

# Het inzicht van Galois

---

## 1. OPLOSBAARHEID

Kun je de nulpunten vinden van de polynoom  $x^2 - 5x + 6$ ? Ongetwijfeld. Met onderbouw wiskunde is het al vrij eenvoudig om erachter te komen dat 2 en 3 beiden nulpunten zijn van dit polynoom.

In dit geval heb je meerdere manieren waarop je de nulpunten kunt vinden. De eerste stap die je neemt is waarschijnlijk dat je een vergelijking maakt van de vorm  $x^2 - 5x + 6 = 0$ . Degene met enige ervaring is waarschijnlijk handig genoeg om tot de volgende oplossing te komen:

$$\begin{aligned}x^2 - 5x + 6 &= 0 \\(x - 2)(x - 3) &= 0 \\(x - 2) = 0 \text{ of } (x - 3) &= 0 \\x = 2 \text{ of } x = 3\end{aligned}$$

Wat we hier doen heet *ontbinden in (lineaire) factoren*. We vinden de oplossing door te zoeken naar getallen waarvan het product en de som de coëfficiënten van de polynoom oplevert. Als we de nulpunten beschrijven met  $a_1$  en  $a_2$  dan kunnen we dat als volgt uitdrukken:

$$\begin{aligned}(1) \quad & (a_1 + a_2) = 5 \\(2) \quad & a_1 a_2 = 6.\end{aligned}$$

Dit is een stelsel van vergelijkingen dat zich dikwijls zo eenvoudig laat oplossen dat leerlingen deze leren oplossen op intuïtieve wijze. Voor  $a_1 = 2$  en  $a_2 = 3$  vinden we inderdaad de coëfficiënten van de polynoom. De meeste leerlingen hebben ook een andere aanpak geleerd. Voor de algemene tweedegraadsvergelijking  $Ax^2 + Bx + C = 0$  leren middelbare scholieren de nulpunten:

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Wat we in deze formule zien is dat we de nulpunten van een tweedegraadsvergelijking kunnen uitdrukken in de coëfficiënten van de bijbehorende polynoom, door  $+$ ,  $-$ ,  $,$ ,  $:$  en worteltrekken. Omgekeerd zagen we in het vorige voorbeeld dat we de coëfficiënten van een polynoom kunnen uitdrukken in relaties tussen de nulpunten. We noemen een vergelijking *oplosbaar* als dit mogelijk is. Je kunt dan dus een exacte oplossing bepalen. Voor vergelijkingen tot en met de vierde graad is dit altijd mogelijk, maar in de tijd van Galois was inmiddels bekend dat vergelijkingen van de vijfde graad of hoger in het algemeen niet oplosbaar zijn.

De algemene oplossing voor de tweedegraadsvergelijking is al sinds de oudheid bekend. Dankzij het werk van Gerolamo Cardano en Nicolo Fontana Tartaglia waren de algemene oplossingen voor de derde- en vierdegraadsvergelijking inmiddels ook al bekend. Maar in de eeuwen na deze vondsten begon men te vermoeden dat een algemene oplossing voor vijfdegraadsvergelijkingen niet bestaat. Het lukte namelijk maar niet om deze te vinden. In 1824 bewees Niels Hendrik Abel dat deze algemene oplossing inderdaad niet mogelijk was.

Dit wil natuurlijk niet zeggen dat het dan nooit mogelijk is om uit de coëfficiënten van een vijfdegraadspolynoom de nulpunten te vinden, soms is dat prima

mogelijk. Hoewel dit proces waarschijnlijk vaak niet eenvoudig zal zijn. Zo blijkt dat  $x^5 - x^4 - x + 1 = 0$  prima oplosbaar is, maar  $x^5 - 6x + 3 = 0$  niet. Het probleem is dat niemand een manier kon bedenken om oplosbare vergelijkingen te onderscheiden van niet oplosbare vergelijkingen.

**Opg. 1** — Los de onderstaande vergelijkingen op

1.  $x^4 - x^2 - 1 = 0$ . Gebruik de abc-formule om de reële nulpunten te vinden.
2.  $x^5 - x = 0$
3. Herleid de abc-formule uit de algemene tweedegraadsvergelijking  $ax^2 + bx + c$ .
4. Probeer zover mogelijk te komen met  $ax^3 + bx^2 + cx + d = 0$ . Wat maakt dit moeilijker dan de vorige vraag?

## 2. SYMMETRIËN VAN NULPUNTEN

Het was de tragisch jong gestorven Évariste Galois die kort voor zijn dood in 1832 het probleem van oplosbaarheid het hoofd bood. Het inzicht dat Galois daarbij had wordt door wiskundigen terecht omschreven als een diep inzicht. Galois introduceerde als oplossing voor een zeer concrete vraag een zeer abstracte vorm van wiskunde, en een nieuwe wiskundige structuur: *de groep*. Om precies te zijn gebruikte hij symmetriegroepen.

Het verbaast mensen dat symmetriegroepen hun oorsprong vinden bij de vraag naar de oplosbaarheid van polynomiale vergelijkingen. Symmetrie is duidelijk toepasbaar op meetkundige problemen, maar wat heeft symmetrie met polynomen te maken? Dat Galois symmetriën beschouwde werd ingegeven door een handige ontdekking van de franse wiskundige Viète.

