Mathematisch Instituut
Universiteit Leiden

Uitwerking tentamen Algebra 3, 12 juni 2006

Opgave 1. (a) Neem $K = \mathbf{Q}$ en $L = \mathbf{Q}(T)$. Er zijn elementen α en β in L die transcendent zijn over K maar zodanig dat $\alpha + \beta$ algebraïsch is over K; neem bijvoorbeeld $\alpha = T$ en $\beta = -T$. Er zijn ook transcendente elementen α en β zodat $\alpha \cdot \beta$ algebraïsch is: neem $\alpha = T$ en $\beta = 1/T$.

(b) Schrijf $\gamma = \alpha + \beta$ en $\delta = \alpha \cdot \beta$. Als γ en δ beide algebraïsch zijn over K, dan is het deellichaam $K(\gamma, \delta)$ van L algebraïsch over K. De elementen α en β zijn nulpunten van het polynoom

$$(X - \alpha)(X - \beta) = X^2 - \gamma X + \delta \in K(\gamma, \delta)[X]$$

en zijn dus algebraïsch over $K(\gamma, \delta)$. Wegens stelling 21.9 volgt hieruit dat α en β algebraïsch zijn over K.

Opgave 2. Zij $K = \mathbf{Q}(\sqrt{3}, \sqrt{7})$.

(a), (b) Neem $\alpha = \sqrt{3} + \sqrt{7}$. We bepalen het minimumpolynoom van α door de machten van α te bepalen ten opzichte van de $\mathbf{Q}$-basis $(1, \sqrt{3}, \sqrt{7}, \sqrt{21})$ van K:

$$\begin{aligned}
\alpha &= \sqrt{3} + \sqrt{7}, \\
\alpha^2 &= 10 + 2\sqrt{21}, \\
\alpha^3 &= 24\sqrt{3} + 16\sqrt{7}, \\
\alpha^4 &= 184 + 40\sqrt{21}.
\end{aligned}$$

We zien dat 1, α, α^2 en α^3 linear onafhankelijk zijn over $\mathbf{Q}$, maar dat $\alpha^4 - 20\alpha^2 + 16 = 0$. We concluderen dat

$$f_{\mathbf{Q}}^{\alpha} = X^4 - 20X^2 + 16$$

en omdat de graad van $f_{\mathbf{Q}}^{\alpha}$ gelijk is aan $[K : \mathbf{Q}]$ is α een voortbrenger van K over $\mathbf{Q}$.

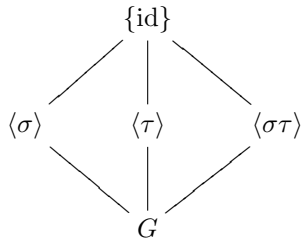
(c) Om de deellichamen van de uitbreiding $\mathbf{Q} \subset K$ te bepalen, gebruiken we de hoofdstelling van de Galoistheorie (24.4). We laten zien dat $\mathbf{Q} \subset K$ een Galoisuitbreiding is waarvan de Galoisgroep een viergroep van Klein is. Elke kwadratische uitbreiding van een lichaam van karakteristiek $\neq 2$ is namelijk Galois (zelfde bewijs als voorbeeld 24.2); wanneer we dit toepassen op de uitbreidingen $\mathbf{Q}(\sqrt{3}) \subset K$ en $\mathbf{Q}(\sqrt{7}) \subset K$ zien we dat er automorfismen σ en τ van K bestaan met

$$\begin{aligned}
\sigma(\sqrt{3}) &= \sqrt{3}, \quad \sigma(\sqrt{7}) = -\sqrt{7}, \\
\tau(\sqrt{3}) &= -\sqrt{3}, \quad \tau(\sqrt{7}) = \sqrt{7}.
\end{aligned}$$

