Tentamen, uitwerkingen
Lichamen & Galoistheorie

9 november 2021, 11.30u - 14.30u

Opgave 1. (18 punten)

Geef voor elk van de volgende beweringen aan of deze **waar** of **onwaar** is. Je hoeft bij deze opgave geen toelichtingen te geven!

(a) Als K/F een Galoisuitbreiding is en E/F is een deeluitbreiding, dan is E ook Galois over F.
(b) Het polynoom $x^3 - 5x + 6$ is irreducibel over $\mathbb{Q}$.
(c) Het splijtlichaam van $x^6 - 1$ heeft graad 2 over $\mathbb{Q}$.
(d) Als F een eindig lichaam is en K/F een eindige uitbreiding, dan is K/F Galois.
(e) Het polynoom $x^6 + 60x^3 + 10$ is irreducibel over $\mathbb{Q}$.
(f) Zij $f(x) \in F[x]$ een polynoom, K/F het splijtlichaam van $f(x)$ en $\alpha, \beta \in K$ twee wortels van $f(x)$. Dan bestaat er een element $\sigma \in \mathrm{Gal}(K/F)$ zodat $\sigma(\alpha) = \beta$.

Uitwerking. 3 punten per vraag.

(a) **Onwaar**. Alleen als de fixgroep van E een normale ondergroep van $\mathrm{Gal}(K/F)$ is.
(b) **Waar**. Dit polynoom heeft geen wortels in $\mathbb{Q}$. Dit kun je expliciet checken door ± 1, ± 2 en ± 3 uit te proberen.
(c) **Waar**. Dit is een cyclotomische uitbreiding van graad $\varphi(6) = 2$.
(d) **Waar**. K is het spijtlichaam van een polynoom van de vorm $x^{p^n} - x$ over $\mathbb{F}_p$, dus Galois over elk van zijn deellichamen.
(e) **Waar**. Eisenstein bij 2 (en ook bij 5).
(f) **Onwaar**. In het algemeen werkt dit alleen als $f(x)$ irreducibel en separabel is.

Opgave 2. (12 punten)

(a) Bepaal een polynoom $f(x) \in \mathbb{F}_3[x]$ zodat $\mathbb{F}_3[x]/(f(x)) \cong \mathbb{F}_9$.
(b) Bepaal een polynoom $f(x) \in \mathbb{F}_2[x]$ zodat $\mathbb{F}_2[x]/(f(x)) \cong \mathbb{F}_{16}$.

Uitwerking. (a) (5 punten) Dit moet een irreducibel polynoom van graad 2 zijn. De monische opties zijn:

$$x^2 + 1, \quad x^2 + 2x + 2, \quad x^2 + x + 2.$$

Deze zijn irreducibel omdat ze geen wortel in $\mathbb{F}_3$ hebben.

(b) (7 punten) Dit moet een irreducibel polynoom van graad 4 zijn. De monische opties zijn:

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

Deze zijn allemaal te vinden door $x^{16} - x$ te factoriseren als het product van irreducibele polynomen van graden 1, 2 en 4 of door gewoon expliciet te checken dat deze polynomen geen wortels hebben in $\mathbb{F}_2$ (dus geen lineaire factor) en geen irreducibele factor van graad 2, namelijk $x^2 + x + 1$.

Opgave 3. (20 punten)

(a) Schrijf $f(x) = x^8 - 1 \in \mathbb{Q}[x]$ als een product van irreducibele polynomen.
(b) Bewijs dat de Galoisgroep van $f(x) = x^8 - 1$ isomorf is aan de Klein 4-groep V_4.
(c) Schrijf $K/\mathbb{Q}$ voor een splijtlichaam van $f(x)$. Bepaal alle deeluitbreidingen $\mathbb{Q} \subseteq E \subseteq K$.

Uitwerking. (a) (6 punten)

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x) = (x-1)(x+1)(x^2+1)(x^4+1).$$

De cyclotomische polynomen $\Phi_d(x)$ zijn irreducibel.

(b) (6 punten) Het splijtlichaam van $x^8 - 1$ is $\mathbb{Q}(\zeta_8)$ en een stelling uit het college zegt dat de Galoisgroep hiervan isomorf is aan $(\mathbb{Z}/8)^\times \cong V_4$. (Het isomorfisme volgt bijvoorbeeld door op te merken dat alle elementen van deze groep orde 2 hebben.) Alternatief: merk op dat $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$ door expliciet ζ_8 te bepalen. Dit is dus ook het splijtlichaam van het polynoom $(x^2-2)(x^2+1)$, waarvan makkelijk te zien is dat de Galoisgroep het product van de Galoisgroepen van de twee factoren is, dus $\mathbb{Z}/2 \times \mathbb{Z}/2 \cong V_4$.

