

De laatste stelling van Fermat
voor reguliere priemmen

Kleine scriptie, Ruden Teuben

23 augustus 2005

Inhoudsopgave

1	Introductie en een korte historische schets	2
1.1	Inleiding	2
1.2	Geschiedenis	2
1.3	De vergelijking met $n = 2$	5
1.4	Een Diophantisch probleem	7
2	Algebraïsche getaltheorie	9
2.1	inleiding	9
2.2	Definities	9
2.3	Norm en spoor van een algebraïsch getal	11
2.4	Ring van gehelen	13
2.5	Unieke factorisatie in irreducibelen en priemmen	18
2.5.1	Factorisatie in irreducibelen	18
2.5.2	Factorisatie in priemmen	19
2.6	Aanpak van de laatste stelling van Fermat in een unieke factorisatie domein.	21
3	Het eerste geval	23
4	Het tweede geval	28
5	Dedekind-ring en unieke factorisatie in idealen	34
5.1	inleiding	34
5.2	Dedekind-ring	37
5.3	De ideaalklassengroep	42
5.4	Uitbreiding voor FLT naar reguliere priemmen	43
6	Appendix	46

1 Introductie en een korte historische schets

1.1 Inleiding

In deze scriptie zullen we een aanpak voor de laatste stelling van Fermat (FLT) bekijken. Deze is door Ernst Kummer (1810-1893) bedacht. Ik zal de scriptie als volgt indelen: als eerste zal ik een korte historische schets geven waarin we het ontstaan van algebraïsche getallen (in dat geval $\mathbb{Z}[i]$) kort zullen behandelen. Daarna zullen we de vergelijking $x^2 + y^2 = z^2$ behandelen en hiervoor zullen we gebruik maken van de unieke factorisatie eigenschap van $\mathbb{Z}[i]$. We zullen ook zien dat deze unieke factorisatie eigenschap niet algemeen geldig is voor algebraïsche getallenlichamen. Ter illustratie zullen we ook een ander, betrekkelijk eenvoudig, voorbeeld behandelen.

In het tweede hoofdstuk zullen we veel dieper op de algebraïsche getaltheorie ingaan; we zullen twee belangrijke afbeeldingen behandelen, namelijk de *norm* en het *spoor* van een getal en we zullen het begrip *ring der gehelen* invoeren als equivalent van de ring \mathbb{Z} in het lichaam \mathbb{Q} . We kunnen FLT in twee gevallen uitsplitsen, deze zijn te bewijzen als we ons in een unieke factorisatie domein (UFD) bevinden. Dit zullen we dan in eerste instantie ook aannemen, vooral omdat later zal blijken dat de andere gevallen (dus wanneer we ons *niet* persé in een UFD bevinden) op bijna dezelfde manier kunnen worden bewezen. Er is maar 1 (cruciaal) punt waarin we een andere route moeten volgen, maar over het algemeen kunnen we hetzelfde bewijs blijven gebruiken.

In hoofdstuk 5 zullen we de aanpak van Kummer tegenkomen. We zullen in plaats van getallen in een ring naar idealen kijken en hiervoor factorisatie eigenschappen afleiden. Uiteindelijk zullen we tot de constructie van de *ideaal klassegroep* komen en dit zal ons de nodige informatie verschaffen om FLT te bewijzen voor een veel grotere klasse van exponenten, namelijk alle *reguliere* priemmen.

Het is goed om te beseffen dat deze methode, ook al heeft het niet FLT voor alle exponenten bewezen, zeker niet een doodlopende weg is geweest; het heeft tot het ontstaan van het ideaalbegrip en de ideaalklassengroep geleid, wat op zijn beurt met behulp van elliptische krommen en modulaire vormen tot de uiteindelijke oplossing door (Andrew Wiles) heeft geleid.

1.2 Geschiedenis

In zijn *Disquisitiones Arithmeticae*, die gepubliceerd werd in 1801, bewees Gauss de kwadratische reciprociteit. In de jaren die daarop volgde probeerde hij dit verder te generaliseren en dit leidde tot het gebruik van de zogenaamde Gaussische getallen; $\mathbb{Z}[i]$, deze ring bestaat uit elementen van de vorm $a + bi$ met $a, b \in \mathbb{Z}$. Generalisaties van zulke uitbreidingen van \mathbb{Z} zullen in deze scriptie onze aandacht hebben, het is goed om het ontstaan en gebruik hiervan te kennen.

Gauss merkte op dat de enige eenheden (i.e. inverteerbare elementen) in deze nieuwe ring de getallen $\pm 1, \pm i$ zijn. Daarna definieert hij de norm van een geheel getal in $\mathbb{Z}[i]$ als het product van zijn geconjugeerden;¹ de norm van het getal $a + bi$ wordt $(a + bi)(a - bi) = a^2 + b^2$ en dit wordt genoteerd als $N(\alpha)$, we zullen deze manier van een norm definiëren later ook terug zien in andere ringen. Omdat we over factorisatie van getallen in priemgetallen willen gaan praten is ook een notie van priemgetal nodig; Gauss definieert een priemgetal als een geheel getal dat niet uitgedrukt kan worden als het produkt van 2 andere gehele getallen (die geen eenheden zijn).² Een priemgetal kan zelf geen eenheid zijn, en als p een priemgetal is en u een eenheid dan is ook $u \cdot p$ een priem, je definieert als het ware "up to units".

¹De gebruikelijke complexe conjugatie: $a + bi \rightarrow a - bi$.

²Voor een priemgetal p en een eenheid u geldt natuurlijk altijd $p = p \cdot u \cdot u^{-1}$.

Dit is hetzelfde als in \mathbb{Z} waar je zowel 7 als -7 een priemgetal noemt, de eenheden van \mathbb{Z} zijn namelijk ± 1 .

Maar wat zijn dan de priemmen in deze nieuwe ring $\mathbb{Z}[i]$? Zijn bijvoorbeeld de priemgetallen p uit \mathbb{Z} ook hier priem?

Lemma 1.1 *Zij p een priemgetal in \mathbb{Z} , dan is p een priemgetal in $\mathbb{Z}[i]$ dan en slechts dan als $p \equiv 3 \pmod{4}$.*

Bewijs: Voor $p = 2$ geldt: $2 = (1 + i)(1 - i)$ daarom 2 is te schrijven als produkt van 2 gehele getallen die beide geen eenheid zijn, en daarom niet priem. Voor $p > 2$ geldt dat p oneven is en daarom $p \equiv 1, 3 \pmod{4}$. Het feit dat $p \equiv 1 \pmod{4}$ is equivalent met te zeggen dat p te schrijven is als de som van 2 kwadraten: $p = a^2 + b^2$ met $a, b \in \mathbb{Z}$ (Voor een bewijs zie [14], theorem 7.2 of [3], paragraaf 8.1). Hieruit verkrijgen we de volgende factorisatie:

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

met $a, b \neq 0$ (stel dat één van beide wel nul was dan zou p een kwadraat zijn). We zien dat p daarom is te schrijven als een produkt van 2 andere gehele getallen die beide geen eenheid zijn en daarom is een priem in \mathbb{Z} van voorgaande vorm geen priem in $\mathbb{Z}[i]$.

Om te bewijzen dat een priem in \mathbb{Z} van de vorm $p \equiv 3 \pmod{4}$ wel priem blijft in $\mathbb{Z}[i]$ moeten we eerst een tussenresultaat behandelen. Voor $a \in \mathbb{Z}[i]$ geldt $a|x \Rightarrow \bar{a}|\bar{x}$. Stel nu dat $x \in \mathbb{Z}$ dan geldt $x = \bar{x}$ en daarom impliceert $a|x$ dat $\bar{a}|x$.

Een $x \in \mathbb{Z}$ is, wegens voorgaande, te schrijven als product van gehele getallen in \mathbb{Z} (i.e. getallen die gelijk zijn aan hun geconjugeerde) en paren van getallen in $\mathbb{Z}[i]$ - \mathbb{Z} (i.e. getallen met een imaginair deel ongelijk nul) en hun geconjugeerden. Met andere woorden; als we x schrijven als:

$$x = \wp_1^{m_1} \wp_2^{m_2} \dots \wp_n^{m_n}.$$

Dan kunnen we de termen zo ordenen dat geldt:³

$$\begin{aligned} \wp_1^{m_1}, \dots, \wp_s^{m_s} &\in \mathbb{Z} \\ \wp_{s+1}^{m_{s+1}}, \dots, \wp_n^{m_n} &\in \mathbb{Z}[i] - \mathbb{Z}. \end{aligned}$$

We weten dat $\wp_{s+1}^{m_{s+1}} \wp_{s+2}^{m_{s+2}} \dots \wp_n^{m_n} = \alpha\bar{\alpha} \in \mathbb{Z}$ en dat er in \mathbb{Z} natuurlijk unieke factorisatie is. Dus als we voor x een priemgetal $p \in \mathbb{Z}$ kiezen, dan kunnen we niet veel factoren overhouden. Omdat p een priemgetal is in \mathbb{Z} , volgt juist dat p niet uit te drukken is als produkt van gehelen in \mathbb{Z} , anders dan zichzelf. Daarom geldt: of $n = 1$ en $p = \wp_1$, dan zijn we klaar (p is blijkbaar ook priem in $\mathbb{Z}[i]$), of $s = 0$ en $p = \alpha\bar{\alpha}$ voor zekere $\alpha \in \mathbb{Z}[i]$ - \mathbb{Z} , maar dat betekent $p \equiv 1 \pmod{4}$ en dit kan niet, aangezien $p \equiv 3 \pmod{4}$. Dus er is geen manier om p te schrijven als produkt van 2 gehele getallen in $\mathbb{Z}[i]$ die geen eenheden zijn. Hieruit volgt een priem p uit \mathbb{Z} van de vorm $p \equiv 3 \pmod{4}$ ook een priem in $\mathbb{Z}[i]$. \square

Gauss bewees dat een getal $a + bi$ priem is als zijn norm $N(a + bi)$ een priemgetal (in \mathbb{Z}) is⁴, zo een norm, die altijd in \mathbb{Z} ligt, kan dan natuurlijk alleen 2 of 1 mod 4 zijn, omdat zoals we gezien hebben, een priemgetal in \mathbb{Z} van de vorm 3 mod 4 niet te schrijven is als produkt van geconjugeerden. Dit volgt uit de feiten $N(\alpha\beta) = N(\alpha)N(\beta)$ en dat de enige getallen in $\mathbb{Z}[i]$ met norm gelijk aan 1 de eenheden,

³Hierbij geldt de volgende conjugentie-relatie: $\wp_i^{m_i} = \overline{\wp_{i+1}^{m_{i+1}}}$, $i = s + 1, s + 3, \dots, n - 1$.

⁴Stel namelijk van niet, stel $a + bi = \alpha\beta$ dan geldt $N(a + bi) = N(\alpha)N(\beta)$ dit is onmogelijk aangezien $N(a + bi)$ een priemgetal is.

namelijk ± 1 en $\pm i$ zijn. Want $N(a + bi) = a^2 + b^2 = 1$ impliceert dat of a^2 is 1 en $b^2 = 0$ of andersom, wat precies overeenkomt met de 4 eenheden.

