De kleinste algoritme van enkele euclidische ringen.

H.W. Lenstra, jr.

§1. Inleiding.

Referentie:

[S] P. Samuel, About Euclidean Rings, Journal of Algebra 19 (1971) 282-301.

Notaties. A is een integriteitsgebied, d.w.z. een commutatieve ring met $1 \neq 0$ zonder nuldelers. A^* is de groep eenheden van A. Met $\mathbb{N}$ wordt de verzameling niet-negatieve gehele getallen bedoeld. $\square$ betekent "einde bewijs" of "na het voorgaande biedt het bewijs geen problemen meer".

Euclidische ringen. Zij W een welgeordende verzameling en $\varphi : A \to W$ een afbeelding. Stel dat geldt:

$$\forall\, a, b \in A : \; b \neq 0 \Rightarrow [\, \exists\, q, r \in A : \; \varphi(r) < \varphi(b) \;\wedge\; a = qb + r \,].$$

Dan zeggen we dat φ een algoritme voor A is. A heet euclidisch als er een welgeordende verzameling W en een algoritme $\varphi : A \to W$ bestaan. Wij zullen hier alleen algoritmen met $W = \mathbb{N}$ beschouwen. Het is een onopgelost probleem of er voor elke euclidische A een algoritme $\varphi : A \to \mathbb{N}$ is.

De kleinste algoritme. Stel er bestaat een algoritme $\varphi : A \to \mathbb{N}$. Definieer dan $\vartheta : A \to \mathbb{N}$ door

$$\vartheta(a) = \min_{\varphi} \varphi(a) \qquad (a \in A)$$

waar het minimum genomen wordt over alle algoritmen $\varphi : A \to \mathbb{N}$. Men gaat gemakkelijk na dat ϑ een algoritme voor A is. Wegens de eigenschap

$$\vartheta(a) \leqslant \varphi(a)$$

voor alle $a \in A$ en elke algoritme $\varphi : A \to \mathbb{N}$ wordt ϑ de kleinste algoritme van A genoemd. Voor $n \in \mathbb{N}$ noteren we

$$A_n = \{a \in A \mid \vartheta(a) \leq n\}.$$

Uit [S] volgt:

(1.1). $A_0 = \{0\}$,

$A_{n+1} = \{a \in A \mid$ de natuurlijke afbeelding $A_n \to A/Aa$ is surjectief$\} \cup \{0\}$ $(n \in \mathbb{N})$.

In het bijzonder $A_1 = A^* \cup \{0\}$. □

(1.2). Laat $a, b \in A$, $ab \neq 0$. Dan $\vartheta(ab) \geq \vartheta(a)$, en $\vartheta(ab) = \vartheta(a)$ impliceert $b \in A^*$. □

Een observatie. Zij $A_1 = A^* \cup \{0\}$, en $x \in A$. De deelverzameling $\{\sum_{i=0}^{n-1} u_i x^i \mid n \in \mathbb{N},\ u_i \in A_1\ (0 \leq i < n)\}$ van A wordt aangegeven met $A_1[x]$. Definieer $\psi_x : A_1[x] \to \mathbb{N}$ door

$$\psi_x(a) = \min\{n \in \mathbb{N} \mid \exists\, u_i \in A_1\ (0 \leq i < n) \text{ met } a = \textstyle\sum_{i=0}^{n-1} u_i x^i\}.$$

Kennelijk geldt $\psi_x(a) = 0 \iff a = 0$, en $\psi_x(a) = 1 \iff a \in A^*$.

(1.3). Laat A euclidisch zijn met kleinste algoritme $\vartheta : A \to \mathbb{N}$. Zij $x \in A$, $x \notin A_1$. Dan zijn equivalent:

(i) $A = A_1[x]$ en ψ_x is een algoritme voor A.

(ii) $\psi_x(a) \geq \vartheta(a)$ voor elke $a \in A_1[x]$.

(iii) $A = A_1[x]$ en $\psi_x = \vartheta$.

Lemma (1.4). Zij $x \in A$, $x \notin A_1$, $a \in A_1[x]$, $a \neq 0$. Dan geldt

$$\psi_x(xa) = \psi_x(a) + 1.$$

Voor $n \in \mathbb{N}$ geldt $\psi_x(x^n) = n + 1$.

Bewijs van (1.4). De ongelijkheid $\psi_x(xa) \leq \psi_x(a) + 1$ is evident. Zij verder $xa = \sum_{i=0}^{n-1} u_i x^i$ met $n = \psi_x(xa)$, $u_i \in A_1$ $(0 \leq i < n)$. Uit $u_0 = x \cdot (a - \sum_{i=1}^{n-1} u_i x^{i-1})$ en $x \notin A^*$ volgt $u_0 = 0$. Delen door x geeft $a = \sum_{i=0}^{n-2} u_{i+1} x^i$, dus $\psi_x(a) \leq n - 1 = \psi_x(xa) - 1$. Dit bewijst de eerste bewering. De tweede bewering volgt uit de eerste met inductie naar n. □

Bewijs van (1.3). (i) $\Rightarrow$ (ii) en (iii) $\Rightarrow$ (i) zijn duidelijk. We bewijzen

(ii) $\Rightarrow$ (iii). Neem (ii) aan. We bewijzen met inductie naar $\vartheta(a)$:

$$a \in A_1[x] \quad \text{en} \quad \psi_x(a) = \vartheta(a)$$

voor $a \in A$. Als $\vartheta(a) = 0$ dan $a = 0$, en $0 \in A_1[x]$, $\psi_x(0) = 0$ is duidelijk. Zij dan $\vartheta(a) = n+1$, met $n \in \mathbb{N}$. Omdat ϑ een algoritme is, zijn er $q, r \in A$ met

$$x^n = q \cdot a + r, \qquad \vartheta(r) < \vartheta(a) = n+1.$$

Uit de inductiehypothese volgt $r \in A_1[x]$ en $\psi_x(r) = \vartheta(r) \leqslant n$. We kunnen dus schrijven $r = \sum_{i=0}^{n-1} t_i x^i$ met $t_i \in A_1$ $(0 \leqslant i < n)$. Uit $\psi_x(x^n) = n+1$ (lemma (1.4)) volgt

$$x^n \neq \sum_{i=0}^{n-1} t_i x^i$$

dus

$$q \cdot a = x^n - \sum_{i=0}^{n-1} t_i x^i \neq 0.$$

Met behulp van (iii) vinden we

$$\vartheta(q \cdot a) = \vartheta\left(x^n - \textstyle\sum_{i=0}^{n-1} t_i x^i\right) \leqslant \psi_x\left(x^n - \textstyle\sum_{i=0}^{n-1} t_i x^i\right) \leqslant n+1 = \vartheta(a),$$

dus uit (1.2) volgt $q \in A^*$. Wegens

$$a = q^{-1} x^n - \sum_{i=0}^{n-1} q^{-1} t_i x^i$$

concluderen we $a \in A_1[x]$ en $\psi_x(a) \leqslant n+1$. Daar (ii) impliceert $\psi_x(a) \geqslant \vartheta(a) = n+1$, volgt $\psi_x(a) = \vartheta(a)$. $\square$

De voorwaarde $x \notin A_1$ kan niet gemist worden: ψ_1 is een algoritme voor $\mathbb{Z}$, maar niet de kleinste, zie (1.6).

Voorbeelden waar ψ_x een algoritme is.

