Hertentamen
Lichamen & Galoistheorie

21 december 2021, 17u - 20u

- Schrijf je naam en studentnummer op elk vel dat je inlevert.
- Het is niet toegestaan het boek of je aantekening te gebruiken tijdens het tentamen.
- Schrijf leesbaar en licht je antwoorden toe (behalve bij Opgave 1).
- In totaal zijn er 90 punten te behalen. Bij elke opgave staat vermeld hoeveel punten deze waard is.
- Je mag resultaten uit een deelopgave altijd gebruiken in een volgende opgave, ook als je deze niet zelf bewezen hebt.

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) De reële getallen $\mathbb{R}$ vormen een algebraïsch gesloten lichaam.
(b) De groep S_3 is oplosbaar.
(c) Het polynoom $x^3 + 5x + 6$ is irreducibel over $\mathbb{Q}$.
(d) Zij F een lichaam, α algebraïsch over F, en $[F(\alpha) : F]$ oneven. Dan geldt $F(\alpha) = F(\alpha^2)$.
(e) Het splijtlichaam van $x^5 - 1$ heeft graad 5 over $\mathbb{Q}$.
(f) Zij $f(x)$ een irreducibel polynoom over een eindig lichaam $\mathbb{F}_{p^n}$. Dan is $f(x)$ separabel.

Uitwerking. 3 punten per vraag.

(a) **Onwaar**. Het polynoom $x^2 + 1$ heeft geen wortels in $\mathbb{R}$. (We hebben gezien dat $\mathbb{C}$ de algebraïsche afsluiting van $\mathbb{R}$ is.)
(b) **Waar**. Een oplossingsreeks is gegeven door $1 \leq \langle(123)\rangle \leq S^3$. De middelste groep is isomorf aan $\mathbb{Z}/3$, dus abels, en het quotiënt $S^3/\langle(123)\rangle$ is isomorf aan $\mathbb{Z}/2$, dus ook abels.
(c) **Onwaar**. -1 is een wortel van dit polynoom, dus het is deelbaar door $x + 1$.
(d) **Waar**. Merk op dat $F(\alpha^2) \subseteq F(\alpha)$ en de graad $[F(\alpha) : F(\alpha^2)]$ is 1 (als $\alpha \in F(\alpha^2)$) of 2 (als dat niet zo is). In het tweede geval geldt dat $[F(\alpha) : F] = 2[F(\alpha^2) : F]$, een tegenspraak.
(e) **Onwaar**. De graad van deze uitbreiding is $\varphi(5) = 4$.
(f) **Waar**. Eindige lichamen zijn perfect, zoals in college bewezen.

Opgave 2. (18 punten)

(a) Bewijs de volgende gelijkheid in de polynoomring $\mathbb{F}_{p^n}[x]$:

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a).$$

(b) Leidt af dat het product van alle $a \in \mathbb{F}_{p^n} - \{0\}$ gelijk is aan -1.
(c) Bewijs de stelling van Wilson, die zegt dat

$$(p-1)! \equiv -1 \pmod{p}.$$

Uitwerking. 6 punten per vraag.

(a) Zoals we hebben gezien geldt voor elke $a \in \mathbb{F}_{p^n}$ dat $a^{p^n} = a$. (Voor $a = 0$ is dit duidelijk en voor $a \neq 0$ gebruik je dat $\mathbb{F}_{p^n}^\times$ een groep van orde $p^n - 1$ is, dus $a^{p^n - 1} = 1$.) In het bijzonder is dus elke $a \in \mathbb{F}_{p^n}$ een wortel van $x^{p^n} - x$, dus het product aan de rechterkant deelt het polynoom aan de linkerkant. Maar beiden zijn monisch en hebben dezelfde graad p^n, dus ze zijn gelijk.

(b) Beide kanten van de eerste deelopgave delen door x geeft

$$x^{p^n-1} - 1 = \prod_{a \in \mathbb{F}_{p^n}^\times} (x - a).$$

Invullen van $x = 0$ geeft $-1 = (-1)^{p^n-1} \prod_{a \in \mathbb{F}_{p^n}^\times} a$. Als p oneven is, dan geldt $(-1)^{p^n-1} = 1$ en de conclusie volgt. Als $p = 2$ dan geldt $-1 = 1$, dus de conclusie volgt ook.

(c) Dit is het speciale geval $n = 1$. Modulo p geldt

$$(p-1)! = \prod_{a \in \mathbb{F}_p^\times} a = -1$$

vanwege de vorige deelopgave.

Opgave 3. (22 punten)

We bekijken de uitbreiding $K = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ van $\mathbb{Q}$ en het element $\alpha = \sqrt{5} + \sqrt{6}$.

(a) Wat is de Galoisgroep $G = \mathrm{Gal}(K/\mathbb{Q})$?

(b) Nummer de elementen van G als $\sigma_1, \ldots, \sigma_n$. Bepaal de som $\sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$ en het product $\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$.