Nadat Gauss de priemmen gedefinieerd had, bewees hij de unieke factorisatie in $\mathbb{Z}[i]$. Verder hield hij zich bezig met veralgemeniseringen van de kwadratische reciprociteitswet. Daartoe gebruikte hij getallen van de vorm $a + b\zeta$, waarbij ζ een oplossing is (ongelijk 1) van $X^3 - 1 = 0$, maar dit werk heeft hij nooit afgekregen.

Zulke nieuwe ringen, de zogenaamde cyclotome uitbreidingen van \mathbb{Z} , bleken erg bruikbaar te zijn, niet alleen om reciprociteitswetten mee te bewijzen, maar bijvoorbeeld ook voor het werk aan de laatste stelling van Fermat (FLT); namelijk dat er geen oplossingen bestaan voor de vergelijking⁵

$$x^n + y^n = z^n, \quad xyz \neq 0, \quad x, y, z, n \in \mathbb{Z}, \quad n > 2. \quad (1)$$

In 1847 kondigde Lamé aan dat hij FLT had bewezen. Hij gaf een korte bewijschets aan, hij wou gebruik maken van de factorisatie:

$$x^p + y^p = (x + y)(x + y\zeta)(x + y\zeta^2) \dots (x + y\zeta^{p-1}), \quad (2)$$

waarbij ζ de oplossing $e^{\frac{2\pi i}{p}}$ is van $X^p - 1 = 0$.⁶ Daarna was hij van plan om te laten zien dat alle factoren in het rechterlid van (2) in feite p -de machten zijn omdat ze relatief priem zijn en een p -de macht (namelijk z^p) delen. Daarna wou hij dit tot een tegenspraak voeren m.b.v de methode van Fermat, genaamd "Descent infinite".

Wat we hier zien is erg interessant, het is een generalisatie van de methode die Gauss al gebruikte, namelijk om naar zogenaamde cyclotome⁷ uitbreidingslichamen van \mathbb{Q} te kijken. Dit zijn lichamen van de vorm $\mathbb{Q}(\zeta)$ waarbij ζ een primitieve p -de eenheids wortel is, d.w.z. een wortel van $X^p - 1$ die alle andere voorbrengt, bijvoorbeeld $e^{\frac{2\pi i}{p}}$. De elementen van dit lichaam $\mathbb{Q}(\zeta)$ zijn te schrijven als

$$a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{p-1}\zeta^{p-1}, \quad a_i \in \mathbb{Q}.$$

Waar het natuurlijk vooral om te doen is, is de ring van gehelen in dit lichaam: $\mathbb{Z}[\zeta] \subset \mathbb{Q}(\zeta)$, omdat eigenschappen als unieke factorisatie in priemmen natuurlijk eigenschappen in ringen zijn en niet in lichamen. We zullen hier veel uitgebreider op terugkomen in het volgende hoofdstuk.

Liouville, die bij deze uiteenzetting aanwezig was, sprak zijn sterke twijfels uit over deze manier. Hij vond dat unieke factorisatie in priemfactoren in deze nieuwe ring $\mathbb{Z}[\zeta]$ helemaal niet zo vanzelfsprekend is, en dat het wel eens heel goed zou kunnen dat dit onmogelijk is. In de weken die daarop volgden probeerde Lamé deze tegenwerping te weerleggen, wat tevergeefs was, todat Kummer een eind aan deze discussie maakte; Liouville kwam een artikel van Kummer tegen, waarin hij een voorbeeld gaf van een ring waarin geen unieke factorisatie gold. Hij gaf een voorbeeld van een geheel getal met meerdere factorisaties in de ring $\mathbb{Z}[\zeta]$ met ζ een primitieve wortel van $X^{23} - 1$.

⁵Merk op dat het voldoende is om de gevallen waarin n priem is te behandelen. Stel dat we kunnen bewijzen dat er daar geen oplossingen van bestaan, dan impliceert dit ook de onmogelijkheid van oplossingen waarbij n samengesteld is: zij $n = p \cdot c$ met p priem dan geeft een oplossing (x, y, z) van $x^n + y^n = z^n$ ook een oplossing (x^c, y^c, z^c) van $x^p + y^p = z^p$ en dat kan niet.

⁶Voor het gemak zullen we aannemen dat p een priemgetal is, dit geldt, indien anders vermeldt, voor al wat volgt. Dit maakt het een stuk makkelijker omdat dan elke macht ζ^i met $1 \leq i \leq p-1$ een voortbrenger van de (cyclische) groep $\{1, \zeta, \dots, \zeta^{p-1}\}$ is.

⁷Cyclotoom komt van de Griekse woorden *cyclus* en *tomos*. Cyclotoom betekent zoveel als cirkel-snijden, aangezien de verschillende ζ^i 's de complexe eenheids cirkel in (gelijke) stukken snijden.

Voorgaande resultaten gaven aanleiding om de unieke factorisatie eigenschappen van zulke ringen te onderzoeken. Of zoals Kummer in *De numeris complexis, qui radicibus unitatus et numeris integris constant* (1847) [9] het zegt:

It is greatly to be lamented that this virtue of the real integers that they can be decomposed into prime factors wich are always the same for a given integer does not belong to the complex integers [of arbitrary cyclotomic number fields], for were this the case, the entire theory, which is still laboring under many difficulties, could be easily resolved and brought to a conclusion. For this reason, the complex integers we are considering are seen to be imperfect, and there arises the question whether other types of complex numbers can be found...wich would preserve the analogy with the real integers with respect to this fundamental property.

Een voorbeeld hiervan is het getal 10 dat in de ring $\mathbb{Z}[\sqrt{15}]$ te schrijven is als:

$$10 = 2 \cdot 5 = (5 + \sqrt{15}) \cdot (5 - \sqrt{15}).$$

Al deze 4 getallen, 2, 5, $(5 \pm \sqrt{15})$ zijn irreducibel, dat wil zeggen niet te schrijven als produkt van andere gehele getallen (die geen eenheden zijn). Kummers inzicht leidde hem ertoe *ideale getallen* te construeren zodat in dit geval:

$$2 = \wp_1 \wp_2, \quad 5 = \wp_3 \wp_4, \quad (5 + \sqrt{15}) = \wp_1 \wp_3, \quad (5 - \sqrt{15}) = \wp_2 \wp_4.$$

De voorgaande factorisatie wordt daardoor:

$$10 = (\wp_1 \wp_2)(\wp_3 \wp_4) = (\wp_1 \wp_3)(\wp_2 \wp_4),$$

waarbij zo de meervoudigheid van factorisatie teniet wordt gedaan. Hiertoe bedacht Kummer zogenaamde "ideale complexe getallen" en definieerde deelbaarheid door zulke getallen. Hij construeerde een uitbreiding, door middel van ideale getallen, zodanig dat unieke factorisatie behouden blijft en dit werd later door Dedekind geformaliseerd en hij voerde hiervoor het hedendaagse begrip ideaal in. Dit voorbeeld komt uit [14] paragraaf 5.1. Een ander soortgelijk voorbeeld is te vinden in [13], p17-18. Ik zal hier verder op in gaan in hoofdstuk 5 paragraaf 1, waarbij bovenstaande wordt uitgewerkt. Vooralsnog is het goed om te realiseren dat er inderdaad uitbreidingen van \mathbb{Q} zijn waarin er geen unieke factorisatie is.

Voor deze paragraaf heb ik stukken uit [8] gebruikt.

1.3 De vergelijking met $n = 2$

In deze paragraaf wil ik een uitbreiding van vergelijking (1) behandelen, namelijk $n = 2$. Hiervoor zullen wel oplossingen bestaan en we kunnen door de manier waarop we de oplossingen verkrijgen veel leren over hoe we andere gevallen, met $n > 2$ kunnen aanpakken. Vooral de zogenaamde cyclotome lichaamsuitbreidingen van \mathbb{Q} en de ring van gehelen $\mathbb{Z}[\zeta] \subset \mathbb{Q}(\zeta)$ hierin zullen we later gebruiken.

We hebben het over de vergelijking:

$$x^2 + y^2 = z^2, \quad xyz \neq 0 \quad (x, y, z \in \mathbb{Z}). \quad (3)$$

De oplossingen (x, y, z) hiervan heten Pythagoreïsche drietallen, dit zijn de lengten van zijden van driehoeken met gehele zijden. We nemen aan dat x, y, z geen factor gemeen hebben, anders delen we die uit. Hieruit volgt dat x, y, z ook paarsgewijs

priem zijn, want stel van niet, dan zouden we de 2 factoren die een factor gemeenschappelijk hebben naar 1 kant kunnen halen in vergelijking (3) en hieruit zou volgen dat ook de 3^e variabele deelbaar door deze factor moet zijn en dus dat x, y, z niet relatief priem zijn. We beginnen met de volgende factorisatie van (3):

$$x^2 + y^2 = (x + yi)(x - yi). \quad (4)$$

Door de vergelijking op deze manier te schrijven wordt een lastige combinatie van optellen en vermenigvuldigen (kwadrateren) teruggebracht tot een louter multiplicatief probleem in $\mathbb{Z}[i]$.

We zullen eerst bewijzen dat er in $\mathbb{Z}[i]$ unieke factorisatie is. Er geldt dat in een ring waar unieke factorisatie is, een zogenaamd "Unique Factorisation Domain" (UFD), elk ideaal een hoofdideaal is, dat wil zeggen; voortgebracht door 1 element. Zo een ring wordt ook wel "Principal Ideal Domain" genoemd (PID) (We zullen hier later op terugkomen in paragraaf 2.5 waar we zullen bewijzen dat UFD \Rightarrow PID, voor een bewijs zie nu alvast [10], theorem 6.2).

We zullen daarom, om aan te tonen dat $\mathbb{Z}[i]$ een UFD is, volstaan met te bewijzen dat het een PID is.

