CWI Syllabus 15

Vacantiecursus 1983
Complexe getallen

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

ISBN 90 6196 328 1
NUGI-code: 811

Printed in the Netherlands

Voorwoord

Deze bundel bevat - in essentie - de voordrachten die gehouden zijn tijdens de vacantiecursus voor leraren in 1983, georganiseerd door het CWI, destijds nog Mathematisch Centrum genaamd. Het onderwerp was: 'Complexe Getallen'. Deze werden daarbij van verschillende kanten belicht: complexe getallen in historisch perspectief, optreden van complexe getallen in verschillende gebieden van de wiskunde met speciale aandacht voor de meetkunde, toepassingen in de techniek, complexe getallen in algebraïsche context en tenslotte: generalisaties tot quaternionen en octaven. De hier opgenoemde afzonderlijke verhandelingen zijn de genoemde voordrachten, in enkele gevallen iets uitgebreid en waar nodig, bijgesteld.

De goede ontvangst van de syllabus van de cursus lijkt deze heruitgave in de serie CWI Syllabi te rechtvaardigen. Als lezerspubliek denken wij ons in de eerste plaats diegenen die het niveau van 1ste jaarsstudent in de faculteit wis- en natuurkunde of een technische faculteit (of hoger) bereikt hebben. Naar de mening van de samenstellers zullen vooral leraren er veel in vinden wat bij hun onderwijs bruikbaar is. Van harte hopen zij dat dit boekje in deze nieuwe gedaante zijn weg zal vinden.

A.W. GROOTENDORST

Inhoud

$\mathbb{C}$ avant la lettre

J.A. van Maanen
Rijksuniversiteit Utrecht
Postbus 80.010, 3508 TA Utrecht

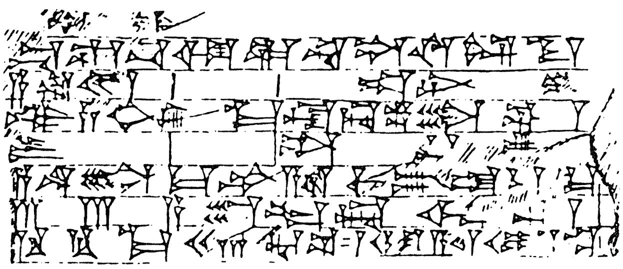
1. Vergelijkingen

Omdat het ontstaan van de complexe getallen nauw samenhangt met het oplossen van vergelijkingen, volgt nu eerst een uiterst oppervlakkig overzicht van de ontwikkelingen op dat gebied tot het jaar 1500.

Eerste- en tweedegraads vergelijkingen in één of meer onbekenden zijn bijna net zo oud als de wiskunde zelf. De volgende twee teksten lichten dit toe. De eerste tekst bevat een eerstegraads vergelijking uit de *Papyrus Rhind*, geschreven in Egypte na 1800 voor Chr., maar gebaseerd op een prototype uit de periode 2000 - 1800.

<table>
<tr><td colspan="2">1
Ik ga drie maal in een schepel; mijn derde deel en een derde van mijn derde deel en mijn negende deel worden bij mij opgeteld en ik kom er helemaal uit (d.w.z. de schepel is geheel gevuld). Wie is het die dit zegt.</td></tr>
<tr><td>Vertaling via het Engels; Van der Waerden 1950, p.32</td><td>parafrase: ik = x
$3x + \frac{x}{3} + \frac{x}{9} + \frac{x}{9} = 1$</td></tr>
</table>

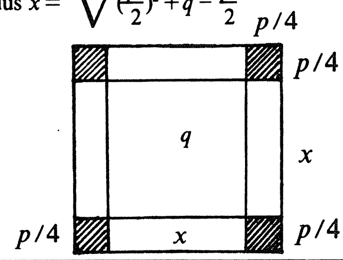
De Babylonische wiskunde was in dezelfde periode al aanzienlijk verder ontwikkeld. Een algemeen procedé voor het oplossen van vierkants-vergelijkingen, waarover de Egyptenaren nog niet beschikten, was er bekend en hiermee werden al ingewikkelde problemen opgelost. Tekst twee geeft bijvoorbeeld een stelsel vergelijkingen met twee onbekenden, dat te herleiden is tot een vierkantsvergelijking. Het hier niet weergegeven vervolg van de tekst geeft een correcte oplossing.

2 	Lengte, breedte. Lengte en breedte heb ik vermenigvuldigd en zo het oppervlak gevormd. Verder heb ik het overschot van de lengte en de breedte bij het oppervlak opgeteld: 3,3 (3,3 is zestigtallig en komt overeen met 3.60 + 3 = 183 tientallig). Verder heb ik de lengte en breedte opgeteld: 27. Gevraagd: lengte, breedte en oppervlak.
vertaling via het Duits; Van der Waerden 1950, 71 reproduktie op p. 72	parafrase: lengte$=x$; breedte$=y$ $xy+(x-y)=183$ $x+y=27$

Bij de Grieken (ca. 600 voor Chr. - 600 na Chr.) komen vergelijkingen in twee vormen voor: in een meetkundige, gebaseerd op de *Elementen* van Euclides (ca. 300 voor Chr.) en in een rekenkundige, gebaseerd op de *Arithmetica* van Diophantos (ca. 250 na Chr.).

De Griekse wetenschap werd met toevoeging van nieuwe elementen (b.v. uit India) opgenomen in de Arabische cultuur (ca. 800 - 1450). Griekse werken werden in het Arabisch vertaald, maar al spoedig volgden ook originele bijdragen. Vergelijkingen werden rond 830 uitgebreid behandeld door Al-Khwārizmī in zijn *Ḫisab al-gabr wa-l-muqābala,* dat in de twaalfde eeuw in het Latijn vertaald werd en zo grote invloed kreeg in West-Europa. Deze Latijnse vertalingen gaven de naam van de auteur weer als 'Algorismus' en namen 'al-gabr' onvertaald over als 'algebra'; woorden die ons nog steeds bekend in de oren klinken. De *Algebra* van Al-Khwārizmī behandelt onder meer systematisch de vierkantsvergelijking en de voorbeelden die erin voorkomen zijn de standaardvoorbeelden geworden van latere West-Europese auteurs. Een voorbeeld is de vergelijking $x^2+10x=39$ uit de derde tekst (zie pagina 3). Ze komt al voor in 1202, dus kort na de eerste vertalingen, in het *Liber abaci* (Boek over de abacus) van Leonardo van Pisa (= Fibonacci).

We slaan nu een aantal schakels over en bespreken de verspreiding van de algebra over West-Europa, die in een later stadium nog gestimuleerd werd

3 فاما الموال والجذور التي تعدل العدد فمثل قولك مال وعشرة اجذاره يعدل تسعة وثلثين درهما ومعناه اي مال اذا زدت عليه مثل عشرة اجذار بلغ ذلك كله تسعة وثلثين * فقياسه ان تنصف الاجذار وهي في هذه المسئله خمسة فتضربها في مثلها فيكون خمسة و عشرين فتزيدها علي التسعة والثلثين فيكون اربعة وستين فتاخذ جذره وهو ثمانية فتنقص منه نصف الاجذار وهو خمسة فيبقي ثلثة وهو جذر المال الذي تريد و كذلك لو ذكرمالين او ثلثة او اقل او اكثر	Een macht en wortels gelijk aan een getal, zoals bijvoorbeeld: Een macht en tien wortels zijn gelijk aan negenendertig drachmen (de munt drachme is hier de rekeneenheid), hetgeen het volgende inhoudt: de macht waaraan we tien maal zijn wortel toevoegen, geeft een totaal van negenendertig. De regel is de helft van het aantal wortels te nemen, hetgeen in dit probleem vijf is. Vermenigvuldigd met zichzelf geven ze vijfentwintig. Door hier negenendertig bij op te tellen krijgen we vierenzestig. Hiervan nemen we de wortel, ofwel acht. Vervolgens nemen we van dit resultaat vijf weg. Er blijft drie over, en dit is de wortel van de macht. En de macht is negen.
vertaling via het Latijn van Gerard van Cremona en het Frans van Dedron; Itard 1959, 324-325. reproduktie: Rosen 1831, Arabische tekst p. 5. Met dank aan J.P. Hogendijk voor het verstrekken van de reproduktie en het controleren van de vertaling.	parafrase: $x^2 + px = q$ voor $p = 10$, $q = 39$ $(x + \frac{p}{2})^2 = q + 4 \cdot (\frac{p}{4})^2 = q + (\frac{p}{2})^2$ dus $x = \sqrt{(\frac{p}{2})^2 + q} - \frac{p}{2}$ 

door de boekdrukkunst, hier verder niet. Ze ging zeer snel en gesteld mag worden dat algebra in de culturele centra rond 1500 een goed ontwikkelde en populaire discipline was, waarvan het oplossen van eerste- en tweedegraads vergelijkingen een hoeksteen was.

2. Negatieve getallen

In zekere zin kwamen negatieve getallen al vrij vroeg voor. De Babyloniërs gebruikten ze reeds in astronomische tafels, maar teksten waarin ze er ook mee rekenden, zijn niet bekend. Diophantos realiseerde zich dat ze er waren, maar koos bewust de coëfficiënten van zijn vergelijkingen zo dat er geen negatieve oplossingen ontstonden, want die vond hij onmogelijk en ongepast.

De Indiërs werkten er met minder aversie mee, getuige het werk van Brahmagupta (7de eeuw na Chr.) en Mahāvīra (9de eeuw na Chr.), die zelfs opmerkte:

4
Het ligt in de aard van de zaak dat een negatieve grootheid geen kwadraat is, en dus geen vierkantswortel heeft.
vertaling via Engels en Duits; Tropfke 1980, 145.

De Arabieren accepteerden geen negatieve oplossingen van vergelijkingen, maar moeten het bestaan ervan wel ingezien hebben. Al-Khwārizmī, bij wie duidelijke Indische invloeden aan te wijzen zijn, geeft bijvoorbeeld ergens als criterium voor het bestaan van een oplossing van een vierkantsvergelijking het positief zijn van (wat wij nu zouden noemen) de discriminant.

Incidenteel waren ook in West-Europa in of voor de 9de eeuw al negatieve getallen voorgekomen, maar de definitieve aanvaarding voor het gebruik in berekeningen vond plaats vanaf de 13de eeuw in Italië. Handel en bankwezen waren daar in opkomst en negatieve getallen hadden grote practische waarde voor het boekhouden. In het *Liber abaci* van Leonardo van Pisa (1202) kwam voor het eerst een negatieve oplossing van een vergelijking voor en geleidelijk werden ze vanaf die tijd in berekeningen ingevoerd. Sporen van bedenkingen bleven echter zichtbaar. Tot in de 16de eeuw bleef men over negatieve getallen spreken als 'numeri ficti' (verzonnen getallen) en zelfs de bepaald niet behoudende Descartes sloot in de 17de eeuw nog negatieve oplossingen van vergelijkingen uit en bestempelde ze als 'racines fausses'.

3. De derdegraads vergelijking in Italië rond 1550

De Arabieren hadden reeds uitgebreide pogingen ondernomen om de algemene derdegraads vergelijking op te lossen en waren daarin geslaagd door het snijden van kegelsneden. Een neerslag van dit onderzoek is te vinden in de *Algebra* van Omar Khayyam (ca. 1050 - 1122). Zijn oplossing komt, in moderne terminologie geformuleerd en sterk samengevat, op het volgende neer. Gegeven de vergelijking $x^3+ax^2+bx+c=0$. Substitutie van $x^2=2py$ in de vergelijking geeft $x\cdot 2py+a\cdot 2py+bx+c=0$, zodat (x,y) zowel op de kromme

$x^2 = 2py$ (een parabool) als op de kromme $2pxy + 2apy + bx + c = 0$ (een hyperbool) ligt. Oplossingen van de gegeven vergelijking zijn dus te vinden als de x-coördinaten van de snijpunten van de parabool en de hyperbool.

Omar Khayyam kon bovendien sommige derdegraads vergelijkingen langs rekenkundige weg oplossen, maar dacht dat dit voor het algemene geval onmogelijk zou zijn. Dit was ook de mening van Luca Pacioli (1445 - 1514). Zijn *Summa de arithmetica,* ... uit 1494 gaf een opsomming (zoals de titel al zegt) van de vorderingen op algebraïsch gebied. Het was het eerste gedrukte algebraboek en kreeg grote invloed. Maar al eerder, bijvoorbeeld door de uitvinding van de boekdrukkunst en de ontdekking van Amerika, was gebleken dat de 'ouden' op wie Pacioli zich beriep, niet alles kenden en konden, zodat Pacioli's mening tevens een uitdaging inhield.

Het eerste wat opgemerkt werd, was (modern geformuleerd) dat de vergelijking

$$x^3 + ax^2 + bx + c = 0$$

door de transformatie $\xi = x + \frac{a}{3}$ overgaat in

$$\xi^3 - a\xi^2 + \frac{a^2}{3}\xi - \frac{a^3}{27} + a\xi^2 - \frac{2}{3}a^2\xi + \frac{a^3}{9} + b\xi - \frac{ab}{3} + c = 0$$

zodat een vergelijking overblijft van de vorm

$$\xi^3 + d\xi + e = 0$$

waarin ξ^2 niet meer voorkomt. Op grond daarvan was het dus voldoende te zoeken naar oplossingen van de volgende drie typen vergelijkingen:

$$x^3 + px = q$$

$$x^3 = px + q$$

$$x^3 + q = px.$$

De notatie met p en q is anachronistisch: in alle gevallen werden voorbeelden gegeven met op de plaats van p en q positieve getallen. Dat men de coëfficiënten positief koos verklaart de noodzaak om drie verschillende typen te bestuderen. Eigenlijk hadden het er vier kunnen zijn, maar het type $x^3 + px + q = 0$ ontbrak, hoewel zoals we zagen negatieve wortels niet meer principieel uitgesloten waren.

Het verhaal van de uiteindelijke oplossing is bekend, maar te fraai om niet kort de revue te passeren. We zullen ons daarbij beperken tot het type $x^3 = px + q$. Omstreeks 1506 vond Scipione dal Ferro (ca. 1465 - 1526), hoogleraar te Bologna, een oplossing. Hij publiceerde zijn vondst niet, maar sprak er wel over en liet ook papieren na. Zo werd na zijn dood de oplossing bekend, of althans het feit dat er een oplossing gevonden was. De Italiaanse rekenmeesters daagden elkaar, om verzekerd te zijn van leerlingen en dus van inkomsten, van tijd tot tijd uit om problemen op te lossen. Zo werd aan Niccolo Tartaglia (ca. 1500 - 1557) een aantal derdegraads vergelijkingen opgegeven. Deze had, volgens zijn eigen woorden, bij geruchte vernomen dat er een oplossing mogelijk was en vond daardoor geïnspireerd in 1534 een eigen methode. Kort daarna deelde hij de oplossingen van de gestelde problemen mee zonder echter de methode te onthullen. Toen Girolamo Cardano (1501 - 1576), arts, astroloog, gokker en wiskundige te Milaan, het succes van Tartaglia vernam, vroeg hij hem met zijn methode voor de dag te komen en Tartaglia stemde hierin toe tijdens een ontmoeting in Milaan, maart 1539, onder de uitdrukkelijke voorwaarde van geheimhouding. In 1545 verscheen echter Cardano's *Ars Magna* mèt daarin de oplossing van de derdegraads vergelijking. Cardano had namelijk in de tussentijd ontdekt dat dal Ferro al lang voor Tartaglia een oplossing gevonden had en voelde zich daardoor gerechtigd de aan Tartaglia beloofde geheimhouding te breken en diens (of dal Ferro's?) oplossing te publiceren. De betreffende oplossing wordt naar Cardano genoemd en niet naar de eerlijke vinder(s).

'Cardano's' oplossing van het type $x^3 = px + q$ verloopt als volgt. Stel $x = u + v$ met $uv = \frac{1}{3}p$. Substitutie in de vergelijking geeft

$$u^3 + 3uv(u+v) + v^3 = p(u+v) + q = 3uv(u+v) + q$$

ofwel u en v voldoen aan het stelsel

$$\begin{cases} u^3 + v^3 = q \\ uv = \frac{1}{3}p \end{cases} \Leftrightarrow \begin{cases} u^3 + v^3 = q \\ u^3 v^3 = (\frac{p}{3})^3. \end{cases}$$

Dit geeft de volgende vierkantsvergelijking voor u^3:

$$(u^3)^2 - qu^3 + (\frac{p}{3})^3 = 0$$

zodat:

$$u^3 = \frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3} \text{ en } v^3 = \frac{q}{2} - \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}$$

(of omgekeerd), waaruit:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}.$$

Dit gaat probleemloos als $(\frac{q}{2})^2 - (\frac{p}{3})^3$ positief is. De problemen ontstonden bij vergelijkingen waarvoor $(\frac{q}{2})^2 - (\frac{p}{3})^3$ negatief was, de zogenaamde 'casus irreducibilis'.

4. DE 'CASUS IRREDUCIBILIS'

Reeds enkele maanden nadat Cardano op de hoogte was gekomen van Tartaglia's methode, vroeg hij Tartaglia bij herhaling wat hij in het geval 'cubo eguale a cose e numero' (d.w.z. het type $x^3 = px + q$) doen moest als $(\frac{q}{2})^2 - (\frac{p}{3})^3$ negatief was. De 'casus irreducibeles' als onoplosbaar verwerpen voldeed niet, want het was duidelijk dat er in dat geval toch oplossingen konden zijn ($x^3 = 15x + 4$ heeft duidelijk $x = 4$ als oplossing terwijl toch $(\frac{q}{2})^2 - (\frac{p}{3})^3 = -121$). Tartaglia antwoordde dat hij er wel een verklaring voor had en dat het alleen zo was dat Cardano er niets van begreep. In de *Ars Magna* omzeilde Cardano de 'casus irreducibilis' door de coëfficiënten geschikt te kiezen en na de publikatie van de *Ars Magna* besloot de teleurgestelde Tartaglia zijn plan om ook een werk over algebra te schrijven te laten varen; zijn grootste ontdekking was hem toch al afgesnoept. Het probleem bleef dus open.

De oplossing kwam uiteindelijk van Rafael Bombelli (1526 - 1572), een ingenieur uit Bologna, die zich realiseerde dat met vierkantswortels uit negatieve getallen op zo'n manier te rekenen was dat de formule van 'Cardano' ook op de 'casus irreducibilis' toegepast kan worden.

Een van de voorbeelden die hij behandelde was de vergelijking $x^3 = 15x + 4$, in zijn eigen notatie ' $1.^{\underset{\smile}{3}}$ Eguale à $15.^{\underset{\smile}{1}}$ p. 4', waarvan de oplossing $x = 4$ zo te zien was. De formule gaf:

$$x = \sqrt[3]{(\frac{4}{2}) + \sqrt{(\frac{4}{2})^2 - (\frac{15}{3})^3}} + \sqrt[3]{(\frac{4}{2}) - \sqrt{(\frac{4}{2})^2 - (\frac{15}{3})^3}}$$
$$= \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}\,.$$

Bombelli begon met het invoeren van een notatie voor vierkantswortels uit negatieve getallen, die gebaseerd was op de gebruikelijke Italiaanse notaties voor 'plus' en 'min', namelijk 'più' en 'meno', meestal afgekort tot '*p.*' en '*m.*'. Zo schreef hij 'più di meno' of kortweg '*p.* di *m.*' voor $\sqrt{-1}$ en 'meno di meno' of '*m.* di *m.*' voor $-\sqrt{-1}$; $2\sqrt{-1}$ werd '*p.* di *m.* 2' en $-1-\sqrt{-1}$ '*m.* di *m.* 1 *m.* 1' (eigenlijk dus $-\sqrt{-1}-1$!). Vervolgens leidde Bombelli een groot aantal van de nog steeds gebruikelijke rekenregels af voor het rekenen met de 'quantitates sophisticae', de vierkantswortels uit negatieve getallen. Bovendien ontdekte hij dat deze getallen bij het oplossen van vergelijkingen voorkwamen in paren (geconjugeerde oplossingen zoals we tegenwoordig zouden zeggen). Met dit alles was hij in staat $\sqrt[3]{2+\sqrt{-121}}$ (waarvoor hij zelf iets geschreven zou hebben als '$R^3\lfloor 2p.R\lfloor 0m.121\rfloor\rfloor$') en $\sqrt[3]{2-\sqrt{-121}}$ in de vorm $a + b\sqrt{-1}$ te brengen. Eerst merkte hij op dat $\sqrt{-121} = 11\sqrt{-1}$ en daarna dat $\sqrt[3]{2+11\sqrt{-1}} = 2+\sqrt{-1}$ en $\sqrt[3]{2-11\sqrt{-1}} = 2-\sqrt{-1}$, zodat de methode van 'Cardano' ook voor de vergelijking $x^3 = 15x + 4$ de verwachte oplossing gaf:

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

$$= (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4.$$

Moraal: de 'quantitates sophisticae' konden afgewezen worden tot het moment dat ze nodig waren om de algemene geldigheid van 'Cardano's' oplossingsmethode te handhaven.

Toch was de in 1572 verschenen en in 1579 herdrukte *Algebra* van Bombelli niet het eerste werk waarin met 'quantitates sophisticae' gerekend werd, want Cardano had dat al gedaan in de *Ars Magna* (1545). Daarin komt het volgende probleem voor: 'Lijn *ab*, die wij 10 zullen noemen, moet verdeeld worden in twee delen, waarvan de rechthoek 40 moet bedragen'. Hij zegt: 'imaginaberis ℞ *m*:15' (men moet zich $\sqrt{-15}$ inbeelden), dan zijn de gevraagde getallen: $5+\sqrt{-15}$ en $-\sqrt{-15}$ want

5 ⌋ duc 5*p*:℞ *m*:15 in 5*m*:℞ *m*:15, dimissis incruciationibus, fit 25 *m*:*m*:15, quod est *p*:15, igitur hoc productum est 40. *Ars Magna* p. 66, gereproduceerd in Struik 1969, 68. Vertaling, Vooys 1959/60, 163.	Vermenigvuldig $5+\sqrt{-15}$ met $5-\sqrt{-15}$ dat wordt met weglating van de kruisprodukten: $25--15$, dat is $+15$; dus dit produkt is 40.

Wieleitner (1927, p.77) vermoedt dat de ideeën achter dit stukje uit de *Ars Magna* wederom niet van Cardano zelf afkomstig waren. Hij merkt op dat Cardano in 1543 in Bologna (de woonplaats van Bombelli!) was en daar verkeerde in kringen van wiskundigen die sterke belangstelling hadden voor de derdegraads vergelijking. Het is mogelijk dat de 'quantitates sophisticae' daar al gebruikt werden en dat Cardano (en wellicht ook Bombelli) zo aan het idee gekomen is. Bovendien is Bombelli's *Algebra* weliswaar pas in 1572 verschenen, maar het bewaard gebleven handschrift is van veel vroeger datum (rond 1550).

In elk geval was de situatie aan het einde van de 16de eeuw zo dat vierkantswortels uit negatieve getallen ingevoerd waren, dat er een notatie voor was, dat er een beperkt aantal rekenregels voor gevonden was, en dat ze toepasbaar waren bij het oplossen van vergelijkingen, het gebied waarin ze ontstaan waren.

Daarbij komt nog dat Bombelli's *Algebra* niet onopgemerkt bleef, zoals we hieronder zullen zien.

5. De eerste reacties

In latere werken is Cardano nog uitgebreid teruggekomen op Bombelli's wijze van invoeren van de 'quantitates sophisticae' (de complexe getallen avant la lettre die we voor het gemak hierna maar zonder meer met complexe getallen zullen aanduiden), maar hij bleef zeer onzeker. In zijn *Sermo de plus et minus*, ontstaan tussen de publikatie van Bombelli's *Algebra* in 1572 en Cardano's dood in 1576, signaleerde Cardano paradoxen die hij maar moeilijk kon verklaren. Zo verbaasde het hem dat een getal als 2*p.* di *m.* 1, waar het positieve deel (2) groter is dan het 'negatieve' ('*p.* di *m.* 1' $=\sqrt{-1}$) als kwadraat 3*p.* di *m.* 4 heeft, waarin het 'negatieve' deel het grootst is. Simon Stevin (1548-1620), die *De Regula Aliza* gelezen had waarin Cardano in 1570 de complexe getallen aarzelend aanvaardde, en die ook de *Algebra* van Bombelli uitgebreid bestudeerd had (getuige het feit dat hij er de notatie voor exponenten aan ontleende), wees in zijn *L'Arithmetique* (1585) complexe getallen af. De toepassing ervan op de 'casus irreducibilis' overtuigde hem geenszins, want ze leverde geen systematische methode voor het vinden van de oplossing. Het was eerder omgekeerd: wanneer je eenmaal de oplossing $x=4$ van de vergelijking $x^3=15x+4$ had, kon voor een uitdrukking als $\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}}$ een interpretatie gevonden worden. Stevin verlangde, zoals Dijksterhuis zei, 'een vasten regel en geen medewerking van het toeval'.

Ook François Viète (of, in het Latijn, Vieta; 1540 - 1603), die toch door de invoering van letters als symbolen voor getallen en door andere bijdragen een belangrijke vernieuwer van de algebra was, verwierp complexe getallen volkomen. Hij werkte, hoewel hij bij voorbeeld de *Ars Magna* kende, zelfs niet met negatieve getallen. Voor de derdegraads vergelijking ontwikkelde hij een totaal nieuwe oplossingsmethode. Bij de 'casus irreducibilis' had hij een ingenieuze goniometrische substitutie nodig om het optreden van wortels uit negatieve getallen te vermijden (zie bij voorbeeld Boyer 1968, 341). Blijkbaar was Viète er veel aan gelegen om niet tot het gebruik van complexe getallen te hoeven overgaan.

Tot een duidelijk van Stevin en Viète afwijkende stellingname kwam Albert Girard (1595 - 1632). Girard, geboren in Frankrijk, vestigde zich rond 1614 in de Nederlanden, aanvankelijk als luitslager in Amsterdam, enige jaren later als student in Leiden. Girard was goed op de hoogte van de recente wiskundige ontwikkelingen. Hij kende het werk van Bombelli, Cardano, Stevin en Viète, nam daaruit nieuwe methoden en notaties over en gaf zelfs in 1625 de *Arithmetique* en in 1634, postuum gepubliceerd, *Les oeuvres mathématiques* van Stevin uit. Naast goniometrische tabellen en edities van werk van andere auteurs verscheen van Girards hand in 1629 *Invention nouvelle en l'algèbre*.

Hierin behandelde hij het oplossen van (voornamelijk derdegraads) vergelijkingen en als eerste gaf hij erin de stelling (later de hoofdstelling van de algebra genoemd) dat elke algebraïsche vergelijking evenveel oplossingen heeft als haar graad:

6
Toutes les equations d'algebre reçoivent autant de solutions, que la denomination de la plus haute quantite le demonstre ....
tekst: Girard, *Invention Nouvelle*, Heruitgave p. 127-28.

Het tweede deel van de stelling geeft het (voor een deel al aan Viète bekende) verband tussen de coëfficiënten van een vergelijking en de symmetrische functies van de optredende wortels.

Het is duidelijk dat Girard hiermee verder ging dan Bombelli, aangezien hij niet alleen voor de 'casus irreducibilis', maar in het algemeen complexe oplossingen van de vergelijkingen moest toelaten. Hij deed dat expliciet door namelijk op te merken dat er drie soorten oplossingen zijn: positieve, negatieve en 'omhulde'.

7
Ainsi qu'on peut donner trois noms aux solutions, veu qu'il y en a qui sont plus que rien; d'autres moins que rien; & d'autres envelopées, comme celles qui ont des $\sqrt{-}$, comme des $\sqrt{-3}$, ou autres nombres semblabes.
tekst: Girard, *Invention nouvelle*, heruitgave p.130.

Overigens bevat de *Invention nouvelle* bijna geen plaatsen waar ook daadwerkelijk met complexe getallen gerekend wordt. Er komt slechts één vergelijking in voor met complexe wortels.

Girards stelling (tekst 6) vinden we terug in de *Géométrie* (1637) van René Descartes (1596 - 1650), de Franse filosoof die vanwege het liberale klimaat evenals Girard in de Nederlanden werkzaam was, van 1628 tot een jaar voor zijn dood. De *Géométrie* wordt algemeen beschouwd als een mijlpaal in de ontwikkeling van de wiskunde omdat erin voor het eerst systematisch een verband tussen algebra (= het oplossen van vergelijkingen) en meetkunde (= het construeren van figuren) gelegd werd. Descartes formuleerde de 'hoofdstelling' als volgt:

8 |

Combien il peut y auoir de racines en chasq; Equatiõ.

Scachés donc qu'en chasque Equation, autant que la quantité inconnue a de dimensions, autant peut il y auoir de diuerses racines, c'est a dire de valeurs de cete quantité.

Géométrie, 372. Uit: Smith; Latham 1954.

Even verderop in de *Géométrie* vinden we de volgende overweging. De positieve of ware wortels ('vrayes racines') en de negatieve of valse wortels ('fausses racines') zijn niet altijd reëel maar soms slechts denkbeeldig ('imaginaires'). Als je dat aanneemt kun je je van een vergelijking altijd het aangegeven aantal wortels voorstellen, namelijk even veel als de graad van de vergelijking, alleen correspondeert er niet altijd met elk van deze wortels een grootheid. In Descartes' woorden:

9 |

Que les racines, tant vrayes que fausses peuuent estre reelles ou imaginaires.

Au reste tant les vrayes racines que les fausses ne sont pas tousiours reelles; mais quelquefois seulement imaginaires; c'est a dire qu'on peut bien tousiours en imaginer autant que iay dit en chasque Equation; mais qu'il n'y a quelquefois aucune quantité, qui corresponde a celles qu'on imagine.

Géométrie, 380. Uit: Smith; Latham 1954.

Grootheden waren voor Descartes lijnstukken en getallen. De imaginaire wortels waren voor hem dus slechts gedachtenconstructies, nodig vanwege de algemeenheid van de stelling; ze werden echter niet als realiteit (grootheid) aanvaard. Descartes heeft er dan ook nergens mee gerekend. Omdat hij zelden meedeelde wat zijn bronnen waren, blijft onduidelijk in hoeverre hij zich baseerde op voorgangers. Cardano wordt wel genoemd, maar het ligt voor de hand dat Descartes ook het werk van Bombelli en Girard kende. Hij zette vergeleken met deze twee een stap terug, maar zijn term 'imaginair', die overigens terugging tot Cardano, kreeg een vaste plaats in de wiskundige terminologie.

Samenvattend: de eerste reacties liepen uiteen van afwijzing tot voorzichtige acceptatie. In de tweede helft van de 17de eeuw namen de bezwaren tegen het werken met complexe getallen weliswaar geleidelijk af, maar de status quo werd pas doorbroken door de nieuwe problemen waarop men in het begin van de 18de eeuw stuitte. We laten daarom de bespreking van de 17de eeuwse bijdragen verder hierbij. Een uitzondering vormt het zoeken naar een meetkundige representatie door Wallis (1673); dit thema komt in een aparte paragraaf aan de orde.

6. ENTREACT

Aan het begin van de 18de eeuw lag een duidelijk breekpunt in de geschiedenis van de complexe getallen. Nieuwe problemen en toepassingen, waarover hieronder meer, leidden tot vele activiteiten en evenzovele publikaties. Dat betekent ook dat het niet meer mogelijk is om alle ontwikkelingen op de voet te volgen. Van de onderzoekingen naar de hoofdstelling van de algebra zal bijvoorbeeld nagenoeg niets meer aan de orde komen. De volgende 'bedrijven' moeten dan ook eerder gezien worden als een selectie van (lang niet alle) hoogtepunten dan als een doorlopend verhaal zoals de vorige 'bedrijven'.

7. NIEUWE PROBLEMEN

Samen met de fundering van de analytische meetkunde door Descartes was de uitvinding van de differentiaal- en integraalrekening door Newton en Leibniz (in de periode 1670 - 1680) de belangrijkste gebeurtenis in de wiskunde van de 17de eeuw. Uit deze gebieden kwamen belangrijke impulsen voort voor de bestudering van de complexe getallen. In 1702 merkte Johann Bernoulli (1667-1748) als eerste op dat gebroken rationale functies integreerbaar zijn met behulp van breuksplitsing. Zijn eerste voorbeeld was

$$\frac{a^2}{a^2-x^2}=\frac{a}{2}\left(\frac{1}{a+x}+\frac{1}{a-x}\right);$$

omdat bekend was dat $d(\ln x)=\frac{dx}{x}$ kon de integratie uitgevoerd worden. Ook Gottfried Wilhelm Leibniz (1646 - 1716) vond in 1702, onafhankelijk van Bernoulli, de methode van breuksplitsing en paste die zonder voorbehoud toe op

$$\int\frac{dx}{ax^2+bx+c}.$$

Dat lineaire factoren van de noemer complexe coëfficiënten zouden kunnen hebben vonden Bernoulli en Leibniz aanvankelijk geen bezwaar.

Leibniz was overigens al geruime tijd geïntrigeerd door de complexe getallen, die in zijn ogen als het ware amfibieën waren tussen 'Ens et non-Ens'. Een van de eerste wiskundeboeken die Leibniz bestudeerde (in 1675) was Bombelli's *Algebra.* Hij had er nogal wat bezwaren tegen: 'Mais il ne s'ensuit pas que l'opération par son piu di meno est bonne' (in een brief uit 1675 aan Huygens).

Bernoulli meende bovendien dat, wanneer je alleen reële coëfficiënten in de factoren wilde toelaten, altijd nog een breuksplitsing mogelijk was met lineaire en kwadratische factoren. Dat was van belang, want men wist dat in dat geval voor de integratie niet meer soorten transcendente functies nodig waren dan goniometrische en logaritmische. Leibniz bracht daar tegen in dat $x^4+a^4=(x+a\sqrt{\sqrt{-1}})(x-a\sqrt{\sqrt{-1}})(x+a\sqrt{-\sqrt{-1}})(x-a\sqrt{-\sqrt{-1}})$

terwijl volgens hem geen enkel tweetal van de vier factoren van het rechterlid een produkt had met reële coëfficiënten. Dat hij zich vergiste, klaarblijkelijk omdat hij niet zag dat zowel $\sqrt{\sqrt{-1}}$ als $\sqrt{-\sqrt{-1}}$ te schrijven waren als $p+q\sqrt{-1}$, werd duidelijk in 1719 toen de volgende ontbinding gepubliceerd werd:

$$x^4+a^4=(a^2+x^2)^2-2a^2x^2=(a^2+x^2-ax\sqrt{2})(a^2+x^2+ax\sqrt{2}).$$

De verwarring werd er niet minder door.

Problemen ontstonden ook bij integraties zoals $\int\frac{dx}{x+a}$ voor complexe a. Dat gaf namelijk $\ln(x+a)$ als primitieve en daarmee kwam de vraag op naar de interpretatie van logaritmen van complexe getallen. Ook de logaritmen van negatieve getallen werden in de discussies tussen Leibniz en Johann Bernoulli (1712 - 1713) en tussen Euler en Johann Bernoulli (1727 - 1731) betrokken.

8. Euler

Er was eigenlijk geen onderdeel van de wiskunde van zijn tijd waarmee Leonhard Euler (1707 - 1783) zich niet bezighield en sterker nog: ongeveer op alle terreinen deed hij baanbrekend werk. De geschiedenis van de complexe getallen bevestigt dit beeld. Van Eulers werk worden enkele stukken besproken: zijn theorie over de logaritmen van negatieve en complexe getallen, de stelling van de Moivre waarvan de huidige gedaante van Euler afkomstig is en de plaats waar hij de notatie i invoert.

8.1 De logaritmen van negatieve en complexe getallen

Zoals gezegd hield de status van de logaritmen van negatieve en complexe getallen Euler al in de periode 1727 - 1731 bezig. In deze periode had hij echter nog geen duidelijk standpunt ingenomen. In 1747 kwam het onderwerp weer op, dit keer in Eulers correspondentie met d'Alembert, en in deze brieven ontwikkelde Euler zijn uiteindelijke theorie, die d'Alembert overigens niet kon overtuigen.

In een artikel uit 1749 (Euler 1749) werkte Euler aan de hand van de 'controverse entre Mrs. Leibniz et Bernoulli' zijn theorie verder uit. Na eerst de standpunten van de twee opponenten besproken te hebben, liet hij zien dat beide standpunten onhoudbaar waren en daarop liet hij zijn eigen 'ontknoping' volgen:

10 |
Theorème. Il y a toujours une infinité de logarithmes qui conviennent également à chaque nombre proposé; ou, si y marque le logarithme de x, je dis que y renferme une infinité de valeurs differentes.
Euler 1749; *Opera Omnia* (1) 17, 210.

Het (in onze ogen niet strenge) argument hiervoor volgt nu. Gegeven x en y zodat $y = \ln x$. Euler kiest als definitie van de natuurlijke logaritme: $\ln x$ is de logaritme $\log x$ waarvoor geldt

$$\log(1+\omega) = \omega \text{ voor een oneindig klein getal } \omega.$$

Wij zouden zeggen : $\ln x$ is die logaritmische functie ${}^g\log x$ waarvoor geldt

$$\lim_{x \to 0} \frac{{}^g\log(1+x)}{x} = 1$$

maar bij Euler zijn 'oneindig klein' en 'oneindig groot' gewoon getallen waarmee, mits voorzichtig, gerekend kan worden. Uit $\ln(1+\omega) = \omega$ volgt $\ln(1+\omega)^n = n\omega$. Laat n een oneindig groot getal zijn zodat $(1+\omega)^n = x$, dan geldt

$$y = \ln x = \ln(1+\omega)^n = n\omega.$$

Druk nu y in x uit: $(1+\omega)^n = x$, dus $1+\omega = x^{1/n}$ en $\omega = x^{1/n} - 1$ zodat $y = n\omega = n(x^{1/n} - 1)$. En omdat voor Euler $x^{1/n}$ elk van de oplossingen van $(1+\omega)^n = x$ kan zijn en n oneindig groot is, zegt Euler dat $x^{1/n}$ oneindig veel verschillende waarden heeft, zodat ook $n(x^{1/n} - 1) = y = \ln x$ oneindig veel waarden heeft. □

Hoe past Euler dit nu toe op de logaritme van een complex getal ? Hij zegt: elke 'quantité imaginaire, quelque compliquée qu'elle soit' is te schrijven als $a + b\sqrt{-1}$. Stel

$$\sqrt{a^2 + b^2} = c$$

en bepaal met de tafel ϕ zo dat

$$\frac{a}{\sqrt{a^2+b^2}} = \cos\phi \quad \text{en} \quad \frac{b}{\sqrt{a^2+b^2}} = \sin\phi,$$

dan heb je

$$x = a + b\sqrt{-1} = c(\cos\phi + \sqrt{-1}\sin\phi).$$

Dan bewijst hij (met een argument dat hier te ver zou voeren) dat

$$\ln(\cos\phi + \sqrt{-1}\sin\phi)$$

de waarden

$$(\phi + k.2\pi)\sqrt{-1} \quad (k \text{ geheel})$$

kan hebben en dus heeft

$$\ln x = \ln c + \ln(\cos\phi + \sqrt{-1}\sin\phi) \text{ oneindig veel waarden.} \quad \square$$

Het artikel bevat nog een aantal bekende resultaten. Een van de waarden van $\ln(\cos\phi + \sqrt{-1}\sin\phi)$ is $\phi\sqrt{-1}$; dit houdt in dat

$$\cos\phi + \sqrt{-1}\sin\phi = e^{\phi\sqrt{-1}}$$

en elk complex getal is dus te schrijven als

$$f+g\sqrt{-1} = \sqrt{f^2+g^2}(\cos\phi + \sqrt{-1}\,\sin\phi) = \sqrt{f^2+g^2}\,e^{\phi\sqrt{-1}}.$$

Daarmee was niet alleen de vraag naar de status van de logaritme van een complex getal beantwoord, maar ook de vraag welke status e^x heeft voor complexe x. Want

$$e^x = e^{f+g\sqrt{-1}} = e^f \cdot e^{g\sqrt{-1}} = e^f(\cos g + \sqrt{-1}\,\sin g) \qquad (*)$$

zodat e^x weer van vorm $a+\sqrt{-1}$ is. Dit laatste bewijst Euler ook voor x^y als x en y beide complex zijn.

