Antwoorden tentamen Galoistheorie
20 januari 2020, 8:30–11:30 uur

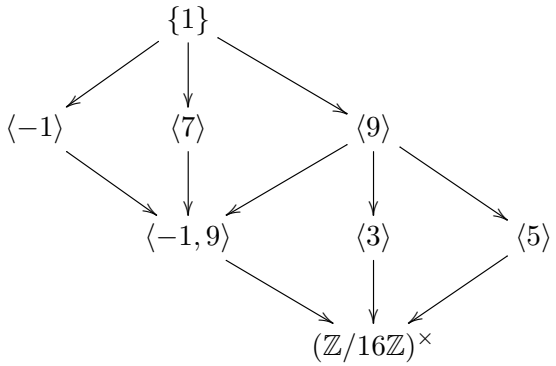
- Schrijf je naam op ieder blad dat je inlevert.
- Dit is een open boek tentamen, je mag de literatuur van het college gebruiken.
- Het gebruik van een (grafische) rekenmachine is toegestaan.
- Je mag bij een opgave de resultaten van eerdere deelopgaven gebruiken, ook als je die niet kon bewijzen.
- Na afloop mag je dit opgavenblad meenemen.
- Veel succes!

Opgave 1. (1 + 3 punten)

a. Laat zien dat $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \cong C_4 \times C_2$. Hier is C_n de cyclische groep met n elementen.

b. Bepaal alle tussenlichamen van de lichaamsuitbreiding $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$, en geef aan met welke ondergroepen van de Galoisgroep ze corresponderen.

Antwoord.
(a) Volgens Stelling 6.9 is $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ Galois met Galoisgroep $(\mathbb{Z}/16\mathbb{Z})^\times$. Dit is de verzameling oneven getallen in $\mathbb{Z}/16\mathbb{Z}$. Deze groep is abels en $\{1, 3, 9, 11\}$ is een ondergroep $\cong C_4$ en $\{1, 5\}$ is een ondergroep $\cong C_2$. Dus $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_4 \times C_2$.
(b) Het diagram van ondergroepen $(\mathbb{Z}/16\mathbb{Z})^\times$ is

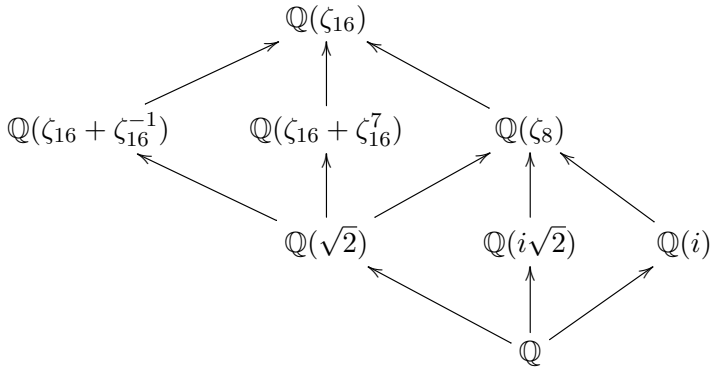


Het element $n \mod 16$ correspondeert met het lichaamsautomorfisme σ_n dat ζ_{16} naar ζ_{16}^n stuurt.

Het lichaam $\mathbb{Q}(\zeta_{16})$ bevat de elementen $\zeta_8 = (1+i)/\sqrt{2}$, $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, $i\sqrt{2} = \zeta_8 + \zeta_8^3$, $i = \zeta_4$. De laatste drie corresponderen met de kwadratische uitbreidingen van $\mathbb{Q}$ bevat in $\mathbb{Q}(\zeta_{16})$. Verder hebben we het tussenlichaam $L = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$. Er geldt

$$[\mathbb{Q}(\zeta_{16}) : L] = \deg(f_L^{\zeta_{16}}) = \deg(x^2 - (\zeta_{16} + \zeta_{16}^{-1})x + 1) = 2. \tag{1}$$

Net zo is er een tussenlichaam $K = \mathbb{Q}(\zeta_{16} + \zeta_{16}^7)$ met $[\mathbb{Q}(\zeta_{16}) : K] = 2$ omdat $f_K^{\zeta_{16}} = x^2 - (\zeta_{16} + \zeta_{16}^7)x - 1$. Hiermee kunnen we het rooster van tussenlichamen invullen:



Opgave 2. (2 punten)
Zij $n \in \mathbb{Z}_{>1}$. Laat zien dat $\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}$ een Galoisuitbreiding is en bepaal de Galoisgroep.

