Uitwerkingen tentamen Algebra 3
8 juni 2017, 14:00 – 17:00

Je mocht zoals gezegd niet zonder uitleg naar opgaven verwijzen. Sommige berekeningen zijn hier weggelaten. Die moest je op je tentamen wel laten zien.

Opgave 1. Bepaal de graad van een ontbindingslichaam van $f = x^3 - 2$ over

(a) $\mathbf{Q}$,
(b) $\mathbf{R}$,
(c) $\mathbf{F}_3$,
(d) $\mathbf{F}_7$,
(e) $\mathbf{F}_{11}$,
(f) $\mathbf{F}_{13}$.

Uitwerking: Voor (c) geldt $f = x^3 + 1 = (x+1)^3$, dus het enige nulpunten van f is -1, dus elk ontbindingslichaam van f over $\mathbf{F}_3$ is $\mathbf{F}_3$ zelf, dus de graad is 1.

Dan de overige gevallen. Zij F een lichaam van karakteristiek ongelijk aan 3 en $\overline{F}$ een algebraïsche afsluiting, en $\Omega = \Omega_F^f \subset \overline{F}$ het lichaam voortgebracht door de nulpunten van f in $\overline{F}$. Zij $\alpha \in \overline{F}$ een nulpunt van f en $\zeta \in \overline{F}$ een primitieve derdemachts eenheidswortel. Dan geldt $\Omega = F(\alpha, \zeta)$.

We bekijken de twee uitbreidingen $F \subset F(\zeta) \subset F(\alpha, \zeta) = \Omega$ en gebruiken $[\Omega : F] = [\Omega : F(\zeta)] \cdot [F(\zeta) : F]$. Omdat ζ een nulpunt is van het polynoom $x^2 + x + 1$, is de graad $[F(\zeta) : F]$ hooguit 2; het is gelijk aan 2 dan en slechts dan als de multiplicatieve groep F^* geen element van orde 3 bevat.

Als f geen nulpunt heeft in F, dan is f irreducibel over F (want f heeft graad 3), dus heeft elk nulpunt van f graad 3 over F; dan zijn ze dus niet bevat in $F(\zeta)$ en dus hebben ze om dezelfde reden ook graad 3 over $F(\zeta)$, dus $[\Omega : F(\zeta)] = 3$ in dat geval.

Als f wel een nulpunt heeft in F, dan ook in $F(\zeta)$, dus zijn alle nulpunten van f (namelijk $\zeta^i\alpha$ voor $0 \leq i \leq 2$) bevat in $F(\zeta)$, dus geldt $[\Omega : F(\zeta)] = 1$.

(a) $F = \mathbf{Q}$. Het lichaam $\mathbf{Q}$ bevat noch een nulpunt van f, noch een derdemachts eenheidswortel, dus de graad is $2 \cdot 3 = 6$.
(b) $F = \mathbf{R}$. Het lichaam $\mathbf{R}$ bevat wel een nulpunt van f, maar geen derdemachts eenheidswortel, dus de graad is $2 \cdot 1 = 2$.
(c) $F = \mathbf{F}_3$. De graad is 1 zoals al eerder opgemerkt.
(d) $F = \mathbf{F}_7$. De groep $\mathbf{F}_7^*$ heeft orde 6 en bevat dus een element van orde 3. Als f een nulpunt $\alpha \in \mathbf{F}_7$ had, dan gold $\alpha^3 = 2$ in de groep $\mathbf{F}_7^*$ van orde 6, dus $1 = \alpha^6 = 2^2 = 4$, tegenspraak. Dus f heeft geen nulpunt in $\mathbf{F}_7$ en de gezochte graad is $1 \cot 3 = 3$.
(e) $F = \mathbf{F}_{11}$. De groep $\mathbf{F}_{11}^*$ heeft orde 10 en bevat dus geen element van orde 3. Het homomorfisme $\mathbf{F}_{11}^* \to \mathbf{F}_{11}^*$ dat x stuurt naar x^3 heeft dus triviale kern en is dus injectief en daarmee ook surjectief. Alle elementen van $\mathbf{F}_{11}$ zijn dus derdemachten, in het bijzonder 2. Dat betekent dat f een nulpunt heeft in $\mathbf{F}_{11}$, dus de gezochte graad is $2 \cot 1 = 2$.
(f) $F = \mathbf{F}_{13}$. De groep $\mathbf{F}_{13}^*$ heeft orde 12 en bevat dus een element van orde 3. Als f een nulpunt $\alpha \in \mathbf{F}_{13}$ had, dan gold $\alpha^3 = 2$ in de groep $\mathbf{F}_{13}^*$ van orde 12, dus $1 = \alpha^{12} = 2^4 = 16$, tegenspraak. Dus f heeft geen nulpunt in $\mathbf{F}_{13}$ en de gezochte graad is $1 \cot 3 = 3$.

