

Algebraïsche vergelijkingen en Galois-theorie, een historisch overzicht*

DR H. J. M. BOS

0. Evariste Galois (1811-1832) loste in de jaren 1827-1830 een centraal probleem in de algebra op, namelijk het probleem welke algebraïsche vergelijkingen oplosbaar zijn. De naam Galois is in de moderne wiskunde verbonden aan een theorie die de structuur van lichamen beschrijft in termen van de structuur van de automorfismen-groepen van die lichamen.

Hoewel deze twee onderwerpen, oplossing van vergelijkingen en structuur van lichamen, op het eerste gezicht zeer verschillend lijken, is de huidige *Galois-theorie* op natuurlijke en begrijpelijke wijze ontstaan uit het onderzoek van vergelijkingen.

In dit historisch overzicht zal die ontwikkeling in grote lijnen worden geschetst.

1. De oplossing van tweede-, derde- en vierdegraadsvergelijkingen

Methoden ter oplossing van tweedegraadsvergelijkingen werden al in de Oudheid (Babylonische en Griekse wiskunde) ontwikkeld. Bij deze methoden werden de coëfficiënten en de wortels steeds positief aangenomen, hetgeen ertoe leidde dat er geen algemene methode voor alle tweedegraadsvergelijkingen werd gevonden; $x^2 + mx = n$ en $x^2 = mx + n$ bijvoorbeeld vergden verschillende methoden, daar beide vergelijkingen niet tot een gemeenschappelijke vorm konden worden gereduceerd.

De Grieken behandelden kwadratische vergelijkingen in een meetkundige context; zij vatten de onbekende op als een lijnstuk, zijn kwadraat als een vierkant en de coëfficiënten als lijnstukken resp. oppervlakken. In de Babylonische wiskunde werden onbekenden en coëfficiënten als getallen opgevat.

Ziet men af van de genoemde verschillen (meetkundige behandeling,

*) Dit is de uitgewerkte versie van een lezing gehouden tijdens de Vakantiecursus 1974 'Algebraïsche vergelijkingen', georganiseerd door het Mathematisch Centrum. De tekst is eerder, in kleine op-laat, verschenen in de syllabus van die cursus (MC VC 28/74 aug.).

beperking tot positieve grootheden), dan waren de methoden equivalent met de bekende formule voor de oplossing van

$$ax^2 + bx + c = 0, \quad (1)$$

namelijk

$$x = \{-b \pm \sqrt{(b^2 - 4ac)}\} / 2a \quad (2)$$

Algemene oplossingen van derde- en vierdegraadsvergelijkingen zijn van veel recenter datum; zij stammen uit de eerste helft van de zestiende eeuw, uit de periode van de Renaissance. Zij vormden een van de eerste verworvenheden van de wiskunde in west-Europa die uitstegen boven wat de Oudheid op wiskundig gebied had gepresteerd.

De ontdekkingsgeschiedenis van deze oplossingen is zeer gecompliceerd. Scipione del Ferro (1465?-1526) vond omstreeks 1500 een oplossingsmethode voor een bepaalde vorm van derdegraadsvergelijkingen. Hij publiceerde de methode niet, maar deelde haar mee aan vrienden. Een van deze vrienden daagde later, in 1535, Niccolo Tartaglia (1500?-1557) in het openbaar uit een serie derdegraadsvergelijkingen op te lossen. Tartaglia slaagde daarin, gaf de oplossingen, maar hield zijn methode geheim. Enige jaren later deelde hij de methode mee aan Geronimo Cardano (1501-1576) die geheimhouding beloofde. Cardano vernam daarna, van del Ferro's vrienden, tevens del Ferro's methode. Hij bemerkte dat beide methoden gelijk waren en publiceerde ze in 1545, waarbij hij del Ferro en Tartaglia als onafhankelijke ontdekkers noemde. Intussen had een vriend van Cardano, Ludovico Ferrari (1522-1565), geïnspireerd door Tartaglia's en del Ferro's methoden, een oplossingsmethode voor vierdegraadsvergelijkingen gevonden; deze methode werd ook door Cardano in 1545 gepubliceerd.

Er ontstonden daarna hooglopende ruzies over prioriteit en schending van geheimhoudingsbeloften. De hevigheid van de ruzies is begrijpelijk omdat voor wiskundigen als Tartaglia de financiële positie sterk afhing van zijn reputatie. Het winnen van een uitdaging, zoals in het geval van Tartaglia gedaan, was dus een zaak van direct eigenbelang en het was wijze voorzorg methoden niet aan mogelijke rivalen te verraden.

De zestiende-eeuwse algebraïci werkten in het algemeen met posi-

tieve grootheden, hoewel af en toe negatieve en zelfs complexe grootheden in hun werk voorkwamen. Het heeft nog tenminste twee eeuwen geduurd voordat deze grootheden algemeen in de wiskundige praktijk werden aanvaard. Hiermee hangt samen dat de hoofdstelling van de algebra - elke n -degraadsvergelijking heeft n wortels - eerst laat kon worden geformuleerd en bewezen. Men vindt een formulering bij Albert Girard (1595-1632). Leonhard Euler (1707-1783) formuleert in 1743 het vermoeden dat elke vergelijking met reële coëfficiënten kan worden ontbonden in lineaire en kwadratische factoren. Jean Le Rond d'Alembert (1717-1783) poogt de hoofdstelling te bewijzen (1746). Carl Friedrich Gauss (1777-1855) levert tenslotte (1799) het definitieve bewijs.

Intussen was, door het werk van François Viète (1540-1603) en René Descartes (1596-1650), het gebruik van onbepaalde coëfficiënten (letters) in de vergelijkingsleer ingevoerd. Hierdoor werd het mogelijk algemene oplossingsmethoden in formules op te schrijven; voordien konden methoden alleen als recept worden omschreven en door voorbeelden worden verduidelijkt.

De succesvolle oplossing van de derde- en vierdegraadsvergelijkingen bepaalde de probleemstelling van de algebra tot het einde van de achttiende eeuw: het centrale probleem in die periode was het vinden van de oplossing van algemeen hogeregraadsvergelijkingen, te beginnen met vergelijkingen van de vijfde graad. Men zocht in verschillende richtingen, geïnspireerd door de verschillende methoden die voor derde- en vierdegraadsvergelijkingen waren ontwikkeld. Zo kan men bijvoorbeeld de derdegraadsvergelijking

$$x^3 + mx^2 + nx + t = 0 \quad (3)$$

reduceren tot een vergelijking

$$y^3 + n'y + t' = 0 \quad (4)$$

door $x = y - a$ te stellen en a zo te bepalen dat na substitutie in (3) de term van y^2 wegvalt (dat lukt voor $a = m/3$). Analoog heeft men gepoogd van hogeregraadsvergelijkingen door middel van ingewikkelder transformaties alle tussentermen te verwijderen (werk van E. W. von Tschirnhaus, 1651-1708).

