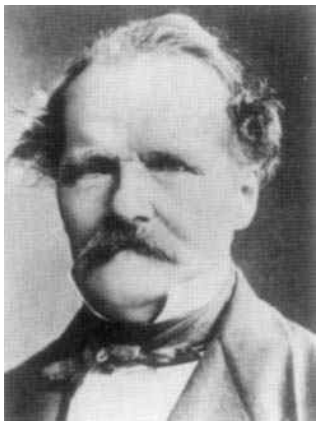
Universiteit Utrecht

Kummer en Dedekind

Een geschiedenis van idealen



Ernst Eduard Kummer, bron: [22]

Richard Dedekind, bron: [23]

Marlien Wennekes

Begeleider: Dr. S.A. Wepster

Bachelorscriptie wiskunde
Universiteit Utrecht
10-05-2020

Inhoudsopgave

Dankwoord

Ik wil hierbij ten eerste mijn begeleider, dr. Steven Wepster, bedanken voor de ondersteuning tijdens het onderzoeks- en schrijfproces. Door hem bleef ik altijd gemotiveerd om de scriptie te blijven verbeteren.

Ten tweede wil ik dhr. dr. Reinhard Bölling bedanken voor het persoonlijk sturen van zijn artikel, *Kummer vor der Erfindung der "idealen complexen Zahlen: Das Jahr 1844"*, dat ik nergens anders kon verkrijgen omdat de universiteitsbibliotheek gesloten was. Bedankt voor de duidelijke analyse en waardevolle nieuwe perspectieven.

Als laatste bedank ik mijn ouders, die mij altijd steunen en zonder wie er immers geen scriptie geweest was.

Inleiding

Deze scriptie zal gaan over de wiskunde van de 19e eeuw. In die tijd verdween de meetkunde steeds meer naar de achtergrond. In plaats daarvan werd de rekenkunde de "koningin van de wiskunde" (Gauss). Pas aan het eind van de 19e eeuw worden complexe en irrationale getallen ook meegeteld als rekenkunde [5, p. 484]. Gauss had in 1832 complexe getallen van de vorm $\{a+b\sqrt{-1}|a,b\in\mathbb{Z}\}$ geïntroduceerd. Deze worden ook wel de complexe gehelen van Gauss genoemd. Gauss bewees dat deze getallen op dezelfde manier factoriseren als de gehele getallen. Hierbij doel ik op het feit dat gehele getallen op unieke wijze geschreven kunnen worden als een product van priemgetallen. Gauss liet zien dat zijn complexe gehelen ook unieke priemfactorisatie toelieten. Gauss zag zijn complexe gehelen daarom als een uitbreiding van de gehele getallen en dus als onderdeel van de rekenkunde [5, p. 485].

In deze scriptie zal ik in deze context wiskunde van Kummer en Dedekind behandelen. Zij waren in zekere zin opvolgers van Gauss. Beiden bestudeerden bepaalde complexe getallen en hun factorisatie. Kummers onderzoek was gebaseerd op cyclotomische getallen: getallen opgebouwd uit gehele getallen met een eenheidswortel.

In tegenstelling tot de complexe gehelen van Gauss, geldt in een domein van cyclotomische getallen niet altijd unieke priemfactorisatie. Hier liep Kummer in zijn onderzoek tegenaan. Zijn oplossing kwam in de vorm van 'ideale getallen'. Naar aanleiding hiervan, maakte Dedekind de stap om te kijken naar mogelijkheden om ook unieke factorisatie te herstellen in de algebraïsche getallen. Dit algemeniseert Kummers theorie; een cyclotomisch getal is immers ook algebraïsch. De ideale getallen gaven zo de basis voor Dedekinds introductie van het begrip ideaal.

In deze scriptie wil ik deze geschiedenis van het ideaal verder bestuderen. Hierbij is het doel om te zien hoe Kummer en Dedekind zich tot elkaar verhouden, met name binnen deze geschiedenis, maar ook binnen de 19e eeuwse wiskunde in het algemeen. Zo zullen we zien waarom Dedekind ervoor koos om idealen te introduceren, in plaats van verder te gaan met de ideale getallen van Kummer.

Met dit doel heb ik werk van Kummer, waarin hij de ideale getallen introduceert, en zijn werk wat hieraan vooraf ging, geanalyseerd. Dit is met name het artikel *Zur Theorie der complexen Zahlen*[16] en een brief uit 1844 van Kummer uit de appendix van [10]. Dit komt terug in hoofdstuk 1. Daarna geef ik een analyse van de introductie van Dedekinds idealen zoals hij die gaf in *Sur la Théorie des Nombres Entiers Algébriques.* Hiervoor gebruik ik de vertaling van John Stillwell, zie [8]. Dit deel staat in hoofdstuk 2. Ik gebruik ook een aantal secundaire bronnen. De meeste zijn voor achtergrondinformatie, met name over wiskunde in de 19e eeuw en over Dedekind en Kummer in het algemeen. Wanneer ik een voorbeeld van iemand anders gebruik, staat dit er expliciet bij. Daarnaast heb ik verschillende opvattingen van H.M. Edwards en R. Bölling besproken. Deze worden gegeven in *The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes*[9] en het postscript[10] door Edwards en door Bölling in *Kummer vor der Erfindung der 'idealen complexen Zahen': Das Jahr 1844*[3]. Ik heb ook *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*[11], van H.M. Edwards gebruikt als naslagwerk voor het begrijpen van bepaalde details uit Kummers wiskunde. Ik heb het vermeld wanneer ik hieruit iets overneem.

Hoofdstuk 1

Kummer

Ernst Eduard Kummer (1810–1893) was een wiskundige uit Pruisen gespecialiseerd in getaltheorie. Hij begon als student theologie in Halle, maar ruilde de studie al gauw in voor wiskunde. Over die beslissing schreef hij als achtienjarige naar zijn moeder:

> Jetzt kann ich mit gutem Gewissen nicht fortfahren Theologie zu studiren, darum habe ich es aufgegeben, und habe mir die Mathematik erwählt, weil es die Wissenschaft ist, in welcher der tiefer forschende von andern nicht mißverstanden, oder für gottlos und schlecht gehalten wird sondern in welcher was einer wahres findet von allen anerkannt werden muß und anerkannt wird. [14, p. 71]

Kummer koos wiskunde uit een voorliefde voor de absolute, onomstreden wiskundige waarheid. Na zijn doctoraat werkte hij een tijd als wiskundeleraar in een gymnasium. In die tijd had Kummer onder andere Kronecker als student. Als gepassioneerd leraar heeft Kummer veel invloed op hem gehad. Daarnaast bleef Kummer het werk van Gauss en andere wiskundigen bestuderen en was hij bezig met zijn eigen werk, in die tijd voornamelijk over de theorie van functies [2]. Ook had Kummer contact met Jacobi, die hem prees voor zijn originaliteit in zijn werk. Jacobi noemde Kummers mogelijke academische carrière "ein großer Gewinn für die Wissenschaften" [19, p. 215]. Uiteindelijk hielp hij, samen met Humboldt en Dirichlet, Kummer aan een positie als professor aan de universiteit van Breslau [19, p. 216]. We zullen in paragraaf 1.3.2 zien dat Kummer in zijn onderzoek dat voorafging aan de introductie van ideale getallen geïnspireerd was door Jacobi.

In dit hoofdstuk zullen we dieper ingaan op het begrip 'ideaal' zoals Kummer het introduceerde in het artikel *Zur Theorie der complexen Zahlen* in 1847. Daar heeft hij het over 'ideale factoren'. Ik zal eerst in paragraaf 1.1 het domein van complexe getallen toelichten waarin Kummer werkt en daarnaast de reden geven waarom het voor Kummer noodzakelijk was om ideale factoren te introduceren. In paragraaf 1.2 maak ik deze reden concreter aan de hand van het werk van Kummer en enkele voorbeelden. Ik zal uiteindelijk in paragraaf 1.4 Kummers verschillende definities van een ideale factor bespreken. We zullen in hoofdstuk 2 zien hoe Dedekind, door Kummers theorie geïnspireerd, kwam tot de moderne definitie van een ideaal in een ring. De 'ideale factoren' kwamen voort uit Kummers onderzoek naar iets dat we tegenwoordig *cyclotomische getallen* noemen. Kummer noemde het echter simpelweg 'complexe getallen'. Zijn interesse hierin kwam voornamelijk van de toepassingen van dit gebied op hogere reprociteitswetten en de laatste stelling van Fermat. Over de precieze motivatie van Kummer zal ik meer schrijven in paragraaf 1.3. Kummer had met zijn nieuwe theorie inderdaad successen geboekt in bovenstaande gebieden; zo had hij hogere reprociteitswetten gevonden en de laatste stelling van Fermat bewezen voor bepaalde priemgetallen [14]. Ik zal nu eerst toelichten wat cyclotomische getallen zijn en wat we kunnen zeggen over de structuur van deze getallen, in moderne zin en in Kummers woorden.

1.1 Cylcotomische getallen en unieke factorisatie

De focus van Kummers studie lag op de 'complexen Zahlen', waarmee hij aanduidde wat we tegenwoordig 'cyclotomische getallen' noemen. Dit zijn getallen die bestaan uit gehele getallen met een eenheidswortel. Een eenheidswortel van graad λ is een getal α zodat $\alpha^\lambda = 1$. Cyclotomische getallen zijn dus van de vorm

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-1}\alpha^{\lambda-1}$$

waarbij de a_i, voor alle $i = 0, 1, ..., \lambda - 1$, gehele getallen voorstellen en α een eenheidswortel van graad λ is. De verzameling van al deze getallen komt overeen met de ring $\mathbb{Z}[\alpha]$, maar dit begrip en deze notatie zijn van na Kummers tijd. Kummer gebruikt de notatie $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-1}\alpha^{\lambda-1}$ voor een cyclotomisch getal zoals hierboven.

Kummer bedacht zijn theorie nadat hij tegen een specifiek probleem aanliep met zijn complexe getallen; namelijk dat ze niet in het algemeen unieke priemfactorisatie toelaten. Een domein van cyclotomische getallen, behorende bij een bepaalde eenheidswortel van graad λ, laat alleen unieke priemfactorisatie toe wanneer $\lambda < 23$. In Kummers tijd waren er nog geen uitgebreide theorieën over factorisatie in verschillende domeinen. Daardoor was er veel ruimte voor overhaaste generalisaties: wat bekend is over de gehele getallen, zal vast ook wel gelden voor uitbreidingen hiervan. Zo is het bekend dat Franse wiskundigen Cauchy en Lamé unieke factorisatie in de cyclotomische getallen hadden aangenomen voor een bewijs van de laatste stelling van Fermat [9, p. 220-222]. Zij kwamen pas achter deze fout nadat ze door Liouville het artikel *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant*[15] onder ogen kregen: hierin beschrijft Kummer dat unieke factorisatie helaas niet geldt in de cyclotomische getallen [9, p. 223-225]. Dit artikel zal in 1.4 nog uitgebreid ter sprake komen.

Het is niet zo dat er nog helemaal niets geschreven was over unieke priemfactorisatie in verschillende domeinen. Gauss had al in 1832 een bewijs gegeven voor het gelden van unieke priemfactorisatie voor getallen van de vorm $a + b\sqrt{-1}$ met a, b gehele getallen (oftewel $\mathbb{Z}[\sqrt{-1}]$, de complexe gehelen van Gauss) [6, p. 81-82][8, p. 53]. Mogelijk was dit werk bij Cauchy en Lamé niet bekend en stonden zij daarom niet stil bij de noodzaak voor een bewijs voor unieke priemfactorisatie voor cyclotomische getallen. Kummer was, als Duitse wiskundige, zeker wel goed op de hoogte was Gauss' werk [9, p.226]. Een belangrijke vraag waar ik in paragraaf 1.3 verder op in zal gaan, is of Kummer wel of niet op een bepaald punt de unieke priemfactorisatie voor cyclotomische getallen had aangenomen. Zo is er speculatie dat ook Kummer een bewijs van de laatste stelling van Fermat had gegeven dat gebruikmaakte van unieke factorisatie. Dit lijkt nu onwaarschijnlijk, omdat Kummer wist dat Gauss wel op de noodzaak van een precies bewijs voor unieke priemfactorisatie stond [9, p. 226]. Aan de andere kant is het niet ondenkbaar dat Kummer dit toch vanzelfsprekend achtte, zeker omdat het voor de gehele getallen van Gauss én voor alle $\lambda < 23$ gewoon goed gaat. Ik ga hier in paragraaf 1.3 verder op in.

We weten tegenwoordig dat het niet gelden van unieke factorisatie een veelvoorkomend probleem is onder complexe uitbreidingen van de gehele getallen. Maar wat betekent het eigenlijk, wanneer we zeggen dat er geen 'unieke priemfactorisatie' geldt in een bepaald domein? Dit zal ik nu bespreken. Hierbij speelt de norm een belangrijke rol. Dit is een functie naar het domein naar de niet-negatieve gehele getallen die op een bepaalde manier de afstand of grootte van een getal uit het domein geeft. Zo definieert Gauss de norm op $\mathbb{Z}[\sqrt{-1}]$ als $N(a + b\sqrt{-1}) = a^2 + b^2$ [21, p. 442].

Ik zal dit nu unieke priemfactorisatie toelichten met het klassieke voorbeeld van de ring $\mathbb{Z}[\sqrt{-5}]$. Hierin geldt *geen* unieke priemfactorisatie. Bekijk namelijk de volgende twee factorisaties:

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

We zien hier dat $3, 2, 1 + \sqrt{-5}$ en $1 - \sqrt{-5}$ irreducibele getallen zijn: ze zijn niet verder te ontbinden in factoren in $\mathbb{Z}[\sqrt{-5}]$. Dit zien we door de norm $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$ te introduceren. Hier nemen we dus het product van $a + b\sqrt{-5}$ met zijn geconjungeerde. Deze norm voldoet aan $N(xy) = N(x)N(y)$ voor alle x, y in de ring $\mathbb{Z}[\sqrt{-5}]$. De norm kan dus de waarden $1, 4, 5, 9, ...$ et cetera

aannemen. Merk op dat $N(2) = 2 \cdot 2 = 4$, $N(3) = 3 \cdot 3$=9 en $N(1 \pm \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 3 \cdot 2$. Er bestaan geen getallen in de ring met norm 2 en 3, dus de vier getallen zijn niet verder te ontbinden in factoren. We noemen dit soort factoren irreducibel. Het zijn echter geen 'priemgetallen' zoals we die kennen in de gehele getallen, want de factorisatie in deze irreducibelen is niet uniek. Met andere woorden: we zien dat $3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, maar $3 \nmid (1 + \sqrt{-5})$ en $3 \nmid (1 - \sqrt{-5})$ binnen $\mathbb{Z}[\sqrt{-5}]$. Om dit verschil te benadrukken, introduceren we hier de definities van een priemgetal en irreducibel in een ring. Hierbij is een eenheid een getal in een ring dat een inverse heeft, oftewel een getal dat vermenigvuldigd met een ander getal uit die ring 1 oplevert. Een getal is een eenheid dan en slechts dan als zijn norm gelijk is aan 1.

Definitie 1.1.1. Een element $q \neq 0$ uit een ring R, dat geen eenheid is, noemen we **irreducibel** wanneer als $a \cdot b = q$ voor $a, b \in R$, a of b een eenheid moet zijn.

Definitie 1.1.2. Een element $p \neq 0$, uit een ring R, dat geen eenheid is, noemen we **priem** wanneer voor alle $a, b \in R$ geldt dat als $p \mid a \cdot b$, $p \mid a$ of $p \mid b$.

De natuurlijke getallen zijn een makkelijk voorbeeld: de enige eenheid is het getal 1 en irreducibele getallen en priemgetallen zijn gelijk. Dit is echter niet zo in elke ring, namelijk niet voor $\mathbb{Z}[\sqrt{-5}]$ zoals we hebben gezien in het voorbeeld. Ook zullen we zien, dat dit niet in het algemeen voor domeinen van cyclotomische getallen $\mathbb{Z}[\alpha]$ geldt. Kummer definieert dit verschil tussen irreducibele en priemgetallen niet, maar was hier zeker wel van op de hoogte tegen de tijd dat hij de ideale getallen introduceerde. Hij benoemt dit in het volgende citaat uit *Zur Theorie der complexen Zahlen*:

> Ich habe nun aber bemerkt, daß, wenn auch $f(\alpha)$ auf keine Weise in complexe Factoren zerlegt werden kann, sie **deshalb noch nicht die wahre Natur einer complexen Primzahl** hat, weil sie schon gewöhnlich der ersten und **wichtigsten Eigenschaft der Primzahlen** ermangelt: nämlich, dass das Product zweier Primzahlen durch keine von ihren verschiedene Primzahlen theilbar ist. [14, p. 203]

Wat hij hier omschrijft, is dat deze belangrijkste eigenschap van priemgetallen in de gehele getallen niet voor alle 'priemgetallen' (oftewel, irreducibelen) geldt in de cyclotomische getallen. Twee factorisaties zoals in bovenstaand voorbeeld in $\mathbb{Z}[\sqrt{-5}]$ zouden niet mogelijk moeten zijn voor priemgetallen. Wat we zien is dat, hoewel Kummer nog niet de moderne achtergrond van ringen had, hij duidelijk wel al het verschil zag tussen de klassieke priemgetallen en bepaalde irreducibele factoren in het nieuwe domein van de cyclotomische getallen. Dit verschil zag hij als een vervelend probleem en de oplossing lag in de toevoeging van ideale factoren die wél aan deze belangrijke eigenschap voldoen. Deze factoren moesten dan de onderliggende structuur van het complexe getal blootleggen. Ze 'bestaan' dus alleen in groepen bij elkaar als onderliggende structuur van het complexe getal. Hij vergelijkt het met fluoratomen die niet los van elkaar voorkomen[1], maar wel samen een fluormolecuul vormen [5, p. 493]. Ik zal nu een voorbeeld van Dedekind, zoals uiteengezet in [5, p. 490], geven dat dit toelicht en aansluit bij het vorige voorbeeld van factorisatie van 6 in $\mathbb{Z}[\sqrt{-5}]$. We kunnen in dit geval de ideale factoren α, β en γ introduceren als onderliggende structuur van $2, 3$, $1 + \sqrt{-5}$ en $1 - \sqrt{-5}$. We kunnen dan afleiden dat 2 zich als een kwadraat gedraagt.[2] De factorisatie van de andere getallen ligt dan vast, als we weten dat deze zich niet gedragen als een kwadraat en als we zo min mogelijk ideale factoren willen gebruiken. Dan kunnen we dus schrijven $2 = \alpha^2$, $3 = \beta\gamma$ en $1 + \sqrt{-5} = \alpha\beta$, $1 - \sqrt{-5} = \alpha\gamma$, zodat $6 = \alpha^2\beta\gamma$. In paragraaf 1.4 zal ik behandelen hoe Kummer deze ideale factoren precies definieert.

