Elisabeth Johanna Leijten
ejleijten@gmail.com

Complexe vermenigvuldiging en transferafbeeldingen

Scriptiebegeleider: Dr. Marco Streng

Bachelorscriptie

Faculteit der Wiskunde en Natuurwetenschappen
Universiteit Leiden
Nederland
7 juli 2023

Inhoudsopgave

1 Inleiding **3**

2 Complexe vermenigvuldiging **6**
2.1 CM-lichamen 6
2.2 CM-typen 10

3 Classificatie van Galoisgroepen van CM-lichamen **13**
3.1 CM-lichamen van graad twee 13
3.2 CM-lichamen van graad vier 13
3.3 CM-lichamen van graad zes 15

4 Classificatie van CM-typen **19**
4.1 CM-lichamen van graad twee 19
4.2 CM-lichamen van graad vier 19
4.3 CM-lichamen van graad zes 21

5 Transferafbeelding **23**

6 Reflex-typen **29**

7 Referenties **33**

1. Inleiding

Dit onderzoek is onderverdeeld in vier delen. Deze zullen achtereenvolgens samengevat worden in deze inleiding.

Eerst bepalen we alle mogelijke Galoisgroepen van *CM-lichamen* van graad 2, 4 en 6 op isomorfie na. (De afkorting CM staat voor *Complex Multiplication* dat Engels is voor *Complexe Vermenigvuldiging*.)

Definitie 1.1. Een *CM-lichaam* K is een getallenlichaam, oftewel een eindige uitbreiding van $\mathbf{Q}$, zo dat er een $\mathrm{id} \neq \rho \in \mathrm{Aut}(K)$ bestaat met $(\varphi \circ \rho)(x) = \overline{\varphi(x)}$ voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en alle $x \in K$.

We beschouwen CM-lichamen van graad 2, 4 en 6, omdat dit de kleinst mogelijke CM-lichamen zijn; CM-lichamen hebben namelijk altijd een even graad over hun grondlichaam $\mathbf{Q}$. In paragraaf 2 zullen we uitgebreider ingaan op deze definitie en andere eigenschappen van CM-lichamen. De classificatie van Galoisgroepen van CM-lichamen van graad 2, 4 en 6 vatten we hieronder in een tabel samen en bespreken we uitgebreider in paragraaf 3.

graad	normaal	niet normaal
2	C_2	$-$
4	V_4, C_4	D_4
6	C_6	$D_6, C_2^3 \rtimes C_3, C_2^3 \rtimes S_3$

Tabel 1: Galoisgroepen bij CM-lichamen van graad 2, 4 en 6.

In het tweede deel van deze scriptie beschouwen we *CM-typen*.

Definitie 1.2. Een *CM-type* Φ van een CM-lichaam K van graad $2n$ is een deelverzameling van $\mathrm{Hom}(K, \mathbf{C})$ zodanig dat $\Phi \cup \overline{\Phi} = \mathrm{Hom}(K, \mathbf{C})$ en $|\Phi| = n$, oftewel $\Phi \cap \overline{\Phi} = \emptyset$.

Een CM-lichaam van graad $2n$ heeft 2^n verschillende *CM-typen*. We zullen ons vooral richten op *primitieve* CM-typen.

Definitie 1.3. Laat K, L twee CM-lichamen zijn waarvoor geldt $K \subseteq L$. Zij Φ een CM-type van K, dan heet

$$\Phi_L = \{(\varphi : L \to \mathbf{C}) : \varphi|_K \in \Phi\}$$

het CM-type van L *geïnduceerd* door Φ. Een CM-type Φ' van L heet *primitief* als er geen CM-lichaam $K \subsetneq L$ en CM-type Φ van K bestaan met $\Phi' = \Phi_L$.

Zij K een CM-lichaam met Galoisgroep G. Laat Φ een CM-type van K zijn. In paragraaf 2.2 bewijzen we dat Φ primitief is dan en slechts dan als $g\Phi$ primitief is voor alle $g \in G$. In paragraaf 4 bepalen we de CM-typen van CM-lichamen van graad 2, 4 en 6 aan de hand van hun Galoisgroep. Verder stellen we vast of ze primitief zijn en bepalen hun baan onder linksvermenigvuldiging met G. De volgende tabel bevat kort de resultaten.

graad	Galoisgroep	primitieve CM-typen
2	C_2	één baan met twee CM-typen
4	V_4	-
4	C_4	één baan met vier CM-typen
4	D_4	één baan met vier CM-typen
6	C_6	één baan met zes CM-typen
6	D_6	één baan met zes CM-typen
6	$C_2^3 \rtimes C_3$	één baan met acht CM-typen
6	$C_2^3 \rtimes S_3$	één baan met acht CM-typen

Tabel 2: Primitieve CM-typen van CM-lichamen van graad 2, 4 en 6.

Als derde zullen we de theorie van de complexe vermenigvuldiging loslaten en een algemeen getallenlichaam L beschouwen dat Galois is over $\mathbf{Q}$. Zij G de Galoisgroep van L en $H_1, H_2 \subseteq G$ twee ondergroepen van G. De ondergroepen H_1 en H_2 corresponderen respectievelijk met deellichamen K_1 en K_2 van L. We beschouwen deze lichamen in combinatie met de groepenring $\mathbf{Z}[G]$. De groepen L^* en $(L,+)$ zijn beide $\mathbf{Z}[G]$-modulen. Via de moduulstructuur geven elementen uit $\mathbf{Z}[G]$ aanleiding tot endomorfismen uit $\mathrm{End}(L^*)$ en $\mathrm{End}((L,+))$. We definiëren de groep

$$T(H_1, H_2) := {}^{H_2}\big(\mathbf{Z}[G]/\,\mathrm{I}(H_1)\big) \tag{1}$$

als analogon van $\mathbf{Z}[G]$. Dat wil zeggen dat we aan de hand van $T(H_1, H_2)$ elementen uit $\mathrm{Hom}(K_1^*, K_2^*)$ en $\mathrm{Hom}((K_1,+),(K_2,+))$ zullen vormen. De manier waarop we dat zullen doen is analoog aan de wijze waarop aan de hand van $\mathbf{Z}[G]$ elementen uit $\mathrm{End}(L^*)$ en $\mathrm{End}((L,+))$ gevormd worden. Daarnaast stelt deze constructie ons in staat om een samenstelling te definiëren tussen elementen uit $T(H_0, H_1)$ en $T(H_1, H_2)$, hierbij is $H_0 \subseteq G$ een ondergroep van G. We geven hier een korte uitleg van

de betekenis van de notatie in (1). Het linksideaal $\mathrm{I}(H_1) \subseteq \mathbf{Z}[G]$ wordt voortgebracht door de verzameling $\{h - 1 : h \in H_1\}$. Het quotiënt $\mathbf{Z}[G]/\mathrm{I}(H_1)$ is het quotiënt van een moduul met een deelmoduul. Er kan worden aangetoond dat H_2 een werking heeft op dit quotiënt. De groep in (1) is de groep van vaste punten onder deze werking. Dit wordt aangegeven door H_2 aan de linkerkant van $\mathbf{Z}[G]/\mathrm{I}(H_1)$ als bovenschrift te schrijven. De groep $T(H_1, H_2)$ wordt in paragraaf 5 uitvoeriger besproken.

Als laatste keren we terug naar de CM-lichamen. We zullen het *reflex-type* van een CM-type beschouwen. We maken hierbij de aanname dat de CM-lichamen die we beschouwen bevat zijn in $\mathbf{C}$.

Definitie 1.4. Zij $L \subseteq \mathbf{C}$ de normale afsluiting van een CM-lichaam K en G de Galoisgroep van K. Laat Φ een CM-type van K zijn en Φ_L het CM-type van L geïnduceerd door Φ zijn. Laat $H^r = \{g \in G : g\Phi = \Phi\}$ zijn en $K^r = L^{H^r}$ zijn. Het *reflex-type* Φ^r van Φ is

$$\Phi^r = \{\varphi^{-1}|_{K^r} : \varphi \in \Phi_L\}.$$

In paragraaf 6 leggen we uit hoe we Φ^r kunnen beschouwen als een element $\tilde{\Phi}^r \in T(H^r, H)$. Laat $H \subseteq G$ de ondergroep van G zijn die correspondeert met K. We beschouwen de ondergroep

$$\mathcal{G}_\Phi = \tilde{\Phi}^r \circ T(H, H^r) + \mathbf{Z} \cdot \sum_{gH \in G/H} (g + \mathrm{I}(H)) \subseteq T(H, H).$$

Er kan eenvoudig worden bewezen dat $\overline{\mathrm{id}} - \overline{\rho} \in T(H, H)$. De volgende stelling geeft aan voor welke primitieve CM-typen uit tabel 2 geldt dat $\overline{\mathrm{id}} - \overline{\rho} \in \mathcal{G}_\Phi$. De stelling wordt in paragraaf 6 bewezen.

Stelling 1.5. *De groep $\mathcal{G}_\Phi$ bevat het element $\overline{\mathrm{id}} - \overline{\rho} \in T(H, H)$ voor alle primitieve CM-typen van CM-lichamen van graad 2 en 4 en voor CM-lichamen van graad 6 als de Galoisgroep van dit lichaam isomorf is aan C_6 of D_6, maar niet voor de primitieve CM-typen van CM-lichamen met Galoisgroep isomorf aan $C_2^3 \rtimes C_3$ of $C_2^3 \rtimes S_3$.*

De resultaten uit dit onderzoek kennen hun toepassing vooral in de theorie rondom abelse variëteiten. Echter ging deze theorie te ver voor deze scriptie, maar de volgende bronnen bevatten meer informatie over de toepassingen: [9, Theorem I.10.3 op p.36] en [1, Proposition 1.3.12 op p.358]. Daarnaast komt specifieke vraag of $\overline{\mathrm{id}} - \overline{\rho}$ bevat is in $\mathcal{G}_\Phi$ uit de derde versie (die op dit moment nog niet gepubliceerd is) van [3, Proposition 5.3 en Equation (5.1)].

2. Complexe vermenigvuldiging

Deze paragraaf bevat de achtergrondinformatie over de theorie van de complexe vermenigvuldiging die nodig is bij dit onderzoek. Het boek *Abelian Varieties with Complex Multiplication and Modular Functions* van G. Shimura, dat in de paragraaf met referenties genoemd is onder [5], vormt de basis voor deze paragraaf.

2.1. CM-lichamen

Om te beginnen geven we drie definities van zogeheten *Complexe Vermenigvuldigingslichamen*, afgekort *CM-lichamen*. De afkorting *CM* komt van het Engelse *Complex Multiplication*. In deze drie definities maken we gebruik van de volgende definitie.

Definitie 2.1. Een *getallenlichaam* K_0 is een lichaamsuitbreiding van $\mathbf{Q}$ met $[K_0 : \mathbf{Q}] < \infty$. Een getallenlichaam K_0 heet *totaal reëel* als voor alle $\varphi \in \mathrm{Hom}(K_0, \mathbf{C})$ geldt dat $\varphi(K_0) \subseteq \mathbf{R}$. Een getallenlichaam K_0 heet *totaal niet-reëel* als voor alle $\varphi \in \mathrm{Hom}(K_0, \mathbf{C})$ geldt dat $\varphi(K_0) \nsubseteq \mathbf{R}$.

Nu volgen de drie definities van *CM-lichamen* en aansluitend bewijzen we dat ze equivalent zijn. Definitie 2.2 is gelijk aan definitie 1.1 uit de inleiding (paragraaf 1).

Definitie 2.2. Een *CM-lichaam* K is een getallenlichaam zodat er een $\mathrm{id} \neq \rho \in \mathrm{Aut}(K)$ bestaat met $(\varphi \circ \rho)(x) = \overline{\varphi(x)}$ voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en alle $x \in K$.

Definitie 2.3. Een *CM-lichaam* K is een getallenlichaam waarvoor geldt dat $K \cong K_0(\sqrt{d})$ voor een totaal reëel deellichaam $K_0 \subseteq K$ en $d \in K_0$ met $\varphi(d) < 0$ voor alle $\varphi \in \mathrm{Hom}(K_0, \mathbf{R})$.

Definitie 2.4. Een *CM-lichaam* K is een totaal niet-reëel getallenlichaam dat een totaal reëel deellichaam $K_0 \subseteq K$ bevat waarvoor geldt dat $[K : K_0] = 2$.

Stelling 2.5. *Definities 2.2, 2.3, 2.4 zijn equivalent.*

Bewijs. **2.2 $\Rightarrow$ 2.4**. Het lichaam K is een getallenlichaam. We zullen uit tegenspraak bewijzen dat K totaal niet-reëel is. Stel dat K niet totaal

niet-reëel is, dan geldt dat er een $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ bestaat met $\varphi(K) \subseteq \mathbf{R}$. Wegens definitie 2.2 geldt ook dat $(\varphi \circ \rho)(x) = \overline{\varphi(x)}$ voor alle $x \in K$ en vanwege onze aanname geldt $\overline{\varphi(x)} = \varphi(x)$ voor alle $x \in K$. Uit de injectiviteit van φ volgt dat $\rho = \mathrm{id}$, wat een tegenspraak oplevert. We bewijzen nu dat $\rho^2 = \mathrm{id}$. Zij $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en $x \in K$, dan geldt dat

$$\varphi(\rho(\rho(x))) = \overline{\varphi(\rho(x))} = \overline{\overline{\varphi(x)}} = \varphi(x).$$

Omdat φ injectief is, volgt hieruit dat $\rho^2 = \mathrm{id}$. Omdat $\rho \neq \mathrm{id}$ volgt dat ρ orde twee heeft in $\mathrm{Aut}(K)$. Laat $K_0 = K^{\langle \rho \rangle}$ zijn, dan geldt $[K : K_0] = 2$. (Zie [8, definitie 24.1 en stelling 24.4.1 op p.45-46].) Laat $x \in K_0$ zijn, dan geldt dat $\rho(x) = x$ en dus $(\varphi \circ \rho)(x) = \varphi(x) = \overline{\varphi(x)}$ voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$. Omdat K_0 een deellichaam is van K volgt hieruit dat ook voor $\varphi \in \mathrm{Hom}(K_0, \mathbf{C})$ geldt dat $\varphi(x) = \overline{\varphi(x)}$. Als er nu een $x \in K_0$ zou bestaan met $\varphi(x) \in \mathbf{C} \backslash \mathbf{R}$, dan geeft dit een tegenspraak. Zo volgt dat K_0 aan definitie 2.1 van een totaal reëel lichaam voldoet.

