Alexander Tonkelaar

Reëel afgesloten lichamen

BACHELORSCRIPTIE

begeleid door dr. L. Taelman

Universiteit Leiden

Een pdf-versie van deze scriptie is te downloaden vanaf http://www.math.leidenuniv.nl/nl/theses/ en vanaf http://www.math.leidenuniv.nl/~atonkela/.

Gezet uit TEX Gyre Pagella, TEX Gyre Heros en TEX Gyre Cursor met behulp van pdfLATEX 3.1415926-1.40.11-2.2 en Tufte-LATEX 3.5.0.

Versie van 21 december 2011

Inhoudsopgave

Inleiding

Het lichaam $\mathbf{R}$ van reële getallen is niet algebraïsch afgesloten, maar heeft wel een algebraïsche afsluiting $\mathbf{C} = \mathbf{R}(i)$ van eindige graad. Het feit dat $\mathbf{C}$ algebraïsch afgesloten is staat bekend als de *hoofdstelling van de algebra*, hoewel ieder bewijs hiervan gebruik maakt van de analytische eigenschappen of ordestructuur van $\mathbf{R}$. Zelfs Galoistheoretische bewijzen gebruiken dat positieve getallen kwadraten zijn, -1 geen som van kwadraten is en dat polynomen van oneven graad een nulpunt hebben. Detzelfde argumenten laten zien dat ook $\overline{\mathbf{Q}} \cap \mathbf{R}$ een algebraïsche afsluiting heeft die ontstaat door een wortel van -1 toe te voegen. Zouden er ook andere voorbeelden zijn van lichamen met niet-triviale eindige algebraïsche afsluitingen die minder op het geval van $\mathbf{R}$ lijken, bijvoorbeeld in een andere karakteristiek?

Een verassend antwoord op deze vraag wordt gegeven door een stelling van Artin en Schreier:[1,2] iedere niet-triviale algebraïsche afsluiting $\overline{K}/K$ van eindige graad ontstaat door een wortel van -1 te adjungeren, in welk geval K karakteristiek 0 heeft, elk element van K een kwadraat of de tegengestelde van een kwadraat is en elk polynoom over K van oneven graad een nulpunt in K heeft. Het lichaam K is ook te voorzien van een unieke lineaire ordening $<$ die compatibel is met de lichaamsoperaties, en polynomen over K voldoen aan de tussenwaardestelling: blijkbaar is de analytische structuur op $\mathbf{R}$ die een eindige algebraïsche afsluiting mogelijk maakt ook echt nodig!

Lichamen K van het zojuist beschreven soort heten *reëel afgesloten*. Hoeveel deze lichamen gemeen hebben met $\mathbf{R}$ blijkt uit een stelling van Tarski:[3] iedere eerste-orde logische zin waarin alleen de lichaamsoperaties en de lineaire ordening in voorkomen is waar in een reëel afgesloten lichaam K dan en slechts dan als hij waar is in $\mathbf{R}$. Er bestaat zelfs een algoritme die voor zulke zinnen beslist of ze waar zijn of niet.

In het eerste hoofdstuk van deze scriptie worden reëel afgesloten lichamen gedefinieerd en aan de hand van hun algebraïsche eigenschappen gekarakteriseerd. Het tweede hoofdstuk is gewijd aan de klassieke theorie van geordende lichamen, en bevat onder andere een bewijs dat reëel afgesloten lichamen een unieke ordestructuur dragen. Het laatste hoofdstuk behandelt de logische theorie van reëel afgesloten lichamen, waaronder de stelling van Tarski en een kwantoreliminatieresultaat. Tenslotte wordt een leuke toepassing

[1] E. Artin en O. Schreier. *Eine Kennzeichnung der reell abgeschlossenen Körper*. Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, 5de band, pp. 225–231, 1927

[2] K. Conrad. *The Artin–Schreier theorem*. `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/artinschreier.pdf`, maart 2011

[3] L. van den Dries. *Alfred Tarski's Elimination Theory for Real Closed Fields*. The Journal of Symbolic Logic, 53(1), pp. 7–19, 1988

gegeven van kwantoreliminatie, afkomstig van ROBINSON, op het zeventiende probleem van HILBERT: iedere niet-negatieve rationale functie met coëfficienten in een reëel afgesloten lichaam K is een som van kwadraten van rationale functies met coëfficienten in K.

Het in hoofdstuk 1 gegeven bewijs van de stelling van ARTIN–SCHREIER is gebaseerd op een bewijs van Hendrik LENSTRA.

1 *Algebraïsche karakterisatie van reëel afgesloten lichamen*

1 DEFINITIE. Een lichaam K heet *reëel afgesloten* als aan de volgende eisen is voldaan.

1. -1 is geen som van twee kwadraten in K.
2. Voor elke $x \in K$ is x of $-x$ een kwadraat in K.
3. Elk polynoom over K van oneven graad heeft een nulpunt in K. «

Het standaardvoorbeeld van een reëel afgesloten lichaam is $\mathbf{R}$, maar ook het lichaam $\overline{\mathbf{Q}} \cap \mathbf{R}$ van reële algebraïsche getallen is reëel afgesloten. In beide gevallen ontstaat een algebraïsch afgesloten lichaam door een wortel van -1 toe te voegen. In feite is dit een voldoende voorwaarde.

2 PROPOSITIE. *Stel dat K een lichaam is waarin -1 geen kwadraat is zodat $K(\sqrt{-1})$ separabel afgesloten is. Dan is K reëel afgesloten.*

In de tweede paragraaf van dit hoofdstuk zal bewezen worden dat deze eigenschap de reëel afgesloten lichamen karakteriseert: de *hoofdstelling van de algebra* (stelling 12) stelt dat als K een reëel afgesloten lichaam is, de uitbreiding $K(\sqrt{-1})$ algebraïsch afgesloten is (en dus ook separabel afgesloten).

In het bewijs van propositie 2 is het volgende lemma nuttig.

3 LEMMA. *Stel dat K een lichaam is waarin -1 geen kwadraat is zodat $K(\sqrt{-1})$ separabel afgesloten is. Dan is een som van kwadraten in K weer een kwadraat in K.*

Bewijs. Zij $L = K(i)$ met $i^2 = -1$. De Galoisgroep $\mathrm{Gal}(L/K)$ is cyclisch van orde twee en wordt voortgebracht door de 'complexe conjugatie' σ met $\sigma(i) = -i$. Zij $N\colon L \to K$ de normafbeelding $z \mapsto z \cdot \sigma(z)$. Voor $x, y \in K$ geldt dan $N(x + iy) = x^2 + y^2$. Omdat L separabel afgesloten is, is $x + iy$ een kwadraat in L, en de normafbeelding is multiplicatief, dus $x^2 + y^2$ is een kwadraat van een element in K. □

Bewijs van propositie 2. Omdat een som van kwadraten in K wegens lemma 3 weer een kwadraat is in K, is -1 is geen som van kwadraten in K.

Omdat elk polynoom over K van oneven graad een irreducibele factor van oneven graad heeft, is het voldoende aan te tonen dat elk monisch irreducibel polynoom $f \in K[X]$ van oneven graad een nulpunt heeft. Zij nu $L = K(i)$ met $i^2 = -1$. Omdat -1 geen som van kwadraten is in K, moet K karakteristiek 0 hebben. Het lichaam L is dus algebraïsch afgesloten, en f heeft een nulpunt α in L. De graad $[K(\alpha)\colon K]$ is dan een deler van $[L\colon K]$, maar de enige oneven deler van 2 is 1. Het nulpunt α van f ligt dus in K.

Stel tenslotte dat $x \in K$ geen kwadraat is in K. Omdat x wel een kwadraat is in L zijn er $a, b \in K$ met $x = (a + bi)^2 = a^2 + 2abi - b^2$. Wegens $b \neq 0$ moet wel $a = 0$ gelden, en hieruit volgt $x = -b^2$. Als x geen kwadraat is in K, dan is $-x$ dus een kwadraat in K. □

De hypothesen in propositie 2 zijn zwakker te nemen: het is voldoende aan te nemen dat K niet separabel afgesloten is en een separabele afsluiting toelaat van eindige graad. Deze versterking is een klassiek resultaat over reëel afgesloten lichamen van ARTIN en SCHREIER.

De stelling van Artin–Schreier

4 STELLING (Artin–Schreier). *Stel dat K een lichaam is dat niet separabel afgesloten is en K^{sep} een separabele afsluiting van K van eindige graad. Dan geldt $K^{\text{sep}} = K(i)$ met $i^2 = -1$, en K is een reëel afgesloten lichaam.*

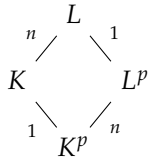
De originele formulering van ARTIN en SCHREIER luidde dat elke niet-triviale *algebraische* afsluiting $\overline{K}/K$ van eindige graad ontstaat door een wortel van -1 te adjungeren. Het bewijs gebruikt echter alleen dat $\overline{K}$ separabel afgesloten is.[1]

[1] K. CONRAD. *The Artin–Schreier theorem*. http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/artinschreier.pdf, maart 2011

5 STELLING. *Stel dat K een lichaam is dat niet algebraïsch afgesloten is en L een algebraïsche afsluiting van K van eindige graad. Dan geldt $L = K(i)$ met $i^2 = -1$, en K is een reëel afgesloten lichaam.*

Bewijs van stelling 5 uit stelling 4. Het gestelde volgt direct uit stelling 4 als L/K een separabele uitbreiding is; het volstaat dus te bewijzen dat K perfect is.

Dit is onmiddelijk duidelijk als K karakteristiek 0 heeft, dus stel dat K karakteristiek $p > 0$ heeft. Omdat L perfect is geldt $L = L^p$. Is $\alpha_1, \ldots, \alpha_n$ nu een K-basis voor L, dan is $\alpha_1^p, \ldots, \alpha_n^p$ een K^p-basis voor L^p. Uit de multiplicativiteit van de graad volgt $[K\colon K^p] = 1$ en dus $K = K^p$, en K is een perfect lichaam. □



Het bewijs van stelling 4 maakt gebruik van twee feiten over cyclische uitbreidingen, die volgen uit het volgende lemma (lemma 23.15 van het dictaat Algebra III[2]).

[2] P. STEVENHAGEN. *Algebra 3*. http://websites.math.leidenuniv.nl/algebra/algebra3.pdf, 2011

6 LEMMA VAN ARTIN–DEDEKIND. *Stel dat L/K een separabele uitbreiding is, en dat er verschillende $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathrm{Aut}_K(L)$ zijn en $c_1, c_2, \ldots, c_n \in L$ met*

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_n\sigma_n(x) = 0 \quad \textit{voor alle } x \in L.$$

Dan geldt $c_1 = c_2 = \cdots = c_n = 0$.

