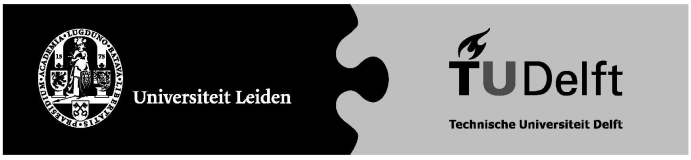
ALGEBRA III

P. Stevenhagen



2008

INHOUDSOPGAVE ALGEBRA III

21. Lichaamsuitbreidingen 5

Uitbreidingslichamen • Algebraïsch en transcendent • Formele adjunctie van nulpunten • Expliciete berekeningen • Algebraïsche afsluiting • Ontbindingslichamen • Eenduidigheidsstellingen • Opgaven

22. Eindige lichamen 21

Het lichaam $\mathbf{F}_{p^n}$ • Frobeniusautomorfisme • Irreducibele polynomen over $\mathbf{F}_p$ • Automorfismen van $\mathbf{F}_q$ • Opgaven

23. Separabele en normale uitbreidingen 31

Fundamentele verzameling • Separabele uitbreidingen • Perfecte lichamen • Primitieve elementen • Normale uitbreidingen • Onafhankelijkheid van karakters • Norm en spoor • Opgaven

24. Galoistheorie 42

Galoisuitbreidingen • Hoofdstelling • Bewijs van de hoofdstelling • Galoisgroep van een polynoom • Twee voorbeelden • Cyclische uitbreidingen • Cyclotomische uitbreidingen • Opgaven

25. Radicaaluitbreidingen 60

Constructieproblemen • Kwadratische afsluiting • Radicaalafsluiting • Onoplosbare polynomen • Wortelformules • Opgaven

26. Toepassingen van Galoistheorie 77

Hoofdstelling van de algebra • Kwadratische reciprociteit • Symmetrische polynomen • Opgaven

27. Categorieën en functoren 80

Categorieën • Functoren • Universele constructies • Opgaven

Literatuurverwijzingen 89

Oude tentamens 92

Index 95

Verschijningsdatum van deze oplage: januari 2008

Iedere volgende versie bevat hopelijk minder typefouten en onnauwkeurigheden dan de huidige – stuur hiertoe alle op- en aanmerkingen naar psh@math.leidenuniv.nl.

Postadres van de auteur:

Prof. dr. P. Stevenhagen
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

21 Lichaamsuitbreidingen

Na de nulring zijn lichamen[1] de commutatieve ringen met de eenvoudigst denkbare ideaalstructuur. Door de afwezigheid van niet-triviale idealen zijn alle homomorfismen $K \to L$ tussen lichamen injectief, en dit stelt ons in staat ze als *inclusies* op te vatten. Gegeven lichamen K en L kunnen er meerdere inclusies bestaan, en vaak (zie 23.2) is het nuttig de hele verzameling $\mathrm{Hom}(K, L)$ van lichaamshomomorfismen $K \to L$ te bestuderen.

▶ Uitbreidingslichamen

Een *uitbreidingslichaam* van een lichaam K is een lichaam L dat K als deellichaam bevat. Men noemt $K \subset L$ een *lichaamsuitbreiding*, ook wel genoteerd als L/K. Klassieke voorbeelden in de analyse zijn de lichaamsuitbreidingen $\mathbf{Q} \subset \mathbf{R}$ en $\mathbf{R} \subset \mathbf{C}$. Ieder lichaam K is als uitbreidingslichaam van een minimaal lichaam $k \subset K$ op te vatten.

21.1. Stelling. *Zij K een lichaam. Dan is de doorsnijding k van alle deellichamen van K weer een lichaam, en het is isomorf met $\mathbf{Q}$ of met een eindig lichaam $\mathbf{F}_p$.*

Bewijs. We bekijken het unieke ringhomomorfisme $\phi : \mathbf{Z} \to K$. Het beeld $\phi[\mathbf{Z}]$ is bevat in ieder deellichaam van K, dus ook in k. Omdat $\mathbf{Z}/\ker(\phi) \cong \phi[\mathbf{Z}]$ als deelring van een lichaam een domein is, is $\ker \phi$ een priemideaal in $\mathbf{Z}$. Als ϕ niet-injectief is, hebben we $\ker \phi = p\mathbf{Z}$ voor een priemgetal p, en dan is $\phi[\mathbf{Z}] \cong \mathbf{F}_p$ een deellichaam van k, en dus gelijk aan k. Als ϕ wel injectief is, bevat k een deelring $\phi[\mathbf{Z}] \cong \mathbf{Z}$. Omdat ieder lichaam dat $\mathbf{Z}$ bevat ook quotiënten van elementen uit $\mathbf{Z}$ bevat, vinden we in dit geval dat k een deellichaam isomorf met $\mathbf{Q}$ bevat, en dus zelf isomorf is met $\mathbf{Q}$. □

Het lichaam k in 21.1 heet het *priemlichaam* van K. Een lichaam K met $k \cong \mathbf{F}_p$ heet *van karakteristiek p*. In het geval $k \cong \mathbf{Q}$ heet K *van karakteristiek* 0.

Opgave 1. Bestaan er homomorfismen tussen lichamen van verschillende karakteristiek?

Voor een lichaamsuitbreiding $K \subset L$ geeft de vermenigvuldiging $L \times L \to L$ door beperking een scalair product $K \times L \to L$. Hierdoor is L een vectorruimte over K.

Opgave 2. Ga na welke ringaxioma's impliceren dat L een K-vectorruimte is.

Wegens 16.6 en 16.7 kunnen we voor iedere lichaamsuitbreiding $K \subset L$ een basis kiezen van L als vectorruimte over K, en is de cardinaliteit van zo'n basis, de dimensie van L over K, onafhankelijk van de gemaakte keuze.

21.2. Definitie. *De graad $[L : K]$ van een lichaamsuitbreiding $K \subset L$ is de dimensie van L als K-vectorruimte.*

Een lichaamsuitbreiding van eindige graad wordt kortweg *eindig* genoemd. Eindige lichaamsuitbreidingen van $\mathbf{Q}$ heten *getallenlichamen*. Voorbeelden hiervan zijn de quotiëntenlichamen $\mathbf{Q}(i)$ en $\mathbf{Q}(\sqrt{-5})$ van de ringen $\mathbf{Z}[i]$ en $\mathbf{Z}[\sqrt{-5}]$ uit §12. Uitbreidingen van graad 2 en 3 heten respectievelijk *kwadratisch* en *kubisch*.

In een *keten* $K \subset L \subset M$ van lichaamsuitbreidingen, ook wel een *toren* van lichamen genoemd, gedraagt de graad zich multiplicatief.

21.3. Stelling. *Zij $K \subset L \subset M$ een toren van lichamen, X een K-basis van L en Y een L-basis van M. Dan vormt de verzameling van elementen xy met $x \in X$ en $y \in Y$ een K-basis van M, en er geldt*

$$[M : K] = [M : L] \cdot [L : K].$$

In het bijzonder is $K \subset M$ eindig dan en slechts dan als $K \subset L$ en $L \subset M$ het zijn.

Bewijs. Elk element $c \in M$ is uniek te schrijven als $c = \sum_{y \in Y} b_y \cdot y$ met coëfficiënten $b_y \in L$ die bijna allemaal 0 zijn. De elementen $b_y \in L$ hebben elk een unieke representatie als $b_y = \sum_{x \in X} a_{xy} x$ met coëfficiënten $a_{xy} \in K$ die bijna allemaal 0 zijn. Gesubstitueerd in de eerste representatie geeft dit een unieke schrijfwijze

$$c = \sum_{y \in Y} (\sum_{x \in X} a_{xy} x) y = \sum_{(x,y) \in X \times Y} a_{xy} xy$$

voor c als eindige K-lineaire combinatie van de elementen xy met $x \in X$ en $y \in Y$. In het bijzonder vormen de elementen xy voor $(x, y) \in X \times Y$ een basis van M over K.

Omdat de cardinaliteit van $X \times Y$ gelijk is aan $\#X \cdot \#Y$ krijgen we de productrelatie $[M : K] = [M : L] \cdot [L : K]$ voor de graden. Het is duidelijk dat $X \times Y$ eindig is dan en slechts dan als X en Y het zijn, want X en Y zijn niet-leeg. □

In een uitbreiding $K \subset L$ brengt ieder element $\alpha \in L$ een deelring

$$K[\alpha] = \{\textstyle\sum_{i \geq 0} c_i \alpha^i : c_i \in K\} \subset L$$

voort bestaande uit polynomiale uitdrukkingen in α met coëfficiënten in K. Als deelring van een lichaam is $K[\alpha]$ een domein, en we geven met $K(\alpha) \subset L$ het quotiëntenlichaam van $K[\alpha]$ aan. Dit lichaam, dat het kleinste deellichaam van L is dat zowel K als α bevat, heet de uitbreiding van K *voortgebracht* door α.

Algemener kan men voor een deelverzameling $S \subset L$ de ring $K[S] \subset L$ vormen bestaande uit polynomiale uitdrukkingen in de elementen van S met coëfficiënten uit K. Deze ring is als deelring van L weer een domein, en met $K(S) \subset L$ geven we zijn quotiëntenlichaam aan. Het lichaam $K(S)$ is het kleinste deellichaam van L dat K en S bevat. Het is de uitbreiding van K *voortgebracht door* S.

Een lichaamsuitbreiding van K voortgebracht door een eindige verzameling S heet *eindig voortgebracht* over K. Voor $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ noteren we $K[S] = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ en $K(S) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Bestaat S uit een enkel element, dan spreken we van een *enkelvoudige* of *primitieve* uitbreiding van K. Zijn K_1 en K_2 deellichamen van L die K bevatten, dan heet het deellichaam $K_1 K_2 \subset L$ voortgebracht door $S = K_1 \cup K_2$ over K het *compositum* van K_1 en K_2 binnen L.

Opgave 3. Laat zien dat een compositum (binnen L) van eindig voortgebrachte uitbreidingen van K weer eindig voortgebracht is.

21.4. Voorbeelden. In de uitbreiding $\mathbf{Q} \subset \mathbf{C}$ brengt $\sqrt{2}$ over $\mathbf{Q}$ de deelring

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$$

voort. Wegens de identiteit $(\sqrt{2})^2 = 2 \in \mathbf{Q}$ zijn er geen hogere machten van $\sqrt{2}$ nodig. De ring $\mathbf{Q}[\sqrt{2}]$ is gelijk aan zijn quotiëntenlichaam $\mathbf{Q}(\sqrt{2})$, want ieder element $a + b\sqrt{2} \neq 0$ heeft een inverse $\frac{1}{a^2-2b^2}(a - b\sqrt{2}) \in \mathbf{Q}[\sqrt{2}]$.

Op soortgelijke wijze geeft ieder element $d \in \mathbf{Q}$ dat geen kwadraat is in $\mathbf{Q}$ aanleiding tot een *kwadratisch lichaam* $\mathbf{Q}(\sqrt{d})$, dat van graad 2 over $\mathbf{Q}$ is.

Voor de verzameling $S = \{i, \sqrt{2}\} \subset \mathbf{C}$ krijgt men $\mathbf{Q}[S] = \mathbf{Q}(S)$ als een kwadratische uitbreiding $L(i)$ van het lichaam $L = \mathbf{Q}(\sqrt{2})$. Immers, -1 is geen kwadraat in het reële lichaam $L \subset \mathbf{R}$. Wegens 21.3 heeft $\mathbf{Q}(\sqrt{2}, i) = L(i)$ graad $[L(i) : L] \cdot [L : \mathbf{Q}] = 2 \cdot 2 = 4$ over $\mathbf{Q}$ met basis $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

▶ Algebraïsch en transcendent

Een element α in een uitbreidingslichaam L van K heet *algebraïsch* over K als er een monisch polynoom $f \in K[X]$ bestaat met $f(\alpha) = 0$. Bestaat zo'n f niet, dan heet α *transcendent* over K. De uitbreiding $K \subset L$ heet *algebraïsch* als ieder element $\alpha \in L$ algebraïsch is over K.

In het geval van de uitbreiding $\mathbf{Q} \subset \mathbf{C}$ spreekt men kortweg van algebraïsche en transcendente getallen. Voorbeelden van algebraïsche getallen zijn 3, $\sqrt{2}$, $\sqrt[3]{10}$ en de primitieve n-de eenheidswortel $\zeta_n = e^{2\pi i/n}$ voor $n \geq 1$. Polynomen in $\mathbf{Q}[X]$ die deze elementen als nulpunt hebben, zijn respectievelijk

$$X - 3, \qquad X^2 - 2, \qquad X^3 - 10, \qquad X^n - 1.$$

Merk op dat de eerste drie polynomen irreducibel zijn in $\mathbf{Q}[X]$, maar dat $X^n - 1$ dat voor $n > 1$ niet is.

Opgave 4. Vind irreducibele polynomen in $\mathbf{Q}[X]$ met nulpunt $e^{2\pi i/n}$ voor $1 \leq n < 10$.

Omdat er maar aftelbaar veel algebraïsche getallen bestaan (opgave 21) en $\mathbf{C}$ overaftelbaar is, zijn er heel veel transcendente getallen. De Fransman Joseph Liouville (1809–1882) liet al rond 1850 zien dat zeer snel convergerende reeksen als $\sum_{k\geq 0} 10^{-k!}$ altijd een transcendente waarde hebben. Het is meestal echter erg moeilijk om te bewijzen dat een getal dat 'geen reden heeft om algebraïsch te zijn' daadwerkelijk transcendent is.

De eerste transcendentiebewijzen[2] voor de bekende reële getallen $e = \exp(1)$ en π werden in 1873 en 1882 gegeven door respectievelijk de Fransman Hermite (1822–1901) en de Duitser Lindemann (1852–1939). Onafhankelijk van elkaar vonden in 1934 de Rus Gelfond (1906–1968) en de Duitser Schneider (1911–1988) een oplossing voor één van de beroemde *Hilbertproblemen*[3] uit 1900: voor ieder tweetal algebraïsche getallen $\alpha \neq 0, 1$ en $\beta \notin \mathbf{Q}$ is α^β transcendent.

Opgave 5. Leid hieruit af dat niet alleen $2^{\sqrt{2}}$, maar ook $\log 3/\log 2$ en e^π transcendent zijn.

Van veel getallen, zoals Euler's constante $\gamma = \lim_{k\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k} - \log k)$ en de getallen 2^e, 2^π en π^e, is zelfs niet bekend of ze rationaal zijn.

21.5. Stelling. *Zij $K \subset L$ een lichaamsuitbreiding en $\alpha \in L$ een element.*

(1) *Als α transcendent is over K, dan is $K[\alpha]$ isomorf met de polynoomring $K[X]$ en $K(\alpha)$ isomorf met het lichaam $K(X)$ van rationale functies.*

(2) *Als α algebraïsch is over K, dan is er een uniek monisch irreducibel polynoom $f = f_K^\alpha \in K[X]$ dat α als nulpunt heeft. In dit geval is er een isomorfisme*

$$\begin{aligned} K[X]/(f_K^\alpha) &\xrightarrow{\sim} K[\alpha] = K(\alpha) \\ g \bmod (f_K^\alpha) &\longmapsto g(\alpha) \end{aligned}$$

van lichamen, en de graad $[K(\alpha) : K]$ is gelijk aan $\deg(f_K^\alpha)$.

Bewijs. We bekijken het ringhomomorfisme $\phi : K[X] \to L$ gegeven door $f \mapsto f(\alpha)$. Het beeld van ϕ is gelijk aan $K[\alpha]$, en net als in het bewijs van 21.1 hebben we twee mogelijkheden.

Als α transcendent is over K, dan is ϕ injectief en krijgen we een isomorfisme $K[X] \xrightarrow{\sim} K[\alpha]$ van $K[\alpha]$ met de polynoomring $K[X]$. Het quotiëntenlichaam $K(\alpha)$ is dan isomorf met $K(X)$.

Is α algebraïsch over K, dan is $\ker \phi$ een niet-triviaal ideaal van $K[X]$. Omdat $K[X]$ een hoofdideaaldomein is, is er een unieke monische voortbrenger $f = f_K^\alpha \in K[X]$ van $\ker \phi$. Dit is het 'kleinste' monische polynoom in $K[X]$ dat α als nulpunt heeft. De isomorfiestelling geeft een isomorfisme $K[X]/(f_K^\alpha) \xrightarrow{\sim} K[\alpha] \subset L$ van domeinen, dus (f_K^α) is een priemideaal in $K[X]$ en f_K^α is irreducibel. Omdat een priemideaal $(f_K^\alpha) \neq 0$ in een hoofdideaaldomein maximaal is (zie 15.6), is $K[X]/(f_K^\alpha) \cong K[\alpha]$ een lichaam, en dus gelijk aan $K(\alpha)$. Ieder polynoom in $K[X]$ heeft modulo (f_K^α) een unieke representant g van graad $\deg(g) < \deg(f_K^\alpha)$: zijn rest bij deling door f_K^α. Als f_K^α graad n heeft, dan vormen de restklassen van $\{1, X, X^2, \ldots, X^{n-1}\}$ een basis van $K[X]/(f_K^\alpha)$ over K. In het bijzonder heeft $K[\alpha] = K(\alpha)$ dan ook dimensie $[K(\alpha) : K] = n = \deg(f_K^\alpha)$ over K. □

21.6. Gevolg. *Iedere eindige lichaamsuitbreiding is algebraïsch.*

Bewijs. Als $\alpha \in L$ transcendent is over K, dan bevat L de deelring $K[\alpha]$, die wegens 21.5.1 oneindige dimensie heeft als K-vectorruimte. In het bijzonder is L zelf dan niet van eindige dimensie over K. □

Het polynoom f_K^α in 21.5.2 heet het *minimumpolynoom* of het *irreducibele polynoom* van α over K. Ieder polynoom $g \in K[X]$ met $g(\alpha) = 0$ is deelbaar door f_K^α. Omgekeerd laten we nu zien dat ieder monisch irreducibel polynoom in $K[X]$ opgevat kan worden als het minimumpolynoom van een element α in een uitbreidingslichaam L van K.

21.7. Stelling. *Zij K een lichaam, en $f \in K[X]$ een niet-constant polynoom. Dan bestaat er een uitbreiding $K \subset L$ waarin f een nulpunt α heeft. Is $f \in K[X]$ monisch en irreducibel, dan geldt bovendien $f = f_K^\alpha$.*

Bewijs. We nemen aan dat f irreducibel is, want voor reducibele f is ieder nulpunt van een irreducibele factor van f in $K[X]$ ook een nulpunt van f. Het ideaal $(f) \subset K[X]$ is dan maximaal, en $L = K[X]/(f)$ een lichaam. De samengestelde afbeelding

$$\varphi : K \to K[X] \to K[X]/(f) = L$$

is als lichaamshomomorfisme injectief, dus we kunnen L via φ als uitbreidingslichaam van K opvatten. Het element $\overline{X} = (X \bmod f) \in L$ is nu 'per definitie' een nulpunt van f, want er geldt

$$f(\overline{X}) = \overline{f(X)} = \overline{0} \in K[X]/(f) = L.$$

Is f behalve irreducibel ook monisch, dan is f het minimumpolynoom van $\overline{X}$. □

Het in het bewijs van 21.7 geconstrueerde lichaam $L = K[X]/(f)$ voor een irreducibel polynoom $f \in K[X]$ is het lichaam verkregen door *formele adjunctie* van een nulpunt van f aan K. Deze belangrijke constructie stelt ons in staat een lichaamsuitbreiding van K te construeren waarin een voorgeschreven polynoom een nulpunt heeft.

21.8. Voorbeelden. 1. Het polynoom $f = X^2+1$ is irreducibel over $\mathbf{R}$, en door formele adjunctie van een nulpunt van f krijgen we het uitbreidingslichaam $\mathbf{R}[X]/(X^2+1)$ van $\mathbf{R}$. In dit lichaam, dat uit uitdrukkingen $a+bX$ met $a, b \in \mathbf{R}$ bestaat, hebben we per definitie de rekenregel $X^2 = -1$. Natuurlijk is dit door adjunctie van een wortel uit -1 aan $\mathbf{R}$ gecreëerde lichaam niets anders dan het bekende lichaam $\mathbf{C}$: de afbeelding $a+bX \mapsto a+bi$ geeft een isomorfisme. Men kan dit isomorfisme ook vinden door 21.5.2 toe te passen op de uitbreiding $\mathbf{R} \subset \mathbf{C}$ met $\alpha = i \in \mathbf{C}$. Merk op dat er heel veel polynomen $g \in \mathbf{R}[X]$ zijn waarvoor $\mathbf{R}[X]/(g) \cong \mathbf{C}$ geldt: ieder kwadratisch polynoom zonder reële nulpunten, zoals $X^2 + X + r$ met $r > \frac{1}{4}$, voldoet.

2. Vervangt men in het bovenstaande het grondlichaam $\mathbf{R}$ door $\mathbf{Q}$, dan is $f = X^2+1$ nog steeds irreducibel. Het lichaam $\mathbf{Q}[X]/(X^2+1)$ is niets anders dan het getallenlichaam $\mathbf{Q}(i)$ dat we voor 12.19 tegenkwamen als quotiëntenlichaam van $\mathbf{Z}[i]$. Algemener geeft het polynoom $g = X^2 - d$ voor een element $d \in \mathbf{Q}$ dat geen kwadraat is in $\mathbf{Q}$ het kwadratische lichaam $\mathbf{Q}(\sqrt{d})$ uit 21.4.

Op soortgelijke wijze kunnen we voor ieder getal $d \in \mathbf{Q}$ dat geen derde macht is in $\mathbf{Q}$ door formele adjunctie van een nulpunt $\sqrt[3]{d}$ van het irreducibele polynoom $X^3 - d \in \mathbf{Q}[X]$ een kubische uitbreiding $\mathbf{Q}(\sqrt[3]{d})$ van graad 3 over $\mathbf{Q}$ maken. Merk op dat er geen reële of complexe getallen aan deze constructie te pas komen: $\sqrt[3]{d}$ is een *formeel nulpunt* van $X^3 - d$ dat niet a priori in $\mathbf{R}$ of $\mathbf{C}$ ligt. De vraag wat binnen $\mathbf{C}$ het compositum van $\mathbf{R}$ en het kubische lichaam $\mathbf{Q}(\sqrt[3]{d})$ is, is daarom ook betekenisloos zolang men geen *keuze* maakt voor een derdemachtswortel $\sqrt[3]{d}$ van d in $\mathbf{C}$: er zijn er drie!

Opgave 6. Laat zien dat het antwoord afhangt van de keuze van $\sqrt[3]{d}$ in $\mathbf{C}$.

3. Het getallenlichaam $\mathbf{Q}(\zeta_p)$ verkregen door een formeel nulpunt ζ_p van het p-de cyclotomische polynoom $\Phi_p \in \mathbf{Z}[X]$ uit voorbeeld 13.9.2 te adjungeren aan $\mathbf{Q}$ heet het *p-de cyclotomische lichaam*. Het heeft graad $\deg(\Phi_p) = p-1$ over $\mathbf{Q}$. We zullen $\mathbf{Q}(\zeta_p)$ nader bestuderen in 24.10.

Voor een lichaamsuitbreiding $K \subset L$ kunnen we de evaluatie-afbeelding $K[X] \to L$ in een punt $\alpha \in L$ ook voor n-tupels van elementen uit L beschouwen. We noemen een deelverzameling $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$ *algebraïsch onafhankelijk* over K als het

homomorfisme

$$\begin{aligned} K[X_1, X_2, \ldots, X_n] &\longrightarrow L \\ f &\longmapsto f(\alpha_1, \alpha_2, \ldots, \alpha_n) \end{aligned}$$

injectief is. Informeel gezegd: als er geen algebraïsche relaties tussen de elementen $\alpha_i \in L$ bestaan. Een oneindige deelverzameling $S \subset L$ heet algebraïsch onafhankelijk over K als ieder van zijn eindige deelverzamelingen dat is. Een uitbreiding $K \subset K(S)$ voortgebracht door een algebraïsch onafhankelijke verzameling $S \subset L$ heet een *zuiver transcendente uitbreiding* van K. Is $S \subset L$ een over K algebraïsch onafhankelijke verzameling met de eigenschap dat L algebraïsch is over $K(S)$, dan heet S een *transcendentiebasis* van L over K. Het is een 'maximale' algebraïsch onafhankelijke verzameling binnen L.

Opgave 7. Bewijs dat iedere lichaamsuitbreiding een transcendentiebasis heeft. [Hint: Zorn...]

▶ Expliciete berekeningen

Het rekenen in een eindige uitbreiding L van K is een tamelijk rechtstreekse combinatie van het rekenen in polynoomringen met technieken uit de lineaire algebra en kan probleemloos worden uitgevoerd door de hedendaagse[4] computeralgebra-pakketten. Het is niettemin zinnig een gevoel te hebben voor de aard van zulke berekeningen, en om ze in eenvoudige gevallen met de hand uit te kunnen voeren. In minder eenvoudige gevallen zijn de pakketten die met formele nulpunten kunnen rekenen een uitkomst.

We illustreren de berekeningen aan de hand van de uitbreiding $\mathbf{Q} \subset M = \mathbf{Q}(i, \sqrt{2})$ uit 21.4. Hier geldt $[M : \mathbf{Q}] = 4$, en we kunnen $\{1, i, \sqrt{2}, i\sqrt{2}\}$ als basis van M over $\mathbf{Q}$ nemen. Ieder element $\alpha \in M$ is wegens 21.6 algebraïsch over $\mathbf{Q}$. Het minimumpolynoom van zo'n element berekent men door net zolang machten van α op de gekozen basis uit te drukken tot er een afhankelijkheid tussen deze machten optreedt. Voor $\alpha = 1+i+\sqrt{2}$ vindt men door stug rekenen de volgende representatie van de machten van α op de gekozen basis:

$$\begin{aligned} \alpha^0 &= (1,\ \ 0,\ \ 0,\ \ 0), \\ \alpha^1 &= (1,\ \ 1,\ \ 1,\ \ 0), \\ \alpha^2 &= (2,\ \ 2,\ \ 2,\ \ 2), \\ \alpha^3 &= (4,\ \ 8,\ \ 2,\ \ 6), \\ \alpha^4 &= (0,24,\ \ 0,16). \end{aligned}$$

Pas de vijfde vector is afhankelijk van de voorafgaande, en met standaardtechnieken vindt men de relatie

$$\alpha^4 - 4\alpha^3 + 4\alpha^2 + 8 = 0.$$

Met de hand zijn er soms handigheidjes die het rekenwerk bekorten. Door de gelijkheid $\alpha - 1 = i + \sqrt{2}$ te kwadrateren vindt men $\alpha^2 - 2\alpha + 1 = 1 + 2i\sqrt{2}$, en nogmaals kwadrateren van $\alpha^2 - 2\alpha = 2i\sqrt{2}$ geeft de gezochte relatie

$$\alpha^4 - 4\alpha^3 + 4\alpha^2 = -8.$$

Anders dan in het eerste geval hebben we geen garantie dat deze relatie van minimale graad is. We moeten daarom apart nagaan of $X^4-4X^3+4X^2+8$ irreducibel is in $\mathbf{Q}[X]$.

Opgave 8. Laat zien dat $\frac{1}{8}X^4 f(\frac{2}{X})$ Eisenstein bij 2 is in $\mathbf{Z}[X]$. Concludeer dat f irreducibel is.

We zien uit het voorafgaande dat $M = \mathbf{Q}(i, \sqrt{2})$ gelijk is aan de enkelvoudige uitbreiding $\mathbf{Q}(\alpha) = \mathbf{Q}[X]/(X^4 - 4X^3 + 4X^2 + 8)$. Men noemt α een *primitief element* voor de uitbreiding $\mathbf{Q} \subset M$, en $\{1, \alpha, \alpha^2, \alpha^3\}$ een *machtsbasis* van M over $\mathbf{Q}$. In 23.9 zullen we zien dat veel lichaamsuitbreidingen een machtsbasis hebben. Omdat algebra-pakketten bij voorkeur met een voortbrengend element werken, kan het nuttig zijn een 'kleine voortbrenger' te zoeken.

Opgave 9. Laat zien dat $\beta = \frac{1}{2}\sqrt{2} + \frac{1}{2}i\sqrt{2}$ voldoet aan $\beta^4 + 1 = 0$, en dat $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$ geldt. Schrijf i en $\sqrt{2}$ op de basis van machten van β.

Vermenigvuldiging in een lichaam als $M = \mathbf{Q}(\alpha)$ geschiedt door uitdrukkingen te vermenigvuldigen als polynomen in α en de uitkomst te reduceren modulo de door het minimumpolynoom van α gegeven relatie. Dit betekent dat men als in 12.1 de rest van het polynoom dat de uitdrukking beschrijft bij deling door $f = f_{\mathbf{Q}}^{\alpha}$ bepaalt. Voor een basis die geen machtsbasis is, zoals de basis $\{1, i, \sqrt{2}, i\sqrt{2}\}$, dient men te weten hoe een product van twee basiselementen er op de gegeven basis uitziet.

De inverse van een element $g(\alpha) \in \mathbf{Q}(\alpha)$ bepaalt men hetzij met lineaire algebra, hetzij met de Euclidische algoritme. Om de inverse van bijvoorbeeld $\alpha^2 + 2\alpha \in M$ te berekenen schrijft men in het eerste geval de vergelijking

$$(a + b\alpha + c\alpha^2 + d\alpha^3)(\alpha^2 + 2\alpha) = 1$$

uit op de basis $\{1, \alpha, \alpha^2, \alpha^3\}$ als

$$(-1 - 8c - 48d) + 2(a - 4d)\alpha + (a + 2b - 4c - 24d)\alpha^2 + (b + 6c + 20d)\alpha^3 = 0.$$

Het stelsel lineaire vergelijkingen verkregen door alle coëfficiënten gelijk aan 0 te stellen lost men nu met standaardmethoden op: $(a, b, c, d) = (-\frac{2}{9}, -\frac{5}{36}, \frac{5}{24}, -\frac{1}{18})$ is de oplossing.

Indien men de Euclidische algoritme gebruikt zoals in 6.14 kan men de inverse van een element $g(\alpha)$ berekenen door herhaald deling met rest toe te passen op de relaties $0 \cdot g(\alpha) = f(\alpha)$ en $1 \cdot g(\alpha) = g(\alpha)$. Nemen we bijvoorbeeld $g(\alpha) = \alpha^2 + 2\alpha \in M = \mathbf{Q}(\alpha)$, dan krijgen we

$$\begin{aligned} 0 \cdot (\alpha^2 + 2\alpha) &= f(\alpha) = \alpha^4 - 4\alpha^3 + 4\alpha^2 + 8 \\ 1 \cdot (\alpha^2 + 2\alpha) &= g(\alpha) = \alpha^2 + 2\alpha \\ (-\alpha^2 + 6\alpha - 16) \cdot (\alpha^2 + 2\alpha) &= -32\alpha + 8 \\ (-4\alpha^3 + 15\alpha^2 - 10\alpha - 16) \cdot (\alpha^2 + 2\alpha) &= 72. \end{aligned}$$

In de laatste vergelijking is met 128 vermenigvuldigd om alle noemers te verdrijven. We vinden nogmaals $g(\alpha)^{-1} = -\frac{1}{18}\alpha^3 + \frac{5}{24}\alpha^2 - \frac{5}{36}\alpha - \frac{2}{9}$. In grotere lichamen wordt het met de hand uitvoeren van dergelijke berekeningen al snel tijdrovend.

▶ Algebraïsche afsluiting

Uit 21.5 volgt dat een element α in een uitbreidingslichaam L van K algebraïsch is over K dan en slechts dan als $K(\alpha)$ een eindige uitbreiding is van K. Algemener is een eindig voortgebrachte uitbreiding $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ van K eindig dan en slechts dan als alle α_i algebraïsch zijn over K. De voorwaarde is evident noodzakelijk: een transcendent element brengt een oneindige uitbreiding voort. Hij is echter ook voldoende, want voor algebraïsche α_i kan $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ verkregen worden als een toren

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

van n enkelvoudige eindige uitbreidingen. Wegens 21.3 levert dit een eindige uitbreiding op, en deze is wegens 21.6 algebraïsch. Voor $n = 2$ zien we dat sommen, verschillen, producten en quotiënten van algebraïsche elementen α_1 en α_2 weer algebraïsch zijn over K. Er volgt dat voor een willekeurige uitbreiding $K \subset L$ de verzameling

$$K_0 = \{\alpha \in L : \quad \alpha \text{ is algebraïsch over } K\}$$

een *deellichaam* van L is. Het heet de *algebraïsche afsluiting van K in L*. Het is de grootste algebraïsche uitbreiding van K binnen L.

21.9. Stelling. *Voor een toren $K \subset L \subset M$ van lichamen geldt:*

$$K \subset M \text{ is algebraïsch} \quad \Longleftrightarrow \quad K \subset L \text{ en } L \subset M \text{ zijn algebraïsch.}$$

Bewijs. Als $K \subset M$ algebraïsch is, dan volgt rechtstreeks uit de definitie dat $K \subset L$ en $L \subset M$ het ook zijn.

Neem nu aan dat $K \subset L$ en $L \subset M$ algebraïsche uitbreidingen zijn, en zij $c \in M$ willekeurig. Dan heeft c een minimumpolynoom $f_L^c = \sum_{i=0}^{n} b_i X^i \in L[X]$ over L. Ieder van de elementen $b_i \in L$ is algebraïsch over K, dus $L_0 = K(b_1, b_2, \ldots, b_n)$ is een eindige uitbreiding van K. Omdat c ook algebraïsch is over L_0, is de uitbreiding $L_0 \subset L_0(c)$ eindig. Wegens 21.3 is de uitbreiding $K \subset L_0(c)$ ook eindig, en wegens 21.6 is hij dan algebraïsch. In het bijzonder volgt dat c algebraïsch is over K, en we concluderen dat $K \subset M$ algebraïsch is. □

Opgave 10. Zij $\overline{\mathbf{Q}}$ de algebraïsche afsluiting van $\mathbf{Q}$ in $\mathbf{C}$. Bewijs: ieder element $\alpha \in \mathbf{C} \setminus \overline{\mathbf{Q}}$ is transcendent over $\overline{\mathbf{Q}}$.

We gaan nu voor een lichaam K een 'grootst mogelijke' algebraïsche uitbreiding $\overline{K}$ maken. Wegens 21.9 kan het lichaam $\overline{K}$ dan zelf geen echte algebraïsche uitbreiding $\overline{K} \subsetneq M$ meer hebben, en wegens 21.7 heeft dus ieder niet-constant polynoom $f \in \overline{K}[X]$ een nulpunt in $\overline{K}$. Dergelijke lichamen, die we al in §15 tegenkwamen, heten *algebraïsch afgesloten*.

21.10. Definitie. *Een lichaam K heet algebraïsch afgesloten als het voldoet aan de volgende equivalente eigenschappen:*

1. *voor iedere algebraïsche uitbreiding $K \subset L$ geldt $L = K$;*

2. *ieder niet-constant polynoom $f \in K[X]$ heeft een nulpunt in K;*
3. *ieder monisch polynoom $f \in K[X]$ is te schrijven als $f = \prod_{i=1}^{n}(X - \alpha_i)$ voor zekere $\alpha_i \in K$.*

Het bekendste voorbeeld van een algebraïsch afgesloten lichaam is het lichaam $\mathbf{C}$. Bewijzen van het feit dat polynomen in $\mathbf{C}[X]$ van graad n bij telling met multipliciteiten precies n complexe nulpunten hebben, werden zo'n 200 jaar geleden al gegeven door Gauss. Het precies maken van zo'n bewijs was toen niet gemakkelijk, want alle bewijzen gebruiken 'topologische eigenschappen' van reële of complexe getallen die pas later in de 19e eeuw exact geformuleerd werden. De naamgeving van de volgende stelling, die we al noemden in §13, is traditioneel.

21.11. Hoofdstelling van de algebra. *Het lichaam $\mathbf{C}$ van de complexe getallen is algebraïsch afgesloten.*

Moderne bewijzen gebruiken vaak (complexe) analyse. Wij geven in 26.3 een bewijs met Galoistheorie dat alleen de tussenwaardestelling uit de reële analyse gebruikt.

Een algebraïsche uitbreiding $K \subset L$ met de eigenschap dat L algebraïsch afgesloten is heet een *algebraïsche afsluiting* van K. Weten we eenmaal dat er een algebraïsch afgesloten lichaam is dat K bevat, dan is zo'n algebraïsche afsluiting gemakkelijk te maken.

21.12. Stelling. *Zij K een lichaam en Ω een algebraïsch afgesloten lichaam dat K bevat. Dan is de algebraïsche afsluiting*

$$\overline{K} = \{\alpha \in \Omega : \quad \alpha \text{ is algebraïsch over } K\}$$

van K in Ω algebraïsch afgesloten. In het bijzonder is

$$\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} : \quad \alpha \text{ is algebraïsch over } \mathbf{Q}\}$$

een algebraïsche afsluiting van $\mathbf{Q}$.

Bewijs. Is $f \in \overline{K}[X] \subset \Omega[X]$ een niet-constant polynoom, dan heeft f wegens 21.10 een nulpunt $\alpha \in \Omega$. Het deellichaam $\overline{K}(\alpha) \subset \Omega$ is algebraïsch over $\overline{K}$, en $\overline{K}$ is per definitie algebraïsch over K. Wegens 21.9 is $\overline{K}(\alpha)$ weer algebraïsch over K, en dus bevat in $\overline{K}$. Er volgt dat f een nulpunt $\alpha \in \overline{K}$ heeft, dus $\overline{K}$ is algebraïsch afgesloten.

Voor $K = \mathbf{Q}$ kunnen we wegens 21.11 het lichaam Ω gelijk nemen aan $\mathbf{C}$. □

Omdat $\mathbf{C}$ transcendente getallen bevat is het lichaam $\overline{\mathbf{Q}}$ in 21.12 niet gelijk aan $\mathbf{C}$.

Voor willekeurige K kan men met behulp van 21.12 een algebraïsche afsluiting van K definiëren indien er een algebraïsch afgesloten lichaam Ω is dat K bevat. Zo'n Ω bestaat altijd. Omdat K echter heel groot kan zijn, berusten algemene constructies van Ω op het keuzeaxioma. De Duitser Ernst Steinitz (1871–1928) gaf in 1910 als eerste zo'n constructie. Onderstaand bewijs met behulp van het gevolg 15.10 van het lemma van Zorn is van de hand van de Oostenrijker Emil Artin (1898–1962).

21.13. Stelling. *Voor ieder lichaam K bestaat er een algebraïsch afgesloten uitbreidingslichaam $\Omega \supset K$.*

Bewijs. Zij $\mathcal{F}$ de collectie van niet-constante polynomen in $K[X]$, en $R = K[\{X_f : f \in \mathcal{F}\}]$ de polynoomring over K in de (oneindig vele) variabelen X_f. In deze grote ring R laten we I het ideaal zijn voortgebracht door alle polynomen $f(X_f)$ met $f \in \mathcal{F}$. We beweren dat I niet gelijk is aan de hele ring R.

Immers, ieder element $x \in I$ is te schrijven als een *eindige* som $x = \sum_f r_f \cdot f(X_f)$ met $r_f \in R$. In deze som komen slechts eindig veel variabelen X_f voor, zeg voor f in de eindige verzameling $\mathcal{F}_x \subset \mathcal{F}$. Door herhaald toepassen van 21.7 kunnen we een uitbreidingslichaam K' van K maken waarin ieder van de polynomen $f \in \mathcal{F}_x$ een nulpunt $\alpha_f \in K'$ heeft. Zij nu $\phi : R \to K'$ de evaluatie-afbeelding gedefinieerd door $X_f \mapsto \alpha_f$ voor $f \in \mathcal{F}_x$ en $X_f \mapsto 0$ voor $f \notin \mathcal{F}_x$. Dan is ϕ een ringhomomorfisme, en wegens $\phi(f(X_f)) = f(\alpha_f) = 0$ voor $f \in \mathcal{F}_x$ hebben we $\phi(x) = 0$. Er volgt dat x niet het constante polynoom $1 \in R$ is, dus $1 \notin I$.

Zij nu M als in 15.12 een maximaal ideaal van R dat I omvat, en definieer $L_1 = R/M$. Dan is L_1 een lichaamsuitbreiding van K waarin elk niet-constant polynoom $f \in K[X]$ een nulpunt $X_f \bmod M$ heeft. Hieruit volgt nog niet dat L_1 algebraïsch afgesloten is, maar we kunnen bovenstaande constructie herhalen en zo inductief een keten $K \subset L_1 \subset L_2 \subset L_3 \subset \ldots$ van lichamen construeren met de eigenschap dat ieder niet-constant polynoom met coëfficiënten in L_k een nulpunt heeft in L_{k+1}. De vereniging $\Omega = \bigcup_{k \geq 1} L_k$ is dan weer een lichaam, en dit lichaam is wegens 21.10.2 *wel* algebraïsch afgesloten. Immers, ieder polynoom in $\Omega[X]$ heeft maar eindig veel coëfficiënten, en is dus bevat in $L_k[X]$ voor voldoend grote k. □

***Opgave 11.** Laat zien dat het lichaam L_1 in feite al een algebraïsche afsluiting van K is.

▶ Ontbindingslichamen

Uit 21.12 en 21.13 volgt dat elk lichaam K een algebraïsche afsluiting $\overline{K}$ bezit. Het bewijs van 21.13 geeft weinig informatie over Ω, en het hiermee gemaakte lichaam $\overline{K}$ is in de meeste gevallen dan ook niet 'expliciet op te schrijven'. We werken daarom meestal met deellichamen van $\overline{K}$ die van eindige graad zijn over K. Bij elk polynoom $f \in K[X] \setminus K$ hoort zo'n eindige uitbreiding, het *ontbindingslichaam* van f over K.

21.14. Definitie. *Zij K een lichaam en $f \in K[X]$ een niet-constant polynoom. Dan heet een algebraïsche uitbreiding L van K een ontbindingslichaam van f over K als het volgende geldt:*

1. *het polynoom f is een product van lineaire factoren in $L[X]$;*
2. *de nulpunten van f in L brengen L voort als lichaamsuitbreiding van K.*

Men kan een ontbindingslichaam van $f \in K[X]$ maken door f in $\overline{K}[X]$ te ontbinden als een product $f = c\prod_{i=1}^{n}(X - \alpha_i)$ en vervolgens het lichaam

$$\Omega_K^f = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \overline{K}$$

te nemen. Dit lichaam, dat van eindige graad is over K, voldoet duidelijk aan de eisen van 21.14. Het is echter niet direct duidelijk wat de graad van Ω_K^f over K is.

Het is niet strikt noodzakelijk eerst de algebraïsche afsluiting $\overline{K}$ te maken; men kan ook met behulp van 21.7 de nulpunten van f één voor één formeel adjungeren. Heeft

men ontbindingslichamen Ω_K^f voor alle niet-constante polynomen $f \in K[X]$, dan kan men in feite in omgekeerde richting hieruit een algebraïsche afsluiting $\overline{K}$ construeren als in opgave 45.

21.15. Voorbeelden. 1. Het polynoom $f = X^3 - 2$ is irreducibel in $\mathbf{Q}[X]$. Het heeft een reëel nulpunt $\sqrt[3]{2}$ en een paar complex geconjugeerde nulpunten $\zeta_3\sqrt[3]{2}$ en $\zeta_3^2\sqrt[3]{2}$. Hier is $\zeta_3 = e^{2\pi i/3} \in \mathbf{C}$ een primitieve derde eenheidswortel. Het deellichaam van $\mathbf{C}$ dat over $\mathbf{Q}$ door de nulpunten van f wordt voortgebracht is

$$\Omega_{\mathbf{Q}}^{X^3-2} = \mathbf{Q}(\sqrt[3]{2}, \zeta_3) \subset \mathbf{C}$$

Omdat het minimumpolynoom $\Phi_3 = X^2+X+1$ van ζ_3 geen nulpunten heeft in $\mathbf{Q}(\sqrt[3]{2})$ (of enig ander deellichaam van $\mathbf{R}$), heeft de uitbreiding $\mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ graad 2. We concluderen dat $\Omega_{\mathbf{Q}}^{X^3-2}$ van graad 6 is over $\mathbf{Q}$.

Vervangen we hierboven het grondlichaam $\mathbf{Q}$ door $\mathbf{R}$, dan is $f = X^3 - 2$ reducibel in $\mathbf{R}[X]$ en het ontbindingslichaam $\Omega_{\mathbf{R}}^{X^3-2} = \mathbf{R}(\zeta_3) = \mathbf{C}$ van f van graad 2 over $\mathbf{R}$.

