de collectie van positief existentiële verzamelingen in R gelijk aan de collectie van diophantische verzamelingen in R.*

Bewijs. Neem $g(x,y) = xy$. Dan voldoet $g(x,y) \in R[x,y]$ aan Propositie 2.13 daar R een integriteitsdomein is. Omdat K niet algebraïsch gesloten is, kunnen we een niettriviale eindige uitbreiding K' van K nemen. Zij dan $\{e_1,e_2\}$ deel van een basis van K' over K. Men kan door een berekening aantonen dat $N_{K'/K}(xe_1 + ye_2) \in K[x,y]$. Door een geschikte $r \in R \setminus \{0\}$ te kiezen kunnen we de noemers van deze veelterm wegwerken, en bekomen zo een veelterm

$$f(x,y) := rN_{K'/K}(xe_1 + ye_2) \in R[x,y].$$

Uit een eigenschap van de norm, en het feit dat $\{e_1, e_2\}$ een vrij deel over K is, volgt nu dat voor alle $a, b \in R$ geldt dat $f(a,b) = 0$ als en slechts als $a = 0$ en $b = 0$. Uit Propositie 2.13 volgt dus het gevraagde, op voorwaarde dat $\mathscr{L}_r$ uitbreid wordt met een voldoende aantal constantesymbolen zodat de coëfficiënten van f kunnen uitgedrukt worden in deze nieuw bekomen taal. Dit beëindigt het bewijs van Propositie 2.14.

■

Definitie 2.15

> Zij R een integriteitsdomein waarvoor geldt dat het breukenveld K van R niet algebraïsch gesloten is. Aan de hand van Propositie 2.14 kiezen we naar eigen keuze een minimaal aantal aan $\mathscr{L}_r$ toe te voegen symbolen waarvoor de uitspraak geldt, welke we met $\mathscr{T}_R$ noteren. We noteren met $\mathscr{S}_R$ de verzameling van alle elementen van R waarvoor geldt dat er een toegevoegd symbool aan $\mathscr{L}_r$ is dat naar dit specifieke element van de ring verwijst.

Merk op dat $\mathscr{S}_R$ onafhankelijk is van de keuze van toegevoegde symbolen $\mathscr{T}_R$.

We geven een aantal voorbeelden om de concepten die we tot hier toe ingevoerd hebben te illustreren.

Voorbeelden.

- Neem $R = \mathbb{Z}$. Dit is het originele geval van Hilberts Tiende Probleem, zoals Hilbert zelf het probleem ingevoerd heeft. Het breukenveld $\mathbb{Q}$ is inderdaad niet algebraïsch gesloten. Uit het bewijs van Propositie 2.14 is het duidelijk dat er geen symbolen aan $\mathscr{L}_r$ toegevoegd dienen te worden. Dus $\mathscr{T}_R = \emptyset$ en $\mathscr{S}_R = \emptyset$.

- Neem $R = \mathbb{R}[t]$. We passen het bewijs van Propositie 2.14 toe om in te zien welke symbolen we eventueel toe moeten voegen aan $\mathscr{L}_r$. Het breukenveld is gelijk aan $\mathbb{R}(t)$. Beschouw dan de kwadratische uitbreiding $\mathbb{R}(t)(\sqrt{t})$ van $\mathbb{R}(t)$. Neem $\{1, \sqrt{t}\}$ als basis van de vectorruimte $\mathbb{R}(t)(\sqrt{t})$ over $\mathbb{R}(t)$. Een eenvoudige berekening levert dat, ten opzichte van de gekozen basis $\{1, \sqrt{t}\}$, de matrix van lineaire transformatie van de afbeelding

  $$m_{x+y\sqrt{t}} : \mathbb{R}(t)(\sqrt{t}) \to \mathbb{R}(t)(\sqrt{t}) : v \mapsto (x + y\sqrt{t})\, v$$

  gelijk is aan

  $$\begin{pmatrix} x & ty \\ y & x \end{pmatrix}.$$

  Door de determinant van deze matrix te nemen volgt hier onmiddellijk uit dat

  $$N_{\mathbb{R}(t)(\sqrt{t})/\mathbb{R}(t)}(x + y\sqrt{t}) = x^2 - ty^2 \in \mathbb{R}[t][x,y].$$

  We concluderen dus dat het voldoende is om één extra symbool aan $\mathscr{L}_r$ toe te voegen, namelijk een symbool verwijzend naar de variabele t, zeg T. Dan is $\mathscr{T}_R = \{T\}$ en $\mathscr{S}_R = \{t\}$. We beschouwen dan de uitgebreide taal der ringen $\mathscr{L}_r \cup \{T\}$. Deze taal gebruikende mogen we dan besluiten dat de collectie

van positief existentiële verzamelingen in $\mathbb{R}[t]$ gelijk is aan de collectie van diophantische verzamelingen in $\mathbb{R}[t]$.

- Neem $R = S[t]$ met S eender welk integriteitsdomein. Een directe veralgemening van het vorige argument leidt tot dezelfde conclusie.
- Neem $R = S(t)$ met S eender welk integriteitsdomein. Een analoge conclusie volgt wederom.

We concluderen deze sectie met de exacte formulering van Hilberts Tiende Probleem. Eerst wordt de definitie gegeven met gehele veeltermen als input, daarna meer algemeen de definitie waarbij de coëfficiënten van de veeltermen waarden aannemen in een aftelbare deelring van de oorspronkelijke ring.

Definitie 2.16

> Zij R een ring. *Hilberts Tiende Probleem over R* is de vraag naar het bestaan van een Turingmachine die als input een veelterm $f \in \mathbb{Z}[x_1, \ldots, x_n]$ in een willekeurig aantal variabelen n neemt, en als output JA of NEE geeft al naargelang er al dan niet $a_1, \ldots, a_n \in R$ bestaan met $f(a_1, \ldots, a_n) = 0$.

Definitie 2.17

> Zij R een ring en $S \subset R$ een aftelbare deelverzameling. *Hilberts Tiende Probleem over R met coëfficiënten in S* is de vraag naar het bestaan van een Turingmachine die als input een veelterm $f \in S[x_1, \ldots, x_n]$ in een willekeurig aantal variabelen n neemt, en als output JA of NEE geeft al naargelang er al dan niet $a_1, \ldots, a_n \in R$ bestaan met $f(a_1, \ldots, a_n) = 0$.

We benadrukken dat er in deze laatste definitie dan wel een codering van de elementen van S gespecificeerd dient te zijn. Daarom dat de ring S noodzakelijkerwijs aftelbaar verondersteld werd in de definitie. Merk nog op dat er een uniek homomorfisme $\mathbb{Z} \to R$ is, voor eender welke ring R, zodat we de gehele getallen op natuurlijke wijze in eender welke ring kunnen zien. Meestal zullen we bij Hilberts Tiende Probleem over een ring de coëfficiënten van de veeltermen geheel laten zijn; in deze thesis zelfs *altijd*.

Volgend evident resultaat legt de link tussen Hilberts Tiende Probleem en de door ons opgebouwde theorie omtrent de taal der ringen.

Propositie 2.18

> *Zij R een integriteitsdomein waarvoor geldt dat het breukenveld K van R niet algebraïsch gesloten is, en zij S de deelring van R voortgebracht door $\mathscr{S}_R$. Dan is Hilberts Tiende Probleem over R met coëfficiënten in S equivalent met de beslisbaarheid van de positief existentiële theorie van R in de uitgebreide taal der ringen $\mathscr{L}_r \cup \mathscr{T}_R$.*

Bewijs. Dit volgt uit de tot nu toe opgebouwde theorie en Propositie 2.14. Dit beëindigt het bewijs van Propositie 2.18. ■

HOOFDSTUK 3

TURINGFORMALISME EN RECURSIETHEORIE

Uit de tot nu toe opgebouwde theorie blijkt dat het concept van een Turingmachine, als het door ons gekozen model van berekening, centraal staat: begrippen zoals berekenbaarheid, beslisbaarheid enzovoort maken er steevast gebruik van. In de eerste sectie voeren we het begrip formeel in.

In de tweede sectie voeren we het begrip van *recursieve functie* in. Dit is een andere, maar equivalente, manier om berekenbaarheid te zien, en dat zal blijken uit de derde sectie.

Tot slot brengen we een aantal definities in herinnering. Een *partiële functie* $A \to B$ is een functie $A' \to B$ voor een zekere $A' \subset A$; bovendien noemen we, dezelfde notaties gebruikend, een partiële functie $A \to B$ *totaal* indien $A' = A$. Dat wil zeggen dit is een functie in de gewoonlijke betekenis, met domein A en codomein B. Indien $f, g : A \to B$ twee partiële functies zijn, dan bedoelen we met $f \simeq g$ dat voor alle $x \in A$ geldt dat $f(x)$ gedefinieerd is als en slechts als $g(x)$ gedefinieerd is en dat in zulk geval ook $f(x) = g(x)$. Met het *domein* van een partiële functie bedoelen we natuurlijk het domein van de onderliggende functie.

Indien A een verzameling is dan bedoelen we met A^* de verzameling van *strings* over het alfabet A, dat wil zeggen alle eindige rijen van elementen van A.

3.1 Turingformalisme

Intuïtief kan een Turingmachine gezien worden als een magneetband die verdeeld is in allemaal kleine cellen die naast mekaar staan. De magneetband is oneindig lang naar de rechtse kant, maar is begrensd aan de linkerkant, en het meest linkse symbool is blanco; zie verderop in Definitie 3.1. Elk zo'n cel kan een symbool uit een bepaald alfabet bevatten, en er is een kop die de cellen kan scannen en overschrijven. Een Turingmachine heeft een eindig aantal mogelijke toestanden, en de machine bevindt zich op elk ogenblik in één van haar toestanden. Een instructie voor de machine is een voorschrift voor de machine om van toestand te veranderen, het huidig symbool te overschrijven met een nieuw symbool en de kop naar links of naar rechts te bewegen, of te blijven staan. Welke instructie uitgevoerd wordt hangt louter en alleen af van de huidige toestand van de machine en het huidige symbool. Eens gestart, blijft de machine instructies uitvoeren tot zij in een toestand komt waarbij er voor het huidig gelezen symbool geen instructie meer voorhanden is. Op dat moment kan

men controleren of de machine al dan niet in een aanvaardbare toestand gestopt is.

3.1.1 Elementaire definities omtrent Turingmachines

Dit alles gieten we in een formeel kader als volgt.

Definitie 3.1

We noemen een zestal $M = (Q, \Sigma, T, P, q_0, F)$ waarbij

- Q een eindige verzameling is van *toestanden*,
- $F \subset Q$ de verzameling is van *aanvaardbare eindtoestanden*,
- $q_0 \in Q$ is de *begintoestand* is,
- Σ een eindige verzameling van *symbolen* is, met een speciaal symbool $\# \in \Sigma$, genaamd het *lege symbool*,
- $T \subset \Sigma \setminus \{\#\}$ de verzameling van *inputsymbolen* is (de verzameling van *strings* over dit inputalfabet T noteren we met T^*),
- $P : (Q \setminus F) \times \Sigma \to Q \times \Sigma \times \{L, R, 0\}$ een partiële functie is genaamd het *programma* of *instructieset*,

een *Turingmachine*.

Wanneer men de machine start is er een inputstring gegeven, dat wil zeggen een element in T^*, en bevindt de machine zich in de begintoestand q_0. Zoals gezegd is het meest linkse element op de magneetband steeds het blanco symbool # met daarnaast de symbolen van de inputstring in volgorde; de rest van de magneetband bestaat louter uit blanco symbolen. De leeskop staat in het begin boven het meest linkse, niet-lege symbool van de magneetband. De machine voert dan het programma P uit, en dit moet als volgt geïnterpreteerd worden. Noem q de toestand waarin de Turingmachine zich *op een bepaald moment*, dat wil zeggen na een zeker aantal stappen, bevindt en zij $\sigma \in \Sigma$ het symbool dat op precies datzelfde moment door de kop gelezen wordt; zulk een koppel (q, σ) wordt ook wel een *situatie* van de Turingmachine, bij input van een zekere gegeven inputstring, genoemd. Nu zijn er twee mogelijkheden:

1. Het koppel (q, σ) behoort tot het definitiegebied van de partiële functie P. Dit betekent dat $P(q, \sigma)$ bestaat en gelijk is aan een drietal $(q', \sigma', X) \in Q \times \Sigma \times \{L, R, 0\}$. Het effect van de uitvoering van deze instructie is dat de Turingmachine haar toestand zal veranderen in een zekere toestand q', dat het huidig gescande symbool σ vervangen wordt door een zeker symbool σ' en dat de kop zich beweegt zoals X aangeeft; dat wil zeggen, indien $X = L$ beweegt de kop zich naar links, indien $X = R$ beweegt de kop naar rechts en indien tenslotte $X = 0$ blijft de kop ter plaatse.
2. Het koppel (q, σ) behoort niet tot het definitiegebied van de partiële functie P.

Definitie 3.2

Zij een Turingmachine M, een inputstring $s \in T^*$ en een bijbehorende situatie (q, σ) gegeven.

- Indien het koppel (q, σ) niet behoort tot het definitiegebied van de partiële functie P, dan zeggen we dat de Turingmachine *M stopt in de situatie* (q, σ) *bij inputstring s*. De toestand q wordt de *eindtoestand* van M, voor die bepaalde invoer s, genoemd.
- De Turingmachine *M stopt* bij gegeven inputstring s indien er een situatie van M bij die inputstring s bestaat waarin M stopt. Indien dit niet zo is zeggen we ook wel dat *M nooit stopt* of ook wel *in een oneindige lus geraakt*, bij inputstring s. De Turingmachine *M stopt altijd* indien M stopt bij iedere gegeven inputstring.
- De inputstring *s wordt aanvaard* indien er een situatie bij inputstring s bestaat, met aanvaardbare eindtoestand, waarin M stopt. In dat geval noemen we de eindige string symbolen op de magneetband, dus zonder het oneindig lange uiteinde van blanco symbolen, de *output* van de Turingmachine.
- De inputstring *s wordt verworpen* indien er een situatie bij inputstring s bestaat, met niet-aanvaardbare eindtoestand, waarin M stopt.

Uit vorige definitie volgt meteen dat er, bij input van een inputstring in een Turingmachine, precies drie mogelijkheden zijn: ofwel raakt de machine in een oneidige lus, ofwel stopt de machine en in dat geval wordt de string ofwel verworpen, indien de eindtoestand niet-aanvaardbaar is, ofwel aanvaard, indien de eindtoestand aanvaardbaar is, en enkel en alleen in dit laatste geval hebben we output; dat is dan de eindige string van symbolen die op dat laatste moment op de magneetband staat.

3.1.2 Turing recursief opsombaarheid en -berekenbaarheid van een verzameling

Definitie 3.3

Zij T een eindige verzameling. Een deelverzameling $S \subset T^*$ is*Turing recursief opsombaar* of *Turing semi-beslisbaar* indien er een Turingmachine bestaat met verzameling van inputsymbolen gelijk aan T, zodat een string $s \in T^*$ door de Turingmachine aanvaard wordt als en slechts als $s \in S$.

Het is duidelijk van waar de naam recursief opsombaar komt. Zij namelijk $S \subset T^*$ Turing recursief opsombaar. De verzameling T^* is aftelbaar dus er bestaat een aftelling $A_1, A_2, A_3, \ldots$ van T^*. We maken nu een nieuwe Turingmachine, als volgt: laat de Turingmachine uit Definitie 3.3 n stappen rekenen op de inputstrings $A_1, A_2, \ldots, A_n$, achtereenvolgens voor $n = 1, 2, 3, \ldots$; zodra een string A_i aanvaard wordt, voegen we

het toe aan de lijst van reeds aanvaarde woorden. Merk op dat hier in feite gebruik wordt gemaakt van een *for-lus*. Men kan aantonen dat deze actie inderdaad een nieuwe Turingmachine creëert, of alternatief kunnen we ook gewoon de Hypothese van Church toepassen. Merk op dat deze procedure oneindig lang duurt. Het is echter zo dat we *uiteindelijk* de volledige lijst van elementen van S krijgen; immers, indien $A_i \in S$ dan en slechts dan zal, voor het aantal stappen n groot genoeg, de initiële Turingmachine A_i aanvaarden, id est stoppen in een aanvaardbare eindtoestand. We kunnen de elementen van S dus opsommen.

Definitie 3.4

> Zij T een eindige verzameling. Een deelverzameling $S \subset T^*$ is *Turing berekenbaar*, *Turing recursief* of *Turing beslisbaar* indien er een Turingmachine bestaat met verzameling van inputsymbolen gelijk aan T, die bij elke gegeven inputstring uiteindelijk stopt en die enkel en alleen S aanvaardt, dat wil zeggen enkel en alleen elementen van S worden aanvaard.

Het is uit de definities onmiddellijk duidelijk dat elke Turing berekenbare verzameling ook Turing recursief opsombaar is. Het omgekeerde is echter niet waar: het zogenaamde *stopprobleem* is hiervan een voorbeeld. Verderop komen we hier nog op terug. Wij zullen echter een variant van het stoprobleem beschouwen.

We willen ons nu toespitsen op de verzameling $\mathbb{N}$. Het is handig om elk natuurlijk getal op een zo eenvoudig mogelijke wijze te coderen. Immers, we zouden als inputsymbolen voor een Turingmachine simpelweg de verzameling $\{0,1,\ldots,9\}$ kunnen gebruiken, maar dat is meer ingewikkeld dan nodig. Een goede optie is als volgt.

Definitie 3.5

> De *canonieke representatie* van een natuurlijk getal $n \in \mathbb{N}$ bestaat uit de rij gevormd door een 0 gevolgd door n keer een 1. De *canonieke representatie* van $(a_1,\ldots,a_n) \in \mathbb{N}^n$ bestaat uit de concatenatie van de canonieke representaties van elk van de natuurlijke getallen $a_1,\ldots,a_n$.

Zo wordt bijvoorbeeld het natuurlijk getal 4 voorgesteld door 01111 en het drietal $(2,1,5) \in \mathbb{N}^3$ door 01101011111.

Voor elke $n \in \mathbb{N}$ zorgt deze canonieke representatie voor een bijectie tussen $\mathbb{N}^n$ en een deelverzameling van de strings over het alfabet $\{0,1\}$. Noteer voor een deelverzameling $S \subset \mathbb{N}^n$ met $\tilde{S}$ het overeenkomstig bijectief beeld. Bovendien noteren we met $\tilde{x} \in \{0,1\}^*$ dit bijectief beeld, voor elke $x \in \mathbb{N}^n$. Zo is bijvoorbeeld $\tilde{3} = 0111$ en $\widetilde{(2,1)} = 01101$.

Definitie 3.6

> Een deelverzameling $S \subset \mathbb{N}^n$ is *Turing recursief opsombaar* of *Turing semi-beslisbaar* indien $\tilde{S} \subset \{0,1\}^*$ Turing recursief opsombaar is.

Definitie 3.7

Een deelverzameling $S \subset \mathbb{N}^n$ noemen we *Turing berekenbaar*, *Turing recursief* of *Turing beslisbaar* indien $\tilde{S} \subset \{0,1\}^*$ Turing berekenbaar is.

3.1.3 Turing berekenbaarheid van een partiële functie

We beschouwen nu een partiële functie $\varphi : \mathbb{N} \to \mathbb{N}$. Wat betekent Turing berekenbaarheid in dit geval? Natuurlijk hebben we al noties van recursief opsombaar en berekenbaar die hier toegepast kunnen worden, namelijk via de grafiek; inderdaad, we kunnen immers de verzameling

$$\text{graf}(\varphi) = \{(x, \varphi(x)) \,|\, x \in \mathbb{N} \text{ en } \varphi(x) \text{ is gedefinieerd}\} \subset \mathbb{N}^2$$

beschouwen. Hieronder geven we echter een andere definitie. Daarna gaan we het verband na tussen de ingevoerde definitie en het zojuist geschetste idee. Dat gebeurt in Propositie 3.9 verderop.

Definitie 3.8

Zij $\varphi : \mathbb{N} \to \mathbb{N}$ een partiële functie. We noemen φ *partieel Turing berekenbaar* indien er een Turingmachine M met verzameling van inputsymbolen $T = \{0,1\}$ bestaat, zodat: indien, voor een $x \in \mathbb{N}$, M als input $\tilde{x}$ krijgt, de string $\tilde{x}$ wordt aanvaard als en slechts als $\varphi(x)$ gedefinieerd is, en in dat geval is de uitvoer van M precies $\tilde{y}$, met y zodat $\varphi(x) = y$. Indien φ bovendien totaal is, dan zeggen we dat φ *totaal Turing berekenbaar* of kortweg *Turing berekenbaar* is.

Opmerking. Voor een partiële functie $\mathbb{N}^n \to \mathbb{N}^m$ gebruiken we meestal de notatie φ. Een partiële functie $\mathbb{N}^n \to \mathbb{N}^m$ die daarenboven totaal is noteren we gemakkelijkheidshalve dikwijls met f.

We merken ook nog op dat Definitie 3.8 op evidente wijze te veralgemenen is naar partiële functies $\mathbb{N}^n \to \mathbb{N}^m$. In deze thesis zullen we steeds $m = 1$ hebben. Wel zal het geval van een partiële functie $\mathbb{N}^n \to \mathbb{N}$ met $n > 1$ voortdurend voorkomen; zie daarvoor ook volgende sectie. Omwille van notationele redenen beperken we ons hier echter tot het geval $m = n = 1$. Zo ook in volgend resultaat, dat bekend staat als de *Graph Theorem*.

Propositie 3.9

Zij $\varphi, f : \mathbb{N} \to \mathbb{N}$ een partiële en een totale functie, respectievelijk. Dan geldt:

1. *φ is partieel Turing berekenbaar als en slechts als graf$(\varphi) \subset \mathbb{N}^2$ Turing recursief opsombaar is.*
2. *f is (totaal) Turing berekenbaar als en slechts als graf$(f) \subset \mathbb{N}^2$ Turing berekenbaar is.*

Bewijs. We tonen enkel 1. aan; 2. is analoog aan de eerste redenering. Veronderstel eerst dat graf$(\varphi) = \{(x, \varphi(x)) \,|\, x \in \mathbb{N}$ en $\varphi(x)$ is gedefinieerd$\} \subset \mathbb{N}^2$ Turing recursief opsombaar is volgens Definitie 3.6. Dan hebben we een Turingmachine M met verzameling van inputsymbolen gelijk aan $\{0,1\}$ die eender welke string s in $\{0,1\}^*$ als input neemt en die s aanvaardt als en slechts als

$$s \in \widetilde{\text{graf}(\varphi)} = \{\widetilde{(x, \varphi(x))} \,|\, x \in \mathbb{N} \text{ en } \varphi(x) \text{ is gedefinieerd}\}.$$

Dat wil zeggen, s wordt aanvaard als en slechts als er een $x \in \mathbb{N}$ bestaat (met $\varphi(x)$ gedefinieerd) zodat s precies de canonieke representatie van $(x, \varphi(x))$ is. Het is nu duidelijk hoe we hieruit een Turingmachine M' maken die Definitie 3.8 bewerkstelligt; veronderstel dat we als input een $\tilde{x}$ met $x \in \mathbb{N}$ hebben. Laat M achtereenvolgens $n+1$ stappen werken op de inputstrings $\widetilde{(x,0)}, \widetilde{(x,1)}, \ldots, \widetilde{(x,n)}$ voor $n = 0,1,2,\ldots$ Indien een inputstring $\widetilde{(x,i)}$ door M aanvaard wordt, laat M' dan accepteren en als output $\tilde{i}$ geven; dan is $i = \varphi(x)$ met $\varphi(x)$ gedefinieerd. Merk op dat we hier een informele, en in zekere zin impliciete, beschrijving van de Turingmachine M' gegeven, maar uit de Hypothese van Church volgt dat elk "intuïtief beschreven" algoritme op een Turingmachine geïmplementeerd kan worden. Dan hebben we inderdaad een Turingmachine M' geconstrueerd die aan het gevraagde voldoet. Dit bewijst de eerste implicatie. De andere implicatie volgt essentieel door de zojuist gegeven redenering om te draaien. Dit beëindigt het bewijs van Propositie 3.9. ■

3.2 Gödel en Kleenes recursietheorie

In de vorige sectie hebben we gedefinieerd wat we bedoelen met berekenbaarheid, en dit met behulp van Turingmachines. De Hypothese van Church geeft echter aanleiding tot het idee dat er ook een definitie van berekenbaarheid moet zijn die onafhankelijk is van een concrete mechanische procedure zoals Turing- en registermachines dat bijvoorbeeld zijn. Dat blijkt inderdaad zo te zijn; Gödel en Kleene (1909-1994) stelden dit als definitie van berekenbaarheid voor. Hun definitie komt kort gezegd op het volgende neer: aan de hand van een set van basisfuncties, van dewelke we eisen dat ze zeker al berekenbaar zijn, genereren we functies die opgebouwd zijn door een aantal basisoperaties toe te passen. In deze sectie maken we dit idee exact.

Tot slot spreken we af dat $\mathbb{N}^0 := \{*\}$ met $*$ een arbitrair element.

3.2.1 Primitief berekenbaarheid

We definiëren eerst wat we bedoelen met een *primitief berekenbare functie*. Na de definitie geven we een aantal opmerkingen en voorbeelden om dit begrip intuïtief wat meer te duiden. Essentieel is dat het primitief berekenbaar zijn van een functie *niet* hetzelfde betekent als de Turing berekenbaarheid van de functie; verderop geven we als voorbeeld hiervan de Ackermannfunctie. Daarvoor is de klasse van primitief berekenbare functies te klein. Om equivalentie te hebben moeten we de operatie van *onbegrensde minimalisatie* nog toevoegen. Dit doen we later.

Definitie 3.10

Zij $\mathfrak{F}_n$ de verzameling van alle functies van $\mathbb{N}^n$ naar $\mathbb{N}$ en zij $\mathfrak{F} = \cup_{n\geq 0}\mathfrak{F}_n$. De verzameling van *primitief berekenbare functies* of *primitief recursieve functies* is dan de kleinste deelverzameling van $\mathfrak{F}$ die al de volgende functies, de zogenaamde *basisfuncties*, bevat

1. $ZERO(x) = 0$
2. $SUCC(x) = x+1$
3. $PROJ_i^n(x_1,\ldots,x_n) = x_i$, met $n \in \mathbb{N}$ en $i \in \{1,\ldots,n\}$

en die bovendien gesloten is onder de operaties

1. *Samenstelling*. Dit wil zeggen dat voor primitief berekenbare functies $g \in \mathfrak{F}_m, h_1,\ldots,h_m \in \mathfrak{F}_n$ ook de functie $COMP(g,h_1,\ldots,h_m) : \mathbb{N}^n \to \mathbb{N}$ gedefinieerd door

   $$(x_1,\ldots,x_n) \mapsto g(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n))$$

   primitief berekenbaar is.

2. *Primitieve recursie*. Dit wil zeggen dat voor primitief berekenbare functies $f_0 \in \mathfrak{F}_n, g \in \mathfrak{F}_{n+2}$, ook de functie $PREC(f_0,g) : \mathbb{N}^{n+1} \to \mathbb{N}$ gedefinieerd door

   $$\begin{aligned}(x_1,\ldots,x_n,0) &\mapsto f_0(x_1,\ldots,x_n)\\ (x_1,\ldots,x_n,y+1) &\mapsto g(x_1,\ldots,x_n,y,PREC(f_0,g)(x_1,\ldots,x_n,y))\end{aligned}$$

   primitief berekenbaar is.

In Definitie 3.11 breiden we deze verzameling van functies uit.

We geven een aantal voorbeelden om met de notie van primitief berekenbaarheid vertrouwd te geraken.

Voorbeelden.

- Beschouw de functie

$$SUM : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto x+y.$$

Deze is duidelijk primitief berekenbaar; immers

$$SUM = PREC(PROJ_1^1, COMP(SUCC, PROJ_3^3)).$$

- Beschouw de functie

$$a : \mathbb{N} \to \mathbb{N} : x \mapsto a,$$

waarbij $a \in \mathbb{N}$. Dan is de functie a voor elke $a \in \mathbb{N}$ primitief berekenbaar; inderdaad, merk op dat de functie $1 = COMP(SUCC, ZERO)$ primitief berekenbaar is. Analoog is de functie $2 = COMP(SUCC, 1)$ primitief berekenbaar, enzovoort. Uiteraard blijft dit gelden als men dezelfde functie beschouwt maar dan meer algemeen met domein $\mathbb{N}^n$; dat wil zeggen de functie

$$a^n : \mathbb{N}^n \to \mathbb{N} : (x_1, \ldots, x_n) \mapsto a$$

is primitief berekenbaar voor elke $a \in \mathbb{N}$.

- Beschouw de functie

$$()^{()} : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto x^y.$$

Ook deze functie is primitief berekenbaar; immers

$$()^{()} = PREC(1, COMP(PROD, PROJ_1^3, PROJ_3^3)).$$

- Beschouw de functie

$$IFZERO : \mathbb{N}^3 \to \mathbb{N} : (x,y,z) \mapsto \begin{cases} y & \text{als } x = 0 \\ z & \text{als } x \neq 0 \end{cases}.$$

Deze functie is primitief berekenbaar; immers

$$IFZERO = COMP(C, PROJ_2^3, PROJ_3^3, PROJ_1^3)$$

met

$$C : \mathbb{N}^3 \to \mathbb{N} : (x,y,z) \mapsto \begin{cases} x & \text{als } z = 0 \\ y & \text{als } z \neq 0 \end{cases}$$

primitief berekenbaar.

- (*Begrensde minimalisatie.*) Zij $R(x_1, \ldots, x_n, y)$ een relatie met primitief berekenbare karakteristieke functie. Dan is de functie

$$f : \mathbb{N}^{n+2} \to \mathbb{N} : (x_1, \ldots, x_n, a, z) \mapsto \mu_{a<y\leq z} R(x_1, \ldots, x_n, y)$$

primitief berekenbaar, waarbij $\mu_{a<y\leq z} R(x_1, \ldots, x_n, y)$ gedefinieerd is als de kleinste y zodat $a < y \leq z$ en $(x_1, \ldots, x_n, y) \in R$ indien zo'n y bestaat, en gelijk aan z in het andere geval.

- En er zijn nog veel voorbeelden van primitief berekenbare functies, onder meer

$$\begin{aligned}
PRED &: \mathbb{N} \to \mathbb{N} : x \mapsto \begin{cases} 0 & \text{als } x = 0 \\ x-1 & \text{als } x \neq 0 \end{cases} \\
MAX &: \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \max(x,y) \\
MIN &: \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \min(x,y) \\
MABS &: \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \max(0,x-y) \\
ABS &: \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto |x-y| \\
ASIGN &: \mathbb{N} \to \mathbb{N} : x \mapsto \begin{cases} 1 & \text{als } x = 0 \\ 0 & \text{als } x \neq 0 \end{cases}.
\end{aligned}$$

  Bovendien, als $f : \mathbb{N}^{n+1} \to \mathbb{N}$ primitief berekenbaar is, dan zijn volgende functies dit ook:

$$\begin{aligned}
S &: \mathbb{N}^{n+2} \to \mathbb{N} : (x_1,\ldots,x_n,a,y) \mapsto \sum_{i=a}^{y} f(x_1,\ldots,x_n,i) \\
P &: \mathbb{N}^{n+2} \to \mathbb{N} : (x_1,\ldots,x_n,a,y) \mapsto \prod_{i=a}^{y} f(x_1,\ldots,x_n,i).
\end{aligned}$$

  Primitieve berekenbaarheid van al de bovenstaande functies wordt op analoge wijze bewezen zoals hierboven reeds een aantal keer werd geïllustreerd.

- Zij $P : \mathbb{N}^n \to \mathbb{N}$ een veelterm in $\mathbb{Z}[x_1,\ldots,x_n]$ die waardes in $\mathbb{N}$ aanneemt. Dan is P primitief berekenbaar. Inderdaad; schrijf P als $P^+ - P^-$, waarbij P^+ en P^- veeltermen in $\mathbb{N}[x_1,\ldots,x_n]$ zijn. Het is omwille van al hetgeen we hierboven al gezien hebben evident dat P^+ en P^- primitief berekenbaar zijn. Merk op dat $P^+ - P^- = P^+ \dot{-} P^-$ vanwege onze veronderstelling dat P waardes in $\mathbb{N}$ aanneemt. De functie $\dot{-}$ hierin word gedefinieerd in Lemma 3.17, en daaruit volgt meteen dat $\dot{-}$ primitief berekenbaar is. Dan is $P = COMP(\dot{-}, P^+, P^-)$ primitief berekenbaar.

Opmerking. Het is duidelijk dat elke primitief berekenbare functie is totaal. Inderdaad, de basisfuncties zijn totaal en toepassing van een operatie behoudt duidelijk de totaliteit van een functie.

3.2.2 Partieel berekenbaarheid

We voeren nu nog een derde en laatste operatie toe, de *onbegrensde minimalisatie* of ook wel μ*-operator* genoemd.

Definitie 3.11

Zij $\mathfrak{P}_n$ de verzameling van alle partiële functies van $\mathbb{N}^n$ naar $\mathbb{N}$ en zij $\mathfrak{P} = \cup_{n\geq 0}\mathfrak{P}_n$. De verzameling van *partieel berekenbare functies* of *partieel recursieve functies* is dan de kleinste deelverzameling van $\mathfrak{P}$ die al de basisfuncties bevat en gesloten is onder de operaties van samenstelling, primitieve recursie, zoals in Definitie 3.10, alsook onder de operatie

3. μ*-operator*. Dit wil zeggen dat voor een partieel recursieve functie $f \in \mathfrak{P}_{n+1}$ de partiële functie $\mu f : \mathbb{N}^n \to \mathbb{N}$, waarbij

   $\mu f(x_1,\ldots,x_n)$ gelijk is aan y, indien er $y \in \mathbb{N}$ bestaat zodat
   $f(x_1,\ldots,x_n,z)$ voor alle $z = 0,1,\ldots,y$ gedefinieerd is
   $f(x_1,\ldots,x_n,z) \neq 0$ als $1 \leq z < y$
   $f(x_1,\ldots,x_n,y) = 0$
   $\mu f(x_1,\ldots,x_n)$ niet gedefinieerd is in het andere geval

   partieel recursief is.

Een partieel berekenbare functie die bovendien totaal is, wordt ook wel een *totaal berekenbare*, *berekenbare*, *totaal recursieve* of *recursieve* functie genoemd.

Merk op dat er in de definitie hierboven sprake is van samenstellingen van partiële functies. Dit wordt op de evidente manier gedaan; dat wil zeggen, de samenstelling in een punt is gedefinieerd als en slechts als elk van de initiële functies in dat punt gedefinieerd zijn. Een analoge opmerking geldt voor de primitieve recursie van partiële functies.

Belangrijk op te merken is dat, in het algemeen, een partieel recursieve functie niet noodzakelijk totaal is, maar slechts een partiële functie is. Beschouw immers bijvoorbeeld de partieel recursieve functie

$$SUCC : \mathbb{N} \to \mathbb{N} : x \mapsto x+1.$$

Dan is de partiële functie $\mu SUCC : \{*\} \to \mathbb{N}$ ongedefinieerd; dat wil zeggen $\mu SUCC(*)$ is ongedefinieerd, of nog, $\mu SUCC = \emptyset$. Dus $\mu SUCC$ is een partieel recursieve functie die niet totaal is.

We geven nu een paar voorbeelden om het gebruik van de onbegrensde minimalisatie operator te illustreren.

Voorbeelden.

- Beschouw de partiële functie

$$FL : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \left\lfloor \frac{x}{y} \right\rfloor$$

met domein $\mathbb{N} \times \mathbb{N}_0$. Merk op dat $FL(x,0)$ inderdaad niet gedefinieerd is voor elk natuurlijk getal x in $\{(x,y) \in \mathbb{N}^2 \mid y \neq 0\}$. Dan is $FL(x,y)$ de kleinste $z \in \mathbb{N}$ zodat $x < y(z+1)$. De functie

$$INEQ : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \begin{cases} 0 & \text{als } x < y \\ 1 & \text{als } x \geq y \end{cases}$$

is primitief berekenbaar, daar

$$INEQ = COMP(IFZERO, COMP(MABS, PROJ_2^2, PROJ_1^2), 1, 0).$$

Dan is ook

$$f : \mathbb{N}^3 \to \mathbb{N} : (x,y,z) \mapsto INEQ(x, y(z+1))$$

primitief berekenbaar daar vermenigvuldiging en samenstelling dit zijn. Dit impliceert dat $FL = \mu f$ partieel berekenbaar is.

- Beschouw de partiële functie

$$REM : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \text{deling van } x \text{ door } y$$

met domein $\mathbb{N} \times \mathbb{N}_0$. Merk op dat

$$REM \simeq MABS(PROJ_1^2, COMP(PROD, PROJ_2^2, d)).$$

Dit WIL eigenlijk gewoon zeggen dat $REM(x,y) = \max(0, x - yFL(x,y))$ voor alle $x, y \in \mathbb{N}$ met $y \neq 0$.

We besluiten dit onderdeel met een opmerking ter verduidelijking.

Opmerking. Per definitie is elke totaal berekenbare functie ook partieel berekenbaar. Bovendien is deze inclusie strikt; inderdaad, de discussie hierboven geeft al meteen een voorbeeld van een partieel berekenbare functie die niet totaal is, en bijgevolg a fortiori niet totaal berekenbaar kan zijn. Per constructie is de verzameling van primitief recursieve functies een deelverzameling van de totaal berekenbare functies. Een andere vraag die men zich nu kan stellen is of elke totaal berekenbare functie noodzakelijkerwijs primitief berekenbaar is. Dit blijkt niet waar te zijn. Het bekendste tegenvoorbeeld is allicht de zogenaamde *Ackermannfunctie* $A : \mathbb{N}^2 \to \mathbb{N}$, recursief gedefinieerd door

$$(x,y) \mapsto A(x,y) := \begin{cases} y+1 & \text{als} \quad x = 0 \\ A(x-1,1) & \text{als} \quad x > 0 \text{ en } y = 0 \\ A(x-1, A(x,y-1)) & \text{als} \quad x > 0 \text{ en } y > 0. \end{cases}$$

Merk op dat het a priori niet evident is dat A totaal is; id est, of de recursieve definitie van de functie wel voor elk koppel $(x,y) \in \mathbb{N}^2$ zinvol is. Het is echter niet heel moeilijk om in te zien dat dit wel het geval is. Eventueel kan men dit formeel aantonen door een dubbele inductie toe te passen op x en y. Men kan eveneens aantonen dat A totaal berekenbaar is. De Ackermannfunctie A stijgt echter buitengewoon snel, veel sneller zelfs dan een exponentiële toename. Dit is meteen ook de reden, en de essentie van het bewijs, waarom A niet primitief recursief is. Samenvattend hebben we tussen de door ons ingevoerde functieverzamelingen volgende onderlinge inclusies:

$$\text{primitief berekenbaar} \subsetneq \text{totaal berekenbaar} \subsetneq \text{partieel berekenbaar}.$$

3.2.3 Recursief opsombaarheid en berekenbaarheid van een verzameling

Definitie 3.12

> Een deelverzameling $S \subset \mathbb{N}^n$ noemen we *berekenbaar*, *recursief* of *beslisbaar* indien de indicatorfunctie $\chi_S : \mathbb{N}^n \to \mathbb{N}$ berekenbaar is.

Een triviaal voorbeeld is dat $\emptyset$ berekenbaar is; immers, $\chi_\emptyset = 0$ is berekenbaar per definitie.

Definitie 3.13

> Een deelverzameling $S \subset \mathbb{N}^n$ noemen we *recursief opsombaar* of *semi-beslisbaar* indien er een partieel berekenbare functie bestaat waarvan het domein precies S is.

Volgend resultaat staat bekend als de *Normal Form Theorem* voor berekenbare relaties.

Propositie 3.14

> *Een deelverzameling $S \subset \mathbb{N}^n$ is recursief opsombaar indien er een berekenbare verzameling $R \subset \mathbb{N}^{n+1}$ bestaat zodat*
>
> $$(x_1,\ldots,x_n) \in S \Leftrightarrow (\exists y \in \mathbb{N})\,(x_1,\ldots,x_n,y) \in R$$
>
> *voor alle $(x_1,\ldots,x_n) \in \mathbb{N}^n$.*

Bewijs. We verwijzen naar [20] of [27]. ■

Volgende stelling is cruciaal met betrekking tot het bewijs van de onbeslisbaarheid van Hilberts Tiende Probleem wat wij gaan geven. Het is een heel diep resultaat. Het bewijs ervan is dan ook erg lang en zou ons hier te ver leiden.

Eerst hebben we nog wat terminologie nodig. Zij $m \in \mathbb{N}$. De *level set in m* van een partiële functie $\varphi : \mathbb{N}^n \to \mathbb{N}$ is de verzameling $\{x \in \mathrm{dom}(\varphi) \,|\, \varphi(x) = m\}$. Herinner ook dat, gegeven een verzameling $S \subset \mathbb{N}^{n+m}$, de *projectie op de ruimte van eerste n coördinaten* de verzameling is gedefinieerd als

$$\{(x_1,\ldots,x_n) \in \mathbb{N}^n \,|\, \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } (x_1,\ldots,x_n,y_1,\ldots,y_m) \in S\}.$$

Propositie 3.15

> *Een deelverzameling $S \subset \mathbb{N}^n$ is recursief opsombaar als en slechts als er een primitief berekenbare functie bestaat zodat S precies een projectie van een zekere level set van die functie is.*

Bewijs. Een bewijs zou ons te ver leiden. Daarom verwijzen we naar [17]. ■

Hieruit volgt meteen volgend praktisch resultaat.

Propositie 3.16

Een verzameling $S \subset \mathbb{N}^n$ is recursief opsombaar als en slechts als

$$S = \{(x_1,\ldots,x_n) \in \mathbb{N}^n \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } g(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0\}$$

voor een zekere primitief berekenbare functie $g : \mathbb{N}^{n+m} \to \mathbb{N}$.

Bewijs. Veronderstel eerst dat $S \subset \mathbb{N}^n$ recursief opsombaar is. Uit Propositie 3.15 volgt dat er een primitief berekenbare functie $g : \mathbb{N}^{n+m} \to \mathbb{N}$ en een $t \in \mathbb{N}$ bestaan zodat

$$S = \{(x_1,\ldots,x_n)\,\mathbb{N}^n \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } g(x_1,\ldots,x_n,y_1,\ldots,y_m) = t\}.$$

Definieer een functie

$$h : \mathbb{N}^{n+m} \to \mathbb{N} : (\vec{x},\vec{y}) \mapsto \begin{cases} g(\vec{x},\vec{y}) - t & \text{als } g(\vec{x},\vec{y}) \geq t \\ 1 & \text{als } g(\vec{x},\vec{y}) < t \end{cases},$$

waarbij ter afkorting $\vec{x} = (x_1,\ldots,x_n) \in \mathbb{N}^n$ en $\vec{y} = (y_1,\ldots,y_m) \in \mathbb{N}^m$. Uit Lemma 3.17 hieronder volgt meteen dat h primitief berekenbaar is, daar $h = COMP(\dot{-},g,t)$ met $t : \mathbb{N} \to \mathbb{N}$ de functie die constant 1 is. Bovendien is door de definitie van h duidelijk dat

$$S = \{(x_1,\ldots,x_n)\,\mathbb{N}^n \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } h(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0\}.$$

Veronderstel nu omgekeerd dat

$$S = \{(x_1,\ldots,x_n) \in \mathbb{N}^n \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } g(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0\}$$

voor een zekere primitief berekenbare functie g. Dan is S de projectie op de ruimte van eerste n coördinaten van de level set in 0 van de primitief berekenbare functie g, en het gevraagde volgt dan wederom meteen uit Propositie 3.15. Dit beëindigt het bewijs van Propositie 3.16. ■

Merk op dat dit een veralgemening van Propositie 3.14 is. Verderop in de thesis gaan we bijna altijd deze karakterisatie van recursief opsombare verzamelingen gebruiken.

Lemma 3.17

De functie gedefinieerd door

$$\dot{-} : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \begin{cases} 1 & \text{als } x < y \\ x - y & \text{als } x \geq y \end{cases}$$

is primitief berekenbaar.

Bewijs. Zij

$$INEQ' : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \begin{cases} 1 & \text{als } x < y \\ 0 & \text{als } x \geq y \end{cases}$$

Dan volgt met een symmetrieargument uit de voorbeelden na Definitie 3.11 dat $INEQ'$ primitief berekenbaar is. Merk dan op dat

$$\dot{-}(x,y) = INEQ'(x,y) + |x-y|\, INEQ(x,y)$$

voor alle $x, y \in \mathbb{N}$. Bijgevolg is het duidelijk dat $\dot{-}$ inderdaad primitief berekenbaar is. Dit beëindigt het bewijs van Lemma 3.17. ■

Men heeft zelfs het volgende: indien er een berekenbare, dus niet noodzakelijk *primitief* berekenbare, functie bestaat waarvan een gegeven verzameling een projectie van een level set is, dan is die verzameling recursief opsombaar. We verwijzen hiervoor naar Theorem 1.2 in [27].

In het geval dat $n = 1$ vermelden we volgende meer intuïtieve karakterisatie. Een evidente veralgemening naar $n > 1$ is mogelijk.

Propositie 3.18

Voor een verzameling $S \subset \mathbb{N}$ zijn de voorwaarden hieronder equivalent.

1. *S is recursief opsombaar, dat wil zeggen $S = dom(\phi)$ voor een zekere $\phi : \mathbb{N} \to \mathbb{N}$ partieel berekenbaar.*
2. *$S = im(\phi)$ met $\phi : \mathbb{N} \to \mathbb{N}$ partieel berekenbaar.*
3. *$S = \emptyset$ of $S = im(f)$ met $f : \mathbb{N} \to \mathbb{N}$ (totaal) berekenbaar.*
4. *De partiële functie*

$$\bar{\chi}_S : \mathbb{N} \to \mathbb{N} : x \mapsto \begin{cases} 1 & \text{als } x \in S \\ \text{ongedefinieerd} & \text{als } x \notin S \end{cases}$$

is partieel berekenbaar.

Bewijs. Het bewijs zou ons hier te ver leiden. In [11] wordt het resultaat aangetoond door concrete Turingmachines te gaan construeren. Alternatieven zijn in [27] en [20] te vinden. ■

Een onmiddellijk gevolg hiervan is volgend resultaat. Merk daarbij de analogie op met de uitspraak onmiddellijk na Definitie 3.4.

Propositie 3.19

Een berekenbare verzameling $S \subset \mathbb{N}$ is recursief opsombaar.

Bewijs. Indien $S = \emptyset$ dan volgt het gevraagde wegens Propositie 3.18. In het andere geval, indien $S \neq \emptyset$, dan kunnen bestaat er een $x_0 \in S$. Daar χ_S per hypothese berekenbaar is, is de functie

$$f : \mathbb{N} \to \mathbb{N} : x \mapsto IFZERO(x_0, x, \chi_S(x))$$

dit ook. Maar we hebben dat $\{f(x) \,|\, x \in \mathbb{N}\} = \{x_0\} \cup S = S$, daar $x_0 \in S$. Daarom volgt wederom uit Propositie 3.18 dat S recursief opsombaar is. Dit beëindigt het bewijs van Propositie 3.19. ■

Volgend resultaat is nogal evident.

Propositie 3.20

> *Doorsnedes, unies, complementen en Cartesische producten van berekenbare verzamelingen in $\mathbb{N}^n$ zijn opnieuw berekenbaar.*

Bewijs. Zij $A, B \subset \mathbb{N}^n$ berekenbaar. Dus zijn χ_A en χ_B per definitie berekenbaar. Dan zijn $\chi_{A\cap B} = COMP(PROD, \chi_A, \chi_B)$ en $\chi_{A\cup B} = COMP(MAX, \chi_A, \chi_B)$ berekenbaar. Analoog hebben we dat $\chi_{A^c} = COMP(ABS, 1, \chi_A)$ berekenbaar is. Tot slot is $\chi_{A\times B}$ gelijk aan $\mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto \chi_A(x)\,\chi_B(y)$, en deze functie is duidelijk berekenbaar. Dit beëindigt het bewijs van Propositie 3.20. ■

Nu kunnen we ons afvragen of we een analoog resultaat voor recursief opsombare verzamelingen hebben.

Propositie 3.21

> *Doorsnedes, unies en Cartesische producten van recursief opsombare verzamelingen in $\mathbb{N}^n$ zijn opnieuw recursief opsombaar.*

Bewijs. Zij $A, B \subset \mathbb{N}^n$ recursief opsombaar. Uit Propositie 3.14 volgt dat er berekenbare relaties R en Q bestaan zodat

$$x \in A \Leftrightarrow (\exists y \in \mathbb{N})\, R(x,y), \quad x \in B \Leftrightarrow (\exists y \in \mathbb{N})\, Q(x,y).$$

Merk op dat

$$A \cap B = \{x \in \mathbb{N} \,|\, (\exists y \in \mathbb{N})(\exists z \in \mathbb{N}) \text{ zodat } f(x,y,z) = 2\}$$

met

$$f : \mathbb{N}^3 \to \mathbb{N} : (x,y,z) \mapsto \chi_R(x,y) + \chi_Q(x,z)$$

duidelijk berekenbaar. Dit wil precies zeggen dat $A \cap B$ de projectie op de eerste coördinaat van de level set in 2 van de berekenbare functie f is. Wegens de opmerking na Propositie 3.15 volgt dat $A \cap B$ recursief opsombaar is. Dat $A \cup B$ recursief opsombaar is volgt op een volledig analoge wijze, en zo ook voor $A \times B$. Dit beëindigt het bewijs van Propositie 3.21. ■

In de formulering van bovenstaand resultaat valt vooral op dat er *niet* staat dat het complement van een recursief opsombare verzameling opnieuw recursief opsombaar is. Die uitspraak is namelijk niet waar, zoals al blijkt uit volgend resultaat. Immers, niet elke verzameling die recursief opsombaar is, is berekenbaar, zoals zal blijken uit Propositie 3.25.

Propositie 3.22

Een deelverzameling $S \subset \mathbb{N}^n$ is berekenbaar als en slechts als S en S^c recursief opsombaar zijn.

Bewijs. We beperken ons omwille van notationele redenen tot het geval $n = 1$. Veronderstel ten eerste dat $S \subset \mathbb{N}$ berekenbaar is. Dan is S a fortiori recursief opsombaar wegens Propositie 3.19. Omdat S berekenbaar is, volgt uit Propositie 3.20 dat S^c ook berekenbaar is. Dan is S^c a fortiori recursief opsombaar wegens Propositie 3.19.
Veronderstel omgekeerd dat S en S^c recursief opsombaar zijn. We mogen aannemen dat beide verzamelingen niet-leeg zijn; immers indien één van beide leeg is dan volgt dat $S = \emptyset$ of $S = \mathbb{N}$ en natuurlijk zijn deze twee verzamelingen berekenbaar, zodat we in dat geval klaar zijn. Uit Propositie 3.14 volgt dat er berekenbare relaties R en Q bestaan zodat

$$x \in S \Leftrightarrow (\exists y \in \mathbb{N})\, R(x,y), \quad x \in S^c \Leftrightarrow (\exists y \in \mathbb{N})\, Q(x,y).$$

Indien we stellen dat $i : \mathbb{N}^2 \to \mathbb{N} : (x,y) \mapsto (1 - \chi_R(x,y))\,(1 - \chi_Q(x,y))$ dan is $f := \mu i : \mathbb{N} \to \mathbb{N}$ per definitie partieel berekenbaar, daar i berekenbaar is. Maar f is zelfs totaal berekenbaar, daar de eerste-orde formule $(\forall x)(\exists y)\, R(x,y) \vee Q(x,y)$ waar is in $\mathbb{N}$ en f bijgevolg totaal is. Het is eenvoudig in te zien dat voor elke $x \in \mathbb{N}$ geldt dat $\chi_S(x) = \chi_R(x, f(x))$. Bijgevolg, daar R en f berekenbaar zijn, is S berekenbaar. Dit beëindigt het bewijs van Propositie 3.22. ■

3.2.4 Constructie van een recursief opsombare maar niet berekenbare verzameling

De *Enumeration Theorem*, zoals bijvoorbeeld in [20], zegt dat er, voor elke $n \in \mathbb{N}$, een rij $\{\varphi_x^n\}_{x \in \mathbb{N}}$ van partieel berekenbare functies in n variabelen bestaat zodat het volgende geldt: als ψ een partieel berekenbare functie in n variabelen is, dan bestaat er een x zodat $\psi \simeq \varphi_x^n$. Deze stelling is een van de cruciale resultaten uit de recursietheorie. In het licht hiervan kunnen we zeggen dat $\{\varphi_x^n\}_{x \in \mathbb{N}}$ een partieel berekenbare opsomming van alle partieel berekenbare functies in n variabelen is. We schrijven kortweg ook wel φ_x in plaats van φ_x^1.

Definitie 3.23

Voor elke $x \in \mathbb{N}$ definiëren we $W_x := \mathrm{dom}(\varphi_x)$.

Aan de hand van deze definitie definiëren we een andere verzameling, als volgt.

Definitie 3.24

Zij $K := \{x \in \mathbb{N} \mid x \in W_x\} = \{x \in \mathbb{N} \mid \varphi_x(x) \text{ is gedefinieerd}\} \subset \mathbb{N}$.

Uit hetgeen volgt zal blijken dat K niet berekenbaar is, maar wel recursief opsombaar. Dit is dus ons eerste voorbeeld van een onbeslisbaar probleem.

Propositie 3.25

De verzameling $K \subset \mathbb{N}$ is recursief opsombaar maar niet berekenbaar.

Bewijs. Uit de Enumeration Theorem (zie ODIFREDDI blz. 130) volgt dat er een partieel berekenbare functie φ bestaat zodat $\varphi \simeq \varphi_x$. Nu is $K = \text{dom}(\varphi)$, zodat K inderdaad recursief opsombaar is.
Omgekeerd, veronderstel uit het ongerijmde dat K wel berekenbaar is. Dan volgt uit Propositie 3.22 dat K^c recursief opsombaar is. De Enumeration Theorem geeft dan dat er een $x_0 \in \mathbb{N}$ bestaat zodat $K^c = \text{dom}(\varphi_{x_0})$. Voor elke $x \in \mathbb{N}$ is

$$x \in K^c \Leftrightarrow x \notin W_x = \text{dom}(\varphi_x).$$

Dus in het bijzonder hebben we

$$x_0 \in K^c \Leftrightarrow x_0 \notin W_{x_0} = \text{dom}(\varphi_{x_0}).$$

Maar dit is in contradictie met het feit dat $K^c = \text{dom}(\varphi_{x_0})$. Dit beëindigt het bewijs van Propositie 3.25. ■

Eigenlijk is deze aanpak heel analoog als het stopprobleem, en het uiteindelijke resultaat is hetzelfde: er bestaat een verzameling van natuurlijke getallen die recursief opsombaar maar niet berekenbaar is.

3.3 Verband: de equivalentie van beide formalismen

In deze sectie bestuderen we het verband tussen de twee verschillende benaderingen gegeven in secties 3.1 en 3.2, respectievelijk. De conclusie is even voorspelbaar als kort: de twee benaderingen zijn equivalent. Deze analyse hangt in feite al lang in de lucht; we hebben immers al meermaals naar de Hypothese van Church verwezen, die er een directe indicatie toe is.

We werken deze equivalentie in deze thesis niet verder uit. Maar waar het eigenlijk op neerkomt is dat men het volgende expliciet kan aantonen.

- De Turing berekenbaarheid van een functie (Definitie 3.8) is equivalent met de berekenbaarheid van diezelfde functie (Definitie 3.11); eenzelfde resultaat geldt algemener voor partiële functies.
- Op eenzelfde manier hebben we dat de Turing recursieve opsombaarheid van een verzameling (Definitie 3.6) precies hetzelfde betekent als de recursief opsombaarheid van die verzameling (Definitie 3.14).

- En analoog is ook de Turing berekenbaarheid van een verzameling (Definitie 3.7) equivalent met de berekenbaarheid van die verzameling (Definitie 3.12).

We zien dat secties 3.1 en 3.2 dus in feite in het geheel equivalent zijn. Cru gesteld hadden we dus onszelf net zo goed de moeite kunnen besparen en slechts één van beide equivalente benaderingen kunnen geven. Echter, het is verhelderend om elk van beide aanpakken te geven, want de aanpak van Turing, id est de Turingmachine (sectie 3.1), geeft ons een concrete voorstellingswijze van iets dat kennelijk ook op een puur wiskundige manier opgebouwd kan worden, id est de recursietheorie van Gödel en Kleene (sectie 3.2).

Deel II

Onoplosbaarheid van Hilberts Tiende Probleem over $\mathbb{Z}$

MEER OVER $\mathbb{N}$

4.1 Reductie

In deze sectie maken we een handige reductie van Hilberts Tiende Probleem over $\mathbb{Z}$. We bewijzen namelijk dat dit probleem equivalent is met Hilberts Tiende Probleem over $\mathbb{N}$. Uit dit resultaat volgt dat we in het bewijs van de onoplosbaarheid steeds met natuurlijke getallen in plaats van gehele getallen mogen werken. Deze reductie is niet essentieel, maar maakt het bewijs wat makkelijker te formuleren.

4.1.1 Equivalentie met Hilberts Tiende Probleem over $\mathbb{N}$

We hebben als doel volgend resultaat te bewijzen. In het bewijs gebruiken we de zogenaamde *Vier-kwadratenstelling van Lagrange*, die we verderop eveneens aantonen.