7 STELLING (Kummertheorie). *Stel dat L/K een cyclische uitbreiding is van graad n en dat K een primitieve n-de eenheidswortel ζ bevat. Dan geldt $L = K(\alpha)$ met $\alpha^n \in K$. Voor elke $k \geq 0$ is er een uniek K-automorfisme σ_k van L met $\sigma_k(\alpha) = \zeta^k\alpha$, en de afbeelding*

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z} &\xrightarrow{\sim} \mathrm{Gal}\,(L/K) \\ k &\mapsto \sigma_k \end{aligned}$$

is een groepsisomorfisme.

Bewijs. Schrijf $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Wegens het lemma van Artin–Dedekind bestaat er een $x \in L$ met

Het bewijs volgt dat van stelling 25.16.1 van het dictaat Algebra III.

$$\alpha := \sum_{k=0}^{n-1} \zeta^{-k}\sigma^k(x) \neq 0.$$

Er geldt $\sigma(\alpha) = \zeta\alpha$, en dus

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n;$$

α^n zit dus in het invariantenlichaam K van σ. Herhaald toepassen van σ geeft de identiteit $\sigma^k(\alpha) = \zeta^k\alpha$ voor alle $k \geq 0$, dus de ondergroep $\mathrm{Gal}(L/K(\alpha)) \subseteq \mathrm{Gal}(L/K)$ van K-automorfismen die α vasthouden is de triviale ondergroep $\langle\sigma^n\rangle = 1$; er volgt $L = K(\alpha)$. De afbeelding $k \mapsto \sigma^k$ is een isomorfisme $\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \mathrm{Gal}(L/K)$. □

In karakteristiek p zijn cyclische uitbreidingen van graad p van een andere vorm.

8 STELLING (Artin–Schreiertheorie). *Stel dat K een lichaam is van karakteristiek $p > 0$ en L/K een cyclische uitbreiding van graad p. Dan geldt $L = K(\alpha)$, met $\alpha^p - \alpha \in K$.*

Bewijs. Schrijf $G = \mathrm{Gal}(L/K)$. Wegens het lemma van Artin–Dedekind is er een $x \in L$ met

$$\mathrm{Tr}(x) = \sum_{\sigma\in G} \sigma(x) \neq 0.$$

In het bijzonder is er dus een $x \in L$ met $\mathrm{Tr}(x) = 1$. Zij σ nu een voortbrenger van G, en definieer

$$\alpha := \sum_{k=0}^{p-1} k\sigma^k(x).$$

Er geldt $\sigma(\alpha) = \alpha - \mathrm{Tr}(x) = \alpha - 1$, en uit de gelijkheid

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p - \alpha,$$

volgt dat $\alpha^p - \alpha$ in het invariantenlichaam K van σ zit. Herhaald σ toepassen geeft $\sigma^k(\alpha) = \alpha - k$, dus de ondergroep van $\mathrm{Gal}(L/K)$ van machten van σ die α vasthouden is de triviale ondergroep, en er geldt $L = K(\alpha)$. □

Artin–Schreiertheorie laat zien dat in karakteristiek p elke cyclische uitbreiding van graad p ontstaat door een nulpunt te adjungeren van een *Artin–Schreierpolynoom*:[3] een (separabel) polynoom van de vorm $X^p - X - a$, met $a \in K$. Het volgende lemma laat hiermee zien dat een lichaam K met een separabele afsluiting van priemgraad p over K niet karakteristiek p heeft.

[3] P. STEVENHAGEN. *Algebra 3*. http://websites.math.leidenuniv.nl/algebra/algebra3.pdf, 2011

9 LEMMA. *Stel dat K een lichaam van karakteristiek $p > 0$ is en $L = K(\alpha)$ een uitbreiding met $\alpha \notin K$ een nulpunt van een Artin–Schreierpolynoom over K. Dan is L niet separabel afgesloten.*

Bewijs. Stel dat L wél separabel afgesloten is, en zij $G = \mathrm{Gal}(L/K)$. Wegens het lemma van Artin–Dedekind is de spoorafbeelding $\mathrm{Tr}\colon L \to K$ gegeven door

$$\mathrm{Tr}(x) = \sum_{\sigma \in G} \sigma(x)$$

niet de nulafbeelding, en dus surjectief. In karakteristiek p is de p-demachtsverheffing additief (de afbeelding $F\colon x \mapsto x^p$ is het *Frobeniusendomorfisme*), dus er geldt

$$\mathrm{Tr}(x^p - x) = \mathrm{Tr}(x)^p - \mathrm{Tr}(x),$$

en het diagram rechts commuteert.

$$\begin{array}{ccc} L & \xrightarrow{F-1} & L \\ \downarrow{\scriptstyle \mathrm{Tr}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ K & \xrightarrow{F-1} & K \end{array}$$

De afbeelding $F - 1\colon x \mapsto x^p - x$ is surjectief omdat L separabel afgesloten is, dus de samenstelling bovenlangs in het diagram is als compositie van surjecties weer surjectief. Wegens de commutativiteit van het diagram moet de compositie onderlangs ook surjectief zijn, maar dit is in tegenspraak met het feit dat $X^p - X - a$ geen nulpunten heeft in K. De uitbreiding L is dus niet separabel afgesloten. □

10 LEMMA. *Als K een lichaam is en K^{sep} een separabele afsluiting van K met $[K^{\mathrm{sep}}\colon K]$ een priemgetal, dan geldt $K^{\mathrm{sep}} = K(i)$, met $i^2 = -1$.*

Bewijs. Omdat de graad van de Galoisuitbreiding K^{sep}/K een priemgetal p is, is de uitbreiding K^{sep}/K cyclisch. Wegens lemma's 8 en 9 is elke p-degraads uitbreiding van een lichaam van karakteristiek p niet separabel afgesloten, dus de karakteristiek van K^{sep} is niet gelijk aan p. Het polynoom $X^p - 1$ is dus separabel, en heeft een nulpunt ζ in K^{sep} ongelijk aan 1. Deze ζ is ook een nulpunt van het polynoom

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1$$

dus er geldt $[K(\zeta) : K] \leq p - 1$. Wegens de multiplicativiteit van de graad is $[K(\zeta) : K]$ een deler van $[K^{\mathrm{sep}} : K] = p$, dus er geldt $[K(\zeta) : K] = 1$ en ζ zit in K. Omdat K^{sep}/K een cyclische uitbreiding van graad p is en K een primitieve p-de eenheidswortel bevat, volgt uit Kummertheorie nu dat $K^{\mathrm{sep}} = K(\gamma)$ geldt, met $\gamma^p \in K$.

Zij nu $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ en beschouw de normafbeelding

$$\begin{aligned} N\colon K^{\mathrm{sep}} &\to K \\ x &\mapsto \prod_{\sigma \in G} \sigma(x). \end{aligned}$$

Met behulp van het isomorfisme uit stelling 7 volgt nu

$$N(\gamma) = \prod_{k \in \mathbf{Z}/p\mathbf{Z}} \sigma_k(\gamma) = \begin{cases} -\gamma^p & \text{in het geval } p = 2 \\ \gamma^p & \text{anders.} \end{cases}$$

In het geval $p > 2$ is de inverse van een p-de eenheidswortel ξ een eenheidswortel ongelijk aan ξ. De enige tweede eenheidswortels zijn ± 1.

Omdat γ in K^{sep} een p-de macht is en de normafbeelding multiplicatief geldt er $N(\gamma) = \alpha^p$, met $\alpha \in K$ de norm van een p-demachtswortel van γ.

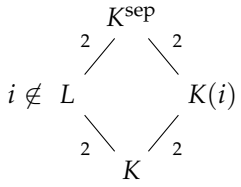
Stel nu dat $p > 2$ geldt. Dan geldt $\alpha^p = \gamma^p$, dus γ/α is een p-de eenheidswortel. Omdat K echter alle p-de eenheidswortels bevat, moet γ ook in K zitten, wat in strijd is met $K \neq K^{\text{sep}}$. Er geldt dus $p = 2$, $(\gamma/\alpha)^2 = -1$ en $K^{\text{sep}} = K(\gamma/\alpha)$. □

Bewijs van stelling 4. Zij $G = \text{Gal}(K^{\text{sep}}/K)$. Dan geldt

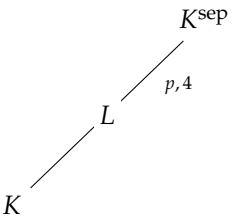
$$[K^{\text{sep}} : K] = \#G.$$

Als de orde van G een priemgetal p is, dan geeft lemma 10 de gelijkheid $K^{\text{sep}} = K(i)$ met $i^2 = -1$.

Stel nu dat $\#G = 4$ geldt. Dan heeft G een ondergroep van orde 2, die onder de Galoiscorrespondentie correspondeert met een tussenlichaam L met $[K^{\text{sep}} : L] = 2$. Er geldt dus $K^{\text{sep}} = L(i)$ met $i^2 = -1$. In het bijzonder geldt $i \notin K$, dus door i aan K te adjungeren ontstaat een deellichaam $K(i)$ van graad 2 over K. De graad van K^{sep} over $K(i)$ is dus ook twee, maar dit is in tegenspraak met $i \in K(i)$. De orde van G is dus niet 4.



Stel tenslotte dat $\#G > 2$ geldt. Dan is $\#G$ deelbaar door een oneven priemgetal p of 4. Omdat er voor elke priemmachtdeler van $\#G$ een ondergroep van die orde is, heeft G een ondergroep van orde p of 4. Onder de Galoiscorrespondentie correspondeert deze met een tussenlichaam L van K^{sep}/K met $[K^{\text{sep}} : L] = p$ of $[K^{\text{sep}} : L] = 4$, maar dat is in tegenspraak met de eerdere opmerkingen. Er geldt dus $\#G = 2$, en $K^{\text{sep}} = K(i)$ met $i^2 = -1$. □



De hoofdstelling van de algebra

De *hoofdstelling van de algebra* is de uitspraak dat elk niet-constant polynoom over $\mathbf{C}$ een nulpunt in $\mathbf{C}$ heeft, en dus dat $\mathbf{C}$ een algebraisch afgesloten lichaam is. Een Galoistheoretisch bewijs voor deze stelling (zoals bijvoorbeeld in het dictaat Algebra III[4]) kan volstaan met het feit dat $\mathbf{R}$ een reëel afgesloten lichaam is.