Viète sprak over *elementaire symmetrische relaties* tussen nulpunten:

$$\begin{aligned} s_1 &= a_1 + a_2 + \dots + a_n \\ s_2 &= a_1a_2 + a_1a_3 + \dots + a_1a_n + a_2a_3 + a_2a_4 + \dots + a_{n-1}a_n \\ s_3 &= a_1a_2a_3 + a_1a_2a_4 + \dots + a_1a_2a_n + a_1a_3a_4 + a_1a_3a_5 + \dots + a_{n-2}a_{n-1}a_n \\ &\vdots \\ s_n &= a_1a_2 \cdots a_{n-1}a_n \end{aligned}$$

Relaties waarin je de  $a_i$  vrij kunt verwisselen zonder dat de relatie verandert. Een eenvoudig voorbeeld is dat  $x + y + z = y + z + x = y + x + z$  voor alle waarden van  $x, y$  en  $z$ . We kunnen de elementaire symmetrische relaties terugvinden als coëfficiënten van het polynoom

$$(x - a_1)(x - a_2)(x - a_3) \cdots (x - a_{n-1})(x - a_n),$$

met de nulpunten  $a_1, \dots, a_n$ .

### Opg. 2 — Elementaire symmetrische relaties

Dat we deze elementaire relaties als coëfficiënten terugvinden in de bovenstaand-  
het polynoom vereist enige verificatie. Daarom werken we een aantal voorbeel-  
den van polynomen uit, om te begrijpen wat hier bedoeld wordt.

1. Bepaal de coëfficiënten van het polynoom met nulpunten  $a_1 = 1$ ,  $a_2 = 3$   
en  $a_3 = -2$ , gegeven door  $(x - 1)(x + 2)(x - 3)$ , door de haakjes weg te  
werken
2. Vermenigvuldig het polynoom  $(x - a_1)(x - a_2)(x - a_3)$  uit en vereenvou-  
dig zo ver mogelijk door. Vind je de elementaire symmetrische relaties van  
Viète terug?
3. Bepaal  $s_2$  voor de algemene vijfdegraadspolynoom  $(x - a_1)(x - a_2)(x -$   
 $a_3)(x - a_4)(x - a_5)$ .
4. Beschouw de algemene tweedegraadsvergelijking  $x^2 + Ax + B$ . Bepaal de  
waarden  $A$  en  $B$  in termen van  $s_1$  en  $s_2$ .

Als opgave 2.4 gelukt is dan is duidelijk dat de algemene tweedegraadsvergelij-  
king, met nulpunten  $a_1$  en  $a_2$  geschreven kan worden als:

$$(x - a_1)(x - a_2) = x^2 - (a_1 + a_2)x + (a_1 a_2) = x^2 - s_1 x + s_2.$$

Dit is meer dan een algebraïsch handigheidje. Het betekent dat we aan elke  
tweedegraadsvergelijking kunnen aflezen wat de waarden van  $s_1$  en  $s_2$  moeten  
zijn. Bijvoorbeeld voor het polynoom  $x^2 + 4x - 2$  vinden we:

$$\begin{aligned} a_1 + a_2 &= -4 \\ a_1 a_2 &= 2 \end{aligned}$$

Nu hebben we gezien dat dit in specifieke gevallen handig is, maar ervaring leert  
dat dit stelsel inspecteren zeker niet altijd de nulpunten oplevert. De handigheid  
ligt dan ook niet in wijze waarop wij gewend zijn dit stelsel te gebruiken, maar  
in de eigenschap dat elke symmetrische relatie tussen  $a_1$  en  $a_2$  te schrijven is in  
termen van  $s_1$  en  $s_2$ . Om te zien hoe Galois deze eigenschap toepaste, gebruiken  
we symmetrische relaties om de nulpunten van een tweedegraadsvergelijking te  
vinden.

We bekijken hiervoor eerst de handig gekozen relatie  $a_1^2 + a_2^2$ , deze is volledig  
symmetrisch. Het verwisselen, of *permuteren*, van  $a_1$  en  $a_2$  laat de uitkomst on-  
veranderd. We zeggen dat de relatie *behouden* blijft onder elke permutatie. Merk  
nu op:

$$a_1^2 + a_2^2 = (a_1 + a_2)^2 - 2a_1 a_2 = s_1^2 - 2s_2$$

De waarde van  $a_1^2 + a_2^2$  kenden we aanvankelijk niet, maar omdat we weten dat  
 $s_1 = -4$  en  $s_2 = 2$  vinden we nu:

$$a_1^2 + a_2^2 = (-4)^2 - 2(2) = 12.$$

En zo kunnen we de waarde bepalen van uitdrukkingen waarin nulpunten voor-  
komen, ook als de nulpunten nog onbekend zijn. Deze relatie komt voornamelijk  
uit de lucht vallen, maar zoals in opgave 3 zal blijken is deze gekozen met een  
specifiek doel in gedachten.

### Opg. 3 — Symmetrie en tweedegraadsvergelijkingen

Om het nut van symmetrische relaties te illustreren onderzoeken we enkele relaties van een tweedegraadsvergelijking.

1. Beschouw de vergelijking  $x^2 + Ax + B = 0$ . Laat zien dat geldt  $a_1^2 + a_2^2 = A^2 - 2B$ .
2. De discriminant is voor tweedegraadsfuncties gedefinieerd als  $(a_1 - a_2)^2$ . Gebruik het resultaat uit de vorige opgave om aan te tonen dat dit overeenkomt met de middelbareschool formule. Ofwel dat:

$$(a_1 - a_2)^2 = A^2 - 4B.$$

3. Gebruik de discriminant, tezamen met  $a_1 + a_2 = -A$  om te laten zien dat  $a_1 = \frac{-A + \sqrt{A^2 - 4B}}{2}$  en dat  $a_2 = \frac{-A - \sqrt{A^2 - 4B}}{2}$ .

