STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1949-006

Existentie van eindige binaire projectieve groepen

"Actualiteiten"

W. Peremans

1949

Existentie van eindige binaire projectieve groepen.

(Voordracht door W. Peremans in de serie Actualiteiten, 24 Sept. 1949)

§1. Bekende feiten.

We beschouwen de draaiingen van de gewone (driedimensionale Euclidische) ruimte om een vast punt O. Deze draaiingen kunnen ook opgevat worden als draaiingen van een boloppervlak met O als middelpunt. De groep van deze draaiingen bevat, zoals bekend, de volgende vijf typen van eindige ondergroepen:

1° cyclische groepen van orde N, bestaande uit N draaiingen met dezelfde as om hoeken $\frac{k2\pi}{N}$, $(k = 0,1,\ldots, N-1)$;

2° diëdergroepen van orde $N = 2n$ bestaande uit een cyclische groep van orde n en n draaiingen over π (van orde 2) om n assen, gelegen in het vlak loodrecht op de as van de cyclische groep;

3° de tetraedergroep van orde 12, bestaande uit alle draaiingen, die een in de bol ingeschreven regelmatig viervlak in zichzelf transformeren. Deze groep is isomorf met de alternerende groep A_4;

4° de octaedergroep van orde 24, bestaande uit alle draaiingen, die een in de bol ingeschreven kubus (of regelmatig achtvlak) in zichzelf transformeren. Deze groep is isomorf met de symmetrische groep S_4;

5° de icosaedergroep van orde 60, bestaande uit alle draaiingen, die een in de bol ingeschreven regelmatig twintigvlak (of twaalfvlak) in zichzelf transformeren. Deze groep is isomorf met de alternerende groep A_5.

Dat deze groepen de enig mogelijke eindige draaiingsgroepen zijn is het eerst door F. Klein [4] bewezen. We kunnen deze stelling in een voor generalisatie geschiktere vorm brengen door de bol met behulp van stereografische projectie op de bekende manier af te beelden op het complexe vlak (met inbegrip van het punt ∞). Boldraaiingen gaan dan over in gebroken lineaire transformaties van een speciaal soort, die unitaire transformaties genoemd worden:

$$z' = \frac{a\,z + b}{-\bar{b}\,z + \bar{a}} .$$

De enige eindige ondergroepen van de groep der unitaire transformaties van een complexe veranderlijke zijn dus ook de bovengenoemde.

We kunnen nu de beperking tot unitaire transformaties laten vervallen en dus vragen naar de eindige ondergroepen van de groep der gebroken

lineaire transformaties van een complexe veranderlijke of, wat op hetzelfde neerkomt als we de veranderlijken homogeen schrijven, van de groep der complexe binaire projectieve transformaties.

Ook deze vraag is door F. Klein bantwoord in die zin, dat de enige ondergroepen weer dezelfde bovengenoemde groepen zijn.

§2. Generalisatie.

Nu kunnen we het probleem onmiddellijk generaliseren tot dat van de eindige ondergroepen van de groep der binaire projectieve transformaties over een willekeurig commutatief grondlichaam. Voor een uitvoerige bespreking van dit probleem zie mijn dissertatie [6] . Het blijkt dat als de karakteristiek van het grondlichaam nul is wederom geen andere dan de bovenstaande eindige groepen mogelijk zijn. Is daarentegen de karakteristiek p, dan treden verscheidene nieuwe typen van groepen op. Dit wordt veroorzaakt door het feit, dat alleen bij karakteristiek p transformaties met een samenvallend paar invariante punten (polen) in een eindige groep kunnen optreden.

Van de verschillende problemen, die in dit verband gesteld kunnen worden, willen we er hier één bespreken. We zullen ons daarbij echter, om niet te uitvoerig te worden, moeten beperken tot het geval dat de karakteristiek nul is. We stellen de vraag naar de existentie van bovenstaande groepen; dus uitvoeriger geformuleerd:

Gegeven een lichaam van karakteristiek nul; gevraagd: welke eindige groepen zijn te realiseren als groepen van binaire projectieve transformaties met coëfficiënten uit dat lichaam. We nemen daarbij als bekend aan, dat daarvoor geen andere dan de bovengenoemde groepen in aanmerking komen.