2. Men kan $\Omega_{\mathbf{Q}}^{X^3-2}$ ook construeren zonder gebruik te maken van complexe getallen. Als in 21.7 maakt men eerst het kubische lichaam $\mathbf{Q}[X]/(X^3 - 2)$. Hierin is $\alpha = (X \bmod X^3 - 2)$ een nulpunt van $f = X^3 - 2$. Over $\mathbf{Q}(\alpha)$ ontbindt f als

$$X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^2) \in \mathbf{Q}(\alpha)[X].$$

Om in te zien dat het polynoom $g = X^2 + \alpha X + \alpha^2$ geen nulpunten heeft in $\mathbf{Q}(\alpha)$ en dus irreducibel is in $\mathbf{Q}(\alpha)[X]$ merken we op dat $\alpha^{-2}g(\alpha X) = X^2 + X + 1$ geldt. Als g een nulpunt heeft in $\mathbf{Q}(\alpha)$, dan heeft $X^2 + X + 1$ ook een nulpunt $\beta \in \mathbf{Q}(\alpha)$. Dit zou betekenen dat het kwadratische lichaam $\mathbf{Q}(\beta) = \mathbf{Q}[X]/(X^2+X+1)$ een deellichaam is van het kubische lichaam $\mathbf{Q}(\alpha)$, in tegenspraak met 21.3. We concluderen dat X^2+X+1 irreducibel is over $\mathbf{Q}(\alpha)$, en formele adjunctie van een nulpunt β van $X^2 + X + 1$ aan $\mathbf{Q}(\alpha)$ geeft een lichaam $\mathbf{Q}(\alpha, \beta)$ van graad 6 over $\mathbf{Q}$. In dit lichaam heeft $X^3 - 2$ de nulpunten α, $\alpha\beta$ en $\alpha\beta^2$, dus we kunnen $\Omega_{\mathbf{Q}}^{X^3-2} = \mathbf{Q}(\alpha, \beta)$ nemen. Merk op dat we op deze manier geen deellichaam van $\mathbf{C}$ krijgen.

3. Het p-de cyclotomische lichaam $\mathbf{Q}(\zeta_p)$ uit 21.8.3 is een ontbindingslichaam van het polynoom $X^p - 1$ over $\mathbf{Q}$. Immers, de p nulpunten van $X^p - 1$ in $\mathbf{Q}(\zeta_p)$ zijn precies de machten van ζ_p.

We zien aan het voorbeeld van $\Omega_{\mathbf{Q}}^{X^3-2}$ dat er weliswaar verschillende manieren kunnen zijn om een ontbindingslichaam te maken, maar dat het resultaat in zekere zin onafhankelijk is van de constructie. Immers, voor de in 21.15 geconstrueerde lichamen krijgt men een isomorfisme

$$\psi : \mathbf{Q}(\alpha, \beta) \xrightarrow{\sim} \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$$

van lichamen door voor $\psi(\alpha)$ een complex nulpunt van $X^3 - 2$ te nemen en voor $\psi(\beta)$ een nulpunt van X^2+X+1 in $\mathbf{C}$. Met drie keuzes voor $\psi(\alpha)$ en twee voor $\psi(\beta)$ hebben we 6 mogelijkheden voor het isomorfisme ψ, en er is geen 'natuurlijke keuze'. Voor ieder tweetal keuzes ψ_1 en ψ_2 is $\psi_2^{-1} \circ \psi_1$ een element van de groep $\mathrm{Aut}(\mathbf{Q}(\alpha, \beta))$ van lichaamsautomorfismen.

Opgave 12. Laat zien dat $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3))$ een groep van orde 6 is. Is het S_3 of C_6?

▶ Eenduidigheidsstellingen

Men noemt twee uitbreidingen L_1 en L_2 van K *isomorf over* K of K*-isomorf* als er een lichaamsisomorfisme $L_1 \to L_2$ bestaat dat op K de identiteit is. Men zegt ook wel dat L_1 en L_2 *geconjugeerd* zijn over K. Op soortgelijke wijze heten elementen α en β in een algebraïsche uitbreiding van K *geconjugeerd* over K als er een lichaamsisomorfisme $K(\alpha) \to K(\beta)$ bestaat dat op K de identiteit is en α op β afbeeldt.

Opgave 13. Bewijs: α en β in een algebraïsche afsluiting $\overline{K}$ van K zijn geconjugeerd over K dan en slechts dan als f_K^α en f_K^β gelijk zijn.

We zagen net voor $f = X^3 - 2$ en $K = \mathbf{Q}$ dat twee ontbindingslichamen Ω_K^f isomorf zijn over K. Dit geldt voor willekeurige K en $f \in K[X]$, en op soortgelijke wijze ligt een algebraïsche afsluiting $\overline{K}$ van K op K-isomorfie na vast.

21.16. Stelling. *Voor een lichaam K en een niet-constant polynoom $f \in K[X]$ geldt:*

1. *ieder tweetal ontbindingslichamen van f over K is K-isomorf;*
2. *ieder tweetal algebraïsche afsluitingen van K is K-isomorf.*

Merk op dat 21.16 slechts zegt dat er in beide situaties *een* K-isomorfisme bestaat. Dit isomorfisme is niet in het algemeen uniek. Het feit dat ieder tweetal isomorfismen een automorfisme van het ontbindingslichaam dan wel de algebraïsche afsluiting 'scheelt' is een fundamentele observatie die in §24 de basis van de Galoistheorie zal vormen. De kern van het bewijs van 21.16, die in het volgende lemma bevat is, zullen we dan ook nog diverse malen tegenkomen.

21.17. Lemma. *Zij $\varphi : K_1 \to K_2$ een isomorfisme van lichamen, $f_1 \in K_1[X]$ een niet-constant polynoom, en $f_2 \in K_2[X]$ het polynoom verkregen door φ op de coëfficiënten van f_1 toe te passen. Laat voor $i = 1, 2$ het lichaam L_i een ontbindingslichaam van f_i over K_i zijn. Dan bestaat er een isomorfisme $\psi : L_1 \to L_2$ met $\psi|_{K_1} = \varphi$.*

Bewijs. We voeren het bewijs met inductie naar de graad $d = [L_1 : K_1]$.

Voor $d = 1$ splitst f_1 in lineaire factoren in de polynoomring $K_1[X]$, zeg als $f_1 = c_1(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$. Omdat f_2 het beeld van f_1 is onder het ringisomorfisme $\widetilde{\varphi} : K_1[X] \xrightarrow{\sim} K_2[X]$ gegeven door $\sum_i a_i X^i \mapsto \sum_i \varphi(a_i)X^i$, volgt dat f_2 eveneens volledig splitst in $K_2[X]$, als $f_2 = \widetilde{\varphi}(f_1) = \varphi(c_1)(X-\varphi(\alpha_1))(X-\varphi(\alpha_2))\cdots(X-\varphi(\alpha_n))$. Er geldt dus $L_2 = K_2$, en we kunnen eenvoudig $\psi = \varphi$ nemen.

Neem nu $d > 1$, en laat $\alpha \in L_1 \setminus K_1$ een nulpunt zijn van f_1. Dan is het minimumpolynoom $h_1 = f_{K_1}^\alpha \in K_1[X]$ een irreducibele deler van f_1. Door het isomorfisme $\widetilde{\varphi}$ toe te passen zien we dat $h_2 = \widetilde{\varphi}(h_1)$ een irreducibele deler is van $f_2 = \widetilde{\varphi}(f_1)$. Omdat f_2 volledig splitst in L_2, geldt dit ook voor h_2. Zij β een nulpunt van h_2. Dan geldt $h_2 = f_{K_2}^\beta$, dus we hebben een samengesteld isomorfisme

$$\begin{array}{ccc} L_1 & \xrightarrow{\psi} & L_2 \\ | & & | \\ K_1(\alpha) & \xrightarrow{\chi} & K_2(\beta) \\ | & & | \\ K_1 & \xrightarrow{\phi} & K_2 \end{array}$$

$$\chi : K_1(\alpha) \xrightarrow{\sim} K_1[X]/(h_1) \xrightarrow{\sim} K_2[X]/(h_2) \xrightarrow{\sim} K_2(\beta).$$

De buitenste pijlen zijn de bekende isomorfismen uit 21.5.2, de middelste pijl is het natuurlijke isomorfisme geïnduceerd door $\widetilde{\varphi}$. Er geldt $\chi|_{K_1} = \widetilde{\varphi}|_{K_1} = \varphi$.

We merken nu op dat L_1 een ontbindingslichaam van f_1 is over $K_1(\alpha)$, en evenzo L_2 een ontbindingslichaam van f_2 over $K_2(\beta)$. Omdat we α buiten K_1 gekozen hebben, is de graad $[L_1 : K_1(\alpha)]$ strikt kleiner dan $[L_1 : K_1] = d$. De inductiehypothese vertelt ons nu dat $\chi : K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$ voortgezet kan worden tot een isomorfisme $\psi : L_1 \to L_2$, en dit bewijst het lemma. □

Bewijs van 21.16. Passen we 21.17 toe met $K_1 = K_2 = K$ en $\varphi = \mathrm{id}_K$, dan krijgen we de uitspraak in 21.16.1.

Laat nu $\overline{K}_1$ en $\overline{K}_2$ algebraïsche afsluitingen van K zijn. Om te bewijzen dat $\overline{K}_1$ en $\overline{K}_2$ isomorf zijn over K passen we het lemma van Zorn toe op de collectie $\mathcal{C}$ van tripels (M_1, μ, M_2). Hier zijn M_1 en M_2 deellichamen van respectievelijk $\overline{K}_1$ en $\overline{K}_2$ die K bevatten, en $\mu : M_1 \xrightarrow{\sim} M_2$ is een K-isomorfisme. We definiëren een partiële ordening op $\mathcal{C}$ door

$$(M_1, \mu, M_2) \leq (\widetilde{M}_1, \widetilde{\mu}, \widetilde{M}_2) \quad \Longleftrightarrow \quad M_1 \subset \widetilde{M}_1,\ M_2 \subset \widetilde{M}_2,\ \text{en } \widetilde{\mu}|_{M_1} = \mu.$$

Het element $(K, \mathrm{id}, K) \in \mathcal{C}$ is een bovengrens voor de lege keten in $\mathcal{C}$. Voor niet-lege ketens maakt men ook hier weer een bovengrens door verenigingen te nemen. Wegens 15.11 heeft $\mathcal{C}$ een maximaal element. We bewijzen dat zo'n element van de vorm $(\overline{K}_1, \mu, \overline{K}_2)$ is, en daarmee het gezochte K-isomorfisme levert.

Zij $(E_1, \phi, E_2) \in \mathcal{C}$ een maximaal element, en stel dat er een element α in $\overline{K}_1 \setminus E_1$ of in $\overline{K}_2 \setminus E_2$ bestaat. Dan is α algebraïsch over K, dus er bestaat een monisch polynoom $f \in K[X]$ met $f(\alpha) = 0$. Geef nu voor $i = 1, 2$ met $L_i \subset \overline{K}_i$ de uitbreiding van E_i aan voortgebracht door de nulpunten van f. Dan is L_i een ontbindingslichaam van f over E_i, en we kunnen 21.17 toepassen voor $\phi : E_1 \to E_2$ en $f_1 = f_2 = f$. Dit levert een tripel $(L_1, \mu, L_2) \in \mathcal{C}$ dat strikt groter is dan (E_1, ϕ, E_2): tegenspraak. □

Opgave 14. Laat $\overline{K}_1$ en $\overline{K}_2$ algebraïsche afsluitingen zijn van K_1 en K_2. Bewijs: ieder isomorfisme $K_1 \xrightarrow{\sim} K_2$ heeft een voortzetting tot een isomorfisme $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$.

Zoals al opgemerkt zijn de K-isomorfismen in 21.16 niet in het algemeen uniek. Men spreekt daarom van *een* ontbindingslichaam van f over K en van *een* algebraïsche afsluiting van K.

Opgaven.

15. Zij K een lichaam en $\psi : K \xrightarrow{\sim} K$ een automorfisme. Bewijs dat ψ de identiteit is op het priemlichaam van K.

16. Zij $\mathbf{C}(X)$ het lichaam van rationale functies met complexe coëfficiënten. Bewijs dat een $\mathbf{C}$-basis van $\mathbf{C}(X)$ gegeven wordt door

$$\{X^i\}_{i=0}^{\infty} \cup \{\frac{1}{(X-\alpha)^k} : \alpha \in \mathbf{C}, k \in \mathbf{Z}_{>0}\}.$$

[Deze *partieelbreuksplitsing* is nuttig bij het integreren van rationale functies.]

*17. Formuleer en maak het analogon van de vorige opgave voor het lichaam $K(X)$ van rationale functies met coëfficiënten in een willekeurig lichaam K.

18. Laat $K \subset L$ een algebraïsche uitbreiding zijn. Bewijs voor $\alpha, \beta \in L$:

$$[K(\alpha,\beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K].$$

Laat zien dat niet altijd gelijkheid optreedt. Is dit wel zo als $[K(\alpha) : K]$ en $[K(\beta) : K]$ onderling ondeelbaar zijn?

19. Zij $K \subset K(\alpha)$ een uitbreiding van oneven graad. Bewijs: $K(\alpha^2) = K(\alpha)$.

20. Bewijs: een algebraïsch afgesloten lichaam is van oneindige graad over zijn priemlichaam.

21. Laat zien dat er slechts aftelbaar veel algebraïsche getallen bestaan. Concludeer dat $\mathbf{C}$ niet algebraïsch is over $\mathbf{Q}$, en dat er overaftelbaar veel transcendente getallen bestaan.

22. Zij B een basis van $\mathbf{C}$ over $\mathbf{Q}$. Is B aftelbaar?

23. Laat zien dat iedere kwadratische uitbreiding van $\mathbf{Q}$ van de vorm $\mathbf{Q}(\sqrt{d})$ is met $d \in \mathbf{Z}$. Voor welke d krijgen we het cyclotomische lichaam $\mathbf{Q}(\zeta_3)$?

24. Is iedere kubische uitbreiding van $\mathbf{Q}$ van de vorm $K = \mathbf{Q}(\sqrt[3]{d})$ voor zekere $d \in \mathbf{Q}$?

25. Neem $M = \mathbf{Q}(i, \sqrt{2})$ en $\alpha = 1 + i + \sqrt{2}$. Bewijs: $G = \mathrm{Aut}(M)$ is isomorf met V_4, en $f = \prod_{\sigma \in G}(X - \sigma(\alpha))$ is het minimumpolynoom van α over $\mathbf{Q}$.
[Deze methode werkt heel algemeen: opgaven 24.13 en 24.14.]

26. Definieer $\sqrt{2}, \sqrt{3} \in \mathbf{R}$ op de gebruikelijke manier, en zij $M = \mathbf{Q}(\alpha) \subset \mathbf{R}$ met $\alpha = 1 + \sqrt{2} + \sqrt{3}$. Bewijs dat M van graad 4 is over $\mathbf{Q}$, bepaal $f_{\mathbf{Q}}^{\alpha}$, en schrijf $\sqrt{2}$ en $\sqrt{3}$ op de basis $\{1, \alpha, \alpha^2, \alpha^3\}$.

27. Laat zien dat $f = X^4 - 4X^3 - 4X^2 + 16X - 8$ irreducibel is in $\mathbf{Q}[X]$, en bepaal de graad van een ontbindingslichaam van f over $\mathbf{Q}$. [Hint: vorige opgave...]

28. Bewijs: $\mathbf{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbf{Q}(\sqrt{2} \cdot \sqrt[3]{3}) = \mathbf{Q}(\sqrt{2} + \sqrt[3]{3})$. Bepaal de minimumpolynomen van $\sqrt{2} \cdot \sqrt[3]{3}$ en $\sqrt{2} + \sqrt[3]{3}$ over $\mathbf{Q}$.

29. Zij $K = \mathbf{Q}(\alpha)$ met $f_{\mathbf{Q}}^{\alpha} = X^3 + 2X^2 + 1$.
    a. Bepaal de inverse van $\alpha + 1$ op de basis $\{1, \alpha, \alpha^2\}$ van K over $\mathbf{Q}$.
    b. Bepaal het minimumpolynoom van α^2 over $\mathbf{Q}$.

30. Definieer het cyclotomische lichaam $\mathbf{Q}(\zeta_5)$ als in 21.8.3, en schrijf $\alpha = \zeta_5^2 + \zeta_5^3$.
    a. Laat zien dat $\mathbf{Q}(\alpha)$ een kwadratische uitbreiding van $\mathbf{Q}$ is, en bepaal $f_{\mathbf{Q}}^{\alpha}$.
    b. Bewijs: $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{5})$.
    c. Bewijs: $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ en $\sin(2\pi/5) = \sqrt{\frac{5+\sqrt{5}}{8}}$.

31. Zij $\overline{K}$ een algebraïsche afsluiting van K en $L \subset \overline{K}$ een lichaam dat K bevat. Bewijs dat $\overline{K}$ een algebraïsche afsluiting van L is.

32. Zij $K \subset L$ een lichaamsuitbreiding en K_0 de algebraïsche afsluiting van K in L. Bewijs dat ieder element $\alpha \in L \setminus K_0$ transcendent is over K_0.

33. Geef een constructie van een ontbindingslichaam Ω_K^f uit 21.14 die alleen 21.7 gebruikt, en niet de existentie van een algebraïsche afsluiting $\overline{K}$ van K.

34. Zij K een lichaam en $\mathcal{F}$ een familie van polynomen in $K[X]$. Definieer een ontbindingslichaam $\Omega_K^{\mathcal{F}}$ van de familie $\mathcal{F}$ over K, en laat zien dat $\Omega_K^{\mathcal{F}}$ bestaat en op K-isomorfie na uniek is.

35. Zij $f \in K[X]$ een polynoom van graad $n \geq 1$. Bewijs: $[\Omega_K^f : K]$ deelt $n!$.

36. Zij $d \in \mathbf{Z}$ een getal dat geen derde macht is in $\mathbf{Z}$. Bewijs dat een ontbindingslichaam $\Omega_{\mathbf{Q}}^{X^3-d}$ graad 6 over $\mathbf{Q}$ heeft. Wat is de graad als d *wel* een derde macht is?

37. Bepaal de graad van een ontbindingslichaam van $X^4 - 2$ over $\mathbf{Q}$.

38. Zelfde vragen voor $X^4 - 4$ en $X^4 + 4$. Leg uit waarom de notaties $\mathbf{Q}(\sqrt[4]{4})$ en $\mathbf{Q}(\sqrt[4]{-4})$ niet gebruikt worden voor de lichamen verkregen door adjunctie van een nulpunt van respectievelijk $X^4 - 4$ en $X^4 + 4$ aan $\mathbf{Q}$.

39. Laat $K \subset L = K(\alpha)$ een enkelvoudige lichaamsuitbreiding van graad n zijn, en definieer $c_i \in L$ door
$$\sum_{i=0}^{n-1} c_i X^i = \frac{f_K^{\alpha}}{X - \alpha} \in L[X].$$
Bewijs: $\{c_0, c_1, \ldots, c_{n-1}\}$ is een K-basis voor L.

40. Zij $K \subset E \subset L = K(\alpha)$ een toren van lichaamsuitbreidingen, met α algebraïsch over K.
    a. Bewijs dat E als lichaamsuitbreiding van K wordt voortgebracht door de coëfficiënten van het polynoom $f_E^{\alpha} \in E[X]$.
    b. Bewijs dat E als K-vectorruimte wordt voortgebracht door de coëfficiënten van het polynoom $f_K^{\alpha}/f_E^{\alpha} \in E[X]$.
    [Hint: gebruik $f_K^{\alpha}/(X-\alpha) = (f_K^{\alpha}/f_E^{\alpha}) \cdot (f_E^{\alpha}/(X-\alpha))$ en de vorige opgave.]

41. Wat is de cardinaliteit[5] van een transcendentiebasis van $\mathbf{C}$ over $\mathbf{Q}$?

42. Zij $\overline{\mathbf{Q}}$ de algebraïsche afsluiting van $\mathbf{Q}$ in $\mathbf{C}$. Is $\mathbf{C}$ zuiver transcendent over $\overline{\mathbf{Q}}$?

*43. Laat zien dat $\mathbf{C}$ overaftelbaar veel automorfismen heeft, en dat de cardinaliteit van $\mathrm{Aut}(\mathbf{C})$ zelfs groter is dan die van $\mathbf{C}$.

44. Laat zien dat $\mathbf{C}$ precies twee *continue* automorfismen heeft.
[Hint: bewijs dat zo'n automorfisme de identiteit is op $\mathbf{R}$.]

45. Zij K een lichaam, en laat voor iedere $f \in \mathcal{F} = K[X]\backslash K$ een ontbindingslichaam Ω_K^f van f over K gegeven zijn.
    a. Zij R de ring $\prod_{f\in\mathcal{F}} \Omega_K^f$, met componentsgewijze ringoperaties, en schrijf voor $g \in \mathcal{F}$

$$I_g = \{(x_f)_{f\in\mathcal{F}} \in R : x_f = 0 \text{ als } g|f\}.$$

    Bewijs: $I = \bigcup_{g\in\mathcal{F}} I_g$ is een ideaal van R verschillend van R.
    b. Bewijs dat R een maximaal ideaal M heeft met $I \subset M$, dat R/M kan worden opgevat als uitbreidingslichaam van K, en dat de algebraïsche afsluiting van K in R/M (zoals gedefinieerd voor 21.9) een algebraïsche afsluiting van K is.

46. Bewijs dat, van elke twee lichamen van dezelfde karakteristiek, één van beide isomorf is met een deellichaam van een algebraïsche afsluiting van de ander.

47. Laten $K \subset L$ en $K \subset M$ twee lichaamsuitbreidingen zijn. Bewijs dat er een lichaamsuitbreiding $K \subset N$ is zodanig dat L en M allebei K-isomorf met een deellichaam van N zijn.

22 Eindige lichamen

In deze paragraaf passen we de theorie van de lichaamsuitbreidingen toe in het geval van *eindige* lichamen. Omdat het priemlichaam van een eindig lichaam niet het oneindige lichaam $\mathbf{Q}$ kan zijn, is voor ieder eindig lichaam $\mathbf{F}$ het priemlichaam een lichaam $\mathbf{F}_p$ van p elementen, met $p = \mathrm{char}(\mathbf{F}) > 0$ de karakteristiek van $\mathbf{F}$. Eindige lichamen zijn daarom niets anders dan eindige uitbreidingen van de priemlichamen $\mathbf{F}_p$.

Omdat voor een priemgetal p alle binomiaalcoëfficiënten $\binom{p}{i}$ met $0 < i < p$ deelbaar zijn door p leidt het binomium van Newton in lichamen (of commutatieve ringen) van karakteristiek p tot de veel gebruikte identiteit $(x+y)^p = x^p + y^p$: de p-de machtsverheffing is *additief* in karakteristiek p.

▶ Het lichaam $\mathbf{F}_{p^n}$

Anders dan in het geval van het priemlichaam $\mathbf{Q}$ kan men de eindige uitbreidingen van $\mathbf{F}_p$ eenvoudig classificeren: op isomorfie na is er voor elke $n \in \mathbf{Z}_{\geq 1}$ precies één uitbreiding $\mathbf{F}_p \subset \mathbf{F}_{p^n}$ van graad n.

22.1. Stelling. *Zij $\mathbf{F}$ een eindig lichaam, en $\mathbf{F}_p$ het priemlichaam van $\mathbf{F}$. Dan is $\mathbf{F}$ een uitbreiding van eindige graad n van $\mathbf{F}_p$, en $\mathbf{F}$ heeft p^n elementen.*

Omgekeerd bestaat er voor iedere priemmacht $q = p^n > 1$ een op isomorfie na uniek lichaam $\mathbf{F}_q$ met q elementen; het is een ontbindingslichaam van $X^q - X$ over $\mathbf{F}_p$.

Bewijs. Als $\mathbf{F}$ eindig is, dan is $\mathbf{F}$ van eindige graad over zijn priemlichaam $\mathbf{F}_p$. Is deze graad gelijk aan n, dan heeft $\mathbf{F}$ als n-dimensionale vectorruimte over $\mathbf{F}_p$ precies p^n elementen. De eenhedengroep $\mathbf{F}^*$ heeft dan orde $p^n - 1$, en hieruit volgt dat de elementen van $\mathbf{F}^*$ precies de $p^n - 1$ nulpunten zijn van het polynoom $X^{p^n-1} - 1 \in \mathbf{F}[X]$. In het bijzonder hebben we

$$\textstyle\prod_{\alpha \in \mathbf{F}} (X - \alpha) = X^{p^n} - X \in \mathbf{F}_p[X].$$

We zien hieruit dat $\mathbf{F}$ een ontbindingslichaam van $X^{p^n} - X$ is over $\mathbf{F}_p$, en uit 21.16 volgt dat er op isomorfie na ten hoogste één lichaam met p^n elementen kan bestaan.

We bewijzen nu dat omgekeerd voor iedere priemmacht $q = p^n > 1$ een ontbindingslichaam van $X^q - X \in \mathbf{F}_p[X]$ over $\mathbf{F}_p$ een lichaam van q elementen is. Omdat de afgeleide $f' = -1$ van $f = X^q - X$ geen nulpunten heeft, heeft f geen dubbele nulpunten in een algebraïsche afsluiting $\overline{\mathbf{F}}_p$ van $\mathbf{F}_p$. De nulpuntsverzameling

$$\mathbf{F}_q = \{\alpha \in \overline{\mathbf{F}}_p : \alpha^{p^n} = \alpha\} \subset \overline{\mathbf{F}}_p \tag{22.2}$$

van f heeft daarom $q = p^n$ elementen. Wegens de kleine stelling van Fermat hebben we $\mathbf{F}_p \subset \mathbf{F}_q$. Het is duidelijk dat $\mathbf{F}_q$ gesloten is onder vermenigvuldiging en deling door niet-nul elementen. De additiviteit van de p-de machtsverheffing impliceert

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

dus $\mathbf{F}_q$ is ook een additieve ondergroep van $\overline{\mathbf{F}}_p$. Er volgt dat $\mathbf{F}_q$ een deellichaam is van $\overline{\mathbf{F}}_p$, en dus een ontbindingslichaam van f over $\mathbf{F}_p$. □

Wellicht ten overvloede wijzen we er op dat het lichaam $\mathbf{F}_q = \mathbf{F}_{p^n}$ in 22.2 voor $n > 1$ *niet* gelijk is aan de ring $\mathbf{Z}/q\mathbf{Z}$.

▶ Frobeniusautomorfisme

Het bewijs van 22.1 berust erop dat de *Frobeniusafbeelding*

$$\begin{aligned} F: \quad \overline{\mathbf{F}}_p &\longrightarrow \overline{\mathbf{F}}_p \\ x &\longmapsto x^p \end{aligned}$$

een *automorfisme* van de algebraïsche afsluiting $\overline{\mathbf{F}}_p$ van $\mathbf{F}_p$ is. De fundamentele eigenschap $F(x+y) = F(x) + F(y)$ is een eigenaardigheid in lichamen van karakteristiek p die geen equivalent heeft voor lichamen van karakteristiek 0. De injectiviteit van F betekent dat elementen in $\overline{\mathbf{F}}_p$ een *unieke* p-de machts wortel bezitten. Uit $\beta^p = \alpha \in \overline{\mathbf{F}}_p$ volgt inderdaad

$$(X - \beta)^p = X^p - \beta^p = X^p - \alpha,$$

en dit laat zien dat β de enige p-de machts wortel van α is. We komen in 23.6 nader op deze *inseparabiliteitseigenschap* terug.

Door herhaald toepassen van het Frobeniusautomorfisme op $\overline{\mathbf{F}}_p$ krijgen we automorfismen $F^n : x \mapsto x^{p^n}$. Herschrijven we 22.2 in termen van F als

$$\mathbf{F}_{p^n} = \{\alpha \in \overline{\mathbf{F}}_p : \quad F^n(\alpha) = \alpha \}, \tag{22.3}$$

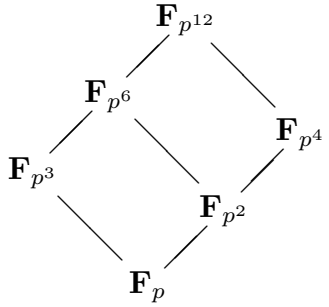
dan zien we dat $\overline{\mathbf{F}}_p$ voor iedere $n \geq 1$ precies één deellichaam van p^n elementen bevat. Hieruit kan men de complete structuur van de collectie van deellichamen van $\overline{\mathbf{F}}_p$ en hun inclusierelaties aflezen.

22.4. Stelling. *Laat $\mathbf{F}_q$ en $\mathbf{F}_r$ deellichamen van $\overline{\mathbf{F}}_p$ zijn van orde respectievelijk $q = p^i$ en $r = p^j$. Dan zijn equivalent:*

1. *$\mathbf{F}_q$ is een deellichaam van $\mathbf{F}_r$;*
2. *r is een macht van q;*
3. *i is een deler van j.*

Bewijs. Als $\mathbf{F}_r$ een uitbreidingslichaam van graad d van $\mathbf{F}_q$ is, dan geldt $r = q^d$, en dus $j = di$. Dit bewijst $1 \Rightarrow 2 \Rightarrow 3$. Is ten slotte i een deler van j, dan geldt voor $\alpha \in \overline{\mathbf{F}}_p$ de implicatie $F^i(\alpha) = \alpha \Rightarrow F^j(\alpha) = \alpha$. Dit is echter equivalent met de inclusierelatie $\mathbf{F}_q = \mathbf{F}_{p^i} \subset \mathbf{F}_{p^j} = \mathbf{F}_r$. □

Uit 22.4 zien we dat de inclusierelatie van eindige deellichamen van $\overline{\mathbf{F}}_p$ overeenkomt met de deelbaarheidsrelatie van hun graden over $\mathbf{F}_p$. Voor $n = 12$ krijgen we het volgende *rooster* van deellichamen van $\mathbf{F}_{p^{12}}$.



Een verbindingslijn tussen lichamen in zo'n rooster, dat naar de Duitser Helmut Hasse (1898–1979) ook wel een *Hasse-diagram* genoemd wordt, dient opgevat te worden als een inclusie in de stijgrichting van de lijn. In ons plaatje geven de korte verbindingslijnen kwadratische uitbreidingen aan, de lange kubische.

► Irreducibele polynomen over $\mathbf{F}_p$.

De beschrijving van $\mathbf{F}_q$ die we tot dusver gegeven hebben is karakteristiek voor de *Galoistheorie*: het is het deellichaam van $\overline{\mathbf{F}}_p$ bestaande uit de elementen die invariant zijn onder een zekere macht van het Frobeniusautomorfisme. Om in eindige lichamen te kunnen rekenen is een beschrijving nodig van $\mathbf{F}_q$ als een uitbreiding van $\mathbf{F}_p$ verkregen door formele adjunctie van een nulpunt van een expliciet polynoom $f \in \mathbf{F}_p[X]$.

22.5. Stelling. *De eenhedengroep $\mathbf{F}_q^*$ van $\mathbf{F}_q$ is een cyclische groep van orde $q-1$. Voor iedere voortbrenger $\alpha \in \mathbf{F}_q^*$ geldt $\mathbf{F}_q = \mathbf{F}_p(\alpha) \cong \mathbf{F}_p[X]/(f^\alpha_{\mathbf{F}_p})$.*

Bewijs. De eenhedengroep $\mathbf{F}_q^*$ is cyclisch wegens 12.5. Hebben we $\mathbf{F}_q^* = \langle\alpha\rangle$, dan geldt $\mathbf{F}_q \subset \mathbf{F}_p(\alpha)$, en dus $\mathbf{F}_q = \mathbf{F}_p(\alpha)$. De isomorfie $\mathbf{F}_p(\alpha) \cong \mathbf{F}_p[X]/(f^\alpha_{\mathbf{F}_p})$ is een speciaal geval van 21.5.2. □

22.6. Gevolg. *Zij p een priemgetal en $n \geq 1$ een geheel getal. Dan bestaat er een irreducibel polynoom van graad n in $\mathbf{F}_p[X]$.*

Bewijs. Schrijf $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$ en neem $f = f^\alpha_{\mathbf{F}_p}$. □

Opgave 1. Is ieder element $\alpha \in \mathbf{F}_q^*$ met $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ noodzakelijk een voortbrenger van $\mathbf{F}_q^*$?

Het 'expliciet construeren' van een lichaam van orde $q = p^n$ komt neer op het vinden van een irreducibel polynoom van graad n in $\mathbf{F}_p[X]$. Voor kleine waarden van n en p kan men met enig proberen wel zo'n polynoom maken. Voor $n = p = 2$ is $X^2 + X + 1$ de enige mogelijkheid, en dit geeft

$$\mathbf{F}_4 \cong \mathbf{F}_2[X]/(X^2 + X + 1).$$

Hiermee krijgen we $\mathbf{F}_4$ als een expliciete $\mathbf{F}_2$-vectorruimte $\mathbf{F}_4 = \mathbf{F}_2 \cdot 1 \oplus \mathbf{F}_2 \cdot \alpha$ met een vermenigvuldiging gebaseerd op de rekenregel $\alpha^2 = \alpha + 1$. De groep $\mathbf{F}_4^*$ heeft orde 3 en wordt voortgebracht door α of door $\alpha^{-1} = \alpha + 1$.

Opgave 2. Maak een complete vermenigvuldigtafel voor $\mathbf{F}_4$.

In de meeste gevallen is er veel keus voor een irreducibel polynoom van graad n in $\mathbf{F}_p[X]$. Omdat 2 en 3 geen kwadraten zijn in $\mathbf{F}_5$ heeft men bijvoorbeeld

$$\mathbf{F}_{25} \cong \mathbf{F}_5(\sqrt{2}) = \mathbf{F}_5[X]/(X^2 - 2) \qquad \text{en} \qquad \mathbf{F}_{25} \cong \mathbf{F}_5(\sqrt{3}) = \mathbf{F}_5[X]/(X^2 - 3).$$

In het bijzonder is er een isomorfisme $\mathbf{F}_5(\sqrt{2}) \xrightarrow{\sim} \mathbf{F}_5(\sqrt{3})$. Wegens $(2\sqrt{3})^2 = 2 \in \mathbf{F}_5$ is een expliciete keuze voor dit isomorfisme de afbeelding $a + b\sqrt{2} \mapsto a + 2b\sqrt{3}$.

Opgave 3. Laat zien dat er *geen* lichaamsisomorfisme $\mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{3})$ bestaat.

Omdat de elementen van $\mathbf{F}_{p^n}$ wegens 22.2 nulpunten van $X^{p^n} - X$ zijn, kan men de irreducibele polynomen van graad n in principe vinden door dit polynoom in irreducibele factoren te ontbinden.

22.7. Stelling. *Voor p een priemgetal en $n \geq 1$ geldt in $\mathbf{F}_p[X]$ de relatie*

$$X^{p^n} - X = \prod_{\substack{f \text{ monisch irreducibel} \\ \deg(f)|n}} f.$$

In het bijzonder voldoet het aantal x_d van monische irreducibele polynomen van graad d in $\mathbf{F}_p[X]$ aan de identiteit $\sum_{d|n} d \cdot x_d = p^n$.

Bewijs. Zij $f \in \mathbf{F}_p[X]$ een monisch irreducibel polynoom van graad d. Een nulpunt α van f in $\overline{\mathbf{F}}_p$ brengt dan een uitbreiding $\mathbf{F}_p(\alpha)$ van graad d voort. Wegens 22.4 geldt $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^n}$ dan en slechts dan als d een deler is van n. Wegens 22.2 geldt $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^n}$ dan en slechts dan als α een nulpunt is van $X^{p^n} - X$, en dit laatste betekent niets anders dan dat het minimumpolynoom f van α een deler is van $X^{p^n} - X$. We concluderen dat f een deler is van $X^{p^n} - X$ dan en slechts dan als $\deg(f)$ een deler is van n. Omdat $X^{p^n} - X$ geen meervoudige nulpunten heeft, krijgen we hieruit de verlangde ontbinding in $\mathbf{F}_p[X]$. Vergelijking van de graden geeft $\sum_{d|n} d \cdot x_d = p^n$. □

Door 22.7 achtereenvolgens toe te passen voor $n = 1, 2, 3, \ldots$ kunnen we inductief de waarden van x_n berekenen. Voor $n = 1$ vinden we niet verrassend dat er $x_1 = p$ monische lineaire polynomen in $\mathbf{F}_p[X]$ zijn. Is n een priemgetal, dan leidt de relatie $x_1 + nx_n = p^n$ tot $x_n = (p^n - p)/n$. Wegens de kleine stelling van Fermat – modulo de priem n, niet p – is dit inderdaad een geheel getal. Voor $n = 2$ of $n = 3$ is deze formule direct na te gaan (opgave 24).

Een algemene formule voor x_n in termen van p kan verkregen worden uit 22.7 door *Möbius-inversie*. Het betreft hier een algemene methode om, gegeven twee functies $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ die gerelateerd zijn door de formule $\sum_{d|n} f(d) = g(n)$, de waarden van f uit te drukken in die van g. Men definieert hiertoe de naar de Duitser August Ferdinand Möbius (1790–1868) genoemde *Möbius-functie* $\mu : \mathbf{Z}_{>0} \to \mathbf{Z}$ door

$$\mu(n) = \begin{cases} 0 & \text{als er een priemgetal } p \text{ is met } p^2|n; \\ (-1)^t & \text{als } n \text{ het product van } t \text{ verschillende priemgetallen is.} \end{cases}$$

We hebben $\mu(1) = 1$, immers 1 is het product van $t = 0$ priemgetallen. De Möbius-functie is eenduidig bepaald door zijn waarde in 1 en de fundamentele eigenschap

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{als } n = 1; \\ 0 & \text{als } n > 1. \end{cases} \tag{22.8}$$

We verwijzen naar opgave 26 voor de details.

22.9. Möbius-inversieformule. *Laat $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ voor alle $n \in \mathbf{Z}_{>0}$ voldoen aan*

$$\textstyle\sum_{d|n} f(d) = g(n).$$

Dan geldt voor alle $n \in \mathbf{Z}_{>0}$ de omkeerformule

$$f(n) = \textstyle\sum_{d|n} \mu(d) g(n/d).$$

Bewijs. Druk g in de tweede formule in f uit en gebruik de fundamentele eigenschap 22.8 van μ:

$$\sum_{d|n} \mu(d)g(n/d) = \sum_{d|n} \sum_{k|\frac{n}{d}} \mu(d)f(k) = \sum_{k|n} \big(\sum_{d|\frac{n}{k}} \mu(d)\big) f(k) = f(n). \qquad \square$$

Passen we 22.9 toe met $f : n \mapsto nx_n$ en $g : n \mapsto p^n$, dan vinden we uit 22.7 de relatie

$$x_n = \tfrac{1}{n} \textstyle\sum_{d|n} \mu(d) p^{n/d}.$$

Men kan hieruit afleiden (opgave 21) dat een willekeurig monisch polynoom van graad n in $\mathbf{F}_p[X]$ voor grote n of p irreducibel is met kans ongeveer $\frac{1}{n}$.

▶ Automorfismen van $\mathbf{F}_q$

We merkten al op dat het Frobeniusautomorfisme $F : x \mapsto x^p$ een centrale rol speelt in de theorie van de eindige lichamen. In essentie zijn er geen andere automorfismen van eindige lichamen.

22.10. Stelling. *Zij $\mathbf{F}_q$ de uitbreiding van graad n van $\mathbf{F}_p$. Dan is $\mathrm{Aut}(\mathbf{F}_q)$ een cyclische groep van orde n voortgebracht door het Frobeniusautomorfisme $F : x \mapsto x^p$.*

Bewijs. We weten al dat F een automorfisme van $\mathbf{F}_q$ is, en we gaan bewijzen dat F orde n heeft in $\mathrm{Aut}(\mathbf{F}_q)$. Wegens 22.3 is F^n de identiteit op $\mathbf{F}_q = \mathbf{F}_{p^n}$, dus de orde van F deelt n. Voor ieder getal $d < n$ is F^d niet de identiteit op $\mathbf{F}_{p^n}$, want het polynoom $X^{p^d} - X$ heeft niet meer dan p^d nulpunten in $\mathbf{F}_{p^n}$.

Om te bewijzen dat de cyclische groep $\langle F \rangle$ van orde n de hele groep $\mathrm{Aut}(\mathbf{F}_q)$ is, laten we zien dat er niet meer dan n automorfismen van $\mathbf{F}_q$ kunnen bestaan. Schrijf hiertoe $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ als in 22.5, en laat $f = \sum_{i=0}^{n} a_i X^i$ het minimumpolynoom van α zijn. Ieder automorfisme $\sigma : \mathbf{F}_p(\alpha) \to \mathbf{F}_p(\alpha)$ is de identiteit op het priemlichaam $\mathbf{F}_p$, dus het ligt vast door de waarde $\sigma(\alpha)$. Omdat f coëfficiënten in $\mathbf{F}_p$ heeft geldt

$$\begin{aligned} f(\sigma(\alpha)) &= \textstyle\sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i \alpha^i) = \sigma(\sum_{i=0}^{n} a_i \alpha^i) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

We zien hieruit dat $\sigma(\alpha)$ een nulpunt van f is, en omdat f niet meer dan $\deg(f) = n$ nulpunten in $\mathbf{F}_q$ heeft zijn er ten hoogste n mogelijkheden voor σ. $\square$

Uit het bewijs van 22.10 zien we dat de nulpunten van het minimumpolynoom over $\mathbf{F}_p$ van een element $\alpha \in \overline{\mathbf{F}}_p$ precies de elementen $\sigma(\alpha)$ zijn, waarbij σ over de elementen van de automorfismengroep $\mathrm{Aut}(\mathbf{F}_p(\alpha))$ loopt. Omdat $\mathrm{Aut}(\mathbf{F}_p(\alpha))$ uit de machten van het Frobeniusautomorfisme bestaat, geeft dit het volgende resultaat.

22.11. Gevolg. *Zij $f \in \mathbf{F}_p[X]$ een monisch irreducibel polynoom van graad d. Dan geldt voor ieder nulpunt α van f in $\overline{\mathbf{F}}_p$ de gelijkheid*

$$f = \prod_{i=0}^{d-1} (X - \alpha^{p^i}) \in \overline{\mathbf{F}}_p[X]. \qquad \square$$

Opgave 4. Formuleer en bewijs het analogon van 22.11 voor een irreducibel polynoom $f \in \mathbf{F}_q[X]$.

Voor een willekeurige uitbreiding $K \subset L$ van eindige lichamen kunnen we binnen de automorfismengroep $\mathrm{Aut}(L)$ die 22.10 ons geeft gemakkelijk de ondergroep

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \sigma|_K = \mathrm{id}_K\}$$

van automorfismen van L *over* K bepalen. Schrijven we $K = \mathbf{F}_q$ met $q = p^m$ en $L = \mathbf{F}_{q^n} = \mathbf{F}_{p^{mn}}$, dan is $\mathrm{Aut}_K(L)$ de ondergroep van $\mathrm{Aut}(L) = \langle F \rangle$ voortgebracht door $F_K = F^m$, het Frobeniusautomorfisme $F_K : x \mapsto x^{\#K}$ behorende bij K.

Opgave 5. Laat zien dat F^k de identiteit is op $\mathbf{F}_{p^m}$ dan en slechts dan als k een veelvoud is van m.

De groep $\mathrm{Aut}_K(L)$ is kennelijk een cyclische groep van orde n. Voor iedere deler d van n is er een ondergroep $H \subset \mathrm{Aut}_K(L)$ van index d en orde n/d voortgebracht door $F_K^d = F^{dm}$. Bij deze ondergroep hoort een *invariantenlichaam*

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

dat gelijk is aan $\mathbf{F}_{q^d} = \mathbf{F}_{p^{md}}$. Vergelijken we dit met de uitspraak in 22.4, dan zien we dat we de volgende *Galoiscorrespondentie* hebben tussen ondergroepen van $\mathrm{Aut}_K(L)$ en *tussenlichamen* E van $K \subset L$.

22.12. Galoistheorie voor eindige lichamen. *Zij $K \subset L$ een uitbreiding van eindige lichamen van graad n. Dan is $\mathrm{Aut}_K(L)$ een cyclische groep van orde n voortgebracht door het Frobeniusautomorfisme $F_K : x \mapsto x^{\#K}$, en er is een bijectie*

$$\begin{aligned} \{E : K \subset E \subset L\} &\longrightarrow \{H : H \subset \mathrm{Aut}_K(L)\} \\ E &\longmapsto \mathrm{Aut}_E(L) \end{aligned}$$

tussen de verzameling van tussenlichamen E van $K \subset L$ en de verzameling van ondergroepen H van $\mathrm{Aut}_K(L)$. Onder deze bijectie correspondeert $H \subset \mathrm{Aut}_K(L)$ met het invariantenlichaam $L^H = \{x \in L : \sigma(x) = x$ voor alle $\sigma \in H\}$. □

In 24.4 zullen we deze stelling, die de *hoofdstelling van de Galoistheorie* is voor $K \subset L$, generaliseren tot het geval van een *willekeurig* grondlichaam K. Voor eindige K is de situatie relatief eenvoudig: iedere eindige uitbreiding $K \subset L$ is *enkelvoudig*, van de vorm $L = K(\alpha)$, en wegens 22.11 liggen met $\alpha \in L$ ook alle andere nulpunten van f_K^α in L. Er zijn precies $[L : K]$ verschillende nulpunten, en de voortbrenger F_K van $\mathrm{Aut}_K(L)$ permuteert deze cyclisch.