[1] Voor zo ver Kummer wist, ten minste.

[2] Dit feit, gegeven door Dedekind, is terug te vinden in [5, p. 490]. Merk op dat voor $z = x + y\sqrt{-5}$ en $z' = x' + y'\sqrt{-5}$ volgt dat $N(z) \equiv z^2 \mod 2$ en $N(z') \equiv z'^2 \mod 2$. Dus ook $z'^2 z^2 \equiv N(z')N(z) \mod 2$. Het getal $N(z')N(z)$ is geheel, dus aangezien 2 een priemgetal is volgt dat als 2 een deler is van $N(z')N(z)$, 2 tenminste een van de normen moet delen. Dan volgt dat 2 ook z'^2 of z^2 deelt. Verder zien we dat als x, y oneven zijn, 2 niet $z = x + y\sqrt{-5}$ deelt. Het volgt dus dat 2 op deze manier een kwadraat is binnen de ring $\mathbb{Z}[\sqrt{-5}]$.

1.2 Kummers stelling

In deze paragraaf zal ik toelichten hoe Kummer werkte en wanneer het niet gelden van unieke factorisatie voor hem een probleem werd. Dit is ook wat hem motiveerde om de ideale factoren te introduceren. Kummer bestudeerde cyclotomische getallen $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-1}\alpha^{\lambda-1}$ waarbij $\alpha^\lambda = 1$ voor een priemgetal $\lambda > 2$. Hier nemen we $\alpha \neq 1$, want dit geval voegt niets toe. Van centraal belang bij de theorie van Kummer is de norm die hij op deze cyclotomische getallen definieert. Die ziet er als volgt uit:

$$N(f(\alpha)) = f(\alpha)f(\alpha^2)f(\alpha^3)...f(\alpha^{\lambda-1}).$$

We zullen zo zien dat er altijd een geheel getal uit bovenstaande functie volgt. Kummer was hier waarschijnlijk geïnspireerd door de eerder genoemde norm van Gauss op de complexe getallen $a+b\sqrt{-1}$ met a, b gehele getallen. Deze luidt: $N(a + b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2$, oftewel de norm van een complex getal is gelijk aan het product met zijn geconjungeerde. Dit is inderdaad precies wat bovenstaande norm doet; het product nemen van $f(\alpha)$ met alle geconjungeerden $f(\alpha^i)$. Deze norm heeft ook de eigenschap dat $N(f(\alpha)g(\alpha)) = N(f(\alpha))N(g(\alpha))$ voor twee cyclotomische getallen $f(\alpha)$ en $g(\alpha)$.

We kunnen als volgt zien dat de bovenstaande norm altijd een geheel getal geeft. Merk op dat aangezien $\lambda > 2$ een priemgetal is, volgt dat $\{1, 2, ..., \lambda - 1\}$ de multiplicatieve groep van gehele getallen modulo λ is. Kummer was waarschijnlijk op de hoogte van deze structuur vanuit Gauss' werk over primitieve wortels [13, p. 44]. Zo zien we dus in bovenstaande vergelijking dat het product aan de rechterkant onder alle transformaties $\alpha \to \alpha^i$ gelijk blijft, want de groep $\{1, 2, ..., \lambda - 1\}$ is gesloten onder vermenigvuldiging. Daarom geldt dus $N(f(\alpha)) = N(f(\alpha^i))$. De norm geeft een product van cyclotomische getallen, en is dus zelf ook een cyclotomisch getal. We kunnen dus schrijven $N(f(\alpha)) = b_0 + b_1\alpha + b_2\alpha^2 + ... + b_{\lambda-1}\alpha^{\lambda-1}$ voor gehele getallen b_i. Dan zien we dat, aangezien de norm gelijk blijft onder elke transformatie $\alpha \to \alpha^i$, moet gelden dat $b_1 = b_2 = ... = b_{\lambda-1}$. Merk op dat aangezien $\alpha \neq 1$, $1 + \alpha + \alpha^2 + ... + \alpha^{\lambda-1} = \frac{\alpha^\lambda - 1}{\alpha - 1} = 0$. Dus volgt dat $N(f(\alpha)) = b_0 + b_1(\alpha + \alpha^2 + ... + \alpha^{\lambda-1}) = b_0 - b_1$. Zo zien we dat voor elk cyclotomisch getal $f(\alpha)$, de norm $N(f(\alpha))$ een geheel getal is. Edwards geeft een soortgelijke redenatie in [11, p. 83].

Nu kunnen we een belangrijk doel in Kummers onderzoek naar de cyclotomische getallen omschrijven. Kummer keek naar priemgetallen $p = m\lambda + 1$, waarbij λ zoals hiervoor de graad van de eenheidswortel α aangeeft. Hij trachtte om voor alle priemgetallen $\lambda > 2$, te bewijzen dat voor alle bijbehorende p, er een cyclotomisch getal $f(\alpha)$ bestaat zodat $p = N(f(\alpha))$. Als zo'n cyclotomisch getal $f(\alpha)$ bestaat, dan volgt gelijk uit de definitie van de norm dat p in de $\lambda - 1$ factoren $f(\alpha), f(\alpha^2), ..., f(\alpha^{\lambda-1})$ te ontbinden is.

Kummer toonde later, in zijn artikel [15], met veel rekenwerk aan dat het goed ging voor alle priemgetallen behorend bij $\lambda < 23$ die kleiner waren dan 1000; hij kon altijd een $f(\alpha)$ vinden zodat $p = N(f(\alpha))$. Tot zover lijken zijn complexe getallen dus precies op de gehele getallen wat betreft factorisatie, net zoals Gauss zijn complexe gehelen van de vorm $a + b\sqrt{-1}$ dat deden. Dat het zo lang goed gaat, was voor Kummer waarschijnlijk de aanleiding om te zoeken naar een algemeen bewijs voor alle priemgetallen λ. Dit 'bewijs' diende hij in 1844 in. Bij $\lambda = 23$, en elk priemgetal λ daarna [4, p. 281], gaat het echter mis. Dit is dus precies wanneer unieke priemfactorisatie in de bijbehorende cyclotomische getallen niet geldt. Kummers bewijs in 1844 was dus niet correct. In de komende paragraaf 1.3 zullen we verder ingaan op dit bewijs. Ik wil nu eerst een belangrijk tegenvoorbeeld laten zien, waaruit blijkt dat de stelling inderdaad niet geldt. Hierna zal ik ook bespreken hoe dit kan leiden tot twee verschillende factorisaties van een cyclotomische getal in irreducibelen. Het is nu bekend dat Kummers stelling en unieke factorisatie van de bijbehorende cyclotomische getallen ook uit elkaar volgen (zie [4, p. 278] en [10, p. 385] voor beide implicaties), maar er zijn geen aanwijzingen dat Kummer hier ook van op de hoogte was.

Het was waarschijnlijk Jacobi, die Kummer erop wees dat zijn bewijs niet klopte [10, p. 384]. Dit wordt aannemlijk in 1.3, waarin ik een citaat geef waarin Jacobi zegt dat hij de publicatie van Kummers 'bewijs' net had voorkomen. Het tegenvoorbeeld dat ik nu ga schetsen komt uit [10, p. 384-385]. Edwards schrijft dat het mogelijkerwijs precies het voorbeeld is wat Jacobi aan Kummer liet zien. We zien in [15, p. 185]

inderdaad dat Kummer de conclusie van dit voorbeeld noemt; namelijk dat de stelling niet geldt voor $\lambda = 23$ omdat priemgetallen $p = 23m + 1$ niet altijd te schrijven zijn als $\frac{x^2+23y^2}{4}$.

Neem $\lambda = 23$ en α een eenheidswortel zodat $\alpha^{23} = 1$. Nu vormen de getallen $\{1, 2, ..., 22\}$ een multiplicatieve, cyclische groep aangezien $\lambda = 23$ een priemgetal is. Daarom volgt dat de groep een voortbrenger heeft. Merk op dat inderdaad $-2 \equiv 21 \mod 23$ deze multiplicatieve groep voortbrengt. Het getal $(-2)^2 = 4$ brengt dus de helft van de getallen, namelijk 11, voort uit deze groep. De te bestuderen norm $N(f(\alpha))$ bestaat uit 22 factoren $f(\alpha^i)$ en blijft onder elke transformatie $\alpha \to \alpha^j$ gelijk. Neem nu een product P dat bestaat uit die $f(\alpha^i)$ zodat i in de groep voortgebracht door 4 modulo 23 zit. Noem P' het product van de 11 overgebleven $f(\alpha^i)$. Nu geldt dus $N(f(\alpha)) = PP'$. Het product P blijft dus gelijk onder de transformatie $\alpha \to \alpha^4$. Dus moet gelden dat $P = b_0 + b_1\theta_1 + b_2\theta_2$ voor bepaalde gehele getallen b_0, b_1, b_2 met

$$\theta_1 = \alpha^{-2} + \alpha^{-8} + \alpha^{-9} + \alpha^{10} + \alpha^{-6} + \alpha^{-1} + \alpha^{-4} + \alpha^7 + \alpha^5 + \alpha^{-3} + \alpha^{11}$$

en

$$\theta_2 = \alpha^4 + \alpha^{-7} + \alpha^{-5} + \alpha^3 + \alpha^{-11} + \alpha^2 + \alpha^8 + \alpha^9 + \alpha^{-10} + \alpha^6 + \alpha.$$

Nu is het zo dat aangezien $\alpha^{23} = 1$, er geldt dat $1+\alpha+\alpha^2+\alpha^3+\cdots+\alpha^{22} = \frac{\alpha^{23}-1}{\alpha-1} = 0$. Dan volgt aangezien $\alpha \neq 1$:

$$\theta_1 + \theta_2 = \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{22} = -1 + \frac{\alpha^{23} - 1}{\alpha - 1} = -1.$$

Hieruit maken we op dat $\theta_2 = -\theta_1 - 1$ en dus $P = A + B\theta_1$ met $A = b_0 - b_2$ en $B = b_1 - b_2$. Herinner dat $N(f(\alpha)) = PP'$. Nu is P' precies P onder de transformatie $\alpha \to \alpha^{-2}$, dus $P' = A + B\theta_2$. Zo volgt dat $N(f(\alpha)) = (A + B\theta_1)(A + B\theta_2)$. Verder kan eenvoudig, maar met wat moeite, aangetoond worden dat $\theta_1\theta_2 = 11 + 5\theta_1 + 5\theta_2 = 6$. Zo volgt dat $Nf(\alpha) = A^2 - AB + 6B^2$. De tegenspraak volgt nu uit het feit dat we dan hebben dat $4Nf(\alpha) = (2A - B)^2 + 23B^2$. Als Kummer inderdaad bewezen zou hebben dat voor elk priemgetal λ alle $p = m\lambda + 1$ de norm van een cylotomisch getal zijn, volgt dus met bovenstaande dat voor alle $p = 23m + 1$ er gehele getallen x, y bestaan zodat $4p$ geschreven kan worden als $x^2 + 23y^2$. Maar voor het priemgetal $p = 23 \cdot 2 + 1 = 47$ geldt dit niet. Dan hebben we namelijk dat $4 \cdot 47 = 188 \equiv 4 \mod 23$ en dus moet ook gelden dat $x^2 \equiv 4 \mod 23$. Dan volgt dat $x = 2$ of $x = -2 = 21$ modulo 23, oftewel $x = 2 + k \cdot 23$ of $x = -2 + k \cdot 23$. Nu moet gelden dat $k = 0$, want anders is het getal al te groot. Dus volgt dat $188 = 4 + 23 \cdot y^2$ en $y^2 = \frac{184}{23} = 8$, en dit is een tegenspraak want y is een geheel getal en 8 is geen kwadraat.

We kunnen nu ook expliciet zien hoe dit leidt tot het falen van unieke factorisatie van de cyclotomische getallen in het volgende voorbeeld van Edwards, zie [12, p. 324]. Bekijk het cyclotomische getal $f(\alpha) = 1 - \alpha + \alpha^{21}$. Dan kan je (met veel werk) aantonen dat:

$$N(1 - \alpha + \alpha^{21}) = 47 \cdot 139$$

Hieruit volgt dat $f(\alpha) = 1 - \alpha + \alpha^{21}$ irreducibel is, oftewel niet verder te schrijven als een product van cyclotomische factoren. We zien namelijk dat 47 en 139 priemgetallen zijn, dus als $f(\alpha)$ niet irreducibel zou zijn, zou het cyclotomische getal een factor hebben met de norm 47 en we zagen net dat dit juist niet mogelijk is. Het complexe getal $f(\alpha)$ is echter niet priem volgens de definitie 1.1.2. Dit zien we als volgt. Uit de definitie van de norm volgt dat $f(\alpha)$ een deler moet zijn van $47 \cdot 139$. Echter deelt $f(\alpha)$ zowel 47 als 139 niet, aangezien $N(f(\alpha))$ niet $N(47) = 47^{22}$ of $N(139) = 139^{22}$ deelt. Niet alle irreducibele cyclotomische getallen zijn dus priem in ringtheoretische zin en daarom is ook bij deze cyclotomische getallen met $\lambda = 23$ net zoals bij $\mathbb{Z}[\sqrt{-5}]$ geen unieke priemfactorisatie mogelijk.

Het getal $47 \cdot 139$ kan dus op meerdere manieren in irreducibele factoren ontbonden worden. Een daarvan is die hierboven, als norm van $N(1 - \alpha + \alpha^{21})$, dus met 22 factoren van elk norm $47 \cdot 139$. Een andere manier verkijgen we door te kijken naar:

$$N(\alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^7 + \alpha^{16}) = 47^2$$

$$N(\alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^4 + \alpha^{19}) = 139^2$$

Edwards merkt dan op dat links steeds een factor dubbel staat, aangezien de transformatie $\alpha \to \alpha^{22} = \alpha^{-1}$ weer dezelfde norm oplevert. We kunnen dus de wortel nemen. Het getal $47 \cdot 139$ kunnen we dus ook ontbinden met 11 factoren van norm 47^2 en 11 factoren van norm 139^2. Dit is een andere factorisatie dan die we hiervoor zagen.

Kummer had de bovenstaande cyclotomische getallen uit Edwards voorbeeld, waarvan de norm respectievelijk 47^2 en 139^2 is, ook genoemd als cyclotomische getallen waarvan de norm 47 en 139 deelt in [15, p. 208]. Het is echter niet duidelijk of Kummer ook op de hoogte was van de dubbele factorisatie van $47 \cdot 139$, zoals Edwards deze geeft. Wat we wel hebben gezien aan het eind van de vorige paragraaf, is dat Kummer doorhad dat factorisaties in irreducibele cyclotomische getallen niet uniek hoeven te zijn. Het lijkt mij waarschijnlijk dat Kummer wel een dergelijk voorbeeld had gezien, al was het misschien niet deze.

1.3 Kummers bewijs in 1844

In de vorige paragraaf hebben we gezien dat $\lambda = 23$ een tegenvoorbeeld geeft voor Kummers stelling. Ter herhaling; die stelling zei dat elk priemgetal van de vorm $p = m\lambda + 1$ te schrijven is als de norm van een cyclotomisch getal. In deze paragraaf zal ik het 'bewijs' dat Kummer in 1844 voor deze stelling gaf analyseren. Ik zal toelichten waar het bewijs niet klopt, en wat Kummers denkwijze waarschijnlijk was. Een belangrijke vraag die terug zal komen, is of Kummer in dit bewijs gebruikmaakte van unieke factorisatie van cyclotomische getallen. Ook zal ik ingaan op de verdere inhoud van de brief waarin het bewijs terug te vinden is, met name wat het zegt over Kummers motivatie.

De brief is te vinden in de appendix van [10]. Kummer verstuurde deze brief met het bewijs in april 1844 naar Encke. Encke was een astronomie professor en een oud-student van Gauss en adviseur van Kronecker. De precieze formulering van Kummers 'Hauptsatz über diese complexen Zahlen' in de brief is als volgt:

> Lehrsatz: Jede reelle Primzahl p von der Form $m\lambda+1$ läßt sich in $\lambda-1$ complexe Factoren zerlegen von der Form $p = f(\alpha)f(\alpha^2)f(\alpha^3)\cdots f(\alpha^{\lambda-1})$ und diese Factoren sind complexe Primzahlen, welche eine weitere Zerlegung in Factoren nicht zulassen. [10, p. 390]

Voorgaand aan deze stelling had Kummer natuurlijk de benodigde termen geïntroduceerd alsook het feit benoemd dat λ een priemgetal is. Merk nu op dat Kummer 'complexe Primzahlen' zegt, waar wij 'irreducibelen' zouden zeggen. Dit taalgebruik impliceert al de mogelijke toekenning van de eigenschappen van priemgetallen in de gehele getallen aan irreducibelen in de cyclotomische getallen. We zullen zien dat Kummer inderdaad zonder bewijs het priem-zijn volgens definitie 1.1.2 van de irreducibelen gebruikt.