Tevens trachtte men op andere manieren hulp-onbekenden in te voeren, waardoor het probleem werd gereduceerd tot het oplossen

van twee vergelijkingen met twee onbekenden, waarbij men een van de vergelijkingen enigszins verstandig kiezen kon. Echter alle pogingen tot oplossing van de algemene vijfdegraadsvergelijkingen liepen vast en wel óf omdat het rekenwerk onoverkomelijk omvangrijk werd, óf omdat de hulpvergelijkingen van dezelfde graad als of van hogere graad dan de oorspronkelijke vergelijking bleken te zijn. Zo ontstond in de laatste helft van de achttiende eeuw het vermoeden dat de oplossing van de algemene vijfdegraadsvergelijking onmogelijk was. Het is van belang precies te omschrijven wat onder het oplossen van een vergelijking werd verstaan. Een vergelijking werd geacht opgelost te zijn, als zijn wortels konden worden uitgedrukt in de coëfficiënten met behulp van $\sqrt{\text{ }}$ -vormen (oplossen door radikalen wordt dat ook wel genoemd). Hierbij was samenstelling van $\sqrt{\text{ }}$ -vormen toegestaan, zoals in de oplossing van de derdegraadsvergelijking

$$x^3 + px + q = 0 \quad (5)$$

(tweede term verwijderd, zie (4)), waarvan een oplossing met $\sqrt{\text{ }}$ -vormen geschreven kan worden:

$$x = \sqrt[3]{\{-q/2 + \sqrt{q^2/4 + p^3/27}\}} + \sqrt[3]{\{-q/2 - \sqrt{q^2/4 + p^3/27}\}}. \quad (6)$$

Het vermoeden van onoplosbaarheid betrof de algemene vijfdegraadsvergelijking; er waren al van speciale vergelijkingen oplossingen bekend. Zo waren omstreeks 1770 de oplossingen bekend van

$$x^n - 1 = 0 \quad (7)$$

(n -de eenheidswortels), voor lage n ; men kon deze met behulp van $\sqrt{\text{ }}$ -vormen schrijven (bijvoorbeeld de derde eenheidswortels $\epsilon = \frac{1}{2}(-1 + \sqrt{-3})$ en $\epsilon^2 = \frac{1}{2}(-1 - \sqrt{-3})$). Gauss bewees in zijn *Disquisitiones Arithmeticae* (1801), dat voor elke n de wortels van $x^n - 1 = 0$ met behulp van $\sqrt{\text{ }}$ -vormen kunnen worden geschreven.

Gauss bepaalde ook voor welke n er alleen kwadraatwortels in de oplossingen optreden; dit betekent dat de bijbehorende regelmatige n -hoek met passer en liniaal construeerbaar is.

Met de oplosbaarheid van (7) is ook in het algemeen de vergelijking

$$x^n - A = 0 \quad (A \text{ reëel; } A > 0) \quad (8)$$

oplosbaar; immers als $\epsilon_1 = 1, \epsilon_2, \epsilon_3, \dots, \epsilon_n$ de n oplossingen van (7) zijn en $\alpha = \sqrt[n]{A}$ de reële positieve n -demachtswortel uit A is, dan zijn de oplossingen van (8): $\alpha, \alpha\epsilon_2, \alpha\epsilon_3, \dots, \alpha\epsilon_n$. (Voor

negatieve A lukt iets dergelijks, maar men moet dan wat voorzigtiger te werk gaan.) Dat wil zeggen dat niet alleen de reële n -de wortels uit een reëel getal A als $\sqrt[n]{A}$ -vorm kunnen worden geschreven maar werkelijk alle, dus ook de complexe, n -de wortels uit A .

2. Lagrange; permutaties van de wortels

Op dit punt van het verhaal, een punt waar alle pogingen om de algemene vijfdegraadsvergelijking op te lossen lijken dood te lopen, komt er een essentiële ommekeer in de probleemstelling en de onderzoeksmethode bij de studie van algebraïsche vergelijkingen. Deze ommekeer is te danken aan Joseph Louis Lagrange (1736-1813), een van de grootste achttiende-eeuwse wiskundigen. Lagrange werd geboren in Turiijn; van 1766 tot 1787 was hij (als opvolger van Euler) verbonden aan de Akademie te Berlijn, daarna werkte hij in Parijs. Zijn belangrijkste werk ligt op het gebied van de analyse en de mechanica. Voor de algebra is eigenlijk alleen zijn in 1770/71 verschenen lange artikel over de oplossing van vergelijkingen van belang, maar dit beïnvloedde dan ook de algebra tot ver in de negentiende eeuw.

De nieuwe aanpak van Lagrange bestond daarin dat hij niet rechtstreeks naar oplossingen van vergelijkingen zocht, maar in het algemeen de relaties onderzocht tussen de coëfficiënten, de wortels van de vergelijking en de voor de oplossingsformules in aanmerking komende $\sqrt[n]{}$ -vormen. Tot Lagrange had men steeds geprobeerd de wortels van de vergelijking uit te drukken in de coëfficiënten door middel van $\sqrt[n]{}$ -vormen. Lagrange keerde deze aanpak om, hij onderzocht hoe de coëfficiënten én de optredende $\sqrt[n]{}$ -vormen kunnen worden uitgedrukt in de wortels van de vergelijking.

Als $x_1, \dots, x_n$ de wortels zijn van

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \quad (9)$$

dan kan men uit

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = (x - x_1)(x - x_2)\dots(x - x_n) \quad (10)$$

direct afleiden dat

$$\begin{aligned} a_0 &= (-1)^n \cdot x_1 \cdot x_2 \cdot \dots \cdot x_n \\ a_1 &= (-1)^{n-1} \{ x_2 x_3 \dots x_n + x_1 x_3 \dots x_n + x_1 x_2 x_4 \dots x_n + \dots \\ &\quad \dots + x_1 x_2 \dots x_{n-1} \} \end{aligned} \quad (11)$$

.....

$$a_{n-1} = -(x_1 + x_2 + \dots + x_n).$$

De coëfficiënten van de vergelijking kunnen dus worden geschreven als functies van de wortels. Deze functies zijn rationaal (ze bevatten geen $\sqrt{\quad}$ -vormen) en ze zijn symmetrisch. Dit laatste betekent dat de functies niet veranderen als men een permutatie (verwisseling) van de wortels $x_1, x_2, \dots, x_n$ uitvoert. Men noemt $a_0, \dots, a_{n-1}$ de elementair symmetrische functies, wat wil zeggen dat elke symmetrische functie van $x_1, \dots, x_n$ als combinatie van de a_i kan worden geschreven. Dit alles was al vóór Lagrange bekend, maar Lagrange onderzocht ook hoe de in de oplossingsformules optredende $\sqrt{\quad}$ -vormen in de wortels kunnen worden uitgedrukt.

We kunnen Lagrange's overwegingen het best weergeven aan de hand van het voorbeeld van een oplossingsformule voor de vierdegraadsvergelijking (waarbij we overigens bewijzen en rekenwerk weglaten). Lagrange zelf onderzocht verschillende oplossingsmethoden zowel voor tweede- als voor derde- en vierdegraadsvergelijkingen.

