Decompositions in algebra

Gent, D.M.H. van

Samenvatting

In dit proefschrift getiteld "*Decompositions in algebra*" bestuderen we ontbindingen van Abelse groepen uitgerust met verscheidene algebraïsche structuren, en relevante algoritmen.

In Hoofdstuk 1 beschouwen we stromen in ongerichte grafen waarvan de waarden, in contrast met de klassieke theorie, leven in niet noodzakelijk Abelse groepen. Voor Abelse stromen is het zo, dat als in alle knopen van de graaf met ten hoogste één uitzondering voldaan is aan de *behoudswet van Kirchhoff*, die stelt dat de inkomende stroom gelijk is aan de uitgaande stroom, dan ook deze uitgezonderde knoop aan de behoudswet voldoet. We bewijzen het verbazende resultaat dat de grafen waarvoor deze implicatie ook geldt voor iedere niet-Abelse stroom, precies de *vlakke grafen* zijn. Ook construeren we van een gegeven groep een ontbinding in zijn maximale Abelse ondergroepen, aan de hand waarvan algoritmisch te beslissen is of deze groep voor alle grafen aan de behoudswet voldoet.

In Hoofdstuk 2 generaliseren we de theorie van roosters naar oneindige dimensie, waar het volgende hoofdstuk op rust. Waar klassiek een rooster een discrete ondergroep vormt van een Euclidische vectorruimte, beschouwen wij discrete ondergroepen van Hilbertruimten, die wij *Hilbertroosters* noemen. We bewijzen dat ieder Hilbertrooster een unieke maximale orthogonale ontbinding in deelroosters heeft, en bestuderen daartoe de *onontbindbare vectoren*. De onontbindbare vectoren ontlenen hun bestaan aan het *Voronoi-polyeder*, waarvan we laten zien dat het een fundamenteel domein is. Aftelbare Hilbertroosters blijken vrije Abelse groepen te zijn. Het is een open probleem of dit algemeen geldt.

In Hoofdstuk 3 beschouwen we de gehele afsluiting van de gehele getallen in een algebraïsche afsluiting van het lichaam van rationale getallen, de *ring van algebraïsch gehelen* genaamd, uitgerust met de natuurlijke Hilbertroosterstructuur zoals bekend uit de theorie van de meetkunde van getallen. We

pogen voor dit rooster invarianten uit te rekenen. In het bijzonder geven we onder- en bovengrenzen op de *overdekkingsstraal*. Hieruit leiden we een partiële oplossing af van de algoritmische tegenhanger van dit probleem, namelijk het *dichtstbijzijnde-vectorprobleem*. Als proeve voor zulke algoritmen dragen wij het berekenen van de onontbindbare vectoren van gegeven graad aan. Het blijkt lastig om alle onontbindbare vectoren van graad drie te bepalen, hoewel het aantal kandidaten beperkt is, omdat de termen van een ontbinding een arbitrair hoge graad kunnen hebben. Om dezelfde reden is het niet eens duidelijk of onontbindbaarheid beslisbaar is. Het is ook onbekend of het rooster isometrieën heeft naast de isometrieën die komen van de ringstructuur.

In Hoofdstuk 4 ontbinden we ringen in *graderingen*, een constructie die de graad van een monoom in een polynoomring generaliseert. We bewijzen dat de roosterstructuur op de ring van algebraïsch gehelen en diens deelringen aanleiding geeft tot het bestaan van een *universele gradering* voor deze ringen, en we bepalen de structuur hiervan in enkele speciale gevallen. In het bijzonder is de maximale orthogonale ontbinding, en dus ook de universele gradering, van het rooster van algebraïsch gehelen triviaal. Los van een roosterstructuur bestaat een universele gradering onder zekere p-adische voorwaarden, en in het verlengde hiervan bewijzen we dat *eenheidswortels* en *idempotenten* 'monomen' zijn. Verder geven we een algoritme om snel de universele gradering van ringen te bepalen die additief worden voortgebracht door hun eenheidswortels en idempotenten.

In Hoofdstuk 5 passen we de theorie van het voorgaande hoofdstuk toe op het speciale geval van *groepenringen*. Voor groepenringen over gereduceerde ordes blijkt ook aan een zekere universaliteit voldaan: op isomorfie na is er een unieke maximale manier om een dergelijke ring als groepenring te ontbinden. In termen hiervan beschrijven we diens automorfismengroep. Zeer verrassend blijkt dat in het samenhangende geval, de deelringen en ondergroepen die gebruikt kunnen worden om een maximale ontbinding te vormen compleet onafhankelijk gekozen kunnen worden. Dit bewijzen we door de theorie van modulen, in het bijzonder ontbindingen van modulen van eindige lengte, toe te passen op een morfisme van eindige abelse groepen, namelijk de *graadafbeelding* beperkt tot de groep van eenheidswortels.

In Hoofdstuk 6 geven we een efficiënte algoritme om *wortels van gebroken idealen* van ordes in getallenlichamen te trekken. We zijn zorgvuldig om deze algoritme zo te formuleren dat de uitvoer voldoende functorieel is. Het is hierbij een obstructie dat een wortel niet hoeft te bestaan of uniek hoeft te zijn. We vinden een toepassing van het worteltrekken in een generalisatie van de *copprieme-basisalgoritme*. Deze algoritme vindt voor een verzameling positieve gehele getallen een verzameling paarsgewijs coprieme gehelen, een *coprieme basis*, waarbij ieder getal uit de eerste verzameling een (uniek) machtsproduct is van getallen uit de tweede. Dit machtsproduct kan gezien worden als de beste polynomiale-tijd benadering van de priemontbinding. Echter, het is nog mogelijk de coprieme basis te verbeteren door wortels te trekken uit diens elementen. Wanneer we de copriemebasisalgoritme generaliseren naar idealen in ordes, zijn we ook daar in staat om deze laatste verbetering te maken.