2.4 ⇒ 2.3. Het lichaam K is een getallenlichaam en K_0 uit definitie 2.4 is totaal reëel. We zullen bewijzen dat $K \cong K_0(\sqrt{d})$ voor $d \in K_0$ met $\varphi(d) < 0$ voor alle $\varphi \in \mathrm{Hom}(K_0, \mathbf{R})$. Hiertoe beschouwen we het minimumpolynoom f van K over K_0. Per definitie is dit een monisch polynoom van graad 2 in $K_0[X]$ en daarmee van de vorm $f(X) = X^2 + aX + b$, $a, b \in K_0$. Laat α een nulpunt zijn van f, dan geldt dat $\beta = \alpha + \frac{1}{2}a$ een nulpunt is van $f(X - \frac{1}{2}a) = X^2 - (\frac{1}{4}a^2 - b)$. Er geldt $K_0(\alpha) = K_0(\beta)$ en we beschouwen vanaf nu $K_0(\beta)$. Als we een willekeurige $\varphi \in \mathrm{Hom}(K_0, \mathbf{R})$ beschouwen, kunnen we deze voortzetten tot een inbedding van $K \cong K_0(\beta)$ in $\mathbf{C}$ door

$$\beta \mapsto \pm\sqrt{\varphi(\tfrac{1}{4}a^2 - b)}$$

te nemen. Stel nu dat $\varphi(\frac{1}{4}a^2 - b) \geq 0$, dan geldt dat de voortzetting van φ bevat is in $\mathbf{R}$, maar dan zou K geen totaal niet-reëel lichaam zijn, dus dit geeft een tegenspraak.

2.3 ⇒ 2.2. Het lichaam K is een getallenlichaam. Laat $\rho \in \mathrm{Aut}(K)$ zijn zodanig dat $\rho(\sqrt{d}) = -\sqrt{d}$ en $\rho|_{K_0} = \mathrm{id}$. Zij $x = a + b\sqrt{d} \in K$ met $a, b \in K_0$ en $\varphi \in \mathrm{Hom}(K, \mathbf{C})$. We zullen bewijzen dat $(\varphi \circ \rho)(x) = \overline{\varphi(x)}$. Er geldt

$$(\varphi \circ \rho)(x) = \varphi(a - b\sqrt{d}) = \varphi(a) - \varphi(b)\varphi(\sqrt{d})$$

en

$$\overline{\varphi(x)} = \overline{\varphi(a) + \varphi(b)\varphi(\sqrt{d})} = \varphi(a) + \varphi(b)\overline{\varphi(\sqrt{d})}.$$

Het volstaat dus om te bewijzen dat $-\varphi(\sqrt{d}) = \overline{\varphi(\sqrt{d})}$. Er is gegeven dat $\varphi(d) < 0$ (en $\varphi(d) \in \mathbf{R}$). Er geldt dus dat $\varphi(\sqrt{d}) \in i\mathbf{R}$ waaruit volgt dat $-\varphi(\sqrt{d}) = \overline{\varphi(\sqrt{d})}$. □

Het volgende voorbeeld illustreert de definities van een CM-lichaam.

Voorbeeld 2.6. Het lichaam $K = \mathbf{Q}(i) \subseteq \mathbf{C}$ is een CM-lichaam. In dit voorbeeld zullen we laten zien dat het aan de drie definities 2.2, 2.3 en 2.4 voldoet. Elk van de drie definities eist dat K een getallenlichaam is en daar wordt door K aan voldaan. De Galoisgroep $G = \mathrm{Gal}(K/\mathbf{Q}) = \{\mathrm{id}, \rho\}$ met id de identiteitsafbeelding en $\rho : K \to K; i \mapsto -i$.

1. We beschouwen definitie 2.2. Er geldt $\rho \neq \mathrm{id}$ en voor de automorfismen uit G geldt $(\mathrm{id} \circ \rho)(x) = \overline{\mathrm{id}(x)}$ en $(\rho \circ \rho)(x) = \overline{\rho(x)}$ voor alle $x \in K$.

2. Vervolgens zullen we nagaan dat K voldoet aan definitie 2.3. Het grondlichaam $\mathbf{Q}$ is totaal reëel en $K = \mathbf{Q}(i) = \mathbf{Q}(\sqrt{-1})$. Er geldt dat $\mathrm{Hom}(\mathbf{Q}, \mathbf{R})$ uit één element id bestaat en $\mathrm{id}(-1) = -1 < 0$.

3. We beschouwen als laatste definitie 2.4. Er geldt $[K : \mathbf{Q}] = 2$. Het lichaam $\mathbf{Q}$ is totaal reëel, maar K is totaal niet-reëel, want voor alle elementen $\varphi \in G$ geldt dat $i \in \varphi(K)$, dus $\varphi(K) \nsubseteq \mathbf{R}$.

Vervolgens geven we lemma's en een stelling die betrekking hebben op CM-lichamen.

Lemma 2.7. *Laat K een CM-lichaam zijn en zij $\rho \in \mathrm{Aut}(K)$ zodanig dat $(\varphi \circ \rho)(x) = \overline{\varphi(x)}$ voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en $x \in K$. Dan geldt dat ρ is bevat in het centrum van $\mathrm{Aut}(K)$.*

Bewijs. Laat $g \in \mathrm{Aut}(K)$ zijn, dan geldt voor $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en alle $x \in K$, dat

$$\varphi(\rho(g(x))) = \overline{\varphi(g(x))} = \varphi(g(\rho(x))).$$

Uit de injectiviteit van φ volgt $\rho(g(x)) = g(\rho(x))$ voor alle $g \in \mathrm{Aut}(K)$ en $x \in K$, oftewel ρ zit in het centrum van $\mathrm{Aut}(K)$. □

Stelling 2.8. *Zij $L \supseteq \mathbf{Q}$ een lichaam en $K_i \subseteq L$ voor alle $i \in \{1, 2, ..., n\}$, $n \in \mathbf{N}$ een CM-lichaam of een totaal reëel getallenlichaam, dan geldt dat ook het compositum $K_1 \cdot K_2 \cdot ... \cdot K_n := \mathbf{Q}(K_1 \cup K_2 \cup ... \cup K_n)$ een CM-lichaam is als minstens één van de K_i $i \in \{1, 2, ..., n\}$ een CM-lichaam is, anders is het compositum totaal reëel.*

Bewijs. Het is voldoende om te bewijzen dat voor twee dergelijke lichamen geldt dat het compositum weer een CM-lichaam of totaal reëel lichaam is.

Zij K_i, $i \in \{1,2\}$ een CM-lichaam of een totaal reëel lichaam. Zij $\varphi_0 : K_1 \cdot K_2 \to \mathbf{C}$ een homomorfisme. We definiëren

$$\begin{aligned} \rho_0 : K_1 \cdot K_2 &\to \mathbf{C} \\ x &\mapsto \overline{\varphi_0(x)}. \end{aligned}$$

We zullen bewijzen dat $\rho_0(K_i) \subseteq \varphi_0(K_i)$, voor $i \in \{1,2\}$. Er geldt dat $\varphi_0|_{K_i}$ een inbedding van K_i in $\mathbf{C}$ is. Omdat K_i een totaal reëel lichaam of een CM-lichaam is, geldt dat ook $\rho_0(K_i) = \overline{\varphi_0(K_i)} \subset \varphi_0(K_i)$, dus $\rho_0(K_i) = \varphi_0(K_i)$. Hieruit volgt dat $\rho_0(K_1 \cdot K_2) = \varphi_0(K_1 \cdot K_2)$. Dan is er dus een $\rho' : K_1 \cdot K_2 \to K_1 \cdot K_2$ zodanig dat $\varphi_0(\rho'(x)) = \overline{\varphi_0(x)}$. Omdat $\varphi_0|_{K_i}$ een inbedding van K_i in $\mathbf{C}$ is, volgt dat $\rho'|_{K_i} = \rho_i$, met $\rho_i \neq \mathrm{id}$ als K_i een CM-lichaam is en $\rho_i = \mathrm{id}$ als K_i totaal reëel is. Hiermee voldoet $K_1 \cdot K_2$ ook aan definitie 2.2 van een CM-lichaam als K_1 en/of K_2 een CM-lichaam is en anders aan definitie 2.1 van een totaal reëel lichaam. □

Gevolg 2.9. Als K een CM-lichaam is en $L/\mathbf{Q}$ een normale afsluiting van K, dan is L ook een CM-lichaam.

Bewijs. De normale afsluiting is het compositum van de verschillende inbeddingen van een lichaam in een algebraïsch afgesloten lichaam. Hiermee volgt dit uit stelling 2.8. □

Dit gevolg zullen we in paragraaf 3 gebruiken. Nu volgt een lemma dat we in het volgende deel van deze paragraaf en paragraaf 4 zullen gebruiken.

Lemma 2.10. *Zij K een CM-lichaam en $K_1 \subseteq K$ een deellichaam, dan geldt dat K_1 een CM-lichaam is dan en slechts dan als $\rho|_{K_1} \neq \mathrm{id}$.*

Bewijs. We mogen zonder verlies van algemeenheid aannemen dat $K/\mathbf{Q}$ Galois met groep G. Zij $K_1 = K^{H_1}$ voor een $H_1 \subseteq G$. Dan geldt $\rho|_{K_1} : K_1 \to \rho(K_1) = K^{\rho H_1 \rho^{-1}} = K^{H_1} = K_1$, dus $\rho|_{K_1} \in \mathrm{Aut}(K_1)$ en $(\varphi \circ \rho|_{K_1})(x) = \overline{\varphi(x)}$ voor alle $\varphi \in \mathrm{Hom}(K_1, \mathbf{C})$ en alle $x \in K_1$. Hiermee voldoet K_1 aan definitie 2.2 dan en slechts dan als $\rho|_{K_1} \neq \mathrm{id}$. □

2.2. CM-typen

Een CM-lichaam heeft meerdere *CM-typen*. De volgende definitie is definitie 1.2 uit de inleiding (paragraaf 1).

Definitie 2.11. Een *CM-type* Φ van een CM-lichaam $K/\mathbf{Q}$ van graad $2n$ is een deelverzameling van $\mathrm{Hom}(K, \mathbf{C})$ zodanig dat $\Phi \cup \overline{\Phi} = \mathrm{Hom}(K, \mathbf{C})$ en $|\Phi| = n$, oftewel $\Phi \cap \overline{\Phi} = \emptyset$.

Een CM-lichaam K van graad $2n$ heeft meerdere CM-typen. In $\mathrm{Hom}(K, \mathbf{C})$ zijn n paren van de vorm φ, $\overline{\varphi}$ bevat. Elk CM-type bevat precies één van de twee elementen uit $\{\varphi, \overline{\varphi}\}$. Een CM-lichaam heeft hiermee 2^n verschillende CM-typen.

In paragraaf 4 zullen we een classificatie van CM-typen geven. Eén van de eigenschappen die daarbij gebruikt wordt, is *primitiviteit* van CM-typen. De volgende definitie is definitie 1.3 uit de inleiding (paragraaf 1).

Definitie 2.12. Laat K, L twee CM-lichamen zijn waarvoor geldt dat $K \subseteq L$. Zij Φ een CM-type van K, dan heet

$$\Phi_L = \{(\varphi : L \to \mathbf{C}) : \varphi|_K \in \Phi\}$$

het CM-type van L *geïnduceerd* door Φ. Een CM-type Φ' van L heet *primitief* als er geen CM-lichaam $K \subsetneq L$ en CM-type Φ van K bestaan met $\Phi' = \Phi_L$.

Het is gemakkelijk uit de definitie van een CM-type na te gaan dat ook Φ_L een CM-type is. In het volgende voorbeeld zien we CM-typen die niet primitief zijn.

Voorbeeld 2.13. Zij $K = \mathbf{Q}(\zeta_8) \subseteq \mathbf{C}$ en $G = \mathrm{Gal}(K/\mathbf{Q}) = \{\varphi_k : \zeta_8 \mapsto \zeta_8^k : k = 1, 3, 5, 7\} \cong V_4$. Het automorfisme φ_7 is complexe conjugatie van dit lichaam, want voor alle $\varphi \in G$ en voor alle $x \in K$ geldt

$$(\varphi \circ \varphi_7)(x) = (\varphi_7 \circ \varphi)(x) = \overline{\varphi(x)},$$

omdat G abels is. Zo volgt uit definitie 2.2 dat K een CM-lichaam is met $\rho = \varphi_7$. Het CM-lichaam K bevat het CM-lichaam $K_1 = \mathbf{Q}(i)$ uit voorbeeld 2.6. De Galoisgroep van K_1 is $\mathrm{Gal}(K_1/\mathbf{Q}) = \{\mathrm{id}, \rho\}$ met $\rho : i \mapsto -i$. Het lichaam K_1 heeft twee verschillende CM-typen, namelijk $\Phi_1 = \{\mathrm{id}\}$ en $\Phi_2 = \{\rho\}$. Er geldt $\varphi_1(i) = \varphi_5(i) = i$ en $\varphi_3(i) = \varphi_7(i) = -i$. Hieruit volgt dat Φ_1 het CM-type $(\Phi_1)_K = \{\varphi_1, \varphi_5\}$ van K induceert en dat Φ_2 het CM-type $(\Phi_2)_K = \{\varphi_3, \varphi_7\}$ van K induceert.

Het gevolg van de volgende propositie maakt het in veel situaties makkelijker om na te gaan of een gegeven CM-type primitief is. Ook formuleren we een tweede gevolg dat we in paragraaf 4 zullen gebruiken.

Propositie 2.14. *Zijn K, L twee CM-lichamen met $K \subseteq L$ waarvoor geldt dat $L/\mathbf{Q}$ een Galoisuitbreiding is met Galoisgroep G. Laat Φ een CM-type van K zijn en Φ_L het CM-type van L geïnduceerd door Φ zijn. Zij $H \subseteq G$ de ondergroep van G die correspondeert met K. Laat*

$$H' = \{\sigma \in G : \Phi_L \sigma = \Phi_L\}$$

en $K' = L^{H'}$ zijn. Voor $K_1 \subseteq K$ geldt: K_1 is een CM-lichaam én er bestaat een CM-type Φ' van K_1 met $\Phi'_K = \Phi$ dan en slechts dan als $K' \subseteq K_1$.