Antwoord.
Ten eerste merken we op dat $\cos(2\pi/n) = (\zeta_n + \zeta_n^{-1})/2$. Uit Stelling 6.9 weten we dat $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ Galois is met Galoisgroep $(\mathbb{Z}/n\mathbb{Z})^\times$. Deze is abels, dus elke ondergroep ervan is normaal. Met de hoofdstelling van de Galoistheorie volgt dat elk tussenlichaam Galois is over $\mathbb{Q}$, in het bijzonder $\mathbb{Q}(\cos(2\pi/n))$.

In (1) hebben we al gezien dat $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))] = 2$. Het lichaamsautomorfisme σ_{-1} gedefinieed door $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$ fixeert $\cos(2\pi/n)$, dus
$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\cos(2\pi/n))) = \{1, \sigma_{-1}\}$. Volgens Stelling 5.30 geldt

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\cos(2\pi/n))) \\ &\cong (\mathbb{Z}/n\mathbb{Z})^\times/\{1,-1\}.\end{aligned}$$

Opgave 3. (2 punten)
Zij L/K een eindige Galoisuitbreiding en zij M een tussenlichaam van L/K. Zij N de normale afsluiting van M in L. Laat zien dat

$$\mathrm{Gal}(L/N) = \bigcap_{\sigma \in \mathrm{Gal}(L/K)} \sigma \mathrm{Gal}(L/M)\sigma^{-1}.$$

Antwoord.
Per definitie is N het kleinste deellichaam van L dat M bevat en normaal is over K. Uit de hoofdstelling van de Galoistheorie volgt dat $\mathrm{Gal}(L/N)$ van $\mathrm{Gal}(L/M)$ is, die normaal is in $\mathrm{Gal}(L/K)$. Voor elke $\sigma \in \mathrm{Gal}(L/K)$ geldt

$$\begin{aligned}\mathrm{Gal}(L/N) &= \sigma \mathrm{Gal}(L/N)\sigma^{-1} \subset \sigma \mathrm{Gal}(L/M)\sigma^{-1}, \\ \mathrm{Gal}(L/N) &\subset \bigcap_{\sigma \in \mathrm{Gal}(L/M)} \sigma \mathrm{Gal}(L/M)\sigma^{-1}.\end{aligned}$$

De doorsnede is ook een ondergroep van $\mathrm{Gal}(L/M)$ die normaal is in $\mathrm{Gal}(L/K)$, dus het is $\mathrm{Gal}(L/N)$.

Opgave 4. (2 + 3 + 2 punten)

a. Zij K een lichaam en $K(\alpha)/K$ een enkelvoudige Galoisuitbreiding.
Bewijs dat het minimumpolynoom van α over K gegeven wordt door

$$\prod_{\sigma\in\mathrm{Gal}(K(\alpha)/K)} (X-\sigma(\alpha)) = f_K^\alpha.$$

b. Zij L/K een eindige Galoisuitbreiding en zij $\beta \in L$. Laat zien dat

$$\prod_{\sigma\in\mathrm{Gal}(L/K)} (X-\sigma(\beta)) = (f_K^\beta)^{[L:K(\beta)]}.$$

c. Zij E/K een eindige normale uitbreiding en zij $\gamma \in E$. Toon aan dat

$$\prod_{\sigma\in\mathrm{Aut}(E/K)} (X-\sigma(\gamma))^{[K(\gamma):K]} = (f_K^\gamma)^{|\mathrm{Aut}(E/K)|}.$$

Antwoord.
(a) Voor elke $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ is $\sigma(\alpha)$ een nulpunt van het minimumpolynoom f_K^α, want $\sigma(f_K^\alpha) = f_K^\alpha$. Bovendien zijn al deze nulpunten verschillend, want $\sigma(\alpha) = \tau(\alpha)$ impliceert $\sigma = \tau$ in $\mathrm{Gal}(K(\alpha)/K)$. Dus $\prod_{\sigma\in\mathrm{Gal}(K(\alpha)/K)} X - \sigma(\alpha)$ deelt f_K^α. Deze polynomen hebben dezelde graad:

$$|\mathrm{Gal}(K(\alpha)/K) = [K(\alpha):K] = \deg(f_K^\alpha).$$

Bovendien zijn ze allebei monisch, dus ze zijn gelijk.

(b) Omdat L/K normaal is ligt elk nulpunt β' van f_K^β in L. Vanwege Propositie 5.13.b kan $K(\beta) \to K(\beta') : \beta \mapsto \beta'$ voortgezet worden tot een automorfisme van L/K. Dus de verzameling $Z := \{\sigma(\beta) : \sigma \in \mathrm{Gal}(L/K)\}$ bestaat precies uit alle nulpunten van f_K^β. Er geldt

$$|\{\sigma \in \mathrm{Gal}(L/K) : \sigma(\beta) = \beta'\}| = |\mathrm{Gal}(L/K(\beta))| = [L:K(\beta)].$$

Dus $\prod_{\sigma\in\mathrm{Gal}(L/K)} X - \sigma(\beta)$ deelt $(f_K^\beta)^{[L:K(\beta)]}$. Beide polynomen zijn monisch en hebben graad

$$|\mathrm{Gal}(L/K)| = [L:K] = [L:K(\beta)][K(\beta):K] = [L:K(\beta)]\deg(f_K^\beta),$$

dus ze zijn gelijk.

