

ALGEBRAISCHE VERGELIJKINGEN EN GALOIS'THEORIE

Een historisch overzicht

door

H.J.M. Bos

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 der automorfismen-groepen van die lichamen.

Hoewel op het eerste gezicht de twee onderwerpen, oplossing van vergelijkingen en structuur van lichamen, 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 geschetst worden.

DE OPLOSSING VAN TWEDE-, DERDE- EN VIERDEGRAADS VERGELIJKINGEN

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

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

Ziet men af van de genoemde verschillen (meetkundige behandeling, beperking tot positieve grootheden) dan waren de methoden equivalent met de bekende formule voor de oplossing van

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

namelijk

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

Algemene oplossingen van derde- en vierdegraads vergelijkingen zijn van veel recenter datum; ze stammen uit de eerste helft der zestiende eeuw, uit de periode der Renaissance. Ze vormden een der eerste verworvenheden van de wiskunde in West-Europa die uitstegen boven wat de Oudheid op wiskundig gebied gepresteerd had.

De ontdekkingsgeschiedenis van deze oplossingen is zeer gecompliceerd. Scipione del Ferro (1465?-1526) vond omstreeks 1500 een oplossingsmethode voor een bepaalde vorm van derdegraads vergelijkingen. Hij publiceerde de methode niet, maar deelde hem mee aan vrienden. Een van deze vrienden daagde later, in 1535, Niccolo Tartaglia (1500?-1557) in het openbaar uit een serie derdegraads vergelijkingen 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 vierdegraads vergelijkingen 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 positieve grootheden, hoewel af en toe negatieve en zelfs complexe grootheden in hun

werk voorkwamen. Het heeft nog minstens twee eeuwen geduurd voordat deze grootheden algemeen in de wiskundige praktijk aanvaard werden. Hiermee hangt samen dat de hoofdstelling der algebra - iedere n-de graads vergelijking heeft n wortels - eerst laat geformuleerd en bewezen kon worden. Men vindt een formulering bij Albert Girard (1595-1632). Leonhard Euler (1707-1783) formuleert in 1743 het vermoeden dat iedere vergelijking met reële coëfficiënten te ontbinden is 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 vergelijkingenleer ingevoerd. Hierdoor werd het mogelijk algemene oplossingsmethoden in formules op te schrijven - voordien konden methoden alleen als recept worden omschreven en door voorbeelden worden aangetoond.

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

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

reduceren tot een vergelijking

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

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 $a = 1/3m$). Analoog hiermee heeft men gepoogd van hogere graads vergelijkingen 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 één van de vergelijkingen enigszins verstandig kiezen kon. Echter alle pogingen tot oplossing van de algemene vijfdegraads vergelijkingen liepen vast, en wel òf omdat het rekenwerk onover-

komelijk omvangrijk werd, òf omdat de hulpvergelijkingen van dezelfde of van hogere graad als de oorspronkelijke vergelijking bleken te zijn.

Zo ontstond in de laatste helft der achttiende eeuw het vermoeden dat de oplossing van de algemene vijfdegraads vergelijking 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 uitgedrukt konden worden in coëfficiënten met behulp van $\sqrt{-}$ vormen (*oplossen door radikalen* wordt dat ook wel genoemd). Hierbij was samenstelling van $\sqrt{-}$ vormen toegestaan, zoals in de oplossing der derdegraads vergelijking

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

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

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

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

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

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

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

oplosbaar; immers als $\varepsilon_1=1, \varepsilon_2, \varepsilon_3, \dots, \varepsilon_n$ de n oplossingen van (7) zijn, en $\alpha = \sqrt[n]{A}$ de reële positieve n-e machtswortel uit A is, dan zijn de oplossingen van (8): $\alpha, \varepsilon_2 \alpha, \varepsilon_3 \alpha, \dots, \varepsilon_n \alpha$. (Voor negatieve A lukt iets dergelijks, maar men moet dan wat voorzichtiger te werk gaan.) Dat wil zeggen dat niet alleen de reële n-de wortels uit een reëel getal A als $\sqrt{-}$ vorm geschreven kunnen worden, maar werkelijk alle, dus ook de complexe, n-de

