E.T.G. Schlebusch

Het Hasse-principe

Bachelorscriptie, 20 juni 2012

Scriptiebegeleider: dr. R.M. van Luijk

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1. Inleiding

Het vinden van een niet-triviale oplossing in $\mathbb{Q}$ van een vergelijking of een stelsel vergelijkingen over $\mathbb{Q}$ is niet altijd even eenvoudig. Soms is het makkelijker om te kijken naar (niet-triviale) oplossingen in completeringen van $\mathbb{Q}$. Het is interessant om te kijken naar de verbanden tussen deze oplossingen en eventuele oplossingen in $\mathbb{Q}$. Heeft het hebben van oplossingen over completeringen van $\mathbb{Q}$ überhaupt iets te maken met het hebben van een oplossing over $\mathbb{Q}$? In de eerste plaats zou je kunnen denken dat een dergelijk verband niet bestaat. Stel je weet bijvoorbeeld dat een vergelijking een oplossing over $\mathbb{R}$ heeft. Zolang je niet weet welke oplossing dit is, kan je niets zeggen over het al dan niet bestaan van een oplossing over $\mathbb{Q}$. Toch blijkt dat we voor bepaalde (groepen) vergelijkingen een dergelijk verband kunnen vinden. Dit verband staat ook wel bekend als het Hasse-principe.
Vanzelfsprekend is het hierbij niet genoeg om alleen te kijken of de vergelijking een oplossing over $\mathbb{R}$ heeft. Maar $\mathbb{Q}$ heeft ook nog andere completeringen, de zogenaamde p-adische lichamen, $\mathbb{Q}_p$, waarbij p een priemgetal is. In deze scriptie zal ik eerst kort beschrijven hoe deze completeringen geconstrueerd worden. Met behulp van deze p-adische lichamen kunnen we dan het Hasse principe formuleren. Een vergelijking voldoet namelijk aan het Hasse-principe als geldt dat, als de vergelijking oplossingen heeft in $\mathbb{R}$ en in $\mathbb{Q}_p$ voor alle priemen p, dan heeft deze vergelijking ook een oplossing in $\mathbb{Q}$.
Dit is natuurlijk een mooi verband, maar helaas blijkt dat niet alle vergelijkingen aan het Hasse-principe voldoen. Zo zal ik in deze scriptie een voorbeeld van een stelsel vergelijkingen geven dat geen oplossing heeft in $\mathbb{Q}$, maar wel in $\mathbb{R}$ en in $\mathbb{Q}_p$ voor alle priemen p. Tot slot zal ik nog bewijzen dat een bepaald type vergelijkingen, namelijk de zogeheten kwadratische vormen, wel altijd voldoen aan het Hasse-principe.

2. Het lichaam van p-adische getallen

Zoals waarschijnlijk bekend, is $\mathbb{R}$ door middel van Cauchyrijtjes te construeren als completering van $\mathbb{Q}$. In deze Cauchyrijtjes wordt de afstand tussen twee elementen gegeven door de absolute waarde van het verschil. Maar we kunnen in plaats van de absolute waarde ook een andere norm als afstand op $\mathbb{Q}$ gebruiken, bijvoorbeeld de p-adische norm. In dit hoofdstuk zal kort worden verteld hoe het lichaam van p-adische getallen, $\mathbb{Q}_p$, wordt geconstrueerd met behulp van de p-adische norm. Voor een uitgebreidere bespreking van het lichaam van p-adische getallen wil ik verwijzen naar [2].

2.1. De p-adische norm.

We zullen de p-adische getallen construeren met behulp van de p-adische norm. Deze p-adische norm zullen we eerst, met behulp van enkele andere definities, definiëren.

Definitie 2.1 (valuatie van $x \in \mathbb{Z} \setminus \{0\}$ bij p)**.** Zij p een priemgetal. Dan is de valuatie van $x \in \mathbb{Z} \setminus \{0\}$ bij p, genoteerd als $v_p(x)$, gedefiniëerd als die n, waarvoor geldt dat $p^n \mid x$ en $p^{n+1} \nmid x$.

Definitie 2.2 (valuatie van $x \in \mathbb{Q} \setminus \{0\}$ bij p)**.** Zij p een priemgetal. Dan is de valuatie van $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ bij p, genoteerd als $v_p(x)$, gedefiniëerd als $v_p(a) - v_p(b)$.

Definitie 2.3 (p-adische norm)**.** De p-adische norm op $\mathbb{Q}$ is de volgende afbeelding:

$$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{als } x \neq 0 \\ 0, & \text{als } x = 0 \end{cases}$$

Opmerking 2.4. Deze p-adische norm is inderdaad een norm, hij voldoet namelijk aan de volgende drie eigenschappen:

$$\begin{aligned} \mid x \mid_p = 0 &\Leftrightarrow x = 0 \\ \mid x \cdot y \mid_p &= \mid x \mid_p \cdot \mid y \mid_p \\ \mid x + y \mid_p &\leq \mid x \mid_p + \mid y \mid_p \end{aligned}$$

De p-adische norm voldoet zelfs aan een sterkere ongelijkheid dan deze derde eigenschap, namelijk de volgende:

$$\mid x + y \mid_p \leq \max(\mid x \mid_p, \mid y \mid_p)$$

Dat de p-adische norm aan bovenstaande eigenschappen voldoet zal ik hier verder niet bewijzen, maar dit is vrij makkelijk na te gaan.

2.2. De p-adische getallen.

We zullen nu het lichaam van p-adische getallen construeren door middel van rijtjes die Cauchy zijn ten opzichte van de p-adische norm. Het is interessant om hierbij de constructie van $\mathbb{R}$ uit $\mathbb{Q}$ door middel van Cauchyrijtjes in het achterhoofd te houden, aangezien deze constructies, op de gebruikte norm na, vrijwel analoog zijn.

Definitie 2.5 (Cauchyrijtjes ten opzichte van de p-adische norm)**.** Een rij $(a_i)_i$ van rationale getallen heet een Cauchyrij ten opzichte van de p-adische norm als geldt: $\forall \epsilon \in \mathbb{Q}_{>0} : \exists N \in \mathbb{Z}_{>0} : \forall i, j > N : |a_i - a_j|_p < \epsilon$.

Definitie 2.6 (Het lichaam van p-adische getallen)**.** Het lichaam van p-adische getallen, $\mathbb{Q}_p$, is de kleinste lichaamsuitbreiding van $\mathbb{Q}$ waarin elk rijtje dat Cauchy is ten opzichte van de p-adische norm, convergeert.

Het blijkt dat ieder p-adisch getal in $\mathbb{Q}_p$ van de volgende vorm is, dit noemen we de p-adische expansie van het getal:
$\frac{a_{-m}}{p^m} + \frac{a_{-m+1}}{p^{m-1}} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + \cdots$

Hierbij geldt $a_i \in \{0, \ldots, p-1\}$.
De valuatie van deze p-adische expansie bij p is gelijk aan $-m$.

Stelling 2.7 (De ring van p-adische gehelen)**.** *De verzameling van elementen uit $\mathbb{Q}_p$ waarvan de p-adische expansie geen negatieve p-machten bevat, oftewel de elementen $x \in \mathbb{Q}_p$ waarvoor geldt dat $v_p(x) \geq 0$, is een ring. Deze ring noemen we $\mathbb{Z}_p$.*

Bewijs. Dit volgt uit het feit dat 0 en 1 bevat zijn in $\mathbb{Z}_p$ (de valuatie van 0 en 1 is bij iedere p namelijk gelijk aan 0) en uit het feit dat het optellen, aftrekken of vermenigvuldigen van twee elementen uit $\mathbb{Z}_p$, oftewel van twee elementen uit $\mathbb{Q}_p$ waarvan de p-adische expansie geen negatieve p-machten bevat, weer een element geeft waarvan de p-adische expansie geen negatieve p-machten bevat, oftewel een element in $\mathbb{Z}_p$. □

3. Het Hasse-principe

Definitie 3.1 (Hasse-principe)**.** Zij F een stelsel homogene vergelijkingen over $\mathbb{Q}$. We noemen een oplossing van F niet-triviaal als niet alle variabelen gelijk aan 0 zijn. Dan voldoet F aan het Hasse-principe als geldt:

$$\begin{gathered} F \text{ heeft niet-triviale oplossingen in } \mathbb{Q}_v \text{ voor alle } v \in V \\ \Leftrightarrow \\ F \text{ heeft een niet-triviale oplossing in } \mathbb{Q}. \end{gathered}$$

Opmerking 3.2. De implicatie

$$\begin{gathered} F \text{ heeft niet-triviale oplossingen in } \mathbb{Q}_v \text{ voor alle } v \in V \\ \Leftarrow \\ F \text{ heeft een niet-triviale oplossing in } \mathbb{Q}, \end{gathered}$$

geldt voor ieder stelsel vergelijkingen, aangezien $\mathbb{Q}_v$ voor alle $v \in V$ uitbreidingen zijn van $\mathbb{Q}$, en dus, als $\mathbb{Q}$ een oplossing bevat, dezelfde oplossing bevatten.