Propositie 4.1

> *Hilberts Tiende Probleem over $\mathbb{Z}$ is equivalent met Hilberts Tiende Probleem over $\mathbb{N}$.*

Bewijs. Veronderstel eerst de oplosbaarheid over $\mathbb{Z}$. We beschrijven dan een algoritme dat Hilberts Tiende Probleem over $\mathbb{N}$ oplost; omwille van de Hypothese van Church zal ons intuïtief beschreven algoritme dan ook echt aanleiding geven tot een Turingmachine. Zij $P(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ als input gegeven. Beschouw dan het stelsel van diophantische vergelijkingen over de gehele getallen

$$\begin{cases} P(x_1,\ldots,x_n) = 0 \\ y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 = x_1 \\ y_{2,1}^2 + y_{2,2}^2 + y_{2,3}^2 + y_{2,4}^2 = x_2 \\ \qquad\qquad \vdots \\ y_{n,1}^2 + y_{n,2}^2 + y_{n,3}^2 + y_{n,4}^2 = x_n \end{cases}$$

in de $5n$ variabelen $x_1,\ldots,x_n,y_{1,1},\ldots,y_{n,4}$. Uit de Vier-kwadratenstelling van Lagrange volgt dat de laatste n vergelijkingen van dit stelsel een oplossing $y_{1,1},\ldots,y_{n,4}$ hebben als en slechts als $x_1,\ldots,x_n$ positief zijn. Dus het gehele stelsel heeft een oplossing in $\mathbb{Z}$ als en slechts als $P(x_1,\ldots,x_n) = 0$ een oplossing in $\mathbb{N}$ heeft. Dit hele stelsel kunnen we op evidente wijze reduceren tot één enkele diophantische vergelij-

king. Inderdaad, indien

$$\begin{aligned} Q(x_1,\ldots,x_n,y_{1,1},\ldots,y_{n,4}) \quad := \quad & P(x_1,\ldots,x_n)^2 \\ & +(y_{1,1}^2+y_{1,2}^2+y_{1,3}^2+y_{1,4}^2-x_1)^2 \\ & +(y_{2,1}^2+y_{2,2}^2+y_{2,3}^2+y_{2,4}^2-x_2)^2 \\ & \qquad\qquad \vdots \\ & +(y_{n,1}^2+y_{n,2}^2+y_{n,3}^2+y_{n,4}^2-x_n)^2 \end{aligned}$$

dan is het stelsel equivalent met $Q(x_1,\ldots,x_n,y_{1,1},\ldots,y_{n,4})=0$. Dus $Q=0$ heeft een oplossing in $\mathbb{Z}$ als en slechts $P=0$ een oplossing in $\mathbb{N}$ heeft. Maar Q is een veelterm over $\mathbb{Z}$, en we kunnen dus per hypothese beslissen of $Q=0$ al dan niet oplossingen in $\mathbb{Z}$ heeft. Op die manier kunnen we ook beslissen of P oplossingen over $\mathbb{N}$ heeft. Dit beëindigt het bewijs van de eerste implicatie.
Veronderstel omgekeerd de oplosbaarheid over $\mathbb{N}$. We beschrijven dan een algoritme dat Hilberts Tiende Probleem over $\mathbb{Z}$ oplost. Zij $P(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n]$ als input gegeven. Beschouw dan de veelterm

$$Q(y_1,\ldots,y_n,z_1,\ldots,z_n) := P(y_1-z_1,\ldots,y_n-z_n)\in\mathbb{Z}[y_1,\ldots,y_n,z_1,\ldots,z_n].$$

Dan hebben we dat $Q=0$ een oplossing heeft in $\mathbb{N}$ als en slechts als het stelsel $P=0$ een oplossing in $\mathbb{Z}$ heeft. Hieruit volgt direct het gezochte algoritme. Dit beëindigt het bewijs van Propositie 4.1. ■

Merk op dat we vanaf nu dus mogen veronderstellen dat we in de taal der ringen werken, *geïnterpreteerd in* $\mathbb{N}$. In feite komt het er dus op neer dat vanaf nu alle kwantoren over de natuurlijke getallen lopen.

4.1.2 Bewijs Vier-kwadratenstelling van Lagrange

We tonen nu de Vier-kwadratenstelling van Lagrange aan, die dateert van 1772. Daartoe formuleren en bewijzen we eerst een aantal lemma's.

Lemma 4.2

Voor $x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\in\mathbb{Z}$ *geldt dat*

$$\begin{aligned} (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \quad = \quad & (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ + \quad & (x_1y_2-x_2y_1-x_3y_4+x_4y_3)^2 \\ + \quad & (x_1y_3+x_2y_4-x_3y_1-x_4y_2)^2 \\ + \quad & (x_1y_4-x_2y_3+x_3y_2-x_4y_1)^2. \end{aligned}$$

Dit wordt de identiteit van Euler genoemd.

Bewijs. Het uitschrijven van de vergelijkingen geeft het gevraagde. Dit beëindigt het bewijs van Lemma 4.2. ■

Lemma 4.3

Zij $p > 2$ een priemgetal. Dan bestaan er $a,b,c,d,m \in \mathbb{Z}$ zodat

$$a^2 + b^2 + c^2 + d^2 = mp.$$

met $0 < m < p$.

Bewijs. We bewijzen iets sterker, namelijk dat er $a,b,m \in \mathbb{Z}$ bestaan zodat

$$a^2 + b^2 + 1 = mp$$

met $0 < m < p$. Schrijf $p = 2n+1$ met $n > 0$. Beschouw de verzamelingen

$$\begin{aligned} A &:= \{a^2 \,|\, a = 0,1,\ldots,n\}, \\ B &:= \{-1-b^2 \,|\, b = 0,1,\ldots,n\}. \end{aligned}$$

Dan hebben we dat $A \cap B = \emptyset$ en bovendien $\#A = n+1$ en $\#B = n+1$. Merk op dat geen twee verschillende elementen in A congruent zijn modulo p; inderdaad, stel dat $a_1^2 \equiv a_2^2 \mod p$ met $a_2 < a_1 \in \{0,1,\ldots,n\}$. Omdat p priem is volgt dat $p \,|\, a_1 - a_2$ of $p \,|\, a_1 + a_2$. Maar dan geldt dat

$$0 < a_1 - a_2 \leq a_1 + a_2 < 2n < p,$$

zodat in beide gevallen een contradictie volgt. Natuurlijk impliceert ditzelfde argument dat er ook in B geen twee verschillende elementen bestaan die congruent modulo p zijn. Merk nu op dat $\#(A \cup B) = 2(n+1) = p+1$. Daar er maar p kwadraatresten modulo p zijn, volgt uit bovenstaande en uit het duivenhokprincipe dat er twee elementen in A respectievelijk B bestaan die dezelfde kwadraatrest modulo p geven; dat wil zeggen er bestaan $a,b \in \{0,1,\ldots,n\}$ zodat $a^2 \equiv -1-b^2 \mod p$, of nog, $a^2 + b^2 + 1 \equiv 0 \mod p$. Dus er bestaat een $m \in \mathbb{Z}$ zodat $a^2 + b^2 + 1 = mp$. Duidelijk moet $m > 0$. Bovendien hebben we dat

$$p^2 = (2n+1)^2 = 4n^2 + 4n + 1 > 2n^2 + 1 = n^2 + n^2 + 1 \geq a^2 + b^2 + 1 = mp$$

zodat $p > m$. We besluiten dat inderdaad $a^2 + b^2 + 1 = mp$ met $0 < m < p$. Dit beëindigt het bewijs van Lemma 4.3. ■

Tenslotte hebben we de stelling zelf.

Propositie 4.4

Zij $a \in \mathbb{N}$. Dan heeft de diophantische vergelijking

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = a$$

voor alle $a \in \mathbb{N}$ oplossingen $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.

Bewijs. We kunnen het getal a ontbinden in zijn unieke priemfactorisatie. Door Lemma 4.2 te gebruiken en op te merken dat $2 = 1^2 + 1^2 + 0^2 + 0^2$, is het voldoende de stelling te bewijzen in het geval dat a een oneven priemgetal p is. Uit Lemma 4.3 volgt dat er $x_1, x_2, x_3, x_4, m \in \mathbb{Z}$ bestaan, met $0 < m < p$, zodat

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp.$$

Als $m = 1$ zijn we klaar, dus veronderstel $m > 1$. Het is nu voldoende te bewijzen dat in dat geval $m'p$ een som van vier kwadraten is voor een zekere m' die voldoet aan $1 \leq m' < m$; inderdaad, want dan kunnen we op dezelfde manier steeds verder redeneren, en dit proces is duidelijk eindig.
Veronderstel eerst dat m even is. Dan zijn x_1, x_2, x_3, x_4 ofwel allemaal even, ofwel allemaal oneven, ofwel zijn er precies twee even en twee oneven. In elk van de drie gevallen kunnen we de getallen x_1, x_2, x_3 en x_4 in twee groepen verdelen waarvoor geldt dat de som van de kwadraten van beide groepen apart even is. Maar indien $2t = x^2 + y^2$ een som van twee kwadraten is, dan is t dit ook, daar in dat geval

$$t = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2.$$

Indien we dit gebruiken vinden we $x_1', x_2', x_3', x_4' \in \mathbb{Z}$ waarvoor geldt dat

$$x_1'^2 + x_2'^2 + x_3'^2 + x_4'^2 = \frac{m}{2}\, p.$$

Bijgevolg kunnen we $m' = m/2$ nemen.
Veronderstel nu dat m oneven is. Dit geval is iets lastiger. Kies $y_1, y_2, y_3, y_4 \in \mathbb{Z}$ zodat $y_i \equiv x_i \mod m$ en bovendien $-m/2 < y_i \leq m/2$ voor alle $i = 1, 2, 3, 4$. Omdat m oneven is geldt voor elke i dat $y_i^2 < m^2/4$. Bijgevolg is

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\,\frac{m^2}{4} = m^2.$$

Ook geldt

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \mod m.$$

Uit de laatste vergelijking volgt dat $y_1^2 + y_2^2 + y_3^2 + y_4^2 = m'm$ voor een zekere $m' \geq 0$. De eerste vergelijking geeft $m' < m$. Bovendien is $m' \neq 0$; stel immers dat $m' = 0$, dan is $y_1 = y_2 = y_3 = y_4 = 0$, zodat x_i voor elke i een veelvoud van m is. Maar dan is $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 = m^2 y$ voor een zekere $y \geq 0$, zodat $m \mid p$, of nog, daar p priem is en $m > 1$, $m = p$. Dit is in contradictie met $m < p$. We concluderen dat $1 \leq m' < m$. Nu passen we opnieuw Lemma 4.2 toe, en bekomen zo

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \;=\; & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ & + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)^2 \\ & + (x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2)^2 \\ & + (x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1)^2.\end{aligned}$$

Het linkerlid is gelijk aan $m'pm^2$, terwijl het rechterlid deelbaar is door m^2; meer specifiek, het rechterlid is gelijk aan

$$m^2q_1^2+m^2q_2^2+m^2q_3^2+m^2q_4^2 = m^2(q_1^2+q_2^2+q_3^2+q_4^2)$$

voor zekere $q_1,q_2,q_3,q_4 \in \mathbb{Z}$. Dit komt omdat elk van de vier factoren binnen de kwadraten deelbaar is door m, vanwege onze specifieke keuze van y_i; immers $y_i \equiv x_i \mod m$ voor elke i. Zo hebben we voor de eerste factor bijvoorbeeld

$$x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2 = mp \equiv 0 \mod m.$$

We besluiten dat

$$m'p = q_1^2+q_2^2+q_3^2+q_4^2$$

een som van kwadraten is met $1 \leq m' < m$. Dit beëindigt het bewijs van Propositie 4.4. ■

Merk op dat dit resultaat op equivalente wijze ook als volgt geformuleerd kan worden: $\mathbb{N}$ is diophantisch in $\mathbb{Z}$. Inderdaad,

$$\mathbb{N} = \{a \in \mathbb{Z} \mid \phi(a) \text{ is waar in } \mathscr{D}_{\mathbb{Z}}\}$$

waarbij $\phi(x)$ de diophantische formule voorstelt met één vrije variabele x,

$$(\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)x_1^2+x_2^2+x_3^2+x_4^2 = x.$$

Tot slot hebben we volgend lemma, dat we nodig zullen hebben in Deel 3. Het is in essentie een rechtstreeks gevolg van de Vier-kwadratenstelling van Lagrange.

Lemma 4.5

Zij $x \in \mathbb{Q}$. Dan is $x \leq 0$ als en slechts als er $x_1,x_2,x_3,x_4 \in \mathbb{Q}$ bestaan zodat de vergelijking

$$x+x_1^2+x_2^2+x_3^2+x_4^2 = 0$$

geldt.

Bewijs. Definieer $x' := -x \in \mathbb{Q}$. Dan moeten we bewijzen dat $x' \geq 0$ als en slechts als er $x_1,x_2,x_3,x_4 \in \mathbb{Q}$ bestaan zodat

$$x_1^2+x_2^2+x_3^2+x_4^2 = x'.$$

De implicatie van rechts naar links is evident daar kwadraten in $\mathbb{R}$ steeds positief zijn. We bewijzen daarom de implicatie van links naar rechts. Schrijf $x' = \frac{a}{b}$ met $a \geq 0$ en $b > 0$ en bovendien $\text{ggd}(a,b) = 1$; dit is duidelijk altijd mogelijk. Door Propositie 4.4 twee keer toe te passen, op a en b respectievelijk, volgt dat er getallen $a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4 \in \mathbb{Z}$ bestaan, met bovendien b_1,b_2,b_3,b_4 niet allen gelijk aan nul, zodat

$$a = a_1^2+a_2^2+a_3^2+a_4^2, \quad b = b_1^2+b_2^2+b_3^2+b_4^2.$$

Wegens Lemma 4.2 geldt dat

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) &= (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2\\ &\quad +(a_1b_2-a_2b_1-a_3b_4+a_4b_3)^2\\ &\quad +(a_1b_3+a_2b_4-a_3b_1-a_4b_2)^2\\ &\quad +(a_1b_4-a_2b_3+a_3b_2-a_4b_1)^2.\end{aligned}$$

Bijgevolg, daar $b = b_1^2+b_2^2+b_3^2+b_4^2 \neq 0$, hebben we dat

$$\begin{aligned}x' &= \frac{a}{b}\\ &= \frac{a_1^2+a_2^2+a_3^2+a_4^2}{b_1^2+b_2^2+b_3^2+b_4^2}\\ &= \left(\frac{a_1b_1+a_2b_2+a_3b_3+a_4b_4}{b_1^2+b_2^2+b_3^2+b_4^2}\right)^2\\ &\quad +\left(\frac{a_1b_2-a_2b_1-a_3b_4+a_4b_3}{b_1^2+b_2^2+b_3^2+b_4^2}\right)^2\\ &\quad +\left(\frac{a_1b_3+a_2b_4-a_3b_1-a_4b_2}{b_1^2+b_2^2+b_3^2+b_4^2}\right)^2\\ &\quad +\left(\frac{a_1b_4-a_2b_3+a_3b_2-a_4b_1}{b_1^2+b_2^2+b_3^2+b_4^2}\right)^2\end{aligned}$$

een som is van vier kwadraten in $\mathbb{Q}$. Dit beëindigt het bewijs van Lemma 4.5. ■

4.2 Diophantische verzamelingen in $\mathbb{N}$

Volgende stelling is in feite evident.

Propositie 4.6

> *Eindige unies, doorsnedes, en Cartesische producten van diophantische verzamelingen in* $\mathbb{N}$ *zijn diophantisch in* $\mathbb{N}$.

Bewijs. Laat $A, B \subset \mathbb{N}^n$ twee diophantische verzamelingen zijn. Gemakkelijkheidshalve gebruiken we de informele notatie aan de hand van gehele veeltermen voor diophantische representaties, zoals uitgelegd in het commentaar na Definitie 2.5 en Definitie 2.11. Stel dus dat

$$A = \{(a_1,\ldots,a_n) \in \mathbb{N}^n \mid (\exists \vec{x} \in \mathbb{N}^{m_1})\, P_1(a_1,\ldots,a_n,\vec{x}) = 0\}$$

en

$$B = \{(b_1,\ldots,b_n) \in \mathbb{N}^n \mid (\exists \vec{y} \in \mathbb{N}^{m_2})\, P_2(b_1,\ldots,b_n,\vec{y}) = 0\}$$

voor zekere veeltermen P_1 en P_2 over $\mathbb{Z}$. Dan zijn

$$A \cap B = \{(c_1,\ldots,c_n) \in \mathbb{N}^n \mid$$

$$(\exists(\vec{x},\vec{y}) \in \mathbb{N}^{m_1+m_2})\, P_1^2(c_1,\ldots,c_n,\vec{x}) + P_2^2(c_1,\ldots,c_n,\vec{y}) = 0\}$$

en

$$A \cup B = \{(c_1,\ldots,c_n) \in \mathbb{N}^n \mid$$
$$(\exists(\vec{x},\vec{y}) \in \mathbb{N}^{m_1+m_2})\, P_1(c_1,\ldots,c_n,\vec{x}) \cdot P_2(c_1,\ldots,c_n,\vec{y}) = 0\}$$

diophantische verzamelingen. Bovendien is

$$A \times B = \{(c_1,\ldots,c_n,c_{n+1},\ldots,c_{2n}) \in \mathbb{N}^{2n} \mid$$
$$(\exists(\vec{x},\vec{y}) \in \mathbb{N}^{m_1+m_2})\, P_1^2(c_1,\ldots,c_n,\vec{x}) + P_2^2(c_{n+1},\ldots,c_{2n},\vec{y}) = 0\} \subset \mathbb{N}^{2n},$$

diophantisch in $\mathbb{N}$. Dit beëindigt het bewijs van Propositie 4.6. ■

Merk op dat hetzelfde resultaat natuurlijk ook voor $R = \mathbb{Z}$ geldt; inderdaad, precies hetzelfde bewijs gaat op. Maar zoals gezegd werken we steeds met $R = \mathbb{N}$ daar het bewijs van de onoplosbaarheid van Hilberts Tiende Probleem dan korter wordt.

In navolging van vorig resultaat kunnen we ons ook afvragen of diophantisch zijn gesloten is onder het nemen van complementen. Dit blijkt niet waar te zijn, maar dit is allesbehalve evident. Echter indien we de DPRM-stelling aannemen dan is dit wel eenvoudig in te zien, als volgt. Neem namelijk een verzameling $K \subset \mathbb{N}$ die recursief opsombaar maar niet berekenbaar is; uit Propositie 3.25 volgt dat zulk een verzameling bestaat. Propositie 3.22 impliceert dan dat K^c niet recursief opsombaar is. Daar recursief opsombaar hetzelfde betekent als diophantisch, wegens de DPRM-stelling, hebben we dat K diophantisch is en zijn complement K^c niet diophantisch is.

We geven in de volgende lijst van voorbeelden een handig overzicht van een aantal diophantische relaties in $\mathbb{N}$, telkens voorzien van een bewijs. We maken voortdurend gebruik van Propositie 4.6. Elke stap volgt uit de reeds bewezen vorige stappen.

Voorbeelden.

- $a \neq b \Leftrightarrow (a-b)^2 > 0 \Leftrightarrow (\exists x)\,(a-b)^2 = x+1$
- $a \leq b \Leftrightarrow (\exists x)\, a + x = b$
- $a < b \Leftrightarrow (\exists x)\, a + x + 1 = b$ $(\Leftrightarrow a \leq b \wedge a \neq b)$
- $a \,|\, b \Leftrightarrow (\exists x)\, ax = b$
- $a = \mathrm{rem}(b,c) \Leftrightarrow a < c \wedge c \,|\, b - a$
- $a \nmid b \Leftrightarrow \mathrm{rem}(b,a) > 0$
- $a = \left\lfloor \frac{b}{c} \right\rfloor \Leftrightarrow ac + \mathrm{rem}(b,c) = b$
- $a \equiv b \mod c \Leftrightarrow \mathrm{rem}(a,c) = \mathrm{rem}(b,c)$
- $a = \mathrm{ggd}(b,c) \Leftrightarrow b \neq 0 \wedge c \neq 0 \wedge a \,|\, b \wedge a \,|\, c \wedge (\exists x)(\exists y)\, a = bx - cy$
- $a = \mathrm{kgv}(b,c) \Leftrightarrow bc = a\,\mathrm{ggd}(b,c)$

- $a = \max(b,c) \Leftrightarrow (a = b \wedge b \geq c) \vee (a = c \wedge c > b)$
- $a = \min(b,c) \Leftrightarrow b + c = a + \max(b,c)$

Tot slot geven we nog een alternatieve karakterisering van diophantische verzamelingen in $\mathbb{N}$: een verzameling van natuurlijke getallen is diophantisch als en slechts als het de verzameling is van alle natuurlijke getalwaardes aangenomen door een zekere veelterm over $\mathbb{Z}$ wiens variabelen over de natuurlijke getallen lopen. Een meer precieze omschrijving volgt hieronder.

Propositie 4.7

Een verzameling $A \subset \mathbb{N}$ is diophantisch in $\mathbb{N}$ als en slechts

$$A = \{P(a_1,\ldots,a_n) \,|\, a_1,\ldots,a_n \in \mathbb{N} \text{ en } P(a_1,\ldots,a_n) \in \mathbb{N}\}$$

voor een gehele veelterm $P(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$.

Bewijs. Stel eerst dat we een gehele veelterm $P(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ gegeven hebben zodat

$$A = \{P(a_1,\ldots,a_n) \,|\, a_1,\ldots,a_n \in \mathbb{N} \text{ en } P(a_1,\ldots,a_n) \in \mathbb{N}\}.$$

Merk op dat deze verzameling gelijk is aan

$$\{a \in \mathbb{N} \,|\, (\exists \vec{x} \in \mathbb{N}^n)\, a - P(\vec{x}) = 0\}.$$

Bijgevolg is A diophantisch in $\mathbb{N}$.
Veronderstel omgekeerd dat A diophantisch is, zeg

$$A = \{a \in \mathbb{N} \,|\, (\exists \vec{x} \in \mathbb{N}^n)\, P(a,\vec{x}) = 0\}$$

voor een zekere veelterm $P(x_0,\vec{x}) \in \mathbb{Z}[x_0,\vec{x}]$. Definieer nu $Q(x_0,\vec{x}) \in \mathbb{Z}[x_0,\vec{x}]$ door

$$Q(x_0,\vec{x}) := (x_0+1)(1-(P(x_0,\vec{x}))^2) - 1.$$

We tonen dan aan dat

$$A = \{Q(a_0,a_1,\ldots,a_n) \,|\, a_0,a_1,\ldots,a_n \in \mathbb{N} \text{ en } Q(a_0,a_1,\ldots,a_n) \in \mathbb{N}\}.$$

Zij $a \in A$, dat wil zeggen er bestaan $x_1,\ldots,x_n \in \mathbb{N}$ zodat $P(a,x_1,\ldots,x_n) = 0$. Dan is inderdaad $Q(a,x_1,\ldots,x_n) = a$. Veronderstel aan de andere kant dat

$$a = Q(a_0,a_1,\ldots,a_n) \in \mathbb{N}$$

met $a_0,a_1,\ldots,a_n \in \mathbb{N}$. Dan is, per definitie van de veelterm Q,

$$a+1 = (a_0+1)(1-(P(a_0,a_1,\ldots,a_n))^2).$$

Dan moet $1-(P(a_0,a_1,\ldots,a_n))^2 > 0$, of nog, $1-(P(a_0,a_1,\ldots a_n))^2 \geq 1$. Bijgevolg is $P(a_0,a_1,\ldots,a_n) = 0$, dat wil zeggen $a_0 \in A$, en dus ook $a = a_0 \in A$. Dit beëindigt het bewijs van Propositie 4.7. ■

Dit resultaat zal het uiteindelijk mogelijk maken een gehele veelterm te construeren waarvan de natuurlijke getallen in het beeld precies de priemgetallen zijn, tenminste indien de variabelen over de natuurlijke getallen lopen. Immers, het zal blijken dat de verzameling van priemgetallen diophantisch is. Dit gevolg van de DPRM stelling werd door Hilary Putnam al in 1960 bedacht, nog voor Hilberts Tiende Probleem opgelost was.

Nog een paar eenvoudige hulpresultaten. Zij $A \subset \mathbb{N}^n$ diophantisch. Herinner dat dit, per definitie, wil zeggen dat er eenveelterm P over $\mathbb{Z}$ bestaat zodat

$$A = \{a \in \mathbb{N}^n \mid (\exists \vec{x} \in \mathbb{N}^m)\, P(a_1, \ldots, a_n, \vec{x}) = 0\}.$$

Merk op dat $m = 0$ hierbij toegelaten is; daarmee wordt dan bedoeld dat er geen existentiële kwantoren zijn.

Lemma 4.8

Een verzameling $A \subset \mathbb{N}^n$ is diophantisch als en slechts als

$$A = \{a \in \mathbb{N}^n \mid (\exists \vec{x} \in \mathbb{N}^m)\, P(a_1, \ldots, a_n, \vec{x}) = 0\}$$

voor een zekere veelterm P die waarden in $\mathbb{N}$ aanneemt.

Bewijs. Dit volgt meteen; indien we

$$P' : \mathbb{N}^{n+m} \to \mathbb{N} : (y_1, \ldots, y_1, x_1, \ldots, x_m) \mapsto (P(y_1, \ldots, y_1, x_1, \ldots, x_m))^2$$

definiëren, dan is

$$A = \{a \in \mathbb{N}^n \mid (\exists \vec{x} \in \mathbb{N}^m)\, P'(a_1, \ldots, a_n, \vec{x}) = 0\}.$$

Dit beëindigt het bewijs van Lemma 4.8. ■

Lemma 4.8 geeft ons dus dat iedere diophantische verzameling van over $\mathbb{N}$ gerepresenteerd kan worden door een veelterm die waardes in $\mathbb{N}$ aanneemt. Het is vaak handiger om deze voorwaarde te hebben.

Lemma 4.9

Zij $A \subset \mathbb{N}^n$ diophantisch. Dan is A recursief opsombaar.

Bewijs. Omwille van Lemma 4.8 mogen we veronderstellen dat A gerepresenteerd wordt door een veelterm over $\mathbb{Z}$ die waardes in $\mathbb{N}$ aanneemt, id est

$$A = \{a \in \mathbb{N}^n \mid (\exists \vec{x} \in \mathbb{N}^m)\, P(a_1, \ldots, a_n, \vec{x}) = 0\}$$

voor een zekere veelterm $P : \mathbb{N}^{n+m} \to \mathbb{N}$ over $\mathbb{Z}$. Het laatste voorbeeld na Definitie 3.10 zegt precies dat P primitief berekenbaar is; bijgevolg is A recursief opsombaar omwille van de karakterisatie van recursief opsombare verzamelingen gegeven in Lemma 3.16. Dit beëindigt het bewijs van Lemma 4.9. ■

HOOFDSTUK 5

EXPONENTIATIE IS DIOPHANTISCH

In dit hoofdstuk tonen we aan dat de grafiek van de exponentiële functie diophantisch is. We volgen hierbij de aanpak van Yuri Manin (1937), dewelke licht verschilt van de originele resultaten.

Het basisidee van Robinson blijft echter hetzelfde, en gaat als volgt. Ze toonde aan dat als we een bepaalde verzameling in $\mathbb{N}^2$ kunnen construeren die diophantisch is en de eigenschap heeft dat een van de twee coördinaten sneller groeit dan eender welke macht van de andere coördinaat, maar aan de andere kant trager dan exponentiële groei, dat we dan mogen concluderen dat *alle* recursief opsombare verzamelingen diophantisch zijn. Matiyasevich en Chudnovsky toonden uiteindelijk aan dat een zekere set die aan dit profiel beantwoordt diophantisch is. Ze gebruikten daarvoor de getallen van Fibonacci.

5.1 Een andere aanpak: de vergelijking van Pell

In plaats van met de getallen van Fibonacci te werken, werkt de aanpak van Manin met de vergelijking van Pell. We herhalen dit begrip eerst.

Definitie 5.1

Zij $d \in \mathbb{N}$ zodat d geen kwadraat is. De diophantische vergelijking

$$x^2 - dy^2 = 1$$

in de onbekenden $(x,y) \in \mathbb{N}^2$ wordt *de vergelijking van Pell met parameter d* genoemd.

Merk op dat de vergelijking van Pell twee triviale oplossingen heeft: indien $y = 0$ dan is $x^2 = 1$, zodat $(x,y) = (\pm 1, 0)$ voldoet. We zoeken dus steeds oplossingen $(x,y) \in \mathbb{N}^2$ waarvoor $y > 0$. Met betrekking tot de oplosbaarheid van de vergelijking van Pell hebben we volgende stelling.

Propositie 5.2

Zij $d \in \mathbb{N}$ zodat d geen kwadraat is. Dan bestaat er een $(x,y) \in \mathbb{N}^2$ met $y > 0$ zodat $x^2 - dy^2 = 1$.

Bewijs. We verwijzen naar Stelling 9.2.2 in [7]. ■

Of, anders gezegd, de vergelijking van Pell heeft steeds niet-triviale oplossingen. Merk op dat we voor zulk een oplossing hebben dat $x > 1$ en $y \neq 0$.

We kunnen wat ambitieuzer zijn, en *alle* oplossingen van de vergelijking van Pell proberen vinden. Dit kan, en dat volgt uit de volgende belangrijke stelling, die we wel aantonen. Het is eenvoudig in te zien dat uit Propositie 5.2 volgt dat er een unieke oplossing (x_1, y_1) van $x^2 - dy^2 = 1$ over $\mathbb{N}$ is met $x_1 > 1$ en $y_1 > 0$, zodat $x_1 + y_1\sqrt{d}$ minimaal is.

Propositie 5.3

> *Zij $d \in \mathbb{N}$ zodat d geen kwadraat is. Laat, met behulp van Propositie 5.2, de natuurlijke getallen $x_1 > 1$ en $y_1 > 0$ de unieke oplossing van $x^2 - dy^2 = 1$ over $\mathbb{N}_0$ zijn waarvoor $x_1 + y_1\sqrt{d}$ minimaal is. Dan geldt dat*
>
> $$\{(x_n, y_n) \in \mathbb{N}_0 \,|\, x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,\ n \in \mathbb{N}_0\}$$
>
> *de verzameling van alle oplossingen van $x^2 - dy^2 = 1$ over $\mathbb{N}_0$ is.*

Bewijs. We herhalen kort een aantal begrippen uit de getaltheorie, zoals bijvoorbeeld ingevoerd in [7]. Beschouw de ring $\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \sqrt{d}\mathbb{Z}$. Zulk een ring noemt men ook wel een *kwadratische ring*. Zij $z = x + y\sqrt{d}$ met $x, y \in \mathbb{Z}$ een willekeurig element van $\mathbb{Z}[\sqrt{d}]$. Op deze ring is een *conjugatie* gedefinieerd door

$$\bar{z} := x - y\sqrt{d} \in \mathbb{Z}[\sqrt{d}],$$

en een *norm* door

$$N(z) := \bar{z}z = (x - y\sqrt{d})\,(x + y\sqrt{d}) = x^2 - dy^2 \in \mathbb{Z}.$$

Met deze terminologie voor handen is hetgeen we moeten aantonen equivalent met het zoeken van alle elementen $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ waarvoor $N(z) = x^2 - dy^2 = 1$. Zij nu $z_0 := x_1 + y_1\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Merk op dat

$$z_0 = x_1 + y_1\sqrt{d} > 1 + y_1\sqrt{d} > 1 + 0 = 1.$$

We gebruiken nu volgend lemma.

Lemma 5.4

> *De elementen $z \in \mathbb{Z}[\sqrt{d}]$ met $N(z) = 1$ worden gegeven door $z = \pm z_0^n$, $n \in \mathbb{Z}$.*

Bewijs. We moeten aantonen dat

$$\{z \in \mathbb{Z}[\sqrt{d}] \,|\, N(z) = 1\} = \{\pm z_0^n \,|\, n \in \mathbb{Z}\}.$$

Stel dat $z \in \mathbb{Z}[\sqrt{d}]$ zodat $N(z) = 1$; veronderstel bovendien zonder verlies van algemeenheid dat $z > 0$, want als $z < 0$ dan levert $z' := -z > 0$ dat $N(z') = N(z) = 1$. De

inclusie hierboven impliceert dan dat $z' = \pm z_0^n$ voor een zekere $n \in \mathbb{Z}$, zodat eveneens $z = -z' = \mp z_0^n \in \{\pm z_0^n \,|\, n \in \mathbb{Z}\}$.
Daar $z_0 > 1$ bestaat er een uniek getal $k \in \mathbb{Z}$ zodat $z_0^k \leq z < z_0^{k+1}$; inderdaad, dit kan men inzien als volgt. Zij

$$G := \{k \in \mathbb{Z} \,|\, z_0^k \leq z\}.$$

Omdat $z_0 > 1$ en $z > 0$ heeft G een maximum, zeg $k \in G$. Dan is $k+1 \notin G$, id est $z_0^{k+1} > z$, dus $z_0^k \leq z < z_0^{k+1}$. Duidelijk is zulk een getal uniek, want stel dat ook $k' \neq k$ voldoet, dat wil zeggen $z_0^{k'} \leq z < z_0^{k+1}$. Dan is $k' \in G$, zodat $k > k'$ daar k het maximum van G is, of nog, $k \geq k' + 1$. Bijgevolg bekomen we de contradictie

$$z_0^{k'+1} > z \geq z_0^k \geq z_0^{k'+1}.$$

Dit toont dat er een uniek getal $k \in \mathbb{Z}$ is zodat $z_0^k \leq z < z_0^{k+1}$.
Voor het getal $z' := z z_0^{-k}$ geldt dat

$$z_0^k \leq z < z_0^{k+1} \quad \Rightarrow \quad 1 \leq z z_0^{-k} = z' < z_0$$

en ook

$$N(z') = N(z z_0^{-k}) = N(z) N(z_0^{-k}) = N(z) N(z_0)^{-k} = 1.$$

Bijgevolg impliceert de minimaliteit van z_0 dat $z_1 = 1$, dat wil zeggen we hebben $z = z_0^k \in \{\pm z_0^n \,|\, n \in \mathbb{Z}\}$. Daar de omgekeerde inclusie evident is zijn we klaar. Dit beëindigt het bewijs van Lemma 5.4. ■

Hiermee tonen we nu de te bewijzen gelijkheid uit Propositie 5.3 aan. Zij $x, y \in \mathbb{N}_0$ dus oplossingen van $x^2 - dy^2 = 1$. Dan is $N(x + y\sqrt{d}) = x^2 - dy^2 = 1$, zodat uit Lemma 5.4 en het feit dat $x + y\sqrt{d} > 1$ volgt dat er een $n \in \mathbb{N}_0$ bestaat zodat

$$x + y\sqrt{d} = z_0^n = (x_1 + y_1\sqrt{d})^n.$$

Dan is inderdaad

$$(x, y) \in \{(x_n, y_n) \in \mathbb{N}_0 \,|\, x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,\ n \in \mathbb{N}_0\}.$$

Omgekeerd, stel dat $(x_n, y_n) \in \mathbb{N}_0$ zulk een koppel is waarvoor

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Dan hebben we

$$x_n^2 - dy_n^2 = N(x_n + y_n\sqrt{d}) = N((x_1 + y_1\sqrt{d})^n) = (N(x_1 + y_1\sqrt{d}))^n = (x_1^2 - dy_1^2)^n = 1.$$

Dit beëindigt het bewijs van Propositie 5.3. ■

Definitie 5.5

> Voor $n \in \mathbb{N}_0$ noemt men de getallen (x_n, y_n) in de formulering van vorige stelling het *n-de paar van oplossingen* van de vergelijking $x^2 - dy^2 = 1$ over $\mathbb{N}_0$.

In de constructie van Manin bekijken we de vergelijking

$$x^2 - (a^2-1)y^2 = 1,$$

id est $d = a^2 - 1$ voor een $a \in \mathbb{N}_0$. Indien $a = 1$ dan krijgen we opnieuw een triviale vergelijking, dus we zullen meestal $a > 1$ veronderstellen. Merk op dat $a^2 - 1$ dan geen kwadraat kan zijn; immers, zou $a^2 - 1 = n^2$ voor een $n \in \mathbb{N}$, dan ook

$$(a-n)(a+n) = a^2 - n^2 = 1.$$

Dan moet $a - n = 1$ en $a + n = 1$, hetgeen $n = 0$ en dus $a = 1$ impliceert, contradictie.

Lemma 5.6

Zij $a \in \mathbb{N}$ met $a > 1$. De oplossingen van de vergelijking $x^2 - (a^2-1)y^2 = 1$ in $\mathbb{N}_0$ zijn gegeven door

$$x + y\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n,$$

voor iedere $n \in \mathbb{N}_0$.

Bewijs. We bepalen eerst de minimale oplossing. Er geldt

$$a^2 - (a^2-1)\,1^2 = 1,$$

dat wil zeggen $(a,1)$ is een oplossing; het is bovendien duidelijk dat $(x,y) = (a,1)$ de oplossing van $x^2 - (a^2-1)y^2 = 1$ over $\mathbb{N}_0$ is waarvoor $x + y\sqrt{a^2-1}$ het kleinst is. Inderdaad, sowieso is $y \geq 1$, dus $y = 1$ is zo klein mogelijk. Dan is

$$x^2 = 1 + (a^2-1)y^2 \geq 1 + (a^2-1) = a^2,$$

zodat $x \geq a$ daar x een natuurlijk getal is. Alle oplossingen $(x,y) \in \mathbb{N}_0$ van de vergelijking zijn dus, omwille van Propositie 5.3, impliciet gegeven door

$$x + y\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n,$$

voor elke $n \in \mathbb{N}_0$. Dit beëindigt het bewijs van Lemma 5.6. ■

Definitie 5.7

Zij $a \in \mathbb{N}$ met $a > 1$, en $n \in \mathbb{N}_0$. Dan zijn $x_n(a)$ en $y_n(a)$ respectievelijk de projectie op de eerste coördinaat en de projectie op de tweede coördinaat van het n-de paar van oplossingen van de vergelijking $x^2 - (a^2-1)y^2 = 1$ over $\mathbb{N}_0$. We noemen de rij $(y_n(a))_{n\in\mathbb{N}_0}$ in $\mathbb{N}_0$ de *a-rij*. Ook definiëren we $x_n(1) := 1$ en $y_n(1) := n$ voor elke $n \in \mathbb{N}_0$.

Wegens Lemma 5.6 geldt dat $x_n(a)$ en $y_n(a)$ voldoen aan

$$x_n(a) + y_n(a)\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n.$$

Het is niet moeilijk om met behulp van dit lemma expliciete uitdrukkingen voor $x_n(a)$ en $y_n(a)$ te vinden. Wij hebben voorlopig echter genoeg aan het volgende: de formule hierboven voor $n+1$ ingevuld geeft

$$\begin{aligned} x_{n+1}(a)+y_{n+1}(a)\sqrt{a^2-1} &= (a+\sqrt{a^2-1})^{n+1} \\ &= (a+\sqrt{a^2-1})\,(a+\sqrt{a^2-1})^n \\ &= (a+\sqrt{a^2-1})\,(x_n(a)+y_n(a)\sqrt{a^2-1}), \end{aligned}$$

zodat

$$x_{n+1}(a)+y_{n+1}(a)\sqrt{a^2-1} = \big(ax_n(a)+(a^2-1)y_n(a)\big)+(x_n(a)+ay_n(a))\sqrt{a^2-1}$$

de geldigheid impliceert van de recursievergelijkingen

$$\begin{cases} x_{n+1}(a) = ax_n(a)+(a^2-1)y_n(a) \\ y_{n+1}(a) = x_n(a)+ay_n(a) \end{cases}.$$

Merk op dat hier meteen uit volgt dat, voor elk natuurlijk getal $a>1$, de rijen $(x_n(a))_{n\in\mathbb{N}_0}$ en $(y_n(a))_{n\in\mathbb{N}_0}$ strikt stijgend zijn; immers

$$x_{n+1}(a) = ax_n(a)+(a^2-1)y_n(a) \geq ax_n(a) > x_n(a),$$

$$y_{n+1}(a) = x_n(a)+ay_n(a) \geq ay_n(a) > y_n(a).$$

Aan de a-rij associëren we nu een relatie in drie variabelen, als volgt.

Definitie 5.8

De relatie

$$y = y_n(a), \quad a>1, \quad n\geq 1$$

in de variabelen (y,a,n) noemen we de *a-rij relatie*.

In het laatste deel van deze sectie tonen we aan dat, om aan te tonen dat exponentiatie diophantisch is, het volstaat te bewijzen dat de a-rij relatie diophantisch is. Dat is precies de inhoud van volgend lemma.

Propositie 5.9

Indien de a-rij relatie diophantisch is, dan is ook de relatie

$$m = a^n, \quad n\geq 1$$

in de variabelen (m,a,n) diophantisch.

Bewijs. Zij

$$G := \{(m,a,n)\in\mathbb{N}^3 \mid m=a^n \text{ en } n\geq 1\}.$$

Dan moeten we aantonen dat G diophantisch is. Het is duidelijk dat het volstaat te bewijzen dat G' diophantisch is, met

$$G' := G\cap\{(m,a,n)\in\mathbb{N}^3 \mid a>1\} = \{(m,a,n)\in\mathbb{N}^3 \mid m=a^n,\ n\geq 1,\ a>1\}.$$

Inderdaad, als $a = 1$ dan reduceert hetgeen te bewijzen is zich tot een trivialiteit.

Lemma 5.10

Indien $a > 1$ dan gelden de ongelijkheden

$$(2a-1)^n \leq y_{n+1}(a) \leq (2a)^n$$

voor alle $n \geq 1$.

Bewijs. We bewijzen dit resultaat per inductie op $n \geq 1$. Eerst het geval $n = 1$; we hebben

$$(a+\sqrt{a^2-1})^2 = a^2+a^2-1+2a\sqrt{a^2-1} = (2a^2-1)+2a\sqrt{a^2-1},$$

zodat $y_2(a) = 2a$. Dan geldt inderdaad $2a-1 \leq 2a \leq 2a$. Veronderstel nu dat de vergelijking

$$(2a-1)^n \leq y_{n+1}(a) \leq (2a)^n$$

geldt; we bewijzen ze dan met n vervangen door $n+1$. Door de recursierelatie voor $y_n(a)$ toe te passen vinden we

$$y_{n+2}(a) = ay_{n+1}(a)+x_{n+1}(a) = \left(a+\frac{x_{n+1}(a)}{y_{n+1}(a)}\right) y_{n+1}(a).$$

Omdat $(x_{n+1}(a), y_{n+1}(a))$ voldoet aan de vergelijking van Pell, is

$$\frac{x_{n+1}(a)}{y_{n+1}(a)} = \sqrt{a^2-1+\frac{1}{y_{n+1}(a)^2}} < \sqrt{a^2-1+1} = \sqrt{a^2} = a.$$

Ook is, daar $a > 1$,

$$a-1 = \sqrt{(a-1)^2} = \sqrt{a^2-1+2-2a} < \sqrt{a^2-1} < \sqrt{a^2-1+\frac{1}{y_{n+1}(a)^2}}.$$

We concluderen dat

$$\begin{aligned}
(2a-1)^{n+1} &= (2a-1)(2a-1)^n \\
&\leq (2a-1)\,y_{n+1}(a) \\
&= (a+(a-1))\,y_{n+1}(a) \\
&< \left(a+\sqrt{a^2-1+\frac{1}{y_{n+1}(a)^2}}\right) y_{n+1}(a) \\
&= \left(a+\frac{x_{n+1}(a)}{y_{n+1}(a)}\right) y_{n+1}(a) \\
&= y_{n+2}(a) \\
&< (a+a)\,y_{n+1}(a) \\
&\leq (2a)(2a)^n \\
&= (2a)^{n+1}.
\end{aligned}$$

Dit beëindigt het bewijs van Lemma 5.10. ■

Daar $a > 1$ volgt uit Lemma 5.10 dat $(2a-1)^n \leq y_{n+1}(a) \leq (2a)^n$ voor elke $n \geq 1$. Voor elke $N \geq 1$ hebben we dan

$$a^n \left(1 - \frac{1}{2Na}\right)^n = \frac{(2Na-1)^n}{(2N)^n} \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq \frac{(2Na)^n}{(2N-1)^n} = a^n \frac{1}{\left(1-\frac{1}{2N}\right)^n}$$

wegens Lemma 5.10. Intuïtief redeneren we als volgt: voor N "groot genoeg" impliceren bovenstaande ongelijkheden dat

$$a^n = \left\lfloor \frac{y_{n+1}(Na)}{y_{n+1}(N)} + c \right\rfloor,$$

waarbij c een zeker vast getal is. Meer precies tonen wij aan dat, voor N groot genoeg,

$$a^n = \left\lfloor \frac{y_{n+1}(Na)}{y_{n+1}(N)} + \frac{1}{2} \right\rfloor.$$

Definieer

$$G'' := \{(m,a,n,N) \in \mathbb{N}^4 \,|\, 0 \leq 2y_{n+1}(Na) + y_{n+1}(N) - 2y_{n+1}(N)m < 2y_{n+1}(N), \\ n \geq 1, \quad a > 1, \quad N > B\}.$$

Hierbij is B een nog nader te bepalen uitdrukking die groot genoeg en bovendien diophantisch is.
We gaan nu op zoek naar zulk een geschikte B; veronderstel daartoe alvast $N \geq n$. Het binomium van Newton geeft

$$\left(1 - \frac{1}{2Na}\right)^n = \sum_{k=0}^{n} (-1)^k \left(\frac{1}{2Na}\right)^k = 1 + \sum_{k=1}^{n} (-1)^k \left(\frac{1}{2Na}\right)^k \geq 1 + \sum_{k=1}^{n} \left(-\frac{1}{2Na}\right),$$

zodat

$$\left(1 - \frac{1}{2Na}\right)^n \geq 1 - \frac{n}{2Na}.$$

Analoog is

$$\frac{1}{\left(1-\frac{1}{2N}\right)^n} \leq \frac{1}{\left(1-\frac{n}{2N}\right)} \leq 1 + \frac{n}{N},$$

daar

$$N \geq n \quad \Rightarrow \quad \left(1 - \frac{n}{2N}\right)\left(1 + \frac{n}{N}\right) = 1 + \frac{n}{N} - \frac{n}{2N} - \frac{n^2}{2N^2} = 1 + \frac{n}{2N}\left(1 - \frac{n}{N}\right) \geq 1.$$

Hierboven hadden we al de ongelijkheden

$$a^n \left(1 - \frac{1}{2Na}\right)^n \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq a^n \frac{1}{\left(1-\frac{1}{2N}\right)^n}$$

gevonden. Samen met de zojuist bekomen ongelijkheden levert dit

$$a^n \left(1 - \frac{n}{2Na}\right) \leq a_n \left(1 - \frac{1}{2Na}\right)^n \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq a^n \frac{1}{\left(1-\frac{1}{2N}\right)^n} \leq a_n \left(1 + \frac{n}{N}\right),$$

of equivalent,

$$a^n - \frac{a^n n}{2Na} \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq a_n + \frac{a^n n}{N}.$$

Indien we $N > 2na^n$ nemen, dan geldt

$$N > 2na^n,\ a > 1 \quad \Rightarrow \quad N > 2na^n = 2a(na^{n-1}) > na^{n-1} \quad \Rightarrow \quad \frac{a^n n}{2Na} < \frac{1}{2}.$$

De conclusie is dat de keuze van N als $N > 2na^n$ de ongelijkheden

$$a^n - \frac{1}{2} < a^n - \frac{a^n n}{2Na} \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq a^n + \frac{a^n n}{N} < a^n + \frac{1}{2}$$

oplevert. En dat is precies wat we wilden, want dan is inderdaad

$$a^n = \left\lfloor \frac{y_{n+1}(Na)}{y_{n+1}(N)} + \frac{1}{2} \right\rfloor.$$

Maar

$$y_{n+1}(a) \geq (2a-1)^n \geq a^n$$

geeft ons dat het volstaat $N > 2ny_{n+1}(a)$, id est $B := 2ny_{n+1}(a)$, te nemen; inderdaad, dan is

$$N > 2ny_{n+1}(a) \geq 2na^n.$$

Merk op dat deze relatie inderdaad, per onze hypothese van de stelling, diophantisch is.
We zijn nu bijna klaar. Zij dus

$$G'' := \{(m,a,n,N) \in \mathbb{N}^4 \,|\, 0 \leq 2y_{n+1}(Na) + y_{n+1}(N) - 2y_{n+1}(N)m < 2y_{n+1}(N), \\ n \geq 1, \quad a > 1, \quad N > 2ny_{n+1}(a)\}.$$

Wegens hetgeen we zopas aangetoond hebben geldt dat G' de projectie van G'' op zijn eerste 3 coördinaten is. En G'' is diophantisch als doorsnede van diophantische verzamelingen; merk op dat we hier de hypothese van de stelling gebruiken, namelijk dat de relatie $z = y_n(a), a > 1$ in de variabelen (z,a,n) diophantisch is. Omdat een projectie van een diophantische verzameling opnieuw diophantisch is, zijn we klaar. Dit beëindigt het bewijs van Propositie 5.9. ■

5.2 De a-rij relatie is diophantisch

We beginnen met meer expliciete uitdrukkingen voor $x_n(a)$ en $y_n(a)$ af te leiden.

Lemma 5.11

Zij $a \in \mathbb{N}$ een natuurlijk getal. Dan gelden de uitdrukkingen

$$\begin{aligned} x_n(a) &= a^n + \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{2k} a^{n-2k}(a^2-1)^k, \\ y_n(a) &= \sum_{k=1}^{\lfloor (n+1)/2 \rfloor} \binom{n}{2k-1} a^{n-2k+1}(a^2-1)^{k-1}, \end{aligned}$$

voor alle $n \in \mathbb{N}_0$, waarbij het onderverstaan is dat de som in de eerste uitdrukking gelijk is aan 0 indien $n = 1$.

Bewijs. Merk op dat de uitspraak ook het geval $a = 1$ toelaat; maar het bewijs hiervan volgt meteen, want bovenstaande uitdrukking zegt dat $x_n(1) = 1$ en $y_n(1) = \binom{n}{1} = n$ voor alle $n \in \mathbb{N}_0$, en dat is inderdaad precies waar wegens Definitie 5.7. Veronderstel vanaf nu dus $a > 1$. We tonen de uitdrukkingen aan door gezamenlijke inductie op $(x_n(a), y_n(a))$. De uitdrukkingen zijn waar voor $n = 1$, want we weten dat

$$x_1(a) = a = a^1 + 0,$$

daar de som in de uitdrukking voor $x_n(a)$ gelijk aan 0 wordt onderstaan in het geval $n = 1$, en ook

$$y_1(a) = 1 = \binom{1}{1} a^0 (a^2-1)^0 = \sum_{k=1}^{\lfloor (1+1)/2 \rfloor} \binom{1}{2k-1} a^{1-2k+1}(a^2-1)^{k-1}.$$

Als we de recursievergelijkingen

$$\begin{cases} x_{n+1}(a) = a x_n(a) + (a^2-1) y_n(a) \\ y_{n+1}(a) = x_n(a) + a y_n(a) \end{cases}$$

gebruiken, en aannemen dat beide formules in de formulering van de stelling gelden voor n, dan is

$$\begin{aligned} x_{n+1}(a) &= a\left(a^n + \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{2k} a^{n-2k}(a^2-1)^k\right) \\ &\quad + (a^2-1) \sum_{k=1}^{\lfloor (n+1)/2 \rfloor} \binom{n}{2k-1} a^{n-2k+1}(a^2-1)^{k-1} \\ &= a^{n+1} + \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{2k} a^{n+1-2k}(a^2-1)^k \\ &\quad + \sum_{k=1}^{\lfloor (n+1)/2 \rfloor} \binom{n}{2k-1} a^{n-2k+1}(a^2-1)^k \end{aligned}$$

Het is niet moeilijk in te zien dat

$$\left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{n}{2} + \frac{1}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{als } n \text{ even is} \\ \frac{n+1}{2} & \text{als } n \text{ oneven is} \end{cases}.$$

Veronderstel eerst dat n even is. Dan is

$$\begin{aligned} x_{n+1}(a) &= a^{n+1} + \sum_{k=1}^{n/2} \binom{n}{2k} a^{n+1-2k}(a^2-1)^k \\ &\quad + \sum_{k=1}^{n/2} \binom{n}{2k-1} a^{n+1-2k}(a^2-1)^k \\ &= a^{n+1} + \sum_{k=1}^{n/2} \left(\binom{n}{2k} + \binom{n}{2k-1} \right) a^{n+1-2k}(a^2-1)^k. \end{aligned}$$

Uit de gekende relatie tussen de binomiaalcoëfficiënten weten we dat

$$\binom{n}{2k-1} + \binom{n}{2k} = \binom{n+1}{2k},$$

zodat

$$\begin{aligned} x_{n+1}(a) &= a^{n+1} + \sum_{k=1}^{n/2} \binom{n+1}{2k-1} a^{n+1-2k}(a^2-1)^k \\ &= a^{n+1} + \sum_{k=1}^{\lfloor (n+1)/2 \rfloor} \binom{n+1}{2k} a^{n+1-2k}(a^2-1)^k. \end{aligned}$$

Dit bewijst de uitdrukking indien n even is. Veronderstel anderzijds dat n oneven is. Dan is

$$\left\lfloor \frac{n+1}{2} \right\rfloor = \frac{n+1}{2}, \quad \left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}.$$

Dus hebben we

$$\begin{aligned}
x_{n+1}(a) &= a^{n+1} + \sum_{k=1}^{(n-1)/2} \binom{n}{2k} a^{n+1-2k}(a^2-1)^k \\
&\quad + \sum_{k=1}^{(n+1)/2} \binom{n}{2k-1} a^{n+1-2k}(a^2-1)^k \\
&= a^{n+1} + \sum_{k=1}^{(n-1)/2} \left(\binom{n}{2k} + \binom{n}{2k-1} \right) a^{n+1-2k}(a^2-1)^k \\
&\quad + \binom{n}{2\frac{n+1}{2}-1} a^{n+1-2\frac{n+1}{2}} (a^2-1)^{\frac{n+1}{2}} \\
&= a^{n+1} + \sum_{k=1}^{(n-1)/2} \binom{n+1}{2k} a^{n+1-2k}(a^2-1)^k + (a^2-1)^{\frac{n+1}{2}} \\
&= a^{n+1} + \sum_{k=1}^{(n+1)/2} \binom{n+1}{2k} a^{n+1-2k}(a^2-1)^k \\
&\quad - \binom{n+1}{2\frac{n+1}{2}} a^{n+1-2\frac{n+1}{2}} (a^2-1)^{\frac{n+1}{2}} + (a^2-1)^{\frac{n+1}{2}} \\
&= a^{n+1} + \sum_{k=1}^{(n+1)/2} \binom{n+1}{2k} a^{n+1-2k}(a^2-1)^k - (a^2-1)^{\frac{n+1}{2}} + (a^2-1)^{\frac{n+1}{2}} \\
&= a^{n+1} + \sum_{k=1}^{\lfloor (n+1)/2 \rfloor} \binom{n+1}{2k} a^{n+1-2k}(a^2-1)^k.
\end{aligned}$$

Zo volgt de conclusie. De uitdrukking voor $y_{n+1}(a)$ wordt op een volledig analoge wijze bekomen. Dit beëindigt het bewijs van Lemma 5.11. ■

Volgend resultaat is cruciaal.

Propositie 5.12

De a-rij relatie

$$y = y_n(a), \quad a > 1, \quad n \geq 1$$

in de variabelen (y,a,n) is diophantisch.

Bewijs. Zij

$$G := \{(y,a,n) \in \mathbb{N}^3 \mid y = y_n(a),\ a > 1,\ n \geq 1\}.$$

Dan moeten we aantonen dat G diophantisch is. Definieer deelverzamelingen van $\mathbb{N}^9$

door

$$\begin{aligned}
G_1 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid y \geq n,\ n \geq 1,\ a > 1\},\\
G_2 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid x^2 - (a^2-1)y^2 = 1\},\\
G_3 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid v \equiv 0 \mod 4y^2\},\\
G_4 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid u^2 - (a^2-1)v^2 = 1,\ v \geq 1\},\\
G_5 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid b = a + u^2(u^2-a)\},\\
G_6 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid s^2 - (b^2-1)t^2 = 1,\ t \geq 1\},\\
G_7 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid s \equiv x \mod u\},\\
G_8 &:= \{(y,a,n,x,u,v,b,s,t) \in \mathbb{N}^9 \mid t \equiv n \mod 4y\}.
\end{aligned}$$

Uit alles wat we tot nog toe gezien hebben over diophantische verzamelingen weten we dat elk van deze verzamelingen diophantisch is; bijgevolg is ook

$$G' := G_1 \cap G_2 \cap G_3 \cap G_4 \cap G_5 \cap G_6 \cap G_7 \cap G_8$$

diophantisch. We beweren nu dat G precies gelijk is aan de projectie van de diophantische verzameling G' op zijn eerste drie coördinaten. Inderdaad, we hebben de volgende lemma's.

Lemma 5.13

De verzameling G is een deel van de projectie van G' op zijn eerste drie coördinaten.

Bewijs. Neem $(y,a,n) \in G$, dat wil zeggen $(y,a,n) \in \mathbb{N}^3$ en $y = y_n(a)$ met $a > 1$ en $n \geq 1$. We moeten $x,u,v,b,s,t \in \mathbb{N}$ vinden zodat $(y,a,n,x,u,v,b,s,t) \in G_i$ voor alle $i \in \{1,2,\ldots,8\}$, zodat er voldaan is aan elk van de acht bovenstaande definiërende vergelijkingen.
Merk ten eerste op dat voor alle $m \in \mathbb{N}_0$ geldt dat $y_m(a) \geq m$; dit volgt door inductie, want $y_1(a) = 1 \geq 1$, en

$$y_{m+1}(a) > y_m(a) \geq m,$$

omdat we weten dat de rij $(y_m)_{m\in\mathbb{N}_0}$ strikt stijgend is. In het bijzonder hebben we dat $y = y_n(a) \geq n$. Aan de vergelijking van G_1 is dus al voldaan. Per definitie is

$$x_n(a)^2 - (a^2-1)y_n(a)^2 = 1.$$

Definieer $x := x_n(a) \in \mathbb{N}$. Omdat $y = y_n(a)$ is dus ook voldaan aan

$$x^2 - (a^2-1)y^2 = 1,$$

id est de definiërende vergelijking van G_2.
Beschouw de vergelijking van Pell met parameter $(a^2-1)(4y^2)$, namelijk

$$X^2 - (a^2-1)(4y^2)^2Y^2 = 1.$$

Merk op dat $(a^2-1)(4y^2)^2$ geen kwadraat is daar a^2-1 geen kwadraat is omdat $a>1$. Uit Propositie 5.2 volgt dat er een oplossing $(u',v') \in \mathbb{N}^2$ is met $v'>0$ zodat aan deze vergelijking voldaan is, dat wil zeggen

$$u'^2-(a^2-1)(4y^2)v'^2=1.$$

Definieer nu $u:=u' \in \mathbb{N}$ en $v:=4y^2v' \in \mathbb{N}$. Dan is $v=4y^2v' \equiv 0 \mod 4y^2$, zodat aan de vergelijking van G_3 voldaan is. Maar ook hebben we per constructie dat

$$u^2-(a^2-1)v^2=u'^2-(a^2-1)(4y^2)^2v'^2=1.$$

Dus ook aan G_4 is voldaan. Definieer $b:=a+u^2(u^2-a)$. We willen dat b een natuurlijk getal is; duidelijk is dat $b \in \mathbb{Z}$, en omdat

$$v \geq 1 \quad \Rightarrow \quad 1=u^2-(a^2-1)v^2 \leq u^2-(a^2-1)=u^2-a^2+1 \quad \Rightarrow \quad u^2 \geq a^2,$$

geldt, daar $a>1$, dat

$$b=a+u^2(u^2-a) \geq a+a^2(a^2-a)=a(1+a^2(a-1))>a>1,$$

id est inderdaad $b \in \mathbb{N}$ en, meer nog, zelfs $b>1$. Dan is er voldaan aan de vergelijking in G_5. Omdat $b>1$ is b^2-1 geen kwadraat. Zij $s:=x_n(b) \in \mathbb{N}$ en $t:=y_n(b) \in \mathbb{N}$. Merk op dat $t \geq 1$. Dan zijn s en t dus de respectievelijke x- en y-componenten van het n-de paar van oplossingen van de vergelijking $x^2-(b^2-1)y^2=1$. In het bijzonder is $s^2-(b^2-1)t^2=1$, zodat aan de definiërende vergelijking van G_6 is voldaan. Rest ons nu enkel nog na te gaan dat ook aan de vergelijkingen van G_7 en G_8 voldaan is. Merk op dat voor alle $i,j \in \mathbb{N}$ met $i>j$ de congruentie

$$x_n(i)-x_n(j) \equiv 0 \mod i-j$$

geldt; inderdaad, voor eender welk natuurlijk getal m geldt $i-j \mid i^m-j^m$, dat wil zeggen $i^m \equiv j^m \mod i-j$, dus

$$\begin{aligned} x_n(i)-x_n(j) &= (i^n-j^n)+\sum_{k=1}^{\lfloor n/2 \rfloor}\binom{n}{2k}(i^{n-2k}(i^2-1)^k-j^{n-2k}(j^2-1)^k) \\ &\equiv (i^n-i^n)+\sum_{k=1}^{\lfloor n/2 \rfloor}\binom{n}{2k}(i^{n-2k}(i^2-1)^k-i^{n-2k}(i^2-1)^k) \\ &\equiv 0 \mod i-j. \end{aligned}$$

Maar in het bijzonder zijn $b,a \in \mathbb{N}$ met $b>a$, zodat $x_n(b) \equiv x_n(a) \mod b-a$. Daar $b-a=u^2(u^2-a)$ geeft dit

$$s=x_n(b) \equiv x_n(a)=x \mod u^2(u^2-a) \quad \Rightarrow \quad s \equiv x \mod u.$$

Dus is ook aan de vergelijking in G_7 voldaan. Tenslotte, omdat $4y \mid 4y^2$ geeft de vergelijking van G_3, namelijk $v \equiv 0 \mod 4y^2$, ons dat $v \equiv 0 \mod 4y$. De vergelijkingen in G_4 gesubstitueerd in die van D_5 geeft

$$b=a+(1-(a^2-1)v^2)(1+(a^2-1)v^2-a).$$

Modulo $4y$ krijgen we

$$b \equiv a + (1-0)(1+0-a) = a + (1-a) = 1 \mod 4y,$$

of nog, $4y \mid b-1$. Identiek zoals we hierboven al hadden voor de x-component, hebben we ook voor alle $i, j \in \mathbb{N}$ met $i > j$ de congruentie $y_n(i) - y_n(j) \equiv 0 \mod i-j$. In het bijzonder voor de natuurlijke getallen $b > 1$ geldt $y_n(b) \equiv y_n(1) \mod b-1$. Maar $y_n(1) = n$ wegens Definitie 5.7, zodat $y_n(b) \equiv n \mod b-1$. Omdat $4y \mid b-1$ impliceert dit

$$t = y_n(b) \equiv n \mod 4y.$$

Dit toont aan dat ook aan de vergelijking in G_8 voldaan is. Bijgevolg geldt dat (y,a,n,x,u,v,b,s,t) een element van de projectie van G' op zijn eerste drie coördinaten is. Dit beëindigt het bewijs van Lemma 5.13. ■

Lemma 5.14

De projectie van G' op zijn eerste drie coördinaten is een deel van G.