(c) Hetzelfde argument als in deel (b) toont aan dat $Z := \{\sigma(\gamma) : \sigma \in \mathrm{Aut}(E/K)\}$ precies uit alle nulpunten van f_K^γ bestaat. De groep $\mathrm{Aut}(E/K)$ werkt transitief op Z, dus elke $\gamma' \in Z$ komt even vaak voor als $\sigma(\gamma)$. Aangezien f_K^γ invariant is onder $\mathrm{Aut}(E/K)$, komt elke $\gamma' \in Z$ ook even vaak voor als nulpunt van f_K^γ. Hieruit volgt dat er natuurlijke getallen $n, m \in \mathbb{N}$ bestaan zodat

$$\prod_{\sigma\in\mathrm{Aut}(E/K)} (X-\sigma(\gamma))^n = (f_K^\gamma)^m.$$

Aangezien $\deg(f_K^\gamma) = [K(\gamma):K]$, laat een vergelijking van de graden zien dat het geldt met $n = [K(\gamma):K]$ en $m = |\mathrm{Aut}(E/K)|$.

Opgave 5. (2 + 2 + 1 + 2 punten)
Zij p een priemgetal en $G \subset S_p$ een ondergroep die transitief werkt op $\{1, 2, \ldots, p\}$.

a. Toon aan dat G een ondergroep C van orde p bevat.

b. Stel dat C normaal in G is. Bewijs dat G/C is isomorf met een ondergroep van de automorfismengroep van C.

c. Neem nu aan dat $|G| \leq p(p-1)$. Uit de theorie van Sylow-ondergroepen is bekend dat C dan de enige ondergroep van G van orde p is.
Laat zien dat G/C een abelse groep is.

d. Zij K een lichaam van karakteristiek 0 en zij $f \in K[X]$ een irreducibel polynoom van graad p, dat splijt over een lichaam $L \supset K$ met $[L : K] < p^2$.
Bewijs dat f oplosbaar is over K.

Antwoord.
(a) Uit de banenformule weten we dat

$$|G| = |G\text{-baan van } 1| \cdot |\text{stabilisator van } 1 \text{ in } G|.$$

Omdat de G transitief werkt heeft de baan van 1 p elementen, dus p deelt $|G|$. De stelling van Cauchy zegt dat G een element van orde p bevat. De daardoor voortgebrachte ondergroep heeft p elementen.
(b) Per aanname G/C is een groep. Aangezien C abels is, geeft de natuurlijke afbeelding van G naar de inwendige automorfismen van G een groepshomomorfisme $\phi : G/C \to \mathrm{Aut}(C)$. De kern van ϕ is de centralisator van C in G, modulo C. Neem een voortbrenger c van C. Dan heeft c orde p in S_p, dus het is een p-cykel. De centralisator van een p-cykel in S_p is niet meer dan de ondergroep daardoor voortgebracht. Dus ook $C = Z_G(c) = Z_G(C)$. Dat betekent $\ker(\phi) = C/C$. Oftewel, ϕ is injectief en volgens de eerste isomorfiestelling is G/C isomorf met de ondergroep $\phi(C)$ van $\mathrm{Aut}(C)$.
(c) Omdat C de enige ondergroep van G is, is zij normaal in G. Volgens onderdeel (b) is G/C dan isomorf met een ondergroep van $\mathrm{Aut}(C)$. Maar $C \cong \mathbb{Z}/p\mathbb{Z}$, dus $\mathrm{Aut}(C) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Die groep is abels, dus G/C ook.
(d) $\mathrm{Gal}_K(f)$ werkt transitief op de nulpunten van f, omdat f irreducibel en separabel is. Volgens deel (a) is $|\mathrm{Gal}_K(f)|$ een p-voud. Per aanname $|\mathrm{Gal}_K(f)| \leq [L : K] < p^2$, dus $|\mathrm{Gal}_K(f)| \leq p(p-1)$. Deel (a) zegt ook dat $\mathbb{Z}/p\mathbb{Z} \cong C \subset \mathrm{Gal}_K(f)$. Volgens deel (b) is $\mathrm{Gal}_K(f)/C$ abels. Uit de rij $1 \triangleleft C \triangleleft \mathrm{Gal}_K(f)$ zien we dat $\mathrm{Gal}_K(f)$ oplosbaar is. De hoofdstelling over oplosbaarheid zegt nu dat f oplosbaar is over K.