4. Een tegenvoorbeeld

We zullen nu een voorbeeld geven van een stelsel vergelijkingen dat niet aan het Hasse-principe voldoet. Hiervoor maken we gebruik van één stelling en twee lemma's, waarvan ik er hier één zal bewijzen.

Definitie 4.1 (Legendre-symbool)**.** Zij p een oneven priemgetal en $x \in \mathbb{Z}$. Het Legendre-symbool modulo p van x is

$$\{-1,0,1\} \ni \left(\frac{x}{p}\right) = \begin{cases} 0 & \text{als } x \equiv 0 \mod p, \\ 1 & \text{als } x \text{ een kwadraat is modulo } p, \\ -1 & \text{als } x \text{ geen kwadraat is modulo } p. \end{cases}$$

Propositie 4.2. *Deze definitie van het Legendre-symbool is equivalent met de volgende definitie:*

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$$

Bewijs. Als x deelbaar is door p, dan geldt $x \equiv 0 \mod p$, en dus ook $x^{\frac{p-1}{2}} \equiv 0 \mod p$.
Als x een kwadraat is modulo p, bijvoorbeeld van a, dan geldt $x^{\frac{p-1}{2}} \equiv a^{p-1} \mod p$. En iets tot de macht $p-1$ is altijd gelijk aan 1 modulo p.
Stel nu dat x geen kwadraat is modulo p.
Dan kunnen we kijken naar $z = x^{\frac{p-1}{2}}$. Er geldt nu $z^2 = x^{p-1} \equiv 1 \mod p$. Hieruit volgt dat $z \equiv \pm 1 \mod p$.
We weten nu dus dat x een nulpunt is van ofwel $f_1(t) = t^{\frac{p-1}{2}} + 1$, ofwel van $f_2(t) = t^{\frac{p-1}{2}} - 1$.
We weten echter dat alle kwadraten modulo p nulpunten zijn van f_2. Modulo p hebben we $\frac{p-1}{2}$ kwadraten, en aangezien f_2 een polynoom van graad $\frac{p-1}{2}$ is, zijn dit ook meteen alle nulpunten van f_2.
Dus als x geen kwadraat is modulo p, is x een nulpunt van f_1. En hieruit volgt dat dan geldt dat $x^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Stelling 4.3 (Kwadratische reciprociteitswet)**.** *Zij p en q oneven priemen, met $p \neq q$. Dan geldt*

$$\left(\tfrac{p}{q}\right)\left(\tfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{als } p \equiv q \equiv -1 \mod 4, \\ 1 & \text{anders.} \end{cases}$$

Bewijs. Voor een bewijs van de kwadratische reciprociteitswet verwijs ik naar pagina 83 en 84 van [4]. □

Lemma 4.4 (Lemma van Hensel)**.** *Zij $f(x) = c_0 + c_1 x + \cdots + c_l x^l$ een polynoom met $c_i \in \mathbb{Z}_p$. Zij $a_0 \in \mathbb{Z}_p$ zodanig dat*

$$v_p(f(a_0)) \geq 2v_p(f'(a_0)) + 1$$

Dan bestaat er een unieke $a \in \mathbb{Z}_p$ zodanig dat $f(a) = 0$ en $a \equiv a_0 \mod p^{v_p(f'(a_0))+1}$.

Bewijs. Voor een bewijs van het lemma van Hensel verwijs ik naar pagina 183 van [1]. □

Lemma 4.5. *Zij $n \in \mathbb{Z}$ en $x, y \in \mathbb{Q}$ zodanig dat $n = x^2 - 5y^2$. Dan geldt voor iedere priem $p \equiv \pm 2 \mod 5$ dat $v_p(n)$ even is.*

Bewijs. Schrijf eerst $x = \frac{a}{b}$ en $y = \frac{c}{d}$. Dan geldt $n = \left(\frac{a}{b}\right)^2 - 5\left(\frac{c}{d}\right)^2$ en dus $b^2d^2n = a^2d^2 - 5b^2c^2$.
Zij nu $\text{ggd}(ad, bc) = e$, zodanig dat $ad = ef$ en $bc = eg$. Dan geldt $\text{ggd}(f, g) = 1$.
Nu hebben we $b^2d^2n = e^2f^2 - 5e^2g^2$. Dus $m = \frac{b^2d^2}{e^2}n = f^2 - 5g^2$. Omdat f en g geheel zijn, is dus ook m geheel.
Zij nu p een deler van m, met $p \neq 5$ en $p \neq 2$.
Dan geldt $f^2 - 5g^2 \equiv 0 \mod p$. Dus $f^2 \equiv 5g^2 \mod p$.
Omdat f en g copriem zijn, en omdat $p \neq 5$, zijn niet allebei de kanten 0 modulo p, want dan zouden f en g allebei 0 modulo p moeten zijn, en dus niet copriem. Dus moet 5 een kwadraat zijn modulo p.
Dus $\left(\frac{5}{p}\right) = 1$. Uit de kwadratische reciprociteitswet (Stelling 4.3) volgt (omdat $5 \equiv 1 \mod 4$) dat dit geldt dan en slechts dan als $\left(\frac{p}{5}\right) = 1$. En dit is alleen het geval als p gelijk is aan ± 1 modulo 5.
Dus als $p \neq 2$ en $p \neq 5$ een deler is van m, dan is $p \equiv \pm 1 \mod 5$.
Stel we hebben nu een priemdeler $p \equiv \pm 2 \mod 5$ van n, met $p \neq 2$. Er geldt $v_p(m) = 2v_p\left(\frac{bd}{e}\right) + v_p(n)$.
Maar we weten dat $v_p(m) = 0$, aangezien er moet gelden dat als p een deler is van m, dan geldt $p \equiv \pm 1 \mod 5$. Dus moet gelden dat $v_p(n) = -2v_p\left(\frac{bd}{e}\right)$, en deze is dus even.
Stel nu dat $p = 2$. Als $2 \mid m$, dan geldt dus $f^2 - 5g^2 \equiv f^2 + g^2 \equiv 0 \mod 2$.
Nu moet dus ofwel gelden dat $f \equiv g \equiv 0 \mod 2$, ofwel dat $f \equiv g \equiv 1 \mod 2$. Omdat f en g copriem zijn, kan het eerste geval niet gelden, dus er geldt $f \equiv g \equiv 1 \mod 2$.
We kijken nu modulo 8. Er moet dan gelden dat f en g of ± 1 of ± 3 modulo 8 zijn. Hieruit volgt dus dat $f^2 \equiv g^2 \equiv 1 \mod 8$.
Nu geldt $m = f^2 - 5g^2 \equiv 4 \mod 8$, en dus $m = f^2 - 5g^2 \equiv 0 \mod 4$.
Dus als m deelbaar is door 2, dan is m ook deelbaar door 4, maar niet door 8. Er geldt dan dus dat $v_2(m)$ even is.
Er geldt $v_2(m) = 2v_2\left(\frac{bd}{e}\right) + v_2(n)$, dus moet ook gelden dat $v_2(n)$ even is.
Dus voor alle priemen $p \equiv \pm 2 \mod 5$ geldt dat $v_p(n)$ even is. □

Voorbeeld 4.6 (Een tegenvoorbeeld)**.** Zij

$$F = \begin{cases} uv = x^2 - 5y^2 \\ (u+v)(u+2v) = x^2 - 5z^2 \end{cases}$$

Dit is een tegenvoorbeeld van het Hasse-principe.

