De Galoisgroep van $X^6 - 2X^3 - 2$

In deze opgave gaan we de Galoisgroep Gal(f) van het polynoom $f = X^6 - 2X^3 - 2 \in \mathbb{Q}[X]$ bepalen. Je kan hiervoor de volgende stappen volgen, maar je mag natuurlijk ook je eigen strategie gebruiken (zolang correct en volledig).

1. Bewijs dat f irreducibel is.
2. Stel $\alpha = \sqrt[3]{1+\sqrt{3}}$, $\beta = \sqrt[3]{1-\sqrt{3}} \in \mathbb{R}$ zijn de reële wortels, en $\zeta_3 \in \mathbb{C}$ is een primitieve derde eenheidswortel. Bewijs dat $\Omega = \mathbb{Q}(\zeta_3, \alpha, \beta)$ een ontbindingslichaam is van f.
3. Bewijs dat Ω het lichaam $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ omvat.
4. Bewijs dat $\sqrt{3} \notin \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Definieer $K = \mathbb{Q}(\zeta_3, \sqrt{3}, \sqrt[3]{2})$. Laat zien dat de afbeelding $\mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\} \times S_3$, $\sigma \mapsto \left(\sigma(\sqrt{3})/\sqrt{3}, \sigma|_{\mathbb{Q}(\zeta_3, \sqrt[3]{2})}\right)$ een isomorfisme is. (Hier identificeren we de groep $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q})$ met S_3)

   Aanwijzing: Gebruik de lemma's uit de aantekeningen voor het polyoom $X^6 - 2X^3 + 2$.
5. Bewijs dat $K = \mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$, waarbij $\zeta_{12} \in \mathbb{C}$ een primitieve twaalfde eenheidswortel is.
6. Bewijs dat $[K : \mathbb{Q}] = 12$ en dat $\Omega = K(\alpha)$. Leid af dat de graad $[\Omega : \mathbb{Q}]$ gelijk is aan 12 of gelijk is aan 36.
7. Bewijs het volgende lemma.

   Lemma. Stel M is een lichaam van karakteristiek verschillend van 3 zó dat M een primitieve derde eenheidswortel bevat. Stel $a, b \in M$ zijn twee elementen die geen derde macht zijn, dus $\sqrt[3]{a}, \sqrt[3]{b} \in \overline{M}$ brengen M-uitbreidingen $M(\sqrt[3]{a}), M(\sqrt[3]{b}) \subset \overline{M}$ van graad 3 voor. Dan geldt

   $$M(\sqrt[3]{a}) = M(\sqrt[3]{b}) \iff \left(\sqrt[3]{a}\sqrt[3]{b} \in M \text{ of } (\sqrt[3]{a})^2\sqrt[3]{b} \in M\right),$$

   (merk op dat $M(\sqrt[3]{a}(\sqrt[3]{b})^2) = M((\sqrt[3]{a})^2\sqrt[3]{b})$, dus de voorwaarde is symmetrisch in a en b).
8. Neem M gelijk aan het lichaam $\mathbb{Q}(\zeta_3, \sqrt{3})$, en bewijs dat $[M : \mathbb{Q}] = 4$. Bewijs dat de elementen $\alpha, \alpha\beta, \alpha^2\beta, \beta \in \Omega$ elk graad deelbaar door 3 hebben over $\mathbb{Q}$, daardoor niet in M kunnen liggen en dus elk een M-uitbreiding van graad 3 voortbrengen.

   Aanwijzing: Voor het element $\alpha^2\beta$ is het handig om modulo 13 te redeneren. Bepaal een expliciet zesde graads polynoom $h \in \mathbb{Z}[X]$ dat nulpunt $\alpha^2\beta$ heeft. Gebruik dat modulo 13 het getal 3 een kwadraatwortel heeft (namelijk 4 en 9) om te laten zien dat het polynoom h modulo 13 splitst in 2 irreducibele factoren van graad 3. Leid hieruit af dat $h \in \mathbb{Z}[X]$ ofwel irreducibel is, ofwel splitst in twee irreducibele factoren van graad 3.
9. Combineer de vorige 2 onderdelen om te laten zien dat $M(\alpha) \neq M(\beta)$. Leid hieruit af dat 9 een deler is van de graad $[\Omega : \mathbb{Q}]$, en dat dus $[\Omega : \mathbb{Q}] = 36$.
10. Bewijs dat in de toren $\mathbb{Q} \to \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \to \Omega$ elke stap Galois is met groep S_3.

