

## Uitwerking Tentamen Galoistheorie 2016/2017

1 juni 2017, 13-16, SP C1.110

Puntenverdeling: Elk opgaveonderdeel is 0, 1 of 2 punten waard.

*Opgave 1.*

- (a) Het minimumpolynoom van  $\sqrt[3]{2}$  is gelijk aan  $X^3 - 2$ . De nulpunten van dit polynoom zijn  $\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}$ . Omdat  $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ , zien we dat  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  niet normaal is. De uitbreiding is separabel, want het is een eindige lichaamsuitbreiding in karakteristiek 0. De uitbreiding is niet Galois.
- (b) Deze uitbreiding is niet separabel, want het minimumpolynoom  $f = X^7 - t$  heeft één 7-voudig nulpunt over  $\mathbb{F}_7(t)[X]/(X^7 - t)$ . De uitbreiding is normaal, want het minimumpolynoom  $f$  splitst in lineaire factoren. De uitbreiding is niet Galois.
- (c) Stel voor een tegenspraak dat de uitbreiding  $\mathbb{Q}(\alpha)/\mathbb{Q}$  normaal is. Het element  $\alpha \in \mathbb{C}$  is nulpunt van het polynoom  $f = (X^2 - 1)^2 - 3 \in \mathbb{Q}[X]$ . Uitwerken geeft  $f = X^4 - 2X^2 + 1 - 3 = X^4 - 2X^2 - 2$ . Dit polynoom is Eisenstein bij 2 en dus irreducibel. De uitbreiding  $\mathbb{Q}(\alpha)/\mathbb{Q}$  heeft dus graad 4. Omdat  $1 + \sqrt{2} > 0$  geldt  $\alpha \in \mathbb{R}$  en  $\mathbb{Q}(\alpha) \subset \mathbb{R}$ . Zij  $\beta \in \mathbb{C}$  een kwadratische wortel van het element  $1 - \sqrt{3} \in \mathbb{R}$ . Dan geldt  $f(\beta) = 0$ . Omdat  $f$  irreducibel is volgt uit de aanname dat  $\mathbb{Q}(\alpha)$  normaal is dat  $\beta \in \mathbb{Q}(\alpha) \subset \mathbb{R}$ . Maar dit is een tegenspraak: Omdat  $1 - \sqrt{3} < 0$  is het element  $\beta \in \mathbb{C}$  niet reëel! De uitbreiding is wel separabel want het polynoom  $f$  is separabel. De uitbreiding is niet Galois.
- (d) Er geldt  $\zeta := \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ . Berekening laat zien dat  $\zeta^2 + \zeta + 1 = 0$ , en dus is  $\zeta$  een primitieve derde eenheidswortel. Het minimum polynoom  $f = X^5 - 3 \in \mathbb{Q}[X]$  (Eisenstein) ontbindt als

$$f = (X - \sqrt[3]{5})(X - \zeta_3 \sqrt[3]{5})(X - \zeta_3^2 \sqrt[3]{5}) \in \mathbb{Q}[X].$$

Dus  $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$  is het splitsingslichaam van  $f$ . Hierom is de uitbreiding normaal. Omdat het een eindige lichaamsuitbreiding is in karakteristiek 0, is de uitbreiding separabel, en dus ook Galois.

