Het cyclotomische ideaal

Dit project gaat over het ideaal voortgebracht door een cyclotomisch polynoom. Het is algebraïsch van aard, maar geïnspireerd door getaltheorie. De student die dit project uitvoert, zal goed met commutatieve ringen moeten kunnen omgaan, en daar ook nieuwe dingen over leren. Het is mogelijk dat enige algebraïsche getaltheorie ook nuttig zal zijn.

Uit het college Algebra is bekend dat de rij $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, …, Φ_n, … van *cyclotomische polynomen* bepaald is door de relaties $\prod_{d|n} \Phi_d = X^n - 1$ ($n \in \mathbf{Z}_{\geq 1}$). Al deze polynomen behoren tot de polynoomring $\mathbf{Z}[X]$, en zijn irreducibel in die ring.

Houd $n \in \mathbf{Z}_{\geq 1}$ nu vast. In dit project zijn we geïnteresseerd in het *ideaal* (Φ_n) van $\mathbf{Z}[X]$. Dit ideaal omvat $(X^n - 1)$, dus het correspondeert met een ideaal van de ring $\mathbf{Z}[X]/(X^n - 1)$. Die laatste ring is isomorf met de groepenring $\mathbf{Z}[C]$, waar C een cyclische groep van orde n is; een isomorfisme wordt verkregen door (X mod $(X^n - 1)$) af te beelden op een voortbrenger σ van C, en het $\mathbf{Z}[C]$-ideaal dat correspondeert met (Φ_n) is dan $(\Phi_n(\sigma))$.

Het is niet erg moeilijk te bewijzen dat het ideaal $(\Phi_n(\sigma))$ van $\mathbf{Z}[C]$ niet afhangt van de keuze van de voortbrenger σ van C. Dit suggereert de vraag of ditzelfde ideaal, dat we het *cyclotomische ideaal* van $\mathbf{Z}[C]$ zullen noemen, ook een beschrijving toelaat waar geen voortbrenger in voorkomt. Dat het antwoord op deze vraag bevestigend is, blijkt uit de *Stelling van De Bruijn–Rédei*, die zegt dat $(\Phi_n(\sigma))$ als ideaal wordt voortgebracht door de elementen $\sum_{\gamma \in C, \gamma^p = 1} \gamma$ als p over de priemgetallen loopt die n delen (zie: N. G. de Bruijn, *On the factorization of cyclic groups* (1953), Theorem 1). Het blijkt ook uit de *Stelling van Katz–Mazur*, die zegt dat $(\Phi_n(\sigma))$ wordt voortgebracht door de coëfficiënten van het polynoom $\big(\prod_{\gamma \in C}(Y - \gamma)\big) - (Y^n - 1) \in \mathbf{Z}[C][Y]$ (zie N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves* (1985), Theorem 1.12.9). In feite laat elk van beide stellingen iets scherpers zien. Namelijk, laat $\mathbf{Z}[C]^{\operatorname{Aut} C}$ de deelring van $\mathbf{Z}[C]$ zijn bestaande uit alle elementen van $\sum_{\gamma \in C} a_\gamma \gamma \in \mathbf{Z}[C]$ (met $a_\gamma \in \mathbf{Z}$) die door $\operatorname{Aut} C$ in zichzelf overgaan, wat erop neerkomt dat $a_\gamma = a_\delta$ als γ en δ dezelfde orde hebben. Dan wordt $(\Phi_n(\sigma))$ in feite voortgebracht door zijn doorsnede met $\mathbf{Z}[C]^{\operatorname{Aut} C}$.

Het project kan uit het beantwoorden van de volgende vragen bestaan:

(1) Hoe kan men alle bovengenoemde resultaten bewijzen?

(2) Is er een verfijning van de Stelling van Katz–Mazur waarin slechts een klein aantal coëfficiënten van het genoemde polynoom gebruikt wordt?

(3) Voor welke n heeft het cyclotomische ideaal een enkele voortbrenger die in de deelring $\mathbf{Z}[C]^{\operatorname{Aut} C}$ ligt? Voor welke n is het $\mathbf{Z}[C]^{\operatorname{Aut} C}$-ideaal $(\Phi_n(\sigma)) \cap \mathbf{Z}[C]^{\operatorname{Aut} C}$ een hoofdideaal? Is het voor elke n tenminste *locaal* een hoofdideaal? (Dit moet gedefinieerd worden.) Kan het voor elke n door *twee* elementen worden voortgebracht?

Afhankelijk van de beschikbare tijd kan ook nog het volgende gedaan worden.

(4) Gebruik de Stelling van De Bruijn–Rédei om een stelling van C. G. Latimer uit de algebraïsche getaltheorie te verscherpen (*On the units in a cyclic field* (1934), Theorem 3).

(5) Begrijp de context waarin Katz en Mazur hun stelling formuleren.

Begeleider: Hendrik Lenstra