[4] P. Stevenhagen. *Algebra 3*. http://websites.math.leidenuniv.nl/algebra/algebra3.pdf, 2011

11 Lemma. *Een kwadratische uitbreiding L/K met* $\text{char}\, K \neq 2$ *is slechts dan in te bedden in een cyclische uitbreiding M/K van graad* 4 *als L een element bevat van norm -1 in L.*

Bewijs. Stel dat M een cyclische uitbreiding van graad 4 is en L een tussenlichaam van M/K van graad 2 over K. Wegens Kummertheorie (stelling 7) geldt er $M = L(\alpha)$ met $\alpha^2 \in L$. Schrijf nu $\text{Gal}(M/K) = \langle \sigma \rangle$ en $\beta = \sigma(\alpha)/\alpha$. Er geldt $\sigma^2(\alpha) = -\alpha$, en β zit in $L = M^{\langle \sigma^2 \rangle}$ wegens $\sigma^2(\beta) = -\sigma(\alpha)/(-\alpha) = \beta$. De norm $\beta\sigma(\beta)$ van β in L is wegens $\sigma(\beta) = -\alpha/\sigma(\alpha) = -1/\beta$ gelijk aan -1. □

12 STELLING. *Als K een reëel afgesloten lichaam is, dan is het uitbreidingslichaam $K(i)$ met $i^2 = -1$ algebraïsch afgesloten.*

Bewijs. Omdat de norm van een element in $K(i)/K$ een som van twee kwadraten in K is, is het voldoende aan te tonen dat iedere niet-triviale eindige uitbreiding $L/K(i)$ een tussenlichaam heeft dat cyclisch van graad 4 is over K. Uit lemma 11 volgt dan dat -1 een som van twee kwadraten in K is, wat niet mogelijk is als K reëel afgesloten is.

Stel dus dat $L/K(i)$ een eindige uitbreiding is, en M de normale afsluiting van L over K; dan is M/K eindig Galois. De groep $G = \mathrm{Gal}(M/K)$ heeft een Sylow-2-ondergroep H (wegens de stelling van LAGRANGE van oneven index in G), dus het invariantenlichaam M^H heeft oneven graad over K. Omdat elk polynoom over K van oneven graad een nulpunt heeft in K geldt er $M^H = K$ en $G = H$, dus G is een 2-groep.

De ondergroep $\mathrm{Gal}(M/K(i))$ is dus ook een 2-groep van orde $n = [M\colon K(i)]$. Geldt er $n > 1$, dan heeft $\mathrm{Gal}(M/K(i))$ een ondergroep van index 2, en $M/K(i)$ dus een tussenlichaam E van graad 2 over $K(i)$. De uitbreiding E/K is Galois van graad 4, en wegens Kummertheorie is elk tussenlichaam van E/K van graad 2 over K van de vorm $K(\alpha)$ met $\alpha^2 \in K$. Omdat K reëel afgesloten is zit α of $i\alpha$ in K, dus er geldt $K(\alpha) = K(i)$, en E/K heeft slechts één tussenlichaam van graad 2 over K. De Galoisgroep van E/K heeft dus slechts één ondergroep van index 2, en is niet een viergroep van KLEIN maar cyclisch van orde 4, in tegenspraak met lemma 11.□

Reële lichamen en reële afsluitingen

Tenslotte nog een karakterisatie van reëel afgesloten lichamen die verklaart in welke zin reëel afgesloten lichamen 'afgesloten' zijn.

13 DEFINITIE. Een lichaam K heet *reëel* als -1 geen som van kwadraten in K is. Een *reële afsluiting* van het lichaam K is een algebraïsche uitbreiding L/K met L reëel afgesloten. «

De term 'reëel afgesloten' is een verkorting van het preciezere 'reeel-algebraïsch afgesloten', in de zin van een lichaam dat voldoet aan uitspraak 2 in propositie 14.

14 PROPOSITIE. *Voor een lichaam K zijn equivalent:*

1. *K is reëel afgesloten;*
2. *K is reëel en er is geen echte algebraïsche uitbreiding L/K met L reëel.*

Voor het bewijs van propositie 14 is het handig te weten welke primitieve uitbreidingen van K reëel zijn.

15 LEMMA. *Stel dat K een reëel lichaam is en $L = K(\alpha)$ een uitbreidingslichaam met $\alpha \notin K$.*

1. *Als α transcendent is over K, dan is L reëel.*
2. *Is $K(\alpha)$ van oneven graad over K, dan is L reëel.*
3. *Is $a = \alpha^2$ een element van K, dan is $K(\alpha)$ precies dan reëel als $-a$ geen som van kwadraten is in K.*

Bewijs. Stel dat α transcendent is over K en dat $K(\alpha)$ niet reëel is. Dan bestaan er $p_1, \ldots, p_n, q_1, \ldots, q_n \in K[\alpha]$ met

$$-1 = \left(\frac{p_1}{q_1}\right)^2 + \cdots + \left(\frac{p_n}{q_n}\right)^2.$$

Door te evalueren in een element $x \in K$ dat geen nulpunt is van de noemers (K is immers oneindig) volgt dan in strijd met de aannamen dat K niet reëel is.

Stel nu dat $K(\alpha)$ niet reëel is en oneven graad m heeft over K, en neem zonder verlies van algemeenheid aan dat er geen uitbreiding E/K bestaat met E niet reëel en $1 < [E\colon K] < m$. Er bestaan polynomen $g_1, \ldots, g_n \in K[X]$ van graad hoogstens $m-1$ zodat voldaan is aan

$$-1 = \sum_{k=1}^{n} g_k(\alpha)^2.$$

Omdat de kern van de evaluatieafbeelding $K[X] \to K[\alpha] = L$ wordt voortgebracht door het minimumpolynoom f_K^α van α over K en K reëel is, bestaat er een $h \in K[X]$ zonder lineaire factoren (dus zonder nulpunten) met

$$1 + \sum_{k=1}^{n} g_k^2 = h \cdot f_K^\alpha.$$

Omdat de g_k graad hoogstens $m-1$ hebben geldt $\deg h < m$, en omdat de graad van het linkerlid even is en de graad van f_K^α oneven moet $\deg h > 0$ ook oneven zijn. Omdat h geen nulpunten heeft, ontstaat door een nulpunt η van h te adjungeren een uitbreiding van K van oneven graad $[K(\eta)\colon K] < [K(\alpha)\colon K] = m$ met $-1 = \sum_{k=1}^{n} g_k(\eta)^2$. Omdat K reëel is geldt er $[K(\eta)\colon K] > 1$, en dus $1 < [K(\eta)\colon K] < m$, in tegenspraak met de aanname over m.

Stel nu dat $a := \alpha^2$ in K zit. Is $K(\alpha)$ niet reëel, dan zijn er elementen $x_1, \ldots, x_n, y_1, \ldots, y_n \in K$ met

$$\begin{aligned} -1 &= \sum_{i=1}^{n} (x_i + y_i\alpha)^2 \\ &= \sum_{i=1}^{n} (x_i^2 + 2x_i y_y \alpha + y_i^2 a). \end{aligned}$$

Wegens $K(\alpha) = K \oplus K\alpha$ als K-vectorruimte geldt er

$$-1 = \sum_{i=1}^{n} x_i^2 + a \sum_{i=1}^{n} y_i^2$$

en dus

$$-a = \frac{1 + \sum_{i=1}^{n} x_i^2}{\sum_{i=1}^{n} y_i^2}.$$

Een quotiënt van sommen van kwadraten is echter weer een som van kwadraten (voor alle $a, b \in K$ geldt immers $a/b = ab(b^{-1})^2$), dus omdat K reëel is geeft dit een tegenspraak.

Stel nu voor de omkering dat $K(\alpha)$ reëel is en $-a$ een som van kwadraten. Dan is ook $-1 = -a/a = -\alpha^2/\alpha^2$ een som van kwadraten, in tegenspraak met de aanname dat $K(\alpha)$ een reëel lichaam is. □

Bewijs van propositie 14. Stel dat K een reëel afgesloten lichaam is en L/K een algebraïsche uitbreiding met $L \neq K$. Dan geldt $L = K(i)$ met $i^2 = -1$, dus L is niet reëel.

Stel nu omgekeerd dat K reëel is en geen echte reële algebraïsche uitbreidingen heeft. Wegens lemma 15 heeft ieder polynoom over K van oneven graad dan een nulpunt in K, en voor iedere $x \in K$ is x of $-x$ een kwadraat in K, dus K is reëel afgesloten. □

16 GEVOLG. *Voor elk reëel lichaam K en elke algebraïsche afsluiting $\overline{K}/K$ is er een reële afsluiting K^{re} van K in $\overline{K}$ met $\overline{K} = K^{\mathrm{re}}(i)$.*

Bewijs. Wegens het lemma van Zorn is er een maximaal reëel tussenlichaam K^{re} van $\overline{K}/K$, en dit is reëel afgesloten wegens propositie 14. □

Uit het niet-constructieve argument in gevolg 16 volgt echter niet dat een reële afsluiting binnen een algebraïsche afsluiting uniek is. Inderdaad zijn er soms meerdere op K-isomorfie na inequivalente afsluitingen mogelijk.

17 VOORBEELD. Het lichaam $K = \mathbf{Q}(t)$ dat ontstaat door een transcendent t aan $\mathbf{Q}$ te adjungeren is wegens propositie 15 reëel. Neem uitbreidingen $K_1 = K(\sqrt{t})$ en $K_2 = K(\sqrt{-t})$. De lichamen K_1 en K_2 zijn als zuiver transcendente uitbreidingen van $\mathbf{Q}$ van transcendentiegraad 1 over $\mathbf{Q}$ isomorf met K en dus ook reëel. Wegens gevolg 16 zijn er reële afsluitingen K_1^{re} en K_2^{re} van K met $K_1 \subset K_1^{\mathrm{re}}$ en $K_2 \subset K_2^{\mathrm{re}}$. Het element $t \in K$ is een kwadraat in K_1^{re}, maar niet in K_2^{re}, dus K_1^{re} en K_2^{re} zijn niet K-isomorf.

Binnen een *reëel* afgesloten lichaam R heeft een deellichaam K echter precies één reële afsluting.

18 PROPOSITIE. *Stel dat R/K een lichaamsuitbreiding is met R reëel afgesloten. Dan is de algebraïsche afsluiting K^{alg} van K in R de unieke reële afsluiting van K tussen K en R.*

Bewijs. Het lichaam K^{alg} is reëel, voor alle $x \in K^{\mathrm{alg}}$ is x of $-x$ een kwadraat in R (en dus ook in K^{alg}) en elk polynoom $f \in K^{\mathrm{alg}}$ van oneven graad heeft een nulpunt in R (en dus ook in K^{alg}), dus K^{alg} is reëel afgesloten. Is L een reëel afgesloten tussenlichaam van R/K dat algebraïsch is over K, dan is L bevat in K^{alg}, en uit propositie 14 volgt $L = K^{\mathrm{alg}}$. □

Voor een concrete transcendent $t \in \mathbf{R}$ over $\mathbf{Q}$ is er dus slechts één reële afsluiting van $\mathbf{Q}(t)$ mogelijk binnen $\mathbf{R}$. In tegenstelling tot in voorbeeld 17 is het hier niet mogelijk te kiezen of t of $-t$ een kwadraat wordt: slechts de *positieve* van de twee is een kwadraat in de reële afsluiting, omdat kwadraten in $\mathbf{R}$ niet-negatief zijn.