Zij

$$x^4 + ax^3 + bx^2 + cx + d = 0 \quad (12)$$

de algemene vierdegraadsvergelijking. De wortels zijn

$$\begin{aligned} x_1 &= -\frac{1}{4}a + \frac{1}{2}R + \frac{1}{2}\sqrt{\{\frac{3}{4}a^2 - R^2 - 2b + \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \\ x_2 &= -\frac{1}{4}a + \frac{1}{2}R - \frac{1}{2}\sqrt{\{\frac{3}{4}a^2 - R^2 - 2b + \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \\ x_3 &= -\frac{1}{4}a - \frac{1}{2}R + \frac{1}{2}\sqrt{\{\frac{3}{4}a^2 - R^2 - 2b - \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \\ x_4 &= -\frac{1}{4}a - \frac{1}{2}R - \frac{1}{2}\sqrt{\{\frac{3}{4}a^2 - R^2 - 2b - \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \end{aligned} \quad (13)$$

waarin $R = \sqrt{\{\frac{1}{4}a^2 - b + y\}}$

en y een wortel is van de derdegraadsvergelijking

$$y^3 - by^2 + (ac - 4d)y - a^2d + 4bd - c^2 = 0. \quad (14)$$

Omdat y een wortel van een derdegraadsvergelijking is, kan y met behulp van $\sqrt{\quad}$ -vormen worden geschreven; de formules (13) geven dus inderdaad de gewenste oplossing. De overige in de oplossing optredende $\sqrt{\quad}$ -vormen zijn:

$$R = \sqrt{\{\frac{1}{4}a^2 - b + y\}} \quad (15)$$

(R is wortel van de tweedegraadsvergelijking $r^2 - (\frac{1}{4}a^2 - b + y) = 0$ als we y in de coëfficiënten toelaten.)

$$\begin{aligned} T_1 &= \sqrt{\{\frac{3}{4}a^2 - R^2 - 2b + \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \\ T_2 &= \sqrt{\{\frac{3}{4}a^2 - R^2 - 2b - \frac{1}{4}R^{-1}(4ab - 8c - a^3)\}} \end{aligned} \quad (15)$$

(T_i is wortel van een tweedegraadsvergelijking

$t^2 - \{ \frac{1}{4}a^2 - R^2 - 2b \pm \frac{1}{4}R^{-1}(4ab - 8c - a^3) \} = 0$ als we R (en dus ook y) in de coëfficiënten toelaten.)

Lagrange merkte nu op dat de optredende $\sqrt{\quad}$ -vormen, evenals de coëfficiënten, geschreven kunnen worden als functies van de wortels, en wel als volgt:

$$y = x_1x_2 + x_3x_4 \quad (17)$$

$$R = \frac{1}{2}(x_1 + x_2 - x_3 - x_4) \quad (18)$$

$$T_1 = x_1 - x_2 \quad T_2 = x_3 - x_4 \quad (19)$$

Verder merkte Lagrange op dat de $\sqrt{\quad}$ -vormen als functie van de wortels een zekere symmetrie vertonen. Weliswaar blijven de functies, zoals in (17), (18) en (19), niet onveranderd onder elke permutatie van de wortels $x_1, \dots, x_4$ (zoals het geval was bij (11)) maar toch zijn er vrij veel permutaties die ze onveranderd laten en bijgevolg nemen ze, onder invloed van de overige permutaties, slechts weinig andere waarden aan. Laat ons bijvoorbeeld de functie y beschouwen. Er zijn $4! = 24$ permutaties van de wortels $x_1, \dots, x_4$; y neemt onder deze permutaties slechts drie verschillende waarden aan, te weten

$$\begin{aligned} y_1 &= x_1x_2 + x_3x_4 \\ y_2 &= x_1x_3 + x_2x_4 \\ y_3 &= x_1x_4 + x_2x_3 \end{aligned} \quad (20)^*$$

y behoudt dezelfde waarde onder de volgende permutaties (in kring-splitsing geschreven):

(1), (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423).

Verder is y wortel van een derdegraadsvergelijking (14) en de drie waarden in (20) zijn precies de drie wortels van die vergelijking. Lagrange merkte analoge eigenschappen op bij de andere hulp-grootheden en $\sqrt{\quad}$ -vormen die optreden in de oplossingen van vergelijkingen tot en met de vierde graad. Hij kwam tot de conclusie dat de belangrijkste hulpgrootheden bij het oplossen van de vergelijkingen juist die functies van de wortels zijn die, onder permuta-

*) 'Waarden' is de vertaling van de term 'valeurs' die Lagrange gebruikt. Hij bedoelt ermee de nieuwe functies die ontstaan als men de plaatsing van de x_i in de formule voor de oorspronkelijke functie verwisselt. Men verwarre 'waarde' dus niet met het moderne begrip 'functiewaarde'.

ties van de wortels, een gering aantal waarden aannemen.

Dit inzicht bracht Lagrange ertoe, bij de studie van de n -degraads-vergelijkingen, in het algemeen zijn aandacht te richten op rationale functies $\varphi(x_1, \dots, x_n)$ van de wortels en het aantal waarden te bestuderen dat een dergelijke functie aanneemt onder permutaties van de $x_1, \dots, x_n$. Hij vond de volgende belangrijke stellingen:

STELLING 1. *Het aantal waarden dat een rationale functie φ van de wortels $x_1, \dots, x_n$ kan aannemen onder permutaties van de x_i is gelijk aan $n!$ of aan een deler van $n!$.*

(Vanwege stelling 1 wordt in de groepentheorie de stelling dat het produkt van orde en index van een ondergroep gelijk is aan de orde van de groep, wel de 'stelling van Lagrange' genoemd. Men ziet namelijk direct in dat de permutaties die φ vast laten, een ondergroep H van de groep S_n van alle permutaties op n elementen vormen en dat het aantal waarden dat φ kan aannemen gelijk is aan de index van H in S_n (d.w.z. gelijk aan het aantal nevenklassen). Lagrange's stelling 1 zegt dus dat de index van de ondergroep de orde van de groep deelt. Aangezien het aantal elementen in een nevenklasse gelijk is aan het aantal elementen van de ondergroep, volgt hieruit:

$$\text{orde groep} = (\text{orde ondergroep}) \times (\text{index ondergroep}).$$

Overigens was het begrip groep bij Lagrange nog niet aanwezig.)

STELLING 2. *Als $\varphi^{(1)}, \dots, \varphi^{(k)}$ de k verschillende waarden zijn die $\varphi(x_1, \dots, x_n)$ onder permutaties van de x_i kan aannemen, en men vormt de vergelijking $(v - \varphi^{(1)})(v - \varphi^{(2)}) \dots (v - \varphi^{(k)}) = 0$, en werkt die uit:*

$$\begin{aligned} (v - \varphi^{(1)})(v - \varphi^{(2)}) \dots (v - \varphi^{(k)}) &= \\ &= v^k + b_{k-1}v^{k-1} + \dots + b_1v + b_0 = 0. \end{aligned} \quad (21)$$

dan zijn de b_i functies van de x_i die onder alle permutaties onveranderd blijven. De b_i zijn dus symmetrische functies en kunnen (zie (11)) geschreven worden als rationale combinaties van de coëfficiënten a_i van de vergelijking (9) waarvan de x_i de wortels zijn.

φ is dus wortel van een k -degraadsvergelijking met coëfficiënten die bekend zijn uit de coëfficiënten van (9).