Door te kijken naar handig gekozen symmetrische relaties hebben we de nulpunten van de tweedegraadsvergelijking gevonden uit de coëfficiënten van het polynoom. Het belangrijkste punt om daarbij in gedachte te houden is dat we op basis van de symmetrische relatie  $(a_1 - a_2)^2$  door worteltrekken de waarde van een niet symmetrische relatie  $(a_1 - a_2)$  konden vinden. Galois ontdekte dat dit alleen mogelijk is bij oplosbare vergelijkingen. We gaan daar in paragraaf 4 wederom gebruik van maken. De symmetrieën in de nulpunten zijn daarmee de sleutel tot het vraagstuk over oplosbaarheid. Of een vergelijking oplosbaar is wordt prijsgegeven door de structuur van de nulpuntsymmetrieën. Maar wij zijn nog geen structuur in symmetrieën tegengekomen. Galois had er zelf ook niet van gehoord, hij introduceerde de *groep* om die structuur te beschrijven.

### 3. GALOISGROEPEN EN LICHAAMSUITBREIDIGNEN

Kijk nu naar de vergelijking  $x^4 - x^2 - 2 = 0$ , met de nulpunten  $a_1 = \sqrt{2}$ ,  $a_2 = -\sqrt{2}$ ,  $a_3 = i$  en  $a_4 = -i$ . Welke permutaties kunnen we op deze nulpunten toepassen, zodat geen enkel nulpuntrelatie verandert? Omdat  $a_1 + a_2 = 0$  en  $a_1 a_2 = -2$  invariant zijn onder alle permutaties van  $a_1$  en  $a_2$ , zijn alle symmetrische relaties invariant onder permutaties van  $a_1$  en  $a_2$ . Ook voor  $a_3$  en  $a_4$  geldt dat  $a_3 + a_4 = 0$  en  $a_3 a_4 = 1$  invariant zijn onder permutaties van  $a_3$  en  $a_4$ . Permutaties die  $a_1$  met  $a_2$  verwisselen en permutaties die  $a_3$  met  $a_4$  verwisselen houden dus alle relaties in stand.

Maar verwisselen we  $a_1$  en  $a_3$ , dan ontstaan er problemen. Relaties zoals  $a_1^2 + a_3^2 = 1$  blijven behouden, maar relaties als  $a_1^2 - a_3^2 = 3$  veranderen in  $a_3^2 - a_1^2 = -3$ . Sterker nog, bij de relatie  $a_1 + a_2 = 0$  krijgen we niet eens een rationale uitkomst:  $a_3 + a_2 = i - \sqrt{2}$ .

### Opg. 4 — Nulpuntrelaties van $x^4 - x^2 - 2 = 0$

In deze opgave onderzoeken we permutaties. Deze staan in *cykelnotatie* genoemd. De cykel (12) houdt in dat je 1 verwisselt met 2. De notatie (123) zou

inhouden dat je 1 verwisselt met 2, 2 verwisselt met 3 en 3 verwisselt met 1. Het is alsof je de elementen tussen haakjes in een rondje doorschuift. De term *cykel* heeft betrekking op dit doorschuiven (denk aan het engelse *cycle*).

1. We schrijven de nulpunten van  $x^4 - x^2 - 2 = 0$  als  $a_1, a_2, a_3$  en  $a_4$ . Bedenk enkele rationale relaties tussen de nulpunten. Probeer de permutaties (12) en (34) uit. Onderzoek of jouw relaties behouden blijven. Deze relaties moeten vergelijkingen zijn in rationale getallen, van eerstegraad of hoger.
2. Pas de permutatie (123) toe op  $a_1^2 + a_2^2 + a_3^2 + a_4^2$ . Noteer de nieuw verkregen relatie en bereken het resultaat.
3. Leg uit dat de permutaties in de groep  $V_4 = \{e, (12), (34), (12)(34)\}$  alle relaties behouden voor de nulpunten van  $x^4 - x^2 - 2 = 0$ , en dat er geen anderen zijn. Hierbij duidt  $e$  de *identiteit* aan, waarmee we bedoelen: niks verwisselen.

De permutatiegroep  $V_4 = \{e, (12), (34), (12)(34)\}$  noemen we de *galoisgroep* van de vergelijking  $x^4 - x^2 - 2 = 0$ , de verzameling van relatiebehoudende permutaties. Voor elke vergelijking kunnen we zo'n groep bepalen. Voor de vergelijking  $x^2 - 5x + 6 = 0$ , in ons eerste voorbeeld, met nulpunten 2 en 3 hebben we enkele symmetrische relaties gezien. Maar de enige permutatie die *alle* relaties in 2 en 3 behoudt is  $e$ .

Het is alsof je jouw klas een cover laat horen van een liedje. Is dit zoals bij de nulpunten van  $x^2 - 5x + 6 = 0$  in een bekende taal, dan zullen er leerlingen zijn die horen dat je niet het origineel draait (zoals  $a_1 - a_2 = 1$ ), en er zullen leerlingen zijn die dit niet horen (zoals  $a_1 + a_2 = 5$ ). Je zult niet de hele klas voor de gek houden. Maar als je een liedje laat horen in een onbekende taal, dan zullen de leerlingen het verschil niet horen. In deze taal zijn zij veel minder gevoelig voor subtiele verschillen in klank en accent. Nu kun je plots wel de hele klas voor de gek houden. Dit was het geval voor de nulpunten van  $x^4 - x^2 - 2 = 0$ . Voor de rationale relaties waren de reële nulpunten als liedjes in een vreemde taal, die konden we vrij permuteren. De complexe nulpunten waren als liedjes in een andere vreemde taal, en ook die konden we vrij verwisselen. Reële en complexe nulpunten konden we echter niet met elkaar verwisselen, dit zou altijd wel opgemerkt worden door minimaal één leerling. In deze context vertelt de galoisgroep ons welke covers en originelen we kunnen verwisselen en welke niet.

