

SYLLABUS ALGEBRA 3  
*voorlopige versie*

PROF. DR G. VAN DER GEER

Korteweg-de Vries Instituut  
Universiteit van Amsterdam  
Science Park 904  
1098 XH Amsterdam  
Versie: 2010

## 1. SYMMETRISCHE FUNCTIES

*permutations sont la metaphysique des équations*

Lagrange\*, 1771

In dit hoofdstuk bestuderen we de invarianten van de werking van de symmetrische groep  $S_n$  op polynoomringen in  $n$  variabelen. De hoofdstelling van de symmetrische functies is het belangrijkste resultaat en zal in het vervolg vaak gebruikt worden.

Laat  $R$  een commutatieve ring met 1 zijn. De symmetrische groep  $S_n$  werkt op  $R[X_1, \dots, X_n]$  door permutatie van de variabelen:

$$f(X_1, \dots, X_n) \mapsto f(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Een polynoom  $f \in R[X_1, \dots, X_n]$  heet *symmetrisch* als  $f$  invariant is onder alle  $\sigma \in S_n$ . Ten duidelijkste zijn alle elementen uit  $R$  invariant, maar interessantere voorbeelden van symmetrische polynomen zijn gemakkelijk te geven; zo zijn

$$\prod_{i=1}^n X_i \quad \text{en} \quad \sum_{i=1}^n X_i^k$$

voor alle  $k \in \mathbb{Z}_{\geq 0}$  ten duidelijkste symmetrische polynomen. Andere voorbeelden worden gegeven door de zogenaamde *elementaire symmetrische polynomen*

$$\begin{aligned} \sigma_1 &= X_1 + X_2 + \dots + X_n, \\ \sigma_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n, \\ \sigma_3 &= \sum_{i < j < k} X_iX_jX_k, \\ &\vdots \\ \sigma_n &= X_1X_2 \cdots X_n. \end{aligned}$$

Dus voor  $1 \leq r \leq n$  is het  $r$ -de elementaire symmetrische polynoom (soms ook wel symmetrische functie genoemd)

$$\sigma_r = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} X_{i_1}X_{i_2} \cdots X_{i_r}.$$

Een belangrijke opmerking is dat deze  $\sigma_r$  op teken na de coëfficiënten van het polynoom

$$\begin{aligned} (Y - X_1)(Y - X_2) \cdots (Y - X_n) = \\ Y^n - \sigma_1 Y^{n-1} + \sigma_2 Y^{n-2} - \dots + (-1)^{n-1} \sigma_{n-1} Y + (-1)^n \sigma_n \end{aligned}$$

zijn. Maar er zijn ook andere standaard symmetrische polynomen, zoals de Newton-polynomen

$$p_k = \sum_{i=1}^n X_i^k \quad (k = 1, 2, \dots).$$

---

\* Luigi Lagrange, 1736–1813, Frans-Italiaans wiskundige.

De volgende stelling die in essentie op Waring\* (1762) teruggaat beschrijft alle symmetrische polynomen.

**(1.1) Hoofdstelling van de symmetrische functies.** *Ieder symmetrisch polynoom in  $R[X_1, \dots, X_n]$  kan op een éénduidige manier geschreven worden als polynoom in de elementaire symmetrische polynomen.*

*Bewijs.* Gegeven een symmetrisch polynoom  $f \in R[X_1, \dots, X_n]$  zullen we een polynoom in de  $\sigma_1, \dots, \sigma_n$  construeren dat gelijk is aan  $f$ . We doen dit met inductie naar de totale graad van  $f$ . De stelling geldt voor polynomen van graad 0. We schrijven  $f$  als som van monomen en ordenen de monomen lexicografisch. Dus een monoom  $aX_1^{r_1} \cdots X_n^{r_n}$  komt eerder dan  $bX_1^{s_1} \cdots X_n^{s_n}$  als  $r_i > s_i$  voor de kleinste  $i$  waarvoor  $r_i$  ongelijk is aan  $s_i$ . Beschouw nu de kopterm van  $f$  in deze schrijfwijze:

$$f = cX_1^{a_1} \cdots X_n^{a_n} + \dots$$

Omdat  $f$  symmetrisch is geldt nu  $a_1 \geq a_2 \geq \dots \geq a_n$ , anders zou een verwisseling van twee variabelen een term geven die eerder komt in deze ordening. Het symmetrische polynoom

$$c\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3} \cdots \sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$$

heeft dezelfde kopterm  $cX_1^{a_1} \cdots X_n^{a_n}$  (ga dit zelf na). Definieer nu

$$f_1 = f - c\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3} \cdots \sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}.$$

Als  $f_1 = 0$  dan zijn we klaar. Zo niet, dan is  $f_1$  een symmetrisch polynoom waarin alle monomen in de lexicografische ordening later komen dan de kopterm van  $f$ . We herhalen dan het proces voor  $f_1$ . Dat geeft een

$$f_2 = f_1 - c_1\sigma_1^{a'_1-a'_2}X_2^{a'_2-a'_3} \cdots X_{n-1}^{a'_{n-1}-a'_n}X_n^{a'_n}.$$

Omdat er maar eindig veel monomen  $X_1^{d_1} \cdots X_n^{d_n}$  mogelijk zijn met vaste totale graad  $d = d_1 + \dots + d_n$ , gaat na eindig veel stappen de totale graad van ons polynoom omlaag. Dan kunnen we de inductiehypothese toepassen en hebben we aangetoond dat de gevraagde schrijfwijze bestaat.

We moeten nog laten zien dat de schrijfwijze eenduidig is. Als dat niet zo is, dan is er een symmetrisch polynoom  $f$  dat op twee verschillende manieren kan worden geschreven. Dat betekent dat de afbeelding van polynoomringen

$$\phi_n : R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n], \quad g(Y_1, \dots, Y_n) \mapsto g(\sigma_1, \dots, \sigma_n)$$

een niet-triviale kern heeft. We laten nu met inductie zien dat dit niet zo is. De lezer mag het geval  $n = 1$  direct controleren. Als  $g$  in de kern van  $\phi_n$  met  $n > 1$  zit, dan krijgen we door substitutie van  $X_n = 0$  (in de  $\sigma_i$ ) en  $Y_n = 0$  in  $g$  een element  $g'$  van de kern van  $\phi_{n-1}$ , en per inductieaanname is dat element nul. Dus  $g$  wordt nul bij substitutie  $Y_n = 0$  en dus is  $g$  deelbaar door  $Y_n$ , zeg  $g = g_1Y_n$  en  $g_1(\sigma_1, \dots, \sigma_n)\sigma_n = 0$ .

---

\* Edward Waring, 1736–1798, Engels wiskundige liet in zijn ‘Miscellanea Analytica’ zien dat alle rationale symmetrische functies van de wortels van een polynoom als rationale functie van de coëfficiënten uitgedrukt kunnen worden

Maar  $\sigma_n$  is geen nuldeeler in  $R[X_1, \dots, X_n]$ , dus  $g_1$  zit in de kern van  $\phi_n$ , en is van lagere totale graad. Met inductie naar de graad volgt nu de stelling. Dit beëindigt het bewijs van de hoofdstelling.

De symmetrische groep  $S_n$  werkt ook op het lichaam  $K(X_1, \dots, X_n)$  van rationale functies. We kunnen dus ook spreken van symmetrische rationale functies.

**(1.2) Gevolg.** *Laat  $K$  een lichaam zijn en laat  $K(X_1, \dots, X_n)$  het quotiëntenlichaam van  $K[X_1, \dots, X_n]$  zijn. Dan is iedere symmetrische rationale functie  $\phi$  in het lichaam  $K(X_1, \dots, X_n)$  een rationale functie in  $\sigma_1, \dots, \sigma_n$ .*

*Bewijs.* Laat  $\phi = f/g$  een rationale functie zijn die symmetrisch is. Hierbij zijn  $f$  en  $g$  elementen van  $K[X_1, \dots, X_n]$ . We maken nu eerst de noemer symmetrisch: het polynoom

$$h := \prod_{\sigma \in S_n} \sigma(g)$$

is ten duidelijkste symmetrisch. We zien dat  $h \cdot \phi$  symmetrisch is, maar ook een polynoom in  $K[X_1, \dots, X_n]$ , dus volgens de hoofdstelling een polynoom in de elementaire symmetrische polynomen  $\sigma_i$ . Maar ook  $h$  is volgens de hoofdstelling een polynoom in de  $\sigma_i$  en daarom is  $\phi$  dan een rationale functie in de  $\sigma_i$ . Q.e.d.

**Opmerking.** De bovenstaande hoofdstelling wordt vaak de hoofdstelling van de symmetrische functies genoemd, alhoewel hier geen sprake is van functies maar van polynomen.

Het bewijs geeft zelfs een algoritme (=recept) voor het verkrijgen van de schrijfwijze van een symmetrisch polynoom als polynoom in de  $\sigma_r$ .

We geven nu een voorbeeld van de bepaling van de schrijfwijze zoals gegeven in de hoofdstelling. We nemen  $n = 3$  en beschouwen het symmetrische polynoom

$$(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2.$$

Dit is ten duidelijkste een symmetrisch polynoom. Als we het uitschrijven dan is de eerste term in de lexicografische ordening de term  $X_1^4 X_2^2$ . Volgens het algoritme moeten we  $\sigma_1^2 \sigma_2^2$  aftrekken van  $f$ ; het resultaat is (gebruik Maple, Mathematica of iets dergelijks)

$$\begin{aligned} & -4(X_1^4 X_2 X_3 + X_1 X_2^3 X_3 + X_1 X_2 X_3^4) - 4(X_1^3 X_2^3 + X_1^3 X_3^3 + X_2^3 X_3^3) + \\ & -6(X_1^3 X_2^2 X_3 + X_1^3 X_2 X_3^2 + X_1^2 X_2^2 X_3 + X_1 X_2^3 + X_3^2 + X_1^2 X_2 X_3^3 + X_1 X_2^2 X_3^3) \end{aligned}$$

en we zien dat de eerste term in de lexicografische ordening nu  $-4X_1^4 X_2 X_3$  is. We tellen er daarom nu  $4\sigma_1^3 \sigma_3$  bij op en krijgen

$$\begin{aligned} & -4(X_1^3 X_2^3 + X_1^3 X_3^3 + X_2^3 X_3^3) + \\ & 6(X_1^3 X_2^2 X_3 + X_1^3 X_2 X_3^2 + X_1^2 X_2^3 X_3 + X_1 X_2^3 X_3^2 + X_1^2 X_2 X_3^3 + X_1 X_2^2 X_3^3) \end{aligned}$$

en vinden nu als eerste term  $-4X_1^3 X_2^3$ . Daarom tellen we er  $4\sigma_2^3$  bij op en vinden

$$18(X_1^3 X_2^2 X_3 + X_1^3 X_2 X_3^2 + X_1^2 X_2^3 X_3 + X_1^2 X_2 X_3^3 + X_1 X_2^3 X_3 + X_1 X_2^2 X_3^3)$$

met als eerste term  $18X_1^3X_2^2X_3$ . We trekken er nu weer  $18\sigma_1\sigma_2\sigma_3$  van af en krijgen dan  $-27X_1^2X_2^2X_3^2$  en herkennen dit als  $-27\sigma_3^2$ . In totaal vinden we dus

$$(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2 = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2.$$

We zien ook dat het nogal een bewerkelijk proces kan zijn om een gegeven symmetrisch polynoom in de standaardgedaante te brengen.

Merk op dat de uitdrukking

$$(X_1 - X_2)(X_1 - X_3) \cdots (X_{n-1} - X_n)$$

niet invariant is onder de hele symmetrische groep  $S_n$ , maar alleen onder de groep  $A_n$  van de even permutaties. Het kwadraat hiervan is wel invariant onder de symmetrische groep en deze symmetrische functie heet de *discriminant* van het polynoom

$$(Y - X_1)(Y - X_2) \cdots (Y - X_n)$$

met wortels  $X_i$ . Zo is de discriminant van

$$Y^2 - (X_1 + X_2)Y + X_1X_2 = Y^2 - \sigma_1Y + \sigma_2$$

gelijk aan

$$(X_1 - X_2)^2 = \sigma_1^2 - 4\sigma_2.$$

De discriminant van een derdegraads polynoom  $Y^3 - a_1Y^2 + a_2Y - a_3$  hebben we zojuist uitgerekend:

$$D = a_1^2a_2^2 - 4a_1^3a_3 - 4a_2^3 + 18a_1a_2a_3 - 27a_3^2.$$

In het bijzonder heeft het derdegraadspolynoom  $X^3 + aX + b$  als discriminant  $-4a^3 - 27b^2$ .

### Opgaven

- 1) Schrijf  $X_1^4 + X_2^4 + X_3^4 \in \mathbb{Z}[X_1, X_2, X_3]$  als polynoom in de elementaire symmetrische polynomen.
- 2) Schrijf  $\sum_{i=1}^n X_i^2$  en  $\sum_{i=1}^n X_i^3$  als polynoom in de elementaire symmetrische functies.
- 3) Schrijf de volgende symmetrische rationale functie in termen van de elementaire symmetrische functies:

$$X_1/X_2 + X_1/X_3 + X_2/X_1 + X_2/X_3 + X_3/X_1 + X_3/X_2.$$

- 4) Laat  $K$  een lichaam zijn en laat  $f \in K[X]$  een monisch polynoom zijn. Dan geldt  $\text{graad}(\text{ggd}(f, f')) > 0 \iff$  de discriminant van  $f$  is nul. Bewijs dit.
- 5) Laat  $p_k = \sum_{i=1}^n X_i^k$  de  $k$ -de machtssom zijn voor  $k \geq 1$ . Bewijs de volgende formules van Newton:

$$\begin{aligned} p_r - p_{r-1}\sigma_1 + p_{r-2}\sigma_2 - \dots + (-1)^{r-1}p_1\sigma_{r-1} + (-1)^r r\sigma_r &= 0 && \text{voor } r \leq n \\ p_r - p_{r-1}\sigma_1 + p_{r-2}\sigma_2 - \dots + (-1)^n p_{r-n}\sigma_n &= 0 && \text{voor } r > n. \end{aligned}$$

6) Laat  $E(t) = \sum_{j=0}^n \sigma_j t^j$ . Bewijs de identiteit

$$E(t) = \prod_{i=1}^n (1 + X_i t).$$

Laat verder  $P(t) = \sum_{j=1}^{\infty} p_j t^{j-1}$ . Bewijs de identiteit

$$P(-t) = E'(t)/E(t).$$

7) Laat  $\alpha_1, \alpha_2$  en  $\alpha_3$  de drie nulpunten van  $X^3 - 2X^2 + 3X - 1$  in  $\mathbb{C}$  zijn. Bereken de coëfficiënten van het monisch polynoom van de derde graad in  $\mathbb{Q}[X]$  met nulpunten  $\alpha_1^2, \alpha_2^2$  en  $\alpha_3^2$ .

8) Laat  $f = (X - a_1)(X - a_2) \cdots (X - a_n) \in K[X]$  een polynoom zijn. Bewijs dat de discriminant van  $f$  op teken na gegeven wordt door

$$D = \pm \prod_{i=1}^n f'(a_i).$$

9) Laat  $R_1 \subset R_2$  een deelring met  $1 \in R_1$  van de commutatieve ring  $R_2$  met 1 zijn. Laat  $f$  een monisch polynoom in  $R_1[X]$  zijn dat in  $R_2[X]$  ontbonden kan worden als  $f = (X - a_1) \cdots (X - a_n)$  met  $a_i \in R_2$  voor  $i = 1, \dots, n$ . Laat zien dat voor elk symmetrisch polynoom  $g \in R_1[X_1, \dots, X_n]$  geldt dat  $g(a_1, \dots, a_n) \in R_1$ .

10) Stel dat  $X^3 - X - 1 \in \mathbb{Z}[X]$  zich laat ontbinden als  $(X - a_1)(X - a_2)(X - a_3)$  in  $\mathbb{C}[X]$ . Laat  $p_k = a_1^k + a_2^k + a_3^k$  voor  $k \in \mathbb{Z}$ . Laat zien dat

i)  $p_k = p_{k-2} + p_{k-3}$  voor alle  $k \in \mathbb{Z}$ .

ii)  $p_k \in \mathbb{Z}$  voor alle  $k \in \mathbb{Z}$ .

11) Laat  $p_r$  de  $r$ -de machtssom zijn in de variabelen  $X_1, \dots, X_n$ . Bewijs voor  $n \leq 5$  de volgende formule van Waring:

$$p_r = r \sum_{\lambda} (-1)^{\lambda_2 + \lambda_4 + \dots} \frac{(\lambda_1 + \lambda_2 + \dots + \lambda_n - 1)!}{\lambda_1! \lambda_1! \cdots \lambda_n!} \sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \cdots \sigma_n^{\lambda_n},$$

waar de som loopt over de  $n$ -tallen  $\lambda = (\lambda_1, \dots, \lambda_n)$  met  $\lambda_i \in \mathbb{Z}_{\geq 0}$  die voldoen aan  $\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = r$ .

## 2. EENHEIDSWORTELS

*Een student die bij Euklides meetkunde was gaan studeren vroeg toen hij de eerste stelling had geleerd aan Euklides ‘Wat heb ik eraan om deze dingen te leren?’ Waarop Euklides zijn bediende riep en zei: ‘Geef hem drie stuivers, want hij moet iets verdienen als hij iets leert.’*  
Stobaeus over Euklides\*, in ‘Uittreksels’

In dit hoofdstuk zijn lichaamsuitbreidingen die met behulp van eenheidswortels gemaakt worden het onderwerp. Deze uitbreidingen zullen later diverse keren aan de orde komen.

**(2.1) Definitie.** Laat  $K$  een lichaam zijn. Een element  $\zeta \in K^*$  heet een  $n$ -de-machts eenheidswortel als  $\zeta$  voldoet aan  $\zeta^n = 1$ . We noemen  $\zeta$  een *primitieve*  $n$ -de-machts eenheidswortel als de orde van  $\zeta \in K^*$  gelijk is aan  $n$ .

Voorbeelden zijn gemakkelijk te geven. Zo zijn in het lichaam  $\mathbb{R}$  van de reële getallen de elementen 1 en  $-1$  eenheidswortels. In het lichaam  $\mathbb{C}$  van de complexe getallen zijn de getallen  $e^{2\pi ia/n}$  met  $0 \leq a \leq n-1$   $n$ -de-machts eenheidswortels, terwijl de getallen  $e^{2\pi ia/n}$  met  $(a, n) = 1$  en  $0 < a \leq n-1$  de primitieve  $n$ -de-machts eenheidswortels zijn. Er zijn dus  $\phi(n)$  primitieve  $n$ -de-machts eenheidswortels in  $\mathbb{C}$ , waarbij  $\phi$  de  $\phi$ -functie van Euler aanduidt.

In een eindig lichaam  $\mathbb{F}_q$  zijn alle elementen  $\zeta \in \mathbb{F}_q^*$  eenheidswortels, en wel  $(q-1)$ -de-machts eenheidswortels.

We definiëren nu het  $n$ -de *cyklotomische polynoom*  $\Phi_n(X)$  (eerst in  $\mathbb{C}[X]$ ) door

$$\Phi_n(X) = \prod_{\zeta \in \mathbb{C}^*, \text{orde}(\zeta)=n} (X - \zeta).$$

Het product loopt hierbij over alle primitieve  $n$ -de-machts eenheidswortels in  $\mathbb{C}$ . Er geldt  $\Phi_1(X) = X - 1$  en door de wortels van gelijke orde bijeen te nemen vinden we

$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$

want als  $\zeta$  een nulpunt is van  $X^n - 1$  dan is de orde van  $\zeta$  een deler van  $n$ . Met inductie zien we nu dat  $\Phi_n(X) \in \mathbb{Z}[X]$ , met andere woorden, de coëfficiënten van  $\Phi_n(X)$  zijn geheel. Immers, dit klopt voor  $n = 1$  en als we het aannemen voor  $d < n$  dan is  $\prod_{d|n, d \neq n} \Phi_d(X)$  een deler van  $X^n - 1$  in  $\mathbb{Q}[X]$  met geheeltallige coëfficiënten en het quotiënt  $\Phi_n(X)$  ligt dan volgens het Lemma van Gauss weer in  $\mathbb{Z}[X]$ . In het vervolg vatten we de  $\Phi_n$  op als elementen van  $\mathbb{Z}[X]$ . Verder volgt uit het bovenstaande dat de graad van  $\Phi_n$  gelijk is aan  $\phi(n)$ .

Als  $n = p$  een priemgetal is, dan zien we direct dat

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + 1.$$

---

\* Euklides, Grieks wiskundige

Substitutie  $X = Y + 1$  geeft

$$\Phi_p(Y + 1) = \frac{(Y + 1)^p - 1}{(Y + 1) - 1}$$

en dit is een Eisensteinpolynoom in  $Y$  bij de priem  $p$ , (ga na, of gebruik Syllabus Algebra2a, (7.14)) dus  $\Phi_p$  is een irreducibel polynoom in  $\mathbb{Q}[X]$  en ook in  $\mathbb{Z}[X]$ .

Meer algemeen geldt de volgende stelling.

**(2.2) Stelling.** *Voor elke  $n \in \mathbb{Z}_{\geq 1}$  is het  $n$ -de cyclotomische polynoom  $\Phi_n$  irreducibel in  $\mathbb{Q}[X]$ .*

*Bewijs.* We gaan laten zien dat  $\Phi_n$  het minimumpolynoom van een primitieve  $n$ -de-machts eenheidswortel is. Kies dus een willekeurige primitieve  $n$ -de-machts eenheidswortel  $\zeta$  en laat  $f$  het minimumpolynoom van  $\zeta$  over  $\mathbb{Q}$  zijn. Als  $p$  een priemgetal is dat  $n$  niet deelt dan is  $\zeta^p$  ook van orde  $n$ . Laat  $g$  het minimumpolynoom van  $\zeta^p$  zijn. We tonen nu eerst aan dat  $g = f$ . Omdat  $\zeta$  en  $\zeta^p$  nulpunten van  $X^n - 1$  zijn is zowel  $f$  als  $g$  een deler van  $X^n - 1$ . Met het Lemma van Gauss volgt dat  $f$  en  $g$  in  $\mathbb{Z}[X]$  liggen.

Als  $f$  niet gelijk is aan  $g$ , dan zijn  $f$  en  $g$  twee verschillende irreducibele factoren van  $X^n - 1$  en dus deelt  $fg$  het polynoom  $X^n - 1$  in de ring  $\mathbb{Z}[X]$ . Omdat  $g(\zeta^p) = 0$  moet  $f$  ook een deler van  $g(X^p)$  in  $\mathbb{Z}[X]$  zijn. Werk nu even modulo  $p$ . In  $\mathbb{Z}/p\mathbb{Z}[X]$  geldt de relatie

$$g(X^p) = g(X)^p.$$

Dus in  $\mathbb{Z}/p\mathbb{Z}[X]$  vinden we dat  $f$  een deler is van  $g^p$ . Omdat we niet weten of  $f$  modulo  $p$  nog irreducibel is, kunnen we niet concluderen dat  $f$  dan ook  $g$  deelt. Daarom kijken we naar een irreducibele factor van  $f$  modulo  $p$ .

Laat  $h$  een irreducibele factor van  $f$  in  $\mathbb{Z}/p\mathbb{Z}[X]$  zijn. Dan moet  $h$  een deler van  $g^p$  zijn, en dus ook een deler van  $g$ . Maar dan is ook  $h^2$  een deler van  $fg$ , dus van  $X^n - 1$ . Dat betekent dat  $h$  een deler van  $X^n - 1$  en van de afgeleide  $nX^{n-1}$  in  $\mathbb{Z}/p\mathbb{Z}[X]$  moet zijn. Maar  $n \neq 0$  in  $\mathbb{Z}/p\mathbb{Z}$ , dus de enige monische irreducibele factor van  $nX^{n-1}$  is  $X$  en dat is geen deler van  $X^n - 1$ . Deze tegenspraak bewijst dat  $f = g$  en  $\zeta^p$  is dus een nulpunt van  $f$ .

We laten nu zien dat iedere primitieve  $n$ -de-machts eenheidswortel een nulpunt van  $f$  is. Merk eerst op dat de  $n$ -de machts eenheidswortels in  $\mathbb{C}$  een cyclische groep vormen voortgebracht door  $\zeta$  (zie ook Opgave 4). Laat  $\zeta^\nu$  een willekeurige primitieve  $n$ -de machts eenheidswortel zijn. We schrijven  $\nu$  als product van priemfactoren

$$\nu = p_1 \cdots p_r$$

met  $(n, p_i) = 1$ . Uit het bovenstaande volgt dat met  $\zeta$  ook  $\zeta^{p_1}$  een nulpunt van  $f$  is. Herhalen van het argument leert dat ook  $\zeta^{p_1 p_2}$  een nulpunt van  $f$  is en met inductie tenslotte ook  $\zeta^\nu$ . Dus alle nulpunten van  $\Phi_n$  zijn nulpunten van  $f$ . Omdat  $\Phi_n$  geen meervoudige nulpunten heeft en omdat  $f$  monisch en irreducibel is volgt  $f = \Phi_n$ . Dat bewijst de irreducibiliteit van het  $n$ -de cyclotomische polynoom.

