De Galoisgroep van het polynoom $f = X^6 - 2X^3 + 2 \in \mathbb{Q}[X]$.

We gaan eerst Ω_f bepalen. Door te schrijven $Y = X^3$, zien we met de abc-formule dat de nulpunten van f zijn $\zeta_3^j \cdot \sqrt[3]{1 \pm i}$ voor $j = 0, 1, 2$, waarbij ζ_3 een primitieve 3-de eenheidswortel is, en $\sqrt[3]{1 \pm i}$ een (willekeurige) derde-machts wortel van $1 \pm i$. In totaal hebben we inderdaad 6 nulpunten. We zien dat $\Omega_f = \mathbb{Q}(\zeta_3, \sqrt[3]{1+i}, \sqrt[3]{1-i})$. Merk op dat $i \in \Omega_f$, en dat $\zeta_{12} = \zeta_3 \cdot i$ een primitieve 12-de eenheidswortel is. Dus $\zeta_{12} \in \Omega_f$. We hebben dus $\mathbb{Q}(\zeta_{12}) \subset \Omega_f$. Het lichaam $\mathbb{Q}(\zeta_{12})$ is het compositum van $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ en $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Met het onderstaande lemma zien we dat $i \notin \mathbb{Q}(\sqrt{-3})$. Het polynoom $X^2 + 1$ is dus irreducibel over $\mathbb{Q}(\sqrt{-3})$, en dus heeft $\mathbb{Q}(i, \sqrt{-3})$ graad 2 over $\mathbb{Q}(\sqrt{-3})$. Wegens de torenwet heeft $\mathbb{Q}(\zeta_{12})$ graad 4 over $\mathbb{Q}$. Schrijf $\alpha = \sqrt[3]{1+i}$ en $\beta = \sqrt[3]{1-i}$. Er geldt $(\alpha\beta)^3 = (1+i)(1-i) = 2$. Omdat ook $\zeta_3 \in \Omega_f$, zien we dus dat $\sqrt[3]{2} \in \Omega_f$. Dus hebben we een inclusie van het compositum $\mathbb{Q}(\zeta_{12})\mathbb{Q}(\sqrt[3]{2}) \subset \Omega_f$. Het lichaam $\mathbb{Q}(\zeta_{12})$ heeft graad 4 over $\mathbb{Q}$, en het lichaam $\mathbb{Q}(\sqrt[3]{2})$ heeft graad 3 over $\mathbb{Q}$. Deze graden zijn copriem, en dus heeft het lichaam $\mathbb{Q}(\zeta_{12}, \sqrt[3]{2}) = \mathbb{Q}(\zeta_{12})\mathbb{Q}(\sqrt[3]{2})$ graad $12 = 4 \cdot 3$ over $\mathbb{Q}$.

Wat is de graad van de uitbreiding $L := \mathbb{Q}(\zeta_{12}, \sqrt[3]{2}) \subset \Omega_f$? Merk op dat $\alpha \cdot \beta \in L$, en dus geldt $\Omega_f = L(\alpha)$. Het element α is een nulpunt van het polynoom $X^3 - (1+i) \in L[X]$, en dus volgt: $f_L^\alpha \mid X^3 - (1+i)$. Is het polynoom $X^3 - (1+i)$ irreducibel over L? Het antwoord blijkt nee te zijn. Na behoorlijk wat peuteren vond ik het element $\gamma = \zeta_{12}^{-1} \cdot (\sqrt[3]{2})^{-1} \cdot (1+i) \in L$, waarbij ik de primitieve 12-eenheids wortel ζ_{12} neem met $\zeta_{12}^3 = i$. Merk op dat dan

$$\gamma^3 = (-i) \cdot \frac{1}{2} \cdot (1+i)^3 = (-i) \cdot \frac{1}{2} \cdot (1+i)^2(1+i) = (-i) \cdot \frac{1}{2} \cdot (2i) \cdot (1+i) = 1 + i,$$

want $(1+i)^2 = 2i$. Omdat α en γ beide nulpunt zijn van het polynoom $X^3 - (1+i)$, zien we dat ze een derde-eenheidswortel schelen. En dus volgt dat $\alpha \in L$. We zien dus dat $[\Omega_f : L] = 1$. (Het polynoom $X^3 - (1+i)$ was dus verre van irreducibel!).

