STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 32

Algebraische getallenlichamen.

Cursus den Haag 1955/56.

B.Meulenbeld.

1956

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

ALGEBRAISCHE GETALLENLICHAMEN 1955/56

door

Prof.Dr B. Meulenbeld

Inleiding

Tot nu toe hebben wij steeds gewerkt met rationale getallen, of getallen uit het getallenlichaam der rationale getallen, aangeduid door P.

Een getallenlichaam is een verzameling van getallen met de volgende eigenschappen:

1. Het lichaam bevat minstens 2 getallen;
2. Als het lichaam α en β bevat, dan ook $\alpha \pm \beta$, $\alpha\beta$ en $\frac{\alpha}{\beta}$ $(\beta \neq 0)$.

Het getallenlichaam van Gauss bestaat uit de complexe getallen a+bi, waarin a en b rationale getallen zijn. Het is gemakkelijk in te zien dat deze getallen een lichaam vormen. Men kan in dit lichaam ook gehele getallen definieren. Het getallenlichaam van Gauss wordt aangeduid door P(i). Evenzo vormen de getallen $a+\rho b$ met $\rho = -\frac{1}{2}+\frac{1}{2}\sqrt{3}$ (a en b rationaal) een getallenlichaam, aangeduid door $P(\rho)$. Een derde voorbeeld is het lichaam $P(i\sqrt{5})$, gevormd door de getallen $a+bi\sqrt{5}$ (a en b rationaal).

Het rationale getallenlichaam P is het eenvoudigste lichaam dat er bestaat, d.w.z. elk willekeurig getallenlichaam Ω bevat steeds P.

Vroeger is bewezen, dat elk natuurlijk getal n op eenduidige wijze in factoren kan worden ontbonden, d.w.z. uit $n=p_1p_2\ldots p_r=q_1q_2\ldots q_s$ volgt r=s, en, afgezien van de volgorde, zijn de p's gelijk aan de q's.

Men kan nu bewijzen, dat ook in P(i) de daarin gedefinieerde gehele getallen een eenduidige factorontbinding bezitten. Dit is ook in $P(\rho)$ het geval. Ook in $P(i\sqrt{5})$ kan men gehele getallen in factoren ontbinden, doch deze ontbinding is niet meer eenduidig. Het bestaan van lichamen, waarin geen eenduidige factorontbinding mogelijk is, is aanleiding geweest om een geheel andere theorie op te bouwen, n.l. die der algebraïsche getallenlichamen en aansluitend hieraan de ideaaltheorie (Dedekind en Kummer).

Eenduidige ontbinding in P(i).

Definitie. Onder een geheel getal verstaan we elk getal $\xi = a+ib$, waarbij a en b geheel rationaal zijn.

De volgende stellingen zijn nu gemakkelijk te bewijzen.

1. i is geheel.
2. Ieder geheel rationaal getal is geheel.
3. Ieder rationaal getal dat geheel is, is een geheel rationaal getal.
4. Is ξ geheel, dan ook het toegevoegd complexe getal $\overline{\xi}$.
5. Zijn ξ en η geheel, dan ook $\xi+\eta$, $\xi-\eta$, $\xi\eta$.

Definitie. Zij $\xi \neq 0$. Dan betekent ξ / η (ξ deelbaar op η): Er bestaat een geheel getal χ met $\eta = \chi\xi$. $\xi \not/ \eta$, dan bestaat er zo'n geheel getal χ niet.

6. Zijn ξ en η rationaal, $\xi \neq 0$, dan is ξ/η dan en slechts dan, als in de vroegere zin ξ/η is.
7. Uit ξ/η, η/ζ volgt ξ/ζ
8. Uit ξ/η, ξ/ζ volgt $\xi/\alpha\eta+\beta\zeta$
9. Voor elke ξ geldt $1/\xi$, $-1/\xi$, i/ξ, $-i/\xi$
   voor elk $\xi \neq 0$ is ξ/ξ, $-\xi/\xi$, $i\xi/\xi$ en $-i\xi/\xi$.

Dit volgt uit $\xi = 1.\xi = (-1)(-\xi) = i(-i\xi) = (-i)i\xi$.

Definitie. Onder de norm van ξ (aangeduid $N(\xi)$) verstaat men het getal $\xi\overline{\xi} = |\xi|^2$.

10. $N(\xi)$ is geheel en voor $\xi \neq 0$ is $\xi / N(\xi)$.
11. $N(a) = a^2$ (a is geheel rationaal).
12. $N(\xi)$ is een geheel rationaal getal.

$$N(\xi) = \begin{cases} 0 \text{ voor } \xi = 0 \\ 1 \text{ voor } \xi = 1, -1, i \text{ en } -i \\ 1 \text{ overigens} \end{cases}$$

13. $N(\xi\eta) = N(\xi)\,N(\eta)$.
    Bewijs: $|\xi\eta| = |\xi||\eta|$, dus $|\xi\eta|^2 = |\xi|^2|\eta|^2$.
14. Uit ξ/ζ volgt $N(\xi)/N(\zeta)$.
    Bewijs: $\xi/\zeta \Rightarrow \zeta = \chi\xi \Rightarrow N(\zeta) = N(\chi).N(\xi) \Rightarrow N(\xi)/N(\zeta)$
    $\xi \neq 0$, dus $N(\xi) \neq 0$.
15. Is ε/ξ voor elke ξ, dan is $\varepsilon = 1$, -1, i of $-i$.
    Bewijs: $\varepsilon/1 \Rightarrow N(\varepsilon)/N(1) \Rightarrow N(\varepsilon)/1 \Rightarrow N(\varepsilon) = 1$.

Definitie. De vier getallen $\varepsilon = 1$, -1, i en $-i$ heten eenheden van P(i). Dit zijn dus de enige getallen die op elk geheel getal deelbaar zijn.

16. Is ε eenheid, dan is ook $\frac{1}{\varepsilon}$ eenheid.
17. Zijn ε_1 en ε_2 eenheden, dan ook $\varepsilon_1\varepsilon_2$.
18. Uit α/ε volgt $\alpha = \varepsilon$.

Definitie. ξ heet geassocieerd met η, als er een ε is met $\xi=\eta\varepsilon$.

19. Het begrip geassocieerd is symmetrisch, reflexief en transitief.

Definitie. Is $N(\xi)>1$, dan heet ξ ondeelbaar of priem, als bij de ontbinding $\xi=\eta\zeta$ òf $N(\eta)=1$ òf $N(\zeta)=1$ is. Elk ondeelbaar getal heeft precies 8 delers.

We zullen de ondeelbare getallen door de letter π voorstellen.

20. Is α met π geassocieerd, dan is ook α ondeelbaar.

Bewijs: Is $\eta/\alpha \Rightarrow \alpha=\chi\eta$, en $\alpha=\varepsilon\pi$, dus $\varepsilon\pi=\chi\eta \Rightarrow$ $\pi=\varepsilon_1\chi\eta \Rightarrow \eta/\pi \Rightarrow \eta=\varepsilon$ of $\eta=\varepsilon\pi=\varepsilon_1\alpha$.

21. Is $N(\xi)=p$, dan is ξ priem.

Bewijs: Uit $\xi=\eta\zeta$ zou volgen $N(\xi)=N(\eta)N(\zeta)$ $p=N(\eta)N(\zeta)$, dus òf $N(\eta)=1$ of $N(\zeta)=1$.

Voorbeeld: $N(2+3i)=13$, dus $2+3i$ is priem.

Niet omgekeerd: Een priemgetal kan het best een samengesteld getal tot norm hebben, b.v. $N(3)=9$. Toch is 3 ondeelbaar, want uit $3=\eta\zeta$ $N(\eta)>1$, $N(\zeta)>1$, zou volgen $9=N(\eta)N(\zeta)$, dus $N(\eta)=3$. Is $\eta=a+ib$, dan zou $a^2+b^2=3$ een oplossing hebben.

22. Is $N(\xi)>1$, dan is er een ontbinding in priemfactoren mogelijk: $\xi=\pi_1\pi_2\ldots\pi_t$.

Bewijs: (inductie naar de norm). Is $N(\xi)=2$, dan is ξ priem, dus klaar. Is $N(\xi)>2$, dan zij de bewering bewezen voor alle gevallen waarvan de norm >1 en $<N(\xi)$ is.

Is ξ priem, dan $\xi=\eta$, klaar.

Is ξ deelbaar, dan is $\xi=\eta\zeta$, $N(\eta)>1$, $N(\zeta)>1$, dus $N(\eta)=\frac{N(\xi)}{N(\zeta)}<N(\xi)$, $N(\zeta)=\frac{N(\xi)}{N(\eta)}<N(\xi)$, dus $\eta=\pi_1\ldots\pi_s$, $\zeta=\pi_{s+1}\ldots\pi_t \Rightarrow \xi=\pi_1\ldots\pi_t$.

Nu de eenduidigheid.

23. Is $\eta\neq0$, ξ willekeurig, dan zijn er 2 getallen ζ en λ met $\xi=\zeta\eta+\lambda$, $N(\lambda)<N(\eta)$ (Euclidische algorithmus).

Bewijs: $\frac{\xi}{\eta}$ is complex = A+iB (A en B rationaal). Er zijn dus 2 gehele rationale getallen x en y met $|A-x|<\frac{1}{2}$, $|B-y|<\frac{1}{2}$.

We stellen nu $x+iy=\zeta$ en $\xi-\zeta\eta=\lambda$, dan is

$$\lambda=\eta\left(\frac{\xi}{\eta}-\zeta\right)=\eta\{(A-x)+i(B-y)\},\ |\lambda|=|\eta|\sqrt{(A-x)^2+(B-y)^2}\leq$$
$$\leq|\eta|\sqrt{\tfrac{1}{4}+\tfrac{1}{4}}<|\eta|,\ N(\lambda)=|\lambda|^2<|\eta|^2=N(\eta).$$

24. Uit $\pi|\xi\zeta$ volgt π/ξ of π/ζ.

Bewijs: We kunnen aannemen $\pi/\xi\eta$, $\pi\nmid\xi$, te bewijzen: π/ζ.

Onder alle getallen $\alpha\xi+\beta\pi\neq0$ moet er een de kleinste norm hebben. Deze kleinste norm is in elk geval $<N(\pi)$, daar $N(\xi+\beta\eta)<N(\pi)$ bij passende β. Wegens $\pi\nmid\xi$ is hierin $\xi+\beta\pi\neq0$. α en β worden zo gekozen, dat $\alpha\xi+\beta\pi=\gamma$ $(0<N(\gamma)<N(\pi))$ en $N(\gamma)$ zo klein mogelijk.

We beweren nu dat $N(\gamma)=1$. Anders zou bij passende χ, λ

$\pi=\chi\gamma+\lambda$, $N(\lambda)<N(\gamma)$ en $N(\lambda)>0$

(anders was γ/π en wegens $N(\gamma)>1$ dus $\gamma=\varepsilon\pi$, $N(\gamma)=N(\pi)$).
Dan zou: $\lambda=\pi-\chi\gamma=\pi-\chi(\alpha\xi+\beta\pi)=\alpha_1\xi+\beta_1\pi$, hetgeen strijdt met de minimaal definitie van γ.
Dus moet bij passende α,β,ε gelden $\alpha\xi+\beta\pi=\varepsilon$.
Nu is gegeven $\pi/\xi\zeta$. Uit $\alpha\xi\zeta+\beta\pi\zeta=\varepsilon\zeta \Rightarrow \pi/\varepsilon\zeta \Rightarrow \pi/\zeta$.

25. Uit $\pi/\xi_1,\dots\xi_n$ volgt π/ξ_m voor minstens één m.
Bewijs door inductie.

26. (Eenduidigheid). Uit $\xi=\pi_1\pi_2\dots\pi_r=\pi_1'\pi_2'\dots\pi_s'$ $(r\geq 1, s\geq 1)$ volgt r=s, en de π's zijn, afgezien van de volgorde, aan de π''s geassocieerd.
Bewijs: Voor $N(\xi)=2$ is stelling triviaal, daar ξ dan priem is, r=s=1 en $\pi_1=\pi_1'$
Zij $N(\xi)>2$ en de bewering bewezen voor elke η met $1<N(\eta)<N(\xi)$.
Is ξ priem, dan r=s=1, $\pi_1=\pi_1'$, en de stelling bewezen.
Zij $r>1$, $s>1$. Dan is volgens stelling 22
$\pi_r/\pi_1'\dots\pi_s' \Rightarrow \pi_r/\pi_m'$, zeg π_r/π_s'.
Dus òf $\pi_1=1$ òf aan π's geassocieerd. Het eerste kan niet, dus $\varepsilon\pi_r=\pi_s'$. Dus $\eta=\frac{\xi}{\pi_r}=\pi_1\dots\pi_{r-1}=\varepsilon\pi_1'\dots\pi_{s-1}'$.
Daar $1<N(\eta)<N(\xi)$ is wegens inductie-onderstelling r-1=s-1 $\Rightarrow$ r=s, en afgezien van de volgorde zijn $\pi_1,\dots,\pi_{r-1}$ aan $\varepsilon\pi_1',\dots,\pi_{s-1}'$, geassocieerd, dus ook aan $\pi_1',\dots,\pi_{s-1}'$.

Men kan dezelfde bewijsgang volgen voor de getallen uit het lichaam $P(-\frac{1}{2}+\frac{1}{2}i\sqrt{3})$. Men kan dan ook weer de eenduidige factorontbinding bewijzen.
Nu het getallenlichaam $P(i\sqrt{5})$.
<u>Definitie.</u> Een <u>geheel</u> getal is elk getal $\xi=a+ib\sqrt{5}$, waarin a en b geheel rationaal zijn.
$i\sqrt{5}$ is geheel. De stellingen 2 t/m 8 gelden weer. De bewijzen zijn analoog aan die in P(i). Stelling 9 wordt nu: Voor elke ξ is $1/\xi$, $-1/\xi$. Voor $\xi\neq 0$ is $\xi/\xi_1 -\xi/\xi$.
1 en -1 zijn dus nu de eenheden. Stelling 10 en 11 gaan weer analoog.
Stelling 12 wordt nu:
$N(\xi)$ is een geheel rationaal getal en wel is $N(\xi)=\begin{cases}0, & \text{voor } \xi=0\\ 1, & \text{voor } \xi=\pm 1\\ 1, & \text{overigens}\end{cases}$

De stellingen 13 t/m 22 weer analoog.
Stelling 23 geldt niet meer. Er is geen Euclidische algorithmus, d.w.z. het is <u>niet</u> waar dat bij iedere $\eta\neq 0$ en iedere ξ twee getallen χ en λ zijn met $\xi=\chi\eta+\lambda$, $N(\lambda)<N(\eta)$.
Tegenvoorbeeld. Neem $\eta=2$, $\xi=i\sqrt{5}$. Noem $\chi=x+iy\sqrt{5}$, dan zou

$4=N(\eta) > N(\lambda)=N(\xi-\chi\eta)=N(-2x+i(\sqrt{5}-2y\sqrt{5}))=4x^2+5(1-2y)^2 \geq 5(1-2y)^2 \geq 5$.

Stelling. Het is niet waar dat uit $\pi/\xi\xi$ volgt π/ξ of π/ξ.

Bewijs. 2 is priem, daar uit $2=\alpha\beta$, $N(\alpha)>1$, $N(\beta)>1$ zou volgen $4=N(\alpha)N(\beta) \Rightarrow 2=N(\alpha)=a^2+5b^2$ en deze heeft geen oplossingen.

Neem nu $\pi=2$, $\xi=1+i\sqrt{5}$, $\xi=1-i\sqrt{5}$.

$\xi\xi=6$. Dus $\pi/\xi\xi$ en $2 \nmid 1+i\sqrt{5}$, $2 \nmid 1-i\sqrt{5}$.

Stelling. Uit $\xi = \pi_1 \cdots \pi_2 = \pi_1' \ldots \pi_s'$ volgt niet dat de π', afgezien van de volgorde aan π' geassocieerd zijn.

Bewijs: $2.3=(1+i\sqrt{5})(1-i\sqrt{5})$.

Alle vier factoren zijn priem. Voor 2 is dit bewezen, voor 3 gaat het bewijs analoog. Voor $1 \pm i\sqrt{5}$ volgt het als volgt: Zou $1 \pm i\sqrt{5} = \alpha\beta$, $N(\alpha)>1$, $N(\beta)>1$ dan zou $6=N(1\pm i\sqrt{5})=N(\alpha)N(\beta) \Rightarrow N(\alpha)=$ $=2$ of 3 en dit kan niet daar $a^2+5b^2=2$ of 3 geen oplossingen hebben.

2 is niet uit $1+i\sqrt{5}$ en niet uit $1-i\sqrt{5}$ geassocieerd.

ALGEBRAISCHE GETALLENLICHAMEN II

door

Prof.Dr B. Meulenbeld

19 October 1955

Definitie: Is een veelterm van de gedaante $f(x) = a_o x^n + \ldots + a_n$, $a_o \neq 0$, dan heet n de graad van die veelterm.

Stelling: Heeft $f(x)$ de graad n_1 en $g(x)$ de graad n_2, dan heeft $f(x)g(x)$ de graad $n_1 + n_2$.

Met P duiden wij aan het lichaam der rationele getallen, met Ω een willekeurig getallenlichaam.

Definitie:Een veelterm $f(x)$ heet veelterm in Ω, als al zijn coëfficiënten tot Ω behoren.

Stelling: Zijn $f(x)$ en $g(x)$ veeltermen in Ω, dan is dit ook het geval met $f(x) \pm g(x)$ en $f(x)g(x)$.

Stelling: $f(x)$ en $g(x)$ zijn veeltermen in Ω, $g(x) \not\equiv 0$. Dan bestaan er twee eenvoudig bepaalde veeltermen $q(x)$ en $r(x)$ in Ω met $f(x) = q(x)g(x) + r(x)$, met $r(x) \equiv 0$ of graad van $r(x) <$ graad van $g(x)$.

Bewijs: Is $f(x) \equiv 0$, dan $r(x) \equiv 0$, $q(x) \equiv 0$, triviaal.

Is $f(x) \equiv a$, dan is $q(x) \equiv 0$, $r(x) \equiv a$, als gr $g > 0$, en als $g(x) \equiv b$, dan is $r(x) \equiv \frac{a}{b}$, $r(x) \equiv 0$, als gr $g = 0$, triviaal.

Is $g(x) = c$ (dus gr $g = 0$), dan is $q(x) = \frac{1}{c} f(x)$, $r(x) \equiv 0$, triviaal. Stel nu gr $g = 1$, en gr $f <$ gr G, dan $q(x) \equiv 0$, $r(x) \equiv f(x)$, triviaal. Wij kunnen dus aannemen gr $f \geq$ gr g.

Volledige inductie. Is gr $f = n$, dan stellen wij de stelling bewezen voor veeltermen van graad n-1.

$f(x) = a_o x^n + \ldots + a_n$, a_m in Ω, $a_o \neq 0$

$g(x) = b_o x^p + \ldots + b_p$, b_m in Ω, $b_o \neq 0$, $n \geq p$.

Beschouwen veelterm: $\varphi(x) = f(x) - \frac{a_o}{b_o} x^{n-p} g(x)$. Dit is veelterm in Ω. Graad $\varphi \leq n-1$, hierop dus stelling toe te passen. $\varphi(x) = q_1(x)g(x) + r(x)$, gr $r <$ gr g, $r(x)$ in Ω

$$f(x) = q_1(x)g(x) + r(x) + \frac{a_o}{b_o} x^{n-p} g(x)$$

$$= g(x)\left\{q_1(x) + \frac{a_o}{b_o} x^{n-p}\right\} + r(x).$$

Dus $q(x) = q_1(x) + \frac{a_o}{b_o} x^{n-p}$.

Eenduidigheid: Uit $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ zou volgen: $\{q_1(x) - q_2(x)\}g(x) = r_2(x) - r_1(x)$.
Rechts graad $<$ gr g, links $\geq$ gr g, tenzij $q_1(x) - q_2(x) = 0$ en $r_2(x) - r_1(x) = 0$.

Gevolg: Is $\Omega = P$ en $b_o = 1$, dan q(x) en r(x) in Ω met geheel rationale coëfficiënten.

Definitie: $\mathfrak{J}$ heet relatief algebraisch t.o.v. Ω, als er een veelterm $f(x) \neq 0$ bestaat, met $f(\mathfrak{J}) = 0$.
Men kan zelfs het bestaan van een veelterm in f(x) in Ω eisen met hoogste coëfficiënt = 1, want als f(x) in Ω en c de hoogste coëfficiënt is, dan is ook $\frac{f(x)}{c}$ een veelterm in Ω met dezelfde wortels.
Is $\Omega = P$, dan spreekt men zonder meer van algebraïsche getallen.

Voorbeelden: $\sqrt[3]{\pi}$ is algebraïsch t.o.v. elke Ω die π bevat, immers $x^3 - \pi = 0$. 2 is algebr., immers $x-2=0$, i is algebr. immers $x^2+1=0$ of $x^4-1=0$.
Definitie: Zij $\mathfrak{J}$ relatief algebraïsch t.o.v. Ω, en n de graad van de veelterm in Ω met de laagste graad met wortel $\mathfrak{J}$, dan heet n de relatief-graad van $\mathfrak{J}$ t.o.v. Ω. Is $\Omega = P$, dan kortweg de graad van $\mathfrak{J}$. n hangt van $\mathfrak{J}$ af, en van Ω. In het lichaam van Gauss P(i) heeft i de relatief graad 1, immers $x - i = 0$, in P de relatief graad 2, immers $x^2 + 1 = 0$. Elk rationaal getal heeft de graad 1.

Stelling: $\mathfrak{J}$ is relatief algebraïsch t.o.v. Ω, relatief graad = n. f(x) is een veelterm met $f(\mathfrak{J}) = 0$ van graad n. g(x) is een willekeurige veelterm met $g(\mathfrak{J}) = 0$. Dan is $g(x) = q(x)f(x)$, q(x) in Ω.

Bewijs: $g(x) = q(x)f(x) + r(x)$, q(x) en r(x) in Ω, $r(x) \neq 0$ of van graad $<$ n. Dit laatste kan niet wegens $r(\mathfrak{J}) = g(\mathfrak{J}) + q(\mathfrak{J})f(\mathfrak{J}) = 0$, en de definitie van n.

Definitie: $f(x) \neq 0$ in Ω. f(x) heet reducibel in Ω, als er twee veeltermen van lagere graad $f_1(x)$ en $f_2(x)$ bestaan, zodat $f(x) = f_1(x)f_2(x)$. Is dit niet het geval, dan heet f(x) irreducibel.

Voorbeelden: Elke veelterm in Ω van de 0^{de} of 1^{ste} graad is irreducibel $x^2 + 1$ is in P irreducibel, in P(i) reducibel, nl. $(x+i)(x-i)$.
$\sqrt[n]{2}$ is algebraïsch van de graad n.
Is $\mathfrak{J}$ relatief algebraïsch t.o.v. Ω van graad n, dan is $a_o\mathfrak{J}^n + a_1\mathfrak{J}^{n-1} + \ldots + a_n = 0$, a_i in Ω, $a_o \neq 0$. Ook kunnen wij zeggen:
$\mathfrak{J}^n + b_1\mathfrak{J}^{n-1} + \ldots + b_n = 0$, b_i in Ω.

Dit is de enige veelterm van deze gedaante van graad n.

Was er nog een, dan was ϑ ook een wortel van het verschil van lagere graad, en dit kan niet.

$x^n + b_1x^{n-1} + \ldots + b_n$ heet kanonieke veelterm van ϑ in Ω. Van $\sqrt[n]{2}$ is $x^n - 2$ de kanonieke veelterm. Iedere kanonieke veelterm is irreducibel.

Stelling: Is $f(\vartheta) = 0$, dan is $f(x)$ deelbaar door de kanonieke veelterm $g(x)$ van ϑ. Is iedere wortel van $f(x) = 0$ ook wortel van $g(x)=0$, dan is $f(x) = c\{g(x)\}^k$, $k \geq 1$.