(1.5). Zij k een lichaam, $A = k[X]$ de polynoomring in één onbepaalde X over k, en $x = X$. Dan $A_1 = k$, en voor $a \in A$ geldt

$$\psi_X(a) = 1 + \text{graad}(a) \qquad (a \neq 0)$$
$$\psi_X(0) = 0.$$

Dit is kennelijk een algoritme. In overeenstemming met [S] concluderen we dat ψ_X de kleinste algoritme van $k[X]$ is.

(1.6). $A = \mathbb{Z}$, $x = 2$. Voor $a \in \mathbb{Z}$ en $n \in \mathbb{N}$ geldt

$$\psi_2(a) \leqslant n \iff |a| < 2^n.$$

Gemakkelijk ziet men dat ψ_2 een algoritme, dus de kleinste algoritme is, opnieuw in overeenstemming met [S]. Voor $n \in \mathbb{N}$ geldt

$$|A_n| = 2 \cdot 2^n - 1.$$

Hoewel $A_1[3] = A$ voor $A = \mathbb{Z}$, is ψ_3 geen algoritme.

(1.7). $A = \mathbb{Z}[\sqrt{-1}]$, $x = 1 + \sqrt{-1}$. Dan is ψ_x de kleinste algoritme van A. Dit wordt bewezen in §2. Men kan aantonen:

$$|A_n| = 14 \cdot 2^n - 34 \cdot 2^m + 4 \cdot n + 21 \quad \text{voor } n = 2m,\ m \in \mathbb{N},$$

$$|A_n| = 14 \cdot 2^n - 48 \cdot 2^m + 4 \cdot n + 21 \quad \text{voor } n = 2m+1,\ m \in \mathbb{N}.$$

(1.8). $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $x = \frac{1}{2}(3+\sqrt{-3})$. Dan is ψ_x de kleinste algoritme van A, en

$$57 \cdot |A_n| = 333 \cdot 3^n - q_n + 114 \cdot n + 266 \quad \text{voor } n \in \mathbb{N},$$

met $q_0 = 542$, $q_1 = 980$, $q_2 = 1724$, $q_{n+3} = 2 \cdot q_{n+1} + 2 \cdot q_n$ $(n \in \mathbb{N})$.

Het bewijs van (1.8) wordt hier niet volledig gegeven.

(1.9). Zij A een discrete valuatiering met valuatie $v : A - \{0\} \to \mathbb{N}$, en $x \in A$ een priemelement, d.w.z. een element met $v(x) = 1$. Dan $A_1[x] = A$, en

$$\psi_x(a) = 1 + v(a)$$

voor $a \in A$, $a \neq 0$. Dit is de kleinste algoritme van A, zoals men gemakkelijk nagaat, in overeenstemming met [S]. □

(1.10). Zij B een euclidisch integriteitsgebied met kleinste algoritme ψ_y, voor een $y \in B$, $y \notin B_1$. Zij $A = B[[X]][X^{-1}]$ de ring van formele Laurentreeksen met coefficienten uit B, vgl. [S]. Zij $x \in A$ een element van de vorm

$$x = \sum_{n \in \mathbb{Z},\ n \geq r} b_n X^n \quad \text{met } r \in \mathbb{Z},\ b_n \in B\ (n \in \mathbb{Z},\ n \geq r),\ b_r = y.$$

Dan is A euclidisch met kleinste algoritme ψ_x. Dit bewijst men door voorwaarde (ii) van (1.3) te controleren. □

Eenduidigheid van de gegeven voorbeelden.

A heet van eindig type over een deelring R, als er een eindige verzameling $Y \subset A$ is zodanig dat de deelring van A voortgebracht door R en Y gelijk is aan A. Is R een lichaam, dan heet R algebraisch afgesloten binnen A als elk element van A dat algebraisch is over R, in R bevat is.

(1.11). Zij k een lichaam en A een integriteitsgebied dat k bevat, zodanig dat (i) A van eindig type over k is, en (ii) k algebraisch afgesloten binnen A is. Stel A is euclidisch met kleinste algoritme ψ_x, met $x \in A$, $x \notin A_1$. Dan $A = k[x]$ en x is transcendent over k. Het bewijs hiervan vindt men in § 3.

(1.12). Zij A een integriteitsgebied dat $\mathbb{Z}$ bevat zodanig dat A van eindig type over $\mathbb{Z}$ is. Stel A is euclidisch met kleinste algoritme ψ_x voor zekere $x \in A$, $x \notin A_1$. Dan $A = \mathbb{Z}$, $x = \pm 2$, of $A = \mathbb{Z}[\sqrt{-1}]$, $x \in A^* \cdot (1+\sqrt{-1})$, of $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $x \in A^* \cdot \frac{1}{2}(3+\sqrt{-3})$. Dit wordt bewezen in § 3.

(1.13). Zij A een integriteitsgebied met slechts eindig veel maximale idealen. Neem aan dat A euclidisch is met kleinste algoritme ψ_x, voor zekere $x \in A$, $x \notin A_1$. Dan is A een discrete valuatiering en x is een priemelement van A. Het bewijs wordt gegeven in § 3.

§2. Een criterium opdat ψ_x een algoritme zij.

Zij A een integriteitsgebied en $x \in A$, $x \notin A_1$. Laten $A_1[x]$ en ψ_x zijn als in § 1. Zij $B = A[x^{-1}]$ de ring voortgebracht door A en x^{-1} binnen het quotiëntenlichaam van A. Voor $W \subset B$ definiëren we

$$F(W) = \{ x^{-1} \cdot (u + w) \mid u \in A_1, \ w \in W \}.$$

Met inductie naar n controleert men gemakkelijk

$$F^n(\{0\}) = \{ \textstyle\sum_{i=1}^{n} u_i x^{-i} \mid u_i \in A_1 \ (1 \leq i \leq n) \} \qquad (n \in \mathbb{N}).$$

Hieruit volgt

$$A \cap x^n \cdot F^n(\{0\}) = \{ a \in A_1[x] \mid \psi_x(a) \leq n \}$$

en uit $x \notin A_1$ volgt dat voor $n < m$ geldt

$$A \cap x^n \cdot F^m(\{0\}) = A \cap x^n \cdot F^n(\{0\}).$$

Definieert men

$$V_x = \bigcup_{m \in \mathbb{N}} F^m(\{0\}) \subset B$$

dan concluderen we:

(2.1). Voor $n \in \mathbb{N}$ geldt:

$$A \cap x^n \cdot V_x = \{ a \in A_1[x] \mid \psi_x(a) \leq n \}. \qquad \square$$

(2.2). Equivalent zijn:

(i) $A = A_1[x]$ en ψ_x is een algoritme voor A.

(ii) A bezit een algoritme $\varphi: A \to \mathbb{N}$, en voor elke $v \in V_x$, $v \neq 0$, is de natuurlijke afbeelding $V_x \to B/Avx$ surjectief.

Hier is Avx de additieve ondergroep $\{avx \mid a \in A\}$ van B, en de pijl $V_x \to B/Avx$ is de samenstelling van de inclusie $V_x \subset B$ en de natuurlijke afbeelding $B \to B/Avx$.

Bewijs.

(ii) $\Rightarrow$ (i). Zij $C_n = \{a \in A_1[x] \mid \psi_x(a) \leqslant n\} = A \cap x^n V_x$ voor $n \in \mathbb{N}$. We bewijzen eerst:

(2.3) $C_n \to A/Ab$ is surjectief voor $b \in C_{n+1}$, $b \neq 0$.