    Aanwijzing: Bewijs eerst dat de graden 6 zijn, en gebruik dan dat er slechts twee groepen van orde 6 zijn, waarvan 1 abels, en de ander niet.
11. Definieer $G = \mathrm{Gal}(\Omega/\mathbb{Q})$, $N = \mathrm{Gal}(\Omega/\mathbb{Q}(\zeta_3, \sqrt[3]{2}))$. Bewijs dat N een normaaldeler is van G, en dat G/N isomorf is met S_3.

12. Bewijs dat er een automorfisme $\sigma \in \mathrm{Aut}(\Omega) = G$ bestaat met $\sigma(\zeta_3) = \zeta_3^{-1}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\sigma(\alpha) = \alpha$ en $\sigma(\beta) = \beta$.

    Aanwijzing: Bewijs eerst dat de lichaamsuitbreiding $\mathbb{Q}(\sqrt{3}, \alpha, \beta) \subset \Omega$ Galois is van graad 2. Identificeer dan $\mathrm{Gal}(\Omega/\mathbb{Q}(\sqrt{3}, \alpha, \beta)) \cong \mathbb{Z}/2\mathbb{Z}$. Concludeer hiermee dat σ bestaat.

13. Bewijs dat er een automorfisme $\tau \in \mathrm{Aut}(\Omega) = G$ bestaat met $\tau(\zeta_3) = \zeta_3$, $\tau(\sqrt{3}) = \sqrt{3}$, $\tau(\alpha) = \zeta_3\alpha$ en $\tau(\beta) = \zeta_3\beta$.

    Aanwijzing: Bewijs dat de uitbreiding $\mathbb{Q}(\zeta_3, \sqrt{3}, \alpha + \beta) \subset \Omega$ graad 3 heeft, en dus Galoisgroep $\mathbb{Z}/3\mathbb{Z}$ heeft.

14. Laat $H \subset G$ de ondergroep zijn die wordt voortgebracht door σ en τ, dus $H = \langle \sigma, \tau \rangle$. Laat zien dat H precies 6 elementen heeft, en leid af dat de reductie afbeelding $H \to G/N = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$, $\sigma \mapsto \sigma N$ een isomorfisme is. Concludeer dat $H \cap N = \{1\}$.

15. Bewijs dat er een automorfisme $s \in \mathrm{Gal}(\Omega/\mathbb{Q}(\zeta_3, \sqrt[3]{2}))$ bestaat met $s(\sqrt{3}) = -\sqrt{3}$, $s(\zeta_3) = \zeta_3$, $s(\alpha) = \beta$, $s(\beta) = \alpha$. Bestudeer hiervoor de uitbreiding

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}, \alpha + \beta) \to \mathbb{Q}(\zeta_3, \sqrt[3]{2}, \alpha + \beta)(\alpha) = \Omega,$$

    en bewijs dat deze uitbreiding Galois is van graad 2. Bewijs dat er een automorfisme $t \in \mathrm{Gal}(\Omega/\mathbb{Q}(\zeta_3, \sqrt[3]{2}))$ bestaat met $t(\sqrt{3}) = \sqrt{3}$, $t(\zeta_3) = \zeta_3$, $t(\alpha) = \zeta_3\alpha$, $t(\beta) = \zeta_3^2\beta$. Laat zien dat t en s de groep $\mathrm{Gal}(\Omega/\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ voortbrengen.

16. Laat zien dat

$$\sigma s \sigma^{-1} = s, \quad \sigma t \sigma^{-1} = t^2, \quad \tau s \tau^{-1} = s, \quad \tau t \tau^{-1} = t \quad \in G,$$

    en beschrijf G als semi-direct product van S_3 met S_3, waarbij $g \in S_3$ werkt op $x \in S_3$ via de formule

$$g * x = u^{\text{teken}(g)} x u^{-\text{teken}(g)} \in S_3,$$

    met $u \in S_3$ een vaste 2-cykel.

Extra

1. Stel $f \in \mathbb{Q}[X]$ is een monisch polynoom van graad 2 zó dat $f(X^3)$ irreducibel is. Bepaal $\mathrm{Gal}(f(X^p))$.
2. Stel $f \in \mathbb{Q}[X]$ is een monisch polynoom van graad 2 en p is een priemgetal zó dat $f(X^p)$ irreducibel is. Bepaal $\mathrm{Gal}(f(X^p))$.
3. Stel $f \in \mathbb{Q}[X]$ is een monisch polynoom, en p is een priemgetal zó dat $f(X^p)$ irreducibel is. Kan je iets zeggen over de groep $\mathrm{Gal}(f(X^p))$ in termen van de groep $\mathrm{Gal}(f)$?