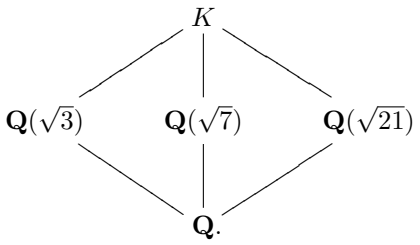
De automorfismen σ en τ hebben elk orde 2 en commuteren met elkaar; hun product $\sigma\tau$ wordt gegeven door

$$\sigma\tau(\sqrt{3}) = -\sqrt{3}, \quad \sigma\tau(\sqrt{7}) = -\sqrt{7}.$$

We hebben dus een ondergroep $G = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ van $\operatorname{Aut} K$ die een viergroep van Klein is. Het invariantenlichaam K^G is gelijk aan $\mathbf{Q}$ (kijk naar de werking van G op een element $a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21}$), dus $\mathbf{Q} \subset K$ is een Galoisuitbreiding met groep $G = \mathrm{Gal}(K/\mathbf{Q}) = \operatorname{Aut} K$.
Het diagram van ondergroepen van G is



en het corresponderende diagram van deellichamen van K is



Opgave 3. Zij $K = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{5})$.

(a) Het lichaam $\mathbf{Q}(\sqrt[3]{5})$ heeft graad 3 over $\mathbf{Q}$, omdat $X^3 - 5$ irreducibel is over $\mathbf{Q}$ wegens het criterium van Eisenstein en het lemma van Gauss. Vatten we $\mathbf{Q}(\sqrt[3]{5})$ op als deellichaam van $\mathbf{R}$ door voor $\sqrt[3]{5}$ de reële wortel te nemen, dan zien we dat $X^2 + 3$ irreducibel is over $\mathbf{Q}(\sqrt[3]{5})$ (de nulpunten $\pm\sqrt{-3} \in \mathbf{C}$ zijn niet reëel). We concluderen dat $\mathbf{Q}(\sqrt{-3}, \sqrt[3]{5})$ van graad 6 is over $\mathbf{Q}$.

(b) We merken op dat $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ een primitieve derde eenheidswortel is, en dat de (complexe) nulpunten van $X^3 - 5$ de elementen $\sqrt[3]{5}$, $\zeta_3\sqrt[3]{5}$ en $\zeta_3^2\sqrt[3]{5}$ zijn. Het lichaam voortgebracht door deze drie nulpunten is gelijk aan

$$\mathbf{Q}(\zeta_3, \sqrt[3]{5}) = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{5}) = K,$$

en we concluderen dat K het ontbindingslichaam van $X^3 - 5$ over $\mathbf{Q}$ is.

(c) Omdat K het ontbindingslichaam van het separabele polynoom $X^3 - 5 \in \mathbf{Q}[X]$ is, is $\mathbf{Q} \subset K$ een Galoisuitbreiding waarvan we de Galoisgroep $G = \mathrm{Gal}(K/\mathbf{Q}) = \mathrm{Aut}\, K$ kunnen opvatten als ondergroep van de groep van alle permutaties van de nulpunten van $X^3 - 5$; deze laatste groep is isomorf met de symmetrische groep S_3 van orde 6. Aangezien $[K : \mathbf{Q}] = 6$ en de hoofdstelling van de Galoistheorie zegt dat $\#G = [K : \mathbf{Q}]$, zien we dat G gelijk moet zijn aan de hele groep van permutaties van de nulpunten $\sqrt[3]{5}$, $\zeta_3\sqrt[3]{5}$ en $\zeta_3^2\sqrt[3]{5}$. Nummeren we deze nulpunten 1, 2 en 3 en identificeren we G met S_3, dan geeft een eenvoudige berekening de volgende werking van G op de voortbrengers $\sqrt{-3}$ en $\sqrt[3]{5}$ van K:

σ	id	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$\sigma(\sqrt{-3})$	$\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$	$\sqrt{-3}$	$\sqrt{-3}$
$\sigma(\sqrt[3]{5})$	$\sqrt[3]{5}$	$\zeta_3\sqrt[3]{5}$	$\sqrt[3]{5}$	$\zeta_3^2\sqrt[3]{5}$	$\zeta_3\sqrt[3]{5}$	$\zeta_3^2\sqrt[3]{5}$

Opgave 4. Zij $K = \mathbf{Q}(\zeta_{15})$ met $\zeta_{15} \in \mathbf{C}$ een primitieve vijftiende eenheidswortel.

(a) Uit stelling 24.15 weten we dat $\mathbf{Q} \subset K$ een Galoisuitbreiding is met groep $(\mathbf{Z}/15\mathbf{Z})^*$.