Verder schrijft Kummer aan Encke over het bewijs: "Es würde mir sehr angenehm sein, wenn dieser Aufsatz in den Memoiren der Academie oder in den monatlichen Berichten einen Platz finden könnte"[10, p. 388]. Dit geeft aan dat Kummer erg zeker van zijn zaak was, zo zeker dat hij klaar was voor publicatie. Het bewijs is echter nooit gepubliceerd. Jacobi had de publicatie namelijk net op tijd voorkomen:

> ... Kaum hatte ich bei meiner Rückkehr von Rom einen Fuss hierher gesetzt, als ich den Druck einer Abhandlung von Kummer in den Monatsberichten inhibiren musste. Der gute Junge hatte ohne Weitres die Zerfällbarkeit von $p = \lambda n + 1$ in complexe von den λt. [λ-ten] Wurzeln abhängigen Zahlen angenommen und daraus allgemeine Sätze abgeleitet. [10, p. 393]

De woorden 'ohne Weitres' ('ohne weiteres') betekenen hier 'zomaar'. Kummer had wel een bewijs gegeven, maar het was een eenvoudig bewijs dat helaas te kort schoot. Dit citaat maakt het ook waarschijnlijk dat Jacobi degene was die Kummer het tegenvoorbeeld van $\lambda = 23$ had laten zien.

Dat Kummer zo overtuigd was van de stelling, is wel te begrijpen. Het gaat immers zo lang goed voor de cyclotomische getallen die Kummer bestudeerde (namelijk voor alle $\lambda < 23$). Edwards noemt als reden

van Kummers fouten, dat hij 'chronisch optimistisch'[10, p. 382] is. Kummer werkte door veel voorbeelden numeriek uit te werken. Zo had hij voor alle priemgetallen van de vorm $p = m\lambda + 1 < 1000$ apart de cyclotomische factor $f(\alpha)$ gevonden zodat $p = N(f(\alpha))$, zie Kummers artikel [15]. Natuurlijk probeert Kummer dan uit deze voorbeelden een algemene conclusie te trekken. Soms is hij echter te optimistisch; te snel in het trekken van algemene conclusies en daardoor te vlug in het geven van een bewijs. Dat bewijs blijkt dan vervolgens niet helemaal waterdicht, of zelfs helemaal niet. Een ander voorbeeld hiervan, is dat Kummer een juist bewijs van onderliggende feiten bij de definitie van de ideale factoren pas tien jaar na de introductie van deze definitie gaf. Chronisch optimisme leidt echter wel tot een visie. Dit moet Kummer zeker geholpen hebben bij het introduceren van de ideale getallen. Kummer noemt ook kort na zijn introductie van deze ideale getallen voor cyclotomische getallen al de mogelijkheid tot uitbreiding naar complexe getallen van de vorm $a + b\sqrt{D}$ [16, p. 325]. In 1859 had Kronecker, de vroegere student van Kummer, een volledige generalisatie van zijn werk naar alle algemene 'complexe getallen' gevonden [12, p. 329]. Dit werd echter pas in 1881 gepubliceerd [12, p. 322]. Het lijkt er echter op dat deze generalisatie niet is waar Kummers voornaamste interesse lag. Kummer was vooral geïnteresseerd in de toepassingen van zijn stelling, zoals we zullen zien in 1.3.2. Het zijn dan ook die toepassingen, die hem motiveerden om ideale factoren te introduceren om het probleem op te lossen. Ik zal nu eerst Kummers bewijs bespreken, en daarna de toepassingen benoemen. Hierbij zal ik ook ingaan op de speculatie rond Kummers motivatie voor zijn introductie van de ideale factoren.

1.3.1 Het bewijs

In het bewijs noemt Kummer zoals hiervoor α een eenheidswortel van graad het priemgetal λ, dus $\alpha^\lambda = 1$, p een priemgetal zodat $p = m\lambda + 1$ en $f(\alpha)$ een cyclotomisch getal. Nieuw is het gehele getal ξ, dat voldoet aan $1 + \xi + \xi^2 + ... + \xi^{\lambda-1} \equiv 0 \mod p$ (en dit impliciteert $\xi^\lambda \equiv 1 \mod p$ door vermenigvuldiging met $\xi - 1$). Dit soort getallen ξ zullen we weer tegenkomen in de definitie van ideale factoren in de volgende paragraaf. Nu kunnen we Kummers bewijs in drie delen opsplitsen, namelijk in de stellingen:

1. De getallen p en $\xi - \alpha$ hebben een gemeenschappelijke factor $f(\alpha)$.
2. Elk cyclotomisch getal $f(\alpha^i)$ met $i \in \{1, 2, \ldots, \lambda - 1\}$ is ook een gemeenschappelijke deler van p en $\xi - \alpha$.
3. Het getal p is te schrijven als het product van de $\lambda - 1$ factoren $f(\alpha^i)$ zoals hierboven.

De cruciale fout in het bewijs zit in het begin, al gelijk in stelling (1). De tweede stelling volgt gelijk uit (1). Stelling (3) is ook een correct gevolg, maar we zullen zien dat er nog iets ontbreekt aan Kummers bewijs. Ik zal nu eerst behandelen wat de redenatie was achter de aanname (1) en hoe we dit kunnen interpreteren. Daarna zal ik de rest van het bewijs toelichten en bespreken wat er ontbreekt bij (3).

Stelling 1: De cruciale fout

Edwards geeft in [10, p. 385] aan waarom Kummers bewijs niet klopt. Stelling (1) zoals hierboven is namelijk niet in het algemeen waar. Kummers 'bewijs' dat de factor $f(\alpha)$ wel bestaat, maakt gebruik van een tegenspraak. Hij zegt:

> Hätten nämlich $\xi - \alpha$ und p keinen gemeinschaftlichen Factor, so müßte man zwei Multiplicatoren $\phi(\alpha)$ und $\psi(\alpha)$, ganze rationale Functionen von α, finden können, von der Art daß $\phi(\alpha)(\xi - \alpha) + \psi(\alpha)p$ einer beliebig gegebenen ganzen rationalen Function von α, also auch der 1 gleich wird. [10, p. 390]

Hieruit volgt nu een tegenspraak, omdat bij $\phi(\alpha)(\xi - \alpha) + \psi(\alpha)p = 1$ de norm links niet gelijk is aan 1 zoals rechts. Dat we $\varphi(\alpha)(\xi - \alpha) + \psi(\alpha) \cdot p = 1$ kunnen schrijven wanneer $\xi - \alpha$ en p geen gemeenschappelijke

factoren hebben, klopt echter niet. Het lijkt op een foute algemenisering van de stelling van Bézout[3]: als $\xi - \alpha$ en p geen factoren gemeen hebben, dan is hun grootste gemene deler 1. Het feit dat Kummer hieraan dacht, heeft volgens Edwards, zie [9, p. 235], waarschijnlijk te maken met dat dit geldt voor polynomen over de **rationale getallen**. Het geldt echter niet voor polynomen over de gehele getallen ('ganze rationale Functionen') en ook niet voor de cyclotomische getallen (die opgebouwd zijn uit gehele getallen en een eenheidswortel). Edwards noemt dit een 'embarrassingly simple-minded error' [9, p. 235], absurd voor een wiskundige van Kummers kaliber [9, p. 235]. Hij rationaliseert dit door het te zien als een voorbeeld van Kummers 'chronisch optimisme'. Mogelijk had Kummer veel voorbeelden gezien waar dit geldt en het daarom te snel algemeen aangenomen [9, p. 235].

Bölling geeft in [3, p. 153] een alternatieve visie waarin deze fout minder absurd lijkt. Kummers aanname kan namelijk ook gezien worden als een gevolg van de aanname van unieke factorisatie met een vrij kort en eenvoudig argument. (Edwards ontkent juist dat Kummer unieke factorisatie aangenomen zou hebben. Hier ga ik in de volgende paragraaf 1.3.2 verder op in.) Hier gebruikt Bölling dat unieke priemfactorisatie equivalent is aan de volgende stellingen [3, p. 156-157]. Hier betekent het 'geen factoren delen', geen factoren behalve factoren die norm gelijk aan 1 hebben.

- Als een element a geen factoren deelt met twee andere elementen b en c, dan deelt het element a ook geen factoren met het product bc van die twee elementen.
- Als een element a door twee elementen b en c zonder gezamenlijke factoren deelbaar is, dan deelt het product van die twee elementen bc ook dit element a.

Hier geeft Bölling een kort bewijs voor. Het is echter mogelijk dat Kummer niet op de hoogte was van deze equivalenties, maar wel van het niet gelden van unieke priemfactorisatie. Dit lijkt mij echter onwaarschijnlijk. Het is vrij logisch dat het niet gelden van unieke priemfactorisatie veel invloed heeft op hoe elementen elkaar delen. Als Kummer zich dit niet besefte, kunnen we in ieder geval stellen dat hij niet lang stil stond bij unieke priemfactorisatie.

Ik zal nu dit argument van Bölling uiteenzetten. Neem β en γ twee cyclotomische getallen die geen factoren (waarvan de norm van 1 verschilt) delen. Bekijk het product $\beta\mu$ voor cyclotomische getallen μ. Wanneer twee van deze producten equivalent zijn, oftewel als

$$\beta\mu_1 \equiv \beta\mu_2 \bmod \gamma,$$

dan volgt

$$\beta(\mu_1 - \mu_2) \equiv 0 \bmod \gamma.$$

Nu gebruiken we dat γ en β geen factoren delen, dus volgt uit unieke priemfactorisatie (met de eerste gegeven equivalentie):

$$\mu_1 - \mu_2 \equiv 0 \bmod \gamma$$

oftewel

$$\mu_1 \equiv \mu_2 \bmod \gamma.$$

Zo volgt dat als μ_1 en μ_2 niet equivalent zijn modulo γ, $\beta\mu_1$ en $\beta\mu_2$ dat ook niet zijn. Neem nu een μ die geen factoren deelt met γ. Dan volgt $\mu \not\equiv 0 \mod \gamma$. Aangezien zowel β als μ geen factoren delen met γ, deelt $\beta\mu$ ook geen factoren met γ volgens de eerst gegeven equivalentie van unieke priemfactorisatie. Als we dus alle *verschillende* waarden voor $\mu \not\equiv 0 \mod \gamma$ langsgaan, dan volgt uit bovenstaande dat de getallen $\beta\mu$ ook allen verschillend en niet-nul modulo γ zijn. Er is dus precies één μ zodat

$$\beta\mu \equiv 1 \bmod \gamma.$$

Daarom is 1 te schrijven als lineaire combinatie van de factoren β en γ, die onderling geen factoren delen. Deze redenatie van Bölling geeft een manier waarop Kummer mogelijk op zijn uitspraak kwam vanuit unieke

[3]De stelling van Bézout zegt dat, als voor gehele getallen x, y geldt dat de grootste gemene deler van x en y 1 is ($ggd(x, y) = 1$), volgt dat er gehele getallen a en b bestaan zodat $ax + by = 1$

factorisatie. Er is echter geen bewijs dat Kummer ook echt zo dacht. De redenatie van Edwards sluit direct aan bij Kummers gebruik van de term 'ganze rationale Functionen'. Bölling geeft dit alternatief omdat, zoals we straks zullen zien bij de analyse van de stellingen (2) en (3), er in Kummers werk meer aanwijzingen zijn dat hij op dat moment overtuigt was van het gelden van unieke factorisatie. Inderdaad is het mogelijk dat Kummer zo'n soort redenatie bedacht zou hebben: hij werkt veel met congruenties. Het is alleen de vraag waarom hij dan dat vervolgens in zijn bewijs niet zou noemen. Toch is het de moeite waard om dit hier te noemen als alternatieve verklaring voor deze uitspraak van Kummer, die gelijk volgt uit unieke factorisatie. Ik zal namelijk in de analyse van (2) en (3), en in onderdeel 1.3.2, een aantal argumenten geven voor de opvatting dat Kummer in het bewijs nog overtuigd was van unieke factorisatie.

Stelling 2 en 3: Aanwijzingen voor de aanname van unieke factorisatie

Wanneer er nu toevallig wel een cyclotomisch getal bestaat dat een factor van zowel $\xi - \alpha$ als p is, dan is het inderdaad waar dat de norm van deze factor gelijk is aan p. Toch is er nog iets op te merken aan Kummers bewijs. Ik zal nu eerst de rest van het bewijs uiteenzetten en daarna de opmerking geven.

Noem $f(\alpha)$ deze gemeenschappelijke factor van $\xi - \alpha$ en p. Dan is $f(\alpha^i)$ ook een factor van $\xi - \alpha^i$ en p. Nu hebben we dus $\lambda - 1$ factoren van p, namelijk $f(\alpha), f(\alpha^2), ..., f(\alpha^{\lambda-1})$. We willen nu laten zien dat deze factoren onderling geen factoren gemeenschappelijk hebben. Bekijk hiervoor de willekeurige factoren $f(\alpha^i)$, $f(\alpha^j)$. Dan is $f(\alpha^i)$ een factor van zowel $\xi - \alpha^i$ als p en $f(\alpha^j)$ een factor van zowel $\xi - \alpha^j$ als p. De claim is nu dat voor elke $i \neq j$ de factoren $f(\alpha^i)$ en $f(\alpha^j)$ geen gemeenschappelijke factoren 'waarvan de norm van 1 verschilt' hebben. Elke gemeenschappelijke factor is dus een eenheid. De redenatie is als volgt. Een gemeenschappelijke factor van $f(\alpha^i)$ en $f(\alpha^j)$ is ook een gemeenschappelijke factor van $\xi - \alpha^i$ en $\xi - \alpha^j$. Dus zo'n factor is ook een factor van het verschil $\alpha^i - \alpha^j$. Maar, zo stelt Kummer, dat is onmogelijk. Hij laat het hierbij, maar we kunnen als volgt inzien waarom dit inderdaad onmogelijk is. Stel dat $j < i$, dan geldt $\alpha^i - \alpha^j = \alpha^j(\alpha^{i-j} - 1)$ en dus:

$$N(\alpha^i - \alpha^j) = N(\alpha^j(\alpha^{i-j} - 1)) = N(\alpha^j)N(\alpha^{i-j} - 1) = 1 \cdot N(\alpha - 1)$$

Verder volgt dat

$$N(\alpha - 1) = (\alpha - 1)(\alpha^2 - 1) \cdots (\alpha^{\lambda-1} - 1) = \lambda^4$$

Voor $j > i$ volgt dan op dezelfde manier $N(\alpha^i - \alpha^j) = N(\alpha^j - \alpha^i) = \lambda$ (want $N(-1) = 1$). Factoren van $\alpha^i - \alpha^j$ hebben dus norm λ of 1, aangezien λ een priemgetal is. Dus nu zijn de enige gemeenschappelijke factoren van $f(\alpha^i)$ en $f(\alpha^j)$, factoren met norm λ of 1. Maar deze gemeenschappelijke factoren moeten ook factoren van p zijn. Nu is het inderdaad onmogelijk dat λ een factor van het priemgetal p is. Dus volgt dat alle $f(\alpha^i)$'s alleen factoren gemeen hebben met norm gelijk aan 1. Dus concludeert Kummer dat we kunnen schrijven $p = f(\alpha) \cdot f(\alpha^2) \cdots f(\alpha^{\lambda-1})$[5].

Dit lijkt overtuigend, maar toch ontbreekt hier nog iets. Met het trekken van de conclusie is Kummer te snel. Het is niet voldoende om alleen te laten zien dat de factoren geen factoren gemeenschappelijk hebben. Dit laat Bölling zien in [3, p. 148-149]. Kummers conclusie volgt namelijk uit de eerder gegeven stellingen die equivalent zijn aan unieke priemfactorisatie.

We kunnen dit ook als volgt zien. Uit het feit dat $f(\alpha), f(\alpha^2), ..., f(\alpha^{\lambda-1})$ factoren van p zijn die onderling geen factoren delen, volgt alleen dat

$$p = f(\alpha)N_1 = f(\alpha^2)N_2 = ... = f(\alpha^{\lambda-1})N_{\lambda-1}$$

[4]Dit legt Edwards uit in [11, p. 91]. Merk op dat $N(\alpha - x) = (\alpha - x)(\alpha^2 - x) \cdots (\alpha^{\lambda-1} - x) = x^{\lambda-1} + x^{\lambda-2} + ... + x + 1$, aangezien $\alpha, \alpha^2, ..., \alpha^{\lambda-1}$ complexe wortels zijn van deze vergelijking. Vul nu $x = 1$ in, en we krijgen $N(\alpha - 1) = \lambda$.

[5]Kummer is zelfs nog preciezer en stelt dat dan geldt $p = f(\alpha) \cdot f(\alpha^2) \cdots f(\alpha^{\lambda-1})\dot{M}$ voor een bepaalde M. Hij voegt toe dat aangezien de norm van $f(\alpha)$ een geheel getal is, M ook een geheel getal moet zijn. Aangezien p een priemgetal is, volgt dat $M = 1$.

voor bepaalde (cyclotomische) factoren N_i, $i \in \{1, 2, ..., \lambda - 1\}$. Als $f(\alpha)$ priem is, dan volgt ook dat $f(\alpha^i) \mid N_j$ voor $j \neq i$ met $i, j \in \{1, 2, ..., \lambda - 1\}$ (want de factoren $f(\alpha^i)$ delen onderling geen factoren) en volgt het resultaat vanzelf. Als $f(\alpha)$ niet priem is, dan hoeft dit niet het geval te zijn en zijn er meerdere factorisaties mogelijk.

Het blijkt inderdaad zo te zijn dat voor $f(\alpha)$ een factor van p en $\xi - \alpha$, volgt dat $f(\alpha)$ priem is. Bölling geeft dit bewijs in Kummers stijl in [4, p. 276]. Wat hier van belang is op te merken, is dat Kummer de noodzakelijkheid van het priem zijn van $f(\alpha)$, of iets equivalent hieraan, niet noemt. Wat dit nog benadrukt, is dat Kummer aan het eind van het bewijs het volgende toevoegt:

> Daß diese $\lambda - 1$ Factoren des p **wirklich Primfactoren** sind, wird sehr leicht bewiesen, wäre nämlich $f(\alpha)$ in zwei Factoren zerlegbar $f(\alpha) = \phi(\alpha)\psi(\alpha)$ deren Normen von Eins verschieden sind, so müßte die Norm von $f(\alpha)$ welche p ist das Product der Norm des $\phi(\alpha)$ und der Norm des $\psi(\alpha)$ sein, also das Product zweier reellen ganzen Zahlen deren keine gleich Eins wird, welches unmöglich ist.