(c) Vind het minimale polynoom van α.

(d) Bepaal alle deeluitbreidingen $\mathbb{Q} \subseteq E \subseteq K$.

Uitwerking. (a) (6 punten) $K/\mathbb{Q}$ is het compositum van de Galoisuitbreidingen $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ en $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$. Beide zijn van graad 2 en hebben dus Galoisgroep $\mathbb{Z}/2$. De groep G is een dus een ondergroep van het product $\mathbb{Z}/2 \times \mathbb{Z}/2 = V_4$. Maar G heeft orde 4 en dus geldt $G \cong V_4$.

(b) (5 punten) De elementen van G kunnen expliciet worden geschreven als $\sigma_1, \ldots, \sigma_4$ met σ_1 de identiteit en

$$\begin{aligned} \sigma_2(\sqrt{5}) &= -\sqrt{5} & \sigma_2(\sqrt{6}) &= \sqrt{6} \\ \sigma_3(\sqrt{5}) &= \sqrt{5} & \sigma_3(\sqrt{6}) &= -\sqrt{6} \\ \sigma_4(\sqrt{5}) &= -\sqrt{5} & \sigma_4(\sqrt{6}) &= -\sqrt{6}. \end{aligned}$$

Hieruit volgt $\sum_i \sigma_i(\alpha) = 0$ en

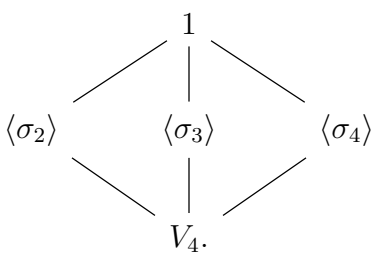
$$\prod_i \sigma_i(\alpha) = (\sqrt{5} + \sqrt{6})(\sqrt{5} - \sqrt{6})(-\sqrt{5} + \sqrt{6})(-\sqrt{5} - \sqrt{6}) = 1.$$

(c) (6 punten) Merk op dat α alleen wordt gefixeerd door $\sigma_1 \in G$, dus α brengt de hele uitbreiding $K/\mathbb{Q}$ voort, i.e., $K = \mathbb{Q}(\alpha)$. Het minimale polynoom van α moet dus graad 4 hebben. Merk nu op dat $\alpha^2 = 11 + 2\sqrt{30}$, dus $(\alpha^2 - 11)^2 = 120$. We krijgen dus

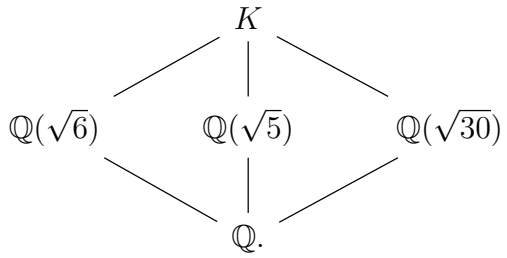
$$\alpha^4 - 22\alpha^2 + 1 = 0,$$

ofwel $x^4 - 22x^2 + 1$ is het minimale polynoom van α.

(d) (5 punten) Het rooster van ondergroepen van G ziet er als volgt uit:



Het corresponderende rooster van fixlichamen is:



Opgave 4. (32 punten)

We bekijken het polynoom $f(x) = x^6 - 2x^3 + 2$ over $\mathbb{Q}$ en schrijven K voor het splijtlichaam van $f(x)$.

(a) Schrijf $g(x) = x^2 - 2x + 2$. Laat zien dat K het splijtlichaam L van $g(x)$ bevat.
(b) Bepaal $[L : \mathbb{Q}]$.
(c) Bewijs dat $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$.
(d) Bewijs dat K ook het splijtlichaam is van het polynoom $h(x) = (x^2 + 1)(x^3 - 2)$.
(e) Wat is de Galoisgroep van $f(x)$?

Uitwerking. (a) (6 punten) Merk op dat $f(x) = g(x^3)$. Daarom zijn de wortels van $f(x)$ de derdemachtswortels van de wortels van $g(x)$. In het bijzonder, als α een wortel is van $g(x)$, dan is er een wortel β van $f(x)$ zodat $\alpha = \beta^3$. Omdat $\beta \in K$ moet dan ook gelden dat $\alpha \in K$.

(b) (5 punten) De wortels van $g(x)$ zijn $1 \pm i$, dus $L = \mathbb{Q}(i)$. Dit heeft duidelijk graad 2 over $\mathbb{Q}$.

