Faculty of Science

Radboud University Nijmegen

2019-2020

Ontnestbare geneste wortels

Jelmer Hinssen

Begeleider: Sep Thijssen

14 oktober 2020

Radboud University

Samenvatting

In deze scriptie wordt de ontnestbaarheid van geneste wortels bestudeerd. Een geneste wortel is een wortel van een element van $\mathbb{Q}^{(1)}$. Hierbij is $\mathbb{Q}^{(1)}$ het lichaam dat ontstaat door aan $\mathbb{Q}$ alle wortels toe te voegen:

$$\mathbb{Q}^{(1)} := \mathbb{Q}(\{a \in \overline{\mathbb{Q}} \mid \exists n \in \mathbb{Z}_{>0} : a^n \in \mathbb{Q}\}),$$

waarbij $\overline{\mathbb{Q}}$ staat voor de algebraïsche afsluiting van $\mathbb{Q}$. In sommige gevallen is een geneste wortel zelf een element van $\mathbb{Q}^{(1)}$. In dat geval noemen we het ontnestbaar. Voor elementen van de vorm $\sqrt[q]{\beta}$ met
$\beta \in \mathbb{Q}(\sqrt[p]{\alpha})$, waarbij p een oneven priemgetal, q een priemgetal ongelijk aan p en $\alpha \in \mathbb{Q}$ geen p^{e} macht, wordt bekeken wanneer $\sqrt[q]{\beta}$ ontnestbaar is en het blijkt dat dit alleen op een flauwe manier kan, namelijk doordat $\beta = c\gamma^q$, met $c \in \mathbb{Q}$ en $\gamma \in \mathbb{Q}(\sqrt[p]{\alpha})$.

Inhoudsopgave

1 Introductie

Een van de eerste die geneste wortels bestudeerde was Ramanujan. Hij publiceerde de opgave om de derdemachts wortel van elementen van de vorm $A + \sqrt[3]{B}$ te vinden en vierkantswortels van elementen van de vorm $\sqrt[3]{A} + \sqrt[3]{B}$ te vinden. [2]

[4] bestudeert de tweede van deze problemen en geeft een voldoende en noodzakelijke conditie voor A en B, die aangeeft wanneer $\sqrt{\sqrt[3]{A} + \sqrt[3]{B}}$ ontnestbaar is.

Het ontnesten van $\sqrt{\sqrt[3]{A} + \sqrt[3]{B}}$ is equivalent met het ontnesten van $\sqrt{1 + \sqrt[3]{\frac{B}{A}}}$. Dit is dus een speciaal geval van een wortel van de vorm $\sqrt{\beta}$ met $\beta \in \mathbb{Q}(\sqrt[3]{\alpha})$. Over deze algemene wortels bewijst [4] dat ze altijd op een flauwe manier te ontnesten zijn: het zijn namelijk op een rationaal getal na kwadraten.

Er is nog meer naar andere versies van dit soort wortels gekeken, waarbij telkens een vergelijkbaar resultaat wordt gegeven dat het op een flauwe manier ontnestbaar is. Ten eerste in [1] voor wortels van de vorm $\sqrt[3]{\beta}$ met $\beta \in \mathbb{Q}(\sqrt[3]{\alpha})$.

In plaats van naar een hogere machts wortel van β te kijken, kijkt [7] naar hogeremachts wortels van α: $\sqrt{\beta}$ met $\beta \in \mathbb{Q}(\sqrt[p]{\alpha})$, waarbij p een willekeurig oneven priemgetal is.

Deze studies kijken allemaal alleen naar enkelvoudig geneste wortels en laten alleen zien waar β aan moet voldoen om ontnestbaar te zijn, maar geven geen expliciete manier om de ontnesting ook daadwerkelijk te berekenen. [5] geeft een algoritme om geneste wortels van willekeurige diepte te ontnesten. Dit algoritme vereist wel dat het grondlichaam alle eenheidswortels bevat. Voor dit algoritme moet een ontbindingslichaam berekend worden, waardoor het niet efficiënt is: de complexiteit is exponentieel. [3] geeft een veel efficiënter algoritme dat geen gebruik maakt van Galoistheorie, waardoor het in lineaire tijd kan.

In deze scriptie gaan we het resultaat van [7] generaliseren naar hogeremachtswortels van β: $\sqrt[q]{\beta}$ met q een priemgetal ongelijk aan p en $\beta \in \mathbb{Q}(\sqrt[p]{\alpha})$.

De opbouw van de rest van deze scriptie is als volgt. In hoofdstuk 2 worden enkele bekende definities en stellingen uit de Galoistheorie herhaald, die later gebruikt worden. In hoofdstuk 3 wordt een alternatief bewijs gegeven voor het resultaat van [7]. In hoofdstuk 4 wordt een generalisatie hiervan naar $\sqrt[q]{\beta}$ gegeven. Tot slot wordt in hoofdstuk 5 nog gekeken naar het geval $p = q = 2$.

2 Voorkennis

In deze scriptie wordt Galoistheorie gebruikt. Hier volgen enkele algemene definities en stellingen uit de Galoistheorie gegeven, die in het vervolg van deze scriptie gebruikt worden.

Definitie 2.1. Een eindige lichaamsuitbreiding $K \subseteq L$ heet normaal als voor elke $\alpha \in L$ het minimumpolynoom f_K^α volledig splitst in $L[X]$.

Propositie 2.2. *Een eindige lichaamsuitbreiding $K \subseteq L$ is normaal dan en slechts dan als L het ontbindingslichaam is van een $f \in K[X]$.*

Bewijs. Stelling 23.14 van [6]. □

Definitie 2.3. Zij $\mathbb{Q} \subseteq K$ een lichaam, dan is de normale afsluiting van K over $\mathbb{Q}$ het kleinste lichaam L, zodat $K \subseteq L$ en $\mathbb{Q} \subseteq L$ een normale uitbreiding. Notatie: $L = K^{\text{norm}}$. De normale afsluiting bestaat altijd en is op isomorfie na uniek [6, p. 38].

Definitie 2.4. Een lichaamsuitbreiding $K \subseteq L$ heet separabel als voor elke $\alpha \in L$ het minimumpolynoom f_K^α in het ontbindingslichaam van f_K^α over K geen dubbele nulpunten heeft.

Propositie 2.5. *Als $\mathbb{Q} \subseteq K$, dan is $K \subseteq L$ een separabele uitbreiding.*

Bewijs. Lemma 23.6 van [6]. □

Definitie 2.6. Een lichaamsuitbreiding $L \supseteq K$ heet Galois als het een separabele en normale uitbreiding is.

Definitie 2.7. Zij $K \subseteq L$ een Galoisuitbreiding. De Galoisgroep van L over K: $\text{Gal}(L/K)$ is de groep

$$\{\sigma \in \text{Aut}(L) \mid \forall \alpha \in K : \sigma(\alpha) = \alpha\}.$$

Propositie 2.8. *Zij $K \subseteq L$ een Galoisuitbreiding, dan is*

$$|\,\text{Gal}(L/K)| = [L : K].$$

Bewijs. Stelling 24.1 van [6]. □

Verder hebben we ook nog wat specifiekere stellingen over commutatorgroepen en cyclotomische uitbreidingingen nodig.

Definitie 2.9. Zij G een groep. Dan is G' de groep voortgebracht door de commutatoren van G. D.w.z $G' = \langle\{[g,h] \mid g,h \in G\}\rangle$, waarbij $[g,h] = ghg^{-1}h^{-1}$.

Definitie 2.10. Een primitieve eenheidswortel van graad n is een element ζ_n zodat n het kleinste positieve gehele getal is waarvoor $\zeta_n^n = 1$.

$\mathbb{Q}(\zeta_m)$ is een Galoisuitbreiding over $\mathbb{Q}$, want het is het ontbindingslichaam van $X^m - 1$.

Propositie 2.11. *Zij ζ_n een primitieve n^{de} eenheidswortel dan*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Bewijs. Stelling 24.15 van [6]. □

Definitie 2.12. Zij $\mathbb{Q} \subseteq K$ een lichaam en $\alpha \in K$. De Galois-geconjugeerden, of gewoon geconjugeerden, van α zijn alle nulpunten van het minimumpolynoom $f_{\mathbb{Q}}^{\alpha}$.

Definitie 2.13. Zij $\mathbb{Q} \subseteq K$ een eindige lichaamsuitbreding en $\alpha \in K$. De norm van α is gedefinieerd door

$$N_{K/\mathbb{Q}}(\alpha) = \left(\prod_{\beta \text{ geconjugeerde van } \alpha} \alpha \right)^{[K:\mathbb{Q}(\alpha)]}.$$

Dit is altijd een element van $\mathbb{Q}$ en de afbeelding $N_{K/\mathbb{Q}} : K^* \to \mathbb{Q}^*$ is een groepshomomorfisme. [6, p. 40]

Propositie 2.14. *Laat $K \subseteq L \subseteq M$ lichamen zijn, met M/K en M/L Galois. Als* $\mathrm{Gal}(M/L)$ *en* $\mathrm{Gal}(L/K)$ *abels zijn, dan is* $\mathrm{Gal}(M/K)'' = \{\mathrm{id}\}$.

Bewijs. Stel $\sigma, \tau \in \mathrm{Gal}(M/K)$ dan $\sigma|_L, \tau|_L \in \mathrm{Gal}(L/K)$ en dus

$$[\sigma, \tau]|_L \in \mathrm{Gal}(L/K)' = \{\mathrm{id}\}.$$

Dit betekent dat $[\sigma, \tau] \in \mathrm{Gal}(M/L)$ en dus $\mathrm{Gal}(M/K)' \subseteq \mathrm{Gal}(M/L)$. Aan beide kanten de commutatorgroep nemen bewijst nu de propositie:

$$\mathrm{Gal}(M/K)'' \subseteq \mathrm{Gal}(M/L)' = \{\mathrm{id}\}.$$ □

Lemma 2.15. *Zij K een lichaam, S_1, S_2 verzamelingen, L een lichaam dat $K(S_1)$ en $K(S_2)$ bevat en $K \subseteq M$ een lichaam. Als $\tau : L \to M$ een lichaamshomomorfisme is zodat $\tau(K) \subseteq K$. Dan $K(S_1) = K(S_2) \implies K(\tau(S_1)) = K(\tau(S_2))$.*

Bewijs. Zij $y \in S_2$ dan zijn er $a_i \in K$ zodat $y = \sum a_i x_i$ met x_i het product van eindig veel elementen van S_1. Dan $\tau(y) = \sum \tau(a_i)\tau(x_i) \in K(\tau(S_1))$. Dus $S_2 \subseteq K(S_1) \implies K(S_2) \subseteq K(S_1)$. Analoog geldt $K(S_1) \subseteq K(S_2)$. □

Propositie 2.16. *Zij p een oneven priemgetal en K een lichaam van karakteristiek 0 met $\zeta_p \notin K$. Dan is er een uniek tussenlichaam $K \subseteq L \subseteq K(\zeta_p)$ zodat $[L : K] = 2$. Dit lichaam is $L = K\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.*