Voor $x=\pi\sqrt{-1}$ geeft (*) bovendien Eulers beroemde identiteit

$$e^{\pi\sqrt{-1}} = -1$$

die in de vorm

$$e^{\pi \cdot i} + 1 = 0$$

de meest fundamentele getallen, operaties en de belangrijkste relatie bijeen brengt. In het artikel zelf komt de identiteit overigens alleen impliciet voor: in de vorm (*) en in de vorm

$$\ln(-1) = \pm\pi\sqrt{-1}.$$

Dat ook $\cos x$ en $\sin x$ voor complexe x weer te schrijven zijn als $a+b\sqrt{-1}$ volgt nu direct uit de door Euler in 1740 ontdekte identiteiten

$$\cos x = \frac{e^{x\sqrt{-1}} + e^{-x\sqrt{-1}}}{2} \quad \text{en} \quad \sin x = \frac{e^{x\sqrt{-1}} - e^{-x\sqrt{-1}}}{2\sqrt{-1}}.$$

Op deze wijze gaf Euler de eerste grote uitbreiding aan de theorie van de complexe getallen sinds de invoering ervan door Bombelli.

8.2 De stelling van de Moivre

Reeds in 1707 had Abraham de Moivre (1667 - 1754) een equivalent van de naar hem genoemde stelling

$$(\cos\phi + \sqrt{-1}\,\sin\phi)^n = \cos n\phi + \sqrt{-1}\,\sin n\phi$$

gevonden. Euler kende de publikaties waarin deze stelling voorkwam (die we hier verder niet zullen bespreken; zie daarover Schneider 1968/69) en gaf de stelling de thans gebruikelijke vorm. Hij gaf er een bewijs van in zijn beroemde leerboek *Introductio in analysin infinitorum* (1748):

$$\begin{aligned}&(\cos z + \sqrt{-1}\,\sin z)(\cos y + \sqrt{-1}\,\sin y)\\ &= \cos y\cos z - \sin y \sin z + \sqrt{-1}(\cos y\sin z + \sin y\cos z)\\ &= \cos(y+z) + \sqrt{-1}\,\sin(y+z).\end{aligned}$$

De stelling volgt dan met inductie uit het bovenstaande:

11	
133. Hinc itaque ſequitur fore $(\cos. z \pm \sqrt{-1}.\sin z)^2 = \cos. 2z \pm \sqrt{-1}.\sin. 2z$, & $(\cos. z \pm \sqrt{-1}.\sin. z)^3 = \cos. 3z \pm \sqrt{-1}.\sin. 3z$. ideoque generaliter erit $(\cos. z \pm \sqrt{-1}.\sin. z)^n = \cos. nz \pm \sqrt{-1}.\sin. nz$:	
Euler 1748, deel 1, 98; *Opera Omnia* (1) 8, 140.	Hieruit volgt dus dat zal gelden ..... en dus zal het algemeen waar zijn dat .....

8.3 i

Eulers werk heeft grote invloed gehad op het tot stand komen van uniforme wiskundige notaties. Veelal voerde hij zelf nieuwe notaties in (voorbeelden: e, $f(x)$, Σ voor sommatie, $\sin\phi$, $\cos\phi$), soms ook werden notaties van anderen (π bijvoorbeeld) door zijn toedoen populair.

In 1777 legde Euler de Academie in St. Petersburg een artikel voor (in 1794 postuum gepubliceerd) waarin hij aan het begin van de oplossing van een probleem een nieuwe notatie voor $\sqrt{-1}$ invoerde (een notatie die vanaf nu ook in dit stuk gebruikt zal worden):

12	
Quoniam mihi quidem alia adhuc via non patet istud praestandi nisi per imaginaria procedendo, formulam $\sqrt{-1}$ littera i in posterum designabo, ita ut sit $ii = -1$ ideoque $\frac{1}{i} = -i$.	Omdat mij evenwel tot nu toe geen andere weg openstaat om dit te doen (d.w.z.: dit probleem op te lossen) dan door te werken met imaginairen, zal ik in het vervolg de uitdrukking $\sqrt{-1}$ aangeven met de letter i zodat $i^2 = -1$ en dus $\frac{1}{i} = -i$ is.
Euler 1794; *Opera Omnia* (1) 19, 184.	

De notatie i kwam algemeen in gebruik doordat Gauss hem systematisch (en al in de *Disquisitiones arithmeticae,* 1801) gebruikte.

8.4 Balans

Eulers werk is op deze wijze maar zeer ten dele besproken. Complexe getallen speelden erin op nog veel meer plaatsen een rol. Dat was bijvoorbeeld het geval in het onderzoek van algebraïsche vergelijkingen. Ook vond Euler toepassingen. Zo was hij in staat om via een complexe substitutie in de integraalvoorstelling van de gammafunctie (die, het wordt eentonig, ook van Euler afkomstig is) te 'bewijzen' dat $\int_0^\infty \frac{\sin x}{x} dx = \frac{\pi}{2}$. Met deze en soortgelijke bijdragen gaf hij de eerste aanzet tot de ontwikkeling van de complexe functietheorie.

Over dit alles (hoe interessant ook voor verdere bestudering) handelde deze paragraaf niet, want in eerste instantie ging het om de getallen zelf. Euler vergrootte de mogelijkheden van het werken met complexe getallen aanzienlijk, legde de basis voor de huidige theorie, maar ook hij was nog niet vrij van bedenkingen: het bleven 'Zahlen, welche ihrer Natur nach ohnmöglich sind' (nog in 1770) en de hierboven genoemde complexe substitutie werd wel gebruikt, maar met de vermelding dat het resultaat door numerieke berekeningen bevestigd werd.

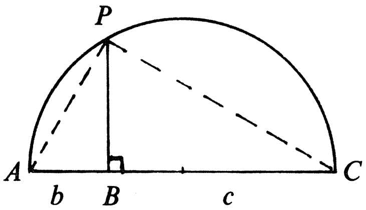
9. De meetkundige representatie

De invoering van de complexe getallen ging, zoals we gezien hebben, gepaard met (psycho-)logische conflicten. Aan de ene kant waren complexe getallen nodig (om de theorie over het oplossen van vergelijkingen algemeen te houden) en nuttig (bijvoorbeeld voor de berekening van integralen), maar ze waren absurd, 'ohnmöglich', denkbeeldig omdat een getal volgens de aanvaarde conventies nu eenmaal geen negatief kwadraat kon hebben.

Sommige wiskundigen, onder wie Euler, lieten zich niet door dit conflict ontmoedigen. Zolang de resultaten maar betrouwbaar leken en omdat sommige problemen complex veel gemakkelijker op te lossen waren dan reëel, gebruikten ze complexe getallen, ook al was er geen bevredigende theorie voor. Maar niet overal werd zo gereageerd. Aan de universiteit van Cambridge werd zelfs rond 1850 nog al het mogelijke in het werk gesteld om complexe functies te vermijden; pas in 1879 werd daar een boek ingevoerd waarin complexe functietheorie toegepast werd. Ook werden nog in 1842 in Engeland de mysterieuze 'imaginaire grootheden' dankbaar aangegrepen als een parallel voor de geheimen van het Christelijk geloof.

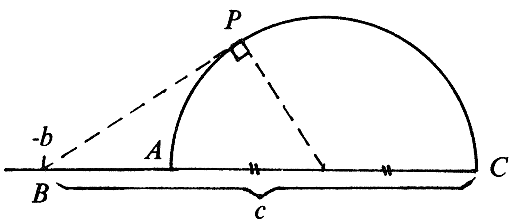
De weerstanden werden uiteindelijk door twee ontwikkelingen weggenomen: enerzijds door het vinden van een meetkundige interpretatie van complexe getallen en hun bewerkingen ('zien doet geloven') en anderzijds door de opkomst van de zuivere wiskunde. De eerste ontwikkeling wordt in deze paragraaf besproken, de tweede in paragraaf 10.

John Wallis (1616 - 1703) was de eerste die probeerde complexe getallen meetkundig voor te stellen (in zijn *Algebra*, 1673). Hij deed dat onder meer via het begrip middenproportionaal. Zoals $\sqrt{bc}$ ($b>0$; $c>0$) de middenproportionaal is tussen b en c of tussen $-b$ en $-c$ (x is de middenproportionaal tussen b en c als x voldoet aan $b:x=x:c$), zo kan, zegt Wallis, $\sqrt{-bc}$ gezien worden als middenproportionaal tussen b en $-c$, of tussen $-b$ en c. En omdat $\sqrt{bc}$ meetkundig voorgesteld kan worden



P op de cirkel met middellijn AC en $PB \perp AC$ geeft $PB = \sqrt{bc}$
(Euclides, *Elementen* VI 13)

is Wallis' idee dat voor $\sqrt{-bc}$ iets dergelijks mogelijk moet zijn. Hij stelt $-b$ voor door punt B op de negatieve as, b eenheden 'Backward from A' (A is de oorsprong) en vindt het punt C door vanuit B c eenheden 'Forward' te gaan.



P op de cirkel met middellijn AC zodat BP de cirkel raakt

Wallis beschouwt dan BP als $\sqrt{-bc}$ (want volgens de machtsstelling geldt $BP^2 = BA.BC$ en BA stelt bij hem $-b$ voor). Dit voldoet duidelijk niet aan de huidige principes, maar wel blijkt eruit dat Wallis bewust op een meetkundige interpretatie uit was. Zie voor deze en andere pogingen van Wallis, waaronder meer succesvolle, verder Smith 1959 (1), 46-54.

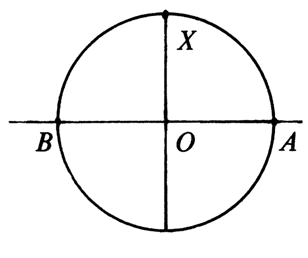
Hierop volgde lange tijd niets. Weliswaar zagen sommige wiskundigen in de 18de eeuw in speciale gevallen een verband tussen complexe getallen en punten in een vlak (bij voorbeeld door de oplossingen $\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ van de vergelijking $x^n = 1$ te beschouwen als hoekpunten van een regelmatige veelhoek), maar dat dit berustte op een algemeen principe en vooral dat ook de bewerkingen met complexe getallen meetkundig te interpreteren waren, werd niet ingezien. Deze stappen werden rond 1800 opeens wel gezet en merkwaardig genoeg zelfs door een aantal wiskundigen tegelijk (een selectie: Wessel 1797, publ. 1799; Argand 1806; Buée 1806; Français 1813; Gauss in of voor 1815, publ. 1831/1832; Warren 1828. Zie Coolidge 1924 voor nadere gegevens). Dit roept vragen op. In hoeverre waren deze ontdekkingen afhankelijk van elkaar. Als ze onafhankelijk waren (en van een aantal is dat aanwijsbaar), hoe is dan te verklaren dat ze alle binnen zo'n korte periode plaatsvonden? Hoe kan het dat een zeer elegante en complete uitwerking (die van Wessel; vgl. Smith 1929 (1), 55-56) onopgemerkt bleef tot de herpublikatie in 1897? Deze vragen zijn fascinerend omdat de antwoorden ons iets zouden kunnen leren over de irrationele processen, die zich bij de ontwikkeling van de wiskunde afgespeeld hebben. Ze zijn echter nog steeds niet bevredigend beantwoord. Beantwoording zou een studie op zich vragen en valt daarom buiten het kader van dit stuk.

Van de talrijke 'ontdekkingen' volgt er hier een, die van Jean Robert Argand (1768 - 1822), geboren in Genève maar als boekhouder werkzaam in Parijs. Zijn werk over de meetkundige voorstelling was dan wel niet het oudste of meest elegante, maar het was wel het eerste dat brede aandacht kreeg.

Het had overigens niet veel gescheeld of het anoniem en in kleine oplage verschenen boekje van Argand, *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques* had hetzelfde lot ondergaan als Wessels artikel. Bij toeval kwam het namelijk pas enige jaren na de publikatie weer boven water. Argand had het voor de publikatie ter advies aan Legendre laten zien, die er op zijn beurt melding van maakte in een brief aan een zekere Français. Toen deze Français overleden was, vond diens broer, die hoogleraar was aan de Franse artillerie- en genieschool, de brief van Legendre tussen de nagelaten papieren. Deze broer, J.-F. Français, werd zo door de inhoud geïntrigeerd dat hij op basis ervan een eigen theorie ontwikkelde, die hij in 1813 publiceerde in de *Annales de mathématiques.* Hij vermeldde echter ook zijn inspiratiebron en sprak de hoop uit dat de eigenlijke grondlegger van het idee zich bekend zou maken. En zo geschiedde. In een volgende aflevering van de *Annales* liet Français een addendum opnemen waarin hij onder meer stelde: '... il n'y a pas le moindre doute qu'on ne doive à M. Argand la première idée de représenter géométriquement les quantités imaginaires.' (geciteerd in Coolidge 1924, 22).

Argand stelt voor om getallen te bepalen door twee grootheden:

1) door hun absolute waarde (evenals 'modulus' een term afkomstig van Argand);
2) door een richting.



Als (zeer anachronistisch geformuleerd) O de oorsprong is en $\overline{OA}$ als positieve eenheid genomen wordt (OA is de absolute waarde van $\overline{OA}$), dan wordt -1 voorgesteld door $\overline{OB}=R_{0,\pi}(\overline{OA})$. Twee maal de afbeelding $R_{0,\pi}$ toepassen beeldt $\overline{OA}$ op zichzelf af, terwijl $\overline{OB}$ middenproportionaal is tussen $\overline{OA}$ en $\overline{OA}$. Als nu algemeen de middenproportionaal van $\overline{OP}$ en $\overline{OR}$ gezien wordt als het getal $\overline{OQ}$ zodat $R_{0,\alpha}(\overline{OP})=\overline{OQ}$ en $R_{0,\alpha}(\overline{OQ})=\overline{OR}$ voor zekere α, dan houdt dat in dat de middenproportionaal $\overline{OX}\equiv i$ van $\overline{OA}\equiv 1$ en $\overline{OB}\equiv -1$ gevonden wordt uit $R_{0,\alpha}(\overline{OA})=\overline{OX}$ en $R_{0,\alpha}(\overline{OX})=\overline{OB}$, ofwel $\alpha=\frac{\pi}{2}+k\pi$. X ligt dus op afstand 1 van O terwijl de lijnen OX en AB loodrecht op elkaar staan. Daarna laat Argand zien, hoe optelling en vermenigvuldiging van gerichte lijnstukken meetkundig geïnterpreteerd kunnen worden en verder geeft hij toepassingen, onder andere op het afleiden van goniometrische identiteiten.

Vaste voet aan de grond kreeg de meetkundige voorstelling door het werk van Carl Friedrich Gauss (1777 - 1855), dat waarschijnlijk los van dat van Argand ontstond. Hoewel het idee impliciet al aanwezig was in de eerste drie bewijzen van de hoofdstelling (1799, 1815, 1816), kwam de precieze formulering pas in 1832 in Gauss' artikel 'Theoria residuorum biquadraticorum'. Uit zijn eigen aankondiging van dit artikel in de *Göttingische gelehrte Anzeigen* (23 april 1831) stammen de volgende teksten, die tevens het slot vormen van deze paragraaf. Hierin vinden we het eerste gebruik van de term 'complexe Zahlen', die door Gauss bewust werd ingevoerd ter voorkoming van de negatieve associaties die het woord 'imaginair' had.

13
Der Verf. nennt jede Grösse $a+bi$, wo a und b reelle Grössen bedeuten, und i der Kürze wegen anstatt $\sqrt{-1}$ geschrieben ist, eine complexe ganze Zahl, wenn zugleich a und b ganze Zahlen sind. Die complexen Grössen stehen also nicht den reellen entgegen, sondern enthalten diese als einen speciellen Fall, wo $b=0$, unter sich.
Hat man diesen Gegenstand (d.w.z.: de complexe getallen) bisher aus einem falschen Gesichtpunkt betrachtet und eine geheimnisvolle Dunkelheit dabei gefunden, so ist diess grossentheils den wenig schicklichen Benennungen zuzuschreiben. Hätte man $+1, -1, \sqrt{-1}$ nicht positive, negative, imaginäre (oder gar unmögliche) Einheit, sondern etwa directe, inverse, laterale Einheit genannt, so hätte von einer solchen Dunkelheit kaum die Rede sein können.
Gauss 1831: *Werke* (2), 171, 177, 178 .

10. De formele definitie

De historisch gegroeide definitie van complexe getallen ging in tegen de bestaande interpretatie van getallen. De eerste reactie hierop was het zoeken naar een interpretatie die beter voldeed (complexe getallen als gerichte lijnstukken; paragraaf 9). De tweede reactie was het loslaten van de gedachte dat de te definiëren objecten een interpretatie moesten hebben. De definitie kon willekeurig zijn en zolang ze maar vrij van tegenspraken was, kon met de gedefinieerde objecten gewerkt worden; in de woorden van Hamilton, die deze gedachten in 1837 voor de complexe getallen uitwerkte:

14 |
... it would be possible to draw legitimate conclusions by rigourous mathematical reasoning, from premises thus arbitrarily assumed.
Hamilton 1837; *Mathematical Papers* (3), 83.

William Rowan Hamilton (1805 - 1865) definieerde complexe getallen als paren reële getallen met de volgende bewerkingen:

15 |
$(b_1,b_2)+(a_1,a_2)=(b_1+a_1,b_2+a_2);$ $(b_1,b_2)-(a_1,a_2)=(b_1-a_1,b_2-a_2);$ $(b_1,b_2)(a_1,a_2)=(b_1,b_2)\times(a_1,a_2)=(b_1a_1-b_2a_2,b_2a_1+b_1a_2);$ $\dfrac{(b_1,b_2)}{(a_1,a_2)}=(\dfrac{b_1a_1+b_2a_2}{a_1^2+a_2^2},\dfrac{b_2a_1-b_1a_2}{a_1^2+a_2^2})$
Hamilton 1837; *Mathematical Papers* (3), 83

Als getal is $\sqrt{-1}$ absurd, zegt hij, omdat het een onmogelijke worteltrekking veronderstelt. Maar in de 'theory of couples' is $\sqrt{-1}$ wel zinvol, namelijk als schrijfwijze voor het paar (0,1) dat voldoet aan

$$(0,1)(0,1)=(-1,0).$$

Hij voegt er een paar bladzijden later geruststellend aan toe:

16 |
and we may write, if we choose, for any couple (a_1,a_2) whatever, $(a_1,a_2)=a_1+a_2\sqrt{-1}$
Hamilton 1837; *Mathematical Papers* (3), 93.

maar dan moet a_1 natuurlijk wel geïdentificeerd worden met $(a_1,0)$, a_2 met $(a_2,0)$ en $\sqrt{-1}$ met $(0,1)$.

In het hoofdstuk 'Reëel, Complex, Quaternionen, komt er nooit een einde aan?' gaat prof.dr. F. van der Blij nader op 'couples' en Hamiltons generalisatie daarvan tot 'quaternions' in.

Het idee dat een formele definitie nodig en zinvol was, leefde niet alleen bij Hamilton getuige het feit dat 10 jaar later door Augustin-Louis Cauchy (1789 - 1857) nog een alternatieve definitie ontwikkeld werd. Bij hem zijn complexe getallen formele polynomen in x waarmee modulo(x^2+1) gerekend wordt. Gelijkheid van polynomen komt overeen met gelijkheid van hun respectieve coëfficiënten.

Stel $a+bi$ voor door $f(x)=a+bx$ en $c+di$ door $g(x)=c+dx$, dan geldt

$$(f+g)(x)=f(x)+g(x)=(a+c)+(b+d)x \text{ en}$$

$$(f{\cdot}g)(x) = f(x) \cdot g(x) = ac + bdx^2 + (ad+bc)x$$
$$\equiv (ac-bd) + (ad+bc)x \mod(x^2+1).$$

Dit doet heel modern aan. Moderne ogen lezen:

$$\mathbb{C} = \mathbb{R}[x]/(x^2+1).$$

In tegenstelling tot Hamilton, die uitgebreid inging op de commutativiteit en de distributiviteit van de 'couples', en die de gebruikelijke stellingen voor complexe getallen afleidde in termen van 'couples', liet Cauchy het hierbij. Maar het is duidelijk dat ook hij op analoge wijze verder had kunnen werken.

11. Conclusion

Tot zover deze schets van de ontwikkeling van de complexe getallen die, zeker als het gaat om de 18de en 19de eeuw, om de theorie van vergelijkingen en van complexe functies, nog aanzienlijk uit te breiden zou zijn.

Opvallend was het schoksgewijze karakter van de ontwikkeling. Nieuwe theorie was telkens een reactie op nieuw opgekomen problemen, die voor een deel van buiten de theorie afkomstig waren (de derdegraads vergelijking in de 16de eeuw, de integraalrekening aan het eind van de 17de eeuw, grondslagenvragen en opkomende strengheid in de loop van de 19de eeuw). Interessant ook was het optreden van de 'definitie achteraf'. Ondanks logische tegenstrijdigheden werden complexe getallen gebruikt omdat dat snel resultaten opleverde. Pas veel later kwam een correcte definitie, die tot een consistente theorie leidde. Dit verschijnsel heeft zich in de geschiedenis van de wiskunde overigens vaker voorgedaan. Een mooi voorbeeld is ook de snel populair geworden Heaviside-calculus die pas achteraf door de theorie van de distributies 'gerechtvaardigd' werd.

Tja, en dan die letter $\mathbb{C}$. Speelde alles wat hier verteld werd, zich inderdaad af *voordat* de notatie $\mathbb{C}$ ingevoerd werd? Met andere woorden: wie voerde die notatie in, en wanneer? Was het Bourbaki? Daar komt de (vetgedrukte) **C** inderdaad voor. Maar wat dan te denken van $\mathbb{Z}$ (van 'Zahl'???) voor 'nombres entiers'? Hoewel: Bourbaki had de E al gebruikt voor 'ensemble'. Wie zich geroepen voelt ...!

Bibliografie

Primaire bronnen zijn te herkennen aan het vermelden van de voornaam van de auteur. Titels voorzien van een ster zijn algemene werken; dit voor wie zich wat verder zou willen verdiepen in de geschiedenis van de wiskunde in het algemeen.

Rafael Bombelli, *L'Algebra*, Bologna 1572; 2de druk Bologna 1579.
(*) C.B. Boyer, *A history of mathematics*, New York etc. 1968.
Girolamo Cardano, *Ars Magna sive de regulis algebraicis*, Neurenberg 1545; Basel 1570, ook *Opera Omnia* (4), 221-302.
De regula Aliza libellus, Basel 1570; ook *Opera Omnia* (4), 377-434.

Sermo de plus et minus in *Opera Omnia* (4), 435-439.
Opera Omnia (10 vols.), Lyon 1663. Herdruk: New York; London 1967.

J.L. COOLIDGE, *The geometry of the complex domain,* Oxford 1924.

(*) P. DEDRON, J. ITARD, *Mathématiques et mathématiciens,* Parijs 1959. Engelse editie: Londen 1974.

[René Descartes; anoniem gepubliceerd], 'la Géométrie', essay in *Discours de la Methode ...* , Leiden 1637, 297-413. herdrukt in:

D.E. SMITH, M.L. LATHAM (vert.), *The geometry of René Descartes with a facsimile of the first edition,* New York 1954.

E.J. DIJKSTERHUIS, *Simon Stevin*, 's-Gravenhage 1943.

G. ENESTRÖM, Hat Tartaglia seine Lösung der kubischen Gleichung von Del Ferro entlehnt?, *Bibl. Math.* (3) 7 (1906/7), 38-43.

LEONHARD EULER, *Introductio in analysin infinitorum* (2 vols.), Lausanne 1748; ook *Opera Omnia* (1) 8,9; fotomechanische herdruk: Brussel 1967.
De la controverse entre Mrs. Leibniz et Bernoulli sur les logarithmes des nombres negatifs et imaginaires, *Mémoires de l'académie des sciences de Berlin* 5 (1749; publ. 1751), 139-179; ook *Opera Omnia* (1) 17, 195-232.
Institutiones calculi integralis (4), Petersburg 1794 (de delen 1-3 verschenen tussen 1768 en 1770); ook *Opera Omnia* (1) 19, 129-140.
Zur Theorie komplexer Funktionen (A.P. Juschkewitsch ed.), Ostwald Klassiker 261, Leipzig 1983 met een zeer bruikbare inleiding van de uitgever (p.8-48).

A. FIJAN, *De ontstaansgeschiedenis van de hoofdstelling van de algebra,* Utrecht 1982 (ongepubliceerde scriptie geschiedenis van de wiskunde, te raadplegen via prof.dr. H.J.M. Bos, Math. Inst. Utrecht).

CARL FRIEDRICH GAUSS, *Göttingische gelehrte Anzeigen,* 1831 April 23; ook *Werke* 2, 169-178.

ALBERT GIRARD, *Invention nouvelle en l'algebre,* Amsterdam 1629; heruitgave door D. Bierens de Haan in *Nieuw Archief voor wiskunde* 11 (1884), 85-152.

WILLIAM ROWAN HAMILTON, Theory of conjugate functions, or algebraic couples ... , *Trans. Roy. Irish Acad.* 17 (1837), 293-422; ook *Mathematical Papers (3),* 3-96.

P.S. JONES, artikel 'Argand' in *Dictionary of Scientific Biography,* (1), 237-240.

(*) A. P. JUSCHKEWITSCH, *Geschichte der Mathematik im Mittelalter,* Leipzig 1964.

(*) M. KLINE, *Mathematical thought from ancient to modern times,* New York 1972.

C.C. MACDUFFEE, Algebra's debt to Hamilton, *Scripta Mathematica* 10 (1944), 25-35.

R.B. MCCLENON, A contribution of Leibniz to the history of complex numbers, *Am. Math. Monthly* 30 (1923), 369-374.

E. NAGEL, 'Impossible numbers': a chapter in the history of modern logic, *Studies in the history of ideas* 3 (1935), 429-474.

F. ROSEN (ed; transl.), *The algebra of Mohammed ben Musā,* Londen 1831, herdruk: New York 1969.

I. SCHNEIDER, Der Mathematiker Abraham de Moivre (1667 - 1754), *Archive*

for history of exact sciences 5 (1968/1969), 177-317.
(*) D.E. SMITH (ed.), *A source book in mathematics* (2 vols.), New York 1929; herdruk 1959.
SIMON STEVIN, *L'Arithmetique,* Leiden 1585.
(*) D.J. STRUIK, *Geschiedenis van de wiskunde,* Amsterdam 1980 (2de uitgebreide ed.).
(*) *A source book in mathematics, 1200-1800,* Cambridge (Mass.) 1969.
(*) J. TROPFKE, *Geschichte der Elementarmathematik,* 4. Auflage Band 1. Arithmetik und Algebra, Berlijn etc. 1980.
C.J. VOOYS, Denkbeeldig getal bij Cardano, *Euclides* 35 (1959/60), 162-166.
(*) B.L. VAN DER WAERDEN, *Ontwakende wetenschap,* Groningen 1950.
H. WIELEITNER, Zur Frühgeschichte des Imaginären, *Jahresbericht der deutschen Mathematiker-Vereinigung* 36 (1927), 74-88.

Complexe Getallen zijn Nuttig, ook voor Wiskundigen.

F. van der Blij
Rijksuniversiteit Utrecht
Postbus 80010, 3508 TA Utrecht

1. Inleiding

Laten we beginnen met persoonlijke jeugdherinneringen.

1. De wortels van de vierkantsvergelijking (v.k.v.) $x^2+2\lambda x+2\lambda=0$ zijn x_1 en x_2. Voor welke waarde van λ is $x_1^2+x_2^2$ minimaal?

Het lijkt een simpele opgave, $x_1^2+x_2^2=(x_1+x_2)^2-2x_1x_2$, dus $x_1^2+x_2^2=4\lambda^2-4\lambda=(2\lambda-1)^2-1$. Voor $\lambda=\frac{1}{2}$ bereikt deze vorm zijn minimum -1. Maar hoe kan dat; $x_1^2+x_2^2\geqslant 0$ geldt toch?

(De subtiele vraag of er wel wortels zijn ontging me.)

2. Bepaal de vergelijking van de lijn door de twee snijpunten van de cirkels $x^2+y^2=1$ en $(x-a)^2+(y-b)^2=1$.

Eliminatie door aftrekking geeft direct de gevraagde vergelijking $2ax+2by=a^2+b^2$. Op deze lijn ligt het punt $(\frac{1}{2}a,\frac{1}{2}b)$, dit punt is het midden van het lijnstuk tussen de twee snijpunten. Maar voor $a=b=2$ b.v. hebben de cirkels helemaal geen snijpunten! En toch bestaat de lijn door de snijpunten en bestaat het midden?

3. De Fibonacci-getallen zijn bekend: $x_0=x_1=1$ en $x_{n+2}=x_{n+1}+x_n$. Een aardige methode om een formule te vinden is: stel $x_n=t^n$. Dan $t^2=t+1$. Dus $t=\frac{1}{2}\pm\frac{1}{2}\sqrt{5}$. Door A en B geschikt te kiezen, vinden we $x_n=A(\frac{1}{2}+\frac{1}{2}\sqrt{5})^n+B(\frac{1}{2}-\frac{1}{2}\sqrt{5})^n$. Omdat

$$|\tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}|<1$$

vinden we voor grote waarden van n een goede benadering via

$x_n = A(\frac{1}{2}+\frac{1}{2}\sqrt{5})^n$ en omdat $x_n \in \mathbf{Z}$ vinden we zo de juiste waarde ook wel.

Nu dezelfde vraag voor de variant $x_0 = x_1 = 1$ en $x_{n+2} = x_{n+1} - x_n$. Passen we dezelfde truc toe, dan stuiten we op

$$t^2 = t - 1,$$

een v.k.v. die geen wortels heeft. En toch is de rij erg regelmatig

$$1, 1, 0, -1, -1, 0, 1, 1, 0, -1, ...$$

Waarom kan het niet met een analoge formule behandeld worden?

U begrijpt het, de complexe getallen zullen in al deze gevallen ons aan inzicht helpen. In voorbeeld 1 zijn er natuurlijk twee toegevoegd complexe wortels met $x_1^2 + x_2^2 = -1$. In voorbeeld 2 zijn er twee toegevoegd complexe snijpunten, met een reële verbindingslijn en een reëel midden. In voorbeeld 3 zijn de complexe wortels van de v.k.v. $\cos\frac{\pi}{3} \pm i \sin\frac{\pi}{3}$ en de formule wordt

$$x_n = \cos\frac{n\pi}{3} + \frac{1}{\sqrt{3}}\sin\frac{n\pi}{3},$$

waarmee de periodiciteit verklaard wordt.

Behalve om te verklaren, zijn complexe getallen ook nuttig om te berekenen.

4. $$\begin{aligned}\int e^{ax}\cos bx dx &= \frac{1}{a}\int \cos bx d(e^{ax}) \\ &= \frac{1}{a}e^{ax}\cos bx + \frac{b}{a}\int e^{ax}\sin bx dx \\ &= \frac{1}{a}e^{ax}\cos bx + \frac{b}{a^2}\int \sin bx d(e^{ax}) \\ &= \frac{1}{a}e^{ax}\cos bx + \frac{b}{a^2}e^{ax}\sin bx - \frac{b^2}{a^2}\int e^{ax}\cos bx dx.\end{aligned}$$

Dus (?) $(1+\frac{b^2}{a^2})\int e^{ax}\cos bx dx = \frac{1}{a}e^{ax}\cos bx + \frac{b}{a^2}e^{ax}\sin bx$. Maar met complexe getallen gaat het sneller en duidelijker:

$$\begin{aligned}\int e^{ax}\cos bx dx &= \mathrm{Re}\int e^{ax}e^{ibx}dx = \mathrm{Re}\frac{e^{ax}e^{ibx}}{a+bi} \\ &= \mathrm{Re}\frac{a-bi}{a^2+b^2}\cdot e^{ax}\cdot(\cos bx + i\sin bx) \\ &= \frac{e^{ax}}{a^2+b^2}(a\cos bx + b\sin bx).\end{aligned}$$

5. Nog veel duidelijker is de opgave

$$\int \frac{x^k}{x^{2n}+1}dx$$

met complexe getallen veel sneller te behandelen dan met enkel reële getallen.

6. Toch geeft 5 wel te denken; voor $k=0$, $n=1$ vinden we

$$\int \frac{dx}{x^2+1} = \int \frac{dx}{(x+i)(x-i)} = \frac{i}{2}\int (\frac{1}{x+i} - \frac{1}{x-i})dx$$
$$= \frac{1}{2}i(\ln(x+i) - \ln(x-i)),$$

terwijl iedereen weet dat de primitieve arctan x is!

Laten we eerst even 'evalueren'. Voorbeelden 1 en 2 lieten zien dat als je ondoordacht formules toepast, je fouten maakt. Complexe getallen waren daar alleen nuttig omdat je een excuus voor je foute antwoord kon verzinnen. Bij voorbeeld 6 is het anders, althans op het eerste gezicht. Maar als we de complexe logaritme goed gedefinieerd hebben, komen we na wat manipulatie toch op het goede antwoord. Bij voorbeeld 4 zijn de complexe getallen een aardige tussenstap om het rekenwerk te vereenvoudigen. De oorzaak is dat differentiatie van goniometrische functies pas na 2 maal de oorspronkelijke functie oplevert; terwijl de complexe e-macht dat al na 1 maal differentiëren doet. Ons 5de voorbeeld berust er op dat complexe breuksplitsing met lineaire noemers aanzienlijk eenvoudiger is dan reële breuksplitsing met kwadratische noemers. Tenslotte voorbeeld 3. Hier is een manier om veel problemen op eenzelfde manier op te lossen .

Laat A een ring zijn, dus een systeem waarin we kunnen optellen, aftrekken en vermenigvuldigen met de gewone rekenregels. Voorbeelden zijn gehele getallen, rationale getallen, getallen modulo N, veeltermen enzovoorts. Als α en β elementen van A zijn, kunnen we heel algemeen vragen naar oplossingen van $x_{n+2}=\alpha x_{n+1}+\beta x_n$. Deze oplossingen vormen een lineaire ruimte. We vinden twee (?) oplossingen uit $x_n=t^n$, $t^2=\alpha t+\beta$ en kunnen lineair combineren. Maar als de v.k.v. geen wortels in A heeft? Zijn dan een soort 'complexe' getallen in te voeren om toch de methode te redden? Voor specialisten nog even de vraag: wat gebeurt er als de v.k.v. meer dan twee of slechts één oplossing heeft ? Bij rekenen modulo N kan dat gebeuren.

MORAAL: Een aantal problemen is eenvoudiger met behulp van complexe getallen op te lossen. Andere (foutieve) resultaten worden verklaard met complexe getallen. Het is een kleine moeite om recurrente rijen via

$$x_{n+k} = \alpha_1 x_{n+k-1} + \alpha_2 x_{n+k-2} + \alpha_3 x_{n+k-3} + \ldots + \alpha_k x_n$$

te definiëren. De substitutie $x_n=t^n$ voert dan tot een $n$de-graads vergelijking. Complexe getallen zijn nuttig om algebraïsche vergelijkingen op te lossen.

2. RUBRICERING

We willen nu enkele gebieden opsommen waar in de wiskunde de invoering van complexe getallen nuttig is. Nuttig zal vaak willen zeggen: de complexe getallen helpen om problemen die zonder complexe getallen geformuleerd zijn, tot een oplossing te brengen. Soms zijn complexe getallen ook nuttig omdat door de invoering ervan problemen die op het eerste gezicht verschillend lijken onder één noemer te brengen zijn. Dan geven de complexe getallen meer inzicht. Tenslotte zijn complexe getallen soms nuttig (in een oneigenlijke zin) in de wiskunde doordat de invoering van complexe getallen in een bestaande theorie nieuwe boeiende problemen oplevert en daarom nuttig is. We stellen nu separaat enkele gebieden van wiskundig onderzoek aan de orde.

1. Lineaire algebra vraagt soms om complexe getallen als hulpmiddel.

In toepassingen van de lineaire algebra heeft men bij bestudering van iteratieve processen soms machten van matrices nodig. In demografie en biologie bestudeert men een populatie verdeeld in deelpopulaties $(x_1, x_2, \ldots, x_n)$. De grootte van deze populaties hangt van het beschouwde tijdstip af; dus $\vec{x}(t) = (x_1(t), x_2(t), \ldots, x_n(t))$. Laat nu gegeven zijn

$$\vec{x}(t+1) = M\vec{x}(t)$$

met een matrix M die niet van t afhangt. Dan volgt

$$\vec{x}(t) = M^t\vec{x}(0).$$

Maar hoe M^t te berekenen? Complexe getallen zullen helpen!

2. Meetkundige beschouwingen over algebraïsche krommen en oppervlakken voeren tot het zoeken naar oplossingen van stelsels algebraïsche vergelijkingen.

Wanneer we werken in een lichaam waarin iedere algebraïsche vergelijking een wortel (en dan precies zoveel wortels als zijn graad bedraagt) heeft, is een uniforme theorie te geven tegenover een theorie met veel onderscheiding van speciale gevallen, indien we over een niet-algebraïsch afgesloten lichaam werken.

3. In de analyse, speciaal bij de bestudering van periodieke processen, heeft men de keuze uit goniometrische functies of complexe e-machten.

Hoewel het slechts een formeel element is, zijn complexe Fourier-reeksen e.d. vaak eenvoudiger te overzien dan Fourier-reeksen met sinus en cosinus. De inversie van de reële Laplace-vergelijking laat zich handig als een complexe Mellin-integraal schrijven. Bij machtreeksen geeft de complexe convergentiecirkel een beter inzicht dan het reële convergentie-interval. Functies die complex differentieerbaar zijn, hebben vele speciale eigenschappen die functies die reëel differentieerbaar zijn, missen. Hieruit is een aparte discipline ontstaan binnen de analyse; de functietheorie is de theorie van de complex differentieerbare functies.

4. In de getaltheorie zijn complexe getallen op twee geheel verschillende manieren nuttig.

Als eerste voorbeeld noemen we de vraag welke getallen, en op hoeveel manieren, voor te stellen zijn als de som van twee kwadraten. De constatering $41=16+25=(4+5i)(4-5i)$ laat zien dat het al of niet voorstelbaar zijn als de som van twee kwadraten samenhangt met de vraag of 41 te ontbinden is in 'complexe factoren'.

Een geheel ander gebruik van complexe getallen in de getaltheorie is bij de bepaling of schatting van een getaltheoretische functie $a(n)$. We construeren

$$F(z) = \sum_{n=0}^{\infty} a(n)z^n,$$

en proberen uit F nu eigenschappen van $a(n)$ af te leiden. De Taylor-formule $a(n)=\frac{1}{n!}F^{(n)}(0)$ is niet altijd bruikbaar. Met complexe integratie hebben we

$$a(n) = \frac{1}{2\pi i}\oint \frac{F(z)}{z^{n+1}}dz,$$

en integralen laten zich soms vernuftig schatten!