(b) Het element ζ_{15} heeft orde 15 in $\mathbf{C}^*$, dus als we $\zeta_5 = \zeta_{15}^3$ definiëren, heeft ζ_5 orde 5 in $\mathbf{C}^*$ en is dus een primitieve vijfde eenheidswortel.

(c) Het is bekend dat $\mathrm{Gal}(K/\mathbf{Q}) = \mathrm{Aut}\, K$ isomorf is met $(\mathbf{Z}/15\mathbf{Z})^*$, een groep van orde $\phi(15) = 8$, via de afbeelding

$$\begin{aligned}(\mathbf{Z}/15\mathbf{Z})^* &\longrightarrow \mathrm{Aut}\, K \\ k &\longmapsto (\sigma_k\colon \zeta_{15} \mapsto \zeta_{15}^k)\end{aligned}$$

(zie stelling 24.15). De ondergroep $\mathrm{Gal}(K/\mathbf{Q}(\zeta_5))$ van $\mathrm{Gal}(K/\mathbf{Q})$ bestaat uit de automorfismen die $\zeta_5 = \zeta_{15}^3$ vasthouden. Dit zijn precies de elementen σ_k met $k \in (\mathbf{Z}/15\mathbf{Z})^*$ waarvoor $\zeta_{15}^{3a} = \zeta_{15}^3$, oftewel $3a \equiv 3 \pmod{15}$. Nagaan van de mogelijkheden geeft

$$\mathrm{Gal}(K/\mathbf{Q}(\zeta_5)) = \{\sigma_1 = \mathrm{id}, \sigma_{11}\}.$$

(d) Om te laten zien dat het element

$$\alpha = \zeta_{15}^2 + \zeta_{15}^7 \in K$$

in $\mathbf{Q}(\zeta_5)$ zit, is het voldoende aan te tonen dat het invariant is onder de werking van $\mathrm{Gal}(K/\mathbf{Q}(\zeta_5))$. Er geldt

$$\begin{aligned}\sigma_{11}(\alpha) &= \zeta_{15}^{22} + \zeta_{15}^{77} \\ &= \zeta_{15}^{7} + \zeta_{15}^{2} \\ &= \alpha\end{aligned}$$

en aangezien σ_{11} het enige niet-triviale element van $\mathrm{Gal}(K/\mathbf{Q}(\zeta_5))$ is, laat dit zien dat $\alpha \in \mathbf{Q}(\zeta_5)$.

(e) De graad van α over $\mathbf{Q}$ is gelijk aan de graad van de lichaamsuitbreiding $\mathbf{Q} \subset \mathbf{Q}(\alpha)$. De hoofdstelling van de Galoistheorie zegt dat $\mathbf{Q}(\alpha) \subset K$ een Galoisuitbreiding is en dat $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ gelijk is aan de index van $\mathrm{Gal}(K/\mathbf{Q}(\alpha))$ in $\mathrm{Gal}(K/\mathbf{Q})$. We weten al dat $\mathrm{Gal}(K/\mathbf{Q})$ een groep van orde 8 is, dus we moeten nog de orde van $\mathrm{Gal}(K/\mathbf{Q}(\alpha)) = \mathrm{Aut}_{\mathbf{Q}(\alpha)} K$ bepalen. Een berekening als in (c) voor alle $k \in (\mathbf{Z}/15\mathbf{Z})^*$ geeft de volgende tabel:

k	1	2	4	7	8	11	13	14
$\sigma_k(\alpha)$	α	β	γ	β	δ	α	δ	γ.

Hier is α als boven en

$$\beta = \zeta_{15}^{4} + \zeta_{15}^{14}, \quad \gamma = \zeta_{15}^{8} + \zeta_{15}^{13}, \quad \delta = \zeta_{15} + \zeta_{15}^{11}.$$

We concluderen dat $\mathrm{Gal}(K/\mathbf{Q}(\alpha)) = \{\sigma_1, \sigma_{11}\}$ en dat

$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathrm{Gal}(K/\mathbf{Q}) : \mathrm{Gal}(K/\mathbf{Q}(\alpha))] = 8/2 = 4.$$

Opgave 5. Laat Φ_n het n-de cyclotomische polynoom zijn.