Zij namelijk $b \in C_{n+1}$, $b \neq 0$, en $a \in A$. We zoeken een $r \in C_n$ met $a \equiv r \bmod Ab$. Uit (ii), met $v = x^{-n-1}b$, volgt dat $V_x \longrightarrow B/Ax^{-n}b$ surjectief is. Er is dus een $w \in V_x$ met $x^{-n}a \equiv w \bmod Ax^{-n}b$. Voor $r = x^n.w$ geldt dan $a \equiv r \bmod Ab$, dus $r \in A$, en bovendien $r \in x^n V_x$, dus $r \in A \cap x^n V_x = C_n$. Dit bewijst (2.3).

Laten ϑ, A_n $(n \in \mathbb{N})$ nu zijn als in §1. Uit (1.1) en (2.3) volgt gemakkelijk met inductie naar n:

$$C_n \subset A_n \qquad (n \in \mathbb{N})$$

oftewel

$$\vartheta(a) \leqslant \psi_x(a) \quad \text{voor alle } a \in A_1[x].$$

Nu volgt (i) direkt uit (1.3).

(i) $\Rightarrow$ (ii). Zij $v \in V_x$, $v \neq 0$ en $a \in B$. We moeten een $w \in V_x$ vinden met $a \equiv w \bmod Avx$. Uit $a \in B$, $v \in B$ volgt dat er een $n \in \mathbb{N}$ is met $x^n a \in A$, $x^{n+1} v \in A$. Zij $m = \psi_x(x^{n+1}.v)$. Uit (2.1) volgt $m \leqslant n+1$. Wegens (i) is er een $r \in A$ met $x^n.a \equiv r \bmod Ax^{n+1}v$, $\psi_x(r) \leqslant n$. Voor $w = x^{-n}r$ geldt dan $a \equiv w \bmod Axv$ en $w \in V_x$. □

Met (2.2) is de vraag of ψ_x een algoritme is vertaald in een vraag over de verzameling V_x. Ons volgende resultaat betreft de bepaling van V_x.

(2.4) Zij $S = (B \setminus A) \cup \{0\}$, en zij T een deelverzameling van B. Dan geldt:

a) $V_x = \bigcup_{m \in \mathbb{N}} F^m(\{0\}) = \bigcap_{m \in \mathbb{N}} F^m(S)$.

b) als T voldoet aan $T \subset S$ en $T \subset F(T)$, dan $T \subset V_x$.

c) als T voldoet aan $0 \in T$ en $F(T) \subset T$, dan $V_x \subset T$.

d) als $0 \in T \subset S$, dan geldt:

$$T = V_x \iff F(T) = T.$$

Bewijs. Voor $W \subset B$ definiëren we

$$G(W) = \{ u + x \cdot w \mid u \in A_1, w \in W \}.$$

Voor $W_1, W_2 \subset B$ geldt kennelijk:

$$F(W_1) \cap W_2 \neq \emptyset \iff W_1 \cap G(W_2) \neq \emptyset.$$

Met inductie naar n volgt:

(2.5) $$F^n(W_1) \cap W_2 \neq \emptyset \iff W_1 \cap G^n(W_2) \neq \emptyset \qquad (n \in \mathbb{N}).$$

We merken verder op:

(2.6) $$W_1 \subset W_2 \Rightarrow F(W_1) \subset F(W_2) \text{ en } G(W_1) \subset G(W_2).$$

Zij nu $n \in \mathbb{N}$. Voor $k \in \mathbb{N}$, $0 \leq k \leq n$, geldt

$$G^k(x^{-n}A) = x^{k-n}A,$$

zoals men gemakkelijk met inductie naar k bewijst. Met $k = n$ en (2.6) volgt:

(2.7) $$\forall a \in x^{-n}A: \quad G^n(\{a\}) \subset A.$$

Bewijs van (2.4) a). We moeten bewijzen

(2.8) $$\bigcup_{m \in \mathbb{N}} F^n(\{0\}) = \bigcap_{m \in \mathbb{N}} F^m(S).$$

Uit $\{0\} \subset F(\{0\})$, $\{0\} \subset S$, $F(S) \subset S$ en (2.6) volgt

$$F^n(\{0\}) \subset F^m(\{0\}) \subset F^m(S) \subset F^n(S)$$

voor $n, m \in \mathbb{N}$, $n \leq m$, waarmee de inclusie $\subset$ van (2.8) bewezen is. Omgekeerd, zij $a \in \bigcap_{m \in \mathbb{N}} F^m(S)$. Kies $n \in \mathbb{N}$ met $a \in x^{-n}A$. Dan $a \in F^n(S)$, dus $F^n(S) \cap \{a\} \neq \emptyset$, en (2.5) impliceert $S \cap G^n(\{a\}) \neq \emptyset$. Uit (2.7) volgt echter $S \cap G^n(\{a\}) \subset S \cap A = \{0\}$. We concluderen $S \cap G^n(\{a\}) = \{0\}$, dus $0 \in G^n(\{a\})$ en $\{0\} \cap G^n(\{a\}) \neq \emptyset$. Uit (2.5)

volgt $F^n(\{0\}) \cap \{a\} \neq \emptyset$, oftewel $a \in F^n(\{0\})$, dus zeker $a \in \bigcup_{m \in \mathbb{N}} F^m(\{0\})$. Dit bewijst inclusie $\supset$ van (2.8).

Bewijs van (2.4) b). Zij $T_0 = T \cup \{0\}$. Dan $T_0 \subset F(T_0)$ en $\{0\} \subset T_0 \subset S$. Met (2.6) volgt hieruit

$$V_x = \bigcup_{m \in \mathbb{N}} F^m(\{0\}) \subset \bigcup_{m \in \mathbb{N}} F^m(T_0) \subset \bigcap_{m \in \mathbb{N}} F^m(S) = V_x,$$

dus

$$V_x = \bigcup_{m \in \mathbb{N}} F^m(T_0)$$

en

$$T \subset T_0 \subset V_x.$$

Bewijs van (2.4) c). Zij $T_1 = T \cap S$. Dan $F(T_1) \subset F(T) \cap F(S) \subset T \cap S \subset$ $\subset T_1$, en $\{0\} \subset T_1 \subset S$. Met (2.6) volgt

$$V_x = \bigcup_{m \in \mathbb{N}} F^m(\{0\}) \subset \bigcap_{m \in \mathbb{N}} F^m(T_1) \subset \bigcap_{m \in \mathbb{N}} F^m(S) = V_x$$

dus

$$V_x = \bigcap_{m \in \mathbb{N}} F^m(T_1)$$

en

$$V_x \subset T_1 \subset T.$$

Bewijs van (2.4) a). $\Rightarrow$ is duidelijk uit de definitie van V_x. $\Leftarrow$ volgt direkt uit b) en c). $\square$

Voorbeeld 1.

$A = \mathbb{Z}$, $x = 2$. Zij

$$T = \{a \in B \mid |a| < \tfrac{1}{2}\},$$

waar $|\ |$ de gewone absolute waarde op $B = \mathbb{Z}[\frac{1}{2}] \subset \mathbb{R}$ is.

Eenvoudig controleert men

$$T = F(T), \quad 0 \in T \subset S$$

dus en volgt $T = V_x$. Omdat $(-v, v] \cap B \subset V_x$ voor $v \in V_x$, volgt dat

$$V_x \longrightarrow B/\mathbb{Z}2v$$

voor $v \in V_x$, $v \neq 0$, surjectief is. Uit (2.2) concluderen we dat ψ_2 een algoritme voor $\mathbb{Z}$ is, zoals we al wisten.