Lemma 1.2 *Elk ideaal in $\mathbb{Z}[i]$ is een hoofdideaal.*

Bewijs: Zij \mathfrak{a} een ideaal in $\mathbb{Z}[i]$. Kies een element $\alpha \in \mathfrak{a} - 0$ zodanig dat zijn norm $N(\alpha)$ minimaal is. De getallen $\gamma\alpha$ met $\gamma \in \mathbb{Z}[i]$ vormen een rooster dat \mathbb{C} overdekt⁸. Dit rooster bestaat uit vierkanten met hoekpunten

$$\{\tilde{\gamma}\alpha, (\tilde{\gamma} + 1)\alpha, (\tilde{\gamma} + i)\alpha, (\tilde{\gamma} + 1 + i)\alpha\}, \quad \tilde{\gamma} \in \mathbb{Z}[i].$$

Er geldt dat $\{\gamma\alpha | \gamma \in \mathbb{Z}[i]\} \subseteq \mathfrak{a}$ per definitie van een ideaal (namelijk dat het gesloten is onder vermenigvuldiging). Nu te bewijzen $\mathfrak{a} \subseteq \{\gamma\alpha | \gamma \in \mathbb{Z}[i]\}$. Stel van niet, dan kunnen we een element $\beta \in \mathfrak{a}$ vinden met $\beta \neq \gamma\alpha$ voor alle $\gamma \in \mathbb{Z}[i]$. β Kan daarom niet op een roosterpunt liggen, maar aangezien het rooster \mathbb{C} overdekt, is er een roosterpunt $\gamma_0\alpha$ te vinden met $N(\beta - \gamma_0\alpha) < \frac{1}{2}\sqrt{2}N(\alpha) < N(\alpha)$ (zie figuur 1). Dit kan niet, want $\beta - \gamma_0\alpha$ is een element van $\mathfrak{a} - 0$ met norm strikt kleiner dan α , maar α was juist zo gekozen dat $N(\alpha)$ minimaal is. Dus er moet gelden $\mathfrak{a} \subseteq \{\gamma\alpha | \gamma \in \mathbb{Z}[i]\}$. Maar dit betekent dat $\mathfrak{a} = (\alpha)$, oftewel \mathfrak{a} is een hoofdideaal. \square

Lemma 1.3 *Stel $x^2 + y^2 = z^2$ dan zijn de getallen $(x + yi)$ en $(x - yi)$ in $\mathbb{Z}[i]$, met $x, y \in \mathbb{Z}$, relatief priem in $\mathbb{Z}[i]$.*

Bewijs: Stel van niet, dan bestaat er een priemfactor p in $\mathbb{Z}[i]$ die beide deelt, en daarom ook hun som: $2x$ en hun produkt: z^2 en daarom ook z . Als we naar de originele vergelijking (3) modulo 4 kijken, valt het volgende op: een kwadraat is altijd 0 of 1 mod 4 en we kunnen niet hebben dat $x, y, z \equiv 0 \pmod{4}$, want dan zouden x, y, z een factor 4 gemeen hebben. We zien dat daarom altijd moet gelden dat x of y 1 mod 4 is, de ander 0 mod 4 en z is altijd 1 mod 4. Hieruit volgt daarom dat z oneven is en daarom relatief priem is met $2x$, want z is oneven dus relatief priem met 2 en per definitie relatief priem met x en daarom ook met hun produkt. Er zijn nu $n, m \in \mathbb{Z}$ te vinden met $m2x + nz = 1$ maar dit impliceert dat p ook 1 deelt, maar dat kan niet, want 1 is een eenheid. Dus $(x + yi)$ en $(x - yi)$ kunnen geen gemeenschappelijke factor hebben en zijn daarom relatief priem. \square

Door bovenstaande resultaten weten we dat $(x + yi)$ de volgende vorm moet hebben: $u\alpha^2$, voor een geheel getal α in $\mathbb{Z}[i]$ en een eenheid u . Dit komt doordat elke (priem)factor die $(x + yi)$ deelt, geen andere getallen in het rechterlid van (4)

⁸Overdekken in de zin dat de "ruiten" van het rooster \mathbb{C} overdekken, niet de roosterpunten.

$$\begin{array}{ccc}
& \gamma_0\alpha & \\
& (\gamma + i)\alpha & (\gamma + 1 + i)\alpha \\
& \beta & \\
N(\gamma_0\alpha - \beta) & & \\
& \gamma\alpha & (\gamma + 1)\alpha
\end{array}$$

Figuur 1: Schets van het rooster behorende bij lemma 1.2

kan delen, maar wel het kwadraat z^2 deelt. Daarom moet deze factor (aan beide kanten) een even aantal keer voorkomen. Als we dit verder uitwerken, door te schrijven $\alpha = m + ni$ voor zekere $m, n \in \mathbb{Z}$ en opmerken dat de eenheden ± 1 en $\pm i$ zijn, verkrijgen we $x + yi = u(m^2 - n^2 + 2mni)$. Afhankelijk van u hebben x, y respectievelijk de vorm: $\pm(m^2 - n^2)$ en $\pm 2mn$. (Anders geeft het verwisselen van x en y het gewenste resultaat.) Bovenstaande notatie ($\alpha = m + ni$) geeft een aftelling voor $\mathbb{Z}[i]$; dus alle oplossingen van (3) zijn:

$$x = \pm(m^2 - n^2), \quad y = \pm 2mn, \quad z = \pm(m^2 + n^2). \quad m, n \in \mathbb{Z}$$

1.4 Een Diophantisch probleem

In deze paragraaf zal ik nog een probleem, vergelijkbaar met het probleem in de vorige paragraaf, behandelen. Ook hier zullen we van soortgelijke methoden gebruik maken. Ik zal hier wat sneller doorheen gaan, omdat hier geen nieuwe dingen worden geïntroduceerd. Het zal vooral handig zijn om dezelfde methoden bij een ander probleem te zien.

Het probleem is een speciaal geval van Catalan's vermoeden, namelijk dat de enige oplossingen van $x^m - y^n = 1$ met $m, n \geq 2$ en x, y positieve gehele getallen de oplossing $3^2 - 2^3 = 1$ is. Wij zullen ons bezig houden met het zoeken naar oplossingen van de vergelijking:

$$x^3 - y^2 = 1, \quad x, y \in \mathbb{Z}. \quad (5)$$

Hierin is x even of oneven. Stel x is even dan geldt $x^3 \equiv 0 \pmod{8}$ en daarom $y^2 \equiv -1 \pmod{8}$, maar -1 is geen kwadraat modulo 8. Daarom moet x oneven zijn, hieruit volgt dat y oneven is aangezien het verschil oneven (namelijk 1) moet zijn en y kan zodoende niet ook oneven zijn.

Als we vergelijking (5) herschrijven als $y^2 + 1 = x^3$ en dit factoriseren (in $\mathbb{Z}[i]$) krijgen we:

$$(y + i)(y - i) = x^3. \quad (6)$$

Lemma 1.4 *In bovenstaande vergelijking zijn de factoren $(y+i)$ en $(y-i)$ relatief priem.*

Bewijs: Stel van niet, dan zou hun gemeenschappelijke factor α ook hun verschil delen: $\alpha|(y+i) - (y-i) = 2i$. Maar $2i = (1+i)^2$ en voor $(1+i)$ geldt dat het priem is aangezien zijn norm 2, een priemgetal in \mathbb{Z} , is (zie paragraaf 2). Aangezien α geen eenheid is moet daarom gelden $u\alpha = (1+i)$ of $(1+i)^2$ voor zekere eenheid u . We hebben dus: $(1+i)|\alpha$ en daarom ook $(1+i)|(y+i)(y-i) = x^3$ aangezien het rechterlid hiervan deelbaar is door α en daardoor zeker ook door een deler van α zoals $(1+i)$. Omdat $(1+i)$ priem is, moet gelden $(1+i)|x$ oftewel: er bestaat een $\beta \in \mathbb{Z}$ met $x = (1+i)\beta$. Nu vermenigvuldigen we deze uitdrukking met zijn complex geconjugeerde: $x\bar{x} = (1+i)(1-i)\beta\bar{\beta}$ maar $x, y \in \mathbb{Z}$ en daarom geeft voorgaande uitdrukking dat $x\bar{x} = x^2 = 2\beta\bar{\beta}$ met andere woorden $2|x^2$, oftewel x is even, maar x was ook oneven, dit kan niet. We concluderen dat $(y+i)$ en $(y-i)$ inderdaad relatief priem zijn. \square

Nu moeten de factoren $(y+i)$ en $(y-i)$ beide van de vorm $u\beta^3$ zijn, waarbij u een eenheid in $\mathbb{Z}[i]$ is en β een geheel getal (in $\mathbb{Z}[i]$). Aangezien de eenheden in $\mathbb{Z}[i]$ de getallen ± 1 en $\pm i$ zijn en deze allemaal te schrijven zijn als 3^e machten, moet daarom gelden dat $(y+i)$ en $(y-i)$ beide te schrijven zijn als 3^e macht in $\mathbb{Z}[i]$. Als we dit uitwerken verkrijgen we voor $a, b \in \mathbb{Z}$:

$$y+i = (a+bi)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i = (a^3 - 3ab^2) + (3a^2b - b^3)i.$$

Dus $y = a(a^2 - 3b^2)$ en $1 = b(3a^2 - b^2)$. Omdat $a, b \in \mathbb{Z}$ en daarom ook $(3a^2 - b^2) \in \mathbb{Z}$ moet gelden dat $b = \pm 1$. Stel $b = 1$ dan $1 = 3a^2 - 1$ wat zou impliceren dat $2 = 3a^2$ maar dit heeft geen oplossing in \mathbb{Z} . Dus we concluderen $b = -1$ en $-1 = 3a^2 - 1$ oftewel $3a^2 = 0$ en daarom $a = 0$. Dit geeft ons dan alle oplossingen van vergelijking (5): $y = 0$ en $x^3 = y^2 + 1$ oftewel $x = 1$ en $y = 0$.

Ik heb voor deze paragraaf [2] gebruikt.

2 Algebraïsche getaltheorie

2.1 inleiding

In het eerste inleidende hoofdstuk hebben we het historisch verloop en 2 voorbeelden gezien. We hebben (gedeeltelijk) laten zien dat $\mathbb{Z}[i]$ een UFD is en daarmee de 2 voorbeelden opgelost. Verder hebben we ook gezien dat voor onze de aanpak van FLT we ook unieke factorisatie eigenschappen van bepaalde cyclotome uitbreidingen van \mathbb{Q} nodig hebben. In dit hoofdstuk willen we hier dieper op in gaan. We zullen beginnen met een aantal definities en een wat formelere aanpak. Dit zal voor een klein gedeelte overlappen met wat we in hoofdstuk 1 al gezien hebben, maar het zal vooral een wat formelere basis daaronder leveren, zodat we in volgende hoofdstukken weten waar we het over hebben en wat mogelijk is bij de aanpak van FLT.

We zullen eerst definiëren wat we met een algebraïsch getallenlichaam bedoelen, daarna definiëren we twee belangrijke afbeeldingen hierop, namelijk de norm en het spoor. Deze zullen handige werktuigen blijken te zijn. Wanneer we zover zijn, zullen we ons richten op de ring der gehelen; dit zal tenslotte de omgeving zijn waarin we aan het werk willen met unieke factorisatie en dergelijke, we zullen dit dan ook daarna behandelen.

2.2 Definities

Een *algebraïsch getallenlichaam* is een eindig dimensionale uitbreiding van \mathbb{Q} . Of anders gezegd: elk element (van een algebraïsch getallenlichaam) is een wortel van een (monisch) polynoom⁹ in $\mathbb{Q}[X]$, dus elk element x in een algebraïsch getallenlichaam is te schrijven als oplossing van:

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = 0, \quad a_i \in \mathbb{Q}.$$

Als voor bovenbeschreven x nu geldt dat alle coëfficiënten a_i in \mathbb{Z} liggen, dan heet x een *algebraïsche geheel* of *algebraïsch geheel getal*. De verzameling van algebraïsche gehelen in een getallenlichaam is een deeling, dit zullen we in de volgende paragraaf bewijzen. Zij x een algebraïsch getal, dan zijn zijn *geconjugeerden* de wortels van zijn minimaal polynoom f_x .