§3. Existentie van cyclische groepen.

We zoeken een transformatie van orde N, d.w.z. een transformatie, waarvan de N^{e} en geen lagere macht de identieke transformatie is. We stellen de transformaties voor door tweerijige niet-singuliere matrices waarbij we, omdat het projectieve transformaties betreft, de (ongebruikelijke) afspraak maken, dat we twee matrices als gelijk beschouwen als de ene uit de andere ontstaat door vermenigvuldiging met een factor $\neq 0$. We noemen het grondlichaam K.

We kunnen door een projectieve coördinatentransformatie een matrix altijd in een van de beide volgende gedaanten brengen:

$$\begin{pmatrix} p & o \\ o & q \end{pmatrix}, \quad \begin{pmatrix} y & 1 \\ z & o \end{pmatrix}.$$

(N.B. De eigenwaarden van de matrix behoeven als oplossing van een vierkantsvergelijking niet in K te liggen; een diagonaal- of driehoeksgedaante is dus niet in alle gevallen te bereiken!)
Nu geldt:

$$\begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}^N = \begin{pmatrix} p^N & 0 \\ 0 & q^N \end{pmatrix} = \begin{pmatrix} (\frac{p}{q})^N & 0 \\ 0 & 1 \end{pmatrix}.$$

Als deze matrix dus orde N heeft, moet $\frac{p}{q}$ een primitieve N^{e} eenheidswortel ζ zijn (primitief omdat anders de orde $< N$ zou zijn), die dan dus in K moet liggen. Bevat omgekeerd K de N^{e} eenheidswortels, dan is

$$\begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

een matrix van orde N. In dat geval is de existentie dus gewaarborgd.
We nemen nu aan dat K de N^{e} eenheidswortels niet bevat. Een eventuele matrix van orde N moeten we dan zoeken onder die van de gedaante

$$A = \begin{pmatrix} y & 1 \\ z & 0 \end{pmatrix}.$$

De karakteristieke vergelijking van deze matrix luidt:

$$f(x) = x^2 - y\,x - z = 0.$$

Deze vergelijking is irreducibel, want als ze reducibel was met wortels λ_1, λ_2 in K dan was A in K toch op een diagonaal- of driehoeksgedaante te brengen, waaruit zou volgen dat λ_1 en λ_2 primitieve N^{e} eenheidswortels zouden zijn in strijd met de veronderstelling.
Dus heeft f(x) in een kwadratisch uitbreidingslichaam van K twee verschillende wortels v en w en in dat lichaam kan A op de diagonaalvorm

$$\begin{pmatrix} v & 0 \\ 0 & w \end{pmatrix}$$

gebracht worden. Als deze matrix orde N heeft moet

(1) $$\frac{v}{w} = \zeta$$

een primitieve N^{e} eenheidswortel zijn. Het kwadratische lichaam moet dus de N^{e} eenheidswortels bevatten. Past men op (1) de substitutie S van de groep van Galois toe, die de beide wortels v en w verwisselt, dan vindt men

$$S\zeta = \frac{w}{v},$$

of

$$S\zeta = \zeta^{-1}.$$

ζ en ζ^{-1} zijn dus geconjugeerd ten opzichte van K en de som

$$\zeta + \zeta^{-1} = c$$

moet tot K behoren.

Deze voorwaarde is ook voldoende. Want als $\zeta + \zeta^{-1}$ in K ligt, zijn ζ en ζ^{-1} wortels van de vierkantsvergelijking:

$$x^2 - c\,x + 1 = 0, \qquad (c = \zeta + \zeta^{-1}).$$

In het kwadratische lichaam $K(\zeta)$ kan men nu twee geconjugeerde elementen v en w zo bepalen, dat (1) geldt:

$$v = \zeta w.$$

Stelt men namelijk

$$v = a + b\zeta ,$$

dan wordt

$$w = S\,v = a + b\,\zeta^{-1} .$$

De voorwaarde $v = \zeta w$ geeft nu

$$a + b\zeta = a\zeta + b .$$

De algemeenste oplossing hiervan is a = b, dus

$$v = \lambda(1 + \zeta),$$
$$w = \lambda(1 + \zeta^{-1}).$$

De karakteristieke vergelijking, waarvan v en w wortels zijn, wordt dan

$$f(x) = x^2 - \lambda(c + 2)\,x + \lambda^2 (c + 2) = 0;\ c = \zeta + \zeta^{-1},$$

en de matrix A wordt

$$A = \begin{pmatrix} \lambda(c+2) & 1 \\ -\lambda^2(c+2) & 0 \end{pmatrix} .$$

Dit geeft ons de volgende stelling:

Stelling 1. Noodzakelijk en voldoende opdat in een lichaam K van karakteristiek nul een matrix van orde N bestaat is dat $\zeta + \zeta^{-1}$ in K ligt, als ζ een primitieve N^{e} eenheidswortel voorstelt.
In deze formulering is het geval, dat ζ zelf in K ligt, begrepen.
Omdat bij de orden 2,3,4 en 6 de cirkeldelingspolynomen van de eerste of tweede graad zijn, bestaan matrices vandeze orden in ieder lichaam.

§4. Existentie van diëdergroepen.

Het is duidelijk, dat het voor de existentie van een diëdergroep van orde 2 n noodzakelijk is dat een cyclische groep van orde n bestaat. We nemen dus aan dat voor n aan de voorwaarden van stelling 1 voldaan is.

We bewijzen eerst een hulpstelling.

Hulpstelling 1. Een niet-singuliere matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

heeft dan en slechts dan orde 2, als $p + s = 0$ is.

Bewijs: $\begin{pmatrix} p & q \\ r & s \end{pmatrix}^2 = \begin{pmatrix} p^2 + qr & q(p+s) \\ r(p+s) & qr + s^2 \end{pmatrix} = E,$

dus $$\left.\begin{aligned} (p^2 + qr)-(qr + s^2) = (p - s)(p + s) &= 0 \\ q\,(p+ s) &= 0 \\ r(p + s) &= 0 \end{aligned}\right\}.$$

Als $p - s = q = r = 0$, is de matrix $= E$. Dus is $p + s = 0$ de gezochte voorwaarde. Als K de n^e eenheidswortels bevat, is een matrix A van orde n in de gedaante

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

te brengen. Stel een matrix B van orde 2:

$$B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

dan is

$$A\,B = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} \zeta a & \zeta b \\ c & -a \end{pmatrix}.$$

AB heeft dus orde 2, als $\zeta a - a = (\zeta - 1)a = 0$ is, dus als $a = 0$ is. Hieraan is te voldoen met een niet-singuliere matrix B, b.v. met $a = 0$, $b = c = 1$.

Als K de n^e eenheidswortels niet bevat is een matrix A van orde n in de gedaante

$$A = \begin{pmatrix} y & 1 \\ z & 0 \end{pmatrix}$$

te brengen; kiezen we weer B als een matrix van orde 2:

$$B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

dan is

$$A\,B = \begin{pmatrix} y & 1 \\ z & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} a\,y + c & b\,y - a \\ a\,z & b\,z \end{pmatrix}.$$

A B heeft dus orde 2, als $a\,y + c + b\,z = 0$, of $c = -a\,y - b\,z$. Hieraan kan voldaan worden met een niet-singuliere matrix B, b.v. $a = 0$, $b = 1$, $c = -z$ (we weten dat $z \neq 0$ is).

In beide gevallen hebben we dus een matrix A van de orde n en een matrix B van de orde 2 gevonden, zo dat hun product A B orde 2 heeft. Maar uit $A\,B\,A\,B = E$, of $A\,B\,A = B$ volgt $A^k\,B\,A^k\,B = A^{k-1}ABAA^{k-1}\,B = A^{k-1}\,B\,A^{k-1}\,B = E$, m.a.w. $A^k\,B$ heeft ook orde 2. Hieruit volgt dat de matrices A^k en A^kB $(k= 0,1,\ldots,n-1)$ een groep vormen, want $B\,A^k = A^{n-k}\,B$,

dus $A^h.A^k = A^{h+k}$, $A^h.A^kB = A^{h+k}B$, $A^kB.A^h = A^{n-h+k}B$, $A^hB.A^kB =$
$= A^{n-k+h}B$. Deze groep is klaarblijkelijk een diëdergroep. Dus

Stelling 2. Noodzakelijk en voldoende voor de existentie van een diëdergroep van orde 2 n als binaire projectieve groep over een lichaam K van karakteristiek nul, is de existentie van de overeenkomstige cyclische groep van orde n.