Bewijs: gr $f \geq$ gr g. Is gr f = gr g en $f(x) = a_0x^n + \ldots + a_n$, $a_0 \neq 1$ dan is $c = a_0$.
Is gr $f >$ gr g, dan volledige inductie. $f(x)$ is deelbaar door $g(x)$, dus $f(x) = q(x)g(x)$. Iedere wortel van $q(x) = 0$ is ook wortel van $f(x) = 0$, dus ook van $g(x) = 0$, $q(x)$ is van lagere graad dan $f(x)$, dus $q(x) = c_1\{g(x)\}^{k_1}$, en $f(x) = c_1\{g(x)\}^{k_1+1} = c\{g(x)\}^k$.

Stelling: Een irreducibele veelterm heeft met geen enkele veelterm $f(x)$ van lagere graad een wortel gemeen.

Bewijs: Gr $f <$ gr g, dan zou $f(x) = q(x)g(x)$ en gr $f >$ gr g. Tegenspraak.

Stelling: Iedere irreducibele veelterm bezit alleen enkelvoudige wortels.

Bewijs: Had $g(x) = 0$ meervoudige wortels, dan waren dit ook wortels van $g'(x) = 0$, en deze is van lagere graad.
Stel kanonieke vergelijking van ϑ in Ω is: $g(x) = x^n + \ldots + a_n = 0$. De wortels zijn $\vartheta = \vartheta_1, \vartheta_2, \ldots \vartheta_n$. Wij weten $\vartheta_i \neq \vartheta_j$.

Stelling: De graad van $\vartheta_2, \ldots \vartheta_n$ is ook n.

Bewijs: Stel graad van ϑ_2 was $m < n$, en de kanonieke vergelijking $f(x) = 0$. Daar $g(\vartheta_2) = 0$ en $f(\vartheta_2) = 0$, zou $g(x) = f(x)q(x)$, en zou $g(x)$ reducibel zijn.

Definitie: $\vartheta_1, \vartheta_2, \ldots \vartheta_n$ heten de aan ϑ toegevoegde getallen t.o.v. Ω. Deze hebben dus dezelfde kanonieke vergelijking.

Voorbeelden: $\vartheta = \sqrt[3]{2}$. Kanonieke vergelijking: $x^3 - 2 = 0$. Toegevoegde getallen: ϑ, $\vartheta(-\frac{1}{2}+\frac{1}{2}i\sqrt{3})$, $\vartheta(-\frac{1}{2}-\frac{1}{2}i\sqrt{3})$.
In P(i): $\vartheta = a + ib$, $b \neq 0$. Kanonieke vergelijking.
$x^2 - 2ax + a^2 + b^2 = 0$. Toegevoegde getallen $a + ib$ en $a - ib$.

Stelling: Is $f(x) = 0$ voor $\mathfrak{J}_1$, dan ook voor $\mathfrak{J}_2, \ldots \mathfrak{J}_n$.

Bewijs: Kanonieke vergelijking van $\mathfrak{J}_1$: $g(x) = 0$. Dan is $f(x) = g(x)q(x)$, dus $f(\mathfrak{J}_2) = \ldots = f(\mathfrak{J}_n) = 0$.

Gehele algebraïsche getallen. Lichaam is P. $\mathfrak{J}$ is algebraïsch met graad n. Kanonieke vergelijking van $\mathfrak{J}$: $x^n + a_1x^{n-1} + \ldots + a_n = 0$. De coëfficiënten zijn rationaal.

Definitie: Zijn alle coëfficiënten geheel rationaal, dan noemt men $\mathfrak{J}$ geheel algebraïsch.
Deze definitie is niet in strijd met het begrip "geheel" in P. Ook niet die in P(i).

Voorbeeld: $\sqrt[3]{2}$ is geheel algebraïsch.

In P is rationaal getal = $\frac{\text{geheel rationaal getal}}{\text{geheel rationaal getal}}$.
Nu de
Stelling: Een algebraïsch getal = $\frac{\text{geheel algebraïsch getal}}{\text{geheel rationaal getal}}$.

Bewijs: $\mathfrak{J}$ is algebraïsch met kanonieke vergelijking
$x^n + a_1x^{n-1} + \ldots + a_n = 0$, met a_i rationaal = $\frac{\text{geheel rationaal}}{\text{geheel rationaal}}$
Wij vermenigvuldigen met het product van de noemer, zodat de vergelijking wordt:

$b_0x^n + b_1x^{n-1} + \ldots + b_n = 0$ $(b_0 \neq 0)$, b_i geheel rationaal.

Stel $x = \frac{y}{b_0}$. Vergelijking wordt dan:

$y^n + b_1y^{n-1} + \ldots + b_0^{n-1}b_n = 0$. Deze vergelijking is kanoniek met geheel rationale coëfficiënten. Dus y = geheel algebraïsch.

$x = \frac{y}{b_0} = \frac{\text{geheel algebraïsch getal}}{\text{geheel rationaal getal}}$.

ALGEBRAISCHE GETALLENLICHAMEN III

door

Prof.Dr B. Meulenbeld

2 November 1955

Stelling. Laten $g(x)$ en $h(x)$ veeltermen zijn met geheel rationale coëfficiënten:

$$g(x)=a_1x^l+\ldots+a_o,\ (a_1,\ldots,a_o)=1,\ a_1\neq 0.$$
$$h(x)=b_mx^m+\ldots+b_o,\ (b_m,\ldots,b_o)=1,\ b_m\neq 0.$$

Zij $g(x)\ h(x)=c_{l+m}x^{l+m}+\ldots+c_o$. Dan is

$$(c_{l+m},\ldots,c_o)=1.$$

Bewijs. Ongerijmde. Was het gestelde niet waar, dan zou er een p zijn die deelbaar was op alle c_i. Daar $(a_1,\ldots a_o)=1$ en $(b_m,\ldots,b_o)=1$ is p niet deelbaar op alle a's en niet op alle b's. Er is dus een λ en een μ met $p\nmid a_\lambda$, $p\nmid b_\mu$ en $p\mid a_o,\ldots,p\mid a_{\lambda-1}$ (als $\lambda>0$), $p\mid b_o,\ldots,b_{\mu-1}$ (als $\mu>0$). Nu is

$$c_o=a_ob_o;\ c_1=a_ob_1+a_1b_o;\ c_2=a_ob_2+a_1b_1+a_2b_o;\ldots.$$

$$c_{\lambda+\mu}=a_ob_{\lambda+\mu}+a_1b_{\lambda+\mu-1}+\ldots+a_\lambda b_\mu+a_{\lambda+1}b_{\mu-1}+\ldots+a_{\lambda+\mu}b_o.$$

p is deelbaar op alle termen behalve op $a_\lambda b_\mu$, dus $p\nmid c_{\lambda+\mu}$. Tegenspraak.

Stelling. Laten $g(x)$ en $h(x)$ veeltermen zijn met geheel rationale coëfficiënten:

$$g(x)=a_1x^l+\ldots+a_o,\quad a_1\neq 0$$
$$h(x)=b_mx^m+\ldots+b_o,\quad b_m\neq 0$$
$$g(x)\ h(x)=c_{l+m}x^{l+m}+\ldots+c_o.\quad \text{Dan is}$$

$$(a_1,\ldots,a_o)(b_m,\ldots,b_o)=(c_{l+m},\ldots,c_o)$$

Bewijs. Noem $(a_1,\ldots,a_o)=A$, $(b_m,\ldots,b_o)=B$.

$\frac{g(x)}{A}=G(x)$, $\frac{h(x)}{B}=H(x)$. Dan is $\frac{g(x)\ h(x)}{AB}=G(x)\ H(x)$.

G(x) en H(x) voldoen aan de veronderstellingen van de vorige stelling.
Dus $(\frac{c_{l+m}}{AB},\ldots,\frac{c_o}{AB})=1$, of $(c_{l+m},\ldots,c_o)=AB$.

Stelling. Onder de veronderstellingen van de vorige stelling geldt, dat als k een geheel rationaal getal is met $k \mid c_\nu$ voor $\nu=0,\ldots,l+m$, ook

$$k \mid a_p b_q \text{ voor } p=0,\ldots,l;\ q=0,\ldots,m.$$

Bewijs: $k \mid (c_{l+m},\ldots,c_o)$, dus $k \mid (a_l,\ldots a_o)(b_m,\ldots,b_o)$ dus $k \mid a_p b_q$.

Stelling (van Gauss) Is een veelterm met geheel rationale coëfficiënten reducibel, dan is deze in twee veeltermen te splitsen met geheel rationale coëfficiënten.
Scherper: Uit $f(x)=f_1(x)f_2(x)$ ($f(x)$ geheel rationale coëfficiënten, $f_1(x)$ en $f_2(x)$ rationale coëfficiënten) volgt, dat bij geschikte rationale $p\neq 0$ de veeltermen $p\,f_1(x)$ en $\frac{1}{p}f_2(x)$ geheel rationale coëfficiënten hebben.
Bewijs. $f(x)=f_1(x)f_2(x)$.
$f_1(x)$ en $f_2(x)$ hebben rationale coëfficiënten. We kiezen nu twee natuurlijke getallen M en N zo, dat alle coëfficiënten van $M\,f_1(x)$ en $N\,f_2(x)$ geheel rationaal zijn.

$$M\,f_1(x)=g(x)=a_l x^l+\ldots+a_o,\quad a_i \text{ geheel rationaal}$$
$$N\,f_2(x)=h(x)=b_m x^m+\ldots+b_o,\quad b_i \text{ geheel rationaal}$$
$$MN\,f(x)=g(x)h(x)=c_{l+m}\,x^{l+m}+\ldots+c_o,\quad c_i \text{ geheel rationaal}$$

Volgens een der vorige stellingen is:

$$(a_l,\ldots,a_o)(b_m,\ldots,b_o)=(c_{l+m},\ldots,c_o)$$

Kortweg: $A\,B = C$.

Duidelijk is: $C=MNQ$, dus $AB=MNQ$.

$$MN\,f(x)=(a_l x^l+\ldots+a_o)(b_m x^m+\ldots+b_o)$$
$$f(x)=\frac{(a_l x^l+\ldots+a_o)}{A}\cdot\frac{(b_m x^m+\ldots+b_o)}{B}\cdot Q$$

Beide veeltermen rechts hebben geheel rationale coëfficiënten.

$$f(x)=\frac{M\,f_1(x)}{A}\cdot\frac{N\,f_2(x)}{B}\cdot Q$$

Noem $\frac{M}{A}=p$, dan is $\frac{NQ}{B}=\frac{1}{p}$; dus $f(x)=\{pf_1(x)\}\{\frac{1}{p}f_2(x)\}$.

Stelling. Is ϑ een wortel van een veelterm met hoogste coëfficiënt 1 en

geheel rationale coëfficiënten, dan is ϑ geheel.
Bewijs. Stel die veelterm is $g(x)=x^m+b_{m-1}x^{m-1}+\ldots+b_o$ en de bij ϑ behorende kanonieke veelterm is

$$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_o.$$

Te bewijzen is, dat alle a's geheel rationaal zijn.
Nu is $g(x)=q(x)f(x)$, $q(x)$ in P. De hoogste coëfficiënt in $q(x)$ (die van x^{m-n}) is hierbij =1.
Volgens de vorige stelling kunnen we nu een geschikte geheel rationale p vinden, zo dat $cq(x)$ en $\frac{1}{c}f(x)$ geheel rationale coëfficiënten hebben. x^{m-n} heeft in $cq(x)$ de coëfficiënt c; x^n heeft in $\frac{1}{c}f(x)$ de coëfficiënt $\frac{1}{c}$. Dus zijn c en $\frac{1}{c}$ geheel rationaal, dus $c=\pm 1$. Alle coëfficiënten in $f(x)$ zijn dus geheel rationaal.

Getallenlichaam Ω. ϑ is een willekeurig getal. Vormen nu $\Omega(\vartheta)$. Dit is het kleinste lichaam dat Ω omvat en ϑ bevat. Ligt ϑ in Ω, dan is $\Omega(\vartheta)\equiv\Omega$. Ligt ϑ niet in Ω, dan is $\Omega(\vartheta)>\Omega$.
Definitie. Is Ω een getallenlichaam, ϑ een relatief algebraïsch getal t.o.v. Ω, dan noemt men het lichaam, bestaande uit alle getallen van de vorm $\frac{F(\vartheta)}{G(\vartheta)}$, waarbij $F(x)$ en $G(x)$ veeltermen in Ω zijn en $G(\vartheta)\neq 0$.
een relatief algebraïsch getallenlichaam t.o.v. Ω.
(Dat het een getallenlichaam is, is zeer eenvoudig te bewijzen).
Is $\Omega=P$, dan spreekt men kortweg van algebraïsche getallenlichamen $P(\vartheta)$.
Voorbeeld. Getallenlichaam van Gauss P(i).
Stelling. Als ϑ de relatiefgraad n heeft t.o.v. Ω, dan kan men elk getal α van $\Omega(\vartheta)$ op eenduidige wijze schrijven in de vorm $\alpha=r(\vartheta)$, waarbij $r(x)\equiv 0$ is, of een veelterm is in Ω van hoogstens graad n-1.
Opmerking $\alpha=r(\vartheta)$ heet dan de karakteristieke schrijfwijze van ϑ.
Bewijs. Voor n=1 behoort ϑ tot Ω, en is de stelling triviaal.

$$\alpha=\frac{F(\vartheta)}{G(\vartheta)},\quad G(\vartheta)\neq 0.$$

Laten $\vartheta_1,\ldots,\vartheta_n$ de relatief toegevoegde getallen van ϑ zijn, met $\vartheta_1=\vartheta$. Dan is ook $G(\vartheta_i)\neq 0$, voor $i=1,2,\ldots,n$.
We schrijven

$$\alpha=\frac{F(\vartheta_1)G(\vartheta_2)\ldots G(\vartheta_n)}{G(\vartheta_1)G(\vartheta_2)\ldots G(\vartheta_n)}.$$

Volgens de stelling van de symmetrische functies is de noemer rationaal uit te drukken in de coëfficiënt van de kanonieke vergelijking van ϑ, is dus gelijk aan een getal β uit Ω.
Is de kanonieke veelterm van ϑ $f(x)$, dan is dus

$$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_0=(x-\vartheta_1)\ldots(x-\vartheta_n)$$

Nu is

$$(x-\vartheta_2)\ldots(x-\vartheta_n)=\frac{f(x)-f(\vartheta_1)}{x-\vartheta_1}=x^{n-1}+g_{n-2}(\vartheta_1)x^{n-2}+\ldots+g_0(\vartheta_1),$$

waarbij $g_{n-2}(\vartheta_1),\ldots,g_0(\vartheta_1)$ veeltermen in Ω zijn.
Dus is $G(\vartheta_2)\ldots G(\vartheta_n)=F_1(\vartheta_1)$, met $F(x)$ in Ω, en

$$\alpha=\frac{F(\vartheta_1)F_1(\vartheta_1)}{\beta}=g(\vartheta_1) \text{ met } g(x) \text{ in } \Omega.$$

Verder is $g(x)=q(x)f(x)+r(x)$ met graad $r(x)\leq n-1$, alles in Ω.

$$\alpha=g(\vartheta_1)=q(\vartheta_1)f(\vartheta_1)+r(\vartheta_1)=r(\vartheta_1).$$

<u>Eenduidigheid</u>: Was $\alpha=r_1(\vartheta)=r_2(\vartheta)$, dan zou $r_1(\vartheta)-r_2(\vartheta)=0$, en ϑ voldoen aan een vergelijking met lagere graad dan n. Tegenspraak.
Elke α uit $\Omega(\vartheta)$ is dus voor te stellen door de karakteristieke schrijfwijze:

$$\alpha=c_0+c_1\vartheta+\ldots c_{n-1}\vartheta^{n-1}. \quad (c_i \text{ in } \Omega)$$

<u>Voorbeeld</u>. $P(\sqrt[7]{2})$.

$$\alpha=\frac{8+\sqrt[7]{2}+\sqrt[7]{2^2}}{6\sqrt[7]{2^6}-\sqrt[7]{2^5}+7\sqrt[7]{2}-2} \text{ is altijd te brengen in de vorm:}$$

$c_0+c_1\sqrt[7]{2}+c_2\sqrt[7]{2^2}+\ldots+c_6\sqrt[7]{2^6}$, met $c_0,\ldots,c_6$ rationaal.

<u>Stelling</u>. ϑ heeft relatief graad n t.o.v. Ω, $\vartheta_1,\ldots\vartheta_n$ zijn toegevoegd aan $\vartheta=\vartheta_1$. Is $\alpha=R(\vartheta)$ ($R(x)$ veelterm in Ω), en $r(x)$ de in de karakteristieke schrijfwijze optredende veelterm, dan is $R(\vartheta_\nu)=r(\vartheta_\nu)$ voor $\nu=1,2,\ldots n$.
<u>Bewijs</u>. Uit $R(\vartheta)-r(\vartheta)=0$ volgt $R(\vartheta_\nu)-r(\vartheta_\nu)=0$.
<u>Stelling</u> 1. ϑ heeft relatief graad n t.o.v. Ω. α is een willekeurig getal in $\Omega(\vartheta)$. Dan is α relatief algebraïsch t.o.v. Ω voor relatief graad l, waarbij l een deler van n is;

2. l is het aantal verschillende onder de getallen $r(\vartheta_1),\ldots,r(\vartheta_n)$ waarbij $r(\vartheta)$ de karakteristieke schrijfwijze voorstelt;

3. Elk der verschillende getallen $r(\vartheta_1),\ldots r(\vartheta_n)$ komt $\frac{n}{l}$ maal voor;

4. De verschillende van deze getallen zijn de aan α toegevoegde getallen.

<u>Bewijs</u>. $\{x-r(\vartheta_1)\}\{x-r(\vartheta_2)\}\ldots\{x-r(\vartheta_n)\}=0 \qquad (A)$

heeft wortel α . Volgens de stelling der symmetrische functies zijn de coëfficiënten van deze veelterm in het linkerlid getallen in Ω. α is dus algebraïsch van de graad $1 \leqq n$.
Kanonieke vergelijking van α: $x^1+b_1x^{1-1}+\ldots+b_1=0$. $\alpha_i \neq \alpha_j$ (B)
b_i in Ω. Een der wortels is $\alpha=r(\vartheta)$. Dus zijn ook wortels: $r(\vartheta_2),\ldots,r(\vartheta_n)$. Alle wortels van (A) zijn ook wortels van (B). Dus volgens een vroegere stelling:

$$\left\{x-r(\vartheta_1)\right\}\ldots\left\{x-r(\vartheta_n)\right\}=c\left\{x^1+b_1x^{1-1}+\ldots+b_1\right\}^k \qquad (c \text{ in } \Omega)$$

Eerste coëfficiënten zijn =1, dus c=1; en n=lk $\qquad k \geqq 1$
Hiermede alles bewezen.

Stelling. Is $\Omega(\vartheta)=\Omega(\Theta)$, dan hebben ϑ en Θ dezelfde relatief graad.
Bewijs. Stel ϑ heeft relatief graad n, en Θ m. Volgens de vorige stelling is, daar Θ tot $\Omega(\vartheta)$ behoort, $m \leqq n$. Evenzo is $n \leqq m$, dus m=n.
De relatief graad van alle voortbrengende getallen van een relatief algebraïsch getallenlichaam t.o.v. Ω is onafhankelijk van dat voortbrengend getal. Men spreekt daarom van de relatief graad van een relatief algebraïsch getallenlichaam. Is $\Omega=P$, dan spreekt men kortweg van de graad van het algebraïsch getallenlichaam.
Voorbeeld. $\alpha = \sqrt[7]{2}$ is van de graad 7. Alle getallen van $P(\sqrt[7]{2})$ zijn voor te stellen door

$$\beta=c_0+c_1\sqrt[7]{2}+\ldots+c_6\sqrt[7]{2^6}.$$

De graad van β is een deler van 7, dus 1 of 7. Is dit 1, dan is β rationaal en $c_1=c_2=\ldots=c_6=0$. Is minstens één der zes getallen $c_1,\ldots,c_6 \neq 0$, dan is β van graad 7.
Stelling. De relatief algebraïsche getallen t.o.v. Ω vormen een getallenlichaam.
Bewijs. We moeten bewijzen dat als α en β relatief algebraïsch t.o.v. Ω zijn, ook $\alpha \pm \beta$, $\alpha\beta$ en $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ dit zijn.
Is β relatief algebraïsch, dan ook $\frac{1}{\beta}$. Immers voldoet β aan

$$\beta^m+b_{m-1}\beta^{m-1}+\ldots+b_0=0, \text{ dan voldoet } \frac{1}{\beta} \text{ aan}$$

$$\left(\frac{1}{\beta}\right)^m b_0+\left(\frac{1}{\beta}\right)^{m-1} b_1+\ldots+1=0.$$

Het bewijs voor $\frac{\alpha}{\beta}$ is dus terug te brengen tot dat van $\alpha \cdot \frac{1}{\beta}$.
Duidelijk is dat met β ook $-\beta$ relatief algebraïsch is. Het bewijs voor $\alpha-\beta$ dus terug te brengen tot dat van $\alpha+(-\beta)$.
We moeten dus bewijzen dat $\alpha+\beta$ en $\alpha\beta$ relatief algebraïsch zijn.

1. $\alpha+\beta$ is relatief algebraïsch.

α is algebraïsch. Kanonieke vergelijking: $x^n+a_{n-1}x^{n-1}+\ldots+a_n=0$.

β is algebraïsch. Kanonieke vergelijking $x^m+b_{m-1}\,x^{m-1}+\ldots+b_m=0$ (a_i en b_i in Ω).

Ik vorm nu de getallen:

$$\eta_{N,M}=\alpha^N\beta^M \qquad \begin{matrix} N=0,1,2,\ldots,n-1 \\ M=0,1,2,\ldots,m-1 \end{matrix} \Big\} \quad \text{totaal } nm=k \text{ getallen } \eta_1,\ldots,\eta_k$$

$\eta_{o,o}=1$. Nu is

$$\alpha\eta_{N,M}=\alpha^{N+1}\beta^M=\eta_{N+1,M} \quad \text{voor } N\leq n-2.$$

Is N=n-1 dan $\alpha\eta_{n-1,M}=\alpha^n\beta^M=-\beta^M(a_1\alpha^{n-1}+\ldots+a_n)$

$=-a_1\eta_{n-1,M}-a_2\eta_{n-2,M}\cdots-a_n\eta_{o,M}$ en is dus een som van η's.
Geldt ook als men vormt $\beta\eta_{N.M}$.
Steeds geldt dus:

$$\alpha\eta_r=A_{r,1}\eta_1+A_{r,2}\eta_2+\ldots+A_{r,k}\eta_k \qquad (A\text{'s in }\Omega)$$

$$\beta\eta_r=B_{r,1}\eta_1+B_{r,2}\eta_2+\ldots+B_{r,k}\eta_k \qquad (B\text{'s in }\Omega)$$

Stel $\alpha+\beta=\gamma$, dan is

$$\gamma\eta_r=C_{r,1}\eta_1+C_{r,2}\eta_2+\ldots+C_{r,k}\eta_k \quad \text{voor } r=1,2,\ldots,k \quad (C\text{'s in }\Omega).$$

Hier staan k lineaire homogene vergelijkingen met k onbekenden $\eta_1,\ldots,\eta_k$.
Alle η's zijn niet 0, want $\eta_1=\eta_{o,o}=1$. Dus de determinant =0.

$$\begin{vmatrix} C_{11}-\gamma & C_{12}\cdots & C_{1k} \\ C_{21} & C_{22}-\gamma\ldots & C_{2k} \\ & & \\ C_{k1} & C_{k2}\cdots & C_{kk} \end{vmatrix} =0$$

Hier staat een vergelijking in γ van de graad k=mn. De coëfficiënten liggen in Ω. Dus $\gamma=\alpha+\beta$ is relatief algebraïsch t.o.v. Ω. met graad $\leq$ mn.
Is $\Omega=P$, dan hebben we hiermede nog meer bewezen voor het geval dat α en β geheel algebraïsch zijn. In dit geval zijn de A's, B's en C's geheel rationaal. De hoogste coëfficiënt van de vergelijking in γ is =1. Dus is dan ook $\gamma=\alpha+\beta$ geheel algebraïsch. Op analoge wijze bewijst men:
2. $\alpha\beta$ is relatief algebraïsch; en als α en β geheel algebraïsch zijn, dan is $\alpha\beta$ dit ook.

