Complex multiplication constructions of abelian extensions of quartic fields

Asuncion, J.G.

Samenvatting

Titel: Constructie van abelse uitbreidingen van kwartische lichamen door complexe vermenigvuldiging

De stelling van Kronecker-Weber is een klassiek resultaat in de getaltheorie. Het doet een uitspraak over *abelse uitbreidingen*, Galoisuitbreidingen van een getallenlichaam met een abelse Galoisgroep.

> **Stelling van Kronecker-Weber.**
> Elke eindige abelse uitbreiding van $\mathbb{Q}$ is een deeluitbreiding van een cyclotomische uitbreiding $\mathbb{Q}(\zeta_m)$ met $\zeta_m = \exp(2\pi i/m)$ voor een $m \in \mathbb{Z}_{>0}$.
>
> De Galoisgroep $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorf met $(\mathbb{Z}/m\mathbb{Z})^\times$ via de afbeelding
>
> $$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a + m\mathbb{Z} &\longmapsto (\zeta_m \mapsto \zeta_m^a). \end{aligned}$$

Deze stelling, gecombineerd met de Galoistheorie, vertelt ons dat elke abelse uitbreiding van $\mathbb{Q}$ kan worden uitgedrukt als $\mathbb{Q}(\boldsymbol{\alpha})$ waarbij $\boldsymbol{\alpha}$ een polynoom is in een m-de eenheidswortel voor een positief geheel getal m. De abelse uitbreiding

$$L = \mathbb{Q}[X]/(X^3 - 3X + 1)$$

bevindt zich bijvoorbeeld in het cyclotomische lichaam $\mathbb{Q}(\zeta_9)$. Het lichaam L is namelijk gelijk aan

$$\mathbb{Q}(\zeta_9 + \zeta_9^8).$$

Hoewel L ook bevat is in andere cyclotomische lichamen $\mathbb{Q}(\zeta_n)$ voor andere positieve gehele getallen n, is het gehele getal 9 het kleinste gehele getal dat aan deze voorwaarde voldoet.

Het twaalfde van de 23 problemen van Hilbert, ook bekend als Kronecker's Jugendtraum[1], vraagt om een analogon van de stelling van Kronecker-Weber te vinden wanneer het grondlichaam $\mathbb{Q}$ wordt vervangen door een ander getallenlichaam.

De Klassenlichamentheorie vertelt ons dat er voor elk getallenlichaam K en voor elk positief geheel getal m een bijectie bestaat tussen de verzameling ondergroepen van de zogenaamde straalklassengroep $\mathrm{Cl}_K(m)$ van K en de verzameling abelse uitbreidingen L/K van conductor[2] die m deelt. Echter, gegeven een ondergroep van $\mathrm{Cl}_K(m)$, geeft de corresponderende bijectie niet noodzakelijkerwijs een expliciete beschrijving van de abelse uitbreiding.

Niet alle hoop is verloren aangezien er een geval bestaat waarvoor een expliciete analogon van de **Stelling van Kronecker-Weber** bekend is. Dit is het geval wanneer het grondlichaam K een imaginair kwadratisch getallenlichaam is, in plaats van de $\mathbb{Q}$ van Kronecker-Weber. De theorie van complexe vermenigvuldiging (CM-theorie) (Paragraaf 1.2) voor elliptische krommen levert deze analoog. Met behulp van de CM-theorie kan men definiërende polynomen vinden van elke abelse uitbreiding van elk imaginair kwadratisch lichaam K.

Shimura en Taniyama ontwikkelden in de jaren vijftig een veralgemening van de CM-theorie naar hoger dimensionale, hoofdgepolariseerde abelse variëteiten. Net als haar tegenhanger binnen de theorie van elliptische krommen, beschrijft de theorie expliciet abelse uitbreidingen van zogenaamde CM-lichamen in termen van speciale waarden van modulaire functies. De theorie dekt echter niet *alle* abelse uitbreidingen van een CM-lichaam en geeft daarom op zichzelf geen analoog van de stelling van Kronecker-Weber.

In dit proefschrift, laten we echter zien dat we Shimura's CM-theorie kunnen gebruiken om expliciet de grootste onvertakte[3] abelse uitbreiding, het Hilbert-klassenlichaam genoemd, van *elk* primitief vierdegraads CM-lichaam te vinden. Met dit proefschrift hopen we verder onderzoek te stimuleren naar het gebruik van CM-theorie om onderzoek naar abelse uitbreidingen te bevorderen.