De vraag naar schattingen voor het aantal priemgetallen $\leqslant x$ is terug te brengen naar de vraag over de nulpunten van een complexe functie $\zeta(z)=\Sigma_{n=1}^{\infty}n^{-z}$, het gaat dan speciaal om complexe nulpunten.

3. De twee wonderen

Voor we de voorbeelden uit paragraaf 2 wat nader uitwerken eerst iets over de twee wonderen. We merkten in paragraaf 2 op dat bepaalde stukken algebra en meetkunde vragen om een *algebraïsch afgesloten* lichaam. Als het lichaam waarin we werken niet algebraïsch afgesloten is, voegen we elementen toe om het algebraïsch af te sluiten. Gaan we uit van de rationale getallen dan moeten we b.v. $\sqrt{2}$ toevoegen. We krijgen dan het lichaam van alle getallen $a+b\sqrt{2}$, $a,b \in \mathbb{Q}$. Maar dit is nog niet algebraïsch afgesloten. Dus b.v. $\sqrt{3}$ toevoegen, dan krijgen we het lichaam van alle getallen $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$; $a,b,c,d \in \mathbb{Q}$. Maar we zien dat er nog veel meer toegevoegd moet worden: $\sqrt{p}$ voor ieder priemgetal, en dan nog $\sqrt[3]{2}, \sqrt[5]{7}$ en nog veel meer want ondanks alle stapelmogelijkheden is niet iedere wortel van een algebraïsche vergelijking met behulp van wortelvormen te schrijven.

Bij eindige lichamen hebben we dezelfde gecompliceerde processen nodig om tot een algebraïsch afgesloten lichaam te komen.

We formuleren nu het eerste wonder:

Adjunctie van een wortel van de vergelijking $x^2+1=0$ aan de reële getallen levert een algebraïsch gesloten lichaam op.

Het is eigenlijk een heel bijzondere eigenschap van de reële getallen, waardoor $\mathbb{R}(\sqrt{-1})$ zo fraai algebraïsch afgesloten is.

Het tweede wonder gaat over differentiëren. Als een complexe functie in zeker gebiedje differentieerbaar is, is de functie ook willekeurig vaak differentieerbaar en in een machtreeks te ontwikkelen. Voor reëel differentieerbare functies is er geen analoge stelling. De functie gedefinieerd door $f(x)=|x|^k$ is voor oneven k in de oorsprong $k-1$ keer, maar niet k keer differentieerbaar. De functie gedefinieerd door $g(x)=e^{-1/x^2}$ is in de oorsprong willekeurig vaak differentieerbaar, maar niet in een machtreeks te ontwikkelen .

Behalve reële en complexe getallen zijn er nog meer lichamen te vinden waarin een differentiaalrekening op te bouwen is. Deze lijken echter niet op de complexe getallen.

We formuleren het tweede wonder:

Differentieerbare complexe functies zijn willekeurig vaak differentieerbaar en in een machtreeks te ontwikkelen.

Een gevolg is dat wanneer twee complex differentieerbare functies in een rij van punten die zich verdichten in een punt dezelfde waarde hebben, deze functies identiek zijn. (Door een 'kiem' is de functie bepaald). Aan de functies gegeven door $x^2 \cdot f(x) \cdot \sin \frac{\pi}{x}$ zien we dat zo'n stelling reëel niet geldt. Er zijn vele functies f te vinden zodat de combinatie differentieerbaar is. Alle punten $\{\frac{1}{n} | n \in \mathbb{N}\}$ zijn nulpunten van al deze functies, die buiten die punten zeker niet noodzakelijk overeenstemmen.

Het is moeilijk een verklaring voor dit tweede wonder te vinden. Dan was het trouwens geen wonder meer! Eén mogelijke 'verklaring' is te vinden in het feit dat voor een complex differentieerbare functie f geldt

$$f(z) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(z + re^{i\phi}) d\phi$$

voor alle $r \geqslant 0$. Het gemiddelde van de functie over een cirkelomtrek is de waarde van de functie in het middelpunt. Reëel differentieerbare functies hebben zo'n eigenschap niet. Want aan

$$f(z) = \frac{1}{2}\{f(z+r) + f(z-r)\}$$

voldoen alleen heel bijzondere reële differentieerbare functies.

Verder zou men een verband kunnen leggen tussen het feit dat de lijn een 'zwakkere' topologische samenhang heeft dan het vlak. Zo is spiegelen in de lijn een lineaire afbeelding; spiegelen in het vlak een reële lineaire afbeelding; maar spiegelen in het (complexe) vlak geen complexe lineaire afbeelding. De afbeelding $z \rightarrow \bar{z}$ is *niet* complex lineair en ook niet differentieerbaar. De eis van complexe differentieerbaarheid is vrij sterk.

4. Lineaire algebra

We bespreken als voorbeeld machten van matrices. Het belang ervan is o.a. te vinden in de iteratie van lineaire afbeeldingen. We beginnen eenvoudig. Laat

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

en

$$A^n = \begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix}$$

dan zijn a_n, b_n, c_n, d_n polynomen van de graad n in a_1, b_1, c_1 en d_1. Maar expliciete formules zijn als regel niet eenvoudig. Maar als $a_1 = \cos\phi$, $b_1 = -\sin\phi$, $c_1 = \sin\phi$, $d_1 = \cos\phi$ is het eenvoudig, namelijk $a_n = \cos n\phi$, $b_n = -\sin n\phi$, $c_n = \sin n\phi$, $d_n = \cos n\phi$. De matrix A hoort nu immers bij draaiing over een hoek ϕ. Enkele andere voorbeelden: als $b_1 = c_1 = 0$, dan $a_n = a_1^n, d_n = d_1^n$; als $a_1 = d_1 = b_1 = 1$, $c_1 = 0$, dan $a_n = d_n = 1$ en $b_n = nb_1$. Maar deze speciale gevallen geven geen inzicht.

Nu heeft een 2×2 matrix altijd 2 (complexe) eigenwaarden λ_1, λ_2. Als $\lambda_1 \neq \lambda_2$ zijn er eigenvectoren bij deze eigenwaarden die we als een basis voor de ruimte kunnen gebruiken. Op deze basis is de lineaire afbeelding gegeven door

$$\tilde{A} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \text{ en } \tilde{A}^n = \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}$$

We merken dus op: Er is een inverteerbare matrix U, zodat

$$U^{-1}AU = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} ; \; U^{-1}A^nU = \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}.$$

Hieruit is A^n direct te bepalen, uitgedrukt in de eigenwaarden λ_1 en λ_2. De getallen a_n, b_n, c_n, d_n zullen symmetrische functies zijn van de wortels λ_1 en λ_2 van de vierkantsvergelijking $\lambda^2 - (a_1 + d_1)\lambda + (a_1 d_1 - b_1 c_1) = 0$. Ook als de wortels λ_1 en λ_2 complex zijn, zijn deze symmetrische functies reëel. Zouden we de $n$de geïtereerde (x_n, y_n) van een beginvector (x_1, y_1) berekenen, dan zou $x_n = \alpha\lambda_1^n + \beta\lambda_2^n$ en $y_n = \gamma\lambda_1^n + \delta\lambda_2^n$. Het gedrag voor $n \to \infty$ van x_n en y_n is direct af te lezen uit de waarden van λ_1 en λ_2. We noemen enkele gevallen:

$|\lambda_1| < 1$, $|\lambda_2| < 1$, x_n en y_n naderen tot 0.
$|\lambda_1| > |\lambda_2|$, $\lambda_1 > 1$, x_n en y_n naderen to ∞.
$|\lambda_1| < 1$, $|\lambda_2| < 1$, λ_1 en λ_2 complex; x_n en y_n naderen schommelend tot 0.
$|\lambda_1| = |\lambda_2|$, λ_1 en λ_2 eenheidswortels; x_n en y_n zijn periodiek.
etc. etc.

In het geval van twee gelijke eigenwaarden kunnen we steeds een basis vinden zo dat

$$A = \begin{bmatrix} \lambda & \alpha \\ 0 & \lambda \end{bmatrix}.$$

In dit geval is λ reëel, de berekening van A^n is eenvoudig.

In het geval van een $k \times k$ matrix geldt een analoge methode. We bepalen eerst de k eigenwaarden uit de vergelijking $\det(A - \lambda I) = 0$. Door geschikte keuze van een basis krijgt A de bovendriehoeken gedaante, in het geval van allemaal verschillende eigenwaarden zelfs diagonaal gedaante. Dan is de $n$de macht weer eenvoudig te berekenen. Het spectrum van de matrix, dat is de collectie eigenwaarden (complex en reëel) bepaalt weer het gedrag van de componenten van de $n$de iteratie voor $n \rightarrow \infty$.

5. Algebraïsche meetkunde

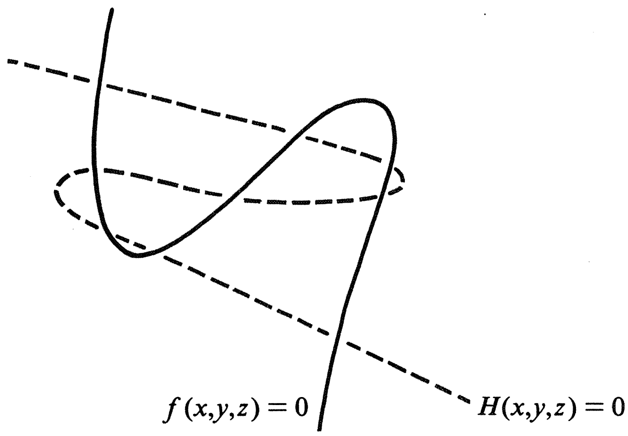
We geven in deze paragraaf een niet te triviaal voorbeeld van een meetkundig probleem waarin complexe getallen een rol spelen. We noemen zonder bewijs twee meetkundige stellingen.

1. Laat $f(x,y,z) = 0$ de vergelijking van een algebraïsche kromme in projectieve coördinaten zijn. Dan voldoen de coördinaten van de buigpunten van de kromme aan de vergelijking

$$H(x,y,z) = \begin{vmatrix} \dfrac{\partial^2 f}{\partial x^2} & \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial x \partial z} \\[2ex] \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial y^2} & \dfrac{\partial^2 f}{\partial x \partial z} \\[2ex] \dfrac{\partial^2 f}{\partial x \partial z} & \dfrac{\partial^2 f}{\partial y \partial z} & \dfrac{\partial^2 f}{\partial z^2} \end{vmatrix} = 0.$$

2. Als A en B buigpunten van een derdegraads kromme zijn en de rechte door A en B snijdt de kromme nog in punt C, dan is C een buigpunt.

We merken op dat voor een kubische kromme ook de kromme $H(x,y,z) = 0$ van de derde graad is. Een kubische kromme zal dus in het algemeen negen buigpunten kunnen hebben, het zijn de snijpunten van de krommen $f(x,y,z) = 0$ en $H(x,y,z) = 0$.



De tekening is echter een falsificatie. Je ziet direct dat niet ieder snijpunt een buigpunt van de kubische kromme is.

Hoewel er dus over de complexe getallen best negen buigpunten kunnen zijn, zal blijken dat deze nooit alle negen reëel kunnen zijn. Eerst een voorbeeld:

$$f(x,y,z) = x^3 + y^3 + z^3.$$

Dan $H(x,y,z) = 216xyz$. De buigpunten zijn

$$(1,-1,0),\ (1,\zeta,0),\ (1,\eta,0)$$
$$(1,0,-1),\ (1,0,\zeta),\ (1,0,\eta)$$
$$(0,1,-1),\ (0,1,\zeta),\ (0,1,\eta) \qquad \text{met } \zeta^3 = \eta^3 = -1.$$

Het kan dus echt voorkomen dat er 9 (complexe) buigpunten zijn. Er wordt door deze 9 punten een affiene meetkunde gevormd met op iedere lijn 3 punten. Deze is aan te vullen tot een projectieve meetkunde van 13 punten. Voor de realisatie van de affiene meetkunde van 9 punten kunnen we coördinaten kiezen, zodat (0,0), (1,0), (0,1) en (1,1) 4 buigpunten zijn, waarvan er geen 3 op een rechte liggen. Noemen we het buigpunt op de rechte door (0,0) en (1,0) nu $(p,0)$ en dat op de rechte door (0,0) en (0,1) nu $(0,q)$, dan voeren de incidentie-eisen tot $pq = p + q = 1$. En alleen in een lichaam waarin $x^2 - x + 1 = 0$ twee wortels heeft, kunnen deze punten dus bestaan. Noodzakelijke voorwaarde is dus dat -3 kwadraat is; hetgeen in de reële getallen niet, in de complexe getallen wel het geval is.

6. ANALYSE

De toepassingen van de complexe getallen in de analyse zijn zo veelvuldig en zo centraal, maar ook zo bekend dat we volstaan met enkele korte opmerkingen. In toepassingen van de analyse is een bijzondere rol weggelegd voor harmonische functies. Dat zijn reële functies f van twee variabelen x en y die voldoen aan $\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0$. Voor iedere complex differentieerbare functie $F(z)$ (met $z = x + iy$) geldt dat het reële deel en het zuiver imaginaire deel harmonische functies zijn. Uit de complexe differentieerbaarheid volgen de differentiaalvergelijkingen van Cauchy-Riemann en combinatie van deze vergelijkingen geeft de harmoniciteit van $\operatorname{Re} F$ en $\operatorname{Im} F$. Randwaardeproblemen voor harmonische functies zijn te vertalen naar de constructie van complex differentieerbare functies, die op een gegeven contour een voorgeschreven reëel deel hebben.

In ieder punt waar $F'(z) \neq 0$ geeft de complex differentieerbare functie F een conforme, d.w.z. hoekgetrouwe afbeelding. Ook dat toont het 'nut' van complexe-functietheorie aan.

De toepassingen van de Laplace-transformatie

$$\mathfrak{L}(f) = g \text{ als } g(t) = \int_0^\infty f(x) e^{-xt}\, dx$$

berusten er o.a. op dat $\mathfrak{L}(f')(t) = f(0) + tg(t)$. Hiermee is een formule-calculus voor het oplossen van bepaalde differentiaalvergelijkingen te krijgen. De inverse transformatie van de Laplace-transformatie, nodig om weer 'terug te vertalen' wordt door een *complexe* integraal gegeven.

$$f(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} g(t) e^{xt} dt$$

met geschikt gekozen reële c.

7. GETALTHEORIE

Over getaltheorie voor getallen $a + bi$, $a, b \in \mathbb{Z}$ en de toepassingen daarvan voor de representatie van natuurlijke getallen door kwadratische vormen (b.v. sommen van kwadraten) handelt een aparte voordracht in deze cursus.

De schattingen van getaltheoretische functies $a(n)$ via bestudering van de complexe machtreeks $\Sigma a(n) z^n$ vraagt in veel gevallen zeer gespecialiseerde en verfijnde methoden uit de complexe analyse. Zowel dubbel periodieke complexe functies als modulaire functies - dat zijn functies f, waarvoor bij een substitutie uit $SL(2, \mathbb{Z}) : z \mapsto Mz = \dfrac{az + b}{cz + b}$ het volgende transformatiegedrag geldt: $f(Mz) = (\dfrac{dMz}{dz})^g f(z)$ - spelen daarbij een rol.

Getaltheoretische functies kunnen ook ingebouwd worden in Dirichlet-reeksen:

$$L(a; z) = \sum_{n=1}^{\infty} \frac{a(n)}{n^z}.$$

Voor multiplicatieve functies: $a(nm) = a(n) \cdot a(m)$ als $(n, m) = 1$ geldt:

$$L(a, z) = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{a(p^\nu)}{p^{\nu z}} \right).$$

Voor sterk multiplicatieve functies: $a(nm) = a(n) \cdot a(m)$ voor alle n, m geldt

$$L(a, z) = \prod_p \left(1 - \frac{a(p)}{p^z}\right)^{-1}.$$

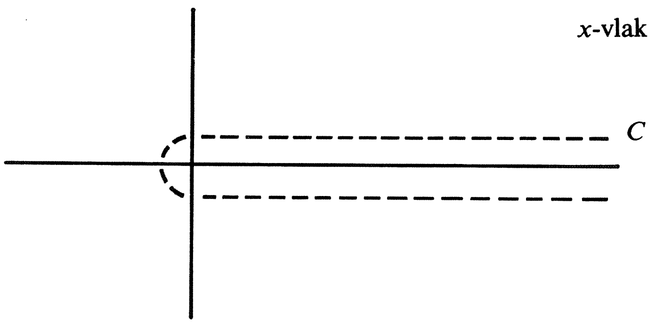
Het eenvoudige geval $a(n) = 1$ voor alle n geeft de ζ-functie van Riemann:

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} = \prod_p \left(1 - \frac{1}{p^z}\right)^{-1}.$$

Deze functie ζ kan b.v. via integraal-representaties voortgezet worden. Zo geldt

$$2 \sin \pi z \cdot \Gamma(z) \zeta(z) = i \int_C \frac{(-x)^{z-1} dx}{e^x - 1}$$

uitgestrekt over een contour C:



Door omvorming van zo'n integraal kreeg B. Riemann in 1859 in een artikel 'Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse' een schatting van het aantal priemgetallen onder een bepaalde grens. Het is duidelijk dat $\log \zeta(z)$ en $\frac{\zeta'(z)}{\zeta(z)}$ reeksontwikkelingen hebben, waarin de priemgetallen expliciet voorkomen. De preciese plaats van de nulpunten van ζ, en dus van de polen van $\frac{\zeta'}{\zeta}$ in de strook $0 \leqslant \operatorname{Re} z \leqslant 1$, is een goed te gebruiken gegeven om het verschil van $\pi(x)$, het aantal priemgetallen $\leqslant x$ en $Li(x) = \int_2^x \frac{dt}{\log t}$ te schatten. Het vermoeden van Riemann (nog steeds onbewezen) is dat voor alle nulpunten geldt $\operatorname{Re} z = \frac{1}{2}$. Zou dit vermoeden juist zijn, dan was het verschil van $\pi(x)$ en $Li(x)$ van de orde $\sqrt{x}$. Maar zover zijn we nog niet met de theorie van de complexe functies gevorderd. En dus is het eenvoudige schattingprobleem over priemgetallen nog niet opgelost. We zoeken nog, of zouden we moeten zoeken naar methoden die geen complexe getallen benutten? Ik vermoed, dat we voorlopig de complexe getallen toch ook hier maar als een nuttig hulpmiddel zullen gebruiken.

8. Conclusie

Hoewel we lang niet alle toepassingen van de complexe getallen in gebieden van de wiskunde, die met complexe getallen gedefinieerd zijn, besproken hebben, moet onze conclusie toch wel zijn dat complexe getallen binnen de wiskunde nuttig zijn. In de analyse speelde het tweede wonder, de speciale eigenschappen van één keer differentieerbare functies een rol, in de (algebraïsche) meetkunde en in de (lineaire) algebra het eerste wonder, de algebraïsche afgeslotenheid.

We spraken b.v. niet over de topologie, maar ook daar zijn complexe getallen nuttig. Het is een heel bijzondere eigenschap als een topologische variëteit een complexe structuur toelaat; maar dat onderwerp moeten we nu maar laten rusten. In andere toepassingen van de wiskunde als toegepaste analyse is het vaak analyse of lineaire algebra, die het wiskundig model beschrijven. En dan zijn complexe getallen weer nuttig.

Meetkundige Aspecten van het Rekenen met Complexe Getallen

H.J.A. Duparc
Technische Universiteit Delft
Postbus 356, 2600 AJ Delft

0. Inleiding

Zoals in de voordracht van Van der Blij is uiteengezet (en iedere wiskundige eigenlijk al lang wist) zijn de complexe getallen bedacht om in de theorie van de algebraïsche vergelijkingen hinderlijke onregelmatigheden weg te nemen. Dankzij de complexe getallen bezitten alle vierkantsvergelijkingen wortels en als men ze wel telt, twee stuks. Van der Blij heeft ook laten zien dat de daarbij gebruikte uitbreiding van de verzameling der reële getallen nog wel meer nuttige eigenschappen heeft dan het alleen maar de theorie van de vierkantsvergelijkingen afhelpen van onregelmatigheden. Zo bezit dankzij de invoering van dat ene ding $i = \sqrt{-1}$ zelfs elke hogere machtsvergelijking wortels en ook - mits men ze wederom verstandig telt - evenveel als de graad bedraagt.

Maar ook daarbij blijft het niet. Met de complexe getallen kun je nog veel meer doen. Het feit dat ze het aantal wortels van een hogere-machts vergelijking redden, werkt door in allerlei meetkundige zaken zoals het aantal snijpunten van twee vlakke kromme lijnen, het aantal snijpunten van drie oppervlakken in de ruimte enz. Ook helpen de complexe getallen om op passende wijze in de projectieve meetkunde een metriek in te voeren.

Anderzijds is het feit dat de complexe getallen twee-dimensionaal zijn aanleiding ze te gebruiken bij problemen in de twee-dimensionale meetkunde, alias het complexe vlak.

Verder kunnen complexe getallen helpen in allerlei algebraïsche en getallentheoretische zaken en juist daarvan zullen hieronder enkele voorbeelden volgen.

1. TOEPASSINGEN IN ALGEBRA/GETALLENTHEORIE

We beschouwen de functie

$$f_n(z) = (z+1)^n - z^n - 1 \quad (n \in \mathbb{N}).$$

Weliswaar komt deze hier uit de lucht vallen, maar verderop zal blijken wat we eraan hebben. Het is duidelijk dat $f_n(z)$ een veelterm van de graad $n-1$ is en dat het getal 0 er een nulpunt van is. Voor bepaalde n (namelijk oneven n) is ook het getal -1 er een nulpunt van. Als gevolg hiervan is $f_3(z)$ direct in lineaire factoren te ontbinden (overigens zou dat ook wel lukken zonder deze beschouwing). Met $f_5(z)$ is het iets ingewikkelder gesteld, maar een korte berekening leert dat geldt

$$f_5(z) = 5z(z+1)(z^2+z+1).$$

De laatste factor heeft de welbekende nulpunten $\rho = -\frac{1}{2}+\frac{1}{2}i\sqrt{3}$ en $\overline{\rho} = \rho^2 = -\frac{1}{2}-\frac{1}{2}i\sqrt{3}$, zodat men tenslotte vindt

$$f_5(z) = 5z(z+1)(z-\rho)(z-\rho^2).$$

Wat zou er met $f_7(z)$ aan de hand zijn? Om die vraag te beantwoorden bekijken we een totaal ander probleem: kan $f_n(z)$ meervoudige nulpunten hebben?

Nu is bekend dat een meervoudig nulpunt van een polynoom f tevens een nulpunt is van de afgeleide f' (en omgekeerd, mits goed geformuleerd).
Uit

$$f'_n(z) = n(z+1)^{n-1} - nz^{n-1}$$

volgt dat zo'n meervoudig nulpunt voldoet aan

$$(z+1)^n - z^n - 1 = 0 \tag{1}$$

$$(z+1)^{n-1} - z^{n-1} = 0. \tag{2}$$

Invullen van (2) in (1) levert

$$(z+1)z^{n-1} - z^n - 1 = 0$$

dus

$$z^{n-1} - 1 = 0. \tag{3}$$

Zo'n nulpunt voldoet dus aan $|z|^{n-1} = 1$, d.w.z. het ligt op de eenheidscirkel $|z| = 1$. Er is echter nog een andere confrontatie van de relaties (1) en (2) mogelijk. Door z^{n-1} te 'elimineren' ontdekt men ook

$$(z+1)^n - z(z+1)^{n-1} - 1 = 0,$$

dus

$$(z+1)^{n-1} - 1 = 0. \tag{4}$$

Ons nulpunt voldoet dus ook aan $|z+1|^{n-1} = 1$, d.w.z. het ligt op de cirkel $|z+1| = 1$.

Het moet dus op beide genoemde cirkels liggen en men behoeft nauwelijks een tekening in het complexe vlak te maken om te zien dat slechts de punten ρ en $\bar{\rho}$ de gezochte snijpunten zijn. We kijken nu naar de argumenten.

Uit $\arg \rho = \frac{2}{3}\pi$ volgt wegens (3) de relatie

$$\frac{2}{3}\pi(n-1) = 2k\pi,$$

dus $n = 3k+1$.

Relatie (4) onthult ons nog meer, want uit $\arg(\rho+1) = \frac{1}{3}\pi$ volgt

$$\frac{1}{3}\pi(n-1) = 2k\pi,$$

dus

$$n = 6k+1.$$

Voorbijgaande aan het flauwe geval $k = 0$ levert het geval $k = 1$, dus $n = 7$ ons dat

$$\begin{aligned} f_7(z) = (z+1)^7 - z^7 - 1 &= 7z(z+1)(z^2+z+1)^2 \\ &= \frac{7}{5}(z^2+z+1)\, f_5(z). \end{aligned}$$

Wie gehoopt had dat voor $k = 2$ iets dergelijks geldt, komt - ten dele - bedrogen uit. Wel bezit $f_{11}(z)$ naast 0 en 1 ook de nulpunten ρ en $\bar{\rho}$; immers $(\rho+1)^{11} - \rho^{11} - 1 = (-\rho^2)^{11} - \rho^{11} - 1 = -\rho^{22} - \rho^{11} - 1 = -\rho - \rho^2 - 1 = 0$, en bezit $f_{13}(z)$ deze nulpunten ook (dat volgt uit het voorgaande, waar bleek dat $f_{13}(z)$ de nulpunten ρ en $\bar{\rho}$ zelfs dubbel heeft), maar $f_{13}(z)$ is niet het product van een constante, z^2+z+1 en $f_{11}(z)$. Er geldt namelijk

$$f_{11}(z) = 11z(z+1)(z^2+z+1)(z^6+3z^5+7z^4+9z^3+7z^2+3z+1)$$

en

$$f_{13}(z) = 13z(z+1)(z^2+z+1)^2(z^6+3z^5+8z^4+11z^3+8z^2+3z+1),$$

zodat men heeft

$$\frac{f_{13}}{13} - (z^2+z+1)\frac{f_{11}}{11} = z^3(z+1)^3(z^2+z+1)^2.$$

Achteraf bezien is deze relatie niet verbazingwekkend, want het linkerlid (en een passend aantal afgeleiden ervan) bezit de nulpunten 0, -1, ρ en ρ^2.

Nu gaan wij in op de reden van ons bovenstaand onderzoek over de polynomen $f_n(z)$. Het zal duidelijk zijn dat zij in nauwe relatie staan tot uitdrukkingen

$$F_n(a,b) = (a+b)^n - a^n - b^n.$$

Zo heeft men bijvoorbeeld

$$F_5(a,b) = (a+b)^5 - a^5 - b^5 = 5ab(a+b)(a^2+ab+b^2)$$

en men vermoedt al dat hier een verband kan worden gelegd met het vermoeden van Fermat dat de diophantische vergelijking $a^n + b^n = c^n$ voor natuurlijke a,b,c en $n > 2$ geen oplossing bezit. Het is bekend dat voor $n = 2^k$ ($k \in \mathbb{N}$) het probleem volledig is opgelost en verder is het duidelijk dat het vermoeden bewezen is voor alle bedoelde n, zodra het bewezen is voor de oneven priemgetallen n. Het gaat dan om de relatie

$$a^p + b^p = c^p \quad (p \text{ oneven priem}).$$

Nu pleegt men daarbij 2 gevallen te onderscheiden:

$$p \mid abc \text{ en } p \nmid abc.$$

In het vervolg beperken wij ons tot het laatste (zgn. eerste) geval. Volgens de (kleine) stelling van Fermat heeft men $a^p - a \equiv b^p - b \equiv c^p - c \pmod p$ zodat geldt

$$a + b \equiv c \pmod p$$

en dus

$$(a+b)^p \equiv c^p \pmod{p^2}.$$

Dan moet dus gelden

$$(a+b)^p - a^p - b^p \equiv 0 \pmod{p^2}.$$

en hier komen onze uitdrukkingen $F_p(a,b)$ voor de dag. Voor $p = 5$ gaan wij nu verder: Er komt

$$(a+b)^5 - a^5 - b^5 \equiv 0 \pmod{25},$$

dus

$$5ab(a+b)(a^2+ab+b^2) \equiv 0 \pmod{25}.$$

Wegens $5 \nmid a$, $5 \nmid b$, $5 \nmid c$ (dus $5 \nmid a+b$) krijgt men

$$a^2 + ab + b^2 \equiv 0 \pmod 5,$$

dus

$$a^3 \equiv b^3 \pmod 5.$$

Ook heeft men $a^4 \equiv b^4$ ($\equiv 1$) (mod 5), waarna men achtereenvolgens vindt

$$a \equiv b \pmod 5.$$

$$a + b \equiv 2b \pmod 5,$$

$$a^5 \equiv b^5 \pmod{25},$$

$$(a+b)^5 \equiv 2^5 b^5 \pmod{25}$$

dus

$$0 = F_5(a,b) \equiv 2^5 b^5 - b^5 - b^5 \pmod{25}$$

$$2^5 - 2 \equiv 0 \pmod{25},$$

een tegenspraak!

Natuurlijk vraagt men zich nu af of een analoge behandeling voor het geval $n = 3$ mogelijk is. Inderdaad voor $a^3 + b^3 = c^3$ met $3 \nmid abc$ heeft men op analoge wijze als bij $n = 5$ successievelijk

$$c \equiv c^3 = a^3 + b^3 \equiv a + b \pmod 3,$$

$$c^3 \equiv (a+b)^3 \pmod 9,$$

dus

$$0 = c^3 - a^3 - b^3 \equiv (a+b)^3 - a^3 - b^3 = 3ab(a+b) \pmod 9,$$

dus

$$3 \mid ab(a+b).$$

Wegens $3 \nmid ab$ heeft men dan $3 \mid a+b$, dus $3 \mid a^3 + b^3$, dus $3 \mid c^3$, dus $3 \mid c$, een contradictie.

Ook voor $p = 11$ is een verwante redenering mogelijk. Evenals in de andere gevallen heeft men $c \equiv a + b \pmod{11}$, $c^{11} \equiv (a+b)^{11} \pmod{11^2}$, dus

$$F_{11}(a,b) = (a+b)^{11} - a^{11} - b^{11} \equiv 0 \pmod{11^2}.$$

Dus

$$11 \mid ab(a+b)(a^2 + ab + b^2)(a^6 + 3a^5b + 7a^4b^2 + 9a^3b^3 + 7a^2b^4 + 3ab^5 + b^6). \quad (5)$$

Nu heeft men $11 \nmid ab$, $11 \nmid (a+b)$ (anders zou gelden $11 \mid c$, zie boven) en ook

$$11 \nmid a^2 + ab + b^2.$$

Gold nl. $11 \mid a^2 + ab + b^2$ dan had men $11 \mid a^3 - b^3$, dus

$$a^3 \equiv b^3 \pmod{11} \text{ en } a^{10} \equiv b^{10} \equiv 1 \pmod{11},$$

dus

$$a \equiv b \pmod{11}.$$

Dan vindt men $c \equiv a + b \equiv 2b \pmod{11}$, dus

$$c^{11} \equiv 2^{11} b^{11} \pmod{11^2} \text{ en } a^{11} \equiv b^{11} \pmod{11^2},$$

dus

$$0 = c^{11} - a^{11} - b^{11} \equiv (2^{11} - 1 - 1) b^{11} \pmod{11^2},$$

d.w.z.

$$11^2 \mid 2^{11} - 2,$$

alweer een contradictie.
Bijgevolg moet het getal 11 dus deelbaar zijn op de 6de graadsvorm in (5). Nu is deze mod 11 te ontbinden in

$$(a^2-ab+b^2)(a^4+4a^3b-a^2b^2+4ab^3+b^4).$$

Nu geldt $11 \nmid a^2-ab+b^2$, want anders had men

$$11 \mid a^3+b^3 \mid a^6-b^6 \mid a^{12}-b^{12},$$

dus

$$a^2 \equiv b^2 \pmod{11},$$

d.w.z.

$$a \equiv \pm b \pmod{11}.$$

Als boven blijkt $a \equiv b \pmod{11}$ niet mogelijk, terwijl $a \equiv -b \pmod{11}$ zou voeren tot $11 \mid c$ wat ook uitgesloten is. Tenslotte komt men tot

$$11 \nmid a^4+4a^3b-a^2b^2+4ab^3+b^4 \equiv (a+b)^4+4a^2b^2 \pmod{11}. \qquad (6)$$

Omdat $11 \equiv 3 \pmod 4$ is de enige mogelijkheid dat 11 deelbaar is op de beide componenten $(a+b)^2$ en $2ab$ van de in (6) optredende vierdegraads vorm en dat is op grond van de reeds eerder genoemde feiten niet mogelijk. Waarmee het vermoeden van Fermat ook voor het geval $n = 11$ is bewezen.

We gaan hier niet mee door, de uitdrukkingen $F_n(a,b)$ schrikken ons voor hogere n te zeer af! Het was al mooi genoeg dat de op complexe getallen geïnspireerde beschouwingen over ontbinding van bepaalde polynomen ons konden helpen aan een elementair bewijs van de stelling van Fermat voor een aantal gevallen.

2. Meetkundige toepassingen

Aardige meetkundige toepassingen van de theorie der complexe getallen ontmoet men op twee plaatsen: in het complexe vlak en in het projectieve vlak.

2A. Wij beginnen met het complexe vlak en beschouwen daarbij een afbeelding $w = f(z)$ van het z-vlak in het w-vlak. De afbeelding heet analytisch in een punt z_0 als in dat punt (en in een omgeving ervan) geldt dat de limiet

$$\lim_{h \to 0} \frac{f(z_0+h)-f(z_0)}{h}$$

bestaat, ongeacht de richting waarin h naar nul gaat.

Voert men de routinesplitsingen $z = x+iy$ en $w = u+iv$ in, dan leidt een en ander tot

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}\,;\; \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

Eliminatie hieruit van v voert via verdere (bij analytische functies toelaatbare) differentiatie tot

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0 \text{ (en analoog } \frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} = 0). \tag{7}$$

Het reële deel van een analytische functie voldoet dus aan de differentiaalvergelijking (7) van Laplace; een feit waarvan in de toegepaste wiskunde veel gebruik wordt gemaakt.

We komen nu terug tot de genoemde limiet en kunnen deze ook als volgt formuleren

$$\lim_{\Delta z \to 0} \frac{\Delta w}{\Delta z} = f'(z_0).$$

We willen nu nagaan of de complexe afgeleide een meetkundige betekenis heeft (evenzeer als de reële dat heeft). Voor voldoend kleine $|\Delta z|$ geldt dus de benaderingsrelatie

$$\Delta w \approx f'(z)\Delta z.$$

Als nu geldt $f'(z) \neq 0$ heeft men

$$|\Delta w| \approx |f'(z)| \cdot |\Delta z|; \text{ arg } \Delta w \approx \text{arg } f'(z) + \text{arg}\Delta z.$$

Dit houdt in dat een kromme in het z-vlak overgaat in een kromme in het w-vlak waarbij een schaalverandering met een factor $|f'(z_0)|$ en een koersverandering met een bedrag arg $f'(z_0)$ plaatsvindt.

Voor twee krommen door een punt z_0 geldt dan dat na transformatie hun hoek behouden blijft; de transformatie heet conform.

We passen dit eens toe op de afbeelding $w = e^z$ en gaan uit in het z-vlak van twee soorten 'krommen':

I rechten evenwijdig met de reële as;

II rechten evenwijdig met de imaginaire as.

De 'krommen' van de typen I en II voldoen respectievelijk aan

$$z = x + ib \text{ (b constant)}; \; z = a + iy \text{ (a constant)}.$$

Hun beeldfiguren voldoen resp. aan

$$w = e^x e^{ib}, \text{ dus arg } w = b;$$

$$w = e^a e^{iy}, \text{ dus } |w| = e^a.$$

Het zijn dus in het w-vlak rechten door 0, resp. cirkels met 0 als middelpunt. Aangezien de 'krommen' I en II loodrecht op elkaar staan, is dat ook het geval met de beeldfiguren, dus met de rechten door 0 en de cirkels 'om' 0. Hiermede is (andermaal) bewezen dat bij een cirkel de raaklijn in een punt loodrecht staat op de straal naar het raakpunt.

Een ander voorbeeld levert ons de transformatie $w = z + \frac{1}{z}$. We beschouwen weer twee onderling orthogonale stelsels figuren in het z-vlak:

I de rechten arg $z =$ constant;

II de cirkels $|z|$ = constant.

Voor de eerste categorie geldt $z = re^{i\alpha}$ (α constant) dus

$$w = re^{i\alpha} + \frac{1}{r}e^{-i\alpha} = (r + \frac{1}{r})\cos\alpha + i(r - \frac{1}{r})\sin\alpha \tag{8}$$

dus

$$u = (r + \frac{1}{r})\cos\alpha;\ v = (r - \frac{1}{r})\sin\alpha.$$

Eliminatie van r geeft (mits $\alpha \neq \frac{1}{2}k\pi$, k geheel)

$$\frac{u^2}{4\cos^2\alpha} - \frac{v^2}{4\sin^2\alpha} = 1,$$

een hyperbool met brandpunten $E(c, 0)$ en $F(-c, 0)$ waarbij

$$c = \sqrt{4\cos^2\alpha + 4\sin^2\alpha} = 2.$$

De beeldkrommen van het tweede type worden ook door (8) bepaald, maar nu met r constant en α variabel. Eliminatie van α uit de formules voor u en v levert (mits $r \neq 1$)

$$\frac{u^2}{(r + \frac{1}{r})^2} + \frac{v^2}{(r - \frac{1}{r})^2} = 1,$$

een ellips met brandpunten $(c, 0)$ en $(-c, 0)$, waarbij

$$c = \sqrt{(r + \frac{1}{r})^2 + (r - \frac{1}{r})^2} = 2$$

Doordat de ellipsen en de hyperbolen dezelfde brandpunten hebben, zullen in hun snijpunten P de raaklijnen loodrecht op elkaar staan (ze zijn immers de binnen- en buitenbisectrices van hoek EPF); dit is geheel in overeenstemming met het feit dat de krommen van de stelsels I en II in het z-vlak ook loodrecht op elkaar staan.

De transformatie is niet-conform in de punten z waarvoor geldt $f'(z) = 1 - \frac{1}{z^2} = 0$, dus in de punten $z = \pm 1$. De lezer kan dit onderkennen door ook de beeldfiguren na te gaan van de buiten beschouwing gelaten uitzonderingsgevallen voor α en r.

Een en ander hangt samen met het feit dat bij een punt z_0 met $f'(z_0) = 0$ (en $f''(z_0) \neq 0$) de Taylor-ontwikkeling van $f(z)$ leert dat

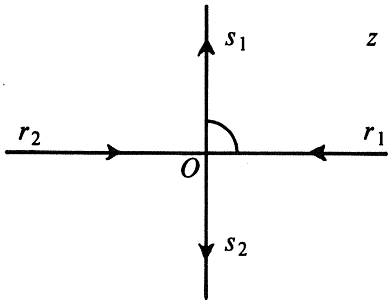
$$\Delta w \approx \frac{1}{2}(\Delta z)^2 f''(z_0),$$

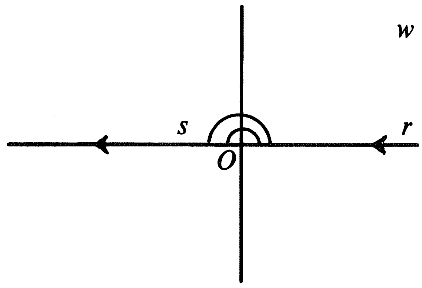
dus

$$\arg\Delta w \approx 2\arg\Delta z + \arg f''(z_0),$$

zodat dan hoekverdubbeling optreedt. Dit komt erop neer dat de hoek tussen twee krommen door z_0 in het z-vlak de helft is van die tussen hun door $w_0 = f(z_0)$ gaande beeldkrommen in het w-vlak.