Bewijs. We laten eerst zien dat dit stelsel vergelijkingen oplossingen in $\mathbb{Q}_v$ voor alle $v \in V$ heeft.
We kunnen laten zien dat over ieder lichaam $\mathbb{Q}_v$ (voor willekeurige $v \in V$) één van de volgende oplossingen is gedefiniëerd:

$$\begin{aligned} (u, v, x, y, z) &= (1, 1, 1, 0, \sqrt{-1}) \\ &= (10, -10, 5, 5, \sqrt{5}) \\ &= (5, 0, 0, 0, \sqrt{-5}) \\ &= (-25, 5, 0, 5, 2\sqrt{-15}) \end{aligned}$$

We zien meteen dat de oplossing $(u, v, x, y, z) = (10, -10, 5, 5, \sqrt{5})$ gedefiniëerd is over $\mathbb{R}$.
Nu zijn er voor $\mathbb{Q}_p$ drie mogelijkheden, namelijk ofwel $p = 2$, ofwel $p = 5$, ofwel $p \neq 2$ en $p \neq 5$.
We kijken eerst naar $p = 2$.
We laten zien dat de oplossing $(u, v, x, y, z) = (-25, 5, 0, 5, 2\sqrt{-15})$ gedefiniëerd is

over $\mathbb{Q}_2$. Het is duidelijk dat $-25, 5, 0$ en 2 bevat zijn in $\mathbb{Q}_2$, aangezien dit een lichaamsuitbreiding is van $\mathbb{Q}$.
Met behulp van het lemma van Hensel (lemma 4.4) laten we nu zien dat -15 een kwadraat is in $\mathbb{Q}_2$.
Zij $f(x) = x^2 + 15$. Dan geldt $f'(x) = 2x$.
We nemen nu $a_0 = 1$.
Nu geldt inderdaad

$$\begin{aligned} v_2(f(a_0)) &= v_2(a_0^2 + 15) \\ &= v_2(16) \\ &= 4 \end{aligned}$$

en

$$\begin{aligned} 2v_2(f'(a_0)) + 1 &= 2v_2(2a_0) + 1 \\ &= 2v_2(2) + 1 \\ &= 3 \end{aligned}$$

Dus $v_2(f(a_0)) \geq 2v_2(f'(a_0)) + 1$.
En volgens het lemma van Hensel (lemma 4.4) geldt nu dat er een $a \in \mathbb{Z}_2$ bestaat met $f(a) = 0$. Oftewel, -15 is een kwadraat in $\mathbb{Z}_2$ (en dus ook in $\mathbb{Q}_2$, aangezien dit een uitbreiding van $\mathbb{Z}_2$ is).

We kijken nu naar $p = 5$.
We laten zien dat de oplossing $(u, v, x, y, z) = (1, 1, 1, 0, \sqrt{-1})$ gedefiniëerd is over $\mathbb{Q}_5$. Het is duidelijk dat 1 en 0 bevat zijn in $\mathbb{Q}_5$, aangezien dit een lichaamsuitbreiding is van $\mathbb{Q}$.
Met behulp van het lemma van Hensel (lemma 4.4) laten we nu zien dat -1 een kwadraat is in $\mathbb{Q}_5$.
Zij $f(x) = x^2 + 1$. Dan geldt $f'(x) = 2x$.
We nemen nu $a_0 = 2$.
Nu geldt inderdaad

$$\begin{aligned} v_5(f(a_0)) &= v_5(a_0^2 + 1) \\ &= v_5(5) \\ &= 1 \end{aligned}$$

en

$$\begin{aligned} 2v_5(f'(a_0)) + 1 &= 2v_5(2a_0) + 1 \\ &= 2v_5(4) + 1 \\ &= 1 \end{aligned}$$

Dus $v_5(f(a_0)) \geq 2v_5(f'(a_0)) + 1$.
En volgens het lemma van Hensel (lemma 4.4) geldt nu dat er een $a \in \mathbb{Z}_5$ bestaat met $f(a) = 0$. Oftewel, -1 is een kwadraat in $\mathbb{Z}_5$ (en dus ook in $\mathbb{Q}_5$, aangezien dit een uitbreiding van $\mathbb{Z}_5$ is).

Stel nu dat $p \neq 2$ en $p \neq 5$. Dan kunnen we de multiplicativiteit van het Legendresymbool toepassen. Er geldt namelijk

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$$

Aangezien $p \neq 5$, geldt dat deze drie termen alledrie ongelijk aan nul zijn. Ze kunnen niet alledrie gelijk zijn aan -1, dus moet er voor iedere p ten minste één van de drie gelijk zijn aan 1. Dus -5, of -1, of 5 is een kwadraat modulo p. Uit het

lemma van Hensel (lemma 4.4) volgt nu dat ook geldt dat -5, -1 of 5 een kwadraat is in $\mathbb{Q}_p$ (we passen het lemma toe op de functies X^2+5, X^2+1 en X^2-5).
Dus voor iedere p ongelijk aan 2 of 5 is één van de volgende drie oplossingen gedefiniëerd over $\mathbb{Q}_p$:

$$\begin{aligned}(u,v,x,y,z) &= (1,1,1,0,\sqrt{-1})\\ &= (10,-10,5,5,\sqrt{5})\\ &= (5,0,0,0,\sqrt{-5})\end{aligned}$$

We hebben nu dus voor alle $v \in V$ laten zien dat één van de gegeven oplossingen gedefiniëerd is over $\mathbb{Q}_v$, dus ons stelsel vergelijkingen heeft niet-triviale oplossingen in $\mathbb{Q}_v$ voor alle $v \in V$.

Nu laten we zien dat ons stelsel vergelijkingen geen niet-nul oplossing heeft in $\mathbb{Q}$.
Merk nu op dat we in ons stelsel vergelijkingen zonder verlies van algemeenheid kunnen aannemen dat u en v copriem en geheel zijn.
Stel dat $5 \mid uv$. Dan moet gelden dat $v_5(x^2) \geq 1$ (want $x^2 = uv + 5y^2$). Dan geldt echter ook dat $5 \mid (u+v)(u+2v)$ (want $(u+v)(u+2v) = x^2 - 5z^2$). Maar $5 \mid u$, of $5 \mid v$, maar niet allebei (want ze zijn copriem). Dus er kan niet gelden dat $5 \mid u+v$ of $5 \mid u+2v$, en dus ook niet dat $5 \mid (u+v)(u+2v)$. Dus onze aanname klopt niet en $5 \nmid uv$.
Omdat u en v copriem zijn, geldt voor iedere priemdeler die uv deelt, dat deze of alleen u, of alleen v deelt. Dit geldt ook voor priemdelers gelijk aan $\pm 2 \mod 5$, en de valuatie van u en v bij deze priemen is volgens lemma 4.5, net als de valuatie van uv bij deze priemen, gelijk aan nul of even. Hetzelfde geldt voor $(u+v)$ en $(u+2v)$.
Hieruit volgt dus dat zowel u, als v, alsmede $u+v$ en $u+2v$ gelijk zijn aan $\pm 1 \mod 5$.
Dit blijkt een tegenspraak, want als u en v gelijk zijn aan $\pm 1 \mod 5$, dan is $u+v$ gelijk aan $-2, 0$ of 2 modulo 5.
Hieruit volgt dat F dus geen niet-triviale oplossingen in $\mathbb{Q}$ heeft.
Dus F voldoet niet aan het Hasse-principe. $\square$

5. Het Hilbertsymbool

Definitie 5.1 ($\mathbb{Q}_v$ met $v \in V$)**.** We definieren de verzameling V als de verzameling die bestaat uit alle priemgetallen en ∞.
Dan geldt dat $\mathbb{Q}_v$ gelijk is aan het lichaam van v-adische getallen als v een priemgetal is en gelijk is aan $\mathbb{R}$ als v gelijk is aan ∞.