Hiermee heeft Kummer zijn eerdere claim bewezen, dat de factoren $f(\alpha^i)$ 'complexe Primzahlen, welche eine weitere Zerlegung in Factorennicht zulassen' zijn, oftewel irreducibel. Het lijkt er niet op dat Kummer stil stond bij het verschil tussen 'priem' en 'irreducibel'. Mogelijkerwijs was hij in de veronderstelling dat de twee hetzelfde waren in de cyclotomische getallen.

In het onderdeel 1.1 zagen we dat Kummer in 1847 in *Zur Theorie der complexen Zahlen* dit verschil juist wel expliciet benoemde; sterker nog, het was het begin van zijn nieuwe theorie.

1.3.2 De toepassingen

Om helderheid te krijgen over wat Kummers motivatie was om bovenstaande stelling te bewijzen, is het van belang om te kijken waarop Kummer deze stelling wilde toepassen. In de inleiding van deze paragraaf kwam al voorbij dat Kummer *niet* voornamelijk geïnteresseerd was in de mogelijke generalisatie van zijn theorie, maar meer in de mogelijke toepassingen. In deze paragraaf zullen we bespreken wat Kummers belangrijkste motivatie was voor het formuleren van de stelling in het bewijs uit 1844. Hieruit volgt ook zijn motivatie voor het introduceren van de ideale factoren toen deze stelling toch niet waar bleek te zijn. We zullen zien dat Kummers voornaamste interesse hogere reciprociteitswetten was. Vaak wordt beweerd dat dit juist de laatste stelling van Fermat was. In deze paragraaf zal ik zowel de hogere reciprociteitswetten als de laatste stelling van Fermat verder toelichten.

De reden dat Kummer vaak met de laatste stelling van Fermat geassocieerd wordt, is een verhaal van Hensel. Hensel beweerde dat Kummer een bewijs had gegeven van de laatste stelling van Fermat, gebaseerd op unieke factorisatie van cyclotomische getallen. Kummer zou vervolgens op het idee van ideale factoren zijn gekomen nadat Dirichlet hem er op wees dat zijn bewijs niet klopte. Hensel had dit verteld in een college over Kummer in 1910. Hij had dit verhaal gehoord van iemand die het van iemand had gehoord die het van Kummer had gehoord [9, p. 225-226]. Dit alleen al is reden genoeg om Hensels verhaal met een flinke korrel zout te nemen. Daarnaast is er nooit een document met een bewijs van de laatste stelling van Fermat van Kummer gevonden. In [9] brengt Edwards Hensels verhaal uitgebreid onderuit. In de rest van deze paragraaf zullen we aanwijzingen zien dat Kummers voornamelijke reden voor zijn theorie lag bij hogere reciprociteitswetten, en dus niet bij Fermat. Hier zijn wiskundig historici het over het algemeen over eens [6, p. 86].

Echter is er in de literatuur wel onenigheid over of Kummer in het bewijs in 1844 uitgaat van unieke factorisatie van cyclotomische getallen. Wanneer dit inderdaad het geval is, lijkt het gelijk waarschijnlijker dat Kummer ook met behulp van deze unieke factorisatie de laatste stelling van Fermat bewezen zou hebben. Edwards spreekt zich in [9] sterk uit tegen deze mogelijkheid. Hier gaat Bölling in een analyse van het genoemde bewijs in [3] tegen in. We hebben in het bewijs van Kummer gezien dat Edwards en Bölling verschillende opvattingen hadden over Kummers incorrecte bewijs van de stelling (1). Ik zal nu eerst verder

ingaan op de laatste stelling van Fermat en de mogelijkheid dat Kummer hier een bewijs voor had gegeven dat beruste op unieke factorisatie. Daarna zal ik het hebben over Kummer en hogere reciprociteitswetten.

De toepassing die sinds Hensel vaak gegeven wordt als Kummers motivatie, is dus de laatste stelling van Fermat. Deze luidt dat voor $x, y, z \in \mathbb{Z}$ en $n > 2$ een natuurlijk getal:

$$x^n + y^n = z^n \implies xyz = 0$$

oftewel de vergelijking $x^n + y^n = z^n$ heeft voor $n > 2$ alleen triviale oplossingen. Deze stelling was in 1637 door Fermat gepresenteerd. Fermat had opgeschreven een geweldig bewijs te hebben, maar dat dit bewijs helaas te groot was voor de kantlijn waarin hij aan het schrijven was [9, p. 219]. Mogelijk hield Fermat hiermee iedereen voor de gek, of had hij een verkeerd bewijs in gedachten. In ieder geval hield dit probleem in de eeuwen na Fermat veel wiskundigen bezig. Het volledige bewijs van 129 pagina's werd pas in 1994 gegeven door Andrew Wiles en bevatte veel nieuwe wiskunde (onder andere over elliptische krommen). Het is absoluut ondenkbaar dat Fermat dit bedacht kon hebben in 1637. Ik heb eerder genoemd dat Cauchy en Lamé een bewijs hadden gegeven dat gebruikmaakte van unieke factorisatie in de cyclotomische getallen, zoals beschreven in [9]. Zo'n bewijs maakt gebruik van factorisatie van $x^n + y^n$ in de cyclotomische getallen, waarbij r een eenheidswortel van graad n is (dus $r^n = 1$). Edwards geeft in [9, p. 220-221] aan hoe dit werkt. Ik zal dit hier uiteenzetten. Merk op dat:

$$z^n = x^n + y^n = (x + y)(x + ry)\left(x + r^2y\right) \cdots \left(x + r^{n-1}y\right) [9, p.\ 220].$$

Hierbij kijken we naar het geval dat $n > 2$ een priemgetal is[6], zodat dus n oneven is en $-1, -r, -r^2$, ..., $-r^{n-1}$ de oplossingen zijn van de vergelijking $z^n + 1 = 0$ en we dus met de hoofdstelling van de algebra vinden dat $z^n + 1 = (z + 1)(z + r) \cdots \left(z + r^{n-1}\right)$. Nu volgt bovenstaande vergelijking door de substitutie $z = \frac{x}{y}$ uit te voeren en te vermenigvuldigen met y^n. Hieruit probeerde (onder andere) Lamé een tegenspraak af te leiden, waarbij hij eigenschappen van de gehele getallen op de factoren $(x + r^iy)$ projecteerde. Zo heeft hij het in zijn bewijs over de grootste gemene deler van deze factoren, een begrip dat zonder unieke factorisatie geen betekenis heeft [9, p. 221].

Edwards beschrijft in [9] dat hij het ondenkbaar vindt dat een wiskundige van Kummers kaliber zo'n soort fout ook gemaakt zou hebben. Hij was immers goed bekend met het werk van Gauss, en die gaf voor de getallen $\mathbb{Z}[\sqrt{-1}]$ een rigoreus bewijs voor unieke priemfactorisatie [9, p. 226]. Ik heb in 1.1 al besproken dat dit mijns inziens toch mogelijk zou kunnen zijn, gezien het feit dat het juist wel geldt voor de complexe gehelen Gauss én voor cyclotomische getallen met $\lambda < 23$. Gezien Kummer veel op voorbeelden gericht was, is het niet onaannemlijk dat dit voldoende was om hem te overtuigen.

Toen Edwards dit schreef, had hij Kummers bewijs in 1844 nog niet gezien. In een appendix, zie [9, p. 232-236], heeft hij later toegevoegd dat hij, hoewel hij zich minder zeker voelt, nog steeds achter zijn mening staat. Volgens Edwards gaat Kummer namelijk in zijn brief aan Encke niet uit van unieke factorisatie. Dit is echter te betwisten.

Kummer noemt niet expliciet dat hij zonder bewijs uitgaat van unieke factorisatie in cyclotomische getallen. Het is echter mogelijk dat hij dit als iets vanzelfsprekends zag. Als we willen concluderen dat Kummer uit ging van unieke factorisatie, zal dit vooral volgen uit wat hij *niet* zegt. We hebben al gezien dat de meningen verdeeld zijn of Kummers fatale foute aanname die leidt tot stelling (1) een gevolg is van zijn aanname van unieke factorisatie of niet. Kummers andere nalatigheid was, dat hij niet bewees dat $f(\alpha)$ priem is. Dit is directer gelinkt aan unieke factorisatie. Echter kan dit ook iets zijn waar Kummer zich wel bewust van was, maar dat hij hier simpelweg achterwege gelaten had. Helemaal overtuigend is dit echter niet, zeker omdat deze nalatigheid zich herhaalt in de toepassingen die Kummer noemt (zie [3] voor de voorbeelden). Verder uitte Kummer in [15] oprechte teleurstelling, over specifiek het feit dat de cyclotomische getallen deze

[6]Merk op dat als $x^n + y^n = z^n$ geen oplossingen heeft, dat dan ook $x^{nm} + y^{nm} = z^{nm}$ geen oplossing heeft voor elk geheel getal $m > 0$, immers is anders x^m, y^m, z^m een oplossing bij graad n. Dus moeten we voor de stelling van Fermat alleen het geval $n = 4$ en n priem behandelen. Het geval $n = 4$ is niet heel lastig, dus bekijken we het geval $n > 2$ priem. [9, p. 220]

specifieke eigenschap van de gehele getallen niet delen (hij noemt dit 'maxime dolendum', zeer jammer [15, p. 182]). Het lijkt dus waarschijnlijk dat hij hier eerder wel vanuit was gegaan. Daarnaast heeft Kummer veel publicaties op zijn naam staan over bewijzen van bepaalde gevallen van de laatste stelling van Fermat. Het lijkt mij daarom niet uitgesloten dat Kummer op een bepaald moment zelf ook, gebruikmakend van unieke factorisatie, een bewijs van de laatste stelling van Fermat gegeven had. Het feit blijft echter dat zo'n document nooit gevonden is. Het is natuurlijk mogelijk dat de publicatie tegengehouden was, net zoals voor Kummers bewijs in 1844.

Wat in ieder geval zeer onwaarschijnlijk is, is dat de laatste stelling van Fermat de reden was voor Kummers introductie van ideale factoren, zoals in het verhaal van Hensel. Dit wordt nu vaak algemeen aangenomen als Kummers belangrijkste motivatie, terwijl dat zeker de hogere reciprociteitswetten waren. Gauss introduceerde de kwadratische reciprociteitswet in de *Disquisitiones Arithmeticae*.[7] Hier maakte Gauss al toespelingen in de richting van hogere reciprociteitswetten, wat opgepakt werd door Eistenstein en Jacobi [6, p.83-85]. Zo gaf Eisenstein een bewijs van een bikwadratische (vierdegraads) reciprociteitswet die Gauss eerder geformuleerd had voor zijn complexe gehelen, zie ook de eerste twee regels van het komende citaat. Hogere reciprociteitswetten waren ook voor Jacobi de reden om onderzoek te doen in de richting van de cyclotomie of cirkeldeling ('Kreistheilung'). Dit is de studie naar de oplossingen van de vergelijking $x^n = 1$ [10, p. 386-387]. In feite correspondeert elke hogere macht (in ons verhaal, elk volgend priemgetal λ), met een mogelijke hogere reciprociteitswet [4, p. 280]. We kunnen Kummer zien als de directe opvolger van Jacobi. Zo had hij ook precies Jacobi's notatie, zoals het gebruik van de letters α en λ als respectievelijk een eenheidswortel en een priemgetal, overgenomen [11, p. 79]. Dat de hogere reciprociteitswetten inderdaad Kummers voornaamste motivatie waren, bevestigen onder andere Edwards in [11] en [9] en Neumann in [18]. Het meest overtuigende bewijs komt van Kummer zelf: de toepassingen (in de cyclotomie) die hij noemt in zijn bewijs in 1844 en na de introductie van ideale factoren en wat hij zelf heeft gezegd over zijn interesse. In de eerste categorie valt bijvoorbeeld de opening van de genoemde brief van Kummer in april 1844:

> Nachdem Gauß zuerst die complexen Zahlen von der Form $a + b\sqrt{-1}$ in die Zahlentheorie eingeführt hatte, welche für die Theorie der biquadratischen Reste die passendsten sind, hat Jacobi gezeigt, was auch bei Gauß sich schon angedeut findet, daß allgemeiner alle ganzzahligen ganzen Functionen der Wurzeln der Gleichung $\alpha^\lambda = 1$ diejenigen complexen Zahlen ausmachen, welche in der Zahentheorie und in der **Kreistheilung** von der größten Wichtigkeit sind. **Für diese hat Jacobi allgemein bewiesen, daß jede Primzahl p von der Form $m\lambda + 1$ sich als Product zweier complexer Zahlen darstellen läßt**, welche aus λ-ten Wurzeln der Einheit gebildet sind, und zwar ist diese Zerlegung in zwei complexe Factoren auf mehrere verschiedene Weisen möglich. [10, p.388]

Dit bevestigt de invloed van Jacobi op Kummer. Ook geeft het aan dat Kummers interesse in cyclotomische getallen voortkwam uit de toepassing op de cyclotomie of cirkeldeling. In bovenstaand citaat schrijft Kummer dat Jacobi een factorisatie ('Zerlegung') gaf van het priemgetal p in twee cyclotomische getallen. Ook zegt hij dat die factorisatie niet uniek is. Daarna schrijft Kummer, verwijzend naar een lezing van Jacobi in 1839:

> Dieser Umstand [...] führte ihn [Jacobi] auf die Vermutung, daß diese complexe Zahlen nicht Primzahlen, sondern aus anderen complexen Zahlen derselben Art zusammengesetzt sein möchten. [10, p.388-389]

Dat de factorisatie van Jacobi van p in twee factoren niet uniek was, deed Jacobi dus vermoeden dat de twee factoren niet priem waren. Hier wordt 'priem' gebruikt als 'irreducibel'; niet verder factoriseerbaar. Jacobi suggereerde dus (volgens Kummers interpretatie) dat een unieke factorisatie in priemfactoren wel bestond, maar nog niet gevonden was. Dit betekent dat er nog geen verschil werd gezien tussen de begrippen priem en irreducibel. In feite wordt geen rekening gehouden met het feit dat er mogelijk (en zoals we weten, is dit

[7] De kwadratische reciprociteitswet luidt: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, waarbij het Legendre-symbool $\left(\frac{p}{q}\right) = 1$ als er een x bestaat $x^2 \equiv p \mod q$, en als dit niet het geval is $\left(\frac{p}{q}\right) = -1$. In woorden geeft de kwadratische reciprociteitswet dus een verband tussen het kwadraat-zijn van $p \mod q$ en $q \mod p$. Een hogere reciprociteitswet geeft dus een verband tussen of $p \mod q$ en $q \mod p$ wel of niet een n-de macht zijn voor $n > 2$.

inderdaad het geval) geen unieke factorisatie geldt in de cyclotomische getallen. Dus tracht Kummer hier de door Jacobi gesuggereerde ontbinding van p in priemfactoren te geven. Specifiek geeft hij een factorisatie van elke $p = m\lambda + 1$ in $\lambda - 1$ complexe factoren.

Jacobi was dus voor Kummer de aanleiding voor het zoeken naar een ontbinding van p in priemfactoren. Terug naar de reden voor Kummer voor het geven van dit bewijs. Dit hangt duidelijk samen met Jacobi's onderzoek naar cirkeldeling, aangezien dat voor hem de reden was voor het geven van de factorisatie van p in twee cyclotomische factoren. Kummer zegt dat zijn resultaat (de factorisatie van p in $\lambda - 1$ factoren) de theorie van de cirkeldeling enorm vereenvoudigt [10, p. 389]. Na zijn bewijs, geeft Kummer inderdaad meteen de toepassing op de theorie van cirkeldeling.

Andere aanwijzingen voor Kummers motivatie, zijn de volgende citaten van Kummer zelf. Deze komt uit Kummers publicatie in 1847, waarbij hij een bewijs geeft van bepaalde gevallen van de laatste stelling van Fermat:

> Der Fermatsche Satz ist zwar **mehr ein Curiosum als ein Hauptpunkt** der Wissenschaft [...] [14, p. 281]

In 1848 schrijft Kummer in een brief aan Kronecker:

> [...] daß ich jetzt versuche von hier aus weiter **gegen meinen Hauptfeind, das simple [sic] Reciprocitätsgesetz**, zu operiren. [14, p. 112]

In 1850 in een publicatie over bepaalde hogere reciprociteitswetten:

> [...] ist es mir gelungen die allgemeinen Reciprocitätsgesetze für beliebig hohe Potenzreste zu entdecken, welche nach dem gegenwärtigen Stande der Zahlentheorie als **die Hauptaufgabe und die Spitze** dieser Wissenschaft anzusehen sind. [14, p. 347]

Duidelijk is dus dat Kummer zowel in de eerste instantie als later, dus als voornaamste reden voor zijn bewijs in 1844 en voor de latere introductie van ideale factoren, de hogere reciprociteitswetten had.

1.4 Ideale factoren

In de vorige paragraaf heb ik uitgebreid aandacht besteed aan Kummers motivatie in zijn studie naar de cyclotomische getallen en de introductie van ideale factoren. Ik heb ook uitgebreid besproken wat er mis gaat in Kummers bewijs uit 1844. De belangrijkste conclusie die we hieruit kunnen trekken, is dat Kummer zich niet liet ontmoedigen. Het moet voor hem een grote tegenslag zijn geweest dat hij zijn bewijs moest terugtrekken. Toch bleef hij cyclotomische getallen bestuderen. Deze keer richtte hij zich specifiek op waar het eerder mis was gegaan: de unieke factorisatie van cyclotomische getallen. Vandaar dat Kummer nu de ideale getallen introduceerde.