Als we de leerlingen nu  $\sqrt{2}$  leren, dan zullen zij wel het verschil horen tussen  $\sqrt{2}$  en  $-\sqrt{2}$ . Onze galoisgroep reduceert tot  $S_2 = \{e, (34)\}$ . Dit komt overeen met  $\sqrt{2}$  toevoegen aan ons grondlichaam  $\mathbb{Q}$ . We noteren deze *lichaamsuitbreiding* als  $\mathbb{Q}(\sqrt{2})$ . Leren wij onze klas nu ook  $i$ , dan horen zij ook het verschil tussen  $i$  en  $-i$ . We werken nu in de lichaamsuitbreiding  $\mathbb{Q}(\sqrt{2}, i)$ , en onze galoisgroep is  $\{e\}$ . De verzameling  $\mathbb{Q}(\sqrt{2}, i)$  is de kleinste lichaamsuitbreiding die alle nulpunten bevat, en in dit getallensysteem ontbindt onze vergelijking dus in lineaire factoren  $(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i) = 0$ . We noemen dit het *splijtlichaam* van het polynoom  $x^4 - x^2 - 2$ .

We zien dat als een vergelijking ontbindt in factoren de galoisgroep slechts de identiteit bevat. Om zover te komen hebben we ons getallensysteem steeds uitgebreid met een nulpunt van de vergelijking, we verkregen  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, i)$ . Dit kwam overeen met de *keten* van galoisgroepen  $V_4 \triangleright S_2 \triangleright \{e\}$ . Dit idee is centraal in de theorie van Galois. Er is een één op één relatie tussen een keten van

lichaamsuitbreidingen en een keten van galoisgroepen. In dit geval konden wij de galoisgroep eenvoudig bepalen omdat de nulpunten bekend waren. In de volgende paragraaf bekijken we een vergelijking waarvan we de nulpunten nog niet weten, en waarbij het bestuderen van de structuur in de galoisgroep ons juist informatie over de nulpunten geeft. De eindige galoisgroep is namelijk veel eenvoudiger te bestuderen dan de verschillende, oneindig grote getallensystemen.

### Opg. 5 — De galoisgroep van $x^3 - 2 = 0$

Beschouw het polynoom  $x^3 - 2 = 0$ . Voor dit polynoom kunnen we ook de nulpunten bepalen en kijken naar de symmetrieën die we op de nulpunten kunnen toepassen.

1. Bepaal alle drie de oplossingen van de vergelijking  $x^3 - 2 = 0$
2. Bedenk enkele relaties tussen de nulpunten van  $x^3 - 2 = 0$ . Welke permutaties behouden de relaties en welke niet?
3. Beschrijf de galoisgroep van  $x^3 - 2 = 0$ . Met welke symmetriegroep komt dit overeen?
4. Bevat de lichaamsuitbreiding  $\mathbb{Q}(\sqrt[3]{2})$  alle oplossingen van  $x^3 - 2 = 0$ ? Wat is de galoisgroep van  $x^3 - 2$  over dit lichaam?

#### 4. EEN DERDEGRAADS VERGELIJKING OPLOSSEN

Voor een vergelijking als  $x^3 - 3x - 1 = 0$  kennen we de nulpunten niet, maar we kunnen proberen de galoisgroep in kaart te brengen. We zullen zien hoe dit ons de nulpunten op kan leveren. Laat  $a_1, a_2$  en  $a_3$  de nulpunten zijn van de vergelijking. De groep van alle permutaties op drie nulpunten is

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Dit zou best de galoisgroep van onze vergelijking kunnen zijn, voorlopig kunnen we dat nog niet zeggen. Allereerst bekijken we de elementaire symmetrische relaties, gegeven door:

$$\begin{aligned} s_1 &= a_1 + a_2 + a_3 = 0 \\ s_2 &= a_1a_2 + a_1a_3 + a_2a_3 = -3 \\ s_3 &= a_1a_2a_3 = 1 \end{aligned}$$

We kunnen andere symmetrische relaties uitdrukken in termen van deze relaties en daardoor de waarde bepalen. Een natuurlijke keuze daarvoor is de discriminant, gegeven door:

$$\Delta = (a_1 - a_2)^2(a_1 - a_3)^2(a_2 - a_3)^2$$

Eerder bekeken we deze functie ook al voor de kwadratische vergelijking, toen we aantoonde dat  $(a_1 - a_2)^2 = A^2 - 4B$ . We hebben die toen niet zo benoemd, maar waarschijnlijk had je deze al als dusdanig herkend. Het is veel werk om de

discriminant te herschrijven in termen van  $s_1, s_2$  en  $s_3$ . Gelukkig is er software die dat voor ons kan doen. We vinden:

$$\Delta = -4s_1^3s_3 + 4s_2^3 + 27s_3^2 - s_1^2s_2^2 - 18s_1s_2s_3.$$

En omdat we de waarden van de elementaire symmetrische relaties weten kunnen we berekenen dat  $\Delta = (-4)(-3)^3 - 27 \cdot 1^2 = 81$ .

Merk nu op dat  $\sqrt{\Delta} = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3) = 9$  een rationale relatie is in de nulpunten. Dat  $\sqrt{\Delta}$  een rationaal getal is gebeurt lang niet altijd. Wat zegt dat in dit geval?

Allereerst geldt dat  $A_3 = \{e, (123), (132)\}$  de galoisgroep is van de vergelijking. Zonder de nulpunten vraagt het bepalen van de galoisgroep creatieve logische argumenten. In dit geval is er een stelling gebruikt die deze conclusie onderbouwt. Oftewel, door het nemen van een wortel reduceerden we  $S_3$  naar de galoisgroep  $A_3$ . In de vorige paragraaf zagen we dat dit overeenkomt met een lichaamsuitbreiding. Maar omdat het worteltrekken wederom een rationale relatie opleverde, hoefden wij onze leerlingen geen nieuwe dingen te leren om hen het verschil tussen een cover en het origineel te laten horen. We begeven ons dus nog steeds in de verzameling van rationale getallen.