Bewijs. $\Rightarrow$ Uit het feit dat $\Phi'_K = \Phi$, volgt dat $\Phi'_L = \Phi_L$, dus voor $\sigma \in \mathrm{Gal}(L/K_1)$ geldt $\Phi_L\sigma = \Phi'_L\sigma = \Phi'_L = \Phi_L$ omdat σ de identiteit is op K_1 en zo volgt dat $\sigma \in \mathrm{Gal}(L/K') = H'$, ofwel $\mathrm{Gal}(L/K_1) \subseteq H'$ en dat betekent dat $K' \subseteq K_1$.

$\Leftarrow$ Er geldt dat $K' \subseteq K_1 \subseteq K$ en in het bijzonder dus $K' \subseteq K$. Ook geldt $\rho \notin H'$, want $\Phi_L\rho = \overline{\Phi_L} \neq \Phi_L$. Wegens propositie 2.10 is K_1 dus een CM-lichaam. Laat $\Phi' = \{\varphi|_{K_1} : \varphi \in \Phi\}$ zijn. We zullen nu bewijzen dat Φ' een CM-type is. Hiermee is namelijk de implicatie bewezen, omdat geldt dat $\Phi'_K = \Phi$. Ten eerste geldt dat $\Phi' \cup \overline{\Phi'} = \mathrm{Hom}(K_1, \mathbf{C})$. Ten tweede geldt dat $\Phi' \cap \overline{\Phi'} = \emptyset$, want stel $\Phi' \cap \overline{\Phi'} \neq \emptyset$, dan geldt dat er $\varphi, \psi \in \Phi_L$ bestaan met $\varphi|_{K_1} = \overline{\psi}|_{K_1}$. Laat $\sigma = \varphi^{-1}\overline{\psi}$ zijn, dan geldt $\sigma \in \mathrm{Gal}(L/K_1)$, want $\sigma|_{K_1} = \varphi^{-1}\varphi|_{K_1} = \mathrm{id}\,|_{K_1}$. Hieruit volgt dat $\sigma \in H'$, want $\mathrm{Gal}(L/K_1) \subseteq H'$, dus $\overline{\psi} = \varphi\sigma \in \Phi_L\sigma = \Phi_L$. Hieruit volgt dat $\overline{\psi} \in \Phi_L$ en dat geeft een tegenspraak, want Φ_L is een CM-type. □

Gevolg 2.15. Laat K, L twee CM-lichamen zijn waarvoor geldt dat $K \subseteq L$ en geldt dat $L/\mathbf{Q}$ een Galoisuitbreiding is met Galoisgroep G. Zij $H \subseteq G$ de ondergroep van G die correspondeert met K. Zij Φ een CM-type van K en Φ_L het CM-type van L geïnduceerd door Φ. Laat

$$H' = \{\sigma \in G : \Phi_L \sigma = \Phi_L\}$$

zijn, dan geldt dat Φ primitief is dan en slechts dan als $H = H'$.

Bewijs. Er geldt $H' = H$ dan en slechts dan als $K = L^{H'}$. Wegens propositie 2.14 is dit equivalent met het feit dat Φ niet geïnduceerd is vanaf een strikt deellichaam. □

Gevolg 2.16. Laat K, L twee CM-lichamen zijn waarvoor L Galois is met Galoisgroep G. Laat Φ een CM-type van K zijn, Φ_L het CM-type van L geïnduceerd door Φ en H' zoals in gevolg 2.15. Zij $g \in G$, dan geldt dat Φ primitief is dan en slechts dan als $g\Phi$ primitief is.

Bewijs. Het is eenvoudig na te gaan dat $(g\Phi)_L = g\Phi_L$. Nu volgt dit gevolg uit de definitie van H' en gevolg 2.15. □

Het volgende voorbeeld illustreert gevolg 2.15 en 2.16.

Voorbeeld 2.17. We het CM-lichaam $K = \mathbf{Q}(\zeta_8) \subseteq \mathbf{C}$ in voorbeeld 2.13. Er is ook laten zien dat de twee CM-typen $(\Phi_1)_K = \{\varphi_1, \varphi_5\}$ en $(\Phi_2)_K = \{\varphi_3, \varphi_7\}$ niet primitief zijn. We kunnen dit ook zien door het resultaat uit gevolg 2.15 te gebruiken. Er geldt namelijk dat de elementen uit $\sigma \in G$ waarvoor geldt dat $(\Phi_1)_K\sigma = (\Phi_1)_K$ gelijk zijn aan $\sigma = \varphi_1$ en $\sigma = \varphi_5$ en de groep $\langle\varphi_5\rangle$ correspondeert niet met K. Er geldt ook voor $(\Phi_2)_K$ dat $(\Phi_2)_K\varphi_1 = (\Phi_2)_K$ en $(\Phi_2)_K\varphi_5 = (\Phi_2)_K$. We hadden ook gevolg 2.16 kunnen gebruiken om uit het feit dat $(\Phi_1)_K$ niet primitief is te concluderen dat $(\Phi_2)_K$ niet primitief is. Er geldt namelijk dat $G \cdot \{\varphi_1, \varphi_5\} = \{\{\varphi_1, \varphi_5\}, \{\varphi_3, \varphi_7\}\}$.

3. Classificatie van Galoisgroepen van CM-lichamen

We zullen voor CM-lichamen van graad 2, 4 en 6 op isomorfie na bepalen wat de mogelijke Galoisgroepen zijn. De resultaten uit deze paragraaf gebruiken we in de volgende paragraaf, paragraaf 4. Verder nemen we in deze paragraaf aan dat alle lichamen bevat zijn in $\mathbf{C}$.

3.1. CM-lichamen van graad twee

Voor kwadratische CM-lichamen is er op isomorfie na maar een mogelijke Galoisgroep.

Propositie 3.1. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 2. Het lichaam K is Galois en er geldt $\mathrm{Gal}(K/\mathbf{Q}) = \langle \rho \rangle \cong C_2$ met $\rho^2 = \mathrm{id}$.*

Bewijs. De uitbreiding is eindig, normaal (want kwadratisch) en separabel (als uitbreiding van $\mathbf{Q}$), hiermee is hij Galois. De Galoisgroep is isomorf aan C_2, want er is op isomorfie na één groep van graad 2. (Zie [6, p.138].) Er geldt dat $\rho \in \mathrm{Aut}(K)$ wegens definitie 2.2. In het bewijs van stelling 2.5 zagen we dat ρ orde 2 heeft. Zo volgt dat $C_2 = \langle \rho \rangle$. □

Het CM-lichaam uit voorbeeld 2.6 heeft Galoisgroep isomorf aan C_2.

3.2. CM-lichamen van graad vier

De classificatie van Galoisgroepen van CM-lichamen van graad 4 wordt samengevat in de volgende propositie.

Propositie 3.2 (Shimura, [5, II.8.4.Examples.(2)(C) op p.65])**.** *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 4 en $L \subseteq \mathbf{C}$ de normale afsluiting van K in $\mathbf{C}$. Laat $G = \mathrm{Gal}(L/\mathbf{Q})$ zijn en $H = \mathrm{Gal}(L/K) \subseteq G$ zijn. Dan geldt één van de volgende drie uitspraken:*

1. *het lichaam K is Galois en $G = \langle \rho, \sigma \rangle \cong V_4$ voor een $\sigma \in G$,*
2. *het lichaam K is Galois en $G = \langle \sigma \rangle \cong C_4$ voor een $\sigma \in G$ met $\sigma^4 = \mathrm{id}$ en $\rho = \sigma^2$,*
3. *het lichaam K is niet Galois, en er geldt $G = \langle r, s \rangle \cong D_4$ voor zekere $r, s \in G$ met $r^4 = s^2 = \mathrm{id}$, $srs = r^3$, $\rho = r^2$ en $H = \langle s \rangle$.*

Bewijs. De uitbreiding $L/\mathbf{Q}$ is per definitie eindig en normaal. Bovendien is zij separabel als uitbreiding van $\mathbf{Q}$, dus $L/\mathbf{Q}$ is Galois. Vanwege de separabiliteit van $K/\mathbf{Q}$, bestaat er een element $\alpha_1 \in K$ met $K = \mathbf{Q}(\alpha_1)$. Dit element α_1 heeft een minimumpolynoom van graad 4 over $\mathbf{Q}$. Laat α_1, $\rho(\alpha_1)$, α_2 en $\rho(\alpha_2)$ de vier nulpunten en tevens de vier geconjugeerden van α_1 zijn. Wegens definitie 2.4 geldt dat K een totaal reëel deellichaam K_0 bevat zodanig dat $[K : K_0] = 2$. In het bewijs van stelling 2.5 zagen we dat $K_0 = K^{\langle\rho\rangle}$. Laat L_0 de normale afsluiting van K_0 in $\mathbf{C}$ zijn en L de normale afsluiting van K in $\mathbf{C}$ zijn. Zijn $G = \mathrm{Gal}(L/\mathbf{Q})$, $G_0 = \mathrm{Gal}(L_0/\mathbf{Q})$ en $V = \mathrm{Gal}(L/L_0)$. Het volgende rijtje is exact:

$$\mathrm{id} \to V \xrightarrow{\chi} G \xrightarrow{\psi} G_0 \to \mathrm{id}\,. \tag{2}$$

We zullen nu de mogelijke Galoisgroepen G bepalen aan de hand van (2). Hiertoe beschouwen we eerst hoe de Galoisgroepen uit (2) op de geconjugeerden van α_1 werken. De groep G werkt transitief op de geconjugeerden van α_1, terwijl G_0 transitief werkt op de verzameling $\{X_1, X_2\}$ met $X_i = \{\alpha_i, \rho(\alpha_i)\}$, $i \in \{1, 2\}$, dus $G_0 \cong S_2$. Voor een element v uit V geldt juist $v(X_i) = X_i$, $i \in \{1, 2\}$. Zo volgt dat V een ondergroep is van C_2^2 die transitief werkt op de elementen uit de verzamelingen X_i, $i \in \{1, 2\}$, oftewel V is een ondergroep van $\langle e_1, e_2\rangle$ waarbij $e_i = (\alpha_i\ \rho(\alpha_i))$, $i \in \{1, 2\}$. Die ondergroep bevat in ieder geval $\rho = e_1e_2$. Zo volgt $V \cong C_2$ of $V \cong C_2^2$. We zullen vanaf nu de notatie i gebruiken voor α_i en de notatie $-i$ voor $\rho(\alpha_i)$, $i \in \{1, 2\}$.

Voor beide gevallen geldt dat G een element σ bevat dat onder ψ op $(X_1\ X_2) \in G_0$ afbeeldt. De mogelijkheden die we voor σ hebben, zijn: $\sigma_1 = (1\ 2\ -1\ -2)$, $\sigma_2 = (1\ -2\ -1\ 2)$, $\sigma_3 = (1\ 2)(-1\ -2)$ en $\sigma_4 = (1\ -2)(-1\ 2)$.

$\mathbf{V \cong C_2}$. In dit geval geldt $V = \langle\rho\rangle$ en $|G| = 4$. De groep G bevat ρ en een σ_i, $i \in \{1, 2, 3, 4\}$. Stel $\sigma = \sigma_1 \in G$, dan geldt $\sigma\rho = \sigma_2$ en er volgt $G = \langle\sigma\rangle \cong C_4$ en $\rho = \sigma^2$. Daarnaast geldt als $\sigma = \sigma_3 \in G$, dat $\sigma\rho = \sigma_4$ en $G = \langle\rho, \sigma\rangle \cong V_4$.

$\mathbf{V \cong C_2^2}$. Ook nu geldt dat $\rho \in V$ en verder geldt dat $|G| = 8$. Uit de eigenschappen van het exacte rijtje volgt dat G vier verschillende elementen bevat die onder ψ op $(X_1\ X_2) \in G_0$ afbeelden. Dit zijn dus σ_i, $i \in \{1, 2, 3, 4\}$. Laat nu $s = (2\ -2)$ en $r = (1\ 2\ -1\ -2)$ zijn, dan geldt $srs = (1\ -2\ -1\ 2) = r^3$, oftewel $D_4 \subset G$ en daarmee $G = D_4$. Verder volgt $\rho = r^2$ en $H = \langle s\rangle$. □

Om deze propositie te illustreren volgt een voorbeeld van drie

CM-lichamen met Galoisgroep isomorf aan respectievelijk V_4, C_4 en D_4.

Voorbeeld 3.3. 1. In voorbeeld 2.13 zagen we dat $K = \mathbf{Q}(\zeta_8) \subseteq \mathbf{C}$ een CM-lichaam is met Galoisgroep isomorf aan V_4.

2. Het lichaam $K = \mathbf{Q}(\zeta_5) \subseteq \mathbf{C}$ heeft Galoisgroep C_4 volgens [8, stelling 24.9(1) op p.53]. Vanwege dezelfde stelling van [8] geldt dat $\varphi_{-1} : \zeta_5 \mapsto \zeta_5^{-1}$ een automorfisme van K is. Omdat C_4 een abelse groep is, geldt voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en alle $x \in K$ dat:

$$(\varphi \circ \varphi_{-1})(x) = (\varphi_{-1} \circ \varphi)(x) = \overline{\varphi(x)}.$$

Zo volgt uit definitie 2.2 dat K een CM-lichaam is met $\rho = \varphi_{-1}$.

3. Tot slot beschouwen we $K = \mathbf{Q}[X]/(X^4 + 8X^2 + 14) \subseteq \mathbf{C}$. We zullen aan de hand van definitie 2.3 laten zien dat K een CM-lichaam is. Het polynoom $X^4 + 8X^2 + 14$ is Eisenstein bij 2 en dus irreducibel. In $\mathbf{C}$ heeft f de vier verschillende nulpunten $x = i\sqrt{4+\sqrt{2}}$, $\overline{x}$, $y = i\sqrt{4-\sqrt{2}}$ en $\overline{y}$. Er geldt $x^2 = -4-\sqrt{2}$ en zo volgt dat het totaal reële lichaam $K_0 = \mathbf{Q}(\sqrt{2})$ een deellichaam is van K. Bovendien geldt dat $\varphi(-4-\sqrt{2}) < 0$ voor alle $\varphi \in \mathrm{Hom}(K_0, \mathbf{R})$. Hiermee voldoet K aan definitie 2.3 van een CM-lichaam. Er geldt $-xy = \sqrt{14}$ en dus bevat de normale afsluiting van K het totaal reële deellichaam $\mathbf{Q}(\sqrt{2}, \sqrt{7})$ van graad 4 en dus is K zelf niet normaal. Uit propositie 3.2 volgt dat K een Galoisgroep heeft die isomorf is aan D_4.