In het volgende hoofdstuk blijkt dat deze aanpak in volle algemeenheid werkt: voor elk reëel lichaam K met een geschikte *ordening* is er op K-isomorfie na slechts één reële afsluiting mogelijk waarin de kwadraten niet-negatief zijn.

2 *Geordende lichamen*

De theorie van geordende lichamen is standaard; zie bijvoorbeeld Lang of Van der Waerden.

S. Lang. *Algebra.* Springer, 3de editie, 2002

B.L. van der Waerden. *Algebra.* Springer, 9de editie, 1993

19 Definities. Een *lineaire ordening* op een verzameling X is een transitieve relatie $<$ zodat voor alle $x, y \in X$ precies één van de volgende uitspraken geldt:

$$x < y, \qquad x = y, \qquad \text{of} \qquad x > y.$$

Een *geordend lichaam* is een lichaam K voorzien van een lineaire ordening $<$ op de onderliggende verzameling van K zodat aan de volgende eisen is voldaan.

1. Voor alle $a, b, c \in K$ met $a < b$ geldt $a + c < b + c$.
2. Voor alle $a, b \in K$ met $a, b > 0$ geldt $ab > 0$.

Elementen $x \in K$ met $x > 0$ heten *positief;* elementen met $x < 0$ (en dus $-x > 0$) heten *negatief*. De *absolute waarde* $|x|$ van $x \in K$ is het unieke niet-negatieve element van $\{x, -x\}$.

Een *uitbreiding* K/L van geordende lichamen is een uitbreiding van de onderliggende lichamen zodat de inclusieafbeelding $K \hookrightarrow L$ ordebewarend is. «

Standaardvoorbeelden van geordende lichamen zijn $\mathbf{Q}$ en $\mathbf{R}$, en ook elk deellichaam van een geordend lichaam is, uitgerust met de geïnduceerde ordening, een geordend lichaam. Geordende lichamen hebben noodzakelijkerwijs karakteristiek 0.

Omdat het mogelijk is ongelijkheden te transleren (er geldt $y > x$ precies als $y - x > 0$ geldt) is een geordend lichaam ook vast te leggen door te specificeren welke elementen positief zijn.

20 Definitie. Stel dat K een lichaam is. Een *positive verzameling in* K is een deelverzameling P van K die aan de volgende eisen voldoet.

1. Voor $x, y \in P$ geldt $x + y \in P$ en $xy \in P$.
2. Voor alle $x \in K$ geldt precies één van de volgende uitspraken:

$$x \in P, \qquad x = 0 \qquad \text{of} \qquad -x \in P.$$ «

21 Propositie. *Stel dat K een lichaam is. Een deelverzameling P van K is een positieve verzameling in K precies als de relatie $<$ gegeven door*

$$x < y \iff y - x \in P$$

een lineaire ordening is die K tot een geordend lichaam maakt.

Bewijs. Stel dat P een positieve verzameling is en x, y en z elementen van K. Geldt er $x < y < z$, dan geldt er $z - x = (z - y) + (y - x) \in P$ en dus $x < z$, dus de relatie $<$ is transitief. Uit $x, y > 0$ volgt $xy > 0$, en geldt er $x < y$, dan volgt uit $(y - z) - (x - z) = y - x \in P$ ook $x + z < y + z$. Uit het feit dat K de disjuncte vereniging van P, $-P$ en $\{0\}$ is volgt dat $<$ voldoet aan de trichotomie-eigenschap, dus de relatie $<$ is een lineaire ordening die K tot een geordend lichaam maakt.

Stel omgekeerd dat K uitgerust met $<$ een geordend lichaam is. Duidelijk is P gesloten onder vermenigvuldiging, en voor $x, y > 0$ geldt $x + y > x + 0 > 0 + 0 = 0$, dus P is ook gesloten onder optelling. Uit de trichotomie-eigenschap volgt dat voor alle $x \neq 0$ óf $x > 0$ óf $-x > 0$ geldt, dus P is een positieve verzameling in K. □

Lichaamsordeningen op een lichaam K corresponderen bijectief met positieve verzamelingen in K langs de constructie in propositie 21.

In geordende lichamen gelden de gebruikelijke ongelijkheden. Zo geldt voor $x \neq 0$ de ongelijkheid $x^2 = (-x)^2 > 0$, aangezien x of $-x$ positief is. Verder is 1 positief: geldt er immers $-1 > 0$, dan volgt uit $1 = (-1)^2 > 0$ een tegenspraak. In het bijzonder is elk geordend lichaam reëel. Ook de driehoeksongelijkheid is waar: voor alle $x, y \in K$ geldt $|x + y| \leq |x| + |y|$.

Reële lichamen en ordeningen

De lichamen die voorkomen als onderliggend lichaam van een geordend lichaam zijn precies de *reële* lichamen.

22 PROPOSITIE. *Voor elk reëel lichaam K is er minstens één positieve verzameling in K.*

Bewijs. De niet-lege sommen van kwadraten van eenheden in K vormen een ondergroep van K^* die gesloten is onder optelling; immers, een quotiënt van sommen van kwadraten van eenheden is wegens $a/b = ab(b^{-1})^2$ weer een som van kwadraten, en is 0 een som van kwadraten van eenheden, dan is er een element $x \in K$ zodat zowel x als $-x$ sommen van kwadraten zijn, en $-1 = -x/x$ dus ook, in tegenspraak met de aanname dat K reëel is.

Wegens het lemma van ZORN is er dus een maximale ondergroep P van de eenhedengroep K^* van K die gesloten is onder optelling en de kwadraten van eenheden bevat. Om aan te tonen dat P een positieve verzameling is, is het voldoende te laten zien dat voor alle $x \in K$ ten minste één van x en $-x$ in P zit; zitten zowel x als $-x$ immers in P, dan zit $0 = x + (-x)$ in P, in tegenspraak met de aanname dat P een ondergroep van de eenhedengroep is.

Stel dus dat x niet is bevat in P. De verzameling $P' = \{x \cdot \alpha + \beta \colon \alpha, \beta \in P\}$ bevat de kwadraten, is gesloten onder optelling en vermenigvuldiging, en voor alle $y \in K^*$ met $y \in P'$ zit $y^{-1} = y(y^{-1})^2$ ook in P'. Uit de maximaliteit van P volgt echter dat P' geen ondergroep van K^* kan zijn, dus er geldt $0 \in P'$. Er zijn dus $\alpha, \beta \in P$ met $x \cdot \alpha + \beta = 0$, en er geldt $-x = \beta/\alpha \in P$. □

In een geordend lichaam K zijn de sommen van kwadraten in K altijd positief. De omkering is ook waar: is x een element van K een reëel lichaam dat positief is volgens elke ordening van K, dan is x een som van kwadraten.

23 GEVOLG. *Is K een reëel lichaam en $x \in K$ een element dat geen som van kwadraten in K is, dan is er een positieve verzameling P in K met $-x \in P$.*

Bewijs. Wegens propositie 15 is voor elk element $x \in K$ dat geen som van kwadraten is het lichaam $K(\sqrt{-x})$ reëel. Uit propositie 22 volgt dat er dan een positieve verzameling P bestaat in $K(\sqrt{-x})$ met $-x \in P$. De doorsnede $K \cap P$ is weer een positieve verzameling in K. □

Gevolg 23 geeft een aanwijzing voor de oplossing van het zeventiende probleem van HILBERT: elke niet-negatieve rationale functie over $\mathbf{R}$ is een som van kwadraten van rationale functies (zie stelling 42 in hoofdstuk 3).

24 STELLING. *Is K een reëel afgesloten lichaam, dan is K^{*2} de unieke positieve verzameling in K.*

Bewijs. Omdat er geen niet-triviale inclusies mogelijk zijn tussen positieve verzamelingen (voor elke $x \in K$ is of x of $-x$ namelijk positief) volstaat het te bewijzen dat K^{*2} zelf een positieve verzameling is.

Een som van kwadraten in K is weer een kwadraat (lemma 3), en een product van kwadraten is ook weer een kwadraat. Voor elke $x \in K$ is (per definitie) x of $-x$ een kwadraat. Geldt er $x \neq 0$, dan zijn x en $-x$ niet beide kwadraten: het element x^{-1} is dan immers ook een kwadraat, en er geldt $-1 = -x \cdot x^{-1}$. De kwadraten in K vormen dus een positieve verzameling K^{*2}. □

Het is mogelijk bij een geordend lichaam K een reële afsluiting K^{re} van het onderliggende lichaam te vinden zodat K^{re}/K een uitbreiding van geordende lichamen is.

25 STELLING. *Als K een geordend lichaam is, dan is er uitbreiding K^{re}/K van geordende lichamen met K^{re} reëel afgesloten.*

Wegens stelling 22 volstaat het een reële uitbreiding van K te vinden waarin de positieve elementen van K kwadraten zijn.

26 PROPOSITIE. *Stel dat K een geordend lichaam is met positieve verzameling P. Dan is $K(\sqrt{P})$ reëel.*

Bewijs. Het volstaat aan te tonen dat voor alle $n > 0$ de vergelijking

$$-1 = \sum_{i=1}^{n} x_i \alpha_i^2$$

met $x_1, \ldots, x_n \in P$ géén oplossingen $(\alpha_1, \ldots, \alpha_n)$ heeft in een *eindige* uitbreiding $K(\sqrt{a_1}, \ldots, \sqrt{a_r})$ met $a_1, \ldots, a_r \in P$.

Stel dus dat $r > 0$ het kleinste natuurlijke getal is waarvoor er $a_1, \ldots, a_r \in P$ en $x_1, \ldots, x_n \in P$ zijn zodat de vergelijking

$$-1 = \sum_{i=1}^{n} x_i \alpha_i^2$$

een oplossing $(\alpha_1, \ldots, a_n)$ heeft in $K(\sqrt{a_1}, \ldots, \sqrt{a_r})$.