**(2.3) Gevolg.** *Laat  $n$  en  $m$  twee onderling ondeelbare natuurlijke getallen zijn. Als  $\zeta_n$  en  $\zeta_m$  primitieve eenheidswortels zijn van orde  $m$  en  $n$  dan geldt in het lichaam  $\mathbb{Q}(\zeta_m, \zeta_n)$  dat  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ .*

*Bewijs.* Omdat  $(n, m) = 1$  volgt dat de orde van  $\zeta_m \zeta_n$  gelijk is aan  $mn$ . Dus we mogen schrijven  $\zeta_{mn} = \zeta_m \zeta_n$ . Uit de voorgaande stelling volgt dat  $[\mathbb{Q}(\zeta_r) : \mathbb{Q}] = \phi(r)$  met  $\phi$  de Euler phi-functie. Laat nu  $K$  het lichaam  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$  zijn. Dan geldt

$$[\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] \leq [K(\zeta_m) : K] = [\mathbb{Q}(\zeta_m) : K]$$

(vgl. Opgave 12) terwijl anderzijds ook geldt

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] = \frac{\phi(mn)}{\phi(n)} = \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

We zien  $[\mathbb{Q}(\zeta_m) : K] \geq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$  terwijl de inclusie  $\mathbb{Q} \subset K$  laat zien dat  $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_m) : K]$ , dus  $[\mathbb{Q}(\zeta_m) : K] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ . Hieruit volgt direkt  $K = \mathbb{Q}$ . Dit bewijst het gevolg.

We kunnen het cyclotomische polynoom  $\Phi_n$  ook modulo een priem  $p$  bekijken en nagaan hoe het te ontbinden is een uitbreidingslichaam  $\mathbb{F}_q$  van  $\mathbb{F}_p$ . De cyclotomische polynomen  $\Phi_n$  zijn in het algemeen niet meer irreducibel modulo een priemgetal. Eenvoudige voorbeelden zijn

$$\begin{aligned} \Phi_3 &= X^2 + X + 1 \equiv (X - 1)^2 \pmod{3} \\ \Phi_7 &\equiv (X^3 + 5X^2 + 4X + 10)(X^3 + 7X^2 + 6X + 10) \pmod{11} \\ \Phi_{11} &\equiv (X + 5)(X + 7)(X + 9)(X + 10)(X + 11)(X + 14)(X + 15) \cdot \\ &\quad \cdot (X + 17)(X + 19)(X + 20) \pmod{23}. \end{aligned}$$

We nemen aan dat  $p$  geen deler is van  $n$ . Er geldt namelijk als  $n = p^k m$  met  $(p, m) = 1$  dat

$$\Phi_n \equiv (\Phi_m)^{\phi(p^k)} \pmod{p},$$

zie Opgave 1 en Opgave 2. Dus dit geval laat zich terugvoeren op het geval dat  $p$  geen deler is van  $n$ .

**(2.4) Lemma.** *Laat  $p$  een priemgetal zijn dat  $n$  niet deelt en  $K$  een lichaam van karakteristiek  $p$ . Dan is ieder nulpunt van  $\Phi_n \pmod{p}$  in  $K$  een primitieve  $n$ -de-machts eenheidswortel.*

*Bewijs.* Laat  $\zeta$  een nulpunt van  $\Phi_n$  in  $K$  zijn. Omdat  $\Phi_n$  een deler is van  $X^n - 1$  volgt dat  $\zeta^n = 1$ . Als de orde van  $\zeta$  gelijk is aan  $m$ , een echte deler van  $n$ , dan is  $\zeta$  een nulpunt van  $X^m - 1$ . Maar uit de formule  $X^n - 1 = \prod_{d|n} \Phi_d$  volgt dat  $(X^m - 1)\Phi_n$  het polynoom  $X^n - 1$  deelt. Dan is  $\zeta$  een dubbel nulpunt van  $X^n - 1$ . Maar  $X^n - 1$  heeft geen dubbele nulpunten als  $p \nmid n$  omdat de afgeleide alleen 0 als wortel heeft. Q.e.d.

**(2.5) Stelling.** *Laat  $\mathbb{F}_q$  een eindig lichaam van karakteristiek  $p$  zijn en  $n \in \mathbb{Z}_{\geq 1}$  een natuurlijk getal met  $(n, q) = 1$ . Dan is de graad van iedere irreducibele factor van  $\Phi_n(\text{mod } p)$  in  $\mathbb{F}_q[X]$  gelijk aan de orde van  $q(\text{mod } n)$  in  $(\mathbb{Z}/n\mathbb{Z})^*$ .*

*Bewijs.* Laat een irreducibele factor  $f$  van  $\Phi_n(\text{mod } p)$  zijn met graad  $d$ . Als  $\zeta$  een nulpunt van  $f$  in een uitbreidingslichaam van  $\mathbb{F}_q$  is, dan geldt  $[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = d$  en  $\mathbb{F}_q(\zeta)$  is isomorf met  $\mathbb{F}_{q^d}$ . Daaruit volgt voor alle  $m \in \mathbb{Z}_{\geq 1}$  dat (zie Algebra 2a, Hoofdstuk 9)

$$\zeta \in \mathbb{F}_{q^m} \iff d|m. \quad (1)$$

Maar we weten dat  $\zeta$  van orde  $n$  is en dat  $\mathbb{F}_{q^m}^*$  een cyclische groep van orde  $q^m - 1$  is gegeven door  $X^{q^m-1} - 1 = 0$ . Dus we concluderen dat  $\zeta \in \mathbb{F}_{q^m}$  dan en slechts dan als  $n$  een deler is van  $q^m - 1$ . We vinden

$$\zeta \in \mathbb{F}_{q^m} \iff q^m \equiv 1(\text{mod } n) \iff \text{de orde van } q \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \text{ deelt } m \quad (2)$$

en dus uit (1) en (2) samen voor alle  $m \in \mathbb{Z}_{\geq 1}$

$$d|m \iff \text{de orde van } q \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \text{ deelt } m$$

Dit bewijst dat  $d$  gelijk is aan de orde van  $q$  in  $(\mathbb{Z}/n\mathbb{Z})^*$  en de stelling volgt.

Als toepassing van cyclotomische polynomen geven we hier het prachtige bewijs van Ernst Witt\* van de Stelling van Wedderburn.

**(2.6) Stelling van Wedderburn.** *Iedere eindige delingsring is een lichaam.*

*Bewijs.* Laat  $R$  een eindige delingsring zijn, dwz.  $R$  is een eindige ring met  $1 \in R$  met de eigenschap dat ieder element  $x \in R$ ,  $x \neq 0$ , een multiplicatieve inverse  $x^{-1}$  in  $R$  heeft met  $x \cdot x^{-1} = x^{-1} \cdot x = 1$ . We moeten laten zien dat de vermenigvuldiging commutatief is.

Laat  $C = \{x \in R : xy = yx \text{ voor alle } y \in R\}$  het centrum van  $R$  zijn. Dat is een eindig lichaam  $C$ , zeg van cardinaliteit  $q$ . De multiplicatieve groep  $R^* = R - \{0\}$  werkt op  $R^*$  via  $y \mapsto x^{-1}yx$  voor  $x \in R^*$ . Merk op dat de baan van  $y$  precies lengte 1 heeft als  $y$  in het centrum ligt. Als de baan uit meer dan een element bestaat dan kan de cardinaliteit geschreven worden als

$$\#R^* / \#C_y^*$$

met  $C_y = \{z \in R : zy = yz\}$  de centralisator van  $y$  in  $R$  en  $C_y^* = C_y - \{0\}$ . Zowel  $R$  als de centralisator  $C_y$  kunnen opgevat worden als vectorruimten over het eindige lichaam  $C$ , zeg van dimensie  $n$  en  $n_y$  respectievelijk. Dan heeft de baan van  $y$  lengte

$$\frac{q^n - 1}{q^{n_y} - 1}.$$

---

\* Ernst Witt, 1911-1991, Duits wiskundige

Stel nu dat  $C \neq R$ , dus  $n > 1$ . Dan kunnen we  $R^*$  schrijven als een disjuncte vereniging van banen en voor de cardinaliteiten vinden we

$$q^n - 1 = q - 1 + \sum_{i=1}^r \frac{q^n - 1}{q^{n_i} - 1}, \quad (2)$$

waar de term  $q - 1$  komt van de elementen ongelijk nul in het centrum, die ieder 1 bijdragen, terwijl de andere termen van banen met lengte  $> 1$  komen. Merk op dat ieder van deze termen een geheel getal is, dus  $n_i < n$  en  $n_i$  deelt  $n$ .

De  $n$ -de cyclotomische veelterm  $\Phi_n \in \mathbb{Z}[X]$  deelt  $X^n - 1$ , maar ook ieder van de termen  $(X^n - 1)/(X^{n_i} - 1)$  omdat een primitieve  $n$ -de machts eenheidswortel  $\zeta_n$  geen wortel is van  $X^{n_i} - 1$  van  $n_i < n$ , dus  $\zeta_n$  is een nulpunt van  $(X^n - 1)/(X^{n_i} - 1)$  en dus deelt zijn minimumpolynoom  $\Phi_n$  het polynoom  $(X^n - 1)/(X^{n_i} - 1)$ .

We zien dus dat  $\Phi_n(q)$  het getal  $q^n - 1$  deelt en ook ieder van de termen  $(q^n - 1)/(q^{n_i} - 1)$ , zodat het vanwege (2) ook  $q - 1$  deelt. Maar als  $\zeta_n$  een primitieve  $n$ -de machtseenheidswortel is dan geldt  $|q - \zeta_n| > q - 1$ , maak een plaatje. Nu is  $\Phi_n(q)$  een product van termen  $q - \zeta_n^a$  met  $(a, n) = 1$  en heeft dus absolute waarde  $> q - 1$ , en kan dus geen deler zijn van  $q - 1$ . Dat is een tegenspraak. Dus  $C = R$  en we zien dat  $R$  commutatief is. Einde bewijs.

Een andere mooie toepassing van cyclotomische polynomen is een speciaal geval van een stelling van Dirichlet over het voorkomen van priemgetallen in rekenkundige reeksen.

**(2.7) Propositie.** *Laat  $n$  een natuurlijk getal zijn. Dan zijn er oneindig veel priemgetallen  $p$  met  $p \equiv 1 \pmod{n}$ .*

*Bewijs.* We laten zien dat er voor ieder geheel getal  $n > 0$  een priemgetal  $p$  is met  $p \equiv 1 \pmod{n}$ . Door dit toe te passen op alle positieve veelvouden  $kn$  van  $n$  vinden we dan oneindig veel priemgetallen met  $p \equiv 1 \pmod{n}$ . Kies een geheel getal  $m$  zodat  $\Phi_n(mn) > 1$ . Zo een getal bestaat want de reële functie  $x \mapsto \Phi_n(x)$  gaat naar  $\infty$  als  $x$  naar  $\infty$  gaat. Kies een priemgetal  $p$  dat  $\Phi_n(mn)$  deelt. Dan is  $mn \pmod{p}$  een nulpunt van  $\Phi_n \pmod{p}$ . Merk op dat  $p$  geen deler is van  $n$  want  $p$  deelt  $(mn)^n - 1$  omdat  $\Phi_n$  het polynoom  $X^n - 1$  deelt. Uit Lemma (2.4) volgt dat  $mn \pmod{p}$  orde  $n$  heeft in  $\mathbb{F}_p^*$ . Dat betekent dat  $n$  een deler is van  $p - 1$ , dus  $p \equiv 1 \pmod{n}$ . Dit bewijst de propositie.

### Opgaven

1) Laat  $p$  een priemgetal zijn en  $n \in \mathbb{Z}_{\geq 1}$ . Bewijs:

$$\Phi_{np}(X) = \begin{cases} \Phi_n(X^p) & \text{als } p|n \\ \Phi_n(X^p)/\Phi_n(X) & \text{als } (n, p) = 1. \end{cases}$$

en verder dat  $\Phi_{2n}(X) = \pm \Phi_n(-X)$  voor oneven  $n \in \mathbb{Z}_{\geq 1}$ .

2) Bewijs dat voor  $n = p^k m$  met  $(p, m) = 1$  in  $\mathbb{F}_p[X]$  geldt

$$\Phi_n = (\Phi_m)^{\phi(p^k)}.$$

3) Bereken  $\Phi_{15}$ .

- 4) Zij  $K$  een lichaam.
- i) Laat zien dat  $K$  maar eindig veel  $n$ -de-machts eenheidswortels bevat voor iedere  $n \in \mathbb{Z}_{\geq 1}$ .
  - ii) Laat zien dat de  $n$ -de-machts eenheidswortels in  $K$  een eindige cyclische groep vormen.
  - iii) Zij  $p$  een priemgetal, en veronderstel dat  $K$  karakteristiek  $p$  heeft. Hoeveel  $p$ -de-machts eenheidswortels bevat  $K$ ?
- 5) Bewijs dat voor elk priemgetal  $p$  het polynoom  $\Phi_{24} \in \mathbb{Z}/p\mathbb{Z}[X]$  reducibel is.
- 6) Bepaal de eenheidswortels in de volgende lichamen:  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{Q}$ ,  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt{-3})$ ,  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{F}_q$  en  $\mathbb{F}_q(X)$ .
- 7) Ontbind  $\Phi_{15}$  in  $\mathbb{F}_2[X]$ ,  $\mathbb{F}_7[X]$  en in  $\mathbb{F}_{11}[X]$ .
- 8) Definieer de *Moebius-functie*  $\mu : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}$  door

$$\mu(n) = \begin{cases} (-1)^r & \text{als } n \text{ product van } r \text{ verschillende priemgetallen is,} \\ 0 & \text{anders.} \end{cases}$$

Merk op  $\mu(1) = 1$ . Bewijs dat

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{als } n = 1, \\ 0 & \text{als } n > 1. \end{cases}$$

- 9) Laat  $f, g : \mathbb{N} \rightarrow G$  twee afbeeldingen zijn met waarden in de additief geschreven groep  $G$ . Bewijs:

$$\sum_{d|n} f(d) = g(n) \quad \text{voor alle } n \in \mathbb{N} \iff \sum_{d|n} \mu(n/d)g(d) = f(n) \quad \text{voor alle } n \in \mathbb{N}$$

- 10) Bewijs voor alle  $n \in \mathbb{Z}_{\geq 1}$  de volgende formule in  $\mathbb{Q}(X)$ :

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

- 11) Laat  $n \in \mathbb{Z}_{\geq 1}$  en laat  $K$  een ontbindingslichaam van  $X^n - 1$  over  $\mathbb{Q}$  zijn. Bewijs dat de graad van  $K/\mathbb{Q}$  gegeven wordt door  $[K : \mathbb{Q}] = \phi(n)$ .
- 12) Laat  $K \subseteq L$  een lichaamsuitbreiding zijn en  $\alpha$  een element van een uitbreidingslichaam van  $L$ . Bewijs dat  $[K(\alpha) : K] \geq [L(\alpha) : L]$ .
- 13) Laat  $p$  een priemgetal zijn. Dan is de discriminant van het polynoom  $X^p - 1$  gelijk aan  $\pm p^p$ . (Zie opgave 8, hoofdstuk 1).
- 14) Laat  $p$  een oneven priemgetal zijn. Voor een geheel getal  $x$  definiëren we het *Legendre-symbool*\*  $\left(\frac{x}{p}\right)$  dat de waarden 0 en  $\pm 1$  aanneemt via

$$x^{(p-1)/2} \equiv \left(\frac{x}{p}\right) \pmod{p}.$$

---

\* Adrien Marie Legendre, Frans wiskundige, 1752–1833

Ga na dat voor  $x$  in  $\mathbb{Z}$  geldt dat  $\left(\frac{x}{p}\right) = -1$  dan en slechts dan als  $x$  geen kwadraat is modulo  $p$ .

15) Laat  $\zeta$  een primitieve  $p$ -de machtseenheidswortel in  $\mathbb{C}$  of in een lichaam  $K$  zijn van karakteristiek ongelijk aan  $p$  zijn. Definiëer de Gauss-som

$$g := \sum_{a \bmod p} \left(\frac{a}{p}\right) \zeta^a.$$

Bewijs dat  $g^2 = \left(\frac{-1}{p}\right) p$ .

16) Laat  $p$  en  $q$  twee verschillende oneven priemgetallen zijn. Laat  $\zeta$  een primitieve  $p$ -de machtseenheidswortel in een lichaam  $K$  zijn van karakteristiek  $q$  en  $g$  de Gauss-som zoals gedefiniëerd in Opgave 15. Bewijs dat geldt  $g^q = \left(\frac{q}{p}\right) g$ .

17) Bewijs de kwadratische reciprociteitswet van Gauss: als  $p$  en  $q$  verschillende oneven priemgetallen zijn geldt

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

Aanwijzing: bereken  $g^{q-1}$  met behulp van Opgaven 15 en 16.

18) Laat  $p$  een oneven priemgetal zijn en definiëer de volgende deelverzamelingen van  $\mathbb{Z}/p\mathbb{Z}$ :

$$P = \{\overline{1}, \overline{2}, \dots, \overline{(p-1)/2}\} \quad N := \{-\overline{1}, -\overline{2}, \dots, -\overline{(p-1)/2}\}.$$

Voor een geheel getal  $a$  met  $(a, p) = 1$  schrijven we  $aP = \{\overline{a}, \overline{2a}, \dots, \overline{(p-1)a/2}\}$ . Bewijs:

$$\left(\frac{a}{p}\right) = (-1)^{\#aP \cap N}.$$

19) Bewijs dat voor een oneven priemgetal  $p$  geldt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

20) Bereken het Legendre-symbool  $\left(\frac{2008}{101}\right)$ . Zo ook  $\left(\frac{2010}{101}\right)$ .

21) Bewijs dat iedere kwadratische lichaamsuitbreiding van  $\mathbb{Q}$  (dwz. ieder uitbreidingslichaam  $K$  met  $[K : \mathbb{Q}] = 2$ ) bevat is in een lichaam dat verkregen wordt door eenheidswortels aan  $\mathbb{Q}$  te adjungeren.

22) Laat  $p$  een priemgetal zijn en  $\zeta$  een primitieve  $p$ -de machts eenheidswortel in  $\mathbb{C}$ . Bekijk de deelring  $\mathbb{Z}[\zeta]$  van  $\mathbb{Q}(\zeta)$ . Laat zien dat  $(1 - \zeta)$  een priemideaal van  $\mathbb{Z}[\zeta]$  is en dat er een eenheid  $\epsilon$  van  $\mathbb{Z}[\zeta]$  is zodat  $p = \epsilon(1 - \zeta)^{p-1}$ .

23) Laat  $\zeta = \zeta_n$  een primitieve  $n$ -de machts eenheidswortel in  $\mathbb{C}$  zijn en laat  $P$  een priemideaal van de deelring  $\mathbb{Z}[\zeta]$  van  $\mathbb{Q}(\zeta)$  zijn. Bewijs dat als  $P$  een priemgetal  $p$  van  $\mathbb{Z}$  met  $\text{ggd}(p, n) = 1$  bevat dat dan  $\#\mathbb{Z}[\zeta]/P \equiv 1 \pmod{n}$ .

## 3. DE HOOFDSTELLING VAN DE GALOISTHEORIE

*studying the great work of the past is still the best education*

André Weil\*

In dit hoofdstuk behandelen we de hoofdstelling van de Galoistheorie. Ruw gesproken geeft deze stelling een verband tussen de symmetrieën van een lichaam en de deellichamen van dat lichaam. We beginnen met de symmetrieën.

Laat  $L$  een lichaam zijn. Onder een automorfisme van  $L$  verstaan we altijd een lichaamsautomorfisme. In het bijzonder geldt dan  $\sigma(1) = 1$  voor zo een automorfisme  $\sigma$  en dit betekent dat  $\sigma$  de identiteit is op het priemlichaam van  $L$ . De automorfismen vormen een groep

$$\text{Aut}(L) := \{\sigma : L \rightarrow L : \sigma \text{ is een lichaamsautomorfisme}\},$$

waarbij samenstelling de groepsbewerking is. Als  $K \subset L$  een deellichaam van  $L$  is dan kunnen we ook kijken naar de lichaamsautomorfismen van  $L$  die  $K$  vast laten:

$$\text{Aut}(L/K) := \{\sigma \in \text{Aut}(L) : \sigma(x) = x \text{ voor alle } x \in K\}.$$

Dit is een ondergroep van  $\text{Aut}(L)$ . Ieder deellichaam van  $L$  bepaalt dus een ondergroep van  $\text{Aut}(L)$ . Ga na dat ieder tussenlichaam  $K \subset L' \subset L$  een ondergroep  $\text{Aut}(L/L')$  van  $\text{Aut}(L/K)$  bepaalt.

Omgekeerd kunnen we ook voor iedere ondergroep  $G \subset \text{Aut}(L)$  een deellichaam van  $L$  definiëren:

$$L^G := \{x \in L : \sigma(x) = x \text{ voor alle } \sigma \in G\}.$$

Ga zelf na dat dit inderdaad een deellichaam van  $L$  is. Dit lichaam heet het *lichaam van invarianten* van  $G$ .

**(3.1) Voorbeeld.** Laat  $K = \mathbb{R}$  en  $L = \mathbb{C}$ . Dan is  $\text{Aut}(\mathbb{C}/\mathbb{R})$  van orde 2 en voortgebracht door complexe conjugatie  $z \mapsto \bar{z}$ . Immers, een automorfisme permuteert de wortels van  $X^2 + 1$  en ligt vast door het beeld van  $i = \sqrt{-1}$ .

**(3.2) Voorbeeld.** Laat  $L = \mathbb{Q}(\sqrt{5})$ . Dan geldt  $\text{Aut}(L) \cong \mathbb{Z}/2\mathbb{Z}$  en een voortbrenger is gegeven door  $\sigma(\sqrt{5}) = -\sqrt{5}$ . Immers, voor een automorfisme  $\sigma$  geldt  $\sigma(\sqrt{5}) = \pm\sqrt{5}$ .

**(3.3) Voorbeeld.** Laat  $L = \mathbb{Q}(\zeta_5)$  met  $\zeta_5 = \exp(2\pi i/5)$  een primitieve vijfdemachts eenheidswortel in  $\mathbb{C}$ . Er geldt nu  $\text{Aut}(L) \cong \mathbb{Z}/4\mathbb{Z}$ . Merk op dat een automorfisme  $\sigma$  van  $L$  de wortels van het minimumpolynoom  $X^4 + X^3 + X^2 + X + 1$  van  $\zeta_5$  moet permuteren en deze wortels zijn  $\zeta_5^1, \zeta_5^2, \zeta_5^3$  en  $\zeta_5^4$ . Dus  $\sigma$  ligt vast door  $\sigma(\zeta_5)$  en  $\sigma(\zeta_5) = \zeta_5^2$  definieert inderdaad een automorfisme dat  $\text{Aut}(L/K)$  voortbrengt.

**(3.4) Voorbeeld.** Laat  $K = \mathbb{F}_p(t)$  het lichaam van rationale functies in  $t$  zijn (d.w.z. het quotiëntenlichaam van de polynoomring  $\mathbb{F}_p[t]$ ). Laat  $L$  de uitbreiding van  $K$  zijn gegeven door adjunctie van een nulpunt  $\alpha$  van het irreducibele polynoom  $X^p - t$ . (Ga na dat dit polynoom irreducibel is.) Een automorfisme  $\sigma$  van  $L$  dat de identiteit is op

---

\* A. Weil, 1906-2000, Frans-Amerikaans wiskundige die een belangrijke rol speelde in de wiskunde van de 20ste eeuw.

$K$  moet  $\alpha$  naar een andere wortel sturen. Maar in  $L$  geldt:  $X^p - t = (X - \alpha)^p$ , dus er is maar één wortel. We zien:  $\text{Aut}(L/K) = \{1\}$ .

**(3.5) Voorbeeld.** Laat  $L = \mathbb{Q}(\alpha)$  met  $\alpha = \sqrt[3]{2} \in \mathbb{R}$ . Er geldt  $\text{Aut}(L) = \{1\}$ . Immers, een automorfisme  $\sigma$  stuurt een derdemachtswortel uit 2 weer naar een derdemachtswortel uit 2. Maar twee van de drie derdemachtswortels uit 2 zijn niet-reële complexe getallen en die liggen niet in  $L$ . Dus er is voor  $\sigma$  weinig keus.

**(3.6) Voorbeeld.** Laat  $K = \mathbb{Q}(\rho)$  met  $\rho = \exp(2\pi i/3)$  en  $L = K(\alpha)$  met  $\alpha = \sqrt[3]{2} \in \mathbb{R}$ . Ga nu zelf na dat  $\text{Aut}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ .

Het eerste belangrijke resultaat over deze groepen van automorfismen is de volgende stelling.

**(3.7) Stelling.** *Laat  $L$  een lichaamsuitbreiding van  $K$  zijn van eindige graad. Dan geldt*

$$\#\text{Aut}(L/K) \leq [L : K].$$

In het bewijs van deze stelling zullen we het volgende lemma van Artin\* (ook wel Lemma van Dedekind\*\* genoemd) gebruiken.

**(3.8) Lemma.** *Laat  $L_1$  en  $L_2$  lichamen zijn. Als  $\sigma_1, \dots, \sigma_r : L_1 \rightarrow L_2$  verschillende lichaamshomomorfismen zijn en  $a_1, \dots, a_r$  elementen uit  $L_2$  zijn zodat voor alle  $x \in L_1$  geldt*

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \dots + a_r\sigma_r(x) = 0,$$

dan geldt  $a_1 = a_2 = \dots = a_r = 0$ .

Het lemma zegt dus dat verschillende lichaamshomomorfismen lineair onafhankelijk zijn.

*Bewijs.* We voeren het bewijs met inductie naar  $r$ . Als  $r = 1$  en  $a_1\sigma_1(x) = 0$  voor alle  $x \in L_1$ , dan ook voor  $x = 1$ , dus  $a_1\sigma_1(1) = a_1 = 0$ . Neem nu aan dat  $r - 1$  of minder verschillende lichaamshomomorfismen lineair onafhankelijk zijn. Stel we hebben nu een relatie tussen verschillende homomorfismen

$$\sum_{i=1}^r a_i\sigma_i(x) = 0 \quad \text{voor alle } x \in L_1. \quad (1)$$

Omdat  $\sigma_1$  verschillend is van  $\sigma_r$  is er een element  $\xi \in L_1$  met  $\sigma_1(\xi) \neq \sigma_r(\xi)$ . Vervangen we  $x$  in (1) door  $\xi x$  dan krijgen we

$$\sum_{i=1}^r a_i\sigma_i(\xi)\sigma_i(x) = 0 \quad \text{voor alle } x \in L_1.$$

Trekken we hier  $\sigma_1(\xi)$  maal de relatie (1), dus  $\sigma_1(\xi) \sum_{i=1}^r a_i\sigma_i(x)$ , van af dan geeft dit

$$a_2(\sigma_2(\xi) - \sigma_1(\xi))\sigma_2(x) + \dots + a_r(\sigma_r(\xi) - \sigma_1(\xi))\sigma_r(x) = 0 \quad \text{voor alle } x \in L_1.$$

\* Emil Artin, Duits wiskundige, 1898–1962, die in 1937 naar Amerika emigreerde.

\*\* Richard Dedekind, Duits wiskundige, 1831–1916, speelde een belangrijke rol in de ontwikkeling van de algebraïsche getaltheorie.

Met de inductieveronderstelling volgt dan voor de coëfficiënten

$$a_j(\sigma_j(\xi) - \sigma_1(\xi)) = 0 \quad \text{voor } j = 2, \dots, r.$$

Omdat  $\sigma_r(\xi) \neq \sigma_1(\xi)$  volgt  $a_r = 0$ . Dan wordt onze relatie (1)

$$a_1\sigma_1(x) + \dots + a_{r-1}\sigma_{r-1}(x) = 0 \quad \text{voor alle } x \in L_1.$$

en met de inductieaanname volgt dan dat  $a_1 = \dots = a_{r-1} = 0$ . Dit bewijst het lemma.

*Bewijs van Stelling (3.7).* Het lichaam  $L$  is een  $K$ -vectorruimte van dimensie  $n = [L : K]$ . Laat  $e_1, \dots, e_n$  een  $K$ -basis van  $L$  zijn. Als de stelling niet juist is, dan zijn er tenminste  $n + 1$  verschillende automorfismen, zeg  $\sigma_1, \dots, \sigma_{n+1}$ , in  $\text{Aut}(L/K)$ . Bekijk voor  $i = 1, \dots, n + 1$  in de vectorruimte  $L^n$  de vectoren

$$v_i := (\sigma_i(e_1), \sigma_i(e_2), \dots, \sigma_i(e_n)) \in L^n.$$

Omdat dit  $n + 1$  vectoren zijn in een  $n$ -dimensionale  $L$ -vectorruimte, zijn de  $v_i$  lineair afhankelijk en vinden we een niet-triviale lineaire relatie  $\sum_{i=1}^{n+1} a_i v_i = 0$  met coëfficiënten  $a_i \in L$ , dus de relatie

$$\sum_{i=1}^{n+1} a_i \sigma_i(e_j) = 0,$$

geldt voor alle  $j = 1, \dots, n$ .

Schrijf nu een willekeurig element  $x \in L$  als  $x = \sum_{j=1}^n \xi_j e_j$  met  $\xi_j \in K$ . Passen we  $\sum_{i=1}^{n+1} a_i \sigma_i$  toe op  $x$  dan vinden we

$$\sum_{i=1}^{n+1} a_i \sigma_i(x) = \sum_{i=1}^{n+1} a_i \left( \sum_{j=1}^n \xi_j \sigma_i(e_j) \right) = \sum_{j=1}^n \xi_j \left( \sum_{i=1}^{n+1} a_i \sigma_i(e_j) \right) = \sum_{j=1}^n \xi_j \cdot 0 = 0.$$

We vinden zo een niet-triviale lineaire relatie tussen de  $\sigma_i$  in tegenspraak met het lemma van Dedekind/Artin. Dit bewijst de stelling.

De volgende propositie is een variant van (3.7) en het bewijs is volledig analoog.

**(3.9) Propositie.** *Laat  $L$  en  $M$  twee lichaamsuitbreidingen van een gegeven lichaam  $K$  zijn. Neem aan dat  $L/K$  een eindige uitbreiding is. Laat  $\text{Hom}_K(L, M)$  de verzameling*

$$\{ \sigma : L \rightarrow M : \sigma \text{ is een lichaamshomomorfisme en } \sigma|_K = \text{id}_K \}$$

*zijn. Dan geldt  $\#\text{Hom}_K(L, M) \leq [L : K]$ .*

De volgende propositie wordt met gelijksoortige middelen bewezen.

**(3.10) Propositie.** *Gegeven een lichaam  $K$  en een eindige ondergroep  $G$  van  $\text{Aut}(K)$  geldt de relatie*

$$\#G \geq [K : K^G].$$

*Bewijs.* Laat  $r$  de orde van  $G$  zijn en schrijf  $G = \{\sigma_1, \dots, \sigma_r\}$ . Stel dat  $\#G < [K : K^G]$ . Dan zijn er  $r + 1$  elementen, zeg  $e_j$  voor  $j = 1, \dots, r + 1$ , in  $K$  die lineair onafhankelijk zijn over  $K^G$ . Bekijk nu voor  $j = 1, \dots, r + 1$  in de  $K$ -vectorruimte  $K^r$  de vectoren

$$w_j := (\sigma_1^{-1}(e_j), \sigma_2^{-1}(e_j), \dots, \sigma_r^{-1}(e_j)) \in K^r.$$

Deze  $r + 1$  vectoren moeten lineair afhankelijk zijn over  $K$ , dus er is een niet-triviale relatie  $\sum_{j=1}^{r+1} a_j w_j = 0$  met  $a_j \in K$ , dus de relatie

$$\sum_{j=1}^{r+1} a_j \sigma_i^{-1}(e_j) = 0 \quad (2)$$

geldt voor alle  $i = 1, \dots, r$ . Er is minstens een coëfficiënt  $a_j$  ongelijk aan nul. Neem aan dat dit  $a_1$  is (anders hernummeren we de  $e_j$ ). Laat nu  $c$  in  $K$  een element zijn met  $\sum_{i=1}^r \sigma_i(c) \neq 0$ . Zo een element bestaat, want anders zijn de  $\sigma_i$  niet verschillend volgens het lemma van Artin. Door vermenigvuldigen van de relatie (2) met  $c/a_1$  mogen we aannemen dat  $a_1 = c$ . Pas nu  $\sigma_i$  op (2) toe en sommeer deze relaties over  $i$ . Dit geeft

$$\sum_{i=1}^r \sum_{j=1}^{r+1} \sigma_i(a_j) e_j = 0, \quad \text{ofwel} \quad \sum_{j=1}^{r+1} c_j e_j = 0$$

met  $c_j = \sum_{i=1}^r \sigma_i(a_j)$  voor  $j = 1, \dots, r + 1$ . Als we nu bewijzen dat deze coëfficiënten  $c_j$  in  $K^G$  liggen en niet allemaal nul zijn weerspreekt dit onze aanname dat de  $e_1, \dots, e_{r+1}$  lineair onafhankelijk over  $K^G$  zijn.

Om in te zien dat  $c_j \in K^G$  nemen we een element  $\sigma \in G$  en schrijven we

$$\sigma(c_j) = \sigma\left(\sum_{i=1}^r \sigma_i(a_j)\right) = \sum_{i=1}^r (\sigma\sigma_i)(a_j) = \sum_{i=1}^r \sigma_i(a_j) = c_j$$

want met  $\sigma_i$  doorloopt ook  $\sigma\sigma_i$  de hele groep  $G$ . Verder is  $c_1 = \sum_{i=1}^r \sigma_i(c) \neq 0$  volgens aanname. Dit bewijst de propositie.

Tezamen geven de bovenstaande stelling en propositie het volgende resultaat.

**(3.11) Stelling.** *Laat  $L$  een lichaam zijn en  $G$  een eindige ondergroep van  $\text{Aut}(L)$ . Dan geldt*

$$G = \text{Aut}(L/L^G) \quad \text{en} \quad \#G = [L : L^G].$$

*Bewijs.* Omdat  $G$  een eindige ondergroep is van  $\text{Aut}(L/L^G)$  is wegens propositie (3.10) de graad  $[L : L^G]$  eindig en er geldt wegens (3.10) en (3.7)

$$[L : L^G] \leq \#\text{Aut}(L/L^G) \leq [L : L^G],$$

dus de  $\leq$ -tekens zijn in feite gelijkheidstekens. Dit bewijst de stelling.

Bovenstaande resultaten motiveren de volgende definitie.

**(3.12) Definitie.** Een algebraïsche uitbreiding  $L/K$  heet een *Galoisuitbreiding* als

$$K = L^{\text{Aut}(L/K)}.$$

Omdat  $[L : L^{\text{Aut}(L/K)}] = \#\text{Aut}(L/K)$  en  $K \subseteq L^{\text{Aut}(L/K)}$  betekent de conditie voor eindige uitbreidingen

$$L/K \text{ is Galois} \iff [L : K] = \#\text{Aut}(L/K).$$

Merk op dat we in geval  $L/K$  een Galoisuitbreiding is,  $K$  met behulp van de automorfismen kunnen terugvinden en dat er voor ieder element  $x \in L$  dat niet in  $K$  ligt er een automorfisme is dat  $x$  niet op zijn plaats laat.

Van de zojuist genoemde voorbeelden zijn  $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$  en  $\mathbb{Q}(\zeta_5)/\mathbb{Q}$  Galoisuitbreidingen. De uitbreiding  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is dat niet omdat de nodige automorfismen ontbreken. Ook het karakteristiek  $p$  voorbeeld (3.4) is niet Galois.

We komen nu aan de hoofdstelling van de Galoistheorie.

**(3.13) Hoofdstelling van de Galoistheorie.** *Laat  $L/K$  een eindige Galoisuitbreiding zijn en laat  $G = \text{Aut}(L/K)$  de automorfismengroep van  $L/K$  zijn. Dan definieert de afbeelding*

$$H \mapsto L^H$$

*een bijectieve afbeelding van de verzameling ondergroepen van  $G$  naar de verzameling van tussenlichamen  $K \subset F \subset L$  met als inverse afbeelding*

$$F \mapsto \text{Aut}(L/F).$$

*Deze correspondentie keert inclusierelaties om en er geldt*

$$[L : F] = \#H \quad \text{en} \quad [F : K] = [G : H].$$

De groep  $\text{Aut}(L/K)$  heet de *Galoisgroep* van de uitbreiding  $L/K$ . Een alternatieve notatie voor deze groep die we soms ook zullen gebruiken is  $\text{Gal}(L/K)$ . Omdat we hier alleen eindige uitbreidingen bekijken is de Galoisgroep  $G$  een eindige groep en er zijn daarom maar eindig veel ondergroepen. Volgens de hoofdstelling zijn er dan ook maar eindig veel tussenlichamen, een feit dat niet a priori duidelijk is.

We bekijken nu eerst een paar eenvoudige voorbeelden.

**(3.14) Voorbeeld.** Laat  $K = \mathbb{Q}$  en laat  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Deze uitbreiding is een Galoisuitbreiding. Het is niet moeilijk in te zien dat de twee automorfismen  $\sigma$  en  $\tau$  gegeven door

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}$$

en

$$\tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}$$

de twee voortbrengers van de automorfismengroep  $G = \text{Aut}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  zijn. De Viergroep van Klein  $G$  heeft drie echte ondergroepen

$$H_1 = \{1, \sigma\}, \quad H_2 = \{1, \tau\} \quad \text{en} \quad H_3 = \{1, \sigma\tau\}.$$

Volgens de hoofdstelling zijn er dan drie echte tussenlichamen en dit zijn

$$\mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{2}), \quad \text{en} \quad \mathbb{Q}(\sqrt{6}).$$

**(3.15) Voorbeeld.** Laat  $K = \mathbb{Q}$  en  $L = \mathbb{Q}(\zeta_7)$  met  $\zeta_7$  een primitieve zevendemachts eenheidswortel, dus een wortel van  $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ . Dit is een Galoisuitbreiding van  $\mathbb{Q}$  van graad 6 en de Galoisgroep is isomorf met  $\mathbb{Z}/6\mathbb{Z}$  en wordt voortgebracht door  $\sigma : \zeta_7 \mapsto \zeta_7^3$ . (Ga dit na.) De groep  $\mathbb{Z}/6\mathbb{Z}$  heeft twee echte ondergroepen, namelijk  $\langle \sigma^2 \rangle$  van orde 3 en  $\langle \sigma^3 \rangle$  van orde 2. Dus hiermee corresponderen twee deellichamen. We beweren dat dit de lichamen

$$L_1 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \quad \text{en} \quad L_2 = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$$

zijn. Om in te zien dat  $L_1 = L^H$  met  $H = \langle \sigma^3 \rangle$  hoeven we alleen na te gaan dat  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  invariant is onder  $H = \langle \sigma^3 \rangle$ , want  $[L : L^H] = 2$  en  $L_1 \neq \mathbb{Q}$  impliceert dat  $L_1 = L^H$ . Analoog zien we de gelijkheid  $L_2 = L^{\langle \sigma^2 \rangle}$  in.

**(3.16) Voorbeeld.** Laat  $p$  een priemgetal zijn,  $m$  een natuurlijk getal en  $q = p^m$  een macht van  $p$ . Dan is de lichaamsuitbreiding  $\mathbb{F}_q/\mathbb{F}_p$  een Galoisuitbreiding van graad  $m$ . Immers de groep  $\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$  is cyclisch van orde  $m$  en wordt voortgebracht door het Frobeniusautomorfisme  $\phi : x \mapsto x^p$ , zie Algebra 2a, Hoofdstuk 9. Volgens de Hoofdstelling moeten de tussenlichamen  $\mathbb{F}_p \subset F \subset \mathbb{F}_q$  corresponderen met de ondergroepen van  $\mathbb{Z}/m\mathbb{Z}$ . We weten al uit Algebra 2a (9.7) dat de tussenlichamen precies de lichamen  $\mathbb{F}_{p^r}$  zijn met  $r$  een deler van  $m$ ; deze kunnen worden beschreven als  $\{x \in \mathbb{F}_q : \phi^r(x) = x\}$ , dus

$$\mathbb{F}_{p^r} = \mathbb{F}_q^H \quad \text{met} \quad H = \langle \phi^r \rangle,$$

in overeenstemming met de hoofdstelling.

We zullen later meer illustraties van de hoofdstelling zien. We geven nu eerst het bewijs.

*Bewijs van (3.13).* We weten al dat voor een tussenlichaam  $K \subset F \subset L$  de verzameling  $\text{Aut}(L/F)$  een ondergroep van  $G = \text{Aut}(L/K)$  is. Ook weten we dat voor een ondergroep  $H$  van  $G$  de verzameling  $L^H$  een tussenlichaam is. We moeten dus aantonen dat de toevoegingen

$$H \mapsto L^H \mapsto \text{Aut}(L/L^H) \tag{3}$$

en

$$F \mapsto \text{Aut}(L/F) \mapsto L^{\text{Aut}(L/F)} \tag{4}$$

de identiteit zijn op de verzameling van de ondergroepen, resp. van de tussenlichamen. Voor (3) betekent dit  $H = \text{Aut}(L/L^H)$  en dit is precies de inhoud van (3.11). Rest ons na te gaan dat voor ieder tussenlichaam  $F$  geldt  $F = L^{\text{Aut}(L/F)}$ . Schrijf nu  $H = \text{Aut}(L/F)$ . Ieder element  $\sigma \in G$  definiëert een lichaamshomomorfisme  $F \rightarrow L$  en twee elementen  $\sigma_1, \sigma_2 \in G$  definiëren precies dan hetzelfde homomorfisme als  $\sigma_1^{-1}\sigma_2 \in H$ . We krijgen dus een welgedefinieerde *injectieve* afbeelding van de verzameling  $G/H$  van linkernevenklassen  $G/H$  naar de verzameling  $\text{Hom}_K(F, L)$  van lichaamshomomorfismen van  $F$  naar  $L$  die  $K$  vastlaten door aan  $\sigma$  de beperking van  $\sigma$  tot  $F$  toe te voegen

$$G/H \longrightarrow \text{Hom}_K(F, L) \quad \sigma H \mapsto \sigma|_F.$$

We zien dus dat  $\#G/H \leq \#\text{Hom}_K(F, L)$ . Anderzijds levert Propositie (3.9) dat  $\#\text{Hom}_K(F, L) \leq [F : K]$ , dus we zien

$$[G : H] \leq [F : K].$$

Daaruit volgt dat

$$\#\text{Aut}(L/F) = \#H = \#G/[G : H] \geq \#G/[F : K] = [L : K]/[F : K] = [L : F].$$

Combineren we dit met (3.7) dan zien we dat  $\#\text{Aut}(L/F) = [L : F]$  en dus is vanwege (3.11)  $L/F$  een eindige Galoisuitbreiding en  $F = L^H$ . We hebben dan ook gezien dat  $\#\text{Aut}(L/F) = [L : F]$  en daaruit volgt ook direct  $[F : K] = [G : H]$ . Dit bewijst de stelling.

Gegeven een Galoisuitbreiding  $L/K$  rijst nu de vraag wanneer voor een tussenlichaam  $K \subset F \subset L$  de lichaamsuitbreiding  $F/K$  zelf ook weer een Galoisuitbreiding is. De volgende propositie geeft het antwoord.

**(3.17) Propositie.** *Laat  $L/K$  een eindige Galoisuitbreiding zijn en  $F$  een deellichaam met  $K \subseteq F \subseteq L$ . Dan is  $F/K$  een Galoisuitbreiding dan en slechts dan als de ondergroep  $H = \text{Aut}(L/F)$  een normaaldeeler van  $G = \text{Aut}(L/K)$  is.*

*Bewijs.* De Galoisgroep  $G$  werkt op  $L$  en voert een tussenlichaam  $F$  van  $L/K$  in een tussenlichaam  $\sigma(F)$  over en dit levert een inbedding van de verzameling linkernevenklassen  $G/H$  in  $\text{Hom}_K(F, L)$ . Omdat  $\#G/H = [F : K]$  levert dit volgens (3.9) een bijectie  $G/H \xrightarrow{1-1} \text{Hom}_K(F, L)$ . In het bijzonder volgt  $\#\text{Hom}_K(F, L) = [F : K]$ .

Anderzijds,  $\text{Aut}(F/K)$  is een deelverzameling van  $\text{Hom}_K(F, L)$  dus  $\#\text{Aut}(F/K) = [F : K]$  dan en slechts dan als iedere  $\sigma \in G$  het tussenlichaam  $F$  in zich voert. De conditie  $\#\text{Aut}(F/K) = [F : K]$  is wegens (3.11) equivalent met  $F/K$  Galois. Dus  $F/K$  is Galois dan en slechts dan als  $\sigma(F) = F$  voor iedere  $\sigma \in G$ .

Volgens de hoofdstelling hoort het lichaam  $\sigma(F)$  bij de ondergroep  $\sigma H \sigma^{-1}$ , d.w.z.  $\text{Aut}(L/\sigma(F)) = \sigma H \sigma^{-1}$ . We zien dat geldt

$$H \text{ is een normaaldeeler} \iff \sigma(F) = F \text{ voor alle } \sigma \in G.$$

Dit bewijst de propositie.

Als het tussenlichaam  $F$  een Galoisuitbreiding van  $K$  is dan is de Galoisgroep van  $F/K$  isomorf met de quotiëntgroep  $G/H$ . We hebben het volgende plaatje:

$$G \text{ werkt op } L/K \quad \left\{ \begin{array}{l} L \\ | \\ F \\ | \\ K \end{array} \right\} \quad \begin{array}{l} H \text{ werkt op } L/F \\ \text{hier werkt } G/H \text{ als } F/K \text{ Galois} \end{array}$$

### Opgaven

- 1) Geef een bewijs van Propositie (3.9).
- 2) Geeft een voorbeeld van een Galoisuitbreiding  $L/K$  en een tussenlichaam  $K \subset F \subset L$  zodat  $F/K$  geen Galoisuitbreiding is.
- 3) Laat  $K = \mathbb{Q}$  en  $L = \mathbb{Q}(\sqrt[4]{3}, \sqrt{-1}) \subset \mathbb{C}$ . Bewijs dat  $L/K$  een Galoisuitbreiding is en vind alle deellichamen van  $L$  die Galois over  $K$  zijn.

- 4) Laat  $k$  een lichaam zijn en  $L = k(x_1, \dots, x_n)$  het lichaam van rationale functies in  $n$  variabelen. Laat  $K = k(\sigma_1, \dots, \sigma_n)$  het lichaam van de symmetrische functies in de  $x_i$  zijn. Laat zien dat  $L/K$  een Galoisuitbreiding met Galoisgroep de symmetrische groep  $S_n$  is. Laat verder zien dat er voor elke eindige groep  $G$  een Galoisuitbreiding  $F_1/F_2$  bestaat met Galoisgroep isomorf met  $G$ .
- 5) Laat  $L/K$  een Galoisuitbreiding zijn zodat  $\text{Gal}(L/K)$  een cyclische groep is. Bewijs dat er voor iedere deler  $d$  van de graad  $[L : K]$  precies één tussenlichaam van graad  $d$  over  $K$  is.
- 6) Bepaal alle deellichamen van  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}, \sqrt{5})$ .
- 7) Laat  $p$  een priemgetal  $> 2$  zijn. Voor welke  $d \in \mathbb{Z}$  bevat  $\mathbb{Q}(\sqrt{d})$  een primitieve  $p$ -de machts eenheidswortel?
- 8) Laat  $f \in \mathbb{Q}[X]$  een irreducibel polynoom van graad 3 zijn met één reële wortel. Bewijs dat het ontbindingslichaam van  $f$  over  $\mathbb{Q}$  graad 6 over  $\mathbb{Q}$  heeft.
- 9) Bereken de graad van het ontbindingslichaam van  $X^4 + 1$  en van  $X^4 - 1$  over  $\mathbb{Q}$ .
- 10) Laat  $K$  het ontbindingslichaam van  $X^{12} - 1$  over  $\mathbb{Q}$  zijn. Bereken  $[K : \mathbb{Q}]$  en maak de correspondentie tussen de tussenlichamen en de ondergroepen van  $\text{Gal}(K/\mathbb{Q})$  expliciet.
- 11) Laat  $K$  het ontbindingslichaam van  $X^3 - 2$  over  $\mathbb{Q}$  zijn. Bewijs dat de Galoisgroep van  $K/\mathbb{Q}$  isomorf is met de symmetrische groep  $S_3$ .
- 12) Laat  $K/\mathbb{Q}$  een Galoisuitbreiding zijn met Galoisgroep  $D_6$ . Hoeveel deellichamen heeft  $K$ ?
- 13) Laat  $K/\mathbb{Q}$  een Galoisuitbreiding van graad 12 zijn met Galoisgroep  $A_4$ . Bewijs dat er geen tussenlichaam  $F$  is met  $[F : \mathbb{Q}] = 2$ .
- 14) Laat  $L$  het ontbindingslichaam van  $(X^2 - 2)(X^3 - 2)$  zijn over  $\mathbb{Q}$ . Bepaal  $[L : \mathbb{Q}]$ .
- 15) Bewijs dat iedere uitbreiding van graad 2 in karakteristiek  $\neq 2$  een Galoisuitbreiding is.
- 16) Laat  $\Omega/\mathbb{Q}$  een Galoisuitbreiding met Galoisgroep  $S_3$  zijn. Is  $\Omega$  het ontbindingslichaam van een irreducibel polynoom  $f$  van graad 3?
- 17) Laat  $K$  een lichaam zijn en  $M$  een lichaamsuitbreiding van  $K$ . Stel dat  $L_1$  en  $L_2$  tussenlichamen van  $M$  zijn die Galoisuitbreidingen van  $K$  zijn. Laat zien dat  $L_1 \cap L_2$  een Galoisuitbreiding van  $K$  is.