STELLING 3. *Laten φ en ψ rationale functies zijn van $x_1, \dots, x_n$ en laat H de verzameling permutaties zijn die φ onveranderd laten.*

Als ϕ , onder de permutaties uit H , r verschillende waarden aanneemt, dan is ϕ wortel van een r -degraadsvergelijking met coëfficiënten die rationaal zijn in de oorspronkelijke coëfficiënten (de a_i uit (9)) en in ϕ .

(In het bijzonder volgt hieruit dat rationale functies die onder precies dezelfde verzameling permutaties ongewijzigd blijven, rationaal in elkaar kunnen worden uitgedrukt; de r is dan namelijk gelijk aan 1, zodat ϕ wortel is van een lineaire vergelijking met ϕ in de coëfficiënten, en omgekeerd.

Van stelling 3 hebben we een voorbeeld in (15): $R = \frac{1}{2}(x_1 + x_2 - x_3 - x_4)$ neemt onder de permutaties die y vast laten, de volgende twee waarden aan:

$$R_1 = \frac{1}{2}(x_1 + x_2 - x_3 - x_4) \quad R_2 = \frac{1}{2}(x_3 + x_4 - x_1 - x_2) \quad (22)$$

en R is inderdaad wortel van een tweedegraadsvergelijking met coëfficiënten $(1 \text{ en } \frac{1}{2}a^2 - b + y)$ die rationaal zijn in de coëfficiënten van de oorspronkelijke vergelijking en in y .

Met deze kennis gewapend onderzocht Lagrange het probleem van de vijfdegraadsvergelijking. De weg die hij wilde volgen, was duidelijk: eerst moest hij een rationale functie ϕ_1 van de wortels $x_1, \dots, x_5$ zoeken, die, onder permutaties van de x_i , minder dan vijf waarden aannam. Deze ϕ_1 zou wortel zijn van een vergelijking van de vierde of lagere graad met coëfficiënten rationaal afhankelijk van de oorspronkelijke coëfficiënten; ϕ_1 zou dus kunnen worden geschreven met behulp van $\sqrt{\quad}$ -vormen en onveranderd blijven onder een verzameling H_1 van permutaties. Vervolgens zou een ϕ_2 moeten worden gevonden die, onder permutaties uit H_1 , minder dan vijf waarden zou aannemen. Deze ϕ_2 zou wortel zijn van een vergelijking van de vierde of lagere graad met coëfficiënten rationaal uitdrukbaar in de oorspronkelijke coëfficiënten en in ϕ_1 , en zou dus met $\sqrt{\quad}$ -vormen kunnen worden geschreven. De permutaties uit H_1 die ϕ_2 vast laten, zouden een verzameling H_2 vormen.

Dit proces zou moeten worden voortgezet. De H_i worden daarbij steeds kleiner tot tenslotte het aantal elementen van H_k kleiner dan vijf zou zijn. Maar dan kan men ϕ_{k+1} gelijk aan een wortel kiezen, zeg $\phi_{k+1} = x_1$. Onder de permutaties uit H_k neemt ϕ_{k+1} ten hoogste vier waarden aan; x_1 kan dus met behulp van $\sqrt{\quad}$ -vormen in

p_k worden uitgedrukt. Men zou dan x_1 volledig met $\sqrt{}$ -vormen kunnen schrijven, waarmee het probleem opgelost zou zijn. In feite zouden bij deze constructie ook functies φ mogen voorkomen die meer dan vier waarden aannemen, maar dan zouden de bijbehorende vergelijkingen (21) van de vorm

$$y^k - A = 0 \quad (23)$$

moeten zijn, daar die vergelijkingen ook met $\sqrt{}$ -vormen kunnen worden opgelost.

Het lukte Lagrange niet zijn programma met succes uit te voeren, of met behulp ervan aan te tonen dat de algemene vijfdegraadsvergelijking onoplosbaar is (dit laatste vermoedde hij overigens wel). Lagrange's bijdrage ligt dus niet in een speciaal resultaat, maar veeleer in het aangeven van een geheel nieuwe richting van onderzoek, die dan ook later zeer vruchtbaar zou blijken.

3. Ruffini en Cauchy; uitwerking van de permutatie-theorie

Met behulp van Lagrange's methoden poogde Paolo Ruffini (1765-1822) in een serie artikelen waarvan het eerste in 1799 verscheen, te bewijzen dat de algemene vijfdegraadsvergelijking niet met $\sqrt{}$ -vormen oplosbaar is. Zijn pogingen waren niet geheel succesvol. Daarbij waren ze zeer moeilijk te volgen voor zijn tijdgenoten, die niet gewend waren aan de nieuwe aanpak. Ruffini leidde veel resultaten af over het aantal waarden dat rationale functies van de wortels $x_1, \dots, x_5$ kunnen aannemen onder permutaties. Zo bewees hij onder meer dat er geen functies zijn die drie of vier waarden aannemen. Het aantal waarden dat zulke functies kunnen aannemen is, zoals we nu weten, gelijk aan de index van de ondergroep van permutaties die de functies vast laten; Ruffini leidde dus in feite een aantal resultaten over orde en index van permutatiegroepen af.

Een expliciete theorie van permutaties werd pas later (1815) ontwikkeld door Augustin Louis Cauchy (1789-1857). Cauchy voerde het begrip produkt van twee permutaties in en hij ontwikkelde een goede terminologie en een goede notatie voor permutaties. Hierdoor was hij in staat Ruffini's resultaat te generaliseren; hij bewees dat als een functie in n variabelen onder permutaties van die variabelen k waarden kan aannemen, en als verder p het groot-

ste priemgetal $\leq n$ is, dat dan ófwel $k = 2$, ófwel $k \geq p$. (Voor het geval $n = 5$ is dit precies Ruffini's resultaat.) Hoewel Cauchy nog geen expliciete groepentheorie ontwikkelde, gebruikte hij in zijn bewijs feitelijk groepentheoretische methoden. Cauchy beschouwde met name cyclische permutaties en gebruikte het feit dat even permutaties kunnen worden geschreven als produkt van 3-cycli.

4. Abel; de vijfdegraadsvergelijking is onoplosbaar

Het definitieve bewijs van de onoplosbaarheid van de algemene vijfdegraadsvergelijking werd, in 1824, geleverd door de Noorse wiskundige Niels Henrik Abel (1802-1829). Abel bezocht de middelbare school in Oslo, waar zijn wiskundig talent werd ontdekt. Na in zijn eerste jaar op de universiteit het gewone programma te hebben gevolgd, studeerde hij verder zelfstandig en begon te publiceren. Omstreeks deze tijd meende hij de oplossing van de algemene vijfdegraadsvergelijking te hebben gevonden. Hij zond zijn oplossing ter publikatie naar Denemarken, maar kreeg het artikel terug met het verzoek het te verduidelijken met voorbeelden en het advies zich met minder steriele takken van de wiskunde, zoals de theorie van elliptische functies, bezig te houden. Abel nam dit advies ter harte; zijn belangrijkste wiskundige werk ligt op het terrein van elliptische functies. Hij poogde ook de gevraagde voorbeelden te leveren en bemerkte daarbij dat hij een fout had gemaakt. Hij kwam tot de overtuiging dat de algemene vijfdegraadsvergelijking niet oplosbaar was en bewees dit in 1824. Een eerste, zeer kort geformuleerde publikatie van zijn bewijs kreeg weinig aandacht. In 1825 vertrok Abel voor een studiereis van twee jaar naar Duitsland en Frankrijk. In Berlijn ontmoette hij Crelle (1780-1855) die onder de indruk kwam van Abel's capaciteiten en hem liet publiceren in zijn pas opgerichte *Journal für die reine und angewandte Mathematik* (bekend als *Crelle's Journal*). In het eerste nummer (1826) verscheen een uitgewerkte versie van Abel's bewijs dat de algemene vijfdegraadsvergelijking niet oplosbaar is. In Parijs ontmoette Abel teleurstellend weinig belangstelling voor zijn werk. In 1827 reisde hij terug naar Noorwegen, waar hij na een jaar een positie aan de universiteit van Oslo kreeg. Zijn

wiskundige produktie was zeer groot in die jaren, maar zijn gezondheid ging achteruit - hij had tuberculose. Hij stierf op 26-jarige leeftijd.