ALGEBRAISCHE GETALLENLICHAMEN IV

door

Prof.Dr B. Meulenbeld

16 November 1955

Stelling.

1. Is $\mu^r+\alpha\mu^{r-1}+\beta\mu^{r-2}+\ldots+\kappa\mu+\lambda=0$ $(r>0)$, en zijn $\alpha,\beta,\ldots,\kappa,\lambda$ algebraisch, dan is μ algebraisch.

2. Zijn de coëfficiënten bovendien geheel, dan is μ geheel.

$\alpha,\beta,\ldots$ zijn algebraisch, voldoen dus aan vergelijking:

$$\alpha^u+a_{n-1}\alpha^{n-1}+\ldots+a_0=0,$$

$$\beta^m+b_{m-1}\beta^{m-1}+\ldots+b_0=0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\lambda^q+l_{q-1}\lambda^{q-1}+\ldots+l_0=0,$$

met rationale (c.q. geheel rationale) coëfficiënten.
Noem nm...qr=k, en noem de getallen $\eta_1,\eta_2,\ldots,\eta_k$

$$\alpha^N\beta^M\ldots\lambda^Q\mu^R \text{ met } \begin{cases} N=0,1,\ldots,u-1,\\ M=0,1,\ldots,m-1,\\ \cdots\cdots\cdots\\ Q=0,1,\ldots,q-1,\\ R=0,1,\ldots,r-1. \end{cases} \quad \eta_1=1\neq 0.$$

$\mu\eta=\alpha^N\beta^M\ldots\lambda^Q\mu^{R+1}$. Is $R<r-1$ dan is $\mu\eta$ een andere η. Is $R=r-1$, dan is $\mu\eta=\alpha^N\beta^M\ldots\lambda^Q\mu^r=\alpha^N\beta^M\ldots\lambda^Q(-\alpha\mu^{r-1}-\ldots-\lambda)$

$$(1)=-\alpha^{N+1}\beta^M\ldots\lambda^Q\mu^{r-1}-\alpha^N\beta^{M+1}\lambda^Q\mu^{r-2}-\ldots-\alpha^N\beta^M\ldots\lambda^{Q+1}$$

Hierin is

$$\alpha^{N+1}\beta^M\ldots\lambda^Q\mu^{r-1}=\begin{cases}\text{een andere } \eta \text{ als } N<n-1\\ \beta^M\ldots\lambda^Q\mu^{r-1}(-a_{n-1}\alpha^{n-1}-\ldots-a_0) \text{ als } N=n-1.\end{cases}$$

In ieder geval is

$$\alpha^{N+1}\beta^M\ldots\lambda\mu^{r-1}=c_1\eta_1+\ldots+c_k\eta_k$$ met rationale (c.q. geheel rationale)coëfficiënten.

Dit past men toe op alle andere termen van (1).
Dus $\mu\eta=d_1\eta_1+\ldots+d_k\eta_k$ met rationale (c.q. geheel rationale) coëfficiënten. Bewijzen dan weer met de determinant dat μ algebraisch (c.q. geheel) is.

Gevolg. Elk relatief algebraisch getal t.o.v. een algebraisch lichaam is een algebraisch getal.

Stelling. Bij twee algebraische getallen α en β t.o.v. Ω bestaat er een algebraisch getallenlichaam $\Omega(\tau)$, waartoe α en β behoren. τ laat zich zelfs schrijven in de vorm $\tau = v\alpha+\beta$, waarin men v geheel rationaal kan kiezen.
Dit is de stelling van Abel. Met deze stelling kan men dus de adjunctie van meerdere algebraische getallen terug brengen tot die van één algebraisch getal.

Bewijs. (van der Waerden). Het is duidelijk dat $\Omega(\alpha,\beta)\supset\Omega(\tau)$. We moeten bewijzen: $\Omega(\alpha,\beta)=\Omega(\tau)$, dus dat ieder getal van $\Omega(\alpha,\beta)$ behoort tot $\Omega(\tau)$. Voldoende is te bewijzen dat α en β tot $\Omega(\tau)$ behoren.

α is algebraisch t.o.v. Ω, voldoet dus aan $f(\alpha)=0$ met graad n, coëfficiënten in Ω. β is algebraisch t.o.v. Ω, voldoet dus aan $g(\beta)=0$ met graad m, coëfficiënten in Ω. Toegevoegde getallen $\alpha=\alpha_1,\alpha_2,..\alpha_n$, resp. $\beta=\beta_1,\beta_2,\ldots,\beta_m$. Dus $\alpha_i\neq\alpha_1$ voor $2,3,\ldots,n$, en $\beta_i\neq\beta_1$ voor $i=2,3,..,m$. We vermijden nu dat $\alpha_i+v\beta_j=\alpha_1+v\beta_1$, of
$v=\frac{\alpha_i-\alpha_1}{\beta_1-\beta_j}$. $(i=2,\ldots n;\ j=2,\ldots,m)$.
Kies dus v zo dat $v\neq\frac{\alpha_i-\alpha_1}{\beta_1-\beta_j}$, kunnen deze dus zelfs geheel rationaal kiezen.
Nu is $\tau=\alpha_1+v\beta_1=\alpha+v\beta$, τ is element van $\Omega(\alpha,\beta)$. β voldoet aan $g(\beta)=0$ en aan $f(\alpha)=f(\tau-v\beta)=0$, alles met coëfficiënten in Ω, dus de vergelijkingen: $g(x)=0$ en $f(\tau-vx)=0$ hebben de wortel β gemeen. Voor de andere wortels zijn $\tau-v\beta_i\neq\alpha_j$. β is enkelvoudige wortel van $g(x)$, dus hebben $g(x)$ en $f(\tau-vx)$ slechts de factor $x-\beta$ gemeen. De g.g.d. van deze veeltermen is dus $x-\beta$. Uit de bepaling van de g.g.d. volgt dat de coëfficiënten van deze g.g.d. $x-\beta$ in $\Omega(\tau)$ liggen, dus β ligt in $\Omega(\tau)$. Uit $\alpha=\tau-\beta$ volgt dat ook α in $\Omega(\tau)$ ligt. Dus $\Omega(\alpha,\beta)=\Omega(\tau)$.

Stelling: Is $f(x)=\delta_r x^r+\ldots+\delta_1 x+\delta_0$ ($\delta_r\neq0$, alle δ geheel) en is μ wortel van $f(x)=0$, dan is $\delta_r\mu$ geheel.

Bewijs.
$$(\delta_r\mu)^r+\delta_{r-1}(\delta_r\mu)^{r-1}+\delta_r\delta_{r-2}(\delta_r\mu)^{r-2}+\ldots+\delta_r^{r-2}\delta_1(\delta_r\mu)+$$
$$+\delta_r^{r-1}\delta_0=0.$$
De coëfficiënten zijn als product van gehele getallen weer geheel.

Stelling. De veelterm $\frac{f(x)}{x-\mu}$ heeft gehele coëfficiënten.

Bewijs: (Volledige inductie). Voor $r=1$ is dit duidelijk, immers dan is $f(x)=\delta_1(x-\mu)$.
Stel $r>1$ en de stelling tot aan $r-1$ bewezen. De veelterm
$f(x)-(x-\mu)\delta_r x^{r-1}=f(x)-\delta_r x^r+\delta_r\mu x^{r-1}=g(x)$ heeft gehele coëfficiën-

ten (volgens de vorige stelling is $\delta_r \mu$ geheel). $g(x)$ is van graad $\leq r-1$, is dus volgens inductie-onderstelling $g(x)=(x-\mu)h(x)$, waarin $h(x)$ gehele coëfficiënten heeft wegens

$$f(x)=(x-\mu)/(\delta_r x^{r-1}+h(x))$$

heeft ook $\frac{f(x)}{x-\mu}$ gehele coëfficiënten.

Stelling. Zijn $\mu_1,\ldots\mu_R$ $(1\leq R\leq r)$ willekeurig gekozen wortels van $f(x)$, dan is $\delta_r\mu_1,\ldots\mu_R$ geheel.

Bewijs. Door telkens de vorige stelling toe te passen vindt men, als men $f(x)=\delta_r(x-\mu_1)\ldots(x-\mu_R)\ldots(x-\mu_r)$ stelt, dat

$$\frac{f(x)}{x-\mu_r},\ \frac{f(x)}{(x-\mu_r)(x-\mu_{r-1})},\ldots,\ \frac{f(x)}{(x-\mu_r)\ldots(x-\mu_{R+1})}=\delta_r(x-\mu_1)\ldots(x-\mu_R)$$

gehele coëfficiënten heeft. De bekende term hiervan is $\pm\delta_r\mu_1\ldots\mu_r$, dus is deze geheel.

Definitie. Laten α en β geheel zijn, $\beta\neq 0$. Dan heet β deelbaar door α, als $\frac{\beta}{\alpha}$ geheel is.

Stelling. Uit $\alpha\mid\beta$, $\beta\mid\gamma$ volgt $\alpha\mid\gamma$.

Stelling. Uit $\alpha\mid\beta_1,\ldots,\alpha\mid\beta_n$ volgt bij willekeurige gehele $\lambda_1,\ldots,\lambda_n$ dat $\alpha\mid\beta_1\lambda_1+\ldots+\beta_n\lambda_n$.

Stelling van Kronecker. Zijn

$$g(x)=\alpha_l x^l+\ldots+\alpha_0 \quad (\alpha_l\neq 0)$$

$$h(x)=\beta_m x^m+\ldots+\beta_0 \quad (\beta_m\neq 0),\quad \alpha \text{ en } \beta \text{ geheel}$$

$g(x)h(x)=\gamma_{l+m}x^{l+m}+\ldots+\gamma_0$, waarbij dus de γ geheel zijn. Is nu λ geheel $\neq 0$, en λ/γ_q $(0\leq q\leq l+m)$ dan is $\lambda/\alpha_L\beta_M$ voor $0\leq L\leq l$, $0\leq M\leq m$.

Opmerking. De omgekeerde stelling is triviaal.

Bewijs. Voor $l=0$ of $m=0$ is de stelling triviaal. Stel dus $l>0$, $m>0$.

$$g(x)=\alpha_l(x-\xi_1)\ldots(x-\xi_l)$$

$$h(x)=\beta_m(x-\eta_1)\ldots(x-\eta_m), \text{ dus is}$$

$$\frac{g(x)h(x)}{\lambda}=\frac{\alpha_l\beta_m}{\lambda}(x-\xi_1)\ldots(x-\eta_m)$$

Deze veelterm heeft volgens het gegeven gehele coëfficiënten, en is dus $\frac{\alpha_l\beta_m}{\lambda}\xi'\xi''\ldots\eta'\eta''$ geheel volgens een der vorige stellingen. Verder is

$$\alpha_L=\pm\alpha_l\textstyle\sum\xi'\xi''\ldots,$$

$$\beta_M=\pm\beta_m\textstyle\sum\eta'\eta''\ldots.$$

(elementair-symmetrische functies). Dus is

$$\frac{\alpha_L \beta_M}{\lambda} = \sum \pm \frac{\alpha_1 \beta_m}{\lambda} \xi' \xi'' .. \eta' \eta'' \quad \text{geheel,}$$

en dus $\lambda \mid \alpha_L \beta_M$.

Stelling. Het lichaam van alle algebraische getallen is geen algebraisch getallenlichaam.

Bewijs. Stel dat het lichaam van graad n was. Dan zou elk getal van dit lichaam van een graad $\leq$ n zijn; maar $\sqrt[n+1]{2}$ is een algebraisch getal, en van graad n+1.

Definitie. Als α een getal van een algebraisch lichaam van de n^{de} graad is, dan worden $N(\alpha)$ (de norm van α) en $S(\alpha)$ (de spoor van α) gedefinieerd als

$$N(\alpha)=r(\vartheta_1)r(\vartheta_2)\ldots r(\vartheta_n)$$
$$S(\alpha)=r(\vartheta_1)+r(\vartheta_2)+\ldots+r(\vartheta_n).$$

In P is $N(a)=a$. In P(i) is $N(\alpha)=N(a+ib)=(a+ib)(a-ib)=a^2+b^2$, in overeenstemming met de vroegere definitie.

Stelling. $N(\alpha)$ en $S(\alpha)$ zijn rationaal; is α geheel, dan zelfs geheel rationaal.

Bewijs. $N(\alpha)$ is volgens een vroegere stelling de $\frac{n}{I}$ - de macht van het product van de aan α toegevoegde getallen, $S(\alpha)$ het $\frac{n}{I}$ voud van de som. Dit product en deze som zijn als elementaire symmetrische functies van de wortels van de kanonieke veelterm van α rationaal c.q. geheel rationaal.

Stelling. Is a rationaal, dan is $N(a)=a^n$.

Bewijs: De karakteristieke schrijfwijze is a, dus

$$N(a) = a..a=a^n.$$

Stelling. $N(\alpha\beta)=N(\alpha)N(\beta)$, $S(\alpha+\beta)=S(\alpha)+S(\beta)$.

Bewijs. Karakteristieke schrijfwijzen:

$$\alpha=r_1(\vartheta);\ \beta=r_2(\vartheta);\ \text{dus } \alpha\beta=r_1(\vartheta)r_2(\vartheta).$$

De veelterm $R(x)=r_1(x)r_2(x)$ kan best hogere graad dan n-1 hebben; men vindt toch de toegevoegde getallen van $\alpha\beta$, door ϑ te vervangen door $\vartheta_2, \vartheta_3, \ldots, \vartheta_n$. Dus

$$N(\alpha\beta)=R(\vartheta_1)\ldots R(\vartheta_n)=r_1(\vartheta_1)\ldots r_1(\vartheta_n)r_2(\vartheta_1)..r_2(\vartheta_n)=N(\alpha)N(\beta).$$

$\alpha+\beta=r_1(\vartheta)+r_2(\vartheta)$. Dus

$$S(\alpha+\beta)=\left\{r_1(\vartheta_1)+r_2(\vartheta_1)\right\}+\left\{r_1(\vartheta_2)+..r_2(\vartheta_2)\right\}+..\left\{r_1(\vartheta_n)+r_2(\vartheta_n)\right\}$$
$$=S(\alpha)+S(\beta).$$

Stelling. $N(a\alpha)=a^nN(\alpha)$; $S(a\alpha)=aS(\alpha)$ voor rationale a.

Bewijs. $N(a\alpha)=N(a)N(\alpha)=a^nN(\alpha)$. Uit $\alpha=r(\vartheta)$ volgt $a\alpha=ar(\vartheta)$. Dus

$$S(a\alpha)=ar(\vartheta_1)+..+ar(\vartheta_n)=a\left\{r(\vartheta_1)+..r(\vartheta_n)\right\}=aS(\alpha).$$

Definitie. Laten $\alpha_1,..\alpha_n$ getallen zijn van het lichaam $P(\vartheta)$ van graad n. Zijn $r_1(x),..,r_n(x)$ de veeltermen van de karakteristieke schrijfwijzen, dan noemt men

$$\Delta(\alpha_1,..,\alpha_n)=\begin{vmatrix} r_1(\vartheta_1)r_1(\vartheta_2)\ldots r_1(\vartheta_n)\\ r_2(\vartheta_1)r_2(\vartheta_2)\ldots r_2(\vartheta_n)\\ \ldots\ldots\ldots\ldots\ldots\\ r_n(\vartheta_1)r_n(\vartheta_2)..r_n(\vartheta_n)\end{vmatrix}^2$$

de discriminant van de n getallen

Stelling. $\Delta(\alpha_1,..,\alpha_n)$ is 1) onafhankelijk van de volgorde der getallen $\alpha_1,..,\alpha_n$; 2) onafhankelijk van de volgorde van $\vartheta_1,..,\vartheta_n$; 3) onafhankelijk van het getal ϑ, dat het lichaam genereert (Δ hangt dus alleen af van α en van het lichaam). 4) een rationaal getal. 5) als α geheel is, een geheel rationaal getal.

Bewijs. 1) Verwisseling van de α's geeft een verwisseling van de rijen.
2) Verwisseling van de ϑ's geeft een verwisseling van de kolommen.
3) Rekent men het kwadraat van de determinant uit, dan vindt men

$$\Delta=\begin{vmatrix} S(\alpha_1\alpha_1) & S(\alpha_1\alpha_2)..S(\alpha_1\alpha_n)\\ S(\alpha_2\alpha_1) & S(\alpha_2\alpha_2)..S(\alpha_2\alpha_n)\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ S(\alpha_n\alpha_1) & S(\alpha_n\alpha_2)..S(\alpha_n\alpha_n)\end{vmatrix}$$

Elke S is van ϑ onafhankelijk, dus Δ ook.

4) Elke S is een rationaal getal, dus Δ ook.
5) Zijn de α's geheel, dan zijn de S geheel rationaal, dus de Δ ook.

Stelling. Zijn $\beta_1,\ldots,\beta_n$ getallen van $P(\vartheta)$, de n^2 getallen $c_{ij}(i=1,..,n;\ j=1,..,n)$ rationaal, en voert men uit de lineaire substitutie: $\alpha_i=\sum_j c_{ij}\beta_j$ (α's zijn dus ook getallen uit $P(\vartheta)$), dan is

$$\Delta(\alpha_1,..,\alpha_n)=\left|c_{ij}\right|^2\Delta(\beta_1,..,\beta_n).$$

Bewijs. Stel $\beta_i=Q_i(\vartheta)$, dan is

$$\Delta(\alpha_1,\ldots,\alpha_n)=$$

$$= \begin{vmatrix} c_{11}Q_1(\vartheta_1)+c_{12}Q_2(\vartheta_1)+\ldots+c_{1n}Q_n(\vartheta_1) & \ldots & c_{11}Q_1(\vartheta_n)+c_{12}Q_2(\vartheta_n)+\ldots+c_{1n}Q_n(\vartheta_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n1}Q_1(\vartheta_1)+c_{n2}Q_2(\vartheta_1)+\ldots+c_{nn}Q_n(\vartheta_1) & \ldots & c_{n1}Q_1(\vartheta_n)+c_{n2}Q_2(\vartheta_n)+\ldots+c_{nn}Q_n(\vartheta_n) \end{vmatrix}^2$$

$$= \begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ \ldots\ldots\ldots\ldots & & & \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix}^2 \begin{vmatrix} Q_1(\vartheta_1) & Q_1(\vartheta_2) & \ldots & Q_1(\vartheta_n) \\ \ldots\ldots\ldots\ldots & \ldots\ldots & & \\ Q_n(\vartheta_1) & Q_n(\vartheta_2) & \ldots & Q_n(\vartheta_n) \end{vmatrix}^2 ,$$

dus $\Delta(\alpha_1,\ldots,\alpha_n)= |c_{ij}|^2 \Delta(\beta_1,\ldots\beta_n)$.

ALGEBRAISCHE GETALLENLICHAMEN V

door

Prof.Dr B. Meulenbeld

30 November 1955

Stelling. Als ϑ het genererend getal van het algebraïsche lichaam is, dan is $\Delta(1,\vartheta,..,\vartheta^{n-1})\neq 0$.

Bewijs. Voor n=1 is $\Delta(1)=1$. Voor $n>1$ is

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \vartheta_1 & \vartheta_2 & & \vartheta_n \\ \dots & \dots & & \dots \\ \vartheta_1^{n-1} & \vartheta_2^{n-1} & \dots & \vartheta_n^{n-1} \end{vmatrix} = \prod_{1\leq k<i\leq n}(\vartheta_i-\vartheta_k)\neq 0$$

en $\Delta(1,\vartheta,..,\vartheta^{n-1})$ is hiervan het kwadraat.

Definitie. q complexe getallen $\xi_1,..,\xi_q$ heten lineair onafhankelijk, als uit iedere vergelijking

$$a_1\xi_1+\dots+a_q\xi_q=0 \quad (a_i \text{ rationaal})$$

volgt: $a_1=..=a_q=0$. Anders heten ze lineair afhankelijk.

Voorbeeld. De getallen $1,\vartheta,..,\vartheta^{n-1}$ zijn lineair onafhankelijk.

Stelling. Elk n+1-tal getallen $\alpha_1\dots\alpha_{n+1}$ van het lichaam zijn lineair afhankelijk.

Bewijs. We stellen de karakteristieke schrijfwijzen van $\alpha_1,\dots,\alpha_{n+1}$:

$$\alpha_i=b_{i1}+b_{i2}\vartheta+\dots+b_{in}\vartheta^{n-1} \quad (i=1,2,..,n+1)$$

Men kan nu altijd rationale $c_1,\dots,c_{n+1}$ vinden, welke niet alle 0 zijn met

$$c_1\alpha_1+\dots+c_{n+1}\alpha_{n+1}=0.$$

Immers uit $\sum_{i=0}^{n-1}\vartheta^i\sum_{k=1}^{n+1}b_{k,i}\,c_k=0$ zou volgen

$$\sum_{k=1}^{n+1}b_{k,i}\,c_k=0 \quad \text{voor } i=0,1,..,n-1.$$

Uit deze n vergelijkingen met n+1 onbekenden zijn altijd de c_i op te lossen, waarbij niet alle c_i gelijk 0 zijn.

Stelling. $\Delta(\alpha_1,..,\alpha_n)$ is dan en slechts dan $\neq 0$, als $\alpha_1,\dots,\alpha_n$ lineair onafhankelijk zijn. Verder is het teken van $\Delta(\alpha_1,..,\alpha_n)$ voor alle systemen van lineair onafhankelijke $\alpha_1,..,\alpha_n$ hetzelfde, dus door het lichaam bepaald.

Bewijs. Karakteristieke schrijfwijze: $\alpha_k=r_k(\vartheta)=\sum_{i=1}^{n}c_{ki}\vartheta^{i-1}\ (1\leq k\leq n)$

met rationale c_{ki}, dus is

$$\Delta(\alpha_1,..,\alpha_n) = |c_{ki}|^2 \Delta(1,..,\vartheta^{n-1}).$$

$\Delta(\alpha_1,..,\alpha_n)$ is dus dan en alleen dan $=0$ als $|c_{ki}|=0$ is, en heeft voor $|c_{ki}| \gtrless 0$ een van de α's onafhankelijk teken. Verder zou uit $a_1\alpha_1+...+a_n\alpha_n=0$ (a_i rationaal),

$$\text{dus} \quad \sum_{k=1}^{n} a_k\alpha_k = \sum_{i=1}^{n} \vartheta^{i-1} \sum_{k=1}^{n} c_{ki}\, a_k = 0$$

volgen (zie bewijs vorige stelling) $\sum_{k=1}^{n} c_{ki}\, a_k = 0$,

en dit stel vergelijkingen heeft dan en alleen dan een oplossing met niet alle a's gelijk aan 0, als $|c_{ki}|=0$.

Stelling. Als $\omega_1,..,\omega_n$ lineair onafhankelijke getallen van het lichaam zijn, dan is elk getal α van het lichaam te schrijven in de gedaante

$$(1) \qquad \alpha = b_1\omega_1+...+b_n\omega_n,$$

met rationale b_i. Deze schrijfwijze is eenduidig.

Bewijs. $\omega_1,...,\omega_n, \alpha$ zijn lineair afhankelijk; dus bestaat er een betrekking:

$$c_1\omega_1+..+c_n\omega_n+c_{n+1}\alpha=0,$$

waarin $c_1,..,c_{n+1}$ rationaal zijn en niet alle $=0$. Verder is $c_{n+1}\neq 0$, daar anders $c_1,..,c_n$ lineair afhankelijk zouden zijn. Dus is

$$\alpha = -\frac{c_1}{c_{n+1}}\omega_1 - \cdots - \frac{c_n}{c_{n+1}}\omega_n = b_1\omega_1+..+b_n\omega_n.$$

De eenduidigheid volgt uit de lineaire onafhankelijkheid van $\omega_1,..,\omega_n$.

Stelling. Er bestaat in het lichaam een systeem van n lineaire onafhankelijke gehele getallen $\omega_1,..,\omega_n$ zodat ieder geheel getal α van het lichaam eenduidig in de vorm (1) te schrijven is met geheel rationale b's.