3.3. CM-lichamen van graad zes

Voor CM-lichamen van graad 6 is de classificatie als volgt samen te vatten in een propositie.

Propositie 3.4 (Dina-Ionica-Sijsling, [1, Theorem 1.1.2 op p.353] en Dodson, [2, Section 5.1.1 op p.19-20])**.** *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 6 en $L \subseteq \mathbf{C}$ de normale afsluiting van K in $\mathbf{C}$. Laat $G = \mathrm{Gal}(L/\mathbf{Q})$ zijn en $H = \mathrm{Gal}(L/K) \subseteq G$ zijn. Dan geldt één van de volgende vier uitspraken:*

1. *het lichaam K is Galois en $G = \langle\sigma\rangle \cong C_6$ voor zekere $\sigma \in G$ met $\sigma^6 = \mathrm{id}$ en $\rho = \sigma^3$.*

2. *het lichaam K is niet Galois en er geldt $G = \langle r, s\rangle \cong D_6$ voor zekere $r, s \in G$ met $r^6 = s^2 = \mathrm{id}$, $srs = r^5$, $\rho = r^3$ en $H = \langle s\rangle$.*

3. *het lichaam K is niet Galois en er geldt dat er een isomorfisme $\psi : C_2^3 \rtimes C_3 \to G$ bestaat, waarbij $C_2^3 = \langle e_1, e_2, e_3 \rangle$, $ve_iv^{-1} = e_{v(i)}$, $v \in C_3$, $i \in \{1,2,3\}$, $\rho = \psi(e_1e_2e_3)$ en $H = \langle \psi(e_2), \psi(e_3) \rangle$.*

4. *het lichaam K is niet Galois en er geldt dat er een isomofisme $\psi : C_2^3 \rtimes S_3 \to G$ bestaat, waarbij $C_2^3 = \langle e_1, e_2, e_3 \rangle$, $ve_iv^{-1} = e_{v(i)}$, $v \in S_3$, $i \in \{1,2,3\}$, $\rho = \psi(e_1e_2e_3)$ en $H = \langle \psi(e_2), \psi(e_3), \psi((2\ 3)) \rangle$.*

Bewijs. De uitbreiding $L/\mathbf{Q}$ is per definitie eindig en normaal. Daarnaast is zij separabel als uitbreiding van $\mathbf{Q}$, dus $L/\mathbf{Q}$ is Galois. Ook de uitbreiding $K/\mathbf{Q}$ is separabel. Er bestaat dus een element $\alpha_1 \in K$ met $K = \mathbf{Q}(\alpha_1)$. Het minimumpolynoom van α_1 heeft zes verschillende nulpunten, de geconjugeerden van α_1, die we α_1, $\rho(\alpha_1)$, α_2, $\rho(\alpha_2)$, α_3, $\rho(\alpha_3)$ zullen noemen. Wegens definitie 2.4 bevat K een totaal reëel deellichaam K_0 zodanig dat $[K : K_0] = 2$. Verder zagen we in het bewijs van stelling 2.5 dat $K_0 = K^{\langle \rho \rangle}$. Laat L_0 de normale afsluiting van K_0 in $\mathbf{C}$ zijn en L de normale afsluiting van K in $\mathbf{C}$ zijn. Zijn $G = \mathrm{Gal}(L/\mathbf{Q})$, $G_0 = \mathrm{Gal}(L_0/\mathbf{Q})$ en $V = \mathrm{Gal}(L/L_0)$. Het volgende rijtje is exact:

$$\mathrm{id} \to V \xrightarrow{\chi} G \xrightarrow{\psi} G_0 \to \mathrm{id}\,. \tag{3}$$

Aan de hand van (3) zullen we alle mogelijkheden voor Galoisgroepen van CM-lichamen van graad 6 bepalen. We beschouwen hiertoe eerst hoe de Galoisgroepen uit (3) op de geconjugeerden van α_1 werken. De groep G werkt transitief op de geconjugeerden. Daarentegen werkt G_0 transitief op $\{X_1, X_2, X_3\}$ met $X_i = \{\alpha_i, \rho(\alpha_i)\}$, $i \in \{1,2,3\}$. Zo volgt dat G_0 een ondergroep van S_3 is die isomorf is aan C_3 of S_3. We noteren vanaf nu e_i voor $(\alpha_i\ \rho(\alpha_i))$, $i \in \{1,2,3\}$. Voor een element v uit V geldt juist $v(X_i) = X_i$, $i \in \{1,2\}$. De groep V is een ondergroep van C_2^3 die transitief werkt op de elementen uit de verzamelingen X_i, $i \in \{1,2,3\}$ en waarvoor geldt dat $\rho = e_1e_2e_3 \in V$. Uit bovenstaande volgt dat V een ondergroep is van $\langle e_1, e_2, e_3 \rangle$ waarvoor geldt $V \cong C_2$, $V \cong C_2^2$ of $V \cong C_2^3$. We zullen vanaf nu de notatie i gebruiken voor α_i en de notatie $-i$ voor $\rho(\alpha_i)$, $i \in \{1,2,3\}$.

Voor alle mogelijkheden voor V en G_0 geldt dat G een element g bevat dat op $(X_1\ X_2\ X_3)$ afbeeldt onder ψ, want ψ is surjectief en als $G_0 \cong C_3$ of als $G_0 \cong S_3$ geldt dat $(X_1\ X_2\ X_3) \in G_0$. Stel dat $g^3(1) = -1$, dan geldt dat $(\rho g)^3(1) = \rho g^3(1) = 1$. Hieruit volgt dat we zonder verlies van algemeenheid aan kunnen nemen dat $g^3(1) = 1$. Na hernummering van de geconjugeerden van α_1 is het voldoende om $g = (1\ 2\ 3)(-1\ -2\ -3)$ te beschouwen. We hebben de volgende mogelijkheden voor V en G_0.

$\mathbf{V \cong C_2^2}$ Naast ρ en id bevat V nog een ander element v. Het element v is van de vorm e_ie_j met $i \neq j$ of e_k, $i, j, k \in \{1, 2, 3\}$. Stel dit element is van de vorm e_ie_j met $i \neq j$, dan geldt dat $\rho e_ie_j = e_k$ met $k \notin \{i, j\}$. We kunnen dus zonder verlies van algemeenheid aannemen dat V een element e_k bevat met $k \in \{1, 2, 3\}$. De permutatie g werkt transitief op e_k, dus $e_i \in V$ voor $i = 1, 2, 3$. Echter geldt dan dat $V \cong C_2^3$, wat een tegenspraak oplevert.

$\mathbf{G_0 \cong C_3, V \cong C_2}$ Er geldt dat $|G| = 6$. We beschouwen het element $\sigma = \rho g \in G$, dan geldt dat $\sigma = (1\ \ {-2}\ 3\ \ {-1}\ 2\ \ {-3})$. De groep G bevat dus een element van orde zes en is hiermee isomorf aan C_6. Daarnaast volgt dat $\rho = \sigma^3$.

$\mathbf{G_0 \cong S_3, V \cong C_2}$ Er geldt dat $|G| = 12$. De groep G_0 wordt voortgebracht door $(X_1\ X_2\ X_3)$ en $(X_2\ X_3)$. Omdat ψ surjectief is, geldt dat G elementen bevat die op deze voortbrengers afbeelden. We hebben al gezien dat $g \in G$ op $(X_1\ X_2\ X_3)$ afbeeldt. Voor een element h dat op ψ op $(X_2\ X_3)$ afbeeldt, geldt dat $h(2) = \pm 3$. Omdat in het geval dat $h(2) = -3$, er geldt $(\rho h)(2) = 3$, kunnen we zonder verlies van algemeenheid aannemen dat $h(2) = 3$. De mogelijkheden voor h zijn dan $h_1 = (2\ 3)({-2}\ \ {-3})$, $h_2 = (1\ \ {-1})(2\ 3)({-2}\ \ {-3})$, $h_3 = (2\ 3\ \ {-2}\ \ {-3})$ en $h_4 = (1\ \ {-1})(2\ 3\ \ {-2}\ \ {-3})$. Daarnaast geldt dat $\ker(\psi) = \chi(V) = \chi(\langle\rho\rangle)$, dus voor een element h dat op $(X_2\ X_3)$ afbeeldt geldt dat $h^2 \in \chi(\langle\rho\rangle)$, want $(X_2\ X_3)^2 = \mathrm{id}$. Echter geldt $h_3^2 = h_4^2 = (2\ \ {-2})(3\ \ {-3}) \notin \chi(\langle\rho\rangle)$, dus $h_3, h_4 \notin G$. Stel dat $h_2 \in G$, dan geldt dat ook $(h_2g)^2 = e_1e_3 \in G$ en e_1e_3 is vast op $\{X_1, X_2, X_3\}$, dus dan zou gelden dat $e_1e_3 \in V$, maar dat geeft een tegenspraak. Stel nu dat $s = h_1 \in G$ en we noteren $\rho g = r$, dan geldt dat $r^6 = s^2 = \mathrm{id}$, $srs = (1\ \ {-3}\ 2\ \ {-1}\ 3\ \ {-2}) = r^5$. Hiermee is G isomorf aan D_6. Verder geldt $\rho = r^3$ en $H = \langle s\rangle$.

$\mathbf{G_0 \cong C_3, V \cong C_2^3}$ We zullen aan de hand van [6, stelling 10.2 op p.124] laten zien dat in dit geval geldt dat er een isomorfisme $\psi : C_2^3 \rtimes C_3 \to G$ bestaat. Er is een sectie $s : C_3 \to G$ met $(X_1\ X_2\ X_3) \mapsto g$. Vanaf nu zullen we alleen i noteren in plaats van X_i. De sectie s geeft aanleiding tot de werking $ve_iv^{-1} = e_{v(i)}$ voor $v \in C_3 = \langle(1\ 2\ 3)\rangle$ en $i \in \{1, 2, 3\}$. Er geldt dat $\psi(cv) = \chi(c)s(v)$, $c \in C_2^3$, $v \in C_3$ en er geldt $\rho = \psi(e_1e_2e_3)$ en $H = \langle\psi(e_2), \psi(e_3)\rangle$.

$\mathbf{G_0 \cong S_3, V \cong C_2^3}$ We zullen aan de hand van van [6, stelling 10.2 op p.124] laten zien dat in dit geval geldt dat er een isomorfisme $\psi : C_2^3 \rtimes C_3 \to G$ bestaat. Er is een sectie $s : S_3 \to G$ met $(X_1\ X_2\ X_3) \mapsto g$ en $(X_2\ X_3) \mapsto (2\ 3)({-2}\ \ {-3})$. Er geldt $(2\ 3)({-2}\ \ {-3}) \in G$, omdat G wegens de eigenschappen van het exacte rijtje acht verschillende

elementen bevat die onder ψ op $(X_2\ X_3)$ afbeelden. Er zijn in totaal ook precies acht mogelijkheden voor een element dat op $(X_2\ X_3)$ afbeeldt; G bevat ze dus alle acht. Eén van de mogelijkheden is $(2\ 3)(-2\ -3)$ en zo volgt $(2\ 3)(-2\ -3) \in G$. Vanaf nu zullen we alleen i noteren in plaats van X_i. De sectie s geeft de werking $ve_iv^{-1} = e_{v(i)}$ voor $v \in S_3 = \langle (1\ 2\ 3), (2\ 3)\rangle$. Samen geeft dit een isomorfisme $\psi(cv) = \chi(c)s(v)$, $c \in C_2^3$, $v \in S_3$. Er geldt $\rho = \psi(e_1e_2e_3)$ en $H = \langle \psi(e_2), \psi(e_3), \psi((2\ 3))\rangle$. $\square$

Er volgt nu een voorbeeld van CM-lichamen met Galoisgroep isomorf aan respectievelijk C_6, D_6, $C_2^3 \rtimes C_3$ en $C_2^3 \rtimes S_3$.

Voorbeeld 3.5. 1. De Galoisgroep van het lichaam $K = \mathbf{Q}(\zeta_7)$ is volgens [8, stelling 24.9(1) op p.53] isomorf aan C_6. Daarnaast geldt wegens dezelfde stelling van [8] dat $\varphi_{-1} : \zeta_7 \to \zeta_7^{-1}$ een automorfisme is van K. Dit automorfisme is conjugatie op de voortbrenger van K en omdat C_6 abels is, geldt dat voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ en alle $x \in K$:

$$(\varphi \circ \varphi_{-1})(x) = (\varphi_{-1} \circ \varphi)(x) = \overline{\varphi(x)}.$$

Het lichaam K is een CM-lichaam met $\rho = \varphi_{-1}$ volgens definitie 2.2.

2. Een voorbeeld van een CM-lichaam met Galoisgroep isomorf aan D_6 is $K = \mathbf{Q}[X]/(X^6 - 2X^3 + 8)$. Dit voorbeeld is afkomstig van [4] en heeft nummer 6.0.4000752.1.

3. Het CM-lichaam $\mathbf{Q}[X]/(X^6 + 13X^4 + 54X^2 + 71)$ heeft Galoisgroep isomorf aan $C_2^3 \rtimes C_3$. Dit lichaam komt van [4] en heeft nummer 6.0.10910144.2.

4. Als laatste geven we een CM-lichaam met Galoisgroep isomorf aan $C_2^3 \rtimes S_3$, namelijk $\mathbf{Q}[X]/(X^6+7X^4+10X^2+2)$, ook afkomstig van [4], met nummer 6.0.103223968.1.

4. Classificatie van CM-typen

In deze paragraaf zullen we alle CM-typen van CM-lichamen van graad 2, 4 en 6 bepalen. Daarnaast stellen we vast of ze primitief zijn en bepalen hun Galoisbaan. Hierbij nemen we aan dat de lichamen bevat zijn in $\mathbf{C}$.