Abel gebruikte in zijn bewijs Cauchy's resultaten over het aantal waarden dat een functie van de wortels kan aannemen. Hij bewees dat, als de algemene n -degraadsvergelijking oplosbaar was (dus als de wortels zouden kunnen worden geschreven met behulp van $\sqrt{\quad}$ -vormen en rationale bewerkingen op de coëfficiënten), dat dan die $\sqrt{\quad}$ -vormen zelf rationale functies van de wortels x_i zouden zijn. (Dit had Lagrange, zoals we hebben gezien, opgemerkt bij de tweede-, derde- en vierdegraadsvergelijkingen. Abel vermeldt niet dat er ook eenheidswortels mogen optreden; het resultaat staat bekend als de stelling van Abel.)

Met behulp van Cauchy's resultaat bewees Abel vervolgens voor het geval van de vijfdegraadsvergelijking dat er in elk geval een kwadraatwortel of een vijfdemachtswortel zou moeten optreden.

Schrijft men zo'n $\sqrt{\quad}$ -vorm als functie van de $x_1, \dots, x_5$, dan moet deze functie ófwel twee, ófwel vijf waarden aannemen onder permutaties van de x_i . Abel bepaalde uit dit gegeven de mogelijke vormen voor de functie en was in staat voor elk van die vormen een tegenspraak af te leiden.

5. Galois; oplosbaarheid van vergelijkingen

Met Abel's bewijs dat de algemene vijfdegraadsvergelijking onoplosbaar is, werd de belangrijkste vraag in de algebra tot dan toe beantwoord. Het zoeken naar de algemene oplossing van hogeregraadsvergelijkingen had tot nu toe de richting van het onderzoek bepaald; nu moest zich een nieuwe probleemstelling ontwikkelen. De nieuwe probleemstelling lag voor de hand: de algemene n -degraadsvergelijking is niet met $\sqrt{\quad}$ -vormen oplosbaar; sommige speciale vergelijkingen, zoals $x^n - 1 = 0$, zijn dat wel en de vraag is dus:

Welke algebraïsche vergelijkingen zijn met $\sqrt{\quad}$ -vormen oplosbaar?

Dit is het probleem dat Galois heeft opgelost.

Evariste Galois is een van de meest tot de verbeelding sprekende figuren uit de geschiedenis van de wiskunde. Hij was een wiskundig genie; hij nam een zeer onorthodoxe houding aan tegenover

de wiskundigen en de wiskundige stijl van zijn tijd. Hij was harts-tochtelijk geëngageerd in de politieke strijd in Frankrijk na de juli-revolutie 1830, een engagement dat leidde tot zijn tragische dood op 21-jarige leeftijd. Ondanks de korte spanne tijds waarin Galois' wiskundige vorming en zijn onderzoek zich ontwikkelden, oefenen zijn (door tijdgenoten grotendeels miskende) geschriften een nog steeds waarneembare invloed op de algebra uit. Een invloed die het feit dat zijn naam verbonden is aan een zo belangrijk onderdeel van de moderne algebra als de Galois-theorie volkomen rechtvaardigt.

Galois werd geboren nabij Parijs in 1811. In Parijs bezocht hij het Collège Louis le Grand, waar hij in 1827 met de hogere wiskunde in aanraking kwam en al gauw zijn leraren overtuigde van zijn uitzonderlijke gaven. In 1829 zakte hij voor het toelatingsexamen van de Ecole Polytechnique, vooral omdat hij rebelleerde tegen de methode van examineren. Hij studeerde verder aan de Ecole Normale. Het jaar bracht nog meer tegenslagen en emotionele spanningen. Zijn vader pleegde zelfmoord; een wiskundige studie die Galois had voorgelegd aan de Académie werd teruggezonden met het advies die te herschrijven; een tweede versie ervan raakte bij de Académie verloren. Hierdoor verviel Galois' deelneming aan de Grand Prix voor wiskunde. Weliswaar publiceerde Galois enige artikelen, maar hij kreeg door deze tegenslagen de indruk dat de wiskundigen, ja zelfs de maatschappij in het algemeen, zich tegen hem keerden. Na de juli-revolutie 1830 werd Galois overtuigd republikein. Hij kon zijn politieke activiteiten en meningen steeds minder in overeenstemming brengen met de discipline op de Ecole Normale; eind 1830 werd hij van de Ecole verwijderd. Hij werd gearresteerd om politieke redenen, maar kwam na een maand weer vrij. Hij legde een nieuwe versie van het verloren gegane artikel voor aan de Académie. Dit stuk bevatte het antwoord op de vraag, welke algebraïsche vergelijkingen oplosbaar zijn. Galois kreeg het echter terug met het commentaar dat de inhoud deels al bekend en deels onbegrijpelijk was. In juli 1831 werd hij weer gearresteerd; in maart 1832 werd hij overgebracht naar een verpleeghuis om er de laatste maand van zijn straf uit te zitten. Hij beleefde er een ongelukkige lief-

desaffaire die, onder nog steeds duistere omstandigheden, leidde tot een uitdaging tot een duel. De nacht vóór dit duel schreef Galois brieven aan zijn republikeinse vrienden, ordende zijn wiskundige papieren en schreef een overzicht van zijn ontdekkingen. Zoals hij voorvoelde, werd hij in het duel dodelijk verwond; hij stierf op 31 mei 1832.

Hoewel het overzicht van zijn ontdekkingen in 1832 werd gepubliceerd, duurde het meer dan tien jaar voor Galois' werk werd erkend. In 1843 maakte J. Liouville (1809-1882) bekend dat Galois inderdaad de vraag had beantwoord, welke vergelijkingen met $\sqrt{\quad}$ -vormen oplosbaar zijn; de betreffende manuscripten werden pas in 1846, door Liouville, gepubliceerd.

Het tot nu toe besproken werk van Lagrange en Abel betrof algemene n -degraadsvergelijkingen, dat wil zeggen: er werd verondersteld dat er geen speciale relaties bestaan tussen de coëfficiënten a_i in

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0; \quad (24)$$

de coëfficiënten werden onderling onafhankelijk verondersteld.