Zo geven ideale factoren een oplossing voor het geval dat $p = m\lambda + 1$, met λ een priemgetal, niet in $\lambda - 1$ factoren te ontbinden is volgens $p = N(f(\alpha)) = f(\alpha)f(\alpha^2)\cdots f(\alpha^{\lambda-1})$ voor een bepaald cyclotomisch getal $f(\alpha)$. We hebben net gezien dat Kummer hier in april 1844 nog wel van overtuigd was: dit was de stelling waarvan we het bewijs bestudeerd hebben. Als dit wel altijd mogelijk is, weten we het behulp van moderne algebraïsche getaltheorie dat dit inderdaad impliceert dat $\mathbb{Z}[\alpha]$ een uniek factorisatiedomein is: zie hiervoor [4, p. 278]. Het is niet duidelijk of Kummer wist dat deze implicatie gold. Kummer moet uiteindelijk na Jacobi's voorbeeld (zie paragraaf 1.2) wel gezien hebben hoe (het niet gelden van) unieke factorisatie een rol speelt bij de stelling. Er zijn namelijk verschillende factorisaties in irreducibelen van p mogelijk. Hij zag dit misschien op dezelfde wijze zoals beschreven aan het eind van paragraaf 1.2, of via een ander voorbeeld. Ideale factoren lossen hoe dan ook beide problemen op.

In het artikel *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant*[15] (vertaald: *Over complexe getallen, die bestaan uit eenheidwortels en gehele getallen*), bestudeert Kummer de werking

van cyclotomische getallen en hun norm, vooral in het geval dat die norm toevallig toch gelijk is aan $p = m\lambda+1$. Ook schrijft hij hier over het falen van de unieke factorisatie in het geval $\lambda = 23$. Kummer geeft wel een methode om de factor te vinden waarvan de norm p oplevert, indien die bestaat. Dit ging identiek aan zijn bewijs in april 1844, alleen neemt hij nu niet aan dat zo'n factor $f(\alpha)$ van $\xi - \alpha$ en p altijd bestaat. In plaats daarvan geeft hij een algoritme om die te vinden (gebaseerd op het Euclidisch algoritme), zie voor een uitgebreide verklaring [4, p. 277-278]. Het resultaat is een overzicht van de cyclotomische getallen waarvan de norm p is voor $\lambda < 23$. Zoals we weten, hield Kummer het hier niet bij. In 1847 werd zijn artikel *Zur Theorie der Complexen Zahlen*[16] gepubliceerd, waarin Kummer voor het eerst de ideale factoren introduceerde.

1.4.1 De definities

Kummer gaf in *Zur Theorie der Complexen Zahlen*[16] aan dat er veel mogelijke definities waren voor zijn begrip 'ideale factor'. Vervolgens geeft hij er eerst een die gebaseerd was op congruenties, en daarna een gebaseerd op de vermenigvuldiging van factoren. Ik zal nu ook eerst de definitie gebaseerd op congruenties geven. Daarna zal ik bespreken wat de minpunten zijn van deze definitie, oftewel waarom Kummer de tweede definitie introduceert. Na de tweede definitie, zal ik bepaalde eigenschappen van ideale factoren benoemen.

De eerste definitie is volgens Kummer de eenvoudigste en algemeenste. Kummer zegt eerst nog het volgende over het op te lossen probleem:

> Ist p eine Primzahl von der Form $m\lambda+1$, so läßt sie sich in vielen Fällen als Product von folgenden $\lambda-1$ complexen Factoren darstellen: $p = f(\alpha)\cdot f(\alpha^2)\cdot f(\alpha^3)\cdots f(\alpha^{\lambda-1})$; wo aber eine Zerlegung in **wirkliche complexe Primfactoren** nicht möglich ist: dann sollen die idealen Primfactoren eintreten, um dieselbe zu leisten. [16, p. 204]

Kummer zegt dat p vaak in $\lambda - 1$ factoren te ontbinden is volgens $p = N(f(\alpha))$. We hebben gezien dat in dat geval volgt dat $f(\alpha)$ dan een cyclotomisch priemgetal is. Wanneer zo'n getal niet bestaat, introduceert Kummer een ideale priemfactor om dit op te lossen. Ik zal nu eerst de definitie van een ideale factor uiteenzetten zoals in Kummers artikel [16], en daarna een lemma uit zijn artikel [15] laten zien waar deze op gebaseerd zijn. Hierin noemt Kummer p een priemgetal met $p = m\lambda + 1$, voor λ een priemgetal. Kummer heeft het volgende nodig voor zijn definitie, ik noem dit citaat 1:

> Ist $f(\alpha)$ eine **wirkliche complexe Zahl** und ein **Primfactor** von p, so hat sie die Eigenschaft, daß, wenn statt der Wurzel der Gleichung $\alpha^\lambda = 1$ eine bestimmte Congruenzwurzel von $\xi^\lambda = 1 \mod p$, substituirt wird, $f(\xi) \equiv 0 \mod p$, ist. [16, p. 204]

Ik zal hier zo een bewijs van uiteenzetten. Kummer maakte in het vorige citaat al een onderscheid tussen *wirkliche complexe Primfactoren* en *idealen Primfactoren*. Hier wil hij dus aangeven dat $f(\alpha)$ een daadwerkelijk (niet ideaal) priemgetal is (voor ons: volgens definitie 1.1.2, want anders is de factorisatie niet uniek en zou Kummer een ideaal priemgetal gebruiken in de plaats) dat voldoet aan $p = N(f(\alpha))$. Uit bovenstaande uitspraak volgt ook het volgende feit van Kummer, citaat 2:

> Also auch, wenn in einer complexen Zahl $\Phi(\alpha)$ der Primfactor $f(\alpha)$ enthalten ist, wird $\Phi(\xi) \equiv 0 \mod p$; und umgekehrt: wenn $\Phi(\xi) \equiv 0 \mod p$, und p in $\lambda - 1$ complexe Primfactoren zerlegbar ist, enlhält $\Phi(\alpha)$ den Primfactor $f(\alpha)$. [16, p. 204]

Nu merkt Kummer op dat $\Phi(\xi) \equiv 0 \mod p$ onafhankelijk is van of p wel of niet in $\lambda-1$ factoren te ontbinden is. Daarom kunnen we daaruit een definitie afleiden. In Kummers woorden is deze dan:

> [...] die complexe Zahl $\Phi(\alpha)$ den idealen Primfactor von p enthält, welcher zu $\alpha = \xi$ gehört, wenn $\Phi(\xi) \equiv 0 \mod p$, ist.[16, p. 204]

Kummer gebruikt congruenties modulo p gebruikt, om zo toch de $\lambda-1$ (ideale) factoren te vinden [5, p. 498-499]. In plaats van te kijken naar α zodat $\alpha^{23} = 1$, zoekt Kummer naar $\xi \mod p$ zodat $\xi^\lambda \equiv 1 \mod p$. In plaats van $\xi^\lambda \equiv 1 \mod p$, noemt Kummer op andere plekken die we zo zullen zien $1+\xi+\xi^2+...+\xi^{\lambda-1} \equiv 0$

mod p. Dit doet hij naar alle waarschijnlijkheid omdat hij zo aan precies $\lambda - 1$ ideale factoren komt, doordat de oplossing $\xi = 1$ wegvalt.[8]. Die triviale oplossing 'hoort bij' $\alpha = 1$ en willen we dus niet hebben. Dat er dan altijd $\lambda - 1$ oplossingen van deze vergelijking zijn, zien we als volgt. Merk op dat we te maken hebben met de multiplicatieve groep modulo p. Dit is een cyclische groep met een voortbrenger g, dus weten we dat $p-1$ het kleinste getal is zodat $g^{p-1} \equiv 1 \mod p$. Een mogelijke oplossing van $\xi^\lambda \equiv 1 \mod p$ is dus van de vorm $\xi = g^k$. Dan geldt $g^{k\lambda} \equiv 1 \mod p$ en dus $p - 1 \mid k\lambda$ oftewel $\frac{p-1}{\lambda} \mid k$. Definieer nu $m := \frac{p-1}{\lambda}$. Dan hebben we voor $1 < \xi < p$, dat $\xi = g^m, g^{2m}, ..., g^{(\lambda-1)m}$: precies $\lambda - 1$ oplossingen.

Er zijn een aantal uitspraken uit de citaten van Kummer die uit het niets lijken te vallen. Waarom geldt bijvoorbeeld dat $f(\xi) \equiv 0 \mod p$? En hoe volgen de eigenschappen van $\Phi(\xi)$ uit het daarop volgende citaat hieruit? Voor de eerste vraag zoeken we een bewijs van het lemma (equivalent aan citaat 1 van Kummer):

Lemma 1.4.1. Wanneer $\xi < p$ een geheel getal is zodat $1 + \xi + \xi^2 + ... + \xi^{\lambda-1} \equiv 0 \mod p$, en α een eenheidswortel van graad λ ($\alpha^\lambda = 1$), met $f(\alpha)$ en $p = m\lambda + 1$ zodat $p = N(f(\alpha))$, dan volgt dat $f(\xi) \equiv 0 \mod p$.

Om dit bewijs te vinden, gaan we eerst terug naar Kummers artikel [15]. Hier geeft Kummer een bewijs dat, onder de voorwaarden van lemma 1.4.1, $\alpha \equiv \xi \mod f(\alpha)$. Hieruit volgt een bewijs van het lemma:

Bewijs. Uit $\alpha \equiv \xi \mod f(\alpha)$ volgt $f(\alpha) \equiv f(\xi) \mod f(\alpha)$ en dus $f(\xi) \equiv 0 \mod f(\alpha)$. Merk nu op dat $f(\xi)$ een geheel getal is. Dus, als $f(\alpha) \mid f(\xi)$, dan geldt dit ook voor elke geconjungeerde van α en dus voor p[9]. We kunnen dit ook als volgt aantonen: Als $f(\alpha) \mid f(\xi)$, dan $N(f(\alpha)) \mid N(f(\xi))$, dus $p \mid f(\xi)^{\lambda-1}$ en dus $p \mid f(\xi)$ (want p is een priemgetal). Zo volgt dus dat $f(\xi) \equiv 0 \mod p$. □

Het bewijs dat $\alpha \equiv \xi \mod f(\alpha)$ is wat langer en te vinden in [15, p. 175-177]. Het berust op het lineair uitwerking van de vergelijking $p = f(\alpha)F(\alpha)$, waarbij $F(\alpha) = f(\alpha^2)f(\alpha^3)\cdots f(\alpha^{\lambda-1})$. Dan vindt Kummer uiteindelijk de juiste ξ, en dat $(\xi - \alpha)F(\alpha) \equiv 0 \mod p$, waaruit het gevraagde volgt.[10]

Citaat 2 van Kummer is nu equivalent aan het volgende lemma.

Lemma 1.4.2. Neem ξ, α, p en $f(\alpha)$ zoals in lemma 1.4.1. Er geldt dus met name dat $p = N(f(\alpha))$. Neem $\Phi(\alpha)$ een cyclotomisch getal. Dan volgt dat $f(\alpha) \mid \Phi(\alpha)$ dan en slechts dan als $\Phi(\xi) \equiv 0 \mod p$.

Dit is eenvoudig te bewijzen uit lemma 1.4.1:

Bewijs. (a) Stel dat $f(\alpha) \mid \Phi(\alpha)$. Dan hebben we $\Phi(\alpha) = f(\alpha)g(\alpha)$ voor een bepaald cyclotomisch getal $g(\alpha)$. Dus ook $\Phi(\xi) = f(\xi)g(\xi)$. Uit lemma 1.4.1 volgt dat $f(\xi) \equiv 0 \mod p$, dus inderdaad $\Phi(\xi) \equiv 0 \mod p$.
(b) Stel dat $\Phi(\xi) \equiv 0 \mod p$. Dan volgt uit $\xi \equiv \alpha \mod f(\alpha)$, dat $\Phi(\xi) \equiv \Phi(\alpha) \mod f(\alpha)$. Dus ook $\Phi(\alpha) \equiv 0 \mod f(\alpha)$ oftewel $f(\alpha) \mid \Phi(\alpha)$. □

[8] Merk namelijk op dat: $x^\lambda - 1 = (1 + x + x^2 + ...x^{\lambda-1})(x - 1)$.

[9] "numerus autem integer realis $f(\xi)$ qui factorem $f(\alpha)$ continet, omnes etiam factores huic conjunctos, ideoque factorem p continere debet"[14, p. 177]; oftewel "maar een reëel geheel getal $f(\xi)$, dat de factor $f(\alpha)$ bevat, bevat ook alle van deze geconjungeerde factoren, en daarom moet deze ook de factor p bevatten."

[10] Overigens gebruikt Kummer in [15] dat $\alpha \equiv \xi \mod f(\alpha)$, om aan te tonen dat het niet mogelijk is om twee verschillende cyclotomische getallen te vinden met norm gelijk aan p; oftewel er bestaan geen $\psi(\alpha)$ en $f(\alpha)$ met $p = N(\psi(\alpha)) = N(f(\alpha))$. Het is ook interessant dat hij dit doet op een voor ons bekende manier. Hij neemt namelijk aan dat dit wel geldt voor bepaalde $\psi(\alpha)$ en $f(\alpha)$, en laat dan zien dat volgt dat er een andere $\phi(\alpha)$ bestaat zodat $\psi(\alpha) = f(\alpha)\phi(\alpha)$ en dus $N(\psi(\alpha)) = N(f(\alpha))N(\phi(\alpha))$ en $N(\phi(\alpha)) = 1$, dus $\phi(\alpha)$ is een eenheid en $\psi(\alpha)$ en $f(\alpha)$ zijn equivalent onder vermenigvuldiging met een eenheid [15, p. 178-179]. Dat het cyclotomische getal $f(\alpha)$ uniek is, is ook van belang voor de gegeven lemma's. Hier nam Kummer dus niet zomaar aan dat een product van irreducibelen uniek is. Op pagina 13 hebben we gezien dat Kummer eerder al bewezen had dat $f(\alpha)$ irreducibel is. In het bewijs uit 1844 zegt hij niets over de uniciteit van $f(\alpha)$. Wat interessant is, is dat hij hier ten tijde van het bewijs uit 1844 wel van op de hoogte was. Hij geeft namelijk een bewijs dat $a \equiv \xi \mod f(\alpha)$ en de daarop volgende uniciteit van getallen $f(\alpha)$ zodat $p = N(f(\alpha))$ al eerder in een brief naar Kronecker die staat in [14, p. 53-57]. Hier zegt Kummer echter over dit feit, 'so finde ich sie trotz dem daß es nur Beweise von Dingen sind, die sich gewissermaßen von selbst verstehen', wat kan verklaren waarom hij dit in het bewijs in 1844 niet noemt. Hier gaat Bölling verder op in in [3, p. 149-150]

We hebben nu gezien waar de stellingen uit Kummers citaten vandaan kwamen (namelijk uit zijn artikel [15]) en hoe de uitspraken volgen.

Samenvattend hebben we nu gezien hoe we met lemma 1.4.2 de $\lambda-1$ oplossingen $1 < \xi < p$ van de vergelijking $\xi^\lambda \equiv 1 \mod p$ kunnen koppelen aan (ideale) factoren van p. De vergelijking $\Phi(\xi) \equiv 0 \mod p$ is namelijk onafhankelijk van of er daadwerkelijk een $f(\alpha)$ bestaat zodat $p = N(f(\alpha))$. De $f(\alpha)$ kan ook een ideaal getal zijn. Kummer omschrijft het als het koppelen van een (ideale) factor β, aan elke oplossing ξ. Dan zeggen we dat $\beta \mid \Phi(\alpha)$, dan en slechts dan als $\Phi(\xi) \equiv 0 \mod p$. Wanneer nu $p = N(f(\alpha))$, dan volgt $\beta = f(\alpha)$, en is de factor β dus een echte (niet-ideale) factor. In feite worden zo de ideale factoren gedefinieerd door hun deelbaarheid. Dit is een creatieve en gewaagde oplossing. Zoals eerder besproken, zag Kummer zijn ideale factoren niet zo zeer als een abstracte uitvinding, maar eerder als de daadwerkelijke, bestaande structuur van de priemgetallen.

Een probleem met deze definitie is dat het nog niets zegt over de factorisatie van priemgetallen die *niet* voldoen aan $p = m\lambda + 1$, de noodzakelijke eis om $\lambda - 1$ factoren te krijgen. Verder is het niet mogelijk om iets te zeggen over de multipliciteit van een ideale factor β. Daarom noemt Kummer in *Zur Theorie der complexen Zahlen* een tweede definitie, die ik hier uiteen zal zetten. Deze definitie is vrij omstreden, aangezien het bewijs voor de onderliggende theorie nog niet klopte in 1847. Kummer rectificeerde dit pas in het in 1857 gepubliceerde artikel *Über die den Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln.*

Ik zal hier geen exact bewijs uiteenzetten, aangezien dit in de eerste instantie überhaupt geen correct bewijs was, maar wel het algemene idee schetsen zoals in [12, p. 326-327]. Kummer maakte in de tweede definitie gebruik van zijn ervaring met het geval dat $\lambda < 23$. Dan kon hij namelijk voor alle priemgetallen $q \neq \lambda$[11], waarvoor hij het probeerde, een cyclotomisch priemgetal $g(\alpha)$ vinden zodat $N(g(\alpha)) = q^f$ en $g(\alpha) = g(\alpha^q)$, waarbij f het kleinste getal is zodat $q^f \equiv 1 \mod \lambda$. De norm $N(g(\alpha))$ bestaat zoals altijd uit $\lambda - 1$ geconjungeerden. Ervan uitgaande dat zo'n $g(\alpha)$ bestaat, zien we dat geldt

$$g(\alpha^j) = g(\alpha^{jq}) = g(\alpha^{jq^2}) = \cdots = g(\alpha^{jq^{f-1}}).$$

Merk nu op dat $g(\alpha^{jq^f}) = g(\alpha^j)$ aangezien $q^f \equiv 1 \mod \lambda$ en $\alpha^\lambda = 1$. Dus de $\lambda - 1$ geconjungeerden in het product $N(g(\alpha))$ kunnen opgedeeld worden in verzamelingen van f geconjungeerden met dezelfde waarde. Neem $g_1(\alpha), g_2(\alpha), ..., g_e(\alpha)$ als alle geconjungeerde cyclotomische getallen in dit product die verschillende waarden hebben. De getallen $g_1(\alpha), g_2(\alpha), ..., g_e(\alpha)$ representeren dus ieder f getallen van dezelfde waarde. Dan geldt $(g_1(\alpha) \cdot g_2(\alpha) \cdots g_e(\alpha))^f = q^f$, en dus $e = \frac{\lambda-1}{f}$. Dus volgt dat $g_1(\alpha) \cdot g_2(\alpha) \cdots g_e(\alpha) = \pm q$: we hebben dus een factorisatie van q in e priemfactoren. In het algemene geval $\lambda \neq q$ verwachtte Kummer nu altijd op deze manier e *ideale* priemfactoren van q te vinden.

