Kummer theory for commutative algebraic groups
Tronto, S.

Samenvatting

Dit proefschrift bestaat uit vier onderzoeksartikelen die verschillende aspecten van de *Kummertheorie voor commutatieve algebraïsche groepen* behandelen, met bijzondere nadruk op expliciete en effectieve resultaten. Om de motivatie achter de studie van dit onderwerp en onze doelen te begrijpen, moeten we een stap terug doen en kijken welke aspecten van de klassieke Kummertheorie we proberen te generaliseren naar algebraïsche groepen.

Kummertheorie

Als n een positief geheel getal is en K een lichaam van karakteristiek copriem met n, kunnen we voor elke $\alpha \neq 0$ in K de *verzameling* $\sqrt[n]{\alpha}$ beschouwen van alle elementen β in een vast gekozen algebraïsche afsluiting $\overline{K}$ van K zodanig dat $\beta^n = \alpha$. Met andere woorden, $\sqrt[n]{\alpha}$ is de verzameling van alle n-de wortels van α. Zij b_0 een n-de wortel van α, dan hebben alle andere wortels de vorm $\zeta\beta_0$ voor een n-de eenheidswortel $\zeta \in \overline{K}$, dat wil zeggen een element zodanig dat $\zeta^n = 1$. Het lichaam voortgebracht over K door alle n-de wortels van α is een Galoisuitbreiding van K die het n-de *cyclotomische lichaam* bevat, dat wil zeggen het lichaam voortgebracht over K door alle n-de eenheidswortels. Dit blijft waar als we α vervangen door een eindig voortgebrachte ondergroep A van de multiplicatieve groep $K^\times$, en we de verzameling $\sqrt[n]{A} = \{\beta \in \overline{K} \mid \beta^n \in A\}$ beschouwen. De klassieke Kummertheorie is grofweg de studie van dit soort lichaamsuitbreidingen.

Het meest klassieke resultaat in de Kummertheorie is de classificatie van de abelse uitbreidingen met exponent die n deelt van een lichaam K dat alle n-de eenheidswortels bevat en waarvan de karakteristiek n niet deelt. Een bijectie tussen de verzameling van dergelijke uitbreidingen, bevat in een vast gekozen algebraïsche afsluiting $\overline{K}$, en de verzameling ondergroepen van $K^\times$ die $(K^\times)^n$ bevatten, wordt namelijk verkregen door L te associëren met $K^\times \cap (L^\times)^n$, zie bijvoorbeeld [Lan02, Theorem VI.8.2].

De Kummertheorie heeft interessante toepassingen bij het bestuderen van bepaalde *dichtheidsproblemen*: als $\alpha \neq 0$ een element is van een getallenlichaam K, dan is de dichtheid van priemidealen $\mathfrak{p}$ van K zodanig dat de multiplicatieve orde van α modulo $\mathfrak{p}$ copriem is met een vast priemgetal ℓ, dan wel een voorgeschreven ℓ-adische valuatie heeft, kan worden uitgedrukt in termen van de graden van de cyclotomische-Kummeruitbreidingen $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha})$ voor alle $n > 0$, waarbij ζ_{ℓ^n} een eenheidswortel van orde ℓ^n is. Zie [Per15] voor het zojuist beschreven geval en [DP16, PS19] voor een generalisatie naar ondergroepen van eindige rang in $K^\times$. Deze problemen hangen nauw samen met het vermoeden van Artin over primitieve wortels, zoals bijvoorbeeld uitgelegd in [Mor12].

Het berekenen van de graden van oneindig veel lichaamsuitbreidingen lijkt misschien een zware taak. Het volgende is echter bekend (zie [PS19, Theorem 1.1] voor een direct bewijs): als A een ondergroep van $K^\times$ is van eindige rang r, dan is er een constante $C > 0$ zodanig dat voor elk positief geheel getal n de verhouding tussen n^r en de graad $[K(\sqrt[n]{A}) : K(\zeta_n)]$ een deler is van C. Dit resultaat kan effectief worden gemaakt, zie [PST20a, Theorem 1.2], en voor het geval $K = \mathbb{Q}$ verschaffen de resultaten van [PST20b] een algoritme waarvan de output een eindige formule is voor deze graden. Dit algoritme is geïmplementeerd in SageMath, zie [Tro19].

Algebraïsche groepen

Tot nu toe hebben we Kummertheorie alleen in de klassieke zin besproken, maar deze concepten kunnen als volgt worden veralgemeend. Zijn K een lichaam, zeg voor de eenvoud van karakteristiek nul, $\overline{K}$ een algebraïsche afsluiting van K, en G een commutatieve algebraïsche groep over K. Als S een deelverzameling van $G(\overline{K})$ is, dan is de *lichaamsuitbreiding van K voortgebracht door S* het deellichaam van $\overline{K}$ verkregen door aan K de coördinaten van de punten van S toe te voegen. Om precies te zijn: als we elke x in S identificeren met een morfisme van schema's $\operatorname{spec} \overline{K} \to \operatorname{spec} K(x)$, dan hebben we een verzameling morfismen $K(x) \to \overline{K}$ als x varieert in S, en de samenstelling van de beelden van deze morfismen is dan per definitie $K(S)$.