Bewijs. Pagina 17 van [8]. □

Propositie 2.17. *Zij K een lichaam en $\alpha \in K$. Dan is elke $\beta \in K(\sqrt{\alpha})$ te schrijven als $\beta = \sqrt{\alpha^n} x$, waarbij $n \in \mathbb{Z}$ en $x \in K$.*

Bewijs. Corollary 18 van [4]. □

3 Geneste vierkantswortels

Een geneste wortel is een wortel van een element van $\mathbb{Q}^{(1)}$. Hierbij is $\mathbb{Q}^{(1)}$ het lichaam dat ontstaat door aan $\mathbb{Q}$ alle wortels toe te voegen:

$$\mathbb{Q}^{(1)} := \mathbb{Q}(\{a \in \overline{\mathbb{Q}} \mid \exists n \in \mathbb{Z}_{>0} : a^n \in \mathbb{Q}\}), \quad [4]$$

waarbij $\overline{\mathbb{Q}}$ staat voor de algebraïsche afsluiting van $\mathbb{Q}$. In dit hoofdstuk kijken we alleen naar vierkantswortels van elementen van $\mathbb{Q}^{(1)}$. In het bijzonder kijken we naar $\sqrt{\beta}$, met $\beta \in \mathbb{Q}(\sqrt[p]{\alpha})$, waarbij p een oneven priemgetal is en $\alpha \in \mathbb{Q}$ geen p^{de} macht in $\mathbb{Q}$. In sommige gevallen is een geneste wortel zelf een element van $\mathbb{Q}^{(1)}$. In dat geval noemen we het ontnestbaar. We willen weten wanneer dit gebeurt. Een voorbeeld hiervan is

$$\sqrt{2\sqrt[5]{6^2} - \sqrt[5]{6} + 4} = \frac{\sqrt[5]{6^3} + 2\sqrt[5]{6^2} - 2\sqrt[5]{6} + 4}{\sqrt{10}}.$$

Dat deze gelijkheid inderdaad geldt, is eenvoudig na te gaan door aan beide kanten een kwadraat te nemen.

In het vervolg van deze scriptie gebruiken we de volgende notaties:

- p is een oneven priemgetal,
- $\alpha \in \mathbb{Q}$ is geen p^{de} macht,
- $\beta \in \mathbb{Q}(\sqrt[p]{\alpha}) \backslash \mathbb{Q}$,
- $N(x) = N_{\mathbb{Q}(\sqrt[p]{\alpha})/\mathbb{Q}}(x)$ voor $x \in \mathbb{Q}(\sqrt[p]{\alpha})$.

We kunnen op een flauwe manier geneste wortels construeren die sowieso ontnestbaar zijn. Namelijk, als we β een kwadraat in $\mathbb{Q}(\sqrt[p]{\alpha})$ nemen, d.w.z. $\beta = \gamma^2$ met $\gamma \in \mathbb{Q}(\sqrt[p]{\alpha})$, dan is $\sqrt{\beta} = \gamma$ duidelijk ontnestbaar. Ook als je $\beta = c\gamma^2$ met $c \in \mathbb{Q}$ geen kwadraat neemt is $\sqrt{\beta} = \sqrt{c}\gamma$ ontnestbaar.

In dit hoofdstuk zullen we zien dat alle $\sqrt{\beta}$ die ontnestbaar zijn van deze vorm zijn. Dit resultaat komt uit [7] en wij zullen globaal dezelfde aanpak gebruiken, maar de details zijn anders. Voor deze aanpak gaan we de Galoisgroep van de normale afsluiting van $\mathbb{Q}(\sqrt{\beta})$ bekijken.

3.1 De groep W_p

We willen de Galoisgroep van $\mathbb{Q}(\sqrt{\beta})^{\text{norm}}$ bekijken om een ontnestbaarheidsconditie te vinden. Om deze groep beter te begrijpen, kijken we eerst naar de Galoisgroep van $\mathbb{Q}(\beta)^{\text{norm}}$. Het zal blijken dat deze dezelfde structuur heeft als de affiene transformaties in $\mathbb{F}_p$. Daarom geven we eerst de definitie en enkele eigenschappen van deze groep.

Definitie 3.1. Voor een priemgetal p is W_p de groep van affiene transformaties van $\mathbb{F}_p$. Dat wil zeggen, W_p is de groep bestaande uit automorfismen van $\mathbb{F}_p$ van de vorm

$$\tau_{a,b} \colon x \mapsto ax + b,$$

met $a, b \in \mathbb{Z}$ en $p \nmid a$. Omdat dit modulo p is, geldt $\forall n, m \in \mathbb{Z}\ \tau_{a+np,b+mp} = \tau_{a,b}$, daarom kunnen rekenen met de indices alsof $a \in \mathbb{F}_p^*$ en $b \in \mathbb{F}_p$.

Propositie 3.2. *Voor een oneven priemgetal p geldt $W_p' = \langle \tau_{1,1} \rangle \cong C_p$.*

Bewijs. Aangezien $a(cx+d)+b = acx + ad + b$, is

$$\tau_{a,b}\tau_{c,d} = \tau_{ac,ad+b}.$$

Dit betekent dat $\tau_{a,b}^{-1} = \tau_{a^{-1},-a^{-1}b}$ en dus

$$\begin{aligned}
[\tau_{a,b}, \tau_{c,d}] &= \tau_{a,b}\tau_{c,d}\tau_{a,b}^{-1}\tau_{c,d}^{-1} \\
&= \tau_{a,b}\tau_{c,d}\tau_{a^{-1},-a^{-1}b}\tau_{c^{-1},-c^{-1}d} \\
&= \tau_{a,b}\tau_{c,d}\tau_{a^{-1}c^{-1},-a^{-1}c^{-1}d-a^{-1}b} \\
&= \tau_{a,b}\tau_{a^{-1},-a^{-1}d-ca^{-1}b+d} \\
&= \tau_{1,-d-cb+ad+b}.
\end{aligned}$$

Alle commutatoren van W_p zijn dus van de vorm $\tau_{1,x}$. De machten van $\tau_{1,1}$ zijn precies alle $\tau_{1,x}$, daarom bevat $\langle \tau_{1,1} \rangle$ alle commutatoren en dus $W_p' \subseteq \langle \tau_{1,1} \rangle$.

Omdat $p > 2$ zit 2 in $\mathbb{F}_p^*$ en kunnen we $a = 1,\ b = 2,\ c = 1 - 2^{-1}$ en $d = 0$ nemen. Hiermee krijgen we $\tau_{1,1} \in W_p'$ en dus $\langle \tau_{1,1} \rangle \subseteq W_p'$. □

Propositie 3.3. *Zij p een oneven priemgetal en M een lichaam van karakteristiek 0 en met $\zeta_p \notin M$ en $\alpha \in M$ geen p^{de} macht. Dan is*

$$\mathrm{Gal}(M(\zeta_p, \sqrt[p]{\alpha})/M) \cong W_p.$$

Bewijs. Zij $\sigma \in \mathrm{Gal}(M(\zeta_p, \sqrt[p]{\alpha})/M)$ dan wordt σ volledig bepaald door $\sigma(\zeta_p)$ en $\sigma(\sqrt[p]{\alpha})$; er zijn unieke a, b zodat

$$\begin{aligned}
\sigma(\zeta_p) &= \zeta_p^a && \text{met } a \in \{1, ..., p-1\}, \\
\sigma(\sqrt[p]{\alpha}) &= \zeta_p^b \sqrt[p]{\alpha} && \text{met } b \in \{0, ..., p-1\}.
\end{aligned}$$

We noteren deze afbeelding met $\sigma_{a,b}$ en we rekenen met de indices alsof $a \in \mathbb{F}_p^*$ en $b \in \mathbb{F}_p$. Dit is goed gedefinieerd omdat $\forall n, m \in \mathbb{Z} : \zeta_p^n = \zeta_p^{n+mp}$.

Definieer

$$\begin{aligned}\phi\colon \mathrm{Gal}(M(\zeta_p, \sqrt[p]{\alpha})/M) &\to W_p\\ \sigma_{a,b} &\mapsto \tau_{a,b}.\end{aligned}$$

We laten zien dat dit een isomorfisme is. Het is duidelijk dat ϕ bijectief is, dus we gaan nog na dat het een homomorfisme is.

Door de definitie van ϕ en $\tau_{a,b}$ weten we al dat

$$\phi(\sigma_{a,b})\phi(\sigma_{c,d}) = \tau_{a,b}\tau_{c,d} = \tau_{ac,ad+b} = \phi(\sigma_{ac,ad+b}).$$

We moeten nog nagaan dat $\phi(\sigma_{ac,ad+b}) = \phi(\sigma_{a,b}\sigma_{c,d})$. Dit doen we door te laten zien dat $\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,ad+b}$.

$$\begin{aligned}\sigma_{a,b}(\sigma_{c,d}(\zeta_p)) &= \sigma_{a,b}(\zeta_p^c) = \zeta_p^{ac},\\ \sigma_{a,b}(\sigma_{c,d}(\sqrt[p]{\alpha})) &= \sigma_{a,b}(\zeta_p^d \sqrt[p]{\alpha}) = \zeta_p^{ad}\zeta_p^b \sqrt[p]{\alpha} = \zeta_p^{ad+b}\sqrt[p]{\alpha},\end{aligned}$$

dus $\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,ad+b}$ en dus

$$\phi(\sigma_{a,b})\phi(\sigma_{c,d}) = \phi(\sigma_{ac,ad+b}) = \phi(\sigma_{a,b}\sigma_{c,d}).$$

Hiermee is ϕ een homomorfisme en dus een isomorfisme. □

3.2 Een geneste worteluitbreiding

We gaan de Galoisgroep van $\mathbb{Q}(\sqrt{\beta})^{\mathrm{norm}}$ in twee stappen bekijken. Eerst bepalen we $\mathrm{Gal}(\mathbb{Q}(\beta)^{\mathrm{norm}}/\mathbb{Q})$ en daarna $\mathrm{Gal}(\mathbb{Q}(\sqrt{\beta})^{\mathrm{norm}}/\mathbb{Q})$.

Zij $p > 2$ een priemgetal en $\alpha \in \mathbb{Q}$ geen p^{de}-macht. Dan is $\mathbb{Q}(\sqrt[p]{\alpha})$ een uitbreiding van $\mathbb{Q}$ van graad p. Als $\beta \in \mathbb{Q}(\sqrt[p]{\alpha})\backslash\mathbb{Q}$, dan is

$$Q \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt[p]{\alpha}).$$

Omdat p priem is en

$$[\mathbb{Q}(\sqrt[p]{\alpha}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{\alpha} : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}]$$

en $[\mathbb{Q}(\beta) : \mathbb{Q}] \neq 1$, volgt $[\mathbb{Q}(\sqrt[p]{\alpha}) : \mathbb{Q}(\beta)] = 1$, oftewel $\mathbb{Q}(\sqrt[p]{\alpha}) = \mathbb{Q}(\beta)$.