Opgave 2. Definieer het polynoom $f = x^4 - 2x^2 + 25 \in \mathbf{Q}[x]$. Zij $\alpha \in \mathbf{C}$ een nulpunt van f.

(a) Laat zien dat $\beta = \alpha^3 + 3\alpha$ en $\gamma = \alpha^3 - 7\alpha$ beide graad 2 over $\mathbf{Q}$ hebben.
(b) Laat zien dat er geldt $\mathbf{Q}(\beta, \gamma) = \mathbf{Q}(\alpha)$.
(c) Bewijs dat f irreducibel is.
(d) Bewijs dat $\mathbf{Q}(\alpha)$ Galois is over $\mathbf{Q}$ en bepaal de Galoisgroep $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$.
(e) Wat zijn de nulpunten van f in $\mathbf{Q}(\alpha)$?
(f) Geef alle deellichamen van $\mathbf{Q}(\alpha)$.

Uitwerking:

(a) Uitwerken geeft $\beta^2 = -200$ en $\gamma^2 = 300$.
(b) Het is duidelijk dat geldt $\beta, \gamma \in \mathbf{Q}(\alpha)$, dus $\mathbf{Q}(\beta, \gamma) \subset \mathbf{Q}(\alpha)$. Uit $\alpha = \frac{1}{10}(\beta - \gamma)$ volgt ook $\alpha \in \mathbf{Q}(\beta, \gamma)$, dus $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\beta, \gamma)$.
(c) We laten eerst zien dat $\mathbf{Q}(\beta, \gamma)$ graad (minstens) 4 heeft. Er geldt $(\beta/10)^2 = -2$ en $(\gamma/10)^2 = 3$, dus $\mathbf{Q}(\sqrt{-2})$ en $\mathbf{Q}(\sqrt{3})$ zijn bevat in $\mathbf{Q}(\beta, \gamma)$. Het lichaam $\mathbf{Q}(\sqrt{3})$ is isomorf met een deellichaam van $\mathbf{R}$, dus -2 is geen kwadraat in dat lichaam. We concluderen $[\mathbf{Q}(\sqrt{3}, \sqrt{-2}) : \mathbf{Q}(\sqrt{3})] \geq 2$, dus

$$[\mathbf{Q}(\beta, \gamma) : \mathbf{Q}] \geq [\mathbf{Q}(\sqrt{3}, \sqrt{-2}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3}, \sqrt{-2}) : \mathbf{Q}(\sqrt{3})] \cdot [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \geq 2 \cdot 2 = 4.$$