Kummer vond echter soms alleen $g(\alpha)$ met de eigenschap dat $N(g(\alpha)) = k^f q^f$ met f het kleinste getal zodat $q^f \equiv 1 \mod \lambda$, voor een bepaald geheel getal k. In dat geval kunnen we op dezelfde manier stellen dat $g_1(\alpha) \cdot g_2(\alpha) \cdots g_e(\alpha) = \pm kq$, en dus zou het wel eens zo kunnen zijn dat de e (ideale) factoren van q ieder precies een andere van de g_i delen. Vandaar de volgende definitie, waarbij $g(\alpha)$ is zoals hierboven.

Definitie 1.4.1. Neem $\Psi(\alpha) = g_2(\alpha)g_3(\alpha) \cdots g_e(\alpha)$, waarbij de g_i verschillende geconjungeerden van g aanduiden (dus ook: $(g_1(\alpha)\Psi(\alpha))^f = q^f$). Dan zeggen we dat *de ideale factor van q die hoort bij $g_1(\alpha)$*, $f(\alpha)$ k keer deelt wanneer $q^k \mid f(\alpha)\Psi(\alpha)^k$. [12, p. 327]

Het probleem met de definitie zit in het bewijs dat zo'n $g(\alpha)$ altijd bestaat, en dit bleef dus uit tot 1957. Als $g(\alpha)$ bestaat, geeft het e ideale factoren van q. Kummer geeft aan aan welke eigenschappen deze ideale factoren voldoen. Eerst zal ik hier een voorbeeld geven met een geval dat we eerder zagen, namelijk wanneer $\lambda = 23$, $p = 47$. Dit voorbeeld geeft Edwards in [12, p. 325]. We hadden eerder dat $N(1-\alpha+\alpha^{21}) = 47 \cdot 139$. We weten al dat 47 niet als norm geschreven kan worden, en dus niet in 22 factoren te ontbinden is. Nu

[11] Wanneer $q = \lambda$, is het probleem makkelijk oplosbaar, want dan kunnen we schrijven: $q = \lambda = N(1-\alpha) = (1-\alpha)(1-\alpha^2)\cdots(1-\alpha^{\lambda-1})$. Zie voetnoot pagina 13.

willen we bereiken dat we 47 toch in 22 *ideale* factoren kunnen ontbinden. Dan moet dus voor elk van de 22 geconjungeerden van $1-\alpha-\alpha^{21}$ gelden dat er een ideale factor van 47 bestaat die de geconjungeerde deelt. Hetzelfde geldt steeds ook voor een ideale factor van 139. Neem β de ideale factor van 47 die $1-\alpha-\alpha^{21}$ deelt. Nu kunnen we schrijven $\Psi(\alpha) = \frac{N(1-\alpha+\alpha^{21})}{1-\alpha+\alpha^{21}}$. Dan zien we dat voor een cyclotomisch getal $f(\alpha)$ geldt dat β $f(\alpha)$ k keer deelt wanneer het zo is dat $47^k \mid f(\alpha)\Psi(\alpha)^k$, zoals we ook zagen in de definitie.

Uit de definitie volgen nu de volgende noodzakelijke eigenschappen van ideale factoren, zoals Kummer ze geeft in [16, p. 206-207][12]:

1. Het product van twee of meer cyclotomische getallen heeft precies dezelfde ideale priemfactoren, als de factoren samengenomen.
2. Wanneer een cyclotomisch getal alle e priemfactoren van q bevat, dan is dat getal ook door q deelbaar; maar als het een van deze priemfactoren niet bevat, dan is het niet door q deelbaar.
3. Wanneer een cyclotomisch getal alle e ideale priemfactoren van q minstens k-maal bevat, is het door q^k deelbaar.
4. Wanneer $f(\alpha)$ precies m ideale priemfactoren van q bevat, het maakt niet uit of deze gelijk zijn of niet, dan bevat de norm $N(f(\alpha))$ precies de factor q^{mf}.
5. Elk cyclotomisch getal bevat slechts een eindig aantal ideale priemfactoren.
6. Twee cyclotomische getallen, die precies dezelfde ideale priemfactoren bevatten, zijn slechts door een complexe eenheid te onderscheiden.
7. Een cyclotomisch getal is door een ander deelbaar, wanneer alle ideale priemfactoren van de deler ook in de noemer staan; en het quotiënt bevat precies de ideale priemfactoren die overblijven in de noemer.

Daarom, zo zegt Kummer, voldoen de cyclotomische getallen na introductie van ideale factoren precies aan dezelfde regels als de gehele getallen en bijbehorende priemgetallen[13]. Kummer noemt verder twee priemfactoren equivalent, wanneer ze vermenigvuldigd met dezelfde ideale priemfactor, hetzelfde (werkelijke) cyclotomische getal geven. Dit is een equivalentierelatie, dus elke ideale factor behoort tot een bepaalde equivalentieklasse waarin de factoren dezelfde eigenschappen hebben onder vermenigvuldiging. De bovenstaande stellingen bewijst Kummer in zijn artikel [17]. De vraag die hem verder bezighoudt is: Welke ideale factoren brengen welke werkelijke factor voort? [16, p. 207]. Dit is een praktische vraag, die typerend is voor de analogie die Kummer geeft met atomen in de scheikunde. Vermenigvuldiging van ideale factoren is dan equivalent met de binding van twee atomen (bijvoorbeeld fluoratomen), die normaal gezien niet los van elkaar bestaan.

[12] Waar Kummer 'complexe getallen' gebruikt, zet ik 'cyclotomische getallen'.

[13] "Aus diesen Sätzen geht hervor, daß die Rechnung mit complexen Zahlen durch Einführung der idealen Primfactoren ganz dieselbe geworden ist, wie die Rechnung mit den ganzen Zahlen und den ganzzahligen realen Primfactoren derselben."[16, p. 207]

Hoofdstuk 2

Dedekind

2.1 Inleiding

Richard Dedekind (1831-1916) was een Duits wiskundige uit Braunschweig. Hij was een student van Gauss, die overigens ook uit Braunschweig kwam. De twee mannen waren studenten aan hetzelfde *Gymnasium* en *Collegium*, en gingen daarna allebei naar de universiteit van Göttingen [1]. Dedekind is ook in wiskundige zin een opvolger van Gauss: hij zette zijn werk voort door algebra toe te passen op getaltheorie.

Veel beroemde Duitse wiskundigen in de 19e en begin 20e eeuw studeerden of werkten aan de universiteit van Göttingen. Naast Gauss en Dedekind moeten Dirichlet, Riemann, en in latere jaren Hilbert en Noether genoemd worden. Göttingen was het centrum van wiskundig onderzoek totdat het nationaalsocialisme in Duitsland daar in 1933 een einde aan maakte. Joodse professoren werden ontslagen en veel wiskundigen, waaronder Emmy Noether, besloten Duitsland te verlaten voor bijvoorbeeld de Verenigde Staten [21, p. 464]. Emmy Noether is bekend als pionier in het gebied van de moderne algebra. Interessant is dat zij in haar lesgeven vaak verwees naar Dedekind; zo zei ze "Es steht alles schon bei Dedekind"[6, p. 64]. Dedekinds theorie geeft in feite een speciaal geval van Noethers algemene ringtheorie [20, p. 46-47].

Toen Dedekind in 1850 student werd in Göttingen, was de wiskundige gemeenschap daar nog volop in leven. Dedekind was als student bevriend met Riemann. Toen hij zelf docent werd, leerde hij Dirichlet goed kennen, die Gauss' positie in Göttingen overnam in 1855. Na Dirichlets dood, heeft Dedekind diens *Vorlesungen über Zahlentheorie* in 1863 uitgegeven met zijn eigen aantekeningen en opmerkingen hierbij. Dirichlets werk was klassieke getaltheorie. Hij hield zich bezig met kwadratische vormen en hiermee breidde hij eerder werk van Gauss uit. Een van zijn belangrijkste ontdekkingen is een formule voor het klassengetal; dit geeft het aantal niet equivalente kwadratische vormen die dezelfde determinant hebben [21, p. 460]. Dirichlet en Kummer waren overigens ook goed bekend met elkaar. Kummer was getrouwd met een nicht van de vrouw van Dirichlet [2]. De twee wiskundigen waren op de hoogte van en hadden invloed op elkaars werk [2]. Dedekind heeft meerdere versies uitgegeven van Dirichlets werk (in 1871, 1879 en 1894), met steeds meer extra aantekeningen. Uiteindelijk was het bijna meer Dedekinds werk dan Dirichets [12, p. 351]. Zo introduceerde Dedekind in de versie van 1871 het begrip 'ideaal' en in latere versies veel Galoistheorie [21, p. 460]. Dit begrip 'ideaal' was gebaseerd op Kummers ideale factoren. Het is ook precies het ideaal zoals bekend uit de moderne algebra; dit zal ik in paragraaf 2.3 verder toelichten.

Dedekinds introductie van het ideaal had als doel om Kummers theorie te algemeniseren. Dit betekent dat hij de cyclotomische getallen inwisselde voor een domein van gehele algebraïsche getallen. Als θ een algebraïsch geheel getal is, houdt dit in dat θ voldoet aan een vergelijking

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_2\theta^2 + +a_1\theta + a_0 = 0$$

voor $a_{n-1}, \ldots, a_1, a_0$ gehele getallen. De complexe gehelen van Gauss en de cyclotomische getallen van Kummer zijn voorbeelden van algebraïsche getallen. Bij de complexe getallen hebben we namelijk $\theta = \sqrt{-1}$ en dus $\theta^2 + 1 = 0$ en bij de cyclotomische getallen met eenheidswortel van graad n, $\theta^n - 1 = 0$. Dedekind wilde nu voor algebraïsche getallen in het algemeen unieke priemfactorisatie herstellen.

Er is een belangrijk verschil tussen Kummer en Dedekind dat in dit hoofdstuk naar voren zal komen. Dedekinds stijl is meer conceptueel, terwijl Kummer een meer algoritmische stijl heeft. In het voorgaande hoofdstuk hebben we gezien dat Kummers methode sterk computationeel was. Zo is het sprekend dat hij voor alle priemgetallen $p < 1000$, met $p = m\lambda + 1$ zoals eerder, wanneer mogelijk het cyclotomische getal vond met norm gelijk aan p. Kummer introduceerde weinig nieuwe concepten; zijn 'ideale factoren' zijn een uitzondering. Deze manier van werken behoort tot de oude stijl. Deze technische, algoritmische stijl staat tegenover de tegenwoordige abstractere stijl. In moderne wiskunde zitten de algoritmes verstopt in concepten. Dedekind was een van de eerste aanhangers van deze abstracte stijl [6, p. 66]. Hij was echter iets te modern voor zijn tijd; de nieuwe stijl bloeit pas op in de 20e eeuw [6, p. 66][20, p. 46]. In de 20e eeuw wilden wiskundigen minder algoritmisch te werk te gaan, en in plaats daarvan met nieuwe concepten de theorie in een klap te bevatten en overzichtelijk te maken [6, p. 67]. Dedekind introduceert veel nieuwe concepten, die in de moderne algebra een belangrijke rol blijven spelen. De begrippen 'lichaam', 'ideaal' en 'moduul', zoals we die tegenwoordig kennen, stammen van Dedekind [6, p. 67-68]. Voor een moderne lezer is Dedekind toegankelijk, maar destijds was zijn conceptuele methode niet algemeen gangbaar. Dedekinds ideaaltheorie kreeg mogelijk daarom in eerste instantie weinig aandacht van medewiskundigen.

Een andere mogelijke reden dat Dedekinds werk niet alom geprezen werd, was zijn omgang met oneindige verzamelingen. In de 19e eeuw was het begrip oneindig en zeker het werken met oneindige verzamelingen niet alom geaccepteerd [1][20, p. 44]. Dedekind heeft er in zijn ideaaltheorie geen enkele moeite mee. Eerder al had hij de irrationale getallen geformaliseerd met Dedekindsnedes. Ook dat werd in de wiskundige gemeenschap destijds niet altijd goed ontvangen [6, p. 75]. Dedekind was gemotiveerd om een fundamentele onderbouwing te geven voor bepaalde elementaire bouwstenen van de analyse, zoals de reële getallen. Dedekind was niet de enige, ook zijn tijdgenoten Weierstrass en Cantor hadden hetzelfde doel [6, p. 69-70]. Toch werd Dedekinds fundamentele aanpak niet altijd gewaardeerd. Niet iedereen was overtuigd van het nut van zijn werk. Men vroeg zich af wat het toevoegt, òf het wel iets toevoegt (staat dit alles niet al beschreven in 'De Elementen' van Euclides?); en of het überhaupt nog wiskunde genoemd moet worden. Bijvoorbeeld Lipschitz was het oneens met Dedekinds filosofie over de reële getallen, zie [6, p. 75] voor details. Dedekinds werk sloeg dus in de algemene wiskundige gemeenschap niet goed aan, en werd vooral door bepaalde logici, zoals Schröder, gewaardeerd [6, p. 67]. Dedekind had moeite met het in bekendheid brengen van zijn ideaaltheorie. Dit kan dus liggen aan zijn aanpak, maar mogelijk lag het ook aan de plaats waar hij het werk publiceerde. Lipschitz vond Dedekinds ideaaltheorie, in tegenstelling tot zijn werk aan de reële getallen, wel van 'zeldzame waarde' [20, p. 44], en drong hem aan om het in het Frans uit te brengen om een breder publiek te bereiken [20, p. 44]. Hierop antwoordde Dedekind:

> Uw brief heeft me grote en onverwachte vreugde gebracht, aangezien ik al jaren de hoop had opgegeven om iemand te interesseren met mijn ideaaltheorie. [20, p. 45]

Zo kwam Dedekinds 'Sur la Théorie des Nombres Entiers Algébrique' tot stand. Dit werkt komt in paragraaf 2.2 uitgebreid ter sprake.

Dedekind heeft een tegenhanger en concurrent van de oude stijl: namelijk Kronecker [20, p. 46]. In 1882 kwam deze student van Kummer met zijn eigen theorie die Kummers werk algemeniseerde naar algebraïsche getallen. Kronecker zoekt ook een vervanging voor Kummers ideale factoren, maar volgt nauwer Kummers algoritmische stijl. Kronecker is, in tegenstelling tot Dedekind, een constructieve wiskundige. Hij herstelt unieke factorisatie door een nieuw domein te construeren door (werkelijke) getallen toe te voegen wanneer nodig [5, p. 497]. Ook was Kronecker tegen het gebruik van het begrip 'oneindig'. De manier waarop Dedekind oneindige verzamelingen ziet als wiskundige objecten (zoals idealen), zou Kronecker niet accepteren. Kronecker heeft zelfs gezegd niet te geloven in irrationale getallen [20, p. 46]. Dit terwijl Dedekind juist de irrationalen had geformaliseerd met zijn Dedekindsnedes. De twee mannen kunnen duidelijk niet verder

uit elkaar liggen. Kroneckers werk was sterk algoritmisch en daardoor technisch vrij ingewikkeld. Net zoals Dedekinds werk, sloeg Kroneckers werk niet aan bij de wiskundige gemeenschap, hoewel om andere redenen [20, p. 46].

In dit hoofdstuk zal ik in paragraaf 2.2 bespreken hoe en waarom Dedekind het begrip 'ideaal' introduceert. Hierbij zal ik eerst Dedekind nauw volgen in paragraaf 2.2.1. We zullen zien hoe Dedekind vanuit de ideale factoren komt tot het nieuwe concept van ideaal. Daarna zal ik dieper ingaan op een aantal zaken. Ten eerste zal ik Dedekinds eerdere poging om zonder idealen Kummers theorie te algemeniseren toelichten in 2.2.2. Daarna zal ik een verdere analyse geven van Dedekinds tekst in paragraaf 2.2.3. Ik zal bespreken waar we concreet het verschil in stijl en filosofie tussen Dedekind en Kummer terug zien. Ook zullen we bestuderen wat Dedekind expliciet heeft gezegd over Kummer. Zo krijgen we een goed beeld van Dedekinds opvattingen over Kummer. Tot slot zal ik in paragraaf 2.3 toelichten hoe Dedekind zich verhoudt tot de moderne algebra.

2.2 Dedekinds idealen

Dedekind geeft in 'Sur la Théorie des Nombres Entiers Algébriques'[7] (1877) een toegankelijke introductie tot zijn theorie over de algebraïsche getallen. Ook noemt Dedekind in dit werk Kummer als zijn inspiratie voor de idealen. Hij legt uit hoe Kummers ideale factoren hem op het idee van idealen brachten. Ik zal nu eerst Dedekinds introductie van de idealen zoals in [8, p. 53-61] schetsen. Daarna volgen meer details en een analyse van deze tekst, met nadruk op het contrast met Kummer.