Definitie 5.2 (Het Hilbertsymbool)**.** Zij $a, b \in \mathbb{Q}_v^*$. Het Hilbertsymbool van a en b ten opzichte van $\mathbb{Q}_v$ is als volgt gedefiniëerd:

$$(a,b)_v = \begin{cases} 1 & \text{als } z^2 - ax^2 - by^2 = 0 \text{ een oplossing } (x,y,z) \neq (0,0,0) \text{ heeft in } \mathbb{Q}_v^3, \\ -1 & \text{anders.} \end{cases}$$

Als we in bovenstaande definitie de subscript v overal weglaten, praten we over het Hilbertsymbool ten opzichte van $\mathbb{Q}$.

Propositie 5.3. *Zij k gelijk aan $\mathbb{Q}$, $\mathbb{R}$ of aan $\mathbb{Q}_p$, met p een priemgetal. Zij $a, b \in k^*$ en zij $k_b = k(\sqrt{b})$ (waarbij geldt dat als b een kwadraat is in k, dan $k_b = k$). Dan geldt:*

$$(a,b) = 1 \Leftrightarrow a \text{ is een norm van een element uit } k_b^*.$$

Waarbij (a,b) het Hilbertsymbool van a en b ten opzichte van k.

Bewijs. We bekijken eerst wat er gebeurt als b een kwadraat is in k. Dan geldt zeker dat a een norm is van een element uit k_b^*, aangezien $a \in k^* = k_b^*$. Ook geldt zeker dat $(a,b) = 1$, neem dan namelijk $z^2 = b$, $x = 0$ en $y = 1$. Dan geldt inderdaad $z^2 - ax^2 - by^2 = 0$. Dus als b een kwadraat is in k, dan geldt de propositie (want dan zijn beide kanten van de dubbele pijl altijd waar).
Stel nu dat b geen kwadraat is in k. Dan is ieder element uit k_b te schrijven als $z + \beta y$, waarbij β een wortel is van b in een lichaamsuitbreiding van k en $z, y \in k$. Normen van elementen uit k_b zijn dan te schrijven als $z^2 - by^2$.
We bewijzen nu eerst de implicatie naar rechts.
Er geldt $(a,b) = 1$, dus er zijn $x, y, z \in k$, zodanig dat $(x,y,z) \neq (0,0,0)$ en $z^2 - ax^2 - by^2 = 0$.
Er geldt nu dus $ax^2 = z^2 - by^2$. We weten ook dat $x \neq 0$, want dan zou b een kwadraat zijn in k, en dat was b niet.
Dus geldt nu $a = \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2$. We weten dat niet kan gelden dat $y = z = 0$, want dan zou uit de vergelijking $z^2 - ax^2 - by^2 = 0$ volgen dat $a = 0$ (aangezien $x \neq 0$), maar $a \in k^*$. Dus a is een norm van het element $\left(\frac{z}{x}\right) - \beta\left(\frac{y}{x}\right) \in k_b^*$.
Nu bewijzen we de implicatie naar links.
We weten dat a een norm is van een element in k_b^*, dus a is van de vorm $z^2 - by^2$, met $y, z \in k$. Als we nu $x = 1$ nemen, dan geldt $z^2 - ax^2 - by^2 = 0$, dus $(a,b) = 1$. □

Propositie 5.4. *Zij k gelijk aan $\mathbb{Q}$, $\mathbb{R}$ of aan $\mathbb{Q}_p$, met p een priemgetal. Als we weten dat twee van de drie Hilbertsymbolen ten opzichte van k, $(aa', b), (a, b)$ en (a', b), gelijk zijn aan 1, dan is de derde dat ook en geldt dus*

$$(aa', b) = (a, b)(a', b).$$

Hetzelfde geldt voor

$$(a, bb') = (a, b)(a, b').$$

Bewijs. We merken eerst op dat $(a,b) = (b,a)$. Dit volgt vrijwel direct uit de definitie (wissel x en y om). We hoeven dus alleen te bewijzen dat $(aa', b) = (a,b)(a',b)$, als twee van deze termen gelijk zijn aan 1.
Dit volgt uit de multiplicativiteit van normen. We kijken eerst wat er gebeurt als

$(a,b) = (a',b) = 1$.
Dan geldt dat a gelijk is aan de norm van α, $N(\alpha)$, en a' is gelijk aan $N(\alpha')$, voor zekere $\alpha, \alpha' \in k(\sqrt{b})$.
Nu geldt $aa' = N(\alpha)N(\alpha') = N(\alpha\alpha')$, en dus is dan ook aa' een norm, oftewel $(aa',b) = 1$.
Stel nu dat $(aa',b) = (a,b) = 1$.
Dan geldt, volgens propositie 5.3, dat a gelijk is aan $N(\alpha)$, en aa' is gelijk aan $N(\alpha')$, voor zekere $\alpha, \alpha' \in k(\sqrt{b})$.
Nu geldt $a' = \frac{aa'}{a} = \frac{N(\alpha')}{N(\alpha)} = N(\frac{\alpha'}{\alpha})$, en dus is dan ook a' een norm, oftewel $(a',b) = 1$.
Hetzelfde geldt als $(aa',b) = (a',b) = 1$.

□

Propositie 5.5 (multipliciteit van Hilbertsymbool in $\mathbb{Q}_v$)**.** *In $\mathbb{Q}_v$ (met $v \in V$) geldt altijd*

$$(aa',b)_v = (a,b)_v(a',b)_v$$

en

$$(a,bb')_v = (a,b)_v(a,b')_v.$$

Bewijs. Ook hier hoeven we, net als bij het bewijs van de vorige propositie, alleen naar $(aa',b)_v = (a,b)_v(a',b)_v$ te kijken. We hebben al laten zien dat er niet kan gelden dat één van de termen gelijk is aan -1, terwijl de andere twee gelijk zijn aan 1. Nu hoeven we dus alleen nog te laten zien dat ze niet allemaal gelijk aan -1 kunnen zijn.
We laten het eerst zien voor $\mathbb{R}$.
Voor $\mathbb{R}$ is het makkelijk in te zien dat $(a,b) = -1$ dan en slechts dan als $a,b < 0$.
Als dus $(aa',b)_v, (a,b)_v$ en $(a',b)_v$ alledrie gelijk zouden zijn aan -1 dan zouden a, a' en aa' alledrie kleiner dan 0 moeten zijn, en dat kan niet. Dus $(aa',b)_v, (a,b)_v$ en $(a',b)_v$ kunnen niet alledrie gelijk zijn aan -1.
Nu kijken we naar $\mathbb{Q}_2$.
We schrijven a als $2^\alpha u$ en b als $2^\beta w$, waarbij $v_2(u) = v_2(w) = 0$. We schrijven

$$\epsilon(u) \equiv \frac{u-1}{2} \mod 2 = \begin{cases} 0 & \text{als} \quad u \equiv 1 \mod 4 \\ 1 & \text{als} \quad u \equiv -1 \mod 4 \end{cases}$$

en

$$\omega(u) \equiv \frac{u^2-1}{8} \mod 2 = \begin{cases} 0 & \text{als} \quad u \equiv \pm 1 \mod 8 \\ 1 & \text{als} \quad u \equiv \pm 3 \mod 8 \end{cases}.$$