Schrijf $L = K(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$. Iedere α_i is als element van de kwadratische uitbreiding $L(\sqrt{a_r}) = K(\sqrt{a_1}, \ldots, \sqrt{a_r})$ van de vorm $\alpha_i = A_i + \sqrt{a_r} B_i$ met $A_i, B_i \in L$, en er geldt

$$\begin{aligned} -1 &= \sum_{i=1}^{n} x_i (A_i + \sqrt{a_r} B_i)^2 \\ &= \sum_{i=1}^{n} x_i (A_i^2 + a_r B_i^2 + 2\sqrt{a_r} A_i B_i). \end{aligned}$$

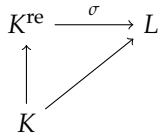
Uit $\sqrt{a_r} \notin L = K(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$ volgt dus

$$-1 = \sum_{i=1}^{n} x_i A_i^2 + \sum_{i=1}^{n} a_r B_i^2,$$

in tegenspraak met de minimaliteit van r. □

Reële nulpunten van polynomen

27 STELLING. *Stel dat L/K een uitbreiding van geordende lichamen is met L reëel afgesloten, en K^{re}/K een reële afsluiting van geordende lichamen. Dan is er een unieke inbedding van geordende lichamen $\sigma\colon K^{\mathrm{re}} \hookrightarrow L$ zodat het diagram rechts commuteert.*



In het bijzonder is de reële afsluiting van een geordend lichaam op een *uniek* ordebewarend K-isomorfisme na uniek.

Het argument van ARTIN en SCHREIER voor de uniciteit van de reële afsluiting gebruikt de stelling van STURM om het aantal nulpunten van een polynoom in een interval te tellen.

28 DEFINITIE. Stel dat K een geordend lichaam is en $f \in K[X]$ een polynoom. De *Sturmketen* van f over K is het rijtje polynomen $f_0, f_1, \ldots, f_n \in K[X]$ met $f_0 = f$, $f_1 = f'$ en

$$f_k = q_{k-1} \cdot f_{k-1} - f_{k-2} \quad \text{en} \quad \deg f_k < \deg f_{k-1} \text{ voor } k > 1,$$

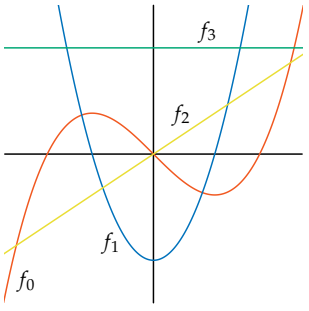
waarbij q_{k-1} het quotiënt en f_k de *tegengestelde* van de rest van f_{k-2} bij deling door f_{k-1} is, en n de eerste index n met $f_n = f_{n+1}$.

De *gereduceerde Sturmketen* van f is het rijtje $f_0/f_n, f_1/f_n, \ldots, f_n/f_n$.

Het *aantal tekenwisselingen* $w(x)$ *bij* $x \in K$ van de Sturmketen $f_1, \ldots, f_n$ is het aantal indices $i \in \{0, 1, \ldots, n\}$ waarvoor er een $j > i$ is met $f_i(x) \cdot f_j(x) < 0$ en $f_k(x) = 0$ voor alle k met $i < k < j$. «

Merk op dat onder het aantal tekenwisselingen dus alleen het aantal overgangen van $+$ naar $-$ of omgekeerd verstaan wordt; tussenliggende tekens 0 tellen niet als een tekenwisseling.

Figuur 1: Het polynoom $X^3 - X$ heeft Sturmketen $X^3 - X$, $3X^2 - 1$, $\frac{2}{3}X$, 1.



x	f_0	f_1	f_2	f_3	$w(x)$
-42	$-$	$+$	$-$	$+$	3
-1	0	$+$	$-$	$+$	2
$-\frac{1}{2}\pi$	$+$	$+$	$-$	$+$	2
$-1/\sqrt{3}$	$+$	0	$-$	$+$	2
$-1/e$	$+$	$-$	$-$	$+$	2
0	0	$-$	0	$+$	2
$1/e$	$-$	$-$	$+$	$+$	1
$1/\sqrt{3}$	$-$	0	$+$	$+$	1
$\frac{1}{2}\pi$	$-$	$+$	$+$	$+$	1
1	0	$+$	$+$	$+$	0
42	$+$	$+$	$+$	$+$	0

29 STELLING VAN STURM. *Stel dat K een reëel afgesloten lichaam is en $f \in K[X]$ een polynoom met Sturmketen $f_0, \ldots, f_n$. Schrijf voor alle $x \in K$ het aantal tekenwisselingen in de Sturmketen van f als $w(x)$.*

Als $a, b \in K$ met $a < b$ geen nulpunten zijn van f, dan is het aantal nulpunten van f in het interval $[a, b]$ gelijk aan $w(a) - w(b)$.

De algoritme voor de berekening van de Sturmketen is een variant op de algoritme van EUCLIDES; het laatste polynoom f_n uit de keten is de ggd van f en f', en dus in het bijzonder nooit het nulpolynoom. Voor het aantal tekenwisselingen maakt het niet uit of er naar de Sturmketen of de gereduceerde Sturmketen van f gekeken wordt; bij elk punt $x \in K$ hebben beide rijtjes evenveel tekenwisselingen. In het geval van een separabel polynoom – en in het bijzonder van een irreducibel polynoom – zijn Sturmketen en gereduceerde Sturmketen hetzelfde.

Om de stelling van STURM te bewijzen zullen we gebruiken dat polynomen over reëel afgesloten lichamen aan de tussenwaardestelling voldoen.

30 TUSSENWAARDESTELLING. *Stel dat K een reëel afgesloten lichaam is en $f \in K[X]$ een polynoom. Als $a, b \in K$ elementen zijn met $a < b$ en $f(a) < 0 < f(b)$, dan is er een $x \in [a, b]$ met $f(x) = 0$.*

De tusenwaardestelling karakteriseert de reëel afgesloten lichamen ook: is K immers een geordend lichaam dat voldoet aan de tussenwaardestelling, dan heeft voor alle $x > 0$ het polynoom $X^2 - x$ een nulpunt, en door af te schatten is te laten zien dat elk polynoom van oneven graad een nulpunt heeft.

Voor het bewijs is slechts het volgende lemma nodig.

31 LEMMA. *Stel dat K een reëel afgesloten lichaam is en $f = X^2 + bX + c \in K[X]$ een monisch polynoom met discriminant $\Delta = b^2 - 4c$. Dan is f irreducibel precies als $\Delta < 0$ geldt, in welk geval er voor alle $x \in K$ voldaan is aan $f(x) > 0$.*

Bewijs. In het geval $\Delta \geq 0$ heeft f een nulpunt vanwege de wortelformule. In het geval $\Delta < 0$ volgt door kwadraatsplitsen

$$\begin{aligned} f(x) &= \left(x + \frac{b}{2}\right)^2 + \left(c - \frac{b^2}{4}\right) \\ &= \left(x + \frac{b}{2}\right)^2 - \frac{\Delta}{4} > 0. \end{aligned}$$

□

Bewijs van de tussenwaardestelling. Schrijf $\alpha_1 < \alpha_2 < \cdots < \alpha_n$ voor de nulpunten van f in K. Dan ontbindt f in irreducibele factoren als

$$f = c \cdot g \cdot \prod_{k=1}^{n} (X - \alpha_k),$$

met $c \in K^*$ en $g \in K[X]$ een product van monische irreducibele kwadratische polynomen. Voor alle $x \in K$ geldt $g(x) > 0$, dus elke tekenwisseling van f is afkomstig van de lineaire factoren. Als er geen index k is met $a < \alpha_k < b$ dan hebben $f(a)$ en $f(b)$ hetzelfde teken, dus er is een nulpunt van f in het interval (a, b). □

32 LEMMA. *Stel dat K een reëel afgesloten lichaam is en $f \in K[X]$ een polynoom met gereduceerde Sturmketen $f_0, f_1, \ldots, f_n$.*

1. *Voor geen enkele $\alpha \in K$ en $k > 0$ geldt $f_k(\alpha) = f_{k+1}(\alpha) = 0$.*
2. *Is $\alpha \in K$ een nulpunt van f_k met $k > 0$, dan geldt er*
$$f_{k-1}(\alpha) f_{k+1}(\alpha) < 0.$$
3. *Is $\alpha \in K$ een nulpunt van f en zijn $a, b \in K$ elementen met $a < \alpha < b$ zodat α het enige nulpunt in $[a, b]$ is van een polynoom f_k, dan hebben $f_0(a)$ en $f_0(b)$ tegengesteld teken, en het teken van $f_0(a)$ is tegengesteld aan dat van $f_1(a)$.*

Bewijs. Stel dat $\alpha \in K$ een nulpunt is van een polynoom f_k met $k > 0$. Geldt er $f_k(\alpha) = f_{k+1}(\alpha) = 0$, dan volgt uit de betrekking $f_{m+1} = q \cdot f_m - f_{m-1}$ inductief dat $f_m(\alpha) = 0$ geldt voor alle $m \geq k$, in tegenspraak met het feit dat f_n een constante ongelijk aan 0 is. Er geldt dus $f_{k+1}(\alpha) \neq 0$, en uit $f_{k+1} = q \cdot f_k - f_{k-1}$ volgt dat $f_{k+1}(\alpha)$ en $f_{k-1}(\alpha)$ tegengesteld teken hebben.

Stel nu dat $\alpha \in K$ een nulpunt van f is en $a, b \in K$ elementen zijn met $a < \alpha < b$ zodat α het enige nulpunt in $[a, b]$ is van een polynoom in de gereduceerde Sturmketen. Als α een nulpunt is van f van multipliciteit m, dan geldt er

$$f_0 = (X - \alpha) \cdot g$$
$$f_1 = m \cdot g + (X - \alpha) \cdot g'$$

met $g \in K[X]$ een polynoom zonder nulpunten in $[a, b]$. Het teken van f_1 op het interval $[a, b]$ is wegens de tussenwaardestelling gelijk aan het teken van $g(\alpha)$, terwijl het teken van $f_1 = (X - \alpha) \cdot g$ op $[a, \alpha)$ tegengesteld is aan het teken van f_1 op $(\alpha, b]$, dat gelijk is aan dat van $g(\alpha)$. □

Bewijs van de stelling van Sturm. Schrijf $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ voor de nulpunten van alle polynomen in de gereduceerde Sturmketen $f_0, f_1, \ldots, f_n$. Wegens de tussenwaardestelling is $w(x)$ constant op de open intervallen (α_k, α_{k+1}). Het volstaat dus aan te tonen dat $w(a) - w(b) = 1$ geldt voor alle $a, b \in K$ met $a < b$ die geen nulpunt van een polynoom f_k zijn zodat er precies één nulpunt α van een polynoom in de gereduceerde Sturmketen bestaat met $a < \alpha < b$.

