STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1957-025

Over een probleem uit de algebraïsche getallentheorie

Dr. W. Peremans

27 november 1957

1957

Over een probleem uit de algebraïsche getallen-theorie.

Rapport ZW 1957-022

27 november 1957

Mevrouw T. van Aardenne-Ehrenfest,
Zuidendijk 263A,
DORDRECHT.

Geachte Mevrouw Van Aardenne,

Hierbij zend ik U de syllabus van Prof.Van der Blij, waarover gisteren gesproken werd. In deze syllabus staat wel hetgeen U nodig hebt. Daar alles er nogal beknopt en veelal zonder bewijzen in staat, ben ik zo vrij hieronder nog een elementair bewijs uitvoerig op te schrijven.

Ik begin met een bekende hulpstelling.

Stelling 1. Als $p_1,\ldots,p_k$ verschillende priemgetallen zijn en $R(x_1,\ldots,x_k)$ een rationale functie met rationale coëfficiënten, dan bestaat er een polynoom $P(x_1,\ldots,x_k)$ met rationale coëfficiënten dat in elk van de veranderlijken hoogstens van de eerste graad is, zodat

$$R(\sqrt{p_1},\ldots,\sqrt{p_k}) = P(\sqrt{p_1},\ldots,\sqrt{p_k}).$$

Bewijs: We passen volledige inductie naar k toe. Het geval k=0 is triviaal. Stel $n \geq 1$ en de stelling bewezen voor $k < n$. We schrijven

$$R(x_1,\ldots,x_n) = \frac{P_1(x_1,\ldots,x_n)}{P_2(x_1,\ldots,x_n)}$$

met P_1 en P_2 polynomen met rationale coëfficiënten. Omdat $(\sqrt{p_1})^2$ rationaal is, bestaan er polynomen $P_3(x_1,\ldots,x_n)$ en $P_4(x_1,\ldots,x_n)$ met rationale coëfficiënten die in elk van de veranderlijken hoogstens van de eerste graad zijn zodat

$$P_1(\sqrt{p_1},\ldots,\sqrt{p_n}) = P_3(\sqrt{p_1},\ldots,\sqrt{p_n})$$
$$P_2(\sqrt{p_1},\ldots,\sqrt{p_n}) = P_4(\sqrt{p_1},\ldots,\sqrt{p_n}) .$$

Stel nu $P_3(\sqrt{p_1},\ldots,\sqrt{p_n}) = P_5+P_6\sqrt{p_n}$ en $P_4(\sqrt{p_1},\ldots,\sqrt{p_n}) = P_7+P_8\sqrt{p_n}$, waarin $P_i=P_i(\sqrt{p_1},\ldots,\sqrt{p_{n-1}})$ voor i=5,6,7,8 polynomen met rationale coëfficiënten zijn. Als nu $P_7-P_8\sqrt{p_n}=0$ is, is $P_7+P_8\sqrt{p_n}=2P_7$. De stelling vinden we door de inductieveronderstelling op $P_5/2P_7$ en $P_6/2P_7$ toe te passen. Als $P_7-P_8\sqrt{p_n}\neq 0$ vermenigvuldigen we teller en noemer met $P_7-P_8\sqrt{p_n}$ en passen na linearisatie weer tweemaal de inductieveronderstelling toe.

Opmerking: Stelling 1 is een speciaal geval van de stelling dat een rationale functie met rationale coëfficiënten van een aantal algebraïsche getallen als een polynoom met rationale coëfficiënten in die algebraïsche getallen is te schrijven.

Stelling 2. Als $p_1,\ldots,p_k$ verschillende priemgetallen zijn en m een kwadraatvrij geheel getal $\neq 1$, dat door geen der getallen $p_1,\ldots,p_k$ deelbaar is, dan is

$$\sqrt{m} \neq R(\sqrt{p_1},\ldots,\sqrt{p_k})$$

voor alle rationale functies R met rationale coëfficiënten.