Voor oneindige K is er geen Frobeniusautomorfisme, en er doen zich nog diverse andere problemen voor. Het is bijvoorbeeld niet duidelijk of alle eindige uitbreidingen van K van de vorm $K(\alpha)$ zijn, of f_K^α altijd $\deg(f_K^\alpha)$ verschillende nulpunten heeft in $\overline{K}$, en of deze nulpunten noodzakelijk in $K(\alpha)$ bevat zijn. Deze problemen worden in de volgende paragraaf behandeld. Alleen voor eindige uitbreidingen $K \subset L$ die in de daar geïntroduceerde terminologie *separabel* en *normaal* zijn is er een analogon van 22.12.

Opgaven.

6. Geef een expliciet isomorfisme $\mathbf{F}_5[X]/(X^2+X+1) \xrightarrow{\sim} \mathbf{F}_5(\sqrt{2})$.

7. Laat zien dat $f = X^2+2X+2$ en $g = X^2+X+3$ irreducibel zijn in $\mathbf{F}_7[X]$, en geef een expliciet isomorfisme $\mathbf{F}_7[X]/(f) \xrightarrow{\sim} \mathbf{F}_7[X]/(g)$.

8. Bereken de orde van $1-\sqrt{2}$, $2-\sqrt{2}$ en $3-\sqrt{2}$ in $\mathbf{F}_5(\sqrt{2})^*$.

9. Zij $\alpha \in \overline{\mathbf{F}}_7$ een nulpunt van $X^3-2 \in \mathbf{F}_7[X]$. Bewijs dat $\mathbf{F} = \mathbf{F}_7(\alpha)$ een lichaam van 343 elementen is, en dat X^3-2 in $\mathbf{F}[X]$ ontbindt als $X^3-2 = (X-\alpha)(X-2\alpha)(X-4\alpha)$. Wat zijn de graden van de irreducibele factoren van $X^{19}-1$ in $\mathbf{F}[X]$ en in $\mathbf{F}_7[X]$?

10. Bepaal de graden van de irreducibele factoren van $X^{13}-1$ in $\mathbf{F}_5[X]$, in $\mathbf{F}_{25}[X]$ en in $\mathbf{F}_{125}[X]$.

11. Zij p een priemgetal. Laat zien dat $\mathbf{F}_p[X]/(X^2+X+1)$ een lichaam is dan en slechts dan als p congruent is met 2 mod 3.

12. Zij q een macht van een priemgetal.
    a. Voor welke q is de kwadratische uitbreiding $\mathbf{F}_{q^2}$ van $\mathbf{F}_q$ van de vorm $\mathbf{F}_q(\sqrt{x})$ met $x \in \mathbf{F}_q$?
    b. Voor welke q is de kubische uitbreiding $\mathbf{F}_{q^3}$ van $\mathbf{F}_q$ van de vorm $\mathbf{F}_q(\sqrt[3]{x})$ met $x \in \mathbf{F}_q$?

13. Zij p een oneven priemgetal.
    a. Laat zien dat $\mathbf{F}_{p^2}$ een primitieve achtste eenheidswortel ζ bevat, en dat $\alpha = \zeta + \zeta^{-1}$ voldoet aan $\alpha^2 = 2$.
    b. Bewijs: $\alpha \in \mathbf{F}_p \Leftrightarrow p \equiv \pm 1 \bmod 8$. Concludeer dat 2 een kwadraat is modulo p dan en slechts dan als $p \equiv \pm 1 \bmod 8$ geldt.

14. Bepaal voor welke priemen p het polynoom $X^2+2 \in \mathbf{F}_p[X]$ reducibel is. [Dit is het sterretje van opgave 12.49.]

15. Bepaal alle priemgetallen p waarvoor $\mathbf{F}_p[X]/(X^4+1)$ een lichaam is.

16. Bewijs: $f = X^3+2$ is irreducibel in $\mathbf{F}_{49}[X]$. Is f irreducibel over $\mathbf{F}_{7^n}$ voor alle even n?

17. Bewijs: $f = X^4+2$ is irreducibel in $\mathbf{F}_{125}[X]$. Is f irreducibel over $\mathbf{F}_{5^n}$ voor alle oneven n?

18. Zij $i \in \overline{\mathbf{F}}_3$ een nulpunt van X^2+1. Bewijs dat $\mathbf{F} = \mathbf{F}_3(i)$ een lichaam van 9 elementen is, en bepaal $f^{\alpha}_{\mathbf{F}_3}$ voor alle $\alpha \in \mathbf{F}$. Ontbind X^9-X in irreducibele factoren in $\mathbf{F}_3[X]$.

19. Zij $\mathbf{F} = \mathbf{F}_{32}$ het lichaam van 32 elementen.
    a. Bewijs: voor alle $x \in \mathbf{F} \setminus \mathbf{F}_2$ geldt $\mathbf{F}^* = \langle x \rangle$.
    b. Voor hoeveel polynomen $f \in \mathbf{F}_2[X]$ geldt $\mathbf{F}_2[X]/(f) \cong \mathbf{F}$?

20. Formuleer en bewijs het analogon van 22.7 voor monische irreducibele polynomen in $\mathbf{F}_q[X]$, met $q = p^k$ een priemmacht.

21. Laat zien dat het aantal x_n van monische irreducibele polynomen van graad n in $\mathbf{F}_p[X]$ voldoet aan de ongelijkheden

$$p^n - \frac{p}{p-1}p^{n/2} < nx_n \leq p^n.$$

Zij $\delta_p(n)$ de kans dat een willekeurig gekozen monisch polynoom van graad n in $\mathbf{F}_p[X]$ irreducibel is. Bewijs: $\lim_{n\to\infty} \delta_p(n)/\frac{1}{n} = 1$ en $\lim_{p\to\infty} \delta_p(n) = \frac{1}{n}$.

22. Formuleer en bewijs het analogon van de vorige opgave voor $\mathbf{F}_q[X]$, met $q = p^k$ een priemmacht.

23. Laat zien dat de fractie $\delta_p(n)$ van monische polynomen van graad n die irreducibel zijn in $\mathbf{F}_p[X]$ voldoet aan $\delta_p(n) \geq \frac{1}{2n}$.

24. Laat zien dat er $(p^2+p)/2$ monische polynomen van graad 2 in $\mathbf{F}_p[X]$ bestaan die *reducibel* zijn. Concludeer: $x_2 = (p^2-p)/2$. Bepaal x_3 eveneens zonder stelling 22.7 te gebruiken.

*25. Voor $n \in \mathbf{Z}_{\geq 1}$ geven we met $\Sigma_T(n)$ de verzameling van monische polynomen van graad n in $\mathbf{Z}[X]$ aan waarvan alle coëfficiënten in absolute waarde begrensd zijn door $T \in \mathbf{R}_{>0}$, en met $\Sigma_T^{\mathrm{irr}}(n) \subset \Sigma_T(n)$ de deelverzameling van irreducibele polynomen.
Bewijs de volgende uitspraken.
   a. Is $T = p_1 p_2 \dots p_k$ het product van k verschillende priemgetallen, dan zijn van de T^n monische polynomen van graad n met coëfficiënten in $\{0, 1, \dots T-1\} \subset \mathbf{Z}$ ten hoogste $(1-\frac{1}{2n})^k T^n$ reducibel in $\mathbf{Z}[X]$.
   b. Voor alle $n \in \mathbf{Z}_{\geq 1}$ geldt
$$\lim_{T\to\infty} \frac{\#\Sigma_T^{\mathrm{irr}}(n)}{\#\Sigma_T(n)} = 1.$$

[Dit laat zien dat een 'random' monisch polynoom in $\mathbf{Z}[X]$ met 'kans 1' irreducibel is.]

26. De ring $\mathcal{R}$ van *aritmetische functies* is de verzameling van functies $f : \mathbf{Z}_{\geq 1} \to \mathbf{C}$ voorzien van de puntsgewijze optelling en het zogenaamde *convolutieproduct*:
$$(f_1 + f_2)(n) = f_1(n) + f_2(n)$$
$$(f_1 \star f_2)(n) = \textstyle\sum_{d|n} f_1(d) f_2(n/d).$$

De deelverzameling $\mathcal{M} \subset \mathcal{R}$ van *multiplicatieve* aritmetische functies bestaat uit de $f \in \mathcal{R} \setminus \{0\}$ die voldoen aan $f(mn) = f(m)f(n)$ voor alle onderling ondeelbare $m, n \in \mathbf{Z}_{\geq 1}$.
   a. Laat zien dat $\mathcal{R}$ een domein is met als eenheidselement e de karakteristieke functie van $\{1\}$ gegeven door $e(1) = 1$ en $e(n) = 0$ voor $n > 1$.
   b. Bewijs: $\mathcal{R}^* = \{f : f(1) \neq 0\}$, en $\mathcal{M}$ is een ondergroep van $\mathcal{R}^*$.
   c. Laat zien dat een element $f \in \mathcal{M}$ vastligt door zijn waarden op de priemmachten in $\mathbf{Z}_{>1}$. Kunnen deze waardes onafhankelijk worden gekozen?
   d. Zij E de aritmetische functie die constant gelijk is aan 1, en μ de inverse van E in $\mathcal{R}$. Bewijs dat de functie μ voldoet aan de identiteit 22.8 en gelijk is aan de Möbius-functie.

27. Laat $f, g : \mathbf{Z}_{>0} \to \mathbf{C}$ voor alle $n \in \mathbf{Z}_{>0}$ voldoen aan de omkeerformule
$$f(n) = \textstyle\sum_{d|n} \mu(d) g(n/d).$$

Bewijs: $\sum_{d|n} f(d) = g(n)$ voor alle $n \in \mathbf{Z}_{>0}$.

28. Laat zien dat de Euler-φ-functie φ en de functies $\sigma_k : n \mapsto \sum_{d|n} d^k$ voor $k \in \mathbf{Z}$ multiplicatieve aritmetische functies zijn. Bewijs: $\sum_{d|n} \mu(d)/d = \varphi(n)/n$.

*29. Zij x_d het aantal monische irreducibele polynomen van graad d in $\mathbf{F}_p[X]$.
   a. Bewijs in $\mathbf{Z}[[T]]$ de machtreeksidentiteit

$$\prod_{n=1}^{\infty}\Big(\frac{1}{1-T^n}\Big)^{x_n} = \frac{1}{1-pT}.$$

   [Hint: gebruik de meetkundige reeks $(1-aT)^{-1} = \sum_{k=0}^{\infty}(aT)^k \in \mathbf{Z}_p[[T]]$ en eenduidige factorisatie in $\mathbf{F}_p[X]$.]
   b. Leid de identiteit $\sum_{d|n} d \cdot x_d = p^n$ af door in het voorafgaande de logaritmische afgeleide $(\log f)' = f'/f$ te berekenen.

30. Bewijs dat het *Artin-Schreier-polynoom* $X^p - X - a \in \mathbf{F}_p[X]$ irreducibel van graad p is voor alle $a \in \mathbf{F}_p^*$. Hoe ontbindt het polynoom $X^q - X - a \in \mathbf{F}_q[X]$ in irreducibele factoren voor een willekeurig eindig lichaam $\mathbf{F}_q$?
[Hint: hoe werkt het Frobeniusautomorfisme op de wortels?]

31. Zij $K \subset L$ een uitbreiding van eindige lichamen en $G = \mathrm{Aut}_K(L)$ de bijbehorende automorfismengroep. Bewijs: voor $\alpha \in L$ met $L = K(\alpha)$ geldt $f_K^\alpha = \prod_{\sigma\in G}(X - \sigma(\alpha))$. Wat is de corresponderende uitspraak voor willekeurige $\alpha \in L$?

32. Neem $K \subset L$ en $G = \mathrm{Aut}_K(L)$ als in de vorige opgave. Definieer de *norm* en het *spoor* van een element $x \in L$ door $N_{L/K}(x) = \prod_{\sigma\in G}\sigma(x)$ en $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in G}\sigma(x)$. Bewijs dat $N_{L/K} : L^* \to K^*$ en $\mathrm{Tr}_{L/K} : L \to K$ surjectieve groepshomomorfismen zijn.

33. Zij $K \subset L$ een lichaamsuitbreiding, en $G = \mathrm{Aut}_K(L)$.
   a. Laat zien dat L^* een natuurlijke moduulstructuur heeft over de groepenring $\mathbf{Z}[G]$.
   b. Laat zien dat L een natuurlijke moduulstructuur heeft over de groepenring $K[G]$.
   c. Bewijs: voor K eindig en $K \subset L$ van eindige graad n zijn de groepenringen in a en b respectievelijk isomorf met $\mathbf{Z}[X]/(X^n - 1)$ en $K[X]/(X^n - 1)$.

*34. Zij $K \subset L$ een uitbreiding van eindige lichamen van graad n, en $G = \mathrm{Aut}_K(L)$ als in de vorige opgave. Vat L op als $K[X]$-moduul door X als het Frobeniusautomorfisme F_K te laten werken. Bewijs de volgende uitspraken:
   a. L is een eindig voortgebracht torsiemoduul over $K[X]$ geannihileerd door $X^n - 1$;
   b. de exponent van L als $K[X]$-moduul is $X^n - 1$;
   c. er bestaat $x \in L$ van orde $X^n - 1$, en voor zo'n x is L een vrij $K[G]$-moduul met basis $\{x\}$;
   d. er bestaat een K-basis voor L van de vorm $\{\sigma(x)\}_{\sigma\in G}$, een zogenaamde *normale basis* van L over K.

35. Zij $q > 3$ een priemmacht. Bewijs: ieder element $\alpha \in \mathbf{F}_q^* \setminus \{1\}$ is een voortbrenger van de multiplicatieve groep $\mathbf{F}_q^*$ dan en slechts dan als $q - 1$ een Mersenne-priem is (als in opgave 6.28).

36. Zij $f \in \mathbf{F}_q[X] \setminus \{0\}$ een polynoom, en t het aantal verschillende monische irreducibele factoren van f.
   a. Laat zien dat de *Berlekamp-deelalgebra* $B \subset \mathbf{F}_q[X]/(f)$ gegeven door

$$\{a \in \mathbf{F}_q[X]/(f) : a^q - a = 0\}$$

   een deelring is van $\mathbf{F}_q[X]/(f)$, en dat B als ring isomorf is met het product van t kopieën van $\mathbf{F}_q$.

b. Laat zien: f is irreducibel dan en slechts dan als $\dim_k B = 1$ en $\mathrm{ggd}(f, f') = 1$.

37. Beschouw $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ als ring met componentsgewijze ringoperaties, en definieer

$$\widehat{\mathbf{Z}} = \{(a_n)_{n\geq 1} \in \textstyle\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z} : \text{ voor alle } n \geq 1 \text{ en } d \mid n \text{ geldt } a_n \equiv a_d \bmod d\}.$$

a. Laat zien dat $\widehat{\mathbf{Z}}$ een deelring van $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ is.
b. Laat zien dat $\widehat{\mathbf{Z}}$ een ring van overaftelbare cardinaliteit is die $\mathbf{Z}$ als strikte deelring bevat.
c. Bewijs: voor $m \in \mathbf{Z}_{\geq 1}$ is de ring $\widehat{\mathbf{Z}}/m\widehat{\mathbf{Z}}$ isomorf is met $\mathbf{Z}/m\mathbf{Z}$.

[De ring $\widehat{\mathbf{Z}}$ heet de *pro-eindige completering van* $\mathbf{Z}$ of de *ring der pro-eindige getallen*.]

38. Zij $\overline{\mathbf{F}}_p$ een algebraïsche afsluiting van $\mathbf{F}_p$. Bewijs dat er een groepsisomorfisme

$$\mathrm{Aut}(\overline{\mathbf{F}}_p) \xrightarrow{\sim} \widehat{\mathbf{Z}}$$

naar de additieve groep van $\widehat{\mathbf{Z}}$ is dat het Frobenius-automorfisme op $1 \in \widehat{\mathbf{Z}}$ afbeeldt.

39. Zij $\mathbf{F}_q \subset L$ een lichaamsuitbreiding en $V \subset L$ een eindige deelverzameling. Bewijs: V is een deel-$\mathbf{F}_q$-vectorruimte van L dan en slechts dan als het polynoom $f = \prod_{v\in V}(X - v) \in L[X]$ van de vorm $f = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i}$ is voor zekere $n \in \mathbf{Z}_{\geq 0}$ en $a_0, \ldots, a_{n-1} \in L$.

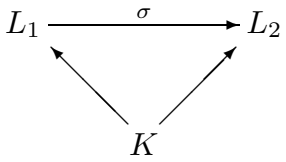
40. Zij $G = \mathbf{F}_q \rtimes \mathbf{F}_q^*$ de affiene groep over $\mathbf{F}_q$, gedefinieerd net als in 8.14.1, en n een positief geheel getal.
a. Bewijs: G heeft een ondergroep van orde n dan en slechts dan als $n = am$ geldt met a en m positieve delers van respectievelijk q en $q-1$ die voldoen aan $a \equiv 1 \bmod m$.
b. Stel dat n geen priemmacht is. Bewijs: er bestaat een groep van orde deelbaar door n die geen ondergroep van orde n heeft.

23 Separabele en normale uitbreidingen

In deze paragraaf behandelen we de twee eigenschappen van algebraïsche lichaamsuitbreidingen die een essentiële rol spelen in de Galoistheorie: *separabiliteit* en *normaliteit*. Voor een grote klasse van grondlichamen, waaronder eindige lichamen en lichamen van karakteristiek 0, blijken *alle* algebraïsche uitbreidingen separabel te zijn.

▶ Fundamentele verzameling

Laat L_1 en L_2 uitbreidingen van een lichaam K zijn. Dan geven we met $\mathrm{Hom}_K(L_1, L_2)$ de verzameling van lichaamshomomorfismen $L_1 \to L_2$ aan die op K de identiteit zijn. Korter gezegd: de K-homomorfismen $L_1 \to L_2$. Het zijn de homomorfismen $\sigma : L_1 \to L_2$ die een commutatief diagram



vormen met de inclusiepijlen $K \to L_i$.

23.1. Lemma. *Zij $K \subset L_1 = K(\alpha)$ een enkelvoudige algebraïsche lichaamsuitbreiding, $K \subset L_2$ een willekeurige lichaamsuitbreiding en S de verzameling van nulpunten van f_K^α in L_2. Dan is er een bijectie $\mathrm{Hom}_K(L_1, L_2) \xrightarrow{\sim} S$ gegeven door $\sigma \mapsto \sigma(\alpha)$.*

Bewijs. Een homomorfisme $\sigma : K(\alpha) \to L_2$ dat de identiteit is op K ligt vast door de keuze van het element $\sigma(\alpha) \in L_2$. Om in te zien dat $\sigma(\alpha)$ een nulpunt van $f = f_K^\alpha$ in L_2 is schrijven we $f = \sum_{i=0}^n a_i X^i \in K[X]$. Als in het bewijs van 22.10 geldt nu

$$f(\sigma(\alpha)) = \textstyle\sum_{i=0}^n a_i \sigma(\alpha)^i = \sigma(\sum_{i=0}^n a_i \alpha^i) = \sigma(0) = 0,$$

want σ is de identiteit op de coëfficiënten van f. Dit bewijst $\sigma(\alpha) \in S$.

Omgekeerd is voor ieder nulpunt $s \in S$ van f de afbeelding $L_1 \to L_2$ gedefinieerd door $\sum_i c_i \alpha^i \mapsto \sum_i c_i s^i$ wegens 21.5.2 een K-homomorfisme $L_1 \to L_2$. □

23.2. Definitie. *Zij $K \subset L$ een algebraïsche uitbreiding en Ω een algebraïsch afgesloten lichaam dat K bevat. Dan heet*

$$X(L/K) = X_\Omega(L/K) = \mathrm{Hom}_K(L, \Omega)$$

een fundamentele verzameling voor de uitbreiding $K \subset L$.

Hoewel een fundamentele verzameling voor $K \subset L$ afhangt van de keuze van een algebraïsch afgesloten lichaam $\Omega \supset K$, zullen we veelal $X(L/K)$ schrijven voor $X_\Omega(L/K)$.

Lemma 23.1 laat zien dat het beeld in Ω van een element $\alpha \in L$ onder $\sigma \in X(L/K)$ weer algebraïsch is over K. We kunnen $X_\Omega(L/K)$ daarom identificeren met $\mathrm{Hom}_K(L, \overline{K})$, met $\overline{K}$ het algebraïsch afgesloten lichaam verkregen door, net als in 21.12, de algebraïsche afsluiting van K in Ω te vormen. In veel gevallen nemen we eenvoudig

$\Omega = \overline{K}$, maar soms is het handig om voor $K = \mathbf{Q}$ ook de keuze $\Omega = \mathbf{C}$ te kunnen maken. Merk ook op dat $X(L/K)$ nooit de lege verzameling is.

Is $\overline{K}'$ een andere algebraïsche afsluiting van K, dan bestaat er een K-isomorfisme $\psi : \overline{K} \xrightarrow{\sim} \overline{K}'$ wegens 21.16. Samenstelling met ψ geeft een bijectie

$$\mathrm{Hom}_K(L, \overline{K}) \xrightarrow{\sim} \mathrm{Hom}_K(L, \overline{K}').$$

We concluderen dat de cardinaliteit van $X(L/K)$ niet afhangt van de keuze van het lichaam Ω in 23.2. Voor een enkelvoudige algebraïsche uitbreiding $L = K(\alpha)$ volgt uit 23.1 dat we de fundamentele verzameling $X(L/K)$ met de verzameling van nulpunten van f_K^α in een algebraïsche afsluiting van K kunnen identificeren. Deze 'explicietere' beschrijving heeft echter het nadeel dat hij, anders dan $X(L/K)$ zelf, van de keuze van een voortbrengend element α afhangt.

Algemener zien we dat voor eindige uitbreidingen $K \subset L$ ook $X(L/K)$ eindig is. Immers, schrijf $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ en merk op dat $\sigma \in X(L/K)$ vastligt door zijn waarden op de elementen α_i. Omdat $\sigma(\alpha_i)$ een nulpunt van $f_K^{\alpha_i}$ is, zijn er slechts eindig veel mogelijkheden voor σ.

Opgave 1. Zijn er algebraïsche uitbreidingen $K \subset L$ waarvoor $X(L/K)$ de lege verzameling is?

▶ Separabele uitbreidingen

Aan een fundamentele verzameling $X(L/K)$ kan men de 'separabiliteitseigenschappen' van de uitbreiding $K \subset L$ aflezen. We noemen een polynoom in $K[X]$ *separabel* als het geen meervoudige nulpunten heeft in een algebraïsche afsluiting $\overline{K}$, en *inseparabel* als dat wel het geval is.

23.3. Definitie. *De separabiliteitsgraad $[L : K]_s$ van een algebraïsche uitbreiding $K \subset L$ is de cardinaliteit van een fundamentele verzameling $X(L/K)$.*

We zagen al dat de cardinaliteit van $X(L/K)$ niet afhangt van de keuze van het algebraïsch afgesloten lichaam Ω in de definitie van $X(L/K)$. Voor een enkelvoudige algebraïsche uitbreiding $K \subset L = K(\alpha)$ is $[L : K]_s$ wegens 23.1 het aantal verschillende nulpunten van f_K^α in $\overline{K}$. Er geldt dus $1 \leq [L : K]_s \leq \deg(f_K^\alpha) = [L : K]$, met gelijkheid dan en slechts dan als f_K^α separabel is.

23.4. Lemma. *Voor iedere eindige lichaamsuitbreiding $K \subset L$ geldt de ongelijkheid*

$$1 \leq [L : K]_s \leq [L : K].$$

Is $K \subset L \subset M$ een toren van eindige uitbreidingen, dan geldt

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Bewijs. Iedere inbedding $\tau : M \to \Omega$ in $X(M/K)$ wordt verkregen door voortzetting van een inbedding $\sigma : L \to \Omega$ uit $X(L/K)$. Nu kan men voor een vaste 'inclusie' $\sigma : L \to \Omega$ de verzameling van voortzettingen $\tau : M \to \Omega$ met $X(M/L)$ identificeren, en dit geeft $\#X(M/K) = \#X(L/K) \cdot \#X(M/L)$. De tweede uitspraak in 23.4 volgt.

Nu we eenmaal weten dat de separabiliteitsgraad zich net als de gewone graad multiplicatief gedraagt in torens van uitbreidingen volgt de algemene ongelijkheid $[L : K]_s \leq [L : K]$ uit de reeds genoemde ongelijkheid voor het enkelvoudige geval. Immers, een willekeurige eindige uitbreiding $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ wordt verkregen als een toren

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

van n enkelvoudige eindige uitbreidingen. Vermenigvuldiging van de ongelijkheden voor deze uitbreidingen levert direct $[L : K]_s \leq [L : K]$. □

Voor willekeurige algebraïsche uitbreidingen $K \subset L$ zeggen we dat een element $\alpha \in L$ *separabel* is over K als f_K^α geen meervoudige nulpunten heeft in $\overline{K}$. De uitbreiding $K \subset L$ zelf heet separabel als ieder element $\alpha \in L$ separabel is over K. Een algebraïsche uitbreiding die niet separabel is, heet *inseparabel*.

23.5. Stelling. *Voor een eindige uitbreiding $K \subset L$ zijn equivalent:*

1. *de uitbreiding $K \subset L$ is separabel;*
2. *er geldt $L = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ voor elementen $\alpha_1, \alpha_2, \ldots, \alpha_t \in L$ die separabel zijn over K;*
3. $[L : K]_s = [L : K]$.

Bewijs. (1 ⇒ 2). Dit is duidelijk, want alle $\alpha_i \in L$ zijn separabel over K.

(2 ⇒ 3). Voor een enkelvoudige uitbreiding $K \subset K(\alpha)$ zagen we al dat de separabiliteit van α wegens 23.1 impliceert dat $[K(\alpha) : K]_s$ gelijk is aan $\deg(f_K^\alpha) = [K(\alpha) : K]$. Voor $L = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ krijgen we L als in het bewijs van 23.4 door achtereenvolgens de α_i te adjungeren. De elementen α_i, die separabel zijn over K, zijn dit ook over elke uitbreiding E van K, want f_E^α is een deler van f_K^α in $\overline{K}[X]$. In elk stapje van de toren zijn daarom de graad en de separabiliteitsgraad gelijk. Wegens multiplicativiteit van graad en separabiliteitsgraad geldt gelijkheid nu ook voor de hele uitbreiding $K \subset L$.

(3 ⇒ 1). Voor alle $\alpha \in L$ hebben we een toren $K \subset K(\alpha) \subset L$. Omdat de separabiliteitgraad begrensd is door de graad volgt uit de gelijkheid $[L : K]_s = [L : K]$ en de multiplicativiteit in torens dat ook voor de uitbreiding $K \subset K(\alpha)$ de gelijkheid $[K(\alpha) : K]_s = [K(\alpha) : K]$ geldt. Dit betekent wegens 23.1 dat f_K^α precies $\deg(f_K^\alpha)$ verschillende nulpunten heeft in $\overline{K}$, dus α is separabel over K. □

▶ Perfecte lichamen

Voor veel grondlichamen K blijken *alle* algebraïsche uitbreidingen separabel te zijn. Irreducibele polynomen hebben namelijk slechts zelden dubbele nulpunten.

23.6. Lemma. *Laat $f \in K[X]$ een irreducibel polynoom zijn, en stel dat f inseparabel is. Dan geldt $p = \mathrm{char}(K) > 0$, en we hebben $f = g(X^p)$ voor zekere $g \in K[X]$. Bovendien zijn niet alle coëfficiënten van f een p-de macht in K.*

Bewijs. Als f een dubbel nulpunt $\alpha \in \overline{K}$ heeft, dan is α ook een nulpunt van de afgeleide f' van f. Omdat f het minimumpolynoom van α over K is, impliceert de

aanname $f'(\alpha) = 0$ dat f' deelbaar is door f. Omdat f' lagere graad heeft dan f kan dit alleen als f' het nulpolynoom is in $K[X]$.

Voor K van karakteristiek 0 vinden we dat f constant is, in tegenspraak met de aanname dat f irreducibel is. We hebben dus $\mathrm{char}(K) = p > 0$, en door expliciet afgeleides te nemen zien we dat we $f' = 0$ krijgen voor de polynomen in $K[X]$ van de vorm $f = \sum_i a_i X^{ip} \in K[X]$. Met $g = \sum_i a_i X^i$ hebben we dan $f = g(X^p)$.

Zouden de coëfficiënten van f alle p-de machten zijn in K, zeg $a_i = c_i^p \in K$, dan hebben we $f = \sum_i a_i X^{ip} = \sum_i c_i^p X^{ip} = (\sum_i c_i X^i)^p$ wegens de additiviteit van de p-de machtsverheffing in karakteristiek p. Een irreducibel polynoom $f \in K[X]$ kan echter geen p-de macht zijn in $K[X]$, dus dit leidt tot een tegenspraak. □

We concluderen uit 23.6 dat irreducibele inseparabele polynomen in $K[X]$ alleen kunnen bestaan voor lichamen K van karakteristiek $p > 0$ waarvoor de Frobeniusafbeelding $F : K \to K$ gegeven door $x \mapsto x^p$ *niet* surjectief is. Merk op dat F als lichaamshomomorfisme $K \to K$ altijd injectief is.

23.7. Definitie. *Een lichaam K heet perfect als het aan één van de volgende twee eisen voldoet:*

1. *de karakteristiek van K is 0;*
2. *de karakteristiek van K is $p > 0$, en de Frobeniusafbeelding $F : x \mapsto x^p$ is een automorfisme van K.*

Merk op dat eindige lichamen en getallenlichamen – voor ons de belangrijkste voorbeelden – perfect zijn. In het lichaam $\mathbf{F}_p(T)$ is T echter geen p-de macht, dus $\mathbf{F}_p(T)$ is imperfect. In de aritmetische algebraïsche meetkunde komt men imperfecte grondlichamen veelvuldig tegen.

23.8. Stelling. *Een lichaam K is perfect dan en slechts dan als iedere algebraïsche uitbreiding van K separabel is.*

Bewijs. Als K een inseparabele algebraïsche uitbreiding heeft, dan bestaan er inseparabele irreducibele polynomen in $K[X]$ en is K niet perfect wegens 23.6.

Als omgekeerd K niet perfect is, dan is er een element $a \in K$ dat geen p-de macht is in K. Laat $\alpha \in \overline{K}$ een nulpunt zijn van het polynoom $X^p - a$. Dan geldt

$$X^p - a = (X - \alpha)^p \in \overline{K}[X],$$

dus $K \subset K(\alpha)$ is een inseparabele uitbreiding. □

Opgave 2. Is het polynoom $X^p - a$ hierboven noodzakelijk *irreducibel* in $K[X]$?

▶ Primitieve elementen

Veel van de bewijzen in deze paragraaf herleiden vragen voor een willekeurige eindige uitbreiding $K \subset L$ tot het geval van een enkelvoudige uitbreiding $K \subset K(\alpha)$. Men kan zich afvragen of iedere eindige uitbreiding $K \subset L$ noodzakelijk van deze vorm is. In dit geval noemt men α een *primitief element* voor de uitbreiding $K \subset L$. Voor expliciete berekeningen is het vaak handig om een primitief element te hebben. Net zoals men

basiskeuzes in de lineaire algebra in (conceptuele) bewijzen bij voorkeur vermijdt, kan men ook in bewijzen in de lichaamstheorie de keuze van een primitief element waar mogelijk vermijden.

Enig proberen laat zien dat men in veel uitbreidingen met meer voortbrengers, zoals $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$, een primitief element vindt door lineaire combinaties van de voortbrengers over het grondlichaam te beschouwen.

Opgave 3. Bewijs: $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\lambda\sqrt{2} + \mu\sqrt{3})$ voor alle $\lambda, \mu \in \mathbf{Q}^*$.

In separabele uitbreidingen kunnen we altijd een primitief element vinden.

23.9. Stelling van het primitieve element. *Zij $K \subset L$ een eindige separabele uitbreiding. Dan bestaat er een element $x \in L$ met $L = K(x)$.*

Bewijs. Het is voldoende te laten zien dat we voor ieder tweetal elementen $\alpha, \beta \in L$ een element $x \in L$ kunnen vinden zodat $K(\alpha, \beta) = K(x)$ geldt. Immers, door herhaald twee voortbrengers door één te vervangen krijgen we zo voor iedere eindig voortgebrachte deeluitbreiding van L over K een primitief element – en dus ook voor L zelf.

Stel nu dat $L = K(\alpha, \beta)$ graad n over K heeft. Wegens de separabiliteit van $K \subset L$ bevat $X(L/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ precies n verschillende inbeddingen. We zoeken een element $\lambda \in K$ zo dat de beelden van $x = \alpha + \lambda\beta$ onder de elementen σ_i alle verschillend zijn. Dit betekent dat λ geen nulpunt is van het polynoom

$$f = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} \Big((\sigma_i(\beta) - \sigma_j(\beta))X + (\sigma_i(\alpha) - \sigma_j(\alpha)) \Big) \in \overline{K}[X].$$

Omdat twee verschillende elementen van $X(L/K)$ niet op zowel α als β overeen kunnen stemmen, is f niet het nulpolynoom. Dit betekent dat f slechts eindig veel nulpunten heeft, en voor oneindige K vinden we dat $\lambda \in K$ met $f(\lambda) \neq 0$ bestaat. Voor eindige K is dit niet duidelijk, maar in dat geval geeft 22.5 het bestaan van een primitief element en zijn we direct klaar.

Voor oneindige K kiezen we $x = \alpha + \lambda\beta$ als boven. Dan heeft $K(x)$ separabiliteitsgraad $\geq n$ over K, en dus ook graad $[K(x) : K] \geq n$. Anderzijds hebben we $[K(x) : K] \leq [L : K] = n$, dus er geldt zoals gewenst $K(x) = L$. □

Ook in inseparabele uitbreidingen kan men soms primitieve elementen vinden, bijvoorbeeld als de graad een priemgetal is. Als er geen primitief element bestaat, hebben we te doen met een uitbreiding met oneindig veel *tussenlichamen*. Voor dergelijke uitbreidingen is er geen *Galoiscorrespondentie* in de zin van 24.4.

23.10. Stelling. *Zij $K \subset L$ een eindige uitbreiding. Dan zijn equivalent:*

1. *er bestaat een element $\alpha \in L$ met $L = K(\alpha)$;*
2. *er zijn slechts eindig veel lichamen E met $K \subset E \subset L$.*

Bewijs. (1 $\Rightarrow$ 2). Laat α een primitief element voor $K \subset L$ zijn, en beschouw voor ieder tussenlichaam E het minimumpolynoom $f_E^\alpha \in E[X]$. Omdat f_E^α een monische deler van f_K^α is in $\overline{K}[X]$ en een polynoom met coëfficiënten in een lichaam slechts

eindig veel monische delers heeft, zijn er slechts eindig veel mogelijkheden voor f_E^α. Uit f_E^α kan men echter E aflezen: het is de uitbreiding van K voortgebracht door de coëfficiënten van f_E^α. Immers, over het deellichaam $E_0 \subset E$ dat deze coëfficiënten voortbrengen over K geldt $[L : E_0] = \deg(f_{E_0}^\alpha) = \deg(f_E^\alpha) = [L : E]$, en dus $E_0 = E$.

$(2 \Rightarrow 1)$. Omdat beide uitspraken voor eindige lichamen K automatisch vervuld zijn nemen we aan dat K oneindig is. Net als in het bewijs van 23.9 is het voldoende te laten zien dat iedere deeluitbreiding $K \subset K(\alpha, \beta)$ van $K \subset L$ primitief is. Gegeven elementen $\alpha, \beta \in L$ weten we nu dat de lichamen $K(\alpha + \lambda\beta)$ met $\lambda \in K$ niet alle verschillend zijn. Stel dus $K(\alpha+\lambda_1\beta) = K(\alpha+\lambda_2\beta)$ met $\lambda_1 \neq \lambda_2$. Dan bevat $K(\alpha+\lambda_1\beta)$ de elementen

$$\alpha = (\lambda_2 - \lambda_1)^{-1}[\lambda_2(\alpha + \lambda_1\beta) - \lambda_1(\alpha + \lambda_2\beta)]$$
$$\beta = (\lambda_1 - \lambda_2)^{-1}[(\alpha + \lambda_1\beta) - (\alpha + \lambda_2\beta)],$$

dus $K(\alpha, \beta) = K(\alpha + \lambda_1\beta)$ is een primitieve uitbreiding. □

Opgave 4. Zij V een vectorruimte over een oneindig grondlichaam K. Bewijs dat V *niet* de vereniging is van een eindig aantal deelruimten $V_i \subsetneq V$. Leid hieruit de implicatie 23.10.2 ⇒ 23.10.1 af.

Opgave 20 geeft een voorbeeld van een inseparabele uitbreiding van graad p^2 die niet primitief is, en dus oneindig veel tussenlichamen heeft.

▶ Normale uitbreidingen

Voor een eindige separabele uitbreiding $K \subset L$ weten we dat L op $[L : K]$ verschillende manieren in een algebraïsch afgesloten uitbreiding Ω van K kan worden ingebed. In het geval dat het beeld $\sigma[L] \subset \overline{K}$ niet van de keuze van $\sigma \in X(L/K)$ afhangt kan men een vaste K-inbedding $\tau : L \subset \Omega$ *kiezen* en als inclusie opvatten. De elementen van $X(L/K)$ worden dan *automorfismen* van het lichaam L, en we krijgen een identificatie

$$X(L/K) \xrightarrow{\sim} \mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \sigma|_K = \mathrm{id}_K\} \tag{23.11}$$

van $X(L/K)$ met de *groep* van automorfismen van L die op K de identiteit zijn. Deze identificatie hangt echter af van de keuze van een element $\tau \in X(L/K)$ dat als identiteit $\mathrm{id}_L \in \mathrm{Aut}_K(L)$ optreedt – zie opgave 28.

Het blijkt nu dat niet in het algemeen voor eindige separabele uitbreidingen $K \subset L$ alle beelden $\sigma[L] \subset \overline{K}$ voor $\sigma \in X(L/K)$ gelijk zijn. Schrijft men namelijk $L = K(\alpha)$ voor een primitief element $\alpha \in L$, dan zijn de beelden van L in Ω de lichamen $K(\alpha_i)$, met α_i lopend over de nulpunten van f_K^α in Ω. De lichamen $K(\alpha_i)$ vallen dan en slechts dan samen als f_K^α *al* zijn nulpunten in $L = K(\alpha)$ heeft, en L dus een ontbindingslichaam is van f_K^α over K. In zo'n geval noemt men L een *normale* separabele uitbreiding van K. De algemene definitie van normaliteit luidt als volgt.

23.12. Definitie. *Een algebraïsche lichaamsuitbreiding $K \subset L$ heet normaal als voor ieder element $\alpha \in L$ het minimumpolynoom f_K^α in lineaire factoren ontbindt in $L[X]$.*

23.13. Voorbeelden. Het lichaam $L = \mathbf{Q}(\alpha)$ uit 21.15.2 verkregen door een derdemachtswortel α uit 2 te adjungeren is geen normale uitbreiding van $\mathbf{Q}$: het polynoom $f_{\mathbf{Q}}^\alpha = X^3 - 2$ heeft slechts 1 nulpunt in L.

Iedere eindige uitbreiding $\mathbf{F}_p \subset L$ van $\mathbf{F}_p$ is normaal. Immers, wegens 22.11 zijn voor iedere $\alpha \in L$ de nulpunten van $f^{\alpha}_{\mathbf{F}_p}$ *machten* van α, en die zijn bevat in L.

De inseparabele uitbreiding $K = \mathbf{F}_p(T) \subset L = \mathbf{F}_p(T^{1/p})$ is normaal. Immers, voor iedere $\alpha \in L$ geldt $\alpha^p \in K$, en $X^p - \alpha^p \in K[X]$ heeft een p-voudige lineaire factor $X - \alpha$ in L.

23.14. Stelling. *Voor een eindige uitbreiding $K \subset L$ met fundamentele verzameling $X(L/K)$ zijn equivalent:*

1. *de uitbreiding $K \subset L$ is normaal;*
2. *L is een ontbindingslichaam Ω^f_K van een polynoom $f \in K[X]$;*
3. *voor alle $\sigma, \tau \in X(L/K)$ geldt $\sigma[L] = \tau[L]$.*

Bewijs. $(1 \Rightarrow 2)$. Schrijf $L = K(\beta_1, \beta_2, \ldots, \beta_t)$. Dan liggen wegens de normaliteit van $K \subset L$ alle nulpunten van $f = f_K^{\beta_1} \cdot f_K^{\beta_2} \cdot \ldots \cdot f_K^{\beta_t} \in K[X]$ in L. Omdat ze L over K voortbrengen geldt $L = \Omega^f_K$.

$(2 \Rightarrow 3)$. Laat $L = \Omega^f_K$, en stel dat f in $\overline{K}[X]$ ontbindt als $f = \prod_{i=1}^n (X - \alpha_i)$. Dit geeft een inclusie $\sigma : L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \overline{K}$. Is nu $\tau \in X(L/K)$ willekeurig, dan geldt $\prod_{i=1}^n (X - \tau(\alpha_i)) = f = \prod_{i=1}^n (X - \alpha_i)$, want τ is de identiteit op de coëfficiënten van f. We vinden dat τ de nulpunten van f permuteert, en dat geeft de gewenste gelijkheid $\tau[L] = K(\tau(\alpha_1), \tau(\alpha_2), \ldots, \tau(\alpha_n)) = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sigma[L] \subset \overline{K}$.

$(3 \Rightarrow 1)$. Kies een element $\sigma : L \to \overline{K}$ in $X(L/K)$, en neem $\alpha \in L$ willekeurig. Stel dat f^{α}_K in $\overline{K}[X]$ ontbindt als $f^{\alpha}_K = \prod_{i=1}^n (X - \alpha_i)$. Wegens 23.1 geeft dit K-isomorfismen $\sigma_i : K(\alpha) \xrightarrow{\sim} K(\alpha_i) \subset \overline{K}$. Elk van de isomorfismen σ_i heeft als in opgave 21.14 een voortzetting tot een isomorfisme $\sigma_i' : \overline{L} \to \overline{K}$, met $\overline{L}$ een algebraïsche afsluiting van L (en dus van $K(\alpha)$). Dit isomorfisme beeldt α af op $\alpha_i \in \sigma_i'[L]$, en wegens aanname 3 hebben we $\sigma_i'[L] = \sigma[L]$ voor alle σ_i'. Er volgt dat f^{α}_K in lineaire factoren ontbindt in $\sigma[L]$, en dus ook in L. □

Het bewijs van 23.14 laat zien dat iedere eindige uitbreiding $K \subset L$ past in een toren van uitbreidingen $K \subset L \subset M$ met M eindig en normaal over K: neem het product f van de minimumpolynomen van een eindig stel elementen β_i dat L voortbrengt over K, en kies $M = \Omega^f_K = \Omega^f_L$. Omdat iedere normale uitbreiding van K die alle β_i bevat ook een deellichaam isomorf met M bevat, is M de 'kleinste' normale uitbreiding van K die L bevat. Zo'n uitbreiding heet een *normale afsluiting* van L over K.

Opgave 5. Laat zien dat een normale afsluiting van L over K op K-isomorfie na eenduidig bepaald is, en dat er binnen een algebraïsche afsluiting $\overline{K}$ van K een *unieke* normale afsluiting van L bestaat.

▶ Onafhankelijkheid van karakters

Het belangrijkste ingrediënt in het bewijs van de hoofdstelling van de Galoistheorie, die we in 24.4 voor eindige *normale* en *separabele* lichaamsuitbreidingen $K \subset L$ formuleren, is de 'lineaire onafhankelijkheid' van de elementen uit de fundamentele verzameling $X(L/K)$. Hiermee bedoelen we het volgende.

23.15. Lemma van Artin-Dedekind. *Zij $K \subset L$ een algebraïsche uitbreiding, en $\sigma_1, \sigma_2, \ldots, \sigma_n \in X(L/K) = \mathrm{Hom}_K(L, \Omega)$ een n-tal paarsgewijs verschillende elementen. Stel dat er $c_1, c_2, \ldots, c_n \in \Omega$ bestaan met*

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \ldots + c_n\sigma_n(x) = 0 \qquad \text{voor alle } x \in L.$$

Dan geldt $c_1 = c_2 = \ldots = c_n = 0$.

Bewijs. We voeren het bewijs met inductie naar n. Voor $n = 1$ volgt uit de relatie $c_1\sigma_1(x) = 0$ voor $x \in L$ onmiddellijk $c_1 = c_1\sigma(1) = 0$.