(c) (7 punten) We schrijven $\zeta_8 = e^{\pi i/4}$ en $\zeta_{24} = e^{\pi i/12}$. Merk op dat $1 + i = \sqrt{2}\zeta_8$ en $1 - i = \sqrt{2}\zeta_8^{-1}$. De wortels van $f(x)$ zijn de derdemachtswortels hiervan. De derdemachtswortels van ζ_8 zijn ζ_{24}, ζ_{24}^9 en ζ_{24}^{17}, dus de wortels van $f(x)$ zijn gegeven door:

$$\sqrt[6]{2}\zeta_{24},\ \sqrt[6]{2}\zeta_{24}^9,\ \sqrt[6]{2}\zeta_{24}^{17},\ \sqrt[6]{2}\zeta_{24}^{-1},\ \sqrt[6]{2}\zeta_{24}^{-9},\ \sqrt[6]{2}\zeta_{24}^{-17}.$$

Daarom zijn ook de elementen

$$\sqrt[6]{2}\zeta_{24} \cdot \sqrt[6]{2}\zeta_{24}^{-1} = \sqrt[3]{2} \quad \text{en} \quad \frac{\sqrt[6]{2}\zeta_{24}}{\sqrt[6]{2}\zeta_{24}^{-1}} = \zeta_{24}^2 = \zeta_{12}$$

bevat in K. Merk op dat $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3, \zeta_4)$, want 3 en 4 zijn copriem. We kunnen nemen $\zeta_3 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ en $\zeta_4 = i$, dus $\mathbb{Q}(\zeta_3, \zeta_4) = \mathbb{Q}(\sqrt{3}, i)$. We concluderen dus dat

$$\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2}) \subseteq K.$$

Om de tegenovergestelde inclusie te krijgen bekijken we eerst de wortel $\sqrt[6]{2}\zeta_{24}$. Omdat 3 en 8 copriem zijn, geldt $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\zeta_3, \zeta_8)$, dus ook

$$\sqrt[6]{2}\zeta_{24} \in \mathbb{Q}(\zeta_3, \sqrt[6]{2}\zeta_8).$$

Er geldt dat $\sqrt[6]{2}\zeta_8 = \sqrt[6]{2} \cdot \frac{1+i}{\sqrt{2}} = \frac{1+i}{\sqrt[3]{2}}$, dus we vinden

$$\sqrt[6]{2}\zeta_{24} \in \mathbb{Q}(\zeta_3, i, \sqrt[3]{2}) = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2}).$$

Merk nu op dat de andere wortels van $f(x)$ te verkrijgen zijn uit $\sqrt[6]{2}\zeta_{24}$ door te vermenigvuldigen met machten van $\zeta_{24}^8 = \zeta_3$ en $\zeta_{24}^2 = \zeta_{12}$. Zoals al opgemerkt zijn zowel ζ_3 als ζ_{12} bevat in $\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$, dus volgt dat alle wortels van $f(x)$ (en dus ook het splijtlichaam K) bevat moeten zijn in dat lichaam.

(d) (7 punten) De wortels van $h(x)$ zijn $\pm i$ en $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$ en $\zeta_3^2\sqrt[3]{2}$. Deze zijn duidelijk bevat in het lichaam beschreven in de vorige deelopgave. Het splijtlichaam van $h(x)$ is dus bevat in K. Andersom bevat het splijtlichaam van $h(x)$ de elementen i en $\sqrt[3]{2}$, alsook het element ζ_3 (deel de wortel $\zeta_3\sqrt[3]{2}$ door de wortel $\sqrt[3]{2}$). Omdat $\zeta_3 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ bevat dit splijtlichaam dus ook $\sqrt{3}$.

(e) (7 punten) Vanwege de vorige deelopgave is de Galoisgroep van $f(x)$ dezelfde als die van $h(x)$, want deze polynomen hebben hetzelfde splijtlichaam. De elementen van de Galoisgroep worden volledig bepaald door hun actie op de wortels van $h(x)$. Daarbij moeten ze de wortels van de polynomen x^2+1 en x^3-2 permuteren (2 wortels in het eerste geval, 3 in het tweede). Op deze manier kunnen we de Galoisgroep G dus zien als ondergroep van het product van symmetrische groepen $S_2 \times S_3$. We zullen laten zien dat $G \cong S_2 \times S_3$ door te laten zien dat G 12 elementen bevat (en dus niet kleiner kan zijn dan $S_2 \times S_3$). Dit doen we door te bewijzen dat $[K:\mathbb{Q}] = 12$. Merk eerst op dat

$$[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2\cdot 2 = 4.$$

Hier hebben we gebruikt dat $[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})] = 2$, wat volgt uit het feit dat i geen element van $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ is en dus minimaal polynoom x^2+1 over dit lichaam heeft. Merk ook op dat het minimale polynoom van $\sqrt[3]{2}$ over $\mathbb{Q}$ gegeven is door x^3-2. Aangezien 3 geen deler is van 4 heeft dit polynoom geen wortels in $\mathbb{Q}(i,\sqrt{3})$, dus geldt

$$[\mathbb{Q}(i,\sqrt{3},\sqrt[3]{2}):\mathbb{Q}(i,\sqrt{3})] = 3.$$

Alles bij elkaar geeft dit

$$[K:\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{3},\sqrt[3]{2}):\mathbb{Q}(i,\sqrt{3})][\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}] = 3\cdot 4 = 12.$$