STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1957-017

Voordracht in de serie
"Elementaire onderwerpen van hoger standpunt belicht"

Prof.dr. F. van der Blij

23 oktober 1957

1957

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

ZW 1957-017

Voordracht in de serie
"Elementaire onderwerpen van hoger standpunt belicht"

door

Prof.Dr F. van der Blij

23 oktober 1957

Algebraïsche beschouwingen bij de herleiding van wortelvormen

§ 1. Inleiding.

De veel gesmade herleiding van $\sqrt{5+2\sqrt{6}}$ en de tot traditie verstarde, haast magische wet: "wortels uit de noemer verdrijven" zijn te begrijpen vanuit het standpunt deze vormen eenvoudig numeriek te bepalen als een tabel van de wortels uit de natuurlijke getallen voorhanden is.

Door adjunctie van de wortels uit priemgetallen, al dan niet gecombineerd met adjunctie van i, ontstaat een lichaam van algebraïsche getallen, waarin ieder positief rationaal getal, resp. ieder rationaal getal, een kwadraat is. Dit lichaam is niet algebraïsch afgesloten, zelfs is niet eens ieder getal uit dit lichaam een kwadraat. Het is een deellichaam van het lichaam van de met passer en lineaal construeerbare getallen.

We zullen ons beperken tot adjunctie van een eindig aantal vierkantswortels, van zo'n lichaam is de graad steeds een macht van 2.

§ 2. Elementaire theorie.

Laat K een uitbreiding van het lichaam k van de rationale getallen zijn. We noemen twee getallen $p,q \in K$ equivalent als pq het kwadraat is van een getal uit K.

Stelling 1.

$K(\sqrt{p}) = K(\sqrt{q})$ dan en slechts dan als $p \sim q$.

Stelling 2.

Als $\sqrt{p} \notin K$, dan is ieder element van $K(\sqrt{p})$ eenduidig te schrijven als $a+b\sqrt{p}$ met $a,b \in K$.

Onder $H = \{h_1,\ldots,h_t\}$ zullen we een willekeurige (niet geordende) deelverzameling van de indices $\{1,\ldots,n\}$ verstaan. Als $p_1 \ldots p_n \in K$

voeren we in $\pi_H = \sqrt{p_{h_1} \ldots p_{h_t}}$. Als H leeg is definiëren we $\pi_H = 1$. Het totaal aantal zo te vormen symbolen π_H is 2^n.

Stelling 3.

Als $p_1 \ldots p_n \in K$ zodat $K(\sqrt{p_1}, \ldots \sqrt{p_n})$ de graad 2^n heeft, zal ieder getal uit $K(\sqrt{p_1}, \ldots \sqrt{p_n})$ éénduidig te schrijven zijn als $\sum n_H \pi_H$ met $n_H \in K$.

Stelling 4.

Als $q \in K$ en $\sqrt{q} \in K(\sqrt{p_1}, \ldots \sqrt{p_n})$, dan is er een H zodat $q \sim \pi^2_H$.

Bewijs.

We mogen veronderstellen dat $K(\sqrt{p_1}, \ldots \sqrt{p_n})$ de graad 2^n heeft en bewijzen nu met inductie naar n. Voor iedere ν $(1 \leq \nu \leq n)$ zijn er getallen α_ν en $\beta_\nu \in K(\sqrt{p_1}, \ldots \hat{\sqrt{p_\nu}}, \ldots \sqrt{p_n})$ met $\sqrt{q} = \alpha_\nu + \beta_\nu \sqrt{p_\nu}$. Dus $\alpha_\nu \beta_\nu \sqrt{p_\nu} \in K(\sqrt{p_1}, \ldots \hat{\sqrt{p_\nu}} \ldots \sqrt{p_n})$ en $\alpha_\nu \beta_\nu = 0$. Is er een ν met $\beta_\nu = 0$ dan $\sqrt{q} = \alpha_\nu \in K(\sqrt{p_1}, \ldots \hat{\sqrt{p_\nu}} \ldots \sqrt{p_n})$ en de stelling volgt uit de inductie aanname. Als voor alle ν geldt $\beta_\nu \neq 0$ kunnen we met een elementaire berekening uit $\sqrt{q} = \beta_\nu \sqrt{p_\nu}$ voor alle ν concluderen dat $\sqrt{q} = \beta \sqrt{p_1 \ldots p_n}$.

Gevolg. Kiezen we K=k en voor $p_1, p_2, \ldots$ of de rij van de priemgetallen of deze rij voorafgegaan door -1, dan heeft $k(\sqrt{p_1}, \ldots \sqrt{p_n})$ de graad 2^n.