Stel nu dat het lemma correct is voor verzamelingen van minder dan n elementen van $X(L/K)$, en laat een nulrelatie tussen $n \geq 2$ elementen als boven gegeven zijn. Omdat σ_1 en σ_2 verschillen op L, bestaat er een element $y \in L$ met $\sigma_1(y) \neq \sigma_2(y)$. Neem zo'n y, en vorm uit de gegeven nulrelatie twee nieuwe relaties door respectievelijk de relatie te vermenigvuldigen met $\sigma_1(y)$ en x in de relatie te vervangen door xy. Omdat de σ_i homomorfismen zijn, geeft dit, voor $x \in L$ willekeurig,

$$\begin{aligned} c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_2(x)\sigma_1(y) + \ldots + c_n\sigma_n(x)\sigma_1(y) &= 0 \\ c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_2(x)\sigma_2(y) + \ldots + c_n\sigma_n(x)\sigma_n(y) &= 0. \end{aligned}$$

Aftrekken van beide relaties geeft een nulrelatie voor de $n-1$ elementen $\sigma_2, \sigma_3, \ldots, \sigma_n$ waarin de coëfficiënt bij σ_2 gelijk is aan $c_2(\sigma_1(y) - \sigma_2(y))$. Wegens de inductiehypothese is deze coëfficiënt gelijk aan 0. De keuze van y impliceert dat $c_2 = 0$ geldt, dus de term met σ_2 in de oorspronkelijke relatie kan worden weggelaten. Passen we nogmaals de inductiehypothese toe, dan volgt dat alle c_i gelijk zijn aan 0. □

Het bovenstaande bewijs gebruikt slechts dat de σ_i *groepshomomorfismen* $L^* \to \Omega^*$ zijn. Definieert men algemener voor een abelse groep A en een lichaam F een *F-waardig karakter* als een groepshomomorfisme $\sigma : A \to F^*$, dan laat exact hetzelfde bewijs zien dat er geen F-lineaire relaties bestaan tussen de F-waardige karakters op A.

Opgave 6. Formuleer en bewijs dit algemenere lemma van Artin-Dedekind.

▶ Norm en spoor

Laat $K \subset L$ een eindige separabele uitbreiding zijn. Dan zijn de *norm* en het *spoor* (Engels: *trace*) naar K van een element $x \in L$ gedefinieerd door

$$N_{L/K}(x) = \prod_{\sigma \in X(L/K)} \sigma(x) \qquad \text{en} \qquad \mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in X(L/K)} \sigma(x). \tag{23.16}$$

Direct duidelijk is de multiplicatieve eigenschap $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$ van de norm en de additieve eigenschap $\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$ van het spoor.

De normafbeelding $N_{\mathbf{Q}(i)/\mathbf{Q}} : \mathbf{Q}(i) \to \mathbf{Q}$, die $a + bi$ naar $(a+bi)(a-bi) = a^2 + b^2$ stuurt, kwamen we vlak voor 12.19 al tegen. In dit geval is de norm van x het product van x met zijn complex geconjugeerde $\overline{x}$. Voor een willekeurige separabele uitbreiding $K \subset L$ zien we uit 23.1 dat, indien $x \in L$ het lichaam L voortbrengt over K, de

norm $N_{L/K}(x)$ het product van de nulpunten van het separabele polynoom $f_K^x = \sum_{i=0}^n a_i X^i \in K[X]$ in een algebraïsche afsluiting van K is, en het spoor $\mathrm{Tr}_{L/K}(x)$ de som van de nulpunten. Deze zijn respectievelijk gelijk aan $(-1)^n a_0$ en $-a_{n-1}$, en liggen dus in K. Algemener vindt men als in het bewijs van 23.4 de elementen van $X(L/K)$ door voor ieder element van $X(K(x)/K)$ de $[L : K(x)]$ verschillende voortzettingen tot L te beschouwen, en dit geeft

$$(23.17) \quad N_{L/K}(x) = N_{K(x)/K}(x)^{[L:K(x)]} \quad \text{en} \quad \mathrm{Tr}_{L/K}(x) = [L : K(x)] \cdot \mathrm{Tr}_{K(x)/K}(x).$$

We concluderen dat de norm een groepshomomorfisme $N_{L/K} : L^* \to K^*$ induceert, en het spoor een groepshomomorfisme $\mathrm{Tr}_{L/K} : L \to K$. Voor een uitbreiding $K \subset L$ van *eindige* lichamen kwamen we deze homomorfismen al tegen in opgave 22.32.

Opgave 7. Is de normafbeelding $N_{\mathbf{Q}(i)/\mathbf{Q}} : \mathbf{Q}(i) \to \mathbf{Q}$ surjectief?

Voor een element x in een eindige uitbreiding L van K is de vermenigvuldiging

$$\begin{aligned} M_x : L &\longrightarrow L \\ y &\longmapsto xy \end{aligned}$$

met x een K-lineaire afbeelding van de K-vectorruimte L, en hebben we het volgende verband met de uit de lineaire algebra bekende determinanten en sporen van matrices.

23.18. Stelling. *Zij $K \subset L$ een eindige separabele uitbreiding, en $M_x : L \to L$ de vermenigvuldiging met x op L. Dan is M_x een K-lineaire afbeelding met determinant $N_{L/K}(x)$ en spoor $\mathrm{Tr}_{L/K}(x)$.*

Bewijs. We kunnen $L = \sum_{k=1}^{[L:K(x)]} K(x) \cdot \omega_k$ opvatten als een som van $[L : K(x)]$ ééndimensionale vectorruimten $K(x) \cdot \omega_k$ over $K(x)$, die elk door M_x in zichzelf worden overgevoerd. Schrijven we $f_K^x = \sum_{i=1}^n a_i X^i \in K[X]$, dan wordt vermenigvuldiging met x op $K(x)$ ten opzichte van de K-basis $\{1, x, x^2, \ldots, x^{n-1}\}$ gerepresenteerd door de matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & \ldots & 1 & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

die als determinant $(-1)^n a_0 = N_{K(x)/K}(x)$ en als spoor $-a_{n-1} = \mathrm{Tr}_{K(x)/K}(x)$ heeft. Wegens (23.17) volgt hieruit het gewenste resultaat. □

Opgave 8. Laat zien dat het karakteristieke polynoom van M_x gelijk is aan $\mathrm{char}(M_x) = (f_K^x)^{[L:K(x)]}$.

Men kan in omgekeerde richting 23.18 als *definitie* nemen van de norm- en spoorafbeelding voor een eindige uitbreiding $K \subset L$, en voor separabele uitbreidingen hieruit de uitdrukking (23.16) afleiden: zie de opgaven 30 en 31.

OPGAVEN.

9. Zij $L_1 = K(T)$ een enkelvoudige transcendente uitbreiding van K en $K \subset L_2$ een willekeurige uitbreiding. Bewijs: de afbeelding $\mathrm{Hom}_K(L_1, L_2) \to L_2$ gegeven door $f \mapsto f(T)$ is injectief. Beschrijf het beeld.

10. Laat $K \subset L \subset M$ een toren van algebraïsche uitbreidingen zijn. Bewijs:
$$K \subset L \text{ en } L \subset M \text{ zijn separabel} \iff K \subset M \text{ is separabel.}$$

11. Zij $K \subset L$ een willekeurige lichaamsuitbreiding. Bewijs dat
$$K_s = \{x \in L : x \text{ is algebraïsch en separabel over } K\}$$
een deellichaam van L is. Het heet de *separabele afsluiting* van K in L.

12. Een lichaam F heet *separabel afgesloten* als de enige separabele algebraïsche uitbreiding $F \subset E$ de triviale uitbreiding $E = F$ is. Een *separabele afsluiting* van een lichaam K is een algebraïsche uitbreiding $K \subset K^{\mathrm{sep}}$ met K^{sep} separabel afgesloten. Bewijs:
    a. ieder lichaam K heeft een separabele afsluiting;
    b. ieder tweetal separabele afsluitingen van K is K-isomorf;
    c. een separabele afsluiting K^{sep} van K is algebraïsch afgesloten dan en slechts dan als K perfect is.

13. Leid de stelling van het primitieve element af uit het vectorruimte-argument in opgave 4. [Hint: kijk naar $\{x \in L : \sigma(x) = \tau(x)\}$ voor $\sigma, \tau \in X(L/K)$.]

14. Zij K een lichaam van karakteristiek $p > 0$ en $f \in K[X]$ een irreducibel polynoom. Bewijs dat er een separabel irreducibel polynoom $g \in K[X]$ bestaat en een getal $n \in \mathbf{Z}_{\geq 0}$ met $f = g(X^{p^n})$. Wat is de separabele afsluiting van K in $L = K[X]/(f)$?

15. Zij $K \subset L$ een eindige uitbreiding met $p = \mathrm{char}(K) > 0$ en K_s de separabele afsluiting van K in L. Bewijs: $[L : K]_s = [K_s : K]$ en $[L : K]_s \cdot p^k = [L : K]$ voor zekere $k \in \mathbf{Z}_{\geq 0}$. [Men noemt: $[L : K]/[L : K]_s$ de *inseparabiliteitsgraad* van L over K.]

16. Laat α algebraïsch zijn over K. Bewijs: $f_K^\alpha = \prod_{\sigma \in X(K(\alpha)/K)} (X - \sigma(\alpha))^i$, met i de inseparabiliteitsgraad van $K(\alpha)$ over K.

17. Zij K een lichaam van karakteristiek $p > 0$ en $a \in K$ een element dat geen p-de macht is. Bewijs: $X^{p^k} - a$ is irreducibel in $K[X]$ voor alle $k \geq 0$.

18. Zij K van karakteristiek $p > 0$ en $f \in K[X]$ monisch irreducibel. Schrijf $L = K(\alpha)$ met α een nulpunt van f, en geef met K^p en L^p het beeld aan van de Frobeniusafbeelding op respectievelijk K en L.
    a. Bewijs: $\alpha \in L^p \Rightarrow f \in K^p[X]$.
    b. Stel $f \notin K^p[X]$. Bewijs: $f(X^{p^k})$ is irreducibel in $K[X]$ voor $k \in \mathbf{Z}_{\geq 0}$.

19. Zij $f \in \mathbf{F}_p[T]$ een irreducibel polynoom en $K = \mathbf{F}_p(T)$ het quotiëntenlichaam van $\mathbf{F}_p[T]$.
    a. Bewijs: $X^p - f$ is irreducibel in $K[X]$.
    b. Bewijs: $K \subset L_f = K[X]/(X^p - f)$ is een inseparabele uitbreiding van graad p, en er geldt $L_f^p = K$.
    c. Zij L het lichaam verkregen door $f = T$ te nemen in b. Bewijs: $L_f \cong L$ voor alle irreducibele $f \in \mathbf{F}_p[T]$.

20. Zij $L = \mathbf{F}_p(S,T)$ het lichaam van rationale functies in twee variabelen over $\mathbf{F}_p$, en $K = L^p$.
    a. Bewijs: $K = \mathbf{F}_p(S^p, T^p)$, en $K \subset L$ is een lichaamsuitbreiding van graad p^2.
    b. Laat zien dat $K \subset L$ geen primitieve uitbreiding is.
    c. Geef oneindig veel verschillende lichamen E aan met $K \subset E \subset L$.

21. Voor een lichaam K van karakteristiek $p > 0$ heet de graad $[K : K^p]$ van de lichaamsuitbreiding $K^p \subset K$ de *imperfectiegraad* van K. Bewijs de volgende uitspraken.
    a. $[K : K^p] = p^{i(K)}$ met $i(K) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$.
    b. Voor iedere eindige uitbreiding $K \subset L$ geldt $i(L) = i(K)$.
    c. Voor iedere algebraïsche uitbreiding $K \subset L$ geldt $i(L) \leq i(K)$.
    d. Er geldt $i(K(T)) = i(K) + 1$.

22. Zij $K \subset L$ een kwadratische uitbreiding. Bewijs: $K \subset L$ is normaal.

23. Laat L een kwadratische uitbreiding zijn van een lichaam K van karakteristiek verschillend van 2. Bewijs: $L \cong K(\sqrt{x}) \cong K[X]/(X^2 - x)$ voor zekere $x \in K$. Laat zien dat de aanname op de karakteristiek niet weggelaten kan worden.

24. Laat $K \subset L \subset M$ een toren van eindige uitbreidingen zijn. Geef voor elk van de volgende uitspraken een bewijs of een tegenvoorbeeld:
    a. als $K \subset L$ en $L \subset M$ normaal zijn, dan is $K \subset M$ normaal;
    b. als $K \subset M$ normaal is, dan is $L \subset M$ normaal;
    c. als $K \subset M$ normaal is, dan is $K \subset L$ normaal.

25. Formuleer en bewijs het analogon van 23.4 voor willekeurige algebraïsche uitbreidingen. [Hint: gebruik een ontbindingslichaam $\Omega_K^{\mathcal{F}}$ van een familie van polynomen $\mathcal{F} \subset K[X]$ over K uit opgave 21.37.]

26. Bepaal de graad over $\mathbf{Q}$ van ontbindingslichamen van de volgende polynomen:
$$X^2 + X - 2, \qquad X^2 + 2X - 2, \qquad X^3 + 2X - 2, \qquad X^4 + 2X^2 + 2.$$

27. Definieer de normale afsluiting van een oneindige algebraïsche uitbreiding $K \subset L$, en laat zien dat deze op L-isomorfie na uniek bepaald is.

28. Laat $\phi_1, \phi_2 : X(L/K) \xrightarrow{\sim} \mathrm{Aut}_K(L)$ de identificaties in (23.11) zijn voor keuzes $\tau_1, \tau_2 \in X(L/K)$. Laat zien dat $\phi_2 \cdot \phi_1^{-1} : \mathrm{Aut}_K(L) \to \mathrm{Aut}_K(L)$ gegeven wordt door linksvermenigvuldiging met $\tau_2^{-1}\tau_1 \in \mathrm{Aut}_K(L)$.

29. Laat zien dat in een toren $K \subset L \subset M$ van eindige separabele uitbreidingen de formules $N_{L/K} \circ N_{M/L} = N_{M/K}$ en $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$ gelden.

30. Definieer de spoorafbeelding voor een eindige uitbreiding $K \subset L$ als in 23.18 door $\mathrm{Tr}_{L/K}(x) = \mathrm{spoor}(M_x)$. Bewijs: $\mathrm{Tr}_{L/K} : L \to K$ is een surjectief groepshomomorfisme als $K \subset L$ separabel is, en de nulafbeelding als $K \subset L$ inseparabel is.

31. Definieer de normafbeelding voor een eindige uitbreiding $K \subset L$ als in 23.18 door $N_{L/K}(x) = \det(M_x)$. Bewijs: $N_{L/K}(x) = N_{K_s/K}(x)^i$ met K_s de separabele afsluiting van K in L en i de inseparabiliteitsgraad van L over K.

24 Galoistheorie

Voor een grote klasse van lichaamsuitbreidingen $K \subset L$ kan men de collectie van tussenlichamen (en hun inclusies) eenvoudig beschrijven in termen van de groep

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \sigma|_K = \mathrm{id}_K\}$$

van lichaamsautomorfismen van L die op K de identiteit zijn. Deze observatie, die teruggaat op Galois (1810–1831), stelt ons in staat met behulp van groepentheorie problemen aan te pakken waarbij dat op het eerste gezicht niet voor de hand ligt.

▶ Galoisuitbreidingen

De grondgedachte van de Galoistheorie is dat men met behulp van de automorfismen van een lichaam L de deellichamen van L in kaart brengt. Voor iedere collectie $G \subset \mathrm{Aut}(L)$ van automorfismen van L heeft men een bijbehorend *invariantenlichaam*

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

Men gaat gemakkelijk na dat dit een deellichaam van L is. Het bevat het priemlichaam van L, dat geen niet-triviale automorfismen toelaat. Merk op dat L^G niet verandert als we G vervangen door de ondergroep $\langle G\rangle \subset \mathrm{Aut}(L)$ voortgebracht door G. We kunnen ons daarom beperken tot invariantenlichamen van *ondergroepen* $G \subset \mathrm{Aut}(L)$.

24.1. Definitie. *Een eindige uitbreiding $K \subset L$ heet Galois als er een ondergroep $G \subset \mathrm{Aut}(L)$ van automorfismen van L bestaat met invariantenlichaam $L^G = K$.*

In de situatie van 24.1 noemen we $K \subset L$ een *eindige Galoisuitbreiding* met *Galoisgroep* G. De groep G in 24.1, die zoals we dadelijk zullen zien eindig is, en uniek bepaald is door de uitbreiding $K \subset L$, wordt genoteerd als $G = \mathrm{Gal}(L/K)$.

Oneindige Galoisuitbreidingen bestaan ook, en men krijgt ze door in 24.1 het woord 'eindig' door 'algebraïsch' te vervangen. Oneindige uitbreidingen $L^G \subset L$ blijken namelijk niet automatisch algebraïsch te zijn (opgave 8), en zelfs in het algebraïsche geval kunnen verschillende oneindige groepen $G \subset \mathrm{Aut}(L)$ aanleiding geven tot hetzelfde invariantenlichaam (opgave 57). Een correcte formulering van de theorie, zoals we die in §28 geven, blijkt enige topologie te vereisen.

24.2. Voorbeeld. Iedere kwadratische uitbreiding $\mathbf{Q} \subset L = \mathbf{Q}(\sqrt{d})$ met $d \in \mathbf{Q}$ niet een kwadraat is Galois. Immers, definieer $\sigma \in \mathrm{Aut}(\mathbf{Q}(\sqrt{d}))$ door

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Dan is de automorfismengroep $G = \langle\sigma\rangle$ cyclisch van orde 2, en het invariantenlichaam L^G is gelijk aan het grondlichaam $\mathbf{Q}$.

Algemener geven ontbindingslichamen van separabele polynomen Galoisuitbreidingen.

24.3. Lemma. *Laat $K \subset L$ een eindige uitbreiding zijn die normaal en separabel is. Dan is $K \subset L$ Galois met groep $G = \mathrm{Aut}_K(L)$.*

Bewijs. Het is voldoende te laten zien dat $K = L^G$ geldt voor $G = \mathrm{Aut}_K(L)$. De inclusies $K \subset L^G \subset L$ zijn duidelijk, dus het is voldoende te laten zien dat $[L : L^G] \geq [L : K]$ geldt. De normaliteit en separabiliteit van $K \subset L$ geven precies de gelijkheden $\#G = \#\mathrm{Aut}_K(L) = \#X(L/K) = [L : K]_s = [L : K]$, dus er zijn ten minste $[L : K]$ automorfismen van L over L^G. Met behulp van 23.4 volgt de ongelijkheid $[L : L^G] \geq [L : K]$. □

Opgave 1. Bewijs de gelijkheid $L^G = K$ door voor $\alpha \in L \setminus K$ een automorfisme $\sigma \in \mathrm{Aut}_K(L)$ aan te geven met $\sigma(\alpha) \neq \alpha$.

▶ Hoofdstelling

Voor een eindige Galoisuitbreiding $K \subset L$ is er de volgende *Galoiscorrespondentie* tussen ondergroepen van $\mathrm{Gal}(L/K)$ en tussenlichamen van $K \subset L$.

24.4. Hoofdstelling. *Zij $K \subset L$ een eindige Galoisuitbreiding met Galoisgroep G. Dan gelden de volgende uitspraken.*

1. *De uitbreiding $K \subset L$ is normaal en separabel. De Galoisgroep G is eindig van orde $[L : K]$ en gelijk aan $G = \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.*
2. *Er is een inclusie-omkerende bijectie, de Galoiscorrespondentie*

$$\begin{array}{rccc} \psi_{L/K} : & \mathcal{E}_{L/K} = \{E : K \subset E \subset L\} & \xrightarrow{\sim} & \mathcal{H}_G = \{H : H \subset G = \mathrm{Aut}_K(L)\} \\ & E & \longmapsto & \mathrm{Aut}_E(L), \end{array}$$

   tussen de verzameling $\mathcal{E}_{L/K}$ van tussenlichamen van $K \subset L$ en de verzameling $\mathcal{H}_G$ van ondergroepen van G. De inverse is $\psi_{L/K}^{-1} : H \mapsto L^H$.
3. *Zij $H = \psi_{L/K}(E)$. Dan is de uitbreiding $E \subset L$ Galois met groep H; er geldt*

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

   Voor iedere $\sigma \in G$ correspondeert het met E geconjugeerde lichaam $\sigma[E] \in \mathcal{E}_{L/K}$ onder $\psi_{L/K}$ met de met H geconjugeerde ondergroep $\sigma H \sigma^{-1}$.
4. *Een tussenlichaam $E \in \mathcal{E}_{L/K}$ is normaal over K dan en slechts dan als de ondergroep $H = \psi_{L/K}(E)$ normaal is in G; voor dergelijke E is de uitbreiding $K \subset E$ Galois en is*

$$\begin{array}{ccc} G/H & \xrightarrow{\sim} & \mathrm{Gal}(E/K) \\ \sigma H & \longmapsto & \sigma|_E \end{array}$$

   een groepsisomorfisme.

Vergelijken we de uitspraken in 24.3 en 24.4.1, dan zien we hoe Galoisuitbreidingen in termen van de vorige paragraaf beschreven kunnen worden.

24.5. Gevolg. *Voor een eindige uitbreiding $K \subset L$ geldt:*

$$K \subset L \text{ is Galois} \iff K \subset L \text{ is normaal en separabel.}$$ □

Oudere bewijzen van 24.4 nemen vaak 24.5 als *definitie* van Galois en de gelijkheid voor G in 24.4.1 als de definitie van de Galoisgroep. Men kan dan met 23.9 een primitief element x voor L/K kiezen en G verder als permutatiegroep op de nulpunten van $f = f_K^x$ beschouwen. In deze aanpak ziet men een Galoisuitbreiding van K als een ontbindingslichaam $L = \Omega_K^f$ van een irreducibel separabel polynoom $f \in K[X]$. Onze aanpak, die teruggaat op E. Artin, is iets anders. Hij leidt de hoofdstelling af uit het lemma van Artin-Dedekind uit de vorige paragraaf.

▶ Bewijs van de hoofdstelling

Zij $K \subset L$ een eindige Galoisuitbreiding met Galoisgroep $G \subset \mathrm{Aut}_K(L)$, en vat $\mathrm{Aut}_K(L)$ op als deelverzameling van $X(L/K)$ door een inclusie $L \subset \overline{K}$ te kiezen. Dan hebben we wegens 23.4 de ongelijkheden $\#G \leq \#X(L/K) = [L:K]_s \leq [L:K]$, en de kern van het het bewijs bestaat uit het bewijzen van de omgekeerde ongelijkheid $[L:K] \leq \#G$.

Laat G orde n hebben, en stel dat er $m > n$ elementen $\omega_1, \omega_2, \ldots, \omega_m \in L$ zijn die lineair onafhankelijk zijn over $K = L^G$. Dan zijn de m vectoren $v_i = (\sigma(\omega_i))_{\sigma\in G} \in L^n$ voor $i = 1, 2, \ldots, m$ lineair afhankelijk over L. Laat $\sum_{i=1}^m c_i v_i = 0$ een niet-triviale relatie met coëfficiënten $c_i \in L$ zijn. Voor iedere $\sigma \in G$ hebben we dan een relatie $\sum_{i=1}^m c_i \sigma(\omega_i) = 0$. Passen we σ^{-1} toe op deze relatie, dan volgt $\sum_{i=1}^m \sigma^{-1}(c_i)\omega_i = 0$ voor iedere $\sigma \in G$. Sommeren we deze relaties voor alle $\sigma \in G$, dan krijgen we

$$\textstyle\sum_{i=1}^m b_i\omega_i = 0 \qquad \text{met} \quad b_i = \sum_{\sigma\in G} \sigma(c_i).$$

Merk hierbij op dat als σ over G loopt, de inversen σ^{-1} dit ook doen. Om eenzelfde reden zijn de elementen $b_i \in L$ alle bevat in het invariantenlichaam $K = L^G$. Immers, voor $\tau \in G$ loopt $\tau\sigma$ over G als σ over G loopt, en dus geldt voor alle $\tau \in G$

$$\tau(b_i) = \textstyle\sum_{\sigma\in G} \tau\sigma(c_i) = \sum_{\sigma\in G} \sigma(c_i) = b_i.$$

Omdat de elementen ω_i lineair onafhankelijk over K zijn volgt $b_i = \sum_{\sigma\in G} \sigma(c_i) = 0$ voor $i = 1, 2, \ldots, m$. Onder de coëfficiënten c_i in de afhankelijkheidsrelatie kan men echter ieder voorgeschreven element $x \in L^*$ voor laten komen: kies een i met $c_i \neq 0$, en vermenigvuldig de relatie met xc_i^{-1}. We zien dat de afbeelding $L \to L$ gegeven door $x \mapsto \sum_{\sigma\in G} \sigma(x)$ de nulafbeelding is. Dit is in tegenspraak met 23.15, dus er geldt $[L:K] \leq \#G$.

We concluderen dat

$$G = \mathrm{Aut}_K(L) = X(L/K) \tag{24.6}$$

geldt. Hieruit volgt direct 24.4.1. Immers, de eerste gelijkheid laat zien dat G van de gestelde vorm is. De tweede gelijkheid $\mathrm{Aut}_K(L) = X(L/K)$ drukt uit dat alle inbeddingen van L in $\overline{K}$ hetzelfde beeld hebben, zodat $K \subset L$ een normale uitbreiding is. Omdat verder $X(L/K)$ cardinaliteit $\#G = [L:K]$ heeft, is $K \subset L$ bovendien separabel.

Nu we eenmaal de fundamentele eigenschap 24.4.1 van Galoisuitbreidingen bewezen hebben is het verdere bewijs van de hoofdstelling 24.4 een tamelijk eenvoudige verificatie. Is H een ondergroep van G, dan is L^H een tussenlichaam van $K \subset L$, en $L^H \subset L$ is per definitie eindig Galois. Uit 24.4.1 volgt dat $\psi_{L/K}(L^H) = \mathrm{Aut}_{L^H}(L)$ gelijk is aan H, dus de afbeelding $\mathcal{H}_G \longrightarrow \mathcal{E}_{L/K} \overset{\psi_{L/K}}{\longrightarrow} \mathcal{H}_G$ gegeven door $H \mapsto L^H \mapsto \mathrm{Aut}_{L^H}(L)$ is de identiteit op $\mathcal{H}_G$. Omgekeerd is voor ieder tussenlichaam E van $K \subset L$ de eindige uitbreiding $E \subset L$ separabel en normaal, dus Galois met groep $H = \mathrm{Aut}_E(L)$ van orde $\#H = [L : E]$. De gelijkheid $L^H = E$ zegt precies dat de afbeelding $\mathcal{E}_{L/K} \overset{\psi_{L/K}}{\longrightarrow} \mathcal{H}_G \longrightarrow \mathcal{E}_{L/K}$ gegeven door $E \mapsto \mathrm{Aut}_E(L) = H \mapsto L^H$ de identiteit is op $\mathcal{E}_{L/K}$. Het is duidelijk dat $\psi_{L/K}$ en $\psi_{L/K}^{-1}$ inclusies omkeren. Dit bewijst 24.4.2.

Door voor $H = \psi_{L/K}(E)$ de orde $\#H = [L : E]$ te delen op $\#G = [L : K]$ krijgen we de relatie $[G : H] = [E : K]$. Voor $\sigma \in G$ geeft het lichaamsisomorfisme $E \xrightarrow{\sim} \sigma[E] \subset L$ aanleiding tot een groepsisomorfisme $\mathrm{Aut}_E(L) \xrightarrow{\sim} \mathrm{Aut}_{\sigma[E]}(L)$ gegeven door $\tau \mapsto \sigma\tau\sigma^{-1}$: een eenvoudige verificatie. In het bijzonder zien we dat $\sigma[E]$ met de geconjugeerde ondergroep $\sigma H \sigma^{-1}$ correspondeert. Dit bewijst 24.4.3.

Omdat de restrictie-afbeelding $G = X(L/K) \to X(E/K)$ surjectief is, volgt dat alle inbeddingen $E \to \overline{K}$ hetzelfde beeld hebben dan en slechts dan als $\sigma[E] = E$ geldt voor alle $\sigma \in G$. Dit betekent dat $\sigma H \sigma^{-1} = H$ geldt voor de corresponderende ondergroep $H \subset G$, dus we zien dat $K \subset E$ normaal is dan en slechts dan als $H = \psi_{L/K}(E)$ normaal is in G. Als de uitbreiding $K \subset E$ normaal is, dan is hij ook Galois, want ieder tussenlichaam is automatisch separabel over K. In dit geval geeft de surjectie $X(L/K) \to X(E/K)$ aanleiding tot een surjectief groepshomomorfisme $G \to \mathrm{Gal}(E/K)$ gegeven door $\sigma \mapsto \sigma|_E$. De kern hiervan is H, dus de isomorfiestelling geeft een groepsisomorfisme $G/H \xrightarrow{\sim} \mathrm{Gal}(E/K)$. Dit bewijst 24.4.4 en besluit het bewijs. □

▶ Galoisgroep van een polynoom

De hoofdstelling vertelt ons dat met iedere eindige uitbreiding $K \subset L$ die normaal en separabel is, een eindige groep $\mathrm{Gal}(L/K)$ intrinsiek verbonden is. Eigenschappen van de groep 'zijn' eigenschappen van de uitbreiding, en men noemt een Galoisuitbreiding dan ook kortweg abels (cyclisch, oplosbaar, ...) als de bijbehorende Galoisgroep deze eigenschap heeft.

Wegens 23.14 is een eindige Galoisuitbreiding L van K op te vatten als een ontbindingslichaam Ω_K^f van een separabel polynoom $f \in K[X]$, dat op grond van 23.9 irreducibel gekozen kan worden. De Galoisgroep $G = \mathrm{Gal}(L/K)$ wordt dan ook wel de Galoisgroep $\mathrm{Gal}(f)$ van het *polynoom* $f \in K[X]$ over K genoemd. Omdat ieder element $\sigma \in G$ vastligt door zijn werking op de nulpunten van f in $L = \Omega_K^f$, geeft dit een beschrijving van G als een permutatiegroep op de nulpunten van f. Heeft f graad n, dan kan men op deze manier $\mathrm{Gal}(f)$ als een ondergroep van de permutatiegroep S_n op n elementen opvatten. Omdat een gegeven uitbreiding $K \subset L$ meestal als een ontbindingslichaam van heel veel verschillende polynomen opgevat kan worden, is deze representatie weinig kanoniek. Zo kan men de kwadratische uitbreiding $\mathbf{F}_3 \subset \mathbf{F}_9$ als in 22.1 zien als een ontbindingslichaam van het separabele polynoom $X^9 - X \in \mathbf{F}_3[X]$.

Kleinere polynomen in $\mathbf{F}_3[X]$ als X^2+1 en X^2-X-1 geven echter hetzelfde ontbindingslichaam.

Opgave 2. Beschrijf de inbeddingen $\mathrm{Gal}(f) \subset S_2$ en $\mathrm{Gal}(f) \subset S_9$ voor $f = X^2 - X - 1$ en $f = X^9 - X \in \mathbf{F}_3[X]$.

De opgave om bij een separabel polynoom $f \in K[X]$ de Galoisgroep $\mathrm{Gal}(f)$ over K te bepalen is niet eenvoudig, en ook in het speciale geval $K = \mathbf{Q}$ al niet-triviaal. Het vermoeden dat voor het grondlichaam $K = \mathbf{Q}$ *iedere* eindige groep als Galoisgroep van een polynoom $f \in \mathbf{Q}[X]$ optreedt is vooralsnog onbewezen: dit is het *omkeerprobleem*[6] van de Galoistheorie.

Een belangrijke stap in de bepaling van $\mathrm{Gal}(f)$ is de bepaling van de graad van het lichaam Ω_K^f verkregen door adjunctie van de nulpunten van f aan K. Deze graad is gelijk aan de orde van $G = \mathrm{Gal}(L/K)$. De groep G is via zijn werking op de nulpunten van f als een eindige permutatiegroep op te vatten. In het fundamentele geval dat f irreducibel is van graad n treden niet alle ondergroepen van S_n als Galoisgroep op.

24.7. Stelling. *Zij $f \in K[X]$ een irreducibel separabel polynoom met nulpunten $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$, en vat $G = \mathrm{Gal}(f) = \mathrm{Gal}(K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K)$ via zijn werking op de nulpunten van f op als ondergroep van S_n. Dan is G een transitieve ondergroep van S_n, en $\#G$ is een deler van $n!$ die deelbaar is door n.*

Bewijs. Omdat f irreducibel is, bestaat er voor $i, j \in \{1, 2, \ldots, n\}$ een isomorfisme $\varphi : K(\alpha_i) \xrightarrow{\sim} K(\alpha_j)$ dat α_i naar α_j stuurt. Passen we voor dit isomorfisme 21.17 toe met $f_1 = f_2 = f$, dan zien we dat φ voortgezet kan worden tot een automorfisme σ van $L = \Omega_K^f = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Er geldt $\sigma(\alpha_i) = \alpha_j$, dus G werkt transitief op de nulpunten van f. De stabilisator van α_1 in G heeft index n in G wegens 5.3. Er volgt dat de orde van G, die een deler is van $\#S_n = n!$, deelbaar is door n. □

Opgave 3. Bewijs dat $\mathrm{Gal}(f)$ transitief werkt op de nulpunten van een separabel polynoom $f \in K[X]$ dan en slechts dan als f irreducibel is.

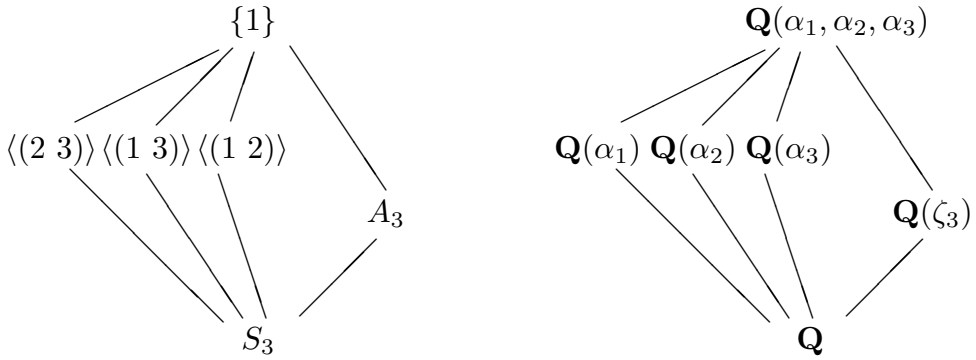
Met het oog op bovenstaande stelling is het interessant om voor gegeven n te bepalen welke (isomorfietypen van) transitieve ondergroepen S_n heeft. Voor $n \leq 5$ is dit niet al te veel werk (opgaven 44–45), voor iets grotere n kan men gebruik maken van de lijsten die sommige computeralgebra-pakketten leveren.[7] De complexiteit van het probleem groeit echter nogal snel met n.

▶ Twee voorbeelden

We bepalen, mede als illustratie van de uitspraken van de hoofdstelling, de Galoisgroepen van de polynomen $X^3 - 2$ en $X^4 - 2$ in $\mathbf{Q}[X]$.

Voor $f = X^3 - 2$ construeerden we een ontbindingslichaam $L = \Omega_{\mathbf{Q}}^{X^3-2}$ op twee manieren in 21.15. We kunnen L als deellichaam van $\mathbf{C}$ opvatten door een reële derdemachtswortel $\sqrt[3]{2}$ en een primitieve derde eenheidswortel $\zeta_3 \in \mathbf{C}$ te nemen: dan geldt $L = \mathbf{Q}(\zeta_3, \sqrt[3]{2})$, en $X^3 - 2$ heeft nulpunten $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$ en $\alpha_3 = \zeta_3^2\sqrt[3]{2}$. De Galoisgroep $\mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbf{Q})$ is via zijn werking op de nulpunten van f een ondergroep van S_3. Omdat we in 21.15 al $[L : \mathbf{Q}] = 6$ vonden, geldt $\#\mathrm{Gal}(f) = 6$ en

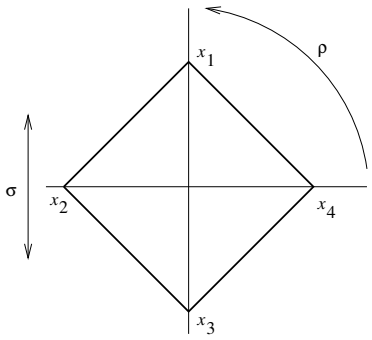
$\mathrm{Gal}(L/\mathbf{Q}) \cong S_3$. Het *rooster* van ondergroepen van S_3 is niet moeilijk te vinden, en het correspondeert met het afgebeelde rooster van deellichamen van $\mathbf{Q} \subset L$. Merk op dat de inclusies in het linker- en rechterdiagram in tegenovergestelde richting lopen.



We zien dat er geen andere tussenlichamen dan de 'voor de hand liggende' zijn. De drie niet-normale uitbreidingen $\mathbf{Q} \subset \mathbf{Q}(\alpha_i)$ corresponderen met de niet-normale ondergroepen van orde 2 in S_3. De isomorfe lichamen $\mathbf{Q}(\alpha_i)$ zijn geconjugeerd over $\mathbf{Q}$, de ondergroepen van orde 2 zijn geconjugeerd in S_3. Het kwadratische lichaam $\mathbf{Q}(\zeta_3)$, dat wel normaal is over $\mathbf{Q}$, correspondeert met de normale ondergroep $A_3 \lhd S_3$. De uitbreiding $\mathbf{Q} \subset \mathbf{Q}(\zeta_3)$ is Galois, en $\mathrm{Gal}(\mathbf{Q}(\zeta_3)/\mathbf{Q}) \cong S_3/A_3$ is cyclisch van orde 2.

Opgave 4. Bewijs: voor ieder irreducibel polynoom $f = X^3 - k \in \mathbf{Q}[X]$ geldt $\mathrm{Gal}(f) \cong S_3$.

We bepalen vervolgens de ondergroep $G \subset S_4$ die optreedt als Galoisgroep over $\mathbf{Q}$ van het irreducibele polynoom $f = X^4 - 2 \in \mathbf{Q}[X]$. We kunnen als in het vorige geval de nulpunten van f in $\mathbf{C}$ gebruiken. Is $x = \sqrt[4]{2}$ de positieve reële vierdemachtswortel uit 2, dan krijgen we de andere nulpunten van f door x te vermenigvuldigen met de machten van $i = \sqrt{-1}$. Met $x_k = i^k x$ voor $k \in \mathbf{Z}$ hebben we $\Omega^f_{\mathbf{Q}} = \mathbf{Q}(x_1, x_2, x_3, x_4) = \mathbf{Q}(x, i)$, waar $x = x_4 = \sqrt[4]{2}$ als boven. Dit is een uitbreiding van graad 8, want $i = \sqrt{-1}$ is niet bevat in het reële lichaam $\mathbf{Q}(x)$. De groep $\mathrm{Gal}(f)$ is kennelijk een ondergroep van orde 8 van S_4. Niet alle permutaties van de nulpunten van f worden dus door automorfismen van $L = \Omega^f_{\mathbf{Q}}$ gerealiseerd. Wegens $x_3 = -x_1$ en $x_4 = -x_2$ is dit geen verrassing.

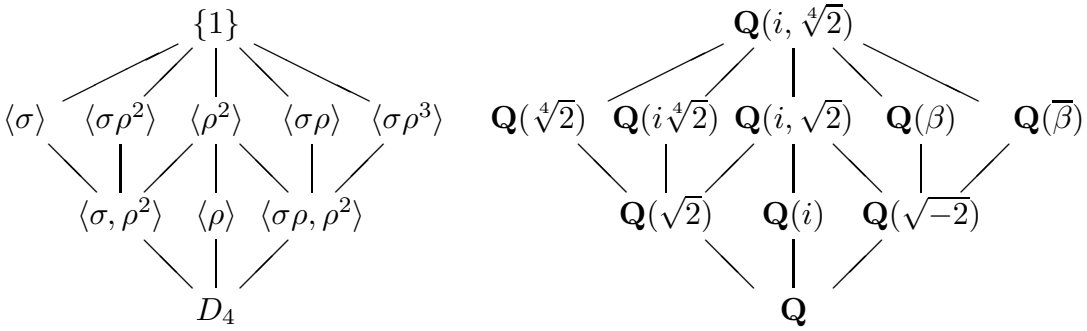


Wie S_4 kent uit 10.11 weet dat de ondergroepen van orde 8 in S_4 de 2-Sylowgroepen zijn, en dat deze isomorf zijn met de dihedrale groep D_4. Men kan echter de isomorfie $\mathrm{Gal}(L/\mathbf{Q}) \cong D_4$ zelf ontdekken door σ de complexe conjugatie op L te laten zijn en $\rho : L \to L$ een automorfisme dat voldoet aan $\rho(x_1) = x_2 = ix_1$. Door eventueel ρ door

$\sigma\rho$ te vervangen mogen we aannemen dat $\rho(i) = i$ geldt, en dus $\rho(x_k) = x_{k+1}$. De actie van ρ en σ op de nulpunten van f, in het complexe vlak getekend als de hoekpunten van een vierkant, zijn dan respectievelijk de kwartslag en de spiegeling in de reële as. Bedenk wel dat ρ niet op $\mathbf{Q}(x_1, x_2, x_3, x_4) \subset \mathbf{C}$ als kwartslag werkt!

Al uit 1.4 weten we dat de kwartslag ρ en de spiegeling σ de groep D_4 voortbrengen. Deze kennis is ook behulpzaam bij het maken van het rooster van ondergroepen van D_4. Het centrumelement ρ^2 en de vier spiegelingen $\sigma\rho^k$ brengen elk een ondergroep van orde 2 voort. De ondergroepen van D_4 van orde 4 zijn de ondergroepen voortgebracht door ρ^2 en een spiegeling – deze zijn isomorf met de viergroep van Klein V_4 – en de unieke cyclische ondergroep $\langle\rho\rangle$ van orde 4.

Tussenlichamen behorende bij de diverse ondergroepen van $\mathrm{Gal}(L/\mathbf{Q}) \cong D_4$ vindt men door voor de hand liggende deellichamen op te schrijven en – indien dit niet alle tussenlichamen zijn – invariante elementen in termen van de x_k te construeren.



Deellichamen van graad 4 zijn $\mathbf{Q}(x_4) = \mathbf{Q}(x_2) = \mathbf{Q}(\sqrt[4]{2})$ en $\mathbf{Q}(x_3) = \mathbf{Q}(x_1) = \mathbf{Q}(i\sqrt[4]{2})$. De niet-triviale symmetrieën van orde 2 die de bijbehorende hoekpunten van het vierkant vasthouden zijn de complexe conjugatie σ en het automorfisme $\sigma\rho^2$ dat x_1 en x_3 vasthoudt. Het lichaam $\mathbf{Q}(\sqrt{2})$ voortgebracht door het kwadraat van een nulpunt van f is invariant onder beide genoemde symmetrieën: het is de doorsnede van $\mathbf{Q}(\sqrt[4]{2})$ en $\mathbf{Q}(i\sqrt[4]{2})$, en hoort bij de ondergroep van D_4 voortgebracht door σ en ρ^2.

Het lichaam $\mathbf{Q}(i)$ is invariant onder ρ, dus het hoort bij de ondergroep $\langle\rho\rangle$ van orde 4. Het *compositum* $\mathbf{Q}(i, \sqrt{2})$ van $\mathbf{Q}(i)$ en $\mathbf{Q}(\sqrt{2})$ behoort bij de doorsnede $\langle\rho^2\rangle$ van $\langle\rho\rangle$ en $\langle\sigma, \rho^2\rangle$. Dit lichaam bevat het deellichaam $\mathbf{Q}(\sqrt{-2})$, en omdat x_1x_4 een wortel uit -2 is, is het niet moeilijk in te zien dat ρ^2 en de spiegelingen $\sigma\rho$ en $\sigma\rho^3$ dit lichaam invariant laten.

We blijken nog twee lichamen van graad 4 te missen, behorende bij de groepen voortgebracht door elk van beide zojuist genoemde spiegelingen. Omdat $\sigma\rho$ de elementen x_1 en x_2 verwisselt is $\beta = x_1 + x_2 = (-1 + i)\sqrt[4]{2}$ een element van het bijbehorende invariantenlichaam. Er geldt $\beta^2 = -2\sqrt{-2}$, dus $\mathbf{Q}(\beta)$ bevat $\mathbf{Q}(\sqrt{-2})$. Wegens $\rho^2(\beta) = -\beta$ ligt β niet in $\mathbf{Q}(\sqrt{-2})$, dus $\mathbf{Q}(\beta)$ is het lichaam van graad 4 behorende bij $\langle\sigma\rho\rangle$. De ondergroep $\langle\sigma\rho\rangle$ gaat onder conjugatie met σ over in $\langle\sigma\rho^3\rangle$. Het lichaam behorende bij $\langle\sigma\rho^3\rangle$ is daarom het lichaam $\sigma[\mathbf{Q}(\beta)] = \mathbf{Q}(\overline{\beta})$ voortgebracht door de complex geconjugeerde $\overline{\beta} = (-1 - i)\sqrt[4]{2}$ van β. We hebben $f^{\beta}_{\mathbf{Q}} = X^4 + 8$.