wortels uit A

LAGRANGE - PERMUTATIES VAN DE WORTELS

Op dit punt in het verhaal - een punt waar alle pogingen om de algemene vijfdegraads vergelijking 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 der grootste achttiende-eeuwse wiskundigen. Lagrange werd geboren in Turijn; van 1766 tot 1787 was hij verbonden (als opvolger van Euler) aan de Akademie te Berlijn, daarna werkte hij in Parijs. Zijn belangrijkste werk ligt op het gebied der Analyse en der 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 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 tussen de coëfficiënten, de wortels van de vergelijking en de voor de oplossingsformules in aanmerking komende $\sqrt{\quad}$ -vormen. Tot Lagrange had men steeds geprobeerd de wortels van de vergelijking uit te drukken in de coëfficiënten door middel van $\sqrt{\quad}$ -vormen. Lagrange keerde deze aanpak om, hij onderzocht hoe de coëfficiënten en de optredende $\sqrt{\quad}$ -vormen uitgedrukt kunnen worden in de wortels van de vergelijking.

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

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

dan kan men uit

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

direct afleiden dat

$$a_0 = (-1)^n \cdot x_1 \cdot x_2 \cdot \dots \cdot x_n$$

$$a_1 = (-1)^{n-1} [x_2 \cdot x_3 \cdot \dots \cdot x_n + x_1 \cdot x_3 \cdot \dots \cdot x_n + x_1 \cdot x_2 \cdot x_4 \cdot \dots \cdot x_n + \dots + x_1 \cdot x_2 \cdot \dots \cdot x_{n-1}]$$

$$(11) \quad a_{n-1} = -(x_1 + x_2 + \dots + x_n)$$

De coëfficiënten van de vergelijking kunnen dus geschreven worden 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 $x_1, \dots, x_n$ uitvoert. $a_0, \dots, a_{n-1}$ zijn de zogenaamde elementair symmetrische functies, wat wil zeggen dat iedere symmetrische functie van $x_1, \dots, x_n$ als combinatie der a_i te schrijven is. Dit alles was al vóór Lagrange bekend, maar Lagrange onderzocht ook hoe de in de oplossingsformules optredende $\sqrt{\quad}$ -vormen uit te drukken zijn in de wortels.

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

Zij

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

de algemene vierdegraads vergelijking. De wortels zijn

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

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

en y een wortel is van de derdegraads vergelijking

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

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

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

R is wortel van de tweedegraads vergelijking

$$r^2 - (\frac{1}{4}a^2 - b + y) = 0,$$

als we y in de coëfficiënten toelaten.

$$\begin{aligned}
 T_1 &= \sqrt{3/4a^2 - R^2 - 2b + \frac{1}{4}R^{-1}(4ab - 8c - a^3)} \\
 T_2 &= \sqrt{3/4a^2 - R^2 - 2b - \frac{1}{4}R^{-1}(4ab - 8c - a^3)}
 \end{aligned}
 \tag{16}$$

T_i is wortel van een tweedegraads vergelijking

$$t^2 - [3/4a^2 - R^2 - 2b \pm \frac{1}{4}R^{-1}(4ab - 8c - a^3)]$$

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:

$$(17) \quad y = x_1 \cdot x_2 + x_3 \cdot x_4$$

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

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

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 iedere permutatie der 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. Beschouwen we bijvoorbeeld de functie y . 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

$$\begin{aligned}
 y_1 &= x_1 \cdot x_2 + x_3 \cdot x_4 \\
 y_2 &= x_1 \cdot x_3 + x_2 \cdot x_4 \\
 y_3 &= x_1 \cdot x_4 + x_2 \cdot x_3 \quad *)
 \end{aligned}
 \tag{20}$$

y behoudt dezelfde waarde onder de volgende permutaties (in kringsplitsing geschreven):

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

Verder is y wortel van een derdegraads vergelijking (14) en de drie waarden in (20) zijn precies de drie wortels van die vergelijking.

*) "Waarden" is de vertaling van de term "valeurs" die Lagrange gebruikt.

Hij bedoelt ermee de nieuwe functies die ontstaan als men de plaatsing der x_i in de formule voor de oorspronkelijke functie verwisselt. Men verwarre dus niet met het moderne begrip "functiewaarde"!

Lagrange merkte analoge eigenschappen op bij de andere hulpgrootheden en $\sqrt{}$ -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 permutaties der wortels, een gering aantal waarden aannemen.