In de ring van algebraïsche gehelen noemen we, in overeen stemming met hoofdstuk 1, een getal een *eenheid* als het een (multiplicatieve) inverse heeft. We noemen een getal *irreducibel* als het niet te schrijven is als produkt van 2 andere getallen die geen eenheid zijn. We noemen een getal, dat geen eenheid is, *priem* als wanneer het een produkt deelt, het 1 van de termen deelt, dus stel p is een priemgetal in een ring van algebraïsche gehelen en er geldt $p|ab$, dan moet gelden dat $p|a$ of $p|b$. Het irreducibel of priem zijn van een getal is in \mathbb{Z} hetzelfde maar dit hoeft in andere ringen niet zo te zijn.

Een commutatieve ring heet een *domein* als geldt dat wanneer $xy = 0$ dat dan $x = 0$ of $y = 0$, oftewel de ring heeft geen "delers van nul". Bijvoorbeeld \mathbb{Z} is een domein, net als de ring van polynomen over een lichaam, of een lichaam zelf. Wat voor ons nu vooral van belang is, is het feit dat $\mathbb{Q}(X)$, uitgedeeld naar een ideaal voortgebracht door een irreducibel polynoom, een domein is. Dit geldt dan ook voor $\mathbb{Q}(\zeta)$, want dit is $\mathbb{Q}(X)$ uitgedeeld naar $\langle f_\zeta \rangle$, hierbij is f_ζ het minimaalpolynoom van ζ , we zullen dit tegenkomen in hoofdstuk 2 paragraaf 3. Hieruit volgt dan dat $\mathbb{Z}[\zeta]$ dat immers in $\mathbb{Q}(\zeta)$ ligt ook een domein moet zijn, later zal blijken dat dit de ring der gehelen van $\mathbb{Q}(\zeta)$ is.¹⁰

⁹Als de uitbreiding eindigdimensionaal is, zeg van dimensie n , dan zijn $1, \alpha, \alpha^2, \dots, \alpha^n$ linear afhankelijk en er bestaat daarom een polynoom f van graad hoogstens n met $f(\alpha) = 0$.

¹⁰Dat $\mathbb{Q}(X)$ geen delers van nul heeft komt doordat voor polynomen ongelijk nul hun graad groter dan nul is, en daarom de graad van hun produkt dit ook zeker is en dit daarom nooit een polynoom gelijk aan nul op kan leveren.

Lemma 2.1 *In een domein is elk priem element irreducibel.*

Bewijs: Stel π is priem in het domein R , en dat $\pi = xy$ voor bepaalde $x, y \in R$. We hebben nu per definitie van priemgetal dat $\pi|x$ of $\pi|y$. Stel $\pi|y$ dan hebben we $y = \alpha\pi$ voor een $\alpha \in R$. Als we nu beide kanten met x vermenigvuldigen, krijgen we: $\pi = xy = \alpha x\pi$, omdat R een domein is en $\pi(1 - \alpha x) = 0$ met $\pi \neq 0$ moet gelden dat $(1 - \alpha x) = 0$ ofwel $\alpha x = 1$. Dit impliceert dat x een eenheid is, (want hij heeft een inverse) en dus dat π irreducibel is. \square

In tegenstelling tot wat je in eerste instantie zou vermoeden is het omgekeerde van bovenstaand lemma niet waar; er bestaan ringen die elementen bevatten die niet priem zijn maar wel irreducibel. Een voorbeeld zou zijn, iets soortgelijks we in hoofdstuk 1 al gezien hebben bij de introductie van Kummers aanpak; in $\mathbb{Z}[\sqrt{-5}]$ geldt:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}).$$

Een getal in $\mathbb{Z}[\sqrt{-5}]$ heeft de vorm $a + b\sqrt{-5}$. We definiëren als norm op deze ring de afbeelding $x \rightarrow N(x)$ als

$$(a + b\sqrt{-5}) \rightarrow (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2,$$

met de multiplicatieve eigenschap $N(\alpha\beta) = N(\alpha)N(\beta)$.

De eenheden in deze ring zijn ± 1 aangezien voor een eenheid x moet gelden dat er een inverse x^{-1} bestaat, zodanig dat $xx^{-1} = 1$ als we aan beide kanten de norm nemen en x als $a + b\sqrt{-5}$ schrijven verkrijgen we: $N(x)N(x^{-1}) = (a^2 + 5b^2)N(x^{-1}) = 1$. Omdat $a, b \in \mathbb{Z}$ zien we dat $N(x) \in \mathbb{N}$, daarom kunnen we concluderen $a^2 + 5b^2 = 1$ oftewel $a = \pm 1$ en $b = 0$. Dit laat ook zien dat in deze ring voor een willekeurig element $x \in \mathbb{Z}[\sqrt{-5}]$ geldt $N(x) = 1$ dan en slechts dan als x een eenheid is.

We beweren dat al de factoren $3, 7, (1 \pm 2\sqrt{-5})$ irreducibel zijn. Stel van niet, dan zijn ze te schrijven als produkt van andere getallen in $\mathbb{Z}[\sqrt{-5}]$, die geen eenheden zijn, oftewel met norm strikt groter dan 1. We zullen nu naar de norm van de getallen kijken en de multiplicativiteit van deze afbeelding gebruiken.

De normen van $3, 7, (1 \pm 2\sqrt{-5})$ zijn respectievelijk 9, 49, 21. We hadden aangenomen dat bovenstaande factoren reducibel zijn en dus te schrijven zijn als produkt. Dit moet dan ook voor hun norm gelden. De enige manier om 9, 49 of 21 te schrijven als produkt van getallen strikt groter dan 1, is respectievelijk $3 \cdot 3, 7 \cdot 7$ en $3 \cdot 7$. Maar er bestaan geen getallen in $\mathbb{Z}[\sqrt{-5}]$ met norm gelijk aan 3 of 7, anders zou $a^2 + 5b^2 = 3, 7$ een oplossing in \mathbb{Z} moeten hebben en dat kan niet. We concluderen dat er geen manier is om $3, 7$ of $(1 \pm 2\sqrt{-5})$ te schrijven als produkt van niet-eenheden en daarom zijn ze irreducibel.

We zullen nu laten zien dat hoewel irreducibel, ze niet priem zijn.

Stel dat de genoemde factoren priem zijn; we hebben $3|(1+2\sqrt{-5}) \cdot (1-2\sqrt{-5})$ en niet $3|(1 \pm 2\sqrt{-5})$, want als we aan beide kanten de norm nemen zou dit impliceren $9|21$ en dat is onjuist, idem 3. Uit $(1 \pm 2\sqrt{-5})|3 \cdot 7$ volgt $(1 \pm 2\sqrt{-5})|3$ of $(1 \pm 2\sqrt{-5})|7$; $(1 \pm 2\sqrt{-5})$ is immers een priem. Aan beide kanten de norm nemen geeft: $21|9$ of $21|49$, oftewel een tegenspraak.

Merk op dat de implicatie $x|y \Rightarrow N(x)|N(y)$ correct is. $x|y$ Betekend immers dat $y = \alpha x$ en daardoor $N(y) = N(\alpha)N(x)$, met andere woorden: $N(x)|N(y)$. Dit is natuurlijk breder geldig dan alleen in deze ring $\mathbb{Z}[\sqrt{-5}]$, maar hangt veeleer af van de multipliciteit van de norm.

We zullen ons vooral concentreren op het algebraïsch getallenlichaam $\mathbb{Q}(\zeta)$, met ζ een p^{de} -machts eenheidswortel (bijvoorbeeld $e^{\frac{2\pi i}{p}}$), en de ring van gehelen hierin. Dit zal immers de ring worden waarin we vergelijking (1) willen factoriseren. We

zullen bewijzen in paragraaf 2.4 dat in zo een algebraïsch getallenlichaam $\mathbb{Q}(\zeta)$ de ring der gehelen van dat lichaam de deelring $\mathbb{Z}[\zeta]$ is.¹¹

Aangezien $\{\zeta^{p-1}, \zeta^{p-2}, \dots, 1\}$ lineair afhankelijk zijn, er geldt namelijk

$$\zeta^{p-1} + \zeta^{p-2} + \dots + 1 = 0,$$

en $\{\zeta^{p-2}, \dots, 1\}$ niet (zie volgende paragraaf), geeft dit een basis voor $\mathbb{Q}(\zeta)$ namelijk $\{\zeta^{p-2}, \dots, 1\}$. Elk element in $\mathbb{Q}(\zeta)$ is daarom te schrijven als:

$$a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0, \quad a_i \in \mathbb{Q}.$$

En voor elk element in $\mathbb{Z}[\zeta]$ geldt dat $a_i \in \mathbb{Z}$.

2.3 Norm en spoor van een algebraïsch getal

Eerder zijn de geconjugeerden van een algebraïsch getal x al gedefinieerd als de wortels van zijn minimaal polynoom. Een equivalente, maar in sommige gevallen bruikbaarere definitie is die aan de hand van monomorfismen¹² van $\mathbb{Q}(\zeta)$ naar \mathbb{C} . Het minimaalpolynoom van ζ kennen we, ζ is namelijk een oplossing van

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots + 1), \quad \zeta \neq 1$$

en daarom is

$$f(X) = X^{p-1} + X^{p-2} + \dots + 1$$

een kandidaat voor het minimaalpolynoom, in ieder geval moet het minimaalpolynoom een deler van f zijn. Wanneer we $f(X + 1)$ uitwerken verkrijgen we:

$$f(X + 1) = X^{p-1} + pX^{p-2} + \dots + \binom{p}{i}X^{p-i-1} + \dots + p$$

en we zien met behulp van Eisensteins irreducibiliteitsprincipe dat dit polynoom irreducibel is.¹³ Dit is equivalent met het irreducibel zijn van $f(X)$ en verkrijgen het minimaalpolynoom van ζ namelijk

$$f_\zeta = X^{p-1} + X^{p-2} + \dots + 1.$$

Dit geeft dat $\mathbb{Q}(\zeta)/\mathbb{Q}$ een *normale* uitbreiding is, het is het splijtlichaam van f_ζ waarbij alle wortels van f_ζ machten van ζ zijn. We kunnen zodoende dus volstaan met het toevoegen van één wortel aan \mathbb{Q} om een splijtlichaam te verkrijgen. Er zijn wegens voorgaande niet al te veel monomorfismen van $\mathbb{Q}(\zeta)$ naar \mathbb{C} mogelijk.¹⁴ Er zijn $p - 1$ monomorfismen mogelijk, te weten

$$\sigma_i : \mathbb{Q}(\zeta) \rightarrow \mathbb{C} : \quad \zeta \rightarrow \zeta^i$$

voor $1 \leq i \leq p - 1$. We noemen de beelden van x onder de afbeeldingen σ_i de geconjugeerden van x , dit is equivalent met de al eerder gegeven definitie, aangezien de σ_i 's homomorfismen zijn geldt $\sigma_i(f(x)) = f(\sigma_i(x))$ en als x een wortel is van een polynoom f dan is $\sigma_i(x)$ dat ook:

$$\sigma_i(f(x)) = \sigma_i(0) = f(\sigma_i(x)) = 0.$$

¹¹Vanaf nu zullen we altijd deze ringen bedoelen wanneer we verwijzen naar $\mathbb{Q}(\zeta)$ of $\mathbb{Z}[\zeta]$.

¹²i.e. injectieve homomorfismen

¹³Deze aanpak komt uit [7], paragraaf 1.8.1. Voor het criterium van Eisenstein zie [15], paragraaf 3.7.