Bewijs. Zij $(y,a,n) \in \mathbb{N}^3$ en $x,u,v,b,s,t \in \mathbb{N}$ gegeven zodat aan al de vergelijkingen D_i is voldaan, met $i \in \{1,2,\ldots,8\}$. We moeten aantonen dat $y = y_n(a)$, id est dat y de tweede coördinaat is van het n-de paar van oplossingen van de vergelijking

$$X^2 - (a^2-1)Y^2 = 1.$$

De vergelijking in G_2 zegt dat $x^2 - (a^2-1)y^2 = 1$; stel dat (x,y) het N-de paar van oplossingen van de vergelijking $X^2 - (a^2-1)Y^2 = 1$ is. Hetgeen we moeten bewijzen is dan precies dat $N = n$; inderdaad, dan is $y = y_N(a) = y_n(a)$. Analoog, stel dat (u,v) het N'-de paar van oplossingen van die vergelijking is. Stel tot slot dat (s,t) het N_b-de paar van oplossingen is van de vergelijking

$$X^2 - (b^2-1)Y^2 = 1.$$

Bijgevolg hebben we, per constructie,

$$(x,y) = (x_N(a), y_N(a)), \quad (u,v) = (x_{N'}(a), y_{N'}(a)), \quad (s,t) = (x_{N_b}(b), y_{N_b}(b)).$$

Merk op dat sowieso $N \geq 1$, $N' \geq 1$ en $N_b \geq 1$. In het bewijs van de andere inclusie hadden we al aangetoond dat de vergelijkingen in G_4 en G_5 impliceren dat $4y \mid b-1$. Uit de vergelijking in G_3 volgt dat $v \geq 1$, zodat $1 = u^2 - (a^2-1)v^2 \leq u^2 - (a^2-1) = u^2 - a^2 + 1$ de ongelijkheid $u^2 \geq a^2$ impliceert. Dus, daar $a > 1$, is

$$b = a + u^2(u^2-a) \geq a + a^2(a^2-a) = a(1 + a^2(a-1)) > a > 1.$$

Helemaal analoog als in het bewijs van de vorige inclusie hebben we dat voor alle $i, j \in \mathbb{N}$ met $i > j$ en alle $m \in \mathbb{N}_0$ de congruenties

$$x_m(i) - x_m(j) \equiv 0 \mod i-j, \quad y_m(i) - y_m(j) \equiv 0 \mod i-j$$

gelden. Omdat $y_{N_b}(1) = N_b$ impliceert dit voor $b > 1$ in het bijzonder

$$t = y_{N_b}(b) \equiv y_{N_b}(1) = N_b \mod b-1.$$

De vergelijking in G_8, zijnde $t \equiv n \mod 4y$, samen met $4y \mid b-1$ levert dan

$$N_b \equiv t \equiv n \mod 4y.$$

Lemma 5.15

Zij $z \in \mathbb{N}$ met $z > 1$. Dan gelden de uitdrukkingen

$$\begin{aligned}
x_{i+j}(z) &= x_i(z)x_j(z) + (z^2-1)y_i(z)y_j(z) \\
y_{i+j}(z) &= x_i(z)\,y_j(z) + x_j(z)\,y_i(z), \\
y_{ij}(z) &= y_{(j-1)i}(z)\,x_i(z) + y_i(z)\,x_{(j-1)i}(z), \\
y_{ij}(z) &= y_{(i-1)j}(z)\,x_j(z) + y_j(z)\,x_{(i-1)j}(z), \\
x_{i-j}(z) &= x_i(z)\,x_j(z) - (z^2-1)y_i(z)\,y_j(z), \\
y_{i-j}(z) &= y_i(z)\,x_j(z) - y_j(z)\,x_i(z).
\end{aligned}$$

Zij $k \in \mathbb{N}_0$. Dan hebben we

$$\begin{aligned}
x_{2k}(z) &\equiv -1 \mod x_k(z), \\
(x_{2k}(z))^2 &\equiv 1 \mod x_k(z), \\
y_{2k}(z) &\equiv 0 \mod x_k(z), \\
(y_{2k}(z))^2 &\equiv 0 \mod x_k(z).
\end{aligned}$$

Zij $i \in \mathbb{N}_0$. Dan hebben we $y_i(z) \mid y_{ij}(z)$ voor alle $j \in \mathbb{N}_0$.

Bewijs. Wegens onze opgedane kennis van de vergelijking van Pell is het evident dat, voor eender welk natuurlijk getal $z > 1$,

$$x_{i+j}(z) + y_{i+j}(z)\sqrt{z^2-1} = (x_i(z) + y_i(z)\sqrt{z^2-1})(x_j(z) + y_j(z)\sqrt{z^2-1}),$$

hetgeen impliceert dat

$$\begin{cases} x_{i+j}(z) = x_i(z)x_j(z) + (z^2-1)y_i(z)y_j(z) \\ y_{i+j}(z) = x_i(z)\,y_j(z) + x_j(z)\,y_i(z) \end{cases}.$$

In de laatste vergelijking j vervangen door $(j-1)i$ levert voor alle $i, j \in \mathbb{N}_0$ dat

$$y_{ij}(z) = y_{(j-1)i}(z)\,x_i(z) + y_i(z)\,x_{(j-1)i}(z).$$

Of, door de rollen van i en j om te draaien, volgt wegens symmetrie dat ook

$$y_{ij}(z) = y_{(i-1)j}(z)\,x_j(z) + y_j(z)\,x_{(i-1)j}(z).$$

We willen nu ook een uitdrukking vinden voor $x_{i-j}(z)$ en $y_{i-j}(z)$. Door op te merken dat

$$\left(x_j(z)+y_j(z)\sqrt{z^2-1}\right)^{-1} = x_j(z)-y_j(z)\sqrt{z^2-1}$$

hebben we dat

$$\begin{aligned} x_{i-j}(z)+y_{i-j}(z)\sqrt{z^2-1} &= (x_i(z)+y_i(z)\sqrt{z^2-1})\left(x_j(z)+y_j(z)\sqrt{z^2-1}\right)^{-1} \\ &= (x_i(z)+y_i(z)\sqrt{z^2-1})(x_j(z)-y_j(z)\sqrt{z^2-1}), \end{aligned}$$

en dus de gewenste uitdrukkingen

$$\begin{aligned} x_{i-j}(z) &= x_i(z)x_j(z)-(z^2-1)y_i(z)y_j(z) \\ y_{i-j}(z) &= y_i(z)x_j(z)-y_j(z)x_i(z). \end{aligned}$$

Tot slot, tonen we de laatste vier vergelijkingen aan. Eerst bewijzen we de eerste van deze vergelijkingen; voor een $k \in \mathbb{N}_0$ hebben we

$$\begin{aligned} x_{2k}(z) &= x_{k+k}(z) \\ &= x_k(z)x_k(z)+(z^2-1)y_k(z)y_k(z) \\ &= (x_k(z))^2+(z^2-1)(y_k(z))^2 \\ &= (x_k(z))^2+((x_k(z))^2-1) \\ &= 2(x_k(z))^2-1 \\ &\equiv -1 \mod x_k(z). \end{aligned}$$

De tweede vergelijking volgt natuurlijk meteen uit de eerste vergelijking. De derde vergelijking dan; er geldt dat

$$y_{2k}(z) = y_{k+k}(z) = x_k(z)y_k(z)+x_k(z)y_k(z) = 2x_k(z)y_k(z) \equiv 0 \mod x_k(z),$$

en dat impliceert meteen ook de vierde vergelijking.
Zij, tenslotte, een $i \in \mathbb{N}_0$ gefixeerd. We tonen per inductie op j aan dat $y_i(z) \mid y_{ij}(z)$ voor alle $j \in \mathbb{N}_0$. Voor $j = 1$ is het gevraagde duidelijk. Stel nu dat $y_i(z) \mid y_{i(j-1)}(z)$, dan bewijzen we dat $y_i(z) \mid y_{ij}(z)$; maar

$$y_i(z) \mid y_{(j-1)i}(z)x_i(z)+y_i(z)x_{(j-1)i}(z) = y_{ij}(z).$$

Het gevraagde volgt dus meteen. Dit beëindigt het bewijs van Lemma 5.15. ■

Veronderstel nu uit het ongerijmde dat $N \nmid N'$. Dan bestaan er een $t,r \in \mathbb{N}$, met $0 < r < N$, zodat $N' = tN+r$. Dus is

$$y_{N'}(a) = y_{tN+r}(a) = y_r(a)x_{tN}(a)+y_{tN}(a)x_r(a).$$

De vergelijking in G_3 zegt dat $y^2 \mid v$, of nog, $(y_N(a))^2 \mid y_{N'}(a)$; a fortiori $y_N(a) \mid y_{N'}(a)$. Wegens de delingseigenschap die we hierboven aangetoond hadden, geldt, daar $N \mid tN$, ook dat $y_N(a) \mid y_{tN}(a)$, en dus

$$y_N(a) \mid y_{N'}(a)-y_{tN}(a)x_r(a) = y_r(a)x_{tN}(a).$$

Maar $\text{ggd}(x_{tN}(a), y_{tN}(a)) = 1$ omdat $(x_{tN}(a))^2 - (a^2-1)(y_{tN}(a))^2 = 1$, per definitie. Bijgevolg geldt $y_N(a) \,|\, y_r(a)$. A fortiori is dan $y_N(a) \leq y_r(a)$. Maar $(y_i(a))_{i\in\mathbb{N}_0}$ is een strikt stijgende rij, en $r < N$, zodat we de contradictie $y_r(a) < y_N(a) \leq y_r(a)$ bekomen. De conclusie is dat $N \,|\, N'$; schrijf $N' = kN$ voor een $k \in \mathbb{N}$.
Merk op dat de uitdrukking

$$x_{kN}(a) + y_{kN}(a)\sqrt{a^2-1} = (x_N(a) + y_N(a)\sqrt{a^2-1})^k$$

geldt. Dan zien we door een expansie met het binomium van Newton eenvoudig in dat

$$v = y_{N'}(a) = y_{kN}(a) = \sum_{i\leq k \text{ oneven}} \binom{k}{i} x^{k-i} y^i (a^2-1)^{\frac{i-1}{2}}.$$

Bekijk deze uitdrukking modulo y^3; dan valt alles weg behalve de eerste term. Dus $v \equiv kx^{k-1}y \mod y^3$. Maar de vergelijking in G_3, zijnde $v \equiv 0 \mod 4y^2$, impliceert in het bijzonder dat $kx^{k-1}y \equiv v \equiv 0 \mod y^2$. Dit impliceert dat $y \,|\, kx^{k-1}$. Maar $\text{ggd}(x,y) = 1$ omdat $x^2 - (a^2-1)y^2 = 1$, zodat $y \,|\, k$, en bovendien $y \,|\, kN = N'$.
We bewijzen nu dat voor alle $t \in \mathbb{N}_0$ geldt dat

$$x_{4N'+t}(a) = x_{4N'}(a)\,x_t(a) + (z^2-1)y_{4N'}(a)\,y_t(a) \equiv x_t(a) \mod x_{N'}(a).$$

Hier hebben we gebruikt dat

$$x_{4N'}(a) = x_{2N'+2N'}(a) = x_{2N'}(a)\,x_{2N'}(a) + (z^2-1)y_{2N'}(a)\,y_{2N'}(a) \equiv 1 \mod x_{N'}(a)$$

en $x_{N'}(a) \,|\, y_{2N'}(a) \,|\, y_{4N'}(a)$.Op analoge wijze hebben we

$$x_{4N'-t}(a) = x_{4N'}(a)\,x_t(a) - (z^2-1)y_{4N'}(a)\,y_t(a) \equiv x_t(a) \mod x_{N'}(a),$$

voor alle $t \in \mathbb{N}_0$ met bovendien $t < 4N'$. Zo dadelijk gaan we deze formules toepassen.

Lemma 5.16

Zij $i \in \mathbb{N}_0$ zodat $x_i(a) \equiv x_N(a) \mod x_{N'}(a)$. Dan is $i \equiv \pm N \mod 4N'$.

Bewijs. Stel dat voor $i \in \mathbb{N}_0$ geldt dat $x_i(a) \equiv x_N(a) \mod x_{N'}(a)$. Deze i is gefixeerd gedurende de hele volgende paragraaf. Merk eerst al op dat $i \neq 4N'$; immers veronderstel uit het ongerijmde dat $i = 4N'$. Dan is

$$1 \equiv x_{4N'}(a) = x_N(a) \mod x_{N'},$$

en dus, daar $N \leq N'$, $x_N(a) \leq x_{N'}(a) \leq x_N(a) - 1$, een contradictie.

We tonen om te beginnen aan dat er een getal $t_i \in \mathbb{N}$ bestaat, met $1 \leq t_i \leq 4N'$, zodat $x_i(a) \equiv x_{t_i}(a) \mod x_{N'}(a)$. Indien $i \leq 4N'$ dan zijn we meteen klaar; veronderstel dus dat $i > 4N'$. Laat $t_1 := i - 4N' > 0$. De uitdrukking gesteld net boven dit lemma impliceert $x_i(a) = x_{4N'+t_1}(a) \equiv x_{t_1}(a) \mod x_{N'}(a)$. Indien $t_1 \leq 4N'$ dan zijn we klaar. In het andere geval, indien $t_1 > 4N'$, laat dan, analoog als zonet, $t_2 := t_1 - 4N' > 0$.

Dan is $x_i(a) \equiv x_{t_1}(a) = x_{4N'+t_2}(a) \equiv x_{t_2}(a) \mod x_{N'}(a)$. Indien $t_2 \leq 4N'$ dan zijn we klaar, en indien $t_2 > 4N'$ dan kunnen we dit proces op analoge wijze verderzetten. Merk op dat de alzo bekomen rij van getallen $t_1, t_2, t_3, \ldots$ strikt dalend is, omdat geldt dat $t_{i+1} := t_i - 4N' < t_i$. Omdat het gaat over een rij van natuurlijke getallen, moet dit proces ooit stoppen, en het laatste getal in die rij voldoet dan aan het gevraagde; met andere woorden er bestaat inderdaad een getal $t_i \in \mathbb{N}$, met $1 \leq t_i \leq 4N'$, zodat $x_i(a) \equiv x_{t_i}(a) \mod x_{N'}(a)$. Deze redenering toont aan dat we zonder verlies van algemeenheid mogen veronderstellen dat $i \in \{1, 2, \ldots, 4N'\}$.
Voor elke $j \in \mathbb{N}_0$ met $j < N'$ geldt de vergelijking

$$x_j(a) < \frac{x_{N'}(a)}{a} \leq \frac{1}{2} x_{N'}(a).$$

Inderdaad, uit de recursievergelijking voor $x_j(a)$, namelijk

$$x_{j+1}(a) = a x_j(a) + (a^2 - 1) y_j(a),$$

volgt dat

$$a x_j(a) = x_{j+1}(a) - (a^2 - 1) y_j(a) < x_{j+1}(a) \leq x_{N'}(a).$$

En de tweede ongelijkheid is meteen duidelijk, want $a > 1$ betekent precies $a \geq 2$. Met behulp van dit resultaat kunnen we nu aantonen dat de getallen in de rij $x_1(a), x_2(a), \ldots, x_{2N'}(a)$ allemaal verschillend zijn, en dat bovendien elk tweetal getallen in die rij een verschillend residu modulo $x_{N'}(a)$ hebben. Dat alle getallen in de rij onderling verschillend zijn is evident, daar de rij strikt stijgt. De rij van hierboven kunnen we als het ware in twee delen, zoals

$$x_1(a), x_2(a), \ldots, x_{N'-1}(a), x_{N'}(a), \quad x_{N'+1}(a), x_{N'+2}(a), \ldots, x_{2N'-1}(a), x_{2N'}(a).$$

Merk nu echter op dat voor elke $c \in \mathbb{N}$ met $c < N'$ geldt dat

$$x_{N'+c}(a) \equiv -x_{N'-c}(a) \mod x_{N'}(a).$$

Dit volgt rechtstreeks uit Lemma 5.15. Het tweede stuk van de rij, namelijk

$$x_{N'+1}(a), x_{N'+2}(a), \ldots, x_{2N'-1}(a), x_{2N'}(a),$$

is dus term per term equivalent modulo $x_{N'}(a)$ met de rij

$$-x_{N'-1}(a), -x_{N'-2}(a), \ldots, -x_1(a), -1.$$

Modulo $x_{N'}(a)$ kunnen we de gegeven rij van lengte $2N'$ dan schrijven als

$$x_1(a), x_2(a), \ldots, x_{N'-1}(a), 0, \quad -x_{N'-1}(a), -x_{N'-2}(a), \ldots, -x_1(a), -1.$$

Veronderstel nu uit het ongerijmde dat er in de originele rij van lengte $2N'$ twee verschillende elementen zijn die dezelfde rest modulo $x_{N'}(a)$ hebben. Dan komt dat er, wegens bovenstaande, op neer dat ofwel $x_{n_1}(a) \equiv x_{n_2}(a) \mod x_{N'}(a)$ ofwel $x_{n_1}(a) \equiv -x_{n_2} \mod x_{N'}(a)$ voor zekere $n_1 < n_2 \in \{1, 2, \ldots, N' - 1\}$; laat ons dit hier verkort met de notatie $x_{n_1}(a) \equiv \pm x_{n_2}(a) \mod x_{N'}(a)$ opschrijven. Er bestaat een

$q \in \mathbb{N}$, met $q \geq 1$ daar n_1 en n_2 verschillend zijn, zodat $qx_{N'}(a) = x_{n_2}(a) - x_{n_1}(a)$. Echter, door de ongelijkheden van eerder te gebruiken bekomen we dan

$$q\,x_{N'}(a) = |x_{n_2}(a) - x_{n_1}(a)| \leq |x_{n_2}(a)| + |x_{n_1}(a)| < \frac{1}{2}x_{N'}(a) + \frac{1}{2}x_{N'}(a) = x_{N'}(a),$$

en dus de contradictie $1 \leq q < 1$. Anderzijds is het ook duidelijk dat $x_j(a) \not\equiv 0 \mod x_{N'}(a)$ voor alle $j \in \{1,2,\ldots,N'-1\}$; immers, als $x_{N'}(a) \,|\, x_j(a)$ dan a fortiori $x_{N'}(a) \leq x_j(a)$, en omdat $j < N'$ en de beschouwde rij strikt stijgend is, zodus de contradictie $x_{N'}(a) \leq x_j(a) < x_{N'}(a)$. Ook hebben we dat $x_j(a) \not\equiv 1 \mod x_{N'}(a)$ voor alle $j \in \{1,2,\ldots,N'-1\}$; immers, als $x_{N'}(a) \,|\, x_j(a) - 1$ dan hebben we de contradictie $x_{N'}(a) \leq x_j(a) - 1 < x_{N'}(a) - 1$. Er rest ons enkel nog te bewijzen dat $x_j(a) \not\equiv -1 \mod x_{N'}(a)$ voor alle $j \in \{1,2,\ldots,N'-1\}$; als $j \neq N'-1$, id est $j < N'-1$, dan volgt uit $x_j(a) \equiv -1 \mod x_{N'}(a)$ opnieuw makkelijk de contradictie

$$x_{N'}(a) \leq x_j(a) + 1 < x_{N'-1}(a) + 1 \leq x_{N'}(a).$$

Maar wat als $j = N'-1$? Immers, de vorige redenering gaat dan niet op. Laten we, uit het ongerijmde, veronderstellen dat $x_{N'-1}(a) \equiv -1 \mod x_{N'}(a)$. Dus bestaat er een $t \in \mathbb{N}_0$ zodat $x_{N'-1}(a) + 1 = t\,x_{N'}(a)$. Wegens een ongelijkheid eerder gezien, hebben we echter $x_{N'-1}(a) \leq x_{N'}(a)/a$, en dus

$$t\,x_{N'}(a) = x_{N'-1}(a) + 1 \leq \frac{x_{N'}(a)}{a} + 1.$$

Omdat $N' \geq 1$, is $x_{N'}(a) \geq x_1(a) = a$, en hieruit volgt dan dat

$$t \leq \frac{1}{a} + \frac{1}{x_{N'}(a)} \leq \frac{1}{a} + \frac{1}{a} = \frac{2}{a} < 2.$$

Dus $t = 1$, id est $x_{N'-1}(a) + 1 = x_{N'}(a)$. Een ongelijkheid eerder gezien geeft echter dat $a\,x_{N'-1}(a) \leq x_{N'}(a) = x_{N'-1}(a) + 1$, en dus de contradictie

$$1 \leq x_{N'-1}(a) \leq (a-1)x_{N'-1}(a) \leq 1 \quad \Rightarrow \quad 1 = x_{N'-1}(a) \geq x_1(a) = a > 1.$$

Dit laat ons toe te besluiten dat inderdaad de getallen in de rij $x_1(a), x_2(a), \ldots, x_{2N'}(a)$ een verschillend residu modulo $x_{N'}(a)$ hebben.
Nu komen we terug op onze op het begin van dit bewijs gefixeerde $i \in \{1,2,\ldots,4N'\}$. We maken een gevalsonderscheid. Stel eerst dat $i \in \{1,2,\ldots,2N'\}$. Omdat geldt dat $1 \leq N \leq N'$, is $N \in \{1,2,\ldots,2N'\}$. Omdat, per hypothese, $x_i(a) \equiv x_N(a) \mod x_{N'}(a)$ impliceert dit dat $i = N$ omwille van wat we zojuist aangetoond hadden.
Veronderstel tenslotte dat $i \in \{2N'+1, 2N'+2, \ldots, 4N'\}$, id est $2N' < i < 4N'$ daar het geval $i = 4N'$ onmogelijk is, zoals we op het begin van het bewijs al gezien hadden. Dan is $0 < 4N' - i < 2N'$. Wegens de formule net boven dit lemma, en per hypothese, is

$$x_{4N'-i}(a) \equiv x_i(a) \equiv x_N(a) \mod x_{N'}(a).$$

Omdat $N \in \{1,2,\ldots,2N'\}$ en omwille van de uitleg van hierboven hebben we dan $4N' - i = N$, of equivalent, $i = 4N' - N$.
We besluiten dat, in elk geval, ofwel $i = N$ ofwel $i = 4N' - N$. Dus is sowieso $i \equiv \pm N \mod 4N'$. Dit beëindigt het bewijs van Lemma 5.16. ■

Uit de vergelijking van G_5 volgt dat $u \mid b-a$. Uit de opmerking net voor Lemma 5.15 volgt dat $x_{N_b}(b) - x_{N_b}(a) \equiv 0 \mod b-a$. Dus is $x_{N_b}(b) \equiv x_{N_b}(a) \mod u$. De vergelijking in G_7, zijnde $s \equiv x \mod u$, betekent precies dat $x_{N_b}(b) = s \equiv x = x_N(a) \mod u$, en dus, daar $u = x_{N'}(a)$,

$$x_N(a) \equiv x_{N_b}(a) \mod x_{N'}(a).$$

Lemma 5.16 impliceert dan dat $N_b \equiv \pm N \mod 4N'$. We hadden eerder al gevonden dat $y \mid N'$, dus ook $N_b \equiv \pm N \mod 4y$. Ook hadden we, aan het begin van het bewijs van dit lemma, gevonden dat $N_b \equiv n \mod 4y$. Dus geldt dat $n \equiv \pm N \mod 4y$.
Uit de vergelijking in G_1 volgt dat $y \geq n$. We weten dat $y_m(a) \geq m$ voor alle $m \in \mathbb{N}_0$, dus in het bijzonder is $y = y_N(a) \geq N$. Bijgevolg is $n+N \leq y+y = 2y$ en $|n-N| < y$. Veronderstel nu uit het ongerijmde dat $n \equiv -N \mod 4y$. Dan bestaat er een $t \in \mathbb{N}$, met $t \geq 1$, zodat $n+N = 4yt$. Dus $4yt = n+N \leq 2y$, of nog, $2t \leq 1$, hetgeen betekent dat $1 \leq t \leq \frac{1}{2} < 1$, contradictie. De conclusie is dat $n \equiv N \mod 4y$. Dan bestaat er een $t \in \mathbb{Z}$ zodat $n-N = 4yt$. Nu is

$$4y|t| = |4yt| = |n-N| < y.$$

Als, uit het ongerijmde, $t \neq 0$, dan is $|t| \geq 1$, zodat uit bovenstaande vergelijking de contradictie $4y \leq 4y|t| < y$ volgt. Dus $t = 0$, dat wil zeggen $n = N$. Dit beëindigt het bewijs van Lemma 5.14. ■

Uit Lemma 5.13 en Lemma 5.14 halen we dat G precies gelijk is aan de projectie van de verzameling G' op zijn eerste drie coördinaten. Daar G' diophantisch is, en projecties van diophantische verzamlingen opnieuw diophantisch zijn, volgt het gevraagde. Dit beëindigt het bewijs van Propositie 5.12. ■

5.3 Exponentiatie is diophantisch

Tot slot vatten we de essentie van het hele hoofdstuk samen in een stelling.

Propositie 5.17

De relatie

$$m = a^n, \quad n \geq 1$$

in de variabelen (m,a,n) diophantisch.

Bewijs. Natuurlijk volgt dit meteen uit Propositie 5.9 tesamen met Propositie 5.12. Dit beëindigt het bewijs van Propositie 5.17. ■

DE DPRM-STELLING

In dit hoofdstuk komen we tot de essentie van Hilberts Tiende Probleem over $\mathbb{Z}$: we tonen de zogenaamde DPRM-stelling aan. We volgen hierbij opnieuw de aanpak van Yuri Manin (1937).

6.1 *D*-sets en algemeen plan van het bewijs

We definiëren eerst het concept van een *D-set*. Daartoe moeten we eerst het volgende invoeren.

Definitie 6.1

> Zij een verzameling $E \subset \mathbb{N}^n$ gegeven. Indien $i \in \{1,2,\ldots,n\}$, dan wordt de verzameling $F \subset \mathbb{N}^n$ gedefinieerd door
>
> $$(x_1,\ldots,x_i,\ldots,x_n) \in F \Leftrightarrow \forall k \in \{0,1,\ldots,x_i\} : (x_1,\ldots,x_{i-1},k,x_{i+1},\ldots,x_n) \in E$$
>
> de verzameling bekomen *door gebonden universele kwantificatie op de i-de coördinaat van E* genoemd.

In feite komt dit ongeveer op hetzelfde neer als de aanpak van Davis; bij hem heeft dit concept dan wel de naam *Davis Normal Form*. Merk op dat we gebonden universele kwantificatie op een zekere coördinaat dus als een operator kunnen zien; we noemen dit ook wel de *gebonden universele kwantor*. Strikt genomen moeten we bij toepassing van de gebonden universele kwantor steeds zeggen op welke coördinaat deze precies toegepast wordt. Echter, indien we in het vervolg praten over de gebonden universele kwantor dan is het impliciet onderverstaan dat deze toegepast wordt op *eender welke* coördinaat van de verzameling.

Definitie 6.2

> De klasse van *D-sets* is de kleinste klasse van verzamelingen die alle diophantische verzamelingen bevat, en bovendien gesloten is onder het nemen van eindige Cartesische producten, eindige unies, eindige doorsnedes, projecties en de toepassing van de gebonden universele kwantor.

Of equivalent, de klasse *D*-sets is de klasse van verzamelingen voortgebracht door de diophantische verzamelingen onder al deze operaties. Of nog, het is de sluiting van de klasse van diophantische verzamelingen onder al die operaties.

In Definitie 6.2 bedoelen we met het toepassen van de gebonden universele kwantor

dus dat toepassing ervan op *elke* coördinaat van een diophantische verzameling opnieuw een diophantische verzameling oplevert.

Nu schetsen we het algemeen plan van het bewijs van de DPRM-stelling dat we zullen volgen. Dit komt helemaal overeen met Manin, en gaat als volgt. We zullen dan volgende twee stappen uitvoeren:

1) Aantonen dat de klasse van recursief opsombare verzamelingen gelijk is aan de klasse van D-sets.

2) Aantonen dat de klasse van D-sets gelijk is aan de klasse van diophantische verzamelingen.

Hieruit volgt natuurlijk de DPRM-stelling; inderdaad, er geldt dan dat elke recursief opsombare verzameling diophantisch is.

Analoog aan Definitie 6.2, en omdat recursief opsombaar in het engels *recursively enumerable* genoemd wordt, hebben we volgende notatie.

Definitie 6.3

De klasse van *r.e.-sets* is de klasse van recursief opsombare verzamelingen.

Bovenstaande stappen houden dan precies in aan te tonen dat

1) r.e. sets = D-sets

2) D-sets = klasse van diophantische verzamelingen.

6.2 De r.e. sets vallen samen met de D-sets

Zoals de titel al zegt tonen we in deze sectie aan dat de klasse van r.e. sets precies samenvalt met de klasse van D-sets. We bewijzen daartoe achtereenvolgens de inclusies D-sets $\subset$ r.e. sets en r.e. sets $\subset$ D-sets.

Propositie 6.4

Er geldt dat D-sets $\subset$ r.e. sets.

Bewijs. Ten eerste, elke diophantische verzameling is recursief opsombaar wegens Lemma 4.9. Analoog aan Propositie 4.6, en door gebruik te maken van Propositie 3.16, kan men eenvoudig aantonen dat recursief opsombare verzamelingen gesloten zijn onder het nemen van eindige Cartesische producten, eindige unies en eindige doorsnedes. Uit Propositie 3.16 volgt dat een projectie van een recursief opsombare verzameling opnieuw recursief opsombaar is. We moeten nu enkel nog aantonen dat de r.e. sets gesloten zijn onder toepassing van de gebonden universele kwantor.
Zij $E \subset \mathbb{N}^n$ een recursief opsombare verzameling, dat wil zeggen

$$E = \{(x_1,\ldots,x_n) \in \mathbb{N}^n \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } g(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0\}$$

voor een zekere primitief berekenbare functie $g : \mathbb{N}^{n+m} \to \mathbb{N}$. Laat F de verzameling zijn bekomen door gebonden universele kwantificatie op de n-de coördinaat van E zijn; dat wil zeggen, $(x_1,\ldots,x_n) \in F$ als en slechts als

$$\forall k \in \{0,1,\ldots,x_n\}\, \exists y_{1,k},\ldots,y_{m,k} \in \mathbb{N} \text{ zodat } g(x_1,\ldots,x_{n-1},k,y_{1,k},\ldots,y_{m,k}) = 0.$$

Het is wegens Propositie 3.16 duidelijk dat het voldoende te bewijzen is dat er een primitief berekenbare functie $h : \mathbb{N}^{n+2m} \to \mathbb{N}$ bestaat zodat

$$F = \{\vec{x} \in \mathbb{N}^n \mid \exists \vec{u},\vec{v} \in \mathbb{N}^m \text{ zodat } h(\vec{x},\vec{u},\vec{v}) = 0\},$$

waarbij we de afkortingen $\vec{x} = (x_1,\ldots,x_n)$, $\vec{u} = (u_1,\ldots,u_m)$ en $\vec{v} = (v_1,\ldots,v_m)$ gebruiken. In Lemma 6.5 hieronder definiëren we de Gödel coderingsfunctie Gd. Deze functie is diophantisch en dus in het bijzonder recursief opsombaar wegens Lemma 4.9. We definiëren de functie $h : \mathbb{N}^{n+2m} \to \mathbb{N}$ door $h(x_1,\ldots,x_n,u_1,\ldots,u_m,v_1,\ldots,v_m)$ gelijk te stellen aan

$$\sum_{k=1}^{x_n} [g(x_1,\ldots,x_{n-1},k,\mathrm{Gd}'(u_1,k,v_1),\ldots,\mathrm{Gd}'(u_m,k,v_m))]^2.$$

Duidelijk is h primitief berekenbaar daar Gd' en g dit zijn en samenstellingen van primitief berekenbare functies per definitie opnieuw primitief berekenbaar zijn. We tonen nu de gelijkheid van hierboven aan.
Veronderstel eerst dat $(x_1,\ldots,x_n) \in F$, dat wil zeggen voor elke $k \in \{0,1,\ldots,x_n\}$ bestaan er $y_{1,k},\ldots,y_{m,k} \in \mathbb{N}$ zodat

$$g(x_1,\ldots,x_{n-1},k,y_{1,k},\ldots,y_{m,k}) = 0.$$

Dus hebben we m rijen gegeven die elk van lengte $x_n + 1$ zijn, namelijk

$$(y_{1,0},\ldots,y_{1,x_n}) \quad (y_{2,0}\ldots,y_{2,x_n}) \quad \ldots \quad (y_{m,0},\ldots,y_{m,x_n}).$$

Elk van deze rijen kunnen we, dankzij Lemma 6.5, coderen met behulp van de Gödel coderingsfunctie Gd'. Voor iedere $i \in \{1,2,\ldots,m\}$ kiezen we u_i, v_i zodat voor alle $k \in \{0,1,\ldots,x_n\}$ geldt dat $\mathrm{Gd}'(u_i,k,v_i) = y_{i,k}$. Zij $k \in \{0,1,\ldots,x_n\}$. Dan is

$$g(x_1,\ldots,x_{n-1},k,\mathrm{Gd}'(u_1,k,t_1),\ldots,\mathrm{Gd}'(u_m,k,t_m)) = g(x_1,\ldots,x_{n-1},k,y_{1,k},\ldots,y_{m,k}) = 0.$$

Dus is

$$h(x_1,\ldots,x_n,u_1,\ldots,u_m,v_1,\ldots,v_m) = 0^2 + \ldots + 0^2 = 0.$$

Bijgevolg geldt inderdaad dat

$$(x_1,\ldots,x_n) \in \{\vec{x} \in \mathbb{N}^n \mid \exists \vec{u},\vec{v} \in \mathbb{N}^m \text{ zodat } h(\vec{x},\vec{u},\vec{v}) = 0\}.$$

Omgekeerd, veronderstel dat

$$(x_1,\ldots,x_n) \in \{\vec{x} \in \mathbb{N}^n \mid \exists \vec{u},\vec{v} \in \mathbb{N}^m \text{ zodat } h(\vec{x},\vec{u},\vec{v}) = 0\}.$$

De definitie van h impliceert dat er $u_1,\ldots,u_m,v_1,\ldots,v_m \in \mathbb{N}$ bestaan zodat

$$g(x_1,\ldots,x_{n-1},k,\mathrm{Gd}'(u_1,k,v_1),\ldots,\mathrm{Gd}'(u_m,k,v_m)) = 0$$

voor alle $k \in \{0,1,\ldots,x_n\}$. Neem zulk een k vast. Zij dan $y_{i,k} := \mathrm{Gd}(u_i,k,v_i)$ voor iedere $i \in \{1,2,\ldots,m\}$. Dan hebben we inderdaad dat

$$\begin{aligned} &g(x_1,\ldots,x_{n-1},k,y_{1,k},\ldots,y_{m,k}) \\ &= g(x_1,\ldots,x_{n-1},k,\mathrm{Gd}'(u_1,k,v_1),\ldots,\mathrm{Gd}'(u_m,k,v_m)) = 0, \end{aligned}$$

en bijgevolg $(x_1,\ldots,x_n) \in F$. Het zojuist gegeven argument toont aan dat toepassing van de gebonden universele kwantor op de laatste coördinaat van een recursief opsombare set opnieuw een recursief opsombare. set oplevert; natuurlijk volgt helemaal analoog dat ook toepassing van de gebonden universele kwantor op andere coördinaten van zulk een r.e. set opnieuw een r.e. set oplevert. Dus de r.e. sets zijn inderdaad gesloten onder toepassing van de gebonden unversele kwantor. Dit beëindig het bewijs van Propositie 6.4. ■

Opmerking. Men kan zich terecht de vraag stellen waarom het nodig is de Gödel coderingsfunctie Gd' te gebruiken. Het lijkt immers dat we net zo goed de functie $h : \mathbb{N}^{n+2m} \to \mathbb{N}$ zouden kunnen definiëren door

$$h(x_1,\ldots,x_n,y_{1,1},\ldots,y_{m,1},y_{1,2},\ldots,y_{m,2},\ldots,y_{1,x_n},\ldots,y_{m,x_n})$$

gelijk te stellen aan

$$\sum_{k=1}^{x_n} [g(x_1,\ldots,x_{n-1},k,y_{1,k},\ldots,y_{m,k})]^2.$$

Het probleem is echter dat het aantal argumenten van deze "functie", $n+mx_n$, stijgt met x_n, en dus niet constant is: we kunnen dus onmogelijk de functie h zo definiëren. Maar door met de functie Gd' te werken wordt dit probleem opgelost.

In het bewijs van Propositie 6.4 maakten we gebruik van volgend lemma.

Lemma 6.5

> *Er bestaat een primitief berekenbare, diophantische, functie* $Gd : \mathbb{N}^3 \to \mathbb{N}$, *genaamd de* Gödel coderingsfunctie*, die volgende eigenschap heeft: voor elke* $n \in \mathbb{N}_0$ *en elke eindige rij van natuurlijke getallen* $a_1,a_2,\ldots,a_n$ *van lengte n, bestaan er een* $u,v \in \mathbb{N}$ *zodat* $Gd(u,k,v) = a_k$ *voor alle* $k \in \{1,2,\ldots,n\}$.

Bewijs. Definieer de Gödel coderingsfunctie door

$$\mathrm{Gd} : \mathbb{N}^3 \to \mathbb{N} : (u,k,v) \mapsto \mathrm{rem}(u, 1+kv).$$

Dat wil zeggen, $\mathrm{Gd}(u,k,v)$ is de rest bij deling van u door $1+kv$. Zij $a_1,a_2,\ldots,a_n \in \mathbb{N}$ een gegeven rij van lengte n. Dan moeten we u en v vinden zodat aan de eigenschap in de formulering van het lemma voldaan is. Kies v zodat $n!$ een deler is van v en zodat $v > \max\{a_1,a_2,\ldots,a_n\}$; bijvoorbeeld kunnen we $v := (n+k)!$ stellen voor een natuurlijk getal k dat groot genoeg is. Merk op dat de n getallen $1+v, 1+2v, 1+3v, \ldots, 1+nv$ dan twee aan twee onderling ondeelbaar zijn; inderdaad, veronderstel

uit het ongerijmde dat $1+iv$ en $1+jv$ een gemeenschappelijke priemdeler p zouden hebben, met $i<j\in\{0,1,\ldots,n\}$. Daar $p\,|\,1+iv$ en $p\,|\,1+jv$ volgt dat

$$p\,|\,(1+jv)-(1+iv)=(j-i)v.$$

Dus $p\,|\,j-i$ of $p\,|\,v$. Omdat $j-i\leq n-0=n$ impliceert $p\,|\,j-i$ dat $p\,|\,n!\,|\,v$. Dus geldt in *elk* van beide gevallen dat $p\,|\,v$. Omdat we aangenomen hadden dat $p\,|\,1+iv$ impliceert dit de contradictie $p\,|\,1$. Bijgevolg zijn de hierboven genoemde n getallen inderdaad twee aan twee onderling ondeelbaar. Beschouw vervolgens het stelsel

$$\begin{cases} x\equiv a_1 & \mod 1+v \\ x\equiv a_2 & \mod 1+2v \\ \quad\vdots & \\ x\equiv a_n & \mod 1+nv \end{cases}.$$

De Chinese reststelling geeft ons een oplossing u van dit stelsel, die natuurlijk in $\mathbb{N}$ gekozen kan worden. Op die manier hebben we, voor de rij $a_1,a_2,\ldots,a_n$, getallen $u,v\in\mathbb{N}$ gevonden; dan moeten we enkel nog aantonen dat Gd inderdaad aan de eigenschap in de formulering van het lemma voldoet. Zij dus $k\in\{1,2,\ldots,n\}$. Dan is $u=t_k(1+kv)+a_k$ voor een zekere $t_k\in\mathbb{Z}$. Bijgevolg is

$$\mathrm{Gd}(u,k,v)=\mathrm{rem}(u,1+kv)=u-(1+kv)\left\lfloor\frac{u}{1+kv}\right\rfloor=u-(1+kv)\,t_k=a_k.$$

De voorlaatste stap geldt daar

$$t_k\leq t_k+\frac{a_k}{1+kv}<t_k+1\quad\Rightarrow\quad\left\lfloor\frac{u}{1+kv}\right\rfloor=\left\lfloor t_k+\frac{a_k}{1+kv}\right\rfloor=t_k.$$

En de tweede ongelijkheid in het linkerlid van deze implicatie is waar precies omdat we v zodanig hadden gekozen dat $v>\max\{a_1,a_2,\ldots,a_n\}\geq a_k$, en bijgevolg ook $1+kv>1+ka_k\geq 1+a_k>a_k$.
De functie Gd is diophantisch omwille van het feit dat de functie rem diophantisch is, en dat volgt uit sectie 4.2. Tot slot is het duidelijk dat Gd primitief berekenbaar is; dit volgt eenvoudig door de argumenten in de voorbeelden van sectie 3.2.2 aan te passen. Dit beëindigt het bewijs van Lemma 6.5. ■

Merk dus op dat de functie Gd de rij van getallen $a_1,a_2,\ldots,a_n$ "codeert", en dat op een primitief berekenbare manier. Vandaar natuurlijk ook de naam *coderingsfunctie*. Dit is een heel belangrijk resultaat dat we in wat volgt nog vaak nodig zullen hebben.

Opmerking. We definiëren $\mathrm{Gd}':\mathbb{N}^3\to\mathbb{N}$ door $\mathrm{Gd}'(u,k,v):=\mathrm{Gd}(u,k+1,v)$ te stellen voor alle $u,k,v\in\mathbb{N}$, die we ook *Gödel coderingsfunctie* noemen. Wegens Lemma 6.5 kan men makkelijk het volgende aantonen: voor elke $n\in\mathbb{N}$ en elke eindige rij van natuurlijke getallen $a_0,a_1,\ldots,a_n$ van lengte $n+1$, bestaan er een $u,v\in\mathbb{N}$ zodat $\mathrm{Gd}'(u,k,v)=a_k$ voor alle $k\in\{0,1,\ldots,n\}$. Het is deze Gödel coderingsfunctie we meestal gebruiken. Duidelijk is ook Gd' primitief berekenbaar en diophantisch.

Vervolgens tonen we de omgekeerde inclusie aan. We gebruiken daarbij volgende definitie. Voor een functie $f : \mathbb{N}^n \to \mathbb{N}$ wordt met Γ_f de grafiek van f bedoeld, dat wil zeggen

$$\Gamma_f := \{(x_1, \ldots, x_n, y) \in \mathbb{N}^{n+1} \mid f(x_1, \ldots, x_n) = y\}.$$

Propositie 6.6

Er geldt dat r.e. sets $\subset$ D-sets.

Bewijs. Beschouw een recursief opsombare verzameling E. Het is duidelijk dat er een primitief berekenbare functie $f : \mathbb{N}^n \to \mathbb{N}$ zodat E precies de level set in 0 van f is; inderdaad, dit geldt omwille van Propositie 3.16. Merk op dat E dus de projectie van de verzameling $\Gamma_f \cap [\mathbb{N}^n \times \{0\}]$ op zijn eerste n coördinaten is. Maar dit is gelijk aan

$$\Gamma_f \cap [\mathbb{N}^n \times \{0\}] = \Gamma_f \cap \Gamma_0,$$

met $0 : \mathbb{N}^n \to \{0\}$ de constante functie 0. Natuurlijk is de nulfunctie primitief berekenbaar. Lemma 6.7 zegt precies dat de grafiek van een primitief berekenbare functie een D-set is. In het bijzonder zijn Γ_f en Γ_0 dus D-sets. Bijgevolg is E de projectie van een doorsnede van twee D-sets. Omdat de D-sets, per definitie, gesloten zijn onder projecties en het nemen van doorsnedes, volgt dat E inderdaad een D-set is. Dit beëindigt het bewijs van Propositie 6.6. ■

Opmerking. In deze thesis hebben we gekozen om de recursietheorie op te bouwen met enkel functies $\mathbb{N}^n \to \mathbb{N}$, dat wil zeggen met als codomein *steeds* $\mathbb{N}$, en geen cartesische producten van $\mathbb{N}$; zie Definitie 3.10 en Definitie 3.11. Echter, men kan nog iets meer algemeen werken, en zo ook de notie van (primitieve) berekenbaarheid voor functies van de vorm $\mathbb{N}^n \to \mathbb{N}^m$ definiëren. Manin doet dit in zijn opbouw van de recursietheorie; meer nog, in het bewijs van volgend lemma zullen we noodgedwongen met primitieve berekenbaarheid van zulke functies moeten werken. Definitie 3.11 veralgemeent op evidente wijze tot de klasse van functies $\mathbb{N}^n \to \mathbb{N}^m$, op volgend extra punt na. Een nieuwe operator, *juxtapositie* genaamd, wordt ingevoerd. Namelijk, indien $f : \mathbb{N}^n \to \mathbb{N}^{m_1}$ en $g : \mathbb{N}^n \to \mathbb{N}^{m_2}$ primitief berekenbare functies zijn, dan wordt de functie $JUXT(f,g) : \mathbb{N}^n \to \mathbb{N}^{m_1+m_2}$ gedefinieerd door

$$(x_1, \ldots, x_n) \mapsto (f(x_1, \ldots, x_n), g(x_1, \ldots, x_n)) \in \mathbb{N}^{m_1} \times \mathbb{N}^{m_2} = \mathbb{N}^{m_1+m_2}.$$

Per definitie levert dit opnieuw een primitief berekenbare functie op. De klasse van *primitief berekenbare functies* wordt dan gedefinieerd als kleinste klasse van functies van de vorm $\mathbb{N}^n \to \mathbb{N}^m$ die alle basisfuncties bevat en gesloten is onder alle veralgemeende operaties uit Definitie 3.10 en bovendien onder de operator JUXT.

Lemma 6.7

De grafiek van een primitief berekenbare functie is een D-set.

Bewijs. Ten eerste, de grafieken van de basisfuncties die de verzameling van primitief berekenbare functies voortbrengen (zie Definitie 3.10) zijn duidelijk diophantisch; inderdaad,

$$\begin{aligned}\Gamma_{ZERO} &= \{(a_1,a_2)\in\mathbb{N}^2 \,|\, a_2=0\},\\ \Gamma_{SUCC} &= \{(a_1,a_2)\in\mathbb{N}^2 \,|\, a_1+1-a_2=0\},\\ \Gamma_{PROJ_i^n} &= \{(a_1,\ldots,a_n,a_{n+1})\in\mathbb{N}^{n+1} \,|\, a_i-a_{n+1}=0\}.\end{aligned}$$

Merk op dat er zelfs geen existentiële kwantoren gebruikt hoeven te worden om aan te tonen dat dit diophantische verzamelingen zijn. In het bijzonder zijn $\Gamma_{ZERO},\Gamma_{SUCC}$ en $\Gamma_{PROJ_i^n}$ dus D-sets.
We bewijzen nu dat de eigenschap van een D-set te zijn bewaard blijft onder samenstelling. Veronderstel daartoe dat $h:\mathbb{N}^n\to\mathbb{N}$ en $g:\mathbb{N}\to\mathbb{N}$ primitieve recursieve functies zijn zodanig dat Γ_h en Γ_g D-sets zijn. We tonen aan dat dan ook $\Gamma_{COMP(g,h)}$ een D-set is, met

$$COMP(g,h):\mathbb{N}^n\to\mathbb{N}:(x_1,\ldots,x_n)\mapsto g(h(x_1,\ldots,x_n)).$$

Trivialerwijs is echter

$$\Gamma_{COMP(g,h)}=\{(x_1,\ldots,x_n,y)\in\mathbb{N}^{n+1} \,|\, g(h(x_1,\ldots,x_n))=y\},$$

en dit is gelijk aan

$$\{(x_1,\ldots,x_n,y)\in\mathbb{N}^{n+1} \,|\, \exists z\in\mathbb{N} \text{ zodat } (x_1,\ldots,x_n,z,y)\in[\Gamma_h\times\mathbb{N}]\cap[\mathbb{N}^n\times\Gamma_g]\}.$$

Daar deze laatste verzameling precies gelijk is aan de projectie van de verzameling $[\Gamma_h\times\mathbb{N}]\cap[\mathbb{N}^n\times\Gamma_g]$ op de eerste n coördinaten *en* de laatste coördinaat, geldt a fortiori dat $\Gamma_{COMP(g,h)}$ een projectie van $[\Gamma_h\times\mathbb{N}]\cap[\mathbb{N}^n\times\Gamma_g]$ is. Maar $\mathbb{N}$ en $\mathbb{N}^n$ zijn diophantisch en dus zeker D-sets. Daar D-sets, per definitie, bewaard blijven onder direct product, doorsnede en projectie, volgt dat $\Gamma_{COMP(g,h)}$ inderdaad een D-set is. Het algemene geval, waarbij we niet één functie $h:\mathbb{N}^n\to\mathbb{N}$ hebben maar m functies $h_1,\ldots,h_m:\mathbb{N}^n\to\mathbb{N}$ met ook $g:\mathbb{N}^m\to\mathbb{N}$ gegeven, volgt op analoge wijze.
We tonen nu aan dat de eigenschap van een D-set te zijn bewaard blijft onder juxtapositie. Eerst bewijzen we het resultaat voor projectiefuncties. Stel dus dat $PROJ_i^n$ en $PROJ_j^n$ gegeven zijn. Dan is duidelijk

$$\Gamma_{JUXT(PROJ_i^n,PROJ_j^n)}=\{(x_1,\ldots,x_n,x_{n+1},x_{n+2})\in\mathbb{N}^{n+2} \,|\, x_{n+1}=x_i \text{ en } x_{n+2}=x_j\}$$

diophantisch en bijgevolg in het bijzonder een D-set. Neem nu primitief berekenbare functies $f:\mathbb{N}^n\to\mathbb{N}^{m_1}$ en $g:\mathbb{N}^n\to\mathbb{N}^{m_2}$ waarvoor bovendien geldt dat Γ_f en Γ_g D-sets zijn. We tonen aan dat dan ook $\Gamma_{JUXT(f,g)}$ een D-set is. Merk op dat

$$\Gamma_{JUXT(f,g)}=[\Gamma_f\times\mathbb{N}^{m_2}]\cap\text{perm}_{n,m_1,m_2}[\Gamma_g\times\mathbb{N}^{m_1}],$$

waarbij $\text{perm}_{n,m_1,m_2}:\mathbb{N}^{n+m_1+m_2}\to\mathbb{N}^{n+m_1+m_2}$ de functie is die de laatste m_1 coördinaten wisselt met de m_2 coördinaten daarvoor. Het is duidelijk dat perm_{n,m_1,m_2} kan geschreven worden als $n+m_1+m_2-1$ juxtapositities van projectiefuncties. Om dit alles wat duidelijker te maken: veronderstel $n=m_1=m_2=1$ en schrijf $S:=\text{perm}_{1,1,1}$, zodat

$$S:\mathbb{N}^3\to\mathbb{N}^3:(x,y,z)\mapsto(x,z,y).$$

Dan is

$$S = JUXT(PROJ_1^3, JUXT(PROJ_3^3, PROJ_2^3)).$$

Maar duidelijk is $\Gamma_g \times \mathbb{N}$ een D-set, per hypothese. Dan is

$$\begin{aligned} S(\Gamma_g \times \mathbb{N}) &= JUXT(PROJ_1^3, JUXT(PROJ_3^3, PROJ_2^3))(\Gamma_g \times \mathbb{N}) \\ &= (PROJ_1^3(\Gamma_g \times \mathbb{N}), JUXT(PROJ_3^3, PROJ_2^3)(\Gamma_g \times \mathbb{N})) \\ &= PROJ_1^3(\Gamma_g \times \mathbb{N}) \times JUXT(PROJ_3^3, PROJ_2^3)(\Gamma_g \times \mathbb{N}). \end{aligned}$$

Duidelijk is $PROJ_1^3(\Gamma_g \times \mathbb{N})$ een D-set. En omdat we het resultaat al bewezen hebben voor projecties, weten we ook dat $JUXT(PROJ_3^3, PROJ_2^3)(\Gamma_g \times \mathbb{N})$ een D-set is. Dit argument geldt in het algemeen, en we concluderen dat $\text{perm}_{n,m_1,m_2}[\Gamma_g \times \mathbb{N}^{m_1}]$ een D-set is. Omdat $\Gamma_f \times \mathbb{N}^{m_2}$ dit duidelijk ook is, besluiten we dat $\Gamma_{JUXT(f,g)}$ inderdaad een D-set is, als doorsnede van twee D-sets.
Tot slot tonen we aan dat de eigenschap van een D-set te zijn bewaard blijft onder toepassing van de operator van primitieve recursie. Veronderstel daartoe dat $f_0 : \mathbb{N}^n \to \mathbb{N}$ en $g \in \mathbb{N}^{n+2} \to \mathbb{N}$ primitieve recursieve functies zijn zodanig dat Γ_{f_0} en Γ_g D-sets zijn. We tonen aan dat dan ook $\Gamma_{PREC(f_0,g)}$ een D-set is, met

$$PREC(f_0, g) : \mathbb{N}^{n+1} \to \mathbb{N}$$

gedefinieerd door

$$\begin{aligned} (x_1, \ldots, x_n, 0) &\mapsto f_0(x_1, \ldots, x_n) \\ (x_1, \ldots, x_n, y+1) &\mapsto g(x_1, \ldots, x_n, y, PREC(f_0, g)(x_1, \ldots, x_n, y)). \end{aligned}$$

Per definitie is

$$\Gamma_{PREC(f_0,g)} = \{(x_1, \ldots, x_n, y, z) \in \mathbb{N}^{n+2} \mid PREC(f_0, g)(x_1, \ldots, x_n, y) = z\}.$$

Definieer

$$\Gamma_1 := \{(x_1, \ldots, x_n, 0, z) \in \mathbb{N}^{n+2} \mid (x_1, \ldots, x_n, 0, z) \in \Gamma_{PREC(f_0,g)}\}$$

en $\Gamma_2 := \Gamma_{PREC(f_0,g)} \setminus \Gamma_1$. Dan is het duidelijk dat

$$\Gamma_{PREC(f_0,g)} = \Gamma_1 \cup [\Gamma_{PREC(f_0,g)} \setminus \Gamma_1] = \Gamma_1 \cup \Gamma_2.$$

Bijgevolg is het voldoende aan te tonen dat Γ_1 en Γ_2 D-sets zijn, want de unie van twee D-sets is per definitie opnieuw een D-set.
Voor elke $(x_1, \ldots, x_n, y, z) \in \mathbb{N}^{n+2}$ geldt dat $(x_1, \ldots, x_n, y, z) \in \Gamma_1$ als en slechts als $y = 0$ en $(x_1, \ldots, x_n, z) \in \Gamma_{f_0}$. Merk op dat

$$\begin{aligned} \Gamma_1 &= \{(x_1, \ldots, x_n, y, z) \in \mathbb{N}^{n+2} \mid y = 0 \text{ en } f_0(x_1, \ldots, x_n) = z\} \\ &= \text{perm}_{n,1,1}(\Gamma_{f_0} \times \mathbb{N}) \cap \{(x_1, \ldots, x_n, y, z) \in \mathbb{N}^{n+2} \mid y = 0\}, \end{aligned}$$

waarbij $\text{perm}_{n,1,1} : \mathbb{N}^{n+2} \to \mathbb{N}^{n+2}$ de functie is die hierboven reeds gedefinieerd werd; het is dus de functie die de laatste twee coördinaten van plaats wisselt en de andere coördinaten onveranderd laat. Uit de analyse van hierboven volgt meteen dat

$\text{perm}_{n,1,1}(\Gamma_{f_0} \times \mathbb{N})$ een D-set is daar $\Gamma_{f_0} \times \mathbb{N}$ dit is. De verzameling $\{(x_1,\ldots,x_n,y,z) \in \mathbb{N}^{n+2} \,|\, y = 0\}$ is zelfs diophantisch en dus in het bijzonder een D-set. Dus is Γ_1 inderdaad een D-set, als doorsnede van twee D-sets.
We analyseren nu Γ_2. Definieer deelverzamelingen van $\mathbb{N}^{n+4}$ door

$$\begin{aligned} G_1 &:= \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, z = \text{Gd}'(u,y,t)\}, \\ G_2 &:= \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, \text{Gd}'(u,0,t) = f_0(x_1,\ldots,x_n)\}, \\ G_3 &:= \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, y > 0 \text{ en } \forall k \in \{1,2,\ldots,y\} : \\ &\qquad\qquad \text{Gd}'(u,k,t) = g(x_1,\ldots,x_n,k-1,\text{Gd}'(u,k-1,t))\}. \end{aligned}$$

Zij $G \subset \mathbb{N}^{n+4}$ dan de verzameling in de variabelen $(x_1,\ldots,x_n,y,z,u,t)$ gedefinieerd door $G := G_1 \cap G_2 \cap G_3$.

Lemma 6.8

Er geldt dat Γ_2 gelijk is aan de projectie van G op zijn eerste $n+2$ coördinaten.

