Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 3 - 14 juni 2012, 10:00 – 13:00

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt. Je mag de syllabus, boeken en aantekeningen gebruiken. Het gebruik van een rekenmachine is niet toegestaan.

Voor een lichaam K noteren we met $\overline{K}$ een algebraïsche afsluiting van K.

Opgave 1. Laat $f = X^6 + 4X^4 + 2X^3 + 4X^2 + 4X + 2 \in \mathbf{Q}[X]$.
(a) Laat zien dat f irreducibel is in $\mathbf{Q}[X]$.
(b) Laat α een nulpunt van f zijn in $\overline{\mathbf{Q}}$. Bereken de minimumpolynomen $f_{\mathbf{Q}}^{\alpha^3+2\alpha}$ en $f_{\mathbf{Q}(\alpha^3+2\alpha)}^{\alpha}$.

Opgave 2.
(a) Welk van de lichamen $\mathbf{Q}, \mathbf{Q}(\sqrt{2}), \mathbf{R}, \mathbf{C}, \mathbf{F}_{125}$ heeft een Galoisuitbreiding met als Galoisgroep een cyclische groep van orde 3? Motiveer je antwoorden.
(b) Laat $g = (X^2 + 6)(X^2 + 10)(X^2 - 15) \in \mathbf{Q}[X]$. Bereken de Galoisgroep $\mathrm{Gal}(g) = \mathrm{Gal}(\Omega_{\mathbf{Q}}^{g}/\mathbf{Q})$.

Opgave 3. Beschouw het polynoom $h = X^7 + X + 1 \in \mathbf{F}_2[X]$. Laat nu $Z = \{x \in \overline{\mathbf{F}_2} : h(x) = 0\}$.
(a) Bereken $(Xh)' \in \mathbf{F}_2[X]$, de afgeleide van $Xh \in \mathbf{F}_2[X]$. Laat zien dat $Z \cup \{0\}$ een additieve ondergroep is van $\overline{\mathbf{F}_2}$ van orde 8.
(b) Laat $F = \mathrm{Frob}\colon \overline{\mathbf{F}_2} \to \overline{\mathbf{F}_2}$, $x \mapsto x^2$ en geef met $F^i = F \circ \ldots \circ F$ de i-voudige iteratie van F aan. Laat zien dat voor $x \in Z$ het volgende geldt:

$$F^3(x) + F(x) + x = 0, \qquad F^7(x) = x.$$

Concludeer dat h irreducibel is in $\mathbf{F}_2[X]$.

Opgave 4. Laat K een lichaam zijn en laat $\zeta \in \overline{K}$, $\zeta \neq 0$.
(a) Toon aan: $[K(\zeta) : K(\zeta + \zeta^{-1})] \in \{1, 2\}$.
(b) Neem aan dat ζ priemorde heeft in de multiplicatieve groep $\overline{K}^*$. Bewijs:

$$[K(\zeta) : K(\zeta + \zeta^{-1})] = 2 \iff 2 \mid [K(\zeta) : K].$$

Oplossingen

1: (a) Eisenstein bij 2. De irreducibiliteit volgt uit het Lemma van Gauss.
(b) Merk op dat $(\alpha^3+2\alpha)^2 = \alpha^6+4\alpha^4+4\alpha^2 = -2\alpha^3-4\alpha-2 = -2(\alpha^3+2\alpha)-2$ en we vinden $f_{\mathbf{Q}}^{\alpha^3+2\alpha} = X^2+2X+2$ (α zit niet in $\mathbf{Q}$, het polynoom is ook Eisenstein bij 2). Merk op dat α een nulpunt is van $X^3+2X-(\alpha^3+2\alpha)$ en dat uit de torenwet volgt dat het minimum polynoom graad 3 heeft: $f^{\alpha}_{\mathbf{Q}(\alpha^3+2\alpha)} = X^3+2X-(\alpha^3+2\alpha)$