Uit (b) volgt dat α graad minstens 4 heeft, dus het minimum polynoom van α heeft minstens graad 4, terwijl het ook een deler is van $f = x^4 - 2x^2 + 25$. Hieruit volgt dat het minimum polynoom van α gelijk is aan f, dus f is irreducibel.
(d) De ongelijkheden uit de middelste regel van het bewijs van (c) zijn dus allemaal gelijkheden, dus volgt $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-2}, \sqrt{3})$, wat een ontbindingslichaam is van $(x^2 + 2)(x^2 - 3)$, dus het is normaal. Separabiliteit volgt omdat de karakteristiek gelijk is aan 0. Hieruit volgt dat $\mathbf{Q}(\alpha)$ Galois is over $\mathbf{Q}$. De Galoisgroep heeft orde 4. Voor elk Galois automorfisme σ zijn de beelden van $\sqrt{-2}$ en $\sqrt{3}$ gelijk aan $\pm\sqrt{-2}$ respectievelijk $\pm\sqrt{3}$, dus σ heeft orde 1 of 2. De Galoisgroep is dus isomorf met de V_4.
(e) Twee van de nulpunten zijn duidelijk $\pm\alpha$. Omdat er geldt $\alpha = \frac{1}{10}(\beta - \gamma)$ en de Galois automorfismen β en γ sturen naar $\pm\beta$ respectievelijk $\pm\gamma$, zijn de geconjugeerden van α gelijk aan

$$\tfrac{1}{10}(\beta - \gamma) = \alpha, \qquad \tfrac{1}{10}(-\beta + \gamma) = -\alpha, \qquad \tfrac{1}{10}(\beta + \gamma) = \tfrac{1}{5}(\alpha^3 - 2\alpha), \qquad \tfrac{1}{10}(-\beta - \gamma) = -\tfrac{1}{5}(\alpha^3 - 2\alpha).$$

(f) De V_4 heeft drie ondergroep van orde 2, corresponderend met de lichamen $\mathbf{Q}(\sqrt{-2}), \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{-6})$. Daarnaast zijn er uiteraard nog $\mathbf{Q}$ en $\mathbf{Q}(\alpha)$.

Opgave 3. Zij $\Phi_{15} \in \mathbf{Z}[x]$ het 15-de cyclotomische polynoom en $K = \Omega_{\mathbf{Q}}^{\Phi_{15}}$ een ontbindingslichaam van Φ_{15} over $\mathbf{Q}$. Zij $\zeta = \zeta_{15} \in K$ een nulpunt van Φ_{15}.

(a) Laat zien dat de Galoisgroep $\mathrm{Gal}(K/\mathbf{Q})$ isomorf is met $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$.
(b) Laat zien dat de elementen $-3, 5, -15 \in K$ kwadraten zijn in K.
(c) Bepaal alle deellichamen F van K waarvoor de graad $[F : \mathbf{Q}]$ gelijk is aan 4.
(d) Laat zien dat de deellichamen $\mathbf{Q}(\zeta^3)$ en $\mathbf{Q}(\zeta + \zeta^{11})$ van K hetzelfde zijn.
(e) Zij p een priemgetal. Laat zien dat Φ_{15} een nulpunt heeft in $\mathbf{F}_{p^4}$.
(f) Zij p een priemgetal. Laat zien dat Φ_{15} niet irreducibel is over $\mathbf{F}_p$.

Uitwerking (met extra opmerkingen):