Het minimumpolynoom van $\sqrt[p]{\alpha}$ over $\mathbb{Q}$ is $X^p - \alpha$ en heeft nulpunten

$$\sqrt[p]{\alpha}, \zeta_p\sqrt[p]{\alpha}, \zeta_p^2\sqrt[p]{\alpha}, \ldots, \zeta_p^{p-1}\sqrt[p]{\alpha}.$$

Het is dus genoeg om ζ_p toe te voegen om alle nulpunten te krijgen. De normale afsluiting is dus

$$Q(\sqrt[p]{\alpha})^{\mathrm{norm}} = \mathbb{Q}(\sqrt[p]{\alpha}, \zeta_p) = \mathbb{Q}(\beta, \zeta_p).$$

Propositie 3.4. $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{\alpha})^{\mathrm{norm}}/\mathbb{Q}) \cong W_p$.

Bewijs. Dit volgt direct uit Propositie 3.3. □

Gevolg 3.5. *We kunnen de Galois-geconjugeerden $\{\beta_0, ..., \beta_{p-1}\}$ van β zo kiezen dat $\beta = \beta_0$ en $\sigma_{a,b}(\beta_i) = \beta_{ai+b}$, waarbij de indices modulo p genomen worden en $\sigma_{a,b} \in \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{\alpha})^{\mathrm{norm}}/\mathbb{Q})$ gedefinieerd is door $\sigma_{a,b}(\zeta_p) = \zeta_p^a$ en $\sigma_{a,b}(\sqrt[p]{\alpha}) = \zeta_p^b \sqrt[p]{\alpha}$.*

Bewijs. β is reëel, dus de waarde van $\sigma_{a,b}(\zeta_p)$ heeft geen invloed op $\sigma_{a,b}(\beta)$, oftewel $\sigma_{a,b}(\beta) = \sigma_{a',b}(\beta)$ voor alle a, a'. Als we nu $\beta_0 = \beta$ nemen, kunnen we de overige β_i definiëren door $\beta_i = \sigma_{1,b}(\beta)$. Dit is inderdaad de gezochte nummering, want

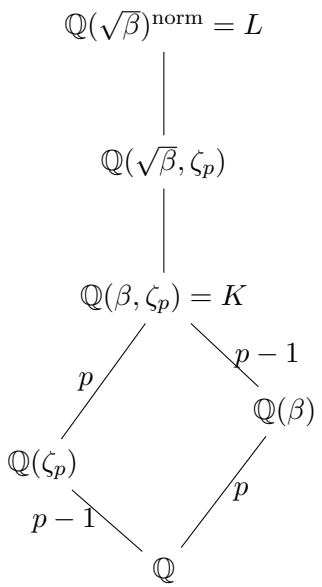
$$\sigma_{a,b}(\beta_i) = \sigma_{a,b}(\sigma_{1,i}(\beta_0)) = \sigma_{a,ai+b}(\beta_0) = \sigma_{1,ai+b}(\beta_0) = \beta_{ai+b}. \qquad \square$$

Nu we weten wat hoe $\mathrm{Gal}(\mathbb{Q}(\beta)^{\mathrm{norm}}/\mathbb{Q}))$ eruit ziet, kunnen we gaan kijken wat er gebeurt als we ook $\sqrt{\beta}$ toevoegen; we bekijken het lichaam $\mathbb{Q}(\sqrt{\beta})^{\mathrm{norm}}$.

Als $f = f_{\mathbb{Q}}^{\beta}$ dan is $\mathbb{Q}(\sqrt{\beta})^{\mathrm{norm}}$ het ontbindingslichaam van $f(X^2)$. $f(X^2)$ heeft als nulpunten

$$\Omega = \{\pm\sqrt{\beta_i} | \beta_i \text{ nulpunt van } f\}.$$

Een $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ wordt dus volledig bepaald door $\sigma(\pm\sqrt{\beta_i})$. Omdat we al weten wat σ met β_i doet, kunnen we ook zeggen wat $\sigma(\sqrt{\beta_i})$ is.



In het vervolg van dit hoofdstuk gebruiken we de notaties:

- $K = \mathbb{Q}(\beta)^{\mathrm{norm}}$,
- $L = \mathbb{Q}(\sqrt{\beta})^{\mathrm{norm}}$.

Propositie 3.6. *De geconjugeerden van β kunnen zo genummerd worden dat er voor elke $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ een $a \in \mathbb{F}_p^*$ en een $b \in \mathbb{F}_p$ bestaan zodat $\sigma(\sqrt{\beta_i}) = \pm\sqrt{\beta_{ai+b}}$ voor alle i. (Het teken hoeft hierbij niet voor alle i hetzelfde te zijn.)*

Bewijs. Uit Gevolg 3.5 volgt dat we de geconjugeerden zo kunnen nummeren dat

$$\forall \sigma_{a,b} \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma_{a,b}(\beta_i) = \beta_{ai+b}.$$

Als $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ dan $\sigma|_K \in \mathrm{Gal}(K/\mathbb{Q})$ en zijn er dus $a \in \mathbb{F}_p^*$ en $b \in \mathbb{F}_p$ zodat $\sigma|_K = \sigma_{a,b}$. Omdat

$$\sigma(\sqrt{\beta_i})^2 = \sigma(\sqrt{\beta_i}^2) = \sigma(\beta_i) = \sigma_{a,b}(\beta_i) = \beta_{ai+b}$$

moet nu

$$\sigma(\sqrt{\beta_i}) = \pm\sqrt{\beta_{ai+b}}. \qquad \square$$

3.3 Een ontnestbaarheidsconditie

We kunnen de informatie over de structuur van $\mathrm{Gal}(K/\mathbb{Q})$ nu gebruiken om een uitspraak te doen over de ontnestbaarheid van $\sqrt{\beta}$. In [7] wordt dit gedaan door te bewijzen dat $\sqrt{\frac{N(\beta)}{\beta}} \in K$ als $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$. Dit is ook wat wij gaan doen, maar de manier waarop is anders. In [7] wordt vanuit de aanname $\sqrt{\frac{N(\beta)}{\beta}} \notin K$ een concreet element van $\mathrm{Gal}(L/\mathbb{Q})''$ geconstrueerd, dat niet de identiteit is. Wat wij gaan doen, is laten zien dat het teken van $\sigma(\sqrt{\beta_i}) = \pm\sqrt{\beta_{ai+b}}$ onafhankelijk is van i, als $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$.

Lemma 3.7. *Zij Ω de nulpuntenverzameling van $f_{\mathbb{Q}}^{\beta}(X^2)$, $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ met $\sigma|_K \neq \mathrm{id}$ en $\tau \in \mathrm{Gal}(L/K)$ met $[\sigma, \tau] = \mathrm{id}$, dan $\tau|_\Omega = \pm\,\mathrm{id}$.*

Bewijs. Eerst kijken we hoe zulke σ en τ eruit zien. Hiervoor nummeren we de geconjugeerden van β volgens Gevolg 3.5. Vanwege Propositie 3.6 weten we wat σ en τ op L doen, als we weten wat ze op K doen. We kijken daarom naar $\sigma|_K \in \mathrm{Gal}(K/\mathbb{Q})'$. Propositie 3.4 en Propositie 3.2 geven dat $\sigma|_K = \sigma_{1,b}$ met $b \in \mathbb{F}_p$, waarbij $b \neq 0$ omdat $\sigma|_K \neq \mathrm{id}$. σ is dus van de vorm

$$\sigma(\sqrt{\beta_i}) = \pm\sqrt{\beta_{i+b}}.$$

We willen ook weten hoe τ eruit ziet. Aangezien $\tau|_K = \mathrm{id}$, is τ van de vorm

$$\tau(\sqrt{\beta_i}) = \pm\sqrt{\beta_i}.$$

De rest van het bewijs is een bewijs uit het ongerijmde; we nemen aan dat $\tau_\Omega \neq \pm\,\mathrm{id}$ en leiden hier een tegenspraak met $[\sigma, \tau]$ uit af.

Stel $\tau|_\Omega \neq \pm\,\mathrm{id}$, dan $\exists n, m : \tau(\sqrt{\beta_n}) = \sqrt{\beta_n}$ en $\tau(\sqrt{\beta_m}) = -\sqrt{\beta_m}$. Omdat b en p copriem zijn, is $\{0, b, 2b, \dots\} = \mathbb{F}_p$. Het kan dus niet zo zijn dat voor alle i

met $\tau(\sqrt{\beta_i}) = \sqrt{\beta_i}$ geldt dat $\tau(\sqrt{\beta_{i+b}}) = \sqrt{\beta_{i+b}}$, want dan zou $\tau(\sqrt{\beta_i}) = \sqrt{\beta_i}$ voor alle i, wat in tegenspraak is met $\tau(\sqrt{\beta_m}) = -\sqrt{\beta_m}$. We kunnen dus z.v.v.a. aannemen dat $m = n + b$.

Nu hebben we

$$\begin{aligned}
[\sigma, \tau](\sqrt{\beta_{n+b}}) &= \sigma\tau\sigma^{-1}\tau^{-1}(\sqrt{\beta_{n+b}}) \\
&= -\sigma\tau\sigma^{-1}(\sqrt{\beta_{n+b}}) \\
&= -\sigma\tau(\pm\sqrt{\beta_n}) \\
&= -\sigma(\pm\sqrt{\beta_n}) \\
&= -\sqrt{\beta_{n+b}}) \neq \sqrt{\beta_{n+b}}.
\end{aligned}$$

Dus $[\sigma, \tau] \neq \mathrm{id}$, wat in tegenspraak is met de aanname, dus $\tau|_\Omega = \pm\,\mathrm{id}$. □

Propositie 3.8. *Als* $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$ *dan is* $[L : K] \leq 2$.

Bewijs. $[L : K] \leq 2$ is equivalent met $|\,\mathrm{Gal}(L/K)| \leq 2$, vanwege Propositie 2.8. Door een geschikte $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ te kiezen, kunnen we dit laten zien met het voorgaande lemma.

We weten dat

$$\mathrm{Gal}(K/\mathbb{Q})' \cong W_p' \cong C_p \supsetneq \{\mathrm{id}\}.$$

Er is dus een $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ met $\sigma|_K \neq \mathrm{id}$.

Zij Ω de nulpuntenverzameling van $f_{\mathbb{Q}}^{\beta}(X^2)$ en $\tau \in \mathrm{Gal}(L/K)$ willekeurig, dan $[\sigma, [\sigma, \tau]] \in \mathrm{Gal}(L/\mathbb{Q})''$ en dus $[\sigma, [\sigma, \tau]] = \mathrm{id}$. Er geldt

$$[\sigma, \tau]|_K = \sigma|_K\tau|_K\sigma|_K^{-1}\tau|_K^{-1} = \sigma|_K\sigma|_K^{-1} = \mathrm{id}$$

en dus $[\sigma, \tau] \in \mathrm{Gal}(L/K)$. Lemma 3.7 geeft nu dat $[\sigma, \tau]|_\Omega = \pm\,\mathrm{id}$.