Bewijs. We tonen eerst aan dat Γ_2 een deelverzameling is van de projectie van G op zijn eerste $n+2$ coördinaten. Neem $(x_1,\ldots,x_n,y,z) \in \Gamma_2$. Merk op dat

$$\Gamma_2 = \{(x_1,\ldots,x_n,y,z) \in \mathbb{N}^{n+2} \,|\, y > 0 \text{ en } \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,y) = z\}.$$

Beschouw de eindige rij van natuurlijke getallen

$$\mathit{PREC}(f_0,g)(x_1,\ldots,x_n,0), \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,1), \ldots, \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,y).$$

Kies, met behulp van Lemma 6.5, $u,t \in \mathbb{N}$ zodat

$$\text{Gd}'(u,k,v) = \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,k)$$

voor alle $k \in \{0,1,\ldots,y\}$. Dan is

$$\text{Gd}'(u,y,t) = \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,y) = z,$$

zodat aan G_1 inderdaad voldaan is. Ook aan G_2 is voldaan, daar

$$\text{Gd}'(u,0,t) = \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,0) = f_0(x_1,\ldots,x_n).$$

Tenslotte is ook aan G_3 voldaan; we hebben dat $y > 0$ en

$$\begin{aligned} \text{Gd}'(u,1,t) &= \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,1) \\ &= g(x_1,\ldots,x_n,1-1,\mathit{PREC}(f_0,g)(x_1,\ldots,x_n,1-1)), \end{aligned}$$

per definitie van $\mathit{PREC}(f_0,g)$. Analoog is

$$\begin{aligned} \text{Gd}'(u,2,t) &= \mathit{PREC}(f_0,g)(x_1,\ldots,x_n,2) \\ &= g(x_1,\ldots,x_n,2-1,\mathit{PREC}(f_0,g)(x_1,\ldots,x_n,2-1)). \end{aligned}$$

Per inductie zien we dat, precies omwille van de definitie van primitieve recursie, inderdaad

$$\forall k \in \{1,2,\ldots,y\} : Gd'(u,k,t) = g(x_1,\ldots,x_n,k-1,\mathrm{Gd}'(u,k-1,t)).$$

Nu tonen we de omgekeerde implicatie aan. Neem daartoe $(x_1,\ldots,x_n,y,z,u,t) \in G$; we moeten dan bewijzen dat $(x_1,\ldots,x_n,y,z) \in \Gamma_2$. Definieer vervolgens

$$\begin{aligned}
a_0 &:= \mathrm{Gd}'(u,0,t) = f_0(x_1,\ldots,x_n) = PREC(f_0,g)(x_1,\ldots,x_n,0),\\
a_1 &:= \mathrm{Gd}'(u,1,t) = g(x_1,\ldots,x_n,0,\mathrm{Gd}(u,0,t)) = PREC(f_0,g)(x_1,\ldots,x_n,1)\\
a_2 &:= \mathrm{Gd}'(u,2,t) = g(x_1,\ldots,x_n,1,\mathrm{Gd}(u,1,t)) = PREC(f_0,g)(x_1,\ldots,x_n,2)\\
&\vdots\\
a_y &:= \mathrm{Gd}'(u,y,t) = g(x_1,\ldots,x_n,y-1,\mathrm{Gd}(u,y-1,t)) = PREC(f_0,g)(x_1,\ldots,x_n,y).
\end{aligned}$$

De rij $a_0,a_1,\ldots,a_y$ van natuurlijke getallen is in feite precies de decodering van de rij die gecodeerd werd door de Gödel coderingsfunctie en de sleutel daarvan is precies het koppel (u,t). De gelijkheden gelden daar $(x_1,\ldots,x_n,y,z,u,t) \in G_2$ en $(x_1,\ldots,x_n,y,z,u,t) \in G_3$. Het feit dat $(x_1,\ldots,x_n,y,z,u,t) \in G_1$ impliceert de gelijkheid

$$z = \mathrm{Gd}'(u,y,t) = a_y = PREC(f_0,g)(x_1,\ldots,x_n,y).$$

Omdat ook $y > 0$, daar $(x_1,\ldots,x_n,y,z,u,t) \in G_3$, hebben we inderdaad dat

$$(x_1,\ldots,x_n,y,z) \in \{(x_1,\ldots,x_n,y,z) \in \mathbb{N}^{n+2} \,|\, y > 0, PREC(f_0,g)(x_1,\ldots,x_n,y) = z\} = \Gamma_2.$$

Hiermee is ook de tweede inclusie aangetoond. Dit beëindigt het bewijs van Lemma 6.8. ■

Uit Lemma 6.8 volgt dat Γ_2 gelijk is aan de projectie van G op zijn eerste $n+2$ coördinaten. Het is dus voldoende aan te tonen dat G een D-set is. En daarvoor volstaat het aan te tonen dat G_1, G_2 en G_3 D-sets zijn.
Ten eerste,

$$\begin{aligned}
G_1 &= \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, z = \mathrm{gd}'(u,y,t)\}\\
&= \mathbb{N} \times \ldots \times \mathbb{N} \times \{(y,z,u,t) \in \mathbb{N}^4 \,|\, z = \mathrm{gd}'(u,y,t)\}.
\end{aligned}$$

Maar de verzameling $\{(y,z,u,t) \in \mathbb{N}^4 \,|\, z = \mathrm{gd}'(u,y,t)\}$ is, op een verwisseling van volgorde van coördinaten na, gelijk aan de grafiek van de functie

$$\mathrm{Gd} : \mathbb{N}^3 \to \mathbb{N} : (u,y,t) \mapsto \mathrm{rem}(u, 1+(y+1)v),$$

die we in Lemma 6.5 ingevoerd hadden. Inderdaad, $\{(y,z,u,t) \in \mathbb{N}^4 \,|\, z = \mathrm{gd}'(u,y,t)\}$ is gelijk aan

$$(m_{0,2,2} \circ m_{1,1,2} \circ m_{2,1,1})(\Gamma_{\mathrm{Gd}}) = (m_{0,2,2} \circ m_{1,1,2} \circ m_{2,1,1})(\{(u,y,t,z) \,|\, \mathrm{gd}'(u,y,t) = z\}),$$

want deze laatste verzameling is gelijk aan

$$\begin{aligned}
(m_{0,2,2} \circ m_{1,1,2})(\{(u,y,z,t) \,|\, \mathrm{Gd}'(u,y,t) = z\}) &= m_{0,2,2}(\{(u,t,y,z) \,|\, \mathrm{Gd}'(u,y,t) = z\})\\
&= \{(y,z,u,t) \,|\, \mathrm{Gd}'(u,y,t) = z\}.
\end{aligned}$$

Lemma 6.5 stelt dat Gd, en dus ook Gd$'$, een diophantische functie is. Per definitie wil dat zeggen dat $\Gamma_{\mathrm{Gd}'}$ een D-set is. Omdat we uit de analyse van hierboven al weten dat al de functies van de vorm $m_{i,j,k}$, en dus ook samenstellingen daarvan, D-sets bewaren, hebben we inderdaad dat

$$\{(y,z,u,t) \in \mathbb{N}^4 \,|\, z = \mathrm{Gd}'(u,y,t)\} = (m_{0,2,2} \circ m_{1,1,2} \circ m_{2,1,1})(\Gamma_{\mathrm{Gd}'})$$

opnieuw een D-set is. Het besluit is dat

$$G_1 = \mathbb{N} \times \ldots \times \mathbb{N} \times \{(y,z,u,t) \in \mathbb{N}^4 \,|\, z = \mathrm{Gd}'(u,y,t)\}$$

een D-set is.
Om aan te tonen dat G_2 een D-set is, definiëren we de verzamelingen

$$\begin{aligned} G_{2,1} &:= \{(x_1,\ldots,x_n,y,z,u,t,w,k) \in \mathbb{N}^{n+6} \,|\, k = 0\}, \\ G_{2,2} &:= \{(x_1,\ldots,x_n,y,z,u,t,w,k) \in \mathbb{N}^{n+6} \,|\, \mathrm{Gd}'(u,k,t) = w\}, \\ G_{2,3} &:= \{(x_1,\ldots,x_n,y,z,u,t,w,k) \in \mathbb{N}^{n+6} \,|\, f(x_1,\ldots,x_n) = w\}. \end{aligned}$$

Het is duidelijk dat $G_{2,1}$ een D-set is. Ook $G_{2,2}$ is een D-set; inderdaad,

$$G_{2,2} = \mathbb{N} \times \ldots \times \mathbb{N} \times \{u,t,w,k) \in \mathbb{N}^4 \,|\, \mathrm{Gd}'(u,k,t) = w\}$$

is een D-set omdat $\{u,t,w,k) \in \mathbb{N}^4 \,|\, \mathrm{Gd}'(u,k,t) = w\}$ op verwisseling van de volgorde van de coördinaten na gelijk is aan de grafiek van Gd$'$, en we uit eerdere discussies reeds weten dat de volgorde van de coördinaten geen rol speelt bij de eigenschap van een D-set te zijn. Analoog hebben we dat $G_{2,3}$, na het schrappen van de overbodige coördinaten y,z,u,t,k, op een verwissling van de volgorde van coördinaten na gelijk is aan de grafiek van f_0. Maar Γ_{f_0} is een D-set, per hypothese. Dus $G_{2,3}$ is inderdaad een D-set. Nu is

$$G_{2,1} \cap G_{2,2} \cap G_{2,3} = \{(x_1,\ldots,x_n,y,z,u,t,w,0) \in \mathbb{N}^{n+6} \,|\, \mathrm{Gd}'(u,0,t) = f(x_1,\ldots,x_n)\},$$

en de projectie hiervan op de eerste $n+4$ variabelen is precies gelijk aan G_2. Bijgevolg is G_2 inderdaad een D-set.
Tot slot tonen we aan dat G_3 een D-set is. Definieer verzamelingen

$$\begin{aligned} G_{3,1} &:= \{(x_1,\ldots,x_n,y',z,u,t,w) \in \mathbb{N}^{n+5} \,|\, \mathrm{Gd}'(u,y',t) = z\}, \\ G_{3,2} &:= \{(x_1,\ldots,x_n,y',z,u,t,w) \in \mathbb{N}^{n+5} \,|\, \mathrm{Gd}'(u,y'+1,t) = w\}, \\ G_{3,3} &:= \{(x_1,\ldots,x_n,y',z,u,t,w) \in \mathbb{N}^{n+5} \,|\, g(x_1,\ldots,x_n,y',z) = w\}. \end{aligned}$$

Merk op dat $G_{3,1}, G_{3,2}$ en $G_{3,3}$ D-sets zijn; inderdaad, dit volgt op precies dezelfde wijze zoals we dit hierboven al een aantal keer gedaan hebben, dat wil zeggen, het resultaat is waar essentieel omdat $\Gamma_{\mathrm{Gd}'}$ en Γ_{g} D-sets zijn en omdat de operatie die coördinaten van plaats verwisselt D-sets bewaart. Dan is dus ook de verzameling

$$G_3' := G_{3,1} \cap G_{3,2} \cap G_{3,3}$$

een D-set. De projectie van G_3' op zijn eerste $n+4$ coördinaten levert dat

$$G_3'' := \{(x_1,\ldots,x_n,y',z,u,t) \in \mathbb{N}^4 \,|\, \mathrm{Gd}'(u,y'+1,t) = g(x_1,\ldots,x_n,y',\mathrm{Gd}'(u,y',t))\}$$

een D-set is. We passen nu de gebonden universele kwantor op y' in de verzameling G_3''; daar D-sets per definitie hieronder bewaard blijven, krijgen we dat

$$\begin{aligned} G_3''' \quad := \quad & \{(x_1,\ldots,x_n,y',z,u,t) \in \mathbb{N}^4 \,|\, \forall k \in \{0,1,\ldots,y'\} \\ & \qquad \mathrm{Gd}'(u,k+1,t) = g(x_1,\ldots,x_n,k,\mathrm{Gd}'(u,k,t))\} \end{aligned}$$

een D-set is. Herinner dat

$$\begin{aligned} G_3 \quad = \quad & \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, y > 0 \text{ en } \forall k \in \{1,2,\ldots,y\} : \\ & \qquad \mathrm{Gd}'(u,k,t) = g(x_1,\ldots,x_n,k-1,\mathrm{Gd}'(u,k-1,t))\}. \end{aligned}$$

Nu is het duidelijk dat G_3 de projectie van de D-set

$$\{(x_1,\ldots,x_n,y,z,u,t,y') \in \mathbb{N}^{n+5} \,|\, y'-(y-1) = 0 \text{ en } (x_1,\ldots,x_n,y',z,u,t) \in G_3'''\}$$

op de eerste $n+4$ coördinaten is; inderdaad, deze projectie is precies gelijk aan

$$\{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, \exists y' \in \mathbb{N} : y = y'+1 \text{ en } (x_1,\ldots,x_n,y',z,u,t) \in G_3'''\},$$

hetgeen hetzelfde is als

$$\{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, y > 0 \text{ en } (x_1,\ldots,x_n,y-1,z,u,t) \in G_3'''\}.$$

Of, meer uitgeschreven, hebben we dat die projectie gelijk is aan

$$\begin{aligned} \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, & y > 0 \text{ en } \forall k \in \{0,1,\ldots,y-1\} \\ & \mathrm{Gd}'(u,k+1,t) = g(x_1,\ldots,x_n,k,\mathrm{Gd}'(u,k,t))\}. \end{aligned}$$

Indien we $k' = k+1$ als verandering van variabelen stellen, dan hebben we natuurlijk dat dit precies

$$\begin{aligned} \{(x_1,\ldots,x_n,y,z,u,t) \in \mathbb{N}^{n+4} \,|\, & y > 0 \text{ en } \forall k' \in \{1,2,\ldots,y\} \\ & \mathrm{Gd}'(u,k',t) = g(x_1,\ldots,x_n,k'-1,\mathrm{Gd}'(u,k'-1,t))\}. \end{aligned}$$

is. En dat is precies gelijk aan G_3. Bijgevolg is G_3 een D-set. Dit beëindigt het bewijs van Lemma 6.7. ■

We concluderen met het hoofdresultaat van deze sectie in herinnering te brengen.

Propositie 6.9

Er geldt dat D-sets = r.e. sets.

Bewijs. Propositie 6.4 samen met Propositie 6.6 impliceert meteen het gevraagde. Dit beëindigt het bewijs van Propositie 6.9. ■

6.3 De D-sets vallen samen met de diophantische verzamelingen

Zoals de titel al zegt tonen we in deze sectie aan dat de klasse van D-sets precies samenvalt met de klasse van diophantische verzamelingen.

Dat elke D-set een diophantische verzameling is werd historisch gezien pas helemaal op het einde bewezen. Het feit dat exponentiatie diophantisch is, is cruciaal in het bewijs van deze inclusie. We zullen zo meteen zien dat de andere inclusie trouwens triviaal is.

Propositie 6.10

Er geldt dat de klasse van diophantische verzamelingen $\subset$ D-sets.

Bewijs. Per definitie van de klasse van D-sets is dit waar. Dit beëindigt het bewijs van Propositie 6.10. ■

Nu tonen we de omgekeerde inclusie aan, die helemaal niet evident is.

Propositie 6.11

Er geldt dat D-sets $\subset$ de klasse van diophantische verzamelingen.

Bewijs. We moeten aantonen dat de operaties van het nemen van eindige unies, eindige doorsnedes, eindige Cartesische producten, projecties en gebonden universele kwantificatie van diophantische verzamelingen opnieuw diophantisch zijn. Dit is evident voor elk van deze operaties behalve de laatst genoemde; zie Propositie 4.6, en merk op dat het duidelijk is dat projecties van diophantische verzamelingen opnieuw diophantisch zijn. Dus moeten we enkel nog aantonen dat applicatie van de gebonden universele kwantor op een diophantische verzameling opnieuw diophantisch is.
Zij $E \subset \mathbb{N}^{n+1}$ een diophantische verzameling. Dit wil zeggen dat er een veelterm $f(x_1,\ldots,x_n,k,y_1,\ldots,y_m) \in \mathbb{Z}[x_1,\ldots,x_n,k,y_1,\ldots,y_m]$ bestaat zodat

$$E = \{(x_1,\ldots,x_n,k) \in \mathbb{N}^{n+1} \mid \exists y_1,\ldots,y_m \in \mathbb{N} \text{ zodat } f(x_1,\ldots,x_n,k,y_1,\ldots,y_m) = 0\}.$$

We mogen veronderstellen dat f niet constant is, want anders is het te bewijzen triviaal. Zij dan $D \subset \mathbb{N}^{n+1}$ de verzameling bekomen door de gebonden universele kwantor op de $(n+1)$-de coördinaat van E toe te passen; id est

$$D := \{(x_1,\ldots,x_n,z) \in \mathbb{N}^{n+1} \mid \forall k \in \{0,1,\ldots,z\}\, \exists y_{1,k},\ldots,y_{m,k} \in \mathbb{N} \text{ zodat } f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) = 0\}.$$

Definieer c als de som van de absolute waardes van de coëfficiënten van f en d als de graad van f.
Zij D' nu de verzameling van alle

$$(x_1,\ldots,x_n,z,Y,N,K,Y_1,\ldots,Y_m) \in \mathbb{N}^{n+m+4}$$

waarvoor voldaan is aan de $m+3$ vergelijkingen

$$\begin{aligned} 1+(K+1)N! &= \prod_{k=0}^{z}(1+(k+1)N!) \\ N &\geq c(x_1x_2\ldots x_nzY)^d, \quad Y<Y_1,\ldots,Y<Y_m \\ f(x_1,\ldots,x_n,K,Y_1,\ldots,Y_m) &\equiv 0 \mod (1+(K+1)N!) \\ \prod_{0\leq j\leq Y}(Y_i-j) &\equiv 0 \mod (1+(K+1)N!) \quad i=1,2,\ldots,m. \end{aligned}$$

Uit Lemma 6.13 tesamen met Lemma 6.14 en Lemma 6.16 volgt meteen dat D' een diophantische verzameling is, als doorsnede van $m+3$ diophantische verzamelingen.

Lemma 6.12

Er geldt dat D de projectie van D' op zijn eerste $n+1$ coördinaten is.

Bewijs. We bewijzen daartoe eerst de inclusie van links naar rechts. Veronderstel dus dat $(x_1,\ldots,x_n,z)\in D$; dan moeten we $Y,N,K,Y_1,\ldots,Y_m\in\mathbb{N}$ vinden zodat aan de $m+3$ definiërende vergelijkingen van D' voldaan is. De variabele K wordt volledig bepaald door de eerste vergelijking; merk namelijk op dat

$$N!\,|\,(1+N!)\ldots(1+(z+1)N!)-1,$$

zodat we inderdaad

$$K:=\frac{(1+N!)\ldots(1+(z+1)N!)-1}{N!}-1\in\mathbb{N}$$

kunnen definiëren. Omdat $(x_1,\ldots,x_n,z)\in D$ bestaan er, per definitie van D, voor elke $k\in\{0,1,\ldots,z\}$ getallen $y_{1,k},\ldots,y_{m,k}\in\mathbb{N}$ zodat

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k})=0.$$

Zij nu

$$Y:=\max\{z,y_{1,0},\ldots,y_{m,0},y_{1,1},\ldots,y_{m,1},\ldots,y_{1,z},\ldots,y_{m,z}\}.$$

Fixeer een $i\in\{1,2,\ldots,m\}$. Beschouw de rij van natuurlijke getallen $y_{i,0},y_{i,1},\ldots,y_{i,z}$. Uit het bewijs van Lemma 6.5 volgt dat er $Y_i,N\in\mathbb{N}$ bestaan zodat

$$\mathrm{Gd}(Y_i,k+1,N!)=y_{i,k},\qquad k\in\{0,1,\ldots,z\},$$

waarbij Y_i en N bovendien willekeurig groot gekozen mogen worden. Meer nog, N *is onafhankelijk van de gekozen* $i\in\{1,2,\ldots,m\}$; dat wil zeggen, voor verschillende $i,j\in\{1,2,\ldots,m\}$ kan men *dezelfde* $N\in\mathbb{N}$ kiezen. Dit alles volgt door inzicht in het bewijs van Lemma 6.5. Op die manier vinden we dus inderdaad $Y_1,\ldots,Y_m,N\in\mathbb{N}$ zodat aan de tweede vergelijking van hierboven is voldaan; id est,

$$N\geq c(x_1x_2\ldots x_nzY)^d,\quad Y<Y_1,\ldots,Y<Y_m.$$

We bewijzen nu dat aan de laatste m vergelijkingen voldaan is. Zij dus opnieuw $i \in \{1,2,\ldots,m\}$. Uit

$$\text{rem}(Y_i, 1+(k+1)N!) = \text{Gd}(Y_i, k+1, N!) = y_{i,k}$$

halen we onmiddellijk dat $1+(k+1)N! \mid Y_i - y_{i,k}$ voor alle $k \in \{0,1,\ldots,z\}$. Per constructie is $y_{i,k} \leq Y < Y_i$, zodat voor alle $k \in \{0,1,\ldots,z\}$ geldt dat

$$1+(k+1)N! \mid Y_i - y_{i,k} \mid \prod_{j \leq Y}(Y_i - j).$$

Merk op dat voor $k_1 < k_2 \in \{0,1,\ldots,z\}$ we

$$\text{ggd}(1+(k_1+1)N!, 1+(1+k_2)N!) = 1$$

hebben; inderdaad, veronderstel dat p een gemeenschappelijke priemdeler is. Dan geldt ook

$$p \mid (1+(k_2+1)N!) - (1+(k_1+1)N!) = (k_2-k_1)N!.$$

Maar de tweede vergelijking van boven geeft $z \leq N$, en dus $k_2 - k_1 \leq z - 0 \leq N$. Bijgevolg hebben we dat $p \mid N!$ en dus ook de contradictie

$$p \mid (1+(k_1+1)N!) - (k_1+1)N! = 1.$$

Dit toont aan dat $\text{ggd}(1+(k_1+1)N!, 1+(k_2+1)N!) = 1$.
Maar deze gegevens impliceren meteen dat

$$1+(K+1)N! = \prod_{k=0}^{z}(1+(k+1)N!) \mid \prod_{j \leq Y}(Y_i - j).$$

Aan de laatste m vergelijkingen is dus inderdaad voldaan.
De eerste vergelijking, die we al hadden bekomen, impliceert voor elke $k \in \{0,1,\ldots,z\}$ de congruentie

$$\begin{aligned}(1+(K+1)N!) - (1+(k+1)N!) &= \prod_{k=0}^{z}(1+(k+1)N!) - (1+(k+1)N!) \\ &\equiv 0 - 0 = 0 \mod (1+(k+1)N!).\end{aligned}$$

Dus is

$$(K-k)N! = ((K+1)-(k+1))N! \equiv 0 \mod (1+(k+1)N!).$$

Omdat duidelijk $\text{ggd}(N!, 1+(k+1)N!) = 1$, impliceert dit de congruentie

$$K \equiv k \mod (1+(k+1)N!).$$

Uit de keuze van de $Y_i's$ halen we dat

$$Y_i \equiv y_{i,k} \mod (1+(k+1)N!)$$

voor alle $k \in \{0,1,\ldots,z\}$. Daar f een gehele veelterm is geldt voor iedere zulke k bijgevolg de congruentie

$$f(x_1,\ldots,x_n,K,Y_1,\ldots,Y_m) \equiv f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) = 0 \mod (1+(k+1)N!).$$

Omdat alle getallen $1+(k+1)N!$, met $k \in \{0,1,\ldots,z\}$, onderling ondeelbaar zijn impliceert dit

$$f(x_1,\ldots,x_n,K,Y_1,\ldots,Y_m) \equiv 0 \mod \prod_{k=0}^{z}(1+(k+1)N!).$$

Omdat $1+(K+1)N! = \prod_{k=0}^{z}(1+(k+1)N!)$ uit de eerste vergelijking, volgt inderdaad de voorlaatste vergelijking, namelijk

$$f(x_1,\ldots,x_n,K,Y_1,\ldots,Y_m) \equiv 0 \mod (1+(K+1)N!).$$

Dit beëindigt het bewijs van de eerste inclusie.
Veronderstel nu omgekeerd dat $(x_1,\ldots,x_n,z)$ een element is van de projectie van D' op zijn eerste $n+1$ coördinaten. Dit betekent precies dat er $Y,N,K,Y_1,\ldots,Y_m \in \mathbb{N}$ gegeven zijn zodat $(x_1,\ldots,x_n,z,Y,N,K,Y_1,\ldots,Y_m)$ aan de $m+3$ definiërende vergelijkingen van D' voldoet. Om aan te tonen dat $(x_1,\ldots,x_n,z) \in D$ volstaat het om te bewijzen dat er voor alle $i \in \{1,2,\ldots,m\}$ en $k \in \{0,1,\ldots,z\}$ een getal $y_{i,k} \in \mathbb{N}$ bestaat zodat $f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) = 0$. Zij $i \in \{1,2,\ldots,m\}$. Kies voor elke $k \in \{0,1,\ldots,z\}$ een priemgetal p_k zodat $p_k \mid 1+(k+1)N!$.
Merk op dat $p_k > N$ voor alle $k \in \{0,1,2,\ldots,z\}$; inderdaad, stel dat $p_k \leq N$, dan is $p_k \mid N!$, zodat we $p_k \mid (1+(k+1)N!) - (k+1)N! = 1$ bekomen. Een contradictie.
Neem $k \in \{0,1,2,\ldots,z\}$ en $i \in \{1,2,\ldots,m\}$. Uit de eerste en laatste vergelijking tesamen volgt dat

$$p_k \mid 1+(k+1)N! \mid \prod_{k=0}^{z}(1+(k+1)N!) = 1+(K+1)N! \mid \prod_{j\leq Y}(Y_i - j).$$

Omdat p_k priem is bestaat er een $j_{i,k} \leq Y$ zodat $p_k \mid Y_i - j_{i,k}$. Definieer nu $y_{i,k} := j_{i,k}$. We beweren dat deze getallen voldoen aan het gevraagde. Meteen volgt $y_{i,k} \leq Y$ voor alle i,k. Zij $k \in \{0,1,2,\ldots,z\}$. Omdat f een veelterm is volgt door een evidente afschatting, per definitie van c en d, dat

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) \leq c(x_1\ldots x_n z Y)^d,$$

en dus, omwille van de tweede van de definiërende vergelijkingen, dat

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) \leq c(x_1\ldots x_n z Y)^d \leq N < p_k.$$

De eerste vergelijking impliceert de congruentie

$$\begin{aligned}(1+(K+1)N!) - (1+(k+1)N!) &= \prod_{k=0}^{z}(1+(k+1)N!) - (1+(k+1)N!) \\ &\equiv 0-0=0 \mod (1+(k+1)N!).\end{aligned}$$

Analoog als in het bewijs van de eerste inclusie is dus $K \equiv k \mod (1+(k+1)N!)$. Per constructie is tevens $Y_i - j_{i,k} \mod p_k$ voor alle $i \in \{1,2,\ldots,m\}$. Omwille van de derde vergelijking en het feit dat $p_k \mid 1+(k+1)N!$ is de conclusie dus dat

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) \equiv f(x_1,\ldots,x_n,K,Y_1,\ldots,Y_m) \equiv 0 \mod p_k.$$

Hierboven hadden we al bekomen dat

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) < p_k.$$

Dan is, inderdaad,

$$f(x_1,\ldots,x_n,k,y_{1,k},\ldots,y_{m,k}) = 0$$

voor elke $k \in \{0,1,2,\ldots,z\}$. Daarmee is ook de tweede inclusie aangetoond. Dit beëindigt het bewijs van Lemma 6.12. ■

Omwille van Lemma 6.12 weten we dus dat D de projectie van D' op zijn eerste $n+1$ coördinaten is. Omdat D' diophantisch is, en projecties van diophantische verzamelingen opnieuw diophantisch zijn, is bijgevolg ook D diophantisch. Dit beëindigt het bewijs van Propositie 6.11. ■

Het bewijs van vorige stelling maakte gebruik van de volgende twee lemma's.

Lemma 6.13

De relatie

$$(z = \prod_{1 \le j \le Y} (Y_1 - j)) \wedge (Y_1 > Y)$$

in de variabelen (z, Y, Y_1) *is diophantisch.*

Bewijs. Merk op dat

$$\begin{aligned} z = (Y+1)!\binom{Y_1}{Y+1} \quad \Leftrightarrow \quad z &= (Y+1)!\,\frac{Y_1!}{(Y+1)!(Y_1-(Y+1))!} \\ &= \frac{Y_1!}{(Y_1-Y-1)!} \\ &= \prod_{0 \le \le j \le Y} (Y_1 - j). \end{aligned}$$

Bijgevolg is

$$(z = \prod_{0 \le j \le Y} (Y_1 - j)) \wedge (Y_1 > Y) \quad \Leftrightarrow \quad (z = (Y+1)!\binom{Y_1}{Y+1}) \wedge (Y_1 > Y).$$

Maar de relaties $z = (Y+1)!\binom{Y_1}{Y+1}$ en $Y_1 > Y$ zijn diophantisch wegens Lemma 6.15 en Lemma 6.16. Bijgevolg is de relatie

$$(z = (Y+1)!\binom{Y_1}{Y+1}) \wedge (Y_1 > Y)$$

diophantisch in (z, Y, Y_1). Dit beëindigt het bewijs van Lemma 6.13. ■

Lemma 6.14

De relatie

$$z = \prod_{0\leq k\leq y} (1+(k+1)n)$$

in de variabelen (z,y,n) is diophantisch.

Bewijs. We voeren twee extra variabelen u,v in; later zullen deze weer verdwijnen door uit te projecteren. Zij $u := n(1+(y+1)n)^{y+1}+1 \in \mathbb{N}$. Dan is $u > 0$. Het is duidelijk dat $\text{ggd}(u,n) = 1$. Dit impliceert dat n een inverse modulo u heeft; dat wil zeggen, er bestaat een $v \in \mathbb{N}$ zodat $vn \equiv 1 \mod u$. Beschouw nu de gelijkheden

$$n^{y+1}(y+1)!\binom{v+y+1}{y+1} = n^{y+1}(v+1)\dots(v+(y+1)) = (vn+n)\dots(vn+(y+1)n).$$

Per constructie van v toont dit aan dat

$$n^{y+1}(y+1)!\binom{v+y+1}{y+1} \equiv (1+n)\dots(1+(y+1)n) = \prod_{0\leq k\leq y} (1+(k+1)n) \mod u.$$

Merk nu op dat

$$\prod_{0\leq k\leq y} (1+(k+1)n) < u.$$

Inderdaad, indien $k \in \{0,1,\dots,y\}$, dan geldt

$$1+(y+1)n \geq 1+(k+1)n \quad \Rightarrow \quad u = n(1+(y+1)n)^{y+1}+1 > \prod_{0\leq k\leq y} (1+(k+1)n).$$

Maar de voorgaande feiten impliceren dan dat

$$\text{rem}\left(n^{y+1}(y+1)!\binom{v+y+1}{y+1}, u\right) = \prod_{0\leq k\leq y} (1+(k+1)n).$$

Omdat rem en exponentiatie diophantisch zijn, en omwille van Lemma 6.15 en Lemma 6.16, volgt hier na projectie op de coördinaten (z,y,n), dadelijk uit dat de relatie

$$z = \prod_{0\leq k\leq y} (1+(k+1)n)$$

met variabelen (z,y,n) diophantisch is. Dit beëindigt het bewijs van Lemma 6.14. ■

De vorige twee lemma's, namelijk Lemma 6.13 en Lemma 6.14, zijn eigenlijk verfijningen op grond van de volgende twee lemma's. Dit zijn echt de basisresultaten die duidelijk maken waarom het diophantisch zijn van exponentiatie belangrijk is; merk inderdaad tijdens de bewijzen van de volgende lemma's op dat we dikwijls gebruikmaken van dit erg belangrijk resultaat.

Lemma 6.15

De relatie

$$r = \binom{n}{k}, \quad n \geq k$$

in de variabelen (r,k,n) *is diophantisch.*

Bewijs. Merk op dat het voldoende is aan te tonen dat voor $u > n^k$ en $n \geq k$ geldt dat

$$\binom{n}{k} = \text{rem}\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u\right).$$

Inderdaad, noem G de verzameling bepaald door de relatie in de formulering van het lemma. Definieer deelverzamelingen van $\mathbb{N}^5$ in de coördinaten (r,k,n,u,v) door

$$\begin{aligned}
G_1 &:= \{(r,k,n,u,v) \in \mathbb{N}^5 \mid u > n^k\},\\
G_2 &:= \{(r,k,n,u,v) \in \mathbb{N}^5 \mid v = \lfloor (u+1)^n/u^k \rfloor\},\\
G_3 &:= \{(r,k,n,u,v) \in \mathbb{N}^5 \mid r \equiv v \mod u\},\\
G_4 &:= \{(r,k,n,u,v) \in \mathbb{N}^5 \mid r < u\},\\
G_5 &:= \{(r,k,n,u,v) \in \mathbb{N}^5 \mid n \geq k\}.
\end{aligned}$$

Natuurlijk is G_1 diophantisch omdat exponentiatie diophantisch is. Het is evident dat G_3, G_4 en G_5 diophantisch zijn. Nu moeten we enkel nog inzien dat G_2 diophantisch is. Merk echter op dat

$$v = \lfloor (u+1)^n/u^k \rfloor \quad \Leftrightarrow \quad (u+1)^n \leq u^k v < (u+1)^n + u^k.$$

Dit laatste is duidelijk diophantisch, opnieuw omdat exponentiatie diophantisch is. Uit de aanname van hierboven volgt dat

$$\begin{aligned}
r = \binom{n}{k}, \quad n \geq k \quad &\Leftrightarrow \quad \exists u \in \mathbb{N} \text{ zodat } r = \text{rem}\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u\right), \quad u > n^k, \quad n \geq k\\
&\Leftrightarrow \quad \exists u, v \in \mathbb{N} \text{ zodat } r < u, \quad v = \lfloor (u+1)^n/u^k \rfloor,\\
&\qquad\qquad r \equiv v \mod u, \quad u > n^k, \quad n \geq k.
\end{aligned}$$

Bijgevolg is G gelijk aan de projectie van $G_1 \cap G_2 \cap G_3 \cap G_4 \cap G_5$ op zijn eerste 3 coördinaten. Daar deze laatste verzameling diophantisch is als doorsnede van diophantische verzamelingen, en daar diophantische verzamelingen gesloten zijn onder projecties, volgt inderdaad dat G diophantisch is. De uitdrukking hierboven gegeven is dus inderdaad voldoende aan te tonen.
Zij nu $k,n,u \in \mathbb{N}$ zodat $n \geq k$ en $u > n^k$. Dan is

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k}.$$

Eerst bekijken we de eerste term; we beweren dat deze term kleiner dan of gelijk aan 1 is. Omdat $\binom{n}{i} \leq n^i$ is

$$\begin{aligned}\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} &\leq \sum_{i=0}^{k-1} n^i u^{i-k} \\ &= \sum_{i=0}^{k-1} n^i \left(\frac{1}{u}\right)^{k-i}.\end{aligned}$$

Omdat $u > n^k$ volgt dat

$$\sum_{i=0}^{k-1} n^i \left(\frac{1}{u}\right)^{k-i} < \sum_{i=0}^{k-1} n^i \left(\frac{1}{n^k}\right)^{k-i}.$$

We moeten nu enkel nog aantonen dat voor alle $i \in \{0,1,\ldots,k-1\}$ de ongelijkheid

$$n^i \left(\frac{1}{n^k}\right)^{k-i} \leq \frac{1}{n}$$

geldt; inderdaad, dit impliceert dan samen met bovenstaande dat

$$\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} < \sum_{i=0}^{k-1} n^i \left(\frac{1}{n^k}\right)^{k-i} \leq \sum_{i=0}^{k-1} \frac{1}{n} = \frac{k}{n} \leq 1.$$

Neem dus $i \in \{0,1,\ldots,k-1\}$. Daar $i \leq k-1$ volgt dat

$$i(k+1) \leq (k+1)(k-1) = k^2 - 1.$$

Of nog, $k(k-i) \geq i+1$. Dus is $n^{k(k-i)} \geq n^{i+1}$, of equivalent hiermee, $\frac{1}{n^{k(k-i)}} \leq \frac{1}{n^{i+1}}$. Vermenigvuldigen met n^i in beide leden levert inderdaad de gevraagde ongelijkheid.
Bekijk nu de tweede term; we hebben dat

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \prod_{i=1}^{k} \frac{n-(k-i)}{i} \leq \prod_{i=1}^{k} n = n^k < u.$$

De eerste ongelijkheid geldt hierboven daar

$$1 \leq i \leq k \quad \Rightarrow \quad i \geq 1 \geq \frac{n-k}{n-1} \quad \Rightarrow \quad n-(k-i) \leq ni \quad \Rightarrow \quad \frac{n-(k-i)}{i} \leq n.$$

Tot slot bestuderen we de laatste term; het is echter meteen duidelijk dat deze term deelbaar is door u.
Door de eigenschappen die we zojuist aangetoond hebben, geldt voor een zekere $t \in \mathbb{N}$ nu

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor = \left\lfloor \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k} \right\rfloor = \left\lfloor \binom{n}{k} + tu \right\rfloor = \binom{n}{k} + tu.$$

Omdat $\binom{n}{k} < u$ impliceert dit

$$\operatorname{rem}\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u \right) = \binom{n}{k}.$$

Dit beëindigt het bewijs van Lemma 6.15. ■

Lemma 6.16

De relatie

$$r = k!$$

in de variabelen (r,k) is diophantisch.

Bewijs. Merk op dat het voldoende is aan te tonen dat voor $k > 0$ en $n \geq (2k)^{k+1}$ geldt dat

$$k! = \left\lfloor \frac{n^k}{\binom{n}{k}} \right\rfloor.$$

Inderdaad, dit is duidelijk daar exponentiatie diophantisch is en omwille van Lemma 6.15; een volledig formeel bewijs kan gegeven worden precies zoals in het bewijs van Lemma 6.15.
Het volstaat dus voor alle $k > 0$ en $n \geq (2k)^{k+1}$ aan te tonen dat

$$k! < \frac{n^k}{\binom{n}{k}} < k! + 1.$$

Neem $k > 0$ en $n \geq (2k)^{k+1}$. Ten eerste,

$$\frac{n^k}{\binom{n}{k}} = \frac{n^k\, k!}{n(n-1)\ldots(n-(k-1))} = k!\,\frac{1}{\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{(k-1)}{n}\right)} > k!.$$

Dit bewijst alvast de eerste ongelijkheid.
De andere ongelijkheid is iets lastiger; neem $k > 0$ en $n \geq (2k)^{k+1}$ en merk om te beginnen op dat

$$\frac{k}{n} \leq \frac{k}{(2k)^{k+1}} = \frac{1}{2^{k+1}}\,\frac{1}{k^k} \leq \frac{1}{2^{k+1}} = \frac{1}{2}\,\frac{1}{2^k} < \frac{1}{2}.$$

Dus is

$$1 + \frac{2k}{n} = 1 + \frac{k}{n}\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots\right) > 1 + \frac{k}{n}\left(1 + \frac{k}{n} + \left(\frac{k}{n}\right)^2 + \ldots\right) = \frac{1}{1-\frac{k}{n}}.$$

Maar ook hebben we

$$\left(1+\frac{2k}{n}\right)^k = \sum_{i=0}^{k}\binom{k}{i}\left(\frac{2k}{n}\right)^i = 1 + \sum_{i=1}^{k}\binom{k}{i}\left(\frac{2k}{n}\right)^i < 1 + \frac{2k}{n}\sum_{i=1}^{k}\binom{k}{i} < 1 + \frac{2k}{n}\,2^k.$$

De eerste ongelijkheid hiervan geldt daar

$$\frac{2k}{n} < 1 \quad \Rightarrow \quad \forall i \in \{1,2,\ldots,k\} \text{ geldt } \left(\frac{2k}{n}\right)^i < \left(\frac{2k}{n}\right).$$

Nu is

$$\frac{n^k}{\binom{n}{k}} = k!\,\frac{1}{\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{(k-1)}{n}\right)} < k!\,\frac{1}{\left(1-\frac{k}{n}\right)^k}$$

$$< k! \left(1 + \frac{2k}{n}\right)^k < k! + k! \frac{2k}{n} 2^k < k! + k^k \frac{2k}{n} 2^k = k! + \frac{(2k)^{k+1}}{n} < k! + 1.$$

Hiermee is ook de andere ongelijkheid aangetoond. Dit beëindigt het bewijs van Lemma 6.16. ■

Tot slot brengen we het hoofdresultaat van deze sectie in herinnering.

Propositie 6.17

Er geldt dat de klasse van diophantische verzamelingen = D-sets.

Bewijs. Propositie 6.10 samen met Propositie 6.11 impliceert meteen het gevraagde. Dit beëindigt het bewijs van Propositie 6.17. ■

6.4 Bewijs van de DPRM-stelling

Uiteindelijk hebben we het hoofdresultaat.

Propositie 6.18

De r.e. sets = klasse van de diophantische verzamelingen. Dat wil zeggen, een verzameling is recursief opsombaar als en slechts als ze diophantisch is.

Bewijs. Propositie 6.9 samen met Propositie 6.17 levert direct dat r.e. sets = klasse van diophantische verzamelingen. Dit beëindigt het bewijs van Propositie 6.18. ■

6.5 Hilberts Tiende Probleem is onoplosbaar

Zoals de titel al zegt, tonen we in deze sectie eindelijk het hoofdresultaat van het eerste deel van de thesis aan: Hilberts Tiende Probleem over $\mathbb{Z}$ is onoplosbaar, dat wil zeggen er bestaat geen algoritme dat beslist of een veeltermvergelijking over de gehele getallen al dan niet een oplossing heeft.

Propositie 6.19

Hilberts Tiende Probleem over $\mathbb{Z}$ is onoplosbaar.

Bewijs. We tonen aan dat Hilberts Tiende Probleem over $\mathbb{N}$ onoplosbaar is; omwille van Propositie 4.1 is dit voldoende te bewijzen. Veronderstel uit het ongerijmde dat Hilberts Tiende Probleem over $\mathbb{N}$ wel oplosbaar is. Dat wil zeggen, er bestaat een Turingmachine die als input gehele veeltermen in een willekeurig aantal variabelen neemt, en als output 1 of 0 geeft, al naargelang de beschouwde veelterm al dan niet oplossingen in $\mathbb{N}$ heeft. Wegens Propositie 3.25 bestaat er een recursief opsombare verzameling van natuurlijke getallen die *niet* berekenbaar is; noem $K \subset \mathbb{N}$ zulk een

verzameling. Uit de DPRM-stelling, zijnde Propositie 6.18, volgt dat K diophantisch is. Dan bestaat er een veelterm $f \in \mathbb{Z}[t, x_1, \ldots, x_n]$ zodat

$$K = \{k \in \mathbb{N} \mid \exists x_1, \ldots, x_n \in \mathbb{N} \text{ zodat } f(k, x_1, \ldots, x_n) = 0\}.$$

Maar onze hypothese uit het ongerijmde samen met Definitie 3.7 geeft onmiddellijk dat $K \subset \mathbb{N}$ Turing berekenbaar is. Echter, uit sectie 3.3 weten we dat Turing berekenbaarheid precies hetzelfde is als berekenbaarheid (zoals in Definitie 3.11). Dit gegeven impliceert dan dat $K \subset \mathbb{N}$ berekenbaar is. Contradictie. Bijgevolg is Hilberts Tiende Probleem over $\mathbb{N}$ onoplosbaar. Dit beëindigt het bewijs van Propositie 6.19. ■

Deel III

Definieerbaarheid van $\mathbb{Z}$ in $\mathbb{Q}$

HOOFDSTUK 7

QUATERNIONENALGEBRA'S

In deze sectie definiëren we wat we bedoelen met een *quaternionenalgebra*. Voor een gegeven veld K voeren we daartoe eerst het begrip *K-algebra* in. Daarna gaan we het verband na met het *Hasse-Minkowski principe*. We tonen dit principe ook in zijn algemeenheid aan.

In dit hoofdstuk, en bij uitbreiding de hele thesis, veronderstellen we voor een gegeven veld steeds dat de karakteristiek ervan verschillend is van 2. Dit maakt sommige resultaten wat makkelijker te formuleren; het geval dat de karakteristiek gelijk is aan 2 is een vervelend geval, en apart te behandelen.

7.1 Definitie

We beginnen meteen met een aantal definities.

Definitie 7.1

Zij K een veld. We noemen A een associatieve *K-algebra* indien A een vectorruimte over K is en bovendien uitgerust met een binaire operatie $\cdot : A \times A \to A$, zodat voor alle $x, y, z \in A$ en alle $a, b \in K$ geldt dat

- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $(x + y) \cdot z = x \cdot z + y \cdot z$
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $(ax) \cdot (by) = (ab)(x \cdot y)$.

Indien er een element in A bestaat, genoteerd als 1_A of ook wel 1 als er geen verwarring mogelijk is, zodat voor alle $a \in A$ geldt dat $a \cdot 1_A = 1_A \cdot a = a$, dan noemen we A een K-algebra met eenheidselement. We definiëren bovendien de *dimensie van A* als $\dim V$.

Op een K-algebra is dus een product gedefinieerd. De drie eigenschappen hierboven zeggen dat de afbeelding $\cdot : A \times A \to A$ bilineair is. Merk op dat indien A een K-algebra met eenheidselement is, dan $(A, +, \cdot)$ een ring is.

We geven een voorbeeld dat later nog van pas komt. Zij een K-algebra A gegeven. Voor elke $n \in \mathbb{N}$ definiëren we $M_n(A)$ als de verzameling van $(n \times n)$-matrices over A. Door componentsgewijs een optelling en scalaire vermenigvuldiging te definiëren is $M_n(A)$ een vectorruimte over K. Op $M_n(A)$ definiëren we het product van twee

matrices als de gewoonlijke matrixvermenigvuldiging. Het is evident dat $M_n(A)$ op deze wijze opnieuw een K-algebra is en bovendien dimensie $n^2 \dim A$ heeft.

Merk op dat indien E een velduitbreiding is van een veld K, dan E een K-algebra met eenheidselement is; het omgekeerde is duidelijk niet altijd waar.

Volgende definitie is erg logisch.

Definitie 7.2

> Een *homomorfisme tussen K-algebra's A* en A' is een afbeelding $f : A \to A'$ zodat voor alle $x, y \in A$ en $a, b \in K$ geldt dat
>
> - $f(ax+by) = af(x)+bf(y)$
> - $f(x \cdot y) = f(x) \cdot f(y)$.
>
> Hierbij stelt $\cdot$ het product van zowel A als A' voor. Indien A en A' eenheidselementen hebben, dan eisen we ook nog dat $f(1) = 1$. Indien f bijectief is, dan noemen we A en A' *isomorf* en dat noteren we met $A \cong A'$.

Indien er sprake is van meerdere eenheidselementen dan schrijven we soms expliciet 1_A of 1_K om verwarring te vermijden.

Definitie 7.3

> Een K-algebra A wordt een *divisiealgebra* genoemd indien A een eenheidselement heeft en elk element van A dat verschillend van nul is, een multiplicatieve inverse heeft, dat wil zeggen voor elke $0 \neq a \in A$ bestaat er een $x \in A$ zodat $a \cdot x = x \cdot a = 1$.

We willen stilaan toewerken naar de definitie van een quaternionenalgebra. Daartoe hebben we volgende definities nodig.

Definitie 7.4

> We noemen een K-algebra A *centraal*, indien A een eenheidselement heeft en het centrum van A gelijk is aan K; dat wil zeggen, $K = Z(A) = \{x \in A \,|\, x \cdot a = a \cdot x$ voor alle $a \in A\}$.

Bij bovenstaande definitie hoort een opmerking. Uiteraard dient K geen deelverzameling van A te zijn. Maar om in A toch over de elementen van K te kunnen spreken, gebruiken we de afbeelding $K \to A : k \mapsto k\,1_A$. Deze afbeelding is immers een injectief ringmorfisme; inderdaad, dit volgt eenvoudig uit verschillende axioma's van een veld, vectorruimte en algebra. Merk op dat $1_K \in K$ onder deze identificatie overeenkomt met het element $1_A \in A$. Tevens is het zo dat de inclusie $K \subset \{x \in A \,|\, x \cdot a = a \cdot x$ voor alle $a \in A\}$ steeds geldt; dat volgt wegens de laatste conditie in Definitie 7.1.

Definitie 7.5

> Een K-algebra A is *simpel*, indien A een eenheidselement heeft en de ring A simpel is; dat wil zeggen, de enige tweezijdige idealen van de ring A zijn $\{0\}$ en A.

Uiteindelijk komen we tot de notie van quaternionenalgebra.

Definitie 7.6

> Een *quaternionenalgebra* is een vierdimensionale K-algebra die centraal en simpel is.

Merk op dat een quaternionenalgebra niet commutatief kan zijn; anders zou immers wegens centraliteit gelden dat $A = K$, hetgeen in contradictie is met $\dim A = 4$.

In het geval dat $K = \mathbb{R}$ is de $\mathbb{R}$-algebra van Hamiltoniaanse quaternionen $\mathbb{H}$ het standaardvoorbeeld van een quaternionenalgebra.

7.2 Classificatie

We willen de quaternionenalgebra's over een gegeven veld K classificeren, op isomorfisme na. Daartoe hebben we volgend resultaat, dat een speciaal geval is van *Wedderburns stelling*.

Propositie 7.7

> *Een quaternionenalgebra over een veld K is ofwel isomorf met de K-algebra $M_2(K)$ ofwel isomorf met een divisiealgebra over K.*

Bewijs. Zie [24] voor Wedderburns stelling. In het algemeen zegt Wedderburns stelling het volgende: een centrale simpele eindigdimensionale K-algebra is isomorf met de K-algebra $M_n(D)$ voor een zekere $n \in \mathbb{N}$ en een divisiealgebra D over K. Dus als A een quaternionenalgebra over K is, dan moet $4 = \dim A = n^2 \dim D$. Bijgevolg deelt n^2 het getal 4, zodat $n = 2$ of $n = 1$. Indien $n = 2$ dan is $D \cong K$, en dus is $A \cong M_2(K)$. Indien $n = 1$ dan is $A \cong M_1(D) = D$ isomorf met de divisiealgebra D over K. Dit beëindigt het bewijs van Propositie 7.7. ■

We mogen dus vanaf nu veronderstellen dat elke quaternionenalgebra over K ofwel $M_2(K)$ is, ofwel een divisiealgebra over K is.

Propositie 7.8

> *Zij A een K-algebra met eenheidselement. Dan is A een quaternionenalgebra over K als en slechts als er $i, j \in A$ en $a, b \in K^\times$ bestaan zodat*
>
> $$i^2 = a, \quad j^2 = b, \quad i \cdot j = -j \cdot i$$
>
> *en zodat $\{1, i, j, i \cdot j\}$ een basis van A over K (als vectorruimte) is.*

Bewijs. Uit de hierboven gegeven relaties voor een quaternionenalgebra volgen een aantal andere relaties; we sommen ze hier op omdat we ze verderop voortdurend zullen gebruiken. We hebben

$$i \cdot j \cdot i = -aj, \quad j \cdot i \cdot j = -bi, \quad i \cdot j \cdot i \cdot j = j \cdot i \cdot j \cdot i = -ab.$$

We beginnen met de eerste implicatie. Veronderstel eerst dat $A = M_2(K)$. Indien

$$i := \begin{pmatrix} 0 & 1_K \\ 1_K & 0 \end{pmatrix} \in A, \quad j := \begin{pmatrix} 0 & 1_K \\ -1_K & 0 \end{pmatrix} \in A$$

dan zien we dat

$$i^2 = \begin{pmatrix} 1_K & 0 \\ 0 & 1_K \end{pmatrix} = 1_K \begin{pmatrix} 1_K & 0 \\ 0 & 1_K \end{pmatrix}, \; j^2 = \begin{pmatrix} -1_K & 0 \\ 0 & -1_K \end{pmatrix} = (-1_K) \begin{pmatrix} 1_K & 0 \\ 0 & 1_K \end{pmatrix}.$$

Onder identificatie, zoals uitgelegd in de opmerking na Definitie 7.19, hebben we dus dat $i^2 = 1_K \in K^\times$ en $j^2 = -1_K \in K^\times$. Duidelijk is ook $i \cdot j = -j \cdot i$. Bovendien is

$$\{1, i, j, i \cdot j\} = \left\{ \begin{pmatrix} 1_K & 0 \\ 0 & 1_K \end{pmatrix}, \begin{pmatrix} 0 & 1_K \\ 1_K & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1_K \\ -1_K & 0 \end{pmatrix}, \begin{pmatrix} -1_K & 0 \\ 0 & 1_K \end{pmatrix} \right\}$$

een basis van A over K. Merk op dat we voor dit laatste gebruikmaken van het feit dat $\mathrm{kar}(K) \neq 2$.
Veronderstel nu dat A een divisiealgebra is. Kies $i \in A \setminus K$ en beschouw de veluitbreiding $K(i')$. Merk op dat $K(i')$ een commutatieve deelalgebra van A is. We hebben $[A : K] = 4$. Dus $[K(i') : K] = 1, 2$ of 4 wegens de productformule. Maar $[K(i') : K] = 1$ impliceert de contradictie $i' \in K$, en $[K(i') : K] = 4$ impliceert dat $K(i') = A$, hetgeen ook niet kan daar $K(i')$ commutatief is maar de quaternionenalgebra A niet. Dus $[K(i') : K] = 2$. We mogen zonder verlies van algemeenheid veronderstellen dat $i' \in A \setminus K$ zodanig is dat $i'^2 =: a' \in K$. Inderdaad; duidelijk is $\{1, i'\}$ een basis van $K(i)$ over K, dus stel dat $i'^2 = a_1 + a_2 i'$ voor $a_1, a_2 \in K$. Definieer nu $t := i' - \frac{a_2}{2} \in K(i') \setminus K$; dit kan omdat we steeds veronderstellen dat $\mathrm{kar}(K) \neq 2$. Dan is $t^2 = a_1 + \frac{a_2}{4} \in K$. Bovendien is het evident dat $K(i') = K(t)$. Nu is $[A : K(i')] = 2$ wegens de productformule. Dus vinden we, analoog als hierboven, een $j \in A \setminus K(i')$ zodanig dat $A = (K(i'))(j') = K(i', j')$ en $j'^2 =: b' \in K(i')$. Nogmaals hetzelfde argument toepassen levert dat we $b' = j'^2$ zonder verlies van algemeenheid zelfs in K mogen veronderstellen. We hebben dus de vierdegraadsuitbreiding $A = K(i', j')$ van K met $i'^2 = a' \in K$ en $j'^2 = b' \in K$. Uit de productformule volgt dat $\{1, i', j', i' \cdot j'\}$ een basis vormt van A over K. Definieer nu $\alpha := i' \cdot j' + j' \cdot i'$. Door ieder element van A in de basis $\{1, i', j', i' \cdot j'\}$ uit te schrijven, bekomen we na een simpele berekening dat α in het centrum van A zit. Per definitie is dat gelijk aan K, zodat $\alpha \in K$. Definieer nu $i := i' - \frac{\alpha}{b'} j'$ en $j := j'$. Men rekent eenvoudigweg na dat dan $i \cdot j = -j \cdot i$. Ook is $i^2 =: a \in K^\times$ en $j^2 =: b \in K^\times$. Bovendien vormt $\{1, i, j, i \cdot j\}$ een basis van A over K als vectorruimte.
Nu tonen we de omgekeerde implicatie aan. Veronderstel dus dat $i^2 = a \in K^\times$, $j^2 = b \in K^\times$ en $i \cdot j = -j \cdot i$ met $i, j \in A$ zodat $\{1, i, j, i \cdot j\}$ een basis is van A over K. Meteen hebben we dat $\dim A = 4$. Dan tonen we aan dat A centraal is. We weten al

dat K een deel van het centrum van A is. Kies dus een $x \in A$ zodat voor elke $t \in A$ geldt dat $x \cdot t = t \cdot x$. Kies een $t \in A$ vast en schrijf zowel x als t uit ten opzichte van de basis $\{1, i, j, i \cdot j\}$, zodat $x = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j$ en $t = t_1 + t_2 i + t_3 j + t_4 i \cdot j$ met $\lambda_i, t_i \in K$ voor alle i. Indien we dan de producten uit de vergelijking $x \cdot t = t \cdot x$ zo uitrekenen, dan krijgen we door de bovenstaande relaties te gebruiken na een lange maar makkelijke berekening het stelsel van drie vergelijkingen

$$\begin{cases} \lambda_3 t_4 = \lambda_4 t_3 \\ \lambda_4 t_2 = \lambda_2 t_4 \\ \lambda_3 t_2 = \lambda_2 t_3 \end{cases}.$$

Dit geldt voor alle $t_1, t_2, t_3, t_4 \in K$. Door $t_3 = 0$ en $t_4 = 1$ te nemen volgt uit de eerste vergelijking meteen dat $\lambda_3 = 0$. Analoog volgt uit vergelijkingen twee en drie dat $\lambda_4 = 0$ en $\lambda_2 = 0$, respectievelijk. Dan is inderdaad $x = \lambda_1 \in K$. Tot slot tonen we aan dat A simpel is. Zij $I \subset A$ een tweezijdig ideaal van A dat verschillend is van $\{0\}$. Zij $x = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j \in I \setminus \{0\}$. We mogen zonder verlies van algemeenheid veronderstellen dat $\lambda_1 = 1$. Inderdaad; dit is duidelijk indien $\lambda_1 \neq 0$, want dan kunnen we beide leden gewoon door λ_1 delen, en dat element zit opnieuw in I daar I een ideaal van A is. Indien $\lambda_1 = 0$ dan is $x = \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j \in I$. Dus is $i \cdot x = \lambda_2 b + a\lambda_4 j + \lambda_3 i \cdot j \in I$, daar I een tweezijdig ideaal is. Opnieuw, indien $\lambda_2 \neq 0$ dan zijn we klaar. Indien $\lambda_2 = 0$, dan is $x \cdot j = \lambda_3 b + \lambda_4 bi \in I$, daar I een tweezijdig ideaal is. Indien $\lambda_3 \neq 0$ dan zijn we klaar. In het geval dat $\lambda_3 = 0$ dan kunnen we analoog verder redeneren zoals we nu al een paar keer gedaan hebben. Uiteindelijk, indien we in het geval $\lambda_1 = \lambda_2 = \lambda_3 = 0$ zijn, dan is $x = \lambda_4 i \cdot j \in I$, met $\lambda_4 \neq 0$ omdat $x \neq 0$. Dus is $\left(\frac{-1}{\lambda_4 ab}\right) i \cdot j \cdot x = 1 \in I$ daar I een tweezijdig ideaal is. Hieruit volgt dat $I = A$, en zijn we klaar. Dit alles om vanaf nu te mogen veronderstellen dat $\lambda_1 = 1$. Definieer vervolgens

$$y := \frac{1}{2}\left(x + \frac{1}{a} i \cdot x \cdot i\right) \in I.$$

Dit geldt daar $x \in I$ en I een tweezijdig ideaal van A is, en ook $\mathrm{kar}(K) \neq 2$. We vinden door te rekenen dat $y = 1 + \lambda_2 i$. Definieer analoog

$$z := \frac{1}{2}\left(y + \frac{1}{b} j \cdot y \cdot j\right) \in I.$$

Dit geldt daar $y \in I$ en I een tweezijdig ideaal van A is, en ook $\mathrm{kar}(K) \neq 2$. We vinden door te rekenen makkelijk dat $z = 1$. Dus is $1 \in I$, hetgeen impliceert dat $I = A$. Dit beëindigt het bewijs van Propositie 7.8. ■

Bovendien kan men aantonen dat, *voor elke keuze van* $a, b \in K^\times$, er een quaternionenalgebra A over K bestaat die een basis $\{1, i, j, i \cdot j\}$, met $i, j \in A$, heeft die voldoet aan

$$i^2 = a, \quad j^2 = b, \quad i \cdot j = -j \cdot i.$$

Uiteraard is zo'n algebra op isomorfisme na uniek. Op die manier komen we bij volgende definitie.