Dit heeft tot gevolg dat de resultaten van Lagrange en Abel niet zonder meer op speciale vergelijkingen kunnen worden toegepast. Voor de algemene n -degraadsvergelijking (24) met wortels $x_1, \dots, x_n$ geldt:

- A. Een rationale functie ϕ van de wortels die onveranderd blijft onder elke permutatie van de wortels, is rationaal uitdrukbaar in de coëfficiënten a_i .
- B. Een rationale functie ϕ van de wortels die rationaal uitdrukbaar is in de coëfficiënten a_i , verandert niet onder permutaties van de wortels x_i .

Deze uitspraken volgen uit het feit dat de coëfficiënten a_i precies de elementair symmetrische functies van de x_i vormen, zie (11). Echter, voor speciale vergelijkingen gaat de uitspraak B niet meer op. Beschouw bijvoorbeeld de speciale vierdegraadsvergelijking

$$x^4 + ax^2 + b = 0. \quad (25)$$

Als x_1 een wortel van (25) is, dan is $-x_1$ ook een wortel; er geldt dus:

$$x_1 + x_2 = 0 \quad x_3 + x_4 = 0. \quad (26)$$

Nu is $\varphi = x_1 + x_2$ rationaal uitdrukbaar in de coëfficiënten (want 0 is rationaal uitdrukbaar in de coëfficiënten) en toch verandert φ onder de permutatie

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_3 & x_2 & x_4 \end{bmatrix}$$

in $x_1 + x_3$. Het blijkt dus dat bij speciale vergelijkingen sommige permutaties 'niet toegelaten' zijn. De uitspraken A en B zullen dus gemodificeerd moeten worden door niet de gehele groep S_n te beschouwen, maar de ondergroep G van 'toegelaten' permutaties. Verder zijn we eigenlijk niet alleen geïnteresseerd in functies die rationaal uitdrukbaar zijn in de coëfficiënten alleen, maar ook in zekere $\sqrt{\quad}$ -vormen, of andere irrationaliteiten, zeg $\theta_1, \dots, \theta_k$ (dit zijn bijvoorbeeld de y , R en T_i in (13) t.e.m. (16)). Men zegt dat de θ_i geadjungeerd zijn bij de coëfficiënten, of dat ze bekend worden verondersteld. Als we nu functies beschouwen die rationaal uitdrukbaar zijn in de coëfficiënten en in zekere dergelijke hulpgrootheden θ_i , dan zullen er weer minder permutaties 'toegelaten' zijn, immers zulke permutaties moeten ook de θ_i onveranderd laten.

We kunnen nu 'Galois' belangrijkste resultaten als volgt omschrijven:

Bij elke n -degraadsvergelijking (algemeen of speciaal)

$$f(x) = 0 \quad (27)$$

en elke keuze van bekend veronderstelde irrationaliteiten

$\theta_1, \dots, \theta_k$, is er een groep G van permutaties van de wortels van (27) zo, dat

- C. Een rationale functie φ van de wortels die onveranderd blijft onder de permutaties uit G , is rationaal uitdrukbaar in de coëfficiënten van f en in de $\theta_1, \dots, \theta_k$.
- D. Een rationale functie φ van de wortels die rationaal uitdrukbaar is in de coëfficiënten van f en in de $\theta_1, \dots, \theta_k$, blijft onveranderd onder alle permutaties uit G .

Galois formuleert deze stelling zonder de θ_i expliciet te noemen; hij spreekt over 'rationaal bekend', bedoelende: rationaal uitdrukbaar in die grootheden die bekend zijn verondersteld.

G wordt de groep van de vergelijking genoemd. Galois bewijst het bestaan van zo'n groep voor elke vergelijking door expliciet aan te geven hoe G kan worden geconstrueerd. Die constructie is in principe steeds mogelijk, maar praktisch, door het vereiste rekenwerk, vrijwel niet uitvoerbaar. G hangt af van de keuze van de θ_i ; voegt men een nieuwe irrationaliteit θ_{k+1} toe, dan wordt de groep van de vergelijking G' ; steeds geldt dat G' gelijk is aan G of aan een ondergroep van G . Dus door adjunctie van irrationaliteiten kan men de groep van een vergelijking reduceren tot een ondergroep. Heeft men door successieve adjunctie van θ_1 t.e.m. θ_k de groep van de vergelijking gereduceerd tot de identiteit, dan is de vergelijking oplosbaar in de $\theta_1, \dots, \theta_k$; immers dan voldoet $\varphi = x_1$ aan de voorwaarde onder C en is daardoor rationaal uitdrukbaar in $\theta_1, \dots, \theta_k$ en de coëfficiënten.

Galois beschouwt het effect van adjunctie van een irrationaliteit θ op de groep G van de vergelijking meer in detail. Laat de irrationaliteit θ wortel zijn van een irreducibele, d.w.z. niet in factoren ontbindbare, vergelijking

$$g(t) = t^m + b_{m-1}t^{m-1} + \dots + b_1t + b_0 = 0 \quad (28)$$

waarbij de b_i rationaal bekend zijn (vergelijk (14) t.e.m. (16)). Laat (28) als wortels hebben $\theta = \theta^{(1)}, \theta^{(2)}, \dots, \theta^{(m)}$. Laat door adjunctie van $\theta^{(i)}$ de groep van de vergelijking gereduceerd worden tot de ondergroep H_i van G . Galois merkt op dat de H_i geconjugeerde ondergroepen zijn (dat wil zeggen dat er bij elke H_p en H_q een permutatie $\pi \in G$ is met $\pi H_p \pi^{-1} = H_q$; Galois formuleert dit overigens op een andere manier). Als deze geconjugeerde ondergroepen onderling gelijk zijn, dus $H_i = H$ voor alle i , dan zijn alle $\theta^{(i)}$ rationaal bekend zodra één ervan geadjungeerd is. In dit geval is H een *normaaldeler* van G ; dit begrip werd door Galois ingevoerd. Omgekeerd, als alle $\theta^{(i)}$ rationaal uitdrukbaar zijn in één van de $\theta^{(i)}$, dan reduceert adjunctie van één van de $\theta^{(i)}$ de groep G van de vergelijking tot een *normale* ondergroep (normaaldeler) H . Met dit begrippenapparaat was Galois in staat het probleem op te lossen welke n -degraadsvergelijkingen oplosbaar zijn met $\sqrt{\quad}$ -vormen. Zo'n vergelijking is namelijk oplosbaar als de successievelijk geadjungeerde θ 's wortels zijn van de vergelij-

maar werkte de theorie nauwelijks verder uit. Zijn publikatie bracht tenslotte de verdiende algemene bekendheid voor Galois' werk. Nog belangrijker voor Galois' theorie was *Traité des substitutions et des équations algébriques* ('substitution' is een term voor permutatie) van Camille Jordan (1838-1922), dat in 1870 verscheen. Het werk gaf een samenvatting van de tot dan toe bekende theorie van permutatiegroepen en van vergelijkingen. Het bevatte ook vele originele bijdragen van Jordan zelf. Met de publikaties van Serret en Jordan was Galoistheorie, in de vorm die we hierboven hebben aangegeven, een geaccepteerd en belangrijk onderdeel van de algebra geworden.

De Galoistheorie heeft in de daaropvolgende jaren een sterke ontwikkeling doorgemaakt, waarbij de theorie essentieel van karakter veranderde. Deze ontwikkeling was drieledig:

Ten eerste werd de vraag naar de oplosbaarheid van vergelijkingen losgelaten, of in elk geval verdrongen naar de status van toepassing van Galoistheorie.