Merk op dat geldt $\epsilon(u) + \epsilon(u') \equiv \epsilon(uu') \mod 2$ en $\omega(u) + \omega(u') \equiv \omega(uu') \mod 2$.
Nu geldt

$$(a,b) = (-1)^{\epsilon(u)\epsilon(w)+\alpha\omega(w)+\beta\omega(u)}.$$

Voor een bewijs dat deze formule inderdaad geldt, verwijs ik naar pagina 20 van [3].
Er geldt nu:

$$\begin{aligned} (a,b)(a',b) &= (-1)^{\epsilon(u)\epsilon(w)+\alpha\omega(w)+\beta\omega(u)}(-1)^{\epsilon(u')\epsilon(w)+\alpha'\omega(w)+\beta\omega(u')} \\ &= (-1)^{\epsilon(u)\epsilon(w)+\alpha\omega(w)+\beta\omega(u)+\epsilon(u')\epsilon(w)+\alpha'\omega(w)+\beta\omega(u')} \\ &= (-1)^{(\epsilon(u)+\epsilon(u'))\epsilon(w)+(\alpha+\alpha')\omega(w)+\beta(\omega(u)+\omega(u'))} \\ &= (-1)^{\epsilon(uu')\epsilon(w)+(\alpha+\alpha')\omega(w)+\beta\omega(uu')} \\ &= (aa',b) \end{aligned}$$

Merk op dat we hierbij gebruik hebben gemaakt van het feit dat $aa' = p^{\alpha+\alpha'}uu'$.
Nu kijken we naar $\mathbb{Q}_p$ met p een oneven priemgetal.
We schrijven a als $p^\alpha u$ en b als $p^\beta w$, waarbij $v_p(u) = v_p(w) = 0$. Dan geldt

$$(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

Waarbij $\epsilon(p) \equiv \frac{p-1}{2} \mod 2$.
Voor een bewijs dat deze formule inderdaad geldt, verwijs ik naar pagina 20 van [3].
Er geldt nu:

$$\begin{aligned}
(a,b)(a',b) &= (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha (-1)^{\alpha'\beta\epsilon(p)} \left(\frac{u'}{p}\right)^\beta \left(\frac{v}{p}\right)^{\alpha'} \\
&= (-1)^{(\alpha+\alpha')\beta\epsilon(p)} \left(\left(\frac{u}{p}\right)\left(\frac{u'}{p}\right)\right)^\beta \left(\frac{v}{p}\right)^{\alpha+\alpha'} \\
&= (-1)^{(\alpha+\alpha')\beta\epsilon(p)} \left(\frac{uu'}{p}\right)^\beta \left(\frac{v}{p}\right)^{\alpha+\alpha'} \\
&= (aa', b)
\end{aligned}$$

Merk op dat we hierbij gebruik hebben gemaakt van de multiplicativiteit van het Legendre-symbool en van het feit dat $aa' = p^{\alpha+\alpha'}uu'$.
Dus voor alle $\mathbb{Q}_v$ met $v \in V$ is het Hilbertsymbool multiplicatief. □

6. Kwadratische vormen

Definitie 6.1 (Kwadratische vorm)**.** Zij W een moduul over een commutatieve ring A. Een functie $Q : W \to A$ heet een kwadratische vorm op W als

(1) $Q(ax) = a^2Q(x)$ voor alle $a \in A$ en $x \in W$, en
(2) de functie $\langle x, y\rangle \mapsto Q(x + y) - Q(x) - Q(y)$ is een bilineaire vorm.

We noemen (W, Q) een kwadratisch moduul.

Definitie 6.2 (Equivalente kwadratische vormen)**.** Twee kwadratische vormen heten equivalent als de corresponderende kwadratische modulen isomorf zijn. Twee kwadratische modulen (W, Q) en W', Q' zijn isomorf als er een isomorfisme bestaat tussen W en W' zodanig dat Q onder dit isomorfisme over gaat in Q'.

Stelling 6.3. *Zij k een lichaam met karakteristiek ongelijk aan 2 en f een kwadratische vorm op een n-dimensionale vectorruimte over k. Dan bestaan er $a_1, \ldots, a_n \in k$ zodanig dat $f \sim a_1X_1^2 + \ldots + a_nX_n^2$ op k^n.*

Bewijs. Voor een bewijs van deze stelling verwijs ik naar pagina 42 en 43 van [5]. □

Definitie 6.4. Zij f een kwadratische vorm in n variabelen en zij $a \in \mathbb{Q}_v$. We zeggen dat f het element a representeert in $\mathbb{Q}_v$ als er een $0 \neq x \in \mathbb{Q}_v^n$ is, zodanig dat $f(x) = a$.

Opmerking 6.5. Merk op dat voor twee equivalente kwadratische vormen f en f' voor alle a geldt dat f het element a representeert in $\mathbb{Q}_v$ dan en slechts dan als f' het element a representeert in $\mathbb{Q}_v$.

Propositie 6.6. *Zij f een niet-gedegenereerde kwadratische vorm. Als f nul representeert in $\mathbb{Q}_v$, dan representeert f alles in $\mathbb{Q}_v$.*

Bewijs. We bekijken de bilineaire vorm $\langle a, b\rangle = f(a + b) - f(a) - f(b)$.
Aangezien f niet-gedegenereerd is, is deze bilineaire vorm dat ook en geldt dus $\forall a : [(\forall b : \langle a, b\rangle = 0) \Rightarrow a = 0]$. f representeert nul, dus er is een $a \neq 0$, zodanig dat $f(a) = 0$.
Dan geldt $\langle a, a\rangle = f(2a) - f(a) - f(a) = 4f(a) - 2f(a) = 2f(a) = 0$.
Omdat de bilineaire vorm niet-gedegenereerd is, is er een b, zodanig dat $\langle a, b\rangle \neq 0$.
We willen nu een x zo zoeken dat $f(x)$ gelijk is aan c, waarbij c een willekeurig element is. We bekijken een $x = pa + qb$. Er geldt

$$\begin{aligned} f(x) &= \frac{\langle x, x\rangle}{2} \\ &= \frac{1}{2}\langle pa + qb, pa + qb\rangle \\ &= \frac{1}{2}(\langle pa, pa\rangle + 2\langle pa, qb\rangle + \langle qb, qb\rangle) \\ &= \frac{1}{2}(p^2\langle a, a\rangle + 2pq\langle a, b\rangle + q^2\langle b, b\rangle) \\ &= \frac{1}{2}(2pq\langle a, b\rangle + q^2 2f(b)) \\ &= pq\langle a, b\rangle + q^2 f(b)) \\ &= q(p\langle a, b\rangle + qf(b)) \end{aligned}$$

We nemen nu $q = 1$, en $p = \frac{c-f(b)}{\langle a,b\rangle}$. Merk op dat dit kan, omdat $\langle a, b\rangle \neq 0$.
Dan geldt

$$\begin{aligned} f(x) &= q(p\langle a, b\rangle + qf(b)) \\ &= \frac{c - f(b)}{\langle a, b\rangle}\langle a, b\rangle + f(b) \\ &= c - f(b) + f(b) \\ &= c \end{aligned}$$

Aangezien we c een willekeurig element hebben genomen, kunnen we voor iedere c een dergelijke x vinden, dus f representeert alle elementen. □

7. Een aantal stellingen

Stelling 7.1 (Chinese reststelling)**.** *Zij $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$, zodanig dat de m_i paarsgewijs copriem zijn. Dan bestaat er een $a \in \mathbb{Z}$ zodanig dat $a \equiv a_i \mod m_i$ voor alle i.*

Bewijs. Voor een bewijs verwijs ik naar pagina 24 van [3]. □

Stelling 7.2 (Benaderingsstelling)**.** *Zij S een eindige deelverzameling van V. Het beeld van $\mathbb{Q}$ in $\prod_{v\in S}\mathbb{Q}_v$ is dicht in dit product (voor de producttopologie).*