¹⁴Voor een definitie van splijtlichaam en voor een bewijs van het feit dat het aantal monomorfismen $p - 1$ is zie [5], hoofdstuk 3 en met name lemma 3.13

Anderzijds is een wortel van het minimaalpolynoom f_x van x het beeld onder σ_i voor zekere i . Voor een $x \in \mathbb{Q}(\zeta)$ geldt namelijk dat $\mathbb{Q}(x) \subseteq \mathbb{Q}(\zeta)$ aangezien $\mathbb{Q}(\zeta)$ een lichaam is dat x bevat en $\mathbb{Q}(x)$ het kleinste lichaam is met deze eigenschap (over \mathbb{Q}). Uit galoistheorie¹⁵ weten we dat er in een lichaamsuitbreiding $\mathbb{Q}(\zeta)/\mathbb{Q}$ en voor een $x \in \mathbb{Q}(\zeta)$ er precies evenveel monomorfismen van $\mathbb{Q}(x)$ naar $\mathbb{Q}(\zeta)$ zijn als wortels van het minimaalpolynoom f_x van x . Deze monomorfismen bestaan uit het naar elkaar sturen van de wortels van f_x en er geldt dat een andere wortel van f_x wel het beeld van x onder σ_i moet zijn, voor zekere i .

In overeenstemming met al het voorgaande definiëren we de *norm* van een getal $a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2} = f(\zeta) \in \mathbb{Q}(\zeta)$ als het produkt van zijn geconjugeerden;

$$N(f(\zeta)) = \prod_{i=1}^{p-1} \sigma_i(f(\zeta)) = \prod_{i=1}^{p-1} f(\zeta^i).$$

Voor deze afbeelding geldt: $N(\alpha\beta) = N(\alpha)N(\beta)$. Verder definiëren we het *spoor* van een getal (in $\mathbb{Q}(\zeta)$) als de som van zijn geconjugeerden:

$$T(f(\zeta)) = \sum_{i=1}^{p-1} \sigma_i(f(\zeta)) = \sum_{i=1}^{p-1} f(\zeta^i).$$

Hiervoor geldt $T(a\alpha + b\beta) = aT(\alpha) + bT(\beta)$, aangezien de σ_i 's homomorfismen zijn. Voor een willekeurig element $a_{p-2}\zeta^{p-2} + \dots + a_0$ geldt:

$$T(a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0) = a_{p-2}T(\zeta^{p-2}) + \dots + T(a_0).$$

Het spoor van een getal $a \in \mathbb{Q}$ is

$$\sum_{i=1}^{p-1} \sigma_i(a) = \sum_{i=1}^{p-1} a = (p-1)a.$$

Aangezien het spoor de som is van de wortels van het minimaalpolynoom van een getal, geldt

$$T(\zeta) = T(\zeta^i) = \zeta + \dots + \zeta^{p-1},$$

dit zijn namelijk al de wortels van $f_\zeta(X) = X^{p-1} + \dots + X + 1$. Voorgaande geeft: $f_\zeta(\zeta) = \zeta^{p-1} + \dots + \zeta + 1 = 0$ en dus $T(\zeta^i) = -1$ voor $1 \leq i \leq p-1$. We kunnen het spoor van een willekeurige getal daardoor uitdrukken als

$$a_{p-2}T(\zeta^{p-2}) + \dots + T(a_0) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i = pa_0 - \sum_{i=0}^{p-2} a_i.$$

Deze norm en spoor zullen belangrijke afbeeldingen blijken te zijn, ze kunnen vaak problemen terugbrengen tot problemen in \mathbb{Q} of \mathbb{Z} . We zullen om hiervan goed gebruik te maken eerst het volgende lemma moeten behandelen.

Lemma 2.2 *Een algebraïsch getal α is geheel dan en slechts dan als zijn minimaalpolynoom f_α een element is van $\mathbb{Z}[X]$.*

Bewijs: Als $f_\alpha \in \mathbb{Z}[X]$ dan is er een polynoom in $\mathbb{Z}[X]$ waarvan α een wortel is en dus α is een algebraïsch geheel. Anderzijds als α een algebraïsch geheel is, dan is er een $f(X) \in \mathbb{Z}[X]$ met $f(\alpha) = 0$. Voor het minimaalpolynoom f_α van α geldt dat $f_\alpha(X) | f(X)$ in $\mathbb{Q}[X]$. Er geldt daardoor $f = f_\alpha g$ voor zekere $g \in \mathbb{Q}[X]$, merk

¹⁵Zie wederom [5], hoofdstuk 3.

op dat al deze polynomen monisch zijn.¹⁶ Volgens Gauss' lemma¹⁷ bestaat er een rationaal getal $\gamma \in \mathbb{Q}$ zodanig dat

$$f(X) = \gamma f_\alpha(X) \cdot \gamma^{-1} g(X),$$

waarbij $(\gamma f_\alpha(X))$ en $(\gamma^{-1} g(X))$ in $\mathbb{Z}[X]$ liggen. Aangezien f, f_α en g allen monisch zijn moet gelden $\gamma = 1$, met andere woorden $\gamma f_\alpha(X) = f_\alpha(X) \in \mathbb{Z}[X]$. \square

Wanneer we nu over een algebraïsch geheel praten, weten we dat dit equivalent is met spreken over een getal met een minimaalpolynoom in $\mathbb{Z}[X]$. Stel dat voor een getal α_1 zijn geconjugeerden $\alpha_1, \alpha_2, \dots, \alpha_r$ zijn, dan zijn dit alle wortels van het minimaalpolynoom f_α . Deze is in een zeker splijtlichaam (van f_α) te schrijven als:

$$f_\alpha(X) = \prod_{i=1}^r (X - \alpha_i) = X^r + N(\alpha)X^{r-1} + \dots + T(\alpha). \quad (7)$$

Aangezien een algebraïsche geheel een minimaalpolynoom met gehele coëfficiënten (in \mathbb{Z}) heeft, concluderen we dat zijn norm en spoor, die beide immers ook een van de coëfficiënten zijn, ook in \mathbb{Z} moeten liggen. Dit zal later gebruikt worden bij het bewijs van het feit dat de ring der gehelen in $\mathbb{Q}(\zeta)$ ook, zoals u misschien op het eerste gezicht zou vermoeden, $\mathbb{Z}[\zeta]$ is. Dit wordt bewezen aan het eind van de volgende paragraaf.

2.4 Ring van gehelen

De ring van gehelen, zoals gedefinieerd in paragraaf 2.2, heeft vooral onze aandacht. We zijn immers, in het algemeen, op zoek zijn naar oplossingen van vergelijkingen (bijvoorbeeld van FLT) in \mathbb{Z} . Daartoe factoriseren we zulke vergelijkingen in een ring van gehelen, die zelf weer in een getallenlichaam ligt. Eigenschappen als unieke factorisatie ed. zijn altijd eigenschappen in *ringen* en niet in lichamen aangezien daar elk element ($\neq 0$) een multiplicatieve inverse heeft en er daar geen niet-triviale irreducibele- en priem-elementen bestaan.

In eerste instantie is men geneigd zeggen dat in een getallenlichaam $\mathbb{Q}(\omega)$ de ring van gehelen wel $\mathbb{Z}[\omega]$ zal zijn, toch is dit niet altijd juist. Neem bijvoorbeeld de ring van Gaussische gehelen $\mathbb{Z}[i]$ in het getallenlichaam $\mathbb{Q}(i)$, dat we net zo goed kunnen schrijven als $\mathbb{Q}(2i)$; dit levert hetzelfde getallenlichaam op, terwijl $\mathbb{Z}[i]$ een andere ring is dan $\mathbb{Z}[2i]$. We zullen hier niet al te diep op ingaan¹⁸. Om te bewijzen dat $\mathbb{Z}[\zeta]$ de ring der gehelen is in het lichaam $\mathbb{Q}(\zeta)$ zullen we eerst een paar begrippen in moeten voeren.

Zij A een domein en L een lichaam dat A bevat, dan noemen we een element $\alpha \in L$ *integraal* over A ¹⁹ als er een monisch polynoom, in $A[X]$, bestaat zodanig dat α hiervan een wortel is. Zo een polynoom is dan natuurlijk deelbaar door het minimaalpolynoom f_α van α , aangezien deze f_α per definitie een voortbrenger is van het ideaal in $A[X]$ van polynomen met α als wortel (zie [10], p215). De verzameling van elementen integraal over A vormen een ring, deze zullen we de *integrale afsluiting* van A noemen.²⁰ Om dit te bewijzen (dat het inderdaad een ring is) hebben we eerst de nodige voorkennis nodig.

¹⁶Dit is belangrijk aangezien Gauss' lemma handelt over primitieve polynomen, i.e. polynomen met coëfficiënten die relatief priem zijn, en een monisch polynoom is zeker primitief.

¹⁷Zie [10], hoofdstuk 4 paragraaf 5 theorem 5.3.

¹⁸Hier is wel een boel over te zeggen zie bijvoorbeeld [14] paragraaf 2.4, wij zullen dit echter links laten liggen.

¹⁹We noemen een ring integraal over A als elk element algebraïsch over A is.

²⁰In hoofdstuk 5 lemma 5.3 zullen we zelfs bewijzen dat wanneer A algebraïsch over B is, en B een lichaam, dat dan ook A een lichaam moet zijn.

We zullen de aanpak uit [12], p21-22 volgen. Hierin bewijst J.S.Milne eerst dat elk symmetrisch polynoom te schrijven is als polynoom in de *elementaire symmetrische polynomen*. We noemen een polynoom symmetrisch als een permutatie van de variabelen hetzelfde polynoom oplevert, dus voor elke permutatie $\sigma \in \text{Sym}_r$, geldt

$$P(X_1, X_2, \dots, X_r) = P(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(r)}),$$

hierbij is Sym_r de groep van permutaties van r elementen, ofwel de symmetrische groep van orde $r!$. De *elementaire symmetrische polynomen* worden gedefinieerd als:

$$\begin{aligned} S_1 &= \sum X_i &&= X_1 + X_2 + \dots + X_r \\ S_2 &= \sum_{i < j} X_i X_j &&= X_1 X_2 + X_1 X_3 + \dots + X_{r-1} X_r \\ \vdots &= \vdots \\ S_r &= X_1 X_2 \dots X_r. \end{aligned}$$

Wat nu bewezen wordt in [12], p21 is dat elk symmetrisch polynoom

$$P(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$$

te schrijven is als polynoom in de elementaire symmetrisch polynomen met coëfficiënten in A , oftewel:

$$P \in A[S_1, \dots, S_r].$$

Dit is van belang omdat we zullen laten zien dat bepaalde elementaire symmetrische polynomen alleen waarden in A aannemen en wegens bovenstaande dit dan geldt voor elk symmetrisch polynoom van die soort, elementair of niet.