Dit inzicht bracht Lagrange er toe om, bij de studie van de n -de graads vergelijkingen in het algemeen zijn aandacht te richten op rationale functies $\phi(x_1, \dots, x_n)$ 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 Groepen-theorie de stelling dat het produkt van orde en index van een ondergroep gelijk is aan de orde van de groep, welke "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 vormt, 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 een 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 $\phi^{(1)}, \dots, \phi^{(k)}$ de k verschillende waarden zijn die $\phi(x_1, \dots, x_n)$ onder permutaties der x_i kan aannemen, en men vormt de vergelijking $(v - \phi^{(1)})(v - \phi^{(2)}) \dots (v - \phi^{(k)}) = 0$, en werkt die uit:*

$$(21) \quad (v - \phi^{(1)})(v - \phi^{(2)}) \dots (v - \phi^{(k)}) = v^k + b_{k-1}v^{k-1} + \dots + b_1v + b_0 = 0$$

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)) geschre-

ven 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 -e-graads vergelijking 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 ψ onder de permutaties uit H , r verschillende waarden aanneemt, dan is ψ wortel van een r -de graads vergelijking met coëfficiënten die rationaal zijn in de oorspronkelijke coëfficiënten de a_i) en in ψ .

(in het bijzonder volgt hieruit dat rationale functies die onder precies dezelfde verzameling permutaties ongewijzigd blijven rationaal in elkaar uit te drukken zijn; de r is dan namelijk gelijk aan 1 zodat ψ wortel is van een lineaire vergelijking met ψ 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:

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

en R is inderdaad wortel van een vergelijking met coëfficiënten (1 en $\frac{1}{4}a^2 - b + y$) die rationaal zijn in de coëfficiënten van de oorspronkelijke vergelijking en in y .

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

Dit proces zou moeten worden voortgezet. De H_i worden daarbij steeds kleiner, tot tenslotte $H_k = (1)$ mogelijk zou zijn. Maar dan kan men $\phi_k = x_1$

kiezen; x_1 wordt alleen door de identieke permutatie vastgelaten. Men zou dan x_1 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

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

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

Het lukte Lagrange niet zijn programma met succes uit te voeren, of met behulp ervan aan te tonen dat de algemene vijfdegraads vergelijking 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.

RUFFINI EN CAUCHY - UITWERKING DER 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 vijfdegraads vergelijking 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 product 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 grootste priemgetal $\leq n$ is, dat dan òfwel $k = 2$, òfwel $k \geq p$. (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 als product van 3-cycli geschreven kunnen worden.

ABEL - DE VIJFDEGRAADS VERGELIJKING IS ONOPLOSBAAR

Het definitieve bewijs van de onoplosbaarheid van de algemene vijfdegraads vergelijking werd, in 1824, geleverd door de Noorse wiskundige Niels Henrik Abel (1802-1829). Abel bezocht de middelbare school in Oslo, waar zijn wiskundig talent ontdekt werd. Na in zijn eerste jaar op de universiteit het gewone programma gevolgd te hebben, studeerde hij verder zelfstandig en begon te publiceren. Omstreeks deze tijd meende hij de oplossing der algemene vijfdegraads vergelijking gevonden te hebben. Hij zond zijn oplossing ter publicatie naar Denemarken, maar kreeg het artikel terug met het verzoek het te verduidelijken met voorbeelden, en het advies zich met minder steriele takken van wiskunde bezig te houden, zoals de theorie van elliptische functies. 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 vijfdegraads vergelijking niet oplosbaar was en bewees dit in 1824. Een eerste zeer kort geformuleerde publicatie 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 vijfdegraads vergelijking 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 productie 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 -de graads vergelijking oplosbaar was, (dus als de wortels $x_1, \dots, x_n$ geschreven kunnen worden met behulp van $\sqrt{}$ -vormen en rationale bewerkingen op de coëfficiënten), dat dan die $\sqrt{}$ -vormen zelf rationale functies van de x_i zouden zijn. (Dit had Lagrange, zoals we gezien hebben, opgemerkt bij de tweede- derde- en vierdegraads vergelijkingen. 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 der vijfdegraads vergelijking dat er in elk geval een kwadraat-wortel of een vijfde-machts-wortel zou moeten optreden. Schrijft men zo'n $\sqrt{}$ -vorm als functie der $x_1, \dots, x_5$, dan moet deze functie òfwel twee, òfwel vijf waarden aannemen onder permutaties der x_i . Abel bepaalde uit dit gegeven de mogelijke vormen voor de functie en was in staat voor elk dier vormen een tegenspraak af te leiden.