Bewijs. Voor het bewijs van deze stelling maken we onder andere gebruik van de Chinese reststelling (stelling 7.1).
Als het beeld van $\mathbb{Q}$ in een verzameling $\prod_{v\in S'}\mathbb{Q}_v$ dicht is, waarbij $S \subset S'$, dan is het beeld van $\mathbb{Q}$ ook dicht in $\prod_{v\in S}\mathbb{Q}_v$. We kunnen S dus uitbreiden tot $S = \{\infty, p_1, \ldots, p_n\}$, waarbij de p_i verschillende priemgetallen zijn. We moeten nu laten zien dat het beeld van $\mathbb{Q}$ dicht is in $\mathbb{R} \times \mathbb{Q}_{p_1} \times \ldots \times \mathbb{Q}_{p_n}$.
Laat nu $(x_\infty, x_1, \ldots, x_n)$ een willekeurig punt in dit product. We laten zien dat dit punt willekeurig dicht bij een punt in het beeld van $\mathbb{Q}$ ligt. Na vermenigvuldigen met een geheel getal kunnen we ervan uitgaan dat $x_i \in \mathbb{Z}_{p_i}$ voor $i = 1, \ldots, n$. Nu gaan we bewijzen dat voor iedere $\epsilon > 0$ en voor iedere $N \in \mathbb{Z}_{>0}$ er een $x \in \mathbb{Q}$ bestaat, zodanig dat $\|x - x_\infty\| \leq \epsilon$ en $v_{p_i}(x - x_i) \geq N$ voor $i = 1, \ldots, n$ (want in de p-adische topologie geldt dat hoe groter de valuatie van het verschil, hoe kleiner de afstand tussen 2 punten).
Uit de Chinese reststelling volgt dat als we $m_i = p_i^N$ nemen, dat er een $x_0 \in \mathbb{Z}$ bestaat zodanig dat $x_0 \equiv x_i \mod p_i^N$, oftewel dat $x_0 - x_i \equiv 0 \mod p^N$, oftewel dat $v_{p_i}(x_0 - x_i) \geq N$ voor alle i.
We nemen nu een $q \in \mathbb{Z}$, zodanig dat deze copriem is met alle p_i (bijvoorbeeld een ander priemgetal). Getallen van de vorm $\frac{a}{q^m} \in \mathbb{Q}$, met $a \in \mathbb{Z}$ en $m \in \mathbb{Z}_{\geq 0}$, zijn dicht in $\mathbb{R}$.
We kiezen nu een dergelijk getal $u = \frac{a}{q^m}$, zodanig dat $\|x_0 - x_\infty + up_1^N \ldots p_n^N\| \leq \epsilon$. Het getal $x = x_0 + up_1^N \ldots p_n^N \in \mathbb{Q}$, voldoet aan onze voorwaarden, want

$$\begin{aligned} \|x - x_\infty\| &= \|x_0 - x_\infty + up_1^N \ldots p_n^N\| \\ &\leq \epsilon \end{aligned}$$

en

$$\begin{aligned} v_{p_i}(x - x_i) &= v_{p_i}(x_0 - x_i + up_1^N \ldots p_n^N) \\ &\geq \min\left(v_{p_i}(x_0 - x_i), v_{p_i}(up_1^N \ldots p_n^N)\right) \\ &\geq N. \end{aligned}$$

□

Stelling 7.3 (Stelling van Dirichlet)**.** *Als $a, m \geq 1$ twee coprieme gehele getallen zijn, dan zijn er oneindig veel priemen p zodanig $p \equiv a \mod m$.*

Bewijs. Voor een bewijs van de stelling van Dirichlet verwijs ik naar pagina 61 tot en met 76 van [3]. □

Stelling 7.4. *Zij $(a_i)_{i\in I}$ een eindige familie van elementen in $\mathbb{Q}^*$ en zij $(\epsilon_{i,v})_{i\in I, v\in V}$ een familie van getallen gelijk aan ± 1 (waarbij I een eindige verzamling is). Opdat er een $x \in \mathbb{Q}^*$ bestaat zodanig dat voor het Hilbertsymbool van a_i en x in $\mathbb{Q}_v$ geldt $(a_i, x)_v = \epsilon_{i,v}$ voor alle $i \in I$ en alle $v \in V$ is het nodig en voldoende dat de volgende dingen gelden:*

- *Op een eindig aantal na, zijn alle* $\epsilon_{i,v}$ *gelijk aan* 1.
- *Voor alle* $i \in I$ *geldt* $\prod_{v \in V} \epsilon_{i,v} = 1$.
- *Voor alle* $v \in V$ *bestaat er een* $x_v \in \mathbb{Q}_v^*$ *zodanig dat* $(a_i, x_v)_v = \epsilon_{i,v}$ *voor alle* $i \in I$.

Bewijs. Het bewijs maakt gebruik van de Chinese Reststelling (stelling 7.1), de benaderingsstelling (stelling 7.2) en de stelling van Dirichlet (stelling 7.3). Voor een volledig bewijs verwijs ik naar pagina 24 tot en met 26 van [3]. □

8. Stelling van Hasse-Minkowski

Stelling 8.1 (Hasse-Minkowski)**.** *Kwadratische vormen over $\mathbb{Q}$ voldoen aan het Hasse-Principe.*

Bewijs. Uit opmerking 5.2 is al gebleken dat de implicatie naar links geldt. We moeten nu dus nog de implicatie naar rechts bewijzen.
We weten vanwege stelling 6.3 dat iedere kwadratische vorm equivalent is met een kwadratische vorm van de vorm $a_1X_1^2 + \cdots + a_nX_n^2$. Ook kunnen we ervan uit gaan dat $a_1 = 1$, door de gehele vergelijking te delen door a_1 (merk hierbij op dat we aan kunnen nemen dat $a_1 \neq 0$), aangezien dit niets verandert aan de nulpunten.
We delen het bewijs op naar het aantal variabelen n.
Geval $n = 2$
We hebben nu $f = X_1^2 + a_2X_2^2$. Omdat we ervan uitgaan dat f een nulpunt heeft in $\mathbb{R}^2$, moet gelden dat a_2 negatief is, aangezien kwadraten altijd positief zijn. We kunnen de vergelijking dus omschrijven naar $f = X_1^2 - aX_2^2$, met $a > 0$. Ook moet voor een niet-triviale oplossing van $f(x_1, x_2) = 0$ gelden dat x_2 ongelijk aan 0 is, want als dat wel het geval zou zijn, dan zou ook x_1 gelijk moeten zijn aan 0, en dan is de oplossing wel triviaal.
We kunnen nu a ontbinden in priemfactoren, oftewel $a = \prod_p p^{v_p(a)}$.
We weten ook dat f een nulpunt heeft in $\mathbb{Q}_p$. Dan geldt dus voor zekere $x_1, x_2 \in \mathbb{Q}_p$

$$\begin{aligned} f &= 0 \\ x_1^2 - ax_2^2 &= 0 \\ a &= \left(\frac{x_1}{x_2}\right)^2 \end{aligned}$$

Dus a is een kwadraat in $\mathbb{Q}_p$, dus $v_p(a)$ is even.
Omdat dit geldt voor iedere priem p die a deelt, geldt dus dat a een kwadraat is in $\mathbb{Q}$.
Geval $n = 3$
We hebben $f = X_1^2 - aX_2^2 - bX_3^2$.
We kunnen ervan uit gaan dat a en b geen kwadraten bevatten (oftewel dat $v_p(a)$ en $v_p(b)$ gelijk zijn aan 0 of 1 voor alle priemen p), omdat we, mochten ze toch kwadraten bevatten, deze kwadraten kunnen opnemen in X_2 en X_3. Daarnaast kunnen we er ook vanuit gaan dat $|a| \leq |b|$.
We gaan nu inductie toepassen naar $m(f) = |a| + |b|$.
Stap 1: $m(f) = 2$.
Er geldt nu $f = X_1^2 \pm X_2^2 \pm X_3^2$.
We weten dat f, als deze 0 representeert in $\mathbb{R}$, niet gelijk is aan $X_1^2 + X_2^2 + X_3^2$.
Voor de andere drie opties hebben we een oplossing in $\mathbb{Q}$.
Dus voor $m(f) = 2$ geldt inderdaad dat f voldoet aan het Hasse-principe.
Stap 2: Stel nu dat voor een bepaalde $m(F) > 2$ geldt dat iedere kwadratische vorm f met $m(f) < m(F)$ voldoet aan het Hasse-principe (dit is de inductie-hypothese).
Er geldt $m(F) > 2$, dus $|b| \geq 2$.
Omdat b geen kwadraten bevat, kunnen we b schrijven als $b = \pm p_1 \dots p_k$, waarbij de p_i verschillende priemgetallen zijn.
Zij nu p een willekeurige p_i. We gaan bewijzen dat a een kwadraat is modulo p.
Per aanname bestaan er $x, y, z \in \mathbb{Q}_p$, zodanig dat $z^2 - ax^2 - by^2 = 0$. We kunnen deze x, y en z zo kiezen dat ze bevat zijn in $\mathbb{Z}_p$ en copriem zijn.
Als geldt dat $a \equiv 0 \mod p$, dan zijn we klaar, want dan is a een kwadraat modulo p. Stel nu dat $a \not\equiv 0 \mod p$.