De lezer mag als oefening zelf nagaan welke tussenlichamen van $\mathbf{Q} \subset L$ normaal zijn over $\mathbf{Q}$, en wat de bijbehorende Galoisgroepen zijn.

▶ Cyclische uitbreidingen

Een eindige Galoisuitbreiding $K \subset L$ heet *cyclisch* als $\mathrm{Gal}(L/K)$ een cyclische groep is. Voor cyclische groepen is het rooster van ondergroepen bijzonder eenvoudig te beschrijven. Immers, als $G = \langle x \rangle$ een cyclische groep van orde n is met voortbrenger x, dan heeft voor iedere deler $d|n$ de ondergroep $\langle x^d \rangle \subset G$ index d in G. Omgekeerd bevat iedere ondergroep $H \subset G$ van index $d|n$ het element x^d, immers $x^d \bmod H$ is het eenheidselement in G/H, dus er geldt $H = \langle x^d \rangle$. We concluderen dat G voor iedere deler $d|n$ een unieke ondergroep $H_d \subset G$ van index d heeft. De bijbehorende factorgroep G/H_d is ook weer cyclisch en van orde d.

Opgave 5. Is omgekeerd iedere groep van orde n die voor elke deler $d|n$ een unieke ondergroep van index d heeft een cyclische groep?

Voor cyclische lichaamsuitbreidingen krijgen we het volgende resultaat.

24.8. Stelling. *Zij $K \subset L$ een cyclische Galoisuitbreiding van graad n. Dan is er voor iedere deler $d|n$ een uniek tussenlichaam K_d van $K \subset L$ van graad d over K. De uitbreiding $K \subset K_d$ is cyclisch van graad d.* □

24.9. Voorbeeld. Iedere uitbreiding $K \subset L$ van eindige lichamen is cyclisch, en in dit speciale geval bewezen we de Galoiscorrespondentie al in 22.12. Schrijven we $K = \mathbf{F}_q$ en $L = \mathbf{F}_{q^n}$, dan hebben we

$$\mathrm{Gal}(L/K) = \langle F_K \rangle \cong \mathbf{Z}/n\mathbf{Z}$$

met $F_K : L \to L$ het *Frobeniusautomorfisme* behorende bij het grondlichaam $K = \mathbf{F}_q$ gedefinieerd door $F_K(x) = x^q$. Voor iedere deler d van de graad $n = [L : K]$ van de uitbreiding is $K_d = \mathbf{F}_{q^d}$ het tussenlichaam van graad d over K. Het behoort bij de ondergroep $\langle F_K^d \rangle$ van index d in $\mathrm{Gal}(L/K)$.

Over $\mathbf{Q}$ is het in 21.8.3 gedefinieerde p-de cyclotomische lichaam een voorbeeld van een cyclische uitbreiding.

24.10. Stelling. *Zij p een priemgetal en $\zeta_p \in \overline{\mathbf{Q}}$ een nulpunt van Φ_p. Dan geldt:*

1. *Voor ieder element $k \in (\mathbf{Z}/p\mathbf{Z})^*$ is er een automorfisme $\sigma_k \in \mathrm{Aut}(\mathbf{Q}(\zeta_p))$ met $\sigma_k(\zeta_p) = \zeta_p^k$, en de afbeelding*

$$\begin{aligned} \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) &\xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^* \\ [\sigma_k : \zeta_p \mapsto \zeta_p^k] &\longmapsto (k \bmod p) \end{aligned}$$

   is een isomorfisme van cyclische groepen van orde $p-1$.

2. *Voor iedere deler $d|p-1$ is er een uniek deellichaam $K_d \subset \mathbf{Q}(\zeta_p)$ met $[K_d : \mathbf{Q}] = d$. Is $H_d \subset (\mathbf{Z}/p\mathbf{Z})^*$ de ondergroep van index d in $(\mathbf{Z}/p\mathbf{Z})^*$, dan geldt $K_d = \mathbf{Q}(\eta_d)$ met*

$$\eta_d = \sum_{k \in H_d} \zeta_p^k.$$

Het element η_d in 24.10.2 heet een *Gauss-periode van graad d* in $\mathbf{Q}(\zeta_p)$. Het *aantal* termen van η_d is $\frac{p-1}{d}$.

Bewijs. Het lichaam $\mathbf{Q}(\zeta_p)$ is als ontbindingslichaam van het irreducibele polynoom Φ_p een eindige Galoisuitbreiding van $\mathbf{Q}$. Ieder automorfisme $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ ligt vast door zijn werking op de *groep* $\mu_p = \langle\zeta_p\rangle$ van p-de eenheidswortels, en omdat de automorfismen van μ_p de k-de machtsverheffingen $\sigma_k : \zeta_p \mapsto \zeta_p^k$ zijn met $p \nmid k$ geeft dit aanleiding tot een injectief homomorfisme

$$\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_p) = (\mathbf{Z}/p\mathbf{Z})^*.$$

Wegens 24.7 worden alle mogelijkheden $k \bmod p$ door elementen van $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ gerealiseerd, dus deze afbeelding is een isomorfisme. We weten uit 7.7 en 12.5 dat $(\mathbf{Z}/p\mathbf{Z})^*$ cyclisch is.

De eerste uitspraak in (2) is een speciaal geval van 24.8. Om te laten zien dat de Gauss-periode η_d behorende bij de ondergroep $H_d \subset (\mathbf{Z}/p\mathbf{Z})^*$ van index d het invariantenlichaam $K_d = \mathbf{Q}(\zeta_p)^{H_d}$ voortbrengt merken we op dat het element σ_a werkt op η_d door

$$\sigma_a(\eta_d) = \textstyle\sum_{k\in H_d} \zeta_p^{ak} = \sum_{k\in aH_d} \zeta_p^k.$$

Voor $a \in H_d$ geldt $aH_d = H_d$ en $\sigma_a(\eta_d) = \eta_d$, dus er geldt $\eta_d \in K_d$. Omdat de elementen ζ_p^k voor $k \in \{1, 2, \ldots, p-1\}$ lineair onafhankelijk zijn over $\mathbf{Q}$ – ze vormen immers een basis voor $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ – zijn de elementen $\sigma_a(\eta_d)$ behorende bij verschillende restklassen aH_d ook weer verschillend. Dit laat zien dat η_d precies $d = [(\mathbf{Z}/p\mathbf{Z})^* : H_d]$ geconjugeerden heeft binnen $\mathbf{Q}(\zeta_p)$. Het lichaam $\mathbf{Q}(\eta_d)$ is daarom van graad d over $\mathbf{Q}$, en we vinden $\mathbf{Q}(\eta_d) = K_d$. □

Het bewijs van 24.10 maakt gebruik van het feit dat $\mathbf{Q}(\zeta_p)$ een $\mathbf{Q}$-basis heeft die bestaat uit de geconjugeerden van het element ζ_p. Algemener noemt men een K-basis voor een Galoisuitbreiding $K \subset L$ bestaande uit de verzameling $\{\sigma(x)\}_{\sigma\in\mathrm{Gal}(L/K)}$ van geconjugeerden van een element $x \in L$ een *normale basis* van L over K.

24.11. Voorbeeld. Voor $p = 7$ geldt $p - 1 = 6$, dus de niet-triviale deellichamen van $\mathbf{Q}(\zeta_7)$ hebben graad 2 en 3 over $\mathbf{Q}$. De corresponderende ondergroepen van index 2 en 3 in $(\mathbf{Z}/7\mathbf{Z})^*$ zijn $H_2 = \langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}\}$ en $H_3 = \langle-\overline{1}\rangle$. Met $\zeta = \zeta_7$ krijgen we $\eta_2 = \zeta + \zeta^2 + \zeta^4$ en $\eta_3 = \zeta + \zeta^{-1}$ als voortbrengers voor $K_2 = \mathbf{Q}(\eta_2)$ en $K_3 = \mathbf{Q}(\eta_3)$. De kwadratische periode η_2 heeft een geconjugeerde $\sigma_{-1}(\eta_2) = \zeta^{-1} + \zeta^{-2} + \zeta^{-4} = \zeta^6 + \zeta^5 + \zeta^3$, en een korte berekening geeft het polynoom

$$f_{\mathbf{Q}}^{\eta_2} = (X - \eta_2)(X - \sigma_{-1}(\eta_2)) = X^2 + X + 2$$

met nulpunten $\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$. We vinden $K_2 = \mathbf{Q}(\sqrt{-7})$.

De kubische Gauss-periode $\eta_3 = \zeta + \zeta^{-1}$ heeft geconjugeerden $\sigma_2(\eta_3) = \zeta^2 + \zeta^{-2}$ en $\sigma_3(\eta_3) = \zeta^3 + \zeta^{-3}$. Uitvermenigvuldigen geeft

$$f_{\mathbf{Q}}^{\eta_3} = (X - \eta_3)(X - \sigma_2(\eta_3))(X - \sigma_3(\eta_3)) = X^3 + X^2 - 2X - 1.$$

Opgave 6. Laat zien dat $f_{\mathbf{Q}}^{\eta_3}$ naast η_3 de nulpunten $\eta_3^2 - 2$ en $-\eta_3^2 - \eta_3 + 1$ heeft.

Men kan heel algemeen het kwadratische deellichaam $\mathbf{Q}(\eta_2) \subset \mathbf{Q}(\zeta_p)$ voortgebracht door de kwadratische Gauss-periode aangeven.

24.12. Stelling. *Zij p een oneven priemgetal en η_2 de kwadratische Gauss-periode in $\mathbf{Q}(\zeta_p)$. Dan geldt*

$$f_{\mathbf{Q}}^{\eta_2} = X^2 + X + \frac{1-p^*}{4} \qquad \textit{met } p^* = (-1)^{(p-1)/2}p.$$

In het bijzonder geldt $\mathbf{Q}(\eta_2) = \mathbf{Q}(\sqrt{p^*})$.

Bewijs. Laat $S \subset (\mathbf{Z}/p\mathbf{Z})^*$ de ondergroep van kwadraten in $(\mathbf{Z}/p\mathbf{Z})^*$ zijn, en schrijf $T = (\mathbf{Z}/p\mathbf{Z})^* \setminus S$. Dan zijn $\eta_2 = \sum_{s\in S}\zeta_p^s$ en $\widetilde{\eta}_2 = \sum_{t\in T}\zeta_p^t$ de nulpunten van $f_{\mathbf{Q}}^{\eta_2}$.

Wegens $\eta_2 + \widetilde{\eta}_2 = \sum_{i=1}^{p-1}\zeta_p^i = -1$ is de lineaire coëfficiënt van $f_{\mathbf{Q}}^{\eta_2}$ gelijk aan 1. De constante coëfficiënt $\eta_2\widetilde{\eta}_2 = \sum_{s\in S,t\in T}\zeta_p^{s+t}$ is een som van $\#S\cdot\#T = (\frac{p-1}{2})^2$ eenheidswortels.

Voor $p \equiv 1 \bmod 4$ merken we als in het bewijs van 12.20 op dat $-1 \in S$ geldt, dus met $s \in S$ hebben we $-s \in S$. Voor $s \in S$ en $t \in T$ geldt dan $s + t \neq 0$, dus $\eta_2\widetilde{\eta}_2$ is een som van $(\frac{p-1}{2})^2$ geconjugeerden van ζ_p. Deze geconjugeerden vormen een basis van $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$. Omdat $\eta_2\widetilde{\eta}_2$ rationaal is, en dus invariant onder de werking van de Galoisgroep, betekent dit dat elk van de $p-1$ verschillende eenheidswortels *even vaak* in de som voorkomt: $\frac{p-1}{4}$ maal. We vinden

$$\eta_2\widetilde{\eta}_2 = \tfrac{p-1}{4}\cdot\big(\sum_{i=1}^{p-1}\zeta_p^i\big) = \tfrac{p-1}{4}\cdot(-1) = \tfrac{1-p}{4}.$$

Stel nu $p \equiv -1 \bmod 4$. Dan geldt $-1 \notin S$, dus bij elke $s \in S$ is er een uniek element $t = -s \in T$ met $s + t = 0$. Dit geeft aanleiding tot $\#S = \frac{p-1}{2}$ termen $\zeta_p^0 = 1$ in de som voor $\eta_2\widetilde{\eta}_2$. De overige $(\frac{p-1}{2})^2 - \frac{p-1}{2} = (p-1)\cdot\frac{p-3}{4}$ eenheidswortels in de som zijn geconjugeerden van ζ_p en tellen op tot een rationale som. Als boven concluderen we dat elk van de $p-1$ eenheidswortels $\frac{p-3}{4}$ maal voorkomt. Dit geeft

$$\eta_2\widetilde{\eta}_2 = \tfrac{p-1}{2} + \tfrac{p-3}{4}\cdot(-1) = \tfrac{1+p}{4}.$$

Daar $f_{\mathbf{Q}}^{\eta_2}$ nulpunten $-\frac{1}{2} \pm \frac{1}{2}\sqrt{p^*}$ heeft is de gelijkheid $\mathbf{Q}(\eta_2) = \mathbf{Q}(\sqrt{p^*})$ duidelijk. □

Het element $\tau_p = \eta_2 - \widetilde{\eta}_2$ is de kwadratische *Gauss-som* in $\mathbf{Q}(\zeta_p)$. Het bewijs van 24.12 laat zien dat τ_p een wortel is van $p^* = \pm p \equiv 1 \bmod 4$.

▶ Cyclotomische uitbreidingen

Men kan zich afvragen hoe stelling 24.10 er uitziet voor de uitbreidingen $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ verkregen door adjunctie van een willekeurige eenheidswortel aan $\mathbf{Q}$ of een ander grondlichaam. Dergelijke uitbreidingen, die in de praktijk veelvuldig voorkomen, heten *cyclotomische uitbreidingen*.

Voor een lichaam K heet de torsieondergroep $\mu_K \subset K^*$ van K^* de groep van *eenheidswortels* in K. Deze groep bestaat uit de elementen $x \in K$ waarvoor $x^n = 1$ geldt voor zekere $n \in \mathbf{Z}_{\geq 1}$. We hebben $\mu_{\mathbf{Q}} = \mu_{\mathbf{R}} = \{\pm 1\}$, en $\mu_K = K^*$ voor ieder

eindig lichaam K. Een element $x \in \mu_K$ heet een n-de eenheidswortel als $x^n = 1$ geldt, en een *primitieve* n-de eenheidswortel als de orde van x in K^* gelijk is aan n.

In een lichaam K van karakteristiek $p > 0$ zijn er geen primitieve p-de eenheidswortels, want $X^p - 1$ ontbindt dan als $(X-1)^p$ in $K[X]$. We nemen daarom aan dat $n \geq 1$ niet deelbaar is door de karakteristiek van K. Dit is in het bijzonder het geval voor $\mathrm{char}(K) = 0$. Het polynoom $f = X^n - 1 \in K[X]$ is dan een separabel polynoom, want de afgeleide $f' = nX^{n-1}$ heeft geen nulpunten gemeen met f in een algebraïsche afsluiting $\overline{K}$. Er volgt dat de n verschillende nulpunten van $X^n - 1$ in $\overline{K}$ een ondergroep $\mu_n \subset \overline{K}^*$ van orde n vormen. Wegens 12.4 is deze groep cyclisch. Omdat iedere cyclische groep van orde n precies $\varphi(n)$ voortbrengers heeft, met φ de Euler-φ-functie, zijn er $\varphi(n)$ primitieve n-de eenheidswortels in $\overline{K}$.

In het geval $\mathrm{char}(K) = 0$ liggen de n-de eenheidswortels in $\overline{\mathbf{Q}}$, en kunnen we μ_n visualiseren in $\overline{\mathbf{Q}} \subset \mathbf{C}$ als de verzameling van n punten in het complexe vlak die de complexe eenheidscirkel $T = \{z \in \mathbf{C} : |z| = 1\}$ in n gelijke stukken deelt, te beginnen bij het punt $z = 1$. Dit verklaart het woord *cyclotomie*, Grieks voor cirkeldeling. In $\mathbf{C}$ is het getal $\zeta_n = \exp(2\pi i/n) = \cos(2\pi/n) + i\sin(2\pi/n)$ een primitieve n-de eenheidswortel, en definieert men het n-de cyclotomische polynoom als

$$\Phi_n = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^*} (X - \zeta_n^k).$$

De nulpunten van Φ_n in $\mathbf{C}$ zijn de $\varphi(n)$ primitieve n-de eenheidswortels. Voor $n = p$ een priemgetal hebben we $X^p - 1 = (X-1)\Phi_p$, dus deze definitie stemt overeen met die in 13.9. Algemener kunnen we de nulpunten van $X^n - 1$ in $\mathbf{C}$ onderverdelen naar hun precieze orde $d|n$. Dit geeft in $\mathbf{C}[X]$ de productrelatie

$$\prod_{d|n} \Phi_d = X^n - 1. \tag{24.13}$$

Hiermee kunnen we inductief de polynomen Φ_n bereken. Door bijvoorbeeld 24.13 achtereenvolgens toe te passen op de delers van 6 vinden we

$$\begin{aligned}
\Phi_1 &= X - 1; \\
\Phi_1 \cdot \Phi_2 &= X^2 - 1, \quad \text{dus} \quad \Phi_2 = X + 1; \\
\Phi_1 \cdot \Phi_3 &= X^3 - 1, \quad \text{dus} \quad \Phi_3 = X^2 + X + 1; \\
\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 &= X^6 - 1, \quad \text{dus} \quad \Phi_6 = (X^6 - 1)/(\Phi_1 \cdot \Phi_2 \cdot \Phi_3) = X^2 - X + 1.
\end{aligned}$$

De Möbius-inversieformule 22.9, toegepast met de multiplicatieve groep $\mathbf{C}(X)^*$ in de rol van de additieve groep $\mathbf{C}$, geeft de identiteit

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

Voor het berekenen van Φ_n kan men echter beter de formules in opgave 31 gebruiken.

24.14. Lemma. *Voor alle $n \geq 1$ is Φ_n een monisch polynoom in $\mathbf{Z}[X]$.*

Bewijs. Het is duidelijk dat Φ_n monisch is. Uit 24.13 volgt met inductie naar n dat Φ_n, als quotiënt van de monische polynomen X^n-1 en $\prod_{d|n,d\neq n}\Phi_d$ met gehele coëfficiënten, wegens 12.1 weer in $\mathbf{Z}[X]$ ligt. □

We gaan bewijzen dat Φ_n voor alle n irreducibel is in $\mathbf{Q}[X]$, zodat 24.13 de factorisatie van X^n-1 in $\mathbf{Q}[X]$ geeft. Hiertoe is het voldoende te laten zien dat het n-de cyclotomische lichaam $\mathbf{Q}(\mu_n)=\mathbf{Q}(\zeta_n)$ verkregen door een nulpunt ζ_n van Φ_n aan $\mathbf{Q}$ te adjungeren graad $\deg(\Phi_n)=\varphi(n)$ heeft.

Voor ieder lichaam K waarvan de karakteristiek n niet deelt is het ontbindingslichaam $K(\mu_n)=K(\zeta_n)$ van X^n-1 over K een Galoisuitbreiding van K, en we kunnen de elementen van $\mathrm{Gal}(K(\mu_n)/K)$ opvatten als automorfismen van de groep $\mu_n=\langle\zeta_n\rangle$ van n-de eenheidswortels. De automorfismen van μ_n zijn de k-de machtsverheffingen $\sigma_k:\zeta_n\mapsto\zeta_n^k$ met $\mathrm{ggd}(k,n)=1$, en dit geeft als in 24.10 aanleiding tot een injectief groepshomomorfisme

$$\mathrm{Gal}(K(\mu_n)/K)\longrightarrow(\mathbf{Z}/n\mathbf{Z})^*.$$

De irreducibiliteit van Φ_n in $\mathbf{Q}[X]$ komt neer op de mededeling dat deze injectie voor $K=\mathbf{Q}$ een *isomorfisme* is.

24.15. Stelling. *De Galoisgroep van het n-de cyclotomische lichaam $\mathbf{Q}(\mu_n)=\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ wordt beschreven door het groepsisomorfisme*

$$\begin{aligned}\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})&\xrightarrow{\sim}(\mathbf{Z}/n\mathbf{Z})^*\\ [\sigma_k:\zeta_n\mapsto\zeta_n^k]&\longmapsto(k \bmod n).\end{aligned}$$

In het bijzonder heeft $\mathbf{Q}(\zeta_n)$ graad $\varphi(n)$ over $\mathbf{Q}$, en is Φ_n het minimumpolynoom van ζ_n over $\mathbf{Q}$.

Bewijs. We hoeven alleen nog te laten zien dat het gegeven homomorfisme *surjectief* is, en dit doen we door te laten zien dat $\mathbf{Q}\subset\mathbf{Q}(\zeta_n)$ voor ieder priemgetal $p\nmid n$ een *lichaams*automorfisme $\sigma_p:\zeta_n\mapsto\zeta_n^p$ toestaat. Laat f het minimumpolynoom zijn van ζ_n over $\mathbf{Q}$, en g het minimumpolynoom van ζ_n^p over $\mathbf{Q}$. Dan zijn f en g irreducibele delers van X^n-1 in $\mathbf{Q}[X]$, en wegens het lemma van Gauss hebben ze gehele coëfficiënten. Omdat ζ_n een nulpunt van $g(X^p)$ is, is f ook een deler van het polynoom $g(X^p)\in\mathbf{Z}[X]$. Bekijken we deze deelbaarheid modulo p, dan zien we dat $\overline{f}=f \bmod p$ een deler is van $\overline{g}(X^p)=\overline{g}(X)^p\in\mathbf{F}_p[X]$. Hieruit volgt dat f en g *gelijk* zijn in $\mathbf{Q}[X]$. Immers, indien dit niet het geval is, dan zijn f en g verschillende irreducibele factoren van X^n-1 in $\mathbf{Q}[X]$, en is ook fg een deler van X^n-1. Modulo p genomen is X^n-1 echter een *separabel* polynoom in $\mathbf{F}_p[X]$: de afgeleide nX^{n-1} is wegens $p\nmid n$ onderling ondeelbaar met X^n-1. De factoren $\overline{f}=f \bmod p$ en $\overline{g}=g \bmod p$ zijn daarom onderling ondeelbaar in $\mathbf{F}_p[X]$, in tegenspraak met de zojuist bewezen deelbaarheidsrelatie $\overline{f}|\overline{g}^p$.

Nu we weten dat ζ_n^p voor alle priemgetallen $p\nmid n$ ook een nulpunt van $f=f_{\mathbf{Q}}^{\zeta_n}$ is, volgt uit 24.7 dat $\mathrm{Gal}(f)=\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ voor dergelijke p een automorfisme

$\sigma_p : \zeta_n \mapsto \zeta_n^p$ bevat. Door samenstellen van dergelijke automorfismen krijgen we alle elementen $\sigma_k : \zeta_n \to \zeta_n^k$ met $k \in (\mathbf{Z}/n\mathbf{Z})^*$, en de te bewijzen surjectiviteit volgt. □

Het in het bewijs van 24.15 voor alle priemgetallen $p \nmid n$ geconstrueerde automorfisme σ_p, dat een soort 'lift naar karakteristiek 0' van het Frobeniusautomorfisme is, blijkt veel algemener voor uitbreidingen van getallenlichamen geconstrueerd te kunnen worden. In de moderne getaltheorie, waar dergelijke Frobeniusautomorfismen een belangrijke rol spelen, wordt het isomorfisme in 24.15 als een speciaal geval van de zogenaamde *Artin-afbeelding* voor abelse uitbreidingen van getallenlichamen gezien.[8]

Omdat de uitbreiding $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ een abelse Galoisgroep heeft, is voor ieder deellichaam $E \subset \mathbf{Q}(\zeta_n)$ de uitbreiding $\mathbf{Q} \subset E$ ook weer Galois met abelse Galoisgroep. Het is tamelijk verrassend dat er ook een omkering van deze mededeling geldt. Deze omkering werd al in 1853 door de Duitser Leopoldt Kronecker (1823–1891) geformuleerd. Zijn onvolledige bewijs werd in 1886 verbeterd door Heinrich Weber (1842–1913), die onder meer als auteur van *het* algebra-leerboek[9] van de vroege twintigste eeuw bekend geworden is.

24.16. Stelling van Kronecker-Weber. *Zij $\mathbf{Q} \subset E$ een eindige Galoisuitbreiding met abelse Galoisgroep. Dan is er een cyclotomisch lichaam $\mathbf{Q}(\zeta_n)$ dat E als deellichaam bevat.*

Voor *kwadratische* uitbreidingen $\mathbf{Q} \subset E$ kan men deze stelling zonder al te veel moeite uit 24.12 afleiden (opgave 30). Het bewijs van 24.16 zelf gebruikt technieken uit de algebraïsche getaltheorie en valt buiten het bestek van deze syllabus.

Zoals stelling 24.16 al suggereert is het abels zijn van de Galoisgroep van een polynoom $f \in \mathbf{Q}[X]$ een sterke eis: er zijn maar 'weinig' abelse uitbreidingen van $\mathbf{Q}$. Neemt men een 'willekeurig' monisch polynoom $f \in \mathbf{Z}[X]$ van graad n, dan geldt in een natuurlijke zin dat f met 'kans 1' irreducibel is (opgave 22.25), en bovendien[10] Galoisgroep $\mathrm{Gal}(f) \cong S_n$ heeft.

Opgave 7. Maak deze uitspraak precies voor $n = 2$, en geef er een bewijs voor.

Abelse uitbreidingen van $\mathbf{Q}$ heten wel *abelse getallenlichamen*. Door hun eenvoudige karakterisering hebben zij een rijkere aritmetische structuur[11] dan 'gewone' getallenlichamen. Het is een open probleem of men *willekeurige* algebraïsche uitbreidingen van $\mathbf{Q}$, of zelfs maar de algebraïsche uitbreidingen met een vaste niet-abelse groep G, net zo 'expliciet' als de abelse uitbreidingen kan beschrijven. De moeilijkheid hangt samen met ons relatief gebrekkige begrip[12] van de oneindige groep $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) = \mathrm{Aut}(\overline{\mathbf{Q}})$, de *absolute Galoisgroep* van $\mathbf{Q}$. De aan 24.15 ten grondslag liggende gedachte om uitbreidingen met 'expliciete' Galoisgroepen te verkrijgen door 'torsiepunten' van geschikte groepen als $\mathbf{C}^*$ te adjungeren kent vele generalisaties. Torsiepunten van elliptische krommen hebben in de 20e eeuw tot fraaie resultaten geleid, en nog algemener leidt de natuurlijke actie van $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ op allerhande algebraïsche structuren tot wat men wel *Galoisrepresentaties* noemt.

Opgaven.

8. Zij $L = \mathbf{Q}(X)$ het lichaam van rationale functies over $\mathbf{Q}$ en $\sigma \in \mathrm{Aut}(L)$ het unieke automorfisme met $\sigma(X) = X+1$. Bewijs dat $G = \langle\sigma\rangle$ een oneindige ondergroep van $\mathrm{Aut}(L)$ is, en dat $L^G \subset L$ *geen* algebraïsche uitbreiding is. Laat ook zien dat de afbeelding $H \mapsto L^H$ van de verzameling van ondergroepen van G naar de verzameling van deellichamen van L in dit geval injectief noch surjectief is.

9. Zij $L = \mathbf{Q}(X)$ als boven, en definieer $\sigma_i \in \mathrm{Aut}(L)$ door

$$\sigma_1(X) = -X, \qquad \sigma_2(X) = 1/X, \qquad \sigma_3(X) = 1 - X.$$

   Bepaal de invariantenlichamen $L^{\langle\sigma_i\rangle}$ voor $i = 1, 2, 3$.

10. Definieer σ_i als in de vorige opgave.
    a. Laat zien dat $\rho = \sigma_2\sigma_3$ orde 3 heeft in $\mathrm{Aut}(L)$, en bepaal $L^{\langle\rho\rangle}$.
    b. Laat zien dat $G = \langle\sigma_2, \sigma_3\rangle$ orde 6 heeft, en isomorf is met S_3. Bepaal $f \in \mathbf{Q}(X)$ met $L^G = \mathbf{Q}(f)$.

11. Zij $L = K(X)$ het lichaam van rationale functies over een lichaam K van karakteristiek $p > 0$ en $\sigma \in \mathrm{Aut}(L)$ het automorfisme met $\sigma(X) = X + 1$. Laat zien dat $G = \langle\sigma\rangle$ eindig is, en bepaal een voortbrenger van L^G over K.

12. Zij K een lichaam, en $f = \frac{p}{q} \in K(X)$ het quotiënt van onderling ondeelbare polynomen $p, q \in K[X]$ van graad respectievelijk m en n. Bewijs: als f niet constant is, dan is $K(f) \subset K(X)$ een algebraïsche uitbreiding van graad $\max(m, n)$.

13. Laat $\alpha_1, \alpha_2, \cdots, \alpha_n$ een verzameling van n algebraïsche getallen zijn die paarsgewijs geconjugeerd zijn over $\mathbf{Q}$, en stel dat $f = \prod_{i=1}^{n}(X - \alpha_i)$ een polynoom met rationale coëfficiënten is. Bewijs: f is irreducibel in $\mathbf{Q}[X]$.
    [Voorbeeld: het monische polynoom met de 4 nulpunten $1 \pm i \pm \sqrt{2}$ uit opgave 21.25.]

14. Zij $K \subset K(\alpha)$ een Galoisuitbreiding met groep G. Bewijs dat het minimumpolynoom van α over K gelijk is aan $f_K^\alpha = \prod_{\sigma\in G}(X - \sigma(\alpha))$.

15. Zij $K \subset L$ een Galoisuitbreiding van graad n. Laat zien dat L een ontbindingslichaam Ω_K^f is voor een polynoom $f \in K[X]$ van graad n. Is zo'n f noodzakelijk irreducibel?

16. Bepaal de Galoisgroep van $f = X^3 - 2$ over $\mathbf{F}_3$, $\mathbf{F}_5$ en $\mathbf{F}_7$.

17. Zij K van karakteristiek verschillend van 2, en $K \subset L$ een kwadratische uitbreiding.
    a. Bewijs: er bestaat een element $m \in K^* \setminus K^{*2}$ met $L = K(\sqrt{m})$, en de ondergroep $\langle\overline{m}\rangle \in K^*/K^{*2}$ is eenduidig bepaald door L;
    b. Bewijs: er is een bijectie tussen de verzameling van kwadratische uitbreidingen van K (binnen een algebraïsche afsluiting $\overline{K}$) en de niet-triviale elementen van K^*/K^{*2} gegeven door $L \longmapsto (L^{*2} \cap K^*) \setminus K^{*2}$.

18. Zij K van karakteristiek 2, en $K \subset L$ een separabele kwadratische uitbreiding. Schrijf $\wp(F) = \{x^2 + x : x \in F\}$ voor een lichaam F. Bewijs:
    a. er bestaat een element $m \in K \setminus \wp(K)$ zodat $L = K(\alpha)$ geldt voor een nulpunt α van $X^2 + X + m \in K[X]$, en de ondergroep $\langle\overline{m}\rangle \in K/\wp(K)$ is eenduidig bepaald door L;

b. er is een bijectie tussen de verzameling van separabele kwadratische uitbreidingen van K (binnen een algebraïsche afsluiting $\overline{K}$) en de niet-triviale elementen van $K/\wp(K)$ gegeven door $L \longmapsto (\wp(L) \cap K) \setminus \wp(K)$.

19. Zij L een ontbindingslichaam van het polynoom $f = X^4 + 20 \in \mathbf{Q}[X]$. Bepaal $\mathrm{Gal}(f)$ en alle tussenlichamen van de uitbreiding $\mathbf{Q} \subset L$.

20. Idem voor $f = X^4 - 4X^2 + 5$ en $f = X^4 - 5X^2 - 5$.

21. Zij K een lichaam van karakteristiek verschillend van 2, en $L = K(\sqrt{m})$ een kwadratische uitbreiding van K. Laat $\delta = a + b\sqrt{m} \in L \setminus K$ een element zijn dat geen kwadraat is in L, en neem $M = L(\sqrt{\delta})$. Schrijf $\delta' = a - b\sqrt{m}$. Bewijs:
    a. er geldt $f_K^{\sqrt{\delta}} = X^4 - 2aX^2 + a^2 - mb^2$ en $\Omega_K^f = L(\sqrt{\delta}, \sqrt{\delta'})$;
    b. equivalent zijn:
        1. $K \subset M$ is normaal;
        2. $N_{L/K}(\delta) = a^2 - mb^2 \in L^{*2} \cap K^* = \langle m, K^{*2} \rangle$;
        3. $\delta/\delta' = \gamma^2$ met $\gamma \in L$.
    c. voor $N_{L/K}(\delta) \in K^{*2}$ geldt $\mathrm{Gal}(M/K) \cong C_2 \times C_2$, en voor $N_{L/K}(\delta) \in m \cdot K^{*2}$ geldt $\mathrm{Gal}(M/K) \cong C_4$.
    d. voor $\gamma \in L$ als in b geldt $N_{L/K}(\gamma) = \pm 1$, en $N_{L/K}(\gamma) = -1$ treedt op dan en slechts dan als $K \subset M$ *cyclisch* is van graad 4.

22. Bepaal $\mathrm{Gal}(f)$ voor elk van de volgende polynomen $f \in \mathbf{Q}[X]$:
$$X^4 - 4X^2 + 2, \qquad X^4 - 2X^2 + 4, \qquad X^4 - 2X^2 + 2.$$

23. Bestaat er een kwadratische uitbreiding van $K = \mathbf{Q}(i)$ die cyclisch is over $\mathbf{Q}$? Zelfde vraag voor $K = \mathbf{Q}(\sqrt{17})$.

24. Laat zien dat $\mathbf{Q} \subset \mathbf{Q}(\zeta_{11})$ precies 2 niet-triviale tussenlichamen heeft, en bepaal voor elk van beide lichamen het minimumpolynoom van een primitief element.

25. Bepaal minimumpolynomen voor voortbrengers van de deellichamen van het cyclotomische lichaam $\mathbf{Q}(\zeta_{13})$.

26. Zij d een deler van 16 en K_d het deellichaam van $\mathbf{Q}(\zeta_{17})$ dat graad d heeft over $\mathbf{Q}$.
    a. Bewijs: $K_2 = \mathbf{Q}(\sqrt{17})$.
    b. Bepaal het minimumpolynoom van een voortbrenger van K_4 over K_2.

27. Zij $\zeta_9 \in \mathbf{C}$ een primitieve negende eenheidswortel.
    a. Bewijs: $f_{\mathbf{Q}}^{\zeta_9} = \Phi_9 = X^6 + X^3 + 1$.
    b. Laat zien dat $\mathbf{Q} \subset \mathbf{Q}(\zeta_9)$ precies 2 niet-triviale tussenlichamen heeft, en bepaal voor elk van beide lichamen het minimumpolynoom van een primitief element.

28. Generaliseer de definitie van Gauss-perioden naar het geval van willekeurige n-de eenheidswortels. Liggen de verkregen elementen in de bijbehorende tussenlichamen? Zijn het noodzakelijk voortbrengers over $\mathbf{Q}$?

29. Bepaal alle tussenlichamen van de uitbreiding $\mathbf{Q} \subset \mathbf{Q}(\zeta_{15})$, en geef aan met welke ondergroepen van $(\mathbf{Z}/15\mathbf{Z})^*$ ze corresponderen.

30. Zij $d \in \mathbf{Z}$ een getal dat geen kwadraat is. Bewijs: het cyclotomische lichaam $\mathbf{Q}(\zeta_{4|d|})$ bevat het kwadratische lichaam $\mathbf{Q}(\sqrt{d})$ als deellichaam.

31. Zij p een priemgetal en $n \in \mathbf{Z}_{\geq 1}$ geheel. Bewijs:
    a. $\Phi_{pn} = \Phi_n(X^p)$ als p een deler is van n;
    b. $\Phi_{pn} = \Phi_n(X^p)/\Phi_n$ als p geen deler is van n;
    c. voor $n > 1$ oneven geldt $\Phi_{2n} = \Phi_n(-X)$.

32. Bereken Φ_n voor alle samengestelde getallen $n \leq 30$.

33. Bereken de waarden $\Phi_n(0)$ en $\Phi_n(1)$ voor alle $n \geq 1$.

34. Bewijs dat Φ_n voor $n > 1$ een symmetrisch polynoom is: $X^{\varphi(n)} \cdot \Phi_n(1/X) = \Phi_n$.

35. Zij $n \geq 1$ geheel en $p \nmid n$ priem. Bewijs: $\Phi_{np^k} = (\Phi_n)^{\varphi(p^k)} \in \mathbf{F}_p[X]$.

36. Zij $n \geq 1$ geheel en $p \nmid n$ priem. Stel dat $p \in (\mathbf{Z}/n\mathbf{Z})^*$ orde d heeft. Bewijs dat $\Phi_n \in \mathbf{F}_p[X]$ het product van $\varphi(n)/d$ irreducibele factoren van graad d is.
    [Hint: wat is $[\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ voor een nulpunt $\alpha \in \overline{\mathbf{F}}_p$ van Φ_n?]

37. Ontbind het polynoom Φ_7 in $\mathbf{F}_p[X]$ voor $p \in \{2, 3, 5, 7, 13, 29\}$.

38. Zij $n \in \mathbf{Z}_{>1}$. Bewijs dat er oneindig veel priemgetallen $p \equiv 1 \bmod n$ bestaan.
    [Hint: imiteer Euclides' bewijs 6.5. Welke priemgetallen delen $\Phi_n(N)$?]

39. Laat zien dat er voor iedere eindige *abelse* groep G een Galoisuitbreiding K van $\mathbf{Q}$ met groep G bestaat.
    [Hint: gebruik de vorige opgave en de structuurstelling 9.12 voor eindige abelse groepen.]

40. Zij K een lichaam en $f \in K[X]$ van graad n met ontbinding $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $\overline{K}[X]$.
    a. Bewijs dat de *discriminant*

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

    van f een element van K is.
    b. Bereken $\Delta(X^2 + aX + b)$.

41. Zij $f \in \mathbf{Q}[X]$ monisch irreducibel, en vat $\mathrm{Gal}(f)$ op als ondergroep van S_n via zijn werking op de nulpunten van f. Bewijs:

$$\mathrm{Gal}(f) \subset A_n \iff \Delta(f) \text{ is een kwadraat in } \mathbf{Q}^*.$$

    Is de keuze van het grondlichaam $\mathbf{Q}$ belangrijk?

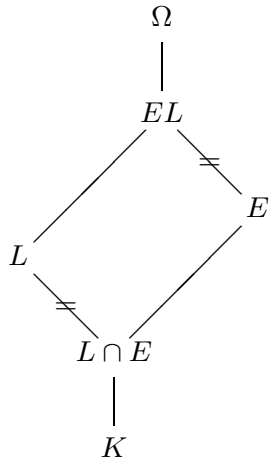
42. Zij $f \in \mathbf{Q}[X]$ monisch irreducibel van graad 3. Bewijs: voor ieder nulpunt $\alpha \in \mathbf{C}$ van f is $\mathbf{Q}(\alpha, \sqrt{\Delta(f)}) \subset \mathbf{C}$ een ontbindingslichaam van f. Is het nodig f irreducibel te nemen?

43. Bereken de discriminant van het polynoom $f_{\mathbf{Q}}^{\eta_3} = X^3 + X^2 - 2X - 1$ in voorbeeld 24.11.

44. Zij K een lichaam en $f \in K[X]$ een irreducibel separabel polynoom van graad 4. Laat zien dat er op isomorfie na niet meer dan 5 mogelijkheden zijn voor de groep $\mathrm{Gal}(f)$.

45. Zij K een lichaam en $f \in K[X]$ een irreducibel separabel polynoom van graad 5.
    a. Bewijs: $\mathrm{Gal}(f)$ bevat een element σ van orde 5.
    b. Bewijs: $\mathrm{Gal}(f)$ is isomorf met C_5, D_5 of de affiene groep $\mathrm{Aff}(\mathbf{Z}/5\mathbf{Z})$ van orde 20 uit 8.14.4 als de ondergroep $\langle\sigma\rangle \subset \mathrm{Gal}(f)$ (met σ als in a) normaal is, en isomorf met A_5 of S_5 indien dit niet zo is.

46. Laat $K \subset \Omega$ een willekeurige lichaamsuitbreiding zijn, en L en E tussenlichamen van de uitbreiding $K \subset \Omega$. Stel dat $K \subset L$ een eindige Galoisuitbreiding is. Bewijs: EL is een eindige Galoisuitbreiding van E, en de natuurlijke restrictie-afbeelding $\mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/(L \cap E))$ is een isomorfisme.



[Vraag: is er een relatie met het diagram van groepen na stelling 8.2?]

47. Zij $K \subset K(\zeta)$ de cyclotomische uitbreiding verkregen door een primitieve n-de eenheidswortel ζ aan K te adjungeren. Bewijs: $K \subset K(\zeta)$ is Galois met groep $G \subset (\mathbf{Z}/n\mathbf{Z})^*$. Wordt iedere ondergroep van $(\mathbf{Z}/n\mathbf{Z})^*$ voor geschikte K als Galoisgroep verkregen?

48. Zij $f \in K[X]$ een polynoom van graad n met Galoisgroep S_n. Zij $L = K(\alpha)$ de uitbreiding van K verkregen door adjunctie van een nulpunt van f, en E een tussenlichaam van de uitbreiding $K \subset L$. Bewijs: $E = K$ of $E = L$.

49. Zij $K \subset \Omega$ een lichaamsuitbreiding, en laat E_1 en E_2 tussenlichamen van $K \subset \Omega$ zijn die eindig zijn over K.
    a. Bewijs dat het compositum E_1E_2 eindig is over K van graad
    $$[E_1E_2 : K] \leq [E_1 : K] \cdot [E_2 : K].$$
    Is $[E_1E_2 : K]$ noodzakelijk een *deler* van $[E_1 : K] \cdot [E_2 : K]$?
    b. Bewijs dat E_1E_2 normaal is over K als E_1 en E_2 dat zijn. Geldt de omkering?
    c. Bewijs dat E_1E_2 abels is over K als E_1 en E_2 dat zijn. Geldt de omkering?

50. Stel dat de lichamen E_1 en E_2 in de voorafgaande opgave K-isomorf zijn, en dat $L \subset \Omega$ een lichaam is dat E_1 bevat en eindig Galois is over K. Bewijs: er bestaat een element $\sigma \in \mathrm{Gal}(L/K)$ met $\sigma[E_1] = E_2$.

51. Zij $K \subset M$ een eindige Galoisuitbreiding met Galoisgroep G en L een tussenlichaam van $K \subset M$ behorende bij een normale ondergroep $N \triangleleft G$. Bewijs dat de exacte rij $0 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 0$ splitst dan en slechts dan als er een tussenlichaam E van $K \subset M$ bestaat met $E \cap L = K$ en $EL = M$.

52. Zij $L = \Omega_{\mathbf{Q}}^{X^5-2}$ een ontbindingslichaam van $X^5 - 2$ over $\mathbf{Q}$. Bewijs dat er een exact rijtje van groepen
    $$0 \longrightarrow \mathbf{Z}/5\mathbf{Z} \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow (\mathbf{Z}/5\mathbf{Z})^* \longrightarrow 1$$

bestaat. Laat zien dat deze rij splitst, en dat $\mathrm{Gal}(L/\mathbf{Q})$ isomorf is met de affiene groep $\mathrm{Aff}(\mathbf{Z}/5\mathbf{Z})$ uit opgave 45.

53. Laat zien dat de Galoisgroep van het polynoom $X^n - a \in \mathbf{Z}[X]$ isomorf is met een ondergroep van $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ uit 8.14.4.

54. Laat de affiene groep $G = \mathrm{Aff}(\mathbf{F}_q) = \mathbf{F}_q \rtimes \mathbf{F}_q^*$ werken op het rationale functielichaam $L = \mathbf{F}_q(X)$ door $(b, a) \in \mathbf{F}_q \rtimes \mathbf{F}_q^*$ als het automorfisme geïnduceerd door $X \mapsto aX + b$ op te vatten.
    a. Bewijs dat $L^G \subset L$ een eindige Galoisuitbreiding met groep G is, en bepaal een voortbrenger van L^G over $\mathbf{F}_q$.
    b. Welke tussenlichamen corresponderen met de ondergroepen $\mathbf{F}_q^*$ en $\mathbf{F}_q$ van G?