GALOIS - OPLOSBAARHEID VAN VERGELIJKINGEN

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

Welke algebraïsche vergelijkingen zijn met $\sqrt{}$ -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 der 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 hartstochtelijk 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 span-

ne tijds waarin Galois' wiskundige vorming en zijn onderzoek zich ontwikkelde, oefenen zijn, (door tijdgenoten grotendeels miskende), geschriften een nog steeds waarneembare invloed uit op de algebra. Een invloed, welke het feit dat zijn naam verbonden is aan een zo belangrijk onderdeel der 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 Hogere Wiskunde Onderwijs 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 het te herschrijven; een tweede versie ervan raakte bij de Académie verloren. Hierdoor verviel Galois' deelname 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 keerde.

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 liefdesaffaire, 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 gepubliceerd werd,

duurde het meer dan 10 jaar voor Galois' werk werd erkend. In 1843 maakte J. Liouville (1809-1882) bekend dat Galois inderdaad de vraag welke vergelijkingen met $\sqrt{\quad}$ -vormen oplosbaar zijn had beantwoord; de betreffende manuscripten werden pas in 1846, door Liouville, gepubliceerd.

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

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

bestaan; 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 -de graads vergelijking (24) met wortels $x_1, \dots, x_n$ geldt:

A. Een rationale functie ϕ van de wortels die onveranderd blijft onder iedere 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 der x_i vormen, zie (11). Echter, voor speciale vergelijkingen gaat uitspraak B niet meer op. Beschouw bijvoorbeeld de speciale vierdegraads vergelijking

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

De wortels van (25) zijn paarsgewijs (als x_1 wortel is, dan ook $-x_1$); er geldt dus ook voor de wortels $x_1, \dots, x_4$:

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

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

$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_3 & x_2 & x_4 \end{pmatrix}$ 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/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 iedere n -de graads vergelijking (algemeen of speciaal)

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

en bij iedere keuze van bekend veronderstelde irrationaliteiten $\theta_1, \dots, \theta_k$, is er een groep G van permutaties der wortels van (27) zodat

- 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 verondersteld zijn. G wordt de groep van de vergelijking genoemd. Galois bewijst het bestaan van zo'n groep voor iedere vergelijking door expliciet aan te geven hoe G geconstrueerd kan worden. Die constructie is in principe steeds mogelijk maar practisch, door het vereiste rekenwerk, vrijwel niet uitvoerbaar. G hangt af van de keuze der 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 tot en met 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 $\phi = x_1$ 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 der vergelijking meer in detail. Laat de irrationaliteit θ wortel zijn van een irreducibele, d.w.z. niet in factoren ontbindbare, vergelijking

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

waarbij de b_i rationaal bekend zijn (vergelijk (14) t/m (16)). Laat (28) als wortels hebben $\theta = \theta^{(1)}, \theta^{(2)}, \dots, \theta^{(m)}$.

Laat door adjunctie van θ_i de groep der 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 iedere 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 (dat wil zeggen dat H een normaaldeler is van G , dit begrip werd door Galois ingevoerd) dan zijn alle $\theta^{(i)}$ rationaal bekend zodra één ervan geadjungeerd is. Omgekeerd als alle $\theta^{(i)}$ rationaal uitdrukbaar zijn in één der $\theta^{(i)}$, dan reduceert adjunctie van één der $\theta^{(i)}$ de groep G der vergelijking tot een normale ondergroep (normaaldeler) H . Met dit begrippenapparaat was Galois in staat het probleem op te lossen welke n -de graads vergelijkingen oplosbaar zijn met $\sqrt{\quad}$ -vormen. Zo'n vergelijking is namelijk oplosbaar als de accessievelijk geadjungeerde θ 's wortels zijn van de vergelijkingen van de vorm

$$(29) \quad t^n - A = 0 \quad (\text{dan } \theta = \sqrt[n]{A})$$

waarbij A rationaal is in de coëfficiënten en de reeds geadjungeerde θ 's. Men kan zich beperken tot priemgetallen n (want als $n = p_1 p_2$, dan $\sqrt[n]{\quad} = \sqrt[p_1]{\quad} \sqrt[p_2]{\quad}$). Galois veronderstelde nu dat de p -de eenheidswortels reeds geadjungeerd zijn (immers sinds Gauss was bekend dat deze met behulp van $\sqrt{\quad}$ -vormen geschreven kunnen worden) en hij merkte op: als θ oplossing is van