Dan geldt modulo p:

$$z^2 - ax^2 \equiv 0 \mod p.$$

Stel nu dat $x \equiv 0 \mod p$. Dan geldt ook dat $z \equiv 0 \mod p$.
Maar als dit geldt dan moet gelden dat $p^2 \mid by^2$, omdat $z^2 - ax^2 - by^2 = 0$. We weten dat p maar één keer b deelt, dus moet gelden dat $p \mid y^2$, en dus ook $p \mid y$. Maar dan deelt p alledrie de variabelen x, y en z en dit kan niet, want we hadden ze copriem gekozen.
Dus $x \not\equiv 0 \mod p$. Hieruit volgt dat a gelijk is aan een kwadraat modulo p.
Uit de Chinese reststelling (stelling 7.1) ($\mathbb{Z}/b\mathbb{Z} = \prod \mathbb{Z}/p_i\mathbb{Z}$) volgt dat als a een kwadraat is modulo iedere priemdeler p van b, dan is a ook een kwadraat modulo b.
We kunnen nu dus gehele getallen t en b' vinden zodanig dat $t^2 = a + bb'$.
We kunnen t zo kiezen dat $|t| \leq \frac{|b|}{2}$.
Omdat geldt dat $bb' = t^2 - a$, is bb' een norm van het element $t + \alpha$ in $\mathbb{Q}(\sqrt{a})$, waarbij $\alpha^2 = a$. Uit propositie 5.3 volgt nu dat $(bb', a) = 1$.
Vanwege propositie 5.4 weten we dat als $(bb', a) = 1$, dan $(b, a) = (b', a)$, oftewel $F = X_1^2 - aX_2^2 - bX_3^2$ representeert 0, dan en slechts dan als $F' = X_1^2 - aX_2^2 - b'X_3^2$ dat doet.
Dus geldt dat f' nulpunten heeft in alle lichamen $\mathbb{Q}_v$.
Er geldt

$$\begin{aligned} |b'| &= \left|\frac{t^2 - a}{b}\right| \\ &\leq \left|\frac{t^2}{b}\right| + \left|\frac{a}{b}\right| \\ &\leq \left|\frac{\frac{b^2}{4}}{b}\right| + 1 \\ &= \frac{|b|}{4} + 1 \\ &< |b| \end{aligned}$$

We schrijven nu $b' = b''u^2$, waarbij b'' kwadraatvrij is. Er geldt nu $|b''| \leq |b'| < |b|$.
Volgens onze inductiehypothese geldt nu dat $f'' = X_1^2 - aX_2^2 - b''X_3^2$ een nulpunt heeft in $\mathbb{Q}$. Deze vergelijking is equivalent met f', welke weer equivalent is met f, dus ook f heeft een nulpunt in $\mathbb{Q}$.
We hebben nu met inductie bewezen dat iedere $f = X_1^2 - aX_2^2 - bX_3^2$ aan het Hasse-principe voldoet.

Geval $n = 4$
We schrijven $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$.
We weten dat f nul representeert in $\mathbb{Q}_v$. We laten eerst zien dat er een $x_v \in \mathbb{Q}_v^*$ bestaat, zodanig dat deze gerepresenteerd wordt door zowel $aX_1^2 + bX_2^2$, als $cX_3^2 + dX_4^2$. Omdat f nul representeert, zijn er dus x_1, x_2, x_3, x_4 in $\mathbb{Q}_v$, zodanig dat $ax_1^2 + bx_2^2 = cx_3^2 + dx_4^2$. Als geldt dat $ax_1^2 + bx_2^2 = cx_3^2 + dx_4^2 = \alpha \neq 0$, dan geldt dus dat $\alpha \in \mathbb{Q}_v^*$ gerepresenteerd wordt door zowel $aX_1^2 + bX_2^2$, als $cX_3^2 + dX_4^2$. Als $\alpha = 0$, dan representeert $aX_1^2 + bX_2^2$ dus 0 in $\mathbb{Q}_v$, en, vanwege propositie 6.6, alles in $\mathbb{Q}_v$, en in het bijzonder alle niet-nul waarden die $cX_3^2 + dX_4^2$ representeert. Er is dan dus ook een x_v die zowel $aX_1^2 + bX_2^2$, als $cX_3^2 + dX_4^2$ representeert.
We weten dus dat $f = x_vZ^2 - aX^2 - bY^2$ nul representeert in $\mathbb{Q}_v$ (neem Z gelijk aan 1).
Als f nul representeert, dan doet f vermenigvuldigd met $-b$, oftewel $-bf =$

$-x_v bZ^2 + abX^2 + b^2Y^2$ dat ook. Schrijven we nu $\tilde{Y} = bY$, dan volgt dat $\tilde{Y}^2 - x_v bZ^2 + abX^2$ nul representeert, oftewel $(x_v b, -ab)_v = 1$.
Nu kunnen we de multiplicativiteit van het Hilbert symbool in $\mathbb{Q}_v$ (propositie 5.5) toepassen (hierbij gebruiken we dat $(b, -b)_v = 1$ (neem $(Z, X, Y) = (0, 1, 1)$, dan geldt inderdaad $Z^2 - bX^2 + bY^2 = 0$)):

$$\begin{aligned} 1 &= (x_v b, -ab)_v \\ &= (x_v, -ab)_v (b, a)_v (b, -b)_v \\ &= (x_v, -ab)_v (a, b)_v \\ (x_v, -ab)_v &= (a, b)_v \end{aligned}$$

Hetzelfde geldt voor $(x_v, -cd)_v = (c, d)_v$.
Nu kunnen we stelling 7.4 toepassen. We nemen dan $(a_i)_{i \in I}$ zo, dat $a_1 = -ab$ en $a_2 = -cd$ (dus $I = \{1, 2\}$) en $(\epsilon_{i,v})_{i \in I, v \in V}$ is gelijk aan $(x_v, -ab)_v$ als $i = 1$ en $(x_v, -cd)_v$ als $i = 2$. Dan geldt inderdaad dat, op een eindig aantal na, alle $\epsilon_{i,v}$ gelijk zijn aan 1. Ook geldt $\prod_{v \in V} (x_v, -ab)_v = \prod_{v \in V} (a, b)_v = 1 = \prod_{v \in V} (c, d)_v = \prod_{v \in V} (x_v, -cd)_v$. Als laatste geldt ook, zoals we net hebben laten zien, dat voor alle $v \in V$ er een x_v bestaat zodanig dat $(a_i, x_v)_v = \epsilon_{i,v}$.
Er bestaat dus een $x \in \mathbb{Q}^*$ zodanig dat $(x, -ab)_v = (a, b)_v$ en $(x, -cd)_v = (c, d)_v$ voor alle $v \in V$.
Hieruit volgt:

$$\begin{aligned} (x, -ab)_v &= (a, b)_v \\ 1 &= (x, -ab)_v (a, b)_v \\ &= (x, -ab)_v (b, a)_v (b, -b)_v \\ &= (xb, -ab)_v \end{aligned} \tag{1}$$

Dus $Y^2 - xbZ^2 + abX^2$ representeert 0 in $\mathbb{Q}_v$ voor alle v. Schrijven we nu $\tilde{Y} = \frac{Y}{b}$ (merk hierbij op dat b niet gelijk is aan 0, omdat dan onze f niet meer van graad 4 is, maar van graad 3), dan volgt dat ook $b\tilde{Y}^2 - xZ^2 + aX^2$ nul representeert.
Hieruit volgt dat de kwadratische vorm $aX_1^2 + bX_2^2 - xZ^2$ nul representeert in iedere $\mathbb{Q}_v$, en dus ook in $\mathbb{Q}$ (want het is een kwadratische vorm van graad 3). Dus $aX_1^2 + bX_2^2$ representeert x in $\mathbb{Q}$. Hetzelfde geldt voor $cX_3^2 + dX_4^2$, dus $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$ representeert 0 in $\mathbb{Q}$.

