Lichamen en Galoistheorie, 12 april 2021, 11:30 – 14:30

Schrijf op elk vel je naam en studentnummer.
Laat bij elke opgave zien hoe je aan je antwoord komt!
Ook als je een onderdeel niet kunt maken, kun je het gevraagde resultaat wel gebruiken voor de daaropvolgende onderdelen.
In totaal zijn er 90 punten te behalen.
Je mag alleen gebruik maken van eigen aantekeningen en van het boek of het pdf-bestand ervan. Als je voor het lezen van het pdf-bestand een computer of ander apparaat gebruikt, moet het geluid uitstaan en de wifi uitgeschakeld zijn. Het apparaat mag geen toegang hebben tot het internet. Alleen het pdf-bestand van het boek mag geopend zijn; je mag niet typen, alleen scrollen. De surveillanten mogen je scherm bekijken.
Veel succes!

1. (**30 pt**) In deze opgave staat ζ_k steeds voor een primitieve k-de machts eenheidswortel in $\mathbb{C}$ (dus ζ_k heeft orde k in $\mathbb{C}^\times$). Bewijs de volgende beweringen:

   (a) (**4 pt**) $\sqrt{2} \in \mathbb{Q}(\zeta_8)$;

   (b) (**4 pt**) $\sqrt{3} \in \mathbb{Q}(\zeta_{12})$;

   (c) (**4 pt**) $\sqrt{5} \in \mathbb{Q}(\zeta_5)$;

   (d) (**4 pt**) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\zeta_{24})$;

   (e) (**6 pt**) als n oneven is, dan $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$;

   (f) (**8 pt**) $\sqrt{3} \notin \mathbb{Q}(\zeta_n)$ als $1 \le n \le 11$. (Hint: het volstaat om te bewijzen dat $\sqrt{3}$ niet in het maximale reële deellichaam $\mathbb{R} \cap \mathbb{Q}(\zeta_n)$ zit als $1 \le n \le 11$.)

2. (**10 pt**) Laat $F = \mathbb{F}_q$ een eindig lichaam met q elementen zijn. Laat K een uitbreiding van F zijn met $[K : F] = k$ en laat L een uitbreiding van F zijn met $[L : F] = \ell$. Neem aan dat K en L bevat zijn in een uitbreiding M van F.

   Laat KL het compositum van K en L zijn. Bewijs dat

   $$[KL : F] = \mathrm{kgv}(k, \ell)$$

   (het kleinste gemene veelvoud (least common multiple)) en dat

   $$[(K \cap L) : F] = \mathrm{ggd}(k, \ell)$$

   (de grootste gemene deler (greatest common divisor)).

3. (**40 pt**) Laat $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}, i)$.

   (a) (**5 pt**) Bewijs: K is het splijtlichaam van $f(x) = (x^3 - 2)(x^4 - 3)$ over $\mathbb{Q}$.

   (b) (**5 pt**) Bewijs: $[K : \mathbb{Q}] = 24$.

   Noteer $\mathrm{Gal}(K/\mathbb{Q})$ met G en laat ρ een primitieve derdemachts eenheidswortel zijn.

   (c) (**5 pt**) Bewijs dat G elementen α, β en γ bevat met

   $$\begin{array}{lll} \alpha(\sqrt[3]{2}) = \rho\sqrt[3]{2}, & \beta(\sqrt[3]{2}) = \sqrt[3]{2}, & \gamma(\sqrt[3]{2}) = \sqrt[3]{2}, \\ \alpha(\sqrt[4]{3}) = \sqrt[4]{3}, & \beta(\sqrt[4]{3}) = i\sqrt[4]{3}, & \gamma(\sqrt[4]{3}) = \sqrt[4]{3}, \\ \alpha(i) = i, & \beta(i) = i, & \gamma(i) = -i. \end{array}$$

   Bewijs ook dat α, β en γ de groep G voortbrengen.

We 'nummeren' de wortels van $f(x)$ als volgt: $\pi_1 = \sqrt[3]{2}$, $\pi_2 = \rho\sqrt[3]{2}$, $\pi_3 = \rho^2\sqrt[3]{2}$, $\pi_4 = \sqrt[4]{3}$, $\pi_5 = i\sqrt[4]{3}$, $\pi_6 = -\sqrt[4]{3}$ en $\pi_7 = -i\sqrt[4]{3}$. Gebruik deze nummering om G als ondergroep van S_7 te zien.

(d) (**5 pt**) Bewijs dat dan $\alpha = (123)$, $\beta = (23)(4567)$ en $\gamma = (23)(57)$.

(e) (**5 pt**) Bewijs dat de discriminant van $f(x)$ een kwadraat is in $\mathbb{Q}$.

(f) (**5 pt**) Bewijs dat G een unieke normale ondergroep van orde 3 bevat. Wat is het bijbehorende tussenlichaam?

(g) (**5 pt**) Bewijs dat G een unieke normale ondergroep van orde 4 bevat. Wat is het bijbehorende tussenlichaam?

(h) (**5 pt**) Bepaal de tussenlichamen van $K/\mathbb{Q}$ die graad 2 over $\mathbb{Q}$ hebben en bepaal de bijbehorende ondergroepen van G.

4. (**10 pt**) Laat $f(x)$ een monisch irreducibel polynoom in $\mathbb{Z}[x]$ zijn.

(a) (**5 pt**) Leg uit waarom er oneindig veel priemgetallen p bestaan zó dat $f(x)$ modulo p volledig splitst in $\mathbb{F}_p[x]$ (d.w.z., een product is van eerstegraadspolynomen in $\mathbb{F}_p[x]$).

(b) (**5 pt**) Geef aan hoe dit tot een theoretische (maar niet noodzakelijk praktische) methode leidt om de **orde** van de Galoisgroep van $f(x)$ te **bepalen**.