Bij de herleiding van wortelvormen valt het op dat $5+2\sqrt{6}$ geen kwadraat is in $k(\sqrt{6})$, maar wel in $k(\sqrt{6}, \sqrt{2}) = k(\sqrt{6}, \sqrt{3})$. We vragen ons nu af in hoeverre een getal dat geen kwadraat is in een of ander lichaam een kwadraat kan worden door adjuncties van wortels uit het grondlichaam.

Stelling 5.

Als $\alpha \in L = K(\sqrt{p_1}, \ldots \sqrt{p_n})$ een kwadraat is in $L(\sqrt{q_1}, \ldots \sqrt{q_r})$ met $q_r \in K$ dan is er een getal $q \in K$ zodat α reeds kwadraat is in $L(\sqrt{q})$.

Bewijs.

Uit $\sqrt{\alpha} \in L(\sqrt{q_1}, \ldots \sqrt{q_r})$ volgt $\sqrt{\alpha} = \beta \sqrt{q_{1_1} \ldots q_{1_t}}$ met $\beta \in L$ (zie stelling 4). Dus is α reeds kwadraat in $L(\sqrt{q})$ met $q = q_{1_1} \ldots q_{1_t}$. We merken op dat zelfs $q\alpha$ reeds in L een kwadraat is.

Voorbeelden.

$9 + 4\sqrt{5} = (2+\sqrt{5})^2$

$5 + 2\sqrt{6} \rightarrow 10+4\sqrt{6} = (2+\sqrt{6})^2$. $5+2\sqrt{6} = (\sqrt{2}+\sqrt{3})^2$

$2 + \sqrt{3} \rightarrow 4+2\sqrt{3} = (1+\sqrt{3})^2$ $\quad 2+\sqrt{3} = (\frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{6})^2$

$18 + 6\sqrt{5} \rightarrow 6+2\sqrt{5} = (1+\sqrt{5})^2$ $\quad 18+6\sqrt{5} = (\sqrt{3}+\sqrt{15})^2$.

We bezien nog even $\sqrt{a+b\sqrt{c}}$. Is er een $q \in K$ met

$qa + qb\sqrt{c} = (x+y\sqrt{c})^2$, $x,y \in K$

dus $x^2 + cy^2 = qa$

$2xy = qb.$

$(2x^2-qa)^2 = q^2(a^2-b^2c).$

Stel nu $a^2-b^2c=d^2$.

$2x^2-qa = \pm qd$

$(2x)^2=2q(a\pm d).$

Steeds q zo te kiezen dat x hieruit rationaal op te lossen is.

Opmerking. Zijn a,b,c gehele rationale getallen, dan kunnen we voor q steeds een deler van $2(a^2-d^2)=2b^2c$ kiezen.

Over het algemene geval is weinig te zeggen. Voldoende is om te onderzoeken of $\alpha = \sum a_H \pi_H$ een kwadraat is van een getal $\xi = \sum x_H \pi_H$ alle uit $K(\sqrt{p_1}, \ldots \sqrt{p_n})$.

$\xi^2 = \sum_{K,L} x_K x_L \pi_K \pi_L = \sum_{K,L} x_K x_L \pi^2_{K\cap L} \pi_{K\cup L-K\cap L}$.

De vergelijkingen worden

$$\sum x_K x_L \pi^2_{K\cap L} = a_H \qquad K\cup L-K\cap L=H.$$

Dit wordt een gecompliceerd stel kwadratische vergelijkingen.

Voorbeeld. $\alpha = 36 - 14\sqrt{6} + 14\sqrt{5} - 6\sqrt{30}$.

Vaak beter aan te pakken door $x+y\sqrt{5}$ te zoeken met $(x+y\sqrt{5})^2 = \alpha$ en $x,y \in k(\sqrt{6})$.

Opmerking. $\sqrt{p}$ met $p \in k$ wordt slechts dan een kwadraat in $k(\sqrt{p},\sqrt{q})$ als $p=-1$ en $q=2$.

Merkwaardig is de situatie in andere dan het rationale lichaam. In een priemlichaam met p elementen wordt na adjunctie van $\sqrt{\varepsilon}$, waar ε een niet rest is, ieder element uit het oorspronkelijke lichaam een kwadraat. In een lichaam van p-adische getallen ($p\neq 2$) wordt na adjunctie van $\sqrt{p}$ en $\sqrt{\varepsilon}$ ieder element van het oorspronkelijke lichaam kwadraat.

§3. Galoistheorie.

We schetsen in grove lijnen de Galoistheorie.