$$(30) \quad g(t) = t^p - A = 0$$

en $\alpha_1, \dots, \alpha_p$ zijn de p -de eenheidswortels, dan zijn de wortels van (30): $\theta^{(1)} = \alpha_1 \theta, \theta^{(2)} = \alpha_2 \theta, \dots, \theta^{(p)} = \alpha_p \theta$. De wortels van (30) zijn dus rationaal uitdrukbaar in één wortel van (30); adjunctie van θ reduceert G tot een normale ondergroep H van G . Galois toonde aan dat de index van H in G gelijk is aan p . Hij merkte ook op dat, omgekeerd, als G een normale ondergroep H heeft met index p , er een p -demachts wortel θ geadjungeerd kan

worden zodat de groep G tot de groep H reduceert.

Hiermee kon Galois het criterium voor oplosbaarheid met $\sqrt{}$ -vormen formuleren: Een vergelijking $f(x) = 0$ is oplosbaar met $\sqrt{}$ -vormen als de Groep G van de vergelijking een decompositie in ondergroepen $H_0, \dots, H_k$ toelaat, waarbij $(1) = H_0 \subset H_1 \subset \dots \subset H_{k-1} \subset H_k = G$, zodat iedere H_i een normale ondergroep van H_{i+1} is met index p_i , p_i priem. De p_i zijn de priemfactoren van de orde van G .

ONTWIKKELING VAN DE GALOISTHEORIE NA GALOIS

Het duurde enige tijd voordat de betekenis van Galois' werk erkend werd. In 1852 verscheen een uiteenzetting van Galois' ideeën door Enrico Betti (1823-1892) in het italiaans; Betti leverde bewijzen voor een aantal uitspraken die Galois zonder volledig bewijs had geponeerd. Charles Hermite (1822-1901), J.A. Serret (1819-1885), Leopold Kronecker (1823-1891) en anderen toonden interesse voor Galois' werk. De derde editie (1866) van Serret's *Cours d'Algèbre Supérieure* was het eerste leerboek waarin Galois' theorie werd behandeld. Serret voltooide vele bewijzen van Galois, maar werkte de theorie nauwelijks verder uit. Zijn publicatie bracht tenslotte de verdiende algemene bekendheid voor Galois' werk.

Nog belangrijker voor Galois' theorie was het *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 nu toe bekende theorie van permutatie-groepen en van vergelijkingen. Het bevatte ook vele originele bijdragen van Jordan zelf. Met de publicatie van Serret en Jordan was Galoistheorie, in de vorm als we hierboven hebben aangegeven, een geaccepteerd en belangrijk onderdeel van de algebra geworden.

De Galoistheorie heeft in de daarop volgende 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 de relaties, die

voordien omschreven werden met termen als "*rationaal uitdrukbaar in*" te verduidelijken.

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

Deze drievoudige ontwikkeling verliep geleidelijk - in tegenstelling tot de veranderingen in de theorie teweeggebracht door Lagrange en Galois. Het is moeilijk om, zonder te veel in detail te treden, deze ontwikkeling precies te vervolgen. We volstaan daarom met een globale beschrijving ervan.

Galois' oplossing van het centrale probleem der 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 gepreciseerd kon worden. Galois zelf onderzocht al het geval waarbij de graad der 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 $\sqrt{\quad}$ -vormen eigenlijk slechts een speciale eigenschap van de groep van de vergelijking of van de aard der te adjungeren irrationaliteiten was. Men ging zich interesseren voor de structuur van de groep der vergelijking en zijn ondergroepen in het algemeen, en 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 mede mogelijk gemaakt door de opkomst van het begrip *lichaam*. In het voorgaande 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 -de graads vergelijking, en in zekere hulpgrootheden $\theta_1, \dots, \theta_k$. Dat wil zeggen dat ϕ en ψ uit de a 's en θ 's gevormd zijn door optelling, aftrekking, vermenigvuldiging en deling (mits niet door 0). Dat houdt dan weer in dat ook $\phi + \psi$, $\phi - \psi$, $\phi \cdot \psi$ en $\frac{\phi}{\psi}$ (mits $\psi \neq 0$) rationaal uitdrukbaar zijn in de a 's en de θ 's rationaal uitdrukbare grootheden (ofwel de *bekend veronderstelde* grootheden) vormen dus een systeem dat gesloten is onder de vier arithmetische

bewerkingen - ze 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 splitslichaam van f genoemd). De bovengeschetste theorie van Galois kan men dus her-interpreteren het behulp van het begrip lichaam: Eerst wordt gevormd het lichaam der vormen die rationaal uitdrukbaar zijn in de coëfficiënten der vergelijking. Zo nodig worden eenheidswortels geadjungeerd; het zo ontstane lichaam wordt *grondlichaam* genoemd. Dit grondlichaam wordt door successieve adjunctie uitgebreid tot het tenslotte gelijk is aan het splitslichaam. De lichamen die door adjunctie ontstaan zijn deellichamen van het splitslichaam.