## 4. NORMALE EN SEPARABELE UITBREIDINGEN

*The experience of past centuries shows that the development of mathematics was not due to technical progress, but rather to discoveries of unexpected interrelations between different domains*

V.I. Arnold\*

In dit hoofdstuk geven we een alternatieve definitie van het begrip Galoisuitbreiding en we laten zien onder welke omstandigheden een eindige lichaamsuitbreiding door één element wordt voortgebracht.

**(4.1) Definitie.** Laat  $L/K$  een lichaamsuitbreiding van eindige graad zijn. We noemen de uitbreiding  $L/K$  *normaal* als voor iedere lichaamsuitbreiding  $M/L$  en ieder lichaamsomomorfisme  $\gamma : L \rightarrow M$  met  $\gamma|_K = \text{id}_K$  geldt  $\gamma(L) = L$ .

**(4.2) Voorbeelden.** i) Laat  $K = \mathbb{Q}$  en  $L = \mathbb{Q}(\alpha)$  met  $\alpha \in \mathbb{R}$  een wortel van  $X^3 - 2$ . Deze uitbreiding is niet normaal, want als  $\rho \in \mathbb{C}$  een primitieve derdemachts eenheidswortel is dan definieert  $\gamma(a + b\alpha + c\alpha^2) = a + b\rho\alpha + c\rho^2\alpha^2$  een lichaamsomomorfisme  $\gamma : L \rightarrow \mathbb{C}$  met  $\gamma(L) \neq L$ . De uitbreiding  $L = K(\alpha)$  met  $K = \mathbb{Q}(\rho)$  is wel normaal. ii) Laat  $K = \mathbb{F}_q$  een eindig lichaam zijn en  $L = \mathbb{F}_{q^r}$  een eindige lichaamsuitbreiding. In ieder uitbreidingslichaam  $M$  van  $L$  wordt  $L$  gegeven als de verzameling van de nulpunten van  $X^{q^r} - X = 0$ . Onder een homomorfisme  $\gamma : L \rightarrow M$  gaan nulpunten van  $X^{q^r} - X$  over in nulpunten van dit polynoom, dus  $\gamma(L) = L$  en  $L/K$  is normaal.

We geven nu equivalente criteria voor normale uitbreidingen.

**(4.3) Stelling.** *Laat  $L/K$  een eindige uitbreiding zijn. Dan zijn de volgende uitspraken equivalent:*

- i)  $L/K$  is normaal;
- ii) Voor iedere  $\alpha \in L$  valt het minimumpolynoom van  $\alpha$  over  $K$  in het lichaam  $L$  volledig in lineaire factoren uiteen;
- iii)  $L$  is het ontbindingslichaam van een monisch polynoom  $f$  over  $K$ .

*Bewijs.* i)  $\implies$  ii). Laat  $\alpha \in L$  met minimumpolynoom  $f$ . We kunnen  $L$  krijgen door eindig veel elementen aan  $K$  te adjungeren, zeg  $L = K(b_1, \dots, b_r)$ . Omdat  $L/K$  algebraïsch is zijn de elementen  $b_i$  algebraïsch over  $K$ . Laat  $g_i$  het minimumpolynoom van  $b_i$  over  $K$  zijn. We bekijken nu het polynoom

$$h := f \cdot g_1 \cdots g_r \in K[X].$$

Het ontbindingslichaam  $\Omega_K^h$  van  $h$  over  $K$  is ook het ontbindingslichaam  $\Omega_L^h$  van  $h$  over  $L$  want  $L$  wordt uit  $K$  verkregen door aan  $K$  van iedere  $g_i$  een nulpunt  $b_i$  te adjungeren. In dit ontbindingslichaam, dat we nu noteren met  $\Omega$ , valt  $f$ , een factor van  $h$ , volledig in lineaire factoren uiteen, zeg

$$f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n).$$

---

\* V.I. Arnold, (1937-) Russisch wiskundige

Neem aan dat  $\alpha = \alpha_1$ . We moeten nu laten zien dat de  $\alpha_i$  voor  $i = 2, \dots, n$  in  $L$  liggen. Omdat  $f$  irreducibel is (want minimumpolynoom) en  $f(\alpha_i) = 0$  geldt voor een  $i$  met  $1 \leq i \leq n$

$$K(\alpha) \cong K[X]/f \cong K(\alpha_i).$$

Laat  $\sigma : K(\alpha) \xrightarrow{\sim} K(\alpha_i)$  het corresponderende lichaamsomorfisme met  $\sigma(\alpha) = \alpha_i$  zijn. Omdat  $K(\alpha_i) \subset \Omega$  geldt

$$\Omega_{K(\alpha)}^h = \Omega_{K(\alpha_i)}^h.$$

Volgens Algebra 2, Propositie (8.20) kunnen we het isomorfisme  $\sigma$  voortzetten tot een lichaamsisomorfisme  $\tau : \Omega \xrightarrow{\sim} \Omega$  dat beperkt tot  $K(\alpha)$  het isomorfisme  $\sigma$  levert. Volgens de definitie van normaal geldt  $\tau(L) = L$ , dus  $\alpha_i = \tau(\alpha) \in L$ . Dus i) impliceert ii).

Voor de implicatie ii)  $\implies$  iii) schrijven we weer  $L = K(b_1, \dots, b_n)$  en laten  $f = g_1 \cdots g_n \in K[X]$  met  $g_i$  het minimumpolynoom van  $b_i$  over  $K$ . Dit polynoom is monisch en valt wegens onze aanname volledig in lineaire factoren uiteen. Omdat de nulpunten  $b_1, \dots, b_n$  de uitbreiding  $L$  over  $K$  voortbrengen is  $L$  het ontbindingslichaam van  $f$  over  $K$ . Dit bewijst iii).

Nu nemen we iii) aan, dus  $L = \Omega_K^f$  met  $f \in K[X]$  een monisch polynoom dat in  $L$  volledig splitst

$$f = (X - \alpha_1) \cdots (X - \alpha_n)$$

en  $L = K(\alpha_1, \dots, \alpha_n)$ . Laat  $M$  een willekeurige lichaamsuitbreiding van  $L$  zijn en  $\gamma : L \rightarrow M$  een  $K$ -homomorfisme van  $L$  in  $M$ . We weten dat voor iedere  $\alpha_i$  ook  $\gamma(\alpha_i)$  een nulpunt van  $f$  is, dus  $\gamma$  permuteert de verzameling nulpunten  $\{\alpha_1, \dots, \alpha_n\}$  van  $f$ . Daaruit volgt direct dat  $\gamma(L) = L$ . Dit bewijst de stelling.

**(4.4) Opmerking.** Voor niet-eindige lichaamsuitbreidingen wordt meestal de eigenschap ii) als definitie van normaal genomen.

**(4.5) Definitie.** Laat  $K$  een lichaam zijn. We noemen een monisch polynoom  $f \in K[X]$  *separabel* als  $f$  niet constant is en in een ontbindingslichaam uiteenvalt in lineaire factoren die allemaal verschillend zijn. We noemen een algebraïsch element  $a$  in een lichaamsuitbreiding  $L$  van  $K$  *separabel over  $K$*  als het minimumpolynoom van  $a$  over  $K$  separabel is. Een eindige lichaamsuitbreiding  $L/K$  heet *separabel* als ieder element van  $L$  separabel over  $K$  is. Een uitbreiding die niet separabel is heet ook wel inseparabel. (Soms worden ook elementen die transcendent zijn over  $K$  separabel over  $K$  genoemd.)

**(4.6) Voorbeeld.** Laat  $K = \mathbb{F}_p(t)$  het lichaam van rationale functies in  $t$  over  $\mathbb{F}_p$  zijn. Dan is  $X^p - t$  niet separabel over  $K$ . Ga dit zelf na.

De volgende propositie geeft een criterium voor het separabel zijn van *irreducibele* polynomen.

**(4.7) Propositie.** *Laat  $K$  een lichaam zijn en  $f \in K[X]$  een monisch irreducibel polynoom. Dan geldt:*

$$f \text{ is separabel} \iff f' \neq 0.$$

*Bewijs.* Laat  $\Omega$  een ontbindingslichaam van  $f$  over  $K$  zijn. Dan valt  $f$  in  $\Omega$  in lineaire factoren uiteen. “ $\implies$ ” Neem nu aan dat  $f$  separabel is. Dan kunnen we schrijven

$$f = (X - \alpha)g \quad \text{met } g(\alpha) \neq 0.$$

We vinden dan  $f' = g + (X - \alpha)g'$  en  $f'(\alpha) = g(\alpha) \neq 0$ , dus  $f' \neq 0$ . “ $\Leftarrow$ ” Voor de omkering nemen we aan dat  $f' \neq 0$  en dat  $f$  niet separabel is en leiden dan een tegenspraak af. Als  $\alpha \in \Omega$  een dubbel nulpunt is van  $f$ , dan geldt  $f'(\alpha) = 0$ . Omdat  $f$  het minimumpolynoom is van  $\alpha$  over  $K$ , geldt dat  $f$  een deler is van  $f'$ . Omdat de graad van  $f'$  kleiner is dan de graad van  $f$ , kan dit alleen als  $f' = 0$ . Omdat  $f' \neq 0$  moet  $f$  wel separabel zijn.

**(4.8) Stelling.** *Laat  $K$  een lichaam zijn.*

- i) *Als  $\text{kar}(K) = 0$  is iedere uitbreiding van  $K$  separabel.*
- ii) *Als  $\text{kar}(K) = p > 0$  en  $f \in K[X]$  monisch en irreducibel is dan is  $f$  separabel of er is een irreducibel separabel polynoom  $g \in K[X]$  en een  $n \in \mathbb{Z}_{\geq 1}$  zodat  $f = g(X^{p^n})$ .*

*Bewijs.* i) Volgens bovenstaande propositie is ieder irreducibel monisch polynoom, en dus ieder minimumpolynoom in karakteristiek 0 separabel. ii) Als  $f$  niet separabel is dan  $f' = 0$ . Dat betekent dat alle exponenten in  $f$  deelbaar zijn door  $p$ , dus er is een monisch irreducibel polynoom  $f_1 \in K[X]$  zodat  $f = f_1(X^p)$ . Als  $f_1$  niet separabel is dan is er een polynoom  $f_2$  zodat  $f_1 = f_2(X^p)$ . Met inductie volgt de bewering.

**(4.9) Lemma.** *Laat  $L/K$  een normale lichaamsuitbreiding zijn en  $F$  een tussenlichaam ( $K \subseteq F \subseteq L$ ). Dan is ieder  $K$ -lichaamshomomorfisme  $\sigma : F \rightarrow L$  voort te zetten tot een lichaamsomomorfisme  $\bar{\sigma} : L \rightarrow L$  met  $\bar{\sigma}|_F = \sigma$ .*

*Bewijs.* Kies een element  $a \in L$  en laat  $f$  het minimumpolynoom van  $a$  over  $K$  zijn en  $g$  het minimumpolynoom van  $a$  over  $F$ . Dan is  $g$  een deler van  $f$  in  $F[X]$ . We schrijven  $g = \sum_{i=0}^n c_i X^i$  en stellen  $\sigma(g) = \sum_{i=0}^n \sigma(c_i) X^i$ . Dan is  $\sigma(g)$  is een deler van  $f = \sigma(f)$  in  $L[X]$ . Omdat  $L$  normaal is valt  $f$  in  $L[X]$  in lineaire factoren uiteen, dus  $\sigma(g)$  heeft een nulpunt, zeg  $b$  in  $L$ . Er geldt  $F(a) \cong F[X]/g \cong F(b)$  en door te stellen  $h(a) \mapsto \sigma(h)(b)$  voor polynomen  $h \in F[X]$  krijgen we een uitbreiding van  $\sigma$  tot  $F(a)$ . Omdat  $L$  door adjunctie van eindig veel elementen verkregen kan worden volgt de bewering.

De volgende stelling geeft de beloofde alternatieve karakterisering van een Galois-uitbreiding.

**(4.10) Stelling.** *Laat  $L/K$  een eindige lichaamsuitbreiding zijn. De volgende beweringen zijn equivalent:*

- i)  *$L/K$  is een Galoisuitbreiding;*
- ii)  *$L/K$  is normaal en separabel.*

*Bewijs.* i)  $\implies$  ii). Laat  $a \in L$ . We gaan laten zien dat het minimumpolynoom van  $a$  over  $K$  in  $L[X]$  in verschillende lineaire factoren uiteenvalt. Beschouw de verzameling beelden  $A = \{\sigma(a) : \sigma \in G = \text{Aut}(L/K)\}$  en definieer het polynoom

$$f = \prod_{\alpha \in A} (X - \alpha).$$

Omdat ieder element  $\sigma$  van  $\text{Aut}(L/K)$  de nulpunten permuteert liggen de coëfficiënten van  $f$  in  $L^G = K$ . We zien dat  $f$  separabel is en vanwege  $f(a) = 0$  dat het minimumpolynoom van  $a$  een deler is van  $f$ . Dus valt het minimumpolynoom van  $a$  in verschillende lineaire factoren in  $L[X]$  uiteen. Dit bewijst dat  $L/K$  separabel en normaal is. ii)  $\implies$  i). We moeten laten zien dat  $K = L^{\text{Aut}(L/K)}$ . De inclusie  $K \subset L^{\text{Aut}(L/K)}$

is duidelijk. Voor de inclusie  $L^{\text{Aut}(L/K)} \subset K$  gaan we aantonen dat een element van  $L$  dat niet in  $K$  ligt niet onder geheel  $\text{Aut}(L/K)$  invariant is. Neem een element  $a \in L$  met  $a \notin K$ . We gaan een  $K$ -automorfisme construeren dat  $a$  niet vast laat. Laat  $f$  het minimumpolynoom van  $a$  over  $K$  zijn en laat  $a'$  een ander nulpunt van  $f$  in  $L$  zijn. Zo een  $a' \neq a$  bestaat wegens de separabiliteit van  $L/K$ . Definieer een lichaamshomomorfisme  $\sigma$  door te eisen dat  $\sigma_K = \text{id}_K$  en  $\sigma(a) = a'$ . Volgens Lemma (4.9) bestaat er zo een  $\sigma \in \text{Aut}(L/K)$ . Dit bewijst dat  $L/K$  een Galoisuitbreiding is.

We laten nu zien dat het al dan niet separabel zijn van een lichaamsuitbreiding gecontroleerd kan worden door na te gaan of de voortbrengers separabel zijn.

**(4.11) Stelling.** *Zij  $K$  een lichaam en  $L/K$  een normale lichaamsuitbreiding. Laat  $a_1, \dots, a_n \in L$  en laat  $F = K(a_1, \dots, a_n)$ . Dan zijn de volgende uitspraken equivalent:*

- i)  $F/K$  is separabel;
- ii)  $a_1, \dots, a_n$  zijn separabel over  $K$ ;
- iii)  $\#\text{Hom}_K(F, L) = [F : K]$ .

*Bewijs.* i)  $\implies$  ii). Dit volgt direct uit de definitie. ii)  $\implies$  iii). Omdat  $a_1$  separabel is en  $L$  normaal over  $K$  heeft het minimumpolynoom  $f_1$  van  $a_1$  over  $K$  precies  $d_1 := \text{graad}(f_1)$  verschillende nulpunten in  $L$ , dus we vinden door  $a_1$  naar een van de andere nulpunten van  $f_1$  te sturen precies  $\text{graad}(f_1)$  homomorfismen  $\sigma : F_1 := K(a_1) \rightarrow L$ . Bekijk nu  $F_2 := K(a_1, a_2) = F_1(a_2)$ . Beschouw het minimumpolynoom  $f_2$  van  $a_2$  over  $F_1$ . Wegens de separabiliteit van  $a_2$  heeft dit polynoom  $f_2$  precies  $d_2 = \text{graad}(f_2)$  nulpunten in  $L$ . We kunnen ieder van onze  $d_1$  homomorfismen  $\sigma \in \text{Hom}(F_1, L)$  dus voortzetten tot  $d_2$  homomorfismen  $F_2 \rightarrow L$ . Zo kunnen we verder gaan met  $F_3 := F_2(a_3)$  etc. Dit bewijst dat  $\#\text{Hom}(F, L) = d_1 d_2 \cdots d_n = [F : K]$ . iii)  $\implies$  i). Stel  $F/K$  is niet separabel. Dan is er een element  $\alpha \in F$  waarvoor het minimumpolynoom  $f$  minder nulpunten heeft in  $L$  dan  $\text{graad}(f)$ . Een homomorfisme  $K(\alpha) \rightarrow L$  moet  $\alpha$  naar een ander nulpunt sturen. Dus we zien

$$\#\text{Hom}_K(K(\alpha), L) < [K(\alpha) : K]. \quad (1)$$

Nu laat ieder homomorfisme  $\tau$  in  $\text{Hom}_K(K(\alpha), L)$  zich voortzetten tot  $F$  omdat  $L$  normaal is. Laat  $\sigma_1$  een voortzetting zijn. Als  $\sigma_2$  een tweede voortzetting is dan komen ze overeen op  $\tau(K(\alpha))$ . Door aan zo een voortzetting  $\sigma_2$  nu het homomorfisme  $\sigma_2 \sigma_1^{-1} : \sigma_1(F) \rightarrow L$  toe te voegen dat de identiteit op  $\tau(K(\alpha))$  is, zien we met Propositie (3.9) dat er hoogstens  $[\sigma_1(F) : \tau(K(\alpha))] = [F : K(\alpha)]$  voortzettingen zijn. In totaal vinden we met (1) dus

$$\#\text{Hom}_K(F, L) < [K(\alpha) : K] \cdot [F : K(\alpha)] = [F : K].$$

Deze tegenspraak bewijst iii)  $\implies$  i).

**(4.12) Stelling van het Primitieve Element.** *Laat  $L/K$  een eindige separabele uitbreiding zijn. Dan is er een element  $a \in L$  met  $L = K(a)$ .*

*Bewijs.* Als  $K$  een eindig lichaam is, dan is  $L$  ook een eindig lichaam. De groep  $L^*$  is dan cyclisch. Door een voortbrenger  $\alpha$  van deze groep te adjungeren wordt  $L$  verkregen. Dus de stelling geldt voor eindige lichamen.

Daarom mogen we nu aannemen dat  $K$  oneindig veel elementen bezit. Stel dat  $L = K(a_1, \dots, a_n)$  met  $a_i \in L$ . Laat  $f_i$  het minimumpolynoom van  $a_i$  over  $K$  zijn en

laat  $g = \prod f_i$ . Dan is het ontbindingslichaam  $\Omega$  van  $g$  over  $K$  een normale uitbreiding (wegens (4.3)) die  $L$  bevat. Iedere  $f_i$  is separabel over  $K$  en dus is wegens (4.11)  $\Omega/K$  ook separabel, dus  $\Omega/K$  is een Galoisuitbreiding. Volgens de hoofdstelling van de Galoistheorie zijn er maar eindig veel tussenlichamen  $K \subset F \subset \Omega$ , en dus ook maar eindig veel tussenlichamen  $K \subset F \subset L$ .

We kiezen nu een element  $a \in L$  waarvoor de graad  $[K(a) : K]$  maximaal is en gaan nu bewijzen dat  $L = K(a)$ . Kies een willekeurig element  $b \in L$ . Bekijk de lichaamsuitbreidingen  $K(ca + b)$  waarbij  $c$  het lichaam  $K$  doorloopt. Omdat er maar eindig veel tussenlichamen zijn, bestaan er verschillende  $c_1$  en  $c_2$  in  $K$  met  $K(c_1a + b) = K(c_2a + b)$ . Uit de identiteit

$$a = \frac{(c_1a + b) - (c_2a + b)}{c_1 - c_2}$$

volgt dat  $a \in K(c_1a + b)$ , dus wegens de maximaliteit volgt  $K(a) = K(c_1a + b)$  en dus  $b \in K(a)$ . Aangezien  $b$  willekeurig was volgt  $L = K(a)$ . Dit bewijst de stelling.

**(4.13) Definitie.** Een lichaam  $K$  heet *perfect* als iedere algebraïsche uitbreiding van  $K$  separabel is.

**(4.14) Stelling.** Een lichaam van karakteristiek 0 is perfect. Een lichaam  $K$  van karakteristiek  $p > 0$  is dan en slechts dan perfect als ieder element van  $K$  een  $p$ -de machts wortel in  $K$  bezit.

*Bewijs.* De eerste bewering volgt direct uit Stelling (4.8) i). Voor de tweede bewering gebruiken we ii) van diezelfde Stelling (4.8). Als ieder element van  $K$  een  $p$ -de machts wortel bezit kan een polynoom van de vorm  $f(X^p)$  in  $K[X]$  geschreven worden als  $p$ -de macht in  $K[X]$ :

$$f(X^p) = \sum_{i=0}^n a_i X^{pi} = \sum_{i=0}^n (\sqrt[p]{a_i} X^i)^p = \left( \sum_{i=0}^n \sqrt[p]{a_i} X^i \right)^p.$$

Daaruit volgt dat ieder monisch irreducibel polynoom in  $K[X]$  separabel is. Dus het lichaam  $K$  is perfect. Omgekeerd, als  $K$  perfect is, dan moet  $X^p - a$  voor elke  $a$  in  $K$  een separabele uitbreiding geven. Dat is alleen dan het geval als  $a$  een  $p$ -de macht in  $K$  is. Dit bewijst de stelling.

**(4.15) Stelling.** Laat  $K$  een lichaam van karakteristiek  $p > 0$  zijn. Een lichaamsuitbreiding  $L/K$  van graad  $[L : K] = p$  is een Galoisuitbreiding dan en slechts dan als  $L = K(\alpha)$  met  $\alpha$  een nulpunt van een irreducibel polynoom  $f \in K[x]$  van de vorm  $x^p - x - a$ .

*Bewijs.* ‘ $\Leftarrow$ ’ Stel  $f = x^p - x - a \in K[x]$  is irreducibel en  $\alpha \in L$  een nulpunt van  $f$ . Dan zijn  $\alpha + i$  met  $i \in \mathbb{F}_p$  ook nulpunten. Dus  $K(\alpha)$  is een ontbindingslichaam van  $f$  en  $f$  is separabel. Dus  $L = K(\alpha)/K$  is een Galoisuitbreiding met als Galoisgroep een cyclische groep van orde  $p$  voortgebracht door  $\alpha \mapsto \alpha + 1$ . Voor ‘ $\Rightarrow$ ’, laat  $L/K$  Galois zijn met een groep van orde  $p$  voortgebracht door  $\sigma$ . Beschouw voor  $x \in L$  het ‘spoor’

$$S(x) = x + \sigma(x) + \sigma^2(x) + \dots + \sigma^{p-1}(x).$$

Omdat  $\sigma(S(x)) = S(x)$  ligt  $S(x)$  in  $K$ . Omdat de  $\sigma^i$  voor  $i = 0, \dots, p-1$  allemaal verschillend zijn is er volgens Lemma (3.8) een element  $x \in L$  zodat  $S(x) \neq 0$ . Laat nu

$$y = \sum_{i=0}^{p-1} i \sigma^i(x).$$

Dan zien we dat

$$\sigma(y) = \sum_{i=0}^{p-1} i \sigma^{i+1}(x) = \sum_{i=1}^p (i-1) \sigma^i(x) = \sum_{i=1}^p i \sigma^i(x) - \sum_{i=1}^p \sigma^i(x)$$

dus we zien

$$\sigma(y) = y - S(x).$$

Stel nu  $\alpha = -y/S(x)$ . Dan vinden we

$$\sigma(\alpha) = -\sigma(y)/S(x) = \frac{-y + S(x)}{S(x)} = \alpha + 1.$$

Laat nu  $a := \alpha^p - \alpha$ . Dan geldt  $\sigma(a) = a$  en dus is  $\alpha$  een nulpunt van  $x^p - x - a$ . Merk op dat  $\alpha \notin K$  want voor  $x \in K$  geldt  $S(x) = px = 0$ . Dus  $\alpha$  brengt een niet-triviale lichaamsuitbreiding van  $K$  voort en die moet gezien de graad gelijk zijn aan  $L$ . Het minimumpolynoom van  $\alpha$  moet dus van graad  $p$  zijn en omdat  $\alpha$  een nulpunt is van  $x^p - x - a$  moet dit het minimumpolynoom zijn. Daarmee is de stelling bewezen.