**Opg. 6** — We gaan na dat de groep  $A_3$ , die een *alternerende* groep heet, inderdaad een ondergroep is van  $S_3$  en onderzoeken de werking van  $A_3$  op  $\sqrt{\Delta}$ .

1. Laat zien dat  $A_3$  een ondergroep is van  $S_3$ .
2. Laat zien dat  $\sqrt{\Delta}$  invariant is onder werking van  $A_3$ .
3. Probeer alle permutaties van  $S_3$  uit op  $\sqrt{\Delta}$  en bepaal de uitkomst. Groepeer de permutaties die dezelfde uitkomst geven.

Herinner je nu dat we zoeken naar een manier om via een machtswortel naar een relatie te komen die alleen onder de identiteit invariant is. Het zal zo blijken dat dit kan in één stap. We hebben onze leerlingen dan geleerd om het verschil tussen origineel en cover te herkennen in alle gevallen. In de praktijk betekent dit dat we een splijtlichaam hebben gevonden voor onze vergelijking.

Er is geen standaard manier om oplossingen voor vergelijkingen te vinden met behulp van galoistheorie. Het zal vaak aankomen op handigheden. In dit geval is de handigheid die wij nodig hebben voor de laatste stap het stelsel van de volgende vergelijkingen:

$$\begin{aligned} f_1^3 &= (a_1 + a_2 + a_3)^3 \\ f_2^3 &= (a_1 + \zeta a_2 + \zeta^2 a_3)^3 \\ f_3^3 &= (a_1 + \zeta^2 a_2 + \zeta a_3)^3 \end{aligned}$$

met  $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ , met  $\zeta^3 = 1$ . We lichten een aantal eigenschappen van deze vergelijkingen toe die ons van pas gaan komen bij het vinden van de nulpunten van  $x^3 - 3x - 1 = 0$ .

**Opg. 7** — In deze opgave onderzoeken we de eigenschappen van  $\zeta$ , de derde eenheidswortel.

1. Laat zien dat  $\zeta^3 = 1$ .
2. Laat zien dat  $\zeta^2 = \bar{\zeta}$ , de complexe geconjugeerde van  $\zeta$  en dat  $\zeta + \bar{\zeta} = -1$ .
3. Laat zien dat  $\zeta = e^{\frac{2\pi i}{3}}$ .

Ten eerste geldt er dat  $(123)[f_2] = a_3 + \zeta a_1 + \zeta^2 a_2 = \zeta f_2$ . Op dezelfde manier geldt dat  $(132)[f_2] = \zeta^2 f_2$ . De relatie is dus zo gekozen dat permutaties uit  $A_3$  op  $f_2$  overeenkomen met vermenigvuldigen met een macht van  $\zeta$ . Er geldt dat  $(123)[f_2^3] = (\zeta f_2)^3 = \zeta^3 f_2^3 = f_2^3$ . En op dezelfde manier geldt er  $(132)[f_2^3] = (\zeta^2 f_2)^3 = \zeta^6 f_2^3 = f_2^3$ . Met andere woorden,  $f_2^3$  is invariant onder de permutaties van  $A_3$ . Voor  $f_3^3$  kunnen we hetzelfde argument construeren, en we zagen in opgave 6 al dat dit ook waar was voor  $\sqrt{\Delta}$ .

**Opg. 8** — Laat zien dat  $f_3^3$  inderdaad invariant is onder permutaties van  $A_3$ .

Omdat  $f_2^3$  en  $f_3^3$  niet volledig symmetrisch zijn kunnen we slechts het symmetrische deel van deze vergelijkingen uitdrukken in termen van  $s_1, s_2$  en  $s_3$ . Het niet symmetrische deel blijkt echter uit te drukken in termen van  $\sqrt{\Delta}$ . Dit betekent dat we  $f_2^3$  en  $f_3^3$  bepalen uit  $s_1, s_2, s_3$  en  $\sqrt{\Delta}$ . Ook nu weer is het lastig werk om deze waarden met de hand te vinden (maar het is leerzaam om het toch te proberen). De computer levert de waarden:

$$\begin{aligned} f_1^3 &= s_1^3 = 0 \\ f_2^3 &= -27\zeta \\ f_3^3 &= -27\zeta^2 \end{aligned}$$

Nemen we nu de derdemachtswortel dan krijgen we:

$$\begin{aligned} f_1 &= a_1 + a_2 + a_3 = 0 \\ f_2 &= a_1 + \zeta a_2 + \zeta^2 a_3 = -3\zeta^{\frac{1}{3}} \\ f_3 &= a_1 + \zeta^2 a_2 + \zeta a_3 = -3\zeta^{\frac{2}{3}} \end{aligned}$$

De relaties  $f_2$  en  $f_3$  zijn alleen onder de identiteit invariant. Het nemen van een derdemachtswortel reduceerde onze galoisgroep tot  $\{e\}$ . Het laatst verkregen stelsel van vergelijkingen is oplosbaar en de oplossing levert de nulpunten van  $x^3 - 3x - 1 = 0$ . De exacte oplossingen zijn een esthetische belediging voor het oog, daarom zullen wij het doen met een benadering van de oplossingen. We vinden  $a_1 \approx -1,532, a_2 \approx 1,878$  en  $a_3 \approx -0,347$ .