§5. Existentie van tetraeder-, octaeder- en icosaedergroep.

Om de existentie van een groep aan te tonen, is het voldoende hetzelfde te doen voor een stelsel voortbrengende elementen van die groep. We beginnen dus een geschikt gekozen stelsel voortbrengenden te kiezen voor de groepen A_4, S_4 en A_5.

Hulpstelling 2. De groepen A_4, S_4 en A_5 zijn isomorf met groepen met twee voortbrengenden A en B met de relaties:

bij A_4 : $A^3 = B^3 = (AB)^2 = E$,

bij S_4 : $A^4 = B^3 = (AB)^2 = E$,

bij A_5 : $A^5 = B^3 = (AB)^2 = E$.

Voor het bewijs zie men Dickson [2], §264, §265 en §267, waar voortbrengenden en relaties opgesteld worden, die op eenvoudige wijze in de bovenstaande te transformeren zijn.

Hulpstelling 3. Als twee matrices A en B gegeven zijn, zo dat de orden van A, B en A B overeenkomen met de relaties in hulpstelling 2, dan brengen A en B een groep van matrices voort isomorf resp. met A_4, S_4 en A_5,
(Men lette op het verschil tussen $P^n = E$ en P heeft orde n, d.w.z. n is het kleinste natuurlijke getal, waarvoor geldt $P^n = E$).

Bewijs: De groep G', voortgebracht door A en B voldoet aan dezelfde relaties als de abstracte groep G gevormd met de relaties van hulpstelling 2. Volgens een bekende stelling uit de groepentheorie is G' homomorf beeld van G: $G' \cong G/N$.
In het eerste geval zijn de orden van A en A B resp. 3 en 2, dus de orde van G' een veelvoud van 6; als niet $G' \cong G$ was, moest N orde 2 hebben; daar echter A_4 geen normale ondergroep van orde 2 heeft, is $G' \cong A_4$.
In het tweede geval zijn de orden van A en B resp. 4 en 3, dus de orde van G' een veelvoud van 12; als niet $G' \cong G$ was, moest N orde 2 hebben; daar echter S_4 geen normale ondergroep van orde 2 heeft, is $G' \cong S_4$.
In het derde geval is de orde van G' zeker > 1; daar A_5 enkelvoudig is, volgt daaruit, dat $G' \cong A_5$.

Hulpstelling 4. Een niet-singuliere matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

heeft dan en slechts dan orde 3, als $p^2 + p\,s + s^2 + q\,r = 0$ is.

Bewijs:

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}^3 = \begin{pmatrix} p^3 + 2\,pqr + qrs & q(p^2 + ps + s^2 + qr) \\ r\,(p^2 + ps + s^2 + qr) & pqr + 2\,qrs + s^3 \end{pmatrix} = E,$$

dus $(p^3 + 2\,pqr + qrs) - (pqr + 2\,qrs + s^3) = (p-s)(p^2 + ps + s^2 + qr) = 0$

$$q\,(p^2 + ps + s^2 + qr) = 0$$

$$r\,(p^2 + ps + s^2 + qr) = 0$$

Als $p - s = q = r = 0$ is, is de matrix $= E$. Dus $p^2 + ps + s^2 + qr = 0$ is de gezochte voorwaarde.