Bewijs: Inductie naar k; k=0 is triviaal omdat $\sqrt{m}$ irrationaal is. Stel $n \geq 1$ en de stelling bewezen voor $k < n$. Stel

$$\sqrt{m} = R(\sqrt{p_1},\ldots,\sqrt{p_n}).$$

Op grond van stelling 1 mogen we aannemen dat R een polynoom met rationale coëfficiënten is, dat in elk van de veranderlijken hoogstens van de eerste graad is. Stel

$$R(\sqrt{p_1},\ldots,\sqrt{p_n}) = P_1 + P_2\sqrt{p_n}$$

met $P_i = P_i(\sqrt{p_1},\ldots,\sqrt{p_{n-1}})$ $(i = 1,2)$.

Als $P_2=0$ leidt de inductieveronderstelling tot een contradictie.

Als $P_2 \neq 0$, $P_1=0$, geldt

$$\sqrt{m\,p_n} = p_n\,P_2 .$$

Omdat p_n niet deelbaar is op m, is $m\,p_n$ een kwadraatvrij getal $\neq 1$, dat door geen der getallen $p_1,\ldots,p_{n-1}$ deelbaar is. Ook nu leidt de inductieveronderstelling tot een contradictie.

Als $P_1 \neq 0$, $P_2 \neq 0$, vinden we door kwadrateren:

$$m = P_1^2 + p_n P_2^2 + 2 P_1 P_2 \sqrt{p_n} ,$$

$$\sqrt{p_n} = \frac{m - P_1^2 - p_n P_2^2}{2 P_1 P_2}$$

en wederom leidt de inductieveronderstelling tot een contradictie.

Stelling 3. Als $m_1,\ldots,m_k$ kwadraatvrije gehele getallen $\neq 1$ zijn en m een geheel getal $\neq 0$, dan is

$$x_1\sqrt{m_1} + \ldots + x_k\sqrt{m_k} = m$$

onoplosbaar in gehele $x_1,\ldots,x_k$.

Bewijs: Inductie naar k; k=0 is triviaal. Stel $n \geq 1$ en de stelling bewezen voor $k < n$. Stel

$$x_1\sqrt{m_1} + \ldots + x_n\sqrt{m_n} = m.$$

Laat $p_1,\ldots,p_j$ de verschillende priemgetallen zijn, die als delers bevat zijn in de getallen $m_1,\ldots,m_n$ en stel (na vernummeren) dat $m_1,\ldots,m_i$ deelbaar zijn door p_j en $m_{i+1},\ldots,m_n$ niet. Dan is $i \geq 1$ en

$$P_1(\sqrt{p_1},\ldots,\sqrt{p_{j-1}})\sqrt{p_j}+x_{i+1}\sqrt{m_{i+1}}+\ldots+x_n\sqrt{m_n}=m.$$

Nu is $P_1(\sqrt{p_1},\ldots,\sqrt{p_{j-1}})=0$ onmogelijk op grond van de inductieveronderstelling. Als $P_1(\sqrt{p_1},\ldots,\sqrt{p_{j-1}})\neq 0$, kunnen we $\sqrt{p_j}$ oplossen als rationale functie van $\sqrt{p_1},\ldots,\sqrt{p_{j-1}}$ met rationale coëfficiënten, hetgeen op grond van stelling 2 onmogelijk is.

Opmerking. Als we bovendien aannemen, dat ~~onder~~ $m_1,\ldots,m_k$ ~~minstens twee~~ verschillend~~e~~ ~~getallen voorkomen~~ zijn, geldt dat uit

$$x_1\sqrt{m_1}+\ldots+x_n\sqrt{m_n}=0$$

met gehele $x_1,\ldots,x_n$, volgt dat $x_1=\ldots=x_n=0$. Het bewijs is analoog.

Hiermede hoop ik U van dienst te zijn geweest.

Met de meeste hoogachting,

(Dr W. Peremans)

11 december 1957

Mevrouw T. van Aardenne-Ehrenfest,
Zuidendijk 263A,
DORDRECHT.