Zij $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in A[X]$ een polynoom met wortels $\alpha_1, \dots, \alpha_n$ in een zeker lichaam dat A bevat. Aangezien $f(X)$ in in dit lichaam te schrijven is als:

$$f(X) = \prod (X - \alpha_i)$$

verkrijgen we wanneer we dit uitwerken:

$$a_1 = -S_1(\alpha_1, \dots, \alpha_n), \quad a_2 = S_2(\alpha_1, \dots, \alpha_n), \quad a_n = (-1)^n S_n(\alpha_1, \dots, \alpha_n).$$

Aangezien f een polynoom in $A[X]$ is geldt $S_i(\alpha_1, \dots, \alpha_n) \in A$. Dus een elementair symmetrisch polynoom in de wortels van een polynoom in A , ligt wederom in A . Wegens voorgaande geldt dit voor elk symmetrisch polynoom in de wortels van een $f \in A[X]$.

Lemma 2.3 *De integrale afsluiting van een ring A , in een lichaam L dat A omvat, is wederom een ring.*

Bewijs: Stel α en β zijn 2 elementen in de afsluiting van A , we zullen bewijzen dat $\alpha + \beta$ dit ook is, $\alpha - \beta$ en $\alpha\beta$ gaan op dezelfde manier.

Aangezien α integraal over A is, is het een wortel van een zeker polynoom

$$f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in A[X]$$

met wortels $\alpha_1, \dots, \alpha_n \in L$. Evenzo geldt voor β dat het de wortel is van een zeker polynoom

$$g(X) = X^m + b_1 X^{m-1} + \dots + b_m \in A[X]$$

met wortels $\beta_1, \dots, \beta_m \in L$. Definieer $\gamma_1, \dots, \gamma_{mn}$ als

$$\gamma_1 = \alpha_1 + \beta_1, \gamma_2 = \alpha_1 + \beta_2, \dots, \gamma_{mn} = \alpha_n + \beta_m.$$

Hiermee construeren we het polynoom

$$h(X) = \prod (X - \gamma_i)$$

en we claimen dat dit polynoom in $A[X]$ ligt.

De coëfficiënten van h zijn symmetrisch in α_i en β_i aangezien de verzameling $\{\gamma_1, \dots, \gamma_{mn}\}$ hierin "symmetrisch" is (dat wil zeggen niet verandert door een permutatie van α_i of β_i). Zij c_i een willekeurige coëfficiënt van $h(X)$, dit is dan een elementair symmetrisch polynoom in de γ_i 's en symmetrisch in de α_i 's en β_i 's, dus

$$c_i = S_i(\gamma_1, \dots, \gamma_{mn}) = P(\alpha_1, \dots, \beta_m)$$

voor een zeker symmetrisch polynoom P . Beschouw nu P als een polynoom in de variabelen β_1, \dots, β_m , dus

$$P(\beta_1, \dots, \beta_m) \in A[\alpha_1, \dots, \alpha_n][X_1, \dots, X_m].$$

Nu zijn de coëfficiënten van dit polynoom in $A[\alpha_1, \dots, \alpha_n]$ symmetrisch in de α_i 's, anders zou $P(\alpha_1, \dots, \beta_m)$ hier ook niet symmetrisch in kunnen zijn. Aangezien de α_i 's, per definitie, zelf wortels zijn van het polynoom $f(X)$ in A geldt dat deze coëfficiënten van $P(\beta_1, \dots, \beta_m)$ in A moeten liggen, het zijn zelf namelijk symmetrische polynomen in de wortels van een polynoom in A . Maar dan is $P(\alpha_1, \dots, \beta_m)$ een symmetrisch polynoom in de β_i 's met coëfficiënten in A , maar ook de β_i 's zijn wortels van een polynoom in A , en volgens dezelfde redenering moeten dan de coëfficiënten in A liggen.

Dit geeft een monisch polynoom in $A[X]$, namelijk $h(X)$, zodanig dat $\alpha + \beta$ hiervan een wortel is. Er geldt namelijk $\alpha + \beta = \alpha_i + \beta_j$ voor zekere i, j en dit geeft:

$$\begin{aligned} h(\alpha + \beta) &= \prod_k \left((\alpha_i + \beta_j) - \gamma_k \right) = \left((\alpha_i + \beta_j) - (\alpha_1 + \beta_1) \right) \cdots \\ &\quad \left((\alpha_i + \beta_j) - (\alpha_i + \beta_j) \right) \cdots \left((\alpha_i + \beta_j) - (\alpha_n + \beta_m) \right) = 0. \end{aligned}$$

Hieruit concluderen we dat ook $\alpha + \beta$ een element is van de algebraïsche afsluiting van A .²¹ We concluderen dat de algebraïsche afsluiting van een ring A zelf ook een ring is. \square

We hebben voorgaande behandeld omdat in een lichaamsuitbreiding K/\mathbb{Q} de ring van gehelen de algebraïsche afsluiting van \mathbb{Z} is. Deze ring van gehelen is dus ook daadwerkelijk een ring, wegens bovenstaande. Nu willen we bewijzen dat deze ring der gehelen $\mathbb{Z}[\zeta]$ is. Tot nu toe weten we immers alleen dat een algebraïsche geheel *voldoet* aan een polynoomvergelijking in $\mathbb{Z}[X]$, wat zo een getal *is* weten we nog niet.²²

Stelling 2.1 *De ring van gehelen in $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$.*

Bewijs:²³ Voor het gemak zullen we de volgende notatie invoeren; de ring van gehelen noteren we met \mathcal{O} . We willen dus bewijzen dat $\mathcal{O} = \mathbb{Z}[\zeta]$. Evident is

²¹We kunnen dezelfde resultaten ook voor $\alpha - \beta$ en $\alpha\beta$ verkrijgen door in die gevallen respectievelijk $\gamma_{i,j} = \alpha_i - \beta_j$ of $\gamma_{i,j} = \alpha_i\beta_j$ te definiëren.

²²Ik weet niet of het goed is om te suggereren dat het voldoen aan een polynoomvergelijking "alleen maar een eigenschap is" terwijl het behoren tot een bepaalde verzameling iets wezelijks anders is; iets dat zijn existentie vastlegt, uiteindelijk is dat ook "maar" een eigenschap. Wat ik bedoel is dat we nu, na deze stelling weten hoe we het (algebraïsch) getal op kunnen schrijven in termen van ζ en getallen uit \mathbb{Z} .

²³Voor dit bewijs heb ik [14], theoreem 3.5 gebruikt.

$\mathbb{Z}[\zeta] \subseteq \mathcal{O}$ omdat zowel ζ als $a_i \in \mathbb{Q}$ in \mathcal{O} liggen en dit wegens lemma 2.3 een ring is. We willen dus bewijzen $\mathcal{O} \subseteq \mathbb{Z}[\zeta]$. Stel²⁴

$$x = a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0$$

is een geheel in $\mathbb{Q}(\zeta)$ dan willen we aantonen dat $a_i \in \mathbb{Z}$ voor alle $0 \leq i \leq p-2$. Hier zal de rest van het bewijs naar toe werken.

Aangezien de ring der geheelen een ring is en ζ^i een geheel, zijn minimaalpolynoom is namelijk $X^{p-1} + \dots + X + 1$, moet ook het getal $x\zeta^{-k} - x\zeta$ een geheel zijn, $0 \leq k \leq p-2$. Zijn spoor is:

$$\begin{aligned} T(x\zeta^{-k} - x\zeta) &= T(a_{p-2}\zeta^{p-2-k} + \dots + a_0\zeta^{-k} - a_{p-2}\zeta^{p-1} - \dots - a_0\zeta) \\ &= T(a_k) + T(\zeta)(a_{p-2} + \dots + a_{k+1} + a_{k-1} + \dots + a_0) - \\ &\quad T(\zeta)(a_{p-2} + \dots + a_0) \\ &= (p-1)a_k - (a_{p-2} + \dots + a_{k+1} + a_{k-1} + \dots + a_0) + \\ &\quad (a_{p-2} + \dots + a_0) \\ &= pa_k - (a_{p-2} + \dots + a_0) + (a_{p-2} + \dots + a_0) \\ &= pa_k \end{aligned} \tag{8}$$

Dit moet een geheel getal zijn (in \mathbb{Z}), zie vergelijking (7), noem dit getal $b_k = pa_k$. Merk op dat we hier gebruikt hebben dat $T(\zeta^i) = T(\zeta)$, deze rekenregels zijn behandeld in paragraaf 2.3. We schrijven $\pi = \zeta - 1$, deze transformatie levert ons op:

$$\begin{aligned} px &= pa_{p-2}\zeta^{p-2} + \dots + pa_0 \\ &= b_{p-2}\zeta^{p-2} + \dots + b_0 \\ &= b_{p-2}(1 + \pi)^{p-2} + \dots + b_0. \end{aligned}$$

Met behulp van het binomium van Newton, kunnen we dit uitwerken:

$$\begin{aligned} px &= b_{p-2} \left[\binom{p-2}{0} \pi^0 + \binom{p-2}{1} \pi^1 + \dots + \binom{p-2}{p-2} \pi^{p-2} \right] + \\ &\quad \dots + b_1 \left[\binom{1}{0} \pi^0 + \binom{1}{1} \pi^1 \right] + b_0. \end{aligned}$$

Wanneer we gelijke termen samennemen verkrijgen we:

$$px = c_{p-2}\pi^{p-2} + \dots + c_0. \tag{9}$$

Voor de coëfficiënten b_i en c_i gelden de relaties:

$$\begin{aligned} c_i &= \sum_{j=i}^{p-2} \binom{j}{i} b_j \in \mathbb{Z} \\ b_i &= \sum_{j=i}^{p-2} \binom{j}{i} c_j \in \mathbb{Z}. \end{aligned} \tag{10}$$

Deze tweede vergelijking volgt uit het feit dat andersom ook geldt: $\zeta = \pi + 1$ en we op dezelfde manier dit kunnen substitueren en uitwerken.

Stel dat al deze c_i deelbaar zijn door p , dan zijn wegens bovenstaande ook alle b_i deelbaar door p en er geldt $a_i = \frac{b_i}{p} \in \mathbb{Z}$, oftewel $x \in \mathbb{Z}[\zeta]$ en we zijn klaar.

²⁴Herinner dat $\{\zeta^{p-2}, \dots, \zeta, 1\}$ een basis is voor $\mathbb{Q}(\zeta)$.

We willen nu aantonen dat alle c_i deelbaar zijn door p . We zullen dit bewijzen door inductie naar i . De uitspraak is zeker waar voor c_0 ; wanneer we namelijk het spoor van x uitwerken, op dezelfde manier als vergelijking (8) verkrijgen we, wederom met behulp van vergelijking (7):

$$T(x) = pa_0 - \sum_{i=0}^{p-2} a_i \in \mathbb{Z},$$

aangezien $b_0 = pa_0$ in \mathbb{Z} ligt moet dit ook voor het tweede gedeelte gelden, uit vergelijking (10) verkrijgen we:

$$c_0 = p \sum_{i=0}^{p-2} a_i \in \mathbb{Z},$$

en we zien dat c_0 deelbaar door p is.

We zullen nu aannemen dat c_i deelbaar is door p voor alle $i \leq k-1$ en bewijzen dat dan c_k ook deelbaar door p moet zijn.