2: (a) $\mathbf{Q}$: Ja, neem de unieke L derdegraadsuitbreiding van $\mathbf{Q}(\zeta_7)/\mathbf{Q}$ (verwijs naar stelling). $\mathbf{Q}(\sqrt{2})$: omdat $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ copriem is met 3, volgt dat $L(\sqrt{2})/\mathbf{Q}(\sqrt{2})$ graad 3 over $\mathbf{Q}$ heeft met Galoisgroep C_3 (verwijs naar opgave). $\mathbf{R}, \mathbf{C}$: er zijn geen uitbreidingen van graad ≥ 3 van $\mathbf{R}$ en $\mathbf{C}$ (verwijs naar stelling). $\mathbf{F}_{125}$: de unieke 3-graads uitbreiding van $\mathbf{F}_{125}$, $\mathbf{F}_{125^3}$, is cyclisch van orde 3 (stelling).
(b) Merk op dat $[\mathbf{Q}(\sqrt{15}, \sqrt{-10}) : \mathbf{Q}] = 4$, omdat $\sqrt{-10}$ niet in de reële uitbreiding $\mathbf{Q}(\sqrt{15})$ zit. Merk op dat $(1/5 \cdot \sqrt{-10}\sqrt{15})^2 = -6$, dus de uitbreiding heeft graad 4. Het is nu makkelijk in te zien dat de Galoisgroep een V_4 is (kijk naar de werking op $\sqrt{-10}$ and $\sqrt{15}$).

3: (a) $Xh = X^8+X^2+X =: h_2$, en duidelijk is dat de afgeleide 1 is. Merk op dat $Z \cup \{0\}$ de nulpuntsverzameling is van Xh en dat deze cardinaliteit 8 heeft. Merk op dat als $h_2(x) = h_2(y) = 0$ for $x, y \in \overline{\mathbf{F}_2}$, dat dan geldt $h_2(x+y) = (x+y)^8 = (x+y)^2+(x+y) = x^8+y^8+x^2+y^2+x+y = h(x)+h_2(y) = 0+0 = 0$. Ook zit 0 in de nulpuntsverzameling en inverses zitten er ook in. De claim volgt nu.
(b) Laat $x \in Z$. Dan volgt $xh(x) = 0$ en $xh(x) = F^3(x)+F(x)+x$. We gaan nu rekenen en vinden $F^2(x)$, $F^3(x) = F(x)+x$, $F^4(x) = F^2(x)+F(x)$, $F^5(x) = F^3(x)+F^2(x) = F^2(x)+F(x)+x$, $F^6(x) = F^3(x)+F^2(x)+F(x) = F^2(x)+x$ en $F^7(x) = F^3(x)+F(x) = x$. We concluderen dat $F^7(x) = x$. Het volgt dat $x \in \mathbf{F}_{2^7}$. Omdat we direct zien dat $x \notin \mathbf{F}_2$, en er geen andere tussenlichamen zijn, concluderen we dat h irreducibel is.

4: (a) Merk op dat $\zeta^2 - (\zeta+\zeta)^{-1}\zeta + 1 = 0$ en hier volgt (a) direct uit.
(b) $\Longrightarrow$: Volgt direct uit de torenwet. $\Longleftarrow$: Laat n de orde van ζ zijn. De Galoisgroep van $K(\zeta)/K$ is een ondergroep van de cyclische groep $(\mathbf{Z}/n\mathbf{Z})^*$, en dus weer cyclisch (gebruik wat stellingen). Merk op dat -1 onder de identificatie $\zeta+\zeta^{-1}$ vasthoudt, en dat -1 het unieke element is van orde 2 (uitzondering: $n = 2$): dus als $2|[K(\zeta) : K]$, dan zit -1 in de Galoisgroep en er volgt uit de Galoistheorie dat $K(\zeta) \supsetneq K(\zeta+\zeta^{-1})$. Als $n = 2$, dan is $K(\zeta) = K$ tenzij $\mathrm{char}(K) = 2$. In dit laatste geval is er geen element van orde precies 2.