4.1. CM-lichamen van graad twee

Het volgende lemma geeft de CM-typen van een kwadratisch CM-lichaam.

Lemma 4.1. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 2 en $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle\rho\rangle \cong C_2$. De CM-typen van K zijn $\{\mathrm{id}\}$ en $\{\rho\}$. Deze vormen één baan onder linksvermenigvuldiging met G en zijn primitief.*

Bewijs. Het is eenvoudig in te zien dat de CM-typen gelijk zijn aan de CM-typen uit het lemma. De CM-typen vormen een baan onder linksvermenigvuldiging met G, oftewel $G \cdot \{\mathrm{id}\} = \{\{\mathrm{id}\}, \{\rho\}\}$. De CM-typen zijn primitief, omdat de graad van een CM-lichaam minstens 2 is. Dat wil zeggen dat er geen CM-lichamen strikt bevat zijn in een CM-lichaam van graad 2. □

4.2. CM-lichamen van graad vier

De volgende twee lemma's geven de CM-typen van CM-lichamen van graad 4 voor alle verschillende Galoisgroepen (op isomorfie na) van CM-lichamen van graad 4 zoals we die in paragraaf 3.2 bepaald hebben.

Lemma 4.2. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 4 en $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle\rho, \sigma\rangle \cong V_4$ voor zekere $\sigma \in G$. De CM-typen van K zijn*

$$\{\mathrm{id}, \sigma\}, \{\rho, \rho\sigma\}, \{\mathrm{id}, \rho\sigma\} \text{ en } \{\rho, \sigma\}.$$

De eerste twee zijn geïnduceerd vanaf het kwadratische lichaam $K^{\langle\sigma\rangle}$ en vormen één baan onder de linksvermenigvuldiging met G, en de laatste twee zijn geïnduceerd vanaf het kwadratische lichaam $K^{\langle\rho\sigma\rangle}$ en vormen één baan onder de linksvermenigvuldiging met G.

Bewijs. Er zijn twee paar complex geconjugeerden uit $\mathrm{Hom}(K, \mathbf{C})$, namelijk id, ρ en $\sigma, \rho\sigma$. Ieder CM-type bevat van elk paar precies één

element. Hieruit volgt dat K de vier CM-typen uit dit lemma heeft.

Er geldt $G \cdot \{\mathrm{id}, \sigma\} = \{\{\mathrm{id}, \sigma\}, \{\rho, \rho\sigma\}\}$, oftewel $\{\mathrm{id}, \sigma\}$ en $\{\rho, \rho\sigma\}$ vormen één baan onder linksvermenigvuldiging met G. Laat $H' = \{\sigma \in G : \Phi\sigma = \Phi\}$ zijn met $\Phi = \{\mathrm{id}, \sigma\}$. Het CM-type Φ is niet primitief volgens gevolg 2.15, want $H' = \langle\sigma\rangle$ voor Φ en H' correspondeert niet met K. Met gevolg 2.16 volgt nu dat ook $\{\rho, \rho\sigma\}$ niet primitief is. We beschouwen nu $K_1 = K^{\langle\sigma\rangle}$. Dit lichaam is kwadratisch. (Zie [8, stelling 24.4.3 op p.46].) Er geldt $\rho(K_1) = K^{\rho\langle\sigma\rangle\rho^{-1}} = K^{\langle\sigma\rangle} = K_1$, dus ρ induceert een automorfisme van K_1 en ook geldt $\rho|_{K_1} \neq \mathrm{id}$, omdat $\rho \notin \langle\sigma\rangle$. Hiermee is K_1 dus zelf een CM-lichaam vanwege lemma 2.10. Het heeft zoals we in propositie 3.1 zagen twee CM-typen: $\{\mathrm{id}\}$ en $\{\rho\}$. Per definitie van geïnduceerde CM-typen, definitie 2.12, geldt dat $\{\mathrm{id}, \sigma\}$ en $\{\rho, \sigma\rho\}$ geïnduceerd worden vanaf $K^{\langle\sigma\rangle}$.

Het verwisselen van σ met $\rho\sigma$ is een automorfisme van G. Door de rollen van σ en $\rho\sigma$ om te wisselen volgt op precies dezelfde manier als hierboven dat $\{\mathrm{id}, \rho\sigma\}$ en $\{\rho, \sigma\}$ één baan vormen onder linksvermenigvuldiging van G en dat ze geïnduceerd worden vanaf het kwadratische lichaam $K^{\langle\rho\sigma\rangle}$. □

Lemma 4.3. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 4 en $L \subseteq \mathbf{C}$ de normale afsluiting van K in $\mathbf{C}$. Stel dat $G = \mathrm{Gal}(L/\mathbf{Q})$ voldoet aan $G \cong C_4$ of $G \cong D_4$ met $G = \langle r, s\rangle$, $r^4 = s^2 = \mathrm{id}$, $H = \langle s\rangle$ en $srs = r^3$ als $G \cong D_4$ (en $s = \mathrm{id}$ als $G \cong C_4$). De CM-typen van K zijn*

$$\{\underline{\mathrm{id}}, \underline{r}\}, \{\underline{\mathrm{id}}, \underline{r^3}\}, \{\underline{r}, \underline{r^2}\} \text{ en } \{\underline{r^2}, \underline{r^3}\},$$

waarbij $\underline{f}$ voor $f \in G$ betekent $f|_K$. Deze vormen één baan onder linksvermenigvuldiging met G en zijn primitief.

Bewijs. Er geldt dat $\mathrm{Hom}(K, \mathbf{C}) = \{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}, \underline{r^3}\}$. Uit propositie 3.2 volgt dat $\rho = r^2$. Er zijn twee paar complex geconjugeerden uit $\mathrm{Hom}(K, \mathbf{C})$, namelijk $\underline{\mathrm{id}}, \underline{r^2}$ en $\underline{r}, \underline{r^3}$. Zo volgt dat er de vier CM-typen uit het lemma zijn voor K.

Voor de CM-typen van K geldt dat $G \cdot \{\underline{\mathrm{id}}, \underline{r}\} = \{\{\underline{\mathrm{id}}, \underline{r}\}, \{\underline{\mathrm{id}}, \underline{r^3}\}, \{\underline{r}, \underline{r^2}\}, \{\underline{r^2}, \underline{r^3}\}\}$, dat wil zeggen dat ze één baan onder linksvermenigvuldiging met G vormen. Laat $H' = \{\sigma \in G : \Phi_L\sigma = \Phi_L\}$ zijn met $\Phi = \{\underline{\mathrm{id}}, \underline{r}\}$. Er geldt dat Φ primitief is, want er geldt $H' = \{\mathrm{id}, s\}$ en H' correspondeert met K. Uit gevolg 2.16 volgt dat ook de andere drie CM-typen van K primitief zijn, omdat ze in dezelfde baan onder linksvermenigvuldiging met G zitten als Φ. □

4.3. CM-lichamen van graad zes

In de volgende twee lemma's geven we de CM-typen van CM-lichamen van graad 6 voor alle verschillende Galoisgroepen (op isomorfie na) van CM-lichamen van graad 6 zoals we die in paragraaf 3.3 bepaald hebben.

Lemma 4.4. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 6, $L \subseteq \mathbf{C}$ de normale afsluiting van K in $\mathbf{C}$. Stel dat $G = \mathrm{Gal}(L/\mathbf{Q})$ voldoet aan $G \cong C_6$ of $G \cong D_6$ met $G = \langle r, s\rangle$, $r^6 = s^2 = \mathrm{id}$, $H = \langle s\rangle$ en $srs = r^5$ als $G \cong D_6$ (en $s = \mathrm{id}$ als $G \cong C_6$). De CM-typen van K zijn*

$$\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\}, \{\underline{\mathrm{id}}, \underline{r}, \underline{r^5}\}, \{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}, \{\underline{\mathrm{id}}, \underline{r^4}, \underline{r^5}\},$$

$$\{\underline{r}, \underline{r^2}, \underline{r^3}\}, \{\underline{r}, \underline{r^3}, \underline{r^5}\}, \{\underline{r^2}, \underline{r^3}, \underline{r^4}\} \text{ en } \{\underline{r^3}, \underline{r^4}, \underline{r^5}\},$$

waarbij $\underline{f}$ voor $f \in G$ betekent $f|_K$. De CM-typen $\{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}$ en $\{\underline{r}, \underline{r^3}, \underline{r^5}\}$ vormen één baan onder linksvermenigvuldiging met G en zijn niet primitief, maar worden geïnduceerd vanaf het kwadratische lichaam $L^{\langle r^2, s\rangle}$. De andere zes CM-typen van K vormen één baan onder linksvermenigvuldiging met G en zijn primitief.

Bewijs. Voor K geldt dat $\mathrm{Hom}(K, \mathbf{C}) = \{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}, \underline{r^3}, \underline{r^4}, \underline{r^5}\}$ Wegens propositie 3.4 geldt dat $\rho = r^3$. De drie paar complex geconjugeerden inbeddingen in $\mathbf{C}$ zijn $\underline{\mathrm{id}}, \underline{r^3}$, $\underline{r}, \underline{r^4}$ en $\underline{r^2}, \underline{r^5}$. Hieruit volgt dat K de acht CM-typen uit het lemma heeft.

Er geldt $G \cdot \{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\} = \{\{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}, \{\underline{r}, \underline{r^3}, \underline{r^5}\}\}$. We zullen bewijzen dat deze worden geïnduceerd vanaf $K_1 = L^{\langle r^2, s\rangle}$. Er geldt dat $\rho(K_1) = L^{\rho\langle r^2, s\rangle\rho^{-1}} = L^{\langle r^2, s\rangle} = K_1$. Ook geldt dat $\rho|_{K_1} \neq \mathrm{id}$, want er geldt $\rho \notin \langle r^2, s\rangle$ en wegens lemma 2.10 betekent dit dat K_1 een CM-lichaam is. Wegens [8, stelling 24.4.3 op p.46] geldt dat K_1 kwadratisch is. Vanwege propositie 4.1 geldt dat dit lichaam $\{\mathrm{id}\}$ en $\{\rho\}$ als CM-typen heeft. Uit definitie 2.12, de definitie van een geïnduceerd CM-type, volgt dat $\{\mathrm{id}\}$ het CM-type $\{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}$ van K induceert en dat $\{\rho\}$ het CM-type $\{\underline{r}, \underline{r^3}, \underline{r^5}\}$ van K induceert.

Verder geldt voor de andere zes CM-typen dat ze één baan vormen onder linksvermenigvuldiging met G. Zij $H' = \{\sigma \in G : \Phi_L\sigma = \Phi_L\}$ met $\Phi = \{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\}$. Er geldt $H' = H$ voor Φ, dus dit CM-type is primitief volgens gevolg 2.15. Met gevolg 2.16 volgt dat alle CM-typen uit de baan van Φ primitief zijn. □

Lemma 4.5. *Zij $K \subseteq \mathbf{C}$ een CM-lichaam van graad 6 met normale afsluiting $L \subseteq \mathbf{C}$ en Galoisgroep $G = Gal(L/Q)$. Stel dat G zo is als in propositie 3.4 geval 3. of 4. Met andere woorden, zij $G_0 = A_3 \cong C_3$ of $G_0 = S_3$ en laat $C_2^3 \rtimes G_0$ het semi-directe product zijn waarbij G_0 werkt op $C_2^3 = \langle e_1, e_2, e_3 \rangle$ via $ve_iv^{-1} = e_{v(i)}$ voor alle $v \in G_0$. Zij $\psi : C_2^3 \rtimes G_0 \to G$ een isomorfisme zo dat $\rho = \psi(e_1e_2e_3)$ en $H = \mathrm{Gal}(L/K) = \langle \psi(e2), \psi(e3), \psi(h) \rangle$ met $h = (2\ 3)$ als $G_0 = S_3$ en $h = \mathrm{id}$ als $G_0 = A_3$. Laat $r = \psi(e_1e_2e_3(1\ 2\ 3))$ zijn. De CM-typen van K zijn*

$$\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\}, \{\underline{\mathrm{id}}, \underline{r}, \underline{r^5}\}, \{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}, \{\underline{\mathrm{id}}, \underline{r^4}, \underline{r^5}\},$$

$$\{\underline{r}, \underline{r^2}, \underline{r^3}\}, \{\underline{r}, \underline{r^3}, \underline{r^5}\}, \{\underline{r^2}, \underline{r^3}, \underline{r^4}\} \text{ en } \{\underline{r^3}, \underline{r^4}, \underline{r^5}\},$$

waarbij $\underline{f}$ voor $f \in G$ betekent $f|_K$. Deze vormen één baan onder linksvermenigvuldiging met G en zijn primitief.

Bewijs. Er geldt dat $\mathrm{Hom}(K, \mathbf{C}) = \{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}, \underline{r^3}, \underline{r^4}, \underline{r^5}\}$. Verder geldt dat $\rho = r^3$. Er zijn drie paar complexe geconjugeerden uit $\mathrm{Hom}(K, \mathbf{C})$, namelijk $\underline{\mathrm{id}}, \underline{r^3}$, $\underline{r}, \underline{r^4}$ en $\underline{r^2}, \underline{r^5}$. Zo volgt dat K de acht CM-typen uit het lemma heeft.

Ze vormen een baan onder linksvermenigvuldiging met G, want er geldt $\psi(e_2)\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\} = \{\underline{\mathrm{id}}, \underline{r^2}, \underline{r^4}\}$, $\psi(e_1e_3)\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\} = \{\underline{r}, \underline{r^3}, \underline{r^5}\}$ en $r^i\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\} = \{\underline{r^i}, \underline{r^{i+1}}, \underline{r^{i+2}}\}$, $i \in \{0, 1, 2, 3, 4, 5\}$. Ze zijn alle primitief en zullen dit bewijzen door te bewijzen dat $\Phi = \{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\}$ primitief is. Uit gevolg 2.16 volgt dan dat ze alle acht primitief zijn. Laat $H' = \{\sigma \in G : \Phi_L\sigma = \Phi_L\}$ zijn. Er geldt $H \subseteq H'$ per definitie van H'. We merken op dat $H = \{\sigma \in G : \sigma(1) = 1\}$, waarbij 1 staat voor een voortbrenger α_1 van K over $\mathbf{Q}$. We noteren de andere vijf nulpunten van het minimumpolynoom van α_1 met 2, 3, -1, -2, -3 op zo'n manier dat $r = (1\ \ -2\ 3\ \ -1\ 2\ \ -3)$. Zij $h \in H'$, dan geldt dat er $\mathrm{id}\, h \in \Phi_L$, ofwel $h(1) \in \{1, -2, 3\}$, $rh \in \Phi_L$, ofwel $h(1) \in \{-3, 1, -2\}$ en $r^2h \in \Phi_L$, ofwel $h(1) \in \{2, -3, 1\}$. Zo volgt dat $h(1) = 1$, dus $H = H'$. Hiermee is $\{\underline{\mathrm{id}}, \underline{r}, \underline{r^2}\}$ primitief en dus is het gevraagde bewezen. □

5. Transferafbeelding

We zullen deze paragraaf beginnen met de definitie van een *verzameling transfers*. De notatie in de definitie komt niet eerder voor in deze scriptie en daarom zullen we die na de definitie voorzien van uitleg.