(a) Volgens Stelling 24.14 is het polynoom Φ_{15} irreducibel en volgens 24.15 is de Galoisgroep isomorf met $(\mathbf{Z}/15\mathbf{Z})^*$, wat volgens de Chinese reststelling isomorf is met $(\mathbf{Z}/3\mathbf{Z})^* \times (\mathbf{Z}/5\mathbf{Z})^*$. Het gevraagde volgt uit het feit dat $(\mathbf{Z}/3\mathbf{Z})^*$ en $(\mathbf{Z}/5\mathbf{Z})^*$ cyclische groepen van orde 2 respectievelijk 4 zijn.
(b) We mogen 24.12 niet direct toepassen op $\mathbf{Q}(\zeta)$ omdat 15 niet priem is. Maar als we definiëren $\zeta_3 = \zeta^5$ en $\zeta_5 = \zeta^3$, dan zijn ζ_3 en ζ_5 primitieve derde- en vijfdemachts eenheidswortels. Passen we 24.12 toe op $\mathbf{Q}(\zeta_3)$ en $\mathbf{Q}(\zeta_5)$, dan vinden we dat in deze deellichamen van $\mathbf{Q}(\zeta) = K$ de elementen -3 respectievelijk 5 kwadraten zijn, dus dat geldt ook in K. Uiteraard is dan ook het product -15 een kwadraat.
(c) Deellichamen van graad 4 corresponderen met ondergroepen van $\mathrm{Gal}(K/\mathbf{Q})$ van index 4. Omdat de orde van $\mathrm{Gal}(K/\mathbf{Q})$ gelijk is aan 8, zijn dit de ondergroepen van orde 2. Er zijn drie ondergroepen van $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$ van orde 2, namelijk voortgebracht door paren van elementen van orde een deler van 2 (behalve het paar $(0, 0)$), dus door de elementen $(0, 2)$, $(1, 0)$, respectievelijk $(1, 2)$. Deze corresponderen met de elementen van $(\mathbf{Z}/15\mathbf{Z})^*$ die kwadraat 1 hebben (en niet zelf 1 zijn); dat zijn $4, -4, -1 \in (\mathbf{Z}/15\mathbf{Z})^*$, dus we zoeken drie deellichamen.

We kunnen nu net als in Stelling 24.10 invariante deellichamen proberen op te schrijven die met deze ondergroepen corresponderen, maar het bewijs vertelt ons niet dat de lichamen die we krijgen daadwerkelijk graad 4 hebben, want het bewijs gebruikt dat p priem is (en 15 is dat niet). We krijgen de lichamen

$$F_1 = \mathbf{Q}(\zeta + \zeta^4), \qquad F_2 = \mathbf{Q}(\zeta + \zeta^{-4}), \qquad F_3 = \mathbf{Q}(\zeta + \zeta^{-1})$$

en zouden dan nog moeten bewijzen dat deze daadwerkelijk graad 4 hebben, of, wat equivalent is, dat $\mathbf{Q}(\zeta)$ graad 2 heeft over deze lichamen. Voor het derde lichaam volgt dat bijvoorbeeld uit het feit dat ζ een nulpunt is van $x^2 - (\zeta + \zeta^{-1})x + 1$.

In plaats van dit argument te completeren, wat voor F_1 en F_2 zeker lastiger is, geven we naast F_3 nog twee deellichamen van graad 4, namelijk $F_4 = \mathbf{Q}(\sqrt{-3}, \sqrt{5})$ en $F_5 = \mathbf{Q}(\zeta_5)$. Het feit dat deze lichamen bevat zijn in K volgt uit onderdeel (b). Het feit dat de graad van F_4 over $\mathbf{Q}$ gelijk is aan 4 volgt analoog aan het argument in opgave 2(c). Het lichaam F_5 heeft graad 4 over $\mathbf{Q}$ volgens 24.10. We laten nu zien dat de drie lichamen F_3, F_4, F_5 verschillend zijn. De lichamen F_4 en F_5 zijn verschillend omdat de bijbehorende Galoisgroepen isomorf zijn met V_4 respectievelijk $\mathbf{Z}/4\mathbf{Z}$.

Het lichaam F_3 is verschillend van F_4 en F_5 omdat F_3 in te bedden is in $\mathbf{R}$ terwijl dat voor F_4 en F_5 niet kan.

Overigens geldt $F_1 = F_4$ en $F_2 = F_5$. Dit laatste zien we in het volgende onderdeel.