We kunnen het minimaalpolynoom van ζ schrijven als

$$\begin{aligned} f_\zeta(X) &= X^{p-1} + \dots + X + 1 \\ &= (X - \zeta^{p-1}) \dots (X - \zeta^2)(X - \zeta). \end{aligned}$$

Wanneer we dit combineren met het feit dat $\sigma_i(1 - \zeta) = (1 - \zeta^i)$, verkrijgen we:

$$\begin{aligned} N(1 - \zeta) &= \prod_{i=1}^{p-1} (1 - \zeta^i) \\ &= f_\zeta(1) \\ &= 1^{p-1} + 1^{p-2} + \dots + 1 \\ &= p \end{aligned} \tag{11}$$

We kunnen $1 - \zeta^i$ schrijven als $(1 - \zeta)(1 + \zeta + \dots + \zeta^{i-1})$, dit geeft aanleiding tot de volgende uitdrukking:

$$\begin{aligned} p &= \prod_{i=1}^{p-1} (1 - \zeta^i) \\ &= (\zeta - 1)^{p-1} (-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1}) \\ &= \pi^{p-1} \kappa. \end{aligned} \tag{12}$$

Hierbij geldt $\kappa \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}$. We zullen nu vergelijking (9) modulo het ideaal $\langle \pi^{k+1} \rangle$ in \mathcal{O} bekijken.²⁵ Als eerste verkrijgen we uit voorgaande vergelijking (11) dat $p \equiv 0 \pmod{\pi^{k+1}}$ en dus

$$px \equiv c_{p-2}\pi^{p-2} + \dots + c_0 \equiv 0 \pmod{\pi^{k+1}}, \quad k < p. \tag{13}$$

We hadden aangenomen dat c_i met $i \leq k-1$ deelbaar door p is en dus 0 modulo $\langle \pi^{k+1} \rangle$ is. De termen $c_{k+1}\pi^{k+1}, c_{k+2}\pi^{k+2}, \dots$ zijn veelvouden van π^{k+1} en dus ook

²⁵Aangezien $\pi^{k+1} \in \mathcal{O}$ brengt dit inderdaad een ideaal in \mathcal{O} voort. Een voorbeeld van een polynoomvergelijking in \mathbb{Z} waaraan π voldoet is $(X+1)^p - 1$.

0 modulo $\langle \pi^{k+1} \rangle$, dus bijna alle termen uit vergelijking 13 zijn congruent nul, we concluderen:

$$px \equiv c_k \pi^k \equiv 0 \pmod{\pi^{k+1}}. \quad (14)$$

Met andere woorden, er is een $\mu \in \mathcal{O}$ zodanig dat:

$$c_k \pi^k = \mu \pi^{k+1}.$$

We concluderen: $c_k = \mu \pi$, aangezien c_k in \mathbb{Z} ligt kennen we zijn norm:

$$N(c_k) = c_k^{p-1} = N(\mu)N(\pi) = pN(\mu),$$

de norm van π is p wegens (11), dit is een priemgetal. We hebben nu $p|c_k^{p-1}$ in \mathbb{Z} met p priem, we concluderen $p|c_k$. Dit geeft, zoals al eerder opgemerkt dat $a_k \in \mathbb{Z}$ en dus $\mathcal{O} \subseteq \mathbb{Z}[\zeta]$. Oftewel de ring der gehelen \mathcal{O} is $\mathbb{Z}[\zeta]$. \square

2.5 Unieke factorisatie in irreducibelen en priemen

Zoals we al gezien hebben in hoofdstuk 1 paragraaf 2 is het al dan niet aanwezig zijn van unieke priemfactorisatie eigenschappen in de desbetreffende ringen $\mathbb{Z}[\zeta]$ van cruciaal belang voor de aanpak van FLT. Alleen op deze manier kunnen we aantonen dat de factoren $(x + \zeta^i y)$ p^{de} -machten zijn en hieruit een tegenspraak afleiden. We zullen eerst factorisatie in irreducibelen behandelen en daarna zullen we net als in \mathbb{Z} getallen in $\mathbb{Z}[\zeta]$ proberen te factoriseren in priemen, later zullen we, in hoofdstuk 5, dit uitbreiden naar factorisatie in idealen.

2.5.1 Factorisatie in irreducibelen

Een domein heet *Noethers*²⁶ als elk ideaal hierin gegeneerd wordt door een eindige verzameling. Dus stel dat $\mathfrak{a} \subseteq D$ een ideaal is in een Noethers domein D , dan bestaan er $x_i \in D$ zodanig dat $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$. We zullen zonder bewijs aannemen dat de ring der gehelen in een getallenlichaam Noethers is.²⁷

Lemma 2.4 *In een Noethers domein D (bijvoorbeeld de ring der gehelen in een getallenlichaam) is factorisatie in irreducibelen mogelijk.*

Bewijs: Stel van niet, dan bestaat er een $x \in D$ met x ongelijk 0, geen eenheid, reducibel²⁸ en zonder factorisatie in irreducibele factoren. Kies x zodanig dat het ideaal $\langle x \rangle$ maximaal is²⁹. Aangezien x reducibel is bestaan er y en z zodat $x = yz$, met x, y geen eenheden. Aangezien $y|x$ moet gelden $\langle y \rangle \subseteq \langle x \rangle$ want elk element $\tilde{x} \in \langle x \rangle$ is te schrijven als $\tilde{x} = dx$ met $d \in D$, maar dit is op zijn beurt te schrijven als $\tilde{x} = dx = dzy$ waarbij $dz \in D$; ofwel $\tilde{x} \in \langle y \rangle$. Er kan niet gelden $\langle y \rangle = \langle x \rangle$ want dat zou volgens bovenstaande redenering betekenen dat $x|y$ én $y|x$ ofwel x en y verschillen op zijn hoogst met een eenheid: $x = uy$. Dit betekent dat z een eenheid moet zijn, dit kan niet. Dus er geldt de strikte implicatie $\langle y \rangle \subsetneq \langle x \rangle$. Volgens dezelfde redenering verkrijgen we $\langle z \rangle \subsetneq \langle x \rangle$. Maar aangezien $\langle x \rangle$ het grootste ideaal is waarvan de voortbrenger *niet* te schrijven is als produkt van irreducibelen, geeft dit

²⁶genoemd naar Emmy Noether

²⁷Een bewijs is te vinden in [14], Theorem 4.7

²⁸Als x irreducibel is dan zijn we klaar, we hebben dan een tegenspraak want x is dan zijn eigen factorisatie.

²⁹Dit kan ook inderdaad, uit het feit dat het domein Noethers is volgt dat elk ideaal eindig voortgebracht is, dus dat de ketting van inclusies $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ uiteindelijk moet stoppen (stabiliseert), er is een N zodanig dat $\mathfrak{a}_n = \mathfrak{a}_{n+1}$ voor alle $n > N$. Voor een bewijs dat een niet-lege verzameling idealen in een Noethers domein een maximaal element heeft zie [14], paragraaf 4.3 "The maximal condition".

dat y en z wel te schrijven moeten zijn als produkt van irreducibelen: $y = p_1 \dots p_n$ en $z = q_1 \dots q_m$. Dit geeft dan een factorisatie in irreducibel van x :

$$x = yz = p_1 \dots p_n q_1 \dots q_m,$$

maar dit kan niet, wegens de vooronderstelling op x . We concluderen dat er geen $x \in D$ bestaat die niet te schrijven is als produkt van irreducibelen. \square

2.5.2 Factorisatie in priemmen

Om factorisatie in priemmen te behandelen, zullen we eerst het begrip *Euclidisch domein* in moeten voeren, er geldt namelijk dat in een Euclidisch domein elk irreducibel element ook priem is. Wanneer we dan wegens voorgaande paragraaf een factorisatie in irreducibelen verkrijgen, is dit in wezen een factorisatie in priemmen. Dan moet natuurlijk nog aangetoond worden dat zo een factorisatie uniek is.

We noemen een domein D *Euclidisch* als er een afbeelding $N : \phi \rightarrow \mathbb{Z}$ bestaat zodanig dat $\phi(x) \geq 0$ voor alle $x \in D$ en $\phi(0) = 0$. Verder moeten er voor gegeven $x, y \in D$ met $y \neq 0$ elementen r, d bestaan zodanig dat $x = yd + r$ met $r = 0$ of $\phi(r) < \phi(y)$. Zo een afbeelding ϕ noemen we een norm op D . De laatste voorwaarde betekent precies dat het gebruik van het Euclidisch algoritme op dit domein mogelijk is.

Er zijn verschillende voorbeelden van Euclidische domeinen, bijvoorbeeld \mathbb{Z} met de afbeelding $x \rightarrow |x|$, $\mathbb{Z}[i]$ met de afbeelding $a + bi \rightarrow a^2 + b^2$, of een polynoomring over een lichaam K , met de afbeelding $f \in K[X] \rightarrow \deg(f)$.

Lemma 2.5 *In een Euclidisch domein D is elk irreducibel element priem.*

Bewijs:³⁰ Stel $x \in D$ met $x \neq 0$ en $x|ab$ dan willen we aantonen dat $x|a$ of $x|b$, aangezien dit een priem defineert.³¹ Stel $\phi(b) = 0$, ϕ is een norm op D , dan moet gelden dat b een eenheid is: als we schrijven $1 = bq + r$ moet gelden $r = 0$ of $\phi(r) < \phi(b)$, dit laatste is onmogelijk aangezien $\phi(b) = 0$ en $\phi(r) \geq 0$, dus er moet gelden $1 = bq$ en b heeft een multiplicatieve inverse (namelijk q) en is zodoende een eenheid. Als dit het geval is moet gelden $x|a$, aangezien $x|ab \Leftrightarrow xc = ab$ voor zekere $c \neq 0$, omdat b een eenheid is geldt: $a = xcb^{-1}$ en we zien $x|a$.

We zullen inductie naar $\phi(b)$ gebruiken, we hebben nu het geval $\phi(b) = 0$ bewezen en zullen vanaf nu aanemen dat de uitspraak waar is voor $x|ac$ met $\phi(c) < \phi(b)$, de uitspraak is dus dat $x|a$ of $x|c$. De inductiestap zal er uit bestaan te bewijzen dat de uitspraak waar is voor $x|ab$. Merk op dat inductie inderdaad geoorloofd is aangezien ϕ waarden in \mathbb{N} aanneemt.

We schrijven $x = bq + r$ met $r = 0$ of $\phi(r) < \phi(b)$, in het geval $r = 0$ zijn we klaar, de irreducibiliteit van x dwingt q of b een eenheid te zijn en $x|b$ of $x|a$ respectievelijk wegens eerder gegeven redenering. We nemen dus aan $r \neq 0$. Wanneer we de vergelijking $x = bq + r$ met a vermenigvuldigen verkrijgen we $ax = abq + ar$ en $ax - abq = ar$, met $x|ab$, oftewel $x|ar$. Omdat $\phi(r) < \phi(b)$ en de uitspraak wegens onze inductie-aanname waar is voor deze gevallen geldt $x|a$ of $x|r$ in het eerste geval zijn we klaar.