Opgave 6. (2 + 2 + 3 punten)
Schrijf $\sqrt{\mathbb{Q}} = \{z \in \mathbb{C} : z^2 \in \mathbb{Q}\}$ en $L = \mathbb{Q}(\sqrt{\mathbb{Q}})$.

a. Laat zien dat $L/\mathbb{Q}$ een Galoisuitbreiding is.

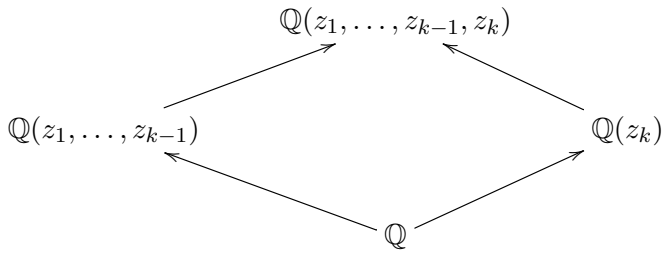
b. Zij $z_1, z_2, \ldots, z_k \in \sqrt{\mathbb{Q}}$ zodat $z_j \notin \mathbb{Q}(z_1, z_2, \ldots, z_{j-1})$ voor $1 \leq j \leq k$. Bewijs dat

$$\mathrm{Gal}(\mathbb{Q}(z_1, z_2, \ldots, z_k)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^k.$$

c. Bewijs dat $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

Antwoord.
(a) Voor $z_i \in \sqrt{Q}$ is $\mathbb{Q}(z_1, z_2, \ldots, z_k)$ het ontbindingslichaam van $\prod_{i=1}^{k}(x^2 - z_i^2)$ over $\mathbb{Q}$. Dus $\mathbb{Q}(z_1, z_2, \ldots, z_k)$ is normaal, separabel en algebräisch over $\mathbb{Q}$. Omdat voor een willekeurige nummering van $\sqrt{\mathbb{Q}}$ geldt $L = \cup_{k=1}^{\infty}\mathbb{Q}(z_1, z_2, \ldots, z_k)$. Dus $L/\mathbb{Q}$ is normaal, separabel en algebraïsch over $\mathbb{Q}$, wat betekent dat deze lichaamsuitbreiding Galois is.

(b) We bewijzen dit met inductie. Het geval $k = 0$ is triviaal. Bekijk het diagram van lichamen



Per aanname $\mathbb{Q}(z_1, \ldots, z_{k-1}, z_k) \cap \mathbb{Q}(z_k) = \mathbb{Q}$. Het is duidelijk dat $\mathrm{Gal}(\mathbb{Q}(z_k)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ en de inductiehypothese zegt dat $\mathrm{Gal}(\mathbb{Q}(z_1, \ldots, z_{k-1})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{k-1}$. Volgens Gevolg 5.55

$$\mathrm{Gal}(\mathbb{Q}(z_1, \ldots, z_{k-1}, z_k)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(z_1, \ldots, z_{k-1})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(z_k)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^k.$$

(c) Kies een rij $(z_i)_{i=1}^{\infty}$ in $\sqrt{\mathbb{Q}}$ met de eigenschap uit deel (b), zodat

$$L = \cup_{k=1}^{\infty}\mathbb{Q}(z_1, z_2, \ldots, z_k). \tag{2}$$

Definieer nu een groepshomomorfisme $\phi : \mathrm{Gal}(L/Q) \to \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ door $\phi(\tau)_i = 0$ als $\tau(z_i) = z_i$ en $\phi(\tau)_i = 1$ als $\tau(z_i) = -z_i$. Omdat $L = \mathbb{Q}(\{z_i : i \in \mathbb{N}\}$, is ϕ injectief. We willen inzien dat ϕ ook surjectief is.

Voor $i \leq k$ geeft deel (b) een lichaamsautomorfisme σ_i met $\sigma_i(z_i) = -z_i$ en $\sigma_i(z_j) = z_j$ voor $j \leq k, j \neq i$. Vanwege (2) breidt σ_i uit tot een element van $\mathrm{Gal}(L/\mathbb{Q})$. Bekijk nu $\sigma = \prod_{i=1}^{\infty}(\sigma_i)^{n_i}$ met $n_i \in \mathbb{Z}/2\mathbb{Z}$. De beperking van σ tot $\mathbb{Q}(z_1, \ldots, z_{k-1}, z_k)$ is een goed gedefinieerd lichaamsautomorfisme, namelijk $\prod_{i=1}^{k}(\sigma_i)^{n_i}$. Dus σ is een element van $\mathrm{Gal}(L/\mathbb{Q})$. Het is duidelijk dat $\phi(\sigma) = (n_i)_{i=1}^{\infty}$.

Dus ϕ is bijectief, oftewel het is een groepsisomorfisme.