Hoe kwam ik bij het magische element γ? Ik probeerde wat dingen. Een van de elementen die ik bekeek was $\alpha/\beta \in \Omega_f$. Dit geeft $(\alpha/\beta)^3 = \frac{1+i}{1-i} = \frac{(1+i)^2}{(1-i)(1+i)} = \frac{2i}{2}$. Dus α/β is een primitieve 12-de eenheidswortel! Dus je weet dan dat $\alpha\beta \in L$ en ook dat $\alpha/\beta \in L$. Het is niet moeilijk om dan te krijgen dat ook $\alpha^2, \beta^2 \in L$, en daarna dan ook dat $\alpha, \beta \in L$. Dit gaf mij de hint om het element γ te bekijken. De conclusie is dat $\Omega_f = \mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$ en dat Ω_f dus graad 12 heeft over $\mathbb{Q}$.

We gaan nu $\mathrm{Gal}(\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})/\mathbb{Q})$ bepalen. Een mogelijke manier is om het probleem te reduceren naar $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q})$, waarvan we weten dat de groep gelijk is aan S_3. We kunnen het lichaam $\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$ schrijven als compositum: $\mathbb{Q}(\zeta_{12}, \sqrt[3]{2}) = \mathbb{Q}(i)\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Als we laten zien dat $\mathbb{Q}(i) \cap \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}$, dan is wegens het tweede onderstaande lemma de afbeelding

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}), \quad \sigma \mapsto \sigma|_{\mathbb{Q}(i)} \times \sigma|_{\mathbb{Q}(\zeta_3, \sqrt[3]{2})}$$

een isomorfisme. En dus geldt $\mathrm{Gal}(f) = \mathrm{Gal}(\Omega_f/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times S_3$.

Rest te bewijzen dat $\mathbb{Q}(i) \cap \mathbb{Q}(\zeta_{12}, \sqrt[3]{2}) = \mathbb{Q}$. Merk op dat deze doorsnede een deellichaam is van $\mathbb{Q}(i)$, en dus gelijk is aan $\mathbb{Q}$ of gelijk aan $\mathbb{Q}(i)$. In het tweede geval (dat we willen uitsluiten) geldt $i \in \mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$. Stel dus voor een tegenspraak dat dit zo is. Dus $\mathbb{Q}(i)$ is een van de kwadratische deellichamen van $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Met behulp van Galoistheorie weten we dat er precies 1 zo'n deellichaam is (want S_3 heeft precies 1 ondergroep van index 2). Dus geldt $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i)$, ofwel $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{-1})$ en dus $\sqrt{3} \in \mathbb{Q}$ (zie lemma hieronder): en dat is een tegenspraak.

Lemma. Stel F is een lichaam van karaketeristiek verschillend van 2 en $\overline{F}$ is een algebraische afsluiting van F. Stel dat $a, b \in F$ twee elementen zijn met kwadratische wortels $\sqrt{a}, \sqrt{b} \in \overline{F}$ die niet in F liggen. Dan geldt $F(\sqrt{a}) = F(\sqrt{b}) \iff \sqrt{ab} \in F$.

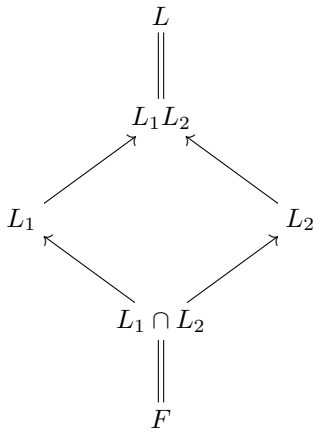
Bewijs. Als $\sqrt{ab} \in F$, dan geldt duidelijk $\sqrt{b} = \pm\sqrt{ab}/\sqrt{a} \in F(\sqrt{a})$ (en omgekeerd). Dit geeft de implicatie "$\Leftarrow$". Nu "$\Rightarrow$". Stel dat $F(\sqrt{a}) = F(\sqrt{b})$. De uitbreiding $F(\sqrt{a})/F$ heeft graad 2, en omdat de karakteristiek van F niet gelijk is aan 2, is de uitbreiding dus separabel. Separabele uitbreidingen van graad 2 zijn normaal, en dus is $F(\sqrt{a})/F$ Galois met groep $\mathbb{Z}/2\mathbb{Z}$, waarbij het niet triviale element $\sigma \in \text{Gal}(F(\sqrt{a})/F)$ werkt op $\sqrt{a}$ door $\sigma\sqrt{a} = -\sqrt{a}$. Omdat $\sqrt{b} \in F(\sqrt{a})$ en $\sqrt{b} \notin F$ is het element $\sqrt{b}$ niet invariant onder σ wegens Galoistheorie. Dus geldt $\sigma\sqrt{b} = -\sqrt{b}$. Uiteindelijk volgt dat $\sigma(\sqrt{a}\sqrt{b}) = \sigma(\sqrt{a}) \cdot \sigma(\sqrt{b})$ gelijk is aan $(-\sqrt{a})(-\sqrt{b}) = \sqrt{a}\sqrt{b}$ en dus $\sqrt{a}\sqrt{b} \in L^{\langle\sigma\rangle} = F$.