(a) Met behulp van de formules uit opgave 24.31 vinden we

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1, \quad \Phi_{12} = X^4 - X^2 + 1.$$

Geen van beide polynomen heeft een nulpunt in $\mathbf{F}_2$. Het enige irreducibele polynoom van graad 2 in $\mathbf{F}_2[X]$ is $X^2 + X + 1$; het is eenvoudig na te gaan dat Φ_5 bij deling door $X^2 + X + 1$ rest $X + 1$ geeft en dat $\Phi_{12} = (X^2 + X + 1)$ in $\mathbf{F}_2[X]$. We zien dus dat de ontbindingen van deze polynomen in irreducibele factoren in $\mathbf{F}_2[X]$ gegeven worden door

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1, \quad \Phi_{12} = (X^2 + X + 1)^2.$$

(b) Een nulpunt van het irreducibele polynoom $\Phi_5 \in \mathbf{F}_2[X]$ aan $\mathbf{F}_2$ adjungeren geeft een uitbreiding van graad 4 van $\mathbf{F}_2$. Kies een algebraïsche afsluiting $\bar{\mathbf{F}}_2$ van $\mathbf{F}_2$. Dit lichaam bevat slechts één deellichaam dat van graad 4 is over $\mathbf{F}_2$, namelijk het in (22.2) gedefinieerde lichaam $\mathbf{F}_{2^4}$ van $2^4 = 16$ elementen. Alle nulpunten van Φ_5 in $\bar{\mathbf{F}}_2$ liggen dus in $\mathbf{F}_{2^4}$, waaruit we concluderen dat de graad van een ontbindingslichaam van Φ_5 over $\mathbf{F}_2$ gelijk is aan 4.
Als ontbindingslichaam van Φ_{12} over $\mathbf{F}_2$ kunnen we (wegens de bovenstaande factorisatie van Φ_{12}) een ontbindingslichaam van $X^2 + X + 1$ over $\mathbf{F}_2$ nemen. Zo'n ontbindingslichaam krijgen we door een nulpunt van $X^2 + X + 1$ aan $\mathbf{F}_2$ te adjungeren; het resultaat is de kwadratische uitbreiding $\mathbf{F}_2[X]/(X^2 + X + 1)$ van $\mathbf{F}_2$. We concluderen dat de graad van een ontbindingslichaam van Φ_{12} over $\mathbf{F}_2$ gelijk is aan 2.

(c) Zij $p \nmid n$ een priemgetal en K een lichaam van karakteristiek p. We kiezen een ontbindingslichaam L van $X^n - 1$ over K. Omdat n geen veelvoud is van p, heeft $X^n - 1$ geen nulpunten gemeen met zijn afgeleide nX^{n-1}, dus $X^n - 1$ heeft n verschillende nulpunten in L. Deze nulpunten vormen een cyclische groep C (zie blz. 54 van het dictaat), en C heeft $\phi(n)$ voortbrengers. We gaan nu laten zien dat al deze voortbrengers nulpunten van Φ_n zijn. De vergelijking (24.13) geldt in $\mathbf{Z}[X]$ (en hiermee ook in $K[X]$) omdat alle cyclotomische polynomen in $\mathbf{Z}[X]$ liggen. Als ζ een voortbrenger van C is, dan is ζ per definitie een nulpunt van $X^n - 1$, maar niet van een Φ_d met d een deler van n die niet gelijk is aan n. Omdat Φ_d een deler is van $X^d - 1$, zou ζ dan namelijk ook een nulpunt van $X^d - 1$ zijn, d.w.z. dat $\zeta^d = 1$ in L^*; dit is echter in tegenspraak met de aanname dat ζ orde n heeft. Wegens (24.13) moet ζ dus een nulpunt zijn van Φ_n. Dit bewijst de bewering dat alle voortbrengers van C nulpunten van Φ_n zijn. Omdat de graad $\phi(n)$ van Φ_n gelijk is aan het aantal voortbrengers van C, volgt hieruit dat de nulpunten van Φ_n *precies* de voortbrengers van C zijn, d.w.z. de primitieve n-de eenheidswortels in L. In het bijzonder is elk nulpunt van Φ_n in K een primitieve n-de eenheidswortel.