Voorbeeld 2.
$A = \mathbb{Z}[\sqrt{-1}]$, $x = 1+\sqrt{-1}$, $\bar{x} = 1-\sqrt{-1}$. We berekenen $B = A[x^{-1}]$ op de gebruikelijke wijze als deel van het complexe vlak. Voor $a_1, \dots, a_n \in B$ zij $C(a_1, \dots, a_n)$ het convex omhulsel van $\{a_1, \dots, a_n\}$; zijn $a_1, a_2, \dots, a_n, a_1$ de hoekpunten van een n-hoek (in die volgorde), dan wordt het inwendige van die n-hoek aangegeven met $I(a_1, \dots, a_n)$.
Voor V_x geldt in dit geval

$$V_x = I(2+\sqrt{-1}, 1+2\sqrt{-1}, -1+2\sqrt{-1}, -2+\sqrt{-1}, -2-\sqrt{-1}, -1-2\sqrt{-1}, 1-2\sqrt{-1}, 2-\sqrt{-1}) \setminus D$$

waar D een zekere zich naar de rand van de achthoek verdichtende deelverzameling van B is, zie figuur 1. Dit controleert men gemakkelijk aan de hand van (2.4) d). We schrijven verder V in plaats van V_x.
We tonen aan dat voor $v \in V$ geldt (vergelijk figuur 3):

(2.9) $$C(0, xv, \bar{x}v, 2v) \subset V \cup (xv+V) \cup (\bar{x}v+V) \cup (2v+V).$$

Dit is een scherpere uitspraak dan de bewering onder (2.2)(i) j), dus uit (2.9) volgt dat ψ_x een algoritme voor A is.

Bewijs van (2.9). Eerst merken we op:

(2.10) voor $v \in V$, $v \in C(x, \bar{x}, -x, -\bar{x})$ is (2.9) waar.

Dit volgt eenvoudig uit $C(v, -v, \sqrt{-1}v, -\sqrt{-1}v) \subset V$, zie figuur 2.
Het algemene geval wordt nu behandeld met inductie naar

$$n(v) = \min\{n \in \mathbb{N} \mid x^n v \in A\}.$$

Begin van de inductie: het geval $n(v) \leq 1$ valt onder (2.10).
Inductiestap. Wegens (2.10) en symmetrieredenen mag men aannemen

$$v \in C(\sqrt{-1}, 1+\sqrt{-1}, 1\tfrac{1}{2} + 1\tfrac{1}{2}\sqrt{-1}, 1+2\sqrt{-1}, 2\sqrt{-1}),$$

zie figuur 2.
Dan kan men schrijven (vgl. figuur 1)

$$v = \tfrac{1}{2}x(1+w) \qquad \text{met } w \in V, \quad n(w) = n(v) - 1.$$

Toepassing van de inductiehypothese op w levert

$$C(0, xw, \bar{x}w, 2w) \subset V \cup (xw+V) \cup (\bar{x}w+V) \cup (2w+V).$$

Na de transformatie $z \mapsto \frac{1}{2}x(1+z)$ $(z \in B)$ wil dit zeggen dat het vierhoek waarvan in fig. 3 drie zijden gestippeld getekend zijn:

$$C\left(\tfrac{1}{2}x, \tfrac{1}{2}x(1+xw), \tfrac{1}{2}x(1+\bar{x}w), \tfrac{1}{2}x(1+2w)\right)$$
$$= C\left(\tfrac{1}{2}x, xv + \tfrac{1}{2}\bar{x}, \bar{x}v - \tfrac{1}{2}\bar{x}, 2v - \tfrac{1}{2}x\right)$$

bevat is in de verzameling

$\frac{1}{2}\pi(1+V) \cup (\pi v + \frac{1}{2}\pi(-\sqrt{-1}+V)) \cup (\bar{\pi} v + \frac{1}{2}\pi(\sqrt{-1}+V)) \cup (2v + \frac{1}{2}\pi(-1+V))$

welke op zijn beurt wegens $F(V) = V$ bevat is in

$$V \cup (\pi v + V) \cup (\bar{\pi} v + V) \cup (2v + V).$$

Om de inductiestap te voltooien, is het wegens symmetrieredenen nu voldoende te bewijzen:

(2.11) $\quad I(0, \bar{\pi} v, \bar{\pi} v - \frac{1}{2}\bar{\pi}, \frac{1}{2}\pi) \cup C(0, \bar{\pi} v) \subset V \cup (\bar{\pi} v + V)$,

vgl. figuur 3.

Stel dat (2.11) onwaar is. Dan is er een $a \in B$, gelegen in het linkerlid van (2.11), waarvoor geldt $a \notin V$ en $a - \bar{\pi} v \notin V$. Met $b = \bar{\pi} v - a$ vinden we:

(2.12) er zijn $a, b \in I(0, \frac{1}{2}\bar{\pi}, \bar{\pi} v - \frac{1}{2}\pi, \bar{\pi} v, \bar{\pi} v - \frac{1}{2}\bar{\pi}, \frac{1}{2}\pi)$ met

$$a, b \notin V, \quad a + b = \bar{\pi} v = 1 + w.$$

Uit (2.12) gaan we een tegenspraak afleiden.

Stel eerst dat geldt $v \in C(\frac{1}{2} + \sqrt{-1}, 1 + \sqrt{-1}, 1\frac{1}{2} + 1\frac{1}{2}\sqrt{-1}, 1 + 2\sqrt{-1}, \frac{1}{2} + 2\sqrt{-1})$, zie figuur 4. Dan zijn a en b bevat in

$$I(0, \tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 2\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 3, 3 + \sqrt{-1}, 2 + 2\sqrt{-1}).$$

En geldt $\mathrm{Re}(a+b) = \mathrm{Re}(\bar{\pi} v) < 3$, $\mathrm{Re}(a) > 0$, $\mathrm{Re}(b) > 0$ (Re = reële deel), dus wegens symmetrie in a en b mogen we aannemen $\mathrm{Re}(a) < \frac{3}{2}$. Dan

$$a \in I(0, \tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 1\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 1\tfrac{1}{2} + 1\tfrac{1}{2}\sqrt{-1})$$

en uit $a \notin V$ volgt dan $a = 1$ (vgl. figuur 1) dus $b = w$, in tegenspraak met $b \notin V$.

Neem vervolgens aan $v \in C(\sqrt{-1}, \frac{1}{2} + \sqrt{-1}, \frac{1}{2} + 2\sqrt{-1}, 2\sqrt{-1})$, zie figuur 5. Dan

$$a, b \in I(0, \tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 2\tfrac{1}{2} + 1\tfrac{1}{2}\sqrt{-1}, 1\tfrac{1}{2} + 2\tfrac{1}{2}\sqrt{-1}, \tfrac{1}{2} + 1\tfrac{1}{2}\sqrt{-1}, \tfrac{1}{2} + \tfrac{1}{2}\sqrt{-1}).$$

Nu $\mathrm{Re}(\bar{\pi} a + \bar{\pi} b) < 4$, $\mathrm{Re}(\bar{\pi} a) > 0$, $\mathrm{Re}(\bar{\pi} b) > 0$, dus we mogen aannemen $\mathrm{Re}(\bar{\pi} a) < 2$. Dan

$$a \in I(0, \tfrac{1}{2} - \tfrac{1}{2}\sqrt{-1}, 1\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-1}, \tfrac{1}{2} + 1\tfrac{1}{2}\sqrt{-1}, \tfrac{1}{2} + \tfrac{1}{2}\sqrt{-1})$$

en ondat deze verzameling in V bevat is (vgl. figuur 1) is dit een tegenspraak met $a \notin V$. Dit voltooit de inductiestap. □

Voorbeeld 3.