**Opg. 9** — Laat zien dat  $f_2$  onder werking van  $A_3$  precies drie verschillende waarden aanneemt.

Merk op dat we aanvankelijk alleen voor de elementaire symmetrische relaties  $s_1, s_2$  en  $s_3$  de waarde wisten. Namelijk  $s_1 = 0, s_2 = -3$  en  $s_3 = 1$ . Die leverden  $\Delta = 81$  op, omdat  $\Delta$  net als  $s_1, s_2$  en  $s_3$  invariant was onder  $S_3$ . Daardoor wisten direct dat  $\sqrt{\Delta} = 9$ , die op diens beurt invariant was onder  $A_3$  (de galoisgroep

van de vergelijking). We kozen handige  $f_2^3$  en  $f_3^3$ , die net als  $\sqrt{\Delta}$  invariant waren onder  $A_3$ . Dit gaf ons op basis van  $\sqrt{\Delta}$  dat  $f_2^3 = -27\zeta$  en  $f_3^3 = -27\zeta^2$ . Ten slotte konden we nu via een derdemachtswortel berekenen wat  $f_2$  en  $f_3$  moesten zijn. Deze laatste waren alleen invariant onder  $e$ , en konden tezamen met  $f_1$  als stelsel van vergelijkingen worden opgelost om de nulpunten te bepalen. Oftewel, deze vergelijking was oplosbaar uit de coëfficiënten door middel van de gewone rekenbewerkingen en machtswortels. Volgens Galois kwam dit juist doordat de gebruikte relaties zo gekozen waren dat ze invariant waren onder de permutaties in de keten  $S_3 \triangleright A_3 \triangleright \{e\}$ . Maar dit geldt echter niet voor zomaar elke keten.

De symmetriegroep  $S_3$  heet in de galoistheorie een oplosbare groep. Dit betekent dat we een keten kunnen construeren die voldoet aan een aantal voorwaarden. We kunnen uit ons proces opmaken welke dat zijn. We zagen in paragraaf 3 dat afdaling in de keten overeenkwam met het uitbreiden van  $\mathbb{Q}$  met nulpunten van een vergelijking. We mondden uiteindelijk uit in  $\{e\}$ , wat overeenkwam met een getallenlichaam waarover de vergelijking ontbond in lineaire factoren. Toch kan dit niet zomaar op elke manier. In opgave 5 zagen we namelijk dat het polynoom  $x^3 - 2$  niet ontbond in lineaire factoren over  $\mathbb{Q}(\sqrt[3]{2})$ , ondanks diens triviale galoisgroep. Dit kwam doordat wel  $\sqrt[3]{2}$ , maar niet de complexe nulpunten  $\zeta\sqrt[3]{2}$  en  $\zeta^2\sqrt[3]{2}$ , in dit lichaam bevat waren. Ondanks dat  $(\sqrt[3]{2})^3 = (\zeta\sqrt[3]{2})^3 = (\zeta^2\sqrt[3]{2})^3 = 2$ , konden we  $\sqrt[3]{2}$  nergens mee verwisselen zonder relaties te schaden. Wel ontbindt  $x^2 - 2$  in lineaire factoren als we  $\mathbb{Q}$  uitbreiden naar  $\mathbb{Q}(\sqrt{2})$ , omdat deze beide nulpunten  $\sqrt{2}$  en  $-\sqrt{2}$  bevat. Na kwadrateren zagen rationale relaties geen verschil meer tussen  $\sqrt{2}^2$  en  $(-\sqrt{2})^2$ . Lichamen uitbreiden zodat polynomen ontbinden in lineaire factoren komt overeen met ketens van zogenaamde *normale* ondergroepen (we zullen hier niet dieper ingaan op de eigenschappen van normale ondergroepen).  $A_3$  was zo een ondergroep.

Ook zagen we in opgave 6 en 9 dat we permutaties in groepen konden verdelen op basis van hun werking op relaties. We konden  $S_3$  in tweeën delen omdat de ene helft van de permutaties  $\sqrt{\Delta} = 9$  gaf en de andere helft  $\sqrt{\Delta} = -9$  gaf. Op dezelfde manier konden we  $A_3$  in drieën opdelen om wat de permutaties deden met de waarden van  $f_2$  en  $f_3$ . In oplosbare groepen is het aantal delen waarin we een groep kunnen opdelen altijd priem.

Galois liet zien dat voor de algemene vergelijkingen van graad  $n \geq 5$  de groep  $S_n$  niet oplosbaar is. De ondergroep  $A_n$  is namelijk een noodzakelijke schakel in elke keten die we kunnen construeren uit  $S_n$ , maar daarna kunnen we geen normale ondergroep van  $A_n$  vinden zodat deze uiteenvalt in een priem aantal delen. Dit betekent dat het onmogelijk is om voor een polynoom van graad  $n$  een oplossing in termen van de coëfficiënten te formuleren als deze de galoisgroep  $S_n$  heeft. En dergelijke polynomen bestaan in grote aantallen. Het polynoom  $x^5 - 4x - 1$  is er een voorbeeld van. Per vergelijking zal de galoisgroep uitwijzen of deze oplosbaar is of niet. Als een vergelijking oplosbaar is, dan vertelt de galoisgroep ook hoe dit moet.

Galois beoogde een zeer concrete vraag te beantwoorden. Wanneer is een vergelijking oplosbaar? Hiervoor moest hij een uitstap nemen naar een zeer abstracte hoek van de wiskunde, waarvoor hij de basisstructuur zelf moest formuleren. Op basis van zijn ideeën hebben latere wiskundigen zijn theorie precies kunnen maken. Hoewel het in detail bespreken van oplosbare groepen voor dit stuk te ver voert, liet Galois zien dat we grote wiskundige structuren, de lichamen en

lichaamsuitbreidingen, kunnen bestuderen aan de hand van overzichtelijke eindige groepen. In deze laatste paragraaf hebben we één toepassing hiervan gezien. Galois heeft de wiskunde misschien wel ingrijpender veranderd dan wie dan ook. Zijn wiskunde bleek nuttig in tal van andere gebieden, zoals bijvoorbeeld getaltheorie en cryptografie.