55. Zij $K(X)$ het lichaam van rationale functies over een lichaam K.
    a. Bewijs dat ieder automorfisme σ van $K(X)$ over K voldoet aan $\sigma(X) = \frac{aX+b}{cX+d}$ met $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$, en dat dit een isomorfisme $G = \mathrm{Aut}_K(K(X)) \cong \mathrm{PGL}_2(K)$ induceert. (Hier is $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^*$ de groep verkregen door $\mathrm{GL}_2(K)$ naar de normaaldeler $K^* = K^* \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ van scalaire matrices uit te delen.)
    b. Bewijs dat $L^G = K$ geldt dan en slechts dan als K oneindig is.

56. Zij $K \subset L$ eindig Galois met groep G, en $X(L/K)$ een fundamentele verzameling. Laat zien dat de afbeelding

$$\begin{aligned} X(L/K) \times G &\longrightarrow X(L/K) \\ (\phi, \sigma) &\longmapsto \phi \circ \sigma \end{aligned}$$

een rechtswerking van G op $X(L/K)$ definieert die trouw en transitief is.

57. Zij $L = \overline{\mathbf{F}}_p$ een algebraïsche afsluiting van $\mathbf{F}_p$, en $H \subset G = \mathrm{Aut}(\mathbf{F}_p)$ de cylische ondergroep voortgebracht door het Frobenius-automorfisme. Bewijs: er geldt $H \subsetneq G$ maar $L^G = L^H = \mathbf{F}_p$.
[Hint: gebruik de opgaven 22.37 en 22.38]

25 Radicaaluitbreidingen

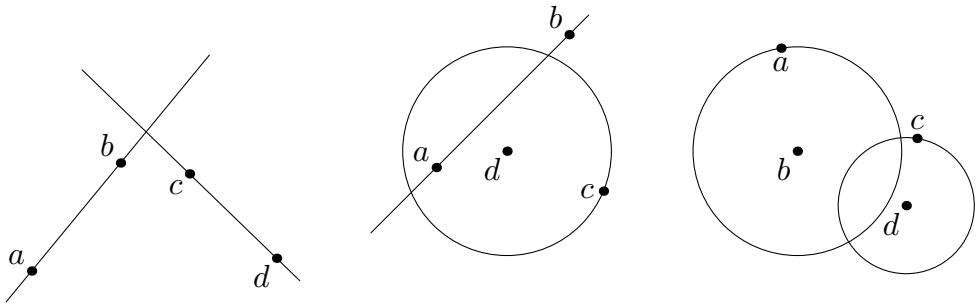
Deze paragraaf bevat twee klassieke toepassingen van de Galoistheorie. De eerste toepassing, het door de Griekse wiskunde opgeworpen probleem van de *construeerbaarheid* van punten in het vlak, laat zien dat de onderliggende vragen op geen enkele manier aan lichaamsuitbreidingen of automorfismengroepen hoeven te refereren. De tweede toepassing, het oplossen van polynoomvergelijkingen door worteltrekkingen, is het probleem dat in zekere zin de aanleiding vormde tot het ontstaan van de Galoistheorie.

▶ Constructieproblemen

In de Griekse wiskunde[13] placht men figuren in het platte vlak te *construeren* met passer en liniaal. Uitgaande van gegeven punten construeert men hierbij nieuwe punten als doorsnijdingen van lijnen en cirkels gedefinieerd in termen van de gegeven punten.

Een *constructiestap* uitgaande van een deelverzameling X van het vlak bestaat eruit dat men een puntenverzameling P in het vlak produceert door toepassen van de volgende algoritme:

1. kies punten $a, b, c, d \in X$ met $a \neq b$ en $c \neq d$;
2. laat ℓ_{ab} hetzij de lijn door a en b, hetzij de cirkel door a met middelpunt b zijn; laat evenzo ℓ_{cd} de lijn door c en d of de cirkel door c met middelpunt d zijn;
3. als ℓ_{ab} en ℓ_{cd} niet samenvallen, neem $P = \ell_{ab} \cap \ell_{cd}$; anders $P = \emptyset$.



Zoals we uit de plaatjes zien, bestaat de verzameling P uit ten hoogste twee punten. Voor sommige keuzen van $a, b, c, d \in X$ kan P leeg zijn. De vereniging van alle P die door een constructiestap uit X geconstrueerd kunnen worden geven we aan met $\mathcal{F}(X)$. Merk op dat $\mathcal{F}(X)$ leeg is als X minder dan 2 punten bevat.

25.1. Definitie. *Zij X een deelverzameling van het platte vlak, en definieer inductief verzamelingen X_i voor $i \in \mathbf{Z}_{\geq 0}$ door*

$$X_0 = X \qquad \text{en} \qquad X_i = X_{i-1} \cup \mathcal{F}(X_{i-1}) \quad \text{voor} \quad i \geq 1.$$

Dan is $\mathcal{C}(X) = \bigcup_{i=0} X_i$ de verzameling van construeerbare punten uitgaande van X.

Naast het construeren van punten spreekt men ook wel van het construeren van lijnen en cirkels. Een lijn noemt men construeerbaar als men er twee verschillende punten op

kan construeren, en een cirkel als men het middelpunt en een punt op de cirkel kan construeren.

De Griekse wiskunde gaf al in de vijfde eeuw voor Christus aanleiding tot een aantal constructieproblemen die de Grieken niet konden oplossen, en waarop gedurende meer dan 2000 jaar vele al dan niet 'professionele' wiskundigen hun tanden stukbeten.[14]

25.2. Kwadratuur van de cirkel. *Construeer een vierkant waarvan de oppervlakte gelijk is aan die van een cirkel met gegeven straal.*

Hippocrates van Chios, die rond 430 voor Christus leefde, liet zien dat 25.2 oplosbaar is indien men in plaats van de cirkel bepaalde figuren begrensd door cirkelbogen neemt: de zogenaamde *maantjes van Hippocrates*[15] (zie opgave 14).

25.3. Verdubbeling van de kubus. *Construeer een lijnstuk dat $\sqrt[3]{2}$ keer zo lang is als een gegeven lijnstuk.*

Dit probleem heet ook wel het *Delische probleem*, naar de legende waarin de god Apollo via zijn orakel op het eiland Delos de door pest geteisterde Atheners verordonneerde hun kubusvormige Apollo-altaar te 'verdubbelen'.

25.4. Trisectie van de hoek. *Deel een gegeven hoek met passer en liniaal in drie gelijke delen.*

Voor een paar hoeken, zoals de rechte hoek, blijkt dit probleem gemakkelijk oplosbaar. In de meeste andere gevallen lijkt de driedeling van de hoek niet mogelijk.

25.5. Constructie van de n-hoek. *Construeer voor $n \geq 3$ in een gegeven cirkel een regelmatige n-hoek.*

Dit probleem hoort strikt genomen niet tot het klassieke 'corpus' van de drie onopgeloste Griekse problemen, maar als n-deling van de volledige hoek van 2π radialen sluit het er nauw bij aan. Omdat bisectie van een hoek met passer en liniaal gemakkelijk is, is de interessante vraag in 25.5 voor welke *oneven* n het probleem oplosbaar is. De Grieken vonden oplossingen voor $n = 3$ en $n = 5$, maar bijvoorbeeld niet voor $n = 7$ of $n = 9$.

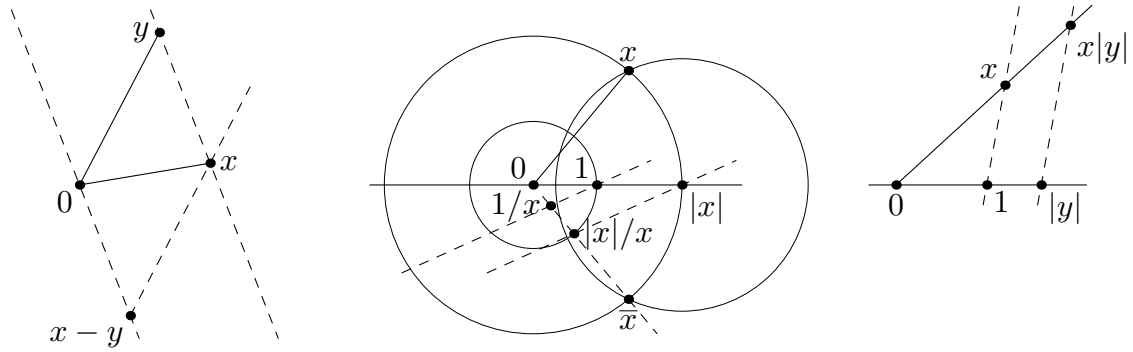
Om constructieproblemen in termen van lichaamsuitbreidingen te kunnen formuleren identificeren we het platte vlak op de bekende wijze met het lichaam $\mathbf{C}$ der complexe getallen. De voorafgaande problemen laten zich dan met behulp van 25.1 herformuleren in termen van construeerbare getallen uitgaande van een deelverzameling $X \subset \mathbf{C}$. We mogen aannemen dat X tenminste twee punten bevat – anders valt er niets te construeren – en we kunnen door schaling $\{0, 1\} \subset X$ kiezen. Voor $X = \{0, 1\}$ heet $\mathcal{C} = \mathcal{C}(X)$ kortweg de verzameling van *construeerbare getallen*. De problemen 25.2, 25.3 en 25.5 behelzen dan precies de vraag of de getallen $\sqrt{\pi}$, $\sqrt[3]{2}$ en de primitieve n-de eenheidswortel $\zeta_n = e^{2\pi i/n} \in \mathbf{C}$ construeerbaar zijn. De vraag in 25.4 is of $\mathcal{C}(\{0, 1, \alpha\})$ voor $\alpha \in \mathbf{C}$ met $|\alpha| = 1$ een derdemachtswortel $\sqrt[3]{\alpha}$ bevat.

25.6. Propositie. *Zij $X \subset \mathbf{C}$ een verzameling die 0 en 1 bevat. Dan is $\mathcal{C}(X)$ een deellichaam van $\mathbf{C}$ dat X bevat. Het is gesloten onder complexe conjugatie en onder het nemen van kwadraatwortels.*

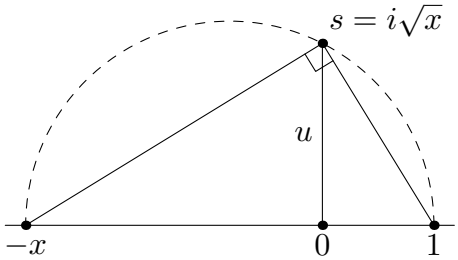
Bewijs. Het bewijs is een exercitie in het uitvoeren van elementaire constructies. We nemen hierbij de standaardconstructies uit opgave 13 als bekend aan – een aanbevolen opgave voor wie nog nooit een constructie uitgevoerd heeft! Het is duidelijk dat X, en dus in het bijzonder 0 en 1, bevat zijn in $\mathcal{C}(X)$. Het is daarom voldoende om te laten zien dat voor $x, y \in \mathcal{C}(X)$ ook het verschil $x - y$, het product xy, de inverse $1/x$, de complex geconjugeerde $\overline{x}$ en de wortels $\pm\sqrt{x}$ construeerbaar zijn uitgaande van X.

Voor $x-y$ past men op de lijn door 0 evenwijdig aan de lijn door x en y de afstand $|x - y|$ af. Voor $\overline{x}$ doorsnijdt men de cirkel om 0 door x eerst met de lijn door 0 en 1 – dat geeft $|x|$ – en vervolgens met de cirkel om $|x|$ door x. Voor $x \notin \mathbf{R}$ is $|x|/x$ de doorsnijding van de cirkel om 0 door 1 met de lijn door 0 en $\overline{x}$; de lijn door 1 evenwijdig aan de lijn door door $|x|/x$ en $|x|$ snijdt nu de lijn door 0 en $\overline{x}$ in $1/x$. Een soortgelijk plaatje laat zien hoe men x met een reëel getal $|y|$ vermenigvuldigt. Het product $x|y|$ wordt vervolgens geroteerd over de hoek $\angle y01$ om xy te krijgen.

Opgave 1. Hoe dienen de constructies te worden aangepast voor $x \in \mathbf{R}$?



De worteltrekking komt neer op het construeren van $\sqrt{x}$ voor $x \in \mathbf{R}_{>0}$. Immers, voor niet-reële x past men eenvoudig $\sqrt{|x|}$ af op de bissectrice van de hoek $\angle x01$. Voor $x \in \mathbf{R}_{>0}$ doorsnijdt men de loodlijn in 0 op de lijn door 0 en 1 met de cirkel die het lijnstuk tussen $-x$ en 1 als middellijn heeft. Zij s een snijpunt.



Omdat de hoek $\angle(-x)s1$ recht is (stelling van Thales), zijn de driehoeken $(-x)s0$ en $s10$ gelijkvormig. De gelijkheid van verhoudingen $x : u = u : 1$ laat zien dat s gelijk is aan $i\sqrt{x}$, en we zijn klaar. □

Opgave 2. *(Voor wie het nog niet wist...)* Formuleer en bewijs de stelling van Thales.

Het hoofdresultaat over construeerbare getallen is dat 25.6 het lichaam $\mathcal{C}(X)$ in feite karakteriseert: $\mathcal{C}(X)$ is het *kleinste* lichaam dat aan de eisen van 25.6 voldoet. Hiertoe moeten we laten zien dat constructiestappen slechts aanleiding kunnen geven tot kwadratische lichaamsuitbreidingen.

25.7. Propositie. *Laat $X \subset \mathbf{C}$ gegeven zijn, en zij $K = \mathbf{Q}(X, \overline{X})$ het deellichaam van $\mathbf{C}$ voortgebracht door de elementen in X en hun complex geconjugeerden. Dan is ieder punt $z \in \mathbf{C}$ dat door een constructiestap uitgaande van X verkregen kan worden algebraïsch over K van graad $[K(z) : K] \leq 2$.*

Bewijs. Stel dat er punten $a, b, c, d \in X$ bestaan met $a \neq b$ en $c \neq d$. We moeten laten zien dat een snijpunt van de lijn of cirkel bepaald door ab en de lijn of cirkel bepaald door cd graad ten hoogste 2 over K heeft. We onderscheiden de drie mogelijkheden gegeven door de plaatjes voorafgaande aan 25.1.

De lijn door de punten a en b bestaat uit de punten $z \in \mathbf{C}$ waarvoor $(z-a)/(a-b)$ reëel is. Uitschrijven van de identiteit $(z-a)/(a-b) = (\overline{z}-\overline{a})/(\overline{a}-\overline{b})$ geeft als vergelijking voor deze lijn

$$\ell_{ab} : (\overline{a}-\overline{b})z - (a-b)\overline{z} = \overline{a}b - a\overline{b}.$$

Het doorsnijden van de lijnen ℓ_{ab} en ℓ_{cd} komt neer op het oplossen van twee lineaire vergelijkingen in z en $\overline{z}$ met coëfficiënten in $\mathbf{Q}(a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}) \subset K$. Als ℓ_{ab} en ℓ_{cd} niet evenwijdig zijn, heeft dit stelsel een unieke oplossing $z \in K$ en hebben we $K(z) = K$. Als ze wel evenwijdig zijn is, omdat ℓ_{ab} en ℓ_{cd} niet samenvallen, het stelsel strijdig en is er geen oplossing.

Voor de cirkel door c met middelpunt d is de vergelijking $|z-d| = |c-d|$, en dit kunnen we herschrijven als $(z-d)(\overline{z}-\overline{d}) = (c-d)(\overline{c}-\overline{d})$ of

$$z\overline{z} - \overline{d}z - d\overline{z} = c\overline{c} - c\overline{d} - \overline{c}d.$$

Voor een punt z op de lijn ℓ_{ab} dat op deze cirkel ligt kunnen we $\overline{z}$ met behulp van de vergelijking voor ℓ_{ab} schrijven als een lineaire uitdrukking in z met coëfficiënten in K. Gesubstitueerd in de vergelijking van de cirkel geeft dit een kwadratische relatie met coëfficiënten in K waar z aan voldoet. We vinden $[K(z) : K] \leq 2$.

In het geval dat z een punt is dat zowel op de cirkel door a met middelpunt b als op de cirkel door c met middelpunt d ligt, krijgen we door aftrekken van de vergelijkingen van de beide cirkels een lineaire relatie tussen z en $\overline{z}$ met coëfficiënten in K. Omdat de cirkels niet samenvallen is dit niet de nulrelatie, en we zijn terug in het voorafgaande geval. Dit bewijst $[K(z) : K] \leq 2$ voor alle constructiestappen. □

▶ Kwadratische afsluiting

Het hoofdresultaat voor construeerbare getallen laat zich bondig formuleren in termen van *kwadratische afsluitingen*. We introduceren eerst de 'maximale kwadraatworteluitbreiding' van een lichaam K (binnen een algebraïsche afsluiting $\overline{K}$) als het deellichaam $K(S) \subset \overline{K}$ voortgebracht door de verzameling

$$S = \{w \in \overline{K} : \quad w^2 \in K\}$$

van kwadraatwortels uit elementen van K. Voor K van karakteristiek niet 2 is deze uitbreiding, die we symbolisch met $K(\sqrt{K})$ aangeven, een algebraïsche uitbreiding van K die normaal en separabel is. In veel gevallen is hij echter van oneindige graad over K.

Opgave 3. Laat zien dat $\mathbf{Q} \subset \mathbf{Q}(\sqrt{\mathbf{Q}})$ een oneindige uitbreiding is.

25.8. Definitie. *Zij K een lichaam van karakteristiek* $\mathrm{char}(K) \neq 2$ *met algebraïsche afsluiting $\overline{K}$. Dan is de kwadratische afsluiting K^{quad} van K in $\overline{K}$ het lichaam*

$$K^{\mathrm{quad}} = \bigcup\nolimits_{i=0}^{\infty} K_i, \qquad \textit{waarbij } K_0 = K \textit{ en } K_i = K_{i-1}(\sqrt{K_{i-1}}) \textit{ voor } i \geq 1.$$

De gelijkenis tussen 25.8 en 25.1 is meer dan oppervlakkig.

25.9. Stelling. *De verzameling $\mathcal{C}(X)$ van construeerbare punten uitgaande van een deelverzameling $X \subset \mathbf{C}$ die 0 en 1 bevat is gelijk aan de kwadratische afsluiting van het lichaam $\mathbf{Q}(X, \overline{X})$ in $\mathbf{C}$.*

Bewijs. Omdat $\mathcal{C}(X)$ wegens 25.6 een lichaam is dat X bevat en dat gesloten is onder complexe conjugatie en het trekken van kwadraatwortels, is het duidelijk dat de kwadratische afsluiting van $K = \mathbf{Q}(X, \overline{X})$ bevat is in $\mathcal{C}(X)$.

Omgekeerd zien we uit 25.7 dat de punten die met een constructiestap uit X gevormd kunnen worden, bevat zijn in $K = \mathbf{Q}(X, \overline{X})$ zelf of in een kwadratische uitbreiding van K. Iedere kwadratische uitbreiding van K is van de vorm $K \subset K(\sqrt{x})$, en dus bevat in $K_1 = K(\sqrt{K})$. Merk op dat met K ook $K(\sqrt{K})$ in zichzelf overgaat onder complexe conjugatie. Herhaling van het voorafgaande argument laat zien dat algemener de punten die in $i \geq 1$ stappen uit X geconstrueerd kunnen worden bevat zijn in K_i, met K_i als in 25.8. Dit laat zien dat $\mathcal{C}(X)$ bevat is in de kwadratische afsluiting van $K = \mathbf{Q}(X, \overline{X})$. □

Zelfs in het eenvoudigste interessante geval $X = \{0, 1\}$ is $\mathcal{C}(X) = \mathbf{Q}^{\mathrm{quad}}$ een oneindige lichaamsuitbreiding van $\mathbf{Q}(X, \overline{X}) = \mathbf{Q}$. Om te bepalen of een complex getal in de kwadratische afsluiting van $K \subset \mathbf{C}$ ligt is de volgende stelling daarom zeer nuttig.

25.10. Stelling. *Zij $K \subset \mathbf{C}$ een lichaam. Dan zijn de volgende uitspraken voor een element $x \in \mathbf{C}$ equivalent:*

1. *x is bevat in de kwadratische afsluiting van K;*
2. *er bestaan $n \in \mathbf{Z}_{\geq 0}$ en een keten*

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \mathbf{C}$$

   van tussenlichamen van $K \subset \mathbf{C}$ met $[E_i : E_{i-1}] = 2$ voor $1 \leq i \leq n$ en $x \in E_n$;
3. *x is algebraïsch over K, en de Galoisgroep van het polynoom f_K^x over K is een eindige 2-groep.*

Bewijs. (2) ⇒ (1). Zij $V \subset \mathbf{C}$ de verzameling van elementen die voldoen aan (2). Dan wordt voor $x \in V$ met bijbehorende keten $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_n$ iedere

kwadratische uitbreiding $E_i \subset E_{i+1}$ verkregen door adjunctie van een kwadraatwortel. Er volgt $E_i \subset K_i$ in de zin van definitie 25.8, en daarmee $x \in E_n \subset K_n \subset K^{\mathrm{quad}}$. Dit bewijst $V \subset K^{\mathrm{quad}}$.

(1) $\Rightarrow$ (2). Voor de inclusie $K^{\mathrm{quad}} \subset V$ met V als boven laten we zien dat V een deellichaam van $\mathbf{C}$ is dat K bevat en gesloten is onder adjunctie van kwadraatwortels. Het is evident dat K in V bevat is. Dat met $x \in V$ ook $\sqrt{x} \in V$ geldt is eveneens duidelijk: bekijk in de situatie van (2) voor $\sqrt{x} \notin E_n$ de verlenging $E_n \subset E_n(\sqrt{x})$ van de keten. Om tenslotte in te zien dat V een *deellichaam* van $\mathbf{C}$ is, verlengen we de keten $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r$ voor $x \in V$ met behulp van de keten $K = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_s$ voor $y \in V$ tot

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r = E_rF_0 \subset E_rF_1 \subset E_rF_2 \subset \ldots \subset E_rF_s.$$

Deze toren bestaat uit successieve uitbreidingen van graad ten hoogste 2, dus alle elementen van $\mathbf{Q}(x, y) \subset E_rF_s$ zijn bevat in V. Dit laat zien dat V een lichaam is.

(2) $\Rightarrow$ (3). Indien er voor $x \in \mathbf{C}$ een keten $K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_n$ bestaat als in (2), dan is x zeker algebraïsch over K. We verlengen nu de keten voor x zodanig dat de laatste uitbreiding *normaal* is over K. Neem hiervoor $M \subset \mathbf{C}$ de normale afsluiting van E_n over K, en $\sigma \in \mathrm{Gal}(M/K)$ willekeurig. Dan is de keten $K = \sigma[E_0] \subset \sigma[E_1] \subset \ldots \subset \sigma[E_n]$ een keten als in (2) voor $\sigma(x)$. Door de ketens voor alle $\sigma \in \mathrm{Gal}(M/K)$ zoals net uitgelegd te combineren tot één lange keten krijgen we een toren van kwadratische uitbreidingen eindigend in het compositum M van de collectie lichamen $\{\sigma[E_n]\}_{\sigma \in \mathrm{Gal}(M/K)}$. Er volgt dat $\mathrm{Gal}(M/K)$ een 2-groep is, en de Galoisgroep $\mathrm{Gal}(f_K^x)$ van de deeluitbreiding $\Omega_K^{f_K^x} \subset M$ over K is het dan ook.

(3) $\Rightarrow$ (2). Uit 10.17 ('oplosbaarheid van p-groepen') weten we dat in de 2-groep $G = \mathrm{Gal}(f_K^x)$ een keten $G = H_0 \supset H_1 \supset \ldots \supset H_n = 1$ van ondergroepen bestaat waarvoor alle indices $[H_i : H_{i+1}]$ gelijk zijn aan 2. De corresponderende deellichamen $E_i \subset \Omega_K^{f_K^x}$ geven een keten die aan de eisen in (2) voldoet. □

Opgave 4. Laat zien dat 25.10 correct is voor ieder lichaam K van karakteristiek verschillend van 2 indien men overal $\mathbf{C}$ door een algebraïsch afgesloten uitbreiding van K vervangt.

We keren nu terug naar de problemen 25.2–5. Indien we het voor 21.5 genoemde resultaat van Lindemann gebruiken, dat zegt dat het getal π transcendent is, volgt uit 25.9 en 25.10.3 dat π en $\sqrt{\pi}$ niet construeerbaar zijn: de cirkel is dus niet kwadrateerbaar met passer en liniaal.

Het getal $\sqrt[3]{2}$ is wel algebraïsch, maar van graad 3 over $\mathbf{Q}$ en derhalve niet bevat in enige uitbreiding van $\mathbf{Q}$ waarvan de graad een 2-macht is. Een verdubbeling van de kubus met passer en liniaal is dus ook niet mogelijk.

Voor $\alpha \in \mathbf{C}$ met $|\alpha|^2 = \alpha\overline{\alpha} = 1$ is de driedeling met passer en liniaal van de hoek $\angle 10\alpha$ behorende bij α niet mogelijk indien $X^3 - \alpha$ irreducibel is over $\mathbf{Q}(\alpha, \overline{\alpha}) = \mathbf{Q}(\alpha)$. Dit is het geval voor 'de meeste' α, waaronder alle transcendente waarden van α – zie de opgaven 20 en 21. In het zeldzame reducibele geval, dat bijvoorbeeld optreedt voor $\alpha = \pm 1$ en $\alpha = i$, is een ontbindingslichaam $\Omega_{\mathbf{Q}(\alpha)}^{X^3-\alpha}$ van graad ten hoogste 2 over K en is driedeling wel mogelijk.

In het geval van de regelmatige n-hoek dienen we te onderzoeken voor welke n de cyclotomische uitbreiding $\mathbf{Q}(\zeta_n)$ van 2-macht-graad over $\mathbf{Q}$ is. Dit is meer een aritmetisch dan een meetkundig probleem: voor welke n is $\varphi(n)$ een 2-macht? Heeft zo'n n priemfactorontbinding $n = \prod_{p|n} p^{e_p}$, dan geeft 6.16 de waarde $\varphi(n) = \prod_{p|n}(p-1)p^{e_p-1}$. We zien hieruit dat behalve de priem $p = 2$ alleen priemgetallen van de vorm $p = 2^m+1$ in de ontbinding van n voorkomen, en dat deze priemen bovendien exponent $e_p = 1$ hebben. Merk op dat $p = 2^m+1$ alleen priem kan zijn als m een macht van 2 is. Immers, indien m een echte deler u heeft waarvoor m/u *oneven* is, dan is $2^m + 1$ deelbaar door $2^u + 1$.

25.11. Definitie. *Een Fermat-priemgetal is een priemgetal van de vorm* $p = 2^{2^k} + 1$.

Schrijven we $F_k = 2^{2^k} + 1$ voor $k \geq 0$, dan zijn $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ en $F_4 = 65537$ priem. Het onvoorzichtige vermoeden van Fermat dat alle getallen F_k priem zijn verklaart de naamgeving in 25.11. Het getal $F_5 = 641 \cdot 6700417$ is niet priem, en de getallen F_k met $6 \leq k \leq 32$ zijn het ook niet. Het is niet bekend[16] of er waarden $k \geq 5$ bestaan waarvoor F_k *wel* priem is – men vermoedt dat dit niet het geval is. Afgezien van deze open vraag is er de volgende volledige oplossing van 25.5.

25.12. Stelling. *Zij $n \geq 3$ een geheel getal, en schrijf $n = 2^k \cdot n_0$ met n_0 oneven. Dan is de regelmatige n-hoek construeerbaar dan en slechts dan als n_0 een product van verschillende Fermat-priemgetallen is.* □

De construeerbaarheid voor n van de gegeven vorm werd door Gauss al in 1801 bewezen met behulp van de cyclotomische perioden uit 24.10.2. Een zeventienpuntige ster siert het Gauss-monument in Brunswijk, want een regelmatige 17-hoek is alleen door heel goed kijken van een cirkel te onderscheiden.

▶ Radicaalafsluiting

Een karakterisering als in 25.10 voor de kwadratische afsluiting van $\mathbf{Q}$ in $\mathbf{C}$ kan ook gegeven worden voor de *radicaalafsluiting* $\mathbf{Q}^{\mathrm{rad}}$ van $\mathbf{Q}$ in $\mathbf{C}$. De definitie lijkt sterk op die in 25.8.

25.13. Definitie. *Zij K van karakteristiek 0 met algebraïsche afsluiting $\overline{K}$. Dan is de radicaalafsluiting K^{rad} van K in $\overline{K}$ het lichaam $K^{\mathrm{rad}} = \bigcup_{i=0}^{\infty} K_{(i)}$, waarbij $K_{(0)} = K$ en*

$$K_{(i)} = K_{(i-1)}(\{w \in \overline{K} : w^n \in K_{(i-1)} \text{ voor zekere } n \geq 1\})$$

voor alle $i \geq 1$.

Het lichaam K^{rad} is het deellichaam van $\overline{K}$ bestaande uit de elementen die uit K verkregen kunnen worden door toepassen van de lichaamsoperaties (optellen, aftrekken, vermenigvuldigen en delen) en het 'trekken van wortels' van willekeurige hoge graad. Het is de kleinste uitbreiding van K die gesloten is onder alle worteltrekkingen.

Om separabiliteitsproblemen te vermijden nemen we in deze sectie verder aan dat K van karakteristiek 0 is. Voor lichamen van positieve karakteristiek p zijn alle

resultaten betreffende wortels van graad n ingeval n *niet* door p deelbaar is. Voor $n = p$ krijgt men de 'correcte' generalisatie door overal in plaats van p-machtwortels, die nulpunten zijn van polynomen $X^p - a \in K[X]$, nulpunten van *Artin-Schreier-polynomen* $X^p - X - a \in K[X]$ te gebruiken. Zie hiervoor de opgaven 32–34.

Binnen de algebraïsche afsluiting $\overline{K}$ van K hebben we een toren van uitbreidingen

$$K \subset K^{\mathrm{quad}} \subset K^{\mathrm{rad}} \subset \overline{K}.$$

Per definitie bestaat $\overline{K}$ uit alle elementen die nulpunten zijn van een monisch polynoom $f \in K[X]$, en het is een klassieke vraag of de nulpunten van een polynoom f 'met behulp van wortels' uit te drukken zijn in elementen van K. Voor $f \in K[X]$ van graad $n \leq 4$ bestaan er expliciete 'wortelformules' om de nulpunten van f in de coëfficiënten van f uit te drukken; we zullen ze nog tegenkomen aan het einde van deze paragraaf. Voor polynomen van graad $n \geq 5$ heeft men tot in de 19e eeuw gezocht naar soortgelijke formules. De beroemde toepassing van Galoistheorie in deze sectie laat zien dat voor $n \geq 5$ zo'n algemene formule *niet* bestaat. Het lichaam $\mathbf{Q}^{\mathrm{rad}}$ is niet gelijk aan $\overline{\mathbf{Q}}$, en we zullen in 25.17 polynomen in $\mathbf{Q}[X]$ construeren waarvan de nulpunten in $\overline{\mathbf{Q}}$ maar niet in $\mathbf{Q}^{\mathrm{rad}}$ liggen.

Een woord van waarschuwing is op zijn plaats bij het gebruiken van de notatie $\sqrt[n]{a}$ om een n-de machts wortel van een element a aan te geven. De meerduidigheid van deze notatie, die voor $n = 2$ nog tot een tekenkeuze beperkt is, leidt voor algemene n gemakkelijk tot vergissingen. Wegens $16 = 2^4$ ligt het bijvoorbeeld voor de hand te denken dat adjunctie van een nulpunt α van $X^8 - 16$ aan $\mathbf{Q}$ tot het lichaam $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2})$ leidt. Er geldt echter ook $16 = (-2)^4$, zodat $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-2})$ een *ander* lichaam is dat evenzeer 'verdedigbaar' is. Soortgelijke problemen doen zich voor bij het trekken van 'een' n-de machts wortel uit 1. Zo kan men de notatie $\sqrt[3]{1}$ beter vermijden, want niet alle nulpunten van $X^3 - 1$ brengen dezelfde uitbreiding van $\mathbf{Q}$ voort. In dit laatste geval hangt zelfs de graad van de uitbreiding van de keuze van de wortel af.

Opgave 5. Laat zien dat $1 + i$ en $1 - i$ eveneens achtstemachts wortels uit 16 zijn.

Men kan de meerduidigheid van de notatie $K \subset K(\sqrt[n]{a})$ voor de lichaamsuitbreiding verkregen door adjunctie van een n-de machts wortel uit $a \in K$ aan K beperken door alleen naar *irreducibele radicalen* te kijken. Hierbij legt men de extra eis op dat men slechts nulpunten van *irreducibele* polynomen $X^n - a \in K[X]$ adjungeert. In veel gevallen kan men de problematische wortelnotatie eenvoudig vermijden.

25.14. Definitie. *Een eindige lichaamsuitbreiding $K \subset L$ heet een radicaaluitbreiding als er een primitief element x voor $K \subset L$ bestaat met $x^n \in K$ voor zekere $n \geq 1$. Kunnen x en n zo gekozen worden dat $X^n - x^n$ irreducibel is in $K[X]$, dan heet $K \subset L$ een irreducibele radicaaluitbreiding.*

Opgave 6. Laat zien dat het cyclotomische lichaam $\mathbf{Q}(\zeta_5)$ een radicaaluitbreiding is van $\mathbf{Q}$, maar geen irreducibele radicaaluitbreiding.

Hoewel niet iedere radicaaluitbreiding irreducibel is, blijkt het lichaam K^{rad} niet af te hangen van het type radicaaluitbreidingen dat men bestudeert (opgave 31). Het hoofdresultaat dat we in deze sectie gaan bewijzen is het volgende analogon van 25.10.

25.15. Stelling. *Zij K een lichaam van karakteristiek 0 met algebraïsche afsluiting $\overline{K}$. Dan zijn de volgende uitspraken voor een element $x \in \overline{K}$ equivalent:*

1. *x is bevat in de radicaalafsluiting van K in $\overline{K}$;*
2. *er bestaan $n \in \mathbf{Z}_{\geq 0}$ en een keten van lichamen*

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \overline{K}$$

   met $E_{i-1} \subset E_i$ voor $1 \leq i \leq n$ een radicaaluitbreiding en $x \in E_n$;
3. *de Galoisgroep van het polynoom f_K^x over K is een oplosbare groep.*

Men noemt een eindige uitbreiding $K \subset E$ *oplosbaar* als de Galoisgroep $\mathrm{Gal}(M/K)$ van een normale afsluiting M van E over K een oplosbare groep is. Dit betekent wegens 10.14 dat er een keten van ondergroepen

$$\mathrm{Gal}(M/K) = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

in $\mathrm{Gal}(M/K)$ bestaat waarvoor steeds H_{i+1} normaal is in H_i en H_i/H_{i+1} cyclisch van priemorde. Uit 25.15 volgt dat een eindige uitbreiding $K \subset K(x)$ van een lichaam K van karakteristiek 0 oplosbaar is dan en slechts dan als men de vergelijking $f_K^x(X) = 0$ met radicalen kan 'oplossen'. Dit verklaart de naamgeving 'oplosbaarheid' in de groepentheorie.

Opgave 7. Laat zien dat een deeluitbreiding van een oplosbare uitbreiding oplosbaar is, en dat het compositum van twee oplosbare uitbreidingen ook weer oplosbaar is.

Alvorens 25.15 te bewijzen kijken we iets preciezer naar radicaaluitbreidingen. Het blijkt dat dergelijke uitbreidingen een elegante beschrijving toelaten ingeval het grondlichaam voldoende eenheidswortels bevat.

25.16. Stelling. *Zij $n \geq 2$ een geheel getal en K een lichaam dat een primitieve n-de eenheidswortel bevat.*

1. *Iedere cyclische uitbreiding $K \subset L$ van graad n is van de vorm $L = K(\sqrt[n]{a})$, met $a \in K$ en $\sqrt[n]{a}$ een nulpunt van $X^n - a \in K[X]$;*
2. *Voor $a \in K$ is $L = \Omega_K^{X^n - a}$ een cyclische uitbreiding van K van graad n/d, met d de grootste deler van n waarvoor a een d-de macht is in K.*

Bewijs. 1. Zij σ een voortbrenger van $\mathrm{Gal}(L/K)$ en $\zeta \in K$ een primitieve n-de eenheidswortel. We construeren een element $\alpha \in L^*$ met $\sigma(\alpha) = \zeta\alpha$ door te kijken naar de zogenaamde *Lagrange-resolvente*

$$\alpha = x + \zeta^{-1}\sigma(x) + \zeta^{-2}\sigma^2(x) + \ldots + \zeta^{1-n}\sigma^{n-1}(x),$$

waarbij $x \in L$ zo gekozen is dat $\alpha \neq 0$ geldt. Merk op dat zo'n x bestaat wegens het lemma van Artin-Dedekind 23.15. Een eenvoudige verificatie geeft nu $\sigma(\alpha) = \zeta\alpha$. Het element $a = \alpha^n$ ligt nu in K, want σ laat a invariant:

$$\sigma(a) = \sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n = a.$$

Omdat $\sigma(\zeta) = \zeta$ geldt, volgt door herhaald toepassen van σ op de identiteit $\sigma(\alpha) = \zeta\alpha$ de relatie $\sigma^i(\alpha) = \zeta^i\alpha$. Hieruit zien we dat de ondergroep $\mathrm{Gal}(L/K(\alpha)) \subset \mathrm{Gal}(L/K)$ van machten van σ die α vasthouden de triviale ondergroep $\langle\sigma^n\rangle = 1$ is. Er volgt $L = K(\alpha)$, met $\alpha = \sqrt[n]{a}$ een nulpunt van $X^n - a$.

2. Is α een nulpunt van $X^n - a$, dan geldt $X^n - a = \prod_{i=0}^{n-1}(X - \zeta^i\alpha)$ en $L = \Omega_K^{X^n-a} = K(\alpha)$. Voor $\alpha = a = 0$ is de uitspraak van de stelling duidelijk, dus we nemen verder $a \in K^*$. Voor $\tau \in \mathrm{Gal}(L/K)$ geldt dan $(\tau(\alpha)/\alpha)^n = (\tau(\alpha^n)/\alpha^n) = \tau(a)/a = 1$, dus de afbeelding

$$\begin{aligned} \psi: \quad \mathrm{Gal}(L/K) &\longrightarrow \langle\zeta\rangle \\ \tau &\longmapsto \frac{\tau(\alpha)}{\alpha} \end{aligned}$$

is welgedefinieerd. Het is ook een homomorfisme; immers, uit $\psi(\tau) = \zeta^i$ en $\psi(\tau') = \zeta^j$ vinden we

$$(\tau\tau')(\alpha) = \tau(\zeta^j\alpha) = \zeta^j\tau(\alpha) = \zeta^{i+j}(\alpha),$$

dus $\psi(\tau\tau') = \zeta^{i+j} = \psi(\tau)\psi(\tau')$. Het homomorfisme ψ is injectief, want een K-automorfisme dat α vasthoudt is de identiteit op $L = K(\alpha)$.

We concluderen dat $\mathrm{Gal}(L/K)$ cyclisch van graad n/d is, met d de index van $\psi[\mathrm{Gal}(L/K)]$ in $\langle\zeta\rangle$. Voor alle $\tau \in \mathrm{Gal}(L/K)$ geldt dan

$$1 = \psi(\tau)^{n/d} = (\tau(\alpha)/\alpha)^{n/d} = \tau(\alpha^{n/d})/\alpha^{n/d},$$

dus $b = \alpha^{n/d}$ is een element van K en $a = b^d$ een d-de macht in K. Hebben we omgekeerd $a = b^t$ met $t|n$ en $b \in K$, dan ligt de t-de eenheidswortel $\alpha^{n/t}/b$ in K, en dus ook $\alpha^{n/t}$ zelf. De identiteit boven (met $d = t$) laat weer zien dat $\psi[\mathrm{Gal}(L/K)]$ door n/t geannihileerd wordt, en in de ondergroep van index t in $\langle\zeta\rangle$ ligt. Er volgt $t \leq d$, dus d is de grootste deler van n waarvoor a een d-de macht is in K. □

Bewijs van 25.15. De equivalentie van (1) en (2) wordt net zo bewezen als voor 25.10: de verzameling V van elementen die aan (2) voldoen vormt een uitbreiding van K die gesloten is onder worteltrekkingen en bevat is in K^{rad}; er volgt $V = K^{\mathrm{rad}}$.

Voor (2) ⇒ (3) merken we eerst op dat we als in het bewijs van 25.10 mogen aannemen – na zo nodig de keten voor x verlengd te hebben – dat het laatste lichaam E_n van de keten normaal is over K. Stel dat $E_{i+1} = E_i(x_i)$ geldt, met $x_i^{n_i} \in E_i$. We laten ζ een primitieve eenheidswortel van orde N in $\overline{K}$ zijn, met N een gemeenschappelijk veelvoud van alle n_i, en nemen $L = E_n(\zeta)$. Dan is $K \subset L$ een normale uitbreiding die een keten

$$K = E_0 \subset E_0(\zeta) \subset E_1(\zeta) \subset E_2(\zeta) \subset \ldots \subset E_{n-1}(\zeta) \subset E_n(\zeta) = L$$

toelaat. In deze keten is de eerste stap $E_0 \subset E_0(\zeta)$ een abelse uitbreiding (opgave 24.47), en de radicaaluitbreidingen $E_i(\zeta) \subset E_{i+1}(\zeta)$ zijn wegens 25.16.2 cyclisch. Kijken we naar de corresponderende keten van ondergroepen in $\mathrm{Gal}(L/K)$, dan concluderen

we dat $\mathrm{Gal}(L/K)$ oplosbaar is. Wegens $\Omega_K^{f_K^x} \subset L$ is dan ook $\mathrm{Gal}(f)$ als quotiënt van $\mathrm{Gal}(L/K)$ oplosbaar.

Voor (3) $\Rightarrow$ (2), laat $f = f_K^x$ een oplosbare Galoisgroep $\mathrm{Gal}(f) = \mathrm{Gal}(\Omega_K^f/K)$ hebben van orde N. Is ζ weer een primitieve eenheidswortel van orde N, dan is in de toren $K = E_0 \subset E_1 = K(\zeta) \subset \Omega_K^f(\zeta)$ de eerste stap een radicaaluitbreiding. Wegens de aanname kan de uitbreiding $E_1 = K(\zeta) \subset \Omega_K^f(\zeta)$ als een keten van cyclische uitbreidingen van graad elk een deler van N worden geschreven. Wegens 25.16 zijn deze cyclische uitbreidingen radicaaluitbreidingen, en dit leidt tot de gewenste keten. □

▶ Onoplosbare polynomen

Om in te zien dat $\mathbf{Q}^{\mathrm{rad}}$ een strikt deellichaam is van $\overline{\mathbf{Q}}$ laten we zien dat er polynomen in $\mathbf{Q}[X]$ bestaan waarvan de Galoisgroep *niet* oplosbaar is. Omdat S_n en zijn ondergroepen oplosbaar zijn voor $n < 5$ heeft zo'n polynoom graad ten minste 5. De groep S_5 is niet oplosbaar, en er bestaan polynomen in $\mathbf{Q}[X]$ met groep S_5.

25.17. Stelling. *Zij $f \in \mathbf{Q}[X]$ een irreducibel polynoom van graad 5 met precies 3 reële nulpunten. Dan geldt $\mathrm{Gal}(f) \cong S_5$, en f heeft geen nulpunten in $\mathbf{Q}^{\mathrm{rad}}$.*

Bewijs. Wegens 24.7 is $\mathrm{Gal}(f)$ een ondergroep van S_5 van orde deelbaar door 5. Dit betekent dat $\mathrm{Gal}(f)$ een element van orde 5 bevat (stelling van Cauchy), en zo'n element in S_5 is noodzakelijkerwijs een 5-cykel. Vatten we $\overline{\mathbf{Q}}$ als deellichaam van $\mathbf{C}$ op, dan geeft complexe conjugatie een automorfisme van $\Omega_{\mathbf{Q}}^f$ dat wegens de aanname twee nulpunten van f verwisselt en de drie andere vasthoudt. Nu is $\mathrm{Gal}(f)$ een ondergroep van S_5 die een 5-cykel en een 2-cykel bevat, en zo'n ondergroep van S_5 is gelijk aan S_5 (opgave 2.54). In het bijzonder is $\mathrm{Gal}(f)$ niet oplosbaar en heeft f wegens 25.15 geen nulpunten in $\mathbf{Q}^{\mathrm{rad}}$. □

Het maken van een irreducibel vijfdegraadpolynoom met precies drie reële nulpunten is niet zo moeilijk. Kiezen we bijvoorbeeld

$$f = (X^2+2)\cdot(X+2)\cdot X\cdot(X-2)+2 = X^5 - 2X^3 - 8X + 2,$$

dan is dit een Eisensteinpolynoom bij 2 dat gemaakt is door een polynoom met precies drie reële nulpunten enigszins te verschuiven. Het polynoom f heeft zeker drie reële nulpunten wegens $f(0) = 2$ en $f(1) = -7$ en de limietwaarden voor $x \to \pm\infty$. Het zijn er niet meer, want $f' = 5X^4 - 6X^2 - 8$ wisselt maar twee keer van teken.