2.2.1 Definitie en motivatie

Dedekind begint met een kleine geschiedenis van de deelbaarheid van getallen. Die geschiedenis begint bij Euclides, die bewijst dat, in de gehele getallen, elk priemgetal dat een product ab deelt, ook a of b moet delen. Een direct gevolg hiervan is dat de gehele getallen unieke priemfactorisatie toelaten. De uitbreiding van de gehele getallen naar complexe gehelen wordt 2000 jaar later pas gegeven door Gauss. Dedekind wil nu de meest algemene uitbreiding geven. Hiervoor bekijkt hij algebraïsche getallen θ. Zoals vermeld is in de inleiding voldoen deze getallen aan een vergelijking

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_2\theta^2 + a_1\theta + a_0 = 0$$

waar iedere a_i met $i \in \{0, 1, \ldots, n-1\}$ een rationaal getal is. Wanneer elke a_i geheel is, noemt Dedekind θ een geheel (algebraïsch) getal. Een geheel algebraïsch getal is dus de wortel van een monisch polynoom met gehele coëfficiënten. De verzameling van alle gehele algebraïsche getallen is gesloten onder optelling, aftrekking en vermenigvuldiging. In het vervolg zal ik, net als Dedekind, in plaats van 'geheel algebraïsch getal', simpelweg 'geheel getal' schrijven. Dan volgen de benodigde definities van deelbaarheid, eenheden en priemgetallen:

- Een geheel getal β deelt α, wanneer er een geheel getal γ bestaat zodat $\alpha = \beta\gamma$.
- Een geheel getal ϵ is een eenheid, wanneer ϵ elk geheel getal α deelt.
- Een geheel getal α is een priemgetal, wanneer de enige delers van α eenheden zijn of van de vorm $\epsilon\alpha$ zijn, voor ϵ een eenheid.

Hier wil ik toelichten dat de definitie die Dedekind geeft voor een eenheid equivalent is aan de eerder gegeven definitie in paragraaf 1.1. Die definitie was dat een eenheid een getal is met een inverse. Als we Dedekinds definitie aanhouden, volgt dat een eenheid ϵ elk getal deelt, dus ook het getal 1 (dit is inderdaad een algebraïsch geheel getal). Dan bestaat er dus een geheel (algebraïsch) getal ϵ^{-1} zodat $\epsilon\epsilon^{-1} = 1$. Daarmee is ϵ een eenheid volgens onze definitie. Andersom volgt met onze definitie dat ϵ een inverse ϵ^{-1} heeft, dus

$\epsilon\epsilon^{-1} = 1$. Er geldt altijd $1 \mid \alpha$, dus $\epsilon\epsilon^{-1} \mid \alpha$ en $\epsilon \mid \alpha$ voor een willekeurig geheel getal α. Dit is precies Dedekinds definitie.

Dedekind stelt na het geven van deze definities dat er in het domein van alle algebraïsche, gehele getallen geen priemgetallen voorkomen.[1] De gehele (algebraïsche) getallen hebben dus niet de gewenste eigenschappen van de gehele getallen en Gauss' complexe gehelen. Dedekind vermeldt nu dat hij, door het *domein* in te perken, priemgetallen weer betekenis kan geven. Dit doet hij als volgt. Neem θ een algebraïsch (niet per se geheel) getal. Dan is er een polynoom met minimale graad zodat θ een wortel is. Oftewel

$$\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

voor minimale graad n. Deze polynoom noemt Dedekind *irreducibel*. Dan neemt hij als het domein getallen van de vorm

$$\phi(\theta) = x_{n-1}\theta^{n-1} + \cdots + x_2\theta^2 + x_1\theta + x_0$$

voor $x_{n-1}, \ldots, x_1, x_0 \in \mathbb{Q}$. In moderne notatie is dit dus $\mathbb{Q}(\theta)$. Dedekind noemt de verzameling van deze getallen Ω, een eindig lichaam van graad n. De elementen van Ω zijn ook algebraïsche getallen, en Ω is gesloten onder vermenigvuldiging, optelling en aftrekking. De deelverzameling van Ω waarin alle $\phi(\theta)$ gehelen zijn, oftewel de wortel van een monisch polynoom met gehele coëfficiënten, noemt Dedekind o. Het punt is nu dat o wel priemgetallen toelaat. Dit laat Dedekind zien door als volgt een norm te introduceren op een geheel algebraïsch getal $\phi(\theta)$:

$$N(\phi(\theta)) = \phi(\theta)\phi(\theta_1)\phi(\theta_2)\ldots\phi(\theta_{n-1})$$

Hier geven $\theta_1, \theta_2, \ldots, \theta_{n-1}$ de andere $n-1$ wortels naast θ van de gegeven irreducibele polynoom van graad n. Dit is precies de norm die Kummer introduceert in paragraaf 1.2. Dedekind benoemt ook de eigenschappen van deze norm. Voor $\phi(\theta)$ een geheel algebraïsch getal, volgt dat $N(\phi(\theta))$ een geheel getal is. Ook geldt $N(\alpha\beta) = N(\alpha)N(\beta)$ voor $\alpha, \beta \in \Omega$. Verder hebben we $N(\phi(\theta)) = \pm 1$ dan en slechts dan als $\phi(\theta)$ een eenheid is. De norm op gehele algebraïsche getallen geeft dus een multiplicatieve functie naar de gehele getallen $\mathbb{Z}$. Aangezien de gehele getallen priemfactorisatie toelaten, volgt met de gegeven eigenschappen dus dat ook elk getal in o eindig factoriseerbaar is op eenheden na.

Het probleem is dat de eindige factorisaties van irreducibele getallen in o niet per se uniek zijn. Nu noemt Dedekind voor het eerst Kummer: die liet dit al zien voor de cyclotomische getallen. Cyclotomische getallen zijn dus precies getallen in het domein o met als algebraïsch getal θ met een vergelijking $\theta^m - 1 = 0$. Een cyclotomisch getal kan op verschillende manieren ontbonden worden in irreducibele factoren. Dit hebben we expliciet gezien aan het eind van hoofdstuk 1.1. Equivalent is dat het mogelijk is dat een irreducibel getal dat een product ab deelt, zowel a als b niet deelt (en dus niet priem is, zie definities 1.1.1 en 1.1.2). Dedekind prijst Kummer, 'die meetkundige' [8, p. 56], voor de uitvinding van de ideale factoren, die alle moeilijkheden oplossen. Met de introductie van ideale factoren voldoen de complexe getallen uit Kummers domein precies aan de regels in het domein van de gehele getallen. Dedekind wil Kummers optimisme voortzetten naar zijn domeinen o van algemene gehele algebraïsche getallen.

Dedekind legt daarop uit waarom hij Kummers ideale getallen inruilt voor zijn idealen. Dedekind noemt dat hij eerder zonder succes geprobeerd had Kummers theorie uit te breiden met behulp van congruenties. Hij licht dit toe in een volgend hoofdstuk. Hier zal ik in paragraaf 2.2.2 uitgebreider op ingaan. Samenvattend was het probleem dat de theorie te ingewikkeld werd. Daarom vond hij een nieuwe, 'fundamenteel envoudigere methode, direct gericht op het doel' [8, p. 57]. Deze methode gebruikte het nieuwe concept idealen, waarvan 'de kracht [...] ligt in de extreme eenvoudigheid' [8, p. 57].

Dedekind beschrijft nu wat volgens hem het probleem is met Kummers definitie van ideale factoren. Ze zijn niet vanuit zichzelf gedefinieerd, maar vanuit hun deelbaarheid. Die deelbaarheid lijkt analoog aan

[1] Dit kunnen we als volgt zien. Een algebraïsch geheel getal θ is altijd te schrijven als $\theta = \sqrt{\theta}\sqrt{\theta}$. Hier is $\sqrt{\theta}$ ook een algebraïsch geheel getal (het voldoet namelijk aan de algebraïsche vergelijking, waarvan θ de wortel is, wanneer we $\theta \to \theta^2$ substitueren.

deelbaarheid van gehele getallen, terwijl ideale factoren niet noodzakelijkerwijs de eigenschappen van gehele getallen hebben. Het gevaar is, zo zegt Dedekind, dat dit leidt tot voorbarige conclusies en incomplete bewijzen. Daarnaast bestaan ideale getallen niet binnen het domein o. Dus is een precieze definitie van het concept en de bijbehorende vermenigvuldiging noodzakelijk.

Dedekind zegt nu dat, aangezien de definitie van een ideaal getal draait om de deelbaarheidseigenschap, het hem natuurlijk leek om te kijken naar de verzameling van alle getallen binnen het domein o die deelbaar zijn door één bepaald ideaal getal. Deze verzameling noemt hij een ideaal. Elk ideaal getal brengt dus een ideaal voort. Ik zal hier de notatie (α) gebruiken voor het ideaal dat voortgebracht wordt door het ideale getal α. Dedekind noemt dat werkelijke getallen opgevat moeten worden als een speciaal geval van ideale getallen. Dan noemt hij (a) voor a een werkelijk getal, een *hoofdideaal*. Dit hoofdideaal bevat dus alle getallen die een veelvoud van a zijn binnen het domein o, oftewel alle getallen ωa voor $\omega \in o$.

In voorbereiding op de fundamentele eigenschap van een ideaal, geeft Dedekind de volgende twee eigenschappen[8, p. 59] van gehele (algebraïsche) getallen:

1. Als twee gehele getallen $\alpha = \mu\omega, \alpha' = \mu\omega'$ deelbaar zijn door μ, dan is hun som $\alpha + \alpha' = \mu(\omega + \omega')$ en hun verschil $\alpha - \alpha' = \mu(\omega - \omega')$ ook deelbaar door μ, aangezien de som $\omega + \omega'$ en het verschil $\omega - \omega'$ zelf gehele getallen zijn.

2. Als $\alpha = \mu\omega$ deelbaar is door μ, dan is elk getal $\alpha\omega' = \mu(\omega\omega')$ dat deelbaar is door α, ook deelbaar door μ, aangezien het product $\omega\omega'$ van de gehele getallen ω, ω', zelf een geheel getal is.

Kijk hierbij terug naar de definitie van deelbaarheid zoals gegeven op pagina 24: het is van belang dat $\omega+\omega'$, $\omega - \omega'$ en $\omega\omega'$ gehele (algebraïsche) getallen zijn. Voor een hoofdideaal (μ) (een ideaal van een werkelijk algebraïsch geheel getal μ) in het domein o volgen dus gelijk de volgende eigenschappen [8, p. 59]:

a) De som en het verschil van twee getallen in (μ) zijn altijd ook getallen in (μ).

b) Het product van een getal in (μ) met een getal in het domein o is een getal in (μ)

Nu wil Dedekind dit algemeniseren naar elk ideaal (α). Voor een ideaal getal α zijn de bovenstaande eigenschappen 1 en 2 zeker wenselijk, om de analogie met factorisatie van gehele getallen te behouden. De deelbaarheid van ideale getallen moet dus in ieder geval zo gedefinieerd zijn, dat deze eigenschappen gelden. Dan volgt dat a en b ook gelden voor alle idealen. Nu zegt Dedekind dat hij na veel moeite ook het omgekeerde bewezen heeft, namelijk dat een verzameling in o die voldoet aan de eigenschappen a en b een ideaal is. Dit betekent dat een verzameling die voldoet aan deze eigenschappen a en b, precies de verzameling is van alle getallen in o die deelbaar zijn door een bepaald werkelijk of ideaal getal. Dit betekent dat de eigenschappen a en b zowel noodzakelijk als voldoende zijn voor de definitie van een ideaal. En het begrip 'ideaal getal' komt er niet eens in voor! Het is dan ook vanaf nu niet meer noodzakelijk voor Dedekind om het over ideale getallen te hebben. Het is niet langer nodig om idealen die geen hoofdideaal zijn, te zien als voortgebracht door een ideaal getal.

We zien hier heel expliciet waar Dedekinds manier van wiskunde doen om draait. Wat hij hier doet, is de essentie van de theorie bevatten in een goede definitie. Kummer gaf een directe definitie vanuit deelbaarheid. Dit was voor hem waarschijnlijk de meest natuurlijke. Daarom is hij wel beperkt tot de tekortkomingen van deze definitie. Dedekind isoleert de karakteristieke eigenschappen van een ideaal. De te wensen deelbaarheidseigenschappen van ideale factoren zitten op deze manier verstopt in de definitie. Het kost Dedekind moeite om aan te tonen dat een verzameling die voldoet aan de eigenschappen a en b, ook echt een ideaal is, oftewel voortgebracht wordt door een (ideaal) getal. Hiermee heeft hij wel de essentie van de theorie gevonden, en daarmee voorkomt hij toekomstig algoritmisch werk.

Overigens gebruikt Dedekind de notatie $\mathbf{a}$ voor een ideaal in plaats van (a). Mijn notatie maakt in feite gebruik van het bestaan van een ideale factor a. In het vervolg gebruik ik beide notaties voor een ideaal, wanneer nuttig.

In de rest van het hoofdstuk behandelt Dedekind wat het nut is van idealen voor het vraagstuk van unieke

factorisatie. Hiervoor moet hij eerst deelbaarheid onder idealen behandelen. Dedekind noemt een ideaal (a) deelbaar door (b), oftewel (b) deelt (a), wanneer $(a) \subset (b)$. Deze definitie komt van het feit dat dan (b) een deler is van (a), dan en slechts dan als $b \mid a$. (Het ideale getal b is een deler van a, wanneer (b) een deler is van (a).) Dan definieert Dedekind een priemideaal, als een ideaal verschillend van o dat alleen o en zichzelf als delers heeft. (Een ideaal priemgetal hoort dan bij een bepaald priemideaal.)

Dedekinds definitie van het product van twee idealen $\mathbf{a}, \mathbf{b}$ is dan de (gebruikelijke) verzameling van alle mogelijke sommen van alle mogelijke producten ab voor alle $a \in \mathbf{a}$ en $b \in \mathbf{b}$. (Het ideale getal horend bij $\mathbf{ab}$ is het product van de ideale getallen die horen bij $\mathbf{a}$ en $\mathbf{b}$.)

Dedekind geeft nu twee stellingen, die hij in het vervolg van 'Sur la Théorie des Nombres Entiers Algébriques' bewijst. Deze zijn:

- Als een ideaal $\mathbf{c}$ deelbaar is door een ideaal $\mathbf{a}$, dan is er een uniek ideaal $\mathbf{b}$ zodat $\mathbf{ab} = \mathbf{c}$.

- Elk ideaal, dat niet gelijk aan o is, is of een priemideaal, of uniek te schrijven als product van priemidealen.

Met deze stellingen bereikt Dedekind de unieke priemfactorisatie in het domein o voor idealen. Natuurlijk kost het hem heel wat werk om deze stellingen te bewijzen. De stellingen en definities zelf lijken echter heel eenvoudig en maken een groot deel van de theorie duidelijk. Dat de stellingen zo eenvoudig zijn, heeft natuurlijk alles te maken met de keuze voor de definities. Het begrip geheel algebraïsch getal is precies gekozen zodat dit geldt. De stellingen zijn ook eenvoudiger te bewijzen met de nieuwe, duidelijke definitie voor een ideaal. Zo zal het erg helpen dat elk element in een ideaal, daadwerkelijk in het domein ligt.

2.2.2 Over ideale factoren in $\mathbb{Z}[\sqrt{-5}]$

We hebben gezien dat Dedekind gezegd had in eerste instantie geprobeerd te hebben Kummers theorie op een andere manier te algemeniseren. Dedekind analyseerde de eigenschappen van ideale factoren met behulp van congruenties. Aan het eind van paragraaf 1.1 kwam een voorbeeld ter sprake van een factorisatie in $\mathbb{Z}[\sqrt{-5}]$. In een voetnoot (zie pagina 7) volgde, waarom het getal 2 in $\mathbb{Z}[\sqrt{-5}]$ zich in feite gedraagt als een kwadraat. Daarom is 2 in $\mathbb{Z}[\sqrt{-5}]$ te schrijven als een kwadraat van een ideale factor. Deze analyse kwam van Dedekind. Een zelfde soort analyse heeft hij voor andere getallen in $\mathbb{Z}[\sqrt{-5}]$ uitgevoerd. Deze volledige analyse is te vinden in [8, p. 89-94]. Zo zijn uiteindelijk alle getallen in het domein geclassificeerd met hun ontbinding in ideale factoren. Dit leidt tot conclusies als 'elk positieve, rationale priemgetal $\equiv 1, 9 \mod 20$ kan geschreven worden als twee verschillende factoren, die echt bestaan en zich gedragen als priemgetallen' en de conclusie die we eerder zagen; 'het getal 2 gedraagt zich als een kwadraat van een ideaal priemgetal α.'

Dedekind concludeerde dat het inderdaad mogelijk was om rigoreus te laten zien dat de ideale getallen de gewenste eigenschappen hebben (namelijk, dat ze zich gedragen zoals gehele getallen). Echter was de methode vrij intensief en zou het nog ingewikkelder worden voor andere domeinen [8, p. 94]. Het grootste probleem was dat elke product van ideale of werkelijke getallen tot in detail geanalyseerd moest worden. Daarnaast lag het gevaar op de loer om te snel conclusies te trekken, omdat het bijvoorbeeld niet echt voor de hand ligt dat 2 zich als een kwadraat gedraagt. Dit gaat dus precies in tegen Dedekinds filosofie die was gebaseerd op het zo eenvoudig mogelijk vastleggen van de theorie. Op deze manier moest hij alles precies uitwerken. Daarom besloot Dedekind dat de theorie eenvoudiger moest kunnen: idealen waren de uitkomst.

2.2.3 Dedekind over Kummer

Die meetkundige?