$A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $\pi = \frac{1}{2}(3+\sqrt{-3})$. In dit geval ziet V_π en iets ingewikkelder uit, zie figuur 6. Men kan bewijzen dat aan (2.2)(i) voldaan is. En volgt dat ψ_π een algoritme voor A is.

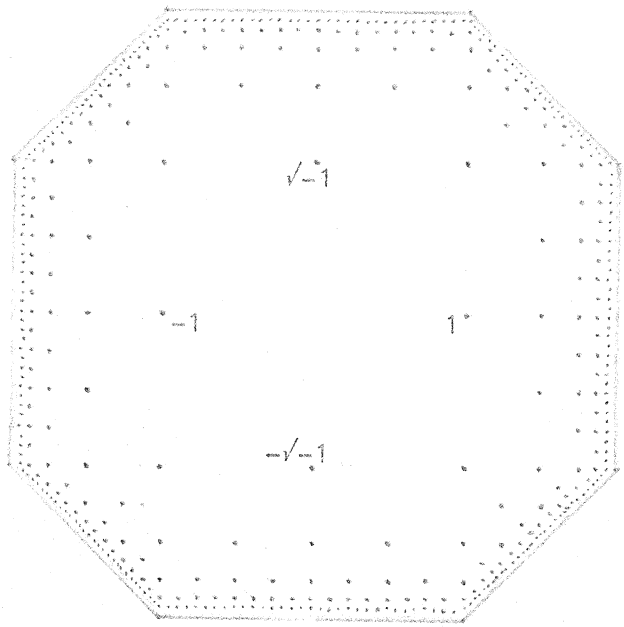

Fig. 1

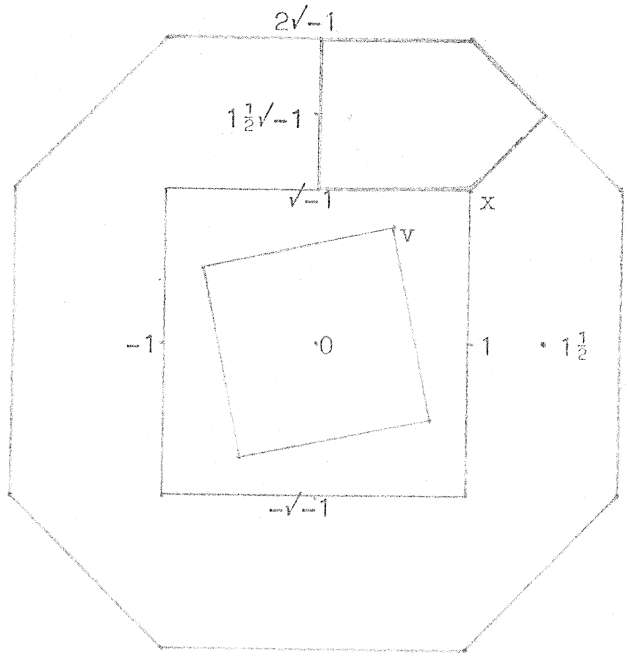

Fig. 2

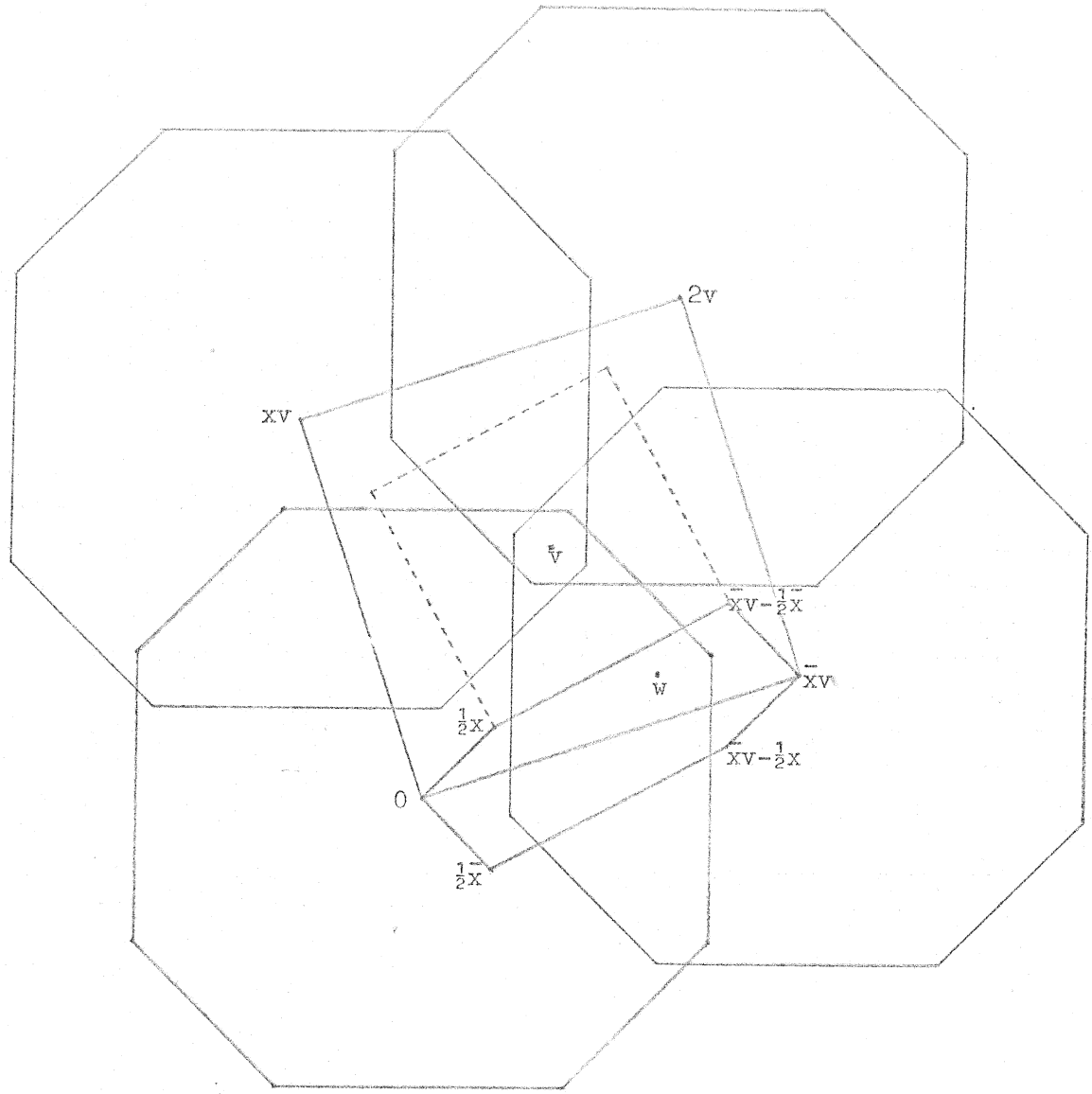
2v
xv
v
$\bar{x}v-\frac{1}{2}\bar{x}$
w
$\bar{x}v$
$\frac{1}{2}x$
$\bar{x}v-\frac{1}{2}x$
0
$\frac{1}{2}\bar{x}$