(c) (8 punten) De voor de hand liggende zijn $\mathbb{Q}(\zeta_8)$, corresponderend met de triviale ondergroep, en $\mathbb{Q}$, corresponderend met de hele Galoisgroep. Dan zijn er nog drie ondergroepen van orde twee, corresponderend met de deeluitbreidingen $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, en $\mathbb{Q}(i\sqrt{2})$. Deze zijn te vinden door eerst de identificatie $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$ zoals hierboven te maken en als voortbrengers voor de Galoisgroep de elementen

$$\tau_1(\sqrt{2}) = -\sqrt{2},\ \tau_1(i) = i \qquad \text{en} \qquad \tau_2(\sqrt{2}) = \sqrt{2},\ \tau_2(i) = -i$$

te nemen. Alternatief in termen van $\mathbb{Q}(\zeta_8)$: de niet-triviale automorfismen σ_3, σ_5 en σ_7 worden bepaald door ζ_8 te sturen naar ζ_8^3, ζ_8^5, en ζ_8^7. Check nu:

$$\zeta_8 + \zeta_8^3 = i\sqrt{2}, \qquad \zeta_8 + \zeta_8^7 = \sqrt{2}.$$

Het eerste element brengt het fixlichaam voor $\langle\sigma_3\rangle$ voort, het tweede het fixlichaam voor $\langle\sigma_7\rangle$. Het element $\zeta_8 + \zeta_8^5$ is nul, dus daar heb je weinig aan, maar je kunt het overblijvende fixlichaam vinden door het product van de twee elementen hierboven te nemen (dus $2i$); dat is dan een element van het fixlichaam voor $\sigma_3\sigma_7 = \sigma_5$. Dit laatste fixlichaam is dus ook te beschrijven als $\mathbb{Q}(i)$.

Opgave 4. (20 punten)

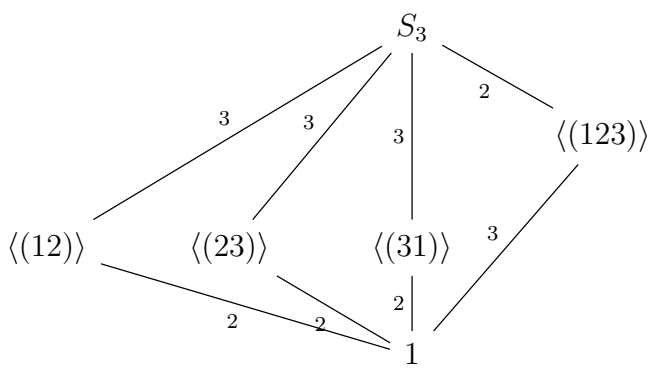
(a) Bepaal de Galoisafsluiting K van $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

(b) Beschrijf de Galoisgroep $\mathrm{Gal}(K/\mathbb{Q})$ en bepaal alle deeluitbreidingen $\mathbb{Q} \subseteq E \subseteq K$.

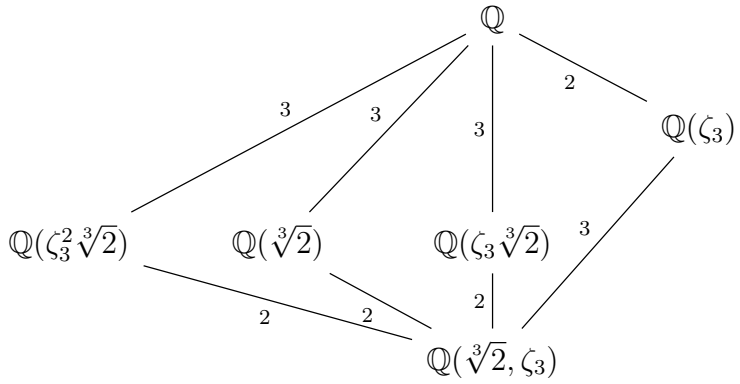
(c) Bewijs dat $\mathbb{Q}(\sqrt[3]{2})$ niet bevat is in een cyclotomische uitbreiding van $\mathbb{Q}$. Met andere woorden, bewijs dat er geen natuurlijk getal n bestaat zodat $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\zeta_n)$.