### Opgaven

- 1) Laat  $K$  een lichaam zijn en  $f \in K[X]$  een monisch polynoom. Bewijs dat de volgende uitspraken equivalent zijn: i)  $f$  is separabel; ii)  $f$  en  $f'$  zijn onderling ondeelbaar in  $K[X]$ ; iii) De discriminant van  $f$  (zie Hoofdstuk 1) is niet nul.
- 2) Laat  $L/K$  een Galoisuitbreiding zijn en  $F$  een tussenlichaam. Bewijs:  $F/K$  is normaal dan en slechts dan als  $\text{Aut}(L/F)$  een normaaldeeler van  $\text{Aut}(L/K)$  is.
- 3) Laat  $K$  een lichaam zijn en  $\zeta$  een primitieve  $n$ -demachts eenheidswortel in een uitbreidingslichaam. Neem aan dat de karakteristiek van  $K$  geen deler is van  $n$ . Bewijs dat  $K(\zeta)$  een Galoisuitbreiding van  $K$  is en dat de Galoisgroep van  $L/K$  abels is.
- 4) Bewijs dat iedere eindige uitbreiding van een perfect lichaam perfect is.
- 5) Laat  $L/K$  een Galoisuitbreiding zijn met abelse Galoisgroep. Bewijs dat ieder tussenlichaam  $F$  Galois over  $K$  is.
- 6) Laat  $K = \mathbb{F}_p(t)$  het lichaam van rationale functies over  $\mathbb{F}_p$  zijn. Laat zien dat  $f = X^p - X - t$  geen wortels in  $K$  heeft. Laat verder zien dat het ontbindingslichaam  $\Omega$  van  $f$  over  $K$  een Galoisuitbreiding van  $K$  is met een Galoisgroep van orde  $p$ .
- 7) Laat  $R = \mathbb{F}_p[s, t]$  de polynoomring in twee variabelen over  $\mathbb{F}_p$  zijn en  $K = Q(R) = \mathbb{F}_p(s, t)$  het quotiëntenlichaam van  $R$ .
  - i) Bewijs dat  $K^p := \{a^p : a \in K\}$  een deellichaam van  $K$  is.
  - ii) Bewijs  $[K : K^p] = p^2$ .
  - iii) Er bestaat geen element  $\alpha$  in  $K$  met  $K = K^p(\alpha)$ . Bewijs dit.

8) Laat  $L/K$  een algebraïsche lichaamsuitbreiding zijn en definiëer

$$L_s := \{a \in L : a \text{ is separabel over } K\}.$$

Bewijs dat  $L_s$  een deellichaam van  $L$  is. Bewijs verder dat  $L$  zuiver inseparabel is over  $L_s$ , d.w.z. als  $p = \text{kar}(K)$  dan is er voor ieder element  $b \in L$  een  $n$  zodat  $b^{p^n} \in L_s$ .

9) Laat  $p > 2$  een priemgetal zijn. Bewijs dat het lichaam  $\mathbb{Q}(\zeta_p)$  van de  $p$ -de machts eenheidswortels precies één kwadratisch deellichaam heeft, namelijk  $\mathbb{Q}(\sqrt{\pm p})$ , waarbij het teken gelijk is aan  $(-1)^{(p-1)/2}$ .

10) Laat  $f \in \mathbb{F}_q[x]$  een polynoom zijn van positieve graad waarvan de afgeleide nul is. Bewijs dat  $f$  niet irreducibel is.

## 5. OPLOSBAARHEID

*Quae quantitas vere est sophistica*  
Cardano\*

De wortels van de algebra zoals wij die nu beoefenen liggen bij het zoeken naar de oplossingen van vergelijkingen. Het zoeken naar een algemene formule voor de oplossing van derdegraads vergelijkingen was het onderwerp van een felle competitie in het begin van de 16de eeuw in Italië. Het lijkt erop dat del Ferro\*\* als eerste de oplossing vond (wellicht al rond 1515), maar dit bleek pas na zijn dood. In de tussentijd had Niccolò Fontana\*\*\*, bijgenaamd Tartaglia (de stotteraar) ook een oplossing gevonden in 1535. Hij heeft zijn vondst na lang aandringen meegedeeld aan Girolamo Cardano, die deze oplossing uitbreidde en als eerste gepubliceerd heeft in zijn boek *Ars Magna*. Ferrari\*\*\*\*, een leerling van Cardano, heeft laten zien dat de algemene vierdegraads vergelijking teruggebracht kan worden tot de derdegraads vergelijking. Lange tijd was het een open probleem of ook voor hogeregraads vergelijkingen dergelijke formules voor de oplossingen te vinden zijn. In het begin van de 19de eeuw werd door Abel en Galois, na voorbereidend werk van Lagrange en Ruffini\*\*\*\*\* definitief bewezen dat voor de algemene vergelijking van graad  $\geq 5$  een dergelijke wortelformule niet bestaat. De sleutel tot dit inzicht was het bestuderen van de symmetrieën van de wortels van de vergelijking en dit leidde uiteindelijk tot de Galoistheorie. Voor een kort overzicht met verdere verwijzingen naar de literatuur zie: van der Waerden, *A History of Algebra*, Springer Verlag, 1985.

**Aanname.** Terwille van de eenvoud beperken we ons in dit hoofdstuk tot lichamen van karakteristiek 0.

We beginnen met een definitie.

**(5.1) Definitie** Een eindige lichaamsuitbreiding  $L/K$  heet een *worteluitbreiding* als er elementen  $a_1, \dots, a_m$  in  $L$  zijn en positieve gehele getallen  $n_1, \dots, n_m$  zodat  $L = K(a_1, \dots, a_m)$  met  $a_1^{n_1} \in K$ , en  $a_i^{n_i} \in K(a_1, \dots, a_{i-1})$  voor  $i = 2, \dots, m$ .

De uitbreiding  $L/K$  wordt dus verkregen door telkens een wortel van een vergelijking

$$X^{n_i} - a_i = 0$$

te adjungeren. Met zo een  $n$ -de machts wortel uit een element is het relatief makkelijk rekenen en in zekere zin begrijpen we dergelijke lichaamsuitbreidingen relatief goed.

Een eenvoudig voorbeeld wordt gegeven door kwadratische uitbreidingen in karakteristiek  $\neq 2$ . Een uitbreiding  $L/K$  van graad twee wordt gegeven door adjunctie van een wortel van een irreducibel polynoom  $f = aX^2 + bX + c$  in  $K[X]$  met  $a \neq 0$ . Zo een wortel is te schrijven als

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

---

\* Girolamo Cardano, Italiaans wiskundige, 1501-1576

\*\* Scipione del Ferro, Italiaans wiskundige, 1465-1526

\*\*\* Niccolò Fontana, bijgenaamd Tartaglia, Italiaans wiskundige 1499-1557

\*\*\*\* Luigi Ferrari, Italiaans wiskundige, 1522-1565

\*\*\*\*\* Paolo Ruffini, Italiaans wiskundige, 1765-1822

dus  $L = K(\sqrt{b^2 - 4ac})$ , waarmee duidelijk is dat dit een worteluitbreiding is.

Laat nu  $f = X^3 + aX^2 + bX + c \in K[X]$  een monisch derdegraads polynoom zijn, waarbij de coëfficiënten uit een lichaam  $K$  komen dat niet van karakteristiek 2 of 3 is. Door een substitutie  $Y = X - a/3$  gaat de vergelijking over in  $Y^3 + pY + q = 0$  en we schrijven nu weer  $X$  voor  $Y$ . Het gaat er dus om een vergelijking

$$X^3 + pX + q = 0 \quad (1)$$

op te lossen. Het idee van Cardano is om een “merkwaardig product” te gebruiken:

$$(\xi + \eta)^3 = \xi^3 + 3(\xi + \eta)\xi\eta + \eta^3,$$

ofwel

$$(\xi + \eta)^3 - 3\xi\eta(\xi + \eta) - \xi^3 - \eta^3 = 0. \quad (2)$$

Als we de twee vergelijkingen (1) en (2) naast elkaar zetten zien we dat we met een substitutie  $X = \xi + \eta$  een oplossing hebben als we de twee volgende vergelijkingen kunnen oplossen

$$3\xi\eta = -p, \quad \xi^3 + \eta^3 + q = 0. \quad (3)$$

De eerste vergelijking in (3) geeft  $\eta = -p/3\xi$  en we substitueren dit in de tweede. Dit geeft

$$\xi^3 - p^3/27\xi^3 + q = 0,$$

en dus

$$27\xi^6 + 27q\xi^3 - p^3 = 0.$$

Maar dit is een vierkantsvergelijking in  $\xi^3$  en die kunnen we oplossen. Schrijf  $u = \xi^3$  dan heeft de vergelijking  $27u^2 + 27qu - p^3 = 0$  de oplossingen

$$u = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Omdat  $\xi = \sqrt[3]{u}$  en  $\eta^3 = -\xi^3 - q$ , geeft dit dan de beroemde formules van Cardano voor  $\alpha = \xi + \eta$  met

$$\xi = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$\eta = \sqrt[3]{-\xi^3 - q} = \sqrt[3]{-\frac{q}{2} \mp \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}},$$

waarbij opgemerkt dient te worden dat deze formules voor Cardano alleen betekenis hadden als de reële wortel  $\sqrt[3]{}$  (resp.  $\sqrt{\quad}$ ) uit een reëel getal (resp. niet-negatief reëel getal) werd getrokken.

We willen deze oplossingen nu begrijpen in het kader van wat de Galoistheorie hierover zegt. Laat  $\Omega$  een ontbindingslichaam van  $f$  over  $K$  zijn. Dan kunnen we  $f$  in  $\Omega[X]$  ontbinden als

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

Als we veronderstellen dat  $f$  irreducibel is in  $K[X]$ , dan is  $K(\alpha_i)$  een derdegraadsuitbreiding van  $K$  bevat in  $\Omega$ . Nu zijn er twee mogelijkheden:

- i)  $\Omega = K(\alpha_1)$ , of
- ii)  $\Omega$  is een uitbreiding van graad 2 van  $K(\alpha_1)$ .

In het eerste geval is  $\Omega$  een Galoisuitbreiding van  $K$  met Galoisgroep van orde 3, dus isomorf met  $\mathbb{Z}/3\mathbb{Z}$ . In het tweede geval is  $\Omega$  een Galoisuitbreiding van graad 6. Immers, na adjunctie van  $\alpha_1$  moeten we nog een kwadratische vergelijking  $f/(X - \alpha_1) = 0$  oplossen. Omdat ieder automorfisme van  $\Omega$  de drie nulpunten  $\alpha_i$  moet permuteren en ook bepaald is door deze permutatie, is  $\text{Gal}(\Omega/K)$  een ondergroep van de symmetrische groep  $S_3$ . In het eerste geval is de Galoisgroep isomorf met de alternerende groep  $A_3$ , en in het tweede geval (als  $[\Omega : K] = 6$ ) is de Galoisgroep isomorf met  $S_3$ .

Stel  $[\Omega : K] = 6$ . Volgens de hoofdstelling hoort bij de ondergroep  $A_3$  een deellichaam  $F$  van  $\Omega$  met  $[F : K] = 2$ . Om dit lichaam te vinden bekijken we de uitdrukking

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

Het is duidelijk dat  $\delta$  invariant is onder  $A_3$ , maar niet onder  $S_3$ . Omdat  $G$  niet bevat is in  $A_3$ , brengt dit element, de wortel uit de discriminant  $D$  van onze vergelijking, een deellichaam van graad 2 over  $K$  voort:  $F = K(\sqrt{D})$  met  $D = \delta^2 = -4p^3 - 27q^2$ .

In het geval dat  $[\Omega : K] = 3$  is  $\delta$  wel invariant onder de gehele Galoisgroep en ligt dus in  $K$ . Dan is de discriminant  $D = \delta^2$  dus een kwadraat in  $K$ .

**(5.2) Conclusie.** *Het ontbindingslichaam  $\Omega$  van een irreducibel polynoom  $f \in K[X]$  van graad 3 (in karakteristiek  $\neq 2$  en  $\neq 3$ ) is van graad 3 over  $K$  dan en slechts dan als de discriminant  $D$  een kwadraat in  $K$  is. Is  $D$  geen kwadraat dan geldt  $[\Omega : K] = 6$ .*

De formules van Cardano spelen in een lichaam dat het ontbindingslichaam van  $f$  over  $K$  en de derdemachtseenheidswortels bevat. In de formules van Cardano treedt  $\sqrt{-3D}$  met  $D$  de discriminant op; vergelijk Opgave 16. Als ons lichaam een derdemachts eenheidswortel bevat dan geldt  $K(\sqrt{D}) = K(\sqrt{-3D})$  en dan is het blijkbaar zo dat de graad 3 uitbreiding  $\Omega/F$  verkregen kan worden door een vergelijking van de vorm  $X^3 - a$  op te lossen met  $a \in F$ .

**(5.3) Lemma.** *Laat  $f \in K[X]$  een polynoom van graad  $n$  zijn en  $\Omega$  het ontbindingslichaam van  $f$  over  $K$ . Dan werkt de Galoisgroep  $\text{Gal}(\Omega/K)$  op de verzameling wortels van  $f$  in  $\Omega$  en dit geeft een inbedding  $G \rightarrow S_n$  in de symmetrische groep van de wortels. Verder geldt:  $f$  is irreducibel dan en slechts dan als de nulpunten van  $f$  één baan vormen onder de werking van  $G$ .*

*Bewijs.* Als  $a$  een nulpunt is van  $f \in K[X]$  in  $\Omega$  en  $\sigma \in G = \text{Gal}(\Omega/K)$  een automorfisme, dan is  $\sigma(a)$  ook weer een nulpunt van  $f$ . Een automorfisme levert dus een permutatie van de wortels van  $f$ . Omdat  $\Omega$  wordt verkregen door adjunctie van de wortels van  $f$  ligt een automorfisme  $\sigma$  volledig vast door deze permutatie. Dit levert een inbedding  $G \rightarrow S_n$ . Voor een nulpunt  $a$  van  $f$  bekijken we de verzameling  $A = \{\sigma(a) : \sigma \in G\}$ . Dan is

$$g = \prod_{b \in A} (X - b)$$

een polynoom dat invariant is onder  $G$  en dat dus in  $K[X]$  ligt. (Hier gebruiken we dat  $\Omega/K$  Galois is.) We beweren dat dit het minimumpolynoom van  $a$  over  $K$  is. Het minimumpolynoom  $h$  van  $a$  deelt  $g$  want  $a$  is een nulpunt van  $g$ . Omgekeerd, ieder nulpunt  $b$  van  $g$  is ook een nulpunt van  $h$  want van de vorm  $\sigma(a)$  met  $\sigma \in G$ . We zien dat  $f$  irreducibel is dan en slechts dan als  $f = cg$  met  $c \in K^*$ . Merk nu op dat de nulpunten van  $g$  precies één baan vormen.

**(5.4) Opmerking.** i) Het bewijs geeft ons een methode om het minimumpolynoom van een element  $a$  in een Galoisuitbreiding  $L/K$  te maken: als  $A = \{\sigma(a) : \sigma \in \text{Gal}(L/K)\}$  dan is

$$g = \prod_{b \in A} (X - b)$$

het minimumpolynoom.

ii) Voor een polynoom  $f \in K[X]$  definiëren we de *Galoisgroep van  $f$*  als de Galoisgroep van het ontbindingslichaam van  $f$  over  $K$ .

We bekijken nu de nulpunten van vierdegraadspolynomen. Laat  $f \in K[X]$  een monisch irreducibel vierdegraads polynoom zijn, zeg

$$f = X^4 + aX^3 + bX^2 + cX + d$$

met ontbindingslichaam  $L$  over  $K$ . Door een transformatie  $x \mapsto x - a/4$  kunnen we bereiken dat het polynoom de gedaante

$$f = X^4 + pX^2 + qX + r$$

krijgt. Volgens Stelling 5.6 is de Galoisgroep  $G$  van  $L/K$  een ondergroep van  $S_4$  en de nulpunten van  $f$ , zeg  $\alpha_1, \dots, \alpha_4$ , vormen één baan onder de werking van  $G$ . Dus  $G$  is een *transitieve ondergroep* van  $S_4$ , m.a.w. deze ondergroep werkt transitief op de nulpunten. Volgens Opgave 14 zijn er de volgende transitieve ondergroepen van  $S_4$ :

$$S_4, A_4, D_4 = \langle (1234), (12)(34) \rangle, V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}, C_4 = (1234),$$

en twee geconjugeerde ondergroepen van deze  $D_4$  en twee geconjugeerde ondergroepen van deze cyclische ondergroep  $C_4$ . De ondergroepen  $A_4$  en  $V_4$  zijn normaaldelers.

Een eerste vraag is nu of  $G \subseteq A_4$ . Hiervoor gebruiken we weer de discriminant  $D$  van  $f$ :

$$\delta = \prod_{1 \leq i < j \leq 4} (\alpha_i - \alpha_j), \quad D = \delta^2.$$

Dit is een polynoom in de coëfficiënten  $p, q$  en  $r$  van  $f$ :

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

Als  $D$  een kwadraat in  $K$  is dan is de Galoisgroep van  $f$  (dus van  $L/K$ ) bevat in  $A_4$ , de alternerende groep. Als  $D$  een kwadraat is in  $K$  dan volgt dat  $G = A_4$  of  $G = V_4$ , want dit zijn de enige transitieve ondergroepen van  $A_4$ .

Als  $D$  geen kwadraat is in  $K$  dan zien we dat  $G$  isomorf is met  $S_4, D_4$  of  $\mathbb{Z}/4\mathbb{Z}$ . We merken nu op dat  $D_4$  de ondergroep van  $S_4$  is die onder conjugatie het element  $(13)(24)$

vastlaat, ofwel de ondergroep die de uitdrukking  $x_1x_3 + x_2x_4$  vastlaat. (Ga dit na.) Als we nu willen weten of  $G \subseteq D_4$  kijken we naar de uitdrukkingen

$$\lambda_1 = \alpha_1\alpha_3 + \alpha_2\alpha_4$$

en

$$\lambda_2 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \lambda_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Er geldt nu dat  $G \subseteq D_4$  dan en slechts dan als  $\lambda_1 \in K$ . Het polynoom

$$g = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

is invariant onder geheel  $S_4$  en ligt dus in  $K[X]$ . Het heet de *cubische resolvent* van  $f$ . Uitrekenen van  $g$  geeft

$$g = X^3 - pX^2 - 4rX + 4pr - q^2.$$

Merk op dat  $\lambda_1 - \lambda_2 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$ , dus de discriminant van  $g$  is gelijk aan de discriminant van  $f$ . (Merk op dat dit een eenvoudige manier geeft om de discriminant van  $f$  te berekenen.) We vinden nu een deellichaam  $\Omega_K^g = K(\lambda_1, \lambda_2, \lambda_3)$  van  $L$ .

**Lemma.** *i) Als  $D$  een kwadraat in  $K$  is en  $g$  is irreducibel dan  $G = A_4$ . ii) Als  $D$  geen kwadraat in  $K$  is en  $g$  is irreducibel dan  $G = S_4$ . iii) Als  $D$  een kwadraat is en  $g$  is reducibel dan  $G = V_4$ . iv) Als  $D$  geen kwadraat in  $K$  is en  $g$  is reducibel dan  $G \cong D_4$  of  $D$  is cyclisch van orde 4.*

*Bewijs.* Als  $D$  een kwadraat in  $K$  is dan is  $G$  bevat in  $A_4$ , dus gelijk aan  $A_4$  of  $V_4$ . Verder is  $G$  alleen bevat in  $D_4$  of een van de twee geconjugeerde ondergroepen van  $D_4$  als  $G$  een van de  $\lambda_i$  vastlaat, dus als  $g$  een nulpunt heeft in  $K$ . Dit bewijst i) en iii). Als  $D$  geen kwadraat is in  $K$  dan  $G \not\subseteq A_4$  en 2 deelt  $[L : K]$ . Als  $g$  irreducibel is moet 3 ook een deler van  $[L : K]$  zijn, dus  $G = S_4$  (zie de lijst transitieve ondergroepen). Dit bewijst ii). Als  $D$  geen kwadraat is en  $g$  is reducibel blijven alleen  $G \cong D_4$  of  $G \cong \mathbb{Z}/4\mathbb{Z}$  over. Dit bewijst iv).

Om nu het geval iv) van dit Lemma verder te analyseren merken we op dat  $G$  alleen alle drie  $\lambda_i$  vastlaat als  $G \subset V_4$ . Dus als  $D$  geen kwadraat is en  $g$  reducibel is mag  $g$  niet volledig in lineaire factoren splitsen. Neem nu aan dat  $\lambda_1 \in K$ . Dan is  $G$  gelijk aan  $D_4$  of de cyclische groep  $\langle (1234) \rangle$ . Er geldt  $K(\sqrt{D}) \subset K(\lambda_1, \lambda_2, \lambda_3)$  en beide lichamen zijn kwadratisch, dus gelijk aan elkaar. Het ontbindingslichaam van  $g$  over  $K(\sqrt{D})$  heeft nu graad 2 of 4. Zie Opgave 15.

We voeren nu een begrip uit de groepentheorie in dat we nodig hebben.

**(5.4) Definitie.** Een eindige groep  $G$  heet *oplosbaar* als er een rij ondergroepen  $G_0 = (0) \subset G_1 \subset \dots \subset G_n = G$  is zodat  $G_i$  een normaaldeeler is van  $G_{i+1}$  voor  $i = 0, \dots, n-1$  en  $G_{i+1}/G_i$  abels is.

**(5.5) Voorbeeld.** De rij  $(0) \subset A_3 \subset S_3$  laat zien dat  $S_3$  oplosbaar is. De groep  $S_5$  is niet oplosbaar. De enige niet-triviale normaaldeeler van  $S_5$  is  $A_5$ , zie hierna. De groep  $A_5$  is simpel, d.w.z. heeft geen niet-triviale normaaldelers, en het quotiënt  $A_5/(0) = A_5$  is niet abels.

**(5.6) Propositie.** *Laat  $K$  een lichaam zijn van karakteristiek 0. Als  $L$  het ontbindingslichaam is van  $X^n - a$  voor zekere  $a \in K$ ,  $a \neq 0$ , dan is de Galoisgroep  $\text{Gal}(L/K)$  een oplosbare groep.*

*Bewijs.* Laat  $\zeta_n$  een primitieve  $n$ -de machts eenheidswortel zijn. Omdat het quotiënt van twee wortels van  $X^n - a$  een  $n$ -de machts eenheidswortel is, zien we in dat  $X^n - a$  in  $L[X]$  uiteen valt als  $\prod_{j=1}^n (X - \zeta_n^j \alpha)$  en zo is  $K(\zeta_n)$  een deellichaam van  $L$ . Dit is het ontbindingslichaam van  $X^n - 1$ , dus dit is volgens (4.3) een Galoisuitbreiding van  $K$ . We weten dat  $K(\zeta_n)/K$  een Galoisuitbreiding met abelse Galoisgroep is, zie Opgave 3 van Hoofdstuk 4. Hiermee correspondeert volgens de Hoofdstelling van de Galoistheorie een normaaldeeler  $H = \text{Gal}(L/K(\zeta_n))$  van  $G = \text{Gal}(L/K)$  en het quotiënt  $G/H$  is de abelse groep  $\text{Gal}(K(\zeta_n)/K)$ .

We laten nu zien dat de Galoisgroep  $H = \text{Gal}(L/K(\zeta_n))$  een abelse groep is. Een automorfisme  $\sigma$  dat de identiteit is op  $K(\zeta_n)$  is volledig bepaald door  $\sigma(\alpha)$ . Stel  $\sigma(\alpha) = \zeta_n^j \alpha$ . Als  $\tau$  een ander automorfisme is met  $\tau(\alpha) = \zeta_n^k \alpha$  dan geldt  $\tau\sigma(\alpha) = \tau(\zeta_n^j \alpha) = \zeta_n^j \tau(\alpha) = \zeta_n^{j+k} \alpha$  en evenzo  $\sigma\tau(\alpha) = \sigma(\zeta_n^k \alpha) = \zeta_n^{j+k} \alpha$ , zodat  $\sigma\tau = \tau\sigma$ . Dus we vinden een rijtje  $(0) \subset \text{Gal}(L/K(\zeta_n)) \subset \text{Gal}(L/K)$  dat laat zien dat  $G$  oplosbaar is, zoals verlangd. Dit bewijst de propositie.

We laten nu zien dat Galoisdeellichamen van een worteluitbreiding een oplosbare Galoisgroep hebben.