Fig. 3

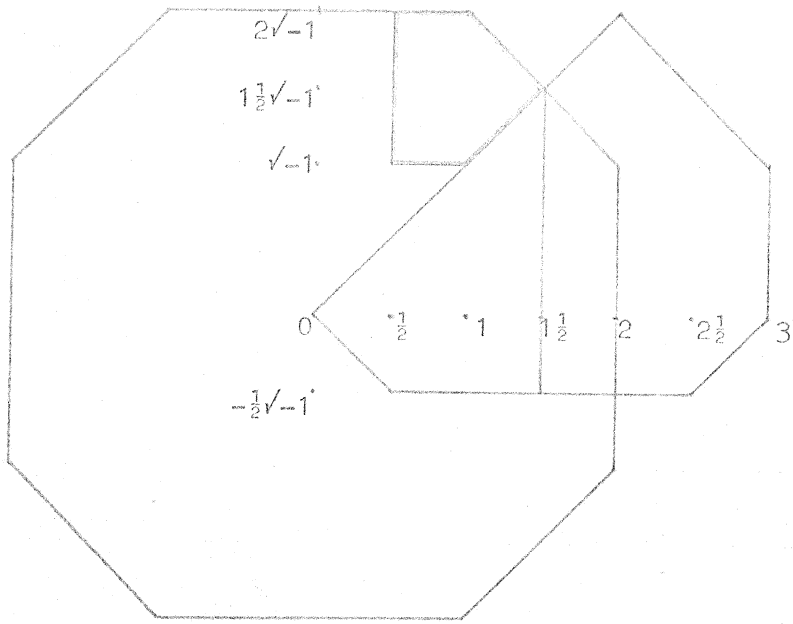
$2\sqrt{-1}$
$1\frac{1}{2}\sqrt{-1}$
$\sqrt{-1}$
0
$\frac{1}{2}$
1
$1\frac{1}{2}$
2
$2\frac{1}{2}$
3
$-\frac{1}{2}\sqrt{-1}$

Fig. 4

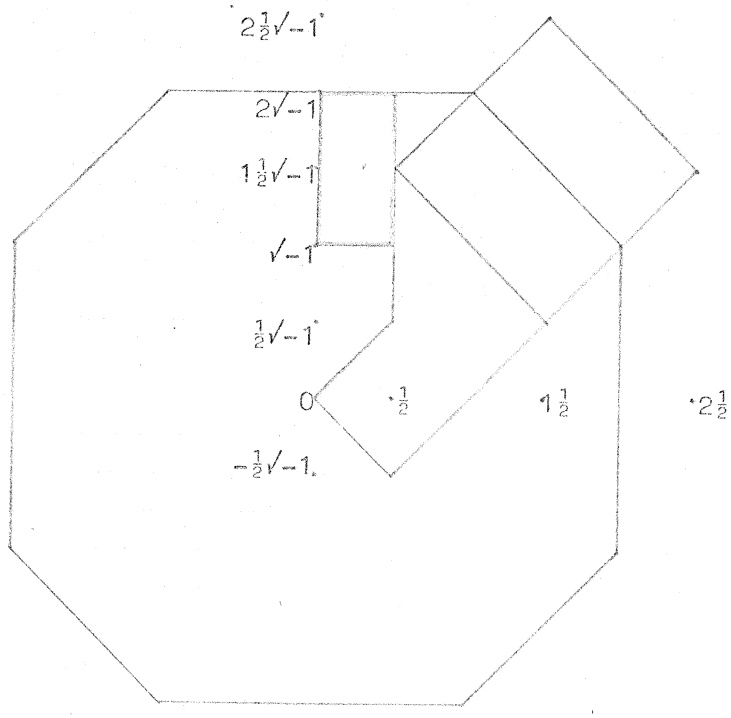
$2\frac{1}{2}\sqrt{-1}$
$2\sqrt{-1}$
$1\frac{1}{2}\sqrt{-1}$
$\sqrt{-1}$
$\frac{1}{2}\sqrt{-1}$
0
$\frac{1}{2}$
$1\frac{1}{2}$
$2\frac{1}{2}$
$-\frac{1}{2}\sqrt{-1}$

Fig. 5

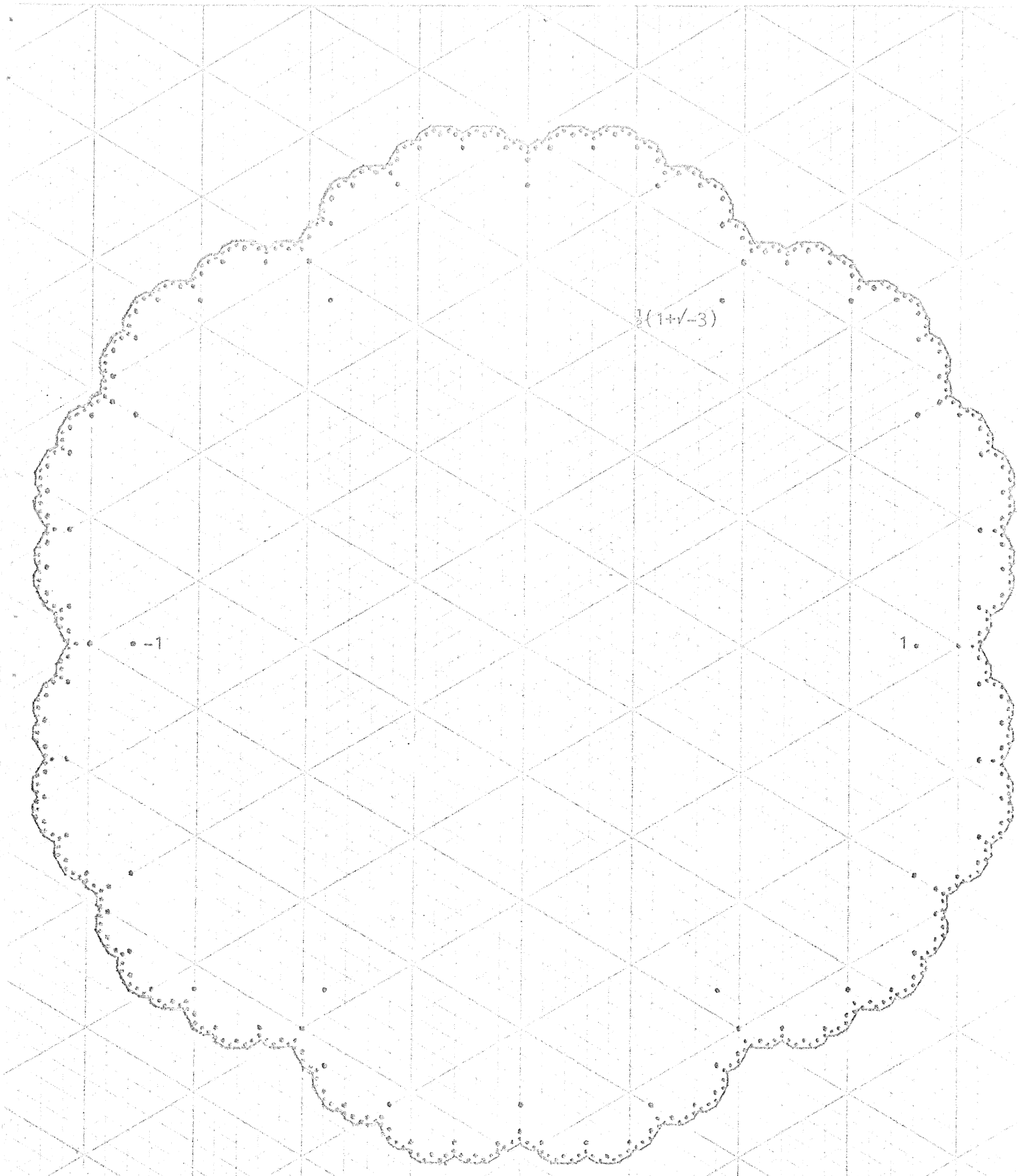

Fig. 6

§3. Eindigheidsbewijzen.