Het is interessant tot slot dit alles te illustreren aan de transformatie $z = w^{\frac{1}{2}}$, die in nauw verband staat met het voorafgaande. We laten w nu de reële as doorlopen van $+\infty$ naar $-\infty$. Is $w = u > 0$, dan heeft het symbool $u^{\frac{1}{2}}$ twee, onderling tegengestelde reële betekenissen; is $u = 0$, dan is $u^{\frac{1}{2}} = 0$ en is $u < 0$, dan heeft het symbool $u^{\frac{1}{2}}$ twee onderling tegengestelde zuiver imaginaire betekenissen





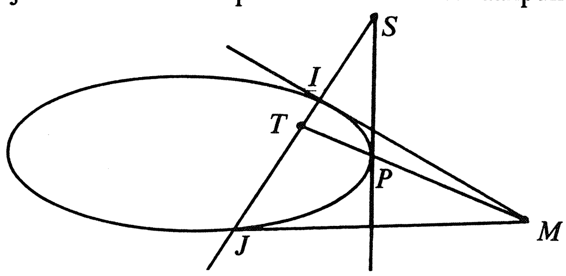
De hoek tussen r_1 en s_1 is de helft van die tussen r en s. Een en ander is toe te passen op de bekende wortelformule $z_{1,2} = \frac{-b + \sqrt{D}}{2a}$ voor de wortels van de vierkantsvergelijking $az^2 + bz + c = 0$ en leert ons andermaal hoe de ligging van de wortels afhangt van de discriminant $D = b^2 - 4ac$.

2B. We willen het meetkundeverhaal besluiten met enkele opmerkingen over het projectieve vlak. Het blijkt nuttig dit uit te breiden tot het complexe projectieve vlak, dat is de verzameling der punten (p_0, p_1, p_2) waarvan de homogene coördinaten p_0, p_1 en p_2 in $\mathbb{C}$ liggen.

Het is bekend dat de punten $I(0,1,i)$ en $J(0,1,-i)$ een belangrijke rol spelen om het Euclidische vlak uit het complexe te verkrijgen.

Kegelsneden (tweedegraads krommen) door I en J ontpoppen zich als cirkels, zodat twee cirkels als rechtschapen tweedegraads krommen inderdaad $2 \times 2 = 4$ snijpunten hebben: de 'gewone' en I en J.

De grootte van een hoek gevormd door twee elkaar in een punt S snijdende rechten a en b blijkt te zijn $\frac{1}{2i}\ln D$, waarbij D de dubbelverhouding is van de 4 rechten a, b, SI en SJ. Met een beetje pooltheorie blijkt nu opnieuw dat bij een cirkel een raaklijn loodrecht staat op de straal door het raakpunt.



Hiermee beschouwen we het middelpunt M van een cirkel als pool van de oneigenlijke rechte IJ. Verder beschouwen we een punt P op de cirkel en de raaklijn in P aan de cirkel, die IJ in een punt S snijdt. Dan is PS de poollijn van P en IJ de poollijn van M. Dus PM is de poollijn van S, zodat S en T harmonisch liggen met I en J. De dubbelverhouding $(STIJ)$ is dus gelijk aan -1 en de grootte van hoek TPS is dan gelijk aan $\frac{1}{2i}\ln(-1)=\frac{1}{2}\pi$.

Bij een kegelsnede kan men de brandpunten typeren als de punten vanwaaruit de raaklijnen aan de kegelsnede door de punten I en J gaan (isotroop zijn). Men kan het ook omgekeerd formuleren: De raaklijnen uit I en J aan een kegelsnede snijden elkaar in brandpunten van die kegelsnede. Bijgevolg heeft een kegelsnede zo beschouwd dus 4 brandpunten. In de praktijk zijn er behalve de twee op de ene as op afstand c van het middelpunt gelegen, ook nog twee op de andere as, op 'afstand' ci van het middelpunt gelegen; die twee 'andere' brandpunten zijn dus niet reëel.

We geven nog een enkele eigenschap bij het bewijs waarvan de punten I en J goede diensten kunnen bewijzen. Trekt men een rechte r door een brandpunt F en de raaklijnen aan de kegelsnede in de snijpunten van r en de kegelsnede, die elkaar in een punt R snijden, dan geldt $FR \perp r$. Inderdaad, omdat R de pool is van r liggen de rechten FR en r dus poolverwant ten opzichte van de kegelsnede en derhalve harmonisch met de raaklijnen FI en FJ uit F aan de kegelsnede. Dus de dubbelverhouding (r,FR,FI,FJ) is -1, zodat de grootte van de hoek tussen r en FR, evenals hierboven, $\frac{1}{2}\pi$ blijkt te zijn.

Algebraïsche en Arithmetische Eigenschappen van Complexe Getallen

A.W. Grootendorst
Technische Universiteit Delft
Postbus 356, 2600 AJ Delft

1. Inleiding

Generalisatie zit de wiskundigen in het bloed. Het onderwerp van deze voordracht is óók een voorbeeld van generalisatie. Het uitgangspunt hierbij is de ring $\mathbf{Z}$ van de 'gewone' gehele getallen $\ldots -3, -2, -1, 0, 1, 2, 3, \ldots$, (officieel de *gehele rationale getallen* genoemd) met de gebruikelijke optelling en vermenigvuldiging als operatie. $\mathbf{Z}$ wordt daarbij beschouwd als een deelring van het lichaam van de rationale getallen. Van de vele daarbij optredende begrippen en eigenschappen lichten we er enkele essentiële uit:

1. Het begrip *deelbaarheid*: $a \in \mathbf{Z}$, heet deelbaar op $b \in \mathbf{Z}$ (notatie $a|b$) indien er een $c \in \mathbf{Z}$ bestaat zodanig dat $b = ac$. Indien $a|b$ maar niet $b|a$ (notatie $b \nmid a$), dan heet a een *echte deler* van b. Indien $a|b$ en $b|a$ (en dus $a = \pm b$) dan heten a en b *geassocieerd*. De studie van de deelbaarheid speelt een belangrijke rol in de arithmetica van de gehele rationale getallen.
2. Het begrip *eenheid*: $e \in \mathbf{Z}$ heet een eenheid indien e een deler is van 1. Het is duidelijk dat in $\mathbf{Z}$ de enige eenheden zijn 1 en -1.
3. Het begrip *priemgetal*: $p \in \mathbf{Z} (p \neq \pm 1)$ heet rationaal priemgetal indien p als enige delers heeft eenheden en met p geassocieerden, dus in $\mathbf{Z}$ zijn die delers ± 1 en $\pm p$. In $\mathbf{Z}$ heeft elk priemgetal de karakteristieke eigenschap: indien $p|ab$, dan $p|a$ of $p|b$ (of beide!).
4. Het begrip *absolute waarde* van $a \in \mathbf{Z}$, notatie $|a|$, waarbij $|a| \in \{0, 1, 2, 3, \ldots\}$ en de multiplicatieve eigenschap geldt: $|ab| = |a| \cdot |b|$.
5. De *delings-algoritme*: bij ieder tweetal elementen a en b van $\mathbf{Z}$ $(b \neq 0)$ bestaan elementen q en r van $\mathbf{Z}$, zodat $a = bq + r$ met $0 \leqslant |r| < |b|$. N.B. q en r zijn niet eenduidig bepaald: $17 = 6 \cdot 2 + 5$ $(0 \leqslant |5| < |6|)$, maar ook: $17 = 6 \cdot 3 + 1(-1)$ $(0 \leqslant |-1| < |6|)$. Aan deze algoritme danken de priemgetallen de sub 3 genoemde karakteristieke eigenschap. Voorts volgt

eruit dat elk 2-tal elementen a en b van $\mathbb{Z}$ een g.g.d. (notatie: (a,b)) heeft die met geschikt gekozen u en v in $\mathbb{Z}$ te schrijven is in de gedaante $ua+bv$. Tenslotte volgt daaruit dat elk rationaal geheel getal een éénduidige ontbinding in priemfactoren heeft.

2. Een voor de hand liggende vraag

Wanneer we nu de beschikking krijgen over een veel uitgebreider lichaam dan $\mathbb{Q}$, namelijk het lichaam $\mathbb{C}$ van de complexe getallen, dan ligt het voor de hand de vraag te stellen wat we nu gehele getallen zullen noemen in dit lichaam. We zouden willen dat de eigenschappen 1 tot en met 5 blijven gelden, maar bovenal dat de 'gewone' gehele getallen ook voldoen aan onze nieuwe definitie van gehele getallen.

Voorlopig stellen we ons enigszins bescheiden op en beschouwen niet alle complexe getallen maar *kwadratische uitbreidingen* $\mathbb{Q}(\sqrt{m})$ van $\mathbb{Q}$, d.w.z. lichamen gevormd door getallen van de gedaante $a+b\sqrt{m}$, met a en $b\in\mathbb{Q}$, $m\in\mathbb{Z}$ en m kwadraatvrij (d.w.z. zonder kwadratische factoren). Men ziet eenvoudig in dat deze getallen, bij vastgekozen m, een *lichaam* vormen. Ook is duidelijk dat $\alpha\in\mathbb{Q}(\sqrt{m})$, met $\alpha=a+b\sqrt{m}$, voldoet aan de vergelijking

$$x^2-2ax+a^2-b^2m=0. \qquad (*)$$

Indien $\alpha\notin\mathbb{Q}$, dan voldoet α niet aan een vergelijking van lagere graad met coëfficiënten in $\mathbb{Q}$. Men noemt de vergelijking (*) de *definiërende vergelijking* van α. Deze is te brengen in de gedaante $Ax^2+Bx+C=0$ met $A,B,C\in\mathbb{Z}$ en $(A,B,C)=1$. Een rationaal getal voldoet aan een vergelijking $Ax+B=0$ met $A,B\in\mathbb{Z}$ en $(A,B)=1$ en heet *geheel rationaal* indien $A=1$. Analoog zullen we $\alpha\in\mathbb{Q}(\sqrt{m})$ *(kwadratisch) geheel algebraïsch* noemen indien α voldoet aan een algebraïsche vergelijking van de gedaante $x^2+Bx+C=0$ met kopcoëfficiënt 1 en $B,C\in\mathbb{Z}$. Men rekent dan eenvoudig na dat de gehelen in $\mathbb{Q}(\sqrt{m})$ een ring vormen (zelfs een integriteitsgebied) en dat alle elementen van $\mathbb{Z}$ er toe behoren.

3. Hoe zien de gehelen in $\mathbb{Q}(\sqrt{m})$ eruit?

We zagen dat $\alpha=a+b\sqrt{m}$, behorende tot $\mathbb{Q}(\sqrt{m})$, voldoet aan:

$$x^2-2ax+a^2-b^2m=0 \quad (a,b\in\mathbb{Q})$$

en geheel algebraïsch is indien alle coëfficiënten in $\mathbb{Z}$ liggen, dus $2a\in\mathbb{Z}$ en $a^2-b^2m\in\mathbb{Z}$. d.w.z. $a=\frac{u}{2}$ $(u\in\mathbb{Z})$ en, omdat m kwadraatvrij is, volgt uit $\frac{u^2}{4}-b^2m\in\mathbb{Z}$ dat $b=\frac{v}{2}(v\in\mathbb{Z})$ dus $\alpha=\frac{u}{2}+\frac{v}{2}\sqrt{m}$ met $\frac{u^2-v^2m}{4}\in\mathbb{Z}$, dus $u^2-v^2m\equiv0$ (mod 4).

Nu is het kwadraat van een even getal een viervoud, en het kwadraat van een oneven getal een viervoud plus één. Wanneer we de volgende congruenties alle modulo 4 opvatten, krijgen we het volgende overzicht:

$m\equiv 1 \pmod 4$			$m\equiv 2 \pmod 4$			$m\equiv 3 \pmod 4$		
u^2	v^2	u^2-mv^2	u^2	v^2	u^2-mv^2	u^2	v^2	u^2-mv^2
$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$	$\equiv 0$
$\equiv 0$	$\equiv 1$	$\equiv 3$	$\equiv 0$	$\equiv 1$	$\equiv -2$	$\equiv 0$	$\equiv 1$	$\equiv -3$
$\equiv 1$	$\equiv 0$	$\equiv 1$	$\equiv 1$	$\equiv 0$	$\equiv 1$	$\equiv 1$	$\equiv 0$	$\equiv 1$
$\equiv 1$	$\equiv 1$	$\equiv 0$	$\equiv 1$	$\equiv 1$	$\equiv -1$	$\equiv 1$	$\equiv 1$	$\equiv -2$

dus:

A. $m\equiv 1 \pmod 4$: $u^2-mv^2\equiv 0 \pmod 4 \Leftrightarrow u^2-v^2\equiv 0 \pmod 4 \Leftrightarrow u+v\equiv 0 \pmod 2 \Leftrightarrow u=-v+2h$ dus $\alpha\in\mathbb{Q}(\sqrt{m})$ is in dit geval geheel algebraïsch dan en slechts dan als $\alpha=\frac{u}{2}+\frac{v}{2}m$ met $u=-v+2h$ dus $\alpha=h+v(-\frac{1}{2}+\frac{1}{2}\sqrt{m})$, waarbij $h,\ v\in\mathbb{Z}$.

B. $\left.\begin{array}{l} m\equiv 2 \pmod 4 \\ m\equiv 3 \pmod 4\end{array}\right\}: u^2-mv^2\equiv 0 \pmod 4 \Leftrightarrow u^2\equiv v^2\equiv 0 \pmod 4.$

Dus u is even en tevens v even; bijvoorbeeld resp. $u=2\lambda$ en $v=2\mu$ dus: $\alpha=\lambda+\mu\sqrt{m}$ $(\lambda,\mu\in\mathbb{Z})$.

We kunnen A en B samenvatten:
De gehelen in $\mathbb{Q}(\sqrt{m})$ hebben een $\mathbb{Z}$-basis:

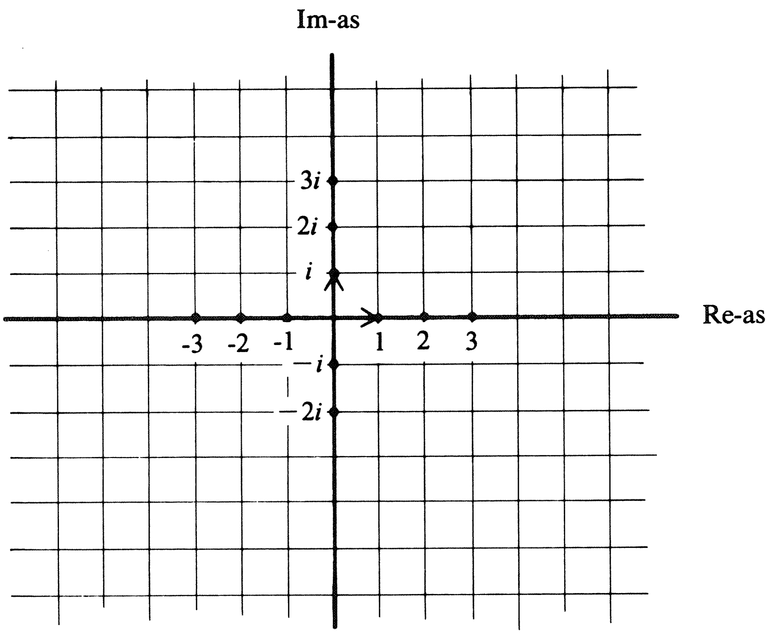
$\{1, \frac{-1+\sqrt{m}}{2}\}$ indien $m\equiv 1 \pmod 4$

$\{1, \sqrt{m}\}$ indien $m\equiv 2$ of $m\equiv 3 \pmod 4$.

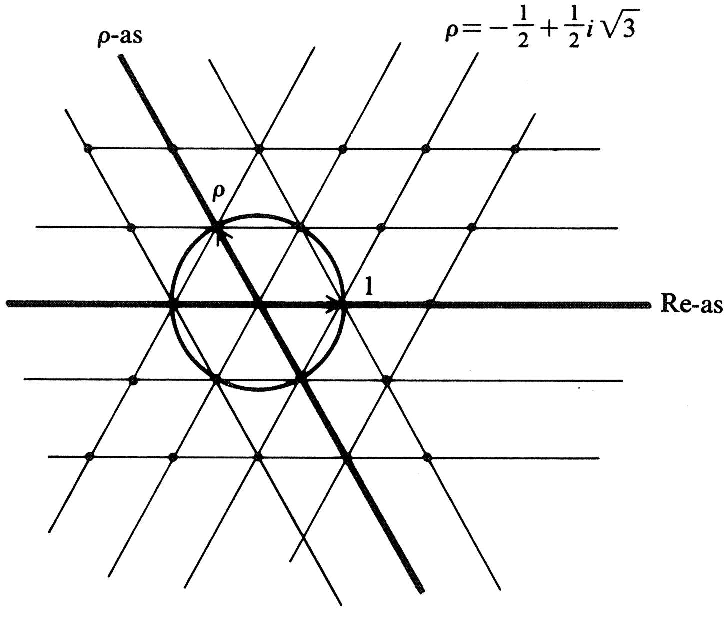
N.B. Wanneer we zeggen dat de gehelen in $\mathbb{Q}(\sqrt{m})$ een $\mathbb{Z}$-basis $\{\alpha,\beta\}$ hebben dan bedoelen we daarmee dat elk geheel getal in $\mathbb{Q}(\sqrt{m})$ op één doch slechts één manier te schrijven is in de gedaante $a\alpha+b\beta$ met $a,b\in\mathbb{Z}$.

De gehelen in $\mathbb{Q}(i)$ zijn dus: $a+bi$ (a en $b\in\mathbb{Z}$). Dit zijn de zogenaamde *gehelen van Gauss* (1777-1855). De gehelen in $\mathbb{Q}(i\sqrt{3})$ (d.w.z. $m=-3$) zijn dus $a+b\frac{-1+i\sqrt{3}}{2}$ (a en $b\in\mathbb{Z}$). Dit zijn de zogenaamde *gehelen van Eisenstein* (1823-1852). We kunnen de gehelen van Gauss weergeven als roosterpunten in een vlak rooster, gevormd door vierkanten met zijdelengte 1 en de gehelen van Eisenstein als roosterpunten in een vlak rooster, gevormd door ruiten met hoeken van 60° en 120° en zijdelengte 1. (Zie figuur 1 en figuur 2.)

In het vervolg stellen we $\rho=\frac{-1+i\sqrt{3}}{2}$, dus ρ is een complexe derdemachts wortel uit 1 en voldoet aan: $\rho^2+\rho+1=0$.



FIGUUR 1



FIGUUR 2

4. Wat blijft er over van de eigenschappen van de 'gewone' gehele getallen?

Het is duidelijk dat het begrip 'deelbaarheid' en het begrip 'eenheid' direct overgenomen kunnen worden. De vraag welke gehelen eenheid zijn, kunnen we eerst beantwoorden als we het begrip *absolute waarde* gegeneraliseerd hebben. Daartoe voeren we het begrip *'norm'* in.

De *norm* van het getal $\alpha = a + b\sqrt{m}$ behorende tot $\mathbb{Q}(\sqrt{m})$, definiëren we m.b.v. de *geconjugeerde* $\bar{\alpha}$ van α die bepaald is door $\bar{\alpha} = a - b\sqrt{m}$. Deze is dus de andere wortel van de definiërende vergelijking van α. De norm $N(\alpha)$ van α is nu gedefinieerd door: $N(\alpha) = \alpha\bar{\alpha}$.

Men ziet direct in: $N(\alpha) \in \mathbb{Q}$ en $N(\alpha) \in \mathbb{Z}$ als α kwadratisch geheel is; $N(\alpha) = 0 \Leftrightarrow \alpha = 0$ en $N(\alpha) \geqslant 0$ als $m < 0$.

Zo geldt in $\mathbb{Z}[i]$: $N(\alpha) = a^2 + b^2$, maar voor de gehelen van Eisenstein geldt:

$$\alpha = a + b\frac{-1 + i\sqrt{-3}}{2} = a + b\rho \quad (a, b \in \mathbb{Z})$$

en

$$\bar{\alpha} = a + b\frac{-1 - i\sqrt{-3}}{2} = a + b\rho^2$$

dus $N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2$. Voorts rekent men eenvoudig na dat deze norm de multiplicatieve eigenschap heeft:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Voor $m = -1$, dus $\alpha = a + bi$ en $\beta = c + di$ $(a, b, c, d \in \mathbb{Z})$ betekent dit:

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2).$$

Met andere woorden: als twee elementen in $\mathbb{Z}$ elk de som zijn van 2 kwadraten, dan is hun produkt dat ook. Dit was al bekend aan Fibonacci (ca. 1200 na Chr.). We zijn nu in staat om de eenheden in de ring F van de gehelen in $\mathbb{Q}(\sqrt{m})$ te karakteriseren, en wel met het volgende

Kenmerk: Indien α geheel is in $\mathbb{Q}(\sqrt{m})$ dan is α eenheid dan en slechts dan als $N(\alpha) = \pm 1$.

Bewijs:

1. Indien α eenheid is, dan is er een geheel getal β z.d.d. $\alpha\beta = 1$ dus $N(\alpha\beta) = N(\alpha).N(\beta) = N(1) = 1$ dus $N(\alpha) = \pm 1$.
2. Indien $N(\alpha) = \pm 1$, dan geldt $\alpha\bar{\alpha} = 1$ of $\alpha\bar{\alpha} = -1$ dus $\alpha(-\bar{\alpha}) = 1$. In beide gevallen is er een kwadratisch geheel getal dat met α vermenigvuldigd 1 oplevert dus $\alpha | 1$, dus α eenheid.

Dit kenmerk stelt ons in staat om alle eenheden in F te berekenen. Voor de *gehelen van Gauss* is direct te zien:

$\alpha = a + bi$ is eenheid dan en slechts dan als $a^2 + b^2 = 1$. De enige mogelijkheden zijn dus $\alpha = \pm 1$, $\alpha = \pm i$.

De eenheden in de andere kwadratische lichamen bepalen we aldus: We zagen eerder: de gehelen van $\mathbb{Q}(\sqrt{m})$ zijn van de gedaante

$$a + b\sqrt{m} \qquad \text{als } m \equiv 2 \text{ of } m \equiv 3 \,(\text{mod } 4)$$

$$a + \frac{-1+\sqrt{m}}{2}b \qquad \text{als } m \equiv 1 \,(\text{mod } 4),$$

waarbij geldt: a en $b \in \mathbb{Z}$.

Het eenvoudigste geval is: $m<0$. We onderscheiden daarbij 2 gevallen:

A. $m<0$, $m\equiv 2$ of $m\equiv 3$ (mod 4)
Dan geldt: $\alpha = a + b\sqrt{m}$ is eenheid dan en slechts dan als $N(\alpha) = \pm 1$, dus $a^2 - mb^2 = \pm 1$, maar $m<0$ dus $a^2 - b^2 m = 1$. Enige mogelijkheid: $a = \pm 1$, $b=0$ als $m < -1$ (en tevens $\equiv 2$ of $\equiv 3$ (mod 4)).

B. $m<0$, $m\equiv 1$ (mod 4).
In dit geval geldt: $\alpha = a + \frac{-1+\sqrt{m}}{2}b$ is eenheid dan en slechts dan als $N(\alpha) = \pm 1$, dus $(a - \frac{b}{2})^2 - \frac{b^2}{4}m = \pm 1$ dus $(2a-b)^2 - b^2 m = \pm 4$. We bekijken $(2a-b)^2 - b^2 m = \pm 4$ nader. Daar $m<0$, vervalt -4, dus we moeten oplossen:

$$(2a - b)^2 - b^2 m = 4.$$

Stel $m = -n$ dan: $(2a-b)^2 + b^2 n = 4$. Direct duidelijk als: $n > 4$ dan geen oplossing, behalve $b=0$, $a = \pm 1$. Dus rest: $n = 1,2,3$ maar $n=1$ en $n=2$ vervallen omdat dan $m \not\equiv 1$ (mod 4). Rest dus alleen $n=3$, $m=-3$ (d.w.z. de gehelen van Eisenstein), en dus $(2a-b)^2 + 3b^2 = 4$. Het is duidelijk dat de enige mogelijke oplossingen zijn:

$$2a - b = \pm 1 \text{ met } b = \pm 1$$

en

$$2a - b = \pm 2 \text{ met } b = 0$$

waaruit na een kleine berekening volgt dat de enige eenheden onder de gehelen van Eisenstein zijn: $\pm 1, \frac{\pm 1 \pm i\sqrt{3}}{2}$, oftewel: $\pm 1, \pm\rho, \pm\rho^2$ (ρ als te voren gedefinieerd).

Samengevat:
De eenheden in de ring van gehelen in $\mathbb{Q}(\sqrt{m})$ zijn voor $m<0$, m kwadraatvrij.

$$m = -1: \ 1, -1, i, -i$$

$$m = -3: \ +1, -1, \frac{\pm 1 \pm i\sqrt{3}}{2}$$

$$m = -2, -5, \ldots \text{ (kwadraatvrij) } : \pm 1.$$

De gevallen waarin $m>0$, dus wanneer het gaat om reële kwadratische getallen, vallen buiten het bestek van deze voordracht. Zij zijn ook veel moeilijker omdat we dan diophantische vergelijkingen van de gedaante

$$x^2 - my^2 = \pm 1 \text{ of } x^2 - my^2 = \pm 4 \quad (m>0)$$

moeten oplossen. Men noemt zo'n vergelijking een vergelijking van Fermat-Pell[1]. We gaan hierop niet nader in maar merken slechts op dat in deze gevallen er steeds *oneindig veel eenheden* zijn. Zo is in de ring van de gehelen van $\mathbb{Q}(\sqrt{2})$ elke macht van $1+\sqrt{2}$ eenheid $((1+\sqrt{2})(-1+\sqrt{2})=1)$ en al deze machten vormen alle eenheden daarin.

Terloops vermelden we nog dat de eenheden in $\mathbb{Q}(\sqrt{m})$ een *multiplicatieve groep* vormen hetgeen gemakkelijk te verifiëren is.

Het begrip *'geassocieerd'* kunnen we zonder meer overnemen voor kwadratische gehele getallen: we noemen α *geassocieerd* met β als $\alpha|\beta$ en tevens $\beta|\alpha$, hetgeen gelijkwaardig is met $\alpha=\beta\epsilon$ en $\beta=\alpha\epsilon'$, waarbij ϵ en ϵ' eenheden zijn. Immers uit $\alpha=\beta\epsilon$ en $\beta=\alpha\epsilon'$ volgt $\alpha(1-\epsilon\epsilon')=0$, dus daar $\alpha\neq 0$, geldt $\epsilon\epsilon'=1$. De relatie 'geassocieerd met' is ten duidelijkste een equivalentierelatie. In dit verband hebben we de volgende

Stelling:
Indien $\alpha|\beta$ en $N(\alpha)=\pm N(\beta)$ dan zijn α en β geassocieerd en omgekeerd: als α en β geassocieerd zijn dan - uiteraard - $\alpha|\beta$, maar ook $N(\alpha)=\pm N(\beta)$.

Bewijs:
1. Indien $\alpha|\beta$ dan is er een γ z.d.d $\beta=\alpha\gamma$, dus $N(\beta)=N(\alpha\gamma)=N(\alpha)N(\gamma)$, dus indien $N(\alpha)=\pm N(\beta)$, dan geldt $N(\gamma)=-\pm 1$, dus γ eenheid.
2. Indien α en β geassocieerd zijn, dan geldt $\alpha=\beta\epsilon$ met ϵ eenheid, dus $N(\alpha)=N(\beta\epsilon)=N(\beta)\cdot N(\epsilon)=\pm N(\beta)$.

Wanneer we nu - voorlopig - een priemgetal (zeg π) in de ring van de gehelen $\mathbb{Q}(\sqrt{m})$ definiëren als een getal dat *geen eenheid* is en dat als enige delers heeft eenheden en met π geassocieerden (dus geen echte delers) dan kunnen we afleiden de

Stelling:
Indien α geheel is in $\mathbb{Q}(\sqrt{m})$ en $N(\alpha)$ een rationaal priemgetal is, dan is α priem in $\mathbb{Q}(\sqrt{m})$.

Bewijs:
Stel $\alpha=\beta\gamma$, dan $N(\alpha)=N(\beta\gamma)=N(\beta)\cdot N(\gamma)$, maar $N(\alpha)$ is rationaal priem, dus $N(\gamma)=\pm N(\alpha)$ of $N(\gamma)=\pm 1$. In het eerste geval zijn α en γ geassocieerd en β een eenheid, in het tweede geval is γ een eenheid en β geassocieerd met α.

1. Pierre de Fermat (1601-1665); John Pell (1611-1685)

Voorbeeld:
$2+i$ is priem in $\mathbb{Z}[i]$, omdat $N(2+i)=5$ en 5 priem in $\mathbb{Z}$.

N.B.
Het omgekeerde van deze stelling geldt niet. Zo zal blijken dat 11 priem is in $\mathbb{Z}[i]$, maar toch geldt: $N(11)=121$ en dit is geen rationaal priemgetal.

5. DE DELINGS-ALGORITME EN DE EENDUIDIGE ONTBINDING IN PRIEMFACTOREN

Zoals bekend is, geldt in de ring $\mathbb{Z}$ van de 'gewone' gehele getallen de stelling van de eenduidige ontbinding in priemfactoren, die inhoudt dat elk geheel rationaal getal ($\neq 0, \neq \pm 1$) op één doch slechts één, manier te schrijven is als het produkt van priemgetallen althans indien men niet let op de volgorde daarvan en de eenheden. Zo is bijvoorbeeld $60=2^2\cdot 3\cdot 5$, maar ook geldt $60=-2\cdot 3\cdot -5\cdot -2$.

Deze stelling kan men voor $\mathbb{Z}$ bewijzen met behulp van de in $\mathbb{Z}$ geldende delings-algoritme. Daaruit volgt namelijk allereerst de existentie van priemgetallen p, d.w.z. de existentie van getallen zonder echte delers. Deze blijken de voor hen karakteristieke eigenschap te bezitten: indien $p|ab$ dan $p|a$ of $p|b$ (of beide) en daaruit volgt de zogenaamde eenduidige ontbinding in priemfactoren.

Voor de gehelen in $\mathbb{Q}(\sqrt{m})$ is de situatie voor veel waarden van m geheel anders. Daarin heeft een getal π zonder echte delers niet steeds de eigenschap dat uit $\pi|\alpha\beta$ volgt $\pi|\alpha$ of $\pi|\beta$. Zo geldt in $\mathbb{Q}(\sqrt{-5})$

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

waarbij men kan bewijzen dat $2, 3, 1+\sqrt{-5}$ en $1-\sqrt{-5}$ geen echte delers hebben, terwijl we zien: $2|(1+\sqrt{-5})(1-\sqrt{-5})$ en toch $2\nmid 1+\sqrt{-5}$ en $2\nmid 1-\sqrt{5}$ omdat $\frac{1}{2}+\frac{1}{2}\sqrt{-5}$ en $\frac{1}{2}-\frac{1}{2}\sqrt{-5}$ niet geheel zijn in $\mathbb{Q}(\sqrt{-5})$, immers $-5\equiv 3 \pmod 4$ dus de gehelen in $\mathbb{Q}(\sqrt{-5})$ hebben als $\mathbb{Z}$-basis $\{1, \sqrt{-5}\}$.

We zullen dus in die lichamen onderscheid moeten maken tussen *getallen zonder echte delers* die we dan *irreducibel* zullen noemen en getallen π met de *eigenschap:* $\pi|\alpha\beta \Rightarrow \pi|\alpha$ of $\pi|\beta$, welke getallen we dan *priemgetallen* noemen. Hier dient zich de vraag aan voor welke m de ring van gehelen in $\mathbb{Q}(\sqrt{m})$ een ééntduidige ontbinding in irreducibele factoren heeft. Dit is een bijzonder gecompliceerde kwestie die nog niet volledig opgelost is. Men weet zelfs niet of er oneindig veel van die getallen zijn. Voor het complexe geval, ($m<0$), het geval dat ons nu bezighoudt is het probleem geheel opgelost. Allereerst zijn er waarden van m waarvoor de ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ *Euclidisch* is. Hierbij hanteren we - naar analogie van de situatie in $\mathbb{Z}$ - de volgende

Definitie: De ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ heet *Euclidisch* indien er bij elk tweetal α en β in $\mathbb{Q}(\sqrt{m})$ (met $\beta\neq 0$) gehele γ en δ in $\mathbb{Q}(\sqrt{m})$ bestaan zodanig dat

$$\alpha = \beta\gamma + \delta$$

met $0 \leqslant |N(\delta)| < |N(\gamma)|$.

In deze ringen kan men te werk gaan als in $\mathbb{Z}$ en tot een eenduidige ontbinding in irreducibele factoren besluiten.

In deze ringen vervalt het onderscheid tussen priem en irreducibel. De existentie van deze zogenaamde *delings-algoritme* is niet moeilijk aan te tonen voor negatieve m.

Voor positieve m liggen de zaken anders: Het eindresultaat dateert uit 1950 toen Chatland en Davenport de laatste hindernissen namen. Het resultaat is:

De ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ *is dan en slechts dan Euclidisch in de volgende (21) gevallen):*

$$m<0: \quad m = -11, -7, -3, -2, -1$$
$$m>0: \quad m = 2,3,5,6,7,11,13,17$$
$$19,21,29,33,37,41,57,73.$$

Het Euclidisch zijn van de ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ is wel voldoende voor de existentie van de eenduidige ontbinding in irreducibele (i.c. tevens priem-) factoren, maar niet noodzakelijk. Zo zijn er waarden voor $\mathbb{Q}(\sqrt{m})$ waarvoor de bijbehorende ring van gehelen niet Euclidisch is, maar toch een eenduidige ontbinding in priemfactoren heeft. Voor negatieve m is dit het geval dan en slechts dan als $m = -19, -43, -67, -163$. Het laatste geval is eerst in 1966 opgehelderd. Voor positieve m is het probleem nog niet opgelost; wel kent men alle gevallen met $2 \leqslant m \leqslant 100$ (38 in aantal) en men vermoedt dat er oneindig veel zijn.

Een ring waarin een eenduidige ontbinding in irreducibele factoren bestaat, Euclidisch of niet, zullen we een *factorontbindingsring* noemen.

6. Bepaling van de priemgetallen in enkele ringen van kwadratische gehele getallen

Opmerking vooraf: indien de ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ een factorontbindingsring is, mogen we de termen 'irreducibel' en 'priem' door elkaar gebruiken. We zullen meestal de term 'priem' hanteren. Fundamenteel is de

Stelling:
Indien de ring F van de gehelen in $\mathbb{Q}(\sqrt{m})$ factorontbindingsring is en π een priemgetal in F is, dan is π op juist één rationaal priemgetal deelbaar.

Bewijs:
Laat π geheel zijn in $\mathbb{Q}(\sqrt{m})$ en priem daarin. Uiteraard geldt $\pi\bar{\pi} \in \mathbb{Z}$, dus $\pi\bar{\pi} = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ (met p_i priem in $\mathbb{Z}$ en $\alpha_i \in \{1,2,\ldots\}$) dus geldt, omdat de ring van de gehelen in $\mathbb{Q}(\sqrt{m})$ een factorontbindingsring is, dat π op één der p_i deelbaar is, maar ook op niet meer dan één, immers als $\pi | p_i$ en $\pi | p_j$ dan $\pi | \lambda p_i + \mu p_j$ met $\lambda, \mu \in \mathbb{Z}$, maar als $p_i \neq p_j$ dan kunnen we λ en μ zó kiezen dat $\lambda p_i + \mu p_j = 1$ en dan zou π een eenheid zijn, hetgeen een tegenspraak is.

Het gevolg is dat ieder priemgetal in $\mathbb{Q}(\sqrt{m})$ te vinden is als factor van een *rationaal* priemgetal. Wanneer we dus de ontbinding in de ring van de gehelen van $\mathbb{Q}(\sqrt{m})$ kennen voor elk rationaal priemgetal, dan hebben we alle priemgetallen in $\mathbb{Q}(\sqrt{m})$ te pakken!!

7. De priemgetallen in de ring $\mathbb{Z}[i]$ van de gehelen van Gauss

We zagen reeds eerder dat $\mathbb{Z}[i]$ een Euclidische ring is, met als $\mathbb{Z}$-basis $\{1,i\}$. Voor $\alpha \in \mathbb{Z}[i]$ geldt dus $\alpha = a + bi$ $(a,b \in \mathbb{Z})$. Op grond van de bovengenoemde fundamentele stelling vinden we alle priemgetallen van $\mathbb{Z}[i]$ door elk *rationaal* priemgetal p te ontbinden in $\mathbb{Z}[i]$ in priemfactoren.

In het volgende stelt steeds π een priemgetal in $\mathbb{Z}[i]$ voor met $\pi = a + bi$ $(a,b \in \mathbb{Z})$, $\pi | p$. We onderscheiden daarbij $p \equiv 1$ (mod 4); $p \equiv 2$ (mod 4); $p \equiv 3$ (mod 4).

A. $p \equiv 1$ (mod 4). Er geldt $\pi | p$, dus $N(\pi) | N(p)$ dus $N(\pi) | p^2$ en, omdat π geen eenheid is, kunnen we volstaan met: $N(\pi) = p^2$ of $N(\pi) = p$. Immers $N(\pi) = -p^2$ of $N(\pi) = -p$ levert niets nieuws op.

A.1. $N(\pi) = p^2$. We zullen laten zien dat dat niet mogelijk is. Indien namelijk $N(\pi) = p^2 = N(p)$ dan zijn π en p geassocieerd en dus geldt dan: $\pi | p$ en $p | \pi$. Nu is er echter een stelling die zegt dat - als $p \in \mathbb{Z}$, priem is en de gedaante $p = 4n+1$ heeft - er een $x \in \mathbb{Z}$ bestaat z.d.d. $p | x^2 + 1$. Omdat dan geldt: $-1 \equiv x^2$ (mod p) zegt men dat -1 een kwadraatrest modulo p is. Aangezien in ons geval $\pi | p$, geldt ook $\pi | x^2 + 1$, dus $\pi | (x+i)(x-i)$ en dus - omdat $\mathbb{Z}[i]$ Euclidisch is - zal gelden: $\pi | x+i$ of $\pi | x-i$ en dus, (omdat ook $p | \pi$) : $p | x+i$ of $p | x-i$. Dit zou betekenen dat $\frac{x}{p} + \frac{i}{p}$ of $\frac{x}{p} - \frac{i}{p}$ tot $\mathbb{Z}[i]$ behoren, hetgeen niet juist is. Gevolg: er is in $\mathbb{Z}[i]$ geen priemgetal π met als norm p^2, waarbij $p \in \mathbb{Z}$, p priem in $\mathbb{Z}$ en $p \equiv 1$ (mod 4).

A.2. Er rest dus slechts de mogelijkheid: $N(\pi) = p$, d.w.z. $a^2 + b^2 = p$, dus $p = (a+bi)(a-bi) = \pi\overline{\pi}$, met $\pi = a + bi$ en $\overline{\pi} = a - bi$, beide priem in $\mathbb{Z}[i]$ omdat hun norm priem is in $\mathbb{Z}$.
We hebben de ontbinding in $\mathbb{Z}[i]$ in priemfactoren daadwerkelijk geconstrueerd en, omdat $\mathbb{Z}[i]$ Euclidisch is, is deze ontbinding eenduidig bepaald. Het is eenvoudig na te gaan dat π en $\overline{\pi}$ niet geassocieerd zijn, d.w.z. $a + bi \neq \pm(a - bi)$ en $a + bi \neq \pm i(a + bi)$.