Als we elementen van $\mathrm{Gal}(L/\mathbb{Q})$ zien als permutaties van Ω dan zijn de tekens:

$$\varepsilon[\sigma, \tau] = \varepsilon(\sigma)\varepsilon(\tau)\varepsilon(\sigma^{-1})\varepsilon(\tau^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1})\varepsilon(\tau)\varepsilon(\tau^{-1}) = 1$$

en

$$\varepsilon(-\,\mathrm{id}_\Omega) = (-1)^p = -1.$$

Hieruit volgt dat alleen $[\sigma, \tau]|_\Omega = \mathrm{id}$ mogelijk is en dus dat $[\sigma, \tau] = \mathrm{id}$. We kunnen Lemma 3.7 dus weer toepassen en krijgen $\tau|_\Omega = \pm\,\mathrm{id}$. Er zijn dus maar hoogstens twee mogelijke $\tau \in \mathrm{Gal}(L/K)$, dus $[L : K] \leq 2$. □

Lemma 3.9. *De volgende beweringen zijn equivalent:*

i) $\sqrt{\beta N(\beta)} \in K$,

ii) $K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$,

iii) $L = K(\sqrt{\beta})$,

iv) $[L : K] \leq 2$.

Bewijs. We noteren de Galois-geconjugeerden van β met $\{\beta_0, ..., \beta_{p-1}\}$. Hiermee is de norm van β:

$$N(\beta) = \beta_0 \cdot ... \cdot \beta_{p-1}.$$

i) $\implies$ *ii)*:
Als $\sqrt{\beta N(\beta)} \in K$ dan

$$\frac{\sqrt{\beta N(\beta)}}{\sqrt{\beta}} = \sqrt{N(\beta)} \in K(\sqrt{\beta})$$

en dus $K(\sqrt{N(\beta)}) \subseteq K(\sqrt{\beta})$.
Andersom hebben we ook

$$\frac{\sqrt{\beta N(\beta)}}{\sqrt{N(\beta)}} = \sqrt{\beta} \in K(\sqrt{N(\beta)})$$

en dus $K(\sqrt{\beta}) \subseteq K(\sqrt{N(\beta)})$.

ii) $\implies$ *i)*:
Omdat $K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$ geldt

$$\sqrt{\beta}, \sqrt{N(\beta)} \in K(\sqrt{N(\beta)})$$

en dus $\sqrt{\beta N(\beta)} \in K(\sqrt{N(\beta)})$. Als $K = K(\sqrt{N(\beta)})$ zijn we dus klaar. We nemen dus aan dat $K \neq K(\sqrt{N(\beta)})$.

Omdat $\sqrt{\beta N(\beta)} \in K(\sqrt{N(\beta)})$, zijn er $a, b \in K$ zodat

$$(a + b\sqrt{N(\beta)})^2 = a^2 + 2ab\sqrt{N(\beta)} + b^2 N(\beta) = \beta N(\beta).$$

Nu moet $2ab = 0$, omdat $\sqrt{N(\beta)}$ en $N(\beta)$ lineair onafhankelijk zijn in de K-vectorruimte $K(\sqrt{\beta})$. Er zijn dus twee gevallen: $a = 0$ of $b = 0$.

- Als $a = 0$ dan $b^2 N(\beta) = \beta N(\beta) \implies \sqrt{\beta} \in K$. Tegenspraak met $K \neq K(\sqrt{N(\beta)}) = K(\sqrt{\beta})$.
- Als $b = 0$ dan $a^2 = \beta N(\beta) \implies \sqrt{\beta N(\beta)} \in K$.

i) $\implies$ *iii)*:
$K/\mathbb{Q}$ is normaal, dus als $\sqrt{\beta N(\beta)} \in K$ dan ook $\sqrt{\beta_i N(\beta)} \in K$ voor alle i en dus

$$\frac{\sqrt{\beta_i N(\beta)}}{\sqrt{\beta N(\beta)}} \sqrt{\beta} = \sqrt{\beta_i} \in K(\sqrt{\beta})$$

voor alle i. Dit geeft de inclusie

$$L = \mathbb{Q}(\sqrt{\beta_0}, \ldots, \sqrt{\beta_{p-1}}) \subseteq K(\sqrt{\beta}).$$

De andere inclusie, $K(\sqrt{\beta}) \subseteq L$, is duidelijk.

iii) $\implies$ *i)*:
Stel $L = K(\sqrt{\beta})$. Dan $\sqrt{\beta_i} \in K(\sqrt{\beta})$ voor alle i, dus er zijn $a, b \in K$ zodat

$$(a + b\sqrt{\beta})^2 = a^2 + 2ab\sqrt{\beta} + b^2\beta = \beta_i.$$

Dit heeft alleen oplossingen als $2ab = 0$, dus $a = 0$ of $b = 0$.

- Als $a = 0$ dan $b^2\beta = \beta_i \implies \sqrt{\frac{\beta_i}{\beta}} \in K \implies \sqrt{\beta\beta_i} \in K$.
- Als $b = 0$ dan $a^2 = \beta_i \implies \sqrt{\beta_i} \in K$. Omdat $K/\mathbb{Q}$ normaal is, geldt ook $\sqrt{\beta} \in K$ en dus $\sqrt{\beta\beta_i} \in K$.

We weten nu voor alle i dat $\sqrt{\beta\beta_i} \in K$ en daarom ook dat

$$\sqrt{\beta\beta_1} \ldots \sqrt{\beta\beta_{p-1}} = \sqrt{\beta^{p-2}\beta_0\beta_1 \ldots \beta_{p-1}} = \beta^{(p-3)/2}\sqrt{\beta N(\beta)} \in K.$$

Omdat p oneven is, geldt dus $\sqrt{\beta N(\beta)} \in K$.

iii) $\implies$ *iv)*: triviaal

iv) $\implies$ *iii)*:
Als $[L : K] = 1$ dan $L = K$ en dan zijn we klaar, omdat $\sqrt{\beta} \in L = K$ en dus

$$L = K = K(\sqrt{\beta}).$$

Als $[L : K] = 2$ dan $\sqrt{\beta} \notin K$. Anders zou K immers de normale afsluiting van $\mathbb{Q}(\sqrt{\beta})$ zijn en dus $L = K$. Er geldt dus $K \subseteq K(\sqrt{\beta}) \subseteq L$ met

$$2 = [L : K] = [L : K(\sqrt{\beta})][K(\sqrt{\beta}) : K] = [L : K(\sqrt{\beta})] \cdot 2$$

en dus $[L : K(\sqrt{\beta})] = 1 \implies L = K(\sqrt{\beta})$. □

We hebben nu alle ingrediënten om hetzelfde resultaat als [7] te bewijzen.

Stelling 3.10. *De volgende beweringen zijn equivalent:*

i) $\sqrt{\beta} \in \mathbb{Q}^{(1)}$,

ii) $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$,

iii) $\exists c \in \mathbb{Q}, \gamma \in \mathbb{Q}(\sqrt[p]{\alpha}) : \beta = c\gamma^2$.

Bewijs. i) $\implies$ *ii)*:
Dit bewijs is hetzelfde bewijs dat gegeven wordt in Theorem 102 van [4], maar met meer details.

We kunnen dit bewijzen met Propositie 2.14. Hiervoor moeten we wel eerst een geschikt lichaam M vinden zodat $\mathbb{Q} \subseteq M \subseteq L$ en $\mathrm{Gal}(L/M)$ en $\mathrm{Gal}(M/\mathbb{Q})$ abels zijn.

Per aanname is $\sqrt{\beta} \in \mathbb{Q}^{(1)}$. Daarom is $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}^{(1)}$ en kunnen we L, vanwege de constructie van $\mathbb{Q}^{(1)}$, schrijven als

$$L = \mathbb{Q}(\alpha_1, \ldots, \alpha_k).$$

Hierbij is er voor elke i een n_i, zodat $\alpha_i^{n_i} \in \mathbb{Q}$. De Galois-geconjugeerde van α_i zijn van de vorm $\zeta_{n_i}^l \alpha_i$. Al deze geconjugeerden zitten in L, omdat $L/\mathbb{Q}$ normaal is. In het bijzonder zitten dus alle $\zeta_{n_i} \in L$ en daarom ook $\zeta_n \in L$, met $n = \mathrm{kgv}\{n_1, ..., n_k\}$. Hierdoor vinden we

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq L = \mathbb{Q}(\zeta_n, \alpha_1, ..., \alpha_k).$$

Nu hoeven we alleen nog aan te tonen dat $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ en $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n))$ abels zijn.

Volgens Propositie 2.11 is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Aangezien $(\mathbb{Z}/n\mathbb{Z})^*$ abels is, is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ dat dus ook.

En voor $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q}(\zeta_n))$ geldt

$$\sigma\tau(\alpha_i) = \sigma(\zeta_{n_i}^l \alpha_i) = \zeta_{n_i}^{lm} \alpha_i = \tau(\zeta_{n_1}^m \alpha_i) = \tau\sigma(\alpha_i).$$

Dus $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n)$ is abels en uit Propositie 2.14 volgt nu dat

$$\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}.$$

ii) $\implies$ *iii)*:
Propositie 3.8 geeft samen met Lemma 3.9 dat $\sqrt{\beta N(\beta)} \in K$. We kunnen laten zien dat zelfs $\sqrt{\beta N(\beta)} \in \mathbb{Q}(\sqrt[p]{\alpha})$ geldt. Dit doen we op dezelfde manier als [7]. Stel $\sqrt{\beta N(\beta)} \notin \mathbb{Q}(\sqrt[p]{\alpha})$, dan hebben we de keten van uitbreidingen

$$\mathbb{Q}(\sqrt[p]{\alpha}) \subseteq \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt{\beta N(\beta)}) \subseteq \mathbb{Q}(\sqrt[p]{\alpha}, \zeta_p) = K$$

met $[\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt{\beta N(\beta)} : \mathbb{Q}(\sqrt[p]{\alpha})] = 2$. Volgens Propositie 2.16 is dan

$$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt{\beta N(\beta)}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt{\pm p}).$$

Met Propositie 2.17 kunnen we nu $\sqrt{\beta N(\beta)} = \sqrt{\pm p^n} x$ schrijven, met $x \in \mathbb{Q}(\sqrt[p]{\alpha})$. We hebben aangenomen dat $\sqrt{\beta N(\beta)} \notin \mathbb{Q}(\sqrt[p]{\alpha})$, dus n is oneven. Door nu de norm te bekijken,

$$N(\sqrt{\beta N(\beta)})^2 = N(\beta N \sqrt{\beta}) = N(\pm p^n x^2) = \pm p^{pn} N(x)^2,$$

vinden we een tegenspraak, omdat p^{pn} geen kwadraat is. Dus $\sqrt{\beta N(\beta)} \in \mathbb{Q}(\sqrt[p]{\alpha})$. Nu kunnen we de $c = \frac{1}{N(\beta)}$ en $\gamma = \sqrt{\beta N(\beta)}$ nemen:

$$\beta = \frac{1}{N(\beta)} \sqrt{\beta N(\beta)}^2.$$

iii) $\implies$ *i)*: $\sqrt{\beta} = \sqrt{c}\gamma \in \mathbb{Q}^{(1)}$. $\square$

De β die geschreven kunnen worden zoals bij *iii*), zijn precies de flauwe gevallen waarvan we aan het begin van het hoofdstuk al gezien hadden dat deze sowieso ontnestbaar zijn. De conclusie van deze stelling is dit andersom ook geldt: als $\sqrt{\beta}$ ontnestbaar is, dan is β te schrijven zoals bij *iii*). Alle ontnestbare $\sqrt{\beta}$ zijn dus op een flauwe manier ontnestbaar.