*Opgave 2.*

- (a) De discriminant van een derde graadspolynoom van de vorm  $X^3 + aX + b \in \mathbb{Q}[X]$  is gelijk aan  $\Delta_f = -4a^3 - 27b^2$ . Dus voor het polynoom  $X^3 - X + 1 \in \mathbb{Q}[X]$  hebben we  $a = -1$  en  $b = 1$ . Dit geeft  $4 - 27 = -23$ . De discriminant van  $f$  is dus geen kwadraat in  $\mathbb{Q}$ . Omdat het ontbindingslichaam van  $f$  een wortel van de discriminant bevat, zien we dat dit ontbindingslichaam een kwadratische deeluitbreiding heeft. De enige transitieve ondergroep van  $S_3$  met een normale ondergroep van index 2 is de groep  $S_3$  zelf. De Galoisgroep van  $f$  is dus isomorf met  $S_3$ .
- (b) Door de substitutie  $Y = X^2$  zien we dat geldt  $f = (X^2 - 2)(X^1 + 1)$ . Het polynoom  $f$  is dus reducibel, en het ontbindingslichaam van  $f$  is het compositum  $\mathbb{Q}(\sqrt{2}, i)$  van de kwadratische uitbreidingen  $\mathbb{Q}(\sqrt{2})$  en  $\mathbb{Q}(i)$  van  $\mathbb{Q}$ . Beschouw het groepsmorphisme  $\psi: \text{Gal}(K/\mathbb{Q}) \rightarrow \{\pm 1\}^2$  gegeven door  $\sigma \mapsto (\sigma(\sqrt{2})/\sqrt{2}, \sigma(i)/i)$ . Stel  $\sigma \in \text{Gal}(K/\mathbb{Q})$  ligt in de kern van  $\psi$ . Dan geldt  $\sigma(\sqrt{2}) = \sqrt{2}$  en  $\sigma(i) = i$ . Omdat  $K/\mathbb{Q}$  wordt voortgebracht door  $\sqrt{2}$  en  $i$  volgt dat  $\sigma = 1$  op  $K$ . De kern van  $\psi$  is dus triviaal, en de afbeelding is injectief. We claimen dat  $K = \mathbb{Q}(\sqrt{2}, i)$  graad 4 heeft over  $\mathbb{Q}$ . Als deze claim waar is, dan zien we dat enerzijds  $\#\text{Gal}(K/\mathbb{Q}) = 4$  en  $\psi$  is een injectie tussen

twee groepen van orde 4, en dus een surjectie, en dus een isomorfisme. Het is dus voldoende om de claim te bewijzen. We weten dat  $\sqrt{2}$  graad 2 heeft over  $\mathbb{Q}$ . Omdat  $\sqrt{2} \in \mathbb{R}$  en  $i \notin \mathbb{R}$ , zien we dat  $i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ , en dus is de graad van  $\mathbb{Q}(i, \sqrt{2})$  over  $\mathbb{Q}(\sqrt{2})$  gelijk aan 2. Ofwel  $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$  heeft graad 4.

- (c) Er geldt  $f = X^5 - 100x + 2 \in \mathbb{Q}[X]$ . Het polynoom is dus Eisenstein bij 2 en irreducibel. De Galoisgroep van  $f$  bevat dus een 5-cykel. De afgeleide van  $f$  is gelijk aan  $5x^4 - 100$  en heeft dus precies 2 nulpunten over  $\mathbb{R}$ , namelijk  $\pm\sqrt[4]{20}$ . Er geldt

$$f(\sqrt[4]{20}) = \sqrt[4]{20}(\sqrt{20} - 4)(\sqrt{20} + 4) + 2 = \sqrt[4]{20}(20 - 16) + 2 > 0$$

$$f(-\sqrt[4]{20}) = -\sqrt[4]{20} \cdot 4 + 2 < -4 + 2 < 0$$

(in de tweede vergelijkingen gebruiken we de ongelijkheid  $\sqrt[4]{20} > 1$ .) Wegens de tussenwaardstelling heeft  $f$  drie nulpunten over  $\mathbb{R}$ . De twee overige nulpunten zijn dus complex en worden verwisseld door de complexe conjugatie. De Galoisgroep van  $f$  bevat dus een 2-cykel en ook een 5-cykel. Dus  $\text{Gal}(f) = S_5$ .