De conclusie met betrekking tot A is dat elk rationaal priemgetal van de gedaante $4n+1$ op één, doch slechts één manier te schrijven is als het produkt van 2 priemgetallen in $\mathbb{Z}[i]$.
Voorbeeld: $5 = (2+i)(2-i); 17 = (4+i)(4-i)$.
We kunnen dit resultaat ook anders formuleren en hebben dan met *behulp van complexe getallen* het volgende resultaat over *gehele rationale getallen* afgeleid:

Ieder rationaal priemgetal p van de gedaante $4n+1$ *is op één, doch slechts één, manier te schrijven in de gedaante* $p = a^2 + b^2$.

Dit belangrijke resultaat kan ook afgeleid worden met gebruikmaking van uitsluitend reële getallen, bijvoorbeeld met de theorie van de kettingbreuken of met de zogenaamde stelling van Thue.

B. $p \equiv 2 \pmod 4$, maar p rationaal priem dus $p = 2 = (1+i)(1-i)$. Hierin zijn $1+i$ en $1-i$ priem in $\mathbb{Z}[i]$ omdat hun norm rationaal priem is. Dus 2 valt uiteen in juist 2 priemfactoren in $\mathbb{Z}[i]$ die geassocieerd zijn, immers $1+i = i(1-i)$.

C. $p \equiv 3 \pmod 4$. Stel weer $\pi | p$, met $\pi = a+bi$ dan geldt weer $N(\pi) = p$ of $N(\pi) = p^2$.

C.1. $N(\pi) = p$. Dit kan zich niet voordoen, immers dan $N(\pi) = a^2 + b^2$. Een kwadraat is echter of $\equiv 0 \pmod 4$ of $1 \pmod 4$, maar $p \equiv 3 \pmod 4$, dus tegenspraak.

C.2. Resteert dus: $N(\pi) = p^2 = N(p)$ dus π en p zijn geassocieerd, p 'blijft' priem in $\mathbb{Z}[i]$.

Samenvattend kunnen we dus concluderen dat de priemgetallen in $\mathbb{Z}[i]$ (de gehelen van Gauss) zijn:

(1) $1+i$ en de daarmee geassocieerden.

(2) de getallen in $\mathbb{Z}[i]$ van de gedaante $a+bi$ met $a^2+b^2 = p$, waarbij p priem is in $\mathbb{Z}$, met $p \equiv 1 \pmod 4$.

(3) de rationale priemgetallen p met $p \equiv 3 \pmod 4$.

Opmerking: Het resultaat onder (3) kan gegeneraliseerd worden tot de volgende

Stelling:
Een positief geheel rationaal getal $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ (met p_i rationaal priem) is dan en slechts dan de som van 2 kwadraten indien de priemfactoren p_j met $p_j \equiv 3 \pmod 4$ een even exponent hebben. We noemen dit slechts als voorbeeld van een stelling over reële getallen die met behulp van complexe getallen bewezen kan worden. Het bewijs verloopt als volgt:

a. Stel $n = a^2 + b^2$, dan geldt $n = N(a+bi)$, maar we kunnen $a+bi$ in $\mathbb{Z}[i]$ ontbinden in priemfactoren en wel in priemfactoren van twee typen, nl. factoren π_t met $N(\pi_t) = p_t \equiv 1 \pmod 4$ en factoren $q_s (\in \mathbb{Z})$ die in $\mathbb{Z}$ priem zijn en dat in $\mathbb{Z}[i]$ blijven omdat geldt: $q_s \equiv 3 \pmod 4$. Er geldt dan: $a+bi = \pi_1 \pi_2 \ldots \pi_m \cdot q_1 q_2 \ldots q_r$ en dus:

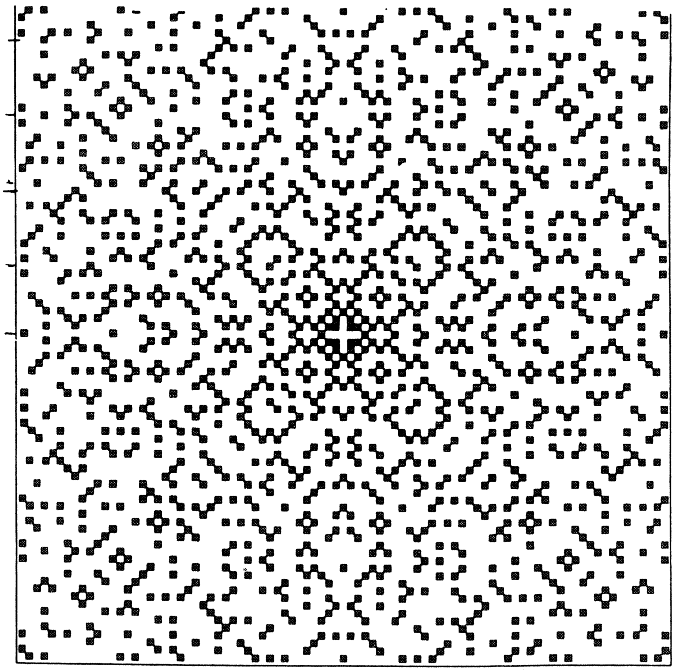
$$\begin{aligned} a^2 + b^2 &= \pi_1 \bar{\pi}_1 \pi_2 \bar{\pi}_2 \ldots \pi_m \bar{\pi}_m \cdot q_1^2 q_2^2 \ldots q_r^2 \\ &= p_1 p_2 \ldots p_m \cdot q_1^2 q_2^2 \ldots q_r^2. \end{aligned}$$

De priemfactoren q_s met $q_s \equiv 3 \pmod 4$ komen dus inderdaad in even machten voor.

b. Stel $n = p_1 p_2 \ldots p_m q_1^2 q_2^2 \ldots q_r^2$ met p_t en q_s als boven. Omdat $p_t \equiv 1 \pmod 4$ geldt, zoals we zagen: $p_t = a_t^2 + b_t^2$. Maar het produkt van 2 (en dus eindig veel) sommen, elk van twee kwadraten is eveneens de som van twee kwadraten dus geldt:

$$n = (A^2 + B^2)C^2 = A^2C^2 + B^2C^2.$$

In figuur 3 zijn de gehelen $a+bi$ van Gauss met $|a|\leqslant 34$ en $|b|\leqslant 34$ aangegeven d.m.v. vierkantjes. De zwarte vierkantjes stellen priemgetallen van Gauss voor. Er bestaat zelfs een kleedje waarin dit patroon is ingeweven.



FIGUUR 3

N.B. Als π priem is, dan zijn ook de overige geassocieerden $i\pi, -\pi, -\pi i$ priem. Vermenigvuldigen met i betekent in de figuur draaien over $\frac{\pi}{2}$ (linksom); vandaar de symmetrie in de figuur.

8. EEN BEKENDE TOEPASSING VAN COMPLEXE GETALLEN BIJ HET BEPALEN VAN PYTHAGOREÏSCHE TRIPLES

Onder een *Phythagoreïsch tripel* verstaan we een drietal gehele rationale getallen (x,y,z) die voldoen aan de vergelijking

$$x^2 + y^2 = z^2.$$

Uiteraard beperken we ons tot de niet-triviale gevallen, d.w.z. $xyz \neq 0$ en $(x,y,z)=1$. We lossen deze Diophantische vergelijking op met behulp van de eigenschappen van $\mathbb{Z}[i]$ en ontbinden daartoe het linkerlid in $\mathbb{Z}[i]$:

$$(x+iy)(x-iy) = z^2$$

Nu hebben $x+iy$ en $x-iy$ geen factor gemeen in $\mathbb{Z}[i]$, immers $(x,y)=1$ in $\mathbb{Z}$, (anders $(x,y,z)\neq 1$) dus er bestaan a en b in $\mathbb{Z}$ z.d.d $ax+by=1$, maar dit betekent dat x en y ook in $\mathbb{Z}[i]$ onderling ondeelbaar zijn.

Stel nu dat er een priemgetal π is in $\mathbb{Z}[i]$, z.d.d. $\pi|x+iy$ en $\pi|x-iy$ dan geldt ook $\pi|2x$ en $\pi|2yi$, dus $\pi|2$, dus $\pi=1+i$ of daarmee geassocieerd. Maar $1+i\nmid x+iy$ omdat $N(1+i)\nmid N(x+iy)$. Immers $N(1+i)=2$ en het is duidelijk dat $N(x+iy)$, zijnde x^2+y^2, oneven is, want $x^2+y^2=z^2$ en een kwadraat is $\equiv 0$ of $\equiv 1$ (mod 4), en dus $x^2+y^2\equiv 0$ òf $\equiv 1$ òf $\equiv 2$ (mod 4), maar $z^2\equiv 0$ of $\equiv 1$ (mod 4). Rest dus $x^2+y^2\equiv 0$ òf $x^2+y^2\equiv 1$ (mod 4).

In het eerste geval zijn x en y en z even, maar $(x,y,z)=1$, dus blijft over $x^2+y^2\equiv 1$ (mod 4) en dus $2\nmid x^2+y^2$. Uit

$$(x+iy)(x-iy)=z^2$$

volgt *op grond van de in $\mathbb{Z}[i]$ bestaande eenduidige ontbinding in priemfactoren* dat $x+iy$ op een eenheidsfactor na, een kwadraat is in $\mathbb{Z}[i]$, m.a.w.

$$x+iy=\pm(c+di)^2 \text{ of } x+iy=\pm i(c+di)^2 \quad (c,d\in\mathbb{Z}).$$

Het geval

$$x+iy=(c+di)^2=c^2-d^2+2cdi$$

geeft

$$x=c^2-d^2\,, y=2cd\,, z=c^2+d^2$$

en dit drietal voldoet inderdaad voor alle $c,d\in\mathbb{Z}$. De overige gevallen gaan analoog en leveren in feite niets nieuws.

Uit het bovenstaande volgt dat als $x^2+y^2=z^2$, de getallen x,y en z resp. de gedaante $x=c^2-d^2$; $y=2cd$ en $z=c^2+d^2$ zullen hebben. Men ziet direct in dat getallen x,y en z van deze gedaante inderdaad voldoen aan $x^2+y^2=z^2$.

Hiermee is bewezen dat genoemde x,y en z ook juist alle oplossingen vertegenwoordigen.

9. De priemgetallen in de ring F van gehelen van Eisenstein

Ook in $\mathbb{Q}(i\sqrt{3})$ is de ring van de gehelen Euclidisch; een $\mathbb{Z}$-basis daarin wordt gevormd door $\{1,\rho\}$ een geheel getal α daarin heeft nu de gedaante $\alpha=a+b\rho$ $(a,b\in\mathbb{Z})$. Evenals in het vorige voorbeeld vinden we alle priemen als factoren van de rationale priemgetallen.

We stellen in het volgende $\pi\in F$, π priem in F, $\pi=a+b\rho$ $(a,b\in\mathbb{Z})$, $\pi|p$. We onderscheiden daarbij: $p\equiv 0$ (mod 3), $p\equiv 1$ (mod 3), $p\equiv 2$ (mod 3).

A. $p\equiv 0$ (mod 3), p priem in $\mathbb{Z}$, dus $p=3$. Eenvoudig is in te zien: $N(1-\rho)=(1-\rho)(1-\rho^2)=(1-\rho)^2(1+\rho)=-\rho^2(1-\rho)^2$, maar ρ is eenheid en $(1-\rho)$ is priem in F omdat $N(1-\rho)=3=$ priem in $\mathbb{Z}$. Dus 3 is - op een eenheidsfactor na - het kwadraat van het priemgetal $(1-\rho)$ in F.

B. $p\equiv 1$ (mod 3). Er geldt dan $\pi|p$, dus $N(\pi)|N(p)$ dus $N(\pi)|p^2$ en dus - omdat π geen eenheid is - $N(\pi)=p^2$ of $N(\pi)=p$.

B.1. $N(\pi)=p^2$. We zullen zien dat dit niet mogelijk is. Er is namelijk een stelling die zegt dat -3 een kwadraatrest modulo p is indien p een rationaal priemgetal is met $p\equiv 1$ (mod 3). Dit betekent dus dat er een $x\in\mathbb{Z}$ is, z.d.d $p|x^2+3$.

Indien nu π een priemdeler is van p, dan geldt ook $\pi|x^2+3$, dus $\pi|(x+i\sqrt{3})(x-i\sqrt{3})$ en dus, vanwege de eenduidige ontbinding in priemfactoren, $\pi | x+i\sqrt{3}$ of $\pi | x-i\sqrt{3}$. Indien nu $N(\pi)=p^2=N(p)$, dan zijn π en p geassocieerd, d.w.z. $p|\pi$ en $\pi|p$. Dus ook $p|x-i\sqrt{3}$ (deelbaarheid in F!); dus zou $\frac{x}{p}-\frac{i}{p}\sqrt{3}$ tot F behoren, hetgeen niet mogelijk is, daar de elementen van F de gedaante $a+b\frac{-1+i\sqrt{3}}{2}$ hebben en $p\neq 2$.

B.2. $N(\pi)=p$. Dit is de enige resterende mogelijkheid. Er geldt dan $p=a^2-ab+b^2=(a+b\rho)(a+b\rho^2)$, dus p heeft de - eenduidig bepaalde - priemdelers $\pi=a+b\rho$ en $\overline{\pi}=a+b\rho^2$, die zoals men gemakkelijk nagaat, niet geassocieerd zijn. Aangezien $N(\pi)\neq N(p)$ zijn het echte priemdelers.

We kunnen het resultaat van B ook weer anders formuleren en hebben dan wederom met *behulp van complexe getallen* een resultaat voor *gehele rationale getallen* gevonden, en wel het volgende:

> *Ieder rationaal priemgetal van de gedaante* $3n+1$ *is op één doch slechts één manier te schrijven in de gedaante* $p=a^2-ab+b^2$.

Hierop komen we nog terug.

C. $p\equiv 2 \pmod 3$. Weer geldt $N(\pi)=p$ of $N(\pi)=p^2$.

C.1. $N(\pi)=p$. We laten zien dat dit uitgesloten is. Immers: $N(\pi)=a^2-ab+b^2$ en $N(\pi)\equiv 4N(\pi) \pmod 3$ dus $p=N(\pi)\equiv 4N(\pi)= 4a^2-4ab+4b^2=(2a-b)^2+3b^2\equiv(2a-b)^2 \pmod 3$. Maar een kwadraat is altijd óf $\equiv 1$ óf $\equiv 0$ (mod 3) dus tegenspraak, daar $p\equiv 2 \pmod 3$.

C.2. $N(\pi)=p^2$. Dit is nu de enige resterende mogelijkheid. In dit geval zijn π en p geassocieerd en dus is p zelf priem. Een rationaal priemgetal van de gedaante $p=3n+2$ 'blijft' dus priem in F.

Samenvattend concluderen we dat de priemgetallen in de ring F van de gehelen van Eisenstein zijn:

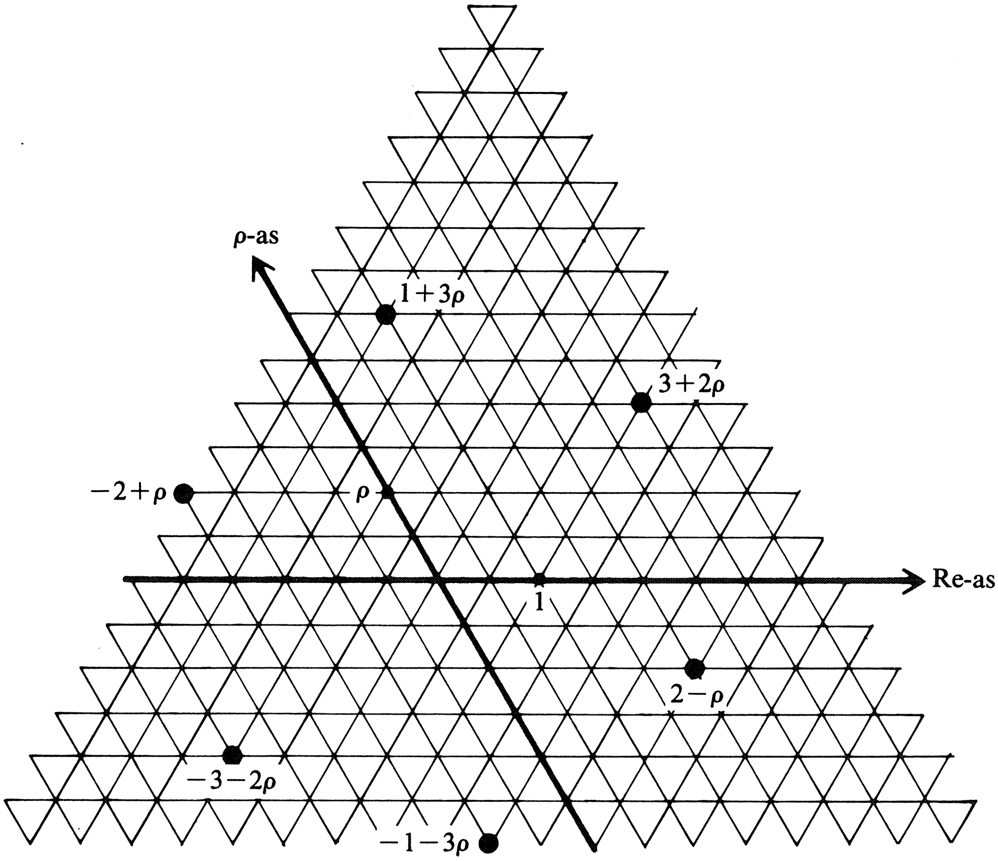
(1) $1-\rho$ en de daarmee geassocieerden.
(2) de factoren in F van de rationale priemgetallen van de gedaante $3n+1$ en de daarmee geassocieerden.
(3) de rationale priemgetallen van de gedaante $3n+2$.

10. Opmerkingen over de ligging van de priemgetallen van Eisenstein

In deze paragraaf gaan we nader in op de vraag hoe de rationale priemgetallen p van de gedaante $p=3n+1$ ontbonden kunnen worden in de ring F van de gehele getallen van Eisenstein. Direct duidelijk is dat n even moet zijn, daar anders p even is ($p=2$ is uitgesloten). We mogen dus stellen $p=6m+1$. De gezochte priemfactoren π in F zijn dan $\pi=a+b\rho$ met $N(\pi)=a^2-ab+b^2=6m+1$ (priem) en de daarmee geassocieerden, dus in totaal

$$\pi, \rho\pi, \rho^2\pi, -\pi, -\rho\pi \text{ en } -\rho^2\pi.$$

Voorbeeld: $\pi=3+2\rho$, dus $N(\pi)=7$. De geassocieerden zijn:
$3+2\rho, -2+\rho, -1-3\rho, -3-2\rho, 2-\rho, 1+3\rho$ (zie figuur 4).



FIGUUR 4

We kunnen in het algemeen iets zeggen over de ligging van de getallen $\alpha = a + b\rho$ met $N(\alpha) = 6m + 1$ (al dan niet priem). Allereerst merken we op dat uit

$$N(\alpha) = a^2 - ab + b^2 = 6m + 1$$

volgt dat a en b niet beide even zijn.

A. Indien *a en b beide oneven zijn,* dan geldt $a - b = d$ met d even. Uit $a^2 - ab + b^2 = 6m + 1$ blijkt door substitutie ook te volgen: $a^2 - ad + d^2 = 6m + 1$. Vanwege de één-éénduidige correspondentie tussen de paren (a,b) en $(a,a-b)$ behoort dus bij elke oplossing (a,b) van $a^2 - ab + b^2 = 6m + 1$ een oplossing (a,d) met even d en omgekeerd.

Deze oplossingen bezien we afzonderlijk. Indien we stellen $d = 2f$ dan blijkt:

$$(a - f)^2 + 3f^2 = 6m + 1,$$

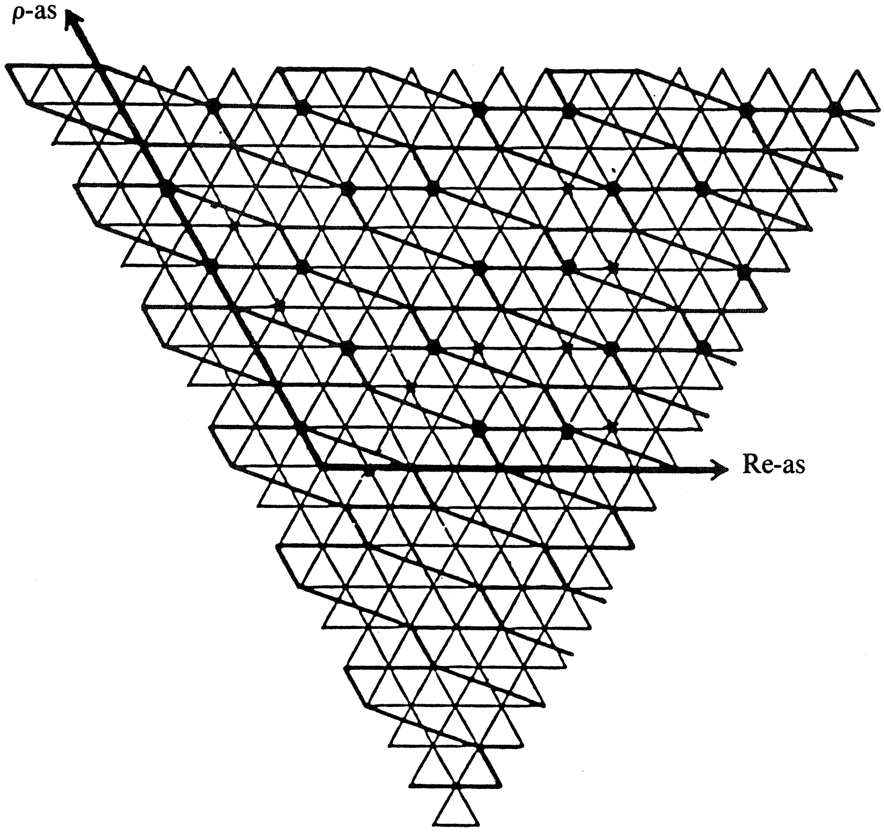
waaruit volgt $a-f \not\equiv 0$ (mod 3), dus $a-f \equiv 1$ (mod 3) of $a-f \equiv 2$ (mod 3). Verder zien we: als $f \equiv 0$ (mod 2) dan $a-f \equiv 1$ (mod 2) en als $f \equiv 1$ (mod 2) dan $a-f \equiv 0$ (mod 2).

Hieruit leiden we af dat de bijbehorende getallen $\alpha = d + a\rho$ (met even d en α al dan niet priem) op een hexagonaal rooster in het vlak van de gehelen van Eisenstein liggen. Het eenvoudigste is dat in te zien door de mogelijkheden op te schrijven. Het systeem blijkt dan vanzelf:

d	f	bijbehorende waarden van a												
0	0	.	1	.	.	.	5	.	7	.	.	.	11	etc.
2	1	.	.	.	3	.	5	.	.	.	9	.	11	etc.
4	2	.	1	.	3	.	.	.	7	.	9	.	.	etc.
6	3	.	1	.	.	.	5	.	7	.	.	.	11	etc.

(zie figuur 5). In de tabel is steeds uitgegaan van een vaste waarde van f; daardoor ligt ook d vast. Bij deze d worden de mogelijke waarden van a berekend, uitgaande van het feit dat $a \equiv 1 + f$ (mod 3) of $a \equiv 2 + f$ (mod 3).

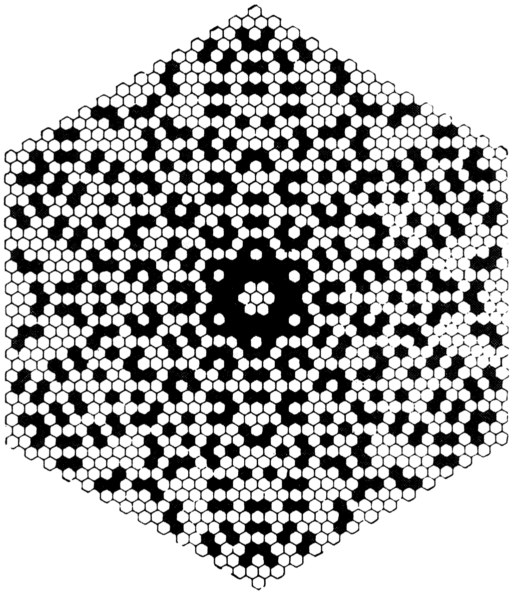
Op deze wijze verkrijgen we een stel getallen $d + a\rho$ met $a^2 - ad + d^2 = 6m + 1$ en d even. Het ging ons om de gehelen van de gedaante $d + a\rho$ met $a^2 - ab + b^2 = 6m + 1$, en hun geassocieerden. Men rekent eenvoudig na dat de collectie $d + a\rho$ en alle daarmee geassocieerden samenvalt met de collectie $a + b\rho$ en alle daarmee geassocieerden. Zoals eerder opgemerkt, verkrijgen we de geassocieerden van $a + b\rho$ door vermenigvuldiging met resp. $1, \rho, \rho^2, -1, -\rho, -\rho^2$ hetgeen meetkundig een rotatie betekent over resp. $0, \frac{2\pi}{3}, \frac{4\pi}{3}, \pi, \frac{5\pi}{3}, \frac{\pi}{3}$. Figuur 5 geeft daarvan een indruk en we zien dat de bijbehorende getallen op een hexagonaal rooster liggen.



FIGUUR 5

De roosterpunten representeren de gehelen van Eisenstein $d+a\rho$ met d even en $a^2-ad+d^2=6m+1$. De dik aangegeven punten representeren *priemgetallen van Eisenstein.* Hierbij zijn alleen die opgenomen met $a>0$, $d>0$, d even. De bijbehorende geassocieerden vindt men door de genoemde rotatie toe te passen.

B. Het geval dat a en b verschillende pariteit hebben, wordt aan de lezer overgelaten. Tot slot een opmerking over figuur 6.



FIGUUR 6

Deze is afkomstig uit het in de literatuurlijst onder [11] vermelde artikel van v.d. Pol. Zijn bedoeling was de bedoelde priemgetallen van Eisenstein af te beelden niet in het vlak van Eisenstein, maar in het 'gewone' complexe vlak, dus met behulp van de representatie $u+iv$ $(u,v\in\mathbb{R})$. De werkwijze is daarbij als volgt: (d is weer even):

$$a+d\rho=a+d(-\tfrac{1}{2}+\tfrac{1}{2}i\sqrt{3})=(a-f)+if\sqrt{3})=c+if\sqrt{3}.$$

De eis is nu:

$$c^2+3f^2=6m+1$$

waaruit volgt:

$$c\equiv 1 \pmod 3 \text{ of } c\equiv 2 \pmod 3$$

en

c en f van verschillende pariteit.

In het platte vlak worden nu twee onderling loodrechte assen getekend. Langs de horizontale as worden de c-waarden uitgezet. Langs de verticale as de f-waarden. Zo krijgt $4+i\sqrt{3}$ de coordinaten (4,1). Het blijkt dan dat men dit vlak kan overdekken met regelmatige zeshoeken met zijdelengte $\frac{1}{3}\sqrt{3}$ en wel zo dat de gezochte getallen α van Eisenstein met $N(\alpha)=6m+1$ in de middelpunten liggen. De priemgetallen daaronder zijn middelpunten van de zwarte zeshoeken. Door rotatie over veelvouden van $\frac{\pi}{3}$ krijgt men de geassocieerden en dus vertoont de figuur een 6-tallige symmetrie.

11. HOE GAAT HET VERDER EN WAAR KOMT HET VANDAAN ?

In paragraaf 2 hebben we ons bescheiden opgesteld en ons beperkt tot *kwadratische gehele getallen,* die we definieerden als oplossingen van vierkantsvergelijkingen van de gedaante $x^2+Ax+B=0$ $(A,B\in\mathbb{Z})$, naar analogie van de eigenschap die een 'gewoon' geheel getal heeft, namelijk dat het voldoet aan een *lineaire* vergelijking van de gedaante $x+A=0$ $(A\in\mathbb{Z})$.

Een voor de hand liggende generalisatie is nu algemene gehele algebraïsche getallen te definieren als oplossingen van vergelijkingen van willekeurige graad en met gehele rationale getallen als coëfficiënten, maar met kopcoëfficiënt 1, dus:

$$x^n+A_{n-1}x^{n-1}+A_{n-2}x^{n-2}+\ldots+A_0=0.\ (*)\quad (n\in\mathbb{N},\ n>0,\ A_i\in\mathbb{Z}).$$

Men gaat daarbij uit van een *algebraïsche* vergelijking met coëfficiënten in $\mathbb{Q}$:

$$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0.$$

Een wortel daarvan noemt men een *algebraïsch* getal, in tegenstelling tot een zogenaamd *transcendent* getal (als e en π) die niet aan een vergelijking van dit type voldoen.

Men adjungeert een wortel, zeg α, aan $\mathbb{Q}$, d.w.z. men beschouwt alle rationale verbindingen van α met coëfficiënten in $\mathbb{Q}$. Deze vormen een lichaam, aan te geven met $\mathbb{Q}(\alpha)$. Dit lichaam $\mathbb{Q}(\alpha)$ blijkt een lineaire vectorruimte te zijn over $\mathbb{Q}$ met als $\mathbb{Q}$-basis $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$. In $\mathbb{Q}(\alpha)$ definieert men een *geheel algebraïsch getal* als element van $\mathbb{Q}(\alpha)$ dat als definiërende vergelijking (over $\mathbb{Q}$) een vergelijking van de gedaante (*) heeft. Het blijkt dan dat er in $\mathbb{Q}(\alpha)$ een $\mathbb{Z}$-basis $\{\beta_1,\beta_2,\ldots,\beta_n\}$ bestaat voor de gehelen in $\mathbb{Q}(\alpha)$, d.w.z. ieder geheel algebraïsch getal in $\mathbb{Q}(\alpha)$ is op één, doch slechts één, manier te schrijven als een lineaire combinatie van $\beta_1,\beta_2,\ldots,\beta_n$ met coëfficiënten in $\mathbb{Z}$.

Zoals we zagen was dat in $\mathbb{Q}(\sqrt{m})$ de basis $\{1,\sqrt{m}\}$ als $m\equiv2$ of 3 (mod 4) en $\{1,\frac{-1+\sqrt{m}}{2}\}$ als $m\equiv1$ (mod 4). Men ziet hier de lineaire algebra om de hoek komen en men heeft inderdaad met behulp van de lineaire algebra veel resultaten die men vroeger b.v. met symmetrische functies bereikte, op elegantere (en kortere) wijze kunnen afleiden zonder verder beroep te doen op de definiërende vergelijking, b.v. het feit dat de gehelen een ring vormen. Deze ring is echter niet in alle uitbreidingen $\mathbb{Q}(\alpha)$ voorzien van een eenduidige ontbinding in irreducibele (d.w.z. niet nader te ontbinden) factoren. Dit zagen we al eerder. Priem en irreducibel is niet meer hetzelfde. Wat wel in al deze ringen geldt is de eenduidige ontbinding in *priemideaalfactoren.* Het gaat namelijk om zogenaamde Dedekindringen[1]; hierop komen we nog terug. Deze worden dan weer op zichzelf bestudeerd - vaak echter zonder de getallentheoretische achtergrond daarbij te betrekken; een achtergrond die men soms nog wel in de terminologie herkent. Wij zijn daarmee gekomen in het gebied van de *commutatieve algebra.*

Tenslotte iets over de *voorgeschiedenis.* Over het getal i is al uitvoerig bericht in het hoofdstuk '$\mathbb{C}$ Avant la lettre'. De getallen van de gedaante $a+bi$ $(a,b\in\mathbb{Z})$ komen weliswaar reeds voor bij Euler (1707-1783) en Lagrange (1736-1813), maar het belang ervan werd eerst duidelijk aangetoond door Gauss (1777-1855) in zijn *Disquisitiones Arithmeticae* (1801) bij de studie van de biquadratische resten. Eerder hebben we gezien wat een kwadraatrest is; de begrippen kubische rest en bikwadraatrest spreken dan voor zichzelf.

Het getal ρ en de getallen $a+b\rho$ $(a,b\in\mathbb{Z})$ kwamen op bij de onderzoekingen van Eisenstein en Jacobi (1804-1851) inzake de kubische resten.

De voornaamste aanzetten tot een verdere ontwikkeling van de theorie van de algebraïsche getallen vindt men echter in de pogingen om het probleem van Fermat op te lossen. Hierbij wordt de vraag gesteld naar de niet-triviale oplossingen met gehele rationale getallen van de vergelijking

$$x^n + y^n = z^n \quad (n\in\mathbb{N}\,;n \text{ vast}\,;n\geqslant 3).$$

Uiteraard kan men zich beperken tot waarden van n die priem zijn. Het ligt voor de hand dit probleem aan te pakken op de wijze analoog aan die waarop de vergelijking $x^2+y^2=z^2$ wordt opgelost. Dit deed Kummer (1810-1893) en schreef

$$x^p + y^p = z^p \quad (p \text{ priem}\,;p\geqslant 3)$$

in de gedaante

$$(x+y)(x+\alpha y)...(x+\alpha^{p-1}y) = z^p$$

met

$$\alpha^p = 1 \quad (\alpha\neq 1)$$

en dus α wortel van

$$\alpha^{p-1} + \alpha^{p-2} + \alpha^{p-3} + ... + \alpha + 1 = 0.$$

De fout die hij toen maakte was dat hij, analoog aan het geval

$$(x+iy)(x-iy) = z^2,$$

veronderstelde dat in de ring van de gehelen onder de getallen van de gedaante

1. R. Dedekind (1831-1916)

$a_0 + a_1\alpha + ... a_{p-2}\alpha^{p-2}$ $(a_i \in \mathbf{Q})$ een éénduidige ontbinding in priemfactoren bestaat en dat dus $x + \alpha y$ een $p$de-macht was. Naar aanleiding van de kritiek van Dirichlet (1805-1854) ontwierp Kummer de theorie van de 'ideale' getallen, een theorie die door Dedekind werd omgebogen in de richting van de ideaaltheorie. Opmerkelijk is daarbij hoe de vraagstelling werd verlegd: i.p.v. te vragen naar eigenschappen van *algebraïsche getallen,* vroeg men naar de eigenschappen van bepaalde *verzamelingen* van algebraïsche getallen, de zogenaamde *idealen,* met de bekende eigenschappen: als A een ideaal is in de ring F van gehelen in een zeker getallenlichaam, dan gelden de beide regels:

$$\alpha, \beta \in A \rightarrow \alpha - \beta \in A \text{ en } \alpha \in A, r \in F \rightarrow \alpha r \in A.$$

Voor deze idealen worden rekenregels opgesteld en het blijkt dat in elke ring van gehele algebraïsche getallen - factorontbinding of niet - de reeds genoemde eenduidige ontbinding in *priemideaal*factoren bestaat.

Aan deze hele kwestie zouden echter vele colleges kunnen worden gewijd. De geïnteresseerde lezer worde - voor zover het een eerste oriëntatie betreft - in eerste instantie verwezen naar de nummers 6 en 7 van de literatuurlijst.

LITERATUURLIJST

Uit de uitgebreide literatuur over dit onderwerp is een uiteraard beperkte keuze gedaan.

1. M.F. ATIYAH, I.G. MACDONALD (1969). *Introduction to Commutative Algebra,* Reading Mass, etc.
2. P. BACHMAN (1976). *Das Fermatproblem in seiner bisherigen Entwicklung,* Berlin.
3.* H.M. EDWARDS (1977). *Fermats Last Theorem,* Berlin.
4. G.H. HARDY, E.M. WRIGHT (1960). *An Introduction to the Theory of Numbers,* New York.
5. HUA LOO KENG (1982). *Introduction to Number Theory,* Berlin.
6.** M. KLINE (1972). *Mathematical Thought from Ancient to Modern Times,* New York.
7.* H.W. LENSTRA JR. (1979). Euclidean Numbers Fields 1. *The Math. Intelligencer Vol. 2 Nr. 1.*
8. H.W. LENSTRA JR. (1980). Euclidean Number Fields 2,3. *The Math. Intelligencer Vol. 2 Nr 2.*
9. F. LOONSTRA (1979). *Inleiding tot de Algebra,* Groningen.
10. I. NIVEN, H.S. ZUCKERMAN (1972). *An Introduction to the Theory of Numbers,* New York etc.
11.* BALTH. V.D. POL, P. SPECIALI (1951). The primes in $k(\rho)$. *Indag. Math. 13.*
12.* BATH. V.D. POL (1946). *Verslagen van de Maatschappij,* Diligentia ('s-Gravenhage).
13. H. POLLARD, H.G. DIAMOND (1974). *The Theory of Algebraic Numbers,* New York.
14. P. RIBENBOIM (1972). *Algebraic Numbers,* New York, etc.
15.* P. RIBENBOIM (1979). 13 *Lectures on Fermat's Last Theorem,* Berlin.

16.* P. SAMUEL (1972). *Algebraic Theory of Numbers,* London.
17. H.M. STARK (1979). *An Introduction to Number Theory,* London.
18. I.N. STUART, J.O. TALL (1979). *Algebraic Number Theory,* London.
19. B.L. V.D. WAERDEN (1966). *Algebra deel I en II,* Berlin.

De met * gemerkte literatuur is geschikt voor een eerste kennisneming.
** geeft een goed historisch overzicht.

Meetkunde met Complexe Getallen

J. van de Craats
Koninklijke Militaire Academie
Postbus 90154, 4800 RG Breda

1. INLEIDING

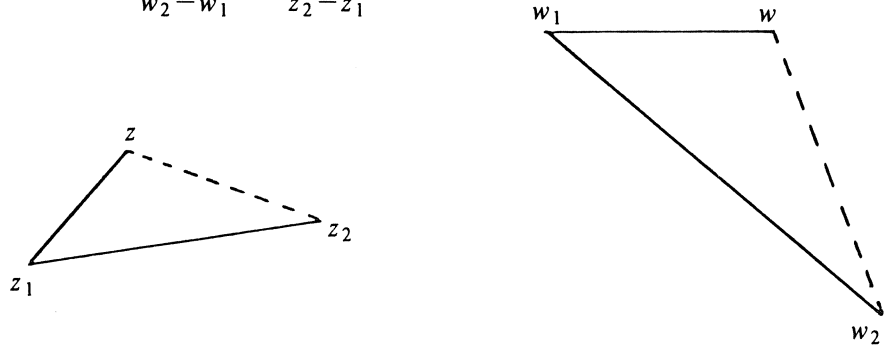
Van nature hebben complexe getallen al iets meetkundigs. Je kunt ze het beste introduceren als de punten van een vlak waarin een orthonormaal coördinatenstelsel vastligt. De optelstructuur is dan niets anders dan de gewone vectoroptelling in $\mathbb{R}^2$. Het bijzondere zit hem in de complexe vermenigvuldiging. Die wordt pas doorzichtig als je met modulus en argument gaat werken. En juist daarvoor is het nodig om uit te gaan van een *orthonormaal* coördinatenstelsel: je moet afstanden en hoeken op de bekende manier in de coördinaten kunnen uitdrukken. Vermenigvuldigen van twee complexe getallen betekent dan meetkundig gezien het vermenigvuldigen van de moduli en het optellen van de argumenten. De elementaire bewerkingen binnen het lichaam van de complexe getallen - optellen en vermenigvuldigen - corresponderen dus met simpele meetkundige bewerkingen in het complexe vlak: de parallellogramconstructie voor de optelling en een gelijkvormigheidsconstructie voor de vermenigvuldiging.