Zij nu $A \subseteq G(K)$ een eindig voortgebrachte ondergroep. Voor elk positief geheel getal n kunnen we de deelverzameling $n^{-1}A = \{P \in G(\overline{K}) \mid nP \in A\}$ beschouwen. Uitbreidingen van K van de vorm $K(n^{-1}A)$ zijn het onderwerp van de studie van de *Kummertheorie voor commutatieve algebraïsche groepen*. Zoals men kan zien door $G = \mathbb{G}_m$ te nemen, waar $\mathbb{G}_m$ de multiplicatieve groep over K is, is deze theorie een directe generalisatie van de klassieke Kummertheorie. Zelfs in deze algemeenheid hebben Kummeruitbreidingen veel van de interessante eigenschappen van hun klassieke tegenhangers. Bijvoorbeeld is $K(n^{-1}A)$ een Galoisuitbreiding van K die het *n-torsielichaam* van G bevat, dat wil zeggen de lichaamsuitbreiding van K voortgebracht door alle n-torsiepunten van $G(\overline{K})$;

bovendien is het Galois en abels over dit lichaam. Torsielichamen zijn de directe veralgemening van cyclotomische lichamen, en veel resultaten over Kummeruitbreidingen kunnen worden afgeleid uit eigenschappen van deze lichamen.

Als K een getallenlichaam is, dan kan het bovengenoemde dichtheidsprobleem *mutatis mutandis* in deze algemenere context worden geformuleerd, en is het nog steeds gerelateerd aan de graden van Kummeruitbreidingen. Zie [Pin04] voor een bespreking in het geval van abelse variëteiten en [Per08, Per11] voor het product van een abelse variëteit en een torus. Dit motiveert de studie van de graden van Kummeruitbreidingen in een algemene context. In zijn fundamentele artikel [Rib79] bewees Ribet het volgende resultaat: als G het product is van een abelse variëteit en een torus en $A \subseteq G(K)$ een vrij $\mathbb{Z}$-moduul van rang r is, met een basis over $\mathbb{Z}$ van punten lineair onafhankelijk over $\mathrm{End}_K(G)$, dan bestaat er een positief geheel getal C zodanig dat de verhouding tussen n^{rs} en de graad $[K(n^{-1}A) : K(G[n])]$ een deler is van C voor elk positief geheel getal n. Hier is s het unieke positieve gehele getal zodanig dat voor elke $n > 1$ geldt $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$. Zie ook [Ber88, Théorème 5.2] en [Hin88, Lemme 14]. De artikelen die in dit proefschrift zijn verzameld, zijn gewijd aan het effectiever maken van dit resultaat, waarbij wordt geprobeerd de constante C uit te drukken in termen van bekende grootheden gerelateerd aan de torsielichamen van G.

Effectieve resultaten voor elliptische krommen

De eerste twee artikelen, geschreven in samenwerking met Lombardo, richten zich op het geval van elliptische krommen. Zij G een elliptische kromme over een getallenlichaam K, zij $\overline{K}$ een algebraïsche afsluiting van K, en zij $\alpha \in G(K)$. In [JR10] hebben Jones en Rouse bewezen dat voor elk priemgetal ℓ, onder bepaalde aannames over α en met een kleine uitzondering voor het priemgetal 2, de surjectiviteit van de ℓ-adische Galoisrepresentatie geassocieerd met G de maximaliteit van de Kummeruitbreidingen $K(n^{-1}\alpha)$ over $K(G[n])$ impliceert als n een macht is van ℓ. Zie [JR10, stelling 5.2] voor het niet-CM-geval en [JR10, stelling 5.8] voor het CM-geval. In het licht hiervan formuleerde Perucca twee vragen: Als de Galoisrepresentatie niet surjectief is, kunnen we dan het falen van de maximaliteit van de Kummeruitbreidingen beschrijven, of op zijn minst begrenzen, in termen van het falen van de maximaliteit van de Galoisrepresentaties? Kunnen deze resultaten worden gegeneraliseerd naar het geval waarin n een positief geheel getal is?