Definitie 7.9

De, op isomorfisme na unieke, K-algebra met eenheidselement die een basis $\{1, i, j, i \cdot j\}$ heeft die voldoet aan

$$i^2 = a, \quad j^2 = b, \quad i \cdot j = -j \cdot i$$

met $i, j \in A$ en $a, b \in K^\times$ wordt genoteerd met $\left(\frac{a,b}{K}\right)$ en wordt de *quaternionenalgebra over K, voortgebracht door i en j, die voldoet aan de relaties* $i^2 = a$, $j^2 = b$ *en* $i \cdot j = -j \cdot i$, genoemd.

Definitie 7.10

Voor $a, b \in \mathbb{Q}^\times$ definiëren we $H_{a,b} := \left(\frac{a,b}{\mathbb{Q}}\right)$.

7.3 Norm en spoor

Beschouw opnieuw een veld K en een willekeurige K-quaternionenalgebra. Wegens de vorige sectie is een K-quaternionenalgebra van de vorm $A = \left(\frac{a,b}{K}\right)$, met basis $\{1, i, j, i \cdot j\}$ en $a, b \in K^\times$ zodat $i^2 = a$, $j^2 = b$ en $i \cdot j = -j \cdot i$.

Ieder element van $\alpha \in A$ kan dus in de vorm $\alpha = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j$ geschreven worden, met $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in K$. We definiëren de *involutie van* α dan als

$$\overline{\alpha} = \overline{\lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j} := \lambda_1 - \lambda_2 i - \lambda_3 j - \lambda_4 i \cdot j.$$

Op die manier definieert de involutie een afbeelding $A \to A : \alpha \mapsto \bar{\alpha}$. Door de regels van vermenigvuldiging in deze quaternionenalgebra te gebruiken, rekent men makkelijk na dat bovendien geldt dat

$$\alpha \cdot \bar{\alpha} = \bar{\alpha} \cdot \alpha = \lambda_1^2 - a\lambda_2^2 - b\lambda_3^2 + ab\lambda_4^2 \in K.$$

We hebben ook dat

$$\alpha + \bar{\alpha} = 2\lambda_1 \in K.$$

Zo komen we bij volgende definitie.

Definitie 7.11

Zij A een quaternionenalgebra over een veld K. Dan noemen we de afbeelding

$$N : A \to K : \alpha \mapsto \alpha \cdot \bar{\alpha}$$

de *gereduceerde norm op A* en $N(\alpha)$ de *norm van* α.
De afbeelding

$$S : A \to K : \alpha \mapsto \alpha + \bar{\alpha}$$

noemen we het *gereduceerde spoor op A* en $S(\alpha)$ het *spoor van* α.

Definitie 7.12

Zij $\alpha \in A$. De veelterm

$$x^2 - S(\alpha)x + N(\alpha) \in K[x]$$

noemen we de *gereduceerde karakteristieke veelterm van* $\alpha \in A$.

Merk op dat

$$\alpha^2 - S(\alpha)\alpha + N(\alpha) = \alpha^2 - (\alpha + \bar{\alpha}) \cdot \alpha + (\alpha \cdot \bar{\alpha}) = 0,$$

voor elke $\alpha \in A$. Dat wil zeggen, elk element van een quaternionenalgebra is een nulpunt van zijn gereduceerde karakteristieke veelterm. Later zullen we hier gebruik van maken.

De norm heeft interessante toepassingen. Het zal ons toelaten te bepalen wanneer we in Propositie 7.7 een divisiealgebra hebben, en wanneer de algebra isomorf is met $M_2(K)$. Maar eerst bewijzen we een paar evidente eigenschappen.

Propositie 7.13

Zij A een quaternionenalgebra over een veld K. Dan is de afbeelding N multiplicatief; dat wil zeggen voor alle $\alpha, \beta \in A$ *geldt dat*

$$N(\alpha \cdot \beta) = N(\alpha)N(\beta),$$

en de afbeelding S is additief; dat wil zeggen, er geldt

$$S(\alpha + \beta) = S(\alpha) + S(\beta)$$

voor alle $\alpha, \beta \in A$.

Bewijs. Neem $\alpha, \beta \in A$. Om de multiplicativiteit te bewijzen moeten we aantonen dat

$$\alpha \cdot \beta \cdot \overline{\alpha \cdot \beta} = N(\alpha \cdot \beta) = N(\alpha)N(\beta) = \alpha \cdot \bar{\alpha} \cdot \beta \cdot \bar{\beta}.$$

We schrijven α en β uit ten opzichte van de basis $\{1, i, j, i \cdot j\}$ van A. Bovenstaande vergelijking kan dan verder uitgerekend worden aan de hand van de formule voor het product $\alpha \cdot \bar{\alpha}$ voor Definitie 7.11 drie maal te gebruiken. Een lange maar triviale berekening geeft inderdaad het gevraagde.
De additiviteit van S volgt sneller; het is immers duidelijk dat

$$S(\alpha + \beta) = \alpha + \beta + \overline{\alpha + \beta} = \alpha + \beta + \overline{\alpha} + \overline{\beta} = \alpha + \overline{\alpha} + \beta + \overline{\beta} = S(\alpha) + S(\beta).$$

Dit beëindigt het bewijs van Propositie 7.13. ■

Propositie 7.14

Zij A een quaternionenalgebra over een veld K en zij $\alpha \in A$. Dan is α inverteerbaar als en slechts als $N(\alpha) \neq 0$, en in dat geval is $\alpha^{-1} = \bar{\alpha}/N(\alpha)$.

Bewijs. Stel eerst dat $\alpha \in A$ inverteerbaar is. Dat wil zeggen dat er een $\beta \in A$ zodat $\alpha \cdot \beta = \beta \cdot \alpha = 1$. Door van deze uitdrukking de norm te nemen en de multiplicativiteit uit Propositie 7.13 toe te passen, verkrijgen we dat

$$N(\alpha)N(\beta) = N(\beta)N(\alpha) = N(1) = 1.$$

Bijgevolg moet $N(\alpha) \neq 0$.
Omgekeerd, veronderstel dat $N(\alpha) \neq 0$. Dan is

$$\frac{\bar{\alpha}}{N(\alpha)} \cdot \alpha = \alpha \cdot \frac{\bar{\alpha}}{N(\alpha)} = 1.$$

Dus α is inderdaad inverteerbaar, en $\alpha^{-1} = \bar{\alpha}/N(\alpha)$. Dit beëindigt het bewijs van Propositie 7.14. ■

We leggen nu een link met de theorie van kwadratische ruimtes. Daartoe herhalen we kort de definitie van *kwadratische ruimte*. In een volgende sectie gaan we er dieper op in; we verwijzen naar Definitie 8.1.

Propositie 7.15

Zij A een quaternionenalgebra over een veld K. Dan is (A,N) een kwadratische ruimte.

Bewijs. De eerste voorwaarde is eenvoudig; kies namelijk $\lambda \in K$ en $x \in A$, en schrijf $x = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 i \cdot j$. Dan is wegens de berekening voor Definitie 7.11

$$N(\lambda x) = \lambda\lambda_1 + \lambda\lambda_2 i + \lambda\lambda_3 j + \lambda\lambda_4 i \cdot j = \lambda^2(\lambda_1^2 - a\lambda_2^2 - b\lambda_3^2 + ab\lambda_4^2) = \lambda^2 N(x).$$

Voor de tweede voorwaarde moeten we nagaan dat de afbeelding

$$B : A \times A \to K(x,y) \mapsto B(x,y) := \frac{1}{2}\left(N(x+y) - N(x) - N(y)\right)$$

bilineair is. Door op te merken dat $\overline{x+y} = \bar{x} + \bar{y}$, dat wil zeggen de lineariteit van de involutie, hebben we voor alle $x,y \in A$ dat $(x+y) \cdot (\overline{x+y} - \bar{x} - \bar{y}) = 0$. Na verdere expansie bekomen we dat

$$(x+y) \cdot \overline{x+y} - x\bar{x} - y\bar{y} = x\bar{y} + y\bar{x}.$$

Dus volgt per definitie van N de identiteit

$$N(x+y) - N(x) - N(y) = (x+y) \cdot \overline{(x+y)} - x\bar{x} - y\bar{y} = x\bar{y} + y\bar{x}.$$

Door opnieuw de lineariteit van de involutie te gebruiken volgt hier onmiddellijk uit dat B bilineair is. Dit beëindigt het bewijs van Propositie 7.15. ■

Deze stelling zegt dat elke quaternionenalgebra via zijn gereduceerde normafbeelding op natuurlijke wijze ook een kwadratische ruimte is.

Nu brengen we het Hilbertsymbool in herinnering, zoals bijvoorbeeld ingevoerd in [7]. Zij K een veld en $a,b \in K^\times$. Het *Hilbertsymbool van a,b over K* is gedefinieerd als

$$(a,b)_K := \begin{cases} +1 & \text{indien er } x,y \in K \text{ bestaan zodat } ax^2+by^2=1, \\ -1 & \text{in het andere geval.} \end{cases}$$

Indien $K=\mathbb{R}$ voor een priemgetal p dan noteren we verkort ook wel $(a,b)_p$ in plaats van $(a,b)_{\mathbb{Q}_p}$. Indien $K=\mathbb{Q}$ dan noteren we dikwijls ter afkorting $(a,b)_\infty$ in plaats van $(a,b)_{\mathbb{R}}$.

Volgend resultaat is essentieel.

Propositie 7.16

Zij K een veld, $a,b \in K^\times$ en de quaternionenalgebra $A = \left(\frac{a,b}{K}\right)$ gegeven. Dan zijn de volgende uitspraken equivalent.

1. *$A \cong \left(\frac{1,-1}{K}\right) \cong M_2(K)$ als K-algebra's.*
2. *A is geen divisiealgebra.*
3. *A is isotropisch als kwadratische ruimte, dat wil zeggen er bestaat een $0 \neq \alpha \in A$ met $N(\alpha)=0$.*
4. *De vergelijking $ax^2+by^2=1$ is oplosbaar over K, dat wil zeggen $(a,b)_K=1$.*
5. *$a \in N_{K(\sqrt{b})/K}(K(\sqrt{b}))$, met $N_{K(\sqrt{b})/K} : K(\sqrt{b}) \to K$ de norm van velden.*

Bewijs. Merk ten eerste op dat $\left(\frac{1,-1}{K}\right) \cong M_2(K)$ als K-algebra's; inderdaad, we hebben dat het K-algebra morfisme geïnduceerd door

$$i \in \left(\frac{1,-1}{K}\right) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(K), \quad j \in \left(\frac{1,-1}{K}\right) \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(K)$$

een K-algebra isomorfisme is, zoals eenvoudig geverifieerd kan worden.
1. $\Rightarrow$ 2.: Stel zonder verlies van algemeenheid dat $A = \left(\frac{1,-1}{K}\right)$. Beschouw het element $i+1 \in A$. Dan is $N(i+1) = 1^2-1^2+0^2-0^2 = 0$, zodat uit Propositie 7.14 volgt dat $i+1$ niet inverteerbaar is. Dus A is geen divisiealgebra.
2. $\Rightarrow$ 1.: Dit volgt uit Propositie 7.7.
2. $\Rightarrow$ 3.: Dit is triviaal wegens Propositie 7.14.
3. $\Rightarrow$ 2.: Ook dit is triviaal wegens Propositie 7.14.

3. $\Rightarrow$ 4.: Dit is de minst eenvoudige implicatie uit de reeks. Hier is wat meer geavanceerde kennis over de theorie van kwadratische vormen voor nodig, die niet moeilijk is maar wel langdradig; daarom geven we een verwijzing, bijvoorbeeld naar Theorem 2.2.10 in [25].
4. $\Rightarrow$ 3.: Stel dat $ax^2 + by^2 = 1$ voor zekere $x, y \in K$. Dan is

$$1^2 - ax^2 - by^2 + ab\,0^2 = 1 - ax^2 - by^2 = 0.$$

Bijgevolg is $N(1 + xi + yj) = 0$ en bovendien is duidelijk $1 + xi + yj \neq 0$.
4. $\Rightarrow$ 5.: Stel dat $ax^2 + by^2 = 1$ voor zekere $x, y \in K$. Herinner dat de norm op kwadratische velduitbreidingen bewezen kan worden gelijk te zijn aan

$$N_{K(\sqrt{b})/K} : K(\sqrt{b}) \to K : \lambda_1 + \lambda_2\sqrt{b} \mapsto \lambda_1^2 - b\lambda_2^2,$$

waarbij we duidelijk mogen veronderstellen dat $b \in K^\times$ geen kwadraat is. Maar het feit dat b geen kwadraat is impliceert dat $x \neq 0$. Dan hebben we dat

$$N_{K(\sqrt{b})/K}\left(\frac{1}{x} + \frac{y}{x}\sqrt{b}\right) = \frac{1}{x^2} - b\frac{y^2}{x^2} = \frac{1 - by^2}{x^2} = a,$$

zodat inderdaad $a \in N_{K(\sqrt{b})/K}(K(\sqrt{b}))$.
5. $\Rightarrow$ 4.: Stel dat er $\lambda_1, \lambda_2 \in K$ bestaan zodat $\lambda_1^2 - b\lambda_2^2 = a$. Dan is $a + b\lambda_2^2 = \lambda_1^2$. Uit Gevolg 7.1.5 en Eigenschap 7.1.4 in [7] volgt dan dat

$$(a, b)_K = (a, \lambda_2^2)_K = 1.$$

Per definitie wil dit zeggen dat er $x, y \in K$ bestaan zodat $ax^2 + by^2 = 1$. Dit beëindigt het bewijs van Propositie 7.16. ■

Definitie 7.17

> Zij A een quaternionenalgebra over een veld K.. Indien een van de equivalente voorwaarden in Propositie 7.16 geldt, dan zeggen we dat A *splijt*, of *niet ramifieert*, over K. In het andere geval zeggen we dat A *niet splijt*, of *ramifieert*, over K.

7.4 Tensorproduct

We zeggen nu wat we bedoelen met het *tensorproduct* van twee algebra's gedefinieerd over eenzelfde veld.

Definitie 7.18

Zij K een veld en A, B twee K-algebra's. Het *tensorproduct van A en B* is dan de K-algebra voortgebracht door K-lineaire combinaties van elementen van de vorm $a \otimes b$, met $a \in A$ en $b \in B$, waarvoor voor alle $a, d \in A$ en $b, c \in B$ de regels

- $\lambda(a \otimes b) = (\lambda a) \otimes b = a \otimes (\lambda b)$
- $(a \otimes b) + (d \otimes b) = (a + d) \otimes b$
- $(a \otimes b) + (a \otimes c) = a \otimes (b + c)$

gelden, en waarvoor het product gedefinieerd wordt door

$$(a \otimes b) \cdot (d \otimes c) := ad \otimes bc$$

voor alle $a, d \in A$, $b, c \in B$. Deze operaties worden vervolgens lineair uitgebreid tot een operatie tussen elk tweetal K-lineaire combinaties van zulke elementen $a_i \otimes b_i$. Deze K-algebra wordt genoteerd als $A \otimes_K B$, of kortweg $A \otimes B$ indien het gebruikte veld uit de context duidelijk is.

Merk op dat deze definitie niet heel exact is: formeel gezien moet deze constructie gedaan worden door eerst de vrije vectorruimte over het veld K op de verzameling $A \times B$ te beschouwen, en daarna de quotiëntvectorruimte hiervan te construeren die bekomen wordt door uit te delen naar de deelruimte voortgebracht door de drie relaties hierboven opgesomd. Men kan aantonen dat op deze manier $A \otimes_K B$ inderdaad een goed gedefinieerde K-algebra is.

We formuleren en bewijzen nu twee evidente lemma's, die we verderop gebruiken om de belangrijke Propositie 7.21 aan te tonen.

Lemma 7.19

Het centrum van een simpele ring is een veld.

Bewijs. Zij A een ring die simpel is. Natuurlijk is $Z(A)$ een commutatieve ring. Bijgevolg is het voldoende aan te tonen dat elk niet-nul element van $Z(A)$ een inverse heeft. Kies een $x \in Z(A)$ zodat $x \neq 0$. Omdat A simpel is, is $(x) = (0)$ of $(x) = A$. Duidelijk kan dit eerste geval niet, daar $x \neq 0$. Dus $(x) = A$. Bijgevolg is $1 \in A = (x)$, zodat er een $a \in A$ bestaat zodat $1 = a \cdot x = x \cdot a$. Nu volstaat het te bewijzen dat $a \in Z(A)$. Maar dit is evident; neem namelijk $t \in A$, dan is $t = a' \cdot x$ voor een $a' \in A$, zodat

$$t \cdot a = (a' \cdot x) \cdot a = a' \cdot (x \cdot a) = a' = (x \cdot a) \cdot a' = x \cdot (a \cdot a') = (a \cdot a') \cdot x = a \cdot (a' \cdot x) = a \cdot t.$$

Dit beëindigt het bewijs van Lemma 7.19. ■

Lemma 7.20

Een simpele algebra over een veld is een centrale simpele algebra over zijn centrum.

Bewijs. Zij K een veld en A een simpele K-algebra. Dan is A een simpele ring, zodat uit Lemma 7.19 volgt dat $Z(A)$ een veld is. Nu is $A \supset Z(A)$ een velduitbreiding van het veld $Z(A)$, zodat A inderdaad een $Z(A)$-algebra is. Per constructie is A dan een centrale $Z(A)$-algebra. Ook is A een simpele $Z(A)$-algebra omdat het simpel zijn van een algebra enkel afhankelijk is van de ring zelf, en niet van het onderliggend veld. Dit beëindigt het bewijs van Lemma 7.20. ■

We hebben volgend resultaat.

Propositie 7.21

Zij K een veld, A een centrale simpele K-algebra, en B een simpele K-algebra. Dan is $A \otimes_K B$ een centrale simpele $Z(B)$-algebra, met $Z(B)$ het centrum van de ring B.

Bewijs. We tonen eerst aan dat $A \otimes_K B$ een simpele K-algebra is. Veronderstel dat $I \subset A \otimes_K B$ een ideaal van $A \otimes_K B$ is dat verschillend is van het nulideaal. Er bestaat een element $x \neq 0$ met $x = \sum_{i=1}^{n} a_i \otimes b_i \in I$ met n minimaal, en alle $a_i \in A$ en $b_i \in B$. Wegens minimaliteit is $a_1 \neq 0$. Omdat de ring A simpel is, volgt dat het ideaal voortgebracht door a_1 gelijk moet zijn aan de hele ring A; met andere woorden $Aa_1A = A$. Daar $1 \in A$ bestaan er bijgevolg $c_j, d_j \in A$ zodat

$$1 = \sum_{j=1}^{m} c_j a_1 d_j.$$

Maar I is een ideaal, dus

$$\sum_{j=1}^{m} (c_j \otimes 1) \cdot x \cdot (d_j \otimes A) \in I.$$

Na invullen van de uitdrukking voor x en door de definitie van het product gedefinieerd op het tensorproduct van twee algebra's te gebruiken, bekomen we

$$\sum_{j=1}^{m} \sum_{i=1}^{n} (c_j a_i d_j \otimes b_i) \in I.$$

Dit laatste element is gelijk aan

$$\sum_{i=1}^{n} \sum_{j=1}^{m} (c_j a_i d_j \otimes b_i) = 1 \otimes b_1 + \sum_{i=2}^{n} \sum_{j=1}^{m} (c_j a_i d_j \otimes b_i) = 1 \otimes b_1 + \sum_{i=2}^{n} \left(\sum_{j=1}^{m} c_j a_i d_j \right) \otimes b_i,$$

omdat

$$\sum_{j=1}^{m} (c_j a_1 d_j \otimes b_1) = \left(\sum_{j=1}^{m} c_j a_1 d_j \right) \otimes b_1 = 1 \otimes b_1.$$

Indien we $a_i' := \sum_{j=1}^{m} c_j a_i d_j$ voor elke $i = 2, \ldots, n$ stellen, dan is

$$y := 1 \otimes b_1 + \sum_{i=2}^{n} a_i' \otimes b_i \in I.$$

Beschouw nu voor elke $a \in A$ het element

$$(a \otimes 1) \cdot y - y \cdot (a \otimes 1) \in I.$$

Dit geldt natuurlijk omdat I een ideaal is. Men rekent eenvoudig na dat dit element gelijk is aan

$$\sum_{i=2}^{n} (aa_i' - a_i'a) \otimes b_i.$$

Wegens minimaliteit impliceert dit dat $aa_i' = a_i'a$ voor alle $i = 2, \ldots, n$. We concluderen hieruit dat voor elke a_i' geldt dat $a_i' \in Z(A) = K$. Bijgevolg is

$$x = \sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} a_i 1 \otimes b_i = \sum_{i=1}^{n} 1 \otimes a_i b_i = 1 \otimes \sum_{i=1}^{n} a_i b_i.$$

Noem $b := \sum_{i=1}^{n} a_i b_i \in B$. Omdat B simpel is en $b \neq 0$, geldt dat het ideaal voortgebracht door b gelijk is aan B; met andere woorden $BbB = B$. Daar $1 \in B$ volgt dat er $e_j, f_j \in B$ bestaan zodat

$$1 = \sum_{j=1}^{m'} e_j b f_j.$$

Men rekent eenvoudig na dat dan

$$1 = \sum_{j=1}^{m'} (1 \otimes e_j) \cdot x \cdot (1 \otimes f_j) \in I.$$

Dus $I = A \otimes_K B$, en de conclusie is dat $A \otimes_K B$ een simpele ring is.
Uit Lemma 7.20 volgt nu dat $A \otimes_K B$ een centrale simpele algebra is over zijn centrum $Z(A \otimes_K B)$. Het volstaat nu dus aan te tonen dat $Z(A \otimes_K B) \cong Z(B)$ als ringen. We tonen aan dat $Z(A \otimes_K B) = K \otimes_K Z(B)$. Hieruit volgt dan het gevraagde, daar we uit elementaire theorie van het tensorproduct weten dat $K \otimes_K Z(B) \cong Z(B)$. De inclusie $K \otimes_K Z(B) \subset Z(A \otimes_K B)$ is eenvoudig. Dus we bewijzen de inclusie $Z(A \otimes_K B) \subset K \otimes_K Z(B)$. Kies een basis $\{b_i\}_{i \in I}$ van de vectorruimte B, met I een indexverzameling. Uit een stelling over het tensorproduct, zoals bijvoorbeeld in [13], volgt dat elk element van $A \otimes_K B$ in de vorm $\sum_{i \in I} a_i \otimes b_i$ kan geschreven worden, met de $a_i \in A$ uniek. Stel nu dat $x = \sum_{i \in I} a_i \otimes b_i \in Z(A \otimes_K B)$. Dan is $(a \otimes 1) \cdot x = x \cdot (a \otimes 1)$ voor elke $a \in A$, of uitgeschreven,

$$\sum_{i \in I} a a_i \otimes b_i = \sum_{i \in I} a_i a \otimes b_i.$$

Wegens uniciteit van de schrijwijze moet $aa_i = a_i a$ voor elke $i = 1, \ldots, n$ en $a \in A$. Bijgevolg zit elke i in $Z(A) = F$, zodat

$$x = \sum_{i \in I} a_i \otimes b_i = \sum_{i \in I} a_i 1 \otimes b_i = \sum_{i \in I} 1 \otimes a_i b_i = 1 \otimes \sum_{i \in I} a_i b_i.$$

Noem $b := \sum_{i\in I} a_i b_i \in B$, zodat $x = 1 \otimes b$. Het is nu voldoende te bewijzen dat $b \in Z(B)$, want dan is $x = 1 \otimes B \in K \otimes_K Z(B)$. Kies daartoe $b' \in B$. Dan is $1 \otimes b' \in A \otimes_K B$. Dus

$$(1 \otimes b) \cdot (1 \otimes b') = x \cdot (1 \otimes b') = (1 \otimes b') \cdot x = (1 \otimes b') \cdot (1 \otimes b).$$

Of nog,

$$1 \otimes bb' = 1 \otimes b'b.$$

Dit impliceert dat $1 \otimes (bb' - b'b) = 0$. Daar $1 \neq 0$ volgt dat $bb' = b'b$, zodat inderdaad $b \in Z(B)$. Merk inderdaad op dat, in dit geval, uit $x \otimes y = 0$ volgt dat $x = 0$ of $y = 0$. Let wel, deze implicatie geldt niet altijd. Dit beëindigt het bewijs van Propositie 7.21. ■

De volgende resultaten zijn min of meer directe gevolgen van Propositie 7.21.

Propositie 7.22

> *Zij K een veld, A een centrale simpele K-algebra, en $K' \supset K$ een velduitbreiding van K. Dan is $A \otimes_K K'$ een centrale simpele K'-algebra.*

Bewijs. Dit is een onmiddellijk gevolg van Propositie 7.21: K' is een simpele K-algebra, omdat K' een veld is en dus als idealen enkel $\{0\}$ en K' heeft, en $Z(K') = K'$ omdat K', als veld zijnde, commutatief is. Dit beëindigt het bewijs van Propositie 7.22. ■

Propositie 7.23

> *Zij K een veld, A een quaternionenalgebra over K, en $K' \supset K$ een velduitbreiding van K. Dan is $A \otimes_K K'$ een quaternionenalgebra over K'.*

Bewijs. Omwille van Propositie 7.22 volstaat het aan te tonen dat de dimensie van de vectorruimte $A \otimes_K K'$ over het veld K' gelijk is aan 4. Beschouw de inclusies

$$K \subset K' \subset A \otimes_K K'.$$

Merk op dat

$$\dim_K(A \otimes_K K') = \dim_K A \cdot \dim_K K' = 4 \cdot \dim_K K'.$$

Dit geldt wegens een welgekende eigenschap van het tensorproduct van algebra's. Wegens de productformule van K-algebra's geldt dat

$$\dim_K(A \otimes_K K') = \dim_{K'}(A \otimes_K K') \cdot \dim_K K'.$$

Daarom is $\dim_{K'}(A \otimes_K K') = 4$. Dit beëindigt het bewijs van Propositie 7.23. ■

7.5 Ramificatie

We noteren met $\mathbb{P} = \{2,3,5,7,\ldots\}$ de verzameling van alle priemgetallen. Voor elk priemgetal $p \in \mathbb{P}$ is $\mathbb{Q}_p$ het veld van de p-adische getallen. Dit is de vervollediging van $\mathbb{Q}$ ten opzichte van de p-adische norm $|\cdot|_p$. Ook definiëren we, zoals gebruikelijk, $\mathbb{Q}_\infty := \mathbb{R}$; dat wil zeggen, de vervollediging van $\mathbb{Q}$ ten opzichte van de Euclidische metriek op de rationale getallen. Uiteraard is $\mathbb{Q}_p \supset \mathbb{Q}$ voor elke $p \in \mathbb{P} \cup \{\infty\}$ een velduitbreiding van $\mathbb{Q}$.

Vanaf nu spitsen we ons toe op algebra's over de rationale getallen. Zij dus A een quaternionenalgebra over $\mathbb{Q}$ en $p \in \mathbb{P} \cup \{\infty\}$. Uit Propositie 7.23 volgt dat $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ een quaternionenalgebra over $\mathbb{Q}_p$ is. Zo komen we bij volgende definitie.

Definitie 7.24

Zij A een quaternionenalgebra over $\mathbb{Q}$ en $p \in \mathbb{P} \cup \{\infty\}$. Uit Propositie 7.7 volgt dat de $\mathbb{Q}_p$-quaternionenalgebra $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ ofwel isomorf is met de $M_2(\mathbb{Q}_p)$, ofwel isomorf is met een divisiealgebra over $\mathbb{Q}_p$.

- Indien $A \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$ dan zeggen we dat *p splijt*, of *ongeramifieerd is*, in A.
- Indien $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ isomorf is met een divisiealgebra over $\mathbb{Q}_p$ dan zeggen we dat *p niet splijt*, of *geramifieerd is*, in A.

Vanaf nu schrijven we kortweg ook wel $A \otimes \mathbb{Q}_p$ in plaats van $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Indien het tensorproduct over een ander veld is, dan noteren we dat steeds expliciet.

Elke $\mathbb{Q}$-quaternionenalgebra is isomorf met een $\mathbb{Q}$-quaternionenalgebra van de vorm $H_{a,b}$, voor zekere $a,b \in \mathbb{Q}^\times$. Dit geldt wegens Propositie 7.8 en de opmerking bij Definitie 7.9; zie ook Definitie 7.10. Dus mogen we veronderstellen dat iedere $\mathbb{Q}$-quaternionenalgebra gelijk is aan zulk een $H_{a,b}$; in Definitie 7.24 mogen we $A = H_{a,b}$ veronderstellen, voor zekere $a,b \in \mathbb{Q}^\times$.

Opmerking. Indien K een veld is en $K' \supset K$ een velduitbreiding, dan bestaat er voor alle $a,b \in K^\times$ een natuurlijk K'-algebra isomorfisme

$$\left(\frac{a,b}{K}\right) \otimes_K K' \cong \left(\frac{a,b}{K'}\right).$$

In het bijzonder, voor $K = \mathbb{Q}$ en $K' = \mathbb{Q}_p$ met $p \in \mathbb{P} \cup \{\infty\}$, hebben we voor alle $a,b \in \mathbb{Q}^\times$ een $\mathbb{Q}_p$-algebra isomorfisme

$$H_{a,b} \otimes_{\mathbb{Q}} \mathbb{Q}_p = \left(\frac{a,b}{\mathbb{Q}}\right) \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \left(\frac{a,b}{\mathbb{Q}_p}\right).$$

Dit toont aan dat Definitie 7.24 consistent is met Definitie 7.17.

Definitie 7.25

We stellen

$$\Delta_{a,b} := \{p \in \mathbb{P} \cup \{\infty\} \mid p \text{ splijt niet in } H_{a,b}\}$$

voor alle $a, b \in \mathbb{Q}^\times$.

We hebben met andere woorden dat $\Delta_{a,b}$ de verzameling van alle $p \in \mathbb{P} \cup \{\infty\}$ is waarvoor p ramifieert in $H_{a,b}$, of nog, $H_{a,b} \otimes \mathbb{Q}_p \ncong M_2(\mathbb{Q}_p)$, of nog,

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) \ncong M_2(\mathbb{Q}_p).$$

En nog een equivalente karakterisatie volgt uit Propositie 7.16; de vorige uitspraken zijn equivalent met het niet-oplosbaar zijn van de vergelijking $ax^2 + by^2 = 1$ over $\mathbb{Q}_p$, hetgeen op zijn beurt, per definitie, weer equivalent is met $(a,b)_p = -1$. Dus geldt voor alle $a, b \in \mathbb{Q}^\times$ dat

$$\Delta_{a,b} = \{p \in \mathbb{P} \cup \{\infty\} \mid (a,b)_p = -1\}.$$

De kwadratische reciprociteitswet voor het Hilbertsymbool, zoals bijvoorbeeld gegeven in Stelling 7.4.1 in [7], zegt dat

$$\prod_{p \in \mathbb{P}} (a,b)_p = (a,b)_\infty,$$

waarbij alle factoren in het linkerlid gelijk zijn aan 1, op een eindig aantal factoren na. Deze formule is duidelijk equivalent met

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a,b)_p = 1.$$

Dit impliceert dat $(a,b)_p = -1$ voor een eindig en even aantal $p \in \mathbb{P} \cup \{\infty\}$. Bijgevolg is het aantal elementen in $\Delta_{a,b}$ eindig en even. Merk ook op dat $\Delta_{a,b} = \emptyset$ als en slechts als $a \in N_{\mathbb{Q}(\sqrt{b})/\mathbb{Q}}(\mathbb{Q}(\sqrt{b}))$, met $N_{\mathbb{Q}(\sqrt{b})/\mathbb{Q}} : \mathbb{Q}(\sqrt{b}) \to \mathbb{Q}$ de normafbeelding van velden. Inderdaad, $\Delta_{a,b} = \emptyset$ betekent dat voor elke $p \in \mathbb{P} \cup \{\infty\}$ geldt dat $(a,b)_p = 1$, of nog, de vergelijking $ax^2 + by^2 = 1$ is oplosbaar in elk veld $\mathbb{Q}_p$. Maar in [7], Stelling 7.3.2, is bewezen dat die veelterm aan het zogenaamde *Hasse principe* voldoet. Bijgevolg is een equivalente bewering dat $ax^2 + by^2 = 1$ een oplossing over $\mathbb{Q}$ heeft. Maar Propositie 7.16 toegepast op $K = \mathbb{Q}$ geeft ons dat dit gegeven op zijn beurt inderdaad equivalent is met $a \in N_{\mathbb{Q}(\sqrt{b})/\mathbb{Q}}(\mathbb{Q}(\sqrt{b}))$.

HASSE-MINKOWSKI PRINCIPE

In deze sectie leggen we het Hasse-Minkowski principe uit voor het veld $\mathbb{Q}$ en zijn completies $\mathbb{Q}_p$, $p \in \mathbb{P} \cup \{\infty\}$. We formuleren en bewijzen het in zijn algemeenheid; in [7] werd enkel een speciaal geval aangetoond, namelijk het geval dat de kwadratische vorm van dimensie 3 is. Het Minkowski-Hasse principe is een voorbeeld van het *lokaal-globaal principe*: we kijken naar zogenaamde lokale velden, zoals bijvoorbeeld de p-adische getallen, om informatie in te winnen over de oplosbaarheid van vergelijkingen over een globaal veld, zoals bijvoorbeeld $\mathbb{Q}$.

8.1 Inleidende voorbeelden

Ter inleiding beginnen we met dit principe te illustreren aan de hand van een aantal heel simpele voorbeelden. Beschouw de diophantische vergelijking

$$f := x^3 + 3x - 8 = 0$$

met $f \in \mathbb{Z}[x]$. Om na te gaan of $f = 0$ gehele oplossingen heeft kunnen we de vergelijking reduceren modulo een natuurlijk getal. Hier kiezen we, niet toevallig, om modulo 5 te werken. Dan zoeken we oplossingen van

$$\bar{f} := x^3 + 3x + 2 = 0$$

met $\bar{f} \in \mathbb{Z}/5\mathbb{Z}[x]$; de coëfficiënten van f worden hier dus in $\mathbb{Z}/5\mathbb{Z}$ gezien. Het is meteen duidelijk dat $\bar{f}$ geen oplossingen in $\mathbb{Z}/5\mathbb{Z}$ heeft. Omdat de projectie

$$\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} : x \mapsto x + 5\mathbb{Z}$$

een ringmorfisme is, impliceert dit trivialerwijs dat elke oplossing van f in $\mathbb{Z}$ aanleiding geeft tot een oplossing van $\bar{f}$ in $\mathbb{Z}/5\mathbb{Z}$. Bijgevolg heeft de diophantische vergelijking geen oplossingen in $\mathbb{Z}$. Ofschoon het voorbeeld triviaal is, illustreert het het lokaal-globaal principe: immers, informatie over de oplosbaarheid van de veelterm beschouwd in de "lokale" ring $\mathbb{Z}/5\mathbb{Z}$ geeft informatie over de oplosbaarheid van de veelterm in de "globale" ring $\mathbb{Z}$, namelijk, in dit geval, de onoplosbaarheid van deze laatste. Op de precieze definities van lokaal en globaal gaan we echter niet in.

Merk echter op dat het omgekeerde natuurlijk niet geldt: een gevonden oplossing in $\mathbb{Z}/5\mathbb{Z}$ geeft niet noodzakelijk aanleiding tot een oplossing in $\mathbb{Z}$. In ons particulier geval bleek modulo 5 te werken handig, maar indien $\bar{f} = 0$ wel een oplossing in $\mathbb{Z}/5\mathbb{Z}$ zou hebben dan is deze aanpak niet relevant. Ook bijvoorbeeld indien $f \in \mathbb{Q}[x]$ dan heeft bovenstaande redenering geen zin. Het is via de p-adische getallen dat we

pas echt een volwaardige lokaal-globaal correspondentie krijgen: dat is het Hasse-Minkowski principe.

We geven nog een voorbeeld van een elementaire toepassing van het lokaal-globaal principe. Beschouw de diophantische vergelijking

$$7x^4y^2 = 49 - 14x^2 + 3x^6,$$

waarvan we dit keer oplossingen $(x,y) \in \mathbb{Q}^2$ zoeken. Omdat $\mathbb{Q} \subset \mathbb{Q}_p$ ingebed is, volgt natuurlijk dat elk zo'n oplossing aanleiding geeft tot een oplossing in $\mathbb{Q}_p^2$ voor alle $p \in \mathbb{P} \cup \{\infty\}$. Verondersel nu uit het ongerijmde dat de vergelijking oplossingen in $\mathbb{Q}_p$ heeft voor elke zulke p. Zij in het bijzonder $x, y \in \mathbb{Q}_7$ oplossingen over $\mathbb{Q}_7$. Noem $a := v_7(x)$ en $b := v_7(y)$, waarbij v_7 de 7-adische valuatie is. Dan geldt dat $a, b \in \mathbb{Z}$. De 7-adische valuatie van het linkerlid is gelijk aan

$$v_7(7x^4y^2) = 1 + 4a + 2b$$

en van het rechterlid gelijk aan

$$v_7(49 - 14x^2 + 3x^6) = \min\{2, 1 + 2a, 6a\},$$

daar de valuaties van $49, -14x^2$ en $3x^6$ allen onderling verschillend zijn; zie de ongelijkheid in Eigenschap 6.3.2. van [7]. De twee termen moeten gelijk zijn. Maar $1 + 4a + 2b$ is oneven, hetgeen impliceert dat

$$\min\{2, 1 + 2a, 6a\} = 1 + 2a.$$

Dit is echter een contradictie, daar het rechterlid van deze gelijkheid steeds oneven is, en voor alle $a \in \mathbb{Z}$ geldt dat ofwel $2 \leq 1 + 2a$ ofwel $6a < 1 + 2a$; in beide gevallen is het minimum, namelijk het linkerlid, even. Dus de initiële vergelijking heeft geen oplossing over $\mathbb{Q}_p$ en bijgevolg ook niet over $\mathbb{Q}$.

8.2 Kwadratische vormen

Het principe van Hasse-Minkowski heeft te maken met kwadratische vormen. We herhalen kort dat begrip en een aantal basisresultaten daaromtrent.

Definitie 8.1

Zij K een veld en A een n-dimensionale K-vectorruimte. Een *n-dimensionale kwadratische vorm Q over K* is een afbeelding $Q : A \to K$ waarvoor de volgende twee voorwaarden gelden.

- $Q(\lambda x) = \lambda^2 Q(x)$ voor alle $\lambda \in K$ en $x \in A$.
- De afbeelding

$$B : A \times A \to K : (x,y) \mapsto \frac{1}{2}\left(Q(x+y) - Q(x) - Q(y)\right)$$

  is bilineair.

In dat geval noemen we het koppel (A, Q) een *kwadratische ruimte over K*.

We zien meteen dat de bilineaire vorm B symmetrisch is.

Merk op dat er bij elke symmetrische bilineaire vorm dus een unieke kwadratische vorm hoort, en omgekeerd geldt dat natuurlijk ook; indien B een symmetrische bilineaire vorm is, dan is $Q(x) := B(x,x)$ een kwadratische vorm, en het omgekeerde is precies de tweede voorwaarde uit Definitie 8.1. We besluiten dat er een equivalentie is tussen kwadratische vormen en symmetrische bilineaire vormen over K.

Nu volgt een korte opsomming van een aantal definities en stellingen omtrent kwadratische vormen. Zij K een veld en A een n-dimensionale vectorruimte over K.

- Een symmetrische bilineaire vorm $B : A \times A \to K$ noemen we *niet-ontaard* indien voor alle $0 \neq x \in A$ geldt dat de lineaire functionaal

  $$B_x : A \to K : y \mapsto B(x,y)$$

  niet gelijk is aan de nulafbeelding.

- Indien Q een kwadratische vorm is zodat de geassocieerde bilineaire vorm B niet-ontaard is, dan zeggen we dat Q *niet-ontaard* is.

- Stel dat de dimensie van de vectorruimte A gelijk is aan n en fixeer vanaf nu een basis $\{e_1, \ldots, e_n\}$ van A. Definieer een matrix $G \in K^{n \times n}$ door $G_{i,j} := B(e_i, e_j)$ voor alle $i, j \in \{1, 2, \ldots, n\}$. Dan noemen we de matrix G de *Gram-matrix*, of kortweg *matrix*, van de kwadratische vorm Q of van de geassocieerde bilineaire symmetrische vorm B. Het feit dat B symmetrisch is impliceert duidelijk dat de matrix G ook symmetrisch is.

- Indien $x \in K^{n \times 1}$ de coördinaatvector van een vector $a \in A$ ten opzichte van de basis $\{e_1, \ldots, e_n\}$ voorstelt, dan geldt dat

  $$Q(a) = B(a,a) = x^t \cdot G \cdot x.$$

  Zie daartoe bijvoorbeeld [28].

- Zij $\{e'_1, \ldots, e'_n\}$ een andere basis van A en G' de matrix van Q ten opzichte van die basis. Zij $P \in K^{n \times n}$ de matrix van basisverandering van $\{e_1, \ldots, e_n\}$ naar $\{e'_1, \ldots, e'_n\}$. Dan geldt dat $G' = P^t \cdot G \cdot P$.

- De *rang* van Q wordt gedefinieerd als de rang van de Gram-matrix van Q ten opzichte van een gekozen basis; het is eenvoudig aan te tonen dat dit onafhankelijk is van basiskeuze.

- Het is niet moeilijk aan te tonen dat een bilineaire vorm niet-ontaard is als en slechts als de Gram-matrix van die bilineaire vorm ten opzichte van een naar eigen keuze gekozen basis inverteerbaar is.

- De *discriminant*, of *determinant*, van Q wordt gedefinieerd als de determinant van de Gram-matrix ten opzichte van een gekozen basis; deze is goed gedefinieerd en maar uniek op vermenigvuldiging met een element van

  $$K^{\times 2} := \{k \in K^\times \mid \text{er bestaat een } k' \in K^\times \text{ zodat } k'^2 = k\}$$

na. Dit ziet men in als volgt. Stel zoals hierboven dat G de matrix van Q is ten opzichte van een eerste basis, en G' de matrix van Q ten opzichte van een tweede basis, en zij bovendien P de matrix van basisverandering van de eerste naar de tweede basis. Dan volgt uit bovenstaande dat

$$\det(G') = \det(P^t \cdot G \cdot P) = \det(P^t)\det(G)\det(P) = (\det P)^2 \det(G).$$

En $\det(P) \in K^\times$ daar P een matrix van basisverandering is. Formeel gezien is de discriminant dus een element van $K/K^{\times 2}$; we noteren $\delta(Q) \in K/K^{\times 2}$.

- Nu volgt de essentie; het resultaat wordt wel eens de *structuurstelling* of *hoofdstelling voor symmetrische bilineaire vormen* genoemd. Voor elke kwadratische vorm Q kunnen we namelijk een basis vinden zodanig dat de Gram-matrix ten opzichte van die basis een diagonaalmatrix is. Merk op dat dit resultaat wel veronderstelt dat de karakteristiek van het gebruikte veld verschillend van 2 is, maar die veronderstelling maken we inderdaad doorheen heel de thesis.

- Kies, met behulp van de structuurstelling, een basis zodanig dat de Gram-matrix van de gegeven kwadratische vorm ten opzichte van deze basis een diagonaalmatrix is. Indien $x = (x_1, \ldots, x_n) \in K^{n\times 1}$ de coördinaatvector van een vector $a \in A$ ten opzichte van die basis voorstelt, dan hebben we dus dat

$$Q(a) = g_1 x_1^2 + \ldots + g_n x_n^2,$$

waarbij $g_1, \ldots, g_n$ de respectievelijke diagonaalelementen van de diagonaalmatrix zijn. Door het isomorfisme $A \cong K^n$ als vectorruimten te gebruiken vinden we dus dat elke kwadratische vorm over K, na keuze van een geschikte basis, dat wil zeggen een lineaire coördinatentransformatie, gelijk is aan een afbeelding

$$Q : K^n \to K : (x_1, \ldots, x_n) \mapsto g_1 x_1^2 + \ldots + g_n x_n^2,$$

met $g_1, \ldots, g_n \in K$.

- Merk op dat de discriminant met behulp van de diagonale Gram-matrix hierboven heel makkelijk te berekenen wordt; deze is gelijk aan $g_1 g_2 \cdots g_n$ op vermenigvuldiging met een kwadraat in $K^\times$ na.

- We zeggen dat een kwadratische vorm Q een element $x \in K$ *representeert* indien er een $a \in A$ bestaat zodat $Q(a) = x$. Bovendien zeggen we dat Q het getal 0 *niet-triviaal representeert* indien er een $0 \neq a \in A$ bestaat zodat $Q(a) = 0$.

- Merk op dat indien een velduitbreiding $K' \supset K$ gegeven is, een kwadratische vorm over K dan op natuurlijke wijze ook een kwadratische vorm over K' is. Bijvoorbeeld, de $\mathbb{Q}$-kwadratische vorm

$$Q : \mathbb{Q}^3 \to \mathbb{Q} : (x_1, x_2, x_3) \mapsto 3x_1^2 - 7x_2^2 + x_3^2$$

induceert vanwege de natuurlijke inbedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ met $p \in \mathbb{P} \cup \{\infty\}$ de $\mathbb{Q}_p$-kwadratische vorm

$$Q : \mathbb{Q}_p^3 \to \mathbb{Q}_p : (x_1, x_2, x_3) \mapsto 3x_1^2 - 7x_2^2 + x_3^2.$$

8.3 Bewijs van het Hasse-Minkowski principe

In deze sectie bewijzen we het principe waar heel dit hoofdstuk over gaat. Maar eerst formuleren we het resultaat in zijn algemeenheid, en dat gaat als volgt.

Propositie 8.2

> *Zij een n-dimensionale kwadratische vorm Q over $\mathbb{Q}$ gegeven, met $n \geq 1$.*
>
> 1. *Zij $r \in \mathbb{Q}^\times$. Dan representeert Q het getal r als en slechts voor elke $p \in \mathbb{P} \cup \{\infty\}$ geldt dat de geïnduceerde $\mathbb{Q}_p$-kwadratische vorm Q het getal r representeert.*
> 2. *De kwadratische vorm Q representeert het getal 0 op niet-triviale wijze als en slechts voor elke $p \in \mathbb{P} \cup \{\infty\}$ geldt dat de geïnduceerde $\mathbb{Q}_p$-kwadratische vorm Q het getal 0 op niet-triviale wijze representeert.*

We bewijzen dit resultaat in stukken. Essentieel werken we per inductie op de dimensie n. Bovendien veronderstellen we steeds dat we te maken hebben met een gediagonaliseerde kwadratische vorm; dit mag bij gratie van de structuurstelling. We kunnen informeel dus spreken van "een kwadratische vorm $Q(x_1,x_2,x_3)$ van de vorm $ax_1^2+bx_2^2+cx_3^2$" van, in dit geval, dimensie 3, met $a,b,c \in \mathbb{Q}$.

Maar we formuleren eerst een op het eerste zicht minder sterk resultaat, waaraan we later steeds zullen refereren als *de reductie van Hasse-Minkowski*.

Propositie 8.3

> *Zij een niet-ontaarde n-dimensionale kwadratische vorm Q op $\mathbb{Q}$ gegeven, $n \geq 1$. De kwadratische vorm Q representeert het getal 0 op niet-triviale wijze als en slechts als voor elke $p \in \mathbb{P} \cup \{\infty\}$ geldt dat de geïnduceerde $\mathbb{Q}_p$-kwadratische vorm Q het getal 0 op niet-triviale wijze representeert.*

Toch blijkt Propositie 8.3 sterk genoeg te zijn om Propositie 8.2 te impliceren; we hebben immers het volgende.

Propositie 8.4

> *Propositie 8.2 en Propositie 8.3 zijn equivalent.*

Bewijs. Het is duidelijk dat Propositie 8.2 impliceert dat Propositie 8.3 waar is, dus laten we nu het omgekeerde bewijzen. Zij Q zulk een kwadratische vorm over $\mathbb{Q}$. Veronderstel ten eerste dat Q niet-ontaard is. Dan is het tweede deel van Propositie 8.2 waar per hypothese. Nu tonen we het eerste deel van Propositie 8.2 aan. Neem dus een $r \in \mathbb{Q}^\times$. Veronderstel dat $Q(x_1,\ldots,x_n) = r$ oplosbaar is over elke $\mathbb{Q}_p$ met $p \in \mathbb{P} \cup \{\infty\}$, zeg $Q(a_{1,p},\ldots,a_{n,p}) = r$, dan bewijzen we dat de vergelijking oplosbaar is over $\mathbb{Q}$; de omgekeerde bewering is triviaal. Beschouw dan de kwadratische vorm

Q' op $\mathbb{Q}^{n+1}$, verwant aan Q; namelijk deze gedefinieerd door

$$Q'(x_1,\ldots,x_n,x_{n+1}) := Q(x_1,\ldots,x_n) - rx_{n+1}^2.$$

Merk op dat Q' niet-ontaard is daar Q dit is en $r \neq 0$. De niet-ontaarde kwadratische vorm Q' representeert bovendien het getal 0 op niet-triviale wijze; inderdaad,

$$Q'(a_{1,p},\ldots,a_{n,p},1) = Q(a_{1,p},\ldots,a_{n,p}) - r = 0,$$

voor alle $p \in \mathbb{P} \cup \{\infty\}$. Propositie 8.3 geeft ons dan dat de kwadratische vorm Q' het getal 0 op niet-triviale wijze representeert, over $\mathbb{Q}$. Lemma 8.6 verderop impliceert nu dat Q het getal r representeert, over $\mathbb{Q}$. Dus Q representeert het getal r.
Veronderstel nu dat Q ontaard is. Het tweede deel van Propositie 8.2 is trivialerwijs waar: voor elke ontaarde kwadratische vorm over een veld bestaat er een $\vec{a} \neq 0$ zodat $Q(\vec{a}) = 0$. Dit ziet men in als volgt, bijvoorbeeld voor de velden $\mathbb{Q}$ en $\mathbb{Q}_p$, waar wij steeds mee te doen hebben. De aan Q geassocieerde bilineaire vorm B is ontaard, id est er bestaat een $0 \neq \vec{a} \in \mathbb{Q}$ (of $\mathbb{Q}_p$) zodat $B(\vec{a},\vec{x}) = 0$ voor alle $\vec{x} \in \mathbb{Q}$ (of $\mathbb{Q}_p$). Dus in het bijzonder is $Q(\vec{a}) = B(\vec{a},\vec{a}) = 0$. Laten we nu het eerste deel van Propositie 8.2 bewijzen. Neem dus een $r \in \mathbb{Q}^\times$. Veronderstel dat $Q(x_1,\ldots,x_n) = r$ oplosbaar is over alle $\mathbb{Q}_p$ met $p \in \mathbb{P} \cup \{\infty\}$, zeg $Q(a_{1,p},\ldots,a_{n,p}) = r$, dan bewijzen we dat de vergelijking oplosbaar is over $\mathbb{Q}$; de omgekeerde bewering is triviaal. Noem A de vectorruimte waarop Q initieel gedefinieerd is. Omdat Q ontaard is, hebben we dat het *radicaal* van A, namelijk de deelruimte

$$A^\perp := \{a \in A \,|\, Q(x,a) = 0 \text{ voor alle } x \in A\}$$

van A, niet-leeg is. We weten ook dat we A dan kunnen schrijven als $A = B \perp A^\perp$, met B een deelruimte van A, zeg van dimensie $k < n$. Voor een bewijs van dit resultaat en de gebruikte begrippen verwijzen we naar [28]. In feite komt het er op neer dat $A^\perp$ het deel van A voorstelt dat voor de ontaarding zorgt; op B is Q niet-ontaard. Definieer dan een nieuwe, niet-ontaarde, kwadratische vorm Q' door $Q' := Q|_B$. Dus hebben we voor alle $x \in B$ en $y \in A^\perp$ dat $Q'(x) = Q(x,y)$. We kunnen Q' diagonaliseren. Beschouw dan de kwadratische vorm Q'' op $\mathbb{Q}^{k+1}$, verwant aan Q'; namelijk deze gedefinieerd door

$$Q''(x_1,\ldots,x_k,x_{k+1}) := Q'(x_1,\ldots,x_k) - rx_{k+1}^2.$$

Ook Q'' is niet-ontaard daar Q' dit is en $r \neq 0$. Merk op dat

$$Q'(a_{1,p},\ldots,a_{k,p}) = Q(a_{1,p},\ldots,a_{k,p},a_{k+1,p},\ldots,a_{n,p}) = Q(a_{1,p},\ldots,a_{n,p}) = r.$$

Dus Q' representeert r, voor elke $p \in \mathbb{P} \cup \{\infty\}$. Uit Lemma 8.6 volgt dat $Q'' = 0$ een niet-triviale oplossing over elke $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$, heeft. Maar uit onze hypothese volgt dan dat $Q'' = 0$ een niet triviale oplossing over $\mathbb{Q}$ heeft. Dus, door opnieuw Lemma 8.6 te gebruiken, hebben we dat er een oplossing over $\mathbb{Q}$ van $Q' = r$ bestaat, dat wil zeggen $Q'(x_1,\ldots,x_n) = r$ oplosbaar is over $\mathbb{Q}$; zeg $Q(a_1,\ldots,a_n) = r$ met $a_1,\ldots,a_n \in \mathbb{Q}$. Maar dan is

$$Q(a_1,\ldots,a_k,0,\ldots,0) = Q'(a_1,\ldots,a_k) = r,$$

zodat $Q(x_1,\ldots,x_n) = r$ inderdaad oplosbaar is over $\mathbb{Q}$. Dit beëindigt het bewijs van Propositie 8.4. ■

Lemma 8.5

Zij een vectorruimte A over een veld K en $Q : A \to K$ een niet-ontaarde kwadratische vorm gegeven. Indien er een $0 \neq x \in A$ bestaat zodat $Q(x) = 0$, dan geldt dat $Q(A) = K$.

Bewijs. Veronderstel dat $0 \neq x \in A$ zodanig is dat $Q(x) = 0$. Zij $B : A \times A \to K$ de bilineaire vorm geassocieerd aan de K-kwadratische vorm Q. Omdat Q niet-ontaard is hebben we per definitie dat B niet-ontaard is. Dit impliceert dat er een $y \in A$ bestaat zodat $B(x,y) \neq 0$. Laat $c \in K$ en beschouw

$$\begin{aligned} Q(cx+y) &= Q(cx)+Q(y)+2B(cx,y) \\ &= c^2Q(x)+Q(y)+2cB(x,y) \\ &= Q(y)+2cB(x,y). \end{aligned}$$

We hebben dat $2B(x,y) \neq 0$ daar we in karakteristiek verschillend van 2 werken en $B(x,y) \neq 0$. Dus kunnen we, door c te variëren, elk getal in K bereiken. Dit beëindigt het bewijs van Lemma 8.5. ■

Lemma 8.6

Zij K een veld en $Q : K^n \to K$ een n-dimensionale niet-ontaarde kwadratische vorm over K. Zij $r \in K$. Definieer een $(n+1)$-dimensionale kwadratische vorm

$$Q' : K^{n+1} \to K : (x_1,\ldots,x_n,x_{n+1}) \mapsto Q(x_1,\ldots,x_n) - rx_{n+1}^2.$$

Dan bestaat er een $(x_1,\ldots,x_n) \in K^n$ zodat $Q(x_1,\ldots,x_n) = r$ als en slechts als er een $0 \neq (x_1,\ldots,x_n,x_{n+1}) \in K^{n+1}$ bestaat zodat $Q'(x_1,\ldots,x_n,x_{n+1}) = 0$.

Bewijs. De implicatie van links naar rechts is triviaal. Het volstaat dus om de implicatie van rechts naar links aan te tonen. Gegeven is een $0 \neq (x_1,\ldots,x_n,x_{n+1}) \in K^{n+1}$ zodat

$$Q(x_1,\ldots,x_n) - rx_{n+1}^2 = Q'(x_1,\ldots,x_n,x_{n+1}) = 0.$$

Indien $x_{n+1} \neq 0$ dan zijn we klaar, want dan is

$$Q\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_n}{x_{n+1}}\right) = \frac{1}{x_{n+1}^2}Q(x_1,\ldots,x_n) = r.$$

Indien $x_{n+1} = 0$ dan is $Q(x_1,\ldots,x_n) = 0$, met bovendien $(x_1,\ldots,x_n) \neq 0$. Omdat Q niet-ontaard is, volgt het gevraagde dan a fortiori uit Lemma 8.5. Dit beëindigt het bewijs van Lemma 8.6. ■

We concluderen dus dat het voldoende is Propositie 8.3 te bewijzen. In concreto betekent dit voor ons dat we voor de coëfficiënten van een gegeven kwadratische vorm, bijvoorbeeld

$$Q(x_1,x_2,x_3) = ax_1^2 + bx_2^2 + cx_3^2$$

in dimensie 3, steeds mogen veronderstellen dat a,b en c allemaal verschillend van 0 zijn, dat wil zeggen $a,b,c \in \mathbb{Q}^\times$; bovendien mogen we ons beperken tot het zoeken van een niet-triviale oplossing in het geval $r = 0$.

8.3.1 Het geval $n = 1$

De reductie van Hasse-Minkowski in dimensie 1 zegt: voor $a \in \mathbb{Q}^\times$ geldt dat de vergelijking $ax^2 = 0$ niet-triviaal oplosbaar is over $\mathbb{Q}$ als en slechts als die vergelijking niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$.

Bewijs. Dit is triviaal aangezien de vergelijking $ax^2 = 0$ zowel over $\mathbb{Q}$ als over elke $\mathbb{Q}_p$ enkel de triviale oplossing $x = 0$ heeft, daar $a \neq 0$. Dit beëindigt het bewijs van het geval $n = 1$. ■

8.3.2 Het geval $n = 2$

De reductie van Hasse-Minkowski in dimensie 2 zegt: voor $a,b \in \mathbb{Q}^\times$ geldt dat de vergelijking $ax^2 + by^2 = 0$ niet-triviaal oplosbaar is over $\mathbb{Q}$ als en slechts als die vergelijking niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$.

Voor het bewijs gebruiken we volgend lemma.