Ten tweede werd het begrip *lichaam* ingevoerd om relaties die voordien werden omschreven met termen als '*rationaal uitdrukbaar in*' te verduidelijken.

Tenslotte werd de opbouw van de theorie van vergelijkingen uit losgelaten; Galoistheorie werd een theorie over lichamen. In plaats van de wortels van een vergelijking werden *automorfismen van lichamen* beschouwd.

Deze drieledige ontwikkeling verliep geleidelijk, dit in tegenstelling tot de veranderingen die door Lagrange en Galois in de theorie werden teweeggebracht. Het is moeilijk om, zonder te veel in detail te treden, deze ontwikkeling precies te volgen. Ik volsta daarom met een globale beschrijving ervan.

Galois' oplossing van het centrale probleem van de algebra na Abel (welke vergelijkingen zijn met $\sqrt{\quad}$ -vormen oplosbaar?) leidde tot een nieuwe vraagstelling. Allereerst rees de vraag of Galois' criterium in speciale gevallen nader kon worden gepreciseerd. Galois zelf onderzocht al het geval waarbij de graad van de vergelijking priem is. Het latere onderzoek in deze richting leidde tot de studie van *eindige lichamen* en *lineaire groepen*.

Belangrijker was dat men ging inzien dat de oplosbaarheid met $\sqrt{}$ -vormen eigenlijk slechts een speciale eigenschap van de groep van de vergelijking of van de aard van de te adjungeren irrationaliteiten was. Men ging zich interesseren voor de structuur van de groep van de vergelijking en de ondergroepen daarvan in het algemeen, alsmede voor de adjunctie van irrationaliteiten in het algemeen en voor het verband tussen beide zaken. De theorie werd dus veel algemener, het oorspronkelijke probleem werd een speciale toepassing ervan.

Deze verschuiving naar een algemene structuurtheorie van groepen en van adjunctie werd mogelijk gemaakt door de opkomst van het begrip *lichaam*. In het voorafgaande is herhaaldelijk sprake geweest van 'rationale uitdrukbaarheid'. Laten φ en ψ twee grootheden zijn die rationaal uitdrukbaar zijn in de coëfficiënten $a_0, \dots, a_{n-1}$ van een zekere n -degraadsvergelijking en in zekere hulp-grootheden $\theta_1, \dots, \theta_k$. Dat wil zeggen dat φ en ψ uit de a 's en de θ 's gevormd zijn door optelling, aftrekking, vermenigvuldiging en deling (mits niet door 0). Dat houdt dan weer in dat ook $\varphi + \psi$, $\varphi - \psi$, $\varphi \cdot \psi$ en φ/ψ (mits $\psi \neq 0$) rationaal uitdrukbaar zijn in de a 's en de θ 's. De rationaal uitdrukbare grootheden (ofwel de *bekend veronderstelde* grootheden) vormen dus een systeem dat gesloten is onder de vier arithmetische bewerkingen, d.w.z. zij vormen een *lichaam*. Adjunctie van een nieuwe θ komt neer op uitbreiding van het oorspronkelijke lichaam tot een groter lichaam van 'bekend veronderstelde' grootheden. De uitdrukkingen die rationaal zijn in de wortels $x_1, \dots, x_n$ van een vergelijking $f(x) = 0$, vormen eveneens een lichaam (dit lichaam wordt in de moderne Galoistheorie het *splijtlichaam* van f genoemd). De bovengeschetste theorie van Galois kan men dus her-interpreteren met behulp van het begrip lichaam: Eerst wordt gevormd het lichaam van de vormen die rationaal uitdrukbaar zijn in de coëfficiënten van de vergelijking. Zo nodig worden eenheidswortels geadjungeerd; het zo ontstane lichaam wordt *grondlichaam* genoemd. Dit grondlichaam wordt door successieve adjunctie uitgebreid tot het ten-slotte gelijk is aan het splijtlichaam. De lichamen die door adjunctie ontstaan, zijn deellichamen van het splijtlichaam.

Het begrip lichaam vindt zijn oorsprong in het werk van Kronecker (die sprak van *Rationalitätsbereich*) en Richard Dedekind (1831-1926) (die de term *Körper* invoerde). Kronecker was vooral geïnteresseerd in uitbreidingen van het lichaam van de rationale getallen als middel om irrationale getallen zuiver arithmetisch constructief te definiëren. Hij publiceerde een samenvatting van zijn studies in deze richting in 1882. In tegenstelling tot Kronecker, wiens 'Rationalitätsbereiche' gedefinieerd werden als bevattende alle grootheden die rationaal uitdrukbaar zijn in zekere gegeven grootheden, voerde Dedekind het begrip lichaam in door middel van de eigenschap van gesloten-zijn onder de arithmetische bewerkingen. Elk systeem van reële of complexe getallen dat gesloten is onder optellen, aftrekken, vermenigvuldigen en delen, noemde hij een lichaam. Dedekind ontwikkelde het begrip in de vijftiger jaren van de 19e eeuw in studies over getaltheorie; het begrip lichaam kreeg echter vooral bekendheid door Dedekinds uiteenzetting ervan in 1894 in een supplement bij de vierde editie van het leerboek van Peter Gustav Lejeune Dirichlet (1805-1859) over getaltheorie.

Zowel Kronecker als Dedekind hebben hun begrippen *Rationalitätsbereich* en *Körper* in verband met Galoistheorie gebracht. Door hun werk was het om de eeuwwisseling algemeen aanvaard dat Galoistheorie een theorie was over vergelijkingen en bijbehorende lichamen en hun uitbreidingen.

In het begin van de 20e eeuw ontstond het inzicht dat de rol van de vergelijkingen in de theorie niet essentieel is, en dat Galoistheorie een theorie van lichamen in het algemeen behoort te zijn. In de Galoistheorie werden vergelijkingen gebruikt om over de permutaties van hun wortels te kunnen praten; deze permutaties vormden de groepen waarmee de structuur van de lichaamsuitbreidingen kon worden beschreven. Om tot een zuivere theorie van lichamen te komen, moesten deze groepen onafhankelijk van vergelijkingen worden gedefinieerd. Dit bleek nu mogelijk doordat de permutaties van de wortels kunnen worden opgevat als automorfismen van het splijtlichaam. Zij f een vergelijking met grondlichaam F en wortels $x_1, \dots, x_n$. Het splijtlichaam (het lichaam van de rationale vor-

men in de x_i) zij M . Men gaat eenvoudig na dat elk automorfisme van M dat F elementsgewijs vast laat, de x_i permuteert. Omgekeerd, een permutatie π uit de Galois-groep van de vergelijking (dus een 'toegestane' permutatie van de wortels) induceert op M een automorfisme dat F elementsgewijs vast laat. De 'groep van de vergelijking' in Galois' zin kan dus worden opgevat als de groep van automorfismen van het splijtlichaam, die het grondlichaam elementsgewijs vast laten. Het inzicht dat de Galois-groep zo kan worden geïnterpreteerd, is al bij Dedekind aanwezig; het werd gemeengoed in de eerste decennia van de 20e eeuw.