## 5. ANTWOORDEN

## Opg. 1

$$(1) x^4 - x^2 - 1 = 0 \Rightarrow x = \pm \sqrt{\frac{1+\sqrt{5}}{2}} \notin \mathbb{Q}$$

$$(2) x^5 - x = x(x^4 - 1) = x(x^2 - 1)(x^2 + 1) = x(x+1)(x-1)(x+i)(x-i) = 0. \text{ Met } x \in \{0, \pm 1, \pm i\}$$

(3)

$$\begin{aligned} ax^2 + bx + c &= 0 \\ ax^2 + bx &= -c \\ x^2 + \frac{b}{a}x &= -\frac{c}{a} \\ \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} &= -\frac{c}{a} \\ \left(x + \frac{b}{2a}\right)^2 &= -\frac{c}{a} + \frac{b^2}{4a^2} = \frac{b^2 - 4ac}{4a^2} \\ x + \frac{b}{2a} &= \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

## Opg. 2

$$(1) (x-1)(x+2)(x-3) = (x^2 + x - 2)(x-3) = x^3 - 2x^2 - 5x + 6.$$

$$(2) (x-a_1)(x-a_2)(x-a_3) = x^3 - (a_1+a_2+a_3)x^2 + (a_1a_2+a_1a_3+a_2a_3)x - (a_1a_2a_3) = x^3 - s_1x^2 + s_2x - s_3.$$

$$(3) s_2 = -C = a_1a_2a_3 + a_1a_2a_4 + a_1a_2a_5 + a_1a_3a_4 + a_1a_3a_5 + a_1a_4a_5 + a_2a_3a_4 + a_2a_3a_5 + a_2a_4a_5 + a_3a_4a_5$$

$$(4) (x-a_1)(x-a_2) = x^2 - (a_1+a_2)x + a_1a_2 = x^2 - s_1x + s_2.$$

## Opg. 3

(1) Bekend is dat  $-A = a_1 + a_2$  en  $B = a_1a_2$ . Nu zien we dat:

$$a_1^2 + a_2^2 = a_1^2 + a_2^2 + 2a_1a_2 - 2a_1a_2 = (a_1 + a_2)^2 - 2a_1a_2 = A^2 - 2B$$

$$(2) (a_1 - a_2)^2 = a_1^2 + a_2^2 - 2a_1a_2 = A^2 - 2B - 2a_1a_2 = A^2 - 2B - 2B = A^2 - 4B$$

- (3) Bekend is dat  $-A = a_1 + a_2 \Leftrightarrow a_2 = -a_1 - A$  (\*) en  $a_1 = -a_2 - A$  (\*\*)

$$\begin{aligned}(a_1 - a_2)^2 &= A^2 - 4B \\ a_1 - a_2 &= \sqrt{A^2 - 4B} \\ a_1 &= a_2 + \sqrt{A^2 - 4B} \\ a_1^* &= -a_1 - A + \sqrt{A^2 - 4B} \\ 2a_1 &= -A + \sqrt{A^2 - 4B} \\ a_1 &= \frac{-A + \sqrt{A^2 - 4B}}{2}\end{aligned}$$

$$\begin{aligned}(a_1 - a_2)^2 &= A^2 - 4B \\ a_1 - a_2 &= \sqrt{A^2 - 4B} \\ -a_2 &= -a_1 + \sqrt{A^2 - 4B} \\ -a_2^{**} &= a_2 + A + \sqrt{A^2 - 4B} \\ -2a_2 &= A + \sqrt{A^2 - 4B} \\ a_2 &= \frac{-A - \sqrt{A^2 - 4B}}{2}\end{aligned}$$

#### Opg. 4

- (1)  $x^4 - x^2 - 2$  heeft nulpunten  $a_1 = \sqrt{2}$ ,  $a_2 = -\sqrt{2}$ ,  $a_3 = i$ ,  $a_4 = -i$ . Enkele voorbeelden van rationale relaties zijn  $a_1^2 + a_3^2 - 1 = 0$  en  $a_1 + a_2 = 0$ . De relatie  $a_1 + a_4 - \sqrt{2} + i = 0$  is een voorbeeld van een ongeldige relatie, omdat die niet rationaal is. Als we (12) uitproberen op  $a_1^2 + a_3^2 - 1$  dan krijgen we  $a_2^2 + a_3^2 - 1$ . Beiden hebben uitkomst 0. De relatie blijft onveranderd. Maar (24)  $[a_2^2 + a_3^2 - 1] = a_4^2 + a_3^2 - 1$  verandert de uitkomst (reken na) en dus ook de relatie.
- (2)  $(123)[a_1^2 + a_2^2 + a_3^2 + a_4^2] = a_2^2 + a_3^2 + a_1^2 + a_4^2 = 2$ . Het resultaat blijft onveranderd. Deze relatie is volledig symmetrisch en daarom onder alle permutaties invariant.
- (3) Rationale relaties in  $a_1, a_2, a_3$  en  $a_4$  vereisen machten van de nulpunten. Er geldt na machtsverheffing dat  $a_1^2 = a_2^2$  en  $a_1^2 = a_2^2$ . Dus (12) en (34) en hun samenstelling laten rationale relaties onveranderd. Dit zijn de enige permutaties die alle nulpuntrelaties onveranderd laten. Dit geeft de permutatiegroep  $\{e, (12), (34), (12)(34)\} = V_4$ .