**(5.7) Stelling.** *Laat  $K$  een lichaam van karakteristiek 0 zijn en  $L/K$  een worteluitbreiding. Als  $F$  een deellichaam van  $L$  is dat Galois is over  $K$  dan is de Galoisgroep  $\text{Gal}(F/K)$  een oplosbare groep.*

*Bewijs.* De eerste stap bestaat eruit te laten zien dat het lichaam  $L$  bevat is in een eindige worteluitbreiding  $M/K$  van  $K$  die Galois is over  $K$  met oplosbare Galoisgroep. We weten dat  $L$  een worteluitbreiding is van  $K$ , dus er zijn  $a_i$  zodat  $L = K(a_1, \dots, a_m)$  met  $a_i^{n_i} \in K(a_1, \dots, a_{i-1})$  voor zekere  $n_i \in \mathbb{Z}_{>0}$ . We nemen nu eerst het ontbindingslichaam  $M_1$  van  $g_1 := X^{n_1} - a_1$ . Dit is een normale uitbreiding en we hebben net gezien dat de Galoisgroep oplosbaar is. Er geldt  $a_2^{n_2} \in K(a_1)$ . Bekijk nu het polynoom

$$g_2 := \prod_{\sigma \in \text{Gal}(M_1/K)} (X^{n_2} - \sigma(a_2)^{n_2});$$

omdat dit invariant is onder  $\text{Gal}(M_1/K)$  ligt dit polynoom  $g_2$  in  $K[X]$ . We laten nu  $M_2$  het ontbindingslichaam van dit polynoom  $g_2$  over  $M_1$  zijn. Dit is een normale worteluitbreiding van  $K$  die  $M_1$  bevat. Merk op dat we de uitbreiding  $M_2/M_1$  kunnen krijgen door achtereenvolgens de wortels van polynomen  $X^{n_2} - \sigma(a_2)^{n_2}$  te adjungeren. Door Propositie (5.6) en Opgave 2 zien we dat de Galoisgroep van  $M_2$  over  $K$  oplosbaar is. Met inductie gaan we verder. Zo verkrijgen we het gewenste lichaam  $M = M_t$ .

Omdat  $F$  een normale uitbreiding van  $K$  is, is de Galoisgroep  $\text{Gal}(M/F)$  een normaaldeeler van  $\text{Gal}(M/K)$ . De Galoisgroep van  $F/K$  is isomorf met de quotiëntgroep  $\text{Gal}(M/K)/\text{Gal}(M/F)$ . Omdat een quotiëntgroep van een oplosbare groep oplosbaar is (zie Opgave 3), kunnen we concluderen dat  $F/K$  een oplosbare Galoisgroep heeft. Dit bewijst de stelling.

We gaan nu laten zien dat er een Galoisuitbreiding  $L/K$  bestaat die het ontbindingslichaam is van een polynoom van graad 5 in  $K[X]$  zodat de Galoisgroep  $\text{Gal}(L/K)$  isomorf is met de symmetrische groep  $S_5$ . Omdat deze groep niet oplosbaar is kan dit volgens de voorgaande stelling geen worteluitbreiding zijn.

Laat gegeven zijn een irreducibel polynoom  $f \in \mathbb{Q}[X]$  van graad 5 met drie reële wortels  $\alpha_1, \alpha_2, \alpha_3$  en twee niet-reële complex geconjugeerde nulpunten  $\alpha_4$  en  $\alpha_5$ . De Galoisgroep  $G$  van het ontbindingslichaam  $\Omega$  van  $f$  over  $\mathbb{Q}$  is een ondergroep van  $S_5$ . Omdat  $\Omega$  een uitbreiding van graad 5 bevat, is  $[\Omega : \mathbb{Q}]$  deelbaar door 5 en dus bevat  $G$  een element van orde 5. Omdat de enige elementen van orde 5 in  $S_5$  de 5-cykels zijn mogen we aannemen dat  $G$  een 5-cykel bevat. Nu is  $F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$  een deellichaam van  $\mathbb{R}$ , dus dit lichaam bevat  $\alpha_4$  en  $\alpha_5$  niet. Omdat  $\Omega/F$  een Galoisuitbreiding is, is er een  $F$ -automorfisme van  $\Omega$  dat  $\alpha_4$  niet vastlaat. Daarvoor geldt dan  $\sigma(\alpha_4) = \alpha_5$ , terwijl  $\sigma(\alpha_i) = \alpha_i$  voor  $i = 1, 2, 3$ . Dus  $\sigma$  is de transpositie  $(4\ 5)$  in  $S_5$ . We gebruiken nu het volgende lemma waarvan in Opgave 4 een bewijs wordt gevraagd.

**(5.8) Lemma.** *Een ondergroep  $G$  van  $S_5$  die een 5-cykel en een transpositie bevat is gelijk aan  $S_5$ .*

Dus de Galoisgroep van  $\Omega$  over  $\mathbb{Q}$  is  $S_5$ . Hoe vinden we een polynoom  $f$  van graad 5 dat irreducibel is en precies drie reële nulpunten heeft? Begin bijvoorbeeld met  $X(X^2 - 9)(X^2 + 9) = X^5 - 81X$ . Dat heeft drie reële wortels, maar is natuurlijk niet irreducibel. Een kleine verstoring maakt het polynoom irreducibel, terwijl het tekenverloop op de reële rechte en dus het aantal reële nulpunten niet verandert:

$$X^5 - 81X + 3,$$

terwijl het Eisensteincriterium direct de irreducibiliteit levert.

**(5.9) Conclusie.** *Er is een irreducibel polynoom  $f \in \mathbb{Q}[X]$  van graad 5 zodat het ontbindingslichaam  $\Omega$  van  $f$  over  $\mathbb{Q}$  een uitbreiding is van  $\mathbb{Q}$  met Galoisgroep  $S_5$ . De uitbreiding  $\Omega/\mathbb{Q}$  is niet een worteluitbreiding.*

We kunnen in dit geval dus geen wortelformule in de stijl van Cardano vinden.

We gaan nu bewijzen dat de alternerende groep  $A_n$  voor  $n \geq 5$  simpel is, dat wil zeggen, geen echte normaaldelers bevat. Allereerst herinneren we eraan dat  $A_n$  voortgebracht wordt door 3-cykels. Omdat  $S_n/A_n$  van orde 2 is en dus abels, bevat  $A_n$  de commutatorondergroep  $[S_n, S_n]$  van  $S_n$ . Een tweede opmerking is dat alle 3-cykels in  $A_n$  voor  $n \geq 5$  geconjugerd zijn. Immers, als  $(abc)$  een 3-cykel is dan is er een  $\sigma \in S_n$  zodat  $\sigma(1\ 2\ 3)\sigma^{-1} = (abc)$ . Als  $\sigma$  even is, dan zijn we klaar, anders vervangen we  $\sigma$  door  $\sigma(4\ 5)$  die op de elementen 1, 2, 3 hetzelfde doet als  $\sigma$ .

**(5.10) Propositie.** *Voor  $n \geq 5$  is de alternerende groep  $A_n$  simpel (dwz heeft geen echte normaaldelers).*

*Bewijs.* Laat  $N$  een niet-triviale normaaldeler van  $A_n$  zijn. Laat  $\tau$  een niet-triviaal element van  $N$  zijn. Het centrum van  $A_n$  is triviaal, en  $A_n$  wordt voortgebracht door 3-cykels, dus is er een 3-cykel  $\sigma$  in  $A_n$  die niet commuteert met  $\tau$ . Dan is de commutator

$$\tau(\sigma\tau^{-1}\sigma^{-1}) = (\tau\sigma\tau^{-1})\sigma^{-1}$$

het product van twee elementen uit  $N$ , dus ligt in  $N$ . Bovendien zijn de twee elementen  $\tau\sigma\tau^{-1}$  en  $\sigma^{-1}$  3-cykels. Op een permutatie na zijn we dan in een van de volgende situaties: we hebben een product  $\gamma = \alpha\beta$  van 3-cykels

- i)  $(1\ 2\ 3)(4\ 5\ 6)$
- ii)  $(1\ 2\ 3)(1\ 4\ 5) = (1\ 4\ 5\ 2\ 3)$
- iii)  $(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$
- iv)  $(1\ 2\ 3)(4\ 2\ 1) = (1\ 4\ 3)$
- v)  $(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$

We laten nu zien dat  $N$  in al deze gevallen een 3-cykel bevat. In de gevallen iv) en v) is dat duidelijk. In geval iii) bekijken we commutator  $[\gamma, (2\ 4\ 5)] = (2\ 4\ 5)$ , een 3-cykel. In geval ii) bekijken we  $[\gamma, (1\ 4\ 3)] = (1\ 3\ 5)$ , wederom een 3-cykel. Tenslotte, voor geval i) nemen we  $[\gamma, (1\ 2\ 4)] = (1\ 4\ 3\ 5\ 2)$ , een 5-cykel, een geval dat we aankunnen met ii). Dit bewijst dat  $N$  een 3-cykel bevat, en dus alle 3-cykels. Dit bewijst dat  $N = A_n$  en daarmee dat  $A_n$  voor  $n \geq 5$  simpel is.

We willen nu voor irreducibele polynomen  $f$  met rationale coëfficiënten aangeven hoe men met reductie modulo een priem veel informatie over de Galoisgroep van  $f$  krijgt. Daartoe geven we eerst een iets andere beschrijving van de Galoisgroep.

Laat  $K$  een lichaam zijn en  $f$  een polynoom in  $K[X]$  met ontbindingslichaam  $L = \Omega_K^f$  dat Galois is over  $K$ . Laat  $\alpha_1, \dots, \alpha_n$  de wortels van  $f$  in  $L$  zijn en laat  $G = \text{Gal}(L/K)$  de Galoisgroep van  $f$  zijn.

De uitdrukking

$$\eta = \alpha_1 y_1 + \alpha_2 y_2 + \dots + \alpha_n y_n$$

definiëert een element van de polynoomring  $L[y_1, \dots, y_n]$  in  $n$  variabelen. De symmetrische groep  $S_n$  werkt op  $L[y_1, \dots, y_n]$  door de variabelen  $y_i$  te permuteren, dus

$$\eta \mapsto \sigma(\eta) = \alpha_1 y_{\sigma(1)} + \dots + \alpha_n y_{\sigma(n)}.$$

Het polynoom

$$F = \prod_{\sigma \in S_n} (X - \sigma(\eta))$$

ligt in  $L[X, y_1, \dots, y_n]$ , maar omdat de coëfficiënten symmetrische functies van de  $\alpha_i$  zijn geldt  $F \in K[X, y_1, \dots, y_n]$ . Schrijf nu  $F$  in  $K[X, y_1, \dots, y_n]$  als product van irreducibele polynomen

$$F = F_1 \cdots F_r.$$

**(5.11) Lemma.** *Laat  $H = \{\sigma \in S_n : \sigma(F_1) = F_1\}$ . Dan is  $H$  gelijk aan de Galoisgroep  $G$  van  $f$  (als ondergroep van  $S_n$ ).*

*Bewijs.* We mogen aannemen dat  $F_1$  de irreducibele factor van  $F$  is die in een ontbindingslichaam de factor  $X - \eta$  als factor heeft. Voor een element  $\sigma \in S_n$  geven we met  $\sigma_y$  de bijbehorende permutatie van de  $y_1, \dots, y_n$  aan en met  $\sigma_\alpha$  de bijbehorende permutatie van de  $\alpha_1, \dots, \alpha_n$ . Dan laat  $\sigma_\alpha \sigma_y$  de uitdrukking  $\eta$  invariant, dus zien we  $\sigma_\alpha^{-1}(\eta) = \sigma_y(\eta)$ .

Er geldt nu voor  $\sigma \in S_n$ :

$$\sigma_y \in H \iff X - \sigma_y(\eta) \text{ is een factor van } F_1.$$

De implicatie  $\Rightarrow$  is duidelijk, terwijl  $\Leftarrow$  volgt uit het feit dat  $\sigma(F_1)$  en  $F_1$  in een uitbreiding een factor gemeen hebben en irreducibel zijn, dus gelijk.

De lichaamsuitbreiding  $L(y_1, \dots, y_n)/K(y_1, \dots, y_n)$  is Galois en heeft dezelfde Galoisgroep als  $L/K$ . Deze groep  $G$  werkt op de  $\alpha$ 's. Laat  $A = \{\sigma_\alpha(\eta) : \sigma \in G\}$ . Dan is

$$h = \prod_{a \in A} (X - a)$$

het minimumpolynoom van  $\eta$  over  $K(y_1, \dots, y_n)$ , zie (5.4). Omdat  $F_1(\eta) = 0$  moet dit  $F_1$  delen, dus is  $h$  wegens de irreducibiliteit van  $F_1$  gelijk aan  $F_1$ . Daaruit volgt dan dat  $A = \{\sigma_\alpha(\eta) : \sigma \in H\}$  en dus wegens  $\sigma_\alpha(\eta) = \sigma_y^{-1}(\eta)$  dat  $G = H$ . Dit bewijst het lemma.

Laat nu  $f \in \mathbb{Z}[X]$  een irreducibel polynoom zijn. Als  $p$  een priemgetal is dan levert reductie modulo  $p$  een polynoom  $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ . We schrijven  $\bar{f}$  als product  $\prod_{i=1}^k g_i$  van irreducibele factoren  $g_i$  van graad  $m_i$  met

$$m_1, m_2, \dots, m_k \quad \text{met} \quad \sum_{i=1}^k m_i = n = \text{graad}(f) \quad \text{en} \quad m_1 \geq m_2 \geq \dots \geq m_k.$$

We noemen  $\{m_1, \dots, m_k\}$  (of ook wel  $n = m_1 + \dots + m_r$ ) de partitie van  $n$  behorende bij de reductie van  $f$  modulo  $p$ .

**(5.12) Stelling.** *Laat  $f$  een irreducibel polynoom van graad  $n$  in  $\mathbb{Z}[X]$  zijn en  $p$  een priemgetal zodat  $p$  de kopcoëfficiënt van  $f$  en de discriminant van  $f$  niet deelt. Als  $f$  modulo  $p$  hoort bij de partitie  $n = m_1 + m_2 + \dots + m_r$  van  $n$  dan bevat de Galoisgroep  $G$  van  $f$  een permutatie van cykeltype  $n = m_1 + m_2 + \dots + m_r$ .*

*Bewijs.* Het irreducibele polynoom  $f$  heeft wortels  $\alpha_1, \dots, \alpha_n$  in  $L$  en de reductie  $\bar{f}$  heeft nog steeds  $n$  verschillende wortels in een uitbreidingslichaam van  $\mathbb{F}_p$  omdat  $p$  de kopcoëfficiënt en de discriminant van  $f$  niet deelt.

De Galoisgroep van  $f$  over  $K$  wordt beschreven in Lemma (5.10). Een element van  $G$  voert  $F_1$  in zich over; de overige elementen van  $S_n$  voeren  $F_1$  in een andere irreducibele factor  $F_j$  over. Dit Lemma kunnen we ook toepassen op  $\bar{f}$ . De reductie modulo  $p$  van het polynoom  $F$  uit het bewijs van lemma (5.10) laat zich in  $\mathbb{Z}/p\mathbb{Z}[X, y_1, \dots, y_n]$  schrijven als product  $\bar{F}_1 \cdots \bar{F}_r$ . Een element  $\tau$  uit de Galoisgroep van  $\bar{f}$  ten opzichte van  $\mathbb{F}_p$  moet een gegeven irreducibele factor van  $\bar{F}_1$  in zichzelf overvoeren, dus voert  $\tau$  geheel  $\bar{F}_1$  in zich over en ligt dus ook in  $H$  en we weten  $H = G$ .

We ontbinden  $\bar{f}$  modulo  $p$  als

$$\bar{f} = g_1 \cdots g_k \quad \text{met graad van } g_i = m_i.$$

De Galoisgroep van  $\bar{f}$  is cyclisch omdat dit een uitbreiding van eindige lichamen is. Als  $\phi$  (Frobenius) de voortbrenger van de Galoisgroep is moet  $\phi$  wegens (5.3) transitief werken op de wortels van iedere factor  $g_i$ . Dus  $\phi$  is een product van disjuncte cyclen van lengte  $m_i$ . Dit bewijst de stelling.

**(5.13) Voorbeeld.** Laat  $f = x^5 + x^3 + 1 \in \mathbb{Z}[x]$ . Dan levert reductie modulo  $p$  de volgende factorisaties:

$p$	$f \bmod p$
2	$x^5 + x^3 + 1$
3	$(x^4 + x^3 + 2x^2 + 2x + 2)(x + 2)$
5	$(x^3 + 3x^2 + 2x + 2)(x^2 + 2x + 3)$
7	$(x^2 + 3x + 6)(x^3 + 4x^2 + 4x + 6)$
11	$(x^4 + 4x^3 + 6x^2 + 2x + 8)(x + 7)$
23	$(x^3 + 22x^2 + 5x + 15)(x + 9)(x + 15)$

waaruit volgt dat geen van de priemenv 2, 3, 5, 7, 11 of 23 de discriminant delen, dat  $f$  irreducibel is en dat de Galoisgroep van  $f$  over  $\mathbb{Q}$  een 5-cykel, een 4-cykel en een 3-cykel bevat en dus gelijk is aan  $S_5$ , vgl. Opgaven 4 en 12.

### Opgaven

- 1) Laat zien dat de symmetrische groep  $S_4$  oplosbaar is.
- 2) Laat  $(0) = G_0 \subset G_1 \subset \dots \subset G_n = G$  een rijtje ondergroepen van de eindige groep  $G$  zijn zodat voor  $i = 0, \dots, n-1$  de groep  $G_i$  een normaaldeeler is van  $G_{i+1}$  en  $G_{i+1}/G_i$  oplosbaar is. Bewijs dat  $G$  oplosbaar is.
- 3) Bewijs dat een quotiëntgroep van een oplosbare groep oplosbaar is.
- 4) Bewijs dat de transpositie  $(1\ 2)$  en de 5-cykel  $(1\ 2\ 3\ 4\ 5)$  de groep  $S_5$  voortbrengen.
- 5) Bereken de Galoisgroepen van de volgende polynomen in  $\mathbb{Q}[X]$ :  $X^3 - 2$ ,  $X^3 + 2X + 1$ ,  $X^3 + X + 1$ ,  $X^3 - 4X + 2$  en  $X^3 - 3X^2 + 1$ .
- 6) Laat  $f \in \mathbb{Q}[X]$  een irreducibel polynoom zijn van graad 3 met één reële wortel. Bewijs dat de Galoisgroep van het ontbindingslichaam van  $f$  over  $\mathbb{Q}$  isomorf is met  $S_3$ .
- 7) Laat  $f \in K[X]$  een irreducibel polynoom van graad 3 zijn met discriminant  $D$ . Bewijs dat  $f$  irreducibel is in  $K(\sqrt{D})[X]$ .
- 8) Bereken de discriminant van  $X^4 + 1 \in \mathbb{Q}[X]$ . Bepaal de Galoisgroep van het ontbindingslichaam van  $f$  over  $\mathbb{Q}$ .
- 9) Laat  $K = \mathbb{Q}(\zeta_{13})$  met  $\zeta_{13}$  een primitieve dertiende machts eenheidswortel. Laat zien dat  $K$  één deellichaam  $F$  van graad 3 over  $\mathbb{Q}$  bezit en geef expliciet een element  $\alpha \in K$  aan zodat  $F = \mathbb{Q}(\alpha)$ .
- 10) Laat  $L/K$  een Galoisuitbreiding zijn met Galoisgroep  $S_4$ . Welke getallen treden op als de graad van een element van  $L$  over  $K$ ?
- 11) Laat  $p$  een priemgetal zijn en  $f = X^p - a \in \mathbb{Q}[X]$  met  $a \in \mathbb{Q}^*$  een rationaal getal dat geen  $p$ -de macht is.
  - i) Bewijs dat de graad van het ontbindingslichaam van  $f$  over  $\mathbb{Q}$  gelijk is aan  $p(p-1)$ .
  - ii) Bewijs dat de Galoisgroep van  $\Omega$  over  $\mathbb{Q}$  isomorf is met de groep van matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_p, a \neq 0 \right\}.$$

12) Laat  $\Omega/\mathbb{Q}$  het ontbindingslichaam zijn van een irreducibel polynoom  $f \in \mathbb{Q}[X]$  van graad 5 met Galoisgroep  $G$ . Laat zien dat als  $G$  een element van orde 3 bevat dan is  $G$  gelijk is aan  $A_5$  of  $S_5$ .

13) Laat  $f \in \mathbb{Q}[X]$  een irreducibel polynoom van graad 4 zijn dat een negatieve discriminant heeft. Welke groepen kunnen Galoisgroep van het ontbindingslichaam van  $f$  over  $\mathbb{Q}$  zijn?

14) Bewijs dat een transitieve ondergroep  $G$  van de symmetrische groep  $S_4$  gelijk is aan i)  $S_4$ , ii)  $A_4$ , iii)  $D_4 = \langle (1234), (12)(34) \rangle$  of een van de twee geconjugeerde ondergroepen van  $D_4$ , iv)  $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ , of v)  $C_4 = \langle (1234) \rangle$  of een van de twee geconjugeerde ondergroepen van  $C_4$ .

15) Laat  $f = X^4 + pX^2 + qX + r \in K[X]$  een monisch irreducibel vierdegraads polynoom zijn met cubische resolvent  $g$ . Stel dat de discriminant  $D$  van  $g$  geen kwadraat is in  $K$  en dat  $g$  als nulpunt  $\lambda_1 = \alpha_1\alpha_3 + \alpha_2\alpha_4$  in  $K$  heeft. i) Ga na dat

$$h = (X - \alpha_1\alpha_3)(X - \alpha_2\alpha_4)(X - \alpha_1 - \alpha_3)(X - \alpha_2 - \alpha_4)$$

gelijk is aan  $(X^2 - \lambda_1 X + r)(X^2 - \lambda_1 + p)$ . ii) Als  $h$  volledig in lineaire factoren uiteenvalt in  $K(\sqrt{D})$  dan voldoet  $\alpha_1$  aan de kwadratische vergelijking

$$(X - \alpha_1)(X - \alpha_3) = 0$$

over  $K(\sqrt{D})$ . iii) Laat verder zien dat  $G \cong \mathbb{Z}/4$  dan en slechts dan als  $h$  in lineaire factoren in  $K(\sqrt{D})[X]$  uiteenvalt.

16) Laat  $K$  een lichaam van karakteristiek ongelijk 2 en 3 zijn en  $f = X^3 + pX + q \in K[X]$  een irreducibel polynoom met nulpunten  $\alpha_1, \alpha_2, \alpha_3$  in een ontbindingslichaam  $L = \Omega_K^f$  van  $f$  over  $K$ . Laat  $\rho$  een primitieve derdemachts eenheidswortel in een uitbreiding  $L(\rho)$  van  $L$  zijn. Definiëer de Lagrange-resolventen

$$\theta_+ = \alpha_1 + \rho\alpha_2 + \rho^2\alpha_3, \quad \theta_- = \alpha_1 + \rho^2\alpha_2 + \rho\alpha_3$$

in  $L(\rho)$ . Bewijs:

$$\theta_+^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}, \quad \theta_-^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D},$$

met  $D$  de discriminant. Vergelijk deze uitkomst met de formules van Cardano.

17) Bereken de Galoisgroepen van de volgende polynomen over  $\mathbb{Q}$ :

$$X^4 + 3, X^5 + 3, X^4 + 9, X^4 + X + 1, X^4 + 3X^2 + 1.$$

18) Bereken de Galoisgroep van  $X^5 - X - 1$  over  $\mathbb{Q}$ .

19) Laat  $G$  een groep zijn. Definiëer  $G^{(0)} = G$ ,  $G^{(1)} = [G, G]$ , de commutatorondergroep, en  $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ , de ondergroep voortgebracht door de commutatoren  $[g, h]$  met  $g, h \in G^{(n)}$ . Laat zien dat voor  $n \geq 0$  de groep  $G^{(n)}$  een normale ondergroep is van  $G$  en dat  $G^{(n+1)} \subseteq G^{(n)}$ .

20) Laat  $G$  een groep zijn. Bewijs:  $G$  is oplosbaar dan en slechts dan als er een  $n \geq 0$  is zodat  $G^{(n)}$  triviaal is.

- 21) Bewijs dat de de Galoisgroep van  $X^4 + 3X + 3 \in \mathbb{Q}[X]$  gelijk is aan  $D_4$ .
- 22) Bewijs dat de Galoisgroep van  $X^4 + 5X + 5 \in \mathbb{Q}[X]$  gelijk is aan  $\mathbb{Z}/4\mathbb{Z}$ .
- 23) Laat  $p$  een priemgetal zijn verschillend van 3 en 5. Bewijs dat de Galoisgroep van  $X^4 + pX + p \in \mathbb{Q}[X]$  gelijk is aan  $S_4$ .
- 24) Laat  $X^4 + aX^2 + b \in \mathbb{Q}[X]$  een irreducibel polynoom zijn. Bewijs dat de Galoisgroep van  $f$  gelijk is aan  $V_4$  dan en slechts dan als  $b$  een kwadraat in  $\mathbb{Q}$  is.
- 25) Bewijs dat het centrum van  $S_n$  triviaal is. Bewijs verder dat  $A_n$  en  $S_n$  niet oplosbaar zijn voor  $n \geq 5$ .
- 26) Bewijs dat een transitieve ondergroep van  $A_5$  isomorf is met  $A_5$ ,  $D_5$  of  $\mathbb{Z}/5\mathbb{Z}$ .
- 27) Een compositierijtje voor een groep  $G$  is een rijtje ondergroepen

$$\{e\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G$$

zodat  $G_i$  een normaaldeler is van  $G_{i+1}$  en  $G_{i+1}/G_i$  een simpele groep is. Laat zien dat iedere eindige groep een compositierijtje bezit.