Opmerking. Daar omgekeerd bij geheel rationale b zeker $b_1\omega_1+..+b_n\omega_n$ geheel is, zijn dus hierdoor alle gehele getallen van het lichaam voorgesteld, en wel ieder precies eenmaal, als de b's onafhankelijk alle systemen van geheel rationale getallen doorloopt.

Bewijs. Men kan altijd in een lichaam een systeem van n lineair onafhankelijk gehele getallen $\omega_1,..,\omega_n$ vinden. Neem nl. n willekeurige lineair onafhankelijke getallen $\alpha_1,...,\alpha_n$ (bijv: $1,\vartheta,..,\vartheta^{n-1}$), dan kan men (zie vroegere stelling) steeds geschikte natuurlijke getallen

$g_1,..,g_n$ vinden, zodat $g_1\alpha_1,\ldots,g_n\alpha_n$ geheel zijn. Noem deze $\omega_1,\ldots,\omega_n$. Voor deze getallen is $|\Delta(\omega_1,\ldots,\omega_n)|$ een natuurlijk getal. Laten nu $\omega_1,..,\omega_n$ zo gekozen zijn dat $|\Delta(\omega_1,\ldots,\omega_n)|$ zo klein mogelijk is. We bewezen dat deze $\omega_1,\ldots,\omega_n$ aan de eisen van de stelling voldoet. Stel er was een geheel getal

$$\alpha = b_1\omega_1 + .. + b_n\omega_n ,$$

waarin de rationale b's niet alle geheel waren. Zonder de algemeenheid te beperken veronderstellen we dat b_1 niet geheel is, dus $b_1=g+t$ (g geheel rationaal, t rationaal en $0<t<1$). Dan zou

$$\omega' = \alpha - g\omega_1 = t\omega_1 + b_2\omega_2 + \ldots + b_n\omega_n \text{ geheel zijn.}$$

Dan was

$$\Delta(\omega'\omega_2,\ldots,\omega_n) = \begin{vmatrix} t & b_2 & b_3..b_n \\ 0 & 1 & 0..0 \\ . & . & .\ .\ . \\ 0 & 0 & 0..1 \end{vmatrix}^2 \Delta(\omega_1,\ldots,\omega_n) = t^2\Delta(\omega_1,\ldots,\omega_n),$$

en zou dus

$0 < |\Delta(\omega',\omega_2,\ldots,\omega_n)| < |\Delta(\omega_1,\ldots,\omega_n)|$ zijn, in strijd met het gegeven dat $\Delta(\omega_1,\ldots,\omega_n)$ zo klein mogelijk is.

Definitie. Elk systeem $\omega_1,\ldots,\omega_n$ in de zin van de vorige stelling heet een basis van het lichaam.

Voorbeeld. Voor P(i) is de basis 1,i.

Stelling. Voor elke basis heeft $\Delta(\omega_1,\ldots,\omega_n)$ dezelfde waarde.

Bewijs. Laten $\omega_1,\ldots,\omega_n$ en ω_1',ω_n' twee bases zijn. De Δ's van beide systemen zijn geheel rationaal. Volgens de vorige stellingen zou elk van de getallen $\Delta(\omega_1,\ldots,\omega_n)$ en $\Delta(\omega_1',\ldots,\omega_n')$ door de andere deelbaar zijn, en het zelfde teken hebben. Ze zijn dus gelijk.

Definitie. De alleen van het lichaam afhangende discriminant van elke basis heet grondtal van het lichaam.

We zullen dit steeds door Δ voorstellen. Δ is dus een positief of negatief geheel rationaal getal.

Voorbeeld. P heeft grondtal 1, daar 1 een basis vormt; P(i) met basis 1,i heeft tot grondtal

$$\begin{vmatrix} 1 & 1 \\ i & -i \end{vmatrix}^2 = (-2i)^2 = -4;$$ P(ρ) met basis 1, ρ heeft tot grondtal

$$\begin{vmatrix} 1 & 1 \\ \rho & \rho^2 \end{vmatrix} = (\rho^2-\rho)^2 = (-i\sqrt{3})^2 = -3.$$

Hoe vindt men nu bij een lichaam een basis? We zullen eerst een voor-

beeld behandelen.
Gegeven: ϑ is wortel van $8x^3+12x^2+4x+13=0$.
Gevraagd: een basis van $P(\vartheta)$.
Bovenstaande vergelijking is irreducibel.
ϑ is niet geheel. We stellen $\vartheta - \lambda = \tau$ en trachten λ zo te bepalen dat τ geheel is. τ voldoet aan:

$$8(\tau+\lambda)^3 + 12(\tau+\lambda)^2 + 14(\tau+\lambda) + 13 = 0.$$

$$(2)\quad \tau^3+(3\lambda+\tfrac{3}{2})\tau^2 + (3\lambda^2+3\lambda+\tfrac{7}{4})\tau+\lambda^3+\tfrac{3}{2}\lambda^2+\tfrac{7}{4}\lambda+\tfrac{13}{8} = 0.$$

Als τ geheel is, zal λ moeten voldoen aan:

$$3\lambda+\tfrac{3}{2} = \text{geheel};\ 3\lambda^2+3\lambda+\tfrac{7}{4} = \text{geheel},\ \lambda^3+\tfrac{3}{2}\lambda^2+\tfrac{7}{4}\lambda+\tfrac{13}{8} = \text{geheel}$$

Uit de eerste voorwaarde volgt:

$$\lambda = \text{geheel} \pm \tfrac{1}{6}, \pm \tfrac{1}{2}.$$

Het blijkt dat $\lambda = -\frac{1}{2}$ voldoet, dus $\vartheta + \frac{1}{2} = \tau$.
Vergelijking (2) wordt dan: $\tau^3+\tau+1=0$.
We proberen of $(1,\tau,\tau^2)$ een basis is, en berekenen daartoe $\Delta(1,\tau,\tau^2)$.
Noemen we de symmetrische functies:

$$\sum\tau = s_1,\ \sum\tau^2 = s_2,\ \sum\tau^3 = s_3,\ \sum\tau^4 = s_4, \text{ dan is}$$

$$\begin{vmatrix} 1 & \tau_1 & \tau_1^2 \\ 1 & \tau_2 & \tau_2^2 \\ 1 & \tau_3 & \tau_3^2 \end{vmatrix}^2 = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & & -32 \end{vmatrix} = -31.$$

Dus $|\Delta| = 31$. Nu is $1, \vartheta+\frac{1}{2}, (\vartheta+\frac{1}{2})^2$ inderdaad een basis, als gevolg van de volgende
Stelling. Ieder systeem waarvan de discriminant geen kwadraat bevat, is een basis.
Bewijs. Gegeven is: $\Delta(\omega_1,\ldots,\omega_n)$ is kwadraatvrij. Van een ander systeem $\omega_1',\ldots,\omega_n'$ is

$$\Delta(\omega_1',\ldots,\omega_n') = D^2\,\Delta(\omega_1,\ldots,\omega_n), \text{ waarin } D = \text{rationaal} =$$

$$\tfrac{A}{B}\ (A \geqq 1, (A,B)=1). \text{ Dus}$$

$$B^2\,\Delta(\omega_1',\ldots,\omega_n') = A^2\,\Delta(\omega_1,\ldots,\omega_n),$$

$$B^2/A^2\,\Delta(\omega_1,\ldots,\omega_n), \text{ dus } B = \pm 1, \text{ en}$$

$$\Delta(\omega_1',\ldots,\omega_n') = A^2\Delta(\omega_1,\ldots,\omega_n), \text{ of}$$

$$|\Delta(\omega_1',\ldots,\omega_n')| \geqq |\Delta(\omega_1,\ldots,\omega_n)|.$$

$\Delta(\omega_1,\ldots,\omega_n)$ is dus minimaal.

Algemene theorie voor het vinden van een basis.

$f(x)=0$ is een irreducibele vergelijking van graad n met geheel rationale coëfficiënten en wortel ϑ. We vormen $\Omega = P(\vartheta)$. Gevraagd een basis van Ω. Is g de begincoëfficiënt van $f(x)$, dan vormen we $1, g\vartheta, \ldots, g^{n-1}\vartheta^{n-1}$. Deze getallen zijn geheel. We noemen deze getallen $\omega_1,\ldots,\omega_n$, en bepalen $\Delta(\omega_1,\ldots,\omega_n)$. Is dit getal kwadraatvrij, dan vormt $\omega_1,\ldots,\omega_n$ een basis.
Is Δ niet kwadraatvrij, dan is $\Delta = AB^2$ met $B>0$ en A kwadraatvrij. Beschouw dan de B^n getallen:

$$\gamma = \frac{1}{B}(d_1\omega_1+\ldots+d_n\omega_n) \text{ met } d_i=0,1,..,B-1.$$

Noem ze $\gamma_0=0, \gamma_1,\ldots \gamma_{B^n-1}$.

a. Stel deze rij bevat behalve γ_0 geen enkel ander geheel getal. We kunnen dan bewijzen dat $\omega_1,\ldots,\omega_n$ een basis vormen.
Is β een geheel getal van Ω, dan is β steeds te schrijven als

$$\beta = \frac{s_1}{q_1}\omega_1+\ldots+\frac{s_n}{q_n}\omega_n \qquad (s_i,q_i)=1.$$

Nu is

$$G_i = \Delta(\omega_1,\omega_2,\ldots,\omega_{i-1},\beta,\omega_{i+1},\ldots,\omega_n) = \left(\frac{s_i}{q_i}\right)^2 \Delta(\omega_1,\ldots,\omega_n)$$

$$= \left(\frac{s_i}{q_i}\right)^2 AB^2,$$

dus $q_i^2G_i = s_i^2AB^2 \Rightarrow q_i^2/s_i^2AB^2 \Rightarrow q_i^2/B^2 \Rightarrow q_i/B$.

Dus

$$\beta = \frac{1}{B}(c_1\omega_1+\ldots+c_n\omega_n) \quad . \quad c_i \text{ geheel rationaal.}$$

$c_i = Bv_i+d_i$. We kiezen v_i zo dat $0 \leqq d_i < B$, v_i en d_i geheel rationaal.

$$\beta = v_1\omega_1+\ldots+v_n\omega_n+\frac{1}{B}(d_1\omega_1+\ldots+d_n\omega_n).$$

$$\beta-(v_1\omega_1+\ldots+v_n\omega_n) = \frac{1}{B}(d_1\omega_1+\ldots+d_n\omega_n)$$

Het getal in het linkerlid is geheel. In het rechterlid staat een van die getallen γ, waarvan alleen 0 geheel is, dus het rechterlid moet =0 zijn, m.a.w.

$$\beta = v_1 \omega_1 + \cdots + v_n \omega_n \quad (v_i \text{ geheel rationaal}).$$

Voor een ander lineair onafhankelijk systeem $\beta_1, \ldots, \beta_n$ geldt $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ en

$$\Delta(\beta_1, \ldots, \beta_n) = D^2 \Delta(\omega_1, \ldots, \omega_n),$$

waarin $D \neq 0$ en geheel rationaal, dus $D^2 \geqq 1$. Het systeem der β's is dus niet beter dan dat der ω's. Dit laatste is dus een basis.

b). Stel in de rij $\gamma_1, \ldots, \gamma_{B^n - 1}$ komt wel een geheel getal $\gamma = \dfrac{d_1 \omega_1 + \cdots + d_n \omega_n}{B}$ voor met minstens één $d_1 \neq 0$, bijv. $d_r \neq 0$.

We nemen nu het systeem met discriminant $\Delta(\omega_1, \ldots, \omega_{r-1}, \gamma, \omega_{r+1}, \ldots \omega_n) = \left(\frac{d_r}{B}\right)^2 \Delta(\omega_1, \ldots, \omega_n)$. $\Delta \neq 0$ en $\left|\frac{d_r}{B}\right| < 1$. Dit systeem is dus beter, daar de discriminant kleiner is. We kunnen zo telkens het systeem verbeteren, tot de basis is gevonden.

ALGEBRAISCHE GETALLENLICHAMEN VI

door

Prof.Dr B. Meulenbeld

14 December 1955

Eenheden

Definitie. Een geheel getal ε van het lichaam heet eenheid als $\varepsilon / 1$. Deze definitie stemt overeen met vroeger gegeven definities over eenheden.

Stelling. Een geheel getal ε van het lichaam is eenheid dan en slechts dan als $N(\alpha) = \pm 1$.

Bewijs.

1) Voldoende: Uit $N(\alpha) = \pm 1$ volgt als de karakteristieke schrijfwijze van α is $\alpha = r(\vartheta)$:

$$r(\vartheta_1) \ldots r(\vartheta_n) = \pm 1.$$

Nu is $\beta = r(\vartheta_2) \ldots r(\vartheta_n)$ geheel in het lichaam, dus $\alpha\beta = \pm 1$, of $\alpha(\pm\beta) = 1$, dus $\alpha / 1$.

2) Noodzakelijk: Uit $\alpha / 1$ volgt: $\alpha\beta = 1$, waarin β een geheel getal van het lichaam is. Dus is $N(\alpha)N(\beta) = N(1) = 1$, dus, daar $N(\alpha)$ en $N(\beta)$ geheel rationale getallen zijn, $N(\alpha) = \pm 1$.

Stellingen. Zijn ε_1 en ε_2 eenheden van het lichaam, dan ook $\varepsilon_1\varepsilon_2$.

Zijn $\varepsilon_1, \ldots, \varepsilon_r$ eenheden van het lichaam, en $a_1, \ldots, a_r$ geheel rationale getallen, dan is ook $\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$ eenheid.

Definitie. Een getal α heet geassocieerd aan een geheel getal β van het lichaam, als er een eenheid ε van het lichaam is met $\alpha = \beta\varepsilon$.

Hieruit volgt dat dan ook α geheel is en tot het lichaam behoort.

Het geassocieerd zijn is symmetrisch, reflexief en transitief.

Idealen

Definitie. $\alpha_1, \ldots, \alpha_q$ zijn vaste gehele getallen van het lichaam, niet alle $= 0$. De verzameling van de getallen van de vorm $\eta_1\alpha_1 + \ldots + \eta_q\alpha_q$, waarin $\eta_1, \ldots, \eta_q$ gehele getallen van het lichaam zijn, heet ideaal.

Notatie: $[\alpha_1, \ldots, \alpha_q] = \underline{a}$.

Voorbeeld. Voor P is $[2] = [4,6]$.

Het linkerlid is de verzameling van alle even getallen. Het rechterlid is de verzameling van alle getallen van de vorm $4x + 6y$ (x en y geheel rationaal), en dit zijn ook juist alle even getallen.

Stelling. Ieder ideaal van het lichaam P laat zich schrijven in de vorm $[d]$, waarin d geheel rationaal is. d is op het teken na bepaald.

Bewijs. Zij het gegeven ideaal $[a_1,\ldots,a_q]$, waarin de a's gehele rationale getallen zijn, niet alle 0 en $q>1$. Noem $(a_1,\ldots,a_n) = d$, dan bewezen wij dat $[a_1,\ldots,a_n] = [d]$.

Rechts stelt de verzameling voor van de veelvouden van d; links die van alle getallen van de vorm: $a_1x_1 + \ldots + a_qx_q$, met gehele rationale x. Maar deze verzameling bestaat ook alleen uit alle veelvouden van d.

Uit $[d_1] = [d_2]$ volgt d_1/d_2, d_2/d_1, dus $d_2 = \pm d_1$, dus $[d_1] = [-d_1]$.

Opmerking 1. Voor P is het nu duidelijk, dat de invoering van idealen onnodig is, omdat elk ideaal aan te geven is door een natuurlijk getal.

Opmerking 2. Deze stelling geldt ook voor $P(i)$ en $P(\rho)$. Hierin kan men ook elk ideaal schrijven in de vorm $[\alpha]$, waarin α tot op een willekeurige eenheid als factor na bepaald is.

Stelling. Niet elk algebraïsch lichaam heeft de eigenschap, dat elk ideaal in de vorm $[\alpha]$ geschreven kan worden.

Bewijs. Een tegenvoorbeeld is voldoende.

Neem $P(i\sqrt{5})$ en het ideaal $[3,\ 1 + i\sqrt{5}]$.

Was nu $[3,\ 1 + i\sqrt{5}] = [\alpha]$, dan zou, daar 3 een getal van het ideaal is, $\alpha/3$ zijn. Ook $\alpha/1 + i\sqrt{5}$. Maar 3 en $1 + i\sqrt{5}$ waren priem, hebben alleen tot delers ± 3, ± 1, resp. $\pm(1 + i\sqrt{5})$, ± 1. Dus moet $\alpha = \pm 1$, en dus $[3,\ 1 + i\sqrt{5}] = [\pm 1]$. Maar $[-1] = [1]$, dus zou $[3,\ 1 + i\sqrt{5}] = [1]$ zijn. Er zouden dus gehele getallen η_1 en η_2 bestaan met $1 = 3\eta_1 + (1 + i\sqrt{5})\eta_2$, of na vermenigvuldiging met $1 - i\sqrt{5}$:

$$1 - i\sqrt{5} = 3(1 - i\sqrt{5})\eta_1 + 6\eta_2,$$

of $3/1 - i\sqrt{5}$, wat niet waar is.

Definitie. Een ideaal heet hoofdideaal, als het in de vorm $[\alpha]$ geschreven kan worden.

In P is dus elk ideaal hoofdideaal. Er zijn algebraïsche getallenlichamen, waarin niet elk ideaal ook hoofdideaal is.

Stelling. Zijn $\underline{a} = [\alpha_1,\ldots,\alpha_q]$, $\underline{b} = [\beta_1,\ldots,\beta_r]$ twee idealen, dan is $\underline{a} = \underline{b}$ dan en slechts dan als

$$\text{elke } \alpha_Q = \sum_{R=1}^{r} \eta_{QR}\beta_R \quad \text{en elke } \beta_R = \sum_{Q=1}^{q} \lambda_{RQ}\alpha_Q.$$

(λ en η gehele getallen van het lichaam).

Bewijs.

1) Noodzakelijk: Als $\underline{a} = \underline{b}$, dan is de bewering duidelijk.

2) Voldoende: Uit de eerste vergelijking volgt met willekeurige gehele getallen η_Q:

$$\sum_{Q=1}^{q} \eta_Q \alpha_Q = \sum_{R=1}^{r} \beta_R \sum_{Q=1}^{q} \eta_Q \eta_{QR} = \sum_{R=1}^{r} \lambda_R \beta_R,$$

met gehele λ en omgekeerd.

Gevolg. Het ideaal $\underline{a} = [\alpha_1, \ldots, \alpha_q]$ verandert niet, als de elementen willekeurig gerangschikt worden, gelijke slechts eenmaal worden geschreven, eventuele nullen worden weggelaten.

Stelling. Zijn α en β getallen van het ideaal $\underline{a}$, dan zijn ook $\alpha + \beta$ en $\alpha - \beta$ dit.

Bewijs duidelijk.

Een definitie van optelling van idealen is er niet.

Stelling. Is α een getal van $\underline{a}$, η een willekeurig geheel getal van het lichaam, dan is $\eta\alpha$ ook een getal van $\underline{a}$.

Bewijs duidelijk.

Stelling. $[\alpha] = [\beta]$ dan en slechts dan als α en β geassocieerd zijn.

Bewijs.

1) Voldoende: Uit $\alpha = \beta\varepsilon$ volgt $\beta = \frac{1}{\varepsilon}\alpha$, dus $[\alpha] = [\beta]$.

2) Noodzakelijk: Uit $[\alpha] = [\beta]$ volgt β/α, α/β, dus $\alpha = \beta\gamma$, $\beta = \delta\alpha = \delta\gamma\beta$ $\rightarrow 1 = \delta\gamma \rightarrow \gamma/1$. $\gamma = \varepsilon$

Definitie. Het hoofdideaal $[1]$, dat uit alle gehele getallen van het lichaam bestaat, heet eenheidsideaal.

Notatie. $[1] = \underline{0}$.

Stelling. $[\alpha] = \underline{0}$ dan en slechts dan, als α eenheid is.

Bewijs. α moet met 1 geassocieerd zijn.

Stelling. $\underline{a} = [\alpha_1, \ldots, \alpha_q]$, $\underline{b} = [\beta_1, \ldots, \beta_r]$.

Het ideaal

$$[\alpha_1\beta_1, \ldots, \alpha_q\beta_1, \alpha_1\beta_2, \ldots, \alpha_q\beta_2, \ldots, \alpha_q\beta_r]$$

hangt slechts van $\underline{a}$ en $\underline{b}$ af, en niet van de $\alpha_1, \ldots, \alpha_q; \beta_1, \ldots, \beta_r$.

Bewijs. Het is een ideaal, want niet alle $\alpha_Q\beta_R$ zijn $= 0$. Uit $[\alpha_1, \ldots, \alpha_q] = [\gamma_1, \ldots, \gamma_u]$ en $[\beta_1, \ldots, \beta_r] = [\delta_1, \ldots, \delta_v]$ volgt:

$$\alpha_Q\beta_R = \sum_{U=1}^{u} \eta_U\gamma_U \cdot \sum_{V=1}^{v} \lambda_V\delta_V = \sum_{U=1}^{u} \sum_{V=1}^{v} \mu_{UV}\gamma_U\delta_V$$

met gehele μ; ook is omgekeerd:

$$\gamma_U\delta_V = \sum_{Q=1}^{q} \sum_{R=1}^{r} \nu_{QR}\alpha_Q\beta_R \quad \text{met gehele } \nu.$$

Dus

$$[\ldots,\alpha_Q\beta_R,\ldots] = [\ldots,\gamma_U\delta_V,\ldots].$$

Definitie. Het in de vorige stelling gedefinieerde ideaal heet het product van $\underline{a}$ met $\underline{b}$.

Notatie. $\underline{a}.\underline{b}$ of $\underline{a}\,\underline{b}$.

In P is $\underline{a} = [a]$, $\underline{b} = [b]$. Dus $\underline{a}\,\underline{b} = [ab]$.

De vermenigvuldiging van idealen in P komt dus overeen met de vermenigvuldiging van de bijbehorende natuurlijke getallen. De invoering van idealen in P is dan ook onnodig.

Stelling. Behoort α tot $\underline{a}$ en β tot $\underline{b}$, dan $\alpha\beta$ tot $\underline{a}\,\underline{b}$.

Bewijs.

$$\alpha = \sum_{Q=1}^{q} \eta_Q\alpha_Q, \quad \beta = \sum_{R=1}^{r} \lambda_R\beta_R,$$

dus

$$\alpha\beta = \sum_{Q=1}^{q}\sum_{R=1}^{r} \eta_Q\lambda_R\alpha_Q\beta_R = \sum_{Q=1}^{q}\sum_{R=1}^{r} \eta_{QR}\alpha_Q\beta_R.$$

Stellingen. $\underline{a}\,\underline{b} = \underline{b}\,\underline{a}$.

$(\underline{a}\,\underline{b})\underline{c} = \underline{a}(\underline{b}\,\underline{c})$. Bewijzen duidelijk.

Definitie. $\underline{a}_1 \ldots \underline{a}_m = (\underline{a}_1,\ldots,\underline{a}_{m-1})\underline{a}_m$ voor $m > 2$ (definitie door inductie)

Uit de vorige stellingen volgt direct:

Stelling. Het product van idealen $\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_m$ hangt niet af van de volgorde der factoren, en van de volgorde van vermenigvuldiging.

Definitie. Voor natuurlijke m is $\underline{a}^m = \underline{a}\,\underline{a} \ldots \underline{a}$ van m factoren. Verder is $\underline{a}^0 = \underline{0}$.

Stellingen. $\underline{a}\,\underline{0} = \underline{a}$, $\underline{a}^m\underline{a}^l = \underline{a}^{m+l}$ $(m \geqq 0,\ l \geqq 0,\ m,l$ geheel rationaal)

$(\underline{a}^m)^l = \underline{a}^{ml}$, $(\underline{a}\,\underline{b})^m = \underline{a}^m\underline{b}^m$.

Bewijzen duidelijk.

Definitie. Het ideaal $\underline{b}$ is door ideaal $\underline{a}$ deelbaar als er tenminste één ideaal $\underline{c}$ bestaat, zodat $\underline{b} = \underline{a}\,\underline{c}$.

Notatie. $\underline{a}/\underline{b}$.