4 Geneste hogeremachtswortels

Tot nu toe hebben we gekeken naar $\sqrt{\beta}$. In dit hoofdstuk gaan we dit generaliseren naar hogeremachtswortels $\sqrt[q]{\beta}$. Hierbij is q een priemgetal, ongelijk aan p en groter dan 2.

Een voorbeeld van een ontnestbare wortel van deze vorm is

$$\sqrt[3]{5\sqrt[5]{2^2} - 4\sqrt[5]{2} - 2} = \frac{\sqrt[5]{2^2} + 2\sqrt[5]{2^2} - 4}{\sqrt[3]{20}}.$$

De aanpak in dit hoofdstuk is zoveel mogelijk hetzelfde als in het vorige hoofdstuk. De resultaten in dit hoofdstuk corresponderen op de volgende manier met de resultaten uit het vorige hoofdstuk:

- Propositie 3.6 $\longleftrightarrow$ Propositie 4.1,
- Lemma 3.7 $\longleftrightarrow$ Lemma 4.3,
- Propositie 3.8 $\longleftrightarrow$ Propositie 4.4,
- Lemma 3.9 $\longleftrightarrow$ Lemma 4.5,
- Stelling 3.10 $\longleftrightarrow$ Stelling 4.6.

Aangezien $\mathbb{Q}(\beta)^{\text{norm}}$ hetzelfde is als in het vorige hoofdstuk, hoeven we alleen de tweede uitbreiding $\mathbb{Q}(\sqrt[q]{\beta})^{\text{norm}}$ te bekijken.

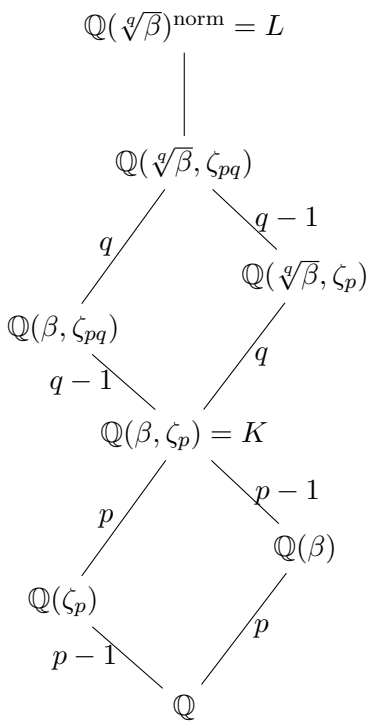
We gebruiken in dit hoofdstuk de notaties:

- q is een oneven priemgetal, ongelijk aan p,
- $K = \mathbb{Q}(\beta)^{\text{norm}}$,
- $L = \mathbb{Q}(\sqrt[q]{\beta})^{\text{norm}}$.

L is nu het ontbindingslichaam van $f^{\beta}_{\mathbb{Q}}(X^q)$ en dat heeft de nulpunten

$$\Omega = \{\zeta_q^i \sqrt[q]{\beta_j} \mid i \in \mathbb{Z}, \beta_j \text{ nulpunt van } f^{\beta}_{\mathbb{Q}}(X^q)\}.$$

Hierbij is elke $\sqrt[q]{\beta_i}$ een willekeurig nulpunt van $X^q - \beta_i$. Aangezien β reëel is, is voor $\sqrt[q]{\beta_0} = \sqrt[q]{\beta}$ het reële nulpunt een voor de hand liggende keuze. De andere β_i zijn niet reëel, dus kiezen we voor de andere β_i een willekeurig, maar vast, nulpunt $\sqrt[q]{\beta_i}$ van $X^q - \beta_i$.



Propositie 4.1. *De geconjugeerden van β kunnen zo genummerd worden dat er voor elke $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ een $a \in \mathbb{F}_p^*$ en $b \in \mathbb{F}_p$ bestaan zodat $\forall i \exists n_i \in \mathbb{Z}$: $\sigma(\sqrt[q]{\beta_i}) = \zeta_q^{n_i} \sqrt[q]{\beta_{ai+b}}$.*

Bewijs. Analoog met het bewijs van Propositie 3.6. □

Om een gegeneraliseerde versie van Lemma 3.7 te bewijzen, hebben we de volgende recurrente betrekking nodig.

Lemma 4.2. *De recurrente betrekking*

$$a_0 = a$$

$$a_1 = b$$

$$a_n = 2a_{n-1} - a_{n-2}$$

heeft als oplossing $a_n = a - (a - b)n$.

Bewijs. Dit is eenvoudig na te gaan met inductie naar n.

Inductiebasis:

$$a_0 = a = a - (a - b) \cdot 0,$$
$$a_1 = b = a - (a - b) \cdot 1.$$

Inductiestap:

$$\begin{aligned} a_n &= 2a_{n-1} - a_{n-2} \\ &= 2(a-(a-b)(n-1)) - (a-(a-b)(n-2)) \\ &= 2a - 2an + 2bn + 2a - 2b - a + an - bn - 2a + 2b \\ &= a - an + bn = a - (a-b)n. \end{aligned}$$ □

Lemma 4.3. *Laat $\{\beta_0, ..., \beta_{p-1}\}$ de geconjugeerden van β zijn, genummerd volgens Gevolg 3.5. Als $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ met $\sigma|_K \neq \mathrm{id}$ en $\tau \in \mathrm{Gal}(L/K(\zeta_q))$ zodat er een $n \in \mathbb{F}_q$ bestaat met $[\sigma,\tau](\sqrt[q]{\beta_i}) = \zeta_q^n \sqrt[q]{\beta_i}$ voor alle i, dan is er een $d \in \mathbb{F}_q$ zodat $\tau(\sqrt[q]{\beta_i}) = \zeta_q^d \sqrt[q]{\beta_i}$ voor alle i.*

De grootste verschillen met Lemma 3.7 zijn de extra aanname dat

$$\tau \in \mathrm{Gal}(L/K(\zeta_q))$$

in plaats van $\tau \in \mathrm{Gal}(L/K)$ en de verzwakking van de aanname $[\sigma,\tau] = \mathrm{id}$ naar het bestaan van een n zodat $[\sigma,\tau](\sqrt[q]{\beta_i}) = \zeta_q^n \sqrt[q]{\beta_i}$. Dit eerste is nodig omdat het anders niet waar is. Het tweede is nodig omdat we bij de generalisatie van Propositie 3.8 niet kunnen garanderen dat $[\sigma,\tau] = \mathrm{id}$.

Bewijs. Net als bij Propositie 3.8 kijken we eerst hoe σ en τ eruit zien.

Als $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ dan $\sigma|_K \in \mathrm{Gal}(K/\mathbb{Q})'$ en dus $\sigma|_K = \sigma_{1,b}$ met $b \in \mathbb{F}_p$ en $b \neq 0$ want $\sigma|_K \neq \mathrm{id}$. σ is dus van de vorm

$$\sigma(\sqrt[q]{\beta_i}) = \zeta_q^{k_i} \sqrt[q]{\beta_{i+b}}.$$

Omdat σ in de commutatorgroep zit van $\mathrm{Gal}(L/\mathbb{Q})$ weten we bovendien dat $\sigma(\zeta_q) = \zeta_q$ en daarom

$$\sigma^{-1}(\sqrt[q]{\beta_i}) = \zeta_q^{k_{i-b}} \sqrt[q]{\beta_{i-b}}.$$

Omdat $\tau|_{K(\zeta_q)} = \mathrm{id}$, is τ van de vorm $\tau(\sqrt[q]{\beta_i}) = \zeta_q^{l_i} \sqrt[q]{\beta_i}$, $\tau(\zeta_q) = \zeta_q$. Voor de inverse geldt

$$\tau^{-1}(\sqrt[q]{\beta_i}) = \zeta_q^{-l_i} \sqrt[q]{\beta_i}.$$

In tegenstelling tot bij Propositie 3.8 is de rest van het bewijs geen bewijs uit het ongerijmde, maar kijken we gewoon hoe $[\sigma,\tau]$ zich gedraagt. Voor alle i hebben we nu

$$\begin{aligned} [\sigma,\tau](\sqrt[q]{\beta_{i+b}}) &= \sigma\tau\sigma^{-1}\tau^{-1}(\sqrt[q]{\beta_{i+b}}) \\ &= \sigma\tau\sigma^{-1}(\zeta_q^{-l_{i+b}} \sqrt[q]{\beta_{i+b}}) \\ &= \sigma\tau(\zeta_q^{-l_{i+b}-k_i} \sqrt[q]{\beta_i}) \\ &= \sigma(\zeta_q^{l_i-l_{i+b}-k_i} \sqrt[q]{\beta_i}) \\ &= \zeta_q^{l_i-l_{i+b}} \sqrt[q]{\beta_{i+b}} = \zeta_q^n \sqrt[q]{\beta_{i+b}}. \end{aligned}$$

Zowel de indices van l als van β worden hierbij modulo p genomen.

Hierop kunnen we de recurrente betrekking uit het vorige lemma gebruiken. Omdat n constant is geld namelijk

$$\forall k : l_{kb} - l_{(k+1)b} = l_{(k+1)b} - l_{(k+2)b} \mod q$$

oftewel $l_{(k+2)b} = 2l_{(k+1)b} - l_{kb} \mod q$. Met Lemma 4.2 vinden we nu dat $l_{kb} = l_0 - (l_0 - l_1)k \mod q$. Dus zien we dat

$$l_{kb} - l_{(k+q)b} = (l_0 - l_1)q = 0 \mod q.$$

Het rijtje $\{l_{kb}\}_{k\in\mathbb{N}}$ is dus zowel q-periodiek als p-periodiek. Aangezien $p \neq q$ en het rijtje hoogstens p verschillende waarden aan kan nemen, volgt dat l_{kb} constant is. Deze constante waarde l_0 is de gezochte d. □

Propositie 4.4. *Als* $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$ *en* $L \neq K$ *dan* $\mathrm{Gal}(L/K) \cong W_q$.