De meetkundige voorstelling van complexe getallen is een grote steun en inspiratiebron als je met complexe getallen werkt. Complexe functietheorie, bijvoorbeeld, is zonder meetkundige beelden in het complexe vlak haast ondenkbaar. Maar ook omgekeerd kunnen allerlei resultaten uit de meetkunde, met name de vlakke euclidische meetkunde, op een elegante manier met behulp van complexe getallen worden afgeleid. We zullen daarvan een aantal voorbeelden geven.

2. Directe gelijkvormigheidstransformaties

Bij een directe gelijkvormigheidstransformatie van het vlak zijn voor elke driehoek origineel en beeld direct gelijkvormig met elkaar. Werken we in het complexe vlak, dan betekent dit dat voor elk drietal z, z_1, z_2 met beelden resp. w, w_1, w_2 geldt:

$$\frac{w-w_1}{w_2-w_1} = \frac{z-z_1}{z_2-z_1}. \tag{1}$$



Figuur 1. Directe gelijkvormigheidstransformatie

Houden we z_1 en z_2 vast, en variëren we z, dan geeft (1) precies de vergelijking van de betreffende transformatie. Na herschrijven:

$$z \mapsto w = w_1 + \frac{w_2-w_1}{z_2-z_1}(z-z_1).$$

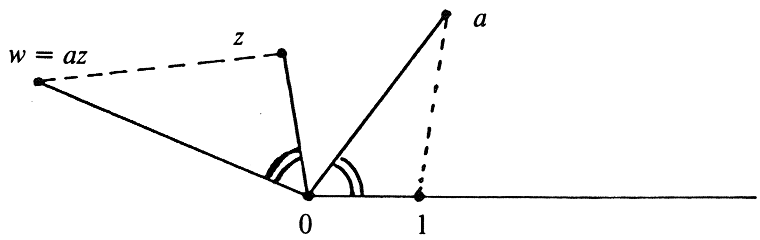
Deze transformatie is van de vorm

$$z \mapsto w = a \cdot z + b \quad (a \neq 0) \tag{2}$$

en omgekeerd stelt (2) ook altijd een directe gelijkvormigheidstransformatie voor.

Enige voorbeelden:

(i)	$z \mapsto w = z + b$	*translatie,*
(ii)	$z \mapsto w = d \cdot z \quad (d = e^{i\phi})$	*draaiing (rotatie)* met *centrum* 0 en *hoek* ϕ,
(iii)	$z \mapsto w = \rho \cdot z \quad (\rho > 0)$	*puntvermenigvuldiging* met *centrum* 0 en *factor* ρ,
(iv)	$z \mapsto w = a \cdot z$	*draaivermenigvuldiging* met *centrum* 0, *factor* $\lvert a \rvert$, *hoek* $\arg(a)$ $(a \neq 0)$.



FIGUUR 2. De draaivermenigvuldiging $w = a \cdot z$

Als $a \neq 1$ heeft (2) precies één invariant punt: $z_0 = \frac{b}{1-a}$. Elk paar (z,w) van origineel z en beeld w voldoet dan aan

$$w - z_0 = a(z - z_0)\,.$$

Blijkbaar is (2) voor $a \neq 1$ een draaivermenigvuldiging met centrum z_0, factor $|a|$ en hoek $\arg(a)$.

De samenstelling van twee directe gelijkvormigheidstransformaties

$$z \mapsto u = a_1 z + b_1$$

$$u \mapsto w = a_2 u + b_2$$

is

$$z \mapsto w = a_2(a_1 z + b_1) + b_2 = a_2 a_1 z + a_2 b_1 + b_2\,.$$

Als $a_2 a_1 = 1$ is dit een translatie (of de identiteit); anders is het een draaivermenigvuldiging met factor $|a_2 a_1|$ en hoek $\arg(a_2) + \arg(a_1)$.

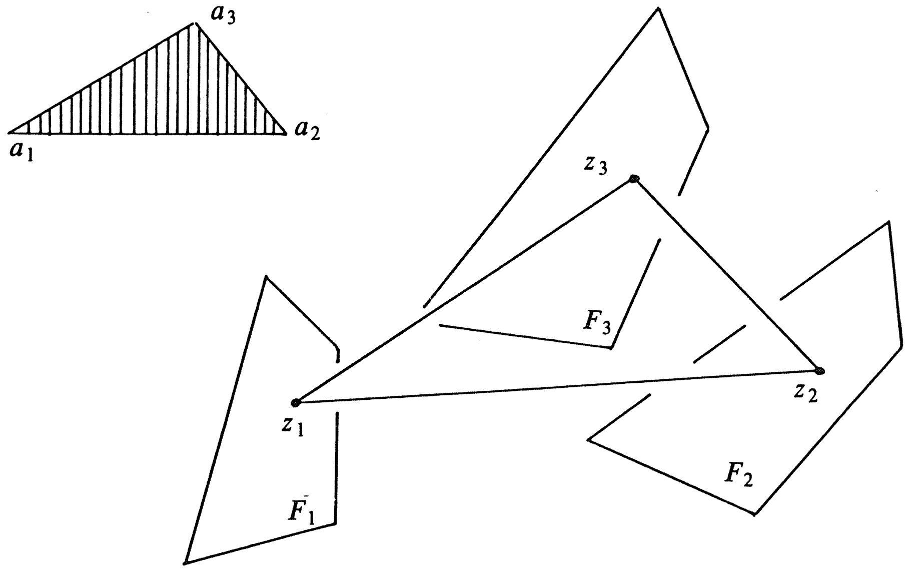
3. DE STELLING VAN PETERSEN-SCHOUTE

Laat gegeven zijn:

- een vaste driehoek $a_1 a_2 a_3$
- een directe gelijkvormigheidstransformatie D
- een figuur F_1.

Stel z_1 doorloopt F_1. Daarbij doorloopt $z_2 = D\, z_1$ een direct gelijkvormige figuur $F_2 = D\, F_1$. Neem z_3 zo, dat steeds $z_1 z_2 z_3$ direct gelijkvormig is met de vaste driehoek $a_1 a_2 a_3$.

STELLING: dan doorloopt z_3 een figuur F_3 die direct gelijkvormig is met F_1 en F_2 (eventueel is F_3 ontaard tot één punt).



FIGUUR 3. De stelling van Petersen-Schoute

BEWIJS: we kunnen aannemen dat $a_1a_2a_3 = 0\ 1\ b$ voor zekere b. Stel $D : z \mapsto pz + q$ $(p \neq 0)$. Omdat $z_1z_2z_3$ direct gelijkvormig is met $0\ 1\ b$, geldt

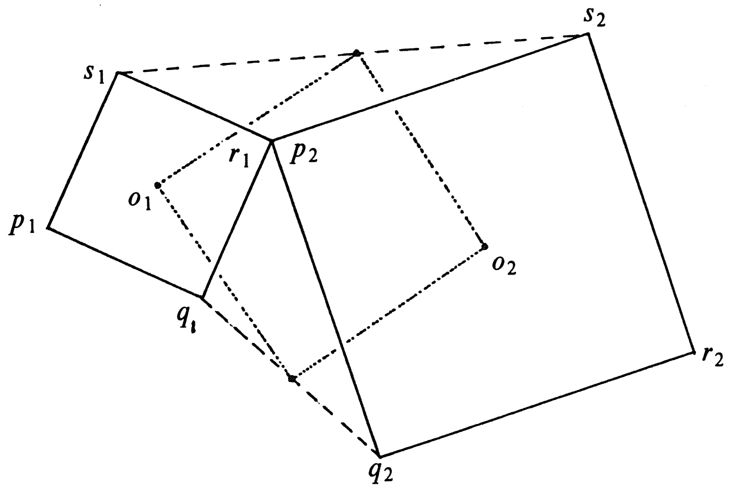
$$z_3 - z_1 = b(z_2 - z_1) = b(pz_1 + q - z_1), \text{ dus}$$

$$z_3 = (1 + bp - b)z_1 + bq\ .$$

Daarom is $D' : z_1 \mapsto z_3$ een directe gelijkvormigheidstransformatie (tenzij $1 + bp - b = 0$; dan is z_3 constant).

Merk nog op:
(i) als $p = 1$ (translatie) dan is D' ook een translatie,
(ii) als $p \neq 1$ dan hebben D en D' hetzelfde invariante punt,
(iii) als $b \in \mathbb{R}$ dan is $a_1a_2a_3 = 0\ 1\ b$ ontaard tot een lijnstuk; de stelling behoudt zijn geldigheid.

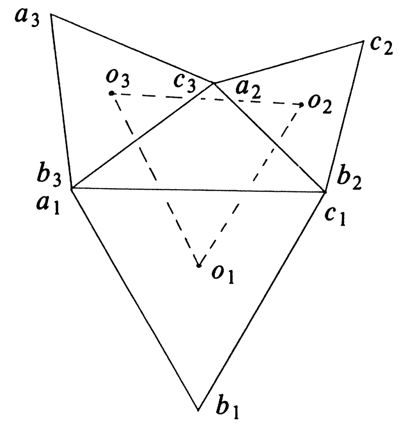
Toepassingen:
1. Stel gegeven zijn twee gelijk georiënteerde vierkanten $p_1q_1r_1s_1$ en $p_2q_2r_2s_2$ met centra resp. o_1 en o_2. Stel dat $r_1 = p_2$. Dan vormen de punten $o_1(= \frac{1}{2}(p_1 + p_2))$, $\frac{1}{2}(q_1 + q_2)$, $o_2(= \frac{1}{2}(r_1 + r_2))$ en $\frac{1}{2}(s_1 + s_2)$ weer een vierkant.



FIGUUR 4. Drie vierkanten

BEWIJS: De figuren F_1 en F_2 zijn hier de gegeven vierkanten, en het getal b uit het bewijs van de stelling is gelijk aan ½.

2. Construeert men op de zijden van een willekeurige driehoek naar buiten toe gelijkzijdige driehoeken, dan vormen de drie centra tezamen weer een gelijkzijdige driehoek.



FIGUUR 5. Gelijkzijdige driehoeken

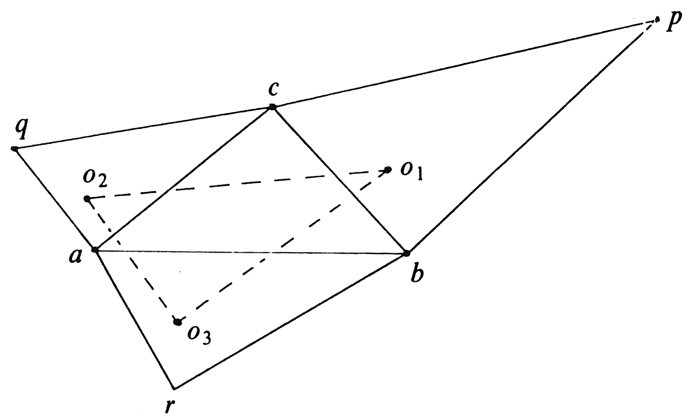
BEWIJS: er zijn drie gelijkzijdige driehoeken $a_1b_1c_1$, $a_2b_2c_2$ en $a_3b_3c_3$ in het spel, met $a_1=b_3$, $a_2=c_3$ en $b_2=c_1$ (fig. 5) en centra o_1, o_2 en o_3. Pas de stelling van Petersen-Schoute toe met

$$F_1=(a_1,\, b_1,\, c_1,\, o_1)\,,$$

$$F_2=(a_2,\, b_2,\, c_2,\, o_2)\,,$$

en $b = \cos \pi/3 + i \sin \pi/3$.

3. *Algemener:*
op de zijden van driehoek *abc* construeert men drie onderling direct gelijkvormige driehoeken *bpc*, *acq* en *rba*.
Zijn o_1, o_2 en o_3 overeenkomstige punten in die driehoeken, dan is driehoek $o_1 o_2 o_3$ ook direct gelijkvormig met *bpc*, *acq* en *rba*.



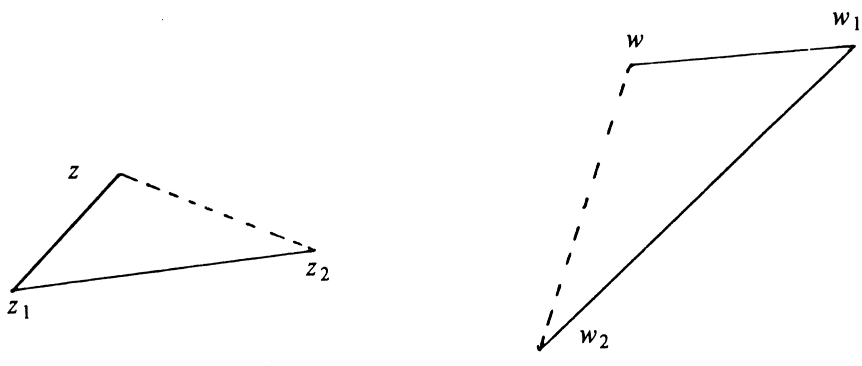
FIGUUR 6. Gelijkvormige driehoeken

BEWIJS: $F_1 = (b, p, c, o_1)$, $F_2 = (a, c, q, o_2)$, $a_1 a_2 a_3 = bar$.

4. INDIRECTE GELIJKVORMIGHEIDSTRANSFORMATIES

Bij een indirecte gelijkvormigheidstransformatie gaat elke driehoek over in een indirect gelijkvormige driehoek, dus met omgeklapte oriëntatie. In termen van complexe getallen:

$$\frac{w - w_1}{w_2 - w_1} = \frac{\bar{z} - \bar{z}_1}{\bar{z}_2 - \bar{z}_1}. \qquad (3)$$



FIGUUR 7. Indirecte gelijkvormigheidstransformatie

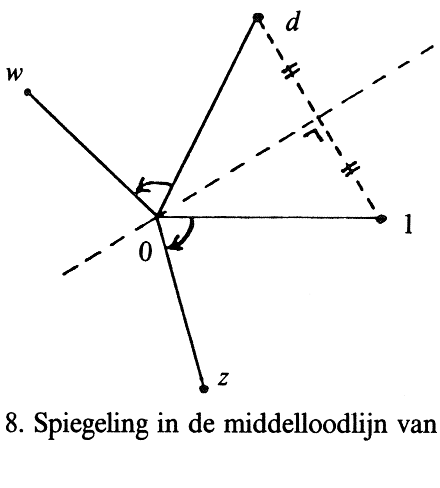
Deze transformaties zijn van de vorm

$$z \mapsto w = a \cdot \bar{z} + b \quad (a \neq 0)\,. \tag{4}$$

Enige voorbeelden:
(i) $z \mapsto w = \bar{z}$ *spiegeling in de reële as,*
(ii) $z \mapsto w = d \cdot \bar{z}$ $(|\, d \,| = 1)$.

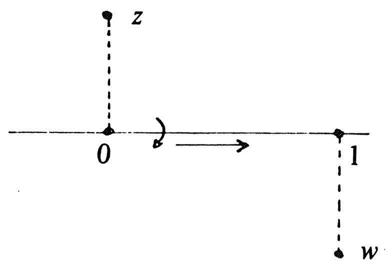
Aangezien $0 \mapsto 0$ en $1 \mapsto d$ geldt voor elke z

$\dfrac{w-0}{d-0} = \dfrac{\bar{z}-\bar{0}}{\bar{1}-\bar{0}}$. De transformatie is dus de *spiegeling in de middelloodlijn van* 1 *en d.*



FIGUUR 8. Spiegeling in de middelloodlijn van 1 *en d*

(iii) $z \mapsto w = \bar{z} + 1$ *glijspiegeling langs de reële as met translatieafstand* 1,



FIGUUR 9. Glijspiegeling

(iv) $z \mapsto w = \rho \cdot \bar{z}$ $(\rho > 0,\ \rho \neq 1)$ *spiegelvermenigvuldiging met centrum* 0, factor ρ *en als as de reële as.*

De transformatie (4) heeft als $|\ a\ | \neq 1$ precies één invariant punt z_0 want uit

$$z_0 = a\bar{z}_0 + b = a(\bar{a}z_0 + \bar{b}) + b\ .$$

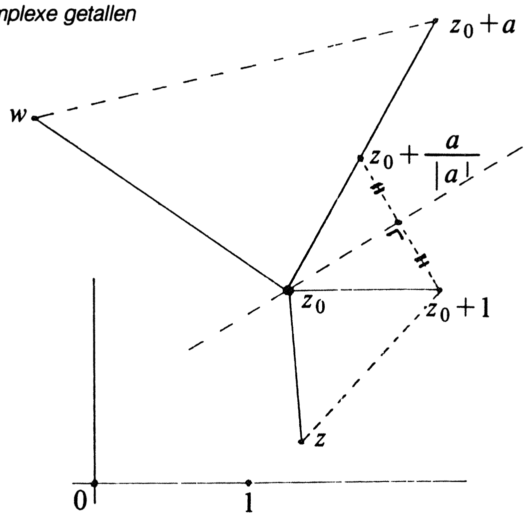
volgt

$$z_0 = \frac{a\bar{b} + b}{1 - a\bar{a}}\ .$$

Dan is (4) te schrijven als

$$w - z_0 = a(\bar{z} - \bar{z}_0)\ . \tag{5}$$

Omdat $z_0 \rightarrow z_0$ en $z_0 + 1 \rightarrow z_0 + a$ is dit blijkbaar een *spiegelvermenigvuldiging met centrum* z_0, *factor* $|a|$ *en als as de middelloodlijn van* $z_0 + 1$ *en* $z_0 + a/|a|$.



FIGUUR 10. Spiegelvermenigvuldiging

Spiegelingen en glijspiegelingen
Stel nu $|a|=1$, dus $a\bar{a}=1$.
Dan geeft (4), twee maal achter elkaar uitgevoerd:

$$z \to w = a(\overline{a\bar{z}+b})+b = a\bar{a}z + a\bar{b} + b = z + a\bar{b} + b \ .$$

Dit is de identiteit of een translatie.

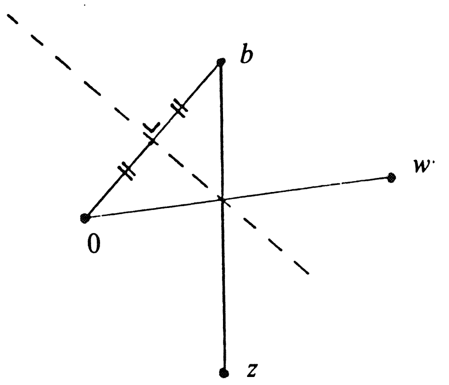
GEVAL 1: $a\bar{b}+b=0$.
Als $b=0$ is (4) een spiegeling in een lijn door 0 (voorbeeld (ii)).
Als $b\neq 0$ dan geldt $0 \longleftrightarrow b$ dus

$$\frac{w-0}{b-0}=\frac{\bar{z}-\bar{b}}{0-\bar{b}} \ , \text{ dat wil zeggen}$$

$$\frac{w}{b}+\frac{\bar{z}}{\bar{b}}=1 \ . \tag{7}$$

Dit is de vergelijking van de spiegeling in de middelloodlijn van 0 en b. De spiegelas, de verzameling van alle punten die invariant zijn, wordt gegeven door

$$\frac{z}{b}+\frac{\bar{z}}{\bar{b}}=1 \ . \tag{8}$$



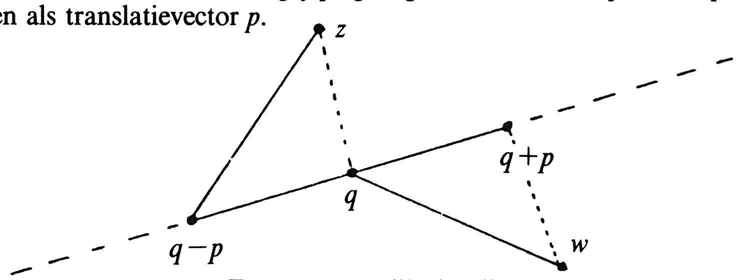
FIGUUR 11. Spiegeling in de middelloodlijn van 0 *en b*

GEVAL 2: $a\bar{b}+b \neq 0$.
Noem $a\bar{b}+b=2p$, $b=2q$.
Merk op:

$$q \mapsto q+p \ ,$$

$$q-p \mapsto q \ ,$$

dus de transformatie (4) is de *glijspiegeling* met als as de lijn door $q-p$, q en $q+p$, en als translatievector p.



FIGUUR 12. Glijspiegeling

SAMENVATTING:

$z=d\cdot\bar{z}$ $(d\cdot\bar{d}=1)$	is de lijn door de oorsprong waarvoor 1 en d elkaars spiegelbeeld zijn,
$w=d\cdot\bar{z}$	is de vergelijking van de spiegeling in die lijn;
$z/b+\bar{z}/\bar{b}=1$	is de vergelijking van de middelloodlijn van 0 en b,
$w/b+\bar{z}/\bar{b}=1$	is de vergelijking van de spiegeling in die lijn.

Overzicht van de groep van de gelijkvormigheidstransformaties:

$$\text{gelijkvormigheids-transformaties}\begin{cases}\text{direct: } w=az+b & \begin{cases} a\neq 1,\ |a|=1 : \text{rotatie} \\ a=1 : \text{translatie} \\ |a|\neq 1 : \text{draaivermenigvuldiging}\end{cases} \\ \\ \text{indirect: } w=a\bar{z}+b & \begin{cases} |a|\neq 1 : \text{spiegelvermenigvuldiging} \\ |a|=1,\ a\bar{b}+b=0\text{:spiegeling} \\ |a|=1,\ a\bar{b}+b\neq 0\text{:glijspiegeling}\end{cases}\end{cases}$$

5. PUNTEN, LIJNEN EN CIRKELS BIJ EEN DRIEHOEK

In het vervolg zal de letter d steeds gebruikt worden om punten aan te geven op de eenheidscirkel, dus $d\cdot\bar{d}=1$, zodat $\bar{d}=1/d$.

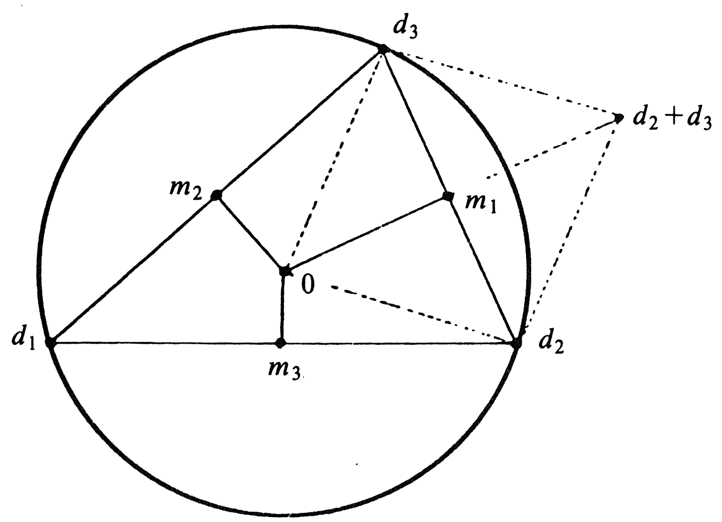
Laat een willekeurige driehoek gegeven zijn. Kies het complexe vlak zo, dat de eenheidscirkel de omgeschreven cirkel van die driehoek is. De hoekpunten noemen we d_1, d_2 en d_3.
Stel

$$s_1=d_1+d_2+d_3\ ,$$
$$s_2=d_1d_2+d_2d_3+d_3d_1\ ,$$
$$s_3=d_1d_2d_3$$

Merk op dat $s_3\bar{s}_3=1$, dus s_3 ligt ook op de eenheidscirkel.
Het midden van zijde d_1d_2 is

$$m_3=\tfrac{1}{2}\,(d_1+d_2)=\tfrac{1}{2}\,(s_1-d_3)$$

en evenzo zijn de andere zijdemiddens $m_1=\tfrac{1}{2}\,(s_1-d_1)$, $m_2=\tfrac{1}{2}\,(s_1-d_2)$.



FIGUUR 13. Driehoek met eenheidscirkel als omcirkel

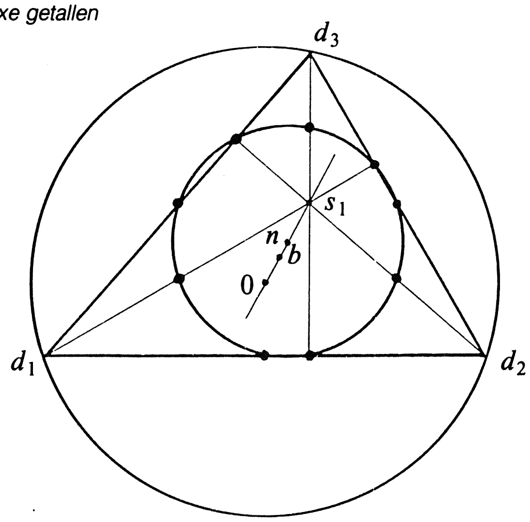
Als d de eenheidscirkel doorloopt, dan doorloopt

$$z = \tfrac{1}{2}(s_1 - d) \quad (d\bar{d} = 1) \tag{9}$$

een cirkel met middelpunt $n = \tfrac{1}{2}s_1$ en straal $\tfrac{1}{2}$. Deze cirkel gaat door m_1, m_2 en m_3. Het is de zg. *negenpuntscirkel* van de driehoek. We kunnen (9) opvatten als een *parametervoorstelling* van die cirkel, met d als parameter.

De verschilvector $s_1 - d_1 = d_2 + d_3$ staat loodrecht op de zijde $d_2 d_3$ want $0d_2(d_2+d_3)d_3$ is een ruit, dus de lijn door s_1 en d_1 is de *hoogtelijn* vanuit d_1. De andere hoogtelijnen zijn natuurlijk $s_1 d_2$ en $s_1 d_3$:
s_1 is het hoogtepunt van de driehoek.

Het *zwaartepunt* is $b = \tfrac{1}{3}(d_1 + d_2 + d_3) = \tfrac{1}{3}s_1$ en het middelpunt van de omcirkel is 0. Bijgevolg geldt:
Middelpunt van de omcirkel, zwaartepunt, middelpunt van de negenpuntscirkel en hoogtepunt van een driehoek liggen (in die volgorde) op één lijn, de zg. rechte van Euler. *Hun afstanden verhouden zich als* 2 : 1 : 3.



FIGUUR 14. Negenpuntscirkel en rechte van Euler

Verder: De negenpuntscirkel ontstaat uit de omcirkel
(i) *door vermenigvuldiging vanuit het hoogtepunt met een factor* ½, maar ook
(ii) *door vermenigvuldiging vanuit het zwaartepunt met een factor* − ½.
Uit (i) volgt dat de drie punten $\frac{1}{2}(s_1+d_i)$, de middens van de verbindingslijnstukken tussen hoekpunt en hoogtepunt, ook op (9) liggen. We laten nu zien dat (9) ook gaat door de voetpunten van de hoogtelijnen. Daarmee is de naam 'negenpuntscirkel' dan verklaard. Spiegeling van 0 in de zijde d_2d_3 geeft d_2+d_3, dus de vergelijking van die spiegeling is (zie (7)):

$$\frac{w}{d_2+d_3}+\frac{\bar{z}}{\bar{d}_2+\bar{d}_3}=1\,.$$

Het beeld w van $z=d_1$ is (na vereenvoudiging)

$$w=d_2+d_3-(d_2d_3)/d_1\,.$$

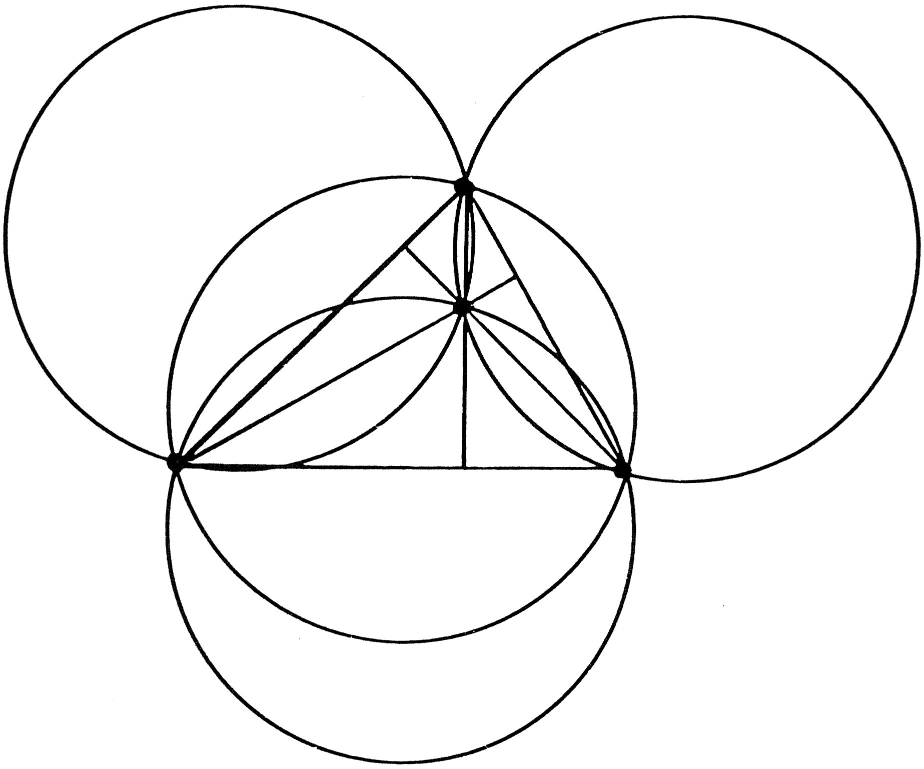
Het midden van het lijnstuk wd_1 is het voetpunt van de hoogtelijn uit d_1:

$$h_1=\tfrac{1}{2}(d_1+d_2+d_3-(d_2d_3)/d_1)=\tfrac{1}{2}(s_1-(d_2d_3)/d_1)\,.$$

Omdat $|(d_2d_3)/d_1|=1$, ligt h_1 op (9).

Nog een paar opmerkingen:

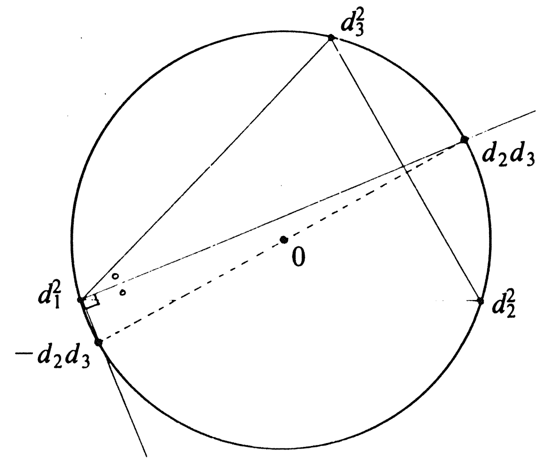
1. s_1 is het hoogtepunt van $d_1d_2d_3$. Maar d_1 is ook het hoogtepunt van $s_1d_2d_3$, d_2 dat van $d_1s_1d_3$, en d_3 dat van $d_1d_2s_1$. De vier punten spelen dus een gelijkwaardige rol: elk punt is het hoogtepunt van de andere drie. Men verifieert dat deze vier driehoeken allemaal *dezelfde* negenpuntscirkel hebben met voor elke driehoek ook *hetzelfde* stel van negen bijzondere punten op die cirkel.
2. Uit het bovenstaande volgt dat de vier driehoeken *congruente* omcirkels moeten hebben, want de straal van de omcirkel is twee maal die van de negenpuntscirkel.



FIGUUR 15. Vier congruente omcirkels

6. EEN RECHTHOEK IN EEN KOORDENVIERHOEK

We beschouwen weer een driehoek met de eenheidscirkel als omcirkel. Om verderop wortels te vermijden, stellen we de hoekpunten nu op d_1^2, d_2^2, d_3^2. Dan zijn d_2d_3 en $-d_2d_3$ de middens van de twee bogen tussen d_2^2 en d_3^2. De verbindingslijnen van die punten met d_1^2 zijn de twee *bissectrices* van de hoek bij d_1^2.



FIGUUR 16. De bissectrices van de hoek bij $d_1{}^2$

De bissectrice vanuit $d_1{}^2$ door d_2d_3 heeft als vergelijking (zie (8)):

$$\frac{z}{d_1{}^2+d_2d_3}+\frac{\bar{z}}{\bar{d}_1{}^2+\bar{d}_2\bar{d}_3}=1 \text{ ,d.w.z.}$$

$$z+\bar{z}d_1{}^2d_2d_3=d_1{}^2+d_2d_3 .$$

De andere bissectrice is

$$z-\bar{z}d_1{}^2d_2d_3=d_1{}^2-d_2d_3 .$$

We noteren weer $s_3=d_1d_2d_3$; dan zijn de bissectrices vanuit $d_i{}^2$ dus:

$$z\pm\bar{z}s_3d_i=d_i{}^2\pm s_3/d_i .$$

Kiezen we één bissectrice vanuit $d_1{}^2$ en één bissectrice vanuit $d_2{}^2$, zeg beide met plustekens, dan is het snijpunt het middelpunt van een ingeschreven of aangeschreven cirkel. Aftrekken van de vergelijkingen:

$$\bar{z}s_3(d_1-d_2)=d_1{}^2-d_2{}^2+s_3(1/d_1-1/d_2), \text{ dus}$$

$$\bar{z}s_3=d_1+d_2-d_3, \text{ zodat}$$

$$z=d_2d_3+d_1d_3-d_1d_2 .$$

Men verifieert dat dit punt juist ligt op de bissectrice van $d_3{}^2$ die hoort bij *mintekens:*

$$z-\bar{z}s_3d_3=d_3{}^2-d_1d_2 .$$

Hebben we *vier* punten $d_1{}^2$, $d_2{}^2$, $d_3{}^2$, $d_4{}^2$ die (in deze volgorde) op de eenheidscirkel liggen, dan krijgen we *vier* driehoeken door telkens één punt weg te laten. Bij geschikte tekenkeuzes worden de vier incentra:

$$z_4=d_1d_2+d_2d_3-d_1d_3$$

$$z_3 = d_1d_2 + d_1d_4 - d_2d_4$$
$$z_2 = d_1d_3 + d_1d_4 - d_3d_4$$
$$z_1 = d_2d_3 + d_2d_4 - d_3d_4\ .$$

Merk op: $z_4 - z_3 = z_1 - z_2$, dus $z_1z_2z_3z_4$ is een parallellogram.
Het is zelfs een rechthoek!

$$\begin{aligned} z_4 - z_3 &= d_2d_3 + d_2d_4 - d_1d_3 - d_1d_4 \\ \bar{z}_4 - \bar{z}_3 &= (d_1d_4 + d_1d_3 - d_2d_4 - d_2d_3)/(d_1d_2d_3d_4) \\ &= -(z_4 - z_3)/(d_1d_2d_3d_4) \end{aligned}$$

dus

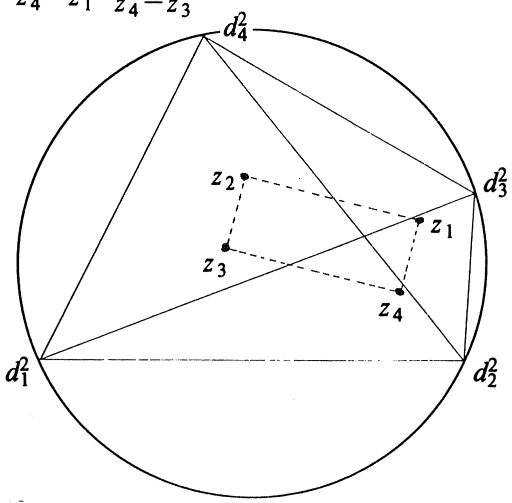
$$\frac{z_4 - z_3}{\bar{z}_4 - \bar{z}_3} = -d_1d_2d_3d_4\ .$$

Evenzo: $z_4 - z_1 = d_1d_2 + d_3d_4 - d_1d_3 - d_2d_4$, dus

$$\frac{z_4 - z_1}{\bar{z}_4 - \bar{z}_1} = d_1d_2d_3d_4\ .$$

Hieruit volgt:

$$\arg\frac{z_4 - z_3}{z_4 - z_1} = \tfrac{1}{2}\arg\left(\frac{z_4 - z_3}{z_4 - z_1}\cdot\frac{\bar{z}_4 - \bar{z}_1}{\bar{z}_4 - \bar{z}_3}\right) = \tfrac{1}{2}\arg(-1) = \frac{\pi}{2}\ .$$



FIGUUR 17. Een rechthoek van incentra

Samengevat:
Als $a_1a_2a_3a_4$ een koordenvierhoek is, en z_1, z_2, z_3 en z_4 zijn de middelpunten van de ingeschreven cirkels van de driehoeken $a_2a_3a_4$, $a_1a_3a_4$, $a_1a_2a_4$ en $a_1a_2a_3$, dan is $z_1z_2z_3z_4$ een rechthoek.

Nog twee operkingen:

1. Tekenen we ook nog de centra van de aangeschreven cirkels van de vier driehoeken, dan krijgen we er nog twaalf punten bij. De zestien punten liggen dan op twee viertallen evenwijdige lijnen die elkaar loodrecht snijden.
2. De richtingen van die viertallen evenwijdige lijnen zijn de bissectricerichtingen van elk paar overstaande zijden van de gegeven koordenvierhoek.

7. DE STELLING VAN FEUERBACH

We nemen nu een driehoek die de eenheidscirkel als *ingeschreven* cirkel heeft. Stel dat de zijden de cirkel raken in de punten d_1, d_2 en d_3. Het beeld van de oorsprong bij spiegeling in zo'n zijde is $2d_i$, dus de vergelijking van die zijde is (zie (8)):

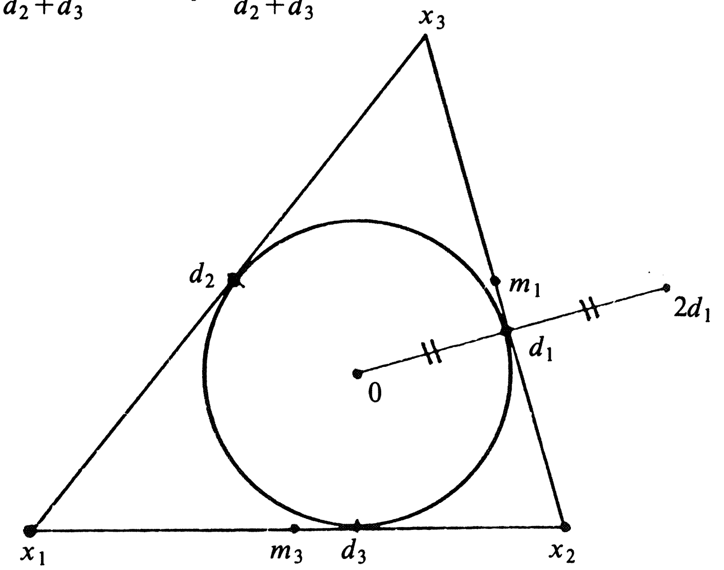
$$\frac{z}{2d_i}+\frac{\bar{z}}{2\bar{d}_i}=1 \text{ , d.w.z.}$$

$$z+\bar{z}d_i^{\,2}=2d_i \,.$$

De hoekpunten x_1, x_2 en x_3 van de driehoek vinden we door twee zijden te snijden, b.v. voor $i=2$, 3:

$$\bar{z}(d_2^{\,2}-d_3^{\,2})=2(d_2-d_3)$$

dus $\bar{x}_1=\dfrac{2}{d_2+d_3}$ zodat $x_1=\dfrac{2d_2d_3}{d_2+d_3}$.