Noodzakelijk en voldoende voor het bestaan van de tetraeder-, octaeder- resp. icosaedergroep is dus het bestaan van een matrix A van orde 3, 4 resp. 5 en een matrix B van orde 3, zodat A B orde 2 heeft. Bevat K een primitieve derde, vierde resp. vijfde eenheidswortel genaamd ε, dan kan voor A gekozen worden

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}.$$

Stellen we

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

dan is

$$A\,B = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \varepsilon a & \varepsilon b \\ c & d \end{pmatrix}.$$

Dit heeft orde 2, als $\varepsilon a + d = 0$ is, of $d = -\varepsilon a$. De voorwaarde, dat B orde 3 heeft, wordt dan $a^2 + ad + d^2 + bc = a^2 - \varepsilon a^2 + \varepsilon^2 a^2 + bc = 0$. Kiest men $b \neq 0$, dan is c hieruit op te lossen. De zo gevonden matrix is zeker niet singulier, mits $a \neq 0$ gekozen wordt, want singulariteit zou betekenen $0 = ad - bc = -\varepsilon a^2 + a^2 - \varepsilon a^2 + \varepsilon^2 a^2 = (1-\varepsilon)^2 a^2$. De existentie is daarmee dus aangetoond.

Bevat K de betreffende eenheidswortel niet, dan is voor existentie toch in ieder geval noodzakelijk, dat matrices van de in de hulpstellingen 2 en 3 vermelde orden bestaan. Matrices van orde 2, 3 en 4 bestaan volgens § 3 altijd; er komt dus alleen voor de icosaedergroep een eis voor orde 5, n.l. dat de vijfde eenheidwortels kwadratisch over K zijn, zo dat $\varepsilon + \varepsilon^{-1}$ in K ligt.

Nu is de vergelijking, waaraan ε voldoet

$$x^4 + x^3 + x^2 + x + 1 = 0$$

en die, waaraan $\varepsilon + \varepsilon^{-1}$ voldoet:

$$x^2 + x - 1 = 0 .$$

De eis dat $\varepsilon + \varepsilon^{-1}$ in K ligt, is dezelfde als dat 5 in K een kwadraat is.

Nu is A in de vorm

$$A = \begin{pmatrix} \lambda(c+2) & 1 \\ -\lambda^2 & 0 \end{pmatrix} , \qquad c = \varepsilon + \varepsilon^{-1} ,$$

te brengen. Stellen we

$$B = \begin{pmatrix} x & y \\ z & u \end{pmatrix},$$

dan is

$$A\,B = \begin{pmatrix} \lambda(c+2) & 1 \\ -\lambda^2(c+2) & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} \lambda(c+2)x + z & \lambda(c+2)y + u \\ -\lambda^2(c+2)\,x & -\lambda^2(c+2)\,y \end{pmatrix}.$$

Dit heeft orde 2 als $\lambda(c+2)x + z - \lambda^2(c+2)y = 0$ is. Lost men z hieruit op: $z = \lambda(c+2)(\lambda y - x)$, dan wordt de voorwaarde dat B orde 3 heeft

$$x^2 + x\,u + u^2 + (c+2)(\lambda y - x)\,\lambda y = 0.$$

Kiezen we nu λy als nieuwe veranderlijke, die we gemakshalve maar weer y noemen, dan vinden we het volgende algebraische criterium voor de existentie:

(2) $$x^2 + x\,u + u^2 + (c+2)(y-x)y = 0.$$

Hier komt nog de eis van niet-singulariteit bij, dat is voor B: $x\,u - y\,z \neq 0$, maar daar $-\,y\,z = x^2 + x\,u + u^2$ is, reduceert deze eis zich tot:

$$x + u \neq 0.$$

De vergelijking (2) is door een niet-singuliere homogene lineaire transformatie in het grondlichaam in een eenvoudiger gedaante te brengen. We doen dit voor de drie groepen afzonderlijk.

1° Tetraedergroep. Hier is $c + 2 = 1$. De vergelijking is te schrijven als:

$$\tfrac{1}{2}(x^2 + x\,u + u^2 + y^2 - x\,y) = 0 .$$

Door de transformatie:

$$\left.\begin{aligned} x &= 2\,x' \\ u &= -\,x' + u' + y' \\ y &= \;\;x' - u' + y' \end{aligned}\right\}, \quad \text{transformatiedeterminant} = 4 \neq 0,$$

gaat dit over in (accenten weglaten):

$$x^2 + u^2 + y^2 = 0 .$$

2^{o} Octaedergroep. Hier is $c + 2 = 2$. De vergelijking is te schrijven als:

$$\tfrac{1}{2} x^2 + \tfrac{1}{2} x u + \tfrac{1}{2} u^2 + y^2 - x y = 0.$$

Door de transformatie

$$\left.\begin{aligned} x &= 2x' - 2u' \\ u &= \quad\; 2u' \\ y &= \; x' - \; u' + y' \end{aligned}\right\}, \text{ transformatiedeterminant} = 4 \neq 0$$

gaat dit over in:

$$x^2 + u^2 + y^2 = 0.$$

3^{o} Icosaedergroep. Hier voldoet c aan $c^2 + c - 1 = 0$. Door de transformatie

$$\left.\begin{aligned} x &= 2(c+1)x' \\ u &= -(c+1)x' + u' \\ y &= \; (c+1)x' \quad + c\,y' \end{aligned}\right\}, \text{transformatiedeterminant} = 2(c^2+c) = 2 \neq 0,$$

gaat (2) over in:

$$x^2 + u^2 + y^2 = 0.$$

In de drie gevallen is de gedaante van de vergelijking dus dezelfde geworden. De bijcondities voor niet-singulariteit kunnen vervangen worden door de eis, dat de x, u en y niet alle drie = 0 zijn (dat de oplossing niet-triviaal is). De bijcondities voor de getransformeerde veranderlijken luiden namelijk als volgt in de drie gevallen:

1^{o} $x + y + u \neq 0$,
2^{o} $x \neq 0$,
3^{o} $(c+1)x + u \neq 0$.

Als er nu in geval 1^{o} een niet-triviale oplossing bestaat, waarvoor $x + y + u = 0$ is, dan is door de waarde van één veranderlijke, die $\neq 0$ is, in zijn tegengestelde te veranderen, een niet-triviale oplossing te verkrijgen, waarvoor $x + y + u \neq 0$ is. In geval 2^{o} kan door verwisseling van de waarden der veranderlijken steeds gezorgd worden, dat $x \neq 0$ is. In geval 3^{o} kan evenzo gezorgd worden, dat $u \neq 0$ is; zou dan $(c+1)x + u = 0$ worden, dan vervange men u door zijn tegengestelde.

Hulpstelling 5. Als in een lichaam de vergelijking

(3) $$x^2 + y^2 + u^2 + z^2 = 0$$

een niet-triviale oplossing heeft, dan heeft ook

(4) $$x^2 + y^2 + u^2 = 0$$

een niet-triviale oplossing.

Bewijs: Stel dat (3) niet triviaal oplosbaar is in het lichaam K als volgt:

$$\xi_1 + \xi_2 + \xi_3 + \xi_4 = 0.$$

Zonder beperking van de algemeenheid kunnen we $\xi_4 \neq 0$ stellen. Als -1 in K een kwadraat is, is (4) ook oplosbaar, namelijk door $(\sqrt{-1}, 1, 0)$. We nemen dus aan, dat -1 in K geen kwadraat is. Dan is

$$(\xi_1\xi_3 - \xi_2\xi_4, \xi_1\xi_4 + \xi_2\xi_3, \xi_3^2 + \xi_4^2)$$

een niet-triviale oplossing van (4). Immers dat zij niet-triviaal is, volgt uit het feit, dat zeker $\xi_3^2 + \xi_4^2 \neq 0$ is (-1 geen kwadraat); dat het een oplossing is, blijkt door substitueren.

Hulpstelling 6. De lichamen waarin

$$x^2 + y^2 + z^2 + u^2 = 0$$

niet-triviaal oplosbaar is, zijn juist de splitsingslichamen (splitting fields, Zerfällungskörper) van het gewone quaternionensysteem.

Bewijs: (zie ook Van der Waerden [8] , Kap. 16). Bij de quaternionen is het feit, dat het grondlichaam splitsingslichaam is, aequivalent met het optreden van nuldelers in het quaternionensysteem. Voor het laatste is evenwel de niet-triviale oplosbaarheid van bovenstaande vergelijking juist de voorwaarde.

Om de twee gevallen, die we aanvankelijk hadden onderscheiden, nu weer samen te smelten tonen we nog het volgende aan.