Bewijs. Net als bij Propositie 3.8 is het idee van het bewijs om een geschikte $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ te kiezen, en dan met het voorgaande lemma een beperkt aantal mogelijke $\tau \in \mathrm{Gal}(L/K)$ te vinden. Lemma 4.3 zegt echter alleen iets over $\mathrm{Gal}(L/K(\zeta_q))$, dus kunnen we niet zomaar een willekeurige $\tau \in \mathrm{Gal}(L/K)$ nemen.

Zij $\tau \in \mathrm{Gal}(L/K)$ willekeurig. Er is een $c \in \mathbb{F}_q^*$ zodat $\tau(\zeta_q) = \zeta_q^c$. Definieer $\rho \in \mathrm{Gal}(L/K)$ door $\rho(\sqrt[q]{\beta_i}) = \sqrt[q]{\beta_i}$ en $\rho(\zeta_q) = \zeta_q^{c^{-1}}$. Voor $\tilde{\tau} = \tau \circ \rho$ geldt nu $\tilde{\tau}(\sqrt[q]{\beta_i}) = \tau(\sqrt[q]{\beta_i})$ en $\tilde{\tau}(\zeta_q) = \zeta_q$, dus $\tilde{\tau} \in \mathrm{Gal}(L/K(\zeta_q))$.

We weten dat

$$\mathrm{Gal}(K/\mathbb{Q})' \cong W_p' \cong C_p \supsetneq \{\mathrm{id}\}.$$

Er is dus een $\sigma \in \mathrm{Gal}(L/\mathbb{Q})'$ met $\sigma|_K \neq \mathrm{id}$.

$[\sigma, [\sigma, \tilde{\tau}]] \in \mathrm{Gal}(L/\mathbb{Q})''$ en dus $[\sigma, [\sigma, \tilde{\tau}]] = \mathrm{id}$. Omdat $\tilde{\tau}|_{K(\zeta_q)} = \mathrm{id}$ geldt

$$[\sigma, \tilde{\tau}]|_{K(\zeta_q)} = \sigma|_{K(\zeta_q)}\tilde{\tau}|_{K(\zeta_q)}\sigma|^{-1}_{K(\zeta_q)}\tilde{\tau}|^{-1}_{K(\zeta_q)} = \sigma|_{K(\zeta_q)}\sigma|^{-1}_{K(\zeta_q)} = \mathrm{id}$$

en dus $[\sigma, \tilde{\tau}] \in \mathrm{Gal}(L/K(\zeta_q))$.

Lemma 4.3 geeft nu dat $\exists d \in \mathbb{F}_q : [\sigma, \tilde{\tau}](\sqrt[q]{\beta_i}) = \zeta_q^d \sqrt[q]{\beta_i}$.

Voor elke $d \neq 0$ is dit een even permutatie op Ω, want het zijn p q-cykels. Als $d = 0$ is het de identiteit en dus ook een even permutatie. We kunnen nu niet zoals bij Propositie 3.8 het teken gebruiken om het aantal mogelijkheden van $[\sigma, \tilde{\tau}]$ nog verder te beperken. Lemma 4.3 vereist dit echter ook niet, dus kunnen we het direct opnieuw toepassen. Dit geeft $\exists d \in \mathbb{F}_q : \tau(\sqrt[q]{\beta_i}) = \tilde{\tau}(\sqrt[q]{\beta_i}) = \zeta_q^d \sqrt[q]{\beta_i}$.

Omdat $L \neq K$ en L normaal is, moet $\zeta_q \in L$. We kunnen dus een injectief homorfisme $\phi : \mathrm{Gal}(L/K) \to W_q$ definiëren door $\tau \mapsto \tau_{c,d}$ waarbij c en d zoals hierboven. Dit is zelfs een isomorfisme, want $K(\zeta_q, \sqrt[q]{\beta}) \subseteq L$ en $\mathrm{Gal}(K(\zeta_q, \sqrt[q]{\beta})/K) \cong W_q$ (Propositie 3.3). Als we dus de kardinaliteiten vergelijken, zien we dat ϕ een bijectie is:

$$|W_q| = |\,\mathrm{Gal}(K(\zeta_q, \sqrt[q]{\beta})/K)| \leq |\,\mathrm{Gal}(L/K)| \leq |W_q|. \qquad \square$$

Lemma 4.5. *De volgende beweringen zijn equivalent:*

i) $\exists r \in \mathbb{Z} : \sqrt[q]{\beta N(\beta)^r} \in \mathbb{Q}(\sqrt[p]{\alpha})$,

ii) $\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$,

iii) $L = K(\zeta_q, \sqrt[q]{\beta})$ *of* $L = K$,

iv) $\mathrm{Gal}(L/K) \cong W_q$ *of* $\mathrm{Gal}(L/K) = \{\mathrm{id}\}$.

Deze beweringen zijn generalisaties van de beweringen van Lemma 3.9. De beweringen *i)* en *ii)* gaan echter over $\mathbb{Q}(\sqrt[p]{\alpha})$ in plaats van over K. Dit is nodig omdat we uiteindelijk een q^{de}-macht in $\mathbb{Q}(\sqrt[p]{\alpha})$ willen vinden en de manier waarop we dat in het vorige hoofdstuk deden in dit geval niet werkt, omdat Propositie 2.16 alleen iets over tweedegraads uitbreidingen zegt.

Bij Lemma 3.9 konden we veel bewijzen omdat we elementen van $K(\sqrt{\beta})$ en kwadraten ervan expliciet uit konden schrijven. Dat gaat nu niet omdat we dan een veel te ingewikkelde uitdrukking

$$(a_0 + a_1 \sqrt[q]{\beta} \ldots a_{q-1} s \sqrt[q]{\beta^{q-1}})^q$$

krijgen, waar niet veel over te zeggen is. Het bewijs wijkt daardoor behoorlijk af van het bewijs van Lemma 3.9.

Bewijs. $N(\beta) = \beta_0 \cdot \ldots \cdot \beta_{p-1}$, waarbij $\{\beta_0, ..., \beta_p\}$ de Galois-geconjugeerden van β zijn.

Definieer het lichaamshomomorfisme $\tau_x : L \to L$ door $\sqrt[q]{\beta_i} \mapsto \sqrt[q]{x\beta_i}$ en $\zeta_{pq} \mapsto \zeta_{pq}$, waarbij $x \in \mathbb{Q}(\sqrt[p]{\alpha})\backslash\{0\}$. Dit voldoet aan de eisen van Lemma 2.15 want op $\mathbb{Q}(\sqrt[p]{\alpha})$ is dit gedefinieerd door $\tau_x(\beta) = x\beta \in K$.

i) $\implies$ *ii)*: Als $q|r$ dan $\sqrt[q]{\beta} \in \mathbb{Q}(\sqrt[p]{\alpha})$, maar dan is β een q^{de} macht en $N(\beta)$ dus ook en dus

$$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)}).$$

Als $q \not| r$ dan is er een s zodat $q|rs - 1$, waardoor $N(\beta)^{rs-1}$ een q^{de}-macht in $\mathbb{Q}$ is. Dus

$$\sqrt[q]{\beta} = \frac{\sqrt[q]{\beta N(\beta)^r}}{\sqrt[q]{N(\beta)^r}} \in \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$$

en

$$\sqrt[q]{N(\beta)} = \frac{\sqrt[q]{\beta N(\beta)^r}^s}{\sqrt[q]{\beta}^s \sqrt[q]{N(\beta)^{rs-1}}} \in \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}).$$

ii) $\implies$ *i)*:

Lemma 2.15 toepassen met τ_x geeft

$$\mathbb{Q}(\sqrt[p]{\alpha}, \tau_x(\sqrt[q]{\beta})) = \mathbb{Q}(\sqrt[p]{\alpha}, \tau_x(\sqrt[q]{N(\beta)})).$$

Aangezien $\sqrt[q]{N(\beta)} = \sqrt[q]{\beta_0}...\sqrt[q]{\beta_{p-1}}$ geldt

$$\tau_x(\sqrt[q]{N(\beta)}) = \tau_x(\sqrt[q]{\beta_0})...\tau_x(\sqrt[q]{\beta_{p-1}}) = x^p N(\beta).$$

Omdat $\text{ggd}(p,q) = 1$ kunnen we een r kiezen zodat $r = -p^{-1} \mod q$. In het bijzonder geldt dan $q|rp+1$. Als we dan $x = N(\beta)^r$ nemen, krijgen we

$$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta N(\beta)^r}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)^{rp+1}}) = \mathbb{Q}(\sqrt[p]{\alpha}, N(\beta)^{\frac{rp+1}{q}}) = \mathbb{Q}(\sqrt[p]{\alpha}),$$

oftewel $\sqrt[q]{\beta N(\beta)^r} \in \mathbb{Q}(\sqrt[p]{\alpha})$.

ii) $\implies$ *iii)*: Merk op dat

$$K(\zeta_q, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta})(\zeta_p, \zeta_q) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})(\zeta_p, \zeta_q) = K(\zeta_q, \sqrt[q]{N(\beta)}).$$

Als $\sqrt[q]{\beta} \in K$ dan $L = K$, want K is normaal. Als $\sqrt[q]{\beta} \notin K$, dan is

$$K(\zeta_q, \sqrt[q]{N(\beta)}) = \mathbb{Q}(\zeta_p, \beta, \zeta_q, \sqrt[q]{N(\beta)})$$

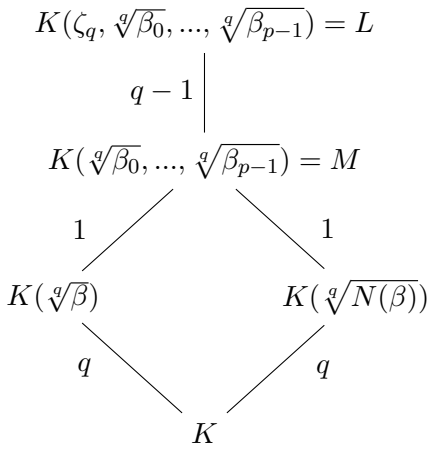
normaal over $\mathbb{Q}$, want het is het ontbindingslichaam van $f_{\mathbb{Q}}^{\beta} \cdot f_{\mathbb{Q}}^{\sqrt[q]{N(\beta)}}$. Dit betekent dat $K(\zeta_q, \sqrt[q]{\beta})$ normaal is en dus $L \subseteq K(\zeta_q, \sqrt[q]{\beta})$. Verder is het duidelijk dat $K(\zeta_q, \sqrt[q]{\beta}) \subseteq L$, want $L = K(\zeta_q, \sqrt[q]{\beta_0}, ..., \sqrt[q]{\beta_{q-1}})$.

iii) $\implies$ *ii)*: $L = K$ is equivalent met $\sqrt[q]{\beta} \in K$. Als we aannemen dat $\sqrt[q]{\beta}, \sqrt[q]{N(\beta)} \notin K$, zitten we dus in het geval $L = K(\zeta_q, \sqrt[q]{\beta})$. We laten eerst zien dat in dit geval $K(\sqrt[q]{\beta}) = K(\sqrt[q]{N(\beta)})$ en zullen daarna concluderen dat zelfs $\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$.