Opgave 8. Laat zien dat ook $f = (X^2+3)(X^2-9)X + 3$ groep S_5 heeft.

De hier gegeven constructie van onoplosbare polynomen van graad 5 kan worden gegeneraliseerd naar priemgraad $p \geq 5$ (opgave 27). Er bestaan ook diverse families[17] van polynomen $\{f_n\}_{n=1}^{\infty}$ met $\mathrm{Gal}(f_n) \cong S_n$.

► Wortelformules

Uit het feit dat S_n en zijn ondergroepen oplosbaar zijn voor $n \leq 4$ volgt dat de nulpunten van polynomen van graad ten hoogste 4 in radicalen uit te drukken zijn. Het bekendste voorbeeld van een 'wortelformule' is zonder twijfel de '*abc*-formule'

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

voor de nulpunten x_1 en x_2 van een kwadratisch polynoom $aX^2 + bX + c \in \mathbf{R}[X]$. De formule is niet alleen voor $\mathbf{R}$, maar voor ieder lichaam K van karakteristiek verschillend van 2 geldig. Merk op dat de formule de nulpunten in feite uitdrukt in b/a en c/a, en dat het geen beperking van de algemeenheid is om $a = 1$ te nemen. Het bewijs van de formule door 'kwadraat afsplitsen' komt erop neer dat men opmerkt dat in termen van de verschoven variabele $X + \frac{b}{2}$ het polynoom

$$X^2 + bX + c = \left(X + \tfrac{b}{2}\right)^2 - \tfrac{b^2-4c}{4} \in K[X]$$

zijn lineaire term verliest en door een kwadraatworteltrekking uit de *discriminant* b^2-4c van het polynoom $X^2 + bX + c$ 'opgelost' kan worden.

Opgave 9. Laat zien dat deze discriminant gelijk is aan die uit opgave 24.40 (b).

Voor polynomen van graad 3 is de situatie gecompliceerder. Schrijft men het polynoom als $X^3 + aX^2 + bX + c \in K[X]$, dan kan men in het geval dat K niet karakteristiek 3 heeft het polynoom in termen van $Y = X + \frac{a}{3}$ herschrijven als

$$Y^3 + pY + q,$$

waarbij p en q polynomiale uitdrukkingen in a, b en c zijn.

Opgave 10. Druk p en q in a, b en c uit.

Men kan verder komen met een truc die rond 1500 door de Italiaan Scipione del Ferro ($\pm$1465–1526) gevonden werd. Schrijf hiertoe $Y = u + v$, en merk op dat het polynoom nu te schrijven is als

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

Deze uitdrukking is gelijk aan 0 als we u en v laten voldoen aan

$$\begin{aligned} u^3 + v^3 &= -q \\ uv &= -p/3. \end{aligned} \tag{25.18}$$

Kennelijk zijn u^3 en v^3 nulpunten van het kwadratische polynoom

$$(X - u^3)(X - v^3) = X^2 + qX - (p/3)^3.$$

Nemen we ook nog aan dat K niet karakteristiek 2 heeft, dan kunnen we u^3 en v^3 met de zojuist gegeven kwadratische formule in radicalen uitdrukken en vinden we

$$Y = u + v = \sqrt[3]{-q/2 + \sqrt{(q/2)^2 + (p/3)^3}} + \sqrt[3]{-q/2 - \sqrt{(q/2)^2 + (p/3)^3}}.$$

Voor de derdemachtswortels u en v heeft men drie keuzes, maar wegens (25.18) ligt $v = -p/(3u)$ vast door de keuze van u, en vinden we zoals verwacht drie nulpunten.

Del Ferro maakte zijn methode niet wereldkundig, en de publicatie ervan in 1545 door zijn landgenoot Girolamo Cardano (1501–1576) staat in het teken van intrige en prioriteitstwisten.[18]

Ook wiskundig waren er de nodige problemen met de oplossing. Neemt men een polynoom met drie reële oplossingen, zoals $Y^3 - 7Y + 6 = (Y-1)(Y-2)(Y+3)$, dan leidt bovenstaande Cardano-Del Ferro-formule namelijk tot een uitdrukking voor de nulpunten in termen van complex geconjugeerde getallen:

$$\frac{1}{3}\sqrt[3]{-81 + 30\sqrt{-3}} + \frac{1}{3}\sqrt[3]{-81 - 30\sqrt{-3}}.$$

Als we ons realiseren dat complexe getallen in de zestiende eeuw onbekend waren en pas laat in de achttiende eeuw met Euler hun mysterieuze aureool verloren, dan laat zich de aanvankelijke verwarring omtrent deze *casus irreducibilis* indenken.

Opgave 11. Laat zien hoe de nulpunten 1, 2 en -3 uit de wortelrepresentatie volgen.
[Hint: $(3 + 2\sqrt{-3})^3 = -81 + 30\sqrt{-3}$.]

Ook de nulpunten van een algemeen polynoom van graad 4 over een lichaam van karakteristiek niet 2 of 3 kan men door een handigheidje in radicalen uitdrukken. De methode, die in Cardano's Ars Magna te vinden is, gaat terug op Cardano's leerling en schoonzoon Ludovici Ferrari (1522–1565). Men schrijft weer het algemene polynoom $X^4 + aX^3 + bX^2 + cX + d$ in termen van $Y = X + \frac{a}{4}$ en lost een vergelijking van de vorm

$$Y^4 = pY^2 + qY + r$$

op door deze te herschrijven als

$$(Y^2 + s)^2 = (p + 2s)Y^2 + qY + (s^2 + r).$$

Hierbij kiezen we s zodat het kwadratische polynoom in het rechterlid het *kwadraat* is van een eerstegraadspolynoom:

$$(Y^2 + s)^2 = (\sqrt{p + 2s}\,Y + \frac{q}{2\sqrt{p + 2s}})^2.$$

Hiertoe dient s te voldoen aan de kubische vergelijking

$$(p + 2s)(s^2 + r) = q^2/4,$$

en de Cardano-Del Ferro-formule geeft ons een radicaaluitdrukking voor s in termen van p, q en r. Men vindt vier waarden van Y door de beide kwadratische vergelijkingen

$$Y^2 + s = \pm\big(\sqrt{p+2s}\,Y + \frac{q}{2\sqrt{p+2s}}\big)$$

op te lossen. De resulterende wortelformule is meer indrukwekkend dan praktisch.

Opgave 12. Hoe moet de methode aangepast worden in het geval $p + 2s = 0$?

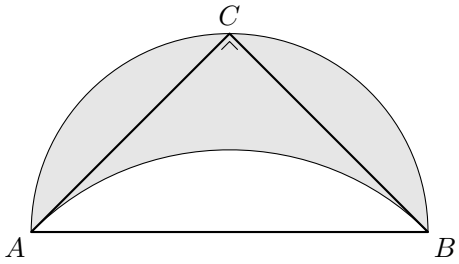
De Galoistheorie leert ons dat de slimmigheden van de Ars Magna niet tot het geval van graad 5 en hoger uitgebreid kunnen worden – niet iets wat direct duidelijk is uit bovenstaande manipulaties. In de volgende paragraaf zullen we de afgeleide wortelformules in Galoistheoretische termen interpreteren.

Zie opgave 37 voor een methode voor de vierdegraadsvergelijking die meer lijkt op de truc die we in het kubische geval toepasten.

Opgaven.

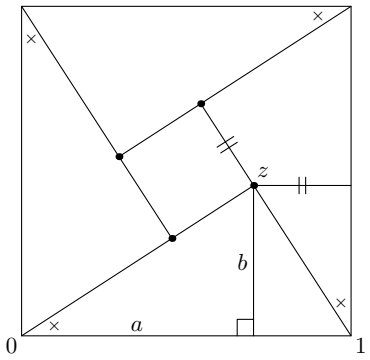
13. *(Standaardconstructies.)* Laat zien dat de volgende objecten construeerbaar zijn uitgaande van drie niet collineaire punten x, y en z in het complexe vlak:
    a. de middelloodlijn van het lijnstuk xy;
    b. de lijn door x loodrecht op de lijn door x en y;
    c. de lijn door z loodrecht op de lijn door x en y;
    d. de lijn door z evenwijdig met de lijn door x en y;
    e. de cirkel om z met straal $|x - y|$;
    f. de bissectrice van de hoek $\angle xyz$;
    g. de cirkel door x, y en z;
    h. rotatie van een punt om y over de hoek $\angle xyz$.

14. Laat AB de diagonaal van een vierkant zijn, en C een derde hoekpunt. Het *maantje van Hippocrates* op ABC is het gearceerde maantje in onderstaande figuur begrensd door de halve cirkel op AB en de kwartcirkel rakende aan AC en BC.



    Bewijs dat de oppervlakte van dit maantje gelijk is aan die van de driehoek ABC.

15. Een in de islamitische architectuur bekende figuur bestaat uit een klein vierkant dat, zoals in onderstaande figuur aangegeven, gelegen is in een groter vierkant met hetzelfde middelpunt. Hierbij is de lengte van de zijde van het kleine vierkant gelijk aan de *afstand* van een hoekpunt van het vierkant tot de dichtstbijzijnde zijde van het grote vierkant.



Ga na of het kleine vierkant construeerbaar is uitgaande van het grote vierkant.
[Hint: Kies coördinaten $0, 1 \in \mathbf{C}$ als in het plaatje, en vind $z = a + bi$.]

16. Zij $X \subset \mathbf{C}$ een deelverzameling, en stel dat z construeerbaar is uitgaande van X. Bewijs dat z construeerbaar is uitgaande van een *eindige* deelverzameling $X_0 \subset X$.

17. Zij $K \subset \mathbf{C}$ een lichaam dat in zichzelf overgaat onder complexe conjugatie. Bewijs dat $K^{\mathrm{quad}} \subset \mathbf{C}$ ook in zichzelf overgaat onder complexe conjugatie.

18. Laat zien dat de kwadratische afsluiting K^{quad} van K geen kwadratische uitbreidingen heeft.

19. Geef uitbreidingen $\mathbf{Q}^{\mathrm{quad}} \subset L$ van graad 3 en graad 5. *Bestaat er ook een uitbreiding van graad 4?

20. Laat zien dat driedeling van de hoek behorende bij $\alpha \in \mathbf{C}$ met $|\alpha| = 1$ niet mogelijk is met passer en liniaal als α transcendent is.

21. Is driedeling met passer en liniaal van de hoeken van een driehoek ABC mogelijk
    a. als ABC gelijkzijdig is?
    b. als de lengtes van de zijden van ABC gelijk zijn aan 44, 117 en 125?
    [Hint: $44^2 + 117^2 = 125^2$.]

22. Zij K een lichaam van karakteristiek niet 2, en definieer $K_1 = K(\sqrt{K})$ als in 25.8. Bewijs: $x \in \overline{K}$ ligt in $K_1 \setminus K$ dan en slechts dan als $K \subset K(x)$ een eindige Galoisuitbreiding is waarvoor de groep $G = \mathrm{Gal}(K(x)/K)$ abels is van exponent 2.

23. Zij $x \in \mathbf{C}$ een construeerbaar element. Definieer K_i als in 25.8 voor $K = K_0 = \mathbf{Q}$. Dan is de *(kwadratische) worteldiepte* van x het kleinste getal $i \geq 0$ waarvoor x bevat is in K_i. Bepaal de worteldiepte van de volgende elementen:
$$\sqrt{1+\sqrt{2}}, \qquad \sqrt{3-2\sqrt{2}}, \qquad \zeta_5, \qquad \zeta_{12}, \qquad \sqrt{1+2\sqrt{-6}}.$$
Hangt het antwoord af van de *keuze* van de diverse (eenheids)wortels in $\mathbf{C}$?

24. Definieer reële getallen $x_i \in \mathbf{R}_{\geq 0}$ recursief door $x_0 = 0$ en $x_{i+1} = \sqrt{2 + x_i}$ voor $i \geq 0$.
    a. Bewijs: $\mathbf{Q} \subset \mathbf{Q}(x_i)$ is cyclisch van graad 2^i.
    b. Bewijs: de worteldiepte van x_i is gelijk aan i voor alle $i \geq 0$.

25. Zij K een getallenlichaam. Bewijs: voor de lichamen K_i in de definitie 25.8 van K^{quad} geldt $K_i \neq K_{i+1}$ voor alle $i \geq 0$.

26. Definieer analoog aan de kwadratische worteldiepte de *radicaaldiepte* van een getal $x \in \mathbf{Q}^{\mathrm{rad}}$, en laat zien dat radicaaldiepte van x slechts van $\mathrm{Gal}(f^x_{\mathbf{Q}})$ afhangt. *Bestaan er elementen van willekeurig grote radicaaldiepte?

27. Zij $p = 2k + 3 > 3$ een priemgetal, en definieer

$$f = (X^2 + 2) \prod_{i=-k}^{k} (X - 2i) + 2 \in \mathbf{Q}[X].$$

    a. Bewijs dat f een irreducibel polynoom van graad p is.
    b. Bewijs dat f' geen $p - 1$ reële nulpunten heeft.
    [Hint: f' is een polynoom in X^2 en het teken van $f'(0)$ is bekend.]
    c. Bewijs dat f precies $p - 2$ reële nulpunten heeft. Concludeer dat f niet oplosbaar is door radicalen over $\mathbf{Q}$.

28. Geef een keten $\mathbf{Q} = E_0 \subset E_1 \subset \ldots \subset E_n$ van *irreducibele* radicaaluitbreidingen met $\zeta_{47} \in E_n$. Hier is ζ_{47} een primitieve 47-ste eenheidswortel.

29. Druk het reële getal $x = \cos(2\pi/7)$ uit in irreducibele radicalen over $\mathbf{Q}$.

30. Laat zien dat iedere uitbreiding $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$ oplosbaar is door *irreducibele* radicalen.
[Hint: inductie naar n.]

31. Zij K een lichaam van karakteristiek 0 en x een element uit $K^{\mathrm{rad}} \subset \overline{K}$. Bewijs: er bestaan $n \in \mathbf{Z}_{\geq 0}$ en een keten van lichamen

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_{n-1} \subset E_n \subset \overline{K}$$

met $x \in E_n$ en $E_{i-1} \subset E_i$ voor $1 \leq i \leq n$ een *irreducibele* radicaaluitbreiding.

32. *(Artin-Schreier-radicalen)* Zij K een lichaam van karakteristiek $p > 0$ en $K \subset L$ een cyclische uitbreiding van graad p. Bewijs: $L = K(\alpha)$ voor een nulpunt α van een Artin-Schreier-polynoom $f = X^p - X - a \in K[X]$.
[Dit is het analogon van 25.16.1 voor $n = p = \mathrm{char}(K)$. Hint: kijk naar de resolvente $\sum_{i=0}^{p-1} i\sigma^i(x)$ voor een element $x \in L$ met spoor 1.]

33. Zij K een lichaam van karakteristiek $p > 0$ en $K \subset L$ de uitbreiding verkregen door de nulpunten van het Artin-Schreier-polynoom $f = X^p - X - a \in K[X]$ aan K te adjungeren. Bewijs: $K \subset L$ is een cyclische uitbreiding van graad 1 of p.
[Dit is het analogon van 25.16.2 voor $n = p = \mathrm{char}(K)$. Hint: opgave 22.30.]

34. Zij K een lichaam van karakteristiek $p > 0$. De radicaalafsluiting van K is gedefinieerd als in 25.13, met de aanpassing dat K_i uit K_{i-1} verkregen wordt door alle $w \in \overline{K}$ te adjungeren die voldoen aan één van onderstaande voorwaarden:
    1. $w^n \in K_{i-1}$ voor zekere $n \geq 1$ met $p \nmid n$;
    2. $w^p - w \in K_{i-1}$ (informeel: w is een Artin-Schreier-radicaal over K).

    Formuleer en bewijs het analogon van 25.15 voor K.

35. Bepaal de reële oplossingen van de vergelijking $X^3 = 15X + 4$ met behulp van de Cardano-Del Ferro-formule.
[Dit wapenfeit werd in 1572 door Bombelli volbracht.]

36. Laat K een lichaam zijn met $\mathrm{char}(K) \neq 2, 3$. Laat zien dat $Y = \xi\eta(\xi + \eta)$ een nulpunt is van $Y^3 + pY + q \in K[Y]$ indien ξ en η voldoen aan

$$\xi^3, \eta^3 = \frac{3q}{2p} \pm \sqrt{(\frac{3q}{2p})^2 + \frac{p}{3}}.$$

Waarom geeft dit geen 9 verschillende nulpunten?
[Dit is Cayley's versie van de Cardano-Del Ferro-formule.]

37. Zij K als in de vorige opgave. Laat zien dat de vierdegraadsvergelijking $Y^4 = pY^2+qY+r$ over K opgelost wordt door $Y = \frac{u+v+w}{2}$ indien u^2, v^2 en w^2 nulpunten zijn van de kubische resolvente
$$X^3 - 2pX^2 + (p^2 + 4r)Y - q^2$$
en de tekens van u, v en w gekozen worden zodat $uvw = q$ geldt.

38. Laat zien dat het lichaam E_n in 25.10.2 altijd zo gekozen kan worden dat $E_n = K(x)$ geldt.

26 Toepassingen van Galoistheorie

De Galoistheorie is een nuttig instrument dat in een veelheid van situaties ingezet kan worden. Ideeën over invariantie van 'symmetrische uitdrukkingen' zijn tegenwoordig gemeengoed in de wiskunde, en er bestaat bijvoorbeeld ook een Galoistheorie van differentiaalvergelijkingen.[19] Deze paragraaf geeft een aantal ongerelateerde voorbeelden, en laat tevens zien hoe sommige uitdrukkingen waarvan de theorie zegt dat ze rationaal zijn expliciet berekend kunnen worden.

▶ Hoofdstelling van de algebra

Als eerste toepassing bewijzen we de in 21.11 genoemde hoofdstelling van de algebra, die zegt dat het lichaam $\mathbf{C}$ van complexe getallen algebraïsch afgesloten is. Er zijn vele bewijzen bekend, die alle bepaalde 'topologische argumenten' gebruiken. Dit is niet zo'n wonder, want de constructie van $\mathbf{R}$ uit $\mathbf{Q}$ middels Dedekindsneden of fundamentaalrijtjes is meer een topologische dan een algebraïsche constructie, en anders dan $\mathbf{C} = \mathbf{R}(i)$ is $\mathbf{Q}(i)$ niet een algebraïsch afgesloten lichaam. Wij gebruiken als topologisch argument de *tussenwaardestelling* voor polynomen in $\mathbf{R}[X]$: een polynoom $f \in \mathbf{R}[X]$ dat zowel een positieve als een negatieve waarde aanneemt, heeft een reëel nulpunt.

26.1. Lemma. *Ieder polynoom $f \in \mathbf{R}[X]$ van oneven graad heeft een reëel nulpunt. Voor iedere lichaamsuitbreiding $\mathbf{R} \subset E$ van oneven graad geldt $E = \mathbf{R}$.*

Bewijs. Voor $f \in \mathbf{R}[X]$ van oneven graad hebben $f(x)$ en $f(-x)$ voor voldoend grote x tegengesteld teken; wegens de tussenwaardestelling heeft f dan een reëel nulpunt.

Voor $\mathbf{R} \subset E$ van oneven graad en $\alpha \in E$ is de graad $[\mathbf{R}(\alpha) : \mathbf{R}]$ als deler van $[E : \mathbf{R}]$ weer oneven. Nu is $f_{\mathbf{R}}^{\alpha}$ een irreducibel polynoom van oneven graad. Omdat het een nulpunt in $\mathbf{R}$ heeft, is $f_{\mathbf{R}}^{\alpha}$ van graad 1. We vinden $\alpha \in \mathbf{R}$ en $E = \mathbf{R}$. □

26.2. Lemma. *Er bestaat geen lichaamsuitbreiding $\mathbf{C} \subset E$ met $[E : \mathbf{C}] = 2$.*

Bewijs. Om te laten zien dat $\mathbf{C}$ geen kwadratische uitbreidingen heeft is het voldoende te laten zien dat ieder element $x \in \mathbf{C}$ een (kwadraat)wortel heeft in $\mathbf{C}$. Schrijven we $x = s + it$ met $s, t \in \mathbf{R}$, dan komt de vergelijking $x = s + it = (c + di)^2$ neer op het vinden van $c, d \in \mathbf{R}$ met

$$\begin{aligned} c^2 - d^2 &= s \\ 2cd &= t. \end{aligned}$$

Voor $t = 0$ is $x = s$ reëel en krijgen we $cd = 0$. Voor $x = s \geq 0$ nemen we dan $d = 0$ en $c = \sqrt{x}$ de reële wortel uit x, voor $x = s < 0$ nemen we $c = 0$ en $d = \sqrt{-x}$ de reële wortel uit $-x$.

Voor $t \neq 0$ substitueren we $d = t/(2c)$ in de eerste vergelijking, hetgeen tot $4c^4 - 4sc^2 - t^2 = 0$ leidt. Omdat het polynoom $4X^4 - 4sX^2 - t^2$ voor $X = 0$ negatief is en voor grote X positief, impliceert de tussenwaardestelling dat er inderdaad een reëel nulpunt c van dit polynoom is. Dit leidt tot de gevraagde wortel. □

26.3. Hoofdstelling van de algebra. *Het lichaam* $\mathbf{C}$ *is algebraïsch afgesloten.*

Bewijs. We moeten bewijzen dat $\mathbf{C}$ geen niet-triviale algebraïsche uitbreidingen heeft. Zij $\mathbf{C} \subset L$ eindig algebraïsch, en laat M de normale afsluiting van L over $\mathbf{R}$ zijn. Dan is $\mathbf{R} \subset M$ een eindige Galoisuitbreiding, zeg met groep G. Is H een 2-Sylowondergroep van G in de zin van 10.7, dan is het invariantenlichaam $E = M^H$ van H een uitbreiding van $\mathbf{R}$ waarvan de graad $[E : \mathbf{R}] = [G : H]$ oneven is. Wegens 26.1 krijgen we $E = \mathbf{R}$ en $G = H$, dus G is een 2-groep. In het bijzonder is de ondergroep $\mathrm{Gal}(M/\mathbf{C}) \subset G$ een 2-groep. Wegens 10.17 is $\mathrm{Gal}(M/\mathbf{C})$ nu *oplosbaar*. Dit betekent als in 10.14 dat er een keten

$$\mathrm{Gal}(M/\mathbf{C}) = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

bestaat waarin steeds H_{i+1} een ondergroep van index 2 in H_i is. Onder de Galois-correspondentie geeft dit een keten $\mathbf{C} = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_k = M$ van kwadratische lichaamsuitbreidingen. Wegens 26.2 heeft deze keten lengte $k = 0$, dus $M = L = \mathbf{C}$. □

▶ Kwadratische reciprociteit

De in 24.12 uitgevoerde berekening van het kwadratische deellichaam van $\mathbf{Q}(\zeta_p)$ voor priemgetallen p stelt ons in staat een verrassende symmetrie te verklaren tussen het 'kwadratische karakter' van priemgetallen modulo elkaar. Een gevolg van dit fenomeen kwamen we al tegen in de opgaven 7.19 en 12.22: als 5 een primitieve wortel is modulo p, dan geldt $p \equiv \pm 2 \bmod 5$.

Is p een oneven priemgetal, dan is $\mathbf{F}_p^*$ een cyclische groep van even orde $p-1$. De unieke ondergroep $S_p \subset \mathbf{F}_p^*$ van index 2 bestaat uit de *kwadraatresten* modulo p. Het is de kern van het samengestelde homomorfisme

$$\begin{aligned} \mathbf{F}_p^* &\longrightarrow \quad \langle -1 \bmod p \rangle \quad \xrightarrow{\sim} \{\pm 1\} \\ x \bmod p &\longmapsto \; x^{(p-1)/2} \bmod p \; \longmapsto \left(\frac{x}{p}\right). \end{aligned}$$

Het symbool $\left(\frac{x}{p}\right)$, dat in karakteristiek 0 leeft, is het *Legendre-symbool* van x modulo p: het is 1 als x een kwadraat is in $\mathbf{F}_p^*$, en -1 als x een niet-kwadraat is in $\mathbf{F}_p^*$. Er lijkt geen enkele symmetrie te bestaan in x en p in de definitie van $\left(\frac{x}{p}\right)$; niettemin ontdekte Euler rond 1744 aan de hand van numerieke voorbeelden een variant van het volgende resultaat.

26.4. Kwadratische reciprociteitswet. *Laat* p *en* q *verschillende oneven priemgetallen zijn. Dan geldt*

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

In woorden: als p en q niet beiden 3 mod 4 zijn, dan kan het symbool $\left(\frac{p}{q}\right)$ 'op zijn kop' gezet worden. Voor $p \equiv q \equiv 3 \bmod 4$ klapt het teken om.

Euler slaagde er niet in dit resultaat te bewijzen, en zijn Franse collega Legendre (1752–1833), wiens naam aan de kwadratische symbolen verbonden is, ontkende ten onrechte dat zijn in 1785 gepubliceerde bewijs onvolledig was. Gauss vond het eerste correcte bewijs van 26.4 in 1796, en gaf later nog een aantal 'andere' bewijzen van zijn *theorema aureum*.

Bewijs. Uit 24.10 en 24.12 weten we dat $\mathbf{Q}(\zeta_p)$ een Galoisuitbreiding van $\mathbf{Q}$ is met groep $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{F}_p^*$, en dat de ondergroep $S_p \subset \mathbf{F}_p^*$ van kwadraten correspondeert met het tussenlichaam $\mathbf{Q}(\sqrt{p^*})$, waar $p^* = (-1)^{(p-1)/2}p$. Dit geeft

$$\left(\frac{q}{p}\right) = 1 \iff (q \bmod p) \in S_p \iff \sigma_q(\sqrt{p^*}) = \sqrt{p^*}.$$

Nu is het automorfisme σ_q een soort 'lift naar karakteristiek 0' van het Frobeniusautomorfisme F_q op $\overline{\mathbf{F}}_q$. Preciezer gezegd, als ζ een primitieve p-de eenheidswortel in een algebraïsche afsluiting $\overline{\mathbf{F}}_q$ van $\mathbf{F}_q$ is, dan heeft de reductieafbeelding $\mathbf{Z} \to \mathbf{F}_q$ een voortzetting

$$\begin{array}{rccc} r: & \mathbf{Z}[\zeta_p] & \longrightarrow & \overline{\mathbf{F}}_q \\ & \sum_i a_i\zeta_p^i & \longmapsto & \displaystyle\sum_i \overline{a}_i\zeta^i \end{array}$$

die voldoet aan $r \circ \sigma_q = F_q \circ r$. Het homomorfisme r stuurt de kwadratische Gauss-som $\tau_p = \sqrt{p^*} \in \mathbf{Z}[\zeta_p]$ naar een nulpunt $w = r(\sqrt{p^*})$ van $X^2 - p^* \in \mathbf{F}_q[X]$. De nulpunten van $X^2 - p^*$ in $\overline{\mathbf{F}}_q$ zijn verschillend, dus σ_q laat $\sqrt{p^*}$ invariant dan en slechts dan als F_q het element w invariant laat. Nu geldt

$$F_q(w) = w \iff w^{q-1} = 1 \iff (p^* \bmod q)^{(q-1)/2} = 1 \iff \left(\frac{p^*}{q}\right) = 1,$$

en we vinden

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \qquad \square$$

Opgave 1. Bewijs: als 5 een primitieve wortel is modulo een priemgetal $p \neq 2$, dan geldt $p \equiv \pm 2 \bmod 5$.

▶ Symmetrische polynomen

[wordt vervolgd....]

Opgaven.

Zie hiervoor een volgende druk van deze syllabus.

27 Categorieën en functoren.

Veel 'conceptuele wiskunde' laat zich kort en precies formuleren in termen van categorieën en functoren. Het betreft hier meer een efficiënt taalgebruik dan een theorie op zichzelf, en de wel gekscherend met 'abstract nonsense' aangegeven argumenten belichamen bij uitstek het al in paragraaf 1 beleden geloof in duidelijkheid en grotere toepasbaarheid door *abstractie*. Categorische begrippen vinden hun rechtvaardiging in de grote hoeveelheden concrete voorbeelden die zij in alle delen van de wiskunde hebben, en kennis van zulke voorbeelden vergemakkelijkt voor velen de appreciatie van categorische abstracties. De wiskundige inhoud van deze paragraaf is voornamelijk gelegen in de talrijke voorbeelden. Een ieder kan voorbeelden die hem niet aanspreken overslaan of, beter nog, door andere vervangen.

▶ Categorieën

27.1. Definitie. *Een categorie $\mathcal{C}$ bestaat uit objecten en, voor ieder tweetal objecten A, B in $\mathcal{C}$, een verzameling $\mathrm{Hom}_{\mathcal{C}}(A,B)$ van morfismen van A naar B. Voor ieder drietal objecten A, B en C in $\mathcal{C}$ is tevens een samenstellingsafbeelding van morfismen*

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(A,B)\times\mathrm{Hom}_{\mathcal{C}}(B,C) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,C)\\ (f,g) &\longmapsto g\circ f\end{aligned}$$

gegeven zodat aan de volgende twee eisen wordt voldaan:

1. *voor iedere $A\in\mathcal{C}$ bevat $\mathrm{Hom}_{\mathcal{C}}(A,A)$ een identiteit id_A die zich als een eenheid gedraagt met betrekking tot samenstellingen;*
2. *voor morfismen $A\xrightarrow{f}B\xrightarrow{g}C\xrightarrow{h}D$ geldt $(h\circ g)\circ f = h\circ(g\circ f)$.*

De *morfismen* in $\mathcal{C}$ heten, in overeenstemming met de in 27.1.2 gebruikte notatie, ook wel de *pijlen* of de *afbeeldingen* in $\mathcal{C}$. Merk echter op dat in de definitie van een categorie nergens over elementen wordt gepraat; we nemen niet per definitie aan dat morfismen afbeeldingen tussen verzamelingen zijn, of zelfs maar dat objecten uit elementen bestaan. Er wordt ook niet uitgesloten dat de verzameling $\mathrm{Hom}_{\mathcal{C}}(A,B)$ voor sommige A en B de lege verzameling is. Is de onderliggende categorie duidelijk, dan schrijft men gewoonlijk $\mathrm{Hom}(A,B)$ voor $\mathrm{Hom}_{\mathcal{C}}(A,B)$.

Om verzamelingstheoretische paradoxen als 'de verzameling van alle verzamelingen' te vermijden eist men niet dat de objecten van $\mathcal{C}$ een verzameling vormen. Ze vormen een *klasse* in de zin van de verzamelingenleer. We zullen niet ingaan op dergelijke logische finesses, die men meestal omzeilt door binnen een geschikt *universum* met zogenaamde *kleine categorieën* te werken.

De existentie van een identiteit voor elk object stelt ons in staat te spreken over inversen van morfismen, en daarmee over *isomorfismen* (morfismen met een tweezijdige inverse). Morfismen in $\mathrm{End}(A)=\mathrm{Hom}(A,A)$ heten *endomorfismen* van A, isomorfismen in $\mathrm{Hom}(A,A)$ heten *automorfismen* van A. Op de verzameling $\mathrm{Aut}(A)\subset\mathrm{End}(A)$ van automorfismen van A vormt samenstelling een groepsoperatie, en $\mathrm{Aut}(A)$ heet de *automorfismengroep* van A.

Opgave 1. Ga na dat de morfismen in $\mathrm{Aut}(A)$ een groep vormen onder samenstelling.

Vaak wordt aan een categorie gerefereerd in termen van de objecten, bijvoorbeeld 'de categorie **Ab** van abelse groepen' of 'de categorie $\mathbf{Mod}_R$ van R-modulen'. De lezer dient dan te begrijpen dat de morfismen in de categorie de 'bijbehorende' afbeeldingen zijn. In het geval van **Ab** zijn dit groepshomomorfismen, in het geval van $\mathbf{Mod}_R$ de R-moduul-homomorfismen.

De categorie **Ab** is op een voor de hand liggende manier een *deelcategorie* van de categorie **Grp** van alle groepen. Men noemt algemener een categorie $\mathcal{C}$ een deelcategorie van $\mathcal{D}$ als de objecten in $\mathcal{C}$ tevens objecten in $\mathcal{D}$ zijn, en er voor ieder tweetal objecten A en B in $\mathcal{C}$ een inclusie $\mathrm{Hom}_{\mathcal{C}}(A,B) \subset \mathrm{Hom}_{\mathcal{D}}(A,B)$ is. Geldt steeds $\mathrm{Hom}_{\mathcal{C}}(A,B) = \mathrm{Hom}_{\mathcal{D}}(A,B)$, dan heet $\mathcal{C}$ een *volle deelcategorie* van $\mathcal{D}$.

27.2. Voorbeelden. We noemen alvorens verder te gaan enkele van de talloze voorbeelden. Iedere lezer kan de lijst in zijn favoriete richting uitbreiden.

1. De categorie **Sets** van verzamelingen met als morfismen de 'gewone' afbeeldingen is een standaardvoorbeeld van een categorie. De deelcategorie **FSets** van eindige verzamelingen is een volle deelcategorie van **Sets**. Voor iedere groep G heeft men een categorie G**-sets** van G-verzamelingen in de zin van definitie 5.1. De morfismen in G**-sets** zijn de G-equivariante afbeeldingen uit opgave 5.31.

2. De categorie **Grp** van groepen met als morfismen de groepshomomorfismen bevat de categorie **Ab** van abelse groepen als volle deelcategorie. Analoog heeft men **Rng** voor ringen en ringhomomorfismen, met een volle deelcategorie **CRng** van commutatieve ringen. Dit zijn 'grote' categorieën, en vaak werkt men in kleinere deelcategorieën als de categorieën van *eindige* abelse groepen of *Noetherse* ringen.

3. De categorie $\mathbf{Vec}_K$ van vectorruimtes over een lichaam K heeft als morfismen de K-lineaire afbeeldingen. Er is de volle deelcategorie $\mathbf{FVec}_K$ van eindig-dimensionale K-vectorruimten.

4. De modulen over een ring R vormen met de R-homomorfismen een categorie $\mathbf{Mod}_R$. Veel van de 'standaardconstructies' die we in paragraaf 16 en 17 voor R-modulen ten tonele voerden (quotiënten, homomorfie- en isomorfiestelling, gevezelde sommen en producten) kan men puur categorisch uitvoeren in zogenaamde *abelse categorieën*, waarvan $\mathbf{Mod}_R$ het generieke voorbeeld is.

Neemt men voor R de groepenring $R = K[G]$ van een groep G over een lichaam K, dan is $\mathbf{Mod}_R = \mathbf{Rep}_K(G)$ de categorie van K-representaties van G. De moduulhomomorfismen hier zijn de K-lineaire afbeeldingen die de G-actie respecteren in de zin dat ze G-equivariant zijn (ga na!).

5. De categorie **Top** van topologische ruimten heeft als morfismen de continue afbeeldingen. Men werkt vaak in een volle deelcategorie van topologische ruimten die één of meer aanvullende eigenschappen hebben (samenhangend, Hausdorff, metrisch, compact, ...). De topologie $\mathbf{T}_X$ op een ruimte X is zelf óók een categorie. De objecten van $\mathbf{T}_X$ zijn de open verzamelingen in X, de morfismen de inclusies van open verzamelingen.

6. Uit iedere categorie $\mathcal{C}$ kan men de *tegengestelde categorie* $\mathcal{C}^{\mathrm{opp}}$ maken door 'alle pijlen om te draaien'. Preciezer gezegd: $\mathcal{C}^{\mathrm{opp}}$ heeft dezelfde objecten als $\mathcal{C}$, en de

morfismenverzameling $\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(A,B)$ staat in bijectief verband met $\mathrm{Hom}_{\mathcal{C}}(B,A)$, zeg door $f^{\mathrm{opp}} \leftrightarrow f$. De compositie van van morfismen in $\mathcal{C}^{\mathrm{opp}}$ is dan gedefinieerd door $f^{\mathrm{opp}} \circ g^{\mathrm{opp}} = (g \circ f)^{\mathrm{opp}}$.

Zoals uit bovenstaande voorbeelden blijkt, erven de verzamelingen $\mathrm{Hom}_{\mathcal{C}}(A,B)$ soms extra structuur van $\mathcal{C}$. Voor $\mathcal{C} = \mathbf{Ab}$ is $\mathrm{Hom}_{\mathcal{C}}(A,B)$ een abelse groep (opgave 4.41), en voor $\mathcal{C} = \mathbf{Mod}_R$ is, in het geval de ring R commutatief is, iedere abelse groep $\mathrm{Hom}_{\mathcal{C}}(A,B)$ op natuurlijke wijze een R-moduul (opgave 16.3).

Opgave 2. Laat zien dat in beide bovenstaande situaties $\mathrm{End}(A)$ op natuurlijke wijze een *ring* met eenhedengroep $\mathrm{Aut}(A)$ is. Is deze ring noodzakelijk commutatief?

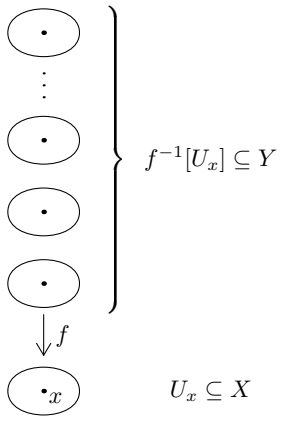
De morfismen in een categorie $\mathcal{C}$ vormen zelf ook weer een categorie, $\mathbf{Mor}(\mathcal{C})$. Een morfisme $\phi : f \to g$ in $\mathbf{Mor}(\mathcal{C})$ van $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ naar $g \in \mathrm{Hom}_{\mathcal{C}}(C,D)$ is een geordend paar $\phi = (\phi_1, \phi_2)$ van morfismen in $\mathcal{C}$ dat het diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi_1} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ B & \xrightarrow{\phi_2} & D \end{array}$$

laat commuteren. Interessant zijn vaak de deelcategorieën van $\mathbf{Mor}(\mathcal{C})$ die men krijgt door morfismen van of naar een vast object in $\mathcal{C}$ te beschouwen. In het eerste geval neemt men in bovenstaand diagram $A = C$ vast en bekijkt alleen de morfismen $\phi = (\phi_1, \phi_2)$ in $\mathbf{Mor}(\mathcal{C})$ met $\phi_1 = \mathrm{id}_A$. In het tweede geval neemt men $B = D$ vast en morfismen $\phi = (\phi_1, \phi_2)$ met $\phi_2 = \mathrm{id}_B$. Men spreekt wel van de categorie van objecten over een vast basisobject.

27.3. Voorbeelden. Voor iedere commutatieve ring R kan men de categorie $\mathbf{CAlg}_R$ van commutatieve R-algebra's opvatten als de categorie van 'ringen over R'. Immers, een morfisme van R-algebra's $A_1 \to A_2$ respecteert de R-algebra-structuur en is daarmee een morfisme van de structuurafbeeldingen $f_i : R \to A_i$ in $\mathbf{CRng}$ dat op R de identiteit is.

Een interessant voorbeeld in de topologie van objecten over een vast basisobject wordt gegeven door de categorie $\mathbf{Cov}_X$ van *overdekkingen* van een topologische ruimte X. Een afbeelding $f : Y \to X$ van topologische ruimten heet een *overdekking* als ieder punt $x \in X$ een omgeving $U_x \subset X$ heeft zodat $f^{-1}[U_x] \xrightarrow{f} U_x$ een *triviale overdekking* is. Dit betekent dat de *vezel* $f^{-1}(x)$ boven x discreet is in Y, en dat er een homeomorfisme $f^{-1}(x) \times U_x \to f^{-1}[U_x]$ is dat samengesteld met f de projectie op de tweede coördinaat geeft. Een morfisme ϕ van een overdekking $f_1 : Y_1 \to X$ naar $f_2 : Y_2 \to X$ (een *dektransformatie*) is een continue afbeelding $\phi : Y_1 \to Y_2$ met $f_2 \circ \phi = f_1$.



▶ Functoren

27.4. Definitie. *Een (covariante) functor $F : \mathcal{C} \to \mathcal{D}$ is een afbeelding die aan elk object $A \in \mathcal{C}$ een object $F(A) \in \mathcal{D}$ toevoegt en aan elk morfisme $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ een morfisme $f_* = F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Hierbij geldt $(\mathrm{id}_A)_* = \mathrm{id}_{F(A)}$ en $(f \circ g)_* = f_* \circ g_*$.*

Men zegt vaak kortweg dat de constructie van $F(A) \in \mathcal{D}$ uit $A \in \mathcal{C}$ 'functorieel is'. Zo'n constructie heeft allerlei prettige 'stabiliteitseigenschappen' die functoriële begrippen aanzienlijk hanteerbaarder maken dan niet-functoriële.

27.5. Voorbeelden. 1. Het vormen van de commutatorondergroep $[G, G]$ van een groep G is een functor **Grp** $\to$ **Grp**. De functor $G \mapsto G^{\mathrm{ab}} = G/[G, G]$ die aan elke groep zijn abels gemaakte quotiënt toevoegt is een functor **Grp** $\to$ **Ab**. De vorming van het centrum $Z(G)$ uit G is *geen* functor **Grp** $\to$ **Ab**, want een groepshomomorfisme $f : G_1 \to G_2$ induceert niet in het algemeen een groepshomomorfisme tussen de centra.

2. De 'eenhedengroepfunctor' U : **Rng** $\to$ **Grp** vormt van een ring R de eenhedengroep R^*. Voor iedere $n \geq 1$ zijn er functoren GL_n : **CRng** $\to$ **Grp** en Mat_n : **CRng** $\to$ **Rng** die aan een commutatieve ring R de groep $\mathrm{GL}_n(R)$ van inverteerbare $n \times n$-matrices en de ring $\mathrm{Mat}_n(R)$ van $n \times n$-matrices met coëfficiënten in R toevoegen. Merk op dat GL_1 en U 'dezelfde' functor zijn.

3. De afbeelding **CRng** $\to$ **CRng** die aan elke commutatieve ring R de *gereduceerde ring* R/N_R toevoegt, met N_R het nilradicaal van R, is een functor. Op de deelcategorie van gereduceerde ringen is het de identiteit.

4. Een *vergeetfunctor* is een functor die een deel van de structuur van een object vergeet. Zo heeft men vergeetfunctoren van de meeste onder 27.2 genoemde categorieën naar **Sets** die aan een groep (ring, vectorruimte, etc.) de onderliggende verzameling toevoegen. Van dezelfde aard zijn de functoren van **Rng** en $\mathbf{Vec}_K$ naar **Ab** die aan een ring of vectorruimte de onderliggende abelse optelgroep toevoegen, of de functoren $\mathbf{Rep}_K(G) \to \mathbf{Vec}_K$ en G-**sets**$\to$**Sets** die de G-werking vergeten.

5. De vorming van de fundamentaalgroep $\pi(X)$ van een topologische ruimte is *geen* functor **Top** $\to$ **Grp**, zelfs niet als we ons tot wegsamenhangende ruimten beperken. Men voert hiertoe de categorie $\mathbf{Top}_*$ van topologische ruimten X met basispunt $x \in X$ in, en definieert een morfisme $(X, x) \to (Y, y)$ als een continue afbeelding $f : X \to Y$ met $f(x) = y$. Merk op dat $\mathbf{Top}_*$ niets anders is dan de categorie van 'topologische ruimten over een éénpuntsruimte' in de zin van het tweede voorbeeld in 27.3. De vorming $(X, x) \mapsto \pi(X, x)$ van de fundamentaalgroep in het basispunt x is nu wel een functor $\mathbf{Top}_* \to$ **Grp**.

6. In iedere categorie $\mathcal{C}$ geeft een object $X \in \mathcal{C}$ aanleiding tot een *representatiefunctor* $\mathrm{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to$ **Sets** gegeven door $A \mapsto \mathrm{Hom}(X, A)$. Er is ook iets als een 'functor' $\mathrm{Hom}_{\mathcal{C}}(-, X)$ naar **Sets**, maar dit is geen functor in de zin van 27.4 omdat alle pijlen worden 'omgedraaid'.

27.6. Definitie. *Een contravariante functor $F : \mathcal{C} \to \mathcal{D}$ is een afbeelding die aan elk object $A \in \mathcal{C}$ een object $F(A) \in \mathcal{D}$ toevoegt en aan elk morfisme $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$*

een morfisme $f^* = F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(B), F(A))$. *Hierbij geldt* $(\mathrm{id}_A)^* = \mathrm{id}_{F(A)}$ *en* $(f \circ g)^* = g^* \circ f^*$.

27.7. Voorbeelden. Zoals we al zagen zijn de representatiefunctoren $\mathrm{Hom}_{\mathcal{C}}(-, X)$ in iedere categorie $\mathcal{C}$ contravariant. Speciale gevallen van zulke functoren zijn diverse *dualiteitsfunctoren* als $M \mapsto M^* = \mathrm{Hom}_R(M, R)$ voor de categorie $\mathbf{Mod}_R$ van modulen over R of de functor $A \mapsto A^\vee = \mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$ op $\mathbf{Ab}$.