- 28) Bewijs: een eindige groep  $G$  is oplosbaar dan en slechts dan als  $G$  een compositierijtje heeft met quotientgroepen  $G_{i+1}/G_i$  van priemorde.

## 6. DE STELLINGEN VAN SYLOW

*We all believe that mathematics is an art*

Emil Artin

In dit hoofdstuk behandelen we stellingen van Sylow over het bestaan van ondergroepen van een eindige groep en we passen dit toe om te bewijzen dat het lichaam  $\mathbb{C}$  van de complexe getallen algebraïsch afgesloten is. De stelling van Cauchy zegt dat als een priemgetal  $p$  de orde van een eindige groep  $G$  deelt,  $G$  een element van orde  $p$  bezit. De Stellingen van Sylow generaliseren dit resultaat. Merk op dat een eindige groep waarvan de orde deelbaar is door  $n$  niet noodzakelijkerwijs een ondergroep van orde  $n$  hoeft te hebben. Bijvoorbeeld heeft de alternerende groep  $A_4$  van orde 12 geen ondergroep van orde 6.

Zoals bekend noemen we twee elementen  $x$  en  $y$  in een groep  $G$  *geconjugerd* als er een element  $g \in G$  is zodat  $x = g^{-1}yg$ . De verzameling

$$K_x := \{g^{-1}xg : g \in G\}$$

heet de conjugatieklasse van  $x$ . De relatie ‘geconjugerd zijn’ is een equivalentierelatie op  $G$ . We roepen ook het begrip *centralisator* in herinnering: de centralisator van een element  $x \in G$  is de ondergroep  $C(x)$  van  $G$  gegeven door

$$C(x) := \{g \in G : g^{-1}xg = x\}.$$

De groep  $G$  werkt op zichzelf via conjugatie  $g \cdot x = g^{-1}xg$  en  $K_x$  is de baan van  $x$  onder deze werking. Het volgende lemma is een toepassing van (?.?) uit Algebra 1.

**(6.1) Lemma.** *Laat  $G$  een eindige groep zijn en  $x \in G$  een element. Dan geldt  $\#K_x = [G : C(x)]$ .*

*Bewijs.* We maken een bijectie tussen de verzameling van rechternevenklassen  $C(x) \backslash G$  en  $K_x$  door aan  $C(x)g$  het element  $g^{-1}xg$  toe te voegen. We laten het aan de lezer over na te gaan dat dit een welgedefinieerde afbeelding is en ook een bijectie levert.

**(6.2) Stelling.** (De Klassenformule). *Laat  $G$  een eindige groep zijn. Dan geldt*

$$\#G = \sum_x [G : C(x)],$$

waarbij de som loopt over een volledige stelsel representanten  $x$  van de conjugatieklassen van  $G$ .

*Bewijs.* Volgens het voorgaande lemma is  $[G : C(x)]$  gelijk aan het aantal elementen van  $K_x$ . De stelling volgt daarom direct uit het feit dat  $G$  de disjuncte vereniging van de conjugatieklassen  $K_x$  is.

We roepen het begrip *centrum* van een groep  $G$  in herinnering: het centrum

$$Z(G) = \{g \in G : gh = hg \text{ voor alle } h \in G\}$$

is de ondergroep van elementen die met alle groepselementen commuteren. Merk op dat voor een  $x \in G$  geldt

$$x \in Z(G) \iff C(x) = G \iff K_x = \{x\}.$$

**(6.3) Gevolg.** *Laat  $G$  een eindige groep zijn waarvan de orde een macht van een priemgetal  $p$  is. Dan is het centrum  $Z(G)$  van  $G$  niet triviaal (dus  $\#Z(G) > 1$ ).*

*Bewijs.* Gezien de opmerking die voorafgaat aan deze stelling leveren de elementen van het centrum ieder een conjugatieklasse en een bijdrage 1 aan de som in de klassenformule. Dus we kunnen schrijven

$$\#G = \#Z(G) + \sum_x [G : C(x)], \quad (1)$$

waarbij de som nu loopt over een volledig stelsel representanten van de conjugatieklassen die uit meer dan een element bestaan. Maar voor zo een  $x$  is de bijdrage  $[G : C(x)] = \#G/\#C(x)$  een positieve macht van  $p$ . We zien dat in de herschikte formule (1)

$$\#Z(G) = \#G - \sum [G : C(x)],$$

de rechterkant door  $p$  deelbaar is. Daarom is ook  $\#Z(G)$  door  $p$  deelbaar en uit  $\#Z(G) > 0$  volgt dat  $\#Z(G) \geq p$ . Dit bewijst het gevolg.

**(6.4) Stelling.** (De Eerste Stelling van Sylow\*). *Laat  $G$  een eindige groep zijn en  $p$  een priemgetal. Als  $p^k$  de orde van  $G$  deelt dan bezit  $G$  tenminste een ondergroep van orde  $p^k$ .*

*Bewijs.* Het bewijs gaat met inductie naar de orde van  $G$  en gebruikt de klassenformule. De stelling is duidelijk voor de triviale groep met 1 element. Stel dat we de stelling bewezen hebben voor groepen van orde kleiner dan  $\#G$ . Als  $G$  een echte ondergroep  $H$  bezit waarvan de orde deelbaar is door  $p^k$  dan heeft  $H$  volgens de inductieveronderstelling een ondergroep van orde  $p^k$  en dit is dan ook een ondergroep van  $G$  van de gevraagde orde. Daarom mogen we nu aannemen dat  $p^k$  de orde van geen enkele echte ondergroep van  $G$  deelt. We schrijven de klassenformule dan in de vorm

$$\#G = \#Z(G) + \sum [G : C(x)],$$

waarbij de som loopt over de conjugatieklassen die uit meer dan een element bestaan. We weten dat  $p^k$  een deler is van  $\#G = \#C(x) \cdot [G : C(x)]$ , maar omdat wegens onze aanname  $p^k$  geen deler is van  $\#C(x)$  moet  $p$  een deler zijn van de index  $[G : C(x)]$  voor alle  $x \notin Z(G)$ . Daarom deelt  $p$  de orde van  $Z(G)$  en wegens de stelling van Cauchy bevat  $Z(G)$  daarom een element van orde  $p$ , zeg  $z$ . De ondergroep  $\langle z \rangle$  is een normaaldeeler van  $G$  omdat  $z$  in het centrum ligt. De orde van de quotiëntgroep  $G/\langle z \rangle$  is deelbaar door  $p^{k-1}$ , dus met de inductieaanname volgt dat deze quotiëntgroep een ondergroep  $H$  van orde  $p^{k-1}$  bezit. Het inverse beeld van  $H$  onder de kanonieke afbeelding

$$\phi : G \longrightarrow G/\langle z \rangle$$

---

\* Ludwig Sylow, 1832–1918, was een Noors wiskundige.

is dan een ondergroep  $H'$  van  $G$  die  $z$  bevat en orde  $p^k$  heeft. Dit bewijst de eerste Sylowstelling.

**(6.5) Definitie.** Laat  $G$  een eindige groep zijn en  $p$  een priemgetal dat de orde van  $G$  deelt. Een ondergroep van  $G$  van orde  $p^k$  met  $k$  de hoogste macht van  $p$  die de orde van  $G$  deelt, heet een  $p$ -Sylow-ondergroep van  $G$ .

**(6.6) Stelling** (De Tweede Stelling van Sylow). *Iedere twee  $p$ -Sylow-ondergroepen van een eindige groep zijn geconjugeerd; m.a.w., als  $A$  en  $B$  twee  $p$ -Sylow-ondergroepen van de eindige groep  $G$  zijn dan is er een  $g \in G$  zodat  $g^{-1}Ag = B$ .*

Voor we het bewijs geven voeren we nog notatie in. Laat  $H \subset G$  een ondergroep van  $G$  zijn en  $\gamma \in G$  een element van  $G$ . We noteren we de geconjugeerde ondergroep  $\gamma^{-1}H\gamma$  met  $H^\gamma$ :

$$H^\gamma := \gamma^{-1}H\gamma$$

en voor een ondergroep  $H$  van  $G$  noteren we de normalisator van  $H$  in  $G$  met  $N_G(H)$ :

$$N_G(H) := \{g \in G : H^g = H\}.$$

Verder gebruiken we ook de handige notatie

$$a^b := b^{-1}ab$$

zodat geldt

$$ab = ba^b \tag{2}$$

*Bewijs.* Laat  $p^k = \#A = \#B$ . Voor  $\gamma \in G$  is  $A^\gamma$  ook weer een  $p$ -Sylowondergroep van  $G$  want  $\#A = \#A^\gamma$ .

*Stap 1.* We beweren dat als  $B$  bevat is in de normalisator  $N_G(A^\gamma)$  voor een  $\gamma$ , dan is  $B$  gelijk aan  $A^\gamma$ . Om dit in te zien gebruiken we de afbeelding

$$A^\gamma \times B \longrightarrow G, \quad (a, b) \mapsto ab.$$

Het beeld  $A^\gamma B$  is een ondergroep van  $G$ , want voor  $a, c \in A^\gamma$  en  $b, d \in B$  ligt met  $ab$  en  $cd$  ook

$$ab(cd)^{-1} = abd^{-1}c^{-1} = a(bd^{-1})c^{-1} = a(c^{-1})^{db^{-1}}(bd^{-1})$$

weer in  $A^\gamma B$  omdat  $bd^{-1} \in B \subset N_G(A^\gamma)$  en dus  $a(c^{-1})^{db^{-1}} \in A^\gamma$ . Verder geldt  $ab = cd \iff c^{-1}a = db^{-1} \in A^\gamma \cap B$ . Dus  $A^\gamma B$  is van orde

$$\frac{\#A^\gamma \#B}{\#(A^\gamma \cap B)}$$

en dit is een  $p$ -macht  $\geq p^k$ . Maar uit de maximaliteit van  $p^k$  volgt dat  $A^\gamma \cap B = B$ , dus  $A^\gamma = B$ , zoals beweerd.

*Stap 2.* We kunnen nu aannemen dat  $B$  niet bevat is in de normalisator  $N_G(A^\gamma)$  van een geconjugeerde ondergroep van  $A$  (voor alle  $\gamma$ ). Laat

$$\mathcal{A} = \{A^\gamma : \gamma \in G\}$$

de verzameling geconjugeerde ondergroepen van  $A$  zijn. We merken op dat  $\#\mathcal{A}$  niet door  $p$  deelbaar is want de afbeelding  $g \mapsto A^g$  geeft een bijectie

$$N_G(A) \backslash G \xrightarrow{1-1} \mathcal{A}, \quad N_G(A)g \mapsto A^g,$$

dus  $\#\mathcal{A} = \#G/\#N_G(A)$  en omdat  $A$  een ondergroep is van  $N_G(A)$  volgt dat  $\#\mathcal{A}$  een quotiënt is van  $\#G/p^k$  en dit is niet door  $p$  deelbaar.

De groep  $B$  werkt op de verzameling  $\mathcal{A}$  door conjugatie:

$$b \cdot A^\gamma = b^{-1}A^\gamma b = A^{\gamma^b}.$$

Voor elke  $\gamma$  is de normalisator  $N_B(A^\gamma) = \{b \in B : A^{\gamma^b} = A^\gamma\}$  wegens de aanname dat  $B \not\subset N_G(A^\gamma)$  een echte ondergroep van  $B$ . Dus is  $p$  een deler van de index  $[B : N_B(A^\gamma)]$ . Kijk nu naar de banen van de werking van  $B$  op  $\mathcal{A}$ . De lengte van de baan van  $A^\gamma$  is  $[B : N_B(A^\gamma)]$  en dus ook deelbaar door  $p$ . Dus moet  $\#\mathcal{A}$  deelbaar zijn door  $p$ , een tegenspraak. Dit bewijst dat  $B$  een geconjugeerde groep van  $A$  is.

**(6.7) Stelling.** (De Derde Stelling van Sylow). *Laat  $G$  een eindige groep zijn. Als  $s_p$  het aantal  $p$ -Sylow-ondergroepen van  $G$  is dan geldt*

ii)  $s_p \equiv 1 \pmod{p}$ ,

ii)  $s_p$  deelt de orde van  $G$ ,

iii) Voor elke  $p$ -Sylow-ondergroep  $S$  van  $G$  geldt  $s_p = [G : N_G(S)]$ .

*Bewijs.* Laat  $\Sigma = \{S_1, \dots, S_r\}$  de verzameling van  $p$ -Sylow-ondergroepen zijn. Kies een  $p$ -Sylow-ondergroep, zeg  $S_1$ . Dan werkt  $S_1$  op  $\Sigma$  via conjugatie  $S_i \mapsto g^{-1}S_i g$ . Het enige vaste punt onder deze werking is  $S_1$ . Immers, in het begin van het bewijs van de tweede Sylowstelling hebben we laten zien dat  $S_1 = S_i$  als  $S_1$  bevat is in de normalisator van  $S_i$ . Dus er is precies één vast punt onder werking. De lengte van de andere banen is een  $p$ -macht. Dus geldt  $s_p \equiv 1 \pmod{p}$ .

Laat  $S$  een  $p$ -Sylow-ondergroep zijn. Dan is  $N = N_G(S) = \{g \in G : g^{-1}Sg = S\}$  een ondergroep van  $G$  die  $S$  bevat. Het aantal geconjugeerde ondergroepen van  $S$  is  $[G : N]$  en is een factor van  $[G : S]$ . Omdat iedere  $p$ -Sylow-ondergroep geconjugerd is met  $S$  volgt de stelling.

**(6.8) Gevolg.** *Een  $p$ -Sylow-ondergroep van een eindige groep  $G$  is normaal dan en slechts dan als het de enige  $p$ -Sylow-ondergroep van  $G$  is.*

We gaan nu als toepassing de zogenaamde ‘Hoofdstelling van de Algebra’ bewijzen die zegt dat ieder polynoom  $f \in \mathbb{C}[X]$  van positieve graad een nulpunt heeft in  $\mathbb{C}$ . De Franse wiskundige Girard beweerde in zijn werk “L’invention en l’algèbre” gepubliceerd in Amsterdam in 1629 “Toutes les equations d’algèbre reçoivent autant de solutions, que la denomination de la plus haute quantité le demonstre...” en illustreerde dit met voorbeelden, maar geeft geen bewijs. In 1742 formuleerde Euler in een brief aan Nikolaus Bernoulli de stelling dat ieder polynoom  $f \in \mathbb{R}[X]$  gefactoriseerd kan worden in lineaire en kwadratische termen. Met de wortelformule voor kwadratische vergelijkingen volgt hieruit dat ieder polynoom van graad  $\geq 1$  met reële coëfficiënten een nulpunt heeft in  $\mathbb{C}$ . Euler heeft voor polynomen van graad  $\leq 6$  in  $\mathbb{C}[X]$  streng bewezen dat zo een polynoom steeds een nulpunt in  $\mathbb{C}$  heeft. Euler heeft ook het algemene geval behandeld, en na

hem ook Lagrange en Laplace. Gauss beschouwde al deze bewijzen als onvolledig en gaf vier verschillende bewijzen, waarvan het tweede ook vanuit ons standpunt nog steeds als een correct bewijs geldt. Alle bewijzen gebruiken niet-algebraïsche hulpmiddelen. De naamgeving “Hoofdstelling” van de Algebra doet nu ietwat vreemd aan.

**(6.9) Stelling.** *Hoofdstelling van de Algebra.* Laat  $f \in \mathbb{C}[X]$  een polynoom van graad  $n \geq 1$  zijn. Dan zijn er elementen  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  en een constante  $c \in \mathbb{C}^*$  zodat  $f$  zich laat schrijven als

$$f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n).$$

We zullen twee bewijzen geven. Het eerste is een kort bewijs als toepassing van de Sylowstellingen. Het tweede stamt van Gauss.

We overtuigen ons er eerst van dat een kwadratisch polynoom  $f = aX^2 + bX + c$  altijd een nulpunt in  $\mathbb{C}$  heeft. Daarvoor merken we op dat we wortels uit niet-negatieve reële getallen kunnen trekken en dat voor een element  $z \in \mathbb{C}$  we een wortel  $\sqrt{z}$  kunnen trekken: als  $z = re^{i\phi}$  een schrijfwijze in poolcoördinaten is dan is  $\sqrt{r}e^{i\phi/2}$  een kwadraatwortel; of meer algebraïsch, laat  $z = x + iy$  met  $x, y \in \mathbb{R}$  met  $y \neq 0$  en neem dan als wortel

$$\sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}} + \frac{y}{|y|} \sqrt{\frac{-x + \sqrt{x^2 + y^2}}{2}} i.$$

In het algemene geval  $f = aX^2 + bX + c$  met  $a \neq 0$  levert dan

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

een wortel.

*Bewijs 1.* Voor het bewijs van de hoofdstelling volstaat het te bewijzen dat iedere algebraïsche uitbreiding  $K$  van  $\mathbb{C}$  gelijk is aan  $\mathbb{C}$ . Als  $K = \mathbb{C}(\alpha_1, \dots, \alpha_n)$  een algebraïsche uitbreiding is bekijken we een eindige normale uitbreiding  $L$  van  $\mathbb{R}$  die  $K$  omvat. Neem bijvoorbeeld het ontbindingslichaam van het product van de minimumpolynomen van de  $\alpha_i$  over  $\mathbb{R}$ . Nu is  $\mathbb{R}$  van karakteristiek nul, dus  $L$  is separabel en normaal over  $\mathbb{R}$ , dus een Galoisuitbreiding. We schrijven de uitbreidingsgraad  $[L : \mathbb{R}]$  als  $2^k m$  met  $m$  oneven. Volgens de Eerste Sylowstelling is er een ondergroep  $H$  van de Galoisgroep  $G = \text{Gal}(L/\mathbb{R})$  van orde  $2^k$ . Volgens de Hoofdstelling van de Galoistheorie heeft het lichaam van invarianten  $L^H$  graad  $m$  over  $\mathbb{R}$ . Kies een element  $\beta$  in  $L^H$ . Het minimumpolynoom  $f$  van  $\beta$  over  $\mathbb{R}$  heeft als graad een deler van  $m$ , is dus oneven. Maar dan heeft  $f$  een nulpunt in  $\mathbb{R}$ , want  $f(-x) < 0$  en  $f(x) > 0$  voor voldoende grote positieve  $x$  en met de Tussenwaardestelling volgt het bestaan van een nulpunt. Maar dan moet  $f$  dus lineair zijn, dus  $L^H = \mathbb{R}$ . Dan volgt dat de graad van  $L/\mathbb{R}$  een tweemacht  $2^k$  is. Neem aan dat  $k > 1$ . Kies nu een ondergroep  $\Gamma$  van  $\text{Gal}(L/\mathbb{C})$  van orde  $2^{k-2}$ . Dan geldt  $[L^\Gamma : \mathbb{C}] = 2$ . Maar we weten al dat we kwadratische polynomen kunnen oplossen in  $\mathbb{C}$ , dus  $L^\Gamma = \mathbb{C}$ , en deze tegenspraak laat zien dat  $k = 1$ , dus  $L = \mathbb{C}$ . Dit bewijst de stelling.

*Bewijs 2.* Het tweede bewijs is van Gauss. We laten zien dat ieder polynoom van graad  $\geq 1$  een nulpunt heeft. Als  $\alpha$  dat nulpunt is volgt dat  $f = (X - \alpha)f_1$  en met inductie naar de graad volgt de stelling dan gemakkelijk.

We beweren dat het voldoende is te laten zien dat ieder polynoom van graad  $\geq 1$  met reële coëfficiënten een nulpunt in  $\mathbb{C}$  heeft. Immers, als

$$f = a_0X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{C}[X]$$

stellen we

$$\bar{f} = \bar{a}_0X^n + \bar{a}_1X^{n-1} + \dots + \bar{a}_n \in \mathbb{C}[X]$$

en krijgen met  $F = f\bar{f}$  een polynoom met reële coëfficiënten. Als we weten dat  $F$  een nulpunt  $\alpha$  in  $\mathbb{C}$  heeft dan geldt  $F(\alpha) = f(\alpha)\bar{f}(\alpha) = 0$ , dus  $f(\alpha) = 0$  of  $\bar{f}(\alpha) = 0$ . In het laatste geval hebben we  $f(\bar{\alpha}) = \overline{\bar{f}(\alpha)} = 0$ , dus  $f$  heeft altijd een nulpunt in  $\mathbb{C}$ .

We mogen daarom aannemen dat  $F \in \mathbb{R}[X]$  een polynoom van graad  $\geq 1$  is. Door  $F$  met een geschikte constante ongelijk nul te vermenigvuldigen kunnen we bereiken dat  $F$  monisch is. We schrijven de graad  $n$  van  $F$  nu als  $n = 2^k n_1$  met  $n_1$  oneven en voeren nu inductie naar  $k$ , de hoogste macht van 2 die  $n$  deelt. Als  $k = 0$  dan is de graad van  $F$  oneven. Voor grote reële waarden van  $x$  is  $F(x)$  dan positief, terwijl voor sterk negatieve waarden van  $x$  het polynoom  $F(x)$  negatief is. Volgens de Tussenwaardestelling neemt  $F$  dan een nulpunt aan op  $\mathbb{R}$ .

De inductieveronderstelling zegt dat ieder polynoom  $H \in \mathbb{R}[X]$  met

$$\text{ord}_2(\text{graad}(H)) < k$$

een nulpunt in  $\mathbb{C}$  heeft. In een ontbindingslichaam  $K$  van  $F$  kunnen we  $F$  ontbinden

$$F = (X - \beta_1)(X - \beta_2) \cdots (X - \beta_n).$$

Voor een element  $t \in \mathbb{R}$  bekijken we dan het polynoom

$$G_t = \prod_{1 \leq i < j \leq n} (X - (\beta_i + \beta_j + t\beta_i\beta_j)).$$

Dit is een polynoom van graad  $n(n-1)/2$  waarvan de coëfficiënten symmetrische polynomen in de  $\beta_i$  zijn met coëfficiënten uit  $\mathbb{R}$ . Volgens de hoofdstelling van de symmetrische functies zijn de coëfficiënten van  $G_t$  dus reëel. Merk nu op dat de hoogste macht van 2 die  $n(n-1)/2$  deelt gelijk is aan  $k-1$  en met onze inductieveronderstelling mogen we dus aannemen dat voor elke  $t \in \mathbb{R}$  het polynoom  $G_t$  een nulpunt in  $\mathbb{C}$  heeft. We zien daarom dat er voor elke  $t \in \mathbb{R}$  er  $i$  en  $j$  zijn met  $1 \leq i < j \leq n$  zodat

$$\beta_i + \beta_j + t\beta_i\beta_j \in \mathbb{C}.$$

Nu kan  $t$  de oneindige verzameling  $\mathbb{R}$  doorlopen, maar voor de  $i$  en  $j$  hebben we maar eindig veel mogelijkheden. Dat betekent dat er verschillende  $t$  en  $t'$  in  $\mathbb{R}$  zijn zodat (met dezelfde  $i$  en  $j$ ) geldt

$$\beta_i + \beta_j + t\beta_i\beta_j \in \mathbb{C}, \quad \beta_i + \beta_j + t'\beta_i\beta_j \in \mathbb{C}.$$

Nemen we het verschil dan volgt dat  $\beta_i\beta_j \in \mathbb{C}$  en daaruit volgt dat ook  $\beta_i + \beta_j$  in  $\mathbb{C}$  ligt. Maar dan heeft het polynoom

$$X^2 - (\beta_i + \beta_j)X + \beta_i\beta_j = (X - \beta_i)(X - \beta_j)$$

coëfficiënten in  $\mathbb{C}$ . Omdat een kwadratisch polynoom in  $\mathbb{C}[X]$  zijn wortels in  $\mathbb{C}$  heeft (zie boven) volgt dat  $\beta_i$  en  $\beta_j$  in  $\mathbb{C}$  liggen. Dus  $F$  heeft een nulpunt in  $\mathbb{C}$ . Daarmee is het bewijs van Gauss van de stelling voltooid.