We definiëren

$$M = K(\sqrt[q]{\beta_0}, ..., \sqrt[q]{\beta_{p-1}})$$

en zien dat $L = K(\zeta_q, \sqrt[q]{\beta_0}, ..., \sqrt[q]{\beta_{p-1}}) = M(\zeta_q)$.



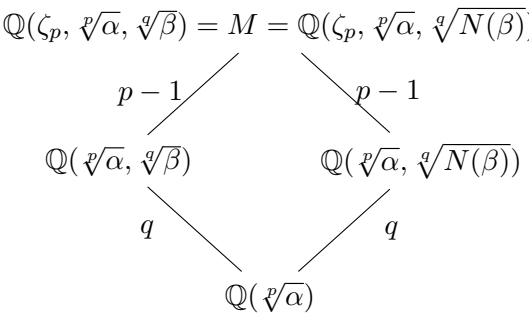
Omdat

$$[L : K(\sqrt[q]{\beta})] = [K(\zeta_q, \sqrt[q]{\beta}) : K\sqrt[q]{\beta}] = q - 1 = [M(\zeta_q) : M] = [L : M],$$

moet $M = K(\sqrt[q]{\beta})$. Op analoge wijze geldt $M = K(\sqrt[q]{N(\beta)})$.

$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta})$ en $\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$ zijn beide tussenlichamen van $\mathbb{Q}(\sqrt[p]{\alpha})$ en M en er geldt

$$[M : \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta})] = p - 1 = [M : \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})].$$



$M = K(\sqrt[q]{N(\beta)}) = \mathbb{Q}(\zeta_p, \sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$ heeft p deellichamen $M' \subseteq M$ met $[M : M'] = p-1$, namelijk $\mathbb{Q}(\zeta_p^n \sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$ met $0 \leq n < p$. Het enige lichaam hiervan dat $\sqrt[p]{\alpha}$ bevat, is $\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$. Dit is dus het enige tussenlichaam $\mathbb{Q}(\sqrt[p]{\alpha}) \subseteq M' \subseteq M$ met $[M : M'] = p - 1$. De twee tussenlichamen die we net gezien hebben, moeten dus wel hetzelfde zijn:

$$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)}).$$

Als $\sqrt[q]{N(\beta)} \in K$ of $\sqrt[q]{\beta} \in K$ dan kunnen we het reduceren tot het geval $\sqrt[q]{\beta}$ en $\sqrt[q]{N(\beta)} \notin K$. We hoeven het geval $\sqrt[q]{\beta} \in K$ niet apart te behandelen, want als $\sqrt[q]{\beta} \in K$ dan ook alle $\sqrt[q]{\beta_i} \in K$, omdat K normaal is en dus ook $\sqrt[q]{N(\beta)} \in K$.

Er is een priemgetal r zodat r de teller en noemer van $N(\beta)$ beide niet deelt. Dit priemgetal is geen q^{de} macht en $N(r\beta) = r^p N(\beta)$ is dus ook geen q^{de} macht. Door $\beta' = r\beta$ te nemen, zitten we in het geval $\sqrt[q]{\beta'}$, $\sqrt[q]{N(\beta')} \notin K$ en krijgen we

$$\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{r\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{r^p N(\beta)}).$$

Hier Lemma 2.15 met $\tau_{r^{-1}}$ op toepassen geeft $\mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{\beta}) = \mathbb{Q}(\sqrt[p]{\alpha}, \sqrt[q]{N(\beta)})$.

iii) $\implies$ *iv)*: Als $L = K$, dan is $\mathrm{Gal}(L/K) = \{\mathrm{id}\}$. Als $L = K(\zeta_q, \sqrt[q]{\beta})$, dan volgt $\mathrm{Gal}(L/K) \cong W_q$ uit Propositie 3.3.

iv) $\implies$ *iii)*: Als $\mathrm{Gal}(L/K) = \{\mathrm{id}\}$, dan $L = K$. $\mathrm{Gal}(L/K) \cong W_q \implies [L : K] = q(q-1)$. Verder weten we dat $K(\zeta_q, \sqrt[q]{\beta}) \subseteq L$ en $[K(\zeta_q, \sqrt[q]{\beta}) : K] = q(q-1)$, dus

$$[L : K(\zeta_q, \sqrt[q]{\beta})] = \frac{[L : K]}{[K(\zeta_q, \sqrt[q]{\beta}) : K]} = \frac{q(q-1)}{q(q-1)} = 1 \implies L = K(\zeta_q, \sqrt[q]{\beta}). \quad \square$$

Stelling 4.6. *De volgende beweringen zijn equivalent:*

i) $\sqrt[q]{\beta} \in \mathbb{Q}^{(1)}$,

ii) $\mathrm{Gal}(L/\mathbb{Q})'' = \{\mathrm{id}\}$,

iii) $\exists c \in \mathbb{Q}, \gamma \in \mathbb{Q}(\sqrt[p]{\alpha}) : \beta = c\gamma^q$.

Bewijs. *i)* $\implies$ *ii)*: Analoog met *i)* $\implies$ *ii)* van Stelling 3.10.

ii) $\implies$ *iii)*: Propositie 3.8 geeft samen met Lemma 3.9 dat $\exists r \in \mathbb{Z} : \sqrt[q]{\beta N(\beta)^r} \in \mathbb{Q}(\sqrt[p]{\alpha})$, oftewel $\exists \gamma \in \mathbb{Q}(\sqrt[p]{\alpha}) : \gamma^q = \beta N(\beta)^r$. Dus $\beta = N(\beta)^{-r}\gamma^q$.

iii) $\implies$ *i)*: $\sqrt[q]{\beta} = \sqrt[q]{c}\gamma \in \mathbb{Q}^{(1)}$. □

Net als in het vorige hoofdstuk, zien we dat wortels $\sqrt[q]{\beta}$ die ontnestbaar zijn, altijd op een flauwe manier ontnestbaar zijn, omdat β op een rationaal getal na altijd een q^{de} macht is in $\mathbb{Q}(\sqrt[p]{\alpha})$. Daarnaast weten we wat de c is, namelijk $c = \frac{1}{N(\beta)^r}$, waarbij we r kunnen bepalen door de inverse van p modulo q te berekenen. Om te testen of $\sqrt[q]{\beta}$ ontnestbaar is, hoeven we dus alleen nog te kijken of $\frac{\beta}{N(\beta)^r}$ een q^{de}-macht is in $\mathbb{Q}(\sqrt[p]{\alpha})$. Dit is eenvoudig te doen met een computeralgebrasysteem.

5 Ontnestbare vierkantswortels in een kwadratische uitbreiding van $\mathbb{Q}$

In de vorige hoofdstukken hebben we ons beperkt tot oneven priemgetallen p. Het liefst willen we een zo algemeen mogelijk resultaat hebben en $p = 2$ niet uitsluiten, daarom gaan we in dit hoofdstuk naar wortels van dezelfde vorm als in hoofdstuk 3, maar dan met $p = 2$. Dat betekent dat in dit hoofdstuk:

- $\alpha \in \mathbb{Q}$ geen kwadraat,
- $\beta \in \mathbb{Q}(\sqrt{\alpha})\backslash\mathbb{Q}$,
- $N(x) = N_{\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}}(x)$ voor $x \in \mathbb{Q}(\sqrt{\alpha})$,
- $K = \mathbb{Q}(\beta)^{\text{norm}} = \mathbb{Q}(\beta)$,
- $L = \mathbb{Q}(\sqrt{\beta})^{\text{norm}}$.

Om te beginnen, kijken we naar een voorbeeld dat laat zien dat hoofdstuk 3 inderdaad alleen opgaat voor oneven p.

Voorbeeld 5.1. Een van de gevolgen van Lemma 3.9 en Stelling 3.10 is dat, als $N(\beta)$ een kwadraat is, $\sqrt{\beta}$ ontnestbaar is $\iff$ β is een kwadraat in K. Om een tegenvoorbeeld te vinden, gaan we dus opzoek naar een β, die geen kwadraat is, maar waarvan de norm wel een kwadraat is. Voor het gemak nemen we $\alpha = 2$. Dus $\beta = a + b\sqrt{2}$ en $N(\beta) = a^2 - 2b^2$. Als we $\beta = 9 + 6\sqrt{2}$ nemen, hebben we $N(\beta) = 81 - 72 = 3^2$.

Stel β is een kwadraat in $K = \mathbb{Q}(\sqrt{2})$. Dan zijn er $a, b \in \mathbb{Q}$ zodat

$$(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} = 9 + 6\sqrt{2}.$$

Dus $b = 3a^{-1}$ en $a^2 + 18a^{-2} - 9 = 0$. Oftewel $a^4 - 9a^2 + 18 = 0$. Dit heeft als oplossing $a^2 = \frac{9 \pm \sqrt{81-72}}{2} = \frac{9 \pm 3}{2}$. Dus $a^2 = 6$ of $a^2 = 3$, maar dat kan niet in $\mathbb{Q}$. β is dus geen kwadraat in K. Toch zien we dat $\sqrt{b}$ wel ontnestbaar is, want als we $a = \sqrt{3}$ nemen, krijgen we

$$(\sqrt{3} + \sqrt{6})^2 = 3 + 6 + 2\sqrt{18} = 9 + 6\sqrt{2} = \beta.$$

We zien zo zelfs dat alle $\beta \in K(\sqrt{\alpha})$ met $N(\beta)$ een kwadraat ontnestbaar zijn.

Propositie 5.2. *Zij $\beta = a + b\sqrt{\alpha}$ en $N(\beta) = a^2 - \alpha b^2$ de norm van β. Als $N(\beta)$ een kwadraat is, dan is $\sqrt{\beta}$ ontnestbaar.*

Bewijs. We zoeken c, d zodat

$$(c + d\sqrt{\alpha})^2 = c^2 + \alpha d^2 + 2cd\sqrt{\alpha} = a + b\sqrt{\alpha}.$$

Zo vinden we $2cd = b$ oftewel $d = \frac{b}{2}c^{-1}$. Dit invullen in $c^2 + \alpha d^2 = a$ geeft

$$c^2 + \frac{b^2\alpha}{4}c^{-2} - a = 0.$$

Door dit te vermenigvuldigen met c^2 krijgen we $c^4 - ac^2 + \frac{b^2\alpha}{4} = 0$ en vinden we de oplossingen

$$c^2 = \frac{a \pm \sqrt{a^2 - \alpha b^2}}{2} = \frac{a \pm \sqrt{N(\beta)}}{2}.$$

Dus we kunnen $c = \sqrt{\frac{a+N(\beta)}{2}}$ nemen. Met

$$\begin{aligned}\sqrt{\frac{a+N(\beta)}{2}}\sqrt{\frac{a-N(\beta)}{2}} &= \frac{1}{2}\sqrt{a^2 - +N(\beta)^2} \\ &= \frac{1}{2}\sqrt{a^2 - (a^2 - b^2\alpha)} = \frac{1}{2}b\sqrt{\alpha}\end{aligned}$$

krijgen we $\sqrt{\frac{a-N(\beta)}{2}} = \frac{b\sqrt{\alpha}}{2c}$. Samen met $d = \frac{b}{2c}$ geeft dit

$$\sqrt{\beta} = c + d\sqrt{\alpha} = \sqrt{\frac{a+N(\beta)}{2}} + \sqrt{\frac{a-N(\beta)}{2}} \in \mathbb{Q}^{(1)}. \qquad \square$$

Als $N(\beta)$ geen kwadraat is, kunnen we het bewijs van Lemma 3.9 aanpassen, door niet via i) te gaan.