FIGUUR 18. De eenheidscirkel als incirkel

Het midden m_1 van de zijde x_2x_3 is

$$m_1 = ½(x_2+x_3) = \frac{d_1d_3}{d_1+d_3} + \frac{d_1d_2}{d_1+d_2} = d_1\frac{s_2+d_2d_3}{(d_1+d_3)\,(d_1+d_2)}\ .$$

Door uitwerken verifieert men dat

$$(d_1+d_2)\,(d_2+d_3)\,(d_3+d_1) = s_1s_2 - s_3\ .$$

Het is geen beperking van de algemeenheid te veronderstellen dat $s_3 = d_1d_2d_3 = 1$. Dan geldt $\bar{s}_1 = (1/d_1 + 1/d_2 + 1/d_3) = d_2d_3 + d_3d_1 + d_1d_2 = s_2$. Daarmee wordt m_1:

$$\begin{aligned} m_1 &= d_1\frac{(s_2+d_2d_3)\,(d_2+d_3)}{(d_1+d_2)\,(d_2+d_3)\,(d_3+d_1)} = \frac{(s_2+d_2d_3)\,(s_2-d_2d_3)}{s_1s_2-s_3} \\ &= \frac{(\bar{s}_1+\bar{d}_1)\,(\bar{s}_1-\bar{d}_1)}{s_1\bar{s}_1-1} = \frac{\bar{s}_1^{\,2}-\bar{d}_1^{\,2}}{s_1\bar{s}_1-1}\ . \end{aligned}$$

Analoog voor m_2 en m_3.

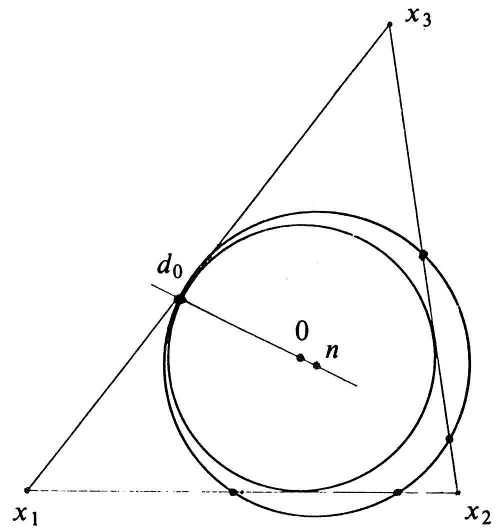
Hieruit is onmiddellijk de parametervoorstelling van de negenpuntscirkel af te lezen:

$$z = \frac{1}{s_1\bar{s}_1-1}\,(\bar{s}_1^{\,2} - d)\ . \qquad (d\bar{d}=1) \tag{10}$$

Het middelpunt is $n = (\bar{s}_1^{\,2})/(s_1\bar{s}_1-1)$.
Kiezen we in (10) $d = d_0 = s_2/s_1 = \bar{s}_1/s_1$ (merk op dat dit punt op de eenheidscirkel ligt!), dan blijkt d_0 ook op de negenpuntscirkel te liggen:

$$z = \frac{1}{s_1\bar{s}_1-1}\,(\bar{s}_1^{\,2} - \frac{\bar{s}_1}{s_1}) = d_0\ .$$

We kunnen d_0 schrijven als $d_0 = (\bar{s}_1)/s_1 = (\bar{s}_1)^2/(s_1\bar{s}_1)$, en daaruit blijkt dat 0, n en d_0 op één lijn liggen. Maar dat betekent dat de incirkel en de negenpuntscirkel elkaar in d_0 *raken.*



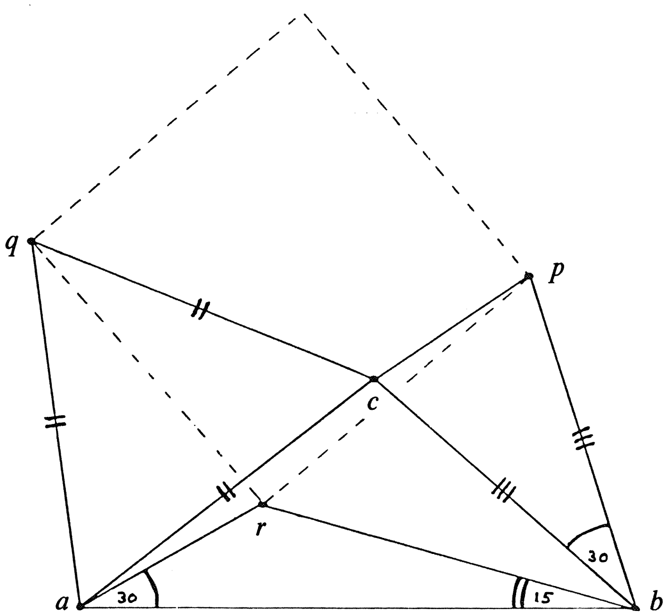
FIGUUR 19. De stelling van Feuerbach

STELLING (K.W. FEUERBACH, 1822): *de negenpuntscirkel raakt de ingeschreven en de drie aangeschreven cirkels.*

OPMERKING: de raakpunten van de in- en aangeschreven cirkels geven nòg vier bijzondere punten op de negenpuntscirkel. Maar in plaats van de oorspronkelijke driehoek hadden we ook een driehoek kunnen nemen die gevormd wordt door twee van de oorspronkelijke hoekpunten en het hoogtepunt. Zo'n driehoek heeft immers dezelfde negenpuntscirkel met hetzelfde stel van negen bijzondere punten. Maar i.h.a. zullen er vier andere raakpunten zijn. Op de negenpuntscirkel hebben we dus op deze manier al $9+4\cdot 4=25$ bijzondere punten!

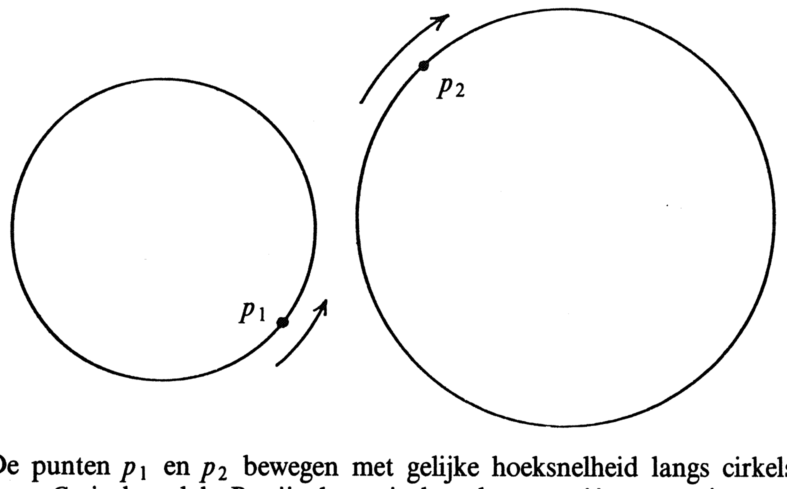
8. VIJF OPGAVEN

1. In figuur 20 zijn de punten p,q en r op de aangegeven wijze geconstrueerd, uitgaande van een willekeurige driehoek abc (de hoeken zijn in graden aangegeven). Bewijs dat p,r en q opvolgende hoekpunten zijn van een vierkant.



FIGUUR 20. Het verborgen vierkant

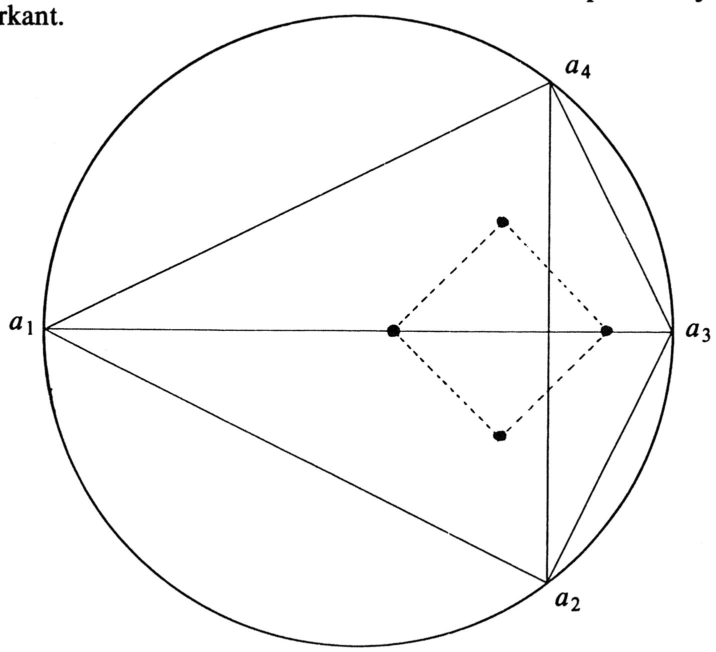
2. Op de zijden van een driehoek $a_1a_2a_3$ worden naar buiten toe gelijkzijdige driehoeken met centra o_1, o_2 en o_3 geconstrueerd. Bewijs dat het zwaartepunt van driehoek $a_1a_2a_3$ samenvalt met het centrum van driehoek $o_1o_2o_3$. Bewijs dat hetzelfde geldt als de drie gelijkzijdige driehoeken naar binnen toe op de zijden worden geconstrueerd.



3. De punten p_1 en p_2 bewegen met gelijke hoeksnelheid langs cirkels C_1 resp. C_2 in het vlak. Bewijs dat er in het algemeen één punt s is waarvoor de uitdrukking $|p_1 - s|^2 - |p_2 - s|^2$ constant is. Onderzoek de uitzonderlijke gevallen (de punten kunnen de cirkels in gelijke of in tegengestelde zin doorlopen).

(J. GILLIS: opgave 802 in CRUX MATHEMATICORUM 9 (1983), p. 21)

4. Zes punten op een cirkel zijn gegeven. Men kiest er drie uit (dat kan op 20 manieren) en verbindt het hoogtepunt van dat drietal met het zwaartepunt van het resterende drietal. Zo ontstaan 20 lijnen.
   Vervolgens verbindt men het centrum van de negenpuntscirkel van elk drietal met het centrum van de negenpuntscirkel van het complementaire drietal. Zo ontstaan nog 10 lijnen.
   Bewijs dat die 30 lijnen door één punt gaan.
5. Gegeven is een vlieger $a_1a_2a_3a_4$ (d.w.z. a_1a_3 deelt a_2a_4 loodrecht middendoor) met hoekpunten op een cirkel. Bewijs dat de incentra van de driehoeken $a_2a_3a_4$, $a_1a_2a_4$, $a_1a_3a_4$ en $a_1a_2a_3$ de hoekpunten zijn van een vierkant.



FIGUUR 22. Een vierkant in een vlieger

LITERATUUR

1. FRANK MORLEY, F.V. MORLEY (1933). *Inversive Geometry,* London, herdruk Chelsea, New York, 1954.
2. HANS SCHWERTFEGER (1962). *Geometry of Complex Numbers,* Toronto, herdruk Dover, New York, 1979.
3. DAN PEDOE (1957). *Circles,* Pergamon Press, herdruk Dover, New York, 1979.
4. DAN PEDOE (1970). *A Course of Geometry for Colleges and Universities,* Cambridge Univ. Press.

Hints bij de opgaven:

1. Deze opgave kan door directe berekening worden opgelost (kies b.v. $a=0$, $b=1$), maar ook via Petersen-Schoute: neem in fig.6 gelijkbenige rechthoekige driehoeken bpc, acq en rba met rechte hoeken in a, r en b. De punten p, q en r in fig.20 zijn dan overeenkomstige punten in deze driehoeken.
2. $o_i=a_{i+2}+t(a_{i+1}-a_{i+2})$ met $t=\dfrac{1}{\sqrt{3}}\,e^{i\,\pi/6}$, dus $\frac{1}{3}(o_1+o_2+o_3)=\frac{1}{3}(a_1+a_2+a_3)$.
3. Neem voor C_1 de eenheidscirkel, schrijf $p_1=d$, $p_2=z$; stel dat $z=a$ op het moment dat $d=1$, en laat m het middelpunt zijn van C_2. Dan geldt:

   (i) $z=m+d(a-m)$ als de cirkels in dezelfde zin worden doorlopen,

   (ii) $z=m+\bar{d}(a-m)=m+\dfrac{1}{d}(a-m)$ als de cirkels in tegengestelde zin worden doorlopen.

   In beide gevallen zoeken we een punt s waarvoor geldt
   $(d-s)(\bar{d}-\bar{s})-(z-s)(\bar{z}-\bar{s})-\gamma=0$.
   voor zekere reële constante γ.
   Dit geeft na substitutie een vierkantsvergelijking in d (schrijf steeds $\bar{d}=1/d$). Omdat het linkerlid een polynoom is dat voor alle d op de eenheidscirkel de waarde 0 aanneemt, moeten de coëfficiënten alle drie nul zijn. Hiermee is de opgave verder op te lossen. De uitzonderlijke gevallen blijken op te treden als:
   in (i): $a-m=1$;
   in (ii): $(a-m)(\bar{a}-\bar{m})=1$.
4. Met de methodes van paragraaf 5 kan deze opgave worden opgelost. Zie ook JAN VAN DE CRAATS: *On Six Concyclic Points,* CRUX MATHEMATICORUM 8 (1982), p. 160-162.
5. De symmetrie-as van de vlieger is ook symmetrie-as van de rechthoek van de incentra. Deze opgave noodt echter wellicht ook tot het zoeken naar een meer 'direct' bewijs.
   Zie ook: CRUX MATHEMATICORUM 6, p. 226-230 (opgave 483), en de daar gegeven referenties.

Toepassingen van Complexe Getallen in de Techniek

J.T. Fokkema
Technische Universiteit Delft
Postbus 356, 2600 AJ Delft

1. De lineaire homogene differentiaalvergelijking

Complexe getallen spelen in de techniek een belangrijke rol bij het oplossen van lineaire differentiaalvergelijkingen. We beperken ons hier tot die technische toepassingen waarbij de grootheden als functie van de tijd moeten voldoen aan genoemde differentiaalvergelijkingen. De tijd t zal dus de onafhankelijke veranderlijke zijn. Essentiëel is deze beperking echter niet voor de hierna volgende geschetste methode. Met het oog op het complexe karakter zullen we de zaak voorzichtig opbouwen.

1.1. De eerste orde differentiaalvergelijking

Laten we ons in eerste instantie eens bezig houden met een eenvoudige differentiaalvergelijking (DV) en wel de eenvoudigste die er is: de lineaire homogene DV van de eerste orde

$$\frac{dy}{dt} + ay = 0.$$

De DV is van de eerste orde omdat de onbekende y slechts éénmaal gedifferentieerd in de vergelijking voorkomt; lineair omdat nergens de onbekende niet-lineair voorkomt (b.v. $\sqrt{y}$ of $(\frac{dy}{dt})^2$); homogeen omdat het rechter lid gelijk aan nul is.

De oplossing van deze DV kunnen we direct door integratie vinden

$$\frac{dy}{y} = -adt,$$

$$\int \frac{dy}{y} = -\int adt + A,$$

$$\ln(y) = -at + A,$$

waarin A een willekeurige constante is. y kan nu expliciet geschreven worden als

$$y = e^{-at+A}.$$

Aangezien A willekeurig is, kunnen we ook schrijven

$$y = Be^{-at}.$$

We leren van deze eenvoudige eerste orde vergelijking dat één constante genoeg is om de oplossing te bepalen. De waarde van deze constante volgt uit een bekende waarde van y voor een bepaalde waarde van t. Deze waarde van y noemt men de beginvoorwaarde. Zoals de naam beginvoorwaarde al doet vermoeden, nemen we meestal de waarde van y voor het tijdstip $t = 0$ als de bekende waarde. Noemen we deze waarde y_0 dan kunnen we de oplossing schrijven als

$$y = y_0 e^{-at}.$$

De oplossing y is dus een exponentiële functie van t. Dit is niet toevallig omdat de afgeleide van een exponentiële functie wederom een exponentiële functie is en we zien uit de structuur van de DV dat, als we de constante in het argument van de exponentiële functie aanpassen, de oplossing eenvoudig volgt uit een algebraïsche vergelijking. Immers, stellen we dat $e^{\lambda t}$ moet voldoen aan de DV, dan gaat deze over in de volgende vergelijking

$$\lambda e^{\lambda t} + a e^{\lambda t} = 0,$$

of

$$e^{\lambda t}(\lambda + a) = 0.$$

Aangezien $e^{\lambda t}$ voor alle eindige waarden van t ongelijk nul is, moet gelden dat $\lambda + a = 0$ oftewel $\lambda = -a$, zodat $y = e^{-at}$ een oplossing is. Verder moet om aan de beginwaarden te voldoen een constante B ingevoerd worden, zodat we weer gevonden hebben dat de oplossing gegeven wordt door $y = Be^{-at}$. We zien dat we het oplossen van dit type differentiaalvergelijking teruggebracht hebben tot het oplossen van een algebraïsche vergelijking.

1.2. De tweede orde DV

Overmoedig geworden, wagen we ons aan de tweede orde DV

$$\frac{d^2y}{dt^2} - a^2 y = 0.$$

We poneren wederom dat de algemene oplossing van de gedaante $e^{\lambda t}$ zal zijn. Dit leidt dan tot de volgende vergelijking

$$\lambda^2 - a^2 = 0$$

of

$$(\lambda + a)\cdot(\lambda - a) = 0,$$

zodat de totale oplossing zal zijn

$$y = B_1 e^{at} + B_2 e^{-at}.$$

We hebben twee constanten (B_1 en B_2) nodig om de oplossing volledig te bepalen (B_1 en B_2 volgen bijvoorbeeld uit de waarde van y en $\frac{dy}{dt}$ voor $t = 0$). Maar als we nu eens geconfronteerd worden met de DV

$$\frac{d^2y}{dt^2} + a^2 y = 0,$$

dan zien we dat met de substitutie $e^{\lambda t}$ we de algebraïsche vergelijking

$$\lambda^2 + a^2 = 0$$

krijgen en nu is de grote vraag: wat zijn de wortels van deze vergelijking? We kunnen natuurlijk de zaak afdoen met te stellen dat er geen oplossing is voor deze DV. Maar dat is nonsens want deze DV is niets anders dan de bekende trillingsvergelijking van fysische systemen. Laten we eens proberen de oplossing via een andere weg te verkrijgen. De oplosfunctie moet als functie van t een zodanige vorm hebben dat als de betreffende functie tweemaal gedifferentiëerd wordt, hij gelijk is aan de oorspronkelijke functie maar dan met een minteken. De klasse van functies die hieraan voldoen zijn de bekende goniometrische functies cosinus en sinus, zodat de oplossing van de DV van de gedaante

$$y = B_1 \cos(at) + B_2 \sin(at)$$

is. Geheel bevredigend is deze aanpak echter niet. Wiskundig als we zijn, vermoeden we dat er een relatie moet bestaan tussen de exponentiële functies en de goniometrische functies. Als we deze relatie willen vaststellen, dan moeten we de oplossingen zien te vinden van $\lambda^2 + a^2 = 0$. In dat geval moet gelden

$$\lambda = \pm\sqrt{-a^2} = \pm(\sqrt{-1})a.$$

De factor $\sqrt{-1}$ geven we een aparte naam en noemen hem de imaginaire grootheid j (in dit geval gebruiken we niet de voor de hand liggende i, omdat we later deze letter zullen reserveren voor de stroom in een elektrisch netwerk, zoals dit gebruikelijk is in elektrische kringen.) De oplossing kan nu geschreven worden als

$$y = C_3 e^{jat} + C_4 e^{-jat}.$$

Nu hebben we via een gekunstelde ingreep een oplossing gecreëerd, maar het verband met de goniometrische functies is nog niet duidelijk. Daartoe beschouwen we eerst de machtreeksontwikkeling van de exponentiële functie:

$$e^t = \sum_{n=o}^{\infty} \frac{1}{n!} t^n.$$

Is nu het argument van de exponentiële functie imaginair, dan splitst de reeks zich in twee reeksen

$$e^{jt} = \sum_{n=0}^{\infty} \frac{1}{n!}(jt)^n = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} t^{2n} + j \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} t^{2n+1},$$

waarbij gebruik gemaakt is van het feit dat $j^2 = -1$, $j^3 = -j$, $j^4 = 1$, $j^5 = j$ enz.

De beide machtreeksen zijn echter weer te herkennen; de eerste reeks in het rechter lid is de machtreeksontwikkeling van de cosinus, de tweede die van de sinus, zodat we kunnen schrijven

$$e^{jt} = \cos(t) + j\sin(t).$$

Deze betrekking wordt wel de formule van Euler genoemd. We zien dat e^{jt} de som is van een reëel getal ($\cos(t)$) en een imaginair getal ($j\sin(t)$). Deze combinatie heeft in de wiskunde de naam van complex getal gekregen. Met deze kennis gewapend laat zich de tweede oplossing van de DV schrijven als

$$y = C_3\{\cos(at) + j\sin(at)\} + C_4\{\cos(at) - j\sin(at)\},$$

waarin C_3 en C_4 nog onbepaalde constanten zijn. De constanten zullen in het algemeen complex zijn. Stellen we daarom dat $C_3 = u_3 + jv_3$ en $C_4 = u_4 + jv_4$, dan gaat y over in:

$$y = (u_3 + u_4)\cos(at) + (v_4 - v_3)\sin(at) + \\ + j\{(v_3 + v_4)\cos(at) + (u_3 - u_4)\sin(at)\}.$$

Omdat y reëel moet zijn (y moet voldoen aan een DV met reële coëfficiënten), moet het imaginaire deel nul zijn. Dus moet gelden dat $u_3 = u_4$ en $v_3 = -v_4$, zodat

$$C_3 = u_4 - jv_4,$$

en

$$C_4 = u_4 + jv_4.$$

Getallen C_3 en C_4 staan dus in een zodanige relatie tot elkaar dat de reële delen gelijk zijn en de imaginaire delen alleen op het teken na aan elkaar gelijk zijn. De getallen C_3 en C_4 noemt men in dat geval toegevoegd complex. Schrijven we $u_3 + u_4 = B_1$ en $v_4 - v_3 = B_2$ dan krijgen we

$$y = B_1\cos(at) + B_2\sin(at),$$

hetgeen we al eerder gevonden hadden door goniometrische substitutie. De zaak is nu vanuit een mathematisch standpunt bekeken rond. Stellen we vervolgens dat $\tan(\Phi) = \dfrac{B_1}{B_2}$ en $A = \dfrac{B_2}{\cos(\Phi)}$ dan kunnen we voor y schrijven

$$y = A\sin(at + \Phi).$$

Beide voorstellingen zijn gelijkwaardig, beide hebben ze twee onbepaalde coëfficiënten die rechtstreeks uit de beginwaarden volgen.

1.3. De n-de orde DV

Met de kennis uit de vorige paragraaf kunnen we nu vrij eenvoudig inzien dat n-de orde lineaire homogene DV met constante coëfficiënten

$$a_0\frac{d^n}{dt^n}y + a_1\frac{d^{n-1}}{dt^{n-1}}y + ... + a_n y = 0,$$

of geschreven in operator vorm

$$L \cdot y = 0,$$

door substitutie van $e^{\lambda t}$ overgaat in het polynoom $P(\lambda)$:

$$P(\lambda) = a_0\lambda^n + a_1\lambda^{n-1} + ... + a_n = 0,$$

hetgeen wel de karakteristieke vergelijking wordt genoemd. Ontbinding van het polynoom geeft

$$P(\lambda) = a_0(\lambda-\lambda_1)(\lambda-\lambda_2)...(\lambda-\lambda_n).$$

Hieruit volgt dat $y_1 = e^{\lambda_1 t}, y_2 = e^{\lambda_2 t}, ..., y_n = e^{\lambda_n t}$ allemaal oplossingen zijn van de DV.

De operator L is een lineaire operator, dat wil zeggen dat voor een willekeurige constante B en twee verschillende oplossingen y_1 en y_2 van de DV geldt:

$$L \cdot (By_1) = BL \cdot y_1,$$

en

$$L \cdot (y_1 + y_2) = L \cdot y_1 + L \cdot y_2,$$

dus ook By_1 en $y_1 + y_2$ zijn oplossingen van de DV. De volledig algemene oplossingen van de DV kan dan geschreven worden als

$$y = B_1 e^{\lambda_1 t} + B_2 e^{\lambda_2 t} + ... + B_n e^{\lambda_n t},$$

waarin $B_1, B_2, ..., B_n$ onbepaalde coëfficiënten zijn die uit de beginvoorwaarden volgen. Bijvoorbeeld uit:

$$\frac{d^n y}{dt^n}\Big|_{t=0}, \frac{d^{n-1}y}{dt^{n-1}}\Big|_{t=0}, ..., y(0).$$

De wortels van de karakteristieke vergelijking zijn in het algemeen complex (een reëel getal is een bijzonder complex getal, namelijk één met het imaginaire deel gelijk aan nul). Aangezien de coëfficiënten van de karakteristieke vergelijking reëel zijn, komen eventuele complexe wortels steeds als paren toegevoegde complexe wortels voor. Naast de wortel $u + jv$ komt dus ook voor de wortel $u - jv$, zodat het effect voor de polynoom-ontbinding weer reëel is, immers

$$(\lambda - u - jv)(\lambda - u + jv) = (\lambda - u)^2 + v^2.$$

De beide toegevoegde complexe wortels geven aanleiding tot de beide oplossingen

$$y_1 = e^{(u+jv)t} = e^{ut}\{\cos(vt) + j\sin(vt)\},$$

en

$$y_2 = e^{(u-jv)t} = e^{ut}\{\cos(vt) - j\sin(vt)\}.$$

Uit het lineaire karakter van de DV volgt dat

$$\frac{1}{2}(y_1 + y_2) = e^{ut}\cos(vt),$$

en

$$\frac{1}{2j}(y_1 - y_2) = e^{ut}\sin(vt),$$

ook twee oplossingen zijn, die we dus in de plaats kunnen stellen van de complexe oplossingen.

2. De niet-homogene lineaire differentiaalvergelijking

Voor de oplossing van de niet-homogene lineaire vergelijking

$$a_0\frac{d^n y}{dt^n} + a_1\frac{d^{n-1}}{dt^{n-1}}y + \dots + a_n y = x(t),$$

of in operator vorm

$$L{\cdot}y = x(t)$$

kunnen we gebruik maken van onze kennis betreffende de homogene vergelijking. Het zal duidelijk zijn dat $Be^{\lambda t}$ nu geen oplossing kan zijn. Met een spitsvondige redenering kunnen we echter de weg tot de oplossing vinden. De algemene oplossing moet weer n onbepaalde constanten bevatten, omdat de vergelijking van de n-de orde is. Stel dat men er op een of andere manier in slaagt één speciale oplossing van de niet-homogene vergelijking te vinden, $y_p = y_p(t)$, die *geen* onbepaalde constanten bevat. Dat noemt men een particuliere oplossing van de vergelijking. De oplossing van de homogene vergelijking die men krijgt door het rechterlid $x(t) = 0$ te stellen, is zoals we al eerder hebben gezien

$$y_h = C_1 e^{\lambda_1 t} + C_2 e^{\lambda_2 t} + \dots + C_n e^{\lambda_n t},$$

dan is de functie

$$y_t = y_h + y_p,$$

een volledige oplossing van de niet-homogene vergelijking. De functie voldoet immers aan $L{\cdot}y = x$ en zij bevat n onbepaalde constanten. De vraag is of dit inderdaad dan ook de enige oplossing is. Laten we eens aannemen dat we twee particuliere oplossingen hebben, $y_{p,1}$ en $y_{p,2}$, dus

$$L{\cdot}y_{p,1} = x$$

en

$$L{\cdot}y_{p,2} = x.$$

Aangezien L een lineaire operator is, kunnen we schrijven dat

$$L\cdot(y_{p,1}-y_{p,2}) = L\cdot y_{p,1}-L\cdot y_{p,2} = x - x = 0,$$

zodat $y_{p,1}-y_{p,2}$ een oplossing is van de homogene vergelijking. Hieruit volgt dat twee verschillende particuliere oplossingen alleen op homogene oplossingen na aan elkaar gelijk moeten zijn, zodat dus inderdaad $y_t=y_p+y_h$ de volledige oplossing is.

De oplossing van de homogene vergelijking is in het algemeen een som van exponentiële functies. Omdat we graag willen dat y_t een begrensde functie blijft, moeten we eisen dat het reële deel van de nulpunten van de karakteristieke vergelijking kleiner dan of ten hoogste gelijk aan nul is. Met andere woorden als we complexe getallen gesitueerd denken in het complexe vlak waarbij het reële deel de abscis en het imaginaire deel de ordinaat is, dan moeten de nulpunten in het linker halfvlak liggen, eventueel met inbegrip van de imaginaire as. Voor de meeste fysische systemen echter liggen de nulpunten geheel in het linker halfvlak. We zien dat dan voor voldoend grote t de invloed van y_h op de volledige oplossing verwaarloosd kan worden. Deze functie wordt daarom het inschakelverschijnsel of de overgangstoestand genoemd. We merken nogmaals op dat deze overgangstoestand door de begincondities via de onbepaalde coëfficiënten bepaald wordt. Dus voor voldoend grote t wordt de totale oplossing alleen beschreven door de particuliere oplossing die door deze eigenschap wel de stationaire toestand genoemd wordt. De particuliere oplossing bevat echter geen constanten die door de beginsituatie bepaald worden! Men drukt dit feit wel aldus uit: de stationaire toestand is die toestand van een systeem dat vergeten is hoe het begonnen is.

3. De niet-homogene vergelijking als systeemvergelijking

We kunnen de niet-homogene DV ook beschouwen als een systeemvergelijking waarbij de bekende functie $x(t)$ aan het systeem aangeboden wordt (ook wel de excitatie van het systeem of bronfunctie genoemd) en de functie y die beschouwd kan worden als het resultaat (de responsie van het systeem). De vraag is nu: is het systeem lineair? Om die vraag te kunnen beantwoorden onderzoeken we de volgende 1ste orde niet-homogene DV:

$$\frac{dy}{dt} + ay = x_1(t),$$

met de volledige oplossing

$$y_1(t) = B_1e^{-at} + y_{p,1}(t).$$

Stel nu dat we als excitatie $x_2(t)$ hebben, dan geldt:

$$\frac{dy}{dt} + ay = x_2(t)$$

en

$$y_2(t) = B_2e^{-at} + y_{p,2}(t).$$

Gaan we ervan uit dat de beginwaarden van $t=0$ gegeven zijn, dan laten de constanten B_1 en B_2 zich bepalen en we kunnen schrijven

$$y_1(t) = \{y_1(0) - y_{p,1}(0)\}e^{-at} + y_{p,1}(t),$$

en

$$y_2(t) = \{y_2(0) - y_{p,2}(0)\}e^{-at} + y_{p,2}(t).$$

Was echter de bronfunctie de som van x_1 en x_2 geweest, dan hadden we de volgende situatie gehad

$$\frac{dy}{dt} + ay = x_1(t) + x_2(t),$$

en

$$y_3(t) = \{y_3(0) - y_{p,1}(0) - y_{p,2}(0)\}e^{-at} + y_{p,1}(t) + y_{p,2}(t),$$

waarbij gebruik gemaakt is van de lineariteit van de DV t.a.v. de particuliere oplossing: $L\cdot(y_{p,1} + y_{p,2}) = L\cdot y_{p,1} + L\cdot y_{p,2} = x_1(t) + x_2(t)$.

Maar als het systeem lineair is dan moet gelden

$$y_3(t) = y_1(t) + y_2(t),$$

en dit kan alleen maar waar zijn als geldt dat $y_3(0) = y_1(0) + y_2(0)$. Deze voorwaarde geldt in het algemeen niet. We zien dat als we een lineair systeem willen garanderen, we moeten eisen dat de beginvoorwaarde gelijk aan nul zal zijn (en in het algemeen moet dan gelden dat voor een n-orde systeem alle betreffende afgeleiden van de responsie in het beginpunt nul zijn). Het feit dat als y_1 de responsie van x_1 en y_2 de responsie van x_2 is, dat dan voor lineaire systemen moet gelden dat $y_1 + y_2$ de responsie van $x_1 + x_2$ is, noemt men het superpositiebeginsel. Gemakkelijk kan nagegaan worden dat dezelfde beschouwing geldt t.a.v de coëfficiëntvermenigvuldig, dus als geldt y_1 is de responsie op x_1 dan is by_1 de responsie op bx_1.

4. De particuliere oplossing bij harmonische excitatie

Tot nu toe hebben we ons nog niet druk gemaakt hoe we de particuliere oplossing moeten bepalen. Voor een bepaalde klasse van functies is echter de zaak heel eenvoudig. Als namelijk de bronfunctie cosinus- of sinusvormig is met een bepaalde radiaalfrequentie ω, is de responsie ook een cosinus- of sinusfunctie met dezelfde ω maar in het algemeen met een verschillende fase en amplitude. Deze klasse van functies worden ook wel harmonische functies genoemd. Dit laat zich als volgt bewijzen.

Als we uitgaan van de excitatie

$$x(t) = A\cos(\omega t + \Phi),$$

waarin A de amplitude en Φ de fase wordt genoemd, dan voldoet $x(t)$ zoals we eerder hebben gezien aan de DV

$$\frac{d^2}{dt^2}x + \omega^2 x = 0.$$

Verder is x de excitatie van de systeemvergelijking $L{\cdot}y = x$, zodat voor de particuliere oplossing geldt

$$L{\cdot}y_p = x.$$

Aangezien L een lineaire operator is, geldt:

$$\frac{d^2}{dt^2}\{L{\cdot}y_p\} = \frac{d^2}{dt^2}x,$$

of

$$L{\cdot}\{\frac{d^2}{dt^2}y_p\} = \frac{d^2}{dt^2}x$$

en tevens geldt volgens dezelfde lineariteit

$$-\omega^2\{L{\cdot}y_p\} = -\omega^2 x,$$

of

$$L{\cdot}\{-\omega^2 y_p\} = -\omega^2 x.$$

Aangezien $\frac{d^2}{dt^2}x = -\omega^2 x$, geldt voor y_p dus ook

$$\frac{d^2}{dt^2}y_p + \omega^2 y_p = 0.$$

Met andere woorden: ook de particuliere oplossing voor y_p is voor dit geval een harmonische functie met dezelfde radiaalfrequentie ω. In het algemeen kunnen we dan de particuliere oplossing schrijven als

$$y_p(t) = B\cos(\omega t + \Psi),$$

waarbij de onbekende amplitude B en de fase volgen uit de DV

$$L{\cdot}y_p = A\cos(\omega t + \Phi).$$

5. De complexe rekenwijze

De complexe rekenwijze verschaft ons een systematische manier om de amplitude en de fase van de particuliere oplossing te bepalen als we een harmonische bronfunctie hebben. De bronfunctie $x = A\cos(\omega t + \Phi)$ kan namelijk geschreven worden als

$$x = \mathrm{Re}\{Xe^{j\omega t}\},$$

met

$$X = Ae^{j\Phi},$$

waarbij Re{ } staat voor het reële deel van { }. X is dus een complexe grootheid die via bovenstaand 'recept' aan x toegevoegd wordt.

Op dezelfde manier kunnen we de particuliere oplossing schrijven als

$$y_p = \mathrm{Re}\{Y_p e^{j\omega t}\}$$

met

$$Y_p = Be^{j\Psi},$$

met Y_p als de complexe representant van y_p.

Hiermee gaat de DV, $L \cdot y_p = x$, over in de vergelijking

$$L \cdot \mathrm{Re}\{Y_p e^{j\omega t}\} = \mathrm{Re}\{Xe^{j\omega t}\},$$

of

$$\mathrm{Re} L \cdot \{Y_p e^{j\omega t}\} = \mathrm{Re}\{Xe^{j\omega t}\},$$

hetgeen weer te schrijven is als

$$\mathrm{Re}\{Y_p P(j\omega) e^{j\omega t}\} = \mathrm{Re}\{Xe^{j\omega t}\},$$

waarbij de DV het complexe polynoom $P(j\omega)$ gegenereerd heeft. Als we vervolgens de vergelijking

$$Y_p P(j\omega) e^{j\omega t} = Xe^{j\omega t},$$

of

$$Y_p P(j\omega) = X$$

oplossen hebben we tevens de vergelijking met de reëele delen opgelost. Immers de vergelijking $Y_p P = X$ is een complexe vergelijking, waarvoor geldt dat zowel de reëele als de imaginaire delen aan elkaar gelijk moeten zijn.

De reëele particuliere oplossing volgt nu uit de complexe oplossing via het 'recept'

$$y_p = \mathrm{Re}\{Y_p e^{j\omega t}\} = \mathrm{Re}\{\frac{X}{P(j\omega)} e^{j\omega t}\}.$$

De complexe rekenwijze voor het vinden van de particuliere oplossing komt dus neer op de transformatie van de reëele grootheden naar het complexe domein via de heentransformatie

$$x \rightarrow X = Ae^{j\Phi},$$

en

$$y_p \rightarrow Y_p = Be^{j\Psi}.$$

Vervolgens gaat in dit domein de differentiaaloperator $\frac{d}{dt}$ over in de vermenigvuldigingsfactor $j\omega$, zodat de DV naar een algebraïsche vergelijking getransformeerd wordt. Tenslotte worden dan de reëele grootheden weer gevonden via de terugtransformatie

$$X \rightarrow x = \mathrm{Re}\{Xe^{j\omega t}\},$$

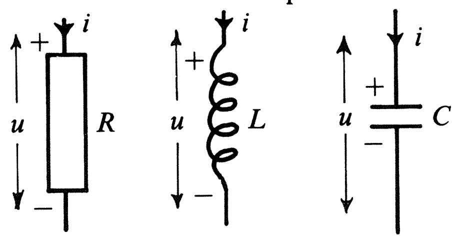
en

$$Y_p \rightarrow y_p = \mathrm{Re}\{Y_p e^{j\omega t}\}.$$

We merken op dat zowel X als Y_p in het algemeen functies van ω zijn.

6. Een elektrotechnische toepassing

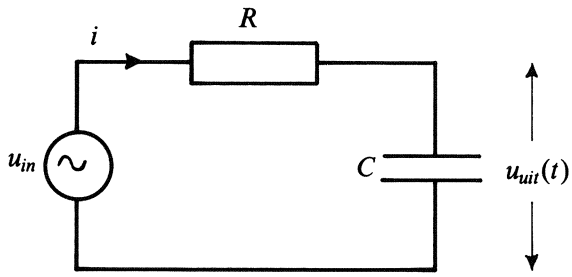
De belangrijkste drie elektrische netwerkelementen zijn de weerstand (R), de spoel (L) en de condensator (C). Hiervoor gelden de volgende spanning-stroomrelaties, aangenomen dat de tekenafspraak is zoals die in figuur 1 is weergegeven.



$$u = Ri,$$
$$u = L\frac{di}{dt},$$
$$en \quad i = C\frac{du}{dt},$$

Figuur 1

waarbij L de coëfficiënt van zelfinductie en C de capaciteit genoemd wordt.
We beschouwen nu het netwerk zoals dat gegeven is in figuur 2.



