Uitwerkingen hertentamen Algebra 3 van 8 juli 2013

Door: Raymond van Bommel

Opgave 1. De lichaamsuitbreiding $\mathbb{Q}(\beta)/\mathbb{Q}(\beta^3)$ wordt voortgebracht door het element β dat een nulpunt is van het polynoom $X^3 - \beta^3 \in \mathbb{Q}(\beta^3)[X]$. In het bijzonder is het minimumpolynoom $f^{\beta}_{\mathbb{Q}(\beta^3)}$ van β over $\mathbb{Q}(\beta^3)$ een deler hiervan en is de graad van de uitbreiding hoogstens 3 wegens stelling 21.5.

Voor $\beta = 1$ heeft $\mathbb{Q}/\mathbb{Q}$ graad 1. Voor $\beta = \zeta_3$ heeft $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ graad 2 vanwege stelling 24.15. Voor $\beta = \sqrt[3]{2} \in \mathbb{R}$ heeft $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ graad 3, omdat $\sqrt[3]{2}$ een nulpunt is van het polynoom $X^3 - 2 \in \mathbb{Q}[X]$, dat Eisenstein is bij 2 en dus irreducibel is. $\square$

Opgave 2. Schrijf $\alpha = x^2$. We berekenen $\alpha^p = (y^p - y)^{2p} = (y^{p^2} - y^p)^2 = (y^p - y^{p^2})^2$. Omdat $y \in \mathbb{F}_{p^2}$ geldt $y^{p^2} = y$ vanwege formule 22.2. In het bijzonder geldt $\alpha^p = (y^p - y)^2 = \alpha$. Vanwege formule 22.2 volgt hieruit dat $\alpha \in \mathbb{F}_p$. $\square$

Opgave 3. (a) Omdat dit polynomen van graad 2 zijn volstaat het om te controleren dat ze geen nulpunten in $\mathbb{F}_5$ hebben. Evalueren in $X = 0, 1, 2, 3, 4$ geeft voor het eerste polynoom de waarden $2, 4, 3, 4, 2$ en voor het tweede polynoom de waarden $3, 4, 2, 2, 4$. Beide polynomen hebben geen nulpunten in $\mathbb{F}_5$ en zijn irreducibel. Een andere methode is de abc-formule te gebruiken, en op te merken dat de discriminanten -2 en 2, beide geen kwadraat zijn. $\square$

(b) De abc-formule geeft: $\alpha = (-1 \pm \sqrt{-2})/2$. Merk op dat $2^2 = -1$, dus $\alpha = (-1 \pm 2\sqrt{2})/2 = 2 \pm \sqrt{2}$. Beschouw het ringhomomorfisme $\varphi : \mathbb{F}_5[X] \to K_2$ dat X naar $2 - \beta$ stuurt. Merk op dat $2 - \beta$ nulpunt is van $X^2 + X + 2$. Daarom is $X^2 + X + 2$ bevat in de kern van φ en factoriseert φ via een homomorfisme $\psi : K_1 \cong \mathbb{F}_5[X]/(X^2 + X + 2) \to K_2$. Nu is ψ een lichaamshomomorfisme. In het bijzonder is ψ injectief. Omdat K_1 en K_2 allebei 25 elementen hebben vanwege onderdeel (a) en stelling 21.5 volgt automatisch dat ψ een isomorfisme is. $\square$

Opgave 4. De werking van S_4 op L is trouw, dus S_4 is een ondergroep van $\mathrm{Aut}(L)$, en $K = L^{S_4}$, dus is L/K Galois met Galoisgroep S_4. Voor elk van de elementen α in de deelopgaven willen we de kleinste deeluitbreiding $K(\alpha)$ van $K \subset L$ vinden die α bevat. In de Galoiscorrespondentie (24.4) correspondeert dat met de grootste ondergroep G_α van S_4 die α invariant laat, dat wil zeggen, met de stabilisator $(S_4)_\alpha$ van α. De graad $[L : K(\alpha)]$ is de orde van G_α, en is ook gelijk aan $24/\#(S_4 {\cdot} \alpha)$.

(a) Voor $\alpha = T_1 + T_2 + T_3 + T_4$ geldt dat $G_\alpha = S_4$. Elk element van S_4 laat α invariant. Er geldt dus $[L : K(\alpha)] = 24$.