Het eerste artikel dat hier [Chapter 1] wordt gepresenteerd, is bedoeld om deze vragen te beantwoorden. De hoofdstelling [Chapter 1, Theorem 1.1] geeft een positief antwoord, maar alleen onder de aanname dat $\mathrm{End}_K(G) = \mathbb{Z}$. Deze stelling is een effectieve versie van het klassieke resultaat van Ribet in het geval van een groep G voortgebracht door een enkel punt α, en het laat zien dat de bovengenoemde constante C alleen afhangt van eigenschappen van de *ℓ-adische* representaties, voor alle priemgetallen ℓ, en andere effectief berekenbare grootheden geassocieerd met G. Voorbeelden die de niet-toepasbaarheid van deze methoden op het CM-geval aantonen, worden gegeven in [Chapter 1, Section 6]. De tweede hoofdstelling [Chapter 1, Theorem 1.2] laat zien dat er over het lichaam $\mathbb{Q}$ een uniforme versie van dit resultaat bestaat onder de aanname dat het punt α niet deelbaar is in $G(\mathbb{Q})/G(\mathbb{Q})_{\mathrm{tors}}$ – dat wil zeggen dat er geen $\beta \in G(\mathbb{Q})$ bestaat zodanig dat α geschreven kan worden als $n\beta + \tau$ voor een geheel getal $n > 1$ en $\tau \in G(\mathbb{Q})_{\mathrm{tors}}$.

Het doel van het tweede artikel met Lombardo [Chapter 2] is om het bovengenoemde resultaat [Chapter 1, Theorem 1.2] expliciet te maken door een werkelijke numerieke waarde te vinden voor de constante C, zie [Chapter 2, Theorem 6.5]. Deze resultaten zijn bereikt door uniforme grenzen te geven aan andere interessante grootheden die verband houden met de Galoisrepresentaties van G. Opmerkelijke voorbeelden van zulke grootheden zijn de exponenten van de cohomologiegroepen van $\mathrm{Gal}(\mathbb{Q}(G(\overline{\mathbb{Q}})_{\mathrm{tors}}) \mid \mathbb{Q})$ met coëfficiënten in de torsieondergroepen van G, beschouwd als Galoismodulen. Grenzen voor vergelijkbare grootheden zijn onafhankelijk gevonden door Cerchia en Rouse [CR21].

Een technisch raamwerk voor de algemene Kummertheorie

Sommige van de bovengenoemde expliciete resultaten zijn afhankelijk van eigenschappen van Galoisrepresentaties die alleen voor elliptische krommen in een effectieve vorm bekend zijn. De methoden die worden gebruikt om aan te tonen dat de graden van Kummeruitbreidingen gerelateerd zijn aan deze grootheden, zijn hier echter onafhankelijk van. In het derde artikel dat in dit proefschrift is opgenomen, wordt dit duidelijk gemaakt door de theoretische achtergrond te conceptualiseren in een raamwerk dat van toepassing is op elke commutatieve algebraïsche groep G over K die voldoet aan $\mathrm{End}_K(G) = \mathbb{Z}$. De methoden die in dit werk worden gebruikt, zijn geïnspireerd op resultaten van Palenstijn [Pal04, Pal14] en op gesprekken met Lenstra en Stevenhagen. Als toepassing worden de resultaten van [Chapter 1] en [Chapter 2] uitgebreid naar groepen A met een rang hoger dan 1.

Tot nu toe hebben we het geval waarin de endomorfismering van G groter is dan $\mathbb{Z}$ nog niet met succes aangepakt, en het lijkt erop dat onze methoden in dat geval een substantiële verfijning nodig hebben. In zijn proefschrift [JP21] gaat Javan Peykar in op dit probleem in het geval van elliptische krommen met complexe vermenigvuldiging door $A \subseteq G(K)$ te nemen als een $\mathrm{End}_K(G)$-moduul, en de modulen van "delingspunten" door een *Steinitzideaal* te beschouwen. Zelfs met enige technische beperkingen is deze methode zeer succesvol.

Gemotiveerd door deze benadering is het laatste artikel in dit proefschrift [Chapter 4] voornamelijk gewijd aan de studie van puur algebraïsche eigenschappen van delingsmodulen over algemene ringen. De door Javan Peykar gebruikte Steinitzidealen worden vervangen door *ideaalfilters*, en er wordt een veralgemening gegeven van het klassieke begrip injectiviteit, dat voor zover de auteur weet nieuw is. Een notie van (J, T)-*uitbreiding*, waarbij J een vast ideaalfilter is en T een geschikt R-moduul, generaliseert de modulen van delingspunten. De eigenschappen van deze objecten worden vervolgens bestudeerd vanuit een categorietheoretisch oogpunt, waarna enkele resultaten over hun automorfismegroepen worden gegeneraliseerd die zijn verschenen in de minder algemene settings van [Pal04], [Pal14] en [JP21].

Deze lange uitweiding in de commutatieve algebra werpt uiteindelijk zijn vruchten af: de zo geconstrueerde theorie, die die van [Chapter 3] generaliseert, wordt uiteindelijk toegepast om de resultaten van [Chapter 1] en [JP21] te verenigen en te veralgemenen, wat aantoont dat de twee schijnbaar verschillende benaderingen eigenlijk gewoon verschillende realisaties zijn van een algemenere theorie. De mate van algemeenheid die in dit artikel wordt gebruikt, opent de deur naar toepassingen op hogerdimensionale abelse variëteiten en andere klassen van commutatieve algebraïsche groepen.