Hiermee was de weg vrij voor een opvatting van de Galoistheorie als theorie van lichamen en bijbehorende automorfismengroepen. Gedurende de 19e eeuw werden in de Galoistheorie uitsluitend deellichamen van de complexe getallen beschouwd; nu konden ook andere lichamen (eindige lichamen bijvoorbeeld) worden bestudeerd met behulp van de Galoistheorie. De opvatting van de Galoistheorie als algemene theorie van lichamen blijkt al in de presentaties van de theorie door wiskundigen als E. Steinitz (1910) en B. L. van der Waerden (*Moderne Algebra*, 1930). Men kan deze ontwikkeling als voltooid beschouwen in de presentatie van de theorie door Emil Artin (colleges in 1926, publikatie in 1938-1942).

7. Slot

Ik heb in het bovenstaande in grote lijnen geschetst hoe zich uit de studie van vergelijkingen de Galoistheorie heeft ontwikkeld. Ik wil het overzicht besluiten met twee algemene opmerkingen. De ontwikkeling van de Galoistheorie is in zeker opzicht typerend voor de ontwikkeling van de wiskunde in de afgelopen periode van circa 100 jaar. Men ziet namelijk bij de Galoistheorie een verschuiving van de interesse van objecten (vergelijkingen en hun wortels) naar structuren (lichamen met hun deellichamen, groepen met hun ondergroepen). In plaats van de afzonderlijke rationale uitdrukkingen in de coëfficiënten of in de wortels, worden de verzamelingen van ál dergelijke uitdrukkingen beschouwd; in die verzamelingen wordt een structuur onderkend (het zijn lichamen); de verzamelingen blijken tezamen weer een structuur te vormen (de door

inclusie geordende verzameling van deellichamen van een lichaam). Een analoge ontwikkeling is zichtbaar in de behandeling van de permutatiegroepen. De nieuwe beschouwingswijze maakt het mogelijk, anderszins nauwelijks formuleerbare eigenschappen te omschrijven (bijvoorbeeld de normaaldeler-eigenschap); zij maakt het ook mogelijk, de resultaten aanmerkelijk te generaliseren. Dit proces nu, het bestuderen van gestructureerde verzamelingen, valt op vele andere gebieden van de wiskunde in de laatste 100 jaar aan te wijzen, bijvoorbeeld in het bestuderen van functieruimten in plaats van afzonderlijke functies in de analyse en, meer recent, in de studie van categorieën.

De ontwikkeling van de Galoistheorie geeft ook een fraai voorbeeld van wat er zo al met wiskundige problemen gebeuren kan, van hoe de probleemstellingen in de wiskunde zich kunnen wijzigen. Voor het probleem van het bepalen van wortels van een n -degraadsvergelijking werd, voor $n \leq 4$, een oplossing gevonden. Voor $n = 4$ had deze oplossing, wegens de ingewikkeldheid, al nauwelijks meer praktische waarde; voor de feitelijke berekening van de wortels bleken benaderende procédés doelmatiger. Voor $n \geq 5$ werd bewezen dat de bepaling van de wortels door middel van een algemene formule onmogelijk was. De dan opkomende vraag: welke vergelijkingen zijn wél oplosbaar? werd beantwoord, maar het antwoord had voor de bepaling of een gegeven vergelijking oplosbaar is, noch voor de feitelijke oplossing ervan, praktisch enige waarde. De Galoistheorie ontwikkelde zich als het ware met achterlating van het probleem van de feitelijke bepaling van de wortels van vergelijkingen.

De door Galois beantwoorde vraag naar een criterium voor oplosbaarheid bleek vervolgens een weinig natuurlijke vraag in het, ter beantwoording ervan, ontwikkelde begrippenapparaat. Er kwam daarom een nieuwe vraagstelling op, namelijk hoe in het algemeen de adjunctie van irrationaliteiten en de reductie van groepen van toegelaten permutaties van wortels van vergelijkingen samenhangen. Ook deze vraagstelling bleek, na de invoering van het begrip lichaam, té speciaal voor het ontwikkelde begrippenapparaat; de vergelijkingen werden geheel losgelaten, de permutaties

van de wortels werden automorfismen van lichamen. Of en hoe de vraagstelling in de Galoistheorie zich verder heeft gewijzigd of zich nog wijzigen zal, past niet meer in deze historische bespreking.

Men ziet echter: de wiskunde schrijdt niet voort door de oplossing van problemen maar door de wijziging ervan.

Literatuur

Het hier behandelde kan men aanmerkelijk meer gedetailleerd beschreven vinden in:

B. M. Kiernan, The Development of Galois Theory from Lagrange to Artin, *Archive for History of Exact Sciences* 8, 40-154 (1971/1972);

B. L. van der Waerden, Die Galois-Theorie von Heinrich Weber bis Emil Artin, *Archive for History of Exact Sciences* 9, 220-248 (1972/1973).

Examens wiskunde m.o. A en m.o. B

Wie zich in 1982 wenst te onderwerpen aan het door de *Algemene Commissie* af te nemen examen ter verkrijging van de akte wiskunde m.o. A of B, dient zich vóór 1 mei 1982 aan te melden door storting van f 80,- op postrekening 172007 ten name van de Algemene examencommissie wiskunde m.o. te 's-Gravenhage met vermelding van de volledige naam en het adres van de kandidaat en met de aanduiding m.o. A of m.o. B. Na 1 mei 1982 ontvangen de aangemelde kandidaten nadere instructies van de examencommissie. Alle kandidaten zullen worden geëxamineerd volgens de nieuwe programma's, zoals die zijn omschreven in het Nieuw Tijdschrift voor Wiskunde jg 63 blz. 86-93. Men kan ze verkrijgen door storting van f 2,- op de bovengenoemde postrekening met vermelding 'examen-programma'.

Zowel van het A-examen als van het B-examen wordt het schriftelijk gedeelte afgenomen op 19 en 20 augustus 1982 in het Congresgebouw te 's-Gravenhage.

18e Nederlands Mathematische Congres

Tijdens het bovengenoemde congres (zie vooraankondiging op het omslag van afl. 69/3) zullen de volgende voordrachten op uitnodiging worden gehouden: 'Geschiedenis en praktijk als leidraad voor wiskundig denken; de casus Felix Klein' (dr E. Glas); 'Enige aspecten van ondiep-water-benaderingen in de scheepshydrodynamica' (prof. dr ir A. J. Hermans); 'Hodge-theorie: analyse of meetkunde?' (prof. dr J. H. M. Steenbrink); 'Mathematische structuren voor het modelleren van dynamische systemen' (prof. dr ir J. C. Willems). De titel van de slotvoordracht luidt: 'Volledige inductie en computing science' (prof. dr E. W. Dijkstra). Leden: f 12,50, niet-leden f 22,50.

Inhoud 69/4

DR H. J. M. BOS, Algebraïsche vergelijkingen en Galois-theorie, een historisch overzicht	143
PROF. DR L. KUIPERS, Uitbreiding van de ongelijkheid van Abi-Khuzam tot meer dan vier hoekgrootten	166
Opmerking bij Sprokkel 251	169
Goede oplossingen, 2543-2552	170
Goede oplossingen 956-963	177
Vraagstukken ter oplossing 2570-2579 en 972-979	183
Boekbespreking	187