Iets algemener zijn er voor veel categorieën $\mathcal{C}$ contravariante functoren die aan $A \in \mathcal{C}$ een verzameling van 'R-waardige functies op A' toevoegen. Hierbij is R meestal een welgekozen ring, hetgeen er toe leidt dat de verzameling van R-waardige functies aanvullende structuur van R erft. Bij wijze van voorbeeld kan men denken aan de verzameling $C(X)$ van continue reëelwaardige functies op een topologische ruimte X, die via de gebruikelijke puntsgewijze operaties een *ringstructuur* van $\mathbf{R}$ erft.

Opgave 3. Laat zien dat de 'identiteit' $\mathcal{C} \to \mathcal{C}^{\mathrm{opp}}$ een contravariante functor is, en dat de contravariante functoren $F : \mathcal{C} \to \mathcal{D}$ bijectief corresponderen met de functoren $F : \mathcal{C} \to \mathcal{D}^{\mathrm{opp}}$.

In de categorieëntheorie is de definitie van de objecten steeds onlosmakelijk verbonden met een definitie van morfismen van dergelijke objecten. De verzameling $\mathbf{Fun}(\mathcal{C}, \mathcal{D})$ van functoren $\mathcal{C} \to \mathcal{D}$ wordt zelf ook weer een categorie indien men *morfismen van functoren*, ook wel *natuurlijke transformaties* genaamd, als volgt definieert.

27.8. Definitie. *Voor morfismen* $F, G : \mathcal{C} \to \mathcal{D}$ *is een natuurlijke transformatie* $F \to G$ *een collectie van morfismen* $\{\tau_C : F(C) \to G(C)\}_{C \in \mathcal{C}}$ *in* $\mathcal{D}$ *zodanig dat voor ieder morfisme* $f : C \to C'$ *in* $\mathcal{C}$ *het diagram*

$$\begin{array}{ccc} F(C) & \xrightarrow{\tau_C} & G(C) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(C') & \xrightarrow{\tau_{C'}} & G(C') \end{array}$$

commuteert. Als alle morfismen τ_C *isomorfismen zijn, heten de functoren* F *en* G *natuurlijk equivalent of isomorf.*

27.9. Voorbeelden. 1. Voor de functoren $\mathrm{GL}_n : \mathbf{CRng} \to \mathbf{Grp}$ en $U : \mathbf{CRng} \to \mathbf{Grp}$ gedefinieerd in 27.5.2 is de determinantafbeelding $\det : \mathrm{GL}_n \to U$ een natuurlijke transformatie. Voor $n = 1$ is het een isomorfisme van functoren.

2. In de categorie van eindige abelse groepen is de vorming $G \mapsto G^\vee$ van de duale groep $G^\vee = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ een contravariante functor $D : \mathbf{FAb} \to \mathbf{FAb}$ die iedere groep op een isomorfe groep afbeeldt, maar er is geen 'natuurlijke keus' voor een isomorfisme $G \xrightarrow{\sim} G^\vee$. Zo'n keuze is er wel voor de vorming $G \mapsto G^{\vee\vee}$ van de dubbel-duale, immers een element $x \in G$ definieert op natuurlijke wijze een homomorfisme $G^\vee \to \mathbf{Q}/\mathbf{Z}$ door $f \mapsto f(x)$. Als gevolg hiervan is de covariante functor $\mathbf{FAb} \to \mathbf{FAb}$ gegeven door $G \mapsto G^{\vee\vee}$ natuurlijk isomorf met de identiteit. Men zegt wel dat een eindige abelse groep G *canoniek isomorf* is met zijn dubbel-duale $G^{\vee\vee}$. Dit betekent dat beide groepen voor praktische doeleinden meestal geïdentificeerd kunnen worden. Soortgelijke opmerkingen gelden voor de vorming van de duale vectorruimte in de

categorie $\mathbf{FVec}_K$ van eindig-dimensionale vectorruimten. Als bij eindige groepen is de eindigheidsconditie op de dimensie essentieel om een canoniek isomorfisme $V \to V^{**}$ te krijgen. In het oneindig-dimensionale geval, dat in de functionaalanalyse bestudeerd wordt, is aanvullende structuur nodig om zogenaamde *reflexieve ruimtes* te krijgen.

3. De vergeetfunctor $\mathbf{Rng} \to \mathbf{Sets}$ van ringen naar verzamelingen is isomorf met de representatiefunctor $\mathrm{Hom}_{\mathbf{Rng}}(\mathbf{Z}[X], -)$. Immers, voor iedere ring R is er een canonieke bijectie $\mathrm{Hom}_{\mathbf{Rng}}(\mathbf{Z}[X], R) \xrightarrow{\sim} R$ gegeven door $f \mapsto f(X)$. Men noemt in het algemeen een functor $F : \mathcal{C} \to \mathbf{Sets}$ die isomorf is met een representatiefunctor een *representeerbare functor*. Dit concept is sinds Grothendieck van fundamenteel belang in de arithmetische algebraïsche meetkunde. Wiles' bewijs van de laatste stelling van Fermat bestaat bijvoorbeeld voor een groot deel uit een bewijs van de representeerbaarheid van bepaalde functoren in de theorie van de elliptische krommen.

27.10. Definitie. *De categorieën $\mathcal{C}$ en $\mathcal{D}$ heten equivalent als er functoren $F : \mathcal{C} \to \mathcal{D}$ en $G : \mathcal{D} \to \mathcal{C}$ bestaan zodat $G \circ F$ en $F \circ G$ isomorf zijn met de identiteit op respectievelijk $\mathcal{C}$ en $\mathcal{D}$. Bestaan er contravariante functoren met deze eigenschap, dan heten $\mathcal{C}$ en $\mathcal{D}$ anti-equivalent.*

27.11. Voorbeelden. 1. Voorbeeld 27.9.2 laat zien dat de categorie **FAb** van eindige abelse groepen anti-equivalent is met zichzelf onder de dualiteitsfunctor D.

2. Zij L/K een eindige Galoisuitbreiding L/K van lichamen met groep G. De *hoofdstelling van de Galoistheorie* zegt dat de categorie van tussenlichamen $\mathbf{Fld}_{L/K}$, met de natuurlijke inclusies als morfismen, anti-equivalent is met de categorie $\mathbf{Sgrp}_G$ van ondergroepen van G, met eveneens de natuurlijke inclusies als morfismen. De functoren $\mathbf{Fld}_{L/K} \to \mathbf{Sgrp}_G$ en $\mathbf{Sgrp}_G \to \mathbf{Fld}_{L/K}$ in definitie 27.10 worden gegeven door $M \mapsto \mathrm{Aut}(L/M)$ en $H \mapsto L^H$.

3*. De hoofdstelling van de Galoistheorie voor topologische ruimten zegt dat de categorie $\mathbf{Cov}_X$ van overdekkingen van een wegsamenhangende topologische ruimte X onder milde voorwaarden anti-equivalent is met de categorie $\pi(X)$**-sets** van verzamelingen met een werking van de fundamentaalgroep $\pi(X)$. Voor elk punt $x \in X$ is er de *vezelfunctor* $F_x : \mathbf{Cov}_X \to \mathbf{Sets}$ die een overdekking $f : Y \to X$ naar $f^{-1}(x)$ stuurt, en de fundamentaalgroep $\pi(X, x)$ werkt op de vezel $f^{-1}(x)$. Het beeld van $y \in f^{-1}(x)$ onder de homotopieklasse van een pad $w \subset X$ in x is hier gedefinieerd als het eindpunt van het unieke pad $w^* \subset Y$ dat beginpunt y heeft en onder f op w projecteert.

▶ Universele constructies

We merkten in paragraaf 17 reeds op dat veel van de standaardconstructies voor groepen, ringen en modulen oplossingen zijn van bepaalde universele problemen in een onderliggende categorie. Men kan dan ook veel van de reeds bekende definities in algemene categorische termen formuleren.

27.12. Definitie. *Een product van een familie objecten $\{A_i\}_{i \in I}$ in $\mathcal{C}$ is een object $P \in \mathcal{C}$ voorzien van morfismen $p_i : P \to A_i$ met de eigenschap dat er gegeven een object $T \in \mathcal{C}$ en morfismen $f_i : T \to A_i$ een uniek morfisme $f : T \to P$ bestaat met*

$p_i \circ f = f_i$.
Een coproduct of som van $\{A_i\}_{i\in I}$ *in* $\mathcal{C}$ *is een object* $S \in \mathcal{C}$ *voorzien van morfismen* $\varepsilon_i : A_i \to S$ *met de eigenschap dat er gegeven een object* $T \in \mathcal{C}$ *en morfismen* $g_i : A_i \to T$ *een uniek morfisme* $f : S \to T$ *bestaat met* $g \circ \varepsilon_i = g_i$.

We zagen al in 17.7 dat objecten met een dergelijke universele karakterisering *als* ze bestaan op een uniek isomorfisme na bepaald zijn. Stelling 17.8 zegt niets anders dan dat sommen en producten bestaan in de categorie $\mathbf{Mod}_R$ van modulen over een ring.

27.13. Voorbeelden. 1. In de categorie **Sets** is de som van een familie verzamelingen niets anders dan de *disjuncte vereniging*. Het product van een aantal verzamelingen is het *cartesisch product* van de verzamelingen. Als de onderliggende verzamelingen groepen of ringen zijn, heeft dit product een natuurlijke groeps- dan wel ringstructuur, en we zien dat producten in **Grp** en **Rng** op de bekende wijze geconstrueerd kunnen worden.

2. In de categorie van topologische ruimten is een som hetzelfde als een disjuncte vereniging. Voor het product neemt men het cartesisch product met de bekende producttopologie.

3. De constructie van sommen in **Grp** is niet zo eenvoudig. In de categorie **Ab** van abelse groepen ($\mathbf{Z}$-modulen) werkt de constructie van 17.8, maar in het niet-abelse geval krijgt men veel ingewikkelder groepen. Zo is de som van twee oneindige cyclische groepen $\langle\sigma\rangle$ en $\langle\tau\rangle$ een 'vrije niet-abelse groep op twee voortbrengers'. De groep in opgave 2.26 is zo'n groep. Men kan laten zien dat de modulaire groep $\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$ de som is van een ondergroep van orde 2 met voortbrenger $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ en een ondergroep van orde 3 met voortbrenger $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$.

4. Ook voor ringen heeft men het bekende product van ringen. In **CRng** heeft men als som het *tensorproduct* uit paragraaf 17 van de ringen als algebra's over $\mathbf{Z}$.

5. In de categorie van objecten over een vast basisobject A is het product van $X \to A$ en $Y \to A$ het *gevezelde product* van X en Y over A. De som van $A \to X$ en $A \to Y$ is de *gevezelde som* van X en Y over A.

Opgave 4. Laat zien dat deze definities in overeenstemming zijn met die in opgave 9.53.

Opgaven.

5. Ga na welke van de volgende constructies functorieel zijn.
   a. de vorming van de automorfismengroep $\mathrm{Aut}(G)$ van G;
   b. de restrictie en extensie van scalairen voor modulen over een ring;
   c. de vorming van de algebraïsche afsluiting van een lichaam;
   d. de vorming van de normale afsluiting van een lichaam;
   e. de vorming van de algebraïsche afsluiting in $\mathbf{C}$ van een deellichaam $K \subset \mathbf{C}$.

   Geef voor de functoriële constructies aan wat de onderliggende categorieën zijn.

6. Zij G een groep en G**-sets** de categorie van verzamelingen met een werking van G. Bepaal de automorfismengroep van G opgevat als G-verzameling onder de reguliere werking. *Is er een vergelijkbare directe beschrijving als we G beschouwen als G-verzameling onder de conjugatiewerking?

7. Laat zien dat ieder isomorfisme $f : A \to B$ in een categorie een groepsisomorfisme $\phi_f : \mathrm{Aut}(A) \to \mathrm{Aut}(B)$ van de corresponderende automorfismengroepen induceert, en dat voor ieder tweetal isomorfismen $f, f' : A \to B$ er inwendige automorfismen α en β van respectievelijk $\mathrm{Aut}(A)$ en $\mathrm{Aut}(B)$ bestaan met $\phi_f \circ \alpha = \phi_{f'} = \beta \circ \phi_f$.

8. Geef de definitie van een automorfisme van een functor $F : \mathcal{C} \to \mathcal{D}$, en laat zien dat deze automorfismen een groep $\mathrm{Aut}(F)$ vormen. Bepaal $\mathrm{Aut}(F)$ voor de vergeetfunctor $F :$G$-$**sets** $\to$ **Sets**.

9. Laten $F : \mathcal{C} \to \mathcal{D}$ en $G : \mathcal{D} \to \mathcal{C}$ functoren zijn. We zeggen dat F en G *geadjungeerde functoren* zijn als voor ieder paar objecten $C \in \mathcal{C}$ en $D \in \mathcal{D}$, er een bijectie

$$\mathrm{Hom}_{\mathcal{C}}(C, G(D)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(F(C), D)$$

   is die natuurlijk is in C en D. Geef expliciet aan wat dit betekent, en bepaal de linksgeadjungeerde F van G in het geval dat G de vergeetfunctor **Ab** $\to$ **Grp**, de vergeetfunctor $\mathbf{Vec}_K \to$ **Sets** of de vergeetfunctor **Fld** $\to$ **Dom** (van lichamen naar domeinen) is.

10. Construeer linksgeadjungeerden bij de vergeetfunctoren $\mathbf{Mod}_R \to$ **Sets** en $\mathbf{Mod}_R \to$ **Ab**.

11. Laten F en G geadjungeerde functoren $\mathbf{Mod}_R \to \mathbf{Mod}_R$ zijn voor een commutatieve ring R. Definieer links- en rechtsexact voor functoren $\mathbf{Mod}_R \to \mathbf{Mod}_R$, en laat zien dat F rechtsexact is dan en slechts dan als G linksexact is.
    [Hint: kijk naar 17.12 voor een concreet voorbeeld.]

12. Een object X in een categorie $\mathcal{C}$ heet een *beginobject* als ieder object $Y \in \mathcal{C}$ een uniek morfisme $X \to Y$ toelaat, en een *eindobject* als als ieder object $Y \in \mathcal{C}$ een uniek morfisme $Y \to X$ toelaat. Laat zien dat dergelijke objecten op een uniek isomorfisme na bepaald zijn *als* ze bestaan. Ga na of ze bestaan in de categorieën **Sets**, **Grp**, **Rng** en $\mathbf{Mod}_R$.

13. Zij R een commutatieve ring. Laat zien dat een som van A_1 en A_2 in de categorie $\mathbf{CAlg}_R$ van commutatieve R-algebra's het tensorproduct $A_1 \otimes_R A_2$ is.

14. Laat zien dat de eenhedengroepfunctor $R \mapsto R^*$, gezien als functor **Rng** $\to$ **Sets**, isomorf is met de representatiefunctor $\mathrm{Hom}_{\mathbf{Rng}}(\mathbf{Z}[X, X^{-1}], -)$.

15. *(Yoneda's lemma.)* Laat zien dat iedere natuurlijke transformatie van de representatiefunctor $F_X = \mathrm{Hom}_{\mathcal{C}}(X, -)$ naar $F_Y = \mathrm{Hom}_{\mathcal{C}}(Y, -)$ geïnduceerd wordt door een uniek morfisme $Y \to X$ in $\mathcal{C}$. Concludeer dat de representatiefunctoren F_X en F_Y isomorf zijn dan en slechts dan als de objecten X en Y isomorf zijn in $\mathcal{C}$.
[Hint: kijk naar het beeld van $\mathrm{id}_X \in F_X(X)$ in $F_Y(X)$.]

16. Zij L/K een eindige Galoisuitbreiding met groep G. Laat zien dat er een contravariante functor $F : \mathbf{Fld}_{L/K} \to \mathbf{Sets}$ is gegeven door $F(M) = \mathrm{Hom}_K(M, L)$, en dat er een natuurlijke (rechts)werking is van G op $F(M)$. Beschrijf het beeld van de functor $F : \mathbf{Fld}_{L/K} \to G\text{-}\mathbf{Sets}$.
[Dit is in feite een formulering van de hoofdstelling van de Galoistheorie.]

17. Zij $\mathcal{C}$ een deelcategorie van $\mathbf{Mod}_R$ voor een ring R. De *Grothendieck-groep* $K(\mathcal{C})$ van $\mathcal{C}$ is de abelse groep met als voortbrengers de isomorfieklassen van de objecten in $\mathcal{C}$ en als relaties $[P] - [Q] + [R] = 0$ voor elk exact rijtje $0 \to P \to Q \to R \to 0$ in $\mathcal{C}$. Laat zien dat er isomorfismen $K(\mathbf{FAb}) \cong \mathbf{Z}$ en $K(\mathbf{FGAb}) \cong \mathbf{Z}$ zijn die respectievelijk de klasse van een eindige groep naar zijn orde sturen en de klasse van een eindig voortgebrachte groep naar zijn vrije rang.

Literatuurverwijzingen

1. De meeste algebraboeken behandelen niet alleen groepen en ringen, maar ook lichamen. In het bijzonder is dit het geval voor de in de vorige syllabi reeds genoemde boeken van Artin, Shafarevich, Lang, Gallian en Van der Waerden.

2. Liouville's constructie van transcendente getallen en transcendentiebewijzen van e en π vind je bij Stewart in hoofdstuk 6, of bij Hardy en Wright in hoofdstuk 11. Recent nog zijn er transcendentieresultaten bewezen voor waarden van modulaire functies, onder meer door de Rus Nesterenko (Ostrowskiprijs 1998). Zo weet men bijvoorbeeld sinds kort dat $\sum_{n=0}^{\infty} 2^{-n^2}$ transcendent is, en dat π en e^{π} niet alleen elk van beiden transcendent zijn, maar zelfs *algebraïsch onafhankelijk*. Dit laatste betekent dat de afbeelding $\mathbf{Q}[X,Y] \to \mathbf{C}$ gegeven door $f \mapsto f(\pi, e^{\pi})$ injectief is.

- I. Stewart, *Galois theory*, 2nd edition, Chapman and Hall, 1989.
- G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1938.

3. De Duitse wiskundige David Hilbert (1862–1943) presenteerde in een beroemd geworden lezing tijdens het Internationaal Mathematisch Congres in Parijs in 1900 een twintigtal open problemen die hij van belang achtte voor de ontwikkeling van de wiskunde in de 20e eeuw. Het genoemde transcendentievermoeden voor α^{β} was er één van.

- D. Hilbert, *Mathematische Probleme*, Gesammelte Abhandlungen, Band III, 290–329. Springer, 1970.

Zie www.mathematik.uni-bielefeld.de/ kersten/hilbert/rede.html voor een webversie.

4. Er bestaat een groot aantal computeralgebra-pakketten, elk met zijn eigen sterke en zwakke punten. Bekende commerciële systemen zijn Magma, Maple, Mathematica en Matlab. Daarnaast zijn er diverse open source pakketten, die voor een groot deel een gezamenlijk onderkomen hebben gevonden in William Stein's pakket SAGE. Zie de webpage modular.math.washington.edu/sage.

5. Het is in het algemeen waar dat de *cardinaliteit* van een transcendentiebasis voor een lichaamsuitbreiding niet afhangt van de gekozen transcendentiebasis. Men noemt dit de *transcendentiegraad* van de uitbreiding. Er is een direct verband tussen de *dimensie* van 'meetkundige ringen' als $K[X_1, X_2, \ldots, X_n]$ over een lichaam K en de transcendentiegraad van hun quotiëntenlichaam over K. Zie bijvoorbeeld hoofdstuk VIII in Lang's Algebra of het al onder [II, **14**] genoemde boek van Matsumura.

6. Het omkeerprobleem van de Galoistheorie is nog steeds onopgelost, maar er is veel vooruitgang geboekt in de afgelopen 50 jaar. Shafarevich bewees dat iedere eindige oplosbare groep als Galoisgroep over $\mathbf{Q}$ optreedt, en voorts is men er in de afgelopen decennia in geslaagd de meeste simpele groepen als Galoisgroep over $\mathbf{Q}$ te realiseren.

- G. Malle, B. Matzat, *Inverse Galois theory*, Springer, 1999.

7. Lijsten van transitieve ondergroepen van S_n voor $n \leq 22$ zijn nu standaard beschikbaar in pakketten voor computeralgebra als Magma en GAP. Het aantal isomorfietypen van dergelijke ondergroepen is voor $n = 6$ nog slechts 16, maar voor $n = 16$ al 1954. Het aantal groeit overigens niet regelmatig met n: voor $n = 19$ zijn er slechts 8 isomorfietypen.

8. Er is een redelijk toegankelijk artikel over de Artin-afbeelding dat het bewijs van stelling 24.15 en de opmerkingen daarna in een breder kader plaatst.

- H. W. Lenstra, Jr, P. Stevenhagen, *Artin reciprocity and Mersenne primes*, Nieuw Arch. Wiskunde **18** (1), 44–54 (2000).

9. Het is interessant om eens te kijken hoe een algebra-leerboek er een eeuw geleden uitzag, en om zich rekenschap te geven van de ontwikkeling in de tijd van wat als 'basiskennis' van een wiskundige wordt gezien.

- H. Weber - *Lehrbuch der Algebra*, 3 delen (1894, 1896, 1908). Herdrukt door Chelsea.

10. De opmerking dat de Galoisgroep van een polynoom $f \in \mathbf{Z}[X]$ met 'kans 1' groep S_n heeft is een klassiek resultaat van Van der Waerden. Het betreft een verfijning van een argument in zijn algebraboek om polynomen met groep S_n te maken. Het belangrijkste ingrediënt hier is het nuttige feit dat men aan de ontbindingen van een polynoom $f \in \mathbf{Z}[X]$ modulo priemen p kan zien welke *cykeltypes* voorkomen onder de permutaties in $\mathrm{Gal}(f) \subset S_n$.

- B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109**, 13–16 (1934).

11. Alle bewijzen van de stelling van Kronecker-Weber, zoals die in hoofdstuk 6 van Long's boek, gebruiken enige algebraïsche getaltheorie. Washington's boek, dat veel moderne wijsheid over de lichamen $\mathbf{Q}(\zeta_n)$ bevat, heeft een bewijs in een appendix.

- R. L. Long, *Algebraic number theory*, Marcel Dekker, 1977.
- L. C. Washington, *Introduction to cyclotomic fields*, Springer GTM, 1982. Second edition 1997.

12. Het 'beschrijven' van de absolute Galoisgroep $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ van $\mathbf{Q}$ wordt door sommigen als een 'heilige graal' van de getaltheorie gezien. Een ongepubliceerd manuscript van de al in §15 genoemde Franse wiskundige Alexander Grothendieck (*'Esquisse d'un programme'*) ligt ten grondslag aan een recente theorie die deze groep tracht te beschrijven middels een actie op zogenaamde 'kindertekeningen'.

- L. Schneps (ed.), *The Grothendieck theory of dessins d'enfants*, LMS Lecture Note Series **200**, Cambridge University Press, 1994.

13. Voor wie zelf eens wil zien hoe Griekse wiskunde er uitziet zijn de twee deeltjes uit de bekende tweetalige Loeb-serie met klassieke Griekse en Romeinse teksten een goed begin.

- *Greek Mathematical Works*, Loeb Classical Library, vols 335 & 362, Harvard University Press, 1939–1941. Diverse herdukken.

14. Sir Thomas Heath's klassieke tekst over de Griekse wiskunde besteedt een apart hoofdstuk *Special problems* aan deze beroemde problemen en hun geschiedenis.

- T. L. Heath, *A history of Greek mathematics*, 2 delen, Oxford University Press, 1921.

15. Een uitgebreide discussie van Hippocrates' kwadratuur van maantjes, en de vraag 'welke maantjes kwadrateerbaar zijn', is te vinden in Heath's boek. De vraag in kwestie werd pas in 1948 door de Russische wiskundige N. G. Chebotarëv – bekend geworden door een hele algemene dichtheidsstelling over priemgetallen – met Galoistheoretische methoden opgelost. Onderstaand artikel bevat de nodige details over zowel de maantjes als de relatie van de genoemde dichtheidsstelling tot de onder **9** genoemde bepaling van Galoisgroepen van polynomen $\mathrm{Gal}(f)$ uit de factorisatie van $(f \bmod p)$

- P. Stevenhagen, H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18**(2), 26–37 (1996).

16. De meest actuele informatie over de Fermatgetallen verandert jaarlijks, en kan dan ook het beste op het web worden nagezocht. De al in [I, noot 25] genoemde website *The Prime Pages* www.utm.edu/research/primes heeft links naar pagina's met informatie over Fermatgetallen, zoals www.prothsearch.net/fermat.html.

17. Er zijn klassieke resultaten van Schur over de Galoisgroepen van polynomen die in de analyse voorkomen als afgekapte machtreeksen. Zo is bijvoorbeeld de n-de deelsom $\sum_{i=0}^{n} \frac{X^i}{i!}$ van de exponentiële reeks een polynoom in $\mathbf{Q}[X]$ met groep S_n als n niet door 4 deelbaar is. Voor $4|n$ wordt de groep A_n. Het n-de Laguerre-polynoom $\sum_{i=0}^{n} \binom{n}{i} \frac{(-X)^i}{i!}$ heeft groep S_n voor alle $n \geq 1$. Men kan bewijzen dat het polynoom $X^n - X - 1$ eveneens groep S_n heeft voor alle $n > 1$.

- I. Schur, *Gleichungen ohne Affekt*, Sitzungsber. der preuß. Akad. der Wiss., Phys.-Math. Kl., 443–449 (1930).

18. De recensie in het Nieuw Archief van Dieter Jörgenson's historische roman *De Rekenmeester* geeft een goede indruk van de omstandigheden waarin de radicaalformules gevonden en verspreid werden. Je kunt natuurlijk ook de roman zelf lezen.

- N.S. Hekster, *Boekbespreking van 'De Rekenmeester'*, Nieuw Archief voor Wiskunde **5/1**(3), pp. 310-313 (2000).

19. De Galoistheorie van differentiaalvergelijkingen wordt onder meer behandeld in een klassiek boek van Kaplansky, en in het recentere boekje van Magid.

- I. Kaplansky, *An introduction to differential algebra*, Hermann, 1952.
- A. R. Magid, *Lectures on Differential Geometry*, AMS University Lecture Series **7**, 1994.

20. $SL_2(\mathbf{Z})$

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 3, woensdag 22 mei 2002, 14.00–17.00 uur

1. Geef een element $\alpha \in K = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ aan met $K = \mathbf{Q}(\alpha)$ en bepaal het minimumpolynoom $f^{\alpha}_{\mathbf{Q}}$.

2. Laat zien dat $K_1 = \mathbf{F}_3[X]/(X^3 - X - 1)$ en $K_2 = \mathbf{F}_3[Y]/(Y^3 - Y - 2)$ isomorfe lichamen zijn, en geef een expliciet isomorfisme $\phi : K_1 \xrightarrow{\sim} K_2$ aan.

3. Zijn de hoeken van een gelijkzijdige driehoek met passer en liniaal in drie gelijke delen te verdelen? (Motiveer je antwoord en formuleer de gebruikte stellingen.)

4. Zij $L = \Omega_{\mathbf{Q}}^{X^4-3}$ het ontbindingslichaam van $X^4 - 3$ over $\mathbf{Q}$.
   a. Laat zien dat $\mathrm{Gal}(L/\mathbf{Q})$ een niet-abelse groep is.
   b. Laat zien dat er een deellichaam $K \subset L$ bestaat zodat $\mathrm{Gal}(K/\mathbf{Q})$ abels van orde 4 is.
   c. Is het lichaam K in onderdeel b uniek bepaald?

5. Definieer K_2 en K_4 als de unieke deellichamen van $\mathbf{Q}(\zeta_{13})$ van graad 2 respectievelijk 4 over $\mathbf{Q}$. Deze lichamen zijn als volgt geordend: $\mathbf{Q} \subset K_2 \subset K_4 \subset \mathbf{Q}(\zeta_{13})$.
   a. Bewijs: $K_2 = \mathbf{Q}(\sqrt{13})$.
   b. Bepaal een element $\alpha \in K_2$ met $K_4 = K_2(\sqrt{\alpha})$.
   c. Bestaat er een element $\beta \in \mathbf{Q}$ met $K_4 = \mathbf{Q}(\sqrt[4]{\beta})$? Motiveer je antwoord.

Uitslagen vanavond op collegekaartnummer op de webpagina van het college.

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 3, 1 juni 2004, 14.00–17.00 uur

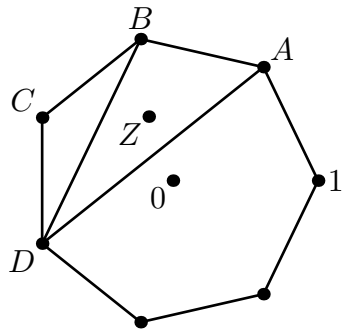
Dit is een open-boek-tentamen.
Motiveer al je antwoorden, eventueel met verwijzingen naar stellingen uit de syllabus.

Opgave 1. Bepaal de volgende lichaamsgraden:
(a) $[\mathbf{Q}(\sqrt{-2},\sqrt{3}):\mathbf{Q}]$;
(b) $[\mathbf{R}(\sqrt{-2},\sqrt{3}):\mathbf{R}]$;
(c) $[\mathbf{F}_7(\sqrt{-2},\sqrt{3}):\mathbf{F}_7]$;
(d) $[\mathbf{F}_{11}(\sqrt{-2},\sqrt{3}):\mathbf{F}_{11}]$.

Opgave 2. Definieer polynomen f_1, f_2, $f_3 \in \mathbf{F}_2[X]$ door $f_1 = X^2+1$, $f_2 = X^2+X$ en $f_3 = X^2+X+1$. Beantwoord voor $i = 1,2,3$ de volgende vragen:
(a) Is f_i een separabel polynoom?
(b) Is $\mathbf{F}_2[X]/(f_i)$ een separabele lichaamsuitbreiding van $\mathbf{F}_2$?

Opgave 3.
(a) Bewijs dat de ring $K = \mathbf{Q}[X]/(X^6+3)$ een lichaam is. Dit lichaam noteren we ook wel als $K = \mathbf{Q}(\sqrt[6]{-3})$.
(b) Is K een Galoisuitbreiding van $\mathbf{Q}$? Zo ja, bepaal de Galois groep. Zo nee, bepaal de normale afsluiting.
(c) Is de ring $K = \mathbf{Q}[X]/(X^6-72)$ een lichaam? Zo ja, is dit lichaam normaal over $\mathbf{Q}$? Zo nee, geef een maximaal ideaal van deze ring.

Opgave 4. Beschouw de regelmatige 7-hoek in $\mathbf{C}$ met middelpunt 0 en hoekpunt 1, en nummer hoekpunten A, B, C, D als aangegeven. Ga na welke punten construeerbaar zijn met passer en liniaal vanuit de verzameling $\{0,1\}$:
(a) het punt A;
(b) het midden van C en D;
(c) het zwaartepunt Z van de driehoek ABD.



— SUCCES —

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 3, maandag 12 juni 2006, 10.00–13.00

Dit is een open boek tentamen.
Vermeld op alle bladen die je inlevert je naam en studentnummer.
Motiveer je antwoorden.

1. Zij $K \subset L$ een lichaamsuitbreiding, en laat α, β in L transcendent zijn over K.
   a. Geef voorbeelden waaruit blijkt dat $\alpha + \beta$ en $\alpha \cdot \beta$ algebraïsch kunnen zijn over K.
   b. Is het mogelijk dat $\alpha + \beta$ en $\alpha \cdot \beta$ beide *tegelijk* algebraïsch zijn over K?

2. Laat $K = \mathbf{Q}(\sqrt{3}, \sqrt{7})$.
   a. Geef een element α in K zodat $K = \mathbf{Q}(\alpha)$.
   b. Bepaal het minimumpolynoom van α over $\mathbf{Q}$.
   c. Bepaal de deellichamen van K.

3. Laat K het lichaam $\mathbf{Q}(\sqrt{-3}, \sqrt[3]{5})$ zijn.
   a. Bereken de graad $[K : \mathbf{Q}]$.
   b. Geef een polynoom f in $\mathbf{Q}[X]$ zodat K het ontbindingslichaam is van f over $\mathbf{Q}$.
   c. Bepaal de lichaamsautomorfismen van K.
   d. Bepaal de graad over $\mathbf{Q}$ van de elementen

$$\sqrt{-3} \cdot \sqrt[3]{5} \qquad \text{en} \qquad (\sqrt{-3} + 1) \cdot \sqrt[3]{5}$$

   van K.

4. Laat $K = \mathbf{Q}(\zeta_{15})$ met ζ_{15} een primitieve 15-de machts eenheidswortel in $\mathbf{C}$.
   a. Bewijs dat K een Galoisuitbreiding is van $\mathbf{Q}$.
   b. Bewijs dat K een primitieve 5-de machtseenheidswortel ζ_5 bevat
   c. Bepaal $[K : \mathbf{Q}(\zeta_5)]$ en $\mathrm{Gal}(K/\mathbf{Q}(\zeta_5))$. Laat $\alpha = \zeta_{15}^2 + \zeta_{15}^7$.
   d. Bewijs: $\alpha \in \mathbf{Q}(\zeta_5)$.
   e. Bepaal de graad van α over $\mathbf{Q}$.

5. Laat Φ_n het n-de cyclotomische polynoom zijn.
   a. Ontbind Φ_5 en Φ_{12} in irreducibele factoren in $\mathbf{F}_2[X]$.
   b. Bepaal voor beide polynomen de graad over $\mathbf{F}_2$ van het ontbindingslichaam.
   c. Laat p een priemgetal zijn dat n niet deelt, en zij K een lichaam van karakteristiek p. Bewijs: ieder nulpunt van Φ_n in K is een primitieve n-e machtseenheidswortel.

—SUCCES—

Index

K-homomorfismen, 31
K-isomorf, 16
π, 61
  transcendentie van, 7, 65
abc-formule, 71
e, transcendentie van, 7
n-de eenheidswortel, 52
p-de cyclotomische lichaam, 9, 15, 49
$\mathbf{F}_q$, 21

abels getallenlichaam, 54
abelse categorie, 81
absolute Galoisgroep, 54
affiene groep, 57, 59
afgeleide, 21, 33
  logaritmische, 29
algebra-pakket, 11
algebraïsch afgesloten, 12–14, 18
algebraïsch element, 7
algebraïsch getal, 7, 18
algebraïsch onafhankelijk, 9, 89
algebraïsche afsluiting, 13, 14, 16, 17, 21, 32
  van K in L, 12
algebraïsche uitbreiding, 7, 12
anti-equivalentie, 85
Apollo, 61
arithmetische algebraïsche meetkunde, 85
aritmetische algebraïsche meetkunde, 34
aritmetische functie, 28
  multiplicatieve, 28
aritmetische functies, 28
Ars Magna, 72, 73
Artin, E., 13, 29, 37, 44, 75
Artin-afbeelding, 54
Artin-Schreier-polynoom, 29, 67, 75
Artin-Schreier-radicaal, 75
automorfisme, 19, 22, 80
  van $\mathbf{C}$, 19
automorfismengroep, 25, 26, 29, 80

basis, 5, 18
basiskeuze, 35
basisobject, 82, 86
basispunt, 83
beginobject, 87
Berlekamp-deelalgebra, 29
binomium van Newton, 21

canoniek isomorf, 84
Cardano-Del Ferro-formule, 72, 73, 76
cartesisch product, 86
casus irreducibilis, 72
categorie, 80, 82
  anti-equivalente, 85
  equivalente, 85
  kleine, 80
Cayley, A., 76
commutatorondergroep, 83
complexe nulpunten, 9
compositum, 6, 9
computeralgebra-pakket, 10, 46
constructiestap, 60
construeerbaar, 65
construeerbaar getal, 61
construeren, 60
contravariante functor, 83, 84
convolutieproduct, 28
coproduct, 86
covariante functor, 83
cyclische Galoisuitbreiding, 49
cyclotomie, 52
cyclotomisch lichaam, 9, 49, 53, 54
cyclotomisch polynoom, 52, 53
  irreducibiliteit van, 53
cyclotomische uitbreiding, 49, 51, 53

Dedekind, R., 37
deelcategorie, 81, 82
  volle, 81
deellichaam, 5, 22
dektransformatie, 82
del Ferro, S., 71
Delisch probleem, 61, 65
determinantafbeelding, 84
dimensie, 5, 89
discriminant, 57
disjuncte vereniging, 86
driedeling van de hoek, 61, 65, 74
duale vectorruimte, 84
dualiteitsfunctor, 84, 85
dubbel nulpunt, 21, 33

dubbel-duale, 84

eenhedengroepfunctor, 83, 87
eenheidswortel, 7, 51, 52
  primitieve n-de, 52
eindig lichaam, 21
eindig voortgebracht, 6
eindige lichaamsuitbreiding, 5
eindobject, 87
elliptische kromme, 54, 85
endomorfisme, 80
enkelvoudige uitbreiding, 6, 34
equivalentie van categorieën, 85
Euclidische algoritme, 11
Euler, L., 78, 79
  constante van, 7
Euler-φ-functie, 28
evaluatie-afbeelding, 9

Fermat, P. de
  kleine stelling van, 21, 24
  laatste stelling van, 85
Fermat-priemgetal, 66
Fermatgetal, 91
formeel nulpunt, 9
formele adjunctie, 9, 15, 23
Frobeniusafbeelding, 22
Frobeniusautomorfisme, 22, 23, 25, 26, 29, 49, 54
functionaalanalyse, 85
functor, 83, 84
  contravariant, 83, 84
  covariant, 83, 84
  geadjungeerde, 87
  representeerbare, 85
functoriële constructie, 83
fundamentaalgroep, 83, 85
fundamentele verzameling, 31, 32, 37, 59

Galois, E., 42
Galoiscorrespondentie, 26, 35, 43
Galoisgroep, 42–44, 46
  van een polynoom, 45, 46
Galoisrepresentatie, 54
Galoistheorie, 13, 16, 23, 31, 42
  hoofdstelling van, 26, 37, 43, 85
  hoofdstelling voor topologische ruimten, 85
  omkeerprobleem van de, 46
Galoisuitbreiding, 42–44
  cyclische, 49
  eindige, 42
Gauss, C. F., 13, 66, 79
  lemma van, 53
  monument in Brunswijk, 66
Gauss-periode, 50
  kubische, 50
  kwadratische, 50, 51
Gauss-som, 51
geadjungeerde functoren, 87
geconjugeerd, 16, 43, 47
geconjugeerde elementen, 16, 50
geconjugeerde lichamen, 16, 43, 47
Gelfond, A. O., 7
gereduceerde ring, 83
getallenlichaam, 5, 9, 34, 54
  abels, 54
gevezeld product, 86
gevezelde som, 86
graad, 5
Griekse wiskunde, 60
groepenring, 29, 81
Grothendieck, A., 85, 90
Grothendieck-groep, 88

Hasse, H., 23
Hasse-diagram, 23
Hermite, C., 7
Hilbert, D., 7
Hippocrates van Chios, 61, 73
hoofdstelling van de algebra, 13, 77
hoofdstelling van de Galoistheorie, 26, 37, 43, 85, 88
  voor topologische ruimten, 85

imperfectiegraad, 41
inclusierelatie, 22
inseparabel, 22, 32, 33
inseparabel polynoom, 22, 32
inseparabele uitbreiding, 33, 40
inseparabiliteitsgraad, 40
invariantenlichaam, 26, 42
inverse
  in een lichaam, 11
irreducibel polynoom van α, 8, 10
irreducibele radicaaluitbreiding, 67, 75
irreducibele radicalen, 67

isomorfisme, 80

karakter, 38
karakteristiek, 5, 21, 34
karakteristieke functie, 28
keten, 5
keuzeaxioma, 13
kindertekeningen, 90
klasse, 80
kleine categorie, 80
Kronecker, L., 54
kubisch lichaam, 9, 15
kubische uitbreiding, 5, 9, 15, 18, 27
kwadraat afsplitsen, 71
kwadraatwortel, 62–65, 71
kwadratisch lichaam, 7, 9
kwadratische afsluiting, 63, 64, 74
kwadratische reciprociteitswet, 78
kwadratische uitbreiding, 5, 7, 18, 27, 55
kwadratische worteldiepte, 74
kwadratuur van de cirkel, 61

Lagrange-resolvente, 68
Laguerre-polynoom, 91
Legendre, A.-M., 79
Legendre-symbool, 78
lemma van Artin-Dedekind, 37, 38, 44, 68
lemma van Gauss, 53
lemma van Zorn, 10, 13, 17
lichaam
  perfect, 33, 34
lichaam van rationale functies, 7, 18, 59
lichaamshomomorfisme, 5, 31, 34
lichaamsuitbreiding, 5
  eindig voortgebrachte, 6
  eindige, 5
  enkelvoudige, 6, 34
  kubische, 5, 9, 18, 27, 47
  kwadratische, 5, 18, 27, 50, 54
  normale, 26, 31, 36, 37, 41, 43
  primitieve, 6, 34
  separabele, 26, 31–34, 43
  voortgebracht door S, 6
lift naar karakteristiek 0, 54
Lindemann, C. L. F. von, 7, 65
lineaire algebra, 11, 39
liniaal, 60
linksexact, 87
linksgeadjungeerde functor, 87
Liouville, J., 7
logaritmische afgeleide, 29

Möbius, A. F., 24
Möbius-functie, 24, 28
Möbius-inversieformule, 24, 28, 52
maantjes van Hippocrates, 61, 73
machtsbasis, 11
meetkundige reeks, 29
Mersenne-priem, 29
minimumpolynoom, 8, 10, 11
modulaire groep, 86
morfisme, 80
  inverse van, 80
  van functoren, 84

natuurlijke equivalentie, 84
natuurlijke transformatie, 84, 88
norm, 29, 38, 39
normaal, 26, 43, 65
normale afsluiting, 37
normale basis, 29, 50
normale uitbreiding, 26, 31, 36, 37, 41, 43

object, 80, 82
omkeerformule, 24, 28
omkeerprobleem van de Galoistheorie, 46
ontbindingslichaam, 14–17, 19, 37, 41, 42, 44
oplosbaar, 68, 70
oplosbare groep, 65, 78
overdekking, 82

partieelbreuksplitsing, 18
passer, 60
perfect lichaam, 33, 34
pest, 61
pijl, 80
polynoom
  inseparabel, 32
  separabel, 32
priemlichaam, 5, 18, 21
primitief element, 11, 34, 35, 44
  stelling van het, 35, 40
primitieve n-de eenheidswortel, 52
primitieve uitbreiding, 6, 34
primitieve wortel, 78
pro-eindige getallen, 30

product, 85
  gevezeld, 86

quotiëntenlichaam, 6, 40

radicaalafsluiting, 66, 75
radicaaluitbreiding, 67
rechtsexact, 87
reflexieve ruimte, 85
representatie, 81
representatiefunctor, 83–85, 87, 88
representeerbare functor, 85
resolvente, 75, 76
  van Lagrange, 68
rooster
  van deellichamen, 22, 23
  van ondergroepen, 47–49
rooster van deellichamen, 47

Schneider, T., 7
Schreier, O., 75
separabel, 26, 32, 33, 43
separabel afgesloten, 40
separabel element, 33
separabel polynoom, 32
separabele afsluiting, 40
separabele uitbreiding, 26, 31–34, 43
separabiliteitsgraad, 32
simpele groep, 89
som
  gevezeld, 86
spoor, 29, 38, 39, 75
Steinitz, E., 13
stelling van Kronecker-Weber, 54
stelling van Thales, 62

tegengestelde categorie, 81
tensorproduct, 86, 87
theorema aureum, 79
topologie, 13, 77, 81
topologische ruimte, 81
toren, 5, 12
trace, 38
transcendent, 7, 65
transcendent getal, 7, 18
transcendentiebasis, 10
transcendentiegraad, 89
transitieve ondergroep van S_n, 46
trisectie van de hoek, 61, 65, 74
triviale overdekking, 82
tussenlichaam, 26, 35, 36, 42, 43
tussenwaardestelling, 13, 77

uitbreiding
  enkelvoudige, 6, 26, 34
  kubische, 5, 9, 15, 18, 27, 47
  kwadratische, 5, 7, 18, 27, 50, 54
  normale, 26, 31, 36, 37, 41, 43
  primitieve, 6, 34
  separabele, 26, 31–34, 43
  voortgebracht door S, 6
uitbreidingslichaam, 5
universele constructie, 85
universum, 80

vectorruimte, 5, 81
verdubbeling van de kubus, 61, 65
vergeetfunctor, 83, 85, 87
vezel, 85
vezelfunctor, 85
volle deelcategorie, 81

Weber, H., 54
Wiles, A., 85
worteldiepte, 74
wortelformule, 67, 71
wortelnotatie, 67
worteltrekking, 66, 67, 69

Yoneda's lemma, 88

Zorn
  lemma van, 10, 13, 17
zuiver transcendent, 10, 19