Geval $n = 5$
We gebruiken inductie naar n. De inductiehypothese is dan dat iedere kwadratische vorm in $N < n$ variabelen voldoet aan het Hasse-principe. Als startwaarde nemen we $n = 4$, waarvoor we net hebben bewezen dat deze kwadratische vormen voldoen aan het Hasse-principe.
We schrijven f als $f = h \dot{+} (-g) = h \dot{-} g$ met $h = a_1 X_1^2 + a_2 X_2^2$ en $g = -(a_3 X_3^2 + \ldots + a_n X_n^2)$ (hierbij geven we met $\dot{+}$ aan dat we de directe som van twee vergelijkingen nemen).
Zij nu S de verzameling bestaande uit $\infty, 2$ en alle priemen p, waarvoor $v_p(a_i) \neq 0$ voor een $i \geq 3$. Merk op dat S een eindige verzameling is.
Neem nu een $v \in S$. We weten dat f een niet-triviaal nulpunt heeft in $\mathbb{Q}_v$. Er is nu een $a_v \in \mathbb{Q}_v^*$ die in $\mathbb{Q}_v$ gerepresenteerd wordt door h en door g. We weten namelijk in ieder geval dat er een $a_v \in \mathbb{Q}_v$ bestaat die door h en g wordt gerepresenteerd (want $f = h \dot{-} g$ representeert 0 in $\mathbb{Q}_v$). Als deze a_v gelijk is aan 0, dan representeert h alle elementen in $\mathbb{Q}_v$ (vanwege propositie 6.6), en dus ook alle niet-nul waarden die g aanneemt. We mogen dus aannemen dat $a_v \neq 0$.
Er bestaan dus $x_i^v \in \mathbb{Q}_v$, met $i = 1, \ldots, n$, zodanig dat $h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots x_n^v)$.

De kwadraten in $\mathbb{Q}_v^*$ vormen een open deelverzameling (voor een bewijs hiervan verwijs ik naar pagina 17 en 18 van [3]). Uit de benaderingsstelling (stelling 7.2) volgt nu dat er $x_1, x_2 \in \mathbb{Q}$ zijn, zodanig dat, als $h(x_1, x_2) = a$, dan geldt $\frac{a}{a_v} \in \mathbb{Q}_v^{*2}$ voor alle $v \in S$.
We kijken nu naar de kwadratische vorm $f_1 = aZ^2 \dot{-} g$.
Als $v \in S$, dan geldt dat g het element a_v representeert in $\mathbb{Q}_v$. We kunnen g vermenigvuldigen met $\frac{a}{a_v}$. Aangezien dit een kwadraat is in $\mathbb{Q}_v^*$, kan dit worden opgenomen in de variabelen van g (dus $g = -(a_3(\frac{a}{a_v}X_3^2) + \ldots + a_n(\frac{a}{a_v}X_n^2)) = -(a_3X_3^{'2} + \ldots + a_nX_n^{'2})$). Dus g representeert ook $a_v\frac{a}{a_v} = a$.
Hieruit volgt dat f_1 nul representeert in $\mathbb{Q}_v$ (neem $Z = 1$).
Stel nu dat $v \notin S$. Dan geldt dus voor alle a_i, met $i \geq 3$, dat $v_v(a_i) = 0$.
We bekijken nu onze $f_1 = aZ^2 + a_3X_3^2 + a_4X_4^2 + \ldots + a_nX_n^2$.
We kunnen nu $Z, X_5, \ldots, X_n$ zo kiezen dat hun valuatie bij v gelijk is aan 0, dat ze niet allemaal gelijk zijn aan 0 en zodat geldt $aZ^2 + a_5X_5^2 + \ldots + a_nX_n^2 = -c$, voor zekere $c \in \mathbb{Q}_v$, met $v_p(c) = 0$.
Nu willen we een x_3 en x_4 vinden zodanig dat geldt $a_3X_3^2 + a_4X_4^2 = c$. Hiervoor kijken we modulo v. We weten dat zowel a_3 als a_4 niet 0 modulo v zijn (aangezien $v_v(a_i) = 0$). We willen dat geldt $a_3x_3^2 + a_4x_4^2 - c \equiv 0 \mod v$. Eerst moeten we kijken of er überhaupt een dergelijke x_3 en x_4 bestaan. Daarvoor kijken we naar de volgende deelverzamelingen van $\mathbb{F}_v$:

$$\{a_3\bar{x}_3^2 : \bar{x}_3 \in \mathbb{F}_v\}$$
$$\{a_4\bar{x}_4^2 - c : \bar{x}_4 \in \mathbb{F}_v\}$$

Deze verzamelingen hebben allebei $\frac{p+1}{2}$ elementen. Aangezien $\mathbb{F}_v$ precies p elementen bevat, zit er dus een overlap in deze twee verzamlingen. Dus we kunnen een $\bar{x}_3$ en een $\bar{x}_4$ in $\mathbb{F}_v$ vinden, zodanig dat $a_3\bar{x}_3^2 + a_4\bar{x}_4^2 - c \equiv 0 \mod v$.
Aangezien a_3, a_4 en c niet gelijk zijn aan 0 modulo v, kan niet gelden dat $\bar{x}_3$ en $\bar{x}_4$ beide gelijk zijn aan 0 modulo v. Zonder verlies van algemeenheid nemen we aan dat $\bar{x}_3$ ongelijk is aan 0 modulo v.
We nemen nu eerst een $x_4 \in \mathbb{Z}_p$, zodanig dat $x_4 \equiv \bar{x}_4 \mod v$.
Nu kijken we naar de vergelijking $h = \frac{c-a_4x_4^3}{a_3} - X_3^2$. Deze vergelijking heeft, vanwege wat we net hebben laten zien een oplossing modulo v, namelijk $\bar{x}_3$. Aangezien $\bar{x}_3 \not\equiv 0 \mod v$, kunnen we het lemma van Hensel toepassen, dus er is een $x_3 \in \mathbb{Z}_p$ zodanig dat $f(x_3) = 0$. Dus we hebben nu inderdaad een x_3 en x_4 gevonden, zodanig dat $a_3X_3^2 + a_4X_4^2 = c$.
Dus $f_1 = aZ^2 + a_3X_3^2 + a_4X_4^2 + \ldots + a_nX_n^2$ representeert nu nul.
Nu geldt dat f_1 nul representeert in alle $\mathbb{Q}_v$ (voor $v \in S$ en voor $v \notin S$).
Voor f_1 geldt dat deze $n-1$ variabelen heeft. Onze inductiehypothese was, dat voor alle kwadratische vormen f met aantal variabelen $m < n$ het Hasse-principe geldt. Dus f_1 representeert ook 0 in $\mathbb{Q}$.
Hieruit volgt dat g het element a representeert. We wisten al dat h het element a representeert in $\mathbb{Q}$, dus f representeert 0 in $\mathbb{Q}$. □

Referenties

[1] David Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Springer-Verlag, New York, 1995.
[2] Neal Koblitz, *P-adic Numbers, P-adic Analysis, and Zeta-functions*, Springer-Verlag, New York, 1977.
[3] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
[4] Peter Stevenhagen, *Algebra III*, 2012 (http://websites.math.leidenuniv.nl/algebra/algebra3.pdf).
[5] Michael Stoll, *Linear Algebra II*, 2007 (http://www.math.leidenuniv.nl/∼desmit/edu/la2_2011/LinAlg2-index.pdf).