Lemma 8.7

> *Zij K een veld met karakteristiek verschillend van 2 en $a,b \in K^\times$. Dan bestaat er een $0 \neq (x,y) \in K^2$ zodat $ax^2 + by^2 = 0$ als en slechts als $-b/a \in K^{\times 2}$.*

Bewijs. Stel eerst dat er een $0 \neq (x,y) \in K^2$ bestaat zodat $ax^2 + by^2 = 0$. Indien $x = 0$ dan is $y = 0$, daar $b \neq 0$, en indien $y = 0$ dan is $x = 0$, daar $a \neq 0$. Bijgevolg zijn zowel x als y verschillend van nul, omdat $(x,y) \neq 0$. Dan hebben we dat

$$-\frac{b}{a} = \frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2 \in K^{\times 2}.$$

Omgekeerd, indien $-b/a \in K^{\times 2}$, dan bestaat er per definitie een $x \in K^\times$ zodat $-b/a = x^2$. Bijgevolg hebben we dat $ax^2 + b1^2 = ax^2 + b = 0$. Dit beëindigt het bewijs van Lemma 8.7. ■

Bewijs. Omwille van Lemma 8.7 is het voldoende aan te tonen dat voor elke $q \in \mathbb{Q}^\times$ geldt dat q een kwadraat is in $\mathbb{Q}$ als en slechts als q een kwadraat is in alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$. Veronderstel eerst dat $q \in \mathbb{Q}^\times$ en q een kwadraat in alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$, is. Schrijf $q = \pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ met p_i een priemgetal en $e_i \in \mathbb{Z}$ voor elke $i \in \{1,\ldots,n\}$, met bovendien de voorwaarde $p_i \neq p_j$ als $i \neq j$. Daar kwadraten in $\mathbb{Q}_\infty = \mathbb{R}$ positief zijn, moet al zeker $q > 0$ zodat $q = p_1^{e_1} \cdots p_n^{e_n}$. Merk op dat voor eender welk priemgetal p en $x \in \mathbb{Q}_p$ geldt dat p-orde van x even is als en slechts als

x een kwadraat in $\mathbb{Q}_p$ is, op vermenigvuldiging met een eenheid van $\mathbb{Z}_p$ na. Kies $i \in \{1,\ldots,n\}$. Dan is

$$\nu_{p_i}(q) = \nu_{p_i}(p_1^{e_1} \cdots p_n^{e_n}) = e_i$$

even omwille van bovenstaande; schrijf $e_i = 2t_i$ met $t_i \in \mathbb{Z}$. Dan is

$$q = p_1^{e_1} \cdots p_n^{e_n} = p_1^{2t_1} \cdots p_n^{2t_n} = (p_1^{t_1} \cdots p_n^{t_n})^2$$

een kwadraat in $\mathbb{Q}$. De omgekeerde implicatie is triviaal. Dit beëindigt het bewijs van het geval $n = 2$. ■

8.3.3 Het geval $n = 3$

De reductie van Hasse-Minkowski in dimensie 3 zegt: voor $a,b,c \in \mathbb{Q}^\times$ geldt dat de vergelijking $ax^2 + by^2 + cz^2 = 0$ niet-triviaal oplosbaar is over $\mathbb{Q}$ als en slechts als die vergelijking niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$.

Bewijs. Merk op dat we, door vermenigvuldiging met geschikte gehele getallen, mogen veronderstellen dat $a,b,c \in \mathbb{Z}$ en allemaal verschillend van nul zijn. Ook mogen a,b en c verondersteld worden kwadraatvrij te zijn; bijvoorbeeld, door de lineaire coördinatentransformatie $u = 3x$ kan $18x^2$ bijvoorbeeld als $2u^2$ geschreven worden. De eventuele kwadraten in a,b en c kunnen dus allemaal opgeslorpt worden in de kwadraten van de kwadratische vorm. We nemen aan dat $ax^2 + by^2 + cz^2 = 0$ een niet triviale oplossing in elke $\mathbb{Q}_p$ heeft, en bewijzen dan dat er een niet-triviale oplossing in $\mathbb{Q}$ is; de omgekeerde implicatie is triviaal. Daar de vergelijking een oplossing heeft in $\mathbb{Q}_\infty = \mathbb{R}$, volgt dat niet alle getallen a,b,c groter aan nul kunnen zijn want dan is er geen niet-triviale oplossing; stel dus zonder verlies van algemeenheid dat $c < 0$. We schrijven dit liever als $-c$ met dan $c > 0$. Dus $ax^2 + by^2 = cz^2$ is onze vergelijking, met $c > 0$. Door tenslotte door $c \neq 0$ te delen vinden we dat we mogen veronderstellen dat we de vergelijking $ax^2 + by^2 = z^2$ gegeven hebben, met $a,b \in \mathbb{Z}$ kwadraatvrij; we tonen dan aan dat, indien deze vergelijking over elke $\mathbb{Q}_p$ een niet-triviale oplossing heeft, er dan ook een niet-triviale oplossing over $\mathbb{Q}$ is. We doen dit per inductie op $n := |a| + |b| \geq 2$. Eerst bewijzen we het geval $n = 2$. Dan is $|a| = |b| = 1$. Er zijn dan maar vier mogelijkheden voor (a,b), namelijk $(a,b) \in \{(-1,-1),(-1,1),(1,-1),(1,1)\}$. De laatste drie vergelijkingen die hiermee corresponderen, namelijk

$$\begin{aligned} -x^2 + y^2 &= z^2 \\ x^2 - y^2 &= z^2 \\ x^2 + y^2 &= z^2, \end{aligned}$$

hebben de respectievelijke oplossingen $(1,1,0),(1,1,0)$ en $(1,0,1)$ over $\mathbb{Q}$, daarmee zijn we klaar; rest ons dus nog het geval dat correspondeert met $(a,b) = (-1,-1)$, namelijk de vergelijking $x^2 + y^2 = -z^2$. Merk echter op dat deze vergelijking in $\mathbb{Q}_p = \mathbb{R}$ enkel de triviale oplossing heeft, dus is er niets te bewijzen in dit geval. Hiermee is het geval $n = 2$ aangetoond. Veronderstel nu dat $n > 2$ en neem aan dat de stelling reeds bewezen is voor alle kleinere waardes. Wegens symmetrie mogen

we zonder verlies van algemeenheid stellen dat $|a| \leq |b|$. Dan is $2|b| \geq |a| + |b| > 2$, of nog, $|b| \geq 2$. We hebben dan volgend lemma.

Lemma 8.8

Er geldt dat a een kwadraat is modulo b.

Bewijs. Daar b kwadraatvrij is hebben we dat $b = p_1 \cdots p_k$ met alle p_i onderling verschillende priemgetallen. Dan is het voldoende aan te tonen dat a een kwadraat is modulo alle priemdelers van b, id est alle p_i met $i \in \{1,2,\ldots,k\}$; inderdaad, dit volgt uit een directe toepassing van de Chinese reststelling. Kies nu zulk een $i \in \{1,2,\ldots,k\}$ en noem $p := p_i$. Per hypothese bestaat er een niet-triviale oplossing $(x_p, y_p, z_p) \in \mathbb{Q}_p$ van de vergelijking, dat wil zeggen $ax_p^2 + by_p^2 = z_p^2$. Door deze vergelijking met gepaste positieve even machten van p te vermenigvuldigen mogen we ervan uitgaan dat $(x_p, y_p, z_p) \in \mathbb{Z}_p$; bovendien kunnen we er op deze manier ook voor zorgen dat in minstens één van de drie p-adische gehelen er geen macht van p meer staat, en dus zelfs in $\mathbb{Z}_p^\times$ zit. We bewijzen nu dat $x_p \in \mathbb{Z}_p^\times$. Stel daartoe uit het ongerijmde dat $p \,|\, x_p$. Omdat $p \,|\, b$ is $0 \equiv ax_p^2 + by_p^2 = z_p^2 \mod p$, zodat $p \,|\, z_p$. Dan is

$$by_p^2 = z_p^2 - ax - p^2 \equiv 0 \mod p^2,$$

hetgeen betekent dat $p \,|\, y_p$, daar $p \,|\, b$. Maar dit geeft een contradictie met het feit dat tenminste één van de p-adische gehelen x_p, y_p, z_p een eenheid in $\mathbb{Z}_p$ was. Bijgevolg is inderdaad $x_p \in \mathbb{Z}_p^\times$. De vergelijking $ax_p^2 \equiv z_p^2 \mod p$ samen met $x_p \in \mathbb{Z}_p^\times$ geeft dan dat $p \,|\, (ax_p^2 - z_p^2)/x_p^2 = a - (z_p/x_p)^2$, of nog, $a \equiv (z_p/x_p)^2 \mod p$, dat wil zeggen a is een kwadraat modulo p. Dit beëindigt het bewijs van Lemma 8.8. ■

Omwille van Lemma 8.8 bestaat er een $m \in \mathbb{Z}$ zodat $a \equiv m^2 \mod b$. Natuurlijk kan dat op zulk een manier dat $|m| \leq \frac{1}{2}|b|$. Dan is $a + bt = m^2$ voor een zekere $t \in \mathbb{Z}$. Als $t = 0$ dan moet $a = 1$ omdat we a kwadraatvrij verondersteld hadden. Maar dat geval is evident want de vergelijking $x^2 + by^2 = z^2$ heeft de niet-triviale oplossing $(1,0,1)$ over $\mathbb{Q}$ en al zijn completies $\mathbb{Q}_p$. Veronderstel nu dat $t \neq 0$. Schrijf $t = cd^2$ met $c \in \mathbb{Z}$ kwadraatvrij en $d \in \mathbb{Z}$, en $c, d \neq 0$. Dan hebben we dat

$$\frac{b}{c} = \frac{m^2 - a}{(cd)^2} = \left(\frac{m}{cd}\right)^2 - \frac{a}{(cd)^2} \in \{x^2 - ay^2 \neq 0 \,|\, x, y \in \mathbb{Q}\}.$$

Lemma 8.9 hieronder toegepast op de hypotheses van de stelling geeft dat er voor elke $p \in \mathbb{P} \cup \{\infty\}$ getallen $x_p, y_p \in \mathbb{Q}_p$ bestaan zodat $b = x_p^2 - ay_p^2$. Kies een p vast. Beschouw dan de inclusies

$$\{x^2 - ay^2 \neq 0 \,|\, x, y \in \mathbb{Q}\} \subset \{x^2 - ay^2 \neq 0 \,|\, x, y \in \mathbb{Q}_p\} \subset \mathbb{Q}_p^\times.$$

Dit zijn in feite zelfs deelgroepen van $\mathbb{Q}_p^\times$. Dit ziet men in als volgt; het product van twee elementen $x^2 - ay^2$ en $x'^2 - ay'^2$ is gelijk aan

$$(x^2 - ay^2)(x'^2 - ay'^2) = (xx' + ayy')^2 - a(xy' + x'y)^2,$$

duidelijk zit $1 = 1^2 - a\,0^2$ er in, en tenslotte heeft ieder element $x^2 - ay^2$ een inverse daar

$$(x^2 - ay^2)\left(\left(\frac{x}{x^2-ay^2}\right)^2 - a\left(\frac{y}{x^2-ay^2}\right)^2\right)^2 = 1.$$

Aangezien $b \in \{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}_p\}$ en

$$\frac{b}{c} \in \{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}\} \subset \{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}_p\}$$

geldt dat $c = (b/c)^{-1}b \in \{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}_p\}$. Bijgevolg kan c geschreven worden als $c = x_p^2 - ay_p^2$ voor zekere $x_p, y_p \in \mathbb{Q}_p$. Door opnieuw Lemma 8.9 te gebruiken vinden we dat de vergelijking $ax^2 + cy^2 = z^2$ voor alle $p \in \mathbb{P} \cup \{\infty\}$ niet-triviale oplossingen over $\mathbb{Q}_p$ heeft. Ten einde de inductiehypothese eindelijk toe te kunnen passen, tonen we nu aan dat $|a| + |c| < |a| + |b| = n$, of nog, $|c| < |b|$. Omdat $|a| \leq |b|$ hebben we dat

$$|bcd^2| = |m^2 - a| \leq |m|^2 + |a| \leq \frac{1}{4}|b|^2 + |b|.$$

Bijgevolg is $|c| \leq |cd^2| \leq \frac{1}{4}|b| + 1 < |b|$. De laatste ongelijkheid volgt omdat $|b| \geq 2$. We passen nu de inductiehypothese toe op de vergelijking $ax^2 + cy^2 = z^2$; dan bestaat er een niet-triviale oplossing over $\mathbb{Q}$ van deze vergelijking. Opnieuw wegens Lemma 8.9 hebben we dat er $r,s \in \mathbb{Q}$ bestaan zodat $c = r^2 - as^2$. Daar b/c en c beiden in de verzameling $\{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}\}$ zitten en dit een groep vormt, volgt dus dat ook

$$b = \frac{b}{c}c \in \{x^2 - ay^2 \neq 0 \,|\, x,y \in \mathbb{Q}\}.$$

Dus er bestaan $x,y \in \mathbb{Q}$ zodat $b = x^2 - ay^2$. Het gevraagde volgt dan uit Lemma 8.9. Dit beëindigt het bewijs van het geval $n = 3$. ■

Lemma 8.9

> *Zij K een veld van karakteristiek verschillend van 2 en $a,b \in K^\times$. Dan bestaat er een $0 \neq (x,y,z) \in K^3$ zodat $ax^2 + by^2 = z^2$ als en slechts als er $x,y \in K$ bestaan zodat $b = x^2 - ay^2$.*

Bewijs. Veronderstel eerst dat er een $0 \neq (x,y,z) \in K^3$ bestaat zodat $ax^2 + by^2 = z^2$. Indien $y \neq 0$ dan kunnen we door y delen en bekomen zo

$$a\left(\frac{x}{y}\right)^2 + b = \left(\frac{z}{y}\right)^2,$$

of nog,

$$b = \left(\frac{z}{y}\right)^2 - a\left(\frac{x}{y}\right)^2.$$

Indien $y = 0$ dan hebben we $ax^2 = z^2$. Dan moet $x \neq 0$ want anders zou $(x,y,z) = 0$; analoog is $z \neq 0$. Bijgevolg is $a = (z/x)^2$ een kwadraat in $K^\times$. Dan is

$$b = \left(\frac{b+1}{2}\right)^2 - \left(\frac{b-1}{2}\right)^2 = \left(\frac{b+1}{2}\right)^2 - a\left(\frac{(b-1)x}{2z}\right)^2.$$

Omgekeerd, stel dat er $x, y \in K$ bestaan zodat $b = x^2 - ay^2$. Dan is

$$ay^2 + b\,1^2 = ay^2 + b = x^2$$

een niet-triviale oplossing van de vergelijking. Dit beëindigt het bewijs van Lemma 8.9. ■

8.3.4 Het geval $n = 4$

De reductie van Hasse-Minkowski in dimensie 4 zegt: voor $a, b, c, d \in \mathbb{Q}^\times$ geldt dat de vergelijking $ax^2 + by^2 + cz^2 + dt^2 = 0$ niet-triviaal oplosbaar is over $\mathbb{Q}$ als en slechts als die vergelijking niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$.

Bewijs. Merk op dat we, analoog als in het geval $n = 3$, door vermenigvuldiging met geschikte gehele getallen mogen veronderstellen dat $a, b, c, d \in \mathbb{Z}$ en allemaal verschillend van nul. We nemen aan dat $ax^2 + by^2 + cz^2 + dt^2 = 0$ een niet triviale oplossing over elke $\mathbb{Q}_p$ heeft, en bewijzen dan dat er een niet-triviale oplossing in $\mathbb{Q}$ is; de omgekeerde implicatie is triviaal. Daar de vergelijking een oplossing in $\mathbb{Q}_\infty = \mathbb{R}$ heeft, volgt dat er van deze getallen minstens één strikt positief en minstens één strikt negatief is; we mogen dus, omwille van symmetrie, zonder verlies van algemeenheid $a > 0$ en $d < 0$ veronderstellen. Indien we

$$Q_1(x,y) := ax^2 + by^2, \quad Q_2(z,t) := -cz^2 - dt^2$$

definiëren dan geeft dit

$$ax^2 + by^2 + cz^2 + dt^2 = Q_1(x,y) - Q_2(z,t).$$

Uit Lemma 8.14 en de veronderstelling dat voor elke $p \in \mathbb{P}$ er een oplossing van de initiële vergelijking is, volgt dat voor iedere zulke p een $\alpha_p \in \mathbb{Q}_p^\times$ bestaat die door zowel Q_1 als Q_2 wordt bereikt. Door even machten van p die deel uitmaken van α_p in de kwadraten van de kwadratische vormen te schuiven, id est een lineaire coördinatentransformatie van de kwadratische vorm, mogen we zonder verlies van algemeenheid veronderstellen dat ofwel $\alpha_p \in \mathbb{Z}_p^\times$ (in het geval dat de p-orde van α_p even is) ofwel $\alpha_p \in p\mathbb{Z}_p^\times$ (in het geval dat de p-orde van α_p oneven is). Kies een $r \in \mathbb{N}$ zodat voor iedere oneven priemdeler p van $abcd$ geldt dat $r \equiv \alpha_p \mod p^2$ in $\mathbb{Z}_p$ en bovendien $r \equiv \alpha_2 \mod 16$ in $\mathbb{Z}_2$; dit kan steeds, als volgt. Noem de verschillende oneven priemfactoren van $abcd$ respectievelijk $p_1, p_2, \ldots, p_k$. Beschouw dan het stelsel

$$\begin{cases} x \equiv \pi_2(\alpha_{p_1}) & \mod p_1^2 \\ \quad \vdots & \\ x \equiv \pi_2(\alpha_{p_k}) & \mod p_k^2 \\ x \equiv \pi_2(\alpha_2) & \mod 2^4 \end{cases}.$$

Hierbij bedoelen we met π_2 de natuurlijke afbeelding $\pi_2 : \mathbb{Z}_p \to \mathbb{Z}/p^2\mathbb{Z}$ zoals bijvoorbeeld in [7]. Uit de Chinese reststelling volgt onmiddellijk dat dit stelsel een oplossing heeft. Deze kan uiteraard in de natuurlijke getallen gekozen worden; zij

$r \in \mathbb{N}$ zulk een oplossing. Neem nu een $i \in \{1,\ldots,k\}$ en beschouw het priemgetal p_i. Dan is

$$\pi_2(r-\alpha_{p_i}) = \pi_2(r) - \pi_2(\alpha_{p_i}) = r - \pi_2(\alpha_{p_i}) = 0.$$

Uit Stelling 6.2.2 uit [7] volgt dan dat $r-\alpha_{p_i}$ deelbaar is door ${p_i}^2$ in $\mathbb{Z}_{p_i}$, of nog, $r \equiv \alpha_{p_i} \mod p_i^2$ in $\mathbb{Z}_{p_i}$. Uiteraard blijft hetzelfde gelden voor het priemgetal 2. Dan hebben we inderdaad een $r \in \mathbb{N}$ gevonden die aan het gevraagde voldoet.
We beweren dat $v_p(r) = v_p(\alpha_p)$ voor elk priemgetal $p \,|\, 2abcd$. Neem zulk een p. Schrijf $r-\alpha_p = p^2 t$ voor een $t \in \mathbb{Z}_p$. Indien $\alpha_p \in \mathbb{Z}_p^\times$ dan moet ook $r \in \mathbb{Z}_p^\times$; indien niet dan geldt $p \,|\, r$ en bijgevolg de contradictie $p \,|\, r - p^2 t = \alpha_p$. Indien $\alpha_p \in p\mathbb{Z}^\times$ dan moet ook $r \in p\mathbb{Z}_p$; indien niet dan is ofwel r niet deelbaar door p, hetgeen in contradictie met $r = p^2 t + \alpha_p$ is, ofwel $p^2 \,|\, r$ en dan volgt de contradictie $p^2 \,|\, r - p^2 t = \alpha_p$. Hieruit volgt dat de ordes van beide getallen inderdaad gelijk zijn. Bijgevolg is $r/\alpha_p \in \mathbb{Z}_p^\times$. Dan is

$$\frac{r}{\alpha_p} - 1 = \frac{r-\alpha_p}{\alpha_p} = \frac{p^2 t}{\alpha_p} = p\left(\frac{pt}{\alpha_p}\right).$$

Omdat steeds $\alpha_p \in \mathbb{Z}_p^\times$ of $\alpha_p \in p\mathbb{Z}_p^\times$ geldt dat $\alpha_p \,|\, p$ in $\mathbb{Z}_p$. Bijgevolg geldt voor alle priemgetallen p waarvoor $p \,|\, abcd$ in $\mathbb{Z}_p$ de congruentie

$$\frac{r}{\alpha_p} \equiv 1 \mod p.$$

Omwille van dezelfde reden hebben we in $\mathbb{Z}_2$ de congruentie

$$\frac{r}{\alpha_2} \equiv 1 \mod 8.$$

Uit Lemma 8.15 volgt dat $r/\alpha_p \in \mathbb{Q}_p^{\times 2}$ voor alle priemgetallen p waarvoor $p \,|\, 2abcd$. Neem zulk een p. Dan bestaat er dus een $q \in \mathbb{Q}_p^\times$ zodat $r/\alpha_p = q^2$. Omdat α_p gekozen was als een waarde die door zowel Q_1 als Q_2 bereikt wordt, hebben we $(x_1,y_1),(x_2,y_2) \in \mathbb{Q}_p^2$ zodat

$$ax_1^2 + by_1^2 = Q_1(x_1,y_1) = \alpha_p = Q_2(x_2,y_2) = -cx_2^2 - dy_2^2.$$

Door deze vergelijking met q^2 te vermenigvuldigen bekomen we dat

$$r = q^2\alpha_p = q^2(ax_1^2 + by_1^2) = a(qx_1)^2 + b(qy_1)^2 = -c(qx_2)^2 - d(qy_2)^2,$$

of nog,

$$r = q^2\alpha_p = Q_1(qx_1,qy_1) = Q_2(qx_2,qy_2).$$

Dat wil zeggen dat Q_1 en Q_2 ook de waarde r aannemen over $\mathbb{Q}_p$. Dit kan men, met behulp van Lemma 8.6, ook formuleren als volgt: de twee driedimensionale kwadratische vormen gedefinieerd door

$$Q_1'(x,y,v_1) := Q_1(x,y) - rv_1^2, \quad Q_2'(x,y,v_2) := Q_2(x,y) - rv_2^2$$

hebben niet-nul oplossingen over $\mathbb{Q}_p$, voor alle priemgetallen p waarvoor geldt $p \,|\, 2abcd$. Volgend lemma zal heel nuttig blijken.

Lemma 8.10

> *We kunnen r vervangen door een ander getal r' die aan precies dezelfde voorwaarden als r voldoet, dat wil zeggen, $r' \in \mathbb{N}$ en $r' \equiv r \mod m^2$, maar waarvoor bovendien geldt dat elke, behalve één, priemfactor van r' het getal $2abcd$ deelt.*

Bewijs. Definieer

$$m := 4\prod_p p,$$

waarbij het product loopt over alle priemgetallen p zodat $p \mid abcd$ en $p \neq 2$. Zij $\delta := \text{ggd}(r, m^2) \geq 1$. Dan is $\text{ggd}(\frac{r}{\delta}, \frac{m^2}{\delta}) = 1$. Uit de stelling van Dirichlet, zoals hieronder gegeven in Propositie 8.11, volgt dan dat er oneindig veel priemgetallen p' zijn zodat

$$p' \equiv \frac{r}{\delta} \mod \frac{m^2}{\delta}.$$

Omdat er oneindig veel priemgetallen zijn die hieraan voldoen, kunnen we zulk een priemgetal p' kiezen zodanig dat $p' \nmid 2abcd$; definieer dan $r' := p'\delta > 0$. Dan voldoet deze r' aan alle condities: $r' \in \mathbb{N}$ en $r' \equiv r \mod m^2$ per constructie. En ook de laatste conditie is vervuld; immers, neem een priemfactor p van r' die verschillend is van p'. Dan geldt $p \mid \delta \mid m^2$. Dus p is gelijk aan 2 of aan een priemdeler van het getal $abcd$. Bijgevolg deelt elke priemfactor van $r' = p'\delta$, behalve de priemfactor p', het getal $2abcd$. Dit beëindigt het bewijs van Lemma 8.10. ■

Aan de hand van Lemma 8.10 blijft dus heel het bewijs wat we tot nu toe gegeven hebben gelden indien we overal r vervangen door r'. Merk op dat we het Hasse-Minkowski principe voor $n = 3$ toe kunnen passen op Q_1' en Q_2', daar deze inderdaad driedimensionale kwadratische vormen met coëfficiënten in $\mathbb{Q}$ zijn. Dus volstaat het om niet-triviale oplossingen van Q_1' en Q_2' in elke $\mathbb{Q}_p$ met $p \in \mathbb{P} \cup \{\infty\}$ te vinden; daaruit verkrijgen we wegens Hasse-Minkowski in $n = 3$ niet-triviale oplossingen van Q_1' en Q_2' in $\mathbb{Q}$. Voor $\mathbb{Q}_\infty = \mathbb{R}$ zijn er inderdaad niet-triviale oplossingen van Q_1' en Q_2' daar $a, r, -d > 0$. Voor alle priemgetallen p zodat $p \mid 2abcd$ zijn we klaar wegens bovenstaande constructie. Voor alle priemgetallen p zodat $p \nmid 2abcd$ en $p \nmid r'$ volgt het gevraagde meteen uit Lemma 8.12. Merk op dat er ons nu nog maar één priemgetal rest waarvoor we het gevraagde nog niet aangetoond hebben, namelijk het unieke priemgetal p zodat $p \nmid 2abcd$ en $p \mid r'$; dit priemgetal hadden we voordien p' genoemd. Dan volgt het gevraagde echter onmiddellijk wegens wegens Lemma 8.13. Hieruit volgt dus, met Hasse-Minkowski in $n = 3$, dat er niet-triviale oplossingen van Q_1' en Q_2' in $\mathbb{Q}$ bestaan. Wegens Lemma 8.6 is dit equivalent met het feit dat er $(x,y),(z,t) \in \mathbb{Q}$ bestaan zodat

$$Q_1(x,y) = r' = Q_2(z,t).$$

Bovendien is $(x,y,z,t) \neq 0$ want anders zou $r' = 0$. We concluderen dat voor deze $0 \neq (x,y,z,t) \in \mathbb{Q}^4$

$$ax^2 + by^2 + cz^2 + dt^2 = Q_1(x,y) - Q_2(z,t) = r' - r' = 0$$

geldt. Dit beëindigt het bewijs van het geval $n = 4$. ■

Propositie 8.11

Zij $a \in \mathbb{Z}$ en $m \in \mathbb{N}$ met $ggd(a,m) = 1$. Dan geldt voor oneindig veel priemgetallen p dat $p \equiv a \mod m$.

Bewijs. Dit bewijs is allesbehalve triviaal en zou ons hier te ver leiden. We verwijzen naar [2] voor een bewijs. ■

Lemma 8.12

Beschouw het veld $\mathbb{Q}_p$ voor een priemgetal $p > 2$. Zij $a,b,c \in \mathbb{Z}_p^\times$. Dan bestaat er een $0 \neq (x,y,z) \in \mathbb{Z}_p^3$ zodat $ax^2 + by^2 + cz^2 = 0$.

Bewijs. Merk op dat in het bijzonder $a,b,c \in \mathbb{Z}_p$. Echter, indien we deze getallen modulo $p\mathbb{Z}_p$ bekijken, dan zijn op deze manier $a,b,c \in \mathbb{Z}/p\mathbb{Z}$; dit geldt daar $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Conclusie: we kunnen de getallen a,b en c zowel in $\mathbb{Z}_p$, $\mathbb{Z}_p/p\mathbb{Z}_p$ als $\mathbb{Z}/p\mathbb{Z}$ zien. Bovendien zijn zowel a,b als c op deze manier verschillend van nul in $\mathbb{Z}/p\mathbb{Z}$ wegens de hypothese dat $a,b,c \in \mathbb{Z}_p^\times$, id est geen van de drie is deelbaar door p in $\mathbb{Z}_p$. Beschouw dan de deelverzamelingen

$$A := \{ax^2 \,|\, x \in \mathbb{Z}/p\mathbb{Z}\}, \quad B := \{-bx^2 - c \,|\, x \in \mathbb{Z}/p\mathbb{Z}\}$$

van $\mathbb{Z}/p\mathbb{Z}$. We weten dat er precies $(p-1)/2$ kwadraten verschillend van nul in $\mathbb{Z}/p\mathbb{Z}$ zitten. Dus $\#A = \frac{p-1}{2} + 1 = \frac{p+1}{2}$ daar $a \neq 0$; analoog is $\#B = \frac{p+1}{2}$ daar $b \neq 0$. Maar

$$\#A + \#B = \frac{p+1}{2} + \frac{p+1}{2} = p+1 > p = \#\mathbb{Z}/p\mathbb{Z}$$

dus kunnen A en B niet disjunct zijn. Bijgevolg bestaan er $\overline{x_0}, \overline{y_0} \in \mathbb{Z}_p/p\mathbb{Z}_p$, met $x_0, y_0 \in \mathbb{Z}_p$, zodat

$$a\overline{x_0}^2 = -b\overline{y_0}^2 - c$$

in $\mathbb{Z}_p/p\mathbb{Z}_p$. Merk op dat dit natuurlijk equivalent is met de bewering

$$ax_0^2 \equiv -by_0^2 - c \mod p$$

in $\mathbb{Z}_p$. Bovendien impliceren de gelijkheden $p \,|\, x_0$ en $p \,|\, y_0$ in de ring $\mathbb{Z}_p$ tesamen de contradictie $p \,|\, c$ in $\mathbb{Z}_p$. Veronderstel dan door symmetrie zonder verlies van algemeenheid dat $p \nmid x_0$ in $\mathbb{Z}_p$, id est $x_0 \in \mathbb{Z}_p^\times$. Omdat $a \in \mathbb{Z}_p^\times$ is a invertibel modulo p en hebben we in $\mathbb{Z}_p$ de congruentie

$$x_0^2 \equiv -\frac{b}{a}y_0^2 - \frac{c}{a} \mod p.$$

Definieer nu een veelterm $f(x) \in \mathbb{Z}_p[x]$ door

$$f(x) := x^2 - \left(-\frac{b}{a}y_0^2 - \frac{c}{a}\right).$$

Merk op dat $f'(x) = 2x$ en dus $f'(x_0) = 2x_0$. We hebben dat

$$\left| x_0^2 + \frac{b}{a} y_0^2 + \frac{c}{a} \right|_p \leq |x_0|_p^2 = |2x_0|_p^2$$

omdat het getal in het linkerlid deelbaar is door p en $|x_0|_p = 1$ daar $x_0 \in \mathbb{Z}_p^\times$, of anders gezegd,

$$|f(x_0)|_p \leq |f'(x_0)|_p^2.$$

Het lemma van Hensel-Richlich, Propositie 8.16, toegepast op de veelterm $f(x)$ levert dan dat er een $x_0' \in \mathbb{Z}_p$ is zodat $f(x_0') = 0$. Dat wil zeggen

$$x_0'^2 + \frac{b}{a} y_0^2 + \frac{c}{a} = 0,$$

of nog,

$$a x_0'^2 + b y_0^2 + 1^2 c = a x_0'^2 + b y_0^2 + c = 0.$$

Dit beïndigt het bewijs van Lemma 8.12. ■

Lemma 8.13

Zij $a,b,c \in \mathbb{Q}^\times$ en $p' \in \mathbb{P} \cup \{\infty\}$. Indien voor alle $p \in \mathbb{P} \cup \{\infty\} \setminus \{p'\}$ een $0 \neq (x,y,z) \in \mathbb{Q}_p^3$ bestaat zodat $ax^2 + by^2 + cz^2 = 0$, dan bestaat er ook een $0 \neq (x,y,z) \in \mathbb{Q}_{p'}^3$ zodat $ax^2 + by^2 + cz^2 = 0$.

Bewijs. Kies een $p \in \mathbb{P} \cup \{\infty\}$ met $p \neq p'$. Stel dat $0 \neq (x,y,z) \in \mathbb{Q}_p$ zodanig is dat $ax^2 + by^2 + cz^2 = 0$. Daar $c \neq 0$ is ook

$$-\frac{a}{c} x^2 - \frac{b}{c} y^2 = z^2.$$

Indien $z \neq 0$ dan is

$$-\frac{a}{c} \left(\frac{x}{z} \right)^2 - \frac{b}{c} \left(\frac{y}{z} \right)^2 = 1,$$

of nog, $(-\frac{a}{c}, -\frac{b}{c})_p = 1$; indien $z = 0$ dan volgt uit Lemma 8.5 dezelfde conclusie. Wegens de kwadratische reciprociteitswet voor het Hilbertsymbool geldt dat

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} \left(-\frac{a}{c}, -\frac{b}{c} \right)_p = 1.$$

Bijgevolg moet ook $(-\frac{a}{c}, -\frac{b}{c})_{p'} = 1$, dat wil zeggen er bestaat een $(x,y) \in \mathbb{Q}_{p'}^2$ zodat

$$-\frac{a}{c} x^2 - \frac{b}{c} y^2 = 1.$$

Dan is

$$ax^2 + by^2 + c\,1^2 = 0,$$

zodat $(x,y,1) \in \mathbb{Q}_{p'}^3$ een niet-triviale oplossing is. Dit beëindigt het bewijs van Lemma 8.13. ■

Lemma 8.14

Zij een vectorruimte A over een veld K en $Q_1, Q_2 : A \to K$ twee niet-ontaarde kwadratische vormen gegeven. Laat

$$Q : A \oplus A \to K : (x,y) \mapsto Q_1(x) - Q_2(y).$$

Dan bereiken Q_1 en Q_2 een gezamenlijke niet-nul waarde als en slechts als er een $0 \neq (x,y) \in A^2$ bestaat zodat $Q(x,y) = 0$.

Bewijs. Veronderstel eerst dat Q_1 en Q_2 een gezamenlijke niet-nul waarde hebben, dat wil zeggen $Q_1(x) = Q_2(y) \neq 0$ voor zekere $x, y \in A$. Dan kunnen zowel x als y niet gelijk aan nul zijn. Bijgevolg is $Q(x,y) = Q_1(x) - Q_2(y) = 0$ met $(x,y) \neq 0$.
Omgekeerd, veronderstel dat er een $0 \neq (x,y) \in A^2$ bestaat zodanig dat $Q(x,y) = 0$.
Stel eerst dat er geen enkele $0 \neq z \in A$ bestaat zodat $Q_1(z) = 0$ of $Q_2(z) = 0$. De vergelijking $Q(x,y) = 0$ betekent precies dat $Q_1(x) = Q_2(y)$. Nu is echter $Q_1(x) = Q_2(y) \neq 0$ daar $(Q_1(x), Q_2(y)) = (0,0)$ wegens bovenstaande impliceert dat $(x,y) = (0,0)$, hetgeen een contradictie is.
Stel nu dat er ofwel een $x \in A$ bestaat zodat $Q_1(x) = 0$ ofwel een $x \in A$ bestaat zodat $Q_2(x) = 0$. Uit Lemma 8.5 volgt dan dat ofwel $Q_1(A) = K$ ofwel $Q_2(A) = K$ daar Q_1 en Q_2 niet-ontaard zijn. Stel bijvoorbeeld dat $Q_1(A) = K$; het andere geval is analoog. Daar Q_2 niet-ontaard is en de nulvorm dat wel is, bestaat er een $0 \neq z \in A$ zodat $Q_2(z) \neq 0$. Natuurlijk is $Q_2(z) \in K$, dus we zijn klaar. Dit beëindigt het bewijs van Lemma 8.14. ■

Lemma 8.15

Indien $p \neq 2$ priem is en $a \in \mathbb{Z}_p$ zodanig is dat $a \equiv 1 \mod p$ in $\mathbb{Z}_p$ geldt, dan bestaat er een $y \in \mathbb{Z}_p$ zodat $y^2 = a$. Indien $p = 2$ en bovendien $a \in \mathbb{Z}_p$ zodanig is dat $a \equiv 1 \mod 8$, dan geldt dezelfde conclusie.

Bewijs. Definieer een veelterm $f(x) \in \mathbb{Z}_p[x]$ door $f(x) := x^2 - a$. Beschouw het element $1 \in \mathbb{Z}$. Merk op dat in $\mathbb{Z}$ de congruentie $1^2 = 1 \equiv a \mod p$ geldt. Bijgevolg is

$$f(1) = 1^2 - a \equiv 0 \mod p.$$

Bovendien hebben we dat $f'(x) = 2x$ voor alle $x \in \mathbb{Z}_p$, zodat in het bijzonder $f'(a) = 2a \not\equiv 0 \mod p$, per hypothese en het feit dat $p \neq 2$. Dan geeft het lemma van Hensel, Eigenschap 6.4.1 in [7], dat er een unieke $y \in \mathbb{Z}_p$ bestaat zodat $f(y) = 0$, of nog, $x^2 = a$.
Nu tonen we het tweede deel aan. Veronderstel dus $p = 2$ en $a \in \mathbb{Z}_p$ zodanig is dat $a \equiv 1 \mod 8$. Beschouw opnieuw de veelterm $f(x)$ van hierboven. Merk op dat

$$|f(1)|_2 = |1^2 - a|_p = |1 - a|_p = p^{-v_p(1-a)} \leq p^{-3}.$$

Ook is

$$|f'(1)|_2 = |2|_2 = p^{-1}.$$

Daar $p = 2 > 1$ hebben we bijgevolg dat

$$|f(1)|_2 \leq p^{-3} < p^{-2} = |f'(1)|_2^2.$$

Uit het lemma van Hensel, Propositie 8.16, volgt dan dat er een $y \in \mathbb{Z}_p$ bestaat zodat $f(y) = 0$, id est $y^2 = a$. Dit beëindigt het bewijs van Lemma 8.15. ■

Volgend resultaat staat bekend als het lemma van Hensel-Richlich.

Propositie 8.16

Zij $f(x) \in \mathbb{Z}_p[x]$ en stel dat er een $a \in \mathbb{Z}_p$ bestaat met $|f(a)|_p < |f'(a)|_p^2$. Dan is er een $y \in \mathbb{Z}_p$ zodat $f(y) = 0$ en bovendien $y \equiv a \mod p$ in $\mathbb{Z}_p$.

Bewijs. Het bewijs is gegeven in [7]. ■

8.3.5 Het geval $n \geq 5$

De reductie van Hasse-Minkowski in dimensie $n \geq 5$ zegt: voor $a_1, \ldots, a_n \in \mathbb{Q}^\times$ geldt dat de vergelijking $a_1x_1^2 + \ldots + a_nx_n^2 = 0$ niet-triviaal oplosbaar is over $\mathbb{Q}$ als en slechts als die vergelijking niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$.

Bewijs. Stel dat $n \geq 5$. We werken per inductie op n. Opnieuw is de ene implicatie triviaal; het is dus voldoende de niet-triviale implicatie te bewijzen. Veronderstel dus dat

$$Q(x_1, \ldots, x_n) := a_1x_1^2 + \ldots + a_nx_n^2 = 0$$

niet-triviaal oplosbaar is over alle $\mathbb{Q}_p$, met $p \in \mathbb{P} \cup \{\infty\}$. Indien we

$$Q_1(x_1, x_2) := a_1x_1^2 + a_2x_2^2, \quad Q_2(x_3, \ldots, x_n) := -a_3x_3^2 - \ldots - a_nx_n^2$$

definiëren, dan is

$$Q(x_1, \ldots, x_n) = Q_1(x_1, x_2) - Q_2(x_3, \ldots, x_n)$$

met Q_1 een 2-dimensionale kwadratische vorm en Q_2 een $(n-2)$-dimensionale kwadratische vorm over $\mathbb{Q}$. Definieer een verzameling

$$V := \{p \text{ is priem} \mid \exists i \geq 3 \text{ zodat } a_i \notin \mathbb{Z}_p^\times\} \cup \{2, \infty\}.$$

Merk op dat V een eindige verzameling is; immers, uit Lemma 8.17 volgt dat

$$V = \{p \text{ is priem} \mid \exists i \geq 3 \text{ zodat de teller of noemer van } a_i \text{ deelbaar is door } p\} \cup \{2, \infty\}.$$

Voor elke $p \in V$ geldt dat Q_1 en Q_2 een zekere niet-nul waarde α_p over $\mathbb{Q}_p$ aannemen; inderdaad, dit volgt uit onze hypothesen en Lemma 8.14. Dus bestaan er $x_{1,p}, x_{2,p}, x_{3,p}, \ldots, x_{n,p} \in \mathbb{Q}_p$ zodat

$$Q_1(x_{1,p}, x_{2,p}) = \alpha_p = Q_2(x_{3,p}, \ldots, x_{n,p}).$$

Beschouw de verzameling $\mathbb{Q}_p^{\times 2}$. In Lemma 8.18 bewijzen we dat $\mathbb{Q}_p^{\times 2}$ open is in $\mathbb{Q}_p^{\times}$. Hieruit volgt natuurlijk dat $\mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p^{\times} \subset \mathbb{Q}_p$ open is in $\mathbb{Q}_p$, daar $\mathbb{Q}_p^{\times} = \mathbb{Q}_p \setminus \{0\}$ open is in $\mathbb{Q}_p$. Daar $\alpha_p \neq 0$ is het makkelijk in te zien dat ook $\alpha_p \mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p$ open is in $\mathbb{Q}_p$. Maar de 2-dimensionale kwadratische vorm

$$Q_1 : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p : (x_1, x_2) \mapsto Q_1(x_1, x_2) := a_1 x_1^2 + a_2 x_2^2$$

is continu, als veelterm, zodat

$$A_p := Q_1^{-1}(\alpha_p \mathbb{Q}_p^{\times 2}) \subset \mathbb{Q}_p \times \mathbb{Q}_p$$

open is in $\mathbb{Q}_p \times \mathbb{Q}_p$. Merk op dat dit alles geldt voor alle $p \in V$. Omdat V eindig is volgt uit Propositie 8.21 dat er $x_1, x_2 \in \mathbb{Q}$ bestaan zodat $(x_1, x_2) \in A_p$ voor alle $p \in V$. Laat nu $q := Q_1(x_1, x_2) \in \mathbb{Q}$. Per constructie is ook $q \in \alpha_p \mathbb{Q}_p^{\times 2}$, of nog, $q/\alpha_p \in \mathbb{Q}_p^{\times 2}$ voor elke $p \in V$; merk ook op dat $q \neq 0$ daar $\alpha_p \neq 0$ en $0 \notin \mathbb{Q}_p^{\times 2}$ voor zulk een p. Definieer nu een $(n-1)$-dimensionale kwadratische vorm

$$Q'(t, x_3, \ldots, x_n) := qt^2 - Q_2(x_3, \ldots, x_n).$$

Dan bestaat er voor elke $p \in V$ een niet-triviale oplossing van $Q' = 0$ in $\mathbb{Q}_p$; inderdaad, merk op dat

$$Q'\left(\sqrt{\frac{\alpha_p}{q}}, x_{3,p}, \ldots, x_{n,p}\right) = q\frac{\alpha_p}{q} - Q_2(x_{3,p}, \ldots, x_{n,p}) = \alpha_p - \alpha_p = 0,$$

met $\left(\sqrt{\frac{\alpha_p}{q}}, x_{3,p}, \ldots, x_{n,p}\right) \neq 0$ daar $\alpha_p \neq 0$. Neem nu een priemgetal $p \notin V$. Dat wil zeggen dat $a_3, a_4, \ldots, a_n \in \mathbb{Z}_p^{\times}$. Omdat $n - 2 \geq 3$ volgt uit Lemma 8.22 dat er een $0 \neq (x_3, \ldots, x_n) \in \mathbb{Q}_p^{n-2}$ bestaat zodat $Q_2(x_3, \ldots, x_n) = 0$. Natuurlijk is $(0, x_3, \ldots, x_n) \neq 0$ dan een niet-triviale oplossing van Q' over $\mathbb{Q}_p$. We besluiten dat er voor elke $p \in \mathbb{P} \cup \{\infty\}$ een niet-triviale oplossing over $\mathbb{Q}_p$ is. Omdat de dimensie van de kwadratische vorm Q' gelijk is aan $n-1$, volgt uit de inductiehypothese dat Q' een niet-triviale oplossing over $\mathbb{Q}$ heeft, dat wil zeggen er bestaat een $0 \neq (t, x_3, \ldots, x_n) \in \mathbb{Q}^{n-1}$ zodat

$$qt^2 - Q_2(x_3, \ldots, x_n) = qt^2 + a_3 x_3^2 + \ldots + a_n x_n^2 = 0.$$

Indien $t = 0$ dan volgt uit Lemma 8.5 dat Q_2 eender welke waarde in $\mathbb{Q}$ bereikt, en dus in het bijzonder $q \in \mathbb{Q}$. Indien $t \neq 0$ dan kunnen we door t delen en bekomen zo dat

$$Q_2\left(\frac{x_3}{t}, \ldots, \frac{x_n}{t}\right) = q.$$

We concluderen dat q wordt bereikt door de kwadratische vorm Q_2 over $\mathbb{Q}$. Maar nu hebben we oplossingen van de vergelijkingen $Q_1 = q$ en $Q_2 = q$ over $\mathbb{Q}$. Voor die bepaalde waarden geldt bijgevolg dat

$$Q = Q_1 - Q_2 = q - q = 0$$

over $\mathbb{Q}$ niet-triviaal oplosbaar is (daar $q \neq 0$). De vergelijking $Q = 0$ is dus niet-triviaal oplosbaar over $\mathbb{Q}$. Dit beëindigt het bewijs van het geval $n \geq 5$. ■

Lemma 8.17

Zij $p \in \mathbb{P}$. Dan is $\mathbb{Q} \cap \mathbb{Z}_p^\times$ precies de verzameling van alle rationale getallen waarvoor geldt dat zowel hun noemer als teller niet deelbaar is door p.

Bewijs. Veronderstel eerst dat $x \in \mathbb{Q} \cap \mathbb{Z}_p^\times$. Schrijf $x = \frac{a}{b}p^k$ met $a,b \in \mathbb{Z}$ en $p \nmid a$, $p \nmid b$, $\text{ggd}(a,b) = 1$. Omdat $x \in \mathbb{Z}_p^\times$ is de p-orde van x gelijk aan 0; dus $k = 0$ en dan zijn zowel de teller als de noemer van x inderdaad niet deelbaar door p.
Stel omgekeerd dat voor $x \in \mathbb{Q}$ geldt dat zowel de teller als noemer niet deelbaar is door p. Schrijf $x = \frac{a}{b}$ met $a,b \in \mathbb{Z}$ en $p \nmid a$, $p \nmid b$, $\text{ggd}(a,b) = 1$. Dan is

$$|x|_p = \left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p} = \frac{p^{-0}}{p^{-0}} = 1,$$

zodat $x \in \mathbb{Z}_p^\times$. Dus geldt dat $x \in \mathbb{Q} \cap \mathbb{Z}_p^\times$. Dit beëindigt het bewijs van Lemma 8.17. ■

Lemma 8.18

Zij $p \in \mathbb{P}$. Dan is $\mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p^\times$ open in $\mathbb{Q}_p^\times$.

Bewijs. Veronderstel eerst dat $p \neq 2$. Kies $x \in \mathbb{Q}_p^{\times 2}$. Dan bestaat er een $k \in \mathbb{Z}$ en een $u \in \mathbb{Z}_p^\times$ zodat $x = p^{2k}u^2$. Zij nu $y \in \mathbb{Q}_p^\times$ willekeurig zodat $|x-y|_p < p^{-2k}$. Uit Lemma 8.19 volgt dat $\nu_p(y) = 2k$. Dus $y = p^{2k}u'$ voor een zekere $u' \in \mathbb{Z}_p^\times$. Bijgevolg is

$$p^{-2k} > |y-x|_p = |p^{2k}u^2 - p^{2k}u'|_p = |p^{2k}|_p\,|u^2-u'|_p = p^{-2k}|u^2-u'|_p,$$

of nog, $|u^2-u'|_p < 1$. Uit Eigenschap 6.3.5. in [7] volgt dan dat u^2 en u' dezelfde eerste digit hebben in hun unieke p-adische expansie. Indien we $u_0, u_0' \in \{0,1,\ldots,p-1\}$ de eerste digit van u respectievelijk u' noemen, dan betekent dit dus dat $u_0^2 \equiv u_0' \mod p$, waarbij we u_0 en u_0' natuurlijk in $\mathbb{Z}/p\mathbb{Z}$ zien. Dus u_0' is een kwadraat modulo p. Indien $p \neq 2$ dan volgt uit Lemma 8.20 dat u' een kwadraat in $\mathbb{Z}_p$ is; zeg $u' = t^2$ met $t \in \mathbb{Z}_p$ en $t \neq 0$. Dan is $y = p^{2k}u' = p^{2k}t^2 = (p^k t)^2 \in \mathbb{Q}_p^{\times 2}$, en in dat geval zijn we dus klaar. Indien $p = 2$ dan is het makkelijk in te zien dat het gevraagde meteen volgt wegens het tweede deel van Lemma 8.20. Dit beëindigt het bewijs van Lemma 8.18. ■

Lemma 8.19

Zij $p \in \mathbb{P}$ en $x \in \mathbb{Q}_p$ een element met $\nu_p(x) = k$. Stel dat $y \in \mathbb{Q}_p$ zodanig is dat $|y-x|_p < p^{-k}$, dan is $\nu_p(y) = k$.

Bewijs. Stel dat $x = p^k u$ met $u \in \mathbb{Z}_p^\times$. Merk op dat

$$|y-x|_p < p^{-k} \Leftrightarrow |p^{-k}y - p^{-k}x|_p < 1.$$

Dit betekent precies dat $p^{-k}y - p^{-k}x \in \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$. Dus $p^{-k}y - p^{-k}x = p^{k'}u'$ met $k' \geq 1$ en $u' \in \mathbb{Z}_p^\times$. Hieruit volgt dat $y - x = p^{k+k'}u'$. Bijgevolg is

$$y = (y-x) + x = p^{k+k'}u' + p^k u = p^k(p^{k'}u' + u).$$

Merk op dat $p \nmid p^{k'}u' + u$ in $\mathbb{Z}_p$ daar dit anders $p \mid u$ zou opleveren, hetgeen niet kan omdat u een eenheid is. Dus $\nu_p(y) = k$. Dit beëindigt het bewijs van Lemma 8.19. ■

Lemma 8.20

Zij $p \in \mathbb{P}$ en veronderstel dat $x \in \mathbb{Z}_p$ een p-adische eenheid is, dat wil zeggen $x_0 \neq 0$, met $x_0 \in \{0, 1, \ldots, p-1\}$ de eerste p-adische digit van x. Indien $p \neq 2$ dan is x een kwadraat in $\mathbb{Z}_p$ als en slechts als x_0 een kwadraat is modulo p. Indien $p = 2$ dan is x een kwadraat in $\mathbb{Z}_2$ als en slechts als $x \equiv 1 \mod 8$.

Bewijs. We kunnen sowieso x op unieke wijze schrijven als $x = x_0 + pt_1$ met $t_1 \in \mathbb{Z}_p$. Stel eerst dat $p \neq 2$. Indien x een kwadraat is in $\mathbb{Z}_p$ dan bestaat er een $y \in \mathbb{Z}_p$ zodat $y^2 = x$. Schrijf y op unieke wijze als $y = y_0 + pt_2$ met $y_0 \in \{1, 2, \ldots, p-1\}$ de eerste p-adische digit van y en $t_2 \in \mathbb{Z}_p$. Uitschrijven van $y^2 = x$ aan de hand van deze uitdrukkingen, en dit modulo p beschouwen, geeft dan meteen dat $x_0 = y_0^2$. Dus $x_0 \equiv y_0^2 \mod p$, id est x_0 is een kwadraat modulo p. Veronderstel nu omgekeerd dat x_0 een kwadraat modulo p is; stel dat $x_0 \equiv y_0^2 \mod p$ voor een $y_0 \in \mathbb{Z}$. Definieer een veelterm $f(x) \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$ door $f(y) := x_0 - y^2$. Merk op dat, daar $p \neq 2$, we hebben dat $f'(y) = -2y \not\equiv 0 \mod p$ voor elke $y \in \mathbb{Z}_p$, dus in het bijzonder is $f'(y_0) = -2y_0 \not\equiv 0 \mod p$ omdat $y_0 \not\equiv 0 \mod p$. En bovendien is $f(y_0) = x_0 - y_0^2 \equiv 0 \mod p$. Uit het lemma van Hensel, Eigenschap 6.4.1 in [7], volgt dan dat er een unieke $t \in \mathbb{Z}_p$ bestaat zodat $f(t) = 0$. Dat betekent precies dat $x_0 = t^2$ een kwadraat in $\mathbb{Z}_p$ is.
Veronderstel nu dat $p = 2$. Indien x een kwadraat is in $\mathbb{Z}_2$ dan bestaat er een $y \in \mathbb{Z}_2$ zodat $y^2 = x$. Stel opnieuw $y = y_0 + 2t$, met $y_0 \in \{0, 1\}$ de eerste 2-adische digit van y en $t \in \mathbb{Z}_2$. Merk op dat noodzakelijkerwijs $y_0 = 1$; inderdaad, x is een eenheid en $y^2 = x$ zodat bijgevolg $y^2 = x \equiv 1 \mod 2$. Na uitschrijven bekomen we dan dat $x = y_0^2 + 4t(t + y_0) = 1 + 4t(t+1)$. Maar sowieso geldt dat $t(t+1) \equiv 0 \mod 2$. Daarom is $x \equiv 1 \mod 8$. De omgekeerde implicatie is precies het tweede deel van Lemma 8.15. Dit beëindigt het bewijs van Lemma 8.20. ■

Volgend resultaat noemt men ook wel de *approximatiestelling*.

Propositie 8.21

Zij $|\cdot|_{p_1}, |\cdot|_{p_2}, \ldots, |\cdot|_{p_n}$ een rij van p-adische metrieken op het veld $\mathbb{Q}$, met $p_i \in \mathbb{P} \cup \{\infty\}$ voor alle $i \in \{1, 2, \ldots, n\}$ en $p_i \neq p_j$ als $i \neq j$. Zij $x_i \in \mathbb{Q}_p$ voor elke $i \in \{1, \ldots, n\}$ en $\varepsilon > 0$ een reëel getal. Dan bestaat er een $x \in \mathbb{Q}$ zodat

$$|x - x_i|_{p_i} < \varepsilon$$

voor alle $i \in \{1, 2, \ldots, n\}$ geldt.

Bewijs. Het bewijs is zou ons te ver leiden; zie [14]. ■

Lemma 8.22

Beschouw het veld $\mathbb{Q}_p$ voor een oneven priemgetal p. Veronderstel dat $n \geq 3$ en $a_1, \ldots, a_n \in \mathbb{Z}_p^\times$. Dan bestaat er een $0 \neq (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ zodat $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$.

Bewijs. Het geval $n = 3$ is precies Lemma 8.12. We bewijzen het lemma eerst voor alle veelvouden van 3, dit wil zeggen voor alle $n = 3k$ met $k \geq 2$. Maar dan kunnen we gewoon k keer Lemma 8.12 toepassen; meer precies gezegd, pas het lemma achtereenvolgens toe op de kwadratische vormen $a_i x_i^2 + a_{i+1} x_{i+1}^2 + a_{i+2} x^{i+2}$ voor $i \in \{1, 4, \ldots, 3k-2\}$. Op die manier krijgen we inderdaad een niet-triviale oplossing. Veronderstel nu dat n geen veelvoud van 3 is. Stel dat $n \equiv 1 \mod 3$. Dan is bestaat er een $k \geq 1$ zodat $n = 3k+1$. Maar het geval $3k$ hebben we reeds aangetoond, en voor de laatste coördinaat kunnen we natuurlijk simpelweg 0 nemen. Dit geeft dan inderdaad een niet-triviale oplossing. Indien $n \equiv 2 \mod 3$ dan kunnen we precies hetzelfde doen, maar dan moeten we wel twee coördinaten de waarde 0 laten aannemen. Dit beëindigt het bewijs van Lemma 8.22. ■

POONENS DEFINITIE VAN $\mathbb{Z}$ IN $\mathbb{Q}$

In deze sectie volgen we Poonens benadering voor het definiëren van $\mathbb{Z}$ in $\mathbb{Q}$. Daarbij maken we op essentiële wijze gebruik van het Hasse-Minkowski principe, zoals uitvoerig uiteengezet in het vorige hoofdstuk. In een volgend hoofdstuk bekijken we dan een op Poonen gebaseerde analoge benadering, namelijk die van Königsmann.

9.1 Begrippen

We herhalen kort de begrippen dewelke we nodig hebben om dit onderdeel te kunnen verstaan. De meeste begrippen werden echter al in Hoofdstuk 7 ingevoerd.

- We noteren met $\mathbb{P} = \{2,3,5,\ldots\}$ de verzameling der priemgetallen.
- Voor $a,b \in \mathbb{Q}^\times$ is $H_{a,b} = \left(\frac{a,b}{\mathbb{Q}}\right)$ de quaternionenalgebra over $\mathbb{Q}$, voortgebracht door i,j, die voldoet aan de relaties $i^2 = a$, $j^2 = b$ en $ij = -ji$.
- Met $\Delta_{a,b}$ bedoelen we de verzameling van $p \in \mathbb{P}$ die ramifiëren in $H_{a,b}$. Voor zulke p hebben we met andere woorden dat $H_{a,b} \otimes \mathbb{Q}_p \ncong M_2(\mathbb{Q}_p)$, of nog,
$$\left(\frac{a,b}{\mathbb{Q}_p}\right) \ncong M_2(\mathbb{Q}_p).$$
- Met $S_{a,b}$ bedoelen we de sporen van alle elementen van $H_{a,b}$ die gereduceerde norm 1 hebben. Aan de hand van de eerder uiteengezette theorie, hebben we dus
$$S_{a,b} = \{2x_1 \in \mathbb{Q} \mid \exists x_2,x_3,x_4 \in \mathbb{Q} : x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\} \subset \mathbb{Q}.$$
Voor een $p \in \mathbb{P} \cup \{\infty\}$ definiëren we de verzameling $S_{a,b}(\mathbb{Q}_p)$ analoog, maar dan voor de quaternionenalgebra $H_{a,b} \otimes \mathbb{Q} \cong \left(\frac{a,b}{\mathbb{Q}_p}\right)$. Dit is dus de verzameling van sporen van elementen van $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ die gereduceerde norm 1 hebben. We zien $S_{a,b}(\mathbb{Q}_p)$ dus als deelverzameling van $\mathbb{Q}_p$.
- Voor een quaternionenalgebra over een veld K, waarin een element a zit, wordt de veelterm
$$x^2 - S(a)x + N(a) \in K[x]$$
de gereduceerde karakteristieke veelterm van a in die quaternionenalgebra genoemd; hierbij is S het gereduceerde spoor en N de gereduceerde norm, respectievelijk.

- Voor een priemmacht q van p is U_q de verzameling van $s \in \mathbb{F}_q$ zodat de veelterm $x^2 - sx + 1$ irreducibel is in $\mathbb{F}_q[x]$. Dat zijn dus precies die waarden van $s \in \mathbb{F}_q$ waarvoor geldt dat $x^2 - sx + 1$ geen oplossingen over $\mathbb{F}_q$ heeft.
- Zij $\mathrm{red}_p : \mathbb{Z}_p \to \mathbb{F}_p$ de natuurlijke reductie, dat wil zeggen de projectie van een p-adisch geheel op zijn eerste p-adische digit.

In Definitie 7.25 definieerden we $\Delta_{a,b}$ als de verzameling van alle $p \in \mathbb{P} \cup \{\infty\}$ waarvoor p niet splijt in $H_{a,b}$, voor alle $a,b \in \mathbb{Q}^\times$. Deze notatie is overgenomen van Königsmann. Poonen gebruikt echter een iets andere notatie, zoals hieronder te zien.

Definitie 9.1

We stellen

$$\Delta_{a,b} := \{p \in \mathbb{P} \mid p \text{ splijt niet in } H_{a,b}\}$$

voor alle $a,b \in \mathbb{Q}^\times$.

Het komt er dus op neer dat Poonen ramificatie op ∞ niet beschouwt. Het is onderverstaan dat we vanaf nu Definitie 9.1 gebruiken, en dat voor de rest van dit hoofdstuk, en *niet* Definitie 7.25 uit Hoofdstuk 5.