### Opgave 3.

- (a) Er geldt dat  $85 = 5 \cdot 17$  een product is van twee Fermatpriemgetallen. De 85-e eenheidswortels zijn dus contruëerbare getallen.
- (b) Neem  $Y = X^3$ , dan geldt  $X^6 + X^3 + 1 = Y^2 + Y + 1$ . Het polynoom  $Y^2 + Y + 1 = \Phi_3$  is het derde cyclotomische polynoom, en de nulpunten zijn dus primitieve derde eenheidswortels. De nulpunten van  $X^6 + X^3 + 1$  zijn dus primitieve negende eenheidswortels. Omdat  $\#(\mathbb{Z}/9\mathbb{Z})^\times = 6$  zijn er 6 primitieve negende eenheidswortels. Dus geldt  $\Phi_9 = X^6 + X^3 + 1$ . De Galoisgroep van  $\Phi_9$  is isomorf met  $(\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ . Deze laatste groep is geen 2-groep, en daarom zijn de nulpunten van  $\Phi_9$  niet construeerbaar.
- (c) Stel  $\alpha \in \mathbb{C}$  is een nulpunt van het polynoom  $X^5 - 100$ . Dan geldt  $\alpha^5 = 100$ . Merk op dat voor  $\beta = 1/10\alpha^3 \in \mathbb{Q}(\alpha)$  geldt  $\beta^5 = \frac{100^3}{10^5} = 10$ . Ofwel  $\beta \in \mathbb{Q}(\alpha)$ , en  $\beta$  is een nulpunt van het polynoom  $X^5 - 10$ . Dit polynoom is Eisenstein bij 5 (en 2), en hierom irreducibel. De graad van  $\mathbb{Q}(\beta)$  over  $\mathbb{Q}$  is dus 5, en de graad van  $\mathbb{Q}(\alpha)$  over  $\mathbb{Q}$  is ook 5 (we weten dat deze laatste graad ten hoogste 5 is). Dus is  $f$  irreducibel. Er volgt dat de Galoisgroep van  $f$  een 5-cykel bevat. Hierom kan deze groep niet een 2-groep zijn. De nulpunten van  $f$  zijn dus niet construeerbaar.

### Opgave 4.

- (a) Een mogelijke manier is om te kijken naar de uitbreiding  $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ , waar  $\zeta_7 \in \mathbb{C}$  een primitieve 7-eenheidswortel is. Deze uitbreiding is Galois met groep  $\mathbb{Z}/6\mathbb{Z}$ . We weten dat  $\zeta_7$  een nulpunt is van een kwadratisch polynoom over  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  (namelijk  $X^2 - (\zeta_7 + \zeta_7^{-1})X + 1$ ), en dus is de graad van  $\mathbb{Q}(\zeta_7)/\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  hoogstens 2. Omdat  $\zeta_7 + \zeta_7^{-1}$  stabiel is onder complexe conjugatie zien we dat  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  een reële inbedding heeft, terwijl  $\mathbb{Q}(\zeta_7)$  dat niet heeft. Dus geldt  $\mathbb{Q}(\zeta_7) \neq \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ , en hierom is  $\mathbb{Q}(\zeta_7)$  van graad 2 over  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ . De graad van  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  over  $\mathbb{Q}$  is dus 3. Dus  $\text{Gal}(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ . Er geldt voor  $\alpha = \zeta_7 + \zeta_7^{-1}$  dat

$$\begin{aligned}(\zeta_7 + \zeta_7^{-1}) &= \zeta_7 + \zeta_7^6 \\(\zeta_7 + \zeta_7^{-1})^2 &= \zeta_7^2 + \zeta_7^5 + 2 \\(\zeta_7 + \zeta_7^{-1})^3 &= \zeta_7^3 + \zeta_7^4 + 3(\zeta_7 + \zeta_7^{-1}),\end{aligned}$$

en dus geldt

$$\alpha + \alpha^2 + \alpha^3 = -1 + 2 + 3\alpha.$$

Ofwel het minimumpolynoom van  $\alpha$  over  $\mathbb{Q}$  is gelijk aan  $X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$ .