Definitie 5.1. Zij G een eindige groep en H_1, H_2 twee ondergroepen van G, dan heet

$$T(H_1, H_2) := {}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1))$$

de *verzameling met transfers* van H_1 naar H_2.

In deze definitie gebruiken we de groepenring $\mathbf{Z}[G]$ en het linksideaal $\operatorname{I}(H_1)$ van $\mathbf{Z}[G]$ voortgebracht door $\{h-1 : h \in H_1\}$, oftewel

$$\operatorname{I}(H_1) = \Big\{ \sum_{i=1}^{n} a_i(h_i - 1) : n \in \mathbf{N}, a_i \in \mathbf{Z}[G], h_i \in H_1 \Big\}.$$

Het linksideaal is tevens een deelmoduul van $\mathbf{Z}[G]$, dat zelf een $\mathbf{Z}[G]$-moduul is. Het quotiënt in definitie 5.1 is dus het quotiënt van een moduul met een deelmoduul. De ondergroep H_2 van G heeft een werking op dit quotiënt, want er geldt $H_2 \subseteq G \subseteq \mathbf{Z}[G]$ en we kunnen de moduulwerking van $\mathbf{Z}[G]$ beperken tot H_2 om zo een werking van H_2 op $\mathbf{Z}[G]$ te krijgen. Die werking induceert een werking op $\mathbf{Z}[G]/\operatorname{I}(H_1)$, zoals beschreven staat in [7, p.77]. Tot slot, geldt er dat de verzameling ${}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1))$ uit de vaste punten van de werking van H_2 op $\mathbf{Z}[G]/\operatorname{I}(H_1)$ bestaat, ofwel ${}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1) = \{\overline{r} \in \mathbf{Z}[G]/\operatorname{I}(H_1) : \forall h \in H_2, h\overline{r} = \overline{r}\}$. Uit de definitie van een moduulwerking kunnen we eenvoudig afleiden dat dit een ondergroep is van $\mathbf{Z}[G]/\operatorname{I}(H_1)$.

We zullen een basis geven voor de groep $T(H_1, H_2)$. Hiervoor gebruiken we de definitie van zogeheten *dubbele nevenklassen*. Laat H_1, H_2 twee ondergroepen zijn van een groep G. Zij $g \in G$, dan is

$$H_2gH_1 = \big\{h_2gh_1 : h_1 \in H_1, h_2 \in H_2\big\}$$

een *dubbele nevenklasse*. De verzameling dubbele nevenklassen H_2gH_1 noteren we met $H_2\backslash G/H_1$. De groep $\mathbf{Z}^{H_2\backslash G/H_1}$ is isomorf aan $T(H_1, H_2)$ en dit geeft een basis voor $T(H_1, H_2)$. Deze laatste uitspraak bewijzen we aan de hand van de volgende twee lemma's.

Lemma 5.2. *De $\mathbf{Z}[G]$-modulen $\mathbf{Z}[G]/I(H_1)$ en $\mathbf{Z}^{G/H_1}$ zijn isomorf.*

Bewijs. We definiëren

$$\begin{aligned} \psi : \mathbf{Z}[G] &\to \mathbf{Z}^{G/H_1} \\ g &\mapsto gH_1 \end{aligned}$$

en zullen bewijzen dat $\ker(\psi) = \mathrm{I}(H_1)$. Om te bewijzen dat $\mathrm{I}(H_1) \subseteq \ker(\psi)$ is het voldoende om te laten zien dat de voortbrengers van $\mathrm{I}(H_1)$ bevat zijn in $\ker(\psi)$. De voortbrengers van $\mathrm{I}(H_1)$ zijn van de vorm $h-1$ met $h \in H_1$. Er geldt $\psi(h-1) = (H_1) - (H_1) = 0$ en zo volgt $\mathrm{I}(H_1) \subseteq \ker(\psi)$.

Om de andere inclusie te bewijzen, kiezen we een volledige verzameling X van representanten van G/H_1. Laat $\alpha \in \mathbf{Z}[G]$ zijn, dan is α van de volgende vorm: $\alpha = \sum_{g\in X} \sum_{h\in H_1} z_{gh} gh$. We beschouwen nu een α met $\psi(\alpha) = 0$. Er geldt $\psi(\alpha) = \sum_{g\in X} \sum_{h\in H_1} z_{gh}(gH_1) = 0$. Hieruit volgt dat voor α geldt dat voor alle $g \in X$: $\sum_{h\in H_1} z_{gh} = 0$. Zo volgt dat $\alpha = \alpha - \sum_{g\in X} \sum_{h\in H_1} z_{gh} g = \sum_{g\in X} \sum_{h\in H_1} z_{gh} g(h-1) \in \mathrm{I}(H_1)$.

Hiermee is bewezen dat $\ker(\psi) = \mathrm{I}(H_1)$. Laat $\alpha = \sum_{g\in X} a_g gH_1 \in \mathbf{Z}^{G/H_1}$ zijn, dan geldt dat $\psi(\beta) = \alpha$ met $\beta = \sum_{g\in X} a_g g$. Er geldt dus dat ψ surjectief is en wegens de isomorfiestelling volgt dat $\mathbf{Z}[G]/\mathrm{I}(H_1)$ en $\mathbf{Z}^{G/H_1}$ isomorf zijn als $\mathbf{Z}[G]$-modulen. □

Lemma 5.3. *Laat H_2 een groep zijn die een werking heeft op een verzameling X, dan zijn de $\mathbf{Z}$-modulen ${}^{H_2}(\mathbf{Z}^X)$ en $\mathbf{Z}^{H_2\backslash X}$ isomorf.*

Bewijs. We definiëren allereerst

$$\begin{aligned} \psi : \qquad \mathbf{Z}^{H_2\backslash X} &\to \mathbf{Z}^X \\ \sum_{H_2x\in H_2\backslash X} n_{H_2x}(H_2x) &\mapsto \sum_{x\in X} n_{H_2x} x. \end{aligned}$$

We zullen bewijzen dat ψ injectief is en dat het beeld van ψ gelijk is aan ${}^{H_2}(\mathbf{Z}^X)$.

Een element $\alpha \in \mathbf{Z}^{H_2\backslash X}$ is van de vorm $\alpha = \sum_{H_2x\in H_2\backslash X} n_{H_2x}(H_2x)$. We beschouwen nu een α waarvoor geldt $\psi(\alpha) = 0$, dat wil zeggen dat $\sum_{x\in X} n_{H_2x} x = 0$. Dit impliceert dat $n_{H_2x} = 0$ voor alle $x \in X$. Hieruit volgt dat $\alpha = 0$, oftewel ψ is injectief.

Om aan te tonen dat het beeld van ψ gelijk is aan ${}^{H_2}(\mathbf{Z}^X)$, bewijzen we eerst dat geldt $\psi(\mathbf{Z}^{H_2\backslash X}) \subseteq {}^{H_2}(\mathbf{Z}^X)$. Zij $\alpha \in \mathbf{Z}^{H_2\backslash X}$ en $\beta \in \mathbf{Z}^X$ zodanig dat $\beta = \psi(\alpha)$. Er geldt $\alpha = \sum_{H_2x\in H_2\backslash X} n_{H_2x}(H_2x)$ en voor

$h \in H_2$ geldt dat

$$h^{-1}\beta = \sum_{x \in X} n_{H_2 x} h^{-1} x = \sum_{hx \in X} n_{H_2 hx} h^{-1} hx = \sum_{x \in X} n_{H_2 x} x = \beta.$$

Zo volgt dat $\beta \in {}^{H_2}\mathbf{Z}^X$, oftewel $\psi(\mathbf{Z}^{H_2 \backslash X}) \subseteq {}^{H_2}(\mathbf{Z}^X)$.

We zullen nu de inclusie ${}^{H_2}(\mathbf{Z}^X) \subseteq \psi(\mathbf{Z}^{H_2 \backslash X})$ bewijzen. Laat daartoe $\gamma = \sum_{x \in X} n_x x \in {}^{H_2}(\mathbf{Z}^X)$ zijn. Voor $h \in H_2$ geldt dus $h^{-1}\gamma = \gamma$. Hieruit volgt dat $h^{-1}\gamma = h^{-1} \sum_{x \in X} n_x x = \sum_{x \in X} n_{hx} x = \gamma$. Waaruit volgt dat voor alle $x \in X$ geldt dat $n_x = n_{hx}$ voor alle $h \in H_2$. Laat nu $n_{H_2 x} := n_x$ zijn voor alle $H_2 x \in H_2 \backslash X$, dan geldt voor alle $y \in H_2 x$, dat $n_y = n_{H_2 x}$. Zo volgt dat voor $\alpha = \sum_{H_2 x \in H_2 \backslash X} n_{H_2 x}(H_2 x)$, geldt dat $\psi(\alpha) = \sum_{x \in X} n_{H_2 x} x = \gamma$. Hiermee is de inclusie ${}^{H_2}\mathbf{Z}^X \subseteq \psi(\mathbf{Z}^{H_2 \backslash X})$ bewezen. Samen met de eerder aangetoonde inclusie geeft dit $\psi(\mathbf{Z}^{H_2 \backslash X}) = {}^{H_2}\mathbf{Z}^X$. Vanwege de injectiviteit van ψ geldt nu dat ${}^{H_2}(\mathbf{Z}^X)$ en $\mathbf{Z}^{H_2 \backslash X}$ isomorf zijn als $\mathbf{Z}$-modulen. □

Propositie 5.4. *De $\mathbf{Z}$-modulen $T(H_1, H_2)$ en $\mathbf{Z}^{H_2 \backslash G / H_1}$ zijn isomorf.*

Bewijs. We gebruiken het feit dat uit lemma 5.2 volgt dat $\mathbf{Z}[G]/\operatorname{I}(H_1)$ en $\mathbf{Z}^{G/H_1}$ isomorf zijn als $\mathbf{Z}[G]$-modulen. Nu kunnen we uit lemma 5.3 concluderen dat ${}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1))$ en $\mathbf{Z}^{H_2 \backslash G/H_1}$ isomorf zijn als $\mathbf{Z}$-modulen, omdat H_2 een werking heeft op G/H_1. Die werking wordt op natuurlijke wijze geïnduceerd door de werking van G op G/H_1. □

Voorbeeld 5.5. We beschouwen de groepenring $\mathbf{Z}[D_4]$, waarbij geldt $D_4 = \langle r, s \rangle$, $srs = r^3$, $r^4 = s^2 = \mathrm{id}$. Laat $H_1 = H_2 = \langle s \rangle$ twee ondergroepen van D_4 zijn. Er geldt dat een $\mathbf{Z}$-basis voor $\mathbf{Z}^{H_2 \backslash G/H_1}$ gegeven wordt door

$$\langle s \rangle, r^2\langle s \rangle, r\langle s \rangle \cup r^3\langle s \rangle.$$

Uit propositie 5.4 volgt nu dat een $\mathbf{Z}$-basis voor $T(H_1, H_2)$ gegeven wordt door $\overline{\mathrm{id}}$, $\overline{r^2}$ en $\overline{r + r^3}$, waarbij $\overline{x}$ staat voor $x + \operatorname{I}(H_1)$, $x \in \mathbf{Z}[D_4]$.

Laat nu L een eindige Galoisuitbreiding zijn van $\mathbf{Q}$ met Galoisgroep G. Zijn K_1, K_2 twee deellichamen van L en H_1 en H_2 de ondergroepen van G die corresponderen met respectievelijk K_1 en K_2. We zullen een spoor-, norm- en samenstellingsafbeelding definiëren die elementen zijn van respectievelijk $\operatorname{Hom}((K_1, +), (K_2, +))$, $\operatorname{Hom}(K_1^*, K_2^*)$ en $\operatorname{Bilin}(T(H_1, H_2) \times T(H_0, H_1), T(H_0, H_2))$, waarbij H_0 een ondergroep is van G (die correspondeert met $K_0 \subseteq L$). Hiervoor gebruiken we de volgende propositie.

Propositie 5.6. *Zij M een $\mathbf{Z}[G]$-moduul. Dan is er een welgedefinieerde $\mathbf{Z}$-bilineaire afbeelding*

$$\begin{aligned}\chi_M : \mathbf{Z}[G]/\operatorname{I}(H_1) \times {}^{H_1}M &\to M \\ (r + \operatorname{I}(H_1),\ m) &\mapsto rm.\end{aligned}$$

Als $\overline{r} \in {}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1))$ en $m \in {}^{H_1}M$, geldt dat $\chi_M(\overline{r}, m) \in {}^{H_2}M$.

Bewijs. We merken allereerst op dat χ_M een $\mathbf{Z}$-bilineaire afbeelding is vanwege de moduuleigenschappen.

We zullen bewijzen dat de keuze van rm representantonafhankelijk is. Laat $r, r' \in \mathbf{Z}[G]$ zijn zodanig dat $r' \equiv r \mod \operatorname{I}(H_1)$ en $m \in {}^{H_1}M$. Dan geldt dat $r'm - rm = (r' - r)m$ wegens het feit dat M een $\mathbf{Z}[G]$-moduul is. In het bijzonder geldt dat $r' - r \in \operatorname{I}(H_1)$. We zullen nu laten zien dat wanneer $x \in \operatorname{I}(H_1)$, er geldt dat $xm = 0$. Het volstaat om voor de voortbrengers $h - 1$, $h \in H_1$ van $\operatorname{I}(H_1)$ aan te tonen dat geldt dat $(h-1)m = 0$. Er geldt $(h-1)m = hm - m = m - m = 0$, waarbij $hm = m$ omdat $m \in {}^{H_1}M$. Hieruit volgt dus $r'm - rm = 0$, oftewel $r'm = rm$.