We hebben met andere woorden dat $\Delta_{a,b}$ de verzameling van alle $p \in \mathbb{P}$ is waarvoor p ramifieert in $H_{a,b}$, of nog, $H_{a,b} \otimes \mathbb{Q}_p \ncong M_2(\mathbb{Q}_p)$, of nog,

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) \ncong M_2(\mathbb{Q}_p).$$

Uit Propositie 7.16 volgt dat de vorige uitspraken equivalent zijn met het niet-oplosbaar zijn van de vergelijking $ax^2 + by^2 = 1$ over $\mathbb{Q}_p$, hetgeen op zijn beurt, per definitie, weer equivalent is met $(a,b)_p = -1$. Dus geldt voor alle $a,b \in \mathbb{Q}^\times$ dat

$$\Delta_{a,b} = \{p \in \mathbb{P} \mid (a,b)_p = -1\}.$$

De kwadratische reciprociteitswet voor het Hilbertsymbool zegt dat

$$\prod_{p \in \mathbb{P}} (a,b)_p = (a,b)_\infty,$$

waarbij alle factoren in het linkerlid gelijk zijn aan 1, op een eindig aantal factoren na. Nu zijn er essentieel twee mogelijkheden:

1. Stel dat a,b een verschillend teken hebben, of $a,b > 0$. Dan is $(a,b)_\infty = 1$. Dit impliceert dat $(a,b)_p = -1$ voor een eindig en even aantal $p \in \mathbb{P}$.
2. Stel dat $a,b < 0$. Dan is $(a,b)_\infty = -1$. Dit impliceert dat $(a,b)_p = -1$ voor een eindig en oneven aantal $p \in \mathbb{P}$.

9.2 Enkele hulpstellingen

Poonens constructie maakt gebruik van een aantal lemma's; we formuleren en bewijzen ze hier.

Lemma 9.2

Zij $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ een $\mathbb{Q}_p$-quaternionenalgebra met $p \in \Delta_{a,b}$, en zij $s \in \mathbb{Q}_p$. Dan geldt dat $x^2 - sx + 1 \in \mathbb{Q}_p[x]$ de gereduceerde karakteristieke veelterm van een zeker element van $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is als en slechts als $x^2 - sx + 1$ een macht van een monische irreducibele veelterm over $\mathbb{Q}_p$ is.

Bewijs. Veronderstel eerst dat $x^2 - sx + 1 \in \mathbb{Q}_p[x]$ de gereduceerde karakteristieke veelterm van een zeker element $\alpha \in \left(\frac{a,b}{\mathbb{Q}_p}\right)$ is; id est

$$x^2 - sx + 1 = x^2 - S(\alpha)x + N(\alpha),$$

met N en S respectievelijk de gereduceerde norm en het gereduceerde spoor van α. We tonen aan dat $x^2 - sx + 1$ dan een macht van een monische irreducibele veelterm over $\mathbb{Q}_p$ is. Er zijn twee mogelijkheden: ofwel is $x^2 - sx + 1$ irreducibel over $\mathbb{Q}_p$ ofwel is $x^2 - sx + 1$ reducibel over $\mathbb{Q}_p$. In het eerste geval zijn we klaar; veronderstel dus dat $x^2 - sx + 1$ reducibel over $\mathbb{Q}_p$ is. We tonen dan aan dat deze veelterm een kwadraat van een monische lineaire veelterm over $\mathbb{Q}_p$ is. Natuurlijk hebben we $N(\alpha) = 1$ en $S(\alpha) = s$. We weten per hypothese dat

$$x^2 - sx + 1 = (x - a_1)(x - a_2)$$

met $a_1, a_2 \in \mathbb{Q}_p$. Veronderstel nu uit het ongerijmde dat $a_1 \neq a_2$. Vanwege de opmerking net na Definitie 7.12 weten we dat een element van een quaternionenalgebra ingevuld in zijn gereduceerde karakteristieke veelterm steeds nul geeft. Dus

$$0 = \alpha^2 - s\alpha + 1 = (\alpha - a_1)(\alpha - a_2).$$

Omdat $p \in \Delta_{a,b}$ is de beschouwde quaternionenalgebra een divisiealgebra, en bijgevolg hebben we dat ofwel $\alpha = a_1$ ofwel $\alpha = a_2$, dus zeker $\alpha \in \mathbb{Q}_p$. Maar dan is

$$1 = N(\alpha) = N(\alpha + 0\,i + 0\,j + 0\,i \cdot j) = \alpha^2.$$

Dus $\alpha = \pm 1$. Ook hebben we $s = S(\alpha) = 2\alpha$, zodat $s = \pm 2$. Als $s = -2$, dan is

$$(x - a_1)(x - a_2) = x^2 - sx + 1 = x^2 + 2x + 1 = (x + 1)^2 = (x + 1)(x + 1),$$

zodat we de contradictie $a_1 = -1 = a_2$ bekomen. Analoog, als $s = 2$, dan is

$$(x - a_1)(x - a_2) = x^2 - sx + 1 = x^2 - 2x + 1 = (x - 1)^2 = (x - 1)(x - 1),$$

zodat we de contradictie $a_1 = 1 = a_2$ hebben. Dit toont de eerste implicatie aan.

De omgekeerde implicatie is lastiger. Veronderstel dat x^2-sx+1 een macht van een monische irreducibele veelterm over $\mathbb{Q}_p$ is. Stel eerst dat x^2-sx+1 een dubbele wortel heeft. Dat impliceert dat de discriminant van x^2-sx+1 gelijk is aan nul, dat wil zeggen $s^2-4=0$, en dus $s=\pm 2$. Beschouw eerst het geval dat $s=2$, zodat $x^2-sx+1=(x-1)^2$. Merk op voor $1\in\left(\frac{a,b}{\mathbb{Q}_p}\right)$ geldt dat

$$N(1)=N(1++0\,i+0\,j+0\,i\cdot j)=1^2=1.$$

Ook is $S(1)=2$. Bijgevolg is de gereduceerde karakteristieke veelterm van 1 precies gelijk aan

$$x^2-S(1)x+N(1)=x^2-2x+1=(x-1)^2$$

en dan zijn we klaar. Beschouw dan het geval dat $s=-2$, zodat $x^2-sx+1=(x+1)^2$. Merk op voor $-1\in\left(\frac{a,b}{\mathbb{Q}_p}\right)$ geldt dat

$$N(-1)=N(-1++0\,i+0\,j+0\,i\cdot j)=(-1)^2=1,$$

en ook $S(-1)=-2$. Dus is de gereduceerde karakteristieke veelterm van -1 precies gelijk aan

$$x^2-S(-1)x+N(-1)=x^2+2x+1=(x+1)^2.$$

Het geval dat x^2-sx+1 een dubbele wortel heeft hebben we daarmee aangetoond. Veronderstel tenslotte dat x^2-sx+1 irreducibel is over $\mathbb{Q}_p$. De vergelijking

$$x^2-sx+1$$

heeft een wortel in $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ want het is duidelijk dat deze vergelijking een wortel heeft in een geschikt niet-geramifieerd kwadratisch uitbreidingsveld van $\mathbb{Q}_p$. Daar niet-geramifieerde kwadratische uitbreidingsvelden van $\mathbb{Q}_p$ steeds isomorf zijn over $\mathbb{Q}_p$, en daar de quaternionendivisiealgebra $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ zulk een deelveld bevat, mogen we vervolgens besluiten dat de vergelijking x^2-sx+1 inderdaad een wortel heeft in $\left(\frac{a,b}{\mathbb{Q}_p}\right)$. We hebben dus een $\alpha\in\left(\frac{a,b}{\mathbb{Q}_p}\right)$ zodat $\alpha^2-s\alpha+1=0$. Merk op dat $\alpha\notin\mathbb{Q}_p$ daar x^2-sx+1 irreducibel is over $\mathbb{Q}_p$ en dus in $\mathbb{Q}_p$ geen wortels kan hebben. De opmerking na Definitie 7.12 geeft $\alpha^2-S(\alpha)\alpha+N(\alpha)=0$. Gelijkstellen van de vergelijkingen levert $s\alpha-1=S(\alpha)\alpha-N(\alpha)$, of nog, $(s-S(\alpha))\alpha=1-N(\alpha)$. Als $s-S(\alpha)\neq 0$, dan volgt $\alpha=\frac{1-N(\alpha)}{s-S(\alpha)}\in\mathbb{Q}_p$, contradictie. Daarom moet $s=S(\alpha)$ en dus ook $N(\alpha)=1$. Dat betekent dat $x^2-sx+1=x^2-S(\alpha)x+N(\alpha)$ de gereduceerde karakteristieke veelterm van $\alpha\in\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is. Dit beëindigt het bewijs van Lemma 9.2. ■

Lemma 9.3

Zij $p\in\mathbb{P}$. Indien $p\notin\Delta_{a,b}$, dan is $S_{a,b}(\mathbb{Q}_p)=\mathbb{Q}_p$. In het geval dat $p\in\Delta_{a,b}$, is $red_p^{-1}(U_p)\subset S_{a,b}(\mathbb{Q}_p)\subset\mathbb{Z}_p$.

Bewijs. Voor $s \in \mathbb{Q}_p$ geldt dat $s \in S_{a,b}(\mathbb{Q}_p)$ als en slechts als $x^2 - sx + 1$ de gereduceerde karakteristieke veelterm van een zeker element van $H_{a,b} \otimes \mathbb{Q}_p \cong \left(\frac{a,b}{\mathbb{Q}_p}\right)$ is; inderdaad, dit volgt meteen uit de definities.
Veronderstel nu eerst dat $p \notin \Delta_{a,b}$. Dit betekent dat $H_{a,b} \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$, per definitie van $\Delta_{a,b}$. Uit Propositie 7.16 volgt dat we $a = 1$ en $b = -1$ mogen veronderstellen. Neem een element $s \in \mathbb{Q}_p$. We construeren dan een matrix $A \in M_2(\mathbb{Q}_p)$ zodat de norm van A gelijk is aan 1 en bovendien het spoor van A gelijk aan s; zeg

$$A = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} \in M_2(\mathbb{Q}_p).$$

Merk op dat

$$N(A) = \lambda_1^2 - \lambda_2^2 + \lambda_3^2 - \lambda_4^2, \quad S(A) = 2\lambda_1.$$

Uit Propositie 7.16 volgt dat de vergelijking $\lambda_3^2 - \lambda_4^2 = 1$ oplosbaar is voor zekere $\lambda_3, \lambda_4 \in \mathbb{Q}_p$. Het is nu duidelijk dat het volstaat om $\lambda_1 = \frac{s}{2}, \lambda_2 = \frac{s}{2}$ te nemen. Dus $s \in S_{a,b}(\mathbb{Q}_p)$. De omgekeerde inclusie is evident.
Veronderstel nu dat $p \in \Delta_{a,b}$. Zij $s \in \mathrm{red}_p^{-1}(U_p)$, dat wil zeggen $\mathrm{red}_p(s) \in U_p$, id est,

$$x^2 - \mathrm{red}_p(s)x + 1$$

is irreducibel in $\mathbb{F}_p[x]$. Dit is equivalent met het feit dat $x^2 - \mathrm{red}_p(s)x + 1$ geen nulpunten in $\mathbb{F}_p$ heeft. We tonen nu aan dat elke oplossing van $x^2 - sx + 1 = 0$ in $\mathbb{Q}_p$ zelfs in $\mathbb{Z}_p$ zit. Veronderstel dat $t^2 - st + 1 = 0$ voor een $t \in \mathbb{Q}_p$. We werken uit het ongerijmde; veronderstel daarom dat $\nu_p(t) < 0$. Duidelijk moet $\nu_p(st) \neq 0$, want als $\nu_p(st) = 0$ dan wordt de contradictie

$$0 > 2\nu_p(t) = \min\{2\nu_p(t), 0\} = \min\{\nu_p(t^2), 0\} = \nu_p(t^2 + 1) = \nu_p(st) = 0$$

bekomen. Omdat $\nu_p(st) \neq 0$ is

$$\nu_p(t^2) = \nu_p(st - 1) = \min\{\nu_p(st), 0\}.$$

Maar deze vergelijking kan niet; immers als $\nu_p(st) \geq 0$ dan impliceert ze de contradictie $0 > 2\nu_p(t) = \nu_p(t^2) = 0$. Als daarentegen $\nu_p(st) < 0$ dan geldt

$$2\nu_p(t) = \nu_p(t^2) = \nu_p(st) = \nu_p(s) + \nu_p(t) \quad \Rightarrow \quad 0 > \nu_p(t) = \nu_p(s) \geq 0,$$

en ook dit is een contradictie. We zijn in alle gevallen tot een contradictie gekomen, en besluiten dat inderdaad elke oplossing van $x^2 - sx + 1 = 0$ in $\mathbb{Q}_p$ zelfs in $\mathbb{Z}_p$ zit. Dan kan de veelterm $x^2 - sx + 1$, beschouwd over het veld $\mathbb{Q}_p$, natuurlijk geen nulpunten in $\mathbb{Q}_p$ hebben; inderdaad, dit nulpunt, dat dan zelfs in $\mathbb{Z}_p$ zit, zou anders aanleiding geven tot een nulpunt van $x^2 - \mathrm{red}_p(s)x + 1$ in $\mathbb{F}_p$. Bijgevolg is $x^2 - sx + 1 \in \mathbb{Q}_p[x]$ irreducibel. Uit Lemma 9.2 volgt dat $x^2 - sx + 1$ een gereduceerde karakteristieke veelterm van een zeker element van $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is. De opmerking aan het begin van het bewijs van dit lemma laat ons dan toe te besluiten dat $s \in S_{a,b}(\mathbb{Q}_p)$.
Neem tenslotte $s \in \mathbb{Q}_p$ met $s \notin \mathbb{Z}_p$. We tonen aan dat de vergelijking $x^2 - sx + 1$ dan een product van twee verschillende lineaire factoren over $\mathbb{Q}_p$ is. Duidelijk is

het voldoende te bewijzen dat de discriminant van de vergelijking, zijnde s^2-4, een kwadraat is in $\mathbb{Q}_p^\times$; inderdaad, indien $s^2-4=t^2$ met $t\in\mathbb{Q}_p^\times$, dan is

$$x^2-sx+1=\left(x-\frac{s+t}{2}\right)\left(x-\frac{s-t}{2}\right).$$

een product van twee lineaire factoren over $\mathbb{Q}_p$, die ook verschillend zijn daar $t\neq 0$. We tonen dus aan dat s^2-4 een kwadraat is in $\mathbb{Q}_p^\times$. Omdat $s\in\mathbb{Q}_p\setminus\mathbb{Z}_p$ kunnen we $s=\frac{u}{p^k}$ op unieke wijze schrijven met een geheel getal $k\geq 1$ en $u\in\mathbb{Z}_p^\times$. Omdat $s\notin\mathbb{Z}_p$ is zeker $s\neq\pm 2$, zodat steeds $s^2-4\neq 0$. Door met het p-adische geheel $p^{2k}u^{-2}$ te vermenigvuldigen zien we dat $s^2-4=\frac{u^2}{p^{2k}}-4\in\mathbb{Q}_p^{\times 2}$ als en slechts als $1-4p^{2k}u^{-2}\in\mathbb{Q}_p^{\times 2}$. Maar er geldt $1-4p^{2k}u^{-2}\in\mathbb{Z}_p$ en bovendien $1-4p^{2k}u^{-2}\equiv 1 \mod p$. Indien $p\neq 2$ dan volgt uit Lemma 8.15 dat $s^2-4=1-4p^{2k}u^{-2}$ een kwadraat is in $\mathbb{Z}_p\subset\mathbb{Q}_p$. Indien $p=2$, dan is duidelijk $1-4p^{2k}\equiv 1 \mod 8$, zodat uit Lemma 8.15 dezelfde conclusie volgt. Dus de veelterm kan geen macht van een monische irreducibele veelterm in $\mathbb{Q}_p[x]$ zijn; uit Lemma 9.2 volgt dan dat $s\notin S_{a,b}(\mathbb{Q}_p)$. Dit beëindigt het bewijs van Lemma 9.3. ■

In volgend lemma komt het Hasse-Minkowski principe tot uiting.

Lemma 9.4

Zij $a,b\in\mathbb{Q}^\times$ en veronderstel bovendien dat ofwel $a>0$, ofwel $b>0$. Dan is $S_{a,b}=\mathbb{Q}\cap\bigcap_{p\in\mathbb{P}}S_{a,b}(\mathbb{Q}_p)$.

Bewijs. De inclusie van links naar rechts is triviaal, aangezien elke oplossing van de vergelijking

$$x_1^2-ax_2^2-bx_3^2+abx_3^2=1$$

over $\mathbb{Q}$ een oplossing over elk van zijn completies $\mathbb{Q}_p$ met $p\in\mathbb{P}$ induceert, daar $\mathbb{Q}\subset\mathbb{Q}_p$. Voor deze implicatie hebben we dus geen enkel resultaat nodig. De inclusie van rechts naar links is echter helemaal niet triviaal. Maar Propositie 8.2, dat is het Hasse-Minkowski principe, levert het gevraagde. Dit beëindigt het bewijs van Lemma 9.4. ■

Merk op dat dan uit Lemma 9.3 volgt dat we kunnen schrijven

$$S_{a,b}=\mathbb{Q}\cap\bigcap_{p\in\mathbb{P}}S_{a,b}(\mathbb{Q}_p)=\mathbb{Q}\cap\bigcap_{p\in\Delta_{a,b}}S_{a,b}(\mathbb{Q}_p).$$

Hierbij is het onderverstaan dat, indien $\Delta_{a,b}=\emptyset$, dan $S_{a,b}=\mathbb{Q}$.

Lemma 9.5

Voor elke priemmacht q is $U_q\neq\emptyset$. Indien $q>11$, dan is $U_q+U_q=\mathbb{F}_q$.

Bewijs. Veronderstel dat q oneven is. Uit Lemma 9.6 hieronder weten we dat

$$U_q=S(\{\alpha\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q\,|\,N(\alpha)=1\}).$$

Hier zijn S en N respectievelijk het spoor en de norm van de velduitbreiding $\mathbb{F}_q \subset \mathbb{F}_{q^2}$. Omdat we weten dat $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ een uitbreiding van graad 2 is, kunnen we een $c \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ kiezen zodat $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{c})$. Ten opzichte van de basis $\{1, \sqrt{c}\}$ van de vectorruimte $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ rekenen we makkelijk na dat het spoor en norm van een zekere $\alpha = \alpha_1 + \alpha_2\sqrt{c}$, met $\alpha_1, \alpha_2 \in \mathbb{F}_q$, gelijk zijn aan

$$S(\alpha) = S(\alpha_1 + \alpha_2\sqrt{c}) = 2\alpha_1, \quad N(\alpha) = N(\alpha_1 + \alpha_2\sqrt{c}) = \alpha_1^2 - c\alpha_2^2.$$

Merk op dat voor elke $\alpha \in \mathbb{F}_{q^2}$ geldt dat $N(\alpha) = \alpha\,\alpha^q = \alpha^{q+1}$. Dit is waar omdat de norm van een element gelijk is aan het product van al zijn conjugeerden over het basisveld, en de geconjugeerden van $\alpha \in \mathbb{F}_{q^2}$ over $\mathbb{F}_q$ zijn precies gelijk aan de elementen α en α^q. We bewijzen dat er $q+1$ elementen in $\mathbb{F}_{q^2}$ zijn met norm 1. Uit bovenstaande volgt dat we precies die elementen $\alpha \in \mathbb{F}_{q^2}^\times$ moeten zoeken waarvoor $\alpha^{q+1} = 1$. Maar merk op dat de multiplicatieve groep van een eindig veld cyclisch is; in dit geval isomorf met $(\mathbb{Z}/(q^2-1)\mathbb{Z}, +)$. Merk op dat $q^2 - 1 = (q-1)(q+1)$. De gezochte elementen vormen dan precies de deelgroep $(\mathbb{Z}/(q+1)\mathbb{Z}, +)$ van de groep $(\mathbb{Z}/(q^2-1)\mathbb{Z}, +)$, en de conclusie volgt dat er precies $q+1$ zulke elementen in $\mathbb{F}_{q^2}$ zijn. Omdat $\mathbb{F}_q$ exact q elementen heeft, en er precies $q+1$ elementen zijn met norm 1, volgt dat $\{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,|\, N(\alpha) = 1\} \neq \emptyset$ en dus ook $U_q \neq \emptyset$.
We tonen nu aan dat, indien $q > 11$ (en oneven is), dan $U_q + U_q = \mathbb{F}_q$. Natuurlijk is de inclusie van links naar rechts evident. We tonen daarom de inclusie van rechts naar links aan. Merk op dat $U_q = -U_q$; dit volgt uit Lemma 9.6 daar de norm van een element gelijk is aan de norm van zijn tegengestelde. Bijgevolg is $0 \in U_q + U_q$. Neem nu $a \in \mathbb{F}_q^\times$. We tonen dan aan dat $a \in U_q + U_q$. Maar duidelijk is $a \in U_q + U_q$ als en slechts als er $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ bestaan zodat

$$x_1^2 - cy_1^2 = 1, \quad x_2^2 - cy_2^2 = 1, \quad 2x_1 + 2x_2 = a, \quad y_1, y_2 \neq 0.$$

Deze voorwaarden definiëren een gladde kromme X in $\mathbb{A}^4_{\mathbb{F}_q}$. We kunnen de variabele x_2 hieruit nog elimineren; op die manier hebben we de projectieve sluiting $\bar{X}$ van X. Duidelijk is dit een doorsnede van twee kwadrieken in $\mathbb{P}^3$, de drie dimensionale projectieve ruimte. Na wat rekenen zien we dat het functieveld van $\bar{X}$ gelijk is aan

$$\mathbb{F}_q(x_1)\left(\sqrt{c\left(1-x_1^2\right)}, \sqrt{c\left(1-\left(\frac{a}{2}-x_1\right)^2\right)}\right).$$

Merk op dat dit inderdaad het functieveld van de doorsnede van twee kwadrieken is. Men kan aantonen dat dit functieveld isomorf is met het functieveld van een vergelijking van de vorm $y^2 = f(x)$ met $f(x)$ een vierdegraadsveelterm over $\mathbb{F}_q$ zodat $f(x)$ in de algebraïsche sluiting van $\mathbb{F}_q$ geen meervoudige wortels heeft. Maar dit toont dan aan dat X birationaal equivalent is met een elliptische kromme. Hieruit volgt dat we uit zowel X als de elliptische kromme een eindige aantal punten kunnen weglaten, zodat de geometrische objecten die overblijven isomorf zijn. Meer geavanceerde theorie over algebraïsche krommen geeft dat het voldoende is om van de elliptische kromme 12 punten weg te laten.
Indien q even is, schrijf dan $\mathbb{F}_{q^2} = \mathbb{F}_q(\gamma)$ waarbij $\gamma^2 + \gamma + c = 0$ voor een zekere $c \in \mathbb{F}_q$; we zoeken dan een $\mathbb{F}_q$-punt op de curve X gedefinieerd door

$$x_1^2 + x_1y_1 + cy_1^2, \quad x_2^2 + x_2y2 + cy_2^2 = 1, \quad y_1 + y_2 = a, \quad y_1, y_2 \neq 0.$$

Men kan dan analoog redeneren zoals net, en dan vindt men dat X ook in dit geval birationaal equivalent is met een elliptische kromme, en dat het bovendien ook in dit geval volstaat om 12 punten weg te laten. We passen nu de ongelijkheid van Hasse omtrent elliptische curves toe op de X; door op te merken dat het, zowel in het geval dat q oneven is als in het geval dat q even is, volstaat 12 punten uit de elliptische kromme weg te nemen, volgt dan voor alle q dat

$$\#X(\mathbb{F}_q) \geq (q+1-2\sqrt{q})-12 = (\sqrt{q}-1)^2-12.$$

Voor alle $q \geq 20$ hebben we dus

$$\#X(\mathbb{F}_q) \geq (\sqrt{20}-1)^2-12 = 20+1-2\sqrt{20}-12 = 9-2\sqrt{20} > 0.$$

Indien $11 < q < 20$ dan zijn de enige mogelijkheden nog $\{13,16,17,19\}$; hiervoor kan men eenvoudig manueel checken dat $U_q + U_q = \mathbb{F}_q$. Dit beëindigt het bewijs van Lemma 9.5. ■

Lemma 9.6

Zij q een priemmacht. Dan kunnen we

$$U_q = S(\{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,|\, N(\alpha) = 1\})$$

schrijven.

Bewijs. Omdat we weten dat $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ een uitbreiding van graad 2 is, kunnen we een $c \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ kiezen zodat $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{c})$. Ten opzichte van de basis $\{1, \sqrt{c}\}$ van de vectorruimte $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ rekenen we makkelijk na dat het spoor en norm van een zekere $\alpha = \alpha_1 + \alpha_2\sqrt{c}$, met $\alpha_1, \alpha_2 \in \mathbb{F}_q$, gelijk zijn aan

$$S(\alpha) = S(\alpha_1 + \alpha_2\sqrt{c}) = 2\alpha_1, \quad N(\alpha) = N(\alpha_1 + \alpha_2\sqrt{c}) = \alpha_1^2 - c\alpha_2^2.$$

We hebben per definitie

$$U_q = \{s \in \mathbb{F}_q \,|\, \text{de veelterm } x^2 - sx + 1 \text{ is irreducibel in } \mathbb{F}_q[x]\}$$

en

$$S(\{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,|\, N(\alpha) = 1\}) = \{2\alpha_1 \in \mathbb{F}_q \,|\, \exists \alpha_2 \in \mathbb{F}_q \setminus \{0\} : \alpha_1^2 - c\alpha_2^2 = 1\}.$$

Ten eerste tonen we voor een $t \in \mathbb{F}_q$ de equivalentie

$$\exists y \in \mathbb{F}_q : (y-t)^2 = t^2 - 1 \;\Leftrightarrow\; \nexists z \in \mathbb{F}_q \setminus \{0\} : t^2 - 1 = cz^2$$

aan. De implicatie van links naar rechts is duidelijk daar c geen kwadraat is in $\mathbb{F}_q$. We tonen nu de implicatie van rechts naar links aan door contrapositie. Veronderstel dus dat er geen enkele $y \in \mathbb{F}_q$ bestaat zodat $(y-t)^2 = t^2 - 1$. Dan is $t^2 - 1$ geen kwadraat in $\mathbb{F}_q$. Dat wil zeggen, $\sqrt{t^2-1} \notin \mathbb{F}_q$. Natuurlijk is wel $\sqrt{t^2-1} \in \mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{c})$, daar $(\sqrt{t^2-1})^2 - (t^2-1) = 0$ impliceert dat $\mathbb{F}_q(\sqrt{t^2-1}) \cong \mathbb{F}_{q^2}$ als vectorruimten over

$\mathbb{F}_q$. Schrijf $\sqrt{t^2-1} = \alpha_1 + \alpha_2\sqrt{c}$, voor zekere $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Merk op dat α_1 en α_2 niet beide nul zijn; anders zou $t^2 - 1 = 0$ wel een kwadraat in $\mathbb{F}_q$ zijn. Kwadrateren geeft

$$t^2 - 1 = \alpha_1^2 + c\alpha_2^2 + 2\alpha_1\alpha_2\sqrt{c}.$$

Daar $\{1, \sqrt{c}\}$ een basis van de vectorruimte $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ is, volgt door uniciteit van schrijfwijze dat $t^2 - 1 = \alpha_1^2 + c\alpha_2^2$ en $2\alpha_1\alpha_2 = 0$. Maar $\alpha_2 \neq 0$, want anders zou $t^2 - 1 = \alpha_1^2$ een kwadraat in $\mathbb{F}_q$ zijn, zodat $\alpha_1 = 0$. Dan is inderdaad $t^2 - 1 = c\alpha_2^2$ met $\alpha_2 \in \mathbb{F}_q \setminus \{0\}$. Dit toont de hierboven gestelde equivalentie aan.
Voor een $t \in \mathbb{F}_q$ geldt dat

$$\begin{aligned}
2t \notin U_q &\Leftrightarrow x^2 - (2t)x + 1 \text{ is reducibel in } \mathbb{F}_q[x] \\
&\Leftrightarrow \exists y \in \mathbb{F}_q : y^2 - (2t)y + 1 = 0 \\
&\Leftrightarrow \exists y \in \mathbb{F}_q : (y-t)^2 = t^2 - 1 \\
&\Leftrightarrow \nexists z \in \mathbb{F}_q \setminus \{0\} : t^2 - 1 = cz^2 \\
&\Leftrightarrow \nexists z \in \mathbb{F}_q \setminus \{0\} : t^2 - cz^2 = 1 \\
&\Leftrightarrow 2t \notin S(\{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,|\, N(\alpha) = 1\}).
\end{aligned}$$

De conclusie is dat inderdaad

$$U_q = S(\{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,|\, N(\alpha) = 1\}).$$

Dit beëindigt het bewijs van Lemma 9.6. ■

Definitie 9.7

Zij $a, b \in \mathbb{Q}^\times$. Laat dan

$$T_{a,b} := S_{a,b} + S_{a,b} + \{0, 1, 2, \ldots, N-1\} \subset \mathbb{Q}.$$

Hierbij is $N := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$.

Equivalent kan men ook stellen

$$T_{a,b} = \{x \in \mathbb{Q} \,|\, \exists s_1, s_2 \in S_{a,b} \text{ en } n \in \{0, 1, 2, \ldots, N-1\} \text{ zodat } x = s_1 + s_2 + n\}.$$

Definitie 9.8

Zij $\mathbb{Z}_{(p)} := \mathbb{Z}_p \cap \mathbb{Q}$ voor elke $p \in \mathbb{P}$.

Merk op dat $\mathbb{Z}_{(p)}$, voor elke $p \in \mathbb{P}$, gelijk is aan de verzameling

$$\{x \in \mathbb{Q} \,|\, \text{de noemer van } x \text{ is niet deelbaar door } p\}.$$

Dit is inderdaad heel eenvoudig aan te tonen.

Volgend lemma is de essentie van Poonens definitie van $\mathbb{Z}$ in $\mathbb{Q}$.

Lemma 9.9

Zij $a,b \in \mathbb{Q}^\times$ zodat ofwel $a > 0$, ofwel $b > 0$. Dan is

$$T_{a,b} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}.$$

In deze notatie is het onderverstaan dat $T_{a,b} = \mathbb{Q}$ indien $\Delta_{a,b} = \emptyset$.

Bewijs. Veronderstel eerst dat $\Delta_{a,b} = \emptyset$. Dan volgt meteen uit de discussie na Lemma 9.4 dat $S_{a,b} = \mathbb{Q}$, zodat inderdaad

$$T_{a,b} = S_{a,b} + S_{a,b} = \mathbb{Q} + \mathbb{Q} + \{0,1,2,\ldots,N-1\} = \mathbb{Q}.$$

Veronderstel nu dat $\Delta_{a,b} \neq \emptyset$. Stel ter afkorting $T'_{a,b} := \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$; dan tonen we de gelijkheid $T_{a,b} = T'_{a,b}$ aan. Zoals reeds eerder opgemerkt volgt uit Lemma 9.3 dat

$$S_{a,b} = \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p).$$

Ook volgt uit Lemma 9.3 dat voor elke $p \in \Delta_{a,b}$ geldt dat $S_{a,b}(\mathbb{Q}_p) \subset \mathbb{Z}_p$. Bijgevolg is

$$S_{a,b} = \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p) \subset \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_p = \bigcap_{p \in \Delta_{a,b}} \mathbb{Q} \cap \mathbb{Z}_p = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}.$$

Daarom is $S_{a,b} \subset T'_{a,b}$. Neem nu een element $s_1 + s_2 + n \in T_{a,b}$, met $s_1, s_2 \in S_{a,b}$ en $n \in \{0,1,2,\ldots,N-1\}$. Het is duidelijk dat $\{0,1,2,\ldots,N-1\} \subset T'_{a,b}$. Daar de som van twee elementen van $T'_{a,b}$ trivialerwijs opnieuw in $T'_{a,b}$ zit, is dus $s_1 + s_2 + n \in T'_{a,b}$. Neem nu omgekeerd een $t \in T'_{a,b}$. Kies vervolgens een $n \in \{0,1,2,\ldots,N-1\}$ zodat $\mathrm{red}_p(t-n) \in U_p + U_p$ voor alle $p \in \Delta_{a,b}$ waarvoor $p \leq 11$; dit als volgt met Lemma 9.10.

Lemma 9.10

Er bestaat een $n \in \{0,1,2,\ldots,N-1\}$ zodat $red_p(t-n) \in U_p + U_p$ voor alle $p \in \Delta_{a,b}$ waarvoor $p \leq 11$.

Bewijs. We bewijzen een sterker resultaat, namelijk dat er een $n \in \{0,1,2,\ldots,N-1\}$ bestaat zodat $\mathrm{red}_p(t-n) = 0$ voor alle $p \in \Delta_{a,b}$ waarvoor $p \leq 11$; a fortiori volgt het gevraagde dan uit Lemma 9.12. Noem daartoe $p_1,\ldots,p_k$ de onderling verschillende priemgetallen $p \in \Delta_{a,b}$ waarvoor $p \leq 11$; k is dus ten hoogste 5, en in dat geval hebben we bovendien dat $\{p_1,p_2,p_3,p_4,p_5\} = \{2,3,5,7,11\}$. Merk op dat $t \in \mathbb{Z}_p$ voor alle p waarvoor $p \in \Delta_{a,b}$, daar $t \in T'_{a,b}$. Beschouw vervolgens het stelsel

$$\begin{cases} x \equiv \mathrm{red}_{p_1}(t) & \mod p_1 \\ x \equiv \mathrm{red}_{p_2}(t) & \mod p_2 \\ \quad \vdots & \\ x \equiv \mathrm{red}_{p_k}(t) & \mod p_k \end{cases}.$$

Wegens de Chinese reststelling bestaat er een oplossing $n \in \mathbb{Z}$, dewelke uniek is modulo $p_1 p_2 \cdots p_k$. Maar $p_1 p_2 \cdots p_k \leq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 = N$, dus dat geheel getal n kan inderdaad in de verzameling $\{0, 1, 2, \ldots, N-1\}$ genomen worden. (Merk trouwens op dat dit ook meteen de reden is *waarom* N precies als het getal 2310 gedefinieerd werd!) Per constructie hebben we dat $\text{red}_{p_i}(t-n) = 0$ in $\mathbb{F}_{p_i}$ geldt, voor alle $i \in \{1, 2, \ldots, k\}$. Of, equivalent hiermee, $\text{red}_p(t-n) = 0$ geldt in $\mathbb{F}_p$, voor alle $p \leq 11$ waarvoor $p \in \Delta_{a,b}$. Dit beëindigt het bewijs van Lemma 9.10. ■

Voor elke $p \in \Delta_{a,b}$ waarvoor $p > 11$ geeft Lemma 9.5 dat $\text{red}_p(t-n) \in \mathbb{F}_p = U_p + U_p$. We hebben nu dus $\text{red}_p(t-n) \in U_p + U_p$ voor alle $p \in \Delta_{a,b}$. Kies een $s \in \mathbb{Z}$ zodat $\text{red}_p(s) \in U_p$ en $\text{red}_p(t-n-s) \in U_p$ voor alle $p \in \Delta_{a,b}$; dit kan met behulp van Lemma 9.11, als volgt.

Lemma 9.11

Met de notaties en voorwaarden zoals hierboven, geldt dat er een $s \in \mathbb{Z}$ bestaat zodat $red_p(s) \in U_p$ en $red_p(t-n-s) \in U_p$, voor alle $p \in \Delta_{a,b}$.

Bewijs. De verzameling $\Delta_{a,b}$ is eindig, zoals opgemerkt aan het einde van de opmerking na Definitie 7.25. Stel nu $\Delta_{a,b} = \{p_1, p_2, \ldots, p_k\}$, met $p_1, \ldots, p_k$ allemaal onderling verschillend. We weten reeds dat $\text{red}_p(t-n) \in U_p + U_p$ voor alle $p \in \Delta_{a,b}$. Schrijf, voor elke $i \in \{1, 2, \ldots, k\}$, $\text{red}_{p_i}(t-n) = \overline{u_{p_i}} + \overline{v_{p_i}}$, voor $\overline{u_{p_i}}, \overline{v_{p_i}} \in U_{p_i}$ en met $u_{p_i}, v_{p_i} \in \mathbb{Z}$; hiermee bedoelen we met $\overline{u_{p_i}}$ en $\overline{v_{p_i}}$ uiteraard de respectievelijke equivalentieklassen van u_{p_i} en v_{p_i}, modulo p_i. Beschouw het stelsel

$$\begin{cases} x \equiv u_{p_1} & \mod p_1 \\ x \equiv u_{p_2} & \mod p_2 \\ \quad \vdots & \\ x \equiv u_{p_k} & \mod p_k \end{cases}.$$

Wegens de Chinese reststelling bestaat er een oplossing, zeg $s \in \mathbb{Z}$, van dit stelsel. Neem $i \in \{1, 2, \ldots, k\}$. Dan is $\text{red}_{p_i}(s) = \bar{s} = \overline{u_{p_i}} \in U_{p_i}$. Ook is

$$\text{red}_{p_i}(t-n-s) = \text{red}_{p_i}(t-n) - \text{red}_{p_i}(s) = \overline{u_{p_i}} + \overline{v_{p_i}} - \overline{u_{p_i}} = \overline{v_{p_i}} \in U_{p_i}.$$

Bijgevolg hebben we inderdaad dat $\text{red}_p(s) \in U_p$ en $\text{red}_p(t-n-s) \in U_p$, voor alle $p \in \Delta_{a,b}$. Dit beëindigt het bewijs van Lemma 9.11. ■

Uit Lemma 9.3 volgt dan dat $s, t-n-s \in \text{red}_p^{-1}(U_p) \subset S_{a,b}(\mathbb{Q}_p)$ voor alle $p \in \Delta_{a,b}$. Maar dan impliceert Lemma 9.4 dat $s, t-n-s \in S_{a,b}$. Bijgevolg is

$$t = s + (t-n-s) + n \in S_{a,b} + S_{a,b} + \{0, 1, 2, \ldots, N-1\} = T_{a,b}.$$

Dit beëindigt het bewijs van Lemma 9.9. ■

Volgend lemma hebben we eerder al in een bewijs gebruikt.

Lemma 9.12

Er geldt dat $0 \in U_p + U_p$ voor alle $p \in \{2, 3, 5, 7, 11\}$.

Bewijs. Men kan door berekening makkelijk aantonen dat

$$U_2 = \{\bar{1}\}, \quad U_3 = \{\bar{0}\}, \quad U_5 = \{\bar{1}, \bar{4}\}, \quad U_7 = \{\bar{0}, \bar{3}, \bar{4}\}, \quad U_{11} = \{\bar{0}, \bar{1}, \bar{5}, \bar{6}, \overline{10}\}.$$

Daaruit halen we de uitdrukkingen

$$U_2 + U_2 = \{\bar{0}\}, \quad U_3 + U_3 = \{\bar{0}\}, \quad U_5 + U_5 = \{\bar{0}, \bar{2}, \bar{3}\},$$

$$U_7 + U_7 = \{\bar{0}, \bar{1}, \bar{3}, \bar{4}, \bar{6}\}, \quad U_{11} + U_{11} = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{9}, \overline{10}\}.$$

De conclusie volgt. Dit beëindigt het bewijs van Lemma 9.12. ■

Volgende stelling geeft bijna onmiddellijk de gezochte definitie.

Propositie 9.13

Er geldt dat $\bigcap_{a,b\in\mathbb{Q}_{>0}} T_{a,b} = \mathbb{Z}$.

Bewijs. We tonen eerst aan dat, voor elke $p \in \mathbb{P}$, er $a, b \in \mathbb{Q}_{>0}$ bestaan zodat $p \in \Delta_{a,b}$; dat wil zeggen, p ramifieert in $H_{a,b}$, of nog, $(a,b)_p = -1$.
Voor $p = 2$ kiezen we $a = b = 7$; dan is, wegens Stelling 7.2.3 in [7], inderdaad $(a,b)_2 = (7,7)_2 = -1$. Voor $p > 2$ kiezen we $a = p$ en $b \in \mathbb{Z}_{>0}$ met $\mathrm{red}_p(b) \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$; dat wil zeggen, b is een geheel getal strikt groter dan 0 dat niet deelbaar is door p, en zodanig dat b, beschouwd in $\mathbb{F}_p^\times$, geen kwadraat is. Het is evident dat zulk een getal bestaat. We passen nu opnieuw Stelling 7.2.3 in [7] toe. Merk op dat $a = 1 \cdot p^1$ en $b = b \cdot p^0$ met $1, b \in \mathbb{Z}_p^\times$. Dan is

$$(a,b)_p = (-1)^{1\cdot 0\cdot (p-1)/2} \left(\frac{1}{p}\right)^0 \left(\frac{b}{p}\right)^1 = \left(\frac{b}{p}\right) = -1,$$

per keuze van b. Merk op dat we hierbij het Legendresymbool over p gebruikten. Bijgevolg bestaan er voor elke $p \in \mathbb{P}$ inderdaad $a, b \in \mathbb{Q}_{>0}$ waarvoor $p \in \Delta_{a,b}$.
Wegens Lemma 9.9 hebben we $T_{a,b} = \bigcap_{p\in\Delta_{a,b}} \mathbb{Z}_{(p)}$, en dus ook

$$\bigcap_{a,b\in\mathbb{Q}_{>0}} T_{a,b} = \bigcap_{a,b\in\mathbb{Q}_{>0}} \bigcap_{p\in\Delta_{a,b}} \mathbb{Z}_{(p)}.$$

Echter, wegens hetgeen we zojuist aangetoond hebben, geldt dat het rechterlid van deze vergelijking gelijk is aan $\bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)}$. Wegens de opmerking na Definitie 9.8 geldt dat deze verzameling precies de verzameling van alle rationale getallen is waarvoor geldt dat de noemer niet deelbaar is door p, en dat voor alle $p \in \mathbb{P}$. Dus is het duidelijk dat $\bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)} = \mathbb{Z}$. Bijgevolg geldt inderdaad de gelijkheid

$$\bigcap_{a,b\in\mathbb{Q}_{>0}} T_{a,b} = \mathbb{Z}.$$

Dit beëindigt het bewijs van Propositie 9.13. ■

9.3 Hoofdresultaat

Tenslotte hebben we het hoofdresultaat van dit hoofdstuk, namelijk Poonens definitie van $\mathbb{Z}$ in $\mathbb{Q}$.

Propositie 9.14

De verzameling $\mathbb{Z}$ is precies gelijk aan de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule

$$\begin{gathered}(\forall a,b)(\exists a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4,x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n)\\ (a+a_1^2+a_2^2+a_3^2+a_4^2)\cdot(b+b_1^2+b_2^2+b_3^2+b_4^2)\\ \cdot[(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2\\ +n^2(n-1)^2\cdots(n-2309)^2+(2x_1+2y_1+n-t)^2]=0\end{gathered}$$

waar is, geïnterpreteerd in $\mathbb{Q}$.

Bewijs. Merk eerst op dat de verzameling van alle $a \in \mathbb{Q}$ waarvoor $a_1,a_2,a_3,a_4 \in \mathbb{Q}$ bestaan zodat $a+a_1^2+a_2^2+a_3^2+a_4^2=0$ precies deze zijn die voldoen aan $a \leq 0$; inderdaad, dit volgt uit Lemma 4.5, dat een rechtstreeks gevolg is van Propositie 4.4. Bijgevolg betekent bovenstaande formule precies hetzelfde als de formule

$$\begin{gathered}(\forall a,b \in \mathbb{Q}_{>0})(\exists x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n)\\ (x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2\\ +n^2(n-1)^2\cdots(n-2309)^2+(2x_1+2y_1+n-t)^2=0,\end{gathered}$$

waarbij de existentiële kwantoren over $\mathbb{Q}$ geïnterpreteerd dienen te worden. Merk op dat de existentiële formule

$$\begin{gathered}(\exists x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n)\\ (x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2\\ +n^2(n-1)^2\cdots(n-2309)^2+(2x_1+2y_1+n-t)^2=0\end{gathered}$$

in woorden uitgedrukt precies zegt dat $n \in \{0,1,\ldots,2309\}=\{0,1,\ldots,N-1\}$, en er elementen van $H_{a,b}$ bestaan met gereduceerde norm gelijk aan 1, zodanig dat t gelijk is aan $2x_1+2y_1+n$ (met x_1 en y_1 de respectievelijke eerste coördinaten van die elementen in $H_{a,b}$). Of nog, die formule is logisch equivalent met

$$t \in S_{a,b}+S_{a,b}+\{0,1,\ldots,N-1\}.$$

Maar deze laatste verzameling is per definitie gelijk aan $T_{a,b}$. Bijgevolg is de te bewijzen formule equivalent met de formule

$$(\forall a,b \in \mathbb{Q}_{>0})\ \ t \in T_{a,b}.$$

Propositie 9.13 zegt dat $\bigcap_{a,b\in\mathbb{Q}_{>0}} T_{a,b}=\mathbb{Z}$; dat wil zeggen,

$$(\forall a,b \in \mathbb{Q}_{>0})\ \ t \in T_{a,b} \ \Leftrightarrow\ t \in \mathbb{Z}.$$

Dit beëindigt het bewijs van Propositie 9.14. ■

We hebben dus dat $\mathbb{Z}$ definieerbaar is in $\mathbb{Q}$, met definiërende veelterm van $\mathbb{Z}$ gelijk aan

$$f \in \mathbb{Z}[a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4,x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n,t],$$

de veelterm van graad $4624 = 2+2+2\cdot 2310$ gedefinieerd door

$$\begin{gathered}
f(a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4,x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n,t) := \\
(a+a_1^2+a_2^2+a_3^2+a_4^2)\cdot(b+b_1^2+b_2^2+b_3^2+b_4^2) \\
\cdot[(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2 \\
+n^2(n-1)^2\cdots(n-2309)^2+(2x_1+2y_1+n-t)^2] = 0 \\
\in \mathbb{Z}[a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4,x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n,t].
\end{gathered}$$

Informeel kunnen we zeggen dat $\mathbb{Z}$ definieerbaar in $\mathbb{Q}$ is *door een $\forall\exists$-formule*. Meer precies, we hebben 2 universele kwantoren gevolgd door 9 existentiële kwantoren. In Poonens artikel staat dat, gegeven de hele constructie, het aantal universele kwantoren op het eerste zicht niet meteen gereduceerd kan worden. Het is echter wel zo dat het aantal existentiële kwantoren in aantal relatief makkelijk gereduceerd kan worden tot 7; we tonen dit aan in de volgende sectie.

9.4 Eliminatie van kwantoren

In de constructie van Poonen is volgend lemma essentieel ten einde het aantal kwantoren te reduceren in de definitie van $\mathbb{Z}$ in $\mathbb{Q}$ gegeven in Propositie 9.14.

Lemma 9.15

De formule

$$\bigcap_{a,b\in\mathbb{Q}} T_{a^2+b^2+1,a^2+a+1+b^2} = \mathbb{Z}$$

geldt.

Bewijs. Neem $a,b \in \mathbb{Q}$. Het is duidelijk dat $a^2+b^2+1 \geq 1 > 0$. Ook hebben we

$$a^2+a+1+b^2 \geq \frac{3}{4}+b^2 \geq \frac{3}{4} > 0,$$

daar

$$a^2+a+\frac{1}{4} = \left(a+\frac{1}{2}\right)^2 \geq 0 \;\Rightarrow\; a^2+a+1 \geq \frac{3}{4}.$$

Dus in het bijzonder is $a^2+b^2+1 > 0$ en $a^2+a+1+b^2 \neq 0$ en natuurlijk ook $a^2+b^2+1, a^2+a+1+b^2 \in \mathbb{Q}$. Met behulp van Lemma 9.9 volgt hieruit voor alle $a,b \in \mathbb{Q}$ de formule

$$T_{a^2+b^2+1,a^2+a+1+b^2} = \bigcap_{p\in\Delta_{a^2+b^2+1,a^2+a+1+b^2}} \mathbb{Z}_{(p)}.$$

Bijgevolg moeten we aantonen dat

$$\bigcap_{a,b\in\mathbb{Q}} \bigcap_{p\in\Delta_{a^2+b^2+1,a^2+a+1+b^2}} \mathbb{Z}_{(p)} = \mathbb{Z}.$$

Omdat we weten dat $\bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)} = \mathbb{Z}$ volstaat het aan te tonen dat voor elke $p \in \mathbb{P}$ getallen $a,b \in \mathbb{Q}$ bestaan zodat $p \in \Delta_{a^2+b^2+1,a^2+a+1+b^2}$. Maar dat is precies Lemma 9.16 hieronder. Dit beëindigt het bewijs van Lemma 9.15. ■

Lemma 9.16

Met de notaties en voorwaarden zoals hierboven, geldt dat voor elke $p \in \mathbb{P}$ er getallen $a,b \in \mathbb{Q}$ bestaan zodat $p \in \Delta_{a^2+b^2+1,a^2+a+1+b^2}$.

Bewijs. Herinner dat voor iedere $p \in \mathbb{P}$ geldt dat

$$p \in \Delta_{a^2+b^2+1,a^2+a+1+b^2} \Leftrightarrow (a^2+b^2+1, a^2+a+1+b^2)_p = -1.$$

Stel eerst $p = 2$. Neem dan $a = -1$ en $b = 1$. Merk op dat $3 = 3 \cdot 2^0$ en $2 = 1 \cdot 2^1$ met $3,1 \in \mathbb{Z}_2^\times$. Dan is, wegens Stelling 7.2.3 in [7], inderdaad

$$(a^2+b^2+1, a^2+a+1+b^2)_2 = (3,2)_2 = (-1)^{\frac{3-1}{2}\frac{1-1}{2}+0\frac{1^2-1}{8}+1\frac{3^2-1}{8}} = (-1)^1 = -1.$$

Stel nu $p = 3$. Neem opnieuw $a = -1$ en $b = 1$. Merk op dat $3 = 1 \cdot 3^1$ en $2 = 2 \cdot 3^0$ met $1,2 \in \mathbb{Z}_2^\times$. Uit het tweede deel van Stelling 7.2.2 in [7] volgt

$$(a^2+b^2+1, a^2+a+1+b^2)_3 = (3,2)_3 = \left(\frac{2}{3}\right) = -1.$$

Stel dat $p = 5$. Neem $a = 2$ en $b = 0$. Het tweede deel van Stelling 7.2.2 in [7] geeft opnieuw

$$(a^2+b^2+1, a^2+a+1+b^2)_5 = (5,7)_5 = \left(\frac{7}{5}\right) = -1.$$

Stel dat $p = 7$. Neem opnieuw $a = 2$ en $b = 0$. Opnieuw wegens hetzelfde resultaat krijgen we inderdaad

$$(a^2+b^2+1, a^2+a+1+b^2)_7 = (5,7)_7 = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{\frac{5-1}{2}\frac{7-1}{2}} = (-1)\cdot 1 = -1.$$

In deze laatste stap gebruikten we de kwadratische reciprociteitswet.
Stel nu $p \in \mathbb{P}$ met $p \geq 11$. Kies $c \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$. Zij nu $X \in \mathbb{A}^2_{\mathbb{F}_p}$ de affiene curve bepaald door de vergelijkingen

$$c^2x^4 + y^2 + 1 = 0, \quad x \neq 0.$$

Analoog als in het bewijs van Lemma 9.5 volgt dat X een curve van genus 1 is, met 4 gaten. Uit de ongelijkheid van Hasse omtrent elliptische curves en het feit dat $t := \sqrt{p} > 3$ volgt dan de vergelijking

$$\#X(\mathbb{F}_p) \geq (p+1-2\sqrt{p}) - 4 = t^2 - 2t - 3 = (t-1)^2 - 2^2 = (t-3)(t+1) > 0.$$

Dus $X(\mathbb{F}_p) \neq \emptyset$; kies $(x_0, y_0) \in X(\mathbb{F}_p)$. Kies $a, b \in \mathbb{Z}$ zodat $\bar{a} = cx_0^2$ en $\bar{b} = y_0$ in $\mathbb{F}_p$. Omdat $(x_0, y_0) \in X(\mathbb{F}_p)$ is dan

$$\mathrm{red}_p(a^2+b^2+1) = \mathrm{red}_p(a^2) + \mathrm{red}_p(b^2) + \mathrm{red}_p(1) = c^2x_0^4 + y_0^2 + 1 = 0.$$

We mogen zonder verlies van algemeenheid ervan uitgaan dat $a^2+b^2+1 \not\equiv 0 \mod p^2$; inderdaad, veronderstel immers dat $a^2+b^2+1 \equiv 0 \mod p^2$. Vervang a dan door $a' := a+p \in \mathbb{Z}$. Dan blijft de conditie

$$\mathrm{red}_p(a') = \mathrm{red}_p(a+p) = \mathrm{red}_p(a) = \bar{a} = cx_0^2$$

in $\mathbb{F}_p$ gelden. Maar $a'^2+b^2+1 \not\equiv 0 \mod p^2$, want anders zou

$$2ap \equiv (a^2+2ap)+b^2+1 \equiv (a+p)^2+b^2+1 = a'^2+b^2+1 \equiv 0 \mod p^2,$$

hetgeen $p \mid a$ impliceert. Maar dan is $\bar{0} = \bar{a} = cx_0^2$ in $\mathbb{F}_p$, zodat $c = 0$ of $x_0 = 0$. Dit is een contradictie daar $c \neq 0$ en $x_0 \neq 0$, per constructie. Dus we mogen inderdaad de veronderstelling $a^2+b^2+1 \not\equiv 0 \mod p^2$ maken. Merk nu op dat

$$a^2+a+1+b^2 \equiv a \mod p$$

omdat $a^2+b^2+1 \equiv 0 \mod p$, per constructie. Ook hebben we dat a geen kwadraat is modulo p; indien dat wel zou zijn, dan zou uit de uitdrukking $\bar{a} = cx_0^2$ de contradictie dat c een kwadraat is in $\mathbb{F}_p^\times$ volgen. Schrijf $a^2+b^2+1 = pt$ en $a^2+a+1+b^2 = a+pt'$ met $t, t' \in \mathbb{Z}$ en bovendien $p \nmid t$, zodat $t \in \mathbb{Z}_p^\times$. Ook geldt $p \nmid a+pt'$ daar $p \nmid a$, zodat $a+pt' \in \mathbb{Z}_p^\times$. Nu volgt uit het tweede deel van Stelling 7.2.2 in [7] dat

$$(a^2+b^2+1, a^2+a+1+b^2)_p = (pt, a+pt')_p = \left(\frac{a+pt'}{p}\right) = \left(\frac{a}{p}\right) = -1.$$

Dit laatste volgt omdat a geen kwadraat is modulo p. Dit beëindigt het bewijs van Lemma 9.16. ■

Tot slot hebben we Poonens elegantere definitie van $\mathbb{Z}$ in $\mathbb{Q}$ na eliminatie van kwantoren, als volgt.

Propositie 9.17

De verzameling $\mathbb{Z}$ is precies gelijk aan de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule

$$\begin{aligned}
&(\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)\\
&[x_1^2-(a^2+b^2+1)x_2^2-(a^2+a+1+b^2)x_3^2+\\
&\qquad (a^2+b^2+1)(a^2+a+1+b^2)x_4^2-1]^2\\
&+\prod_{n=0}^{2309}[(t-n-2x_1)^2-4(a^2+b^2+1)y_2^2-4(a^2+a+1+b^2)y_3^2\\
&\qquad +4(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-4]^2=0
\end{aligned}$$

waar is, geïnterpreteerd in $\mathbb{Q}$.

Bewijs. Lemma 9.15 zegt dat voor een $t \in \mathbb{Q}$ geldt dat

$$(\forall a,b \in \mathbb{Q})\ t \in T_{a^2+b^2+1,a^2+a+1+b^2} \ \Leftrightarrow\ t \in \mathbb{Z}.$$

De uitspraak $t \in T_{a^2+b^2+1,a^2+a+1+b^2}$ betekent precies dat

$$t \in S_{a^2+b^2+1,a^2+a+1+b^2} + S_{a^2+b^2+1,a^2+a+1+b^2} + \{0,1,2,\ldots,N-1\},$$

hetgeen equivalent is met

$$\begin{gathered}(\exists x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n)\\ (2x_1+2y_1+n-t)^2\\ +[x_1^2-(a^2+b^2+1)x_2^2-(a^2+a+1+b^2)x_3^2+(a^2+b^2+1)(a^2+a+1+b^2)x_4^2-1]^2\\ +[y_1^2-(a^2+b^2+1)y_2^2-(a^2+a+1+b^2)y_3^2+(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-1]^2\\ +n^2(n-1)^2(n-2)^2\cdots(n-2309)^2=0.\end{gathered}$$

Merk op dat de $\exists n$ makkelijk weggewerkt kan worden daar n maar waardes aanneemt in de eindige verzameling $\{0,1,2,\ldots,2309\}$. Nu elimineren we de $\exists y_1$ door de vergelijking $2x_1+2y_1+n-t=0$ naar y_1 op te lossen; dit geeft dan $2y_1 = t-n-2x_1$. Samen met de vergelijking

$$y_1^2-(a^2+b^2+1)y_2^2-(a^2+a+1+b^2)y_3^2+(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-1]^2$$

geeft die vergelijking precies

$$\begin{aligned}0 &= y_1^2-(a^2+b^2+1)y_2^2-(a^2+a+1+b^2)y_3^2\\ &\quad +(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-1]^2\\ &= (2y_1)^2-4(a^2+b^2+1)y_2^2-4(a^2+a+1+b^2)y_3^2+\\ &\quad 4(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-4]^2\\ &= (t-n-x_1)^2-4(a^2+b^2+1)y_2^2-4(a^2+a+1+b^2)y_3^2+\\ &\quad 4(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-4.\end{aligned}$$

De hierboven bekomen formule is dus inderdaad equivalent met

$$\begin{gathered}(\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)\\ [x_1^2-(a^2+b^2+1)x_2^2-(a^2+a+1+b^2)x_3^2+\\ (a^2+b^2+1)(a^2+a+1+b^2)x_4^2-1]^2\\ +\prod_{n=0}^{2309}[(t-n-2x_1)^2-4(a^2+b^2+1)y_2^2-4(a^2+a+1+b^2)y_3^2\\ +4(a^2+b^2+1)(a^2+a+1+b^2)y_4^2-4]^2=0.\end{gathered}$$

Dit beëindigt het bewijs van Propositie 9.17. ■

Merk op dat de definiërende veelterm van $\mathbb{Z}$, beschouwd als element van

$$\mathbb{Z}[a,b,x_1,x_2,x_3,x_4,y_2,y_3,y_4,t],$$

dit keer van graad $27720 = 12\cdot 2310$ is.

9.5 Alternatieve eliminatie van kwantoren

We hebben volgende definitie van $\mathbb{Z}$ in $\mathbb{Q}$.

Propositie 9.18

De verzameling $\mathbb{Z}$ is precies gelijk aan de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule

$$(\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)$$
$$(a+x_1^2+x_2^2+x_3^2+x_4^2)\cdot(b+x_1^2+x_2^2+x_3^2+x_4^2)\cdot[(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2$$
$$+\prod_{n=0}^{2309}\left((t-n-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2-4\right)^2]=0$$

waar is, geïnterpreteerd in $\mathbb{Q}$.