Stelling. In P is als $a > 0$, $b > 0$ is, $[a]$ / $[b]$ equivalent met a/b.

Bewijs. $[b] = [a][c]$ is equivalent met $[b] = [ac]$, dus met $b = \pm ac$.

Stellingen. Uit $\underline{a}/\underline{b}$, $\underline{b}/\underline{d}$ volgt $\underline{a}/\underline{d}$.

Uit $\underline{a}/\underline{b}$ volgt $\underline{a}\,\underline{d}/\underline{b}\,\underline{d}$.

Voor elke $\underline{a}$ is $\underline{0}/\underline{a}$ en $\underline{a}/\underline{a}$.

Elk ideaal $\underline{a} \neq \underline{0}$ heeft dus minstens de beide triviale delers $\underline{0}$ en $\underline{a}$.

Het ideaal $\underline{0}$ heeft minstens de deler $\underline{0}$.

Stelling. Uit $\underline{a}/\underline{b}$ volgt, dat elk getal van $\underline{b}$ een getal van $\underline{a}$ is.

Bewijs. Zij $\underline{a}\,\underline{c} = \underline{b}$, dan is, als $\underline{a} = [\alpha_1,\ldots,\alpha_q]$, $\underline{c} = [\gamma_1,\ldots,\gamma_r]$ gesteld wordt: $\underline{b} = [\ldots,\alpha_Q\gamma_R,\ldots]$.

Elk getal van $\underline{b}$ heeft dus de vorm

$$\sum_{Q,R} \eta_{QR} \alpha_Q \eta_R = \sum_Q \eta_Q \alpha_Q,$$

behoort dus tot $\underline{a}$.

Opmerking. De deler bevat dus minstens alle getallen van het deeltal. In P is $[3] / [6]$: elk veelvoud van 6 is veelvoud van 3, er zijn meer veelvouden van 3 dan van 6.

Stelling. Uit $\underline{a}/\underline{0}$ volgt $\underline{a} = \underline{0}$.

Bewijs. Elk getal van het lichaam is volgens de vorige stelling getal van $\underline{a}$, dus moet $\underline{a} = \underline{0}$ zijn.

ALGEBRAISCHE GETALLENLICHAMEN VII

door

Prof.Dr B. Meulenbeld

11 Januari 1956

Priemidealen en Hoofdstelling der ideaaltheorie.

Definitie. Een ideaal $\mathfrak{p} \neq 0$ heet priemideaal; als het precies twee delers 0 en $\mathfrak{p}$ heeft.

De priemidealen van P zijn de $[p]$.

We weten nog niet of er in ieder lichaam een priemideaal is.

Definitie. We zeggen dat twee idealen $\mathfrak{a}$ en $\mathfrak{b}$ geen gemeenschappelijke deler hebben als 0 de enige gemeenschappelijke deler is.

Stelling. Zijn een priemideaal $\mathfrak{p}$ en een willekeurig ideaal $\mathfrak{a}$ gegeven, dan is òf $\mathfrak{p}/\mathfrak{a}$ òf $\mathfrak{p}$ en $\mathfrak{a}$ hebben geen gemeenschappelijke deler.

Bewijs duidelijk.

Stelling. Elk natuurlijk getal a behoort slechts tot een eindig aantal idealen.

Bewijs. Zij $\omega_1, .., \omega_n$ een willekeurige vaste basis van het lichaam. Dan heeft elk geheel getal α van het lichaam de gedaante: $\alpha = g_1 \omega_1 + .. + g_n \omega_n$ (g_i geheel rationaal). Nu is $g_i = q_i\, a + k_i$ ($0 \leq k_i < a$, $1 \leq i \leq n$, q_i en k_i geheel rationaal).

Dus $\alpha = \sum_{i=1}^{n} (q_i . a + k_i)\, \omega_i = a \sum_{i=1}^{n} q_i \omega_i + \sum_{i=1}^{n} k_i \omega_i = \gamma a + \beta$, waarin γ geheel is, en $\beta = \sum_{i=1}^{n} k_i \omega_i$.

Daar k_i begrensd is, zijn er slechts een eindig aantal β.

Behoort nu a tot het ideaal $\mathfrak{a} = [\alpha_1, .., \alpha_q]$, en past men op al deze de vorige redenering toe, dan is $\mathfrak{a} = [\gamma_1 a + \beta_1, \ldots, \gamma_q a + \beta_q]$. Daar a tot $\mathfrak{a}$ behoort, kan men hier ook voor schrijven:

$$\mathfrak{a} = [\gamma_1 a + \beta_1, .., \gamma_q a + \beta_q, a] = [\beta_1, .., \beta_q, a].$$

Daar er slechts een eindig aantal β zijn, behoort a slechts tot een eindig aantal idealen.

Stelling. Bij elk ideaal $\mathfrak{a}$ bestaat een ideaal $\mathfrak{b}$, zó dat $\mathfrak{a}\,\mathfrak{b}$ een hoofdideaal is, zelfs een van de vorm $\mathfrak{a}\,\mathfrak{b} = [a]$, waarin a een natuurlijk getal is.

Bewijs. Zij $\mathfrak{a} = [\alpha_1, \alpha_{1-1}, \ldots, \alpha_0]$ met $\alpha_1 \neq 0$. Aan dit ideaal voegen wij een veelterm $g(x) = \alpha_1 x + \cdots + \alpha_0$ toe, en definieren nu h(x) door

$$g(x)\, h(x) = \prod_{q=1}^{n} \{ r_1(\vartheta_q) x^1 + \ldots + r_0(\vartheta_q) \},$$

waarin $\alpha_L = r_L(\vartheta)$ de karakteristieke schrijfwijze van α_L is. Volgens de

stelling over de symmetrische functies is

$$g(x)\ h(x) = c_{l+m}\ x^{l+m}+..+c_o$$

een veelterm in P. De coëfficiënten zijn zelfs geheel rationaal.
Daar g(x) h(x) en g(x) veeltermen in $P(\vartheta)$ zijn, is

$$h(x)=\beta_m x^m+..+\beta_o \quad (m=(n-1)l)$$

dit ook; de β zijn geheel. $\beta_m \neq 0$, daar $r_1(\vartheta_q)\neq 0$ is.

We definieren nu $\underline{b}$ als het ideaal

$$\underline{b} = [\beta_m,..,\beta_q] \text{ en beweren } \underline{a}\ \underline{b} = [a]\ ,$$

waarin $$a = \begin{cases} |c_o| & \text{voor } l+m=0 \\ (c_{l+m},..,c_o) & \text{voor } l+m>0 \end{cases}$$

We behoeven daarvoor alleen maar aan te tonen:

1^o $$a = \sum_{L=0}^{l}\ \sum_{M=0}^{m} \eta_{LM}\ \alpha_L \beta_M;$$

2^o $$\alpha_L \beta_M = \lambda_{LM}\ a (0 \leqq L \leqq l,\ 0 \leqq M \leqq m) \text{ met } \lambda \text{ en } \eta \text{ geheel.}$$

Het bewijs van 1^o volgt uit:

$$a = C_{l+m}\ c_{..+m}+..+C_o c_o$$

met geschikte geheel rationale C_1 en $C_N = \sum_{\substack{L+M \leqq N \\ 0 \leqq L \leqq l \\ 0 \leqq M \leqq m}} \alpha_L \beta_M$.

Het bewijs van 2^o volgt uit de Stelling van Kronecker.
<u>Stelling</u>: Uit $[\gamma]\ \underline{a} = [\gamma]\ \underline{b}$ $\gamma \neq 0$ volgt $\underline{a} = \underline{b}$.
<u>Bewijs</u>. Dit volgt uit het feit dat $[\gamma]\ \underline{a}$ alle γ-vouden voorstellen van de getallen van $\underline{a}$.
<u>Stelling.</u> Uit $\underline{a}\ \underline{c} = \underline{a}\ \underline{d}$ volgt $\underline{c} = \underline{d}$.
<u>Bewijs</u>. Men kan f zo bepalen dat $\underline{a}\ \underline{f}$ een hoofdideaal $[\alpha]$ is. Dus $\underline{a}\ \underline{f} = [\alpha]$.
Uit $\underline{a}\ \underline{c} = \underline{a}\ \underline{d}$ volgt $\underline{f}\ \underline{a}\ \underline{c} = \underline{f}\ \underline{a}\ \underline{d}$ of $[\alpha]\ \underline{c} = [\alpha]\ \underline{d}$ of $\underline{c} = \underline{d}$.
<u>Gevolg.</u> Als $\underline{a}/\underline{b}$ dan is er <u>slechts</u> één $\underline{c}$ met $\underline{a}\ \underline{c} = \underline{b}$.
<u>Stelling</u>. Uit $\underline{a}\ \underline{b}/\underline{a}\ \underline{c}$ volgt $\underline{b}/\underline{c}$.
<u>Bewijs.</u> $\underline{a}\ \underline{c} = \underline{a}\ \underline{b}\ \underline{d}$ of $\underline{c} = \underline{b}\ \underline{d}$.
<u>Stelling</u> (omgekeerde van een vroegere stelling).
Als elk getal van $\underline{b}$ een getal van $\underline{a}$ is, dan is $\underline{a}/\underline{b}$.

Bewijs. We bepalen $\underline{f}$ zo dat $\underline{a}\,\underline{f} = [\alpha]$. Elk getal van $\underline{b}\,\underline{f}$ is een getal van $\underline{a}\,\underline{f}$, dus van $[\alpha]$. Elk getal van $\underline{b}\,\underline{f}$ is dus door α deelbaar. Is $\underline{b}\,\underline{f} = [\delta_1,..,\delta_\nu]$, dan is met gehele $\gamma_1,..,\gamma_\nu$: $\underline{b}\,\underline{f} = [\alpha\gamma_1,..,\alpha\gamma_\nu] = [\alpha][\gamma_1,..,\gamma_\nu] = \underline{a}\,[\gamma_1,..,\gamma_\nu]\,\underline{f}$, dus $\underline{b} = \underline{a}\,[\gamma_1,..,\gamma_\nu]$ of $\underline{a}/\underline{b}$.

Stelling. Elk ideaal $\underline{a}$ heeft slechts eindig veel delers.

Bewijs. Er bestaat een ideaal $\underline{b}$ en een natuurlijk getal a, zo dat $\underline{a}\,\underline{b} = [a]$. Uit $\underline{c}/\underline{a}$ volgt $\underline{c}/[a]$. a behoort dus tot $\underline{c}$, maar deze eigenschap hebben slechts eindig veel $\underline{c}$.

Stelling. Is $\underline{a} = \underline{c}\,\underline{d}$ en $\underline{d}\neq 0$ (dus $\underline{c}$ een echte deler van $\underline{a}$), dan heeft $\underline{c}$ minder delers dan $\underline{a}$.

Bewijs. Elke deler van $\underline{c}$ is een deler van $\underline{a}$. Nu is $\underline{a}$ wel deler van $\underline{a}$, maar niet van $\underline{c}$, want uit $\underline{a}/\underline{c}$ zou volgen: $\underline{c}\,\underline{d}\,/\underline{c}$, $\underline{d}/0$, $\underline{d}=0$.

Stelling. Elk ideaal $\underline{a}\neq 0$ is door een priemideaal deelbaar.

Bewijs. Onder al de delers van $\underline{a}$, die $\neq 0$ zijn, zij $\underline{c}$ die met het kleinste aantal delers. Dan is $\underline{c}$ priemideaal; anders immers was $\underline{c} = \underline{d}\,\underline{e}$ met $\underline{d}\neq 0$, $\underline{e}\neq 0$, dus $\underline{e}$ een deler van $\underline{a}$, die $\neq 0$ was en minder delers had dan $\underline{c}$.

Opmerking. Er is dus een priemideaal.

Stelling. Er zijn oneindig veel priemidealen.

Bewijs. Bij elk priemgetal p is er een priemideaal $\underline{p}/[p]$. Voor twee verschillende priemgetallen p_1, p_2 en $\underline{p}_1/[p_1]$, $\underline{p}_2/[p_2]$ geldt $\underline{p}_1 \neq \underline{p}_2$. Men kan steeds geschikte geheel rationale x en y vinden, zó dat $1 = p_1x + p_2y$. Was $\underline{p}_1 = \underline{p}_2$, dan zou $\underline{1}$ een getal van $\underline{p}_1$ zijn, dus $\underline{p}_1/\underline{0}$, of $\underline{p}_1 = \underline{0}$. Tegenspraak. Er zijn oneindig veel priemgetallen, dus ook oneindig veel priemidealen.

Stelling. Elk ideaal $\underline{a}\neq 0$ kan als product van priemidealen worden geschreven.

Bewijs. Laat $\underline{a}$ k delers hebben, waarbij $k \geq 2$ is. Is k=2, dan is $\underline{a}$ zelf priemideaal. Zij de stelling voor $k > 2$ en tot k-1 toe bewezen. Nu is $\underline{a} = \underline{p}\,\underline{b}$ met $\underline{b} \neq 0$. $\underline{b}$ heeft minder dan k delers. Dus is $\underline{b}$, en dus ook $\underline{a}$, product van priemidealen.

Stelling. Zijn $\underline{a}$ en $\underline{b}$ idealen, dan is er één en slechts één ideaal $\underline{d}$ met de volgende eigenschappen:

$\underline{d}/\underline{a}$, $\underline{d}/\underline{b}$. Uit $\underline{e}/\underline{a}$, $\underline{e}/\underline{b}$ volgt $\underline{e}/\underline{d}$.

Bewijs. Is $\underline{a} = [\alpha_1,..,\alpha_q]$, $\underline{b} = [\beta_1,..,\beta_2]$, dan heeft het ideaal $\underline{d} = [\alpha_1,..,\alpha_q,\beta_1,..,\beta_r]$ de gewenste eigenschappen. Immers elk getal in $\underline{a}$ heeft de gedaante:

$\sum_{Q=1}^{q} \eta_Q \alpha_Q = \sum_{Q=1}^{q} \eta_Q \alpha_Q + \sum_{R=1}^{r} 0.\beta_R$, behoort dus tot $\underline{d}$, dus is $\underline{d}/\underline{a}$. Evenzo: $\underline{d}/\underline{b}$. Verder behoort $\sum_{Q=1}^{q} \eta_Q \alpha_Q$ tot $\underline{e}$, evenzo: $\sum_{R=1}^{r} \lambda_R \beta_R$ tot $\underline{e}$, dus ook

$\sum_{Q=1}^{q} \eta_Q \alpha_Q + \sum_{R=1}^{r} \alpha_R \beta_r$ tot $\underline{e}$, dus $\underline{e}/\underline{d}$.

Eenduidigheid: Hebben $\underline{d}_1$ en $\underline{d}_2$ de verlangde eigenschappen, dan is $\underline{d}_1/\underline{d}_2$, $\underline{d}_2/\underline{d}_1 \rightrightarrows \underline{d}_1 = \underline{f}\ \underline{d}_2$, $\underline{d}_2 = \underline{g}\ \underline{d}_1 = \underline{f}\ \underline{g}\ \underline{d}_2, \rightarrow \underline{0} = \underline{f}\ \underline{g} \rightrightarrows \underline{f}/\underline{0} \rightrightarrows \underline{f} = \underline{0} \rightrightarrows \underline{d}_1 = \underline{d}_2$.

Definitie. Het ideaal $\underline{d}$ uit de vorige stelling heet de grootst gemene deler van $\underline{a}$ en $\underline{b}$. Notatie: $(\underline{a},\underline{b})$.

Stelling. Hebben $\underline{a}$ en $\underline{b}$ geen gemeenschappelijke delers, dan is $(\underline{a},\underline{b}) = \underline{0}$ en omgekeerd. Duidelijk.

Stelling. De getallen van $(\underline{a},\underline{b})$ zijn de verschillende onder de getallen $\alpha+\beta$, waarin α tot $\underline{a}$ en β tot $\underline{b}$ behoort.

Bewijs. $(\underline{a},\underline{b})$ is de verzameling van de verschillende getallen van de gedaante: $\eta_1 \alpha_1 + .. + \eta_Q \alpha_Q + \lambda_1 \beta_1 + .. + \lambda_R \beta_R$; dit zijn dus die, welke juist de gedaante $\alpha+\beta$ hebben.

Stelling. Uit $(\underline{a},\underline{b}) = \underline{0}$ volgt dat er een α in $\underline{a}$ en een β in $\underline{b}$ is met $\alpha+\beta = 1$. Duidelijk.

Stelling. Uit $\underline{p}/\underline{a}\ \underline{b}$ volgt $\underline{p}/\underline{a}$ of $\underline{p}/\underline{b}$ of beide.

Bewijs. Is $\underline{p} \not/ \underline{a}$ dan moeten we bewijzen $\underline{p}/\underline{b}$. $(\underline{a}/\underline{p}) = \underline{0}$, dus $1 = \alpha + \pi$, met α in $\underline{a}$ en π in $\underline{p}$. Voor elk getal β van $\underline{b}$ geldt dus $\beta = \alpha\beta + \pi\beta$. $\alpha\beta$ in $\underline{a}\ \underline{b}$; wegens $\underline{p}/\underline{a}\ \underline{b}$ dus $\alpha\beta$ in $\underline{p}$; $\pi\beta$ in $\underline{p}$, dus β in $\underline{p}$, dus $\underline{p}/\underline{b}$.

Stelling. Uit $\underline{p}/\underline{a}_1 .. \underline{a}_m$ volgt dat $\underline{p}$ deelbaar is op minstens één van de idealen $\underline{a}_1, .., \underline{a}_m$. Duidelijk.

Stelling. Uit $\underline{p}/\underline{p}_1 .. \underline{p}_m$ volgt dat $\underline{p}$ gelijk is aan minstens één der priemidealen $\underline{p}_1, .., \underline{p}_m$.

Hoofdstelling der ideaaltheorie. Elk van $\underline{0}$ verschillend ideaal laat zich, afgezien van de volgorde der factoren, slechts op één wijze schrijven als product van priemidealen.

Bewijs. Beweerd wordt dat uit $\underline{a} = \underline{p}_1 .. \underline{p}_m = \underline{p}_1' .. \underline{p}_l'$, $m \geq 1$, $l \geq 1$, volgt: $m=l$, en afgezien van de volgorde zijn de $\underline{p}$ gelijk aan de $\underline{p}'$. Laat $\underline{a}$ k factoren hebben, dan is $k \geq 2$. Voor $k=2$ is $\underline{a}$ priemideaal, dus $m=l=1$, $\underline{p}_1 = \underline{p}_1'$. Zij $k > 2$, dus $m > 1$, $l > 1$ en tot $k-1$ alles bewezen, dan is $\underline{p}_1' = \underline{p}_M$, zeg $\underline{p}_1' = \underline{p}_1$. Dan is $\underline{p}_2 .. \underline{p}_m = \underline{p}_2' .. \underline{p}_l'$. Dit ideaal heeft hoogstens $k-1$ delers, dus is $m-1 = l-1$, of $m=l$ en $\underline{p}_2 .. \underline{p}_m$ zijn afgezien van de volgorde $= \underline{p}_2', .., \underline{p}_m'$.

De volgende stellingen zijn duidelijk.

Stelling. Elk ideaal $\underline{a} \neq \underline{0}$ is, afgezien van de volgorde der factoren, op één wijze in de gedaante $\underline{p}_1^{a_1} .. \underline{p}_r^{a_r}$ $(r \geq 1)$ te schrijven, waarin de $\underline{p}$ verschillend zijn en de a natuurlijke getallen zijn.

Stelling. $(\underline{a},\underline{b}) = \prod_{\underline{p}} \underline{p}^c$,

$\underline{p}$ zijn alle gemeenschappelijke priemidealen van $\underline{a}$ en $\underline{b}$, en voor elke $\underline{p}$ is $c = \min(a,b)$, als a resp. b de exponent voorstelt, waarmede $\underline{p}$ in de ontbinding van $\underline{a}$ resp. $\underline{b}$ optreedt.

ALGEBRAISCHE GETALLENLICHAMEN VIII

door

Prof.Dr B. Meulenbeld

Dinsdag, 24 januari 1956

Definitie. Een getal α heet door het ideaal $\underline{a}$ deelbaar als α een getal van $\underline{a}$ is (α is dus geheel), dus òf $\alpha=0$ of $\underline{a}/[\alpha]$.

Notatie. $\underline{a}/\alpha$.

Stelling. Is $\underline{a}$ een hoofdideaal $[\beta]$, dan geldt $\underline{a}/\alpha$, dan en alleen dan als β/α.

Bewijs. Als β/α is, dan behoort α tot $[\beta]$ en omgekeerd.

Stelling. Is $\underline{b}$ een hoofdideaal $[\alpha]$, dan geldt $\underline{a}/\alpha$, dan en alleen dan als $\underline{a}/\underline{b}$ is.

Bewijs. $\underline{b}$ bestaat uit de veelvouden van α.

Definitie. Een geheel getal μ van het lichaam heet congruent resp. incongruent mod $\underline{a}$, als

$$\underline{a}/\mu-\nu \text{ , resp. } \underline{a}\nmid\mu-\nu .$$

Notatie. $\mu\equiv\nu \pmod{\underline{a}}$, resp. $\mu\not\equiv\nu \pmod{\underline{a}}$.

Voorbeeld. In P is, als a een natuurlijk getal is, $m\equiv n \pmod{[a]}$ identiek met het vroeger ingevoerde begrip $m\equiv n \pmod a$.

Stelling. Het begrip congruent is reflexief, symmetrisch en transitief. Duidelijk.

Stelling. Uit $\mu\equiv\nu \pmod{\underline{a}}$ en $\underline{c}/\underline{a}$ volgt $\mu\equiv\nu \pmod{\underline{c}}$.

Bewijs. $\mu-\nu$ ligt in $\underline{a}$, dus in $\underline{c}$.

Stelling. Het aantal klassen waarin alle gehele getallen van het lichaam mod $\underline{a}$ uiteenvallen, is eindig.

Bewijs. We bepalen $\underline{b}$ zo dat $\underline{a}\,\underline{b}=[a]$ $(a>0)$. Uit $\mu\equiv\nu \pmod{[a]}$ volgt $\mu\equiv\nu \pmod{\underline{a}}$. Het aantal klassen mod $[a]$ is echter reeds eindig. Immers in het bewijs van een vroegere stelling is reeds opgemerkt, dat mod $[a]$ elk geheel getal van het lichaam congruent is aan een der a^n getallen:

$\sum_{m=1}^{n} k_n\omega_n$ $(0\leqq k_n<n)$, waarin $\omega_1,\ldots,\omega_n$ een basis van het lichaam voorstelt. Daar bovendien uit $\mu\not\equiv\nu \pmod{\underline{a}}$ volgt $\mu\not\equiv\nu \pmod{[a]}$ is dus ook het aantal klassen mod $\underline{a}$ eindig.

Definitie. Dit aantal klassen heet de norm van $\underline{a}$ (is dus een natuurlijk getal).

Notatie. N $\underline{a}$.

Stelling. Uit $\mu\equiv\nu \pmod{\underline{a}}$, $\rho\equiv\sigma \pmod{\underline{a}}$ volgt:

$$\mu+\rho\equiv\nu+\sigma \pmod{\underline{a}} \text{ en } \mu-\rho\equiv\nu-\sigma \pmod{\underline{a}}.$$

Bewijs. $\underline{a}/\mu-\nu$, $\underline{a}/\rho-\sigma \Rightarrow \underline{a}/(\mu-\nu)\pm(\rho-\sigma) \Rightarrow \underline{a}/(\mu\pm\rho)-(\nu\pm\sigma)$.

Stelling. Uit $\mu \equiv \nu \pmod{\underline{a}}$ volgt voor elk geheel getal η van het lichaam: $\mu\eta \equiv \nu\eta \pmod{\underline{a}}$.

Bewijs. $\underline{a}/\mu-\nu$ $\underline{a}/(\mu-\nu)\eta \Rightarrow \underline{a}/\mu\eta-\nu\eta$.

Stelling. Uit $\mu \equiv \nu \pmod{\underline{a}}$, $\rho \equiv \sigma \pmod{\underline{a}}$ volgt: $\mu\rho \equiv \nu\sigma \pmod{\underline{a}}$.