Figuur 2

We nemen aan dat de harmonische bron $u_{in} = \hat{u}_{in}\cos(\omega t)$ op het tijdstip $t = 0$ ingeschakeld wordt. Aangezien de stroom i door het netwerk bepaald wordt door $C\frac{d}{dt}u_{uit}$, geldt de volgende DV

$$iR + u_{uit} = u_{in},$$

of

$$RC\frac{d}{dt}u_{uit} + u_{uit} = u_{in},$$

waarbij gebruik is gemaakt van de spanningswet van Kirchoff. Volgens deze wet geldt dat voor elk gesloten circuit (kringloop) in een netwerk de som van alle spanningen nul is. De homogene oplossing van de DV is:

$$u_{uit,h} = Be^{-t/RC}.$$

Voor het vinden van de particuliere oplossing maken we gebruik van de complexe rekenwijze. De DV gaat dan over in

$$j\omega RC U_{uit,p} + U_{uit,p} = U_{in},$$

met $U_{in} = \hat{u}_{in}$ aangezien de fase van de bron in dit geval nul is. Voor $U_{uit,p}(\omega)$ kunnen we dan schrijven

$$U_{uit,p} = \frac{U_{in}}{j\omega RC+1} = \frac{\hat{u}_{in}}{j\omega RC+1} = \frac{(1-j\omega RC)\hat{u}_{in}}{1+\omega^2 RC},$$

zodat $u_{uit,p}(t)$ via de terugtransformatie geschreven kan worden als

$$u_{uit,p}(t) = \frac{\hat{u}_i}{\sqrt{1+\omega^2 RC}}\cos(\omega t - \Psi),$$

met $\Psi = \arctan(\omega RC)$.

De totale oplossing is nu

$$u_{uit}(t) = Be^{-t/RC} + \frac{\hat{u}_{in}}{\sqrt{1+\omega^2 RC}}\cos(\omega t - \Psi).$$

Met de beginconditie $u_{uit}(0)=0$ krijgen we dan tenslotte

$$u_{uit}(t) = \frac{\hat{u}_{in}}{\sqrt{1+\omega^2 RC}}[\cos(\omega t - \Psi) - \cos(\Psi)e^{-t/RC}].$$

Voor het geval we met een gelijkspanningsbron te maken hebben ($\omega=0$), krijgen we

$$u_{uit}(t) = \hat{u}_{in}[1-e^{-t/RC}].$$

We merken op dat het inschakelverschijnsel exponentiëel uitdempt en dat de particuliere oplossing de bron volgt en verder dat de particuliere oplossing de hoek Ψ (frequentie-afhankelijk) naijlt t.o.v. de bronfunctie. Tevens zien we dat ook de amplitude van $U_{uit,p}$ frequentie-afhankelijk is. Als we echter alleen in de particuliere oplossing geïnteresseerd zijn, hoeven we niet de DV op te stellen. Dit is als volgt in te zien. In het complexe domein gaan de spanning-stroomrelaties van de drie genoemde netwerkelementen over in

$$U = RI,$$
$$U = j\omega LI,$$
$$U = \frac{I}{j\omega C}$$

Hieruit blijkt dat in dit domein R, $j\omega L$ en $\frac{1}{j\omega C}$ alle drie de functie van weerstand vervullen.

Maar in het geval van de spoel en de condensator hebben we te maken met een imaginaire grootheid. Dan spreekt men niet van weerstand maar van impedantie (in het algemeen is de impedantie van samengestelde netwerkelementen complex). dus kan in het complexe domein de spanning $U_{uit,p}$ gevonden worden uit de spanningsdeling

$$U_{uit,p} = \frac{\frac{1}{j\omega C}}{\frac{i}{j\omega C} + R} U_{in} = \frac{\hat{u}_{in}}{1 + j\omega RC},$$

hetgeen overeenkomt met het eerder gevonden resultaat.

Dit is echter dezelfde methode zoals die gevolgd wordt als we te maken hebben met gelijkspanningen. We kunnen dus concluderen dat het rekenen met wisselstroomgrootheden in het complexe domein isomorf is aan het rekenen met gelijkspanningsgrootheden in het reële domein.

7. Het wijzerdiagram

De bepaling van de particuliere oplossing kan ook geschieden met behulp van een grafische methode. De complexe spanningen en stromen, die we in de vorige paragraaf ontmoet hebben, kunnen we ook afbeelden in het complexe vlak met de horizontale as als het reëele deel en de verticale as als het imaginaire deel. In het algemeen zijn de complexe spanning en stroom gegeven door $U = Ae^{j\Phi}$ en $I = Be^{j\Psi}$. We kunnen ons de spanning en stroom dan voorstellen als vectoren met respectievelijk de lengte A en B en een fasehoek Φ en Ψ t.o.v. de positieve reële as (de polaire voorstelling van het complexe getal).

Verder maken we gebruik van de faserelaties tussen spanning en stroom van de drie netwerkelementen:

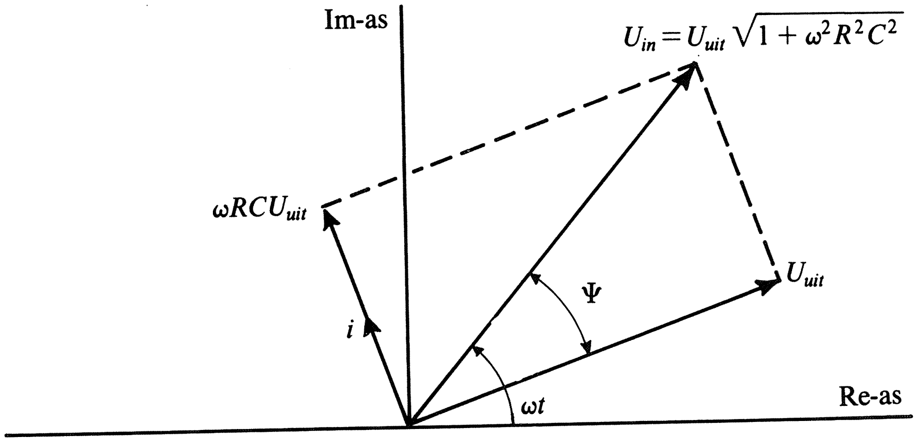
Weerstand: $U = RI$, spanning en stroom zijn in fase,

Spoel: $U = j\omega LI = \omega LIe^{j\frac{\pi}{2}}$, spanning is $\frac{\pi}{2}$ voor op de stroom,

Condensator: $U = \frac{I}{j\omega C} = \frac{I}{\omega C} e^{-j\frac{\pi}{2}}$, spanning ijlt $\frac{\pi}{2}$ na op de stroom

De spanningswet van Kirchoff is nu een vectorrelatie: de vectoriële optelling van de spanningen in een gesloten circuit is nul. Soms dient ook de stroomwet van Kirchoff toegepast te worden: de vectoriële optelling van de stromen in een knooppunt van het netwerk is nul. Toepassing van bovenstaande wetten en fasenrelaties leidt dan tot een diagram, ook wel het wijzerdiagram genoemd, waarmee langs meetkundige weg de verschillende amplitude-verhoudingen en fasehoeken berekend kunnen worden.

De faserelaties hebben echter een relatief karakter; de absolute status wordt verkregen doordat de faserelatie van de bron bekend is. De fasehoek van de bron is namelijk ωt (ω is het aantal radialen per seconde). Voor ons RC-netwerk krijgen we met toepassing van de spanningswet van Kirchoff en de spannings-stroom faserelatie van de weerstand en de condensator het volgende diagram



FIGUUR 3

We zien dat ωt lineair met de tijd toeneemt, met als gevolg dat het de totale figuur rondwentelt in het complexe vlak als functie van t en ω. De terugtransformatie naar het reële domein komt nu neer op de horizontale projectie van de stroom- en spanningsvectoren. Het resultaat van deze projectie wordt de momentele waarde genoemd.

8. EEN TOEPASSING VAN HET SUPERPOSITIEBEGINSEL

Laten we eens aannemen dat de bronfunctie van ons RC-netwerk geen harmonisch signaal is, maar wel periodiek in de tijd met periode T. Noem de bronfunctie $f = f(t)$ dan geldt

$$f(t) = f(t + T).$$

Een dergelijke functie kan worden gepresenteerd door een oneindig voortlopende reeks van Fourier.

$$f(t) = \sum_{n=0}^{\infty} f_n,$$

met

$$f_n = a_n \cos(\omega_n t) + b_n \sin(\omega_n t),$$

en

$$\omega_n = n\frac{2\pi}{T};$$

a_n en b_n noemt men de Fouriercoëfficënten. Nu hebben we weer harmonische functies en als we eisen dat $u_{uit}(0)=0$ dan kunnen we het superpositiebeginsel toepassen. We kunnen dan voor elke n de particuliere oplossing bepalen en de constante van de homogene oplossing.

Voor een bepaalde n is namelijk de complexe waarde F_n van f_n

$$F_n = a_n + b_n e^{-j\frac{\pi}{2}} = a_n - jb_n,$$

zodat de complexe particuliere oplossing van een bepaalde n gegeven wordt door

$$U_{p,n} = \frac{(a_n - jb_n)}{(1 + j\omega_n RC)} = \frac{(a_n - b_n\omega_n RC) - j(b_n + a_n\omega_n RC)}{(1 + \omega_n^2 R^2 C^2)}$$

zodat tenslotte de totale oplossing van de gedaante is

$$u_{uit}(t) = \sum_{n=0}^{\infty} B_n \cos(\omega_n t - \Psi_n) - e^{-t/RC} \sum_{n=0}^{\infty} B_n \cos(\Psi_n),$$

$$\text{met } B_n = \sqrt{\frac{a_n^2 + b_n^2}{1 + \omega_n^2 R^2 C^2}}, \text{ en } \Psi_n = \arctan\left(\frac{a_n\omega_n RC + b_n}{a_n - b_n\omega_n RC}\right).$$

Hebben we te maken met een bronfunctie die willekeurig in de tijd verandert, dan kunnen we via de Fourieranalyse onder bepaalde omstandigheden de functie ontwikkelen in een continu spectrum van harmonische functies en weer het superpositiebeginsel toepassen. We zijn dan tenslotte aangeland bij de harmonische analyse, maar laten we dat onderwerp voor een andere keer bewaren.

LITERATUUR

W.E. BOYCE, R.C. DIPRIMA (1977). *Elementary Differential Equations,* Joh. Wiley & Sons Inc., New York etc.

H.J. BUTTERWECK (1974). *Elektrische Netwerken,* Spectrum, Utrecht/Antwerpen.

Reëel, Complex, Quaternionen,
komt er nooit een eind aan?

F. van der Blij
Rijksuniversiteit Utrecht
Postbus 80010, 3508 TA Utrecht

1. Getalparen

Eén van de meest voor de hand liggende manieren om de complexe getallen, uitgaande van de reële getallen, te construeren is de vorming van paren reële getallen (a,b) door deze paren als vectoren op te tellen en een distributieve vermenigvuldiging te definiëren door

$$(a,0)\cdot(p,0) = (ap,0)$$
$$(0,b)\cdot(p,0) = (0,bp)$$
$$(a,0)\cdot(0,q) = (0,aq)$$
$$(0,b)\cdot(0,q) = (-bq,0).$$

Deze vermenigvuldiging is commutatief, heeft een eenheidselement en met wat werk is te controleren dat de vermenigvuldiging ook associatief is. Omdat

$$(a,b)\cdot(a,-b) = (a^2+b^2,0)$$

en dus

$$(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right) = (1,0),$$

heeft ieder paar (a,b) waarvoor $a^2+b^2 \neq 0$ een inverse. Over de reële getallen geldt $a^2+b^2 = 0$ impliceert $a=b=0$. Dus alle paren ongelijk $(0,0)$ hebben een inverse. De paren vormen een lichaam, het lichaam van de complexe getallen. Van de reële getallen gebruikten we alleen de eigenschap dat zij een lichaam vormen waarin de som van twee kwadraten alleen 0 is als beide kwadraten 0 zijn.

Wanneer we de constructie herhalen met nu de complexe getallen als begin lichaam, vormen de paren (α,β) wel een ring, maar met nuldelers; er zijn immers dan $\alpha \neq 0$, $\beta \neq 0$ te vinden met $\alpha^2+\beta^2=0$ en deze zijn nuldelers en hebben dus geen inverse.

De complexe getallen hebben enkele typische eigenschappen. In het lichaam van de complexe getallen is een involutie, een automorfisme van de orde 2. Het is de complexe conjugatie, voor de paren de afbeelding $(a,b) \mapsto (a,-b)$. We schrijven deze voor $\alpha \in \mathbb{C}$ als $\alpha \mapsto \overline{\alpha}$. We merken op $\overline{\overline{\alpha}}=\alpha$, $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$ en $\overline{\alpha\beta}=\overline{\alpha}\cdot\overline{\beta}$. Als $\alpha=\overline{\alpha}$ geldt $\alpha \in \mathbb{R}$.

We merken nog op dat

$$\alpha+\overline{\alpha} \in \mathbb{R} \text{ en } \alpha\overline{\alpha} \in \mathbb{R}.$$

Bijgevolg voldoet ieder complex getal α aan een vierkantsvergelijking met reële coëfficiënten, namelijk

$$\alpha^2-(\alpha+\overline{\alpha})\alpha+(\alpha\overline{\alpha})=0.$$

Tenslotte bezitten de complexe getallen een kwadratische, multiplicatieve norm $N(\alpha)=\alpha\overline{\alpha}$

$$N(k\alpha)=k^2N(\alpha), \quad k \in \mathbb{R}, \ \alpha \in \mathbb{C}.$$

$$N(\alpha\beta)=N(\alpha)\cdot N(\beta), \quad \alpha,\beta \in \mathbb{C}.$$

In de volgende paragraaf zullen we verdere stappen pogen te zetten op de weg reëel, complex en ons daarbij steeds de vraag stellen of een nieuw geconstrueerd systeem een lichaam is, een involutie bezit, de elementen voldoen aan een v.k.v. met coëfficiënten in een 'eenvoudiger' lichaam, een multiplicatieve, kwadratische norm bezit.

2. Twee bij twee matrices

We kunnen de complexe getallen ook invoeren als 2×2 matrices over de reële getallen. De matrices

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

hebben de eigenschap dat zowel de som als het produkt van twee matrices van dit speciale type, weer van hetzelfde type is. Alle matrices met $a,b \in \mathbb{R}$ vormen een ring. De determinant van deze matrices is a^2+b^2. Alle matrices, behalve de nulmatrix, hebben een inverse. Matrixoptelling correspondeert met vectoroptelling van de paren (a,b). Matrixvermenigvuldiging

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} p & q \\ -q & p \end{bmatrix} = \begin{bmatrix} ap-bq & aq+bp \\ -aq-bp & ap-bq \end{bmatrix}$$

correspondeert met de in paragraaf 1 ingevoerde vermenigvuldiging van paren. Deze verzameling 2×2 matrices vormt een lichaam, het lichaam van de complexe getallen. De involutie is eenvoudig: spiegelen van de matrix in de hoofddiagonaal, de kwadratische norm is de determinant van de matrix; de stelling van Cayley-Hamilton, dat iedere matrix voldoet aan zijn karakteristieke vergelijking det $(A-\lambda I)$ = Pol $(\lambda)=0$ geeft hier de vierkantsvergelijking:

$$A^2-(\text{ spoor } A)\cdot A+(\det A)=0.$$

Proberen we nu 2×2 complexe matrices, dan vinden we weer een involutie, een kwadratische norm, de vierkantsvergelijking, maar er treden weer nuldelers op. We merken nog even op dat we bij invoering van het nieuwe systeem als 2×2 matrices nu de associatieve wet, die immers voor matrixvermenigvuldiging geldt om niet krijgen!

3. HOE HET LUKT

Een kleine variant van paragraaf 2 voert tot een systeem dat wel de eigenschap heeft dat ieder element ongelijk 0 een inverse heeft. We verspelen echter de commutativiteit van de vermenigvuldiging; de associativiteit en het bestaan van een eenheidselement blijven behouden. Het idee is nu voor ons eenvoudig en voor de hand liggend. In de historische ontwikkeling heeft het Hamilton meer moeite gekost.

In plaats van de 'pseudo-orthogonale' matrices

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \quad \alpha,\beta\in\mathbb{C}$$

bestuderen we de 'pseudo-unitaire' matrices

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \quad \alpha,\beta\in\mathbb{C}$$

Dit stelsel is weer gesloten onder optelling en matrixvermenigvuldiging. De determinant is $\alpha\overline{\alpha}+\beta\overline{\beta}$, dus hebben alle matrices ongelijk aan het nulelement een inverse. We schrijven de vermenigvuldiging nog even uit:

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \begin{bmatrix} \rho & \sigma \\ -\overline{\sigma} & \overline{\rho} \end{bmatrix} = \begin{bmatrix} \alpha\rho-\beta\overline{\sigma} & \alpha\sigma+\beta\overline{\rho} \\ -\overline{\beta}\rho-\overline{\alpha}\,\overline{\sigma} & \overline{\alpha}\,\overline{\rho}-\overline{\beta}\sigma \end{bmatrix}$$

In de notatie van paren complexe getallen (α,β) is de vermenigvuldiging dus

$$(\alpha,\beta)\cdot(\rho,\sigma)=(\alpha\rho-\beta\overline{\sigma},\alpha\sigma+\beta\overline{\rho}). \qquad (*)$$

Omdat de vermenigvuldiging afgeleid is uit matrixvermenigvuldiging is deze associatief. De formule laat duidelijk zien dat de vermenigvuldiging niet commutatief is.

De bewerking spiegelen *en* complex geconjugeerde nemen is nu de involutie, weliswaar een anti-automorfisme voor de vermenigvuldiging: $\overline{PQ}=\overline{Q}\cdot\overline{P}$, in matrixvorm is de involutie

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \mapsto \begin{bmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{bmatrix}.$$

De determinant is weer de kwadratische, multiplicatieve norm. De elementen voldoen aan een vierkantsvergelijking met zelfs reële coëfficiënten:

$$\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}^2 - (\alpha+\bar{\alpha}) \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} + (\alpha\bar{\alpha}+\beta\bar{\beta}) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Het zo geconstrueerde scheve lichaam zijn de quaternionen van Hamilton.

We kunnen de quaternionen dus opvatten als paren complexe getallen (met (*) als vermenigvuldigregel) of als pseudo-unitaire 2×2 matrices. We kunnen ze ook opvatten als een vierdimensionale lineaire ruimte over $\mathbb{R}$. Schrijven we $\alpha=a+bi$, $\beta=c+di$, dan geldt

$$\begin{aligned} \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} &= a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \\ &= a.1 + bI + cJ + dK. \end{aligned}$$

We kunnen de quaternionen invoeren als viertallen reële getallen met vectoroptelling en een distributieve vermenigvuldiging, gedefinieerd door

$$I^2=J^2=K^2=-1, \quad I.J=-J.I=K,$$
$$J.K=-K.J=I, \quad K.I=-I.K=J.$$

De involutie wordt gegeven door

$$a+bI+cJ+dK \mapsto a-bI-cJ-dK;$$

de kwadratische, multiplicatieve norm door

$$a+bI+cJ+dK \mapsto a^2+b^2+c^2+d^2.$$

De vierkantsvergelijking tenslotte door:

$$(a+bI+cJ+dK)^2 - 2a(a+bI+cJ+dK)+a^2+b^2+c^2+d^2=0.$$

Behalve door complex 'pseudo-unitaire' matrices kunnen we de quaternionen ook representeren door reële 'pseudo-orthogonale' 4×4 matrices.

$$(a+bI+cJ+dK) \mapsto \begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}.$$

De quaternionenvermenigvuldiging correspondeert met de matrixvermenigvuldiging. De involutie (geconjugeerde nemen) correspondeert met het spiegelen van de matrix. De determinant van de matrix is nu het kwadraat van de multiplicatieve, kwadratische norm, namelijk $(a^2+b^2+c^2+d^2)^2$.

4. OOK QUATERNIONEN ZIJN NUTTIG

De quaternionen zijn ingevoerd om bewegingen, rotaties in de ruimte algebraïsch te beschrijven. Het beschrijven van rotaties in het vlak door middel van complexe getallen maakt het verlangen duidelijk.

We kiezen een moderne methode om het verband tussen quaternionen en draaiingen in de $\mathbb{R}^3$ duidelijk te maken. We gebruiken de representatie van quaternionen door 'pseudo-unitaire' complexe 2×2 matrices.

Bovendien voegen we aan 'pseudo-unitaire' matrices met spoor 0, dus matrices

$$\begin{bmatrix} iy & z+it \\ -z+it & -iy \end{bmatrix} = yI + zJ + tK,$$

een vector in de $\mathbb{R}^3$ toe door

$$\begin{bmatrix} iy & z+it \\ -z+it & -iy \end{bmatrix} \mapsto (y,z,t)\,.$$

Onder transformaties $A \mapsto U^{-1}AU$ gaan matrices met spoor 0 in matrices met spoor 0 over. Laat nu aan de vector (y,z,t) de matrix

$$A = \begin{bmatrix} iy & z+it \\ -z+it & -iy \end{bmatrix}$$

toegevoegd worden. Laat U een willekeurige 'pseudo-unitaire' 2×2 matrix zijn.

Dan wordt aan

$$A' = U^{-1}AU$$

een vector (y',z',t') toegevoegd.

Omdat $\det A = y^2+z^2+t^2$ geldt

$$y'^2+z'^2+t'^2 = \det A' = \det A = y^2+z^2+t^2.$$

De transformatie

$$(y,z,t) \mapsto (y',z',t'),$$

waarvan men zonder moeite inziet dat hij lineair is, behoudt de lengte van de vectoren. Het is dus een orthogonale transformatie van de $\mathbb{R}^3$. Uit de definitie volgt dat samenstellen van orthogonale transformaties in de $\mathbb{R}^3$ correspondeert met de quaternionenvermenigvuldiging.

We gaan op verdere details hier niet in, maar merken op dat met het quaternion

$$\cos\frac{\phi}{2} + y\sin\frac{\phi}{2}I + z\sin\frac{\phi}{2}J + t\sin\frac{\phi}{2}K$$

een rotatie over een hoek ϕ om de as door de oorsprong en (y,z,t) voorgesteld wordt.

De klassieke boeken over quaternionen geven veel toepassingen van de quaternionen in de stereometrie. De 'wonderen' van de complexe getallen laten zich niet zo direct vertalen naar de quaternionen. Algebraïsche vergelijkingen in een *scheef* lichaam zijn niet zo eenvoudig te behandelen. De pogingen om een functietheorie voor functies van een quaternionenvariabele in te voeren, geven resultaten in de richting dat differentieerbaarheid hier een nog sterkere eis is dan in het complexe geval. Er is een verband tussen oplossingen van bepaalde partiële differentiaalvergelijkingen, afgeleid uit een generalisatie van de Cauchy-Riemann-vergelijkingen en differentieerbare quaternionenfuncties.

5. En hoe verder?

We zijn geneigd om voor twee quaternionen P en Q de 2×2 matrix

$$\begin{bmatrix} P & Q \\ -\overline{Q} & \overline{P} \end{bmatrix}$$

te bezien.

Maar helaas, het produkt van twee zulke 'pseudo-unitaire quaternionen' matrices is niet meer van deze zelfde vorm. Bovendien zijn er moeilijkheden om de determinant van een matrix met elementen in een niet-commutatief lichaam te definiëren! Zo gaat het niet. We zouden gewoon paren quaternionen, optellen als vectoren en vermenigvuldigen door

$$(A,B)\cdot(P,Q)=(AP-B\overline{Q},\ AQ+B\overline{P})$$

kunnen proberen, maar ook deze poging loopt vast. We vinden geen inverse en geen goede kwadratische multiplicatieve norm.

Toch bestaat er een vermenigvuldiging van quaternionenparen die ons verder helpt. We moeten dan de produktdefinitie een beetje veranderen:

$$(A,B)\cdot(P,Q)=(AP-\overline{Q}B,\ QA+B\overline{P}).$$

Nu geldt

$$(A,B)\cdot(\overline{A},-B)=(A\overline{A}+B\overline{B},0).$$

Nu ligt $A\overline{A}+\overline{B}B$ voor ieder quaternionenpaar (A,B) in de reële getallen. Dus vinden we de inverse

$$(A,B)\cdot\left(\frac{\overline{A}}{A\overline{A}+\overline{B}B},\frac{B}{A\overline{A}+\overline{B}B}\right) = (1,0),$$

voor ieder paar (A,B) met $A\overline{A}+\overline{B}B\neq 0$, dat is voor ieder paar ongelijk $(0,0)$. Het is duidelijk dat de inverse zowel rechts- als linksinverse is. De conjugatie wordt gegeven door

$$(P,Q) \mapsto (\overline{P},-Q),$$

de multiplicatieve norm door

$$(P,Q) \mapsto P\overline{P}+Q\overline{Q}\ .$$

Het is niet geheel triviaal dat deze multiplicatief is. We zouden direct kunnen berekenen:

$$(AP-\overline{Q}B)\cdot\overline{(AP-\overline{Q}B)}+(QA+B\overline{P})\cdot\overline{(QA+B\overline{P})}\,.$$

Na wat handig manipuleren komt er inderdaad

$$(A\overline{A}+B\overline{B})\cdot(P\overline{P}+Q\overline{Q})$$

uit.

We zouden sneller kunnen werken door

$$((A,B)\cdot(P,Q))\cdot\overline{((A,B)\cdot(P,Q))}\ =((A,B)\cdot(P,Q))\cdot(\overline{(P,Q)}\cdot\overline{(A,B)}).$$

Maar om verder te komen hebben we associativiteit nodig. En die controleerden we nog niet! Zou de wet gelden, dan konden we verder.

$$(A,B)\{(P,Q)\cdot\overline{(P,Q)}\}\overline{(A,B)}=\{(A,B)\cdot\overline{(A,B)}\}\cdot\{(P,Q)\cdot\overline{(P,Q)}\}$$

omdat $(P,Q)\cdot\overline{(P,Q)}$ een reëel getal is.

Helaas is de associatieve wet niet algemeen geldig bij de boven ingevoerde vermenigvuldiging van quaternionenparen! We geven één tegenvoorbeeld.

$$\{(0,I)\cdot(0,J)\}\cdot(0,K)\ =\ (-\overline{J}I,0)\cdot(0,K)\ =\ (0,1).$$

$$(0,I)\cdot\{(0,J)\cdot(0,K)\}\ =\ (0,I)\cdot(-\overline{K}J,0)\ =\ (0,-1).$$

We construeerden dus een niet-associatief, niet-commutatief lichaam, met een involutie, een kwadratische multiplicatieve norm. Terwijl ook de elementen nog voldoen aan een v.k.v. met reële coëfficiënten. Dit systeem wordt de Cayley-Dickson-algebra van de octaven genoemd.

Er geldt wel in dit systeem een zwakke vorm van associativiteit. Ieder door twee elementen voortgebrachte deelalgebra is associatief. Als a,b en c octaven zijn, is de associator $(ab)c-a(bc)$ een alternerende functie van het tripel (a,b,c) d.w.z. bij toepassing van oneven permutaties keert het teken van de associator om. Uit deze regels is af te leiden dat $(ab)(\overline{b}\overline{a})=a(b\overline{b})\overline{a}$ zodat het foutieve bewijs van de multiplicativiteit van de norm achteraf toch nog goed is.

Zijn de octaven nuttig? Zeker voor bepaalde meetkundige verschijnselen in de 7-dimensionale ruimte. Er is zelfs een meetkundige generalisatie van dualiteit, namelijk trialiteit mee te construeren. Over differentieerbare octavenfuncties praten we maar niet. Wel zijn octaven erg nuttig bij de bestudering van exceptionele Liegroepen, van G_2 tot en met E_8.

6. En hoe verder?

We gaan nu natuurlijk zoeken naar paren octaven en daar een vermenigvuldiging voor definiëren.

Op onze weg komen we direct al een waarschuwing tegen. De kwadratische multiplicatieve norm komt neer op een identiteit

$$(\sum_{i=1}^{n}x_i^2)\cdot(\sum_{i=1}^{n}y_i^2)=\sum_{i=1}^{n}z_i^2,$$

waarbij de z_i zowel lineair in de x_i als in de y_i zijn, bijv.

$$(x_1^2+x_2^2)(y_1^2+y_2^2)=(x_1y_1-x_2y_2)^2+(x_1y_2+x_2y_1)^2\,.$$

De quaternionen en de octaven geven zulke identiteiten voor $n=4$ en 8. Zou er ook één voor $n=16$ bestaan? Wanneer we na de octaven verder konden komen, zouden we er op stuiten! Hoewel er in de geschiedenis verschillende van zulke 16-dimensionale identiteiten gepubliceerd zijn, waren alle voorbeelden fout. In 1898 bewees Hurwitz dat voor 16 zo'n identiteit niet bestaat. Zulke identiteiten bestaan alleen voor $n=1,2,4,8$. Een rand-opmerking voor fijnproevers: Een topologische delingsalgebra, locaal compact en samenhangend is òf de reële getallen, òf de complexe getallen òf de quaternionen, òf de octaven!

Op allerlei manieren krijgen we de indruk dat we met de octaven een eindpunt van de rij 1,2,4,8 bereikt hebben.

7. De 'alternatieve' weg

We gebruiken hier alternatief in de moderne sociaal-wetenschappelijke, eventueel politicologische betekenis; niet in de wiskundige betekenis, alternatief als generalisatie van associatief.

De 'alternatieve' complexe getallen zijn in te voeren als $a+b\epsilon$ met $\epsilon^2=1$. Dit systeem heeft nuldelers. Maar er is conjugatie $a+b\epsilon \mapsto a-b\epsilon$. Er is een multiplicatieve kwadratische norm $a+b\epsilon \mapsto (a^2-b^2)$ en ieder element voldoet aan een vierkantsvergelijking. We noemen deze getallen ook wel split-complexe getallen. Zijn er ook splitquaternionen? De algebra van de viertallen (a,b,c,d) met

$$a1+bI_0+cJ_0+dK_0 \quad en$$

$$I_0^2=J_0^2=-K_0^2=1 \qquad \begin{array}{l} I_0J_0=-J_0I_0=K_0 \\ J_0K_0=-K_0J_0=-I_0 \\ K_0I_0=-I_0K_0=-J_0 \end{array}$$

is het systeem van de splitquaternionen met normvorm $(a,b,c,d) \mapsto a^2-b^2-c^2+d^2$.

Deze splitquaternionen zijn ook eenvoudig te beschrijven als gewone 2×2 matrices over de reële getallen, waarbij de determinant weer de kwadratische multiplicatieve normvorm is. We moeten dan als volgt afbeelden

$$(a+bI_0+cJ_0+dK_0) \mapsto \begin{pmatrix} a+b & c+d \\ c-d & a-b \end{pmatrix}.$$

Natuurlijk, u begrijpt het al, zijn er ook splitoctaven met een normvorm die de gedaante

$$x_1^2+x_2^2+x_3^2+x_4^2-x_5^2-x_6^2-x_7^2-x_8^2$$

heeft. Voor deze niet-associatieve algebra bestaat een voorstelling in de vorm van een soort gegeneraliseerde matrices. Natuurlijk zo gegeneraliseerd dat de associativiteit verloren is gegaan.

MC SYLLABI

1.1 F. Göbel, J. van de Lune. *Leergang besliskunde, deel 1: wiskundige basiskennis.* 1965.

1.2 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 2: kansberekening.* 1965.

1.3 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 3: statistiek.* 1966.

1.4 G. de Leve, W. Molenaar. *Leergang besliskunde, deel 4: Markovketens en wachttijden.* 1966.

1.5 J. Kriens, G. de Leve. *Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde.* 1966.

1.6a B. Dorhout, J. Kriens. *Leergang besliskunde, deel 6a: wiskundige programmering 1.* 1968.

1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. *Leergang besliskunde, deel 6b: wiskundige programmering 2.* 1977.

1.7a G. de Leve. *Leergang besliskunde, deel 7a: dynamische programmering 1.* 1968.

1.7b G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7b: dynamische programmering 2.* 1970.

1.7c G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7c: dynamische programmering 3.* 1971.

1.8 J. Kriens, F. Göbel, W. Molenaar. *Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie.* 1968.

2.1 G.J.R. Förch, P.J. van der Houwen, R.P. van de Riet. *Colloquium stabiliteit van differentieschema's, deel 1.* 1967.

2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. *Colloquium stabiliteit van differentieschema's, deel 2.* 1968.

3.1 H.A. Lauwerier. *Randwaardeproblemen, deel 1.* 1967.

3.2 H.A. Lauwerier. *Randwaardeproblemen, deel 2.* 1968.

3.3 H.A. Lauwerier. *Randwaardeproblemen, deel 3.* 1968.

4 H.A. Lauwerier. *Representaties van groepen.* 1968.

5 J.H. van Lint, J.J. Seidel, P.C. Baayen. *Colloquium discrete wiskunde.* 1968.

6 K.K. Koksma. *Cursus ALGOL 60.* 1969.

7.1 *Colloquium moderne rekenmachines, deel 1.* 1969.

7.2 *Colloquium moderne rekenmachines, deel 2.* 1969.

8 H. Bavinck, J. Grasman. *Relaxatietrillingen.* 1969.

9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. *Colloquium elliptische differentiaalvergelijkingen, deel 1.* 1970.

9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, E.M. de Jager, N.M. Temme, R.J. de Vogelaere. *Colloquium elliptische differentiaalvergelijkingen, deel 2.* 1970.

10 J. Fabius, W.R. van Zwet. *Grondbegrippen van de waarschijnlijkheidsrekening.* 1970.

11 H. Bart, M.A. Kaashoek. H.G.J. Pijls, W.J. de Schipper, J. de Vries. *Colloquium halfalgebra's en positieve operatoren.* 1971.

12 T.J. Dekker. *Numerieke algebra.* 1971.

13 F.E.J. Kruseman Aretz. *Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8.* 1971.

14 H. Bavinck, W. Gautschi, G.M. Willems. *Colloquium approximatietheorie.* 1971.

15.1 T.J. Dekker, P.W. Hemker, P.J. van der Houwen. *Colloquium stijve differentiaalvergelijkingen, deel 1.* 1972.

15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. *Colloquium stijve differentiaalvergelijkingen, deel 2.* 1973.

15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. *Colloquium stijve differentiaalvergelijkingen, deel 3.* 1975.

16.1 L. Geurts. *Cursus programmeren, deel 1: de elementen van het programmeren.* 1973.

16.2 L. Geurts. *Cursus programmeren, deel 2: de programmeertaal ALGOL 60.* 1973.

17.1 P.S. Stobbe. *Lineaire algebra, deel 1.* 1973.

17.2 P.S. Stobbe. *Lineaire algebra, deel 2.* 1973.

17.3 N.M. Temme. *Lineaire algebra, deel 3.* 1976.

18 F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. *Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971.* 1973.

19 A. Hordijk, R. Potharst, J.Th. Runnenburg. *Optimaal stoppen van Markovketens.* 1973.

20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E. Slagt. *ALGOL 60 procedures voor begin- en randwaardeproblemen.* 1976.

21 J.W. de Bakker (red.). *Colloquium programmacorrectheid.* 1975.

22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. *Asymptotische methoden in de toetsingstheorie; toepassingen van naburigheid.* 1976.

23.1 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 1.* 1976.

23.2 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 2.* 1977.

24.1 P.J. van der Houwen. *Numerieke integratie van differentiaalvergelijkingen, deel 1: eenstapsmethoden.* 1974.

25 *Colloquium structuur van programmeertalen.* 1976.

26.1 N.M. Temme (ed.). *Nonlinear analysis, volume 1.* 1976.

26.2 N.M. Temme (ed.). *Nonlinear analysis, volume 2.* 1976.

27 M. Bakker, P.W. Hemker, P.J. van der Houwen, S.J. Polak, M. van Veldhuizen. *Colloquium discretiseringsmethoden.* 1976.

28 O. Diekmann, N.M. Temme (eds.). *Nonlinear diffusion problems.* 1976.

29.1 J.C.P. Bus (red.). *Colloquium numerieke programmatuur, deel 1A, deel 1B.* 1976.

29.2 H.J.J. te Riele (red.). *Colloquium numerieke programmatuur, deel 2.* 1977.

30 J. Heering, P. Klint (red.). *Colloquium programmeeromgevingen.* 1983.

31 J.H. van Lint (red.). *Inleiding in de coderingstheorie.* 1976.

32 L. Geurts (red.). *Colloquium bedrijfsystemen.* 1976.

33 P.J. van der Houwen. *Berekening van waterstanden in zeeën en rivieren.* 1977.

34 J. Hemelrijk. *Oriënterende cursus mathematische statistiek.* 1977.

35 P.J.W. ten Hagen (red.). *Colloquium computer graphics.* 1978.

36 J.M. Aarts, J. de Vries. *Colloquium topologische dynamische systemen.* 1977.

37 J.C. van Vliet (red.). *Colloquium capita datastructuren.* 1978.

38.1 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part I.* 1979.

38.2 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part II.* 1979.

39 O.J. Vrieze, G.L. Wanrooy. *Colloquium stochastische spelen.* 1978.

40 J. van Tiel. *Convexe analyse.* 1979.

41 H.J.J. te Riele (ed.). *Colloquium numerical treatment of integral equations.* 1979.

42 J.C. van Vliet (red.). *Colloquium capita implementatie van programmeertalen.* 1980.

43 A.M. Cohen, H.A. Wilbrink. *Eindige groepen (een inleidende cursus).* 1980.

44 J.G. Verwer (ed.). *Colloquium numerical solution of partial differential equations.* 1980.

45 P. Klint (red.). *Colloquium hogere programmeertalen en computerarchitectuur.* 1980.

46.1 P.M.G. Apers (red.). *Colloquium databankorganisatie, deel 1.* 1981.

46.2 P.G.M. Apers (red.). *Colloquium databankorganisatie, deel 2.* 1981.

47.1 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60: general information and indices.* 1981.

47.2 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 1: elementary procedures; vol. 2: algebraic evaluations.* 1981.

47.3 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra, part I.* 1981.

47.4 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3B: linear algebra, part II.* 1981.

47.5 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems, part I.* 1981.

47.6 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 5B: analytical problems, part II.* 1981.

47.7 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation.* 1981.

48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 1.* 1982.

48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 2.* 1982.

49 T.H. Koornwinder (ed.). *The structure of real semisimple Lie groups.* 1982.

50 H. Nijmeijer. *Inleiding systeemtheorie.* 1982.

51 P.J. Hoogendoorn (red.). *Cursus cryptografie.* 1983.

CWI SYLLABI

1 Vacantiecursus 1984: *Hewet - plus wiskunde.* 1984.

2 E.M. de Jager, H.G.J. Pijls (eds.). *Proceedings Seminar 1981-1982. Mathematical structures in field theories.* 1984.

3 W.C.M. Kallenberg, et al. *Testing statistical hypotheses: worked solutions.* 1984.

4 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 1.* 1984.

5 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 2.* 1984.

6 P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls, J.W. de Roever. *Proceedings Seminar 1982-1983. Mathematical structures in field theories.* 1985.

7 Vacantiecursus 1985: *Variatierekening.* 1985.

8 G.M. Tuynman. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.1 Geometric quantization.* 1985.

9 J. van Leeuwen, J.K. Lenstra (eds.). *Parallel computers and computations.* 1985.

10 Vacantiecursus 1986: *Matrices.* 1986.

11 P.W.H. Lemmens. *Discrete wiskunde: tellen, grafen, spelen en codes.* 1986.

12 J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener.* 1986.

13 G.M. Tuynman, M.J. Bergvelt, A.P.E. ten Kroode. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.2.* 1987.

14 Vacantiecursus 1987: *De personal computer en de wiskunde op school.* 1987.

15 Vacantiecursus 1983: *Complexe getallen.* 1987.