Stel dus dat $a, b \in K$ elementen zijn die geen nulpunt zijn van een polynoom in de Sturmketen zodat er precies één $\alpha \in K$ is met $a < \alpha < b$ die nulpunt is van een polynoom f_k. Voor alle $k > 0$ met $f_k(\alpha) = 0$ hebben $f_{k-1}(\alpha)$ en $f_{k+1}(\alpha)$ wegens lemma 32 tegengesteld teken, en wegens de tussenwaardestelling hebben ook $f_{k-1}(x)$ en $f_{k+1}(x)$ tegengesteld teken voor alle $x \in [a, b]$. Het aantal tekenwisselingen in het rijtje

$$f_1(x), f_2(x), \ldots, f_n(x)$$

is dus hetzelfde voor alle $x \in [a, b]$ Als α geen nulpunt is van f_0, dan is het aantal tekenwisselingen $w(x)$ dus constant op $[a, b]$.

Stel nu dat α wel een nulpunt is van f_0. Wegens lemma 32 hebben $f_0(a)$ en $f_0(b)$ dan tegengesteld teken, en het teken van $f_0(a)$ is tegengesteld aan dat van $f_1(a)$. Het aantal tekenwisselingen bij a is dus één meer dan bij b, en er geldt $w(a) - w(b) = 1$. □

33 LEMMA. *Stel dat K een geordend lichaam is, $f \in K[X]$ een polynoom. Dan heeft f in elke reële afsluiting van K evenveel nulpunten.*

Bewijs. Schrijf $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Het volstaat aan te tonen dat elk nulpunt α van f in een uitbreiding L/K van geordende lichamen voldoet aan $|\alpha| < M$, met

$$M = 1 + |a_{n-1}| + \cdots + |a_0|.$$

Immers, elk nulpunt van f in een reële afsluiting L/K ligt dan in het interval $(-M, M)$, en het aantal nulpunten $w(-M) - w(M)$ van f in L hangt slechts af van het aantal tekenwisselingen $w(\cdot)$ van de Sturmketen van f over K.

Stel dus dat α een nulpunt van f in een uitbreiding L/K van geordende lichamen is. De ongelijkheid volgt meteen als $|\alpha| \leq 1$ geldt. Geldt er $|\alpha| > 1$, dan volgt uit de driehoeksongelijkheid

$$|\alpha|^n \leq |a_{n-1}||\alpha|^{n-1} + |a_{n-2}||\alpha|^{n-2} + \cdots + |a_0|.$$

Delen door $|\alpha|^{n-1}$ geeft

$$\begin{aligned} |\alpha| &\leq |a_{n-1}| + |a_{n-2}||\alpha|^{-1} + \cdots + |a_0||\alpha|^{-(n-1)} \\ &\leq |a_{n-1}| + \cdots + |a_0| < M. \end{aligned}$$ □

Bewijs van stelling 27. Wegens lemma 24 heeft elk polynoom over K evenveel nulpunten in K^{re} als in L. Noteer voor elke $\alpha \in K^{\mathrm{re}}$ de nulpunten van het minimumpolynoom f_K^α in K als $\alpha_1, \alpha_2, \ldots, \alpha_n$ en de nulpunten van f_K^α in L als $\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*$, waarbij de α_i en α_i^* zo geordend zijn dat voldaan is aan

$$\alpha_1 < \alpha_2 < \cdots < \alpha_n \quad \text{en} \quad \alpha_1^* < \alpha_2^* < \cdots < \alpha_n^*.$$

Definieer een afbeelding $\sigma\colon K^{\mathrm{re}} \to L$ door $\sigma(\alpha) = \alpha_k^*$, met k de unieke index k met $\alpha = \alpha_k$. Deze afbeelding is welgedefinieerd: voor elk nulpunt $\beta \in K$ van een monisch irreducibel polynoom $f \in K[X]$ is het minimumpolynoom f_K^β een deler van f, en dus gelijk aan f.

Duidelijk is σ de enige ordebewarende afbeelding $K^{\mathrm{re}} \to L$ die K laat liggen. Omdat er voor alle $\alpha, \beta \in K^{\mathrm{re}}$ een polynoom in $K[X]$ te construeren is dat α, β, $\alpha + \beta$ en $\alpha\beta$ als nulpunten heeft (het product van de minimumpolynomen over K volstaat bijvoorbeeld), is het voldoende aan te tonen dat voor elk polynoom $f \in K[X]$ er een inbedding $\tau\colon E \to L$ over K bestaat van het tussenlichaam E van K^{re}/K voortgebracht door de nulpunten van f in K^{re} met $\tau(\alpha) = \sigma(\alpha)$ voor elk nulpunt α van f.

Stel dus dat E een tussenlichaam van K^{re}/K is voortgebracht door de nulpunten van een polynoom $f \in K[X]$ in K^{re}. Zij M het

tussenlichaam van K^{re}/E dat ontstaat door voor alle nulpunten $x, y \in E$ van f met $x < y$ een element $\delta \in K^{\mathrm{re}}$ met $\delta^2 = y - x$ te adjungeren. Wegens de stelling van het primitieve element is er een $\eta \in M$ met $M = K(\eta)$. Het minimumpolynoom f_K^η van η heeft een nulpunt η^* in L, en er is een K-isomorfisme $\tau\colon K(\eta) \to K(\eta^*)$.

Stel nu dat $x, y \in E$ nulpunten van f zijn. Er geldt precies dan $x < y$ als $y - x$ een kwadraat is in $M = K(\eta)$, en dit is precies als $\tau(y) - \tau(x)$ een kwadraat is in $K(\eta^*)$, dus precies als $\tau(x) < \tau(y)$ geldt. Voor elk nulpunt $\alpha \in E$ van f geldt dus

$$\tau(\alpha_1) < \tau(\alpha_2) < \cdots < \tau(\alpha_n).$$

Omdat σ de unieke ordebewarende afbeelding $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \to L$ is, geldt er $\tau(\alpha) = \sigma(\alpha)$. □

Eerste-orde theorie van reëel afgesloten lichamen

3

Het leven is te kort om alle begrippen uit de eerste-orde logica rigoureus te definiëren – wie echte definities wil hebben, zie bijvoorbeeld het boek van Chang en Keisler.[1]

[1] C.C. Chang en H.J. Keisler. *Model Theory*. North-Holland, 3de editie, 1990

Eerste-orde theorieën

Een *eerste-orde formule in de taal van geordende ringen* is een logische uitdrukking, waarin de ringoperaties, de ordening en de constantes 0 en 1 in mogen voorkomen, en waarin alleen over de elementen van de ring gekwantificeerd wordt.[2] Voorbeelden zijn

$$\forall x\, x^2 > 0, \quad \neg\exists x \exists y\, x^2 + y^2 = -1, \quad \text{en} \quad y \neq 0 \to \exists x\, xy = -1.$$

[2] Er mag dus niet over deelverzamelingen, functies, relaties of natuurlijke getallen gekwantificeerd worden.

Uitdrukkingen die geen eerste-orde formule zijn, zijn bijvoorbeeld

- $\exists A \forall x\, x \notin A$ (kwantificeren over deelverzamelingen mag niet), en
- $\forall a \forall n \exists\, \alpha\ \alpha^n = a$ (kwantificeren over natuurlijke getallen mag niet).

De zojuist beschreven taal is het speciale geval van een *eerste-orde taal* met twee constantesymbolen 0 en 1, tweeplaatsige functiesymbolen $+$ en $\cdot$, een unair functiesymbool $-$ en een relatiesymbool $<$. Door het symbool $<$ weg te laten ontstaat de *taal van ringen*, maar men kan bijvoorbeeld ook nieuwe constantsymbolen toevoegen aan een taal om een grotere taal te krijgen. Een *structuur* X voor een eerste-orde taal L bestaat uit een verzameling X uitgerust met constanten $c \in X$ voor elk constantesymbool c van L, functies $f\colon X^n \to X$ voor elk n-plaatsig functiesymbool f van L en relaties $R \subseteq X^n$ voor elk n-plaatsig relatiesymbool R in L.

Een variabele v die in een formule φ niet door een kwantor $\exists$ of $\forall$ gebonden wordt heet *vrij in* φ. Een formule zonder vrije variabelen heet een *zin*. Van de voorbeeldformules zijn de eerste twee zinnen, de laatste bevat een vrije variabele y. Een verzameling zinnen heet een *theorie*.

Van een zin φ in een taal L is te zeggen of deze *waar* is of niet in een structuur; een structuur X voor L heet een *model* voor een theorie T in L als elke zin $\varphi \in T$ waar is in X. Als elk model van een theorie T ook een model is van de zin ψ, dan heet ψ een *gevolg* van T (notatie: $T \models \psi$).

Voorbeelden van theorieën in de taal van ringen zijn

- de lege theorie,

- de *theorie van ringen*, bestaande uit zinnen die de ringaxioma's uitdrukken (met als modellen precies de ringen),
- de *theorie van lichamen*, bestaand uit de axioma's voor commutatieve ringen en de axioma's $\forall x(x \neq 0 \to \exists y\, xy = 1)$ en $0 \neq 1$, en
- de *theorie van reëel afgesloten lichamen*, die ontstaat door de theorie van lichamen uit te breiden met de zinnen $\neg\exists x \exists y\, x^2 + y^2 = -1$ en

$$\forall x(x \neq 0 \to (\exists y\, y^2 = x \vee \exists y\, y^2 = -x))$$

en, voor alle oneven natuurlijke getallen n, de zin

$$\forall a_0 \ldots \forall a_{n-1} \exists x\, x^n + a_{n-1}x^{n-1} \cdots + a_0 = 0.$$

Voorbeelden van theorieën in de taal van geordende ringen zijn naast de theorieën in de taal van ringen ook

- de *theorie van geordende ringen*, die bestaat uit de theorie van ringen en de axioma's voor de ordening uit hoofdstuk 2, en
- de *theorie van geordende lichamen*, die bestaat uit de theorie van geordende ringen en de lichaamsaxioma's, en
- de *theorie van reëel afgesloten lichamen met ordening*, die bestaat uit de theorie van reëel afgesloten lichamen met de axioma's voor de ordening uit hoofdstuk 2.

Voorbeelden van gevolgen van de theorie van geordende lichamen zijn de zinnen $\forall x\, x^2 \geq 0$ en $\neg\exists x_1 \ldots \exists x_n\, x_1^2 + \cdots + x_n^2 = -1$. Een voorbeeld van een gevolg van de theorie van reëel afgesloten lichamen met ordening is de zin $\forall x(x > 0 \leftrightarrow \exists y(y \neq 0 \wedge y^2 = x))$.