Uitwerking. (a) (6 punten) K bevat een wortel van het irreducibele polynoom $x^3 - 2$, dus moet ook het splijtlichaam van dit polynoom bevatten. Dit splijtlichaam is Galois over $\mathbb{Q}$, dus is precies de Galoisafsluiting van K. Expliciet is dit het lichaam $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, anders te schrijven als $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

(b) (8 punten) De Galoisgroep is (isomorf aan) een ondergroep van S_3, want $x^3 - 2$ heeft graad 3. Het lichaam $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is van graad 6 over $\mathbb{Q}$ (merk op dat ζ_3 graad 2 over $\mathbb{Q}(\sqrt[3]{2})$ heeft, bijvoorbeeld), dus de Galoisgroep is (isomorf aan) heel S_3. Het rooster van ondergroepen ziet er als volgt uit:



Als we de drie wortels labellen als $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$, en $\alpha_3 = \zeta_3^2\sqrt[3]{2}$, dan vinden we de bijbehorende fixlichamen als volgt:



De drie fixlichamen corresponderend met de wortels zijn eenvoudig te zien: bijvoorbeeld, de transpositie (12) houdt precies de wortel α_3 vast en de andere twee niet. Het fixlichaam horend bij (123) is dan op verschillende manieren te bepalen. Het makkelijkst is om direct op te merken dat $\mathbb{Q}(\zeta_3)$ een uitbreiding van $\mathbb{Q}$ is die bevat is in $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$, dus moet corresponderen met een ondergroep van index 2. De enige optie is $\langle(123)\rangle$. Een andere manier om te laten zien dat ζ_3 in het fixlichaam ligt is door op te merken dat (123) het element $\zeta_3 = \alpha_2/\alpha_1$ stuurt naar $\alpha_3/\alpha_2 = \zeta_3$. Daardoor is ζ_3 bevat in het fixlichaam. Aangezien dit fixlichaam graad 2 over $\mathbb{Q}$ heeft, brengt ζ_3 het hele lichaam voort.

(c) (6 punten) Cyclotomische uitbreidingen zijn abels, dus hetzelfde geldt voor elke deeluitbreiding van een cyclotomische uitbreiding. Stel dat $\mathbb{Q}(\sqrt[3]{2})$ bevat is in een cyclotomische uitbreiding. Dan geldt hetzelfde voor de Galoisafsluiting K. Maar de Galoisgroep $\mathrm{Gal}(K/\mathbb{Q})$ is niet abels, tegenspraak.

Opgave 5. (20 punten)

(a) Bepaal het cyclotomische polynoom $\Phi_{24}(x)$. (Hint: Je werk uit Opgave 3 kan hier van pas komen.)
(b) Bewijs dat $\mathbb{Q}(\zeta_{24})$ het compositum is van $\mathbb{Q}(\zeta_8)$ en $\mathbb{Q}(\zeta_3)$.
(c) Bewijs dat $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2},\sqrt{3},i)$.

Uitwerking. (a) (7 punten) Merk op dat alle delers van 24 ook delers van 12 zijn, behalve 8 en 24 zelf. Daarom geldt

$$x^{24}-1 = \prod_{d|24}\Phi_d(x) = (x^{12}-1)\Phi_8(x)\Phi_{24}(x).$$

Als in Opgave 3(a) zien we dat $\Phi_8(x) = x^4+1$. Daarom geldt

$$\Phi_{24}(x) = \frac{x^{24}-1}{(x^{12}-1)(x^4+1)} = \frac{x^{12}+1}{x^4+1} = x^8-x^4+1.$$

(b) (6 punten) Merk op dat ζ_{24}^3 een primitieve 8ste eenheidswortel is en ζ_{24}^8 een primitieve 3de eenheidswortel, dus zowel $\mathbb{Q}(\zeta_8)$ en $\mathbb{Q}(\zeta_3)$ zijn bevat in $\mathbb{Q}(\zeta_{24})$. Andersom is het product $\zeta_3\zeta_8$ een primitieve 24ste eenheidswortel (want 24 is het kleinste gemene veelvoud van 3 en 8), dus $\mathbb{Q}(\zeta_{24})$ is bevat in het compositum van de twee lichamen.

(c) (7 punten) Een primitieve 8ste eenheidswortel wordt gegeven door

$$\zeta_8 = \frac{1+i}{\sqrt{2}},$$

waaruit eenvoudig volgt dat $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$. (Merk bijvoorbeeld op dat $\zeta_8 + \zeta_8^7 = \sqrt{2}$, dus $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.) Een primitieve 3de eenheidswortel wordt gegeven door

$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2},$$

waaruit volgt dat $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$. Dit combineren geeft

$$\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\zeta_3, \zeta_8) = \mathbb{Q}(\sqrt{2}, i, i\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i).$$