Hulpstelling 7. Lichamen, die de derde, vierde of vijfde eenheidswortels bevatten, zijn splitsingslichamen van het quaternionensysteem. Voor de derde en vierde eenheidswortels is dat triviaal; het volgt onmiddellijk uit hun definiërende vergelijking: $0 = \varepsilon^2 + \varepsilon + 1 = \varepsilon^2 + (\varepsilon^2)^2 + 1^2$; resp. $0 = \varepsilon^2 + 1 = \varepsilon^2 + 1^2$.

Voor de vijfde eenheidswortels zullen we het bewijs hier achterwege laten. Met hulpmiddelen uit de algebraische getallentheorie is het heel eenvoudig. Het kan ook rechtstreeks met behulp van de in het bovenstaande gegeven beschouwingen; het vereist dan evenwel een vrij omvangrijk en vervelend gereken.

De bovenstaande hulpstellingen stellen ons nu in staat de gezochte existentiestelling uit te spreken:

Stelling 3. De tetraeder-, octaeder- en icosaedergroepen zijn als groepen van binaire projectieve transformaties te realiseren in die en slechts die lichamen K van karakteristiek nul, die splitsingslichamen van het gewone quaternionensysteem zijn. In het geval van de icosaedergroep komt daar nog de eis bij dat 5 een kwadraat is in K.

§6. Toepassing op getallenlichamen.

Bij de beantwoording van de vraag, welke lichamen splitsingslichamen der quaternionen zijn, kan gebruik gemaakt worden van hetgeen daarover uit de algebra bekend is. Als K een algebraisch getallenlichaam is, is het mogelijk daarbij arithmetische hulpmiddelen toe te passen. Dat geval beschouwen we nog wat nader. Voor de resultaten uit de theorie der hypercomplexe systemen, die in het vervolg gebruikt worden, zie b.v. Deuring [1], Kap. 6 en 7.

Als R het lichaam der rationale getallen is en K een getallenlichaam, dan is noodzakelijk en voldoende opdat K splitsingslichaam is van een algebra (hypercomplex systeem) A over R, dat alle $\mathfrak{p}$-adische uitbreidingen $K_{\mathfrak{p}}$ van K, behorende bij een priemideaal $\mathfrak{p}$ in K, splitsingslichamen zijn van de eveneens p-adisch uitgebreide algebra A_p, waarbij p het priemgetal is, dat veelvoud van $\mathfrak{p}$ is, benevens de (reële of complexe) uitbreidingen behorende bij de oneindige priemplaatsen. Zie hiervoor Hasse [3] en Köthe [5].

Nu geldt evenwel voor een enkelvoudige algebra over een p-adisch getallenlichaam; dat de splitsingslichamen die en slechts die zijn, waarvan de graad een veelvoud is van de index van de algebra.

De p-index van een algebra is echter slechts dan $\neq 1$, als p deler is van de discriminant van de algebra.

Er wordt dus slechts iets geëist van de priemdelers van de discriminant, die met de oneindige priemplaatsen samen, de vertakkingsplaatsen van de algebra heten.

Bij het quaternionensysteem is de discriminant = -16. Er komen als vertakkingsplaatsen dus alleen ∞ en 2 en we behoeven in K alleen ∞ en de priemdelers van 2 te beschouwen. Nu geeft ∞ de eis, dat het lichaam K niet formeel reëel is: de rang van de perfecte uitbreiding van K moet >1 zijn over het erin bevatte reëel afgesloten lichaam. Deze eis is evident, want in een reëel lichaam kan nooit een som van kwadraten op niet-triviale wijze nul zijn:

De priemdelers $\mathfrak{p}$ van 2 geven aanleiding tot $\mathfrak{p}$-adische uitbreidingen van K, die men als volgt vindt: (zie Van der Waerden [7], §76) ontbind de definiërende vergelijking van K in 2-adisch irreducibele factoren. Laat deze factoren de graden $g_1,\ldots, g_r$ hebben. Dan hebben de $\mathfrak{p}$-adische uitbreidingen van K, die bij de priemdelers van 2 behoren, eveneens de graden $g_1,\ldots,g_r$.