Lemma 5.3. *Zij $\beta = a + b\sqrt{\alpha}$, $N(\beta) = a^2 - \alpha b^2$, $L = \mathbb{Q}(\sqrt{\beta})^{\text{norm}}$ en $K = \mathbb{Q}(\beta)^{\text{norm}}$. Als $N(\beta)$ geen kwadraat is, dan zijn de volgende beweringen equivalent:*

i) $K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$,

ii) $L = K(\sqrt{\beta})$,

iii) $[L : K] \leq 2$.

Bewijs. *i)* $\implies$ *ii)*: $K(\sqrt{\beta}) = K(\sqrt{N(\beta)}) = \mathbb{Q}(\zeta_p, \beta, \sqrt{N(\beta)})$ is normaal over $\mathbb{Q}$ want het is het ontbindingslichaam van $f_{\mathbb{Q}}^{\beta} \cdot f_{\mathbb{Q}}^{\sqrt{N(\beta)}}$. Daarom is $L \subseteq K(\sqrt{\beta})$. Bovendien is $K(\sqrt{\beta}) \subseteq L$.

ii) $\implies$ *i)*: $[L : K] = [K(\sqrt{\beta}) : K] = 2$ en $[K(\sqrt{N(\beta)}) : K] = 2$, dus

$$[L : K(\sqrt{N(\beta)})] = \frac{[L : K]}{[K(\sqrt{N(\beta)}) : K]} = \frac{2}{2} = 1,$$

dus $K(\sqrt{\beta}) = L = K(\sqrt{N(\beta)})$.

i) $\iff$ *iii)* gaat op dezelfde manier als bij Lemma 3.9. $\square$

Helaas kunnen we dit aangepaste lemma niet direct gebruiken om een variant van Stelling 3.10 te bewijzen omdat Propositie 3.8 niet geldt voor $p = 2$. Toch kunnen we wel wat zeggen over de ontnestbaarheid van $\sqrt{\beta}$ als $N(\beta)$ geen kwadraat is.

Lemma 5.4. *Zij $\beta = a + b\sqrt{\alpha}$, $N(\beta) = a^2 - \alpha b^2$ en $K = \mathbb{Q}(\beta)^{\text{norm}}$. Als $N(\beta)$ geen kwadraat is in $\mathbb{Q}$, dan $K(\sqrt{\beta}) \neq K(\sqrt{N(\beta)})$.*

Bewijs. Stel $K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$. Omdat $N(\beta)$ geen kwadraat is in $\mathbb{Q}$, is β geen kwadraat in K. Dus $K \neq K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$ en $N(\beta)$ is dus ook geen kwadraat in K. $\beta \in K(\sqrt{\beta}) = K(\sqrt{N(\beta)})$ dus er zijn $a, b \in K$ zodat

$$(a + b\sqrt{N(\beta)})^2 = a^2 + N(\beta)b^2 + 2ab\sqrt{N(\beta)} = \beta = c + d\sqrt{\alpha}.$$

$2ab = 0 \implies a = 0$ of $b = 0$.
Als $b = 0$ dan $a^2 = \beta$, maar dat kan niet omdat β geen kwadraat is in K.
Als $a = 0$, dan $N(\beta)b^2 = \beta$. We schrijven $b = b_0 + b_1\sqrt{\alpha}$ en krijgen

$$N(\beta)b_0^2 + N(\beta)\alpha b_1^2 + 2b_0b_1\sqrt{\alpha} = c + d\sqrt{\alpha}.$$

Dit geeft $b_1 = \frac{d}{2b_0N(\beta)}$. Hiermee krijgen we $N(\beta)b_0^4 - cb_0^2 + \frac{\alpha d^2}{4N(\beta)} = 0$ en vinden we de oplossingen

$$b_0^2 = \frac{c \pm \sqrt{c^2 - \alpha d^2}}{2N(\beta)} = \frac{c \pm \sqrt{N(\beta)}}{2N} \in \mathbb{Q} \iff \sqrt{N(\beta)} \in \mathbb{Q}.$$

Aangezien $N(\beta)$ geen kwadraat is, heeft dit geen oplossingen. Dus $K(\sqrt{\beta}) \neq K(\sqrt{N(\beta)})$. □

Propositie 5.5. *Als $\beta = x + y\sqrt{\alpha}$ en $N(\beta) = x^2 - \alpha y^2$ geen kwadraat dan is $\sqrt{\beta}$ ontnestbaar $\iff$ $y^2 - \frac{x^2}{\alpha}$ is een kwadraat.*

Bewijs. Als $\sqrt{\beta}$ ontnestbaar is, dan $\mathbb{Q}(\sqrt{\beta}) \subseteq \mathbb{Q}^{(1)}$, dus $\mathbb{Q}(\sqrt{\beta}) = \mathbb{Q}(a_1, ..., a_n)$ met $a_i^{m_i} \in \mathbb{Q}$. Omdat $[\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\beta}) : K][K : \mathbb{Q}] = 2 \cdot 2 = 4$ zijn hier 2 mogelijkheden voor: $\mathbb{Q}(\sqrt{\beta}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ of $\mathbb{Q}(\sqrt{\beta}) = \mathbb{Q}(\sqrt[4]{a})$. In het eerste geval is $L = \mathbb{Q}(\sqrt{\beta})^{\text{norm}} = \mathbb{Q}(\sqrt{a}, \sqrt{b})^{\text{norm}} = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ en dus $[L : K] = 2$. Dit is een tegenspraak met Lemma 5.3 en Lemma 5.4.

In het tweede geval hebben we $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(\sqrt[4]{a})$. Dit kan alleen als $\mathbb{Q}(\sqrt[4]{a}) = \mathbb{Q}(\sqrt{\alpha})$ oftewel als $a = k^2\alpha$.

Hieruit volgt

$$\sqrt{\beta} \text{ is ontnestbaar} \iff \exists a, b, c, d, k \in \mathbb{Q} : (a + b\sqrt[4]{k^2\alpha} + kc\sqrt{\alpha} + kd\sqrt[4]{k^2\alpha^3})^2 = x + y\sqrt{\alpha}.$$

Oftewel:

$$\begin{aligned} a^2 + k^2\alpha c^2 + 2k^2\alpha bd &= x, \\ k(b^2 + k^3\alpha d^2 + 2kac) &= y, \\ 2(ab + k^2\alpha cd) &= 0, \\ 2k(ad + bc) &= 0. \end{aligned}$$

Als $d = 0$ dan $ab = 0$ en $bc = 0$, dus $d = b = 0$ of $a = c = 0$.

Als $d \neq 0$ dan $a = \frac{-bc}{d} \implies b^2c = \alpha cd^2 \implies c = 0$ of $b^2 = k^2\alpha d^2$. Dit laatste kan niet omdat $d \neq 0, k \neq 0$ en α geen kwadraat, dus $a = \frac{-bc}{d} = 0 = c$.

Voor een oplossing geldt dus ofwel $a = c = 0$ of $b = d = 0$. Als $b = d = 0$ wordt de vergelijking $(a + kc\sqrt{\alpha})^2 = x + y\sqrt{\alpha}$. Dit heeft alleen oplossingen als β een kwadraat is in K, maar $N(\beta)$ is geen kwadraat dus dit kan niet. Hierdoor hebben we

$$\sqrt{\beta} \text{ is ontnestbaar } \iff \exists b, d, k \in \mathbb{Q} : (b\sqrt[4]{k^2\alpha} + kd\sqrt[4]{k^2\alpha^3})^2 = x + y\sqrt{\alpha}.$$

Oftewel $2k^2\alpha bd = x$ en $b^2 + k^2\alpha d^2 = \frac{y}{k}$.

Als $x = 0$ dan is $y^2 - \frac{x^2}{\alpha} = y^2$ een kwadraat en is $b = 1, d = 0, k = y$ een oplossing.

Als $x \neq 0$ dan $b \neq 0$ en $d = \frac{x}{2k^2\alpha b}$. Dit invullen in de andere vergelijking geeft $b^2 - \frac{y}{k} + \frac{x^2}{4k^2\alpha b^2} = 0$, oftewel $b^4 - \frac{y}{k}b^2 + \frac{x^2}{4k^2\alpha} = 0$. Oplossingen hiervoor worden gegeven door

$$b^2 = \frac{\frac{y}{k} \pm \sqrt{\frac{y^2}{k^2} - \frac{x^2}{k^2\alpha}}}{2} = \frac{y \pm \sqrt{y^2 - \frac{x^2}{\alpha}}}{2k}$$

en dit heeft alleen oplossingen in $\mathbb{Q}$ als $y^2 - \frac{x^2}{\alpha}$ een kwadraat is. Als dit zo is, is een oplossing $b = 1, k = \frac{y+\sqrt{y^2-\frac{x^2}{\alpha}}}{2}, d = \frac{x}{2k^2\alpha b}$. □

Referenties

[1] Antipov, M. A., and Pimenov, K. I. Ramanujan Denesting Formulas for Cubic Radicals. *Vestnik St. Petersburg University, Mathematics 53* (2020), 115–221.

[2] Berndt, B., Choi, Y.-S., and Kang, S.-Y. The Problems Submitted by Ramanujan to the Journal of the Indian Mathematical Society. *Contemporary Mathematics 236* (1999), 15–56.

[3] Blömer, J. How to denest Ramanujan's nested radicals. In *Proceedings., 33rd Annual Symposium on Foundations of Computer Science* (1992), pp. 447–456.

[4] Honsbeek, M. *Radical extensions and Galois groups*. PhD thesis, Radboud Universiteit Nijmegen, 2005.

[5] Landau, S. Simplification of Nested Radicals. *SIAM Journal on Computing 21* (1992), 85–110.

[6] Stevenhagen, P. Algebra III. Course Reader, 2012. `http://websites.math.leidenuniv.nl/algebra/algebra3.pdf`.

[7] Thijssen, S. *Denesting Conditions*. Bachelor thesis, Radboud Universiteit Nijmegen, 2008. `https://www.math.ru.nl/~bosma/Students/SepThijssen/SepBScThesis.pdf`.

[8] Washington, L. C. *Introduction to cyclotomic fields*, vol. 83. Springer Science & Business Media, 1997.