(d) Merk op dat K ingebed kan worden in $\mathbf{C}$ door ζ te sturen naar $e^{2\pi i/15}$. De beelden van ζ, ζ^6 en ζ^{11} vormen dan een gelijkzijdige driehoek met middelpunt 0, dus de som van deze drie elementen is 0, dus $\zeta + \zeta^{11} = -\zeta^6 = -\zeta_5^2$. Een andere manier om dit in te zien is door te gebruiken dat $\zeta_3 = \zeta^5$ een nulpunt is van $x^2 + x + 1$, dus we vinden $\zeta^{10} + \zeta^5 + 1 = 0$, waaruit ook volgt $\zeta + \zeta^{11} = \zeta(1 + \zeta^{10}) = -\zeta^6$.

Er volgt dus dat $\zeta + \zeta^{11} = -\zeta^6$ bevat is in $\mathbf{Q}(\zeta^3)$. Andersom geldt $\zeta^3 = \zeta^{18} = -(-\zeta^6)^3 = -(\zeta + \zeta^{11})^3$, dus ζ^3 is bevat in $\mathbf{Q}(\zeta + \zeta^{11})$ en we vinden dat de twee lichamen gelijk zijn.

Veel mensen probeerden het volgende. Beide lichamen zijn invariant onder het Galoisautomorfisme τ dat ζ naar ζ^{11}, want $(\zeta^{11})^3 = \zeta^{33} = \zeta^3$ en $\zeta^{11} + (\zeta^{11})^{11} = \zeta^{11} + \zeta^{121} = \zeta^{11} + \zeta$. Maar dit is nog geen compleet bewijs, want het laat alleen zien dat beide lichamen bevat zijn in het invariante deellichaam dat hoort bij de ondergroep van orde 2 voortgebracht door τ. Dit invariante deellichaam heeft graad 4, dus het zou voldoende zijn om nog laten zien dat zowel $\mathbf{Q}(\zeta^3) = \mathbf{Q}(\zeta_5)$ als $\mathbf{Q}(\zeta + \zeta^{11})$ graad 4 hebben over $\mathbf{Q}$. Voor $\mathbf{Q}(\zeta_5)$ is dit duidelijk (zie onderdeel (c)), maar voor $\mathbf{Q}(\zeta + \zeta^{11})$ is dat a priori niet duidelijk.

(e) Voor $p = 3$ geldt $x^{15} - 1 = (x^5)^3 - 1 = (x^5 - 1)^3 = (x - 1)^3\Phi_5^3$, dus Φ_{15} is het product van factoren $x - 1$ en Φ_5 over $\mathbf{F}_3$. Omdat Φ_5 geen nulpunten heeft in $\mathbf{F}_3$ is Φ_5 ofwel irreducibel, of het product van twee irreducibele kwadratische polynomen. In beide gevallen liggen de nulpunten van Φ_5, en dus van Φ_{15}, in $\mathbf{F}_{p^4}$ (in het laatste geval zelfs in $\mathbf{F}_{p^2}$).

Voor $p = 5$ geldt $x^{15} - 1 = (x^3)^5 - 1 = (x^3 - 1)^3 = (x - 1)^5\Phi_3^5$, dus Φ_{15} is het product van factoren $x - 1$ en Φ_3 over $\mathbf{F}_5$. De nulpunten van Φ_{15} hebben dus graad 1 of 2 over $\mathbf{F}_5$ en ze liggen dus allemaal in $\mathbf{F}_{5^2}$ en dus zeker in $\mathbf{F}_{5^4}$.

Stel nu $p \neq 3, 5$. Dan geldt $p^4 \equiv 1 \pmod 3$ en $p^4 \equiv 1 \pmod 5$, dus wegens de Chinese reststelling ook $p^4 \equiv 1 \pmod{15}$. De orde $p^4 - 1$ van de groep $\mathbf{F}_{p^4}^*$ is dus een veelvoud van 15. Omdat deze groep cyclisch is, bevat die groep dus een element van orde 15 en dus een primitieve 15-e eenheidswortel. Dat is een nulpunt van Φ_{15}.