Dedekind noemt Kummer 'ce géomètre' [7, p. 267], *die meetkundige*. Dit lijkt tegenstrijdig aangezien Kummers werk voornamelijk getaltheoretisch is. Daarnaast is nu Kummers uitvinding van ideale factoren, als *getallen* of in ieder geval als onderdeel van getallen, relevant. Waarom noemt Dedekind Kummer dan een meetkundige? Mogelijk was dit simpelweg nog de gebruikelijke aanspreekvorm voor wiskundige in het Frans. Het kan ook opgevat worden als een verwijzing naar Kummers werk in de cirkeldeling. Het is echter ook mogelijk dit te interpreteren als een aanwijzing dat Dedekind zichzelf als een ander soort wiskundige beschouwt dan Kummer. In de inleiding van dit hoofdstuk is al de tegenstelling van Dedekinds conceptuele en Kummers algoritmische stijl besproken. Kummer presenteert zijn ideale factoren als onderliggende structuur van getallen. Zo maakt Kummers analogie met scheikunde duidelijk dat hij de ideale factoren als de werkelijke, onderliggende structuur van getallen zag. Voor Dedekind draait het echter niet meer om eigenschappen van getallen, maar wetten in domeinen [5, p. 494]. Daarom is Kummer vanuit Dedekinds oogpunt vergelijkbaar met meetkundigen, die eigenschappen van meetkundige objecten bestuderen [5, p. 494]. Inderdaad maakte Kummers naast de analogie met scheikunde ook gebruik van meetkundige analogieën [5, p. 494]. Daar komt bij dat Dedekind de meetkundige introductie van irrationalen van Euclides geformaliseerd had met een algebraïsch analytische aanpak. In zekere zin doet Dedekind nu iets vergelijkbaars met Kummers ideale factoren: hij maakt van die ideale factoren iets wat beter bij zijn eigen filosofie past.

Bezwaar tegen Kummers definitie en computationele methodes

Het probleem met Kummers definitie, vanuit Dedekinds filosofie, is dat de ideale factoren gedefinieerd zijn vanuit de eigenschap van hun deelbaarheid (zie paragraaf 1.4). Hierin ligt het gevaar van de stilsluipende aanname van eigenschappen van de gehele getallen op ideale factoren. De ideale factoren, als elementen buiten het domein o, hebben volgens Dedekind een precieze definitie van deze factoren zelf en hun vermenigvuldiging hard nodig. Dedekind noemt hier zijn formalisatie van de irrationale getallen als voorbeeld van de noodzaak van het precies definiëren van getallen en hun vermenigvuldiging. Hier zien we duidelijk dat Dedekind de nadruk legt op wat geldt binnen een domein, in plaats van wat de eigenschap is van een getal. De focus van Kummer op eigenschappen van getallen, in plaats van domeinen, verklaart waarom het voor hem geen punt was dat de ideale getallen niet tot het domein van de cyclotomische getallen behoren [5, p. 494-495]. Bovendien lijkt dat niet van belang voor de toepassingen waarin Kummer geïnteresseerd was. Het is ook opvallend dat Kroneckers oplossing lag in het toevoegen van *werkelijke* elementen *buiten het domein* om unieke factorisatie te herstellen [8, p. 94-95][5, p. 497]. Dit is een uitbreiding volgens de methode van Galois. Voor Dedekind was dit echter niet bevredigend, met name vanwege de toevoeging van elementen buiten het domein. Ook zal Kroneckers meer algoritmische aanpak voor Dedekind niet wenselijk geweest zijn. Het verschil in stijl tussen Dedekind en Kummer is echter natuurlijk niet compleet zwart-wit. Dedekind werkt in [7] ook voorbeelden uit en gaat daarbij computationeel te werk. Het grote verschil met Kummer is, dat Dedekind dit zo veel mogelijk probeert te voorkomen. Hij spreekt zich er zelfs sterk tegen uit. In eerste instantie werkt Dedekind zijn ideaaltheorie op computationele wijze uit in het domein $\mathbb{Z}[\sqrt{-5}]$. Andere domeinen zullen vaak op dezelfde manier te behandelen zijn. Dedekind schrijft echter niet van plan te zijn om deze berekeningen voor andere domeinen uit te werken, aangezien deze manier van werken niet zijn voorkeur heeft. In Dedekinds woorden:

> Het verdient de voorkeur om, net zoals in de moderne functietheorie, bewijzen te geven gebaseerd op fundamentele eigenschappen, in plaats van berekeningen, en om de theorie zo op te bouwen dat die de resultaten van berekeningen kan voorspellen. [8, p. 102]

Dedekinds bezwaren tegen computationele methodes maken duidelijk dat hij tot de nieuwe school (zoals beschreven in de inleiding) behoort. Dit zien we ook terug in Dedekinds introductie van de ideaal. Hij

isoleert daar de belangrijkste eigenschappen van een ideaal, de kern van de deelbaarheidseigenschappen, en laat zien dat dit voldoende is voor de definitie. Dit blijkt inderdaad de theorie sterk te vereenvoudigen.

2.3 Dedekind nu

Idealen zijn nog altijd belangrijk in de ringtheorie. De definitie van ideaal gegeven door Dedekind is in essentie precies die zoals we hem nu kennen in moderne algebra. De moderne definitie zegt dat een verzameling van elementen I uit een ring R een ideaal is, wanneer $x-y \in I$ voor alle $x, y \in I$, oftewel, I is een ondergroep van R, en $rx \in I$ voor alle $r \in R$ en $x \in I$. Dit zijn precies de eigenschappen die Dedekind ook noemt. Dedekind heeft het niet over een algebraïsche structuur als een groep of een ring in het algemeen. Hij gebruikt wel het begrip *moduul* om een verzameling aan te duiden die gesloten is onder vermenigvuldiging en optelling. De eerste eigenschap van Dedekinds ideaal (zoals gegeven in 2.2.1), was dat het ideaal gesloten was onder optelling en aftrekking. Hieruit volgt dus dat een ideaal ook een moduul is [8, p. 119]. In dit geval is de moduul ook een deelverzameling van een ring, namelijk de ring $o \subset \mathbb{Q}(\theta)$. Zo zien we dus dat Dedekinds definitie equivalent is aan idealen in de ring o in moderne zin. Ook interessant is Dedekinds definitie voor een hoofdideaal. Een hoofdideaal is ook in de moderne definitie een ideaal voortgebracht door één element uit de ring. Met Kummers theorie en Dedekinds definitie kunnen we elk ideaal dat geen hoofdideaal is, en dat dus niet door slechts één getal uit de ring voortgebracht wordt, zien als een ideaal behorend bij een ideale factor (oftewel een element buiten de ring).

Tegenwoordig noemen we een een ring waarin elk ideaal (die niet nul of de hele ring is) te ontbinden is in priemidealen, een *Dedekind domein*. Noem α een algebraïsch getal. Dan wordt in het algemeen ook de term 'ring van gehele getallen' van $\mathbb{Q}[\alpha]$ gebruikt om de verzameling aan te duiden van alle getallen uit $\mathbb{Q}[\alpha]$ die een wortel zijn van een monisch polynoom met als coëfficiënten gehele getallen: oftewel het domein o van Dedekind. Dedekind heeft dus bewezen dat zo'n ring van gehele getallen altijd een Dedekind domein is.

Ook zien we dat Dedekinds definitie voor een priemideaal precies is wat we tegenwoordig een maximaal ideaal noemen. In een Dedekind domein geldt ook dat elk priemideaal maximaal is. In normale ringen (die commutatief met 1 zijn) geldt sowieso altijd dat elk maximaal ideaal priem is. Het maakt dus voor Dedekind niet uit of hij de definitie van een maximaal of priemideaal gebruikt.

Dedekind laat ook zien dat wanneer je een kleiner domein kiest dan de hele verzameling o, dit niet meer vanzelfsprekend een Dedekind domein is. Zo noemt hij dat in de moduul $[1, \sqrt{-3}]$, wat in moderne notatie $\mathbb{Z}[\sqrt{-3}]$ is, geen unieke priemfactorisatie van idealen geldt [8, p. 127]. In feite had Kummer geluk dat $\mathbb{Z}[\alpha]$, voor α een cyclotomisch getal, de ring van gehele getallen van $\mathbb{Q}(\alpha)$ was, aangezien het nu duidelijk is dat hier heel zijn theorie op berust [20, p. 40].

Hier moet vermeld worden dat, hoe dicht Dedekind ook bij de moderne algebra komt, hij nog niet zo ver was. De moderne algebra pas begint bij Noether. Dedekind bekijkt idealen in de verzameling van de gehele getallen in $\mathbb{Q}(\theta)$. Hij noemt dat deze verzameling gesloten is onder optelling, aftrekking en vermenigvuldiging. Echter algemeniseert hij dit niet naar een abstract concept zoals een ring, waarin zijn idealen ook betekenis zouden hebben. Hij doet ook geen poging om de coëfficiënten van de elementen uit Ω, die liggen in het lichaam $\mathbb{Q}$, te vervangen door elementen uit een algemeen abstract lichaam. Wel gebruikt hij 'lichaam' als aanduiding voor Ω (wat in moderne zin ook een lichaam is). Dedekinds voornaamste doel was het herstellen van unieke factorisatie voor bepaalde gehele getallen in $\mathbb{Q}[\theta]$. Dit was hem gelukt zover mogelijk, en maakte de theorie en toepassingen een stuk eenvoudiger.

Conclusie

In mijn scriptie zijn allerlei verbanden tussen Kummer en Dedekind naar voren gekomen. We hebben in detail gezien dat de oorsprong van Dedekinds idealen lag in Kummers introductie van de ideale factoren. Deze geschiedenis heb ik besproken tot Kummers reden voor het introduceren van de ideale getallen. Ook hebben we hebben gezien hoe verschillend van stijl en werkwijze de twee mannen waren. Kummers aanpak was in zekere zin meer 19e eeuws, terwijl Dedekinds methode meer 20e eeuws lijkt. Kummer werkte meer algoritmisch en computationeel, terwijl Dedekind meer abstract te werk ging. Bij Dedekind ligt de nadruk op het vinden van de essentie van een theorie. Op die manier worden berekeningen zo veel mogelijk overbodig gemaakt. Tegelijkertijd was Dedekinds werk in eerste instantie een generalisatie van Kummers werk. We hebben gezien hoe Dedekind de ideale getallen binnen zijn eigen filosofie herdefinieerde. Zo maakte hij de ideale getallen, nu idealen, klaar voor een toekomst in de ringtheorie van Noether.

Van Kummer hebben we een bewijs uit 1844 bekeken. Dit bewijs was niet gepubliceerd, omdat de stelling niet bleek te kloppen. Dit stond in verband staat met het niet gelden van unieke priemfactorisatie in cyclotomische getallen. Ook was het voor Kummer de aanleiding voor zijn introductie van ideale getallen. We hebben gezien dat achter deze stelling uit 1844 van Kummer, een invloed van Jacobi zat. Zowel Kummer als Jacobi hadden als motivatie de zoektocht naar hogere reciprociteitswetten.

In een verhaal stammend van Hensel, wordt juist de laatste stelling van Fermat genoemd als Kummers reden voor de introductie van de ideale getallen. Kummer zou een bewijs van de laatste stelling van Fermat hebben gegeven, dat gebruikmaakte van unieke factorisatie van cyclotomische getallen. Ik heb behandeld waarom dit verhaal niet als een bewijs gezien kan worden. Daarnaast heb ik het belang van hogere reciprociteitswetten in de 19e eeuw benadrukt. Echter heb ik ook uitgelegd waarom het mij niet zou verbazen als het toch zou blijken dat Kummer zo'n bewijs zou hebben gegeven. Dit heeft te maken met dat het mij lijkt dat Kummer in zijn bewijs in 1844 wel overtuigd was van unieke factorisatie binnen het domein van cyclotomische getallen. Dit is echter open voor discussie. Ik heb behandeld wat hier argumenten voor en tegen zijn.

In ieder geval was Kummer duidelijk gemotiveerd door toepassingen. Daarom richtte hij zich ook niet tot de algemenisering van zijn theorie, maar liet hij dat aan zijn student Kronecker over. Bij Dedekind zien we juist echt een motivatie om unieke priemfactorisatie te herstellen als doel op zich.

Na de toepassingen van Kummers theorie, heb ik de definities van zijn ideale factoren behandeld. Hieruit blijkt later een tegenstelling met Dedekind. Kummer ziet ideale factoren namelijk als een noodzakelijke onderliggende structuur van cyclotomische getallen. Hij bekeek de cyclotomische getallen meer als getallen, dan als een domein. Daarom maakte het voor Kummer niet uit dat ideale factoren buiten het domein liggen. Een ander punt punt waarin hij botste met Dedekind, is dat hij de ideale factoren vanuit hun deelbaarheid definieerde. Volgens Dedekind was het juist nodig om ook de deelbaarheid van nieuwe getallen apart te definiëren, zoals hij dat gedaan had voor de reële getallen. Kummers definitie zou leiden tot een mogelijk onterechte analogie met de gehele getallen. We zien deze punten terug in Dedekinds definitie van idealen als verzamelingen en hun deelbaarheid binnen zijn domein. Dedekind had de belangrijkste twee eigenschappen van idealen gevonden en laten zien dat deze twee inderdaad genoeg zijn voor het definiëren van een ideaal. Hierin zien we Dedekinds zoektocht naar de essentie van de theorie terug. Het bleek ook mogelijk deze essentie vast te leggen zonder gebruik te maken van ideale getallen. Dit vereenvoudigt de theorie enorm.

Dedekinds manier van denken over domeinen en algebraïsche structuren lijkt al erg modern. Hij lijkt al vooruit te lopen naar de ringentheorie uit de 20e eeuw. Aan de andere kant zien we dat Dedekind toch nog echt gericht was op getaltheorie. De idealen waren het resultaat van Dedekinds doel om unieke factorisatie van algebraïsche getallen te herstellen, net als Kummers ideale getallen dit deden voor cyclotomische getallen.

Bibliografie

[1] Biermann, Kurt-R. "Dedekind, (Julius Wilhelm) Richard." Uit *Complete Dictionary of Scientific Biography*, vol. 4. Charles Scribner's Sons, 2008. p. 1-5. Gale eBooks, `https://link-gale-com.proxy.library.uu.nl/apps/doc/CX2830901117/GVRL?u=utrecht&sid=GVRL&xid=eb242fd4`. Accessed 14 May 2020.

[2] Biermann, Kurt-R. "Kummer, Ernst Eduard." Uit *Complete Dictionary of Scientific Biography*, vol. 7. Charles Scribner's Sons, 2008. p. 521-524. Gale eBooks, `https://link-gale-com.proxy.library.uu.nl/apps/doc/CX2830902404/GVRL?u=utrecht&sid=GVRL&xid=7bca05eb`. Accessed 14 May 2020.

[3] Bölling, Reinhard. "Kummer vor der Erfindung der 'idealen complexen Zahen': Das Jahr 1844." Acta historica Leopoldina 27 (1997): p. 145-147.

[4] Bölling, Reinhard. "From Reciprocity Laws to Ideal Numbers: An (Un)Known Manuscript by E.E. Kummer." Uit *The Shaping of Arithmetic after C.F.Gauss's Disquisitiones Arithmeticae*. New York: Springer, 2007. p. 271-291.

[5] Boniface, Jacqueline. "A process of generalization: Kummer's creation of ideal numbers." Uit *The oxford handbook of generality in mathematics and the sciences*. Oxford: Oxford University Press, 2016. p. 483-501.

[6] Corry, Leo. *Modern Algebra and the Rise of Mathematical Structures*. 2e ed. Basel: Springer Basel AG, 2004.

[7] Dedekind, Richard. "Sur la Théorie des Nombres Entiers Algébriques" Uit: *Über die Theorie der ganzen algebraischen Zahlen*. Frierdr. Vieweg & Sohn. Braunschweig: 1964: p. 263-313.

[8] Dedekind, Richard, and John Stillwell. *Theory of Algebraic Integers*. [Bevat het origineel 'Sur la Théorie des Nombres Entiers Algébriques' (1877), vertaald door John Stillwell.] Cambridge Mathematical Library. Cambridge: Cambridge University Press, 1996.

[9] Edwards, Harold. *The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes* Archive for History of Exact Sciences 14-3 (1975): p. 219-236.

[10] Edwards, Harold. *Postscript to 'The Background of Kummer's Proof...'* Archive for History of Exact Sciences 17-4 (1977): p. 381-394.

[11] Edwards, Harold. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory* New York: Springer-Verlag, 1977.

[12] Edwards, Harold. *The Genesis of Ideal Theory.* Archive for History of Exact Sciences 23-4 (1980): p. 321-378.

[13] Goldstein, Catherine, and Norbert Schappacher. "A Book in Search of a Discipline (1801–1860)." Uit *The Shaping of Arithmetic after C.F.Gauss's Disquisitiones Arithmeticae*. New York: Springer, 2007. p. 3-67.

[14] Kummer, Ernst. *Collected Papers Volume I: Contributions to Number Theory.* Aangepast door André Weil. Berlijn: Springer-Verlag, 1975.

[15] Kummer, Ernst. *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant.* Journal de mathematiques pures et appliquees XII (1847): p. 185-212. Uit [14, p. 165-192].

[16] Kummer, Ernst. *Zur Theorie der complexen Zahlen.* Journal für die reine und angewandte Mathematik 35 (1847): p. 319-326. Uit [14, p. 203-210].

[17] Kummer, Ernst. *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren.* Journal für die reine und angewandte Mathematik 35 (1847): p. 327-367. Uit [14, p. 211-251].

[18] Neumann, Olaf. "Über die Anstöße zu Kummers Schöpfung der 'Idealen Complexen Zahlen'" Uit *Mathematical Perspectives Essays on Mathematics and Its Historical Development* New York: Academic Press, 1981. p. 179-200.

[19] Pieper, Herbert. 'A Highschool Teacher, Who Would Be an "Ornament for Any University": Ernst Eduard Kummer.' "A Network of Scientific Philanthropy: Humboldt's Relations with Number Theorists." Uit *The Shaping of Arithmetic after C.F.Gauss's Disquisitiones Arithmeticae.* New York: Springer, 2007. p. 214-216.

[20] Stillwell, John. "Translator's introduction" Uit [8, p. 3-47]

[21] Stillwell, John. "Algebraic Number Theory." Uit *Mathematics and its History.* 3e ed. New York: Springer, 2010. p. 439-466.

[22] Ernst Eduard Kummer. MacTutor History of Mathematics Archive, University of St. Andrews. `https://mathshistory.st-andrews.ac.uk/Biographies/Kummer/pictdisplay/` (bekeken op 01-06-2020).

[23] Julius Wilhelm Richard Dedekind. MacTutor History of Mathematics Archive, University of St. Andrews. `https://mathshistory.st-andrews.ac.uk/Biographies/Dedekind/pictdisplay/` (bekeken op 01-06-2020).