- (b) Zij  $f \in \mathbb{Q}[X]$  een irreducibel polynoom met  $\text{Gal}(f) \cong \mathbb{Z}/3\mathbb{Z}$ . Embed het ontbindingslichaam  $\Omega$  van  $f$  in  $\mathbb{C}$ . Omdat de uitbreiding  $\Omega/\mathbb{Q}$  normaal is, is  $\Omega$  stabiel onder complexe conjugatie. Dus complexe conjugatie definieert een element  $\sigma \in \text{Gal}(f)$ . Er geldt  $\sigma^2 = 1$ , en dus  $\sigma = 1$  omdat kwadrateren een automorfisme is van  $\mathbb{Z}/3\mathbb{Z}$ . Ofwel de complexe conjugatie werkt triviaal op  $\Omega$ , en dus geldt  $\Omega \subset \mathbb{R} = \mathbb{C}^{(\sigma)}$ .

*Opgave 5.* (a) Zie pag. 43 van het dictaat.

- (b) Stel  $H \subset G$  is een 37-Sylow ondergroep. We gaan laten zien dat  $H$  normaal is. Stel (voor een tegenspraak) dat  $g \in G$  een element is zó dat  $gHg^{-1} \neq H$ . Dan is  $H' = gHg^{-1}$  een 37-Sylow groep verschillend van  $H$ . Er geldt dus  $H \cap H' = 1$ , en dus is de afbeelding  $H \times H' \rightarrow G$ ,  $(h, h') \mapsto hh'$  injectief. Dit is een tegenspraak, want  $\#(H \times H') = 37^2 > 148$ . Dus  $H \subset G$  is normaal, en  $G$  is niet simpel.

### Bonusopgave

*Opgave 6.* Het zou kunnen dat je herkent dat het polynoom  $x^4 - x^3 + x^2 - x + 1$  gelijk is aan het 10-de cyclotomische polynoom  $\Phi_{10}$ . Er geldt namelijk

$$(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1) = x^8 + x^6 + x^4 + x^2 + 1,$$

en dit is een meetkundige reeks in  $y = x^2$ , en dus

$$(x^2 - 1)(x^8 + x^6 + x^4 + x^2 + 1) = x^{10} - 1.$$

De nulpunten van  $\Phi_{10}$  zijn dus de primitieve 10-de eenheidswortels. De afbeelding  $x \mapsto x^3$  induceert een bijectie op de verzameling primitieve 10-de eenheidswortels in  $\mathbb{C}$ , en dus geldt

$$a^3 + b^3 + c^3 + d^3 = a + b + c + d = -(\text{coeff. van } x^3 \text{ in } \Phi_{10}) = 1.$$

• Je kan de uitspraak ook uit de Newton identiteiten halen (dit is makkelijker, misschien was dit een opgave?). Anders, kan je ook direct rekenen. Schrijf

$$\begin{aligned} m_i &= a^i + b^i + c^i + d^i \\ s_i &= i\text{-de symmetrische polynoom.} \end{aligned}$$

Er geldt

$$\begin{aligned} s_2 p_1 &= (ab + \dots)(a + \dots) = (a^2 b + \dots) + 3(abc + \dots) \\ s_1 p_2 &= (a + \dots)(a^2 + \dots) = (a^3 + \dots) + (a^2 b + \dots) \end{aligned}$$

waar met een uitdrukking als  $(X + \dots)$  de  $\mathfrak{S}_4$ -symmetrisatie van het monoom  $X$  wordt bedoeld. Er volgt

$$p_3 = s_1 p_2 - s_2 p_1 + 3s_3 = s_1(s_1^2 - 2s_2) - s_2 s_1 + 3s_3.$$

Er geldt

$$\begin{aligned} s_1 &= a + b + c + d = 1 \\ s_2 &= (ab + \dots) = 1 \\ s_3 &= (abc + \dots) = 1 \\ s_4 &= abcd = 1. \end{aligned}$$

4

Dus

$$p_3 = 1(1^2 - 2) - 1 + 3 = -2 + 3 = 1.$$