(f) Elk nulpunt van Φ_{15} heeft volgens onderdeel (e) hooguit graad 4 over $\mathbf{Q}$, dus het minimumpolynoom van elk nulpunt heeft hooguit graad 4. Omdat Φ_{15} graad 8 heeft, volgt dat Φ_{15} niet irreducibel is.

Opgave 4. Voor elke gehele $n \geq 1$ en $a \in \mathbf{Q}^*$ definiëren we

$$f_{a,n} = x^{2n} + x^n + a \in \mathbf{Q}[x].$$

Voor welke $n \geq 1$ en $a \in \mathbf{Q}^*$ is de Galoisgroep $\mathrm{Gal}(\Omega_{\mathbf{Q}}^{f_{a,n}}/\mathbf{Q})$ oplosbaar?

Uitwerking (met extra opmerkingen): Het antwoord is voor alle n en a.

We claimen eerst dat om dit te bewijzen het voldoende is om te laten zien dat alle nulpunten van $f_{a,n}$ zijn bevat in een radicale afsluiting $\mathbf{Q}^{\mathrm{rad}}$ van $\mathbf{Q}$.

De meeste mensen die dit gebruikten hebben dit gewoon aangenomen, maar deze claim volgt niet direct uit Stelling 25.15, want onderdeel 3 van die stelling heeft alleen betrekking op minimale, en dus irreducibele polynomen. Om de claim te bewijzen merken we op dat als alle nulpunten bevat zijn in $\mathbf{Q}^{\mathrm{rad}}$, dan is ook $\Omega_{\mathbf{Q}}^{f_{a,n}}$ bevat in $\mathbf{Q}^{\mathrm{rad}}$. Wegens Stelling 23.9 kunnen we een primitief element $x \in \Omega_{\mathbf{Q}}^{f_{a,n}}$ vinden. Dat element x is bevat in $\mathbf{Q}^{\mathrm{rad}}$, dus Stelling 25.15 geeft dat de Galoisgroep van $f_{\mathbf{Q}}^x$, dat wil zeggen de Galoisgroep $\mathrm{Gal}(\Omega_{\mathbf{Q}}^{f_{a,n}}/\mathbf{Q})$, oplosbaar is.

Een schets van een alternatief bewijs van de claim: schrijf $\Omega_{\mathbf{Q}}^{f_{a,n}}$ als een toren van uitbreidingen waarbij we telkens een nulpunt van $f_{a,n}$ toevoegen. Stelling 25.15 geeft dan dat elke stap in de toren een oplosbare Galoisgroep heeft. Hieruit volgt dat de hele groep $\mathrm{Gal}(\Omega_{\mathbf{Q}}^{f_{a,n}}/\mathbf{Q})$ een filtratie (keten van ondergroepen) heeft waarin in elke stap de volgende ondergroep normaal is in de vorige en het bijbehorende quotient oplosbaar is. Dit impliceert dat de hele groep $\mathrm{Gal}(\Omega_{\mathbf{Q}}^{f_{a,n}}/\mathbf{Q})$ oplosbaar is. Vergelijk dit met opgave 10.18.

Nu we de claim hebben bewezen, hoeven we dus alleen maar te laten zien dat de nulpunten van $f_{a,n}$ bevat zijn in $\mathbf{Q}^{\mathrm{rad}}$. Zij α een nulpunt van $f_{a,n}$. Dan is α^n een nulpunt van $g_a = x^2 + x + a$. Omdat g_a kwadratisch is zijn de nulpunten van g_a bevat in $\mathbf{Q}^{\mathrm{rad}}$. Om precies te zijn, zijn ze bevat in de kwadratische uitbreiding $\mathbf{Q}(\sqrt{1-4a})$. Dus α^n is bevat in $\mathbf{Q}^{\mathrm{rad}}$, dus α is zelf bevat in $\mathbf{Q}^{\mathrm{rad}}$. Dit geldt voor alle nulpunten van $f_{a,n}$, dus uit de claim volgt dat de genoemde Galoisgroep inderdaad oplosbaar is.