Volledige theorieën en kwantoreliminatie

In een aantal gevallen wordt een eerste-orde theorie T volledig vastgelegd door een enkel model X, in de zin dat de gevolgen van T precies die zinnen zijn die waar zijn in X. Dit geldt altijd voor theorieën van de vorm

$$\operatorname{Th} X \coloneqq \{\varphi : \varphi \text{ is een zin die waar is in } X\},$$

maar er zijn ook minder triviale voorbeelden.

34 PRINCIPE VAN LEFSCHETZ. *Voor elke eerste-orde zin φ in de taal van ringen en elk algebraïsch afgesloten lichaam K van karakteristiek 0 geldt*

$$\varphi \textit{ is waar in } K \iff \varphi \textit{ is waar in } \mathbf{C}.$$

Dit principe is ook modeltheoretischer te formuleren. Een theorie T in een taal L heet *volledig* als voor elke zin φ ófwel $T \models \varphi$ ófwel $T \models \neg\varphi$ geldt. Het principe van LEFSCHETZ zegt dan dat de theorie van algebraïsch afgesloten lichamen van karakteristiek 0 in de taal van ringen een volledige theorie is.

Er is een analoog principe voor reëel afgesloten lichamen.

35 STELLING. *De theorie van reëel afgesloten lichamen is volledig.*

Propositie 34 wordt hier niet bewezen, maar een schets van een bewijs is als volgt. Is T een theorie zonder eindige modellen en κ een oneindig kardinaalgetal groter dan de kardinaliteit van de taal van T zodat alle modellen van T van kardinaliteit κ isomorf zijn, dan stelt de toets van ŁOŚ–VAUGHT dat T een volledige theorie is. Elke twee algebraïsch afgesloten lichamen van karakteristiek 0 en kardinaliteit $\kappa > \aleph_0$ hebben transcendentiegraad κ over $\mathbf{Q}$ en zijn dus isomorf, dus de theorie van algebraïsch afgesloten lichamen van karaktersitiek 0 is volledig.

Deze stelling is voor het eerst door TARSKI bewezen door een algoritme te geven dat voor elke zin φ een bewijs vindt voor ofwel φ ofwel $\neg\varphi$. De theorie van reëel afgesloten lichamen is dus *beslisbaar*. Het is echter ook mogelijk stelling 35 te bewijzen zonder TARSKI's algoritme, aan de hand van een semantische eigenschap van de theorie van reëel afgesloten lichamen.

36 DEFINITIE. Een theorie T in een eerste-orde taal L *laat kwantoreliminatie toe* als er voor elke formule $\varphi(v_1, \ldots, v_n)$ in L een kwantorvrije formule $\psi(v_1, \ldots, v_n)$ in L is (dus met dezelfde vrije variabelen) met

$$T \models \forall v_1 \ldots \forall v_n \, (\varphi(v_1, \ldots, v_n) \leftrightarrow \psi(v_1, \ldots, v_n)).$$

De formule $\psi(v_1, \ldots, v_n)$ in L heet een *kwantorvrij equivalent van* $\varphi(v_1, \ldots, v_n)$ *ten opzichte van* T. «

Een voorbeeld uit de theorie van reëel afgesloten lichamen: de formule

$$\exists x \, ax^2 + bx + c = 0$$

heeft een kwantorvrij equivalent $b^2 - 4ac \geq 0$.

37 STELLING. *De theorie van reëel afgesloten lichamen met ordening laat kwantoreliminatie toe.*

Stelling 35 is een gevolg van stelling 37: in een kwantorvrije zin ψ in de taal van geordende ringen figureren alleen 0, 1, de ringoperaties en $<$, dus ψ is waar in een reëel afgesloten lichaam K met de unieke ordening dan en slechts dan als ψ waar is in de geordende ring $\mathbf{Z}$. Merk op dat het relatiesymbool $<$ hier cruciaal is; de theorie van reëel afgesloten lichamen in de taal van ringen is weliswaar volledig, maar laat geen kwantoreliminatie toe.

38 PROPOSITIE. *Er is geen kwantorvrij equivalent $\psi(x)$ van $\exists y \, y^2 = x$ ten opzichte van de theorie van reëel afgesloten lichamen in de taal van ringen.*

Bewijs. Voor elke kwantorvrije formule $\psi(x)$ in de taal van ringen is de verzameling $P = \{x \in \mathbf{R} \colon \psi(x) \text{ is waar in } \mathbf{R}\}$ een eindige vereniging van verzamelingen van de vorm

$$A = \Big\{ x \in \mathbf{R} \colon \bigwedge_k f_k(x) = 0 \wedge \bigwedge_k g_k(x) \neq 0 \Big\},$$

met $f_1, \ldots, f_n, g_1, \ldots, g_m \in \mathbf{R}[X]$ ongelijk aan 0. In het geval $n > 0$ is A eindig, en anders is $\mathbf{R} \setminus A$ eindig. Ook P of $\mathbf{R} \setminus P$ is dus eindig. Voor $S = \{x \in \mathbf{R} \colon \exists y \, y^2 = x\} = \{x \in \mathbf{R} \colon x \geq 0\}$ is echter S noch $\mathbf{R} \setminus S$ eindig, dus er is geen kwantorvrij equivalent van $\exists y \, y^2 = x$. □

Om aan te tonen dat een theorie T kwantoreliminatie toelaat, is het voldoende te laten zien dat er kwantorvrije equivalenten ten opzichte van T zijn voor formules van een heel eenvoudige vorm.

39 LEMMA. *Stel dat L een eerste-orde taal is en T een theorie in L zodat er voor elke kwantorvrije formule $\theta(w, v_1, \ldots, v_n)$ een kwantorvrije formule $\psi(v_1, \ldots, v_n)$ in L is met*

$$T \models \forall v_1 \ldots \forall v_n (\exists w \; \theta(w, v_1, \ldots, v_n) \leftrightarrow \psi(v_1, \ldots, v_n)).$$

Dan laat T kwantoreliminatie toe.

Bewijs. Elke formule in L is equivalent met een formule die alleen uit atomaire formules, de connectieven $\wedge$ en $\neg$ en de existentiele kwantor $\exists$ bestaat. Het is dus voldoende aan te tonen dat de formules $\varphi_1 \wedge \varphi_2$, $\neg\varphi_1$ en $\exists w\ \varphi_1$ kwantorvrije equivalenten ten opzichte van T hebben in L als φ_1 en φ_2 die hebben – inductief volgt dan dat T kwantoreliminatie toelaat. Zij φ dus een formule in L. Is φ van de vorm $\varphi_1 \wedge \varphi_2$ of $\neg\varphi_1$ met φ_1 en φ_2 equivalent ten opzichte van T met kwantorvrije formules in L, dan is ook φ equivalent ten opzichte van T met een kwantorvrije formule.

Is $\varphi(v_1, \ldots, v_n)$ van de vorm $\exists w\ \theta$, waarbij $\theta(w, v_1, \ldots, v_n)$ een formule is zodat er een kwantorvrije formule $\psi(v_1, \ldots, v_n)$ bestaat met $T \models \forall v_1 \ldots \forall v_n(\exists w\ \theta \leftrightarrow \psi)$, dan is φ equivalent ten opzichte van T met de kwantorvrije formule ψ.

Met inductie volgt nu dat T kwantoreliminatie toelaat. □

Of een formule φ een kwantorvrij equivalent heeft ten opzichte van een theorie T is ook af te lezen aan de modellen van T. Het volgende lemma is een specialisering van een algemene kwantoreliminatietoets,[3,4] die voor het geval van de taal van geordende ringen met weinig machinerie te bewijzen is.

[3] D. MARKER. *Introduction to Model Theory*. In D. HASKELL, A. PILLAY, en C. STEINHORN (red.), *Model theory, algebra, and geometry*, uit de reeks *Mathematical Sciences Research Institute publications*. Cambridge University Press, 2000

[4] L. VAN DEN DRIES. *Alfred Tarski's Elimination Theory for Real Closed Fields*. The Journal of Symbolic Logic, 53(1), pp. 7–19, 1988

40 LEMMA. *Stel dat T een theorie is in de taal van geordende ringen die de theorie van geordende ringen met $0 \neq 1$ omvat en $\varphi(v_1, \ldots, v_n)$ een formule. Dan zijn de volgende uitspraken equivalent.*

1. *Er is een kwantorvrije formule $\psi(v_1, \ldots, v_n)$ in L met*
$$T \models \forall v_1 \ldots \forall v_n(\varphi(v_1, \ldots, v_n) \leftrightarrow \psi(v_1, \ldots, v_n)).$$
2. *Als R_1 en R_2 modellen van T zijn en R een deelring is van zowel R_1 als R_2, dan geldt voor alle $a_1, \ldots, a_n \in R$ de equivalentie*
$$\varphi(a_1, \ldots, a_n) \text{ is waar in } R_1 \iff \varphi(a_1, \ldots, a_n) \text{ is waar in } R_2.$$

Het bewijs maakt gebruik van een fundamentele stelling uit de modeltheorie, de *compactheidsstelling*[5] voor de eerste-orde logica.

[5] C.C. CHANG en H.J. KEISLER. *Model Theory*. North-Holland, 3de editie, 1990

41 COMPACTHEIDSSTELLING. *Stel dat Σ een verzameling zinnen in een taal L is en φ een formule in L. Dan geldt $\Sigma \models \varphi$ dan en slechts dan als er een eindige deelverzameling Σ_0 van Σ is met $\Sigma_0 \models \varphi$.*

Bewijs van lemma 40. Stel dat er een kwantorvrije formule $\psi(v_1, \ldots, v_n)$ is met $T \models \forall v_1 \ldots \forall v_n(\varphi \leftrightarrow \psi)$. Omdat ψ kwantorvrij is, gelden voor alle $a_1, \ldots, a_n \in R$ equivalenties

$$\begin{aligned}\varphi(a_1, \ldots, a_n) \text{ is waar in } R_1 &\iff \psi(a_1, \ldots, a_n) \text{ is waar in } R_1\\ &\iff \psi(a_1, \ldots, a_n) \text{ is waar in } R\\ &\iff \psi(a_1, \ldots, a_n) \text{ is waar in } R_2\\ &\iff \varphi(a_1, \ldots, a_n) \text{ is waar in } R_2.\end{aligned}$$

Stel omgekeerd dat voor alle modellen R_1 en R_2 van T met gezamenlijke deelstructuur R en voor alle $a_1, \ldots, a_n \in R$ voldaan is aan de equivalentie

$$\varphi(a_1, \ldots, a_n) \text{ is waar in } R_1 \iff \varphi(a_1, \ldots, a_n) \text{ is waar in } R_2.$$

Geldt er $T \models \forall v_1 \ldots \forall v_n \, \varphi(v_1, \ldots, v_n)$, dan is $\varphi(v_1, \ldots, v_n)$ equivalent ten opzichte van T met de formule $0 = 0$. Geldt er echter $T \models \forall v_1 \ldots \forall v_n \, \neg\varphi(v_1, \ldots, v_n)$, dan is $\varphi(v_1, \ldots, v_n)$ equivalent ten opzichte van T met de formule $0 \neq 0$. Stel dus dat $\varphi(v_1, \ldots, v_n)$ noch $\neg\varphi(v_1, \ldots, v_n)$ een gevolg is van T.