Lemma. Stel dat L/F een eindige Galoisuitbreiding is, en $L_1, L_2 \subset L$ zijn twee deellichamen met $L_1, L_2 \supset F$. Stel dat $L_1 \cap L_2 = F$ en dat $L_1 L_2 = L$. Dan is de afbeelding

$$\psi\colon \text{Gal}(L/F) \to \text{Gal}(L_1/F) \times \text{Gal}(L_2/F), \quad \sigma \mapsto \sigma|_{L_1} \times \sigma|_{L_2},$$

een isomorfisme.

Bewijs. We hebben het rooster van tussenlichamen



We weten dat alle pijlen in dit rooster Galoisuitbreidingen zijn. Bekijk de afbeelding

$$\varphi\colon \text{Gal}(L_1L_2/L_2) \to \text{Gal}(L_1/L_1 \cap L_2), \quad \sigma \mapsto \sigma|_{L_1}$$

We gaan eerst bewijzen dat deze afbeelding φ een isomorfisme is. Injectief: De kern van de afbeelding φ bestaat uit alle $\sigma \in \text{Gal}(L_1L_2/L_2)$ die de identiteit op L_1 zijn. Maar als σ de identiteit is op zowel L_1 als L_2, dan is hij ook de identiteit op het compositum. En dus $\sigma = 1 \in \text{Gal}(L_1L_2/L_2)$. Ofwel: De afbeelding is injectief. Surjectief: Stel $H \subset \text{Gal}(L_1/L_1 \cap L_2)$ is het beeld van de afbeelding φ. Zij α een element van het invariantenlichaam $(L_1)^H$. Dan geldt voor alle $\sigma \in H$ dat $\sigma(\alpha) = \alpha$. Er geldt dan ook voor alle $\sigma \in \text{Gal}(L_1L_2/L_2)$ dat $\sigma(\alpha) = \alpha$ (want H is het beeld van $\text{Gal}(L_1L_2/L_2)$ in $\text{Gal}(L_1/L_1 \cap L_2)$). Dus $\alpha \in L_2$. Dus α ligt zowel in L_1 als in L_2. Dus $\alpha \in L_1 \cap L_2 = F$. Dus volgt $(L_1)^H = L_1 \cap L_2$. Wegens Galoistheorie voor de uitbreiding L_1/F volgt dus dat H gelijk is aan de groep $\text{Gal}(L_1/F)$. Ofwel φ is surjectief. Dus φ is inderdaad een isomorfisme.

We gaan nu bewijzen dat de afbeelding ψ uit het lemma surjectief is. Kies $\sigma \in \text{Gal}(L_1/F)$ willekeurig. We laten zien dat het element $(\sigma, 1) \in \text{Gal}(L_1/F) \times \text{Gal}(L_2/F)$ in het beeld van ψ ligt. Omdat $\varphi\colon \text{Gal}(L/L_2) \to \text{Gal}(L_1/F)$ een isomorfisme is, kunnen we een element $\tau \in \text{Gal}(L/L_2)$ vinden met $\varphi(\tau) = \sigma$. Merk op dat τ de identiteit is op L_2. Dus beeldt τ af op $(\sigma, 1)$ onder ψ. Dus ligt $(\sigma, 1)$ inderdaad in het beeld. Merk op dat alles wat we gedaan hebben volledig symmetrisch is in L_1 en L_2. Door de rollen om te draaien zien we dat ook elk element van de vorm $(1, \sigma) \in \text{Gal}(L_1/F) \times \text{Gal}(L_2/F)$ geraakt wordt

door de afbeelding ψ. Omdat we elk element $(\sigma_1, \sigma_2) \in \text{Gal}(L_1/F) \times \text{Gal}(L_2/F)$ kunnen schrijven als een product $(\sigma_1, \sigma_2) = (\sigma_1, 1) \cdot (1, \sigma_2)$ zien we dat ψ surjectief is. Voor elk compositum weten we dat $[L_1 L_2 : K] \leq [L_1 : K][L_2 : K]$. Omdat ψ surjectief is volgt dat omgekeerd

$$[L : F] = \#\text{Gal}(L/F) \geq \#\text{Gal}(L_1/F) \times \#\text{Gal}(L_2/F) = [L_1 : F] \cdot [L_2 : F]$$

Dus moet gelden $[L : K] = [L_1 : K][L_2 : K]$ en dus is ψ een surjectie tussen twee verzamelingen met hetzelfde aantal elementen. Dus ψ is bijectief, en daarom een isomorfisme.