(b) Voor $\alpha = T_1 + T_2 + T_3$ geldt dat G_α de ondergroep S_3 van S_4 is die alleen T_1, T_2 en T_3 permuteert, het is de stabilisator van T_4. Er geldt dus $[L : K(\alpha)] = 6$.

(c) Voor $\alpha = T_1 + T_2$ geldt dat G_α de ondergroep van S_4 is voortgebracht door de 2 2-cykels (T_1, T_2) en (T_3, T_4). Er geldt dus $[L : K(\alpha)] = 4$. Ter controle: de baan van $T_1 + T_2$ is de verzameling $T_i + T_j$ met $i \neq j$, die $\binom{4}{2} = 6$ elementen heeft, en $24/6 = 4$.

(d) Voor $\alpha = T_1$ geldt dat G_α de stabilisator van T_1 is, die heeft 6 elementen. Er geldt dus $[L : K(\alpha)] = 6$. Controle: de baan van T_1 is $\{T_1, T_2, T_3, T_4\}$, en $24/4 = 6$.

Opgave 5. De uitbreiding $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois en de Galoisgroep is $\mathbb{F}_{11}^*$ volgens stelling 24.15: $a \in \mathbb{F}_{11}^*$ werkt als σ_a en $\sigma_a(\zeta) = \zeta^a$. De groep $\mathbb{F}_{11}^*$ is cyclisch van orde 10 en heeft vier cyclische ondergroepen van orde 1, 2, 5 resp. 10. Vanwege de Galois-correspondentie (24.4) heeft de lichaamsuitbreiding $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ vier tussenlichamen van graad 10, 5, 2 resp. 1 over $\mathbb{Q}$. Vanwege stelling 25.10 is het element z_S construeerbaar dan en slechts dan als het in het tussenlichaam $L \subset \mathbb{Q}(\zeta)$ van graad 2 over $\mathbb{Q}$ is bevat. Vanwege de Galoiscorrespondentie geldt dit dan en slechts dan als z_S invariant gelaten wordt door de ondergroep van orde 5 van $(\mathbb{Z}/11\mathbb{Z})^*$. Die ondergroep is $H := \langle 3 \rangle = \{1, 3, 4, 5, 9\} \subset (\mathbb{Z}/11\mathbb{Z})^*$.

(a) De verzameling $S = \{1, \zeta, \zeta^3, \zeta^4, \zeta^5, \zeta^9\}$ is de vereniging van de banen van ζ en 1 onder H, dus is z_S invariant onder H, dus in $\mathbb{Q}(\zeta)^H = L$, en dus construeerbaar. $\square$

(b) Laat $B = \mathbb{F}_{11}^* \cdot \zeta = \{\zeta^a : a \in \mathbb{F}_{11}^*\}$. Vanwege het bewijs van 24.10 is B een $\mathbb{Q}$-basis van $\mathbb{Q}(\zeta)$, en zelfs een normale basis: de Galoisgroep werkt op B. Voor $T \subset \mathbb{F}_{11}^*$ laat $z_T := \sum_{a \in T} \sigma_a(\zeta)$. Dan is het construeerbaar zijn van z_T equivalent met $z_T \in L$, dus met $z_T = \sigma_3(z_T)$. Maar $\sigma_3(z_T) = \sigma_3(\sum_{a \in T} \sigma_a(\zeta)) = \sum_{a \in T} \sigma_3 \sigma_a(\zeta) = \sum_{a \in T} \sigma_{3a}(\zeta) = \sum_{a \in 3T} \sigma_a(\zeta)$, waar $3T = \{3a : a \in T\}$. Omdat B een basis is, is $z_T = z_{3T}$ equivalent met $T = 3T$, en dat is weer equivalent met: T is invariant onder de actie van H op $\mathbb{F}_{11}^*$, en dat is equivalent met de voorwaarde dat T invers beeld is van een deelverzameling van $\mathbb{F}_{11}^*/H$. Het aantal deelverzamelingen van $\mathbb{F}_{11}^*/H$ is $2^2 = 4$. Dus precies 4 van de z_T zijn construeerbaar.

Voor S als in de opgave is het construeerbaar zijn van z_S equivalent met het construeerbaar zijn van z_T, voor $T = \{a \in \mathbb{F}_{11}^* : \sigma_a(\zeta) \in S\}$: het hangt er niet van af of $1 \in S$ of $1 \notin S$. Dus precies 8 van de z_S zijn construeerbaar.