### Opgaven

- 1) Laat  $N$  een normaaldeeler van een eindige groep  $G$  zijn. Bewijs dat als  $x \in N$  dan ook  $K_x \subset N$ . Concludeer dat de orde van  $N$  gelijk is aan de som van de ordes van de conjugatieklassen bevat in  $N$ .
- 2) Laat zien dat de orde van een conjugatieklasse van  $A_5$  gelijk is aan 1, 12, 15 of 20. Maak de Klassenformule expliciet in dit geval.
- 3) Gebruik Opgaven 1) en 2) om te laten zien dat  $A_5$  simpel is (dwz geen echte normaaldelers heeft).
- 4) Bewijs dat een groep van orde 15 cyclisch is.
- 5) Laat  $G$  een groep van orde 21 zijn. Bewijs dat de 7-Sylowondergroep een normaaldeeler van  $G$  is.
- 6) Laat zien dat een groep van orde 200 niet simpel is.
- 7) Laat zien dat een groep van orde 45 abels is.
- 8) Laat  $p$  een priemgetal zijn. Vind een  $p$ -Sylowgroep van  $GL(2, \mathbb{F}_p)$ . Zelfde vraag voor  $GL(n, \mathbb{F}_p)$  voor  $n \geq 3$ .
- 9) Laat  $G$  een groep zijn van orde 21 die niet abels is. Laat  $x$  een voortbrenger zijn van de 7-Sylowondergroep en  $y$  een voortbrenger van een 3-Sylowondergroep. Laat zien dat geldt  $yx y^{-1} = x^2$  of  $yx y^{-1} = x^4$ . Laat verder zien dat er precies twee isomorfiëklassen van groepen van orde 21 zijn.
- 10) Bewijs dat een normaaldeeler  $N$  van een eindige groep  $G$  met  $\#N = p^k$  met  $p$  een priemgetal bevat is in iedere  $p$ -Sylow-ondergroep van  $G$ .
- 11) Hoeveel 2-Sylow ondergroepen bezit  $S_4$ ?
- 12) Laat  $G$  een eindige groep zijn en  $p$  een priemgetal. Laat  $\Sigma$  de verzameling van  $p$ -Sylowondergroepen van  $G$  zijn. Laat verder  $H$  een ondergroep van  $G$  zijn waarvan de orde een macht van  $p$  is.
  - i) Laat zien dat de werking van  $H$  op  $\Sigma$  door middel van conjugatie een vast punt in  $\Sigma$  heeft.
  - ii) Bewijs dat  $H$  bevat is in een  $p$ -Sylowondergroep.

## 7. HILBERT 90 EN CYKLISCHE UITBREIDINGEN

*damit auch hier der Grundsatz von Riemann verwirklicht würde  
demzufolge man die Beweise nicht durch Rechnung,  
sondern lediglich durch Gedanken zwingen soll.*  
Hilbert in zijn *Zahlbericht* (1897)

Laat  $L/K$  een separabele lichaamsuitbreiding zijn van eindige graad. We kiezen een algebraïsche afsluiting  $\bar{K}$  van  $K$ . Als de graad  $[L : K] = r$  is, dan zijn er precies  $r$  verschillende lichaamsinbeddingen van  $L$  in  $\bar{K}$ . Immers, we kunnen  $L$  verkrijgen door een element  $\alpha$  te adjungeren,  $L = K(\alpha)$ , en door  $\alpha$  naar een van de  $r$  verschillende nulpunten van het minimumpolynoom van  $\alpha$  te sturen krijgen we  $r$  zulke inbeddingen. Wegens Propositie (3.9) kunnen het er ook niet meer zijn. Noem deze inbeddingen

$$\sigma_i : L \rightarrow \bar{K}, \quad i = 1, \dots, r.$$

We definiëren nu de *norm* en het *spoor* van een element  $x \in L$  ten opzichte van  $K$  door

$$N(x) = N_K^L(x) = \prod_{i=1}^r \sigma_i(x)$$

en

$$S(x) = S_K^L(x) = \sum_{i=1}^r \sigma_i(x).$$

Ga nu zelf na dat de norm  $N(x)$  en het spoor  $S(x)$  van  $x$  in  $K$  liggen. Als  $L = K(\alpha)$  en  $f = X^r + a_1 X^{r-1} + \dots + a_r$  het minimumpolynoom van  $\alpha$  ten opzichte van  $K$  is, dan weten we uit het bewijs van Stelling (4.10) dat

$$f = \prod_{i=1}^r (X - \sigma_i(\alpha)),$$

zodat dan  $S(x) = -a_1$  en  $N(x) = (-1)^r a_r$ .

De norm levert een homomorfisme van multiplicatieve groepen  $N : L^* \rightarrow K^*$  en het spoor is een homomorfisme van additieve groepen  $L \rightarrow K$ . De norm en het spoor gedragen zich netjes bij achtereenvolgende lichaamsuitbreidingen zoals uit de volgende propositie blijkt.

**(7.1) Propositie.** *Laat  $K \subset L \subset M$  eindige separabele lichaamsuitbreidingen zijn. Dan geldt*

$$N_K^M = N_K^L \circ N_L^M \quad \text{en} \quad S_K^M = S_K^L \circ S_L^M.$$

*Bewijs.* Laat  $\sigma_i$  voor  $i = 1, \dots, r$  de inbeddingen van  $L$  in  $\bar{K}$  zijn. Via  $\sigma_1$  kunnen we  $L$  als deellichaam van  $\bar{K}$  opvatten. Volgens Algebra 2, Hoofdstuk 8, kunnen we deze inbeddingen voortzetten tot inbeddingen  $M \rightarrow \bar{K}$ . We noteren deze voortzettingen weer met  $\sigma_i$ . Beschouw nu al de inbeddingen van  $M$  in  $\bar{K}$  die beperkt tot  $L$  gelijk zijn aan  $\sigma_1$ . We schrijven  $\tau_j$  voor  $j = 1, \dots, s$  met  $s = [M : L]$  voor deze inbeddingen. Dan is een willekeurige inbedding  $\rho$  van  $M$  in  $\bar{K}$  gelijk aan  $\sigma_i \tau_j$ . Immers,  $\rho$  beperkt tot  $L$  is gelijk

aan een  $\sigma_i$  en dus is  $\rho \circ \sigma_i^{-1}$  gelijk aan een  $\tau_j$ . Daarmee hebben we alle inbeddingen van  $M$  in  $\bar{K}$  gevonden. Als nu  $x \in L$  dan geldt

$$N_K^M(x) = \prod_{i,j} \sigma_i \tau_j(x) = \prod_{i=1}^r \sigma_i \left( \prod_{j=1}^s \tau_j(x) \right) = N_K^L(N_L^M(x)).$$

De identiteit voor het spoor gaat analoog.

**(7.2) Lemma.** *Laat  $L/K$  een eindige separabele uitbreiding zijn. Dan definieert de afbeelding*

$$L \times L \rightarrow K, \quad (x, y) \mapsto S(xy),$$

voor  $x, y \in L$  een niet-ontaarde symmetrische  $K$ -bilineaire vorm.

*Bewijs.* Omdat  $S(x) = \sum_{i=1}^r \sigma_i(x)$  volgt uit Lemma (3.8) dat  $S$  niet identiek nul is. Voor vaste  $y \in L$  is de afbeelding

$$S_y : L \rightarrow K, \quad x \mapsto S(xy)$$

duidelijk een  $K$ -lineaire afbeelding. Dit geeft ons een afbeelding

$$L \rightarrow L^\vee := \text{Hom}_K(L, K), \quad y \mapsto S_y$$

met  $K^\vee$  de duale  $K$ -vectorruimte, en de kern hiervan is  $(0)$ , want  $S_y$  is alleen de triviale afbeelding als  $y = 0$ , (ga na). Omdat  $\dim_K(L) = \dim_K(L^\vee)$  volgt dat dit een isomorfisme is. Maar dit betekent precies dat onze bilineaire afbeelding niet-ontaard is.

**(7.3) Stelling.** *(Hilbert 90) Laat  $L/K$  een Galoisuitbreiding zijn met een cyclische Galoisgroep  $G = \langle \sigma \rangle$  van orde  $n$ . Dan geldt voor elk element  $x \in L$ :*

$$N_K^L(x) = 1 \iff \text{er is een } y \in L^* \text{ met } x = y/\sigma(y).$$

*Bewijs.* ' $\Leftarrow$ ' Stel  $x = y/\sigma(y)$ . Omdat de norm een groepshomomorfisme  $L^* \rightarrow K^*$  levert volgt dat  $N(x) = N(y)/N(\sigma(y))$ . Maar duidelijk is uit de definitie van de norm dat  $N(y) = N(\sigma(y))$ , dus  $N(x) = 1$ . ' $\Rightarrow$ ' Laat  $x \in L$  met  $N(x) = 1$ . Beschouw de afbeelding  $L \rightarrow L$  gegeven door

$$z \mapsto z + x\sigma(z) + x\sigma(x)\sigma^2(z) + \dots + x\sigma(x)\sigma^2(x) \cdots \sigma^{n-2}(x)\sigma^{n-1}(z).$$

Merk op dat dit een som is van de verschillende karakters  $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$  (met coëfficiënten  $1, x, x\sigma(x), \dots$ ) dus wegens Lemma (3.8) is deze afbeelding niet identiek 0. Dus is er een  $\xi$  zodat

$$y := \xi + x\sigma(\xi) + x\sigma(x)\sigma^2(\xi) + \dots + x\sigma(x)\sigma^2(x) \cdots \sigma^{n-2}(x)\sigma^{n-1}(\xi)$$

ongelijk nul is. Men gaat nu eenvoudig na dat

$$x\sigma(y) = y$$

omdat  $N(x) = 1$ . Dit bewijst de stelling.

**(7.4) Voorbeeld.** Beschouw het lichaam  $\mathbb{Q}(i)$ . Dan geldt voor een element  $a + bi$  van  $\mathbb{Q}(i)$  dat  $a^2 + b^2 = 1$  dan en slechts dan als er een  $c + di$  in  $\mathbb{Q}(i) - \{0\}$  is met

$$a + bi = \frac{c + di}{c - di} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i.$$

Met andere woorden, de punten op de eenheidskring met rationale coördinaten  $(a, b)$  kunnen geparametriseerd worden door de punten  $(c : d)$  van de projectieve lijn over het lichaam  $\mathbb{Q}$  (het komt alleen op de verhouding van  $c$  en  $d$  aan). We zien hiermee dan ook hoe we alle Pythagoreïsche drietallen  $(x, y, z) \in \mathbb{Z}^3$  kunnen maken: als  $x^2 + y^2 = z^2$  en  $z \neq 0$  dan levert dit een punt  $(x/z, y/z)$  op de eenheidskring met rationale coördinaten:  $(x/z)^2 + (y/z)^2 = 1$ .

**(7.5) Stelling.** *Laat  $K$  een lichaam zijn en  $n$  een natuurlijk getal. Als de karakteristiek van  $K$  positief is eisen we dat die  $n$  niet deelt. Neem aan dat  $K$  een primitieve  $n$ -de machts eenheidswortel  $\zeta$  bevat. Dan is iedere cyclische Galoisuitbreiding van  $K$  van graad  $n$  van de vorm  $K(\alpha)$  met  $\alpha$  een nulpunt van een polynoom van de vorm  $x^n - a$  voor een  $a \in K$ .*

*Bewijs.* Laat  $L/K$  een cyclische Galoisuitbreiding van  $K$  zijn van graad  $n$  en  $\sigma$  een voortbrenger van de Galoisgroep  $G$ . We passen nu Hilbert 90 toe op  $\zeta$ . Omdat  $N(\zeta) = 1$  volgt dat er een  $y \in L$  is met  $\zeta = y/\sigma(y)$ , met andere woorden,  $\sigma(y) = \zeta^{-1}y$  en dan ook  $\sigma^i(y) = \zeta^{-i}y$ . We vinden zo  $n$  verschillende elementen  $\sigma^i(y)$  en dus geldt  $[K(y) : K] \geq n$ . We zien dus dat  $L = K(y)$ . Verder geldt

$$\sigma(y^n) = \zeta^{-n}y^n = y^n,$$

dus  $y^n \in K$ . Neem  $\alpha = y$  en  $a = y^n$ . Daarmee is de stelling bewezen.

**(7.6) Opmerking.** In Hoofdstuk 4 hebben we een analogon van bovenstaande stelling bewezen voor het geval dat  $n = p$  gelijk is aan de karakteristiek van  $K$ , namelijk Stelling (4.15). Een cyclische Galoisuitbreiding van graad  $p > 0$  van een lichaam van karakteristiek  $p$  wordt voortgebracht door adjunctie van een element  $\alpha$  met een minimumpolynoom van de vorm  $X^p - X - a$ . Zulke uitbreidingen heten Artin-Schreieruitbreidingen. Ga nu zelf de analogie tussen de twee bewijzen na.

We formuleren het behaalde resultaat (Stelling (7.5)) nog wat om. Hierbij gebruiken we de notatie

$$\mu_n = \mu_n(K)$$

voor de (multiplicatieve) groep van de  $n$ -de machts eenheidswortels in  $K$ .

**Stelling.** *Laat  $K$  een lichaam zijn dat  $n$  verschillende  $n$ -de machts eenheidswortels bevat. Laat  $K^*$  de multiplicatieve groep van  $K$  zijn en  $(K^*)^n$  de ondergroep van de  $n$ -de machten van elementen van  $K^*$ . Dan is er een bijectie tussen cyclische Galoisuitbreidingen van  $K$  en cyclische ondergroepen van orde  $n$  van  $K^*/(K^*)^n$  gegeven door*

$$K^*/(K^*)^n \supset \Delta \mapsto K(\Delta^{1/n})$$

en

$$L/K \mapsto K^* \cap (L^*)^n,$$

waarbij  $K(\Delta^{1/n})$  het lichaam is verkregen door de  $n$ -de machts wortels van de elementen van  $\Delta$  te adjungeren, en  $K^* \cap (L^*)^n$  de groep is bestaande uit de  $n$ -de machten van elementen uit  $L^*$  in  $K^*$ . Er is verder een groepsisomorfisme

$$\Delta \xrightarrow{\sim} \text{Hom}(\text{Gal}(L/K), \mu_n), \quad a \mapsto (\sigma \mapsto \sigma(\alpha)/\alpha)$$

met  $\alpha$  een (willekeurige)  $n$ -de machts-wortel van  $a$ .

*Bewijs.* Volgens de voorgaande stelling weten we dat een cyclische Galoisuitbreiding van de gedaante  $K(\sqrt[n]{a})$  is. Dus aan zo een  $K$  kunnen we de ondergroep van  $K^*/(K^*)^n$  voortgebracht door  $a$  toevoegen. Omgekeerd, aan een cyclische ondergroep van  $K^*/(K^*)^n$  voortgebracht door, zeg,  $a$  voegen we  $K(\sqrt[n]{a})$  toe. Dit geeft de gevraagde bijjectie. (Ga na.)

Als  $L = K(\alpha)$  een cyclische Galoisuitbreiding is van  $K$  met  $\alpha^n = a \in K$  en  $\sigma$  een voortbrenger van  $\Delta = \text{Gal}(L/K)$  dan is  $\sigma(\alpha)/\alpha$  een primitieve  $n$ -de machtseenheidswortel; was dat niet het geval, dan had  $\sigma$  niet orde  $n$ . Dit geeft het gevraagde isomorfisme.

Stelling (7.4), ook wel Hilbert 90 genoemd omdat het de negentigste stelling in het fameuze ‘Zahlbericht’ van Hilbert was, is een manifestatie van het begrip *cohomologie*. We herformuleren en bewijzen dit resultaat daarom in deze context.

Laat  $G$  een groep zijn en  $M$  een abelse groep. We nemen aan dat de groep  $G$  werkt op  $M$  door middel van automorfismen:

$$\rho : G \rightarrow \text{Aut}(M),$$

met  $\text{Aut}(M)$  de groep van automorfismen van  $M$ . We zeggen dan dat  $M$  een  $G$ -moduul is.

**(7.7) Definitie.** Een 1-cocykel van  $G$  met waarden in  $M$  is een afbeelding  $\xi : G \rightarrow M$ , geschreven als  $\sigma \mapsto \xi_\sigma$ , die voldoet aan

$$\xi_\sigma + \sigma(\xi_\tau) = \xi_{\sigma\tau} \quad \text{voor alle } \sigma, \tau \in G. \quad (1)$$

Zo een afbeelding  $\xi : G \rightarrow M$  die aan (1) voldoet heet wel een *gekruist homomorfisme*.

We kunnen 1-cocykels optellen door de waarden in  $M$  op te tellen. Dit maakt van de verzameling van zulke 1-cocykels een abelse groep, die we noteren met  $Z^1(G, M)$ . Een 1-cocycland is een 1-cocykel  $\xi$  van de vorm  $\xi_\sigma = \sigma(a) - a$  voor alle  $\sigma \in G$  en een element  $a \in M$ . Er geldt dan inderdaad dat  $\xi_\sigma + \sigma(\xi_\tau) = \sigma(a) - a + \sigma(\tau(a)) - a = \xi_{\sigma\tau}$ . De 1-cocyclanden vormen een ondergroep  $B^1(G, M)$  van  $Z^1(G, M)$ .

**(7.8) Definitie.** De eerste cohomologiegroep van  $G$  met waarden in  $M$  is het quotient

$$H^1(G, M) := Z^1(G, M)/B^1(G, M).$$

Een voorbeeld van een abelse groep met een werking van een groep  $G$  wordt gegeven door een Galoisuitbreiding  $L/K$  met Galoisgroep  $G$  en voor  $M$  de multiplicatieve groep  $L^*$  of de additieve groep  $L$  te nemen. Dan werkt  $G$  op de natuurlijke manier op  $L^*$  en  $L$ .

**(7.9) Stelling.** *Laat  $L/K$  een Galoisuitbreiding zijn met (eindige) Galoisgroep  $G$ . Dan geldt*

$$H^1(G, L^*) = \{1\} \quad \text{en} \quad H^1(G, L) = \{0\}.$$

*Bewijs.* We doen het multiplicatieve geval en laten het analoge bewijs in het additieve geval aan de lezer. Een 1-cocykel  $\xi$  voldoet dan aan de relatie

$$\xi_\sigma \sigma(\xi_\tau) = \xi_{\sigma\tau} \quad \text{voor alle } \sigma, \tau \in G.$$

(Merk op dat de relatie (1) hier multiplicatief wordt geschreven.) Wegens Lemma (3.8) ('verschillende karakters zijn lineair onafhankelijk') weten we dat er een element  $y \in L$  is zodat

$$u = \sum_{\sigma \in G} \xi_\sigma \sigma(y)$$

ongelijk nul is. Passen we nu  $\tau \in G$  toe op  $u$  dan vinden we

$$\tau(u) = \sum_{\sigma \in G} \tau(\xi_\sigma) \tau \sigma(y) = \sum_{\sigma \in G} \xi_{\tau\sigma} \xi_\tau^{-1} \tau \sigma(y) = \xi_\tau^{-1} \sum_{\sigma \in G} \xi_{\tau\sigma} \tau \sigma(y) = \xi_\tau^{-1} u.$$

We zien dus dat  $\xi_\tau = u/\tau(u)$ . Dat is niet helemaal wat we wilden, maar als we  $u$  door  $u^{-1}$  vervangen zien we dat  $\xi$  een 1-corand is. Dit bewijst het resultaat.

**(7.10) Opmerking.** We gaan nu na dat Stelling (7.3) een gevolg is van Stelling (7.9). Laat  $G$  een eindige cyclische groep van orde  $n$  zijn met voortbrenger  $\sigma$ . Als  $f : G \rightarrow M$  een gekruist homomorfisme is dan geldt  $f(\sigma^2) = f(\sigma) + \sigma(f(\sigma))$  en algemener

$$f(\sigma^i) = f(\sigma) + \sigma(f(\sigma)) + \dots + \sigma^{i-1}(f(\sigma)) \quad \text{voor } i = 1, \dots, n,$$

zoals met inductie uit (1) volgt. Omdat voor het eenheidselement van  $G$  geldt dat  $f(e) = 0$  volgt dat

$$f(\sigma) + \sigma(f(\sigma)) + \dots + \sigma^{n-1}(f(\sigma)) = 0. \quad (2)$$

Omgekeerd, als  $m \in M$  een element is in  $M$  dat voldoet aan de relatie

$$m + \sigma(m) + \dots + \sigma^{n-1}(m) = 0,$$

dan definieert de afbeelding  $\sigma^i \mapsto m + \sigma(m) + \dots + \sigma^{i-1}(m)$  een gekruist homomorfisme zoals men eenvoudig nagaat. Kortom, als  $G$  cyclisch is corresponderen gekruiste homomorfismen 1 – 1 met elementen  $m$  die aan (2) voldoen.

De gekruiste homomorfismen die corresponderen met 1-coranden zijn die afbeeldingen  $f$  met  $f(\sigma) = \sigma(\nu) - \nu$  voor een (vaste)  $\nu \in M$ .

Laat  $L/K$  een cyclische Galoisuitbreiding zijn en  $x \in L$  een element met norm  $N(x) = 1$ . De conditie  $N(x) = 1$  is het multiplicatieve equivalent van (2). Dan levert de afbeelding

$$\text{Gal}(L/K) = \langle \sigma \rangle \rightarrow L^*, \quad \sigma \mapsto x$$

een gekruist homomorfisme, ofwel een 1-cocykel van  $\text{Gal}(L/K)$  met waarden in  $L^*$ . Omdat de cohomologiegroep triviaal is, is er dus een element  $y$  in  $L^*$  zodat  $x = \sigma(y)/y$ . Dus de trivialiteit van de eerste cohomologiegroep  $H^1(G, L^*)$  bewijst Stelling (7.3), dat wil zeggen, Hilbert 90.

### Opgaven

1) Laat  $L/K$  een separabele uitbreiding zijn. Laat  $\alpha \in L$ . Dan geeft vermenigvuldiging met  $\alpha$  een  $K$ -lineaire afbeelding  $\phi_\alpha : L \rightarrow L$ . Laat zien dat  $\det(\phi_\alpha) = N_K^L(\alpha)$  en  $\text{Tr}(\phi_\alpha) = S_K^L(\alpha)$ .

2) Laat  $K$  een lichaam zijn en  $p$  een priemgetal. Laat  $x^p - a \in K[x]$  een reducibel polynoom zijn. Bewijs dat het een nulpunt heeft in  $K$ .

3) Laat  $p$  een priemgetal zijn en  $a \in \mathbb{Q}$  een rationaal getal dat geen  $p$ -de macht is. Laat  $K$  het ontbindingslichaam van  $x^p - a$  over  $\mathbb{Q}$  zijn.

i) Bewijs dat  $[K : \mathbb{Q}] = p(p-1)$ .

ii) Bewijs dat  $\text{Gal}(K/\mathbb{Q})$  isomorf is met de groep van matrices

$$\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x, y \in \mathbb{F}_p \right\}.$$

iii) Geef expliciet aan hoe de elementen  $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$  en  $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$  op  $K$  werken.

4) Laat  $L = K(\alpha)$  een eindige separabele uitbreiding zijn en laat  $f \in K[x]$  het minimumpolynoom van  $\alpha$  over  $K$  zijn. Schrijf

$$f/(x - \alpha) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$$

met  $b_i \in L$ . Bewijs:

i) De elementen  $1, \alpha, \dots, \alpha^{n-1}$  vormen een  $K$ -basis van  $L$ .

ii) Bewijs de identiteit

$$\sum_{i=1}^n \frac{f}{(x - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r$$

waarbij  $0 \leq r \leq n-1$  en de  $\alpha_i$  de nulpunten van  $f$  zijn.

iii) Bewijs

$$S\left(\alpha^i \frac{b_j}{f'(\alpha)}\right) = \delta_{ij}.$$

iv) De elementen  $b_i/f'(\alpha)$  met  $i = 0, \dots, n-1$  vormen ook een  $K$ -basis van  $L$ ;

5) Bekijk het Frobeniusautomorfisme  $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$  gegeven door  $x \mapsto x^p$  op een eindig lichaam  $\mathbb{F}_q$  met  $q = p^m$ . Laat zien dat  $F$  een  $\mathbb{F}_p$ -lineaire afbeelding van  $\mathbb{F}_q$  naar zichzelf is. Bepaal de eigenvectoren en de eigenwaarden.

6) Laat  $G$  een eindige groep zijn en  $A$  en  $B$   $G$ -modulen. Een homomorfisme van  $G$ -modulen is een groepshomomorfisme  $f : A \rightarrow B$  met  $f(\sigma(a)) = \sigma(f(a))$  voor alle  $a \in A$  en  $\sigma \in G$ . Definiëer

$$M^G := \{m \in M : \sigma(m) = m, \forall \sigma \in G\}.$$

Bewijs: als  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  een exact rijtje  $G$ -modulen is dan is er een exacte rij

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C).$$

7) Leid Stelling (4.15) over Artin-Schreier-uitbreidingen af uit de additieve variant van Stelling (7.9) die zegt dat  $H^1(G, L) = (0)$ .