1. Als $f(x)$ irreducibel van de graad n is en $f(\vartheta)=0$, dan is $K(\vartheta)$ een algebraïsche uitbreiding van de graad n. Deze uitbreiding (en $f(x)$) heet normaal als $f(x)$ in $K(\vartheta)$ volledig in lineaire factoren uiteen-

valt.
2. De Galoisgroep van een normale vergelijking heeft de graad n.
3. Het "lattice" van de ondergroepen van de Galoisgroep en dat van de tussenlichamen tussen K en $K(\vartheta)$ zijn duaal. Bij iedere ondergroep hoort het lichaam van de onder deze groep invariante elementen.
4. De graad van de uitbreiding en de index van de corresponderende ondergroep zijn gelijk.

Stelling 6.
$\vartheta = \sqrt{a+b\sqrt{c}}$ is te schrijven als $\sqrt{x}+\sqrt{y}$ als ϑ wortel is van een normale vierdegraads vergelijking.

Bewijs. ϑ voldoet aan $x^4-2ax^2+(a^2-b^2c)=0$. We ontbinden $(x-\vartheta)(x+\vartheta)(x^2-\frac{a^2-b^2c}{\vartheta^2})$.
De vergelijking is normaal als $a^2-b^2c=d^2$.
De Galoisgroep bestaat dan uit
E identiteit
A $\vartheta \longleftrightarrow -\vartheta \qquad \vartheta' \longleftrightarrow -\vartheta' \qquad (\vartheta'\vartheta = d)$
B $\vartheta \longleftrightarrow \vartheta' \qquad -\vartheta \longleftrightarrow -\vartheta'$
AB $\vartheta \longleftrightarrow -\vartheta' \qquad -\vartheta \longleftrightarrow \vartheta'$.
De Galoisgroep heeft drie ondergroepen van index 2. Er zijn dus zeker twee (zelfs drie) onderlichamen van $K(\vartheta)$ met de graad 2, hiervoor kunnen $K(\sqrt{c})$ en $K(\sqrt{f})$ met $f=2(a+d)$ of $2(a-d)$ gekozen worden. Dan zal $K(\sqrt{c},\sqrt{f})=K(\vartheta)$ en dus $\vartheta=a_0+a_1\sqrt{c}+a_2\sqrt{f}+a_3\sqrt{cf}$.

4. Derde wortels.

De methode van Cardanus voor de oplossing van $x^3+\alpha x+\beta=0$ voert op natuurlijke wijze tot vormen als $\zeta = \sqrt[3]{a+b\sqrt{c}}$. We kunnen ons de vraag stellen of deze vorm te schrijven is als $u+v\sqrt{c}$. Schrijven we eenvoudig $a+b\sqrt{c}=(u+v\sqrt{c})^3$ en stellen we vergelijkingen voor u en v op dan komen we tot een derdegraadsvergelijking, die opgelost via Cardanus tot de oude vormen terugleidt.
Als $\sqrt[3]{a+b\sqrt{c}}=u+v\sqrt{c}$ dan ook $\sqrt[3]{a-b\sqrt{c}}=u-v\sqrt{c}$ en dus moet a^2-b^2c een derde macht van een getal in het grondlichaam zijn, stel dus $a^2-b^2c=d^3$.
Verder moet ook $\tau=\sqrt[3]{a+b\sqrt{c}}+\sqrt[3]{a-b\sqrt{c}}=2u$ in het grondlichaam liggen. We merken op dat τ voldoet aan

$$z^3 - 3dz - 2a = 0.$$

Een verdere voorwaarde is dus dat deze vergelijking een wortel in het grondlichaam heeft. De beide andere wortels zijn dan

$\tau_1 = \varepsilon\sqrt[3]{a+b\sqrt{c}} + \varepsilon^2\sqrt[3]{a-b\sqrt{c}}$ en $\tau_2 = \varepsilon^2\sqrt[3]{a+b\sqrt{c}} + \varepsilon\sqrt[3]{a-b\sqrt{c}}$ met $\varepsilon^3=1$ en alle wortels moeten liggen in $K(\sqrt{-3c})$.

Voorbeelden.

$\sqrt[3]{7-5\sqrt{2}}$. We berekenen $a^2-b^2c = 49-50=(-1)^3$, dus $d=-1$. De vergelijking $z^3+3z-14=0$ heeft een wortel $z=2$.
We vinden dus $u=1$ en dan eenvoudig $v=-1$.

$$\sqrt[3]{7-5\sqrt{2}} = 1 - \sqrt{2}.$$

Bizonder eenvoudig is het probleem voor

$$\zeta = \sqrt[3]{a + b\sqrt{-3}}.$$

ζ voldoet aan $x^6-2ax^3+a^2+3b^2=0$. Als ζ herleidbaar is dan moet a^2+3b^2 een derde macht zijn en deze vergelijking normaal.