Neem dus aan $x|r$ en schrijf $b = rq' + s$ met wederom $s = 0$ of $\phi(s) < \phi(r)$. In het geval $s = 0$ zijn we klaar, er geldt $r|b$ en $x|r$ dus ook $x|b$. We nemen dus aan $\phi(s) < \phi(r) < \phi(b)$, wanneer we $b = rq' + s$ met a vermenigvuldigen geeft dit: $ab = arq' + as$ en dus ook $x|as$ aangezien $x|ab, x|r$. Met dezelfde redenering als bij het geval $x|ar$ concluderen we $x|a$, en we zijn klaar, of $x|s$. In het laatste geval zien we dat omdat $b = rq' + s$ en $x|r$ en $x|s$ dat ook $x|b$. \square

³⁰Voor dit bewijs heb ik [2], lecture 2 gebruikt.

³¹zie eventueel paragraaf 2.2 voor de definitie.

Factorisatie in priemmen is dus mogelijk in een Euclidisch domein, zo een factorisatie is zelfs uniek.

Lemma 2.6 *In een domein is een factorisatie in priemelementen uniek.*

Bewijs: Stel van niet, stel dat er 2 priemfactorisaties van hetzelfde element bestaan, dan hebben we $f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m$, aangezien alle f_i en g_i priem zijn geldt $f_1 | g_i$ voor zekere i , we kunnen de termen in het rechterlid zo ordenen dat geldt: $i = 1$, dus $f_1 | g_1$, aangezien beide priem zijn moet gelden $f_1 = u g_1$ voor een eenheid u . Wanneer we dit uitwerken krijgen we $f_1 (f_2 \cdots f_n - g_2 \cdots g_m) = 0$ ³² in een domein betekent dit dat $f_2 \cdots f_n = g_2 \cdots g_m$ dit kan niet zo doorgaan aangezien n, m eindig zijn en we verkrijgen uiteindelijk $f_n = g_m$ en vanuit daar kunnen we de reeks terug gaan: uit $f_{n-1} f_n = g_{m-1} g_m$ volgt dan $f_{n-1} = g_{m-1}$, etc. oftewel $m = n$ en $f_i = g_i$ voor alle i . \square

Het is ook mogelijk, zoals we al in paragraaf 1.3 gedaan hebben voor $\mathbb{Z}[i]$, om eerst te bewijzen dat een Euclidisch domein een PID³³ is en dat voor een PID geldt, dat het een unieke factorisatie domein (UFD) is. Het bewijs van het feit, dat een Euclidisch domein D een PID is, is niet moeilijk. Het kan op dezelfde manier als lemma 1.2 voor $\mathbb{Z}[i]$: je kiest een element $x \in D$ zodanig dat zijn norm $\phi(x)$ minimaal is. Voor een willekeurig element $y \in D$ geldt $y = xd + r$ voor zekere d, r . We kunnen niet hebben dat $\phi(r) < \phi(x)$ aangezien we deze minimaal hebben verondersteld, dus $r = 0$ en y is een veelvoud van x , en we concluderen $D = \langle x \rangle$. De tweede uitspraak, namelijk dat elk PID een UFD is zullen we in een lemma behandelen, aangezien dit al in paragraaf 1.3 beloofd is.

Lemma 2.7 *Een hoofdideaal-domein (PID) D is een unieke factorisatie domein (UFD).*

Bewijs: D Is zeker een Noethers domein; elk ideaal wordt immers door 1 element voortgebracht en dat is zeker eindig. Dit impliceert, zie paragraaf 2.5.1, dat factorisatie in irreducibelen mogelijk is. We zullen aantonen dat elke irreducibele factor een priem is. Zoals al eerder opgemerkt, moet zo een factorisatie in priemmen uniek zijn. Zij p een irreducibel getal in D , het ideaal $\langle p \rangle$ is maximaal in D , dit wil zeggen, er is geen ideaal $\mathfrak{a} \subseteq D$ met $\mathfrak{a} \neq \langle p \rangle$, D zodanig dat $\langle p \rangle \subset \mathfrak{a} \subset D$. Stel van wel, dan zou de voortbrenger³⁴ van \mathfrak{a} een deler van p moeten zijn en dat kan niet want p is irreducibel. Stel $p | ab$ en $p \nmid a$, we willen bewijzen dat dan $p | b$ en dus dat p priem is. Het feit dat $p \nmid a$, impliceert dat $\langle p, a \rangle \supsetneq \langle p \rangle$ en dus $\langle p, a \rangle = D$, aangezien $\langle p \rangle$ maximaal was verondersteld. Dus ook $1 \in D = \langle p, a \rangle$, met andere woorden: er bestaan c, d zodanig dat $1 = cp + da$. Wanneer we dit met b vermenigvuldigen, verkrijgen we $b = bcp + dab$. Omdat $p | ab$, moet ook gelden $p | b$; ofwel p is priem. \square

³²Herinner de opmerking aan het eind van de tweede alinea in paragraaf 1.2 waarin zowel g als ug een priem wordt genoemd, je deelt als het ware uit naar eenheden.

³³Herinner, PID komt van Principal Ideal Domain, oftewel een domein waarin elk ideaal een hoofdideaal is

³⁴Herinner dat elk ideaal een hoofdideaal is in een PID.

2.6 Aanpak van de laatste stelling van Fermat in een unieke factorisatie domein.

Stel dat we weten dat $\mathbb{Z}[\zeta]$ een UFD is, dit is inderdaad zo voor ζ een primitieve oplossing van $X^p - 1 = 0$ met $p < 23$, hoe kunnen we dan verder? Het idee is net als bij het geval $n = 2$, met het verschil dat we nu aantonen dat er *geen* oplossingen zijn. Voor we dit uitwerken is het goed om een overzicht van de verschillende gevallen te zien.

- Voor $p = 2$ zijn er oneindig veel oplossingen; de zogenaamde Pythagoreïsche drietallen.
- Voor $p = 3$ zijn er geen oplossingen, hiervoor bestaat een elementair bewijs van Euler³⁵.
- Voor $p = 4$ bestaan er ook geen oplossingen dit zullen we bewijzen in lemma 2.8 hier vlak na.

Het is daarom voldoende om te kijken naar de gevallen waarin p een oneven priem is: voor alle even n geldt namelijk $n = 2n'$ met n' even of oneven, in het eerst geval geldt $4|n$ en er bestaan geen oplossingen³⁶ $x^n + y^n = z^n$. In het tweede geval bestaan er ook geen oplossingen want we zullen bewijzen dat er geen zijn voor p een oneven priem.³⁷

Dit zullen we doen door naar twee gevallen uit te splitsen het zogenaamde *eerste geval* waarbij $p \nmid xyz$ en het *tweede geval* waarbij $p \mid xyz$. Deze gevallen zullen in de gelijknamige hoofdstukken behandeld worden. Hierbij zal vergelijking (1) op de manier van vergelijking (2) gefactoriseerd worden en zullen we aantonen, net als bij $n = 2$ dat de factoren $(x + \zeta^i y)$ allen p^{de} machten zijn, wegens unieke factorisatie in $\mathbb{Z}[\zeta]$ (op eenheden na).

We hebben al opgemerkt dat $\mathbb{Z}[\zeta]$ niet een UFD is voor alle p , we zullen later dan ook op een andere manier $(x + \zeta^i y) = ua^p$ proberen te verkrijgen en zo de stelling nog bredere geldigheid verlenen. Hier zal hoofdstuk 5 over gaan.

Lemma 2.8 *Er bestaan geen oplossingen van $x^4 + y^4 = z^4$, $xyz \neq 0$ in \mathbb{Z} .*

Bewijs:³⁸ Stel dat er wel zo een oplossing bestaat dan is x^2, y^2, z^2 een oplossing van $x^2 + y^2 = z^2$ en x, y, z^2 een oplossing van $x^4 + y^4 = w^2$, kies x, y, w zodanig dat w in deze oplossing minimaal is. Aangezien x^2, y^2, w een oplossing is van $x^2 + y^2 = z^2$ is het een Pythagoreïsch drietal en zodoende van de vorm:

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad w = m^2 + n^2.$$

We veronderstellen dat n, m relatief priem zijn, anders zouden x, y, z een factor gemeen hebben en niet een primitieve oplossing zijn.³⁹ Verder zien we dat n en m niet beide even of oneven kunnen zijn aangezien x oneven moet zijn wegens lemma 1.3. Wanneer we naar voorgaande vergelijking kijken valt op dat $x^2 + n^2 = m^2$ en dat dus ook x, n, m een Pythagoreïsch drietal is. Er bestaan r, s met alle voorgaande eigenschappen, zodanig dat:

$$x = r^2 - s^2, \quad n = 2rs, \quad m = r^2 + s^2.$$

³⁵Een uitgebreide versie van het bewijs voor $n = 3$ is te vinden in [6], paragraaf 13.4, p192-195 theoreem 227.

³⁶Herinner dat dit anders een oplossing $x^{\frac{n}{4}}, y^{\frac{n}{4}}, z^{\frac{n}{4}}$ van $x^4 + y^4 = z^4$ zou geven en dat is onmogelijk.

³⁷Aangezien een oneven getal n' altijd een oneven priemfactor heeft, zou het bestaan van een oplossing x, y, z van $x^{2n'} + y^{2n'} = z^{2n'}$ ook het bestaan van een oplossing $x^{\frac{2n'}{p}}, y^{\frac{2n'}{p}}, z^{\frac{2n'}{p}}$ van $x^p + y^p = z^p$ geven, met p een oneven priem, dit is onmogelijk.

³⁸Hiervoor heb ik [11], excersise 15 van hoofdstuk 1 gebruikt.

³⁹In zo een geval delen we de betreffende factor uit om wel een primitieve oplossing te krijgen.

Omdat n, m relatief priem zijn moeten ook r, s, m paarsgewijs priem zijn, anders zou uit het tweede deel van bovenstaande vergelijking volgen dat wanneer bijvoorbeeld r een factor met m gemeen had, n deze factor ook met m gemeen moet hebben en dat kan niet, verder wisten we al dat r, s relatief priem zijn. Wanneer we dit resultaat combineren met bovenstaande 2 vergelijkingen verkrijgen we: $y^2 = 4rsm$ en uit het paarsgewijs priem zijn van r, s, m volgt dat ze allen een kwadraat moeten zijn, aangezien ze een kwadraat delen; stel namelijk dat p een priemfactor is die y deelt, dan $p^2|y^2$ en p^2 deelt $4, r, s$ of m .⁴⁰ We noteren r, s, m respectievelijk als a^2, b^2 en c^2 . Uit $m = r^2 + s^2$ concluderen we $a^4 + b^4 = c^2$, oftewel a, b, c is een andere oplossing, naast x^2, y^2, w van de vergelijking $x^4 + y^4 = w^2$, in de tweede oplossing was w minimaal verondersteld, aangezien $w = m^2 + n^2 = c^2 + 4r^2s^2$ en $4r^2s^2 > 0$ concluderen we $c^2 < w$. We hebben $m, n \neq 0$ en dus $w \neq 0$, verder, omdat $w, c \in \mathbb{Z}$ moet gelden $c < w$. We hebben een oplossing a, b, c die kleiner is dan de minimale oplossing x^2, y^2, w , dit kan niet, we concluderen dat er geen oplossingen van FLT voor $n = 4$ bestaan. \square

⁴⁰Ook het geval $p = 2$ gaat goed; wanneer y een factor