Bewijs. We bewijzen dat bovenstaande eerste-orde formule equivalent is met de formule

$$(\forall a,b\in\mathbb{Q}_{>0})(\exists x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n)$$
$$(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2$$
$$+n^2(n-1)^2(n-2)^2\cdots(n-2309)^2+(t-2x_1-2y_1-n)^2=0.$$

Hierbij lopen de existentiële kwantoren over $\mathbb{Q}$. Wegens de uitleg aan het begin van het bewijs van Propositie 9.14 volgt dat de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule van hierboven waar is, precies gelijk is aan $\mathbb{Z}$. De equivalentie van de eerste-orde formule uit de formulering van de stelling en degene hierboven is dus voldoende aan te tonen om het bewijs van deze stelling te leveren.
We tonen eerst de implicatie van boven naar onder aan; dat wil zeggen we veronderstellen dat de formule in de formulering van de stelling waar is en bewijzen daaruit de waarheid van de formule hierboven. Neem dus $a,b \in \mathbb{Q}_{>0}$. Per hypothese bestaan er dan $x_1,x_2,x_3,x_4,y_2,y_3,y_4 \in \mathbb{Q}$ zodat

$$a+x_1^2+x_2^2+x_3^2+x_4^2=0 \quad \text{of} \quad b+x_1^2+x_2^2+x_3^2+x_4^2=0$$

of

$$(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+\prod_{n=0}^{2309}[(t-n-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2-4]^2=0.$$

Omdat $a,b>0$ zijn de eerste twee mogelijkheden onmogelijk. Bijgevolg geldt de laatste mogelijkheid, id est

$$x_1^2-ax_2^2-bx_3^2+abx_4^2=1 \quad \text{en} \quad (t-n-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2=4$$

voor een zekere $n\in\{0,1,2,\ldots,2309\}$. Definieer $y_1 := \frac{t-n-2x_1}{2} \in \mathbb{Q}$. Dan is bijgevolg $2y_1 = t-n-2x_1$. Dan volgt na invullen in de laatste vergelijking

$$y_1^2-ay_2^2-by_3^2+aby_4^2=1.$$

Dit bewijst de eerste implicatie.
Omgekeerd, neem $a,b \in \mathbb{Q}$. Indien $a > 0$ en $b > 0$ dan volgt per hypothese meteen dat er $x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4,n \in \mathbb{Q}$ bestaan zodat

$$x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1, \quad y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = 1, \quad n \in \{0,1,2\ldots,2309\},$$

en

$$t = 2x_1 + 2y_1 + n.$$

Daarom geldt

$$(t - n - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4 = 0.$$

Voor deze keuzes van $x_1,x_2,x_3,x_4,y_2,y_3,y_4$ is bijgevolg in het bijzonder de formule in de formulering van de stelling waar. In dat geval zijn we dus klaar met het bewijs. Veronderstel nu dat $a \leq 0$ of $b \leq 0$; stel, vanwege symmetrie, zonder verlies van algemeenheid dat $a \leq 0$. Uit Lemma 4.5 volgt dan dat er $x_1,x_2,x_3,x_4 \in \mathbb{Q}$ bestaan zodat

$$a + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$

Voor de andere variabelen, y_2,y_3,y_4, kunnen we dan eender wat als waarden nemen, bijvoorbeeld $y_2 = y_3 = y_4 = 0 \in \mathbb{Q}$, en in het bijzonder geldt voor deze keuze van $x_1,x_2,x_3,x_4,y_2,y_3,y_4 \in \mathbb{Q}$ de gelijkheid

$$\begin{aligned}(a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot [(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 \\ + \prod_{n=0}^{2309} [(t - n - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4]^2] = 0\end{aligned}$$

Dat bewijst de tweede implicatie. Dit beëindigt het bewijs van Propositie 9.18. ■

De definiërende veelterm van $\mathbb{Z}$, beschouwd als element van

$$\mathbb{Z}[a,b,x_1,x_2,x_3,x_4,y_2,y_3,y_4,t],$$

is nu van graad $18484 = 2 + 2 + 8 \cdot 2310$.

Opmerking. De logische complexiteit van deze definitie, bekomen door toepassing van de alternatieve eliminatie van kwantoren, is dezelfde als de definitie van Poonen, id est Propositie 9.17: beide definities van $\mathbb{Z}$ in $\mathbb{Q}$ bestaan uit twee universele kwantoren, namelijk a,b, gevolgd door zeven existentiële kwantoren, namelijk $x_1,x_2,x_3,x_4,y_2,y_3,y_4$. In dat opzicht kan men dus zeggen dat de twee verschillende definities dus even wenselijk zijn. Echter, Poonens aanpak vereist Lemma 9.15. Zoals we gezien hebben is dit lemma helemaal niet triviaal; daarenboven bekomt Poonen dan uiteindelijk een definiërende veelterm die nog steeds graad 27720 heeft. Onze alternatieve aanpak, namelijk Propositie 9.18, vereist helemaal geen diep resultaat maar is daarentegen ad hoc; daarbij komt dan nog eens dat de zo bekomen definiërende veelterm slechts graad 18484 heeft, hetgeen kleiner is dan 27720. Na correspondentie met Poonen blijkt dat iemand anders hem eerder al op deze overbodigheid in zijn redenering gewezen had. Hij heeft het, in een latere versie van zijn artikel, dan ook aangepast. Ik heb de initiële versie van Poonens artikel uitgewerkt; deze verschilt van de nieuwste versie enkel op dit punt.

KÖNIGSMANNS SIMPLIFICATIE

In dit hoofdstuk volgen we Königsmanns benadering voor het definiëren van $\mathbb{Z}$ in $\mathbb{Q}$. Dit levert ons een wat elegantere en minder bombastische definitie op: Poonens aanpak zonder kwantoreliminatie leverde een definiërende veelterm van maar liefst graad 4624 op, met 2 universele kwantoren gevolgd door 9 existentiële kwantoren. En na eliminatie van kwantoren bracht dat een definiërende veelterm van graad 18484 op, met 2 universele kwantoren gevolgd door 7 existentiële kwantoren. Zoals reeds uitgelegd aan het eind van het vorige hoofdstuk geeft Königsmanns aanpak ons een definitie bestaande uit precies 2 universele kwantoren gevolgd door 7 existentiële kwantoren; bovendien heeft de definiërende veelterm slechts graad 12. De werkwijze van Königsmann is wel geheel gebaseerd op deze van Poonen. Ook zullen we de hulpstellingen uit Hoofdstuk 9 opnieuw gebruiken.

10.1 Constructie

In dit hoofdstuk gebruiken we precies dezelfde definities en begrippen zoals gegeven in sectie 9.1 van Hoofdstuk 9, met uitzondering van de volgende twee punten.

Ten eerste, in Definitie 7.25 definieerden we de verzameling $\Delta_{a,b}$ als de verzameling van alle $p \in \mathbb{P} \cup \{\infty\}$ waarvoor p niet splijt in $H_{a,b}$, voor alle $a,b \in \mathbb{Q}^\times$. In vorig hoofdstuk, bij Poonen, gebruikte we echter een iets andere terminologie. Maar nu volgen we terug Definitie 7.25. Om verwarring te voorkomen herhalen we hier nogmaals Königsmanns definitie van $\Delta_{a,b}$.

Definitie 10.1

We stellen

$$\Delta_{a,b} := \{p \in \mathbb{P} \cup \{\infty\} \mid p \text{ splijt niet in } H_{a,b}\}$$

voor alle $a,b \in \mathbb{Q}^\times$.

Königsmann beschouwt in zijn artikel dus, in tegenstelling tot Poonen, *wel* ramificatie op ∞. Onder deze definitie hebben we dat $\Delta_{a,b}$, voor alle $a,b \in \mathbb{Q}^\times$, eindig is en bovendien heeft deze verzameling steeds een even aantal elementen; dit volgt onmiddellijk wegens de kwadratische reciprociteitswet voor het Hilbertsymbool; zie de uitleg na Definitie 7.25.

Ten tweede wijken we van Poonens terminologie af op het volgende punt.

Definitie 10.2

Zij $a,b \in \mathbb{Q}^\times$. Laat dan $T_{a,b} := S_{a,b} + S_{a,b}$.

Merk op dat Poonen $T_{a,b}$ definieerde als $S_{a,b} + S_{a,b} + \{0,1,\ldots,2309\}$.

Ter uitbreiding van Definitie 9.8 stellen we $\mathbb{Z}_\infty := \{x \in \mathbb{Q} \mid -4 \leq x \leq 4\}$, en ook

$$\mathbb{Z}_{(\infty)} := \mathbb{Z}_\infty \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid -4 \leq x \leq 4\}.$$

Volgend lemma is eigenlijk louter rekenwerk.

Lemma 10.3

We hebben

$$S_{a,b}(\mathbb{R}) = \begin{cases} \mathbb{R} & \text{indien } a > 0 \text{ of } b > 0 \\ [-2,2] & \text{indien } a,b < 0 \end{cases}$$

voor alle $a,b \in \mathbb{Q}^\times$.

Bewijs. Per definitie is

$$S_{a,b}(\mathbb{R}) = \{2x_1 \in \mathbb{R} \mid \exists x_2,x_3,x_4 \in \mathbb{R} : x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\} \subset \mathbb{R}.$$

Kies $2x_1 \in \mathbb{R}$ willekeurig. Veronderstel eerst dat $a > 0$ en $b > 0$. Indien $|x_1| > 1$ dan is $\frac{x_1^2-1}{a} > 0$, zodat de vierkantswortel hiervan in $\mathbb{R}$ bestaat, daar $a > 0$. Dan is

$$x_1^2 - a\left(\sqrt{\frac{x_1^2-1}{a}}\right)^2 - b0^2 + ab0^2 = 1,$$

zodat inderdaad $2x_1 \in S_{a,b}(\mathbb{R})$. Indien $|x_1| \leq 1$ dan is $\frac{1-x_1^2}{ab} \geq 0$, zodat de vierkantswortel hiervan in $\mathbb{R}$ bestaat, daar $a,b > 0$. Dan is

$$x_1^2 - a0^2 - b0^2 + ab\left(\sqrt{\frac{1-x_1^2}{ab}}\right)^2 = 1,$$

zodat inderdaad $2x_1 \in S_{a,b}(\mathbb{R})$.
Veronderstel vervolgens dat $a > 0$ en $b < 0$. Indien $|x_1| > 1$ dan geldt precies dezelfde redenering als hierboven. Indien $|x_1| \leq 1$ dan is $\frac{1-x_1^2}{-b} \geq 0$, zodat de vierkantswortel hiervan in $\mathbb{R}$ bestaat, daar $b < 0$. Dan is

$$x_1^2 - a0^2 - b\left(\sqrt{\frac{1-x_1^2}{-b}}\right)^2 + ab0^2 = 1,$$

zodat inderdaad $2x_1 \in S_{a,b}(\mathbb{R})$.
Het geval $a < 0$ en $b > 0$ volgt wegens symmetrie.

Kies tenslotte $2x_1$, met $x_1 \in [-1,1] \subset \mathbb{R}$, willekeurig. Veronderstel dat $a<0$ en $b<0$. Dan is $\frac{1-x_1^2}{ab} > 0$, zodat de vierkantswortel hiervan in $\mathbb{R}$ bestaat, daar $ab>0$ omdat $a<0$ en $b<0$. Dus hebben we

$$x_1^2 - a0^2 - b0^2 + ab\left(\sqrt{\frac{1-x_1^2}{ab}}\right)^2 = 1.$$

De conclusie volgt wederom.
Dan moeten we enkel nog aantonen dat $S_{a,b}(\mathbb{R}) \subset [-2,2]$ indien $a<0$ en $b<0$. Kies $2x_1$, met $x_1 \in \mathbb{R}$, willekeurig, waarvoor geldt dat $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1$ voor zekere $x_2, x_3, x_4 \in \mathbb{R}$. Omdat $-a, -b, ab > 0$ en kwadraten in $\mathbb{R}$ positief zijn, volgt meteen

$$x_1^2 \leq x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1.$$

Bijgevolg moet inderdaad $x_1 \in [-1,1]$, of nog, $2x_1 \in [-2,2]$. Dit beëindigt het bewijs van Lemma 10.3. ■

Volgend lemma hebben we eigenlijk al aangetoond, zie Lemma 9.4, maar formuleren we nu aan de hand van Königsmanns gebruikte definities. Het is essentieel het Hasse-Minkowski principe.

Lemma 10.4

Zij $a,b \in \mathbb{Q}^\times$. Dan is $S_{a,b} = \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p)$.

Bewijs. Dit is een rechtstreeks gevolg van het Hasse-Minkowski principe. Dit beëindigt het bewijs van Lemma 10.4. ■

Merk het subtiele verschil op tussen de formulering van Lemma 9.4 ten opzichte van de formulering van Lemma 10.4: deze laatste wordt geformuleerd zonder tekenvoorwaarde op $a,b \in \mathbb{Q}^\times$. Dit geldt natuurlijk daar $\infty \in \Delta_{a,b}$ bij Königsmann toegelaten is maar bij Poonen niet.

Nu volgt Königsmanns resultaat dat uiteindelijk leidt tot de gewenste definitie van $\mathbb{Z}$ in $\mathbb{Q}$. We tonen het gestelde aan met behulp van de lemma's uit Hoofdstuk 9 en de lemma's eerder in dit hoofdstuk gegeven.

Lemma 10.5

Zij $a,b \in \mathbb{Q}^\times$. Dan is

$$T_{a,b} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}.$$

In deze notatie is het onderverstaan dat $T_{a,b} = \mathbb{Q}$ indien $\Delta_{a,b} = \emptyset$.

Bewijs. Veronderstel eerst dat $\Delta_{a,b} = \emptyset$. Dan hebben we wegens Lemma 10.4 meteen dat $S_{a,b} = \mathbb{Q}$, zodat inderdaad

$$T_{a,b} = S_{a,b} + S_{a,b} = \mathbb{Q} + \mathbb{Q} = \mathbb{Q}.$$

Veronderstel nu dat $\Delta_{a,b} \neq \emptyset$. Stel ter afkorting $T'_{a,b} := \bigcap_{p\in\Delta_{a,b}} \mathbb{Z}_{(p)}$; dan tonen we de gelijkheid $T_{a,b} = T'_{a,b}$ aan. Lemma 10.4 zegt dat

$$S_{a,b} = \mathbb{Q} \cap \bigcap_{p\in\Delta_{a,b}} S_{a,b}(\mathbb{Q}_p).$$

Ook volgt uit Lemma 9.3 dat voor elke $p \in \Delta_{a,b} \setminus \{\infty\}$ geldt dat $S_{a,b}(\mathbb{Q}_p) \subset \mathbb{Z}_p$. Bovendien is, wegens Lemma 10.3 hierboven,

$$S_{a,b}(\mathbb{R}) = \begin{cases} \mathbb{R} & \text{indien } a > 0 \text{ of } b > 0 \\ [-2,2] & \text{indien } a,b < 0 \end{cases}.$$

We bewijzen nu de inclusie $T_{a,b} \subset T'_{a,b}$. Stel eerst dat $\infty \in \Delta_{a,b}$. Merk op dat dit $(a,b)_\infty = -1$ impliceert, en dit is equivalent met $a,b < 0$. Bijgevolg is

$$\begin{aligned} S_{a,b} &= \mathbb{Q} \cap \bigcap_{p\in\Delta_{a,b}} S_{a,b}(\mathbb{Q}_p) \\ &= \mathbb{Q} \cap \bigcap_{p\in\Delta_{a,b}\setminus\{\infty\}} S_{a,b}(\mathbb{Q}_p) \cap S_{a,b}(\mathbb{R}) \\ &= \mathbb{Q} \cap \bigcap_{p\in\Delta_{a,b}\setminus\{\infty\}} S_{a,b}(\mathbb{Q}_p) \cap [-2,2] \\ &\subset \bigcap_{p\in\Delta_{a,b}\setminus\{\infty\}} \mathbb{Z}_{(p)} \cap [-2,2]. \end{aligned}$$

Neem $s_1 + s_2 \in T_{a,b} = S_{a,b} + S_{a,b}$, met $s_1, s_2 \in S_{a,b}$. Het is evident dat dan

$$s_1 + s_2 \in \bigcap_{p\in\Delta_{a,b}\setminus\{\infty\}} \mathbb{Z}_{(p)} \cap \{x \in \mathbb{Q} \mid -4 \leq x \leq 4\} = \bigcap_{p\in\Delta_{a,b}} \mathbb{Z}_{(p)} = T'_{a,b}.$$

Indien $\infty \notin \Delta_{a,b}$ dan is de te bewijzen inclusie duidelijk. We besluiten dat $T_{a,b} \subset T'_{a,b}$. We tonen vervolgens de inclusie $T'_{a,b} \subset T_{a,b}$ aan. Definieer nu voor elke $p \in \mathbb{P} \cup \{\infty\}$ een verzameling $V_p \subset \mathbb{Z}_p$ door

$$V_p := \begin{cases} \phi_2^{-1}(U_2) \cup (4 + 8\mathbb{Z}_2) & \text{voor } p = 2 \\ \phi_p^{-1}(U_p) \cup [(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)] & \text{voor } 3 \leq p \leq 11 \\ \phi_p^{-1}(U_p) & \text{voor } 11 < p \in \mathbb{P} \\ [-2,2] \cap \mathbb{Q} & \text{voor } p = \infty \end{cases}.$$

Uit Lemma 10.8 volgt voor alle $p \in \mathbb{P} \cup \{\infty\}$ dat $V_p \subset S_{a,b}(\mathbb{Q}_p)$. Bovendien is $V_p \subset \mathbb{Z}_p$ een open verzameling indien $p \neq \infty$. En uit Lemma 10.10 volgt voor alle $p \in \mathbb{P} \cup \{\infty\}$ dat $\mathbb{Z}_p = V_p + V_p$. Zij nu $t \in T'_{a,b} = \bigcap_{p\in\Delta_{a,b}} \mathbb{Z}_{(p)}$ en $p \in \Delta_{a,b}$. Dan is $t \in \mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q} \subset \mathbb{Z}_p$. Omwille van bovenstaande zijn er dus $s_p, r_p \in V_p$ zodanig dat $t = s_p + r_p$. Dus $t - s_p = r_p \in V_p$. Bijgevolg hebben we voor elke $p \in \Delta_{a,b}$ een s_p zodat $s_p \in V_p$ en $t - s_p \in V_p$.
Indien $t = \pm 4$, dan is $t = \pm 2 \pm 2 \in S_{a,b} + S_{a,b} = T_{a,b}$; inderdaad, per definitie van $S_{a,b}$ is het duidelijk dat $-2, 2 \in S_{a,b}$. In dat geval zijn we dus klaar. En indien $t = 0$ dan is

$t = 0 = 2 + (-2) \in S_{a,b} + S_{a,b} = T_{a,b}$, zodat dezelfde conclusie geldt.
Veronderstel daarom dat $t \notin \{-4, 0, 4\}$. Indien $\infty \in \Delta_{a,b}$ dan is in het bijzonder $t \in \mathbb{Z}_{(\infty)} \setminus \{0, \pm 4\}$. Voor het geval $p = \infty$ verscherpen we nu het zojuist bekomen resultaat, namelijk het feit dat er een $s_p \in V_p$ bestaat zodat $s_p \in V_p$ en $t - s_p \in V_p$, voor elke $p \in \Delta_{a,b}$; in feite herdefiniëren we s_∞. Merk op dat

$$\mathbb{Z}_{(\infty)} \setminus \{0, \pm 4\} = \{x \in \mathbb{Q}^\times \mid -4 < x < 4\} = (\,]-2,2[\, + \,]-2,2[\,) \cap \mathbb{Q}.$$

Dus $t = s_\infty + r_\infty$ voor zekere $s_\infty, r_\infty \in]-2,2[\cap \mathbb{Q}$. Bijgevolg is $s_\infty, t - s_\infty \in]-2,2[\cap \mathbb{Q}$. (De reden waarom we deze aanpassing, namelijk een herdefiniëring van s_∞ zodat $s_\infty, t - s_\infty \in]-2,2[$, doen, wordt pas later duidelijk. We verwijzen naar de opmerking na deze stelling voor een duidelijke uitleg.) We hebben nu dus een eindig aantal s_p gegeven, voor $p \in \Delta_{a,b}$. Hierbij is ∞ al dan niet een element van $\Delta_{a,b}$; in elk geval is $s_p \in V_p$ voor alle $\Delta_{a,b} \setminus \{\infty\}$, en, meer nog, $s_\infty \in]-2,2[\cap \mathbb{Q}$ indien $\infty \in \Delta_{a,b}$. We gebruiken nu Propositie 8.21: we benaderen de eindige verzameling van s_p, $p \in \Delta_{a,b}$, door een uniek getal $s \in \mathbb{Q}$, zodanig dat

$$s - s_p \in \begin{cases} 8\mathbb{Z}_2 & \text{indien } p = 2 \\ p^2\mathbb{Z}_p & \text{indien } 3 \leq p \leq 11 \\ p\mathbb{Z}_p & \text{indien } 11 < p \in \mathbb{P} \\ ]-\varepsilon, \varepsilon[& \text{indien } p = \infty \end{cases}.$$

Hierbij is $\varepsilon := \min\{|2 \pm s_\infty|, |2 \pm (t - s_\infty)|\}$. Hoe precies Propositie 8.21 in deze situatie toegepast wordt, wordt geïllustreerd in Lemma 10.6 hieronder.

Lemma 10.6

Uit Propositie 8.21 volgt dat er een $s \in \mathbb{Q}$ bestaat zodat

$$s - s_p \in \begin{cases} 8\mathbb{Z}_2 & \textit{indien } p = 2 \\ p^2\mathbb{Z}_p & \textit{indien } 3 \leq p \leq 11 \\ p\mathbb{Z}_p & \textit{indien } 11 < p \in \mathbb{P} \\ ]-\varepsilon, \varepsilon[& \textit{indien } p = \infty \end{cases}$$

voor alle $p \in \Delta_{a,b}$.

Bewijs. Definieer voor elke $p \in \Delta_{a,b}$ een getal $M_p \in \mathbb{Q}$ door

$$M_p := \begin{cases} \frac{1}{4} & \text{indien } p = 2 \\ \frac{1}{p} & \text{indien } 3 \leq p \leq 11 \\ 1 & \text{indien } 11 < p \in \mathbb{P} \\ \varepsilon & \text{indien } p = \infty \end{cases}.$$

Definieer dan $\varepsilon' := \min\{M_p \mid p \in \Delta_{a,b}\}$. Merk op dat $\varepsilon' > 0$ daar $\varepsilon > 0$; dit laatste geldt slechts door onze speciale definitie van s_∞ zodat $s_\infty, t - s_\infty \in]-2,2[$, zie ook de opmerking na Lemma 10.5. Pas dan Propositie 8.21 toe op alle priemgetallen p

waarvoor $p \in \Delta_{a,b}$, met $s_p \in V_p \subset \mathbb{Z}_p \subset \mathbb{Q}_p$ voor alle $p \in \Delta_{a,b}$, en op het reëel getal $\varepsilon' > 0$. Daaruit halen we een $s \in \mathbb{Q}$ zodat $|s - s_p| < \varepsilon'$ voor alle $p \in \Delta_{a,b}$. Door te gebruiken dat voor een p-adisch getal $a \in \mathbb{Q}_p$ de equivalentie

$$|a|_p < \frac{1}{p^{i-1}} \Leftrightarrow |a|_p \leq \frac{1}{p^i}$$

geldt, geeft dit ons exact het gevraagde. Dit beëindigt het bewijs van het Lemma10.6. ■

En we hebben ook volgend lemma.

Lemma 10.7

Er geldt dat $s, t - s \in V_p$ voor alle $p \in \Delta_{a,b}$.

Bewijs. Veronderstel eerst dat $p = 2 \in \Delta_{a,b}$. We weten dat $s_2 \in V_2$ en $t - s_2 \in V_2$. Per constructie is $s - s_2 \in 8\mathbb{Z}_2$, dus $s - s_2 = 8t'$ voor een zekere $t' \in \mathbb{Z}_2$. Maar $V_2 = \phi_2^{-1}(U_2) \cup (4 + 8\mathbb{Z}_2)$, dus $s_2 \in \phi_2^{-1}(U_2)$ of $s_2 \in 4 + 8\mathbb{Z}_2$.
Stel dat $s_2 \in \phi_2^{-1}(U_2)$. Dan is ook $s \in \phi_2^{-1}(U_2) \subset V_2$, daar

$$\phi_2(s) = \phi_2(s_2 + 8t') = \phi_2(s_2) + \phi_2(8t') = \phi_2(s_2) \in U_2.$$

Stel dat $s_2 \in 4 + 8\mathbb{Z}_2$; schrijf $s_2 = 4 + 8t''$ voor een zekere $t'' \in \mathbb{Z}_2$. Dan is ook $s \in 4 + 8\mathbb{Z}_2 \subset V_2$, daar

$$s = s_2 + 8t' = (4 + 8t'') + 8t' = 4 + 8(t' + t'') \in 4 + 8\mathbb{Z}_2.$$

We weten ook dat $t - s_2 \in V_2 = \phi_2^{-1}(U_2) \cup (4 + 8\mathbb{Z}_2)$, en een volledig analoog gevalsonderscheid als zojuist levert dat $t - s \in V_2$. Daarmee is het geval $p = 2$ afgehandeld.
Veronderstel nu dat $3 \leq p \leq 11$, met $p \in \Delta_{a,b}$. We weten dat $s_p \in V_p$ en $t - s_p \in V_p$. Per constructie is $s - s_p \in p^2\mathbb{Z}_p$, dus $s - s_p = p^2 t'$ voor een zekere $t' \in \mathbb{Z}_p$. Maar

$$V_p = \phi_p^{-1}(U_p) \cup [(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)],$$

dus $s_p \in \phi_p^{-1}(U_p)$ of $s_p \in (\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)$.
Stel dat $s_p \in \phi_p^{-1}(U_p)$. Dan is ook $s \in \phi_p^{-1}(U_p) \subset V_p$, daar

$$\phi_p(s) = \phi_p(s_p + p^2 t') = \phi_p(s_p) + \phi_p(p^2 t') = \phi_p(s_p) \in U_p.$$

Stel dat $s_p \in (\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)$; schrijf $s_p = \pm 2 + pt''$ voor een zekere $t'' \in \mathbb{Z}_p$ waarvoor $p \nmid t''$. Dan is ook $s \in (\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p) \subset V_p$, daar

$$s = s_p + p^2 t' = (\pm 2 + pt'') + p^2 t' = \pm 2 + pt'' + p^2 t' \in (\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p).$$

In de laatste stap gebruikten we dat $p \nmid t''$.
We weten ook dat

$$t - s_p \in V_p = \phi_p^{-1}(U_p) \cup [(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)],$$

en een volledig analoog gevalsonderscheid als zojuist levert dat $t-s \in V_p$. Daarmee is het geval $3 \leq p \leq 11$ afgehandeld.
Veronderstel nu dat $11 < p \in \mathbb{P}$, met $p \in \Delta_{a,b}$. We weten dat $s_p \in V_p$ en $t-s_p \in V_p$. Per constructie is $s-s_p \in p\mathbb{Z}_p$, dus $s-s_p = pt'$ voor een zekere $t' \in \mathbb{Z}_p$. Maar $V_p = \phi_p^{-1}(U_p)$, zodat $s_p \in \phi_p^{-1}(U_p)$.
Dan is ook $s \in \phi_p^{-1}(U_p) \subset V_p$, daar

$$\phi_p(s) = \phi_p(s_p + pt') = \phi_p(s_p) + \phi_p(pt') = \phi_p(s_p) \in U_p.$$

We weten ook dat $t-s_p \in V_p = \phi_p^{-1}(U_p)$. Dan is ook $t-s \in \phi_p^{-1}(U_p) = V_p$, daar

$$\phi_p(t-s) = \phi_p(t-s_p-pt') = \phi_p(t-s_p) - \phi_p(pt') = \phi_p(t-s_p) \in U_p.$$

Daarmee is het geval $p > 11$ afgehandeld.
Veronderstel tot slot dat $p = \infty \in \Delta_{a,b}$. Door onze speciale constructie weten we dat

$$s_\infty, t-s_\infty \in]-2,2[\cap \mathbb{Q} \subset]-2,2[.$$

We moeten aantonen dat $s,t-s \in V_\infty = [-2,2] \cap \mathbb{Q}$, id est, $s,t-s \in [-2,2]$. Per constructie hebben we $s-s_\infty \in]-\varepsilon,\varepsilon[$, waarbij $\varepsilon = \min\{|2 \pm s_\infty|, |2 \pm (t-s_\infty)|\}$, of nog, $|s-s_\infty| < \varepsilon$. Hieruit volgt dat

$$s-s_\infty, s_\infty - s \leq |s-s_\infty| < \varepsilon \leq |2 \pm s_\infty|, |2 \pm (t-s_\infty)|.$$

Omdat $2-s_\infty > 0$ is $|2-s_\infty| = 2-s_\infty$. Uit de vergelijking hierboven volgt dus dat $s-s_\infty < 2-s_\infty$, of nog, $s < 2$. Analoog, omdat $2+s_\infty > 0$ is $|2+s_\infty| = 2+s_\infty$. Dan geldt wegens de vergelijking hierboven dat $s_\infty - s < 2+s_\infty$, of nog, $s > -2$. Bijgevolg is $s \in]-2,2[\subset [-2,2]$. Op precies dezelfde wijze volgt ook dat $t-s \in]-2,2[\subset [-2,2]$. Daarmee is het geval $p = \infty$ afgehandeld. Dit beëindigt het bewijs van Lemma 10.7. ■

Nu volgt uit Lemma 10.7 dat voor alle $p \in \Delta_{a,b}$ geldt dat $s,t-s \in V_p$. Maar we wisten al dat $V_p \subset S_{a,b}(\mathbb{Q}_p)$; dus $s,t-s \in S_{a,b}(\mathbb{Q}_p)$ voor alle $p \in \Delta_{a,b}$. Bijgevolg is

$$s,t-s \in \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p) = S_{a,b}$$

wegens Lemma 10.4. We concluderen dat inderdaad

$$t = s + (t-s) \in S_{a,b} + S_{a,b} = T_{a,b}.$$

Dit beëindigt het bewijs van Lemma 10.5. ■

Opmerking. Men kan zich terecht de vraag stellen waarom het in het bewijs van vorig resultaat nodig was s_∞ te herdefiniëren; met andere woorden, waarom hebben we nodig dat $s_\infty, t-s_\infty \in]-2,2[$ en is het niet voldoende dat $s_\infty, t-s_\infty \in [-2,2]$? Het antwoord ligt in de definitie van ε. Immers

$$\varepsilon := \min\{|2 \pm s_\infty|, |2 \pm (t-s_\infty)|\},$$

en om Propositie 8.21 toe te mogen passen moeten we hebben dat $\varepsilon > 0$; indien $s_\infty \in \{-2,2\}$ of $t-s_\infty \in \{-2,2\}$, dan zou $\varepsilon = 0$.

Ook gebruikten we de volgende technische lemma's.

Lemma 10.8

> *Er geldt voor alle $p \in \mathbb{P} \cup \{\infty\}$ dat $V_p \subset S_{a,b}(\mathbb{Q}_p)$. Bovendien, indien $p \neq \infty$, dan is $V_p \subset \mathbb{Z}_p$ een open verzameling.*

Bewijs. We bewijzen ten eerste dat we $V_p \subset S_{a,b}(\mathbb{Q}_p)$ voor alle $p \in \mathbb{P} \cup \{\infty\}$ hebben. Voor $p = \infty$ is het gevraagde duidelijk wegens Lemma 10.3.
Zij nu $p > 11$. Indien $p \notin \Delta_{a,b}$ dan volgt uit Lemma 9.3 dat $S_{a,b}(\mathbb{Q}_p) = \mathbb{Q}_p$ en is het gevraagde aldus triviaal. Indien $p \in \Delta_{a,b}$ dan volgt opnieuw uit Lemma 9.3 dat $\phi_p^{-1}(U_p) \subset S_{a,b}(\mathbb{Q}_p)$, hetgeen het gevraagde aantoont.
Voor het geval $p \in \{3,5,7,11\}$ volstaat het voor alle $p \in \{3,5,7,11\}$ aan te tonen dat

$$(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p) \subset S_{a,b}(\mathbb{Q}_p).$$

Maar dit volgt uit Lemma 10.9.
Het geval $p = 2$ vereist een speciale behandeling; we verwijzen hiervoor naar de appendix van [16].
Tot slot tonen we aan dat $V_p \subset \mathbb{Z}_p$ een open verzameling is indien $p \neq \infty$. Zij dus $p \neq \infty$. Merk op dat $\phi_p : \mathbb{Z}_p \to \mathbb{F}_p$ continu is indien we $\mathbb{F}_p$ met de discrete topologie beschouwen; inderdaad, de topologie op $\mathbb{Z}_p$ is precies zodanig gedefinieerd dat alle projecties $\mathbb{Z}_p \to \mathbb{F}_{p^i}$, met $i \geq 1$, continu zijn. Bijgevolg is in het bijzonder $\phi_p^{-1}(U_p) \subset \mathbb{Z}_p$ open. Het gevraagde volgt dan eenvoudig: $4 + 8\mathbb{Z}_2 \subset \mathbb{Z}_2$ is een basisopen, en ook is

$$(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p) \subset \mathbb{Z}_p$$

open daar $\pm 2 + p\mathbb{Z}_p \subset \mathbb{Z}_p$ open is, als basisopen, en $\pm 2 + p^2\mathbb{Z}_p \subset \mathbb{Z}_p$ gesloten, aangezien het, als basisopen, zowel open als gesloten is in $\mathbb{Z}_p$. Dit beëindigt het bewijs van Lemma 10.8. ■

Lemma 10.9

> *Er geldt dat*
>
> $$(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p) \subset S_{a,b}(\mathbb{Q}_p)$$
>
> *voor alle $p \in \mathbb{P}$ met $p > 2$.*

Bewijs. Neem $s \in (\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)$. Indien $p \notin \Delta_{a,b}$ dan is $S_{a,b}(\mathbb{Q}_p) = \mathbb{Q}_p$ wegens Lemma 9.3 en is het te bewijzen triviaal. Veronderstel dus dat $p \in \Delta_{a,b}$. We weten dat $S_{a,b}(\mathbb{Q}_p)$ als en slechts als $x^2 - sx + 1$ de gereduceerde karakteristieke veelterm van een zeker element van $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is; dit is triviaal. Echter, $p \in \Delta_{a,b}$ en Lemma 9.2 impliceren dat deze laatste bewering equivalent is met de bewering dat $x^2 - sx + 1 \in \mathbb{Z}_p[x] \subset \mathbb{Q}_p[x]$ een macht van een monische irreducibele veelterm over $\mathbb{Q}_p$ is. Daarom is het voldoende te bewijzen dat $x^2 - sx + 1$ een macht van een monische irreducibele veelterm over $\mathbb{Q}_p$ is. Zij $D := s^2 - 4$ de discriminant van de vergelijking $x^2 - sx + 1$ over $\mathbb{Q}_p$. We tonen vervolgens aan dat $x^2 - sx + 1$ over $\mathbb{Q}_p$ irreducibel is. Dit is equivalent met het feit dat $x^2 - sx + 1$ geen nulpunten in $\mathbb{Q}_p$ heeft.

En dat is op zijn beurt weer equivalent met het feit dat de discriminant $D = s^2 - 4$ geen kwadraat is in $\mathbb{Q}_p$, en dat geldt als en slechts als D geen kwadraat is in $\mathbb{Z}_p$. Dit tonen we nu aan. Merk op dat

$$D = s^2 - 4 \equiv (\pm 2)^2 - 4 = 0 \mod p,$$

dus $p \mid D$ in $\mathbb{Z}_p$. Echter, uit het ongerijmde dat $D \equiv 0 \mod p^2$ Dit impliceert

$$(s-2)(s+2) = s^2 - 4 = D \equiv 0 \mod p^2.$$

Er zijn dan drie mogelijkheden, namelijk $p^2 \mid s-2$ of $p^2 \mid s+2$, of $p \mid s-2$ en $p \mid s+2$. Maar dit laatste kan niet; anders zou ook $p \mid (s+2) - (s-2) = 4$, en dat is een contradictie daar $p > 2$ priem is. Indien $p^2 \mid s-2$ dan is $s \equiv 2 \mod p^2$, hetgeen in tegenspraak is met de keuze van s.. Indien $p^2 \mid s+2$ dan is $s \equiv -2 \mod p^2$, en dit is opnieuw een tegenspraak. We concluderen dat $D \not\equiv 0 \mod p^2$, of nog, $p^2 \nmid D$ in $\mathbb{Z}_p$. Daar we al $p \mid D$ hadden, volgt dat de p-orde van D precies gelijk is aan 1. Maar dan kan D natuurlijk geen kwadraat zijn, want kwadraten in $\mathbb{Z}_p$ hebben om evidente redenen een even p-orde. Dit beëindigt het bewijs van Lemma 10.9. ■

Lemma 10.10

Zij V_p voor elke $p \in \mathbb{P} \cup \{\infty\}$ gedefinieerd zoals in het bewijs van Lemma 10.5. Dan geldt er voor alle $p \in \mathbb{P} \cup \{\infty\}$ dat $\mathbb{Z}_p = V_p + V_p$.

Bewijs. Voor $p = \infty$ is het gevraagde meteen duidelijk, per definitie van V_∞ en $\mathbb{Z}_\infty$. Zij nu $p > 11$. Uit Lemma 9.5 volgt dat $\mathbb{F}_p = U_p + U_p$. We tonen eerst aan dat

$$\phi_p^{-1}(U_p + U_p) = \phi_p^{-1}(U_p) + \phi_p^{-1}(U_p).$$

Per definitie is

$$\phi_p^{-1}(U_p + U_p) = \{x \in \mathbb{Z}_p \mid \phi_p(x) \in U_p + U_p\},$$

$$\phi_p^{-1}(U_p) + \phi_p^{-1}(U_p) = \{x_1 + x_2 \in \mathbb{Z}_p \mid x_1, x_2 \in \mathbb{Z}_p \text{ en } \phi_p(x_1) \in U_p, \phi_p(x_2) \in U_p\}.$$

De inclusie $\phi_p^{-1}(U_p) + \phi_p^{-1}(U_p) \subset \phi_p^{-1}(U_p + U_p)$ is triviaal. Neem nu omgekeerd een $x \in \mathbb{Z}_p$ zodanig dat $\phi_p(x) \in U_p + U_p$; zeg $\phi_p(x) = u_1 + u_2$ met $u_1, u_2 \in U_p$. Neem $x_1' \in \phi_p^{-1}(u_1)$ en $x_2' \in \phi_p^{-1}(u_2)$; merk op dat dit steeds mogelijk is daar deze verzamelingen niet-leeg zijn. Dan is

$$\phi_p(x - (x_1' + x_2')) = \phi_p(x) - \phi_p(x_1') - \phi_p(x_2') = u_1 + u_2 - u_1 - u_2 = 0,$$

of nog, $x - (x_1' + x_2') \in p\mathbb{Z}_p$; zeg $x = x_1' + x_2' + tp = x_1' + (x_2' + tp)$ voor een zekere $t \in \mathbb{Z}_p$. Definieer $x_1 := x_1' \in \mathbb{Z}_p$ en $x_2 := x_2' + tp \in \mathbb{Z}_p$. Dan is $x = x_1 + x_2$ met

$$\phi_p(x_1) = \phi_p(x_1') = u_1 \in U_p, \quad \phi_p(x_2) = \phi_p(x_2' + tp) = \phi_p(x_2') + \phi_p(tp) = u_2 \in U_p.$$

Dus de andere inclusie volgt. Bijgevolg is

$$\mathbb{Z}_p = \phi_p^{-1}(\mathbb{F}_p) = \phi_p^{-1}(U_p + U_p) = \phi_p^{-1}(U_p) + \phi_p^{-1}(U_p) = V_p + V_p.$$

Beschouw nu het geval $p = 2$. We moeten dan aantonen dat

$$\mathbb{Z}_2 = \phi_2^{-1}(U_2) \cup (4+8\mathbb{Z}_2) + \phi_2^{-1}(U_2) \cup (4+8\mathbb{Z}_2).$$

Uit het bewijs van Lemma 9.12 volgt dat $U_2 = \{\bar{1}\} \subset \mathbb{F}_2$. De inclusie van rechts naar links is duidelijk. Merk op dat $\phi_2^{-1}(\{\bar{1}\})$ precies de verzameling van 2-adische getallen is, met de eerste 2-adische digit gelijk aan 1, of nog, precies die elementen die niet deelbaar zijn door 2. Zij dus $x \in \mathbb{Z}_2$. Schrijf $x = a_0 + a_1 p + t p^2$ met $a_0, a_1 \in \{0,1\}$ en $t \in \mathbb{Z}_2$ uniek bepaald. We gaan nu de mogelijkheden voor a_0 en a_1 af. Ter afkorting stellen we $M := \phi_2^{-1}(U_2)$ en $L := 4+8\mathbb{Z}_2$.

- Stel $a_0 = 0$ en $a_1 = 0$. Dan is

$$x = tp^2 = 4t = 1 + (4t-1) \in M + M.$$

- Stel $a_0 = 0$ en $a_1 = 1$. Dan is

$$x = p + tp^2 = 2 + 4t = 1 + (1+4t) \in M + M.$$

- Stel $a_0 = 0$ en $a_1 = 2$. Dan is

$$x = 2p + tp^2 = 4 + 4t = 1 + (3+4t) \in M + M.$$

- Stel $a_0 = 1$ en $a_1 = 0$. Dan is

$$x = 1 + tp^2 = 1 + 4t = (4+8t) + (-3-4t) \in L + M.$$

- Stel $a_0 = 1$ en $a_1 = 1$. Dan is

$$x = 1 + p + tp^2 = 3 + 4t = (4+8t) + (-1-4t) \in L + M.$$

- Stel $a_0 = 1$ en $a_1 = 2$. Dan is

$$x = 1 + 2p + tp^2 = 5 + 4t = (4+8t) + (1-4t) \in L + M.$$

- Stel $a_0 = 2$ en $a_1 = 0$. Dan is

$$x = 2 + tp^2 = 2 + 4t = 1 + (1+4t) \in M + M.$$

- Stel $a_0 = 2$ en $a_1 = 1$. Dan is

$$x = 2 + p + tp^2 = 4 + 4t = 1 + (3+4t) \in M + M.$$

- Stel $a_0 = 2$ en $a_1 = 2$. Dan is

$$x = 2 + 2p + tp^2 = 6 + 4t = 1 + (5+4t) \in M + M.$$

Bijgevolg geldt de inclusie van links naar rechts inderdaad.
Beschouw nu het geval $p = 3$. We moeten dan aantonen dat

$$\mathbb{Z}_3 = \phi_3^{-1}(U_3) \cup [(\pm 2 + 3\mathbb{Z}_3) \setminus (\pm 2 + 3^2\mathbb{Z}_3)] + \phi_3^{-1}(U_3) \cup [(\pm 2 + 3\mathbb{Z}_3) \setminus (\pm 2 + 3^2\mathbb{Z}_3)].$$

Uit het bewijs van Lemma 9.12 volgt dat $U_3 = \{\bar{0}\} \subset \mathbb{F}_3$. De inclusie van rechts naar links is duidelijk. Merk op dat $\phi_3^{-1}(\{\bar{0}\})$ precies de verzameling van 3-adische getallen is, met de eerste 3-adische digit gelijk aan 0, of nog, precies die elementen die deelbaar zijn door 3. Zij dus $x \in \mathbb{Z}_3$. Schrijf $x = a_0 + a_1 p + t p^2$ met $a_0, a_1 \in \{0,1,2\}$ en $t \in \mathbb{Z}_p$ uniek bepaald. We gaan hieronder alle mogelijkheden voor a_0 en a_1 af; daarbij stellen we ter afkorting $M := \phi_3^{-1}(U_3)$ en

$$L := (\pm 2 + 3\mathbb{Z}_3) \setminus (\pm 2 + 3^2\mathbb{Z}_3).$$

- Stel $a_0 = 0$. Dan is
$$x = 0 + a_1 p + t p^2 = 0 + (a_1 p + t p^2) \in M + M.$$
- Stel $a_0 = 1$ en $a_1 = 0$. Dan is
$$x = 1 + t p^2 = (1 + t p^2) + 0 \in L + M.$$
- Stel $a_0 = 1$ en $a_1 = 1$. Dan is
$$x = 1 + p + t p^2 = (1 + t p^2) + p \in L + M.$$
- Stel $a_0 = 1$ en $a_1 = 2$. Dan is
$$x = 1 + 2p + t p^2 = (1 + t p^2) + 2p \in L + M.$$
- Stel $a_0 = 2$ en $a_1 = 0$. Dan is
$$x = 2 + t p^2 = 1 + (1 + t p^2) \in L + L.$$
- Stel $a_0 = 2$ en $a_1 = 1$. Dan is
$$x = 2 + p + t p^2 = 1 + (1 + p + t p^2) \in L + L.$$
- Stel $a_0 = 2$ en $a_1 = 2$. Dan is
$$x = 2 + 2p + t p^2 = (1 + p) + (1 + p + t p^2) \in L + L.$$

Bijgevolg geldt de inclusie van links naar rechts inderdaad.
De gevallen $p \in \{5,7,11\}$ volgen door een analoog gevalsonderscheid te maken. Dit beëindigt het bewijs van Lemma 10.10. ■

Volgende stelling geeft bijna onmiddellijk de gezochte definitie.

Propositie 10.11

Er geldt dat $\bigcap_{a,b \in \mathbb{Q}_{>0}} T_{a,b} = \mathbb{Z}$.

Bewijs. Uit het bewijs van Propositie 9.13 weten we dat er voor elke $p \in \mathbb{P}$ er $a,b \in \mathbb{Q}_{>0}$ bestaan zodat $p \in \Delta_{a,b}$. Uit Lemma 10.5 volgt dat

$$T_{a,b} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)},$$

en dus ook

$$\bigcap_{a,b \in \mathbb{Q}_{>0}} T_{a,b} = \bigcap_{a,b \in \mathbb{Q}_{>0}} \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)} = \bigcap_{p \in \mathbb{P}} \mathbb{Z}_{(p)} = \mathbb{Z}.$$

Dit beëindigt het bewijs van Propositie 10.11. ■

Dan nu Königsmanns equivalent van Propositie 9.17.

Propositie 10.12

> *De verzameling $\mathbb{Z}$ is precies gelijk aan de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule*
>
> $$(\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)$$
> $$(a+x_1^2+x_2^2+x_3^2+x_4^2)\cdot(b+x_1^2+x_2^2+x_3^2+x_4^2)$$
> $$\cdot[(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+((t-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2-4)^2]=0$$
>
> *waar is, geïnterpreteerd in $\mathbb{Q}$.*

Bewijs. We bewijzen eerst dat bovenstaande eerste-orde formule equivalent is met de formule

$$(\forall a,b \in \mathbb{Q}_{>0})(\exists x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4)$$
$$(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+(y_1^2-ay_2^2-by_3^2+aby_4^2-1)^2+(t-2x_1-2y_1)^2=0.$$

Hierbij lopen de existentiële kwantoren over $\mathbb{Q}$. Merk op dat het gevraagde hier dan meteen uit volgt, wegens Lemma 10.11 en de definitie van $T_{a,b}$ als $S_{a,b}+S_{a,b}$.
We tonen eerst de implicatie van boven naar onder aan; dat wil zeggen we veronderstellen dat de formule in de formulering van de stelling waar is en bewijzen daaruit de waarheid van de formule hierboven. Neem dus $a,b \in \mathbb{Q}_{>0}$. Per hypothese bestaan er dan $x_1,x_2,x_3,x_4,y_2y_3,y_4 \in \mathbb{Q}$ zodat

$$a+x_1^2+x_2^2+x_3^2+x_4^2=0 \quad \text{of} \quad b+x_1^2+x_2^2+x_3^2+x_4^2=0$$

of

$$(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2+((t-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2-4)^2]=0.$$

Omdat $a,b>0$ zijn de eerste twee mogelijkheden onmogelijk. Bijgevolg geldt de laatste mogelijkheid, id est

$$x_1^2-ax_2^2-bx_3^2+abx_4^2=1 \quad \text{en} \quad (t-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2=4.$$

Definieer $y_1 := \frac{t-2x_1}{2} \in \mathbb{Q}$, zodat $2y_1 = t - 2x_1$. Dan volgt na invullen de vergelijking

$$y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = 1.$$

Dit bewijst de eerste implicatie.
Omgekeerd, neem $a, b \in \mathbb{Q}$. Indien $a > 0$ en $b > 0$ dan volgt per hypothese meteen dat er $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Q}$ bestaan zodat

$$x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1, \quad y_1^2 - ay_2^2 - by_3^2 + aby_4^2 = 1 \quad \text{en} \quad t = 2x_1 - 2y_1.$$

Door de voorlaatste vergelijking met 4 te vermenigvuldigen en vervolgens de laatste vergelijking, geschreven als $2y_1 = 2x_1 - t$, hierin in te vullen, bekomen we

$$(t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4 = 0,$$

en dus hebben we inderdaad $x_1, x_2, x_3, x_4, y_2, y_3, y_4$ gevonden zodanig dat

$$(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + ((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4)^2 = 0.$$

Veronderstel nu dat $a \leq 0$ of $b \leq 0$; stel, omwille van symmetrie, zonder verlies van algemeenheid $a \leq 0$. Uit Lemma 4.5 volgt dan dat er $x_1, x_2, x_3, x_4 \in \mathbb{Q}$ bestaan zodat

$$a + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$

Voor de andere variabelen, y_2, y_3, y_4, kunnen we dan eender wat als waarden nemen, bijvoorbeeld $y_2 = y_3 = y_4 = 0 \in \mathbb{Q}$, en in het bijzonder geldt voor deze keuze van $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Q}$ de gelijkheid

$$(a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2)$$
$$\cdot [(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + ((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4)^2] = 0.$$

Dat bewijst de tweede implicatie. Dit beëindigt het bewijs van Propositie 10.12. ■

Het is duidelijk dat de definiërende veelterm hier van graad 12 is.

Opmerking. Verdergaand op de opmerking na Propositie 9.18 zien we dat de logische complexiteit van Königsmanns definitie van $\mathbb{Z}$ in $\mathbb{Q}$ van dezelfde orde is als deze van de vorige twee definities, die werden bekomen na eliminatie: namelijk twee universele kwantoren gevolgd door zeven existentiële kwantoren. Maar de definiërende veelterm in Königsmanns definitie is slechts van graad 12, terwijl de veeltermen van de twee definities uit vorig hoofdstuk van respectievelijk graad 27720 en 18484 waren. Van alle definities van $\mathbb{Z}$ in $\mathbb{Q}$ die we in deze thesis bestudeerd hebben is Königsmanns definitie dus de meest preferabele.

10.2 Verdere resultaten

Het resultaat van Königsmann dat wij in deze thesis bestudeerd hebben is feitelijk maar de eerste stap in een reeks van vijf stappen uit Königsmanns artikel. Na die uitvoerige studie wordt dan volgende stelling bekomen, die we enkel postuleren.

Propositie 10.13

> *Er bestaat een veelterm $f \in \mathbb{Z}[x_1, x_2, \ldots, x_{418}, t]$ zodat $\mathbb{Z}$ precies gelijk is aan de verzameling van alle $t \in \mathbb{Q}$ waarvoor geldt dat de eerste-orde formule*
>
> $$(\forall x_1, x_2, \ldots, x_{418})\, f(x_1, x_2, \ldots, x_{418}, t) \neq 0$$
>
> *waar is, geïnterpreteerd in $\mathbb{Q}$.*

Dus is $\mathbb{Z}$ definieerbaar in $\mathbb{Q}$ door een $\forall$-formule: $\mathbb{Z}$ is *universeel definieerbaar in* $\mathbb{Q}$.

Gewoonlijk wordt logische complexiteit gemeten in termen van het aantal veranderingen van kwantoren. Bijvoorbeeld: een formule van de vorm $\forall\exists$ is van lagere logische complexiteit dan een formule van de vorm $\forall\exists\forall$, daar er een kwantorverandering minder is. Daarom is de eerste formule preferabel over de tweede als definitie van een verzameling. In eerste instantie is het *aantal* kwantoren van eenzelfde type niet zo belangrijk. Zo is op vlak van logische complexiteit bijvoorbeeld een formule van de vorm $(\forall x, y, z)(\exists t)$ nog altijd te prefereren boven een formule van de vorm $(\forall x)(\exists y)(\forall z)$, ook al wordt er in het totaal een kwantor minder gebruikt.

Op het aantal universele kwantoren na is Königsmanns definitie van $\mathbb{Z}$ in $\mathbb{Q}$ van hierboven dus ook de meeste simpele; immers, er bestaat geen definitie van $\mathbb{Z}$ in $\mathbb{Q}$ waarbij geen kwantoren worden gebruikt. Maar zoals juist gezegd is het precieze aantal universele kwantoren in eerste instantie niet echt relevant.

Wat verderop in zijn artikel toont Königsmann aan dat $\mathbb{Z}$ definieerbaar is in $\mathbb{Q}$ door een $\forall\exists$-formule met precies één universele kwantor. Onafhankelijk werd hetzelfde resultaat ook gevonden door Shlapentokh; zij gebruikte echter een volledig andere methode, gebaseerd op elliptische krommen.

Königsmann bekomt tenslotte volgend resultaat: indien we veronderstellen dat de Bombieri-Lang conjectuur waar is, dan is er geen oneindige deelverzameling van $\mathbb{Q}$ existentieel definieerbaar in $\mathbb{Q}$. In het bijzonder impliceert dit dat $\mathbb{Z}$ niet existentieel definieerbaar is in $\mathbb{Q}$, of nog, $\mathbb{Z}$ is niet diophantisch in $\mathbb{Q}$. Hierbij merken we op dat het al langer geweten is dat als de Mazur conjectuur waar is, dit impliceert dat $\mathbb{Z}$ niet diophantisch is in $\mathbb{Q}$. Maar de aanname van de Mazur conjectuur is veel zwaarder dan de aanname van de Bombieri-Lang conjectuur; Königsmanns resultaat is met andere woorden wel degelijk een vooruitgang. In feite hebben we zelfs slechts een zwakker gevolg van de Bombieri-Lang conjectuur nodig. We formuleren dit exact in onderstaande, maar tonen dit niet aan.

Conjectuur 10.14

> *Zij $n \geq 2$. Indien $V \subset \mathbb{A}^n$ een hyperoppervlak over $\mathbb{Q}$ is zodat $V(\mathbb{Q})$ Zariski dicht is, dan is ook $V(\mathbb{Q}) \cap ((\mathbb{Q} \setminus \mathbb{Z}) \cap \mathbb{Q}^{n-1})$ Zariski dicht.*

Men kan met behulp van de stelling van Siegel, die handelt over de eindigheid van integrale punten op krommen over $\mathbb{Q}$, aantonen dat de conjectuur alvast waar is voor het geval $n = 2$.

Propositie 10.15

> *Conjectuur 10.14 impliceert dat $\mathbb{Z}$ niet diophantisch is over $\mathbb{Q}$.*

Een diophantische definitie van $\mathbb{Z}$ in $\mathbb{Q}$ zou, op evidente wijze, impliceren dat Hilberts Tiende Probleem over $\mathbb{Q}$ onoplosbaar zou zijn. Echter, indien we ons vertrouwen leggen in de conjectuur hierboven vermeld, dan is $\mathbb{Z}$ dus *niet* diophantisch over $\mathbb{Q}$. Er is dus verder onderzoek nodig naar Hilberts Tiende Probleem over $\mathbb{Q}$. Maar misschien kunnen de technieken gebruikt door Poonen en Königsmann hiertoe wel bijdragen.

Bibliografie

[1] L. Cabusora. *Diophantine Sets, Primes and the Resolution of Hilbert's 10th Problem*. 2004. Senior Thesis, http://www.math.harvard.edu/theses/senior/cabusora/thesis1.pdf.

[2] R. Courant, en H. Robbins. *Primes in Arithmetical Progressions*. What Is Mathematics? An Elementary Approach to Ideas and Methods. Oxford University Press, Oxford, England, second edition, 1996.

[3] J. Demeyer. *Diophantine Sets over Polynomial Rings and Hilbert's Tenth Problem for Function Fields*. PhD thesis, UGent, 2007. http://cage.ugent.be/~jdemeyer/papers/demeyer_phd.pdf.

[4] B. Demoen. *Automaten en Berekenbaarheid*. 2010. cursustekst, http://people.cs.kuleuven.be/~bart.demoen/AB/ab16dec2010.pdf.

[5] B. Demoen., en K. Dekimpe. *Fundamenten voor de Informatica*. 2009. cursustekst, http://people.cs.kuleuven.be/~bart.demoen/FVI/fundamenten.pdf.

[6] J. Denef. *Algebra II*. 2010. cursustekst.

[7] J. Denef. *Getaltheorie*. 2010. cursustekst.

[8] J. Denef. *Wiskundige logica*. 2010. cursustekst.

[9] H.-D. Ebbinghaus. *Numbers*. Springer-Verlag, New York, 1990.

[10] A. Gamzon. *The Hasse-Minkowski Theorem*. 2006. Honors Scholar Theses. Paper 17, http://digitalcommons.uconn.edu/srhonors_theses/17.

[11] P. Gardner. *Models of Computation*. 2010. cursustekst, http://www.doc.ic.ac.uk/~pg/Computation/.

[12] J. Hatley. *Hasse-Minkowski and the Local-to-Global principle*. 2009. Senior Thesis, http://www.math.umass.edu/~hatley/Capstone.pdf.

[13] T. Hungerford. *Algebra*. Springer-Verlag, New York, 1974.

[14] N. Jacobson. *Basic Algebra II*. W.H. Freeman and Co., New York, second edition, 1989.

[15] N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta-Functions*. Springer-Verlag, New York, second edition, 1984.

[16] J. Koenigsmann. *Defining $\mathbb{Z}$ in $\mathbb{Q}$*. 2010. http://arxiv.org/pdf/1011.3424v1.

[17] Y. I. Manin. *A Course in Mathematical Logic*. Springer-Verlag, New York, 1977. translated from the Russian by Neal Koblitz.

[18] Y. Matiyasevich. *Hilbert's Tenth Problem*. The MIT Press, 1993. with a foreword by Martin Davis.

[19] P. J. Morandi. *Central Simple Algebras*. 1998, http://sierra.nmsu.edu/morandi/notes/centralsimplealgebras.pdf.

[20] P. Odifreddi. *Classical Recursion Theory*, volume I. North-Holland, 1989.

[21] PlanetMath. *Proof of Lagrange's Four-Square Theorem*. 2011. http://planetmath.org/encyclopedia/ProofOfLagrangesFourSquareTheorem.html.

[22] B. Poonen. *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest*. 2003. http://math.mit.edu/~poonen/papers/aws2003.pdf.

[23] B. Poonen. *Characterizing integers among rational numbers with a universal-existential formula*. 2007. http://fr.arxiv.org/PS_cache/math/pdf/0703/0703907v1.pdf.

[24] W. Scharlau. *Quadratic and Hermitian Forms*. Springer-Verlag, New York, 1985.

[25] Z. Y. Sham. *Quaternion Algebras and Quadratic Forms*. 2008. thesis, http://uwspace.uwaterloo.ca/bitstream/10012/3656/1/second2.pdf.

[26] T. R. Shemanske. *Perspectives on the Albert-Brauer-Hasse-Noether Theorem for Quaternion Algebras*. 2007, http://www.math.dartmouth.edu/~trs/expository-papers/tex/ABHN.pdf.

[27] R. I. Soare. *Recursively Enumerable Sets and Degrees*. Perspectives in Mathematical Logic. Springer-Verlag, New York, second edition, 1987.

[28] W. Veys. *Lineaire algebra*. 2007. cursustekst.

[29] J. Voight. *The arithmetic of quaternion algebras*. 2010. http://www.cems.uvm.edu/~voight/crmquat/book/quat-modforms-041310.pdf.