Bewijs $\mu\rho \equiv \nu\rho$, $\nu\rho \equiv \nu\sigma \Rightarrow \mu\rho \equiv \nu\sigma$

Stelling. N $\underline{a}$ = 1, dan en alleen dan als $\underline{a}$ = $\underline{0}$.

Bewijs. N $\underline{a}$ = 1 betekent dat alle gehele getallen van het lichaam aan elkaar congruent zijn, dus elk $\equiv 0$ is, d.w.z. tot $\underline{a}$ behoort.

Stelling. N($\underline{a}$ $\underline{p}$) = N $\underline{a}$.N $\underline{p}$.

Bewijs. $\underline{a}/\underline{a}$ $\underline{p}$, met $\underline{a} \neq \underline{a}$ $\underline{p}$.

Er is dus een α , zo dat $\underline{a}/\alpha$, $\underline{a}$ $\underline{p} \nmid \alpha$. Dus is $\alpha \neq 0$, $\underline{a}/[\alpha]$, $\underline{a}$ $\underline{p} \nmid [\alpha]$. Er is dus een $\underline{b}$ zó dat $\underline{a}$ $\underline{b}$= $[\alpha]$, dan is $\underline{a}$ $\underline{p} \nmid \underline{a}$ $\underline{b}$, dus $\underline{p} \nmid \underline{b}$.

Laten nu $A_1,..,A_{N\,\underline{a}}$ resp. $\Pi_1,..,\Pi_{N\,\underline{p}}$ elk een representanten systeem van alle klassen mod $\underline{a}$ resp. mod $\underline{p}$ voorstellen. We beweren, dat de N $\underline{a}$.N $\underline{p}$ getallen $\alpha\Pi_k+A_m$, $1 \leqq K \leqq N\,\underline{p}$, $1 \leqq m \leqq N\,\underline{a}$ 1) alle onderling incongruent zijn, en 2) dat elk geheel getal van het lichaam aan een van deze congruent mod $\underline{a}$ $\underline{p}$ is. Daarmede is dan bewezen, dat er mod $\underline{a}$ $\underline{p}$ precies N $\underline{a}$ .N $\underline{p}$ klassen zijn.

1) Uit $\alpha\Pi_k + A_m \equiv \alpha\Pi_{k'} + A_{m'} \pmod{\underline{a}\,\underline{p}}$ volgt:

$$\alpha\Pi_k + A_m \equiv \alpha\Pi_{k'} + A_{m'} \pmod{\underline{a}}.$$

Daar $\alpha\Pi_k \equiv 0 \equiv \alpha\Pi_{k'} \pmod{\underline{a}}$ is dus:

$$A_m \equiv A_{m'} \pmod{\underline{a}}, \text{ dus } m=m',\ A_m=A_{m'}.$$

Derhalve: $\alpha\Pi_k \equiv \alpha\Pi_{k'} \pmod{\underline{a}\,\underline{p}}$, of

$$\underline{a}\,\underline{p} \,/\, \alpha(\Pi_k-\Pi_{k'}).$$

Was nu $k \neq k'$, dan was $\Pi_k-\Pi_{k'}$ niet door $\underline{p}$ deelbaar, dus $\underline{p} \nmid (\Pi_k-\Pi_{k'})$.

Uit $\underline{a}\,\underline{p}/\,[\alpha]\,(\Pi_k-\Pi_{k'})$ zou dan volgen:

$\underline{a}\,\underline{p}/\underline{a}\,\underline{b}\,(\Pi_k-\Pi_{k'})$, dus $\underline{p}/\underline{b}\,(\Pi_k-\Pi_{k'})$, dus $\underline{p}/\underline{b}$. Tegenspraak.

2) Laat ω een willekeurig geheel getal van het lichaam zijn. Voor één m is dan $\omega = A_m+\alpha_1$, $\underline{a}/\alpha_1$. Wegens $\underline{p} \nmid \underline{b}$ is $([\alpha]\,,\,\underline{a}\,\underline{p})=(\underline{a}\,\underline{b},\underline{a}\,\underline{p})=\underline{a}$. Verder is $\alpha_1 = \eta\alpha+\mu_1$, η geheel, $\underline{a}\,\underline{p}/\mu_1$. Nu is voor één k: $\eta = \Pi_k+\Pi_1$, $\underline{p}/\pi$, dus

$$\omega = A_m + \eta\alpha + \mu_1 = A_m + \Pi_k + \Pi_1\alpha + \mu_1.$$

Daar $\underline{p}$ $\underline{a}/\Pi_1\alpha$ is $\underline{a}\,\underline{p}/\Pi_1\alpha+\mu_1$, dus

$$\omega = A_m+\Pi_k\alpha+\mu_2,\ \underline{a}\,\underline{p}/\mu_2, \text{ dus } \omega \equiv A_m+\Pi_k\alpha \pmod{\underline{a}\,\underline{p}}.$$

Stelling. $N(\underline{a}\ \underline{b}) = N\ \underline{a}\ N\ \underline{b}$.

Bewijs. Inductie naar het aantal priemidealen van $\underline{b}$. Voor $\underline{b}=\underline{0}$ triviaal, voor $\underline{b}=\underline{p}$ zo juist bewezen:

Laat nu $\underline{b}$ een product zijn van $m>1$ priemidealen, en de stelling geldig zijn in alle gevallen, waarin de tweede factor een product van m-1 priemidealen is. Nu is $\underline{b} = \underline{p}\ \underline{c}$, waarin $\underline{c}$ een product van m-1 priemidealen is, dus is: $N(\underline{a}\ \underline{b}) = N(\underline{a}\ \underline{p}.\underline{c}) = N(\underline{a}\ \underline{p})\ N\ \underline{c} = N\ \underline{a}.N\ \underline{p}.N\ \underline{c} = N\ \underline{a}.N(\underline{p}\ \underline{c}) = N\ \underline{a}.N\ \underline{b}$.

Stelling. Voor elk natuurlijk getal a is $N\ [a] = a^n$.

Bewijs. Bij het bewijs van een vroegere stelling is reeds opgemerkt, dat elk geheel getal van het lichaam mod $[a]$ congruent is met een van de a^n getallen:

$\sum_{m=1}^{n} k_m\ \omega_m$, $0 \leqq k_m < a$. Elke twee van deze a^n getallen zijn echter incongruent. Immers uit

$$\sum_{m=1}^{n} k_n\ \omega_m \equiv \sum_{m=1}^{n} k'_m\ \omega_m \pmod{[a]}, \quad 0 \leqq k_m < a, \quad 0 \leqq k'_m < a \quad \text{volgt:}$$

$$\sum_{m=1}^{n} (k_m - k'_m)\ \omega_m \equiv 0 \pmod{[a]},$$

dus is $\sum_{m=1}^{n} \frac{k_m - k'_m}{a}\ \omega_m$ geheel. Volgens de definitie van basis is dus $k_m \equiv k'_m \pmod{a}$, of $k_m = k'_m$.

Stelling. $\underline{a}$ zij een ideaal of slechts een verzameling van niet alleen uit 0 bestaande getallen met de eigenschappen:

1) Als α en β er toe behoren, dan ook $\alpha \pm \beta$.

2) Als α er toe behoort, dan ook $\eta\alpha$ (η willekeurig geheel uit het lichaam).

Bewering: Er bestaat een systeem van n lineair onafhankelijke getallen $\alpha_1, \ldots, \alpha_n$ van de verzameling $\underline{a}$, zo dat in de voorstelling:

$$(1) \qquad \alpha = h_1\alpha_1 + \ldots + h_n\alpha_n$$

met rationale h de getallen h geheel zijn als α tot $\underline{a}$ behoort.

Opmerkingen 1. $\underline{a}$ is dan dus de verzameling van getallen α met geheel rationale h.

2. Voor $\underline{a} = \underline{0}$ verkrijgt men de vroegere basis-stelling.

Bewijs. (geheel analoog aan de vroegere). Er bestaat in $\underline{a}$ een systeem van n lineair onafhankelijke getallen; immers als α een getal $\neq 0$ is uit

$\underline{a}$ en $\eta_1,\ldots,\eta_n$ een systeem van lineair onafhankelijke gehele getallen uit het lichaam is, dan is $\alpha\eta_1,\ldots,\alpha\eta_n$ zulk een systeem.
Onder alle systemen van n lineair onafhankelijke getallen $\alpha_1,\ldots,\alpha_n$ van $\underline{a}$ kies ik er een, waarvoor $|\Delta(\alpha_1,\ldots,\alpha_n)|$ zo klein mogelijk is. We beweren dat dit systeem het gevraagde is. Anders zou er in $\underline{a}$ een getal (1) zijn met rationale, doch niet geheel rationale h. Laat bijv. h_1 niet geheel rationaal zijn, dus $h_1=g+t$ (g geheel rationaal $0<t<1$). Dan was $\alpha'=\alpha-g\,\alpha_1=t\,\alpha_1+h_2\,\alpha_2+\ldots+h_n\alpha_n$ een getal van $\underline{a}$. Dan zou verder

$$\Delta(\alpha',\alpha_2,\ldots,\alpha_n)=\begin{vmatrix} t & h_2 & \ldots & h_n \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix}\Delta(\alpha_1,\ldots,\alpha_n)=$$
$$=t^2\,\Delta(\alpha_1,\ldots,\alpha_n),$$

dus $0<|\Delta(\alpha',\alpha_2,\ldots,\alpha_n)|<|\Delta(\alpha_1,\ldots,\alpha_n)|$. Tegenspraak.

Stelling. Elke verzameling van niet alleen uit 0 bestaande getallen met de eigenschappen der vorige stelling, is een ideaal.
Bewijs. Worden de getallen $\alpha_1,\ldots,\alpha_n$ gekozen als in de vorige stelling is aangegeven, dan is het ideaal $[\alpha_1,\ldots,\alpha_n]$ gelijk aan de gegeven verzameling. Immers elk getal van de verzameling is van de gedaante $h_1\alpha_1+\ldots+h_n\alpha_n=\eta_1\alpha_1+\ldots+\eta_n\alpha_n$, en elk getal $\eta_1\alpha_1+\ldots+\eta_n\alpha_n$ met gehele η behoort tot de verzameling.

Definitie. $\underline{a}$ zij een ideaal. Elk systeem $\alpha_1,\ldots,\alpha_n$ in de zin van de vorige stellingen heet een basis van het ideaal $\underline{a}$.
Opmerking. De basis van het lichaam is dus een basis van het eenheidsideaal $\underline{0}$.
Stelling. Voor elke basis $\alpha_1,\ldots,\alpha_n$ van $\underline{a}$ heeft $\Delta(\alpha_1,\ldots,\alpha_n)$ dezelfde waarde.
Bewijs. Zijn $\alpha_1,\ldots,\alpha_n$ en $A_1,\ldots,A_n$ bases, dan is wegens $A_k=\sum h_{kl}\alpha_l$ de h_{kl} geheel rationaal; dus $\Delta(A_1,\ldots,A_n)=$
$=|h_{kl}|^2\,\Delta(\alpha_1,\ldots,\alpha_n)$, dus $\Delta h_{kl}\neq 0$, dus $\Delta(\alpha_1,\ldots,\alpha_n)/\Delta(A_1,\ldots,A_n)$.
Uit symmetrie overwegingen is $\Delta(A_1,\ldots,A_n)/\Delta(\alpha_1,\ldots,\alpha_n)$. De tekens zijn volgens een vorige stelling gelijk, dus

$$\Delta(A_1,\ldots,A_n)=\Delta(\alpha_1,\ldots,\alpha_n).$$

Definitie. De gemeenschappelijke waarde van $\Delta(\alpha_1,\ldots,\alpha_n)$ voor alle bases van het ideaal heet discriminant van het ideaal.
Notatie. $\Delta(\underline{a})$.
Opmerking. Het grondtal van het lichaam Δ is dus $\Delta(\underline{0})$.

ALGEBRAISCHE GETALLENLICHAMEN IX

door

Prof.Dr B. Meulenbeld

8 februari 1956

Stelling. Is $\omega_1,\ldots,\omega_n$ een lichaamsbasis, dan is er voor elk ideaal $\underline{a}$ een basis van de gedaante:

$$\alpha_1 = a_{11}\omega_1,$$
$$\alpha_2 = a_{21}\omega_1+a_{22}\omega_2,$$
$$\text{- - - - - - - - - -}$$
$$\alpha_n = a_{n1}\omega_1+a_{n2}\omega_2+\ldots+a_{nn}\omega_n,$$

waarin de a's geheel rationaal, en $a_{11},a_{22},\ldots,a_{nn}$ positief zijn.

Bewijs. Elk ideaal $\underline{a}$ bevat een geheel positief getal a. $a\omega_1$ ligt dus in $\underline{a}$. We kiezen nu voor a_{11} dat positieve getal, zó dat $a_{11}\omega_1$ nog in $\underline{a}$ ligt, en a_{11} zo klein mogelijk is. Op dezelfde wijze versta ik onder a_{mm} het kleinste natuurlijke getal, zó dat $\alpha_m=a_{m1}\omega_1+\ldots+a_{mm}\omega_n$ in $\underline{a}$ ligt. We beweren dat $(\alpha_1,\ldots,\alpha_n)$ dan een basis voor $\underline{a}$ vormt. In de eerste plaats zijn $\alpha_1,\ldots,\alpha_n$ lineair onafhankelijk, daar

$$\Delta(\alpha_1,\ldots,\alpha_n) = \begin{vmatrix} a_{11} & 0 & .. & 0 \\ a_{21} & a_{22} & & \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & .. & a_{nn} \end{vmatrix}^2 \Delta(\omega_1,\ldots,\omega_n)=(a_{11}\ldots a_{nn})^2\Delta\neq 0.$$

Zij verder α een getal van $\underline{a}$, dan is zeker $\alpha=b_1\omega_1+\ldots+b_n\omega_n$ met geheel rationale b. Deel b_n door a_{nn}: $b_n=h_n a_{nn}+r_n$ $(0\leqq r_n<a_{nn})$. Dan behoort $\alpha-h_n\alpha_n=b_1'\omega_1+\ldots+b'_{n-1}\omega_{n-1}+r_n\omega_n$ met geheel rationale b' tot $\underline{a}$; volgens de definitie van a_{nn} is dus $r_n=0$, en dus $\alpha-h_n\alpha_n=b_1'\omega_1+\ldots+b'_{n-1}\omega_{n-1}$. Hierin is evenzo b'_{n-1} door $a_{n-1,n-1}$ deelbaar, dus $\alpha-h_n\alpha_n-h_{n-1}\alpha_{n-1}=b''_1\omega_1+\ldots+b''_{n-2}\omega_{n-2}$, enz. tot

$$\alpha-h_n\alpha_n-h_{n-1}\alpha_{n-1}-\ldots-h_1\alpha_1=0 \text{ met geheel rationale h.}$$

Stelling. $\Delta(\underline{a}) = (N\underline{a})^2\Delta$.

Bewijs. We hebben gezien $\Delta(\alpha_1,\ldots,\alpha_n)=(a_{11}\ldots a_{nn})^2\Delta$.

We moeten dus bewijzen: $a_{11}\ldots a_{nn}=N\underline{a}$. Daarvoor is het voldoende aan te tonen, dat

1°. elk tweetal van de $a_{11}a_{22}\ldots a_{nn}$ getallen:

$$r_1\omega_1+\ldots+r_n\omega_n,\quad 0\leqq r_m<a_{mm} \text{ voor } 1\leqq m\leqq n$$

incongruent mod $\underline{a}$ zijn, en dat

2^{o}. elk geheel getal η van het lichaam met een van deze getallen congruent mod $\underline{a}$ is.

1^{o}. Uit $r_1\omega_1+\ldots+r_n\omega_n \equiv r_1'\omega_1+\ldots+r_n'\omega_n \pmod{\underline{a}}$, $0 \leqq r_m < a_{mm}$, $0 \leqq r_m' < a_{mm}$ volgt:

$$\sum_{m=1}^{n}(r_m-r_m')\omega_m \equiv 0 \pmod{\underline{a}}, \text{ of}$$

$$\pm \sum_{m=1}^{n-1}(r_m-r_m')\omega_m + |r_n-r_n'|\omega_n \equiv 0 \pmod{\underline{a}}.$$

Volgens de definitie van a_{nn} is dus $r_n=r_n'$. Op dezelfde wijze volgt voor $n>1$ ook: $r_{n-1}=r_{n-1}', \ldots, r_1=r_1'$.

2^{o}. Elk geheel getal η van het lichaam heeft de gedaante:

$$\eta = b_1\omega_1+\ldots+b_n\omega_n \text{ met geheel rationale b.}$$

Deelt men b_n door a_{nn}: $b_{n1}=h_n a_{nn}+r_n$, $0 \leqq r_n < a_{nn}$, dan is $\eta - h_n\alpha_n = b_1'\omega_1+\ldots+b_{n-1}\omega_{n-1}+r_n\omega_n$, enz. tot

$$\eta - h_n\alpha_n - \ldots - h_1\alpha_1 = r_1\omega_1+\ldots+r_n\omega_n, \quad 0 \leqq r_n < a_{mm} \quad (m=1,\ldots,n).$$

$$\eta \equiv r_1\omega_1+\ldots+r_n\omega_n \pmod{\underline{a}}.$$

<u>Stelling</u>. Is $\alpha_1,\ldots,\alpha_n$ een basis van het ideaal $\underline{a}$ en $\omega_1,\ldots,\omega_n$ een lichaamsbasis, dus

$$\alpha_k = \sum_{l=1}^{n} c_{kl}\omega_l, \quad 1 \leqq k \leqq n, \text{ met geheel rationale c,}$$

dan is $$|c_{kl}| = \pm N\underline{a}.$$

<u>Bewijs</u>.

$\Delta(\underline{a}) = |c_{kl}|^2\Delta$; volgens de vorige stelling is:

$\Delta(\underline{a}) = (N\underline{a})^2\Delta$, dus $|c_{kl}| = \pm N\underline{a}$.

<u>Stelling</u>. Is $\alpha \neq 0$ een geheel getal van het lichaam, dan is

$$N[\alpha] = |N\alpha|.$$

<u>Bewijs</u>. Is $\omega_1,\ldots,\omega_n$ een lichaamsbasis, dan is $\alpha\omega_1,\ldots,\alpha\omega_n$ een basis van het ideaal $[\alpha]$, daar $\alpha(h_1\omega_1+\ldots+h_n\omega_n)=h_1\alpha\omega_1+\ldots+h_n\alpha\omega_n$, h's geheel rationaal.

Nu is

$$\Delta[\alpha] = \Delta(\alpha\omega_1,\ldots,\alpha\omega_n)$$

$$= \begin{vmatrix} \alpha_1\omega_{11} \cdots \alpha_1\omega_{n1} \\ \vdots \\ \alpha_n\omega_{1n} \cdots \alpha_n\omega_{nn} \end{vmatrix}^2 = (\alpha_1\alpha_2\ldots\alpha_n)^2 \Delta(\omega_1,\ldots,\omega_n)$$

$$= (N\alpha)^2 \Delta(\omega_1,\ldots,\omega_n).$$

Ook is $\Delta[\alpha] = \{N[\alpha]\}^2 \Delta(\omega_1,\ldots,\omega_n)$. Daar $\Delta(\omega_1,\ldots,\omega_n)\neq 0$ is, geldt $N[\alpha] = \pm N\alpha$.

Stelling. Elk priemideaal $\underline{p}$ bevat precies één priemgetal p.
Bewijs. We hebben reeds bewezen dat $\underline{p}$ hoogstens één priemgetal bevat. We zullen nu bewijzen, dat $\underline{p}$ tenminste één priemgetal bevat. $\underline{p}$ bevat zeker een natuurlijk getal a. Uit $a=\pi p$ volgt $\underline{p}/[a] \rightrightarrows \underline{p}/[\pi p] \rightrightarrows \underline{p}/\pi[p]$, dus voor minstens één p $\underline{p}/[p] \rightrightarrows \underline{p}/p$.

Stelling. Als p het priemgetal is dat bij $\underline{p}$ behoort, dan volgt uit $\underline{p}/a$, a geheel rationaal, dat p/a is.
Bewijs. Voor a=0 is de stelling duidelijk. Zij verder $|a| = \pi p'$. Uit $\underline{p}/a$ volgt $\underline{p}/\pi p'$, dus voor één p' $\underline{p}/p' \rightrightarrows p'=p. \rightrightarrows p/a$.

Stelling. Als p het priemgetal is dat in $\underline{p}$ ligt, dan is $N\underline{p}=p^f$, waarin f een natuurlijk getal $\leqq n$ is.
Bewijs. Uit $\underline{p}/p$ volgt $[p] = \underline{p}\,\underline{a}$, dus

$$p^n = N[p] = N(\underline{p}\,\underline{a}) = N\underline{p}.N\underline{a}, \text{ dus } N\underline{p}/p^n.$$

Verder is $N\underline{p} > 1$.

Definitie. De f uit de vorige stelling heet de graad van $\underline{p}$
Stelling. $\underline{a}/N\underline{a}$.
Bewijs. Is $\beta_1,\ldots,\beta_{N\underline{a}}$ een representantensysteem van de $N\underline{a}$ klassen mod $\underline{a}$, dan is blijkbaar $\beta_1+1,\ldots,\beta_{N\underline{a}}+1$ er ook een; want dit zijn $N\underline{a}$ incongruente getallen van het lichaam; dus is

$$\beta_1+\ldots+\beta_{N\underline{a}} \equiv (\beta_1+1) + \ldots + (\beta_{N\underline{a}}+1) \pmod{\underline{a}}$$

$$0 \equiv N\underline{a} \pmod{\underline{a}}.$$

Stelling. $\alpha^{N\underline{p}-1} \equiv 1 \pmod{\underline{p}}$ voor $\underline{p} \nmid \alpha$.
Opmerking. Voor P is dit de stelling van Fermat.
Bewijs. Zij $\beta_1,\beta_{N\underline{p}}$ het representantensysteem van de $N\underline{p}$ klassen mod $\underline{p}$. Hiervan laten wij de representant van die klasse weg, die uit de voor $\underline{p}$ deelbare getallen bestaat, zeg $\beta_{N\underline{p}}$.
Dan zijn de niet door $\underline{p}$ deelbare getallen

$\alpha\beta_1,\ldots,\alpha\beta_{N\underline{p}-1}$ representanten van de $N\underline{p}-1$ klassen, daar het aantal $N\underline{p}-1$ is, en uit

$$\alpha\beta_r \equiv \alpha\beta_s \pmod{\underline{p}},\ 1 \leqq r < N\underline{p},\ 1 \leqq s < N\underline{p}$$

volgt.

$$\underline{p} / \alpha(\beta_r - \beta_s), \text{ en dus } \beta_r = \beta_s.$$

Dus is $$\alpha\beta_1\, \alpha\beta_2 \ldots \alpha\beta_{N\underline{p}-1} \equiv \beta_1\beta_2\ldots\beta_{N\underline{p}-1} \pmod{\underline{p}},$$

$$\alpha^{N\underline{p}-1}\, \beta_1\beta_2\ldots\beta_{N\underline{p}-1} \equiv 1\cdot\beta_1\beta_2\ldots\beta_{N\underline{p}-1} \pmod{\underline{p}}.$$

$$\underline{p} / (\alpha^{N\underline{p}-1} - 1)\beta_1\beta_2\ldots\beta_{N\underline{p}-1}$$

$$\underline{p} / \alpha^{N\underline{p}-1} - 1.$$

Stelling. Er zijn slechts eindig veel idealen met een zelfde norm.
Bewijs. Is een natuurlijk getal m gegeven, dan is als er een ideaal met de norm m is, $\underline{a}/m$. Er zijn slechts eindig veel van zulke idealen.

Stelling. Uit $N\underline{a}=p$ volgt dat $\underline{a}$ priemideaal is.
Bewijs. Uit $\underline{a} = \underline{b}\,\underline{c}$ zou volgen

$p = N\,\underline{a} = N\,\underline{b}\;N\,\underline{c}$, dus òf $N\,\underline{b} = 1$, of $N\,\underline{c} = 1$,

dus òf $\underline{b} = \underline{0}$ of $\underline{c} = \underline{0}$.