Vervolgens bewijzen we het tweede deel van de propositie. Laat $\overline{r} \in {}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1))$ zijn, dan geldt voor alle $h \in H_2$ dat $h\overline{r} = \overline{hr} = \overline{r}$. Zo volgt voor alle $m \in M$ dat $rm = \chi_M(\overline{r}, m) = \chi_M(\overline{hr}, m) = hrm$, oftewel $\chi_M((\overline{r}, m)) \in {}^{H_2}M$. □

We noteren Γ_M voor het homomorfisme

$$\begin{aligned}\Gamma_M : {}^{H_2}(\mathbf{Z}[G]/\operatorname{I}(H_1)) &\to \operatorname{Hom}({}^{H_1}M, {}^{H_2}M) \\ \overline{r} &\mapsto (m \mapsto \chi_M(\overline{r}, m))\end{aligned}$$

die aan de hand van χ_M gedefinieerd is. We nemen M gelijk aan respectievelijk $(L, +)$, L^* en $\mathbf{Z}[G]/\operatorname{I}(H_0)$. Allereerst beschouwen we het geval dat $M = (L, +)$. Ook nemen we in $\mathbf{Z}[G]/\operatorname{I}(H_1)$ de vaste punten onder H_2. Er geldt dat

$$\chi_{(L,+)} : T(H_1, H_2) \times (K, +) \to (K_2, +).$$

Dit volgt omdat ${}^{H_i}(L, +) = (K_i, +)$, $i \in \{1, 2\}$. Vanwege de $\mathbf{Z}$-bilineairiteit volgt hieruit het volgende homomorfisme dat ons een spoorafbeelding $\operatorname{Tr}_{\overline{r}}$ met $\overline{r} \in T(H_1, H_2)$ geeft:

$$\begin{aligned}\Gamma_{(L,+)} := \operatorname{Tr} : T(H_1, H_2) &\to \operatorname{Hom}((K_1, +), (K_2, +)) \\ \overline{r} &\mapsto \operatorname{Tr}_{\overline{r}} := \big(m \mapsto \chi_{(L,+)}(\overline{r}, m)\big)\end{aligned} \tag{4}$$

Analoog krijgen we als we $M = L^*$ nemen het volgende homomorfisme dat ons een normafbeelding geeft:

$$\begin{aligned} \Gamma_{L^*} := N : T(H_1, H_2) &\to \mathrm{Hom}(K_1^*, K_2^*) \\ \overline{r} &\mapsto N_{\overline{r}} := \big(m \mapsto \chi_{L^*}(\overline{r}, m)\big) \end{aligned} \tag{5}$$

Tot slot nemen we $M = \mathbf{Z}[G]/\operatorname{I}(H_0)$, dan volgt

$$\circ := \chi_{\mathbf{Z}[G]/\operatorname{I}(H_0)} : T(H_1, H_2) \times T(H_0, H_1) \to T(H_0, H_2),$$

oftewel we verkrijgen een bilineaire samenstellingsafbeelding van elementen van $T(H_1, H_2)$ en $T(H_0, H_1)$ naar elementen uit $T(H_0, H_2)$.

Aan de hand van bovenstaande afbeeldingen krijgen we het volgende diagram:

$$\begin{array}{ccc} T(H_1, H_2) \times T(H_0, H_1) & \xrightarrow{\quad\circ\quad} & T(H_0, H_2) \\ \big\downarrow{\scriptstyle (\Gamma_M, \Gamma_M)} & & \big\downarrow{\scriptstyle \Gamma_M} \\ \mathrm{Hom}({}^{H_1}M, {}^{H_2}M) \times \mathrm{Hom}({}^{H_0}M, {}^{H_1}M) & \xrightarrow{\circ} & \mathrm{Hom}({}^{H_0}M, {}^{H_2}M) \end{array}$$

Wegens propositie 5.6 zijn de afbeeldingen in dit diagram welgedefinieerd. We gaan na dat het diagram commuteert. Laat $r + \operatorname{I}(H_1) \in T(H_1, H_2)$, $s + \operatorname{I}(H_0) \in T(H_0, H_1)$ en $m \in {}^{H_0}M$ zijn. Door het diagram van linksboven naar rechtsonder te doorlopen via $T(H_0, H_2)$, krijgen we

$$(m \mapsto \chi_M(\overline{rs}, m)) = (m \mapsto (rs)m) \in \mathrm{Hom}({}^{H_0}M, {}^{H_2}M).$$

Door het diagram van linksboven naar rechtsonder te doorlopen via $\mathrm{Hom}({}^{H_1}M, {}^{H_2}M) \times \mathrm{Hom}({}^{H_0}M, {}^{H_1}M)$ verkrijgen we

$$(m \mapsto \chi_M(\overline{r}, \chi_M(\overline{s}, m)) = (m \mapsto r(sm)) \in \mathrm{Hom}({}^{H_0}M, {}^{H_2}M).$$

Vanwege de moduuleigenschappen geldt $(rs)m = r(sm)$, waarmee is bewezen dat bovenstaand diagram commuteert.

Als $M = (L, +)$, krijgen we het volgende commutatieve diagram, waarin F^+ staat voor $(F, +)$ met F een willekeurig lichaam uit het diagram.

$$\begin{array}{ccc} T(H_1, H_2) \times T(H_0, H_1) & \xrightarrow{\quad\circ\quad} & T(H_0, H_2) \\ \big\downarrow{\scriptstyle (\mathrm{Tr}, \mathrm{Tr})} & & \big\downarrow{\scriptstyle \mathrm{Tr}} \\ \mathrm{Hom}(K_1^+, K_2^+) \times \mathrm{Hom}(K_0^+, K_1^+) & \xrightarrow{\circ} & \mathrm{Hom}(K_0^+, K_2^+) \end{array}$$

Net zo krijgen we een commutatief diagram met de hierboven gedefinieerde normafbeelding N, door in het commutatieve diagram hierboven alle Tr te vervangen voor N en alle F^+ te vervangen voor F^* waarbij F een lichaam uit het diagram is.

$$\begin{array}{ccc} T(H_1,H_2)\times T(H_0,H_1) & \xrightarrow{\ \circ\ } & T(H_0,H_2) \\ \downarrow{\scriptstyle (N,N)} & & \downarrow{\scriptstyle N} \\ \mathrm{Hom}(K_2^*,K_3^*)\times \mathrm{Hom}(K_1^*,K_2^*) & \xrightarrow{\ \circ\ } & \mathrm{Hom}(K_1^*,K_3^*) \end{array}$$

Voorbeeld 5.7. In dit voorbeeld staat F^+ voor $(F,+)$ met F een willekeurig lichaam. Als we nu $\mathbf{Z}[G] = \mathbf{Z}[D_4]$ nemen, net als in voorbeeld 5.5 en $H_0 = H_1 = H_2 = \langle s \rangle$. Dan volgt dat $\overline{r+r^3} \in T(H_0,H_1)$ en $2\overline{\mathrm{id}} + \overline{r^2} \in T(H_1,H_2)$, omdat $\overline{\mathrm{id}}$, $\overline{r^2}$ en $\overline{r+r^3}$ een basis vormt voor zowel $T(H_0,H_1)$ als $T(H_1,H_2)$ (zie voorbeeld 5.5). We doorlopen het commutatieve diagram eerst van linksboven naar rechtsonder via $T(H_0,H_2)$. Er geldt dat $(2\overline{\mathrm{id}}+\overline{r^2})\circ(\overline{r+r^3}) = \chi_{\mathbf{Z}[G]/\,\mathrm{I}(H_0)}(2\overline{\mathrm{id}}+\overline{r^2},\overline{r+r^3}) = 3\overline{r+r^3}$. We passen vervolgens de spoorafbeelding op toe om het volgende te verkrijgen:

$$\begin{aligned} \mathrm{Tr}_{3\overline{r+r^3}} : K_0^+ &\to K_2^+ \\ x &\mapsto 3r(x) + 3r^3(x). \end{aligned}$$

Nu doorlopen we het diagram van linksboven naar rechtsonder via $\mathrm{Hom}(K_1^+,K_2^+)\times\mathrm{Hom}(K_0^+,K_1^+)$. Er geldt $\mathrm{Tr}_{2\overline{\mathrm{id}}+\overline{r^2}} = (x \mapsto 2x + r^2(x)) \in \mathrm{Hom}(K_1^+,K_2^+)$ en $\mathrm{Tr}_{\overline{r+r^3}} = (x \mapsto r(x)+r^3(x)) \in \mathrm{Hom}(K_0^+,K_1^+)$. Dan stellen we deze homomorfismen samen en verkrijgen het homomorfisme:

$$\begin{aligned} \mathrm{Tr}_{2\overline{\mathrm{id}}+\overline{r^2}} \circ \mathrm{Tr}_{\overline{r+r^3}} &= (x \mapsto 2(r(x)+r^3(x)) + r^2(r(x)+r^3(x)) \\ &= (x \mapsto 3r(x)+3r^3(x)) = \mathrm{Tr}_{3\overline{r+r^3}} \in \mathrm{Hom}(K_0^+,K_2^+), \end{aligned}$$

net als toen we het diagram via $T(H_0,H_2)$ doorliepen.

6. Reflex-typen

We zullen resultaten over primitieve CM-typen (paragraaf 4) combineren met de resultaten over de verzameling transfers (paragraaf 5). Hiertoe beschouwen we de volgende definitie, die we ook in paragraaf 1 gezien hebben (als definitie 1.4). Hier zullen we deze definitie illustreren met een voorbeeld. Verder nemen we aan dat elk lichaam bevat is in $\mathbf{C}$.

Definitie 6.1. Zij $L \subseteq \mathbf{C}$ de normale afsluiting van een CM-lichaam K en G de Galoisgroep van K. Laat Φ een CM-type van K zijn en Φ_L het CM-type van L geïnduceerd door Φ zijn. Laat $H^r = \{g \in G : g\Phi = \Phi\}$ zijn en $K^r = L^{H^r}$ zijn. Het *reflex-type* Φ^r van Φ is

$$\Phi^r = \{\varphi^{-1}|_{K^r} : \varphi \in \Phi_L\}.$$

Er geldt $\rho \notin H^r$, hiermee geldt $\rho|_{K^r} \neq \mathrm{id}$ en omdat $\rho(K^r) = L^{\rho H^r \rho^{-1}} = L^{H^r} = K^r$ geldt dat ρ een automorfisme van K^r induceert. En daaruit volgt met lemma 2.10 dat K^r een CM-lichaam is. In [5, Proposition II.28 op p.62] wordt bewezen dat Φ^r een CM-type is.

Voorbeeld 6.2. Het CM-lichaam $K = \mathbf{Q}(X)/(X^4 + 8X^2 + 14)$ uit voorbeeld 3.3(3) heeft D_4 als Galoisgroep. Laat $D_4 = \langle r, s\rangle$ zijn waarvoor geldt dat $srs = r^3$ en $r^4 = s^2 = \mathrm{id}$. Zij L de normale afsluiting van K. Een CM-type van K is $\Phi = \{\mathrm{id}\,|_K, r|_K\}$ wegens lemma 4.3. Er geldt $\Phi_L = \{\mathrm{id}, r, rs, s\}$, $H^r = \{\mathrm{id}, rs\}$ en $K^r = L^{\langle rs\rangle}$. De inversen van de elementen uit Φ_L zijn gelijk aan respectievelijk id, r^3, rs en s. Zo volgt dat $\Phi^r = \{\mathrm{id}\,|_{K^r}, s|_{K^r}\}$.

Laat K een CM-lichaam zijn en G de Galoisgroep van $K/\mathbf{Q}$ zijn. De ondergroepen $H, H^r \subseteq G$ corresponderen respectievelijk met K en K^r. In het vervolg van deze paragraaf zullen we de CM-typen Φ van K en Φ^r van K^r opvatten als elementen van respectievelijk $T(H, H^r)$ en $T(H^r, H)$. We zullen uitleggen op welke manier we dit doen. Er geldt dat voor alle $\varphi \in \mathrm{Hom}(K, \mathbf{C})$ er een $\tilde{\varphi} \in G$ bestaat met $\tilde{\varphi}|_K = \varphi$. We beschouwen Φ als

$$\tilde{\Phi} = \sum_{\varphi \in \Phi} \tilde{\varphi} + \mathrm{I}(H) \in \mathbf{Z}[G]/\,\mathrm{I}(H).$$

We bewijzen dat $\tilde{\Phi}$ onafhankelijk is van de keuze van $\tilde{\varphi}$. Laat $\tilde{\varphi}_1, \tilde{\varphi}_2 \in G$ zijn waarvoor geldt dat $\tilde{\varphi}_1|_K = \tilde{\varphi}_2|_K = \varphi$, dan geldt dat $\tilde{\varphi}_1 - \tilde{\varphi}_2 = \tilde{\varphi}_1(1 - {\tilde{\varphi}_1}^{-1}\tilde{\varphi}_2) \in \mathrm{I}(H)$. Dit geldt, omdat ${\tilde{\varphi}_1}^{-1}\tilde{\varphi}_2|_K = \mathrm{id}$ en daaruit volgt

dat ${\tilde{\varphi_1}}^{-1}\tilde{\varphi_2} \in H$. Per definitie van H^r geldt $h\Phi = \Phi$ voor alle $h \in H^r$. Deze gelijkheid blijft behouden als we Φ opvatten als $\tilde{\Phi}$, dat wil zeggen dat $h\tilde{\Phi} = \tilde{\Phi}$, dus er geldt dat $\tilde{\Phi} \in T(H, H^r)$.