In deze paragraaf is A een euclidisch integriteitsgebied met kleinste algoritme $\delta = \psi_x$, $x \in A$, $x \notin A_1$. Volgens [5] is A een hoofdidealring, en omdat $x \notin A_1$, impliceert dat A geen lichaam is, is de Krulldimensie $\dim(A)$ van A gelijk aan 1.
Met behulp van (1.1) bewijst men eenvoudig:

Lemma (3.1). Voor $a \in A$ zijn equivalent:

(i) $\psi_x(a) = 2$

(ii) $a \neq 0$ is een priemelement, en de natuurlijke afbeelding

$$A^* \to (A/Aa)^*$$

is surjectief. □

In het bijzonder volgt dat x een priemelement is.

Lemma (3.2). Stel $y \in A$ is een priemelement $\neq 0$ waarvoor de natuurlijke afbeelding

$$A^* \to (A/Ay^2)^*$$

surjectief is. Dan geldt $y \in A^*.x$.

Bewijs. Stel $y \notin A^*.x$. Dan zijn x en y relatief priem, dus $(x \bmod Ay^2) \in (A/Ay^2)^*$. Er is dus een $u \in A^*$ met $x \equiv u \bmod Ay^2$, zeg $x - u = b.y^2$. Kennelijk geldt $\psi_x(x-u) \leq 2$.
Als $\psi_x(x-u) = 0$ dan $x - u = 0$ en $x = u \in A_1$, tegenspraak.
Als $\psi_x(x-u) = 1$ dan $x - u = b.y^2 \in A^*$ dus $y \in A^*$, tegenspraak.
Als $\psi_x(x-u) = 2$ dan is $x - u = b.y^2$ een priemelement wegens lemma (3.1).
Dit is een tegenspraak omdat y een priemelement is. □

Bewijs van (1.13). Stel A heeft slechts eindig vele maximale idealen. Omdat A hoofdidealring is volgt dan uit de chinese reststelling dat $A^* \to (A/Aa)^*$ voor elke $a \in A$ surjectief is. Lemma (3.2) impliceert dan dat voor elk priemelement y geldt $y \in A^*.x$ of $y = 0$. Op eenheden na is x dus het enige priemelement $\neq 0$ van A, dus A is een discrete valuatiering. □

De bewijzen van (1.11) en (1.12) worden tegelijk gevoerd. Overwegingen die slechts op (1.11) betrekking hebben worden voorafgegaan door (FF), overwegingen die slechts op (1.12) betrekking hebben door (NF), overwegingen die op beide betrekking hebben door (FF + NF).

(FF) Zij k een lichaam en A als in (1.11). Zij R de deelring $k[x]$ van A. Uit $x \notin A_1$ volgt dat x transcendent over k is.

(NF) Zij A als in (1.12), en R de deelring $\mathbb{Z}$ van A.

(FF+NF) Zij K het quotiëntenlichaam van A en $F \subset K$ het quotiëntenlichaam van R. Omdat A van eindig type over R is, geldt

$$\dim(A) = \operatorname{trgr}_F(K) + 1$$

waar "trgr" betekent "transcendentiegraad". Aangezien we $\dim(A) = 1$ al wisten volgt dat K algebraisch over F is.

(FF) Zij M de verzameling niet-triviale priëndivisoren van K die beperkt tot k triviaal zijn, en zij $M_\infty \subset M$ de verzameling polen van x.

(NF) Zij M de verzameling niet-triviale priëndivisoren van K, en zij $M_\infty \subset M$ de verzameling archimedische priëndivisoren van K.

(FF+NF) Kies absolute waarden $|\ |_v : K \to \mathbb{R}_{\geq 0}$ voor $v \in M$, zodanig dat de produktformule geldt. Zij T de gehele afsluiting van R binnen K:

$$T = \{a \in K \mid |a|_v \leq 1 \text{ voor alle } v \in M \setminus M_\infty\}.$$

Omdat A, als hoofdideaalring, geheel afgesloten is, geldt $T \subset A \subset K$, waar K het quotiëntenlichaam van T is. T is een Dedekindring, en A is van eindig type over T, dus er is een eindige deelverzameling $S \subset M$ met $M_\infty \subset S$ en

$$A = \{a \in K \mid |a|_v \leq 1 \text{ voor alle } v \in M \setminus S\}.$$

Er volgt

$$A^* = \{a \in K \mid |a|_v = 1 \text{ voor alle } v \in M \setminus S\}.$$

Definiëer $S_0 \subset S$ door

$$S_0 = \{v \in S \mid |u|_v = 1 \text{ voor alle } u \in A^*\}$$

en $V = S \setminus S_0$ (niet te verwarren met de V en S uit §2).

Uit de produktformule volgt nu:

Lemma (3.3). $\prod_{v \in V} |u|_v = 1$ voor elke $u \in A^*$. □

Definiëer het groepshomomorfisme

$$h : A^* \to \mathbb{R}^{*V}$$

door $h(u) = (|u|_v)_{v \in V}$. Kennelijk geldt

$$\ker(h) = \{a \in K \mid |a|_v = 1 \text{ voor alle } v \in M\}.$$

(FF) Lemma (3.4). $\ker(h) = k^*$ en A^*/k^* is eindig voortgebracht.

Bewijs. De gegeven beschrijving van $\ker(h)$ impliceert

$$\ker(h) = \{a \in K^* \mid a \text{ is algebraisch over } k\}$$
$$= \{a \in A^* \mid a \text{ is algebraisch over } k\}.$$

Omdat k algebraisch afgesloten binnen A is, volgt $\ker(h) = k^*$. Verder $A^*/k^* \cong \mathrm{Im}(h) \subset \prod_{v \in V} \mathrm{Im}(|\ |_v)$ en deze laatste groep is $\cong \mathbb{Z}^V$ omdat alle v discreet zijn in dit geval. Omdat V eindig is volgt dat A^*/k^* eindig voortgebracht is. □

(NF) Lemma (3.4). $\ker(h)$ is de verzameling eenheidswortels in K, en is eindig.

Bewijs. Dit volgt uit de gegeven beschrijving van $\ker(h)$. □

(FF + NF) Lemma (3.5).

a) $\exists\, u \in A^* : \forall\, v \in V : |u|_v \neq 1$.

b) Stel $y \in A$ voldoet aan $\psi_x(y) = 2$. Dan geldt:
$\exists\, u \in A^* : u \equiv 1 \bmod Ay \wedge [\forall v \in V : |u|_v \neq 1]$.

Bewijs. a) Uit de definitie van V volgt dat er voor elke $v \in V$ een eenheid $u_v \in A^*$ is met $|u_v|_v \neq 1$. Een eenvoudig inductief argument toont dan aan dat voor geschikte $n_v \in \mathbb{N}$ $(v \in V)$ de eenheid $u = \prod_{v \in V} u_v^{n_v}$ voldoet aan $|u|_v \neq 1$ voor alle $v \in V$.

b) Zij $u \in A^*$ als in a).