Voorbeelden van idealen in $P(i\sqrt{5})$.
We willen $[6]$ in priemidealen ontbinden.
Noch $[6] = [2]\,[3]$, noch $[6] = [1 + i\sqrt{5}]\,[1-i\sqrt{5}]$ is een ontbinding in priemidealen. We hebben vroeger reeds gezien dat $[3,1+i\sqrt{5}]$ geen hoofdideaal is, toch is $[3,1+i\sqrt{5}] \mid [6]$. Niet elk priemideaal van $[6]$ kan dus hoofdideaal zijn.
We noemen nu: $[2,1+i\sqrt{5}] = \underline{a}_1$, $[3,1+i\sqrt{5}] = \underline{a}_2$, $[3,1-i\sqrt{5}] = \underline{a}_3$.
Dan is
$\underline{a}_1^2 = [2,1+i\sqrt{5}]\,[2,1+i\sqrt{5}] = [4,2+2i\sqrt{5},\ 2+2i\sqrt{5},\ -4+2i\sqrt{5}] =$
$[2]\,[2,1+i\sqrt{5},\ -2+i\sqrt{5}]$.
Nu is $2.2+(-1)(1+i\sqrt{5})+(-2+i\sqrt{5})=1$, dus het laatste ideaal $=\underline{0}$, dus
$\underline{a}_1^2 = [2]$.
$(N\underline{a}_1)^2 = N[2] = 4$, dus $N\underline{a} = 2$, dus $\underline{a}_1$ is priemideaal. Verder is

$$\underline{a}_1\underline{a}_2 = [3,1+i\sqrt{5}]\,[3,1-i\sqrt{5}] = [9,3+3i\sqrt{5},\ 3-3i\sqrt{5},6] =$$

$[3]\,[3,1+i\sqrt{5},\ 1-i\sqrt{5},2] = [3]$, dus daar $\underline{a}_2$ geen hoofdideaal is $\underline{a}_2 \neq \underline{0}$, $\underline{a}_2 \neq [3]$, dus $\underline{a}_3 \neq 0$, $N\underline{a}_2 > 1$, $N\underline{a}_3 > 1$. Uit $N\underline{a}_2 N\underline{a}_3 = N(3) = 9$ volgt dus $N\underline{a}_2 = N\underline{a}_3 = 3$. Dus $\underline{a}_2$ en $\underline{a}_3$ zijn priemidealen.
Verder is $\underline{a}_2 \neq \underline{a}_3$, anders zou $\underline{a}_2 / 1-i\sqrt{5}$, $\underline{a}_2 / 1+i\sqrt{5}$, dus $\underline{a}_2 / 2$. Daar $\underline{a}_2 / 3$ zou $\underline{a}_2 = \underline{0}$ zijn.
De ontbinding van $[6]$ is dus:

$$[6] = [2]\,[3] = [2,1+i\sqrt{5}]^2\,[3,1+i\sqrt{5}]\,[3,1-i\sqrt{5}].$$

In de ontbinding: $[6] = [1 + i\sqrt{5}]\,[1-i\sqrt{5}]$ vallen de factoren rechts uiteen in $[1+i\sqrt{5}] = \underline{a}_1\underline{a}_2$, en $[1-i\sqrt{5}] = \underline{a}_1\underline{a}_3$. Dit kan men als volgt inzien:

$$[1 + i\sqrt{5}]\,[1-i\sqrt{5}] = \underline{a}_1^2\,\underline{a}_2\,\underline{a}_3, \text{ dus}$$

$$\underline{a}_1 / [1+i\sqrt{5}]\,,\ \underline{a}_2 / [1+i\sqrt{5}] \rightrightarrows \underline{a}_1\underline{a}_2 / [1+i\sqrt{5}]\,.$$

($\underline{a}_1$ en $\underline{a}_2$ zijn verschillende priemidealen)

$$N(\underline{a}_1\underline{a}_2) = 2.3 = 6,\quad N[1+i\sqrt{5}] = 6; \text{ dus}$$

$$\underline{a}_1\,\underline{a}_2 = [1+i\sqrt{5}]\,; \text{ dus } \underline{a}_1\,\underline{a}_3 = [1-i\sqrt{5}]\,.$$

ALGEBRAISCHE GETALLENLICHAMEN X

door

Prof.Dr B. Meulenbeld

22 februari 1956

Kwadratische Getallenlichamen.

Beschouwen getallenlichamen van de tweede graad $P(\vartheta)$, waarbij ϑ wortel is van een vierkantsvergelijking. Elk getal van $P(\vartheta)$ is dus te schrijven als $x+y\vartheta$, met x en y rationaal.

Stelling 1) Elk kwadratisch getallenlichaam heeft de gedaante $P(\sqrt{C})$, waarin C geheel rationaal is, $\neq 0$, $\neq 1$ en kwadraatvrij.

2) Voor elke C is $P(\sqrt{C})$ een kwadratisch lichaam.

3) Van twee verschillende C's zijn de lichamen verschillend.

Bewijs. 1. Laat de vierkantsvergelijking waaraan ϑ voldoet zijn: $ax^2+bx+c=0$, dan is

$$\vartheta = \frac{-b \pm \sqrt{b^2-4ac}}{2a} .$$

Elk getal van $P(\vartheta)$ is dan te schrijven als $x+y\vartheta = x-\frac{b}{2a}y \pm \frac{y}{2a}\sqrt{b^2-4ac}$. Nu is $x-\frac{b}{2a}y$ en ook $\frac{y}{2a}$ rationaal; dus het getal te schrijven als $x_1+y_1\sqrt{b^2-4ac}$, met x_1 en y_1 rationaal. Het lichaam is dus $P(\sqrt{b^2-4ac})$. b^2-4ac kan niet 0 of een kwadraat zijn, dus $b^2-4ac=q^2C$ met $C\gtrless 0$, $C\neq 1$, C kwadraatvrij. $x_1+y_1\sqrt{b^2-4ac}=x_1+y_1q\sqrt{C}$. Het lichaam is dus $P(\sqrt{C})$.

2. Duidelijk daar $\sqrt{C}$ wortel is van de irreducibele veelterm x^2-C.

3. Uit $P(\sqrt{C_1})=P(\sqrt{C_2})$, waarin C_1 en C_2 geheel rationaal, $\neq 0$, $\neq 1$ en kwadraatvrij zijn, volgt $\sqrt{C_1}=a+b\sqrt{C_2}$, met rationale a en b. Hierin is zeker $b\neq 0$, daar anders $\sqrt{C_1}$ rationaal zou zijn. Uit $C_1=a^2+2ab\sqrt{C_2}+b^2C_2$ volgt dus $a=0$, dus $C_1=b^2C_2$, met b rationaal $=\pm\frac{p}{q}$, $p>0$, $q>0$. $(p,q)=1$. Dus $q^2C_1=p^2C_2$. Nu is q^2/C_2 en p^2/C_1, dus $p=1$, $q=1$, $b=\pm 1$ of $C_1=C_2$.

Stelling. Het lichaam $P(\vartheta)$ met $\vartheta=\sqrt{C}$ (C geheel rationaal $\neq 0$, $\neq 1$, kwadraatvrij) heeft de basis

$$1,\ \vartheta \quad \text{als } C \equiv 2 \text{ of } 3 \pmod 4,$$
$$1,\ \frac{1+\vartheta}{2} \quad \text{als } C \equiv 1 \pmod 4.$$

Bewijs. ϑ is geheel want is wortel van $x^2-C=0$. Proberen als basis $(1,\vartheta)$. Dit is zo als voor gehele $\alpha=x+y\vartheta$ de x en y geheel rationaal zijn. Nu is α geheel als α wortel is van $\alpha^2-S\alpha+N=0$ en S en N geheel rationaal zijn (noodzakelijke en voldoende voorwaarde). $S=\alpha+\bar{\alpha}$, $N=\alpha\bar{\alpha}$. $\alpha=x+y\vartheta$, $\bar{\alpha}=x-y\vartheta$, dus $S(\alpha)=2x$, $N(\alpha)=x^2-y^2C$. Uit $2x$=geheel en x^2-y^2C=geheel, zouden wij dan moeten concluderen tot x=geheel, y=geheel. x^2-y^2C=geheel, dus $(2x)^2-(2y)^2C$=4 voud, dus $(2y)^2C$=geheel.

Hieruit volgt 2y=geheel. Was nl. $2y=\frac{p}{q}$ (p en q geheel rationaal (p,q)=1), dan zou $\frac{p^2C}{q^2}$ = geheel zijn, en dit kan niet daar C kwadraatvrij is. Dus 2x=geheel, 2y=geheel.

Stel <u>C=4v +2.</u> Nu is $(2x)^2=4v$ of $4v+1$, $(2y)^2=4v$ of $4v+1$, dus

$(4v+0$ of $+1)-(4v+0$ of $+1)(4v+2)=4v$, of $(0$ of $+1)-(0$ of $2)=4^v$.
Dit kan alleen als wij beide 0 nemen, d.w.z. $(2x)^2=4v$ en $(2y)^2=4v$, of 2x en 2y beide even, of x en y geheel. Als $C=4v+2$, is dus $(1,\vartheta)$ een basis.

Stel <u>C=4v +3</u>. Dan $(4v+0$ of $+1)-(4v+0$ of $+1)(4v+3)=4$ voud, of
$(0$ of $+1)-(0$ of $3))=4$ voud.
Weer beide 0, dus ook nu is $(1,v)$ een basis.

Stel <u>C=4v +1</u>. Dan $(4v+0$ of $+1)-(4v+0$ of $+1)(4v+1)=4v$, of
$(0$ of $+1)-(0$ of $+1)=4v$.

Nu kan dus optreden 0 en 0 òf 1 en 1, d.w.z. òf 2x en 2y zijn beide even, òf 2x en 2y zijn beide oneven. 2x en 2y hebben dezelfde pariteit. Is 2y = M (geheel rationaal), dan kunnen we stellen 2x = M + 2L. (L geheel rationaal).
$\alpha = x+y\vartheta = \frac{M+2L}{2} + \frac{M}{2}\vartheta = L + M(\frac{1+\vartheta}{2})$.

Elk geheel getal α is dus te schrijven in de gedaante

$$\alpha = L.1 + M.\frac{1+\vartheta}{2},$$ d.w.z. $(1, \frac{1+\vartheta}{2})$ is een basis, als $\frac{1+\vartheta}{2}$ geheel is. Is $\eta=\frac{1+\vartheta}{2}$, dan is $\bar{\eta}=\frac{1-\vartheta}{2}$. $\eta+\bar{\eta}=1$, $\eta\bar{\eta}=\frac{1-\vartheta^2}{4}=$
$=\frac{1-C}{4}$.

Daar $C=4v+1$, is $\frac{1-C}{4}$ geheel; dus η is geheel. Hiermede is de stelling volledig bewezen.

<u>Stelling.</u> Het grondtal is:

$$\Delta = 4C \text{ als } C \equiv 2 \text{ of } 3 \pmod 4,$$
$$\Delta = C \text{ als } C \equiv 1 \pmod 4.$$

<u>Bewijs</u>. Is $C \equiv 2$ of $3 \pmod 4$, dan is de basis $(1,\vartheta)$; dus
$\Delta = \begin{vmatrix} 1 & \vartheta \\ 1 & \vartheta \end{vmatrix}^2 = 4\vartheta^2 = 4C.$

Is $C \equiv 1 \pmod 4$, dan is de basis $(1, \frac{1+\vartheta}{2})$;
dus
$$\Delta = \begin{vmatrix} 1 & \frac{1+\vartheta}{2} \\ 1 & \frac{1-\vartheta}{2} \end{vmatrix}^2 = \vartheta^2 = C.$$

<u>Opmerking</u>. Als $C \equiv 2$ of $3 \pmod 4$, dan is $\Delta \equiv 8$ of $12 \pmod{16}$; is $C \equiv 1 \pmod 4$, dan is $\Delta \equiv 1 \pmod 4$. Voor grondtallen komen dus alleen

in aanmerking 16 vouden + 8 en + 12, en 4 vouden + 1., die kwadraatvrij zijn. 7 en 25 kunnen bijv. geen grondtallen zijn.

Stelling.1) Elk kwadratisch lichaam is $P(\sqrt{\Delta})$, als Δ het grondtal is. Δ heet fundimentaal discriminant
2) Is Δ een fundimentaal discriminant, dan is $P(\sqrt{\Delta})$ een kwadratisch lichaam met grondtal Δ .
3) Met twee verschillende fundimentaal discriminanten komen verschillende kwadratische lichamen overeen.

Bewijs. 1. Daar $C = \frac{\Delta}{4}$ resp. Δ , is $P(\sqrt{C})=P(\sqrt{\Delta})$.
2. Is Δ fundimentaal discriminant, dan is $P(\sqrt{\Delta})=P(\sqrt{C})$, waarin

$$C = \begin{cases} \frac{\Delta}{4} \text{ voor } \Delta \equiv 8 \text{ of } 12 \pmod{16} \\ \Delta \text{ voor } \Delta \equiv 1 \pmod 4. \end{cases}$$

Deze C is $\neq 0$, $\neq 1$ en kwadraatvrij. Is $\Delta \equiv 8$ of 12 (mod 16), dan is $C \equiv 2$ of 3 (mod 4); is $\Delta \equiv 1$ (mod 4), dan is $C \equiv 1$ (mod 4). Dus heeft $P(\sqrt{\Delta})=P(\sqrt{c})$ als grondtal Δ .
3. Volgens een vorige stelling volgt uit $P(\sqrt{\Delta_1})=P(\sqrt{\Delta_2})$ dat $\Delta_1 = \Delta_2$.

Stelling. Het lichaam $P(\sqrt{\Delta})$ met grondtal Δ heeft steeds tot basis
$1, \frac{\sqrt{\Delta}}{2}$ voor $\Delta \equiv 0 \pmod 4$;

$$1, \frac{1+\sqrt{\Delta}}{2} \text{ voor } \Delta \equiv 1 \pmod 4.$$

Bewijs. Voor $\Delta \equiv 0 \pmod 4$ is $C = \frac{\Delta}{4}$, $\vartheta = \sqrt{C} = \frac{\sqrt{\Delta}}{2}$;
voor $\Delta \equiv 1 \pmod 4$ is $C = \Delta$, $\frac{1+\vartheta}{2} = \frac{1+\sqrt{\Delta}}{2}$.

Voorbeelden. $P(i)$: $\Delta = -4$, $\frac{\sqrt{\Delta}}{2} = i$
$P(\rho)$: $\Delta = -3$, $\frac{1+\sqrt{\Delta}}{2} = \frac{1+i\sqrt{3}}{2}$.
$P(i\sqrt{5})$: $\Delta = -20$, $\frac{\sqrt{\Delta}}{2} = i\sqrt{5}$.

Onderzoek idealen:

De basis van een ideaal uit $P(\sqrt{\Delta})$ bestaat uit twee getallen α_1, α_2, die beide geheel algebraisch zijn.

Stelling. Elk ideaal $\underline{a}$ van het lichaam heeft een basis van de gedaante $A, G+B\omega$, waarin $0 \leq G < A$, $B > 0$ en A,B,G geheel rationaal zijn.
Bewijs. Volgens een vorige stelling is er een basis te vinden van de vorm:

$$\alpha_1 = a_{11}\omega_1$$
$$\alpha_2 = a_{21}\omega_1 + a_{22}\omega_2,$$

waarin $a_{11} > 0$, $a_{22} > 0$, en a_{11}, a_{21}, a_{22} geheel rationaal zijn. Kortweg: er is een basis van de gedaante ($(1,\omega)$ is een basis van het lichaam): $A, G+B\omega$, waarin A het kleinste natuurlijke getal van $\underline{a}$ is, en B het

kleinste natuurlijke getal is, waarvoor bij passende gehaal rationale G_0 het getal $G_0+B\omega$ in $\underline{a}$ voorkomt. Daar met α ook α-MA voor elke geheel rationale M in $\underline{a}$ voorkomt, kan men het zo inrichten dat $0 \leq G < A$ is.

Stelling. $\underline{a}$ heeft slechts één basis van de gedaante $A, G+B\omega$ waarin A,G en B geheel rationaal zijn, $0 \leq G < A$ en $B > 0$.

Bewijs. Elk getal van $\underline{a}$ heeft, als $A, G+B\omega$ een basis vormen, de gedaante $xA+y(G+B\omega)$, x en y geheel rationaal.

1) De geheel rationale getallen van het ideaal zijn de getallen xA. A is dus het kleinste natuurlijke getal van $\underline{a}$, dus door $\underline{a}$ eenduidig bepaald.

2) In $(xA+yG)+yB\omega$ is yB als $y > 0$ is $\geq B$.
B is dus het kleinste natuurlijke getal, waarvoor $G_0+B\omega$ bij passende G_0 in $\underline{a}$ voorkomt, is dus door $\underline{a}$ eenduidig bepaald.

3) Heeft $\underline{a}$ de bases $A, G_1+B\omega$ en $A, G_2+B\omega$, met $0 \leq G_1 < A, 0 \leq G_2 < A$, $B > 0$, dan is $(G_1-G_2) = (G_1+B\omega)-(G_2+B\omega)$ een getal van $\underline{a}$. Daar $(G_1-G_2) < A$ is, moet dus $G_1=G_2$ zijn.

Definitie. De bovengevormde eenduidig bepaalde basis heet de kanonieke ideaalbais. Voor $\underline{a} = \underline{0}$ is A=1, G=0, B=1.

Stelling. In de kanonieke ideaalbasis is

$$B/A,\ B/G.$$

Bewijs. 1) $A\omega$ behoort tot $\underline{a}$. Dus is:

$$A\omega = xA + y(G+B\omega),$$

$$A = yB \rightrightarrows B/A.$$

2) $G+B\omega$ behoort tot $\underline{a}$; $-\bar{\omega}(G+B\omega)$ behoort tot $\underline{a}$.
$-\bar{\omega}(G+B\omega) = -BN(\omega) - \bar{\omega}G = -BN(\omega) - G(S(\omega)-\omega)$
$= (-BN(\omega) - G\,S(\omega)) + G\omega = t + G\omega$.
Dus moet $t+G\omega = uA+v(G+B\omega)$ $\qquad G=vB \rightrightarrows B/G.$

Opmerking. De kanonieke basis van $\underline{a}$ kan men dus ook schrijven als:
$BM,\ BR + B\omega$ met $0 \leq R < M$.
Ieder getal van $\underline{a}$ is dus te schrijven in de gedaante:
$c_1\,BM + c_2(BR + B\omega) = B\{c_1M + c_2(R+\omega)\}$.
Dus $\underline{a} = [B]\,\underline{a}_1$, $B > 0$, waarin $\underline{a}_1$ een ideaal is met basis $M, R+\omega$, en $0 \leq R < M$.

ALGEBRAISCHE GETALLENLICHAMEN XI

door

Prof.Dr B. Meulenbeld

7 maart 1956

Stelling. Is $B > 0$, $0 \leqslant R < M$ (B,M en R geheel rationaal, dan vormen BM, $BR + B\omega$ de kanonieke basis van een ideaal, dan en alleen dan als $M/N\ (R+\omega)$ is.

Bewijs. Zal BM, $BR + B\omega$ een basis zijn van het ideaal, dan moet elk getal van het ideaal $[BM, BR + B\omega]$ te schrijven zijn als $xBM + y(BR+B\omega)$ (x en y geheel rationaal). Daarvoor is nodig en voldoende dat de twee getallen $BM\omega$ en $(BR + B\omega)\omega$ in deze vorm zijn te schrijven.

Nodig. $BM\omega$ en $(BR + B\omega)\omega$ zijn getallen van het ideaal.

Voldoende: Elk getal α van het ideaal is te schrijven als $\alpha = \eta_1 BM + \eta_2(BR + B\omega)$ waarin η_1 en η_2 gehele getallen zijn van het lichaam η_1 en η_2 zijn te schrijven als $\eta_1 = c_1 + c_2\omega$, $\eta_2 = c_3 + c_4\omega$ (c_1, c_2, c_3, c_4 geheel rationaal).

Dus $\alpha = (c_1+c_2\omega)BM + (c_3+c_4\omega)(BR + B\omega)$

$= c_1BM + c_3(BR + B\omega) + c_2\, BM\omega + c_4(BR + B\omega)\omega$.

Zijn dus $BM\omega$ en $(BR + B\omega)\omega$ te schrijven in de vorm $xBM+y(BR+B\omega)$, dan is dit dus ook het geval met α.

Nu is $BM\omega = -RBM + M(BR + B\omega)$, dus in de gewenste vorm met $x=-R$ en $y=M$.

De vraag is dus of geldt:

$$(BR + B\omega)\omega = xBM + y(BR + B\omega), \text{ of}$$

$$(R + \omega)\omega = xM + y(R + \omega)$$

met x en y geheel rationaal. In elk geval is

$$(R + \omega)\omega = -(R+\omega)(R+\bar{\omega}) + (R+\bar{\omega}+\omega)(R+\omega)$$

$$= -\frac{N(R+\omega)}{M} M + (R + s(\omega))(R + \omega).$$

We hebben dus de gewenste voorstelling met

$$x = -\frac{N(R+\omega)}{M}, \quad y = R + S(\omega).$$

y is zeker geheel rationaal, x is alleen dan geheel rationaal als

$$M/N\ (R + \omega).$$

Opmerking. $M/N(R+\omega)$ betekent in het geval $\Delta \equiv 0 \pmod 4$:

$M/N\ (R + \frac{\sqrt{\Delta}}{2})$, $M/R^2 - \frac{\Delta}{4}$ of $4M/(2R)^2 - \Delta$

of $(2R)^2 \equiv \Delta \pmod{4M}$.

In het geval $\Delta \equiv 1 \pmod 4$:

$M/N(R + \frac{1+\sqrt{\Delta}}{2})$, $M/\frac{(2R+1)^2 - \Delta}{4}$ of $4M/(2R+1)^2 - \Delta$.

of $(2R+1)^2 \equiv \Delta \pmod{4M}$.

Dus steeds is Δ kwadraatrest mod $4M$.

Priemidealen

Elk priemideaal $\underline{p}$ bevat één priemgetal p. Door $\underline{p}$ is p bepaald. Niet omgekeerd. Uit $\underline{p}/p$ volgt $\underline{p}/[p]$. In het algemeen behoeft dit hoofdideaal geen priemideaal te zijn. We trachten nu $[p]$ te ontbinden. $[p] = \underline{p}_1\underline{p}_2 \ldots \underline{p}_r$. In het algemeen is $N[g] = g^n$, als g geheel rationaal en n de graad van het lichaam is. In ons geval is $N[p] = p^2$. Dus $p^2 = N\underline{p}_1 N\underline{p}_2 \ldots N\underline{p}_r$. Mogelijkheden: $r=1$: $N\underline{p}_1 = p^2$, dus $[p] = \underline{p}$. Hoofdideaal = priemideaal. $r=2$: $[p] = \underline{p}\,\underline{q}$ met $N\underline{p} = N\underline{q} = p$.
Het kan zijn dat $\underline{p} = \underline{q}$ in dit laatste geval. We onderscheiden dus de volgende gevallen:

I $\quad [p] = \underline{p}, \quad N\underline{p} = p^2$.

II $[p] = \underline{p}\,\underline{q}$, $N\underline{p} = p$, $N\underline{q} = q$, en hierin:

IIa. $\quad \underline{p} \neq \underline{q}$.

IIb. $\quad \underline{p} = \underline{q}$.

Stelling. Het geval II doet zich dan en alleen dan voor, als Δ kwadraatrest mod $4p$ is. Dan is $\underline{p} = [p, R+\omega]$, $\underline{q} = [p, R+\bar{\omega}]$ bij passende R.

Bewijs 1. Nodig. Stel geval II doet zich voor. Dan is er dus een $\underline{p}$ met $N\underline{p} = p$. We nemen de kanonieke basis BM, $BR + B\omega$ van $\underline{p}$, waarbij dus

$$0 \leq R < M, \quad B > 0, \quad \Delta \text{ kwadraatrest mod } 4M \text{ is.}$$

Vroeger gehad de stelling: Is $\alpha_1 \ldots, \alpha_n$ een basis van $\underline{a}$ en $\omega_1, \ldots \omega_n$ een lichaamsbasis en

$$\alpha_k = \sum_{i=1}^{n} c_{ki}\,\omega_i, \quad 1 \leq k \leq n, \text{ met geheel rationale } c,$$

dan is

$$|c_{ki}| = \pm N\underline{a}.$$

Volgens deze stelling is $p = N\underline{p} = \begin{vmatrix} BM & 0 \\ BM & B \end{vmatrix} = B^2M$.
dus $B = 1$, $M = p$, $\underline{p} = [p, R+\omega]$; en Δ is kwadraatrest mod $4p$.