Het bewijs dat

$$\tilde{\Phi}^r = \sum_{\varphi \in \Phi^r} \tilde{\varphi} + \mathrm{I}(H^r) \in \mathbf{Z}[G]/\mathrm{I}(H^r)$$

onafhankelijk is van de keuze van $\tilde{\varphi}$, gaat analoog aan het bewijs dat $\tilde{\Phi}$ onafhankelijk is van de keuze van $\tilde{\varphi}$. We zullen dat bewijs dus hier niet uitschrijven. Wel zullen we bewijzen dat $h\tilde{\Phi}^r = \tilde{\Phi}^r$ voor $h \in H$. Er geldt $\Phi_L = \Phi_L h$, omdat $h|_K = \mathrm{id}$. Het nemen van inversen geeft ons de gelijkheid $\Phi_L^{-1} = h^{-1}\Phi_L^{-1}$. Door met h te vermenigvuldigen, volgt $h\Phi_L^{-1} = \Phi_L^{-1}$. Als we deze gelijkheid beperken tot K^r, verkrijgen we $h\Phi^r = \Phi^r$. Deze gelijkheid blijft behouden als we Φ^r opvatten als $\tilde{\Phi}^r$, dat wil zeggen dat $h\tilde{\Phi}^r = \tilde{\Phi}^r$, dus er geldt $\tilde{\Phi}^r \in T(H, H^r)$.

Omdat $\tilde{\Phi}$ en $\tilde{\Phi}^r$ elementen zijn van respectievelijk $T(H, H^r)$ en $T(H^r, H)$, kunnen we vergelijking (4) en (5) uit de vorige paragraaf, paragraaf 5 toepassen op $\tilde{\Phi}$ en $\tilde{\Phi}^r$. Op deze manier definiëren we de spoor- en normafbeelding van $\tilde{\Phi}$: $\mathrm{Tr}_{\tilde{\Phi}}$ en $N_{\tilde{\Phi}}$. Evenzo definiëren we de spoor- en normafbeelding van $\tilde{\Phi}^r$: $\mathrm{Tr}_{\tilde{\Phi}^r}$ en $N_{\tilde{\Phi}^r}$. De rekenregels die uit de commutatieve diagrammen uit voorbeeld 5.7 volgen, kunnen dus toegepast worden op deze homomorfismen.

Voorbeeld 6.3. We zullen het CM-lichaam $K = \mathbf{Q}(X)/(X^4+8X^2+14)$ uit voorbeeld 3.3(3) beschouwen dat D_4 als Galoisgroep heeft. In voorbeeld 6.2 zagen we dat een CM-type van dit lichaam gelijk is aan $\Phi = \{\mathrm{id}\,|_K, r|_K\}$ en dat het reflex-type van Φ gelijk is aan $\Phi^r = \{\mathrm{id}\,|_{K^r}, s|_{K^r}\}$. Uit bovenstaande volgt dat we Φ als $\tilde{\Phi} = \sum_{\varphi\in\Phi} \tilde{\varphi} + \mathrm{I}(H) = \overline{\mathrm{id}} + \overline{r} \in T(H, H^r)$. Zo geldt ook dat we Φ^r op kunnen vatten als $\tilde{\Phi}^r = \sum_{\varphi\in\Phi} \tilde{\varphi} + \mathrm{I}(H^r) = \overline{\mathrm{id}} + \overline{s} \in T(H^r, H)$.

Nu beschouwen we de volgende ondergroep van $T(H, H)$ die aan de hand van $\tilde{\Phi}^r$ gedefinieerd is:

$$\mathcal{G}_\Phi = \tilde{\Phi}^r \circ T(H, H^r) + \mathbf{Z} \cdot \sum_{gH \in G/H} (g + \mathrm{I}(H)).$$

Het is eenvoudig na te gaan dat $\overline{\mathrm{id}} - \overline{\rho} \in T(H, H)$. We zullen de vraag of ook geldt dat $\overline{\mathrm{id}} - \overline{\rho} \in \mathcal{G}_\Phi$ voor alle primitieve CM-typen van CM-lichamen van graad 2, 4 en 6 beantwoorden. Deze vraag komt uit [3, Proposition 5.3 en Equation (5.1)]. Bij het beantwoorden van deze vraag is het volgende lemma handig.

Lemma 6.4. *Zij K een CM-lichaam en Φ een CM-type van K. Laat G de Galoisgroep zijn van $K/\mathbf{Q}$ en laat $H \subseteq G$ de ondergroep van G zijn die correspondeert met K. Laat verder Υ een CM-type zijn uit de baan van Φ onder linksvermenigvuldiging met G en $H^r_\Upsilon = \{g \in G : g\Upsilon = \Upsilon\}$, dan geldt*

$$\Upsilon^r \circ T(H, H^r_\Upsilon) = \Phi^r \circ T(H, H^r).$$

Bewijs. Zij $K^r_\Upsilon = K^{H^r_\Upsilon}$. Omdat Υ in dezelfde baan zit als Φ onder linksvermenigvuldiging met G, geldt dat $\Upsilon = g \cdot \Phi$ voor een $g \in G$. Laat $h \in H^r$ zijn, dan geldt $ghg^{-1}(g\Phi) = (ghg^{-1}g)\Phi = (gh)\Phi = g\Phi$, dus zo volgt dat $gH^rg^{-1} \subseteq H^r_\Upsilon$. Laat nu $h \in H^r_\Upsilon$ zijn, dan geldt dat $h\Upsilon = \Upsilon$, ofwel $hg\Phi = g\Phi$ en zo volgt dat $g^{-1}hg\Phi = \Phi$ en dat wil zeggen dat $g^{-1}hg \in H^r$, waaruit volgt dat $h \in gH^rg^{-1}$. Er geldt dus dat $H^r_\Upsilon \subseteq gH^rg^{-1}$ en samen met de eerdere inclusie volgt $H^r_\Upsilon = gH^rg^{-1}$. Wegens de Galoiscorrespondentie geldt $K^r_\Upsilon = L^{gH^rg^{-1}} = g(K^r)$. Er geldt dus dat $g|_{K^r}$ een isomorfisme van K^r naar K^r_Υ is. Het is eenvoudig na te gaan dat $\Upsilon_L = g \cdot \Phi_L$. Inversen van elementen uit Υ_L zijn hiermee van de vorm $\varphi^{-1} \circ g^{-1}$ met $\varphi \in \Phi_L$. Het element $g^{-1}|_{K^r_\Upsilon}$ beeldt af in K^r, want het is de inverse van $g|_{K^r}$. Hieruit volgt dat $\Upsilon^r = \Phi^r \circ g^{-1}$. Laat nu $\overline{x} \in T(H, H^r)$ zijn, dan geldt voor $h \in H^r$ dat $ghg^{-1}(g\overline{x}) = gh\overline{x} = g\overline{x}$, dus $g\overline{x}$ is vast onder werking van H^r_Υ. Zo volgt dat $gT(H, H^r) \subseteq T(H, H^r_\Upsilon)$. We zullen nu de inclusie $T(H, H^r_\Upsilon) \subseteq gT(H, H^r)$ bewijzen. Zij $\overline{y} \in T(H, H^r_\Upsilon) = T(H, gH^rg^{-1})$, dan geldt voor alle $h \in H^r$ dat $ghg^{-1}\overline{y} = \overline{y}$, oftewel $hg^{-1}\overline{y} = g^{-1}\overline{y}$, dus $\overline{y} \in gT(H, H^r)$, dat wil zeggen $T(H, H^r_\Upsilon) \subseteq gT(H, H^r)$ en met de andere inclusie samen geeft dit $T(H, H^r_\Upsilon) = gT(H, H^r)$. Zo volgt $\Phi^r \circ T(H, H^r) = \Phi^r \circ g^{-1} \circ g \circ T(H, H^r) = \Upsilon^r \circ T(H, H^r_\Upsilon)$. □

De volgende stelling, die dezelfde is als stelling 1.5 uit de inleiding (paragraaf 1), geeft aan of $\overline{\mathrm{id}} - \overline{\rho} \in T(H, H)$ bevat is in de groep $\mathcal{G}_\Phi$ voor verschillende primitieve CM-typen van CM-lichamen van graad 2, 4 en 6.

Stelling 6.5. *De groep $\mathcal{G}_\Phi$ bevat het element $\overline{\mathrm{id}} - \overline{\rho} \in T(H, H)$ voor alle primitieve CM-typen van CM-lichamen van graad 2 en 4 en voor CM-lichamen van graad 6 als de Galoisgroep van dit lichaam isomorf is aan C_6 of D_6, maar niet voor de primitieve CM-typen van CM-lichamen met Galoisgroep isomorf aan $C_2^3 \rtimes C_3$ of $C_2^3 \rtimes S_3$.*

Bewijs. De notatie die in dit bewijs gebruikt wordt om de Galoisgroepen te beschrijven, is dezelfde als in de lemma's uit paragraaf 4.1, 4.2 en 4.3

voor CM-lichamen van graad respectievelijk 2, 4 en 6. We lichten de notatie hier niet expliciet toe, maar verwijzen naar deze paragrafen voor meer uitleg. Verder noteren we $\underline{f}$ in plaats van $f|_K$ voor $f \in G$.

Wegens lemma 6.4 is het voldoende om voor één CM-type per baan na te gaan of $\overline{\mathrm{id}} - \overline{\rho} \in T(H,H)$ bevat is in de groep $\mathcal{G}_\Phi$. In paragraaf 4 zagen we dat er per CM-lichaam één of geen (voor V_4) baan met primitieve CM-typen is. In de volgende tabel is per Galoisgroep waarvoor $\overline{\mathrm{id}} - \overline{\rho}$ wel in $\mathcal{G}_\Phi$ zit, aangegeven voor welke waarden $\alpha \in T(H,H^r)$ en $z \in \mathbf{Z}$ geldt dat $\overline{\mathrm{id}} - \overline{\rho} = \tilde{\Phi}^r \circ \alpha + z \cdot \sum_{gH \in G/H}(g + \mathrm{I}(H))$ voor één CM-type Φ. Er is ook aangegeven welk CM-type dat is.

graad	Galoisgroep	CM-type	α	z
2	$C_2 = \langle \rho \rangle$	$\{\mathrm{id}\}$	$\overline{\mathrm{id}} - \overline{\rho}$	0
4	$V_4 = \langle \rho, \sigma \rangle$	n.v.t.	n.v.t.	n.v.t.
4	$C_4 = \langle r \rangle$	$\{\mathrm{id}, r\}$	$\overline{\mathrm{id}} + \overline{r}$	-1
4	$D_4 = \langle r, s \rangle$	$\{\underline{\mathrm{id}}, \underline{r}\}$	$\overline{\mathrm{id}} + \overline{r}$	-1
6	$C_6 = \langle r \rangle$	$\{r^{-1}, \mathrm{id}, r\}$	$\overline{\mathrm{id}} + \overline{r^3} - \overline{r^4} + \overline{r^5}$	-1
6	$D_6 = \langle r, s \rangle$	$\{\underline{r^{-1}}, \underline{\mathrm{id}}, \underline{r}\}$	$\overline{\mathrm{id}} + \overline{r^3} - \overline{r^4} + \overline{r^5}$	-1

Tabel 3: Waarden voor α en z.

Dit bewijst dat $\overline{\mathrm{id}} - \overline{\rho}$ wel in $\mathcal{G}_\Phi$ bevat is als de Galoisgroep isomorf is aan een groep uit tabel 3. We gaan nu bewijzen dat $\overline{\mathrm{id}} - \overline{\rho} \notin \mathcal{G}_\Phi$ als G isomorf is aan $C_2^3 \rtimes C_3$ of $C_2^3 \rtimes S_3$. Voor deze Galoisgroepen geeft propositie 5.4, samen met een berekening van $H^r \backslash G / H$ de basis $\overline{\mathrm{id} + r^2 + r^4}$, $\overline{r + r^3 + r^5}$ voor $T(H,H^r)$, dus zou $\alpha = a\overline{\mathrm{id} + r^2 + r^4} + b\overline{r + r^3 + r^5}$ moeten gelden met $a, b \in \mathbf{Z}$. Het expliciet uitrekenen van $\tilde{\Phi}^r \circ \alpha + z \cdot \sum_{gH \in G/H}(g + \mathrm{I}(H))$ geeft

$$(4a + z)\overline{\mathrm{id}} + (4b + z)\overline{\rho} + (2a + 2b + z)\overline{r^2 + r^4} + (2a + 2b + z)\overline{r + r^5},$$

waarbij $\overline{\rho} = \overline{r^3}$ geldt. Door het oplossen van het volgende stelsel vinden we voor welke waarden van a, b en z het bovenstaande element gelijk is aan $\overline{\mathrm{id}} - \overline{\rho}$:

$$\begin{cases} 4a + z & = 1 \\ 4b + z & = -1 \\ 2a + 2b + z & = 0 \end{cases}$$

Voor de oplossing geldt onder andere $1 \equiv z \equiv -1 \pmod 4$, wat een tegenspraak oplevert. □

7. Referenties

[1] B. Dina, S. Ionica en J.R. Sijsling. "Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal complex multiplication". In: *Mathematics of computation* 92.339 (2023), p. 349–383. ISSN: 0025-5718.

[2] B. Dodson. "The Structure of Galois Groups of CM-Fields". In: *Transactions of the American Mathematical Society* 283.1 (1984), p. 1–32. ISSN: 0002-9947.

[3] A. Enge en T.C. Streng. "Schertz style class invariants for quartic CM fields". [Online, nog niet gepubliceerd], `https://arxiv.org/abs/1610.04505v3`.

[4] The LMFDB Collaboration. *The L-functions and modular forms database*. [Online; geraadpleegd 16 april 2023], `https://www.lmfdb.org`. 2023.

[5] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Princeton mathematical series. Princeton, NJ: Princeton University Press, 1998. ISBN: 0-691-01656-9.

[6] P. Stevenhagen. "Algebra I". Collegedictaat Universiteit Leiden. [Online; geraadpleegd 29 april 2023], `https://websites.math.leidenuniv.nl/algebra/algebra1.pdf`. 2023.

[7] P. Stevenhagen. "Algebra II". Collegedictaat Universiteit Leiden. [Online; geraadpleegd 13 juni 2023], `https://websites.math.leidenuniv.nl/algebra/algebra2.pdf`. 2022.

[8] P. Stevenhagen. "Algebra III". Collegedictaat Universiteit Leiden. [Online; geraadpleegd 29 april 2023], `https://websites.math.leidenuniv.nl/algebra/algebra3.pdf`. 2020.

[9] T.C Streng. "Complex multiplication of abelian surfaces". Proefschrift. Universiteit Leiden, 2010. ISBN: 978-90-5335-291-5.