WP/LN

Geachte Mevrouw Van Aardenne,

Het bewijs, dat de in Uw brief van 8 dezer gedefinieerde R_∞ het getal 1 niet bevat, wil ik over een andere boeg gooien, omdat de oude methode me niet lukken wilde. Als we van enkele eenvoudige stellingen uit de algebraïsche getallentheorie gebruik maken, is het bewijs echter heel simpel. De volgende twee stellingen ontleen ik aan de algebraïsche getallentheorie.

Stelling 1. Als het algebraïsche getal α nulpunt is van een polynoom met gehele coëfficiënten en hoogste coëfficiënt 1, dan heeft het irreducibele polynoom met rationale coëfficiënten en hoogste coëfficiënt 1, dat α als nulpunt bezit, ook gehele coëfficiënten.
Een dergelijk algebraïsch getal noemen we geheel algebraïsch.

Stelling 2. De vierkantswortel uit een geheel algebraïsch getal is geheel algebraïsch. Een lineaire combinatie met gehele coëfficiënten van gehele algebraïsche getallen is geheel algebraïsch.

Stelling 1 vindt U in leerboeken over algebraïsche getallentheorie of ook in Van der Waerden, Moderne Algebra, b.v. tweede druk Kapitel IV, § 23 Faktorzerlegung, blz.77. Stelling 2 is eenvoudig uit stelling 1 af te leiden.
Definiëren we nu R_n recursief als de verzameling van de lineaire combinaties met gehele coëfficiënten van vierkantswortels uit elementen van R_{n-1} (R_0 is de verzameling van de even gehele getallen), dan geldt

Stelling 3. Als $r \in R_n$, dan is

$$2^{-2^{-n}}\, r$$

geheel algebraïsch.

Bewijs. Volledige inductie naar n. Voor n=0 is de stelling triviaal, want gewone gehele getallen zijn geheel algebraïsch. Stel nu $k \geq 1$ en de stelling juist voor $n < k$. Als $r \in R_k$, dan is

$$r = \sum_{j=1}^{m} h_j \alpha_j^{\frac{1}{2}}$$

met h_j geheel en $\alpha_j \in R_{k-1}$, dus

$$2^{-2^{-k}} r = \sum_{j=1}^{m} h_j (\rho^{-2^{-(k-1)}} \alpha_j)^{\frac{1}{2}} .$$

De inductieveronderstelling en stelling 2 leveren het gevraagde.

Stelling 4. Voor alle gehele $n \geq 0$ geldt $1 \notin R_n$.

Bewijs. Stel $1 \in R_n$, dan is, volgens stelling 3,

$$2^{-2^{-n}}$$

geheel algebraïsch. Dit is echter niet zo, want dit getal is nulpunt van het irreducibele polynoom

$$x^{2^n} - \tfrac{1}{2}$$

en dus volgens stelling 1 niet geheel algebraïsch.

Als ook ringen met nuldelers toegelaten worden, is er wel een eenvoudiger methode om ringen te krijgen, die geen eenheidselement hebben en waarin ieder element product is van twee elementen.

We gaan uit van een willekeurige ring R_0 met minstens twee elementen en met eenheidselement, dat we met 1 aanduiden. We vormen oneindige rijen

$$\rho = (r_1, r_2, \ldots)$$

met $r_n \in R_0$ en alle $r_n = 0$ op eindig vele na. Optelling, aftrekking en vermenigvuldiging worden componentsgewijze gedefinieerd. Het is duidelijk dat we dan een ring R verkregen hebben. Het is duidelijk, dat R geen eenheidselement heeft, want het eenheidselement zou de oneindige rij met uitsluitend enen moeten zijn en die zit niet in R. Ieder element is wel een product, want iedere $\rho \in R$ is te schrijven als $\rho\sigma$ met $\sigma \in R$. Als n.l. N een (van ρ afhankelijk) natuurlijk getal is, zodat $r_n = 0$ voor $n \geq N$, dan voldoet

$$\sigma = (s_1, s_2, \ldots),$$

gedefinieerd door $s_n = 1$ voor $n \leq N$ en $s_n = 0$ voor $n > N$ aan de eisen.

Hiermee hoop ik U van dienst te zijn geweest.

Met vriendelijke groeten,

(Dr W. Peremans)