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 der 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. Ieder 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 1850'er jaren 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 gebracht met Galoistheorie. 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 der twintigste 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 Galois -

theorie werden vergelijkingen gebruikt om over de permutaties van hun wortels te kunnen praten; deze permutaties vormden de groepen waarmee de structuur van de lichaamsuitbreidingen beschreven kon worden. Om tot een zuivere theorie van lichamen te komen moesten deze groepen gedefinieerd worden onafhankelijk van vergelijkingen. Dit bleek nu mogelijk doordat de permutaties der wortels opgevat kunnen worden als automorfismen van het splijtlichaam. Zij f een vergelijking met grondlichaam F en wortels $x_1, \dots, x_n$. Het splijtlichaam (het lichaam der rationale vormen in de x_i) zij M . Men gaat eenvoudig na dat ieder automorfisme van M dat F elementsgewijs vast-laait, de x_i permuteert. Omgekeerd, een permutatie π uit de groep der vergelijking (dus een "toegestane" permutatie der wortels) induceert op M een automorfisme dat F elementsgewijs vast-laait. 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 van een vergelijking zo geïnterpreteerd kan worden is al bij Dedekind aanwezig; het werd gemeengoed in de eerste decennia der twintigste eeuw.

Hiermee was de weg vrij voor een opvatting van de Galoistheorie als theorie van lichamen en bijbehorende automorfismengroepen. Gedurende de negentiende 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 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, publicatie in 1938-1942).

SLOT

We hebben in het bovenstaande in grote lijnen geschetst hoe zich uit de studie van vergelijkingen de Galoistheorie heeft ontwikkeld. We willen het overzicht besluiten met twee algemene opmerkingen:

De ontwikkeling der Galoistheorie is in zeker opzicht typerend voor de ontwikkeling der wiskunde in de afgelopen periode van ca. honderd 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 al 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 der permutatiegroepen. De nieuwe beschouwingswijze maakt het mogelijk om anderszins nauwelijks formuleerbare eigenschappen te omschrijven (bijvoorbeeld de normaaldeeler-eigenschap); zij maakt het ook mogelijk de resultaten aanmerkelijk te generaliseren. Dit proces nu, het bestuderen van gestuctureerde verzamelingen, valt op vele andere gebieden der wiskunde in de laatste honderd 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 der Galoistheorie geeft ook een fraai voorbeeld van wat er zo al met wiskundige problemen gebeuren kan; hoe de probleemstellingen in de wiskunde zich kunnen wijzigen. Voor het probleem van het bepalen van wortels van een n -de graads vergelijking werd, voor $n < 4$, een oplossing gevonden. Voor $n = 4$ had deze oplossing, wegens de ingewikkeldheid, al nauwelijks meer praktische waarde; voor de feitelijke berekening der 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 wel oplosbaar, werd beantwoord, maar het antwoord had praktisch geen waarde, noch voor de bepaling of een gegeven vergelijking oplosbaar is, noch voor de feitelijke oplossing ervan. 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, te speciaal voor het ontwikkelde begrippenapparaat; de vergelijkingen werden geheel losgelaten, de permutaties der wortels werden automorfismen van de lichamen. Of en hoe de vraagstelling zich in de Galois theorie verder gewijzigd heeft of zich nog wijzigen zal, past niet meer in deze historisch bespreking; daarover vergelijk men de andere voordrachten in de cursus.

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

KIERNAN, B.M. *"The Developement of Galois Theory from Lagrange to Artin"* in *Archive for History of Exact Sciences* 8 (1971/2) pp 40-154;

en in een onmisbare aanvulling op het voorgaande artikel, namelijk

WAERDEN, B.L. van der, *"Die Galois-Theorie von Heinrich Weber bis Emil Artin"* in *Archive for History of Exact Sciences* 9 (1972/3) pp 240-248.