(FF met k oneindig). Zij l de lichaamsuitbreiding A/Ay van k. Wegens (3.1) is $A^* \to l^*$ surjectief, dus uit (3.4) volgt dat l^*/k^* eindig voortgebracht is. Omdat k oneindig is, impliceert [S, prop. 18, corollary] dat $k = l$. Er is dus een constante $c \in k^*$ met $c \equiv u \bmod Ay$. De eenheid $u' = c^{-1}u$ van A voldoet nu aan $u' \equiv 1 \bmod Ay$ en $|u'|_v = |u|_v \neq 1$ voor alle $v \in V$. □

(FF met k eindig, + NF). In dit geval is A/Ay een eindig lichaam, zeg van orde q. Voor $u' = u^{q-1}$ geldt nu $u' \in A^*$, $u' \equiv 1 \bmod Ay$ en $|u'|_v = |u|_v^{q-1} \neq 1$ voor alle $v \in V$. □

(FF + NF) Lemma (3.6). Stel $V \neq \emptyset$. Dan is er een $t \in A^*$ met $x + t \notin A^*$.

Bewijs. Zij $u \in A^*$ als in (3.5) a). Uit (3.3) en $V \neq \emptyset$ volgt

$$\{v \in V \mid |u|_v < 1\} \neq \emptyset \neq \{v \in V \mid |u|_v > 1\}.$$

Nu geldt

$$\lim_{n\to\infty} |x+u^n|_v = \infty \quad \text{als } |u|_v > 1$$

$$\lim_{n\to\infty} |x+u^n|_v = |x|_v \neq 0 \quad \text{als } |u|_v < 1,$$

dus

$$\lim_{n\to\infty} \prod_{v\in V} |x+u^n|_v = \infty.$$

Wegens (3.3) impliceert dit $x+u^n \notin A^*$ voor n groot genoeg. □

Lemma (3.7). $A^* = \ker(h)$.

Bewijs Neem eerst aan $V \neq \emptyset$.
Zij $t \in A^*$ als in (3.6), en $y = x+t$. Dan $\psi_x(y) \leq 2$. Uit $\psi_x(y) = 0$ zou volgen $y = 0$, $x = -t \in A^*$, tegenspraak. Uit $y \notin A^*$ volgt $\psi_x(y) \neq 1$. We concluderen $\psi_x(y) = 2$. Kies $u \in A^*$ als in (3.5) b) en zet $y_n = x + u^n.t$ voor $n \in \mathbb{N}$. Kennelijk $\psi_x(y_n) \leq 2$, en $y_n \neq 0$, dus $\psi_x(y_n) \in \{1,2\}$. Uit $u \equiv 1 \bmod Ay$ volgt $y_n \equiv 0 \bmod Ay$, zeg $y_n = a_n \cdot y$. En volgt $y_n \notin A^*$, dus $\psi_x(y_n) = 2$. Wegens (3.1) zijn y_n en y priemelementen, dus $a_n \in A^*$ voor $n \in \mathbb{N}$. Uit

$$a_n = \frac{x}{y} + \frac{u^n.t}{y}$$

volgt

$$\lim_{n\to\infty} |a_n|_v = \infty \quad \text{als } |u|_v > 1$$

$$\lim_{n\to\infty} |a_n|_v = \left|\frac{x}{y}\right|_v \neq 0 \quad \text{als } |u|_v < 1$$

dus

$$\lim_{n\to\infty} \prod_{v\in V} |a_n|_v = \infty$$

in tegenspraak met (3.3)
Deze tegenspraak bewijst $V = \emptyset$. Dus $h: A^* \to \mathbb{R}^{*V}$ is de triviale afbeelding en $A^* = \ker h$. □

(FF) Bewijs van (1.11). Uit (3.4) en (3.7) volgt $A^* = k^*$ dus $A_1 = k$. Uit $A_1[x] = A$ volgt nu $A = k[x]$, en boven hebben we al gezien dat x transcendent over k is. □

(NF) Bewijs van (1.12). Uit (3.4) en (3.7) volgt dat A^* eindig is. Aangezien, zoals bekend,

$$A^* \cong (\text{eindige groep}) \oplus \mathbb{Z}^{|S|-1},$$

volgt $|S| = 1$. Wegens $|M_\infty| \geq 1$ en $M_\infty \subset S$ krijgen we

$S = \{v_\infty\}$, v_∞ = de enige archimedische priemdivisor van K.

Er volgt dat $K = \mathbb{Q}$ of $K = \mathbb{Q}(\sqrt{-d})$ voor zekere $d \in \mathbb{Z}$, $d > 0$, d kwadraatvrij, en dat $A = T$ de gehele afsluiting van $\mathbb{Z}$ in K is. Uit [S, prop. 14] volgt $d \in \{1, 2, 3, 7, 11\}$. We onderscheiden zes gevallen:

a) $K = \mathbb{Q}$, $A = \mathbb{Z}$. Omdat $\mathbb{Z}^* \to (\mathbb{Z}/4\mathbb{Z})^*$ surjectief is volgt uit (3.2) dat $2 \in A^*.x$ dus $x = \pm 2$.

b) $K = \mathbb{Q}(\sqrt{-1})$, $A = \mathbb{Z}[\sqrt{-1}]$. Voor $y = 1+\sqrt{-1}$ is $A^* \to (A/y^2A)^*$ surjectief, dus met (3.2) vinden we $y \in A^*.x$ oftewel $x \in A^*.(1+\sqrt{-1})$.

c) $K = \mathbb{Q}(\sqrt{-2})$, $A = \mathbb{Z}[\sqrt{-2}]$. Met behulp van (1.1) berekent men

$$A_2 = \{0, \pm 1, \pm\sqrt{2}, \pm\sqrt{2} \pm 1\}, \quad |A_2| = 9$$

en wegens $A_2 = A_1 + x.A_1$ volgt $x = \pm\sqrt{2}$. Voor $a = 3+\sqrt{-2}$ geldt $a = 1 + \sqrt{-2} - \sqrt{-2}^2$ dus $\psi_x(a) \leqslant 3$ en $a \in A_3$. Volgens (1.1) is dan

$$A_2 \to A/Aa$$

surjectief. Dit is een tegenspraak met $|A_2| = 9$, $|A/Aa| = 11$.

d) $K = \mathbb{Q}(\sqrt{-3})$, $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$. Voor $y = \frac{1}{2}(3+\sqrt{-3})$ is $A^* \to (A/y^2A)^*$ surjectief, dus (3.2) zegt $\frac{1}{2}(3+\sqrt{-3}) \in A^*.x$.

e) $K = \mathbb{Q}(\sqrt{-7})$, $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$. Zowel voor $y = \frac{1}{2}(1+\sqrt{-7})$ als voor $y = \frac{1}{2}(1-\sqrt{-7})$ is $A^* \to (A/y^2A)^*$ surjectief, dus $x \in A^*.\frac{1}{2}(1+\sqrt{-7}) \cap A^*.\frac{1}{2}(1-\sqrt{-7}) = \emptyset$, tegenspraak.

f) $K = \mathbb{Q}(\sqrt{-11})$, $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})]$. In dit geval $A_2 = \{0, \pm 1, \frac{1}{2}(\pm 1 \pm \sqrt{-11})\}$, en men gaat gemakkelijk na dat er geen $x \in A_2$ is met $A_2 = A_1 + x.A_1$. □