2. Voldoende. Zij Δ kwadraatrest mod 4p. Dan kiezen we x zo,dat $x^2 \equiv \Delta \pmod{4p}$. Bij even Δ is x even, we noemen dan x=2R. Bij oneven Δ is x oneven; we noemen dan x=2R+1. Dan is

$$N(R+\omega) = \begin{cases} \frac{(2R)^2 - \Delta}{4} & \text{voor } 2/\Delta \ , \\ \frac{(2R+1)^2 - \Delta}{4} & \text{voor } 2 \nmid \Delta \ ; \end{cases}$$

dus $p/N(R+\omega)$.
Voor de idealen $\underline{p} = [p, R+\omega]$, $\underline{q} = [p, R+\bar{\omega}]$ geldt $\underline{p}\,\underline{q} = [p^2, p(R+\omega), p(R+\bar{\omega}), N(R+\omega)] = [p]\left[p, R+\omega, R+\bar{\omega}, \frac{N(R+\omega)}{p}\right] = [p]\,\underline{a}$, dus

$$N\underline{p}\ N\underline{q} = N(\underline{p}\,\underline{q}) = N([p]\,\underline{a}) = p^2 N\underline{a}.$$

Nu is $\underline{p}/[p]$, maar $[p] \nmid \underline{p}$, daar $R+\omega$ geen veelvoud van p is, en $\underline{q}/[p]$, doch $[p] \nmid \underline{q}$, dus $N\underline{p} = 1$ of p, $N\underline{q} = 1$ of p. Dus is $N\underline{p} = N\underline{q} = p$. Dus zijn $\underline{p}$ en $\underline{q}$ priemidealen; $N\underline{a} = 1$, $\underline{a} = \underline{O}$, $\underline{p}\,\underline{q} = [p]$.

Opmerkingen. 1. Geval I doet zich dan en alleen dan voor, als Δ niet-rest mod 4p is.

2. Geval II doet zich in elk geval voor als p/Δ is. Want dan is $\Delta \equiv 0^2$ of $1^2 \pmod 4$, $\Delta \equiv 0^2 \pmod p$, dus als $p > 2$ is Δ kwadraatrest mod 4p. Als p=2 en $2/\Delta$, dan is $\Delta = 16v + 8$ of 12, dus $\Delta \equiv 0^2$ of $2^2 \pmod 8$, dus Δ kwadraatrest mod 4p.

Voorbeeld. Lichaam van Gauss P(i) of $P(\sqrt{-4})$.
$\Delta = -4$, $\omega = i$.

Is $[7] = \underline{p}$ of $\underline{p}\,\underline{q}$? Hangt ervan af of -4 kwadraatrest mod 28 is. Is $x^2 \equiv -4 \pmod{28}$ oplosbaar? x moet even zijn, dus x=2R, dus is een R met $R^2 \equiv -1 \pmod 7$. Er blijkt geen oplossing te zijn. Dus $[7] = \underline{p}$, een priemideaal met norm 49.
Is $[13] = \underline{p}$ of $\underline{p}\,\underline{q}$? Hangt ervan af of -4 kwadraatrest mod 52 is. Is $x^2 \equiv -4 \pmod{52}$ of $R^2 \equiv -1 \pmod{13}$ oplosbaar? R=5 voldoet, dus $[13] = \underline{p}\,\underline{q} = [13, 5+i]\,[13, 5-i]$. Dit zijn 2 priemidealen met norm 13.

Hoe kunnen wij nu de gevallen IIa en IIb onderscheiden? Daarvoor geldt de

Stelling. Zij Δ kwadraatrest mod 4p (dus II). Dan en alleen dan is $\underline{p} = \underline{q}$ als p/Δ is.
Bewijs. $\underline{p} = \underline{q}$ betekent $[p, R+\omega] = [p, R+\bar{\omega}]$. Dit betekent hetzelfde als $[p, R+\omega] / [p, R+\bar{\omega}]$, daar het hier over priemidealen gaat. Dus moet $[p, R+\omega] / R+\bar{\omega}$, en ook $[p, R+\omega] / (R+\bar{\omega}) + (R+\omega)$, of $[p, R+\omega] / 2R+S(\omega)$. Daar $2R+S(\omega)$ geheel rationaal is, moet dus $p/2R+S(\omega)$. Wegens:

$$\{2R+S(\omega)\}^2 - 4p\,\frac{N(R+\omega)}{p} = (2R+\omega+\bar{\omega})^2 - 4(R+\omega)(R+\bar{\omega})$$
$$= 4R^2 + 4R(\omega+\bar{\omega}) + (\omega+\bar{\omega})^2 - 4R^2 - 4R(\omega+\bar{\omega}) - 4\omega\bar{\omega}$$

$= (\omega - \bar{\omega})^2 = \begin{vmatrix} 1 & 1 \\ \omega & \bar{\omega} \end{vmatrix}^2 = \Delta$,

luidt de noodzakelijke en voldoende voorwaarde p/Δ .

We kunnen het bovenstaande samenvatten door het symbool van Kronecker te gebruiken.

Symbool van Legendre. $(\frac{n}{p})$, p priem > 1, $p \nmid n$;

$(\frac{n}{p}) = 1$, als n kwadraatrest mod p is;

$(\frac{n}{p}) = -1$, als n niet-rest mod p is.

Symbool van Jacobi $(\frac{n}{m})$ m oneven, $(m,n) = 1$.

Is m = priem, dan = symbool van Legendre. Verder

$$(\frac{n}{m}) = \prod_{p/m} (\frac{n}{p}).$$

Symbool van Kronecker.

$(\frac{d}{m})$ met d= 4 voud of 4voud + 1; d geen kwadraat $m > 0$. Zijn d en m onderling deelbaar, dan is $(\frac{d}{m}) = 0$. Is m even $= 2^l m'$ (m' oneven), dan is

$$(\frac{d}{m}) = (\frac{d}{2})^l \, (\frac{d}{m'})$$

$(\frac{d}{2})$ = 0 als d even is

= + 1, als d = 8 voud + 1

= + 5, als d = 8 voud - 1.

Stelling. De gevallen I, IIa of IIb doen zich voor al naargelang

$$(\frac{\Delta}{p}) = -1, 1, 0. \quad \text{(Kronecker)}$$

Bewijs. a) Geval IIb doet zich voor als p/Δ , maar dan is $(\frac{\Delta}{p}) = 0$.

b) Geval IIa doet zich voor als $p \nmid \Delta$ en Δ kwadraatrest mod 4p is. Te bewijzen is dan: $(\frac{\Delta}{p}) = 1$.
Stel eerst p=2, dan is $\Delta = 4$ voud + 1, dus òf 8 voud + 1 of 8 voud + 5.
Nu is Δ kwadraatrest mod 8. Maar $x^2 \not\equiv 5 \pmod 8$ heeft geen oplossing, dus moet gelden: $\Delta = 8$ voud + 1; maar dan is $(\frac{\Delta}{2}) = 1$.

Stel $p \neq 2$. Te bewijzen $(\frac{\Delta}{p}) = 1$, en dan stelt dit het symbool van Legendre voor. Nu is Δ kwadraatrest mod 4p, dus zeker kwadraatrest mod p, dus $(\frac{\Delta}{p}) = 1$.

c) Geval I doet zich voor, dan is Δ een niet-rest mod 4p. Hieruit volgt $p \nmid \Delta$.
Stel p=2, dan is $\Delta = 4$ voud + 1, dus 8v + 1 of 8v + 5.
In het eerste geval was Δ wel kwadraatrest mod 8, dus moet $\Delta = 8v + 5$,

en $(\frac{\Delta}{2}) = -1$ zijn.
Stel p oneven. Te bewijzen $(\frac{\Delta}{p}) = -1$, of Δ is een niet-rest mod p, terwijl gegeven is dat Δ een niet-rest mod 4p is. Stel Δ was een kwadraatrest mod p. Er zou dus een x zijn met $x^2 \equiv \Delta \pmod{p}$.
Stel $x^2 - \Delta = 4$ voud, dan is $x^2 \equiv \Delta \pmod{4p}$ en zou Δ een kwadraatrest mod 4p zijn. Tegenspraak. Stel $x^2 - \Delta \neq 4$ voud.
Is $\Delta = 16v + 8$ of 12 dan kon x niet even zijn, dus x = oneven. Maar dan is p-x = even en $(p-x)^2 - \Delta = 4$ voud; terwijl $(p-x)^2 - \Delta = p^2 - 2xp + x^2 - \Delta = p$ voud, dus een 4p voud is. $x^2 \equiv \Delta \pmod{4p}$ zou dan wel een oplossing hebben, nl. p-x. Is $\Delta = 16v + 1$, dan kan x niet even zijn, dus x = even. Maar dan is p-x = oneven, en is $(p-x)^2 - \Delta =$ 4 voud, dus een 4p voud, en $x^2 \equiv \Delta \pmod{4p}$ had weer een oplossing.
Δ is dus een niet-rest mod p, dus $(\frac{\Delta}{p}) = -1$.

ALGEBRAISCHE GETALLENLICHAMEN XII

door

Prof.Dr B. Meulenbeld

28 maart 1956

Stelling. Het aantal oplossingen F(k) van Na=k is van elk natuurlijk getal k gegeven door

$$F(k) = \sum_{n/k} \left(\frac{\Delta}{n}\right) \qquad \text{(symbool van Kronecker).}$$

Zo is het aantal idealen met $N\bar{a}=3$ gelijk aan

$$1 + \left(\frac{\Delta}{3}\right) = 0 \text{ of } 1 \text{ of } 2.$$

Stelling. $F(k_1k_2) = F(k_1)F(k_2)$.
Zo is $F(105^2) = F(3^2)F(5^2)F(7^2)$.

We hebben bij de kwadratische getallenlichamen reeds gezien dat een noodzakelijke en voldoende voorwaarde voor het deelbaar zijn van [p] door het kwadraat van een priemideaal is p/Δ.
Ook hebben wij bij een voorbeeld uit $P(i\sqrt{5})$ afgeleid dat [2] door het kwadraat van een priemideaal $[2,1+i\sqrt{5}]^2$ deelbaar is en [3] geen kwadraat van een priemideaal bevat. Nu is het grondtal Δ van

$$P(i\sqrt{5}) = \begin{vmatrix} 1 & 1 \\ i\sqrt{5} & -i\sqrt{5} \end{vmatrix} = -20.$$

In het eerste geval is $2/-20$ en $3 \nmid -20$.
Deze gevallen zijn bijzondere gevallen van de volgende algemene stelling, die voor elk algebraisch getallenlichaam geldt:
Stelling. Bij een priemgetal bestaat er een p met p^2/p, dan en alleen dan als p/Δ.
Het bewijs van het eerste deel van deze stelling:
"Uit p^2/p volgt p/Δ" is niet lastig;
Het tweede deel: "Uit p/Δ volgt p^2/p" is ingewikkelder.

De stelling van Minkowski over het grondtal: van n=1 is er slechts het lichaam P met grondtal 1. Minkowski heeft nu als eerste het vermoeden bewezen dat voor elk ander algebraisch lichaam, dus met $n \geqslant 2$, het grondtal van ± 1 verschillend is, dus absoluut $\geqslant 2$ is.

Stelling van Minkowski: Voor elk algebraisch lichaam van de n^{de} graad met $n > 1$ is $|\Delta| > 1$.

Elk ideaal is een "tweeledig" ideaal.
Aan het bewijs van deze stelling laten we een hulpstelling voorafgaan.

Hulpstelling. Zijn twee idealen $\underline{a}$ en $\underline{b}$ gegeven, dan bestaat er een α met

$$\left(\frac{[\alpha]}{\underline{a}}, \underline{b}\right) = \underline{0}.$$

Opmerking. α moet men dus zoeken onder de van 0 verschillende getallen van het ideaal $\underline{a}$.

Bewijs. Voor $\underline{b} = \underline{0}$ is de stelling triviaal. Zij $\underline{b} \neq \underline{0}$ en $\underline{p}_1,\ldots,\underline{p}_r$ de verschillende op $\underline{b}$ deelbare priemidealen.
Is r=1, dus $\underline{b} = \underline{p}^b$, $b>0$, dan hebben we dus α zo te kiezen dat

$$\left(\frac{[\alpha]}{\underline{a}}, \underline{p}\right) = \underline{0}.$$

Dit is zeer eenvoudig; men kieze α zo, dat $\underline{a}/\alpha$, $\underline{a}\,\underline{p} \nmid \alpha$ is, dan kan niet $\left(\frac{[\alpha]}{\underline{a}}, \underline{p}\right) = \underline{p}$ zijn. Is $r>1$, dan moet α zo gekozen worden dat $\left(\frac{[\alpha]}{\underline{a}}, \underline{p}_m\right) = \underline{0}$ gelijktijdig voor m=1,...,r vervuld is.
Daar de stelling voor r=1 bewezen is, kan, als we $\underline{a}$ door $\frac{\underline{a}\,\underline{p}_1\underline{p}_2\cdots\underline{p}_r}{\underline{p}_m}$ vervangen, α_m voor m=1,...,r zo gekozen worden dat $\left(\frac{\frac{[\alpha_m]}{\underline{a}\,\underline{p}_1\underline{p}_2\cdots\underline{p}_r}}{\underline{p}_m}, \underline{p}_m\right)=\underline{0}$ is. We stellen dan $\alpha = \alpha_1+\alpha_2+\ldots+\alpha_r$. Wegens $\underline{a}/\alpha_m$ is dan $\underline{a}/\alpha$; verder is $\underline{a}\,\underline{p}_m \nmid \alpha$, want $\alpha_1,\ldots,\alpha_r$ behalve α_m zijn door $\underline{a}\,\underline{p}_m$ deelbaar, en α_m is het niet. Dus is $\left(\frac{[\alpha]}{\underline{a}}, \underline{p}_m\right) = \underline{0}$.

Stelling. Elk ideaal $\underline{a}$ laat zich in de vorm $[\alpha,\beta]$ schrijven. Bovendien kan β hierin een willekeurig van 0 verschillend getal van $\underline{a}$ zijn (bijv.Na).
Bewijs. β willekeurig $\neq 0$ in $\underline{a}$. Neem voor $\underline{b} = \frac{[\beta]}{\underline{a}}$ en pas de hulpstelling toe. Men kan dus een α vinden met $\left(\frac{[\alpha]}{\underline{a}}, \frac{[\beta]}{\underline{a}}\right) = \underline{0}$, dus $\underline{a} = ([\alpha],[\beta]) = [\alpha,\beta]$.

Opmerking. Deze stelling wil zeggen dat men elk ideaal $\underline{a}=[\alpha_1,\alpha_2,\ldots,\alpha_s]$ kan terugbrengen tot $[\alpha,\beta]$, zodat alle getallen $\eta_1\alpha_1+\ldots+\eta_s\alpha_s$ dezelfde zijn als $\eta\alpha+\xi\beta$ ($\eta_1,\ldots,\eta_s,\eta,\xi$ geheel algebraische getallen van het lichaam). Dit wil echter niets zeggen over het terugbrengen van een basis van $\underline{a}$. Deze laatste bestaat steeds uit n elementen (n= graad lichaam) $\alpha_1,\ldots,\alpha_n$, zodat elk getal van $\underline{a}$ te schrijven is als $c_1\alpha_1+\ldots+c_n\alpha_n$ met $c_1,\ldots,c_n$ geheel rationaal. Zo kan men in P(i) het ideaal $[13,5+i]$ ook schrijven als $[2+3i]$. Nu is 13,5+i een basis van het ideaal, zodat elk getal ervan te schrijven is als $c_1 13+c_2(5+i)$ met c_1 en c_2 geheel rationaal; ook te schrijven als $(2+3i)\eta$, maar nu is η een geheel getal van P(i), dus van de gedaante a+bi. De basis blijft hier steeds uit 2 elementen bestaan.

Ideaalklassen.

Gegeven is een vast algebraisch lichaam. Wij zullen op een bepaalde manier alle idealen van het lichaam in klassen indelen; en dan de eindigheid van het aantal klassen bewijzen.

Definitie. Een ideaal heet equivalent met een ideaal $\underline{b}$, als er twee hoofdidealen $[\alpha]$, $[\beta]$ bestaan, zo dat

$$[\alpha]\,\underline{a} = [\beta]\,\underline{b}.$$

Notatie. $\underline{a} \sim \underline{b}$.

Stelling. De drie bekende postulaten.

Bewijs. a) Symmetrie: $[1]\ \underline{a} = [1]\ \underline{a}$, dus: $\underline{a} \sim \underline{a}$.

b) Reflexiviteit: Uit $\underline{a} \sim \underline{b}$ volgt $[\beta]\ \underline{b} = [\alpha]\ \underline{a}$, dus: $\underline{b} \sim \underline{a}$.

c) Transitiviteit: Uit $\underline{a} \sim \underline{b}$, $\underline{b} \sim \underline{c}$ volgt:

$$[\alpha]\underline{a} = [\beta]\ \underline{b},\ [\gamma]\ \underline{b} = [\delta]\ \underline{c},\ [\alpha\gamma]\ \underline{a} = [\beta\gamma]\ \underline{b} = [\beta\delta]\ \underline{c},$$

dus: $\underline{a} \sim \underline{c}$.

Alle idealen vallen dus uiteen in klassen van equivalente idealen.

Stelling. Een der klassen wordt door alle hoofdidealen gevormd.

Opmerking. Als, zoals bij P, elk ideaal hoofdideaal is, is er dus slechts één klasse.

Bewijs. 1) Zijn $[\alpha]$ en $[\beta]$ twee willekeurige hoofdidealen, dan is $[\beta][\alpha] = [\alpha][\beta]$, dus $[\alpha] \sim [\beta]$.

Elke twee hoofdidealen zijn dus equivalent.

2) Is $[\alpha] \sim \underline{a}$, dan is bij passende γ, δ:

$$[\gamma][\alpha] = [\delta]\ \underline{a}, \text{ dus } [\delta] / [\gamma\alpha] \text{ of } \delta / \gamma\alpha, \quad \text{, dus}$$

$\gamma\alpha = \delta\beta$ met gehele $\beta \neq 0$, dus $[\delta]\ \underline{a} = [\gamma\alpha] = [\delta\beta] = [\delta][\beta]$

of: $\underline{a} = [\beta]$.

Elk ideaal, dat equivalent is met een hoofdideaal, is dus ook hoofdideaal.

Stelling. Uit $\underline{a} \sim \underline{b}$, $\underline{c} \sim \underline{d}$ volgt $\underline{a}\ \underline{c} \sim \underline{b}\ \underline{d}$.

Bewijs. $[\alpha]\ \underline{a} = [\beta]\ \underline{b}$, $[\gamma]\ \underline{c} = [\delta]\ \underline{d}$, dus

$$[\alpha\gamma]\ \underline{a}\ \underline{c} = [\beta\delta]\ \underline{b}\ \underline{d}.$$

Stelling. Uit $\underline{a}\ \underline{c} \sim \underline{b}\ \underline{c}$ volgt $\underline{a} \sim \underline{b}$.

Bewijs. $[\alpha]\ \underline{a}\ \underline{c} = [\beta]\ \underline{b}\ \underline{c}$, dus $[\alpha]\ \underline{a} = [\beta]\ \underline{b}$.

Stelling. Er bestaat een alleen van het lichaam afhankelijk positief getal M, zo dat er in elk ideaal $\underline{a}$ een getal $\alpha \neq 0$ bestaat met

$$|N\alpha| \leq M.N\underline{a}.$$

Bewijs. Zij $\omega_n\ (1 \leq m \leq n)$ een lichaamsbasis, $\omega_m = r_m(\vartheta)$ de kanonnieke schrijfwijze, $r_m(\vartheta_s) = \omega_m^{(s)}\ (s=1,\ldots,n)$

$$M = \prod_{s=1}^{n} (|\omega_1^{(s)}| + \ldots + |\omega_n^{(s)}|).$$

beweren dat M de verlangde eigenschap heeft. Zij $\underline{a}$ het gegeven ideaal.

We kiezen het natuurlijke getal k zo dat $k \leqslant \sqrt[n]{N\underline{a}} < k+1$. Dan is $k^n \leqslant N\underline{a} < (k+1)^n$. Onder de $(k+1)^n$ verschillende getallen $x_1\omega_1+\ldots+x_n\omega_n$, met $x_m=0,1,2,\ldots,k$, komen dus twee mod $\underline{a}$ congruente voor:

$$y_1\omega_1+\ldots+y_n\omega_n \equiv z_1\omega_1+\ldots+z_n\omega_n \pmod{\underline{a}},$$

waarbij dus $0 \leqslant y_m \leqslant k$, $0 \leqslant z_m \leqslant k$, maar niet alle y_m-z_m gelijk aan 0 zijn. We stellen nu $\alpha=(y_1-z_1)\omega_1+\ldots+(y_n-z_n)\omega_n$, dan is α een getal van $\underline{a}$ en $\neq 0$. Verder is:

$$|N\alpha| = \left|\prod_{s=1}^{n}\sum_{m=1}^{n}(y_m-z_m)\omega_m^{(s)}\right| \leqslant \prod_{s=1}^{n}\sum_{m=1}^{n} k|\omega_n^{(s)}| \leqslant M.N\underline{a}.$$

Gevolg. Stelt men $[\alpha] = \underline{a}\,\underline{b}$ dan geldt: Door elk ideaal $\underline{a}$ is een zeker hoofdideaal $\underline{a}\,\underline{b}$ deelbaar waarbij $N(\underline{a}\,\underline{b}) = N[\alpha] = |N\alpha| \leqslant MN\underline{a}$, dus

$$N\underline{b} \leqslant M.$$

Stelling. Het aantal der ideaalklassen van het lichaam is eindig (dus een positief, alleen van het lichaam afhangend getal).

Bewijs. Wij behoeven slechts aan te tonen dat er in elke klasse minstens een ideaal $\underline{b}$ bestaat met $N\underline{b} \leqslant M$, want volgens een vroegere stelling zijn er slechts eindig veel idealen die hieraan voldoen.
Zij een ideaalklasse gegeven, $\underline{c}$ een willekeurig ideaal ervan en $\underline{a}$ zo gekozen dat $\underline{c}\,\underline{a} \sim \underline{0}$. We passen nu de vorige stelling toe op $\underline{a}$. Dan bestaat er dus een $\underline{b}$ met $\underline{a}\,\underline{b} \sim \underline{0}$ en $N\underline{b} \leqslant M$. Uit $\underline{c}\,\underline{a} \sim \underline{a}\,\underline{b}$ volgt $\underline{b} \sim \underline{c}$. In de gegeven klasse hebben we dus een $\underline{b}$ gevonden met $N\underline{b} \leqslant M$.

Stelling. Is h het aantal klassen, dan geldt voor ieder ideaal $\underline{a}$: $\underline{a}^h \sim \underline{0}$.

Opmerking. De h'de macht van elk ideaal is een hoofdideaal (h onafhankelijk van $\underline{a}$).

Bewijs (zie bewijs kleine stelling van Fermat): zijn $\underline{a}_1,\ldots,\underline{a}_h$ representanten van de h ideaalklassen, dan zijn $\underline{a}\,\underline{a}_1,\ldots,\underline{a}\,\underline{a}_h$ het ook, daar hun aantal klopt en geen twee van deze idealen equivalent zijn. Dus is ook:

$$\underline{a}\,\underline{a}_1 \cdot \underline{a}\,\underline{a}_2 \cdots \underline{a}\,\underline{a}_h \sim \underline{a}_1\,\underline{a}_2 \cdots \underline{a}_h \text{ of}$$

$$\underline{a}^h(\underline{a}_1\,\underline{a}_2\,\underline{a}_h) \sim \underline{0}(\underline{a}_1\,\underline{a}_2 \cdots \underline{a}_h)$$

$$\underline{a}^h \sim \underline{0}.$$