Men kan ook 2 in K in priemidealen ontbinden:

$$2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r}.$$

Laat $\mathfrak{P}_i$ de graad f_i hebben. Dan is

$$g_i = e_i f_i \ .$$

De $\mathfrak{p}$-adische uitbreidingen van de graden $g_1,..,g_r$ zijn volgens de zo juist genoemde stelling slechts dan splitsingslichaam van de quaternionenalgebra, als hun graden $g_1,...,g_r$ alle even zijn. We krijgen dus het volgende criterium:

Stelling 4. Nodig en voldoende, opdat een getallenlichaam K splitsingslichaam van de quaternionen is, is:
1^o dat K niet formeel reëel is, dus geen reële geconjugeerden heeft,
2^o dat in de priemideaalontbinding van 2 de producten $e_i f_i$ van exponenten en graden alle even zijn.

Men kan dit criterium ook formuleren met behulp van de definiërende vergelijking van K:

Stelling 5. Nodig en voldoende, opdat een getallenlichaam K splitsingslichaam van de quaternionen is, is, dat de definiërende vergelijking van K zowel reëel als 2-adisch in priemfactoren van even graad uiteenvalt.

§7. Voorbeelden.

Het evidente feit dat een reëel lichaam nooit splitsingslichaam kan zijn van de quaternionen stelt ons in staat onmiddellijk alle bestaande groepen over het lichaam R der rationale getallen op te schrijven, n.l. cyclische groepen van orden 2,3,4 en 6 en de bijbehorende diëdergroepen van orden 4,6,8 en 12.

Als toepassing van de in § 6 behandelde getallentheoretische hulpmiddelen behandelen we het geval van de kwadratische getallenlichamen $R(\sqrt{D})$, waarin D een kwadraatvrij geheel rationaal getal voorstelt. De definiërende vergelijking is dus

$$x^2 - D = 0 \ . \tag{5}$$

Deze moeten we reëel en 2-adisch ontbinden. Het lichaam zal splitsingslichaam zijn, als ze in beide gevallen irreducibel blijft. Reëel is dat dan en slechts dan het geval als $D < 0$ is. Voor de 2-adische ontbinding beschouwen we eerst

$$x^2 - D \equiv 0 \ (8) \ . \tag{6}$$

Deze congruentie is dan en slechts dan oplosbaar als $D \equiv 0(4)$ of $D \equiv 1(8)$. Het geval $D \equiv 0(4)$ is evenwel uitgesloten, omdat D kwadraatvrij verondersteld was. Als dus $D \not\equiv 1(8)$ is, is (6) onoplosbaar, dus zeker (5) 2-adisch onoplosbaar, dus 2-adisch irreducibel.

Als $D \equiv 1(8)$ is, stellen we $1 - D = 8k$ en transformeren x door $x = 2y + 1$; de vergelijking wordt dan

$$4(y^2 + y + 2k) = 0.$$

Nu is de vergelijking

$$y^2 + y + 2k = 0,$$

opgevat als congruentie mod 2, ontbindbaar in relatief prieme factoren (n.l. y en y + 1). Daaruit volgt, dat dit ook in het lichaam der 2-adische getallen het geval is (zie van der Waerden [7], §76 Reduzibilitätskriterium), en daaruit weer hetzelfde voor de oorspronkelijke vergelijking (5). In dit geval dus geen splitsingslichaam. Dus we vinden:

Stelling 6. De kwadratische getallenlichamen $R(\sqrt{D})$, D kwadraatvrij, zijn splitsingslichamen der quaternionen dan en slechts dan, als $D < 0$ en $D \not\equiv 1(8)$.

Literatuur.

[1] M. Deuring, Algebren, Erg.d.Math., IV 1, Berlin 1935.

[2] L.E. Dickson, Linear groups, Leipzig 1901.

[3] H. Hasse, Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math.Ann. 107 (1933), 731-760.

[4] F. Klein, Ueber binäre Formen mit linearen Transformationen in sich selbst, Math. Ann. 9 (1876), 183-208.

[5] G. Köthe, Erweiterung des Zentrums einfacher Algebren, Math.Ann. 107 (1933), 761-766.

[6] W. Peremans, Eindige binaire projectieve groepen, diss. Amsterdam 1949.

[7] B.L. van der Waerden, Moderne Algebra I, 2. Aufl. Berlin 1937.

[8] B.L. van der Waerden, Moderne Algebra II, 2. Aufl. Berlin 1940.