Dit proefschrift is onderverdeeld in de volgende hoofdstukken.

[1] Kroneckers jeugddroom
[2] Zie de definitie van conductor op pagina 22
[3] Een abelse uitbreiding is onvertakt als en slechts dan als de conductor 1 is.

In Hoofdstuk 1 bekijken we hoe de CM-theorie wordt gebruikt om alle abelse uitbreidingen van een imaginair kwadratisch getallenlichaam te vinden. In Hoofdstuk 2, bespreken we de algemenere CM-theorie.

Een aanpassing van [30, Theorem 2] van Shimura laat zien dat er een positief geheel getal m bestaat waarvoor het Hilbert-klassenlichaam $H_{K^r}(1)$ van een primitief vierdegraads CM-lichaam K^r met reëel kwadratische deellichaam K_0^r zich in de compositum Ξ_m van het straalklassenlichaam $H_{K_0^r}(m)$ van K_0^r en een abelse uitbreiding

$$\mathrm{CM}_{K^r,\Phi^r}(m)$$

van K^r (gedefinieerd in Paragraaf 2.1.3, gegeven door CM-theorie) bevindt.

In Hoofdstuk 3 doen we verschillende dingen die verband houden met dit resultaat van Shimura. Om te beginnen geven we een stelling die ons een geheel getal m geeft waarvoor het resultaat van Shimura waar is. Vervolgens definiëren we, voor elk positief geheel getal m, de Shimura-straalklassengroep $\mathfrak{C}_K(m)$ van een CM-lichaam K gerelateerd aan K^r. Met behulp van deze Shimura-straalklassengroep geven we een algoritme dat een positief geheel getal m' als invoer neemt en teruggeeft of het Hilbert-klassenlichaam al dan niet is opgenomen in $\Xi_{m'}$. Dit algoritme stelt ons in staat om het kleinste positieve gehele getal m te vinden waarvoor het resultaat van Shimura waar is.

Het bovengenoemde resultaat van Shimura is nuttig voor rekenkundige doeleinden omdat beide delen van het compositum expliciet kunnen worden berekend. In Hoofdstuk 4 laten we zien hoe de abelse uitbreiding $\mathrm{CM}_{K^r,\Phi^r}(m)$ berekend kan worden. Straalklassenlichamen van reëel kwadratische lichamen, zoals $H_{K_0^r}(m)$, kunnen in de praktijk efficiënt worden berekend en we citeren de relevante artikelen in de inleiding van het hoofdstuk.

Om de bovenstaande theorie echt expliciet te maken, hebben we de meeste van de in dit proefschrift besproken algoritmen geïmplementeerd.

Het algoritme voor het berekenen van de Shimura-straalklassengroep maakt gebruik van algoritmen voor het berekenen van kernen, affbeeldingen, quotiënten en groepsuitbreidingen met eindig voortgebrachte abelse groepen en homomorfismen daartussen. Deze algoritmen zijn bekend en kunnen worden gevonden in [6, Chapter 4].

In Hoofdstuk 5 herhalen we deze algoritmen in detail, waarbij we zorgvuldig noteren welke informatie nodig is om welke groepen te berekenen.

Voor zover wij weten, zijn deze algoritmen niet geïmplementeerd in een computer-algebrasysteem op een manier die ze beschikbaar maakt voor de gebruiker. Daarom hebben we deze algoritmen geïmplementeerd en beschikbaar gemaakt als een paar PARI/GP [21] scripts – `fgag.gp` en `fgagshimuray.gp`. De eerste implementeert de vereiste algoritmen uit [6] en de laatste gebruikt de eerste om het algoritme te implementeren dat de Shimura-straalklassengroep berekent.

We gebruiken onze code en andere ingebouwde functies van PARI/GP [21] en SAGE [27] om te laten zien hoe onze methode voor het construeren van een CM-lichaam werkt. In Hoofdstuk 6 geven we expliciete voorbeelden met behulp van ons CM-theorie-algoritme, vergelijken we hoe onze methode presteert ten opzichte van de bekende generieke Kummer-theorie-algoritme en bespreken we de beperkingen van beide benaderingen.