Zij Γ de verzameling van alle kwantorvrije formules $\psi(v_1, \ldots, v_n)$ in de taal van geordende ringen met

$$T \models \forall v_1 \ldots \forall v_n (\varphi(v_1, \ldots, v_n) \to \psi(v_1, \ldots, v_n)),$$

en definieer voor voor alle polynomen $\tau_1, \ldots, \tau_n$ in de constantesymbolen van de taal en de variabelen $v_1, v_2, \ldots$ en met coëfficienten in $\mathbf{Z}$ de verzameling

$$\Gamma(\tau_1, \ldots, \tau_n) \coloneqq \{\psi(\tau_1, \ldots, \tau_n) \colon \psi(v_1, \ldots, v_n) \in \Gamma\}.$$

Zij L de taal die ontstaat door aan de taal van geordende ringen nieuwe constantesymbolen $t_1, \ldots, t_n$ toe te voegen (één voor elke vrije variabele in φ). Het volstaat aan te tonen dat $T \cup \Gamma(t_1, \ldots, t_n) \models \varphi(t_1, \ldots, t_n)$ geldt. Immers, wegens de compactheidsstelling bestaan er dan $\psi_1, \ldots, \psi_m \in \Gamma(v_1, \ldots, v_n)$ met

$$T \models \forall v_1 \ldots \forall v_n \Big(\bigwedge_k \psi_k(v_1, \ldots, v_n) \to \varphi(v_1, \ldots, v_n) \Big),$$

waaruit volgt dat $\bigwedge_k \psi_k(v_1, \ldots, v_n)$ een kwantorvrij equivalent is van $\varphi(v_1, \ldots, v_n)$ ten opzichte van T.

Stel dus dat $\varphi(t_1, \ldots, t_n)$ géén gevolg is van $T \cup \Gamma(t_1, \ldots, t_n)$, en dat er dus een model R_1 van $T \cup \Gamma(t_1, \ldots, t_n)$ bestaat zodat $\neg\varphi(t_1, \ldots, t_n)$ waar is in R_1. Zij S verder de verzameling van alle kwantorvrije formules $\psi(t_1, \ldots, t_m)$ in L die waar zijn in de deelring $\mathbf{Z}[t_1, \ldots, t_n]$ van R_1.

Neem nu $\Sigma = T \cup S \cup \{\varphi(t_1, \ldots, t_n)\}$. Als Σ inconsistent is, dan bestaan er kwantorvrije formules $\psi_1(v_1, \ldots, v_n), \ldots, \psi_m(v_1, \ldots, v_n)$ in de taal van geordende ringen met $\psi_k(t_1, \ldots, t_n) \in S$ voor alle k en

$$T \models \forall v_1 \ldots \forall v_n \Big(\bigwedge_k \psi_k(v_1, \ldots, v_n) \to \neg\varphi(v_1, \ldots, v_n) \Big).$$

Per contrapositie geldt dan

$$T \models \forall v_1 \ldots \forall v_n \Big(\varphi(t_1, \ldots, t_n) \to \bigvee_k \neg\psi_k(v_1, \ldots, v_n) \Big),$$

waaruit volgt dat $\bigvee_k \neg\psi_k(v_1, \ldots, v_n) \in \Gamma(v_1, \ldots, v_n)$ geldt, dus $\bigvee_k \neg\psi_k(t_1, \ldots, t_n)$ is waar in $\mathbf{Z}[t_1, \ldots, t_n]$, in tegenspraak met het feit dat $\bigwedge_k \psi_k(t_1, \ldots, t_n)$ waar is in $\mathbf{Z}[t_1, \ldots, t_n]$. De verzameling Σ is dus consistent.

Stel nu dat R_2 een model van Σ is. Omdat S alle relaties tussen de elementen t_k bevat, is de deelring $\mathbf{Z}[t_1, \ldots, t_n]$ van R_1 ook als deelring van R_2 op te vatten. Omdat $\neg\varphi(t_1, \ldots, t_n)$ waar is in R_1 volgt dan per aanname dat $\neg\varphi(t_1, \ldots, t_n)$ waar is in R_2, in tegenspraak met de keuze van R_2 als model van $\varphi(t_1, \ldots, t_n)$.

De verzameling $T \cup \Gamma(t_1, \ldots, t_n)$ is dus consistent, waaruit volgt dat φ een kwantorvrij equivalent ten opzichte van T heeft. □

Bewijs van stelling 37. Wegens lemma 39 is het voldoende aan te tonen dat elke formule van de vorm $\exists w\, \varphi(w, v_1, \ldots, v_2)$ met φ kwantorvrij een kwantorvrij equivalent heeft ten opzichte van de theorie van reëel afgesloten lichamen.

Stel dus dat K een reëel afgesloten lichaam is en zij $\mathbf{Q}^{\mathrm{re}}$ de reele afsluiting van $\mathbf{Q}$ in K. Zij $\varphi(w, v_1, \ldots, v_n)$ een kwantorvrije formule is in de taal van geordende lichamen en $a_1, \ldots, a_n \in \mathbf{Q}^{\mathrm{re}}$. Door φ in disjunctieve normaalvorm te brengen[6] is te zien dat er $f_1, \ldots, f_j, g_1, \ldots, g_m \in \mathbf{Q}^{\mathrm{re}}[X]$ zijn zodat $\varphi(w, a_1, \ldots, a_n)$ waar is in K voor alle elementen $w \in K$ met

$$\bigwedge_{k=1}^{j} f_k(w) = 0 \wedge \bigwedge_{k=1}^{m} g_k(w) > 0. \qquad (*)$$

[6] Iedere kwantorvrije formule is equivalent met een disjunctie van conjuncties van atomaire formules. Zo'n conjunctie van atomaire formules is van de vorm $(*)$.

In het geval dat één van de f_k niet het nulpolynoom is zijn alle $w \in K$ waarvoor $\varphi(w, a_1, \ldots, a_n)$ waar is in K algebraïsch over $\mathbf{Q}^{\mathrm{re}}$, en dus bevat in $\mathbf{Q}^{\mathrm{re}}$. In dit geval is de formule $\exists w\, \varphi(w, a_1, \ldots, a_n)$ slechts waar in K als ze waar is in $\mathbf{Q}^{\mathrm{re}}$, en volgt uit lemma 40 dat $\exists w\, \varphi(v_1, \ldots, v_n)$ een kwantorvrij equivalent heeft ten opzichte van de theorie van reëel afgesloten lichamen.

Stel nu dat alle f_k het nulpolynoom zijn. De verzameling U van alle $x \in K$ met $\bigwedge_{k=1}^{m} g_k(x) > 0$ is wegens de tussenwaardestelling een vereniging van open intervallen (α, β) met $\alpha, \beta \in \mathbf{Q}^{\mathrm{re}}$. Stel dus dat α, β elementen van $\mathbf{Q}^{\mathrm{re}}$ zijn met $(\alpha, \beta) \subseteq U$. Dan geldt er

$$\bigwedge_{k=1}^{m} g_k\left(\frac{\alpha+\beta}{2}\right) > 0,$$

dus $\exists w\, \varphi(w, v_1, \ldots, v_n)$ is ook waar in $\mathbf{Q}^{\mathrm{re}}$. Uit lemma 40 volgt nu dat $\exists w\, \varphi(w, v_1, \ldots, v_n)$ ten opzichte van de theorie van reëel afgesloten lichamen een kwantorvrij equivalent $\psi(v_1, \ldots, v_n)$ heeft. □

Het zeventiende probleem van Hilbert

Stelling 37 heeft ook nog de volgende leuke toepassing, een versie van ROBINSON van ARTINS oplossing voor het zeventiende probleem van HILBERT.

42 STELLING. *Elke niet-negatieve rationale functie $f \in K(X_1, \ldots, X_n)$ met K een reëel afgesloten lichaam is een som van kwadraten in $K(X_1, \ldots, X_n)$.*

Bewijs. Stel dat f geen som van kwadraten is in het reële lichaam $K(X_1, \ldots, X_n)$. Wegens gevolgen 23 en 25 is er dan een reële afsluiting $L = K(X_1, \ldots, X_n)^{\mathrm{re}}$ waarin $f = f(X_1, \ldots, X_n)$ negatief is. Schrijf $f(x_1, \ldots, x_n)$ als een quotiënt p/q van polynomen over $\mathbf{Z}[x_1, \ldots, x_n]$ in de coëfficienten $a_1, \ldots, a_k$ van f met $p(a_1, \ldots, a_k)(X_1, \ldots, X_n) < 0 < q(a_1, \ldots, a_k)(X_1, \ldots, X_n)$. Als $\varphi(v_1, \ldots, v_k)$ de formule $\exists x_1 \ldots \exists x_n p(v_1, \ldots, v_k) < 0 < q(v_0, \ldots, v_k)$ is, dan is $\varphi(a_1, \ldots, a_k)$ waar in L.

Wegens lemma 40 is $\varphi(a_0, \ldots, a_k)$ ook waar in K, dus er bestaan $x_1, \ldots, x_n \in K$ met $f(x_1, \ldots, x_n) < 0$, in tegenspraak met de aanname dat f niet-negatief is. □

Bibliografie

[1] E. Artin en O. Schreier. *Eine Kennzeichnung der reell abgeschlossenen Körper*. Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, 5de band, pp. 225–231, 1927.

[2] K. Conrad. *The Artin–Schreier theorem*. `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/artinschreier.pdf`, maart 2011.

[3] L. van den Dries. *Alfred Tarski's Elimination Theory for Real Closed Fields*. The Journal of Symbolic Logic, 53(1), pp. 7–19, 1988.

[4] P. Stevenhagen. *Algebra 3*. `http://websites.math.leidenuniv.nl/algebra/algebra3.pdf`, 2011.

[5] S. Lang. *Algebra*. Springer, 3de editie, 2002.

[6] B.L. van der Waerden. *Algebra*. Springer, 9de editie, 1993.

[7] C.C. Chang en H.J. Keisler. *Model Theory*. North-Holland, 3de editie, 1990.

[8] D. Marker. *Introduction to Model Theory*. In D. Haskell, A. Pillay, en C. Steinhorn (red.), *Model theory, algebra, and geometry*, uit de reeks *Mathematical Sciences Research Institute publications*. Cambridge University Press, 2000.