#### Opg. 5

- (1) Deze vergelijking heeft  $a_1 = \sqrt[3]{2}$ ,  $a_2 = \zeta \sqrt[3]{2}$ ,  $a_3 = \zeta^2 \sqrt[3]{2}$ .
- (2) Bijvoorbeeld de elementaire symmetrische relaties,  $a_2 a_3 - a_1^2 = 0$ ,  $a_1^3 - a_2^3 = 0$ ,  $a_1^6 a_2^3 - 8 = 0$  en  $a_1^3 - 2 = 0$ . Al deze relaties zijn invariant onder permutatie van de nulpunten.
- (3) De galoisgroep is  $\{e, (12), (13), (23), (123), (132)\}$  en deze komt overeen met  $S_3$ .

- (4) Nee, deze uitbreiding bevat alleen  $\sqrt[3]{2}$ . Het bevat hooguit nog het kwadraat van  $\zeta\sqrt[3]{2}$ , maar we kunnen  $\sqrt[3]{2}$  alleen met zichzelf verwisselen. Ofwel, de galoisgroep is  $\{e\}$ . Toch ontbindt  $x^3 - 2$  niet in lineaire factoren over dit lichaam.

### Opg. 6

- (1) Duidelijk is  $A_3$  een deelverzameling van  $S_3$ , dus  $A_3$  bevat het eenheidselement  $e$ . Omdat  $(123)(132) = e$  geldt dat elk element van  $A_3$  een inverse heeft en dat  $A_3$  gesloten is onder samenstelling. Er volgt dat  $A_3$  een ondergroep is van  $S_3$

(2)

$$\sqrt{\Delta} = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$$

$$(123)\sqrt{\Delta} = (a_2 - a_3)(a_2 - a_1)(a_3 - a_1) = -(a_1 - a_2) \cdot -(a_1 - a_3)(a_2 - a_3) = \sqrt{\Delta}$$

$$(132)\sqrt{\Delta} = (a_3 - a_1)(a_3 - a_2)(a_1 - a_2) = (a_1 - a_2) \cdot -(a_1 - a_3) \cdot -(a_2 - a_3) = \sqrt{\Delta}$$

- (3) De permutaties van  $A_3$  laten  $\sqrt{\Delta}$  onveranderd en laten de waarde daarom gelijk aan 9. We missen nog drie permutaties in  $S_3$  en zien dat:

$$(12)\sqrt{\Delta} = (a_2 - a_1)(a_2 - a_3)(a_1 - a_3) = -(a_1 - a_2)(a_1 - a_3)(a_2 - a_3) = -\sqrt{\Delta} = -9$$

$$(13)\sqrt{\Delta} = (a_3 - a_2)(a_3 - a_1)(a_2 - a_1) = -(a_1 - a_2) \cdot -(a_1 - a_3) \cdot -(a_2 - a_3) = -\sqrt{\Delta} = -9$$

$$(23)\sqrt{\Delta} = (a_1 - a_3)(a_1 - a_2)(a_3 - a_2) = (a_1 - a_2)(a_1 - a_3) \cdot -(a_2 - a_3) = -\sqrt{\Delta} = -9$$

We zien dat  $S_3$  in twee delen uiteen valt.

### Opg. 7

- (1) Uitschrijven levert:  $(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i)^3 = (-\frac{1}{2} + \frac{1}{2}\sqrt{3}i)^2(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) = (\frac{1}{4} - 2 \cdot \frac{1}{4}\sqrt{3}i - \frac{3}{4})(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) = (-\frac{1}{2} - \frac{1}{2}\sqrt{3}i)(-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) = \frac{1}{4} + \frac{3}{4} = 1$

- (2) Uit het vorige onderdeel zagen we dat  $\zeta^2 = (-\frac{1}{2} - \frac{1}{2}\sqrt{3}i) = \bar{\zeta}$ .

- (3) Omdat  $\zeta$  een complex getal is moet deze te schrijven zijn als  $re^{i\theta} = r(\cos\theta + i\sin\theta)$  volgens Euler, voor zekere  $\theta, r \in \mathbb{R}$ . We zien  $r = |\zeta| = 1$  en  $\theta = \arctan\left(\frac{\frac{1}{2}\sqrt{3}}{-\frac{1}{2}}\right) = -\frac{\pi}{3}$ , krijgen we  $\zeta = e^{-\frac{\pi}{3}i} = e^{\frac{2\pi}{3}i}$ .

**Opg. 8**  $(123)f_3^3 = (123)(a_1 + \zeta^2 a_2 + \zeta^4 a_3)^3 = (123)(a_1 + \zeta^2 a_2 + \zeta a_3)^3 = (a_2 + \zeta^2 a_3 + \zeta^4 a_4)^3 = (\zeta f_3)^3 = f_3^3$ . Analoog voor  $(132)f_3^3$ .

### Opg. 9

$$f_3 = -3\zeta^{\frac{2}{3}}$$

$$(123)f_3 = (123)(a_1 + \zeta^2 a_2 + \zeta^4 a_3)$$

$$= (a_2 + \zeta^2 a_3 + \zeta^4 a_1) = \zeta(a_1 + \zeta^2 a_2 + \zeta^4 a_3) = \zeta \cdot -3\zeta^{\frac{2}{3}} = -3\zeta^{\frac{5}{3}}$$

$$(132)f_3 = (123)(a_1 + \zeta^2 a_2 + \zeta^4 a_3)$$

$$= (a_3 + \zeta^2 a_1 + \zeta^4 a_2) = \zeta^2(a_1 + \zeta^2 a_2 + \zeta^4 a_3) = \zeta^2 \cdot -3\zeta^{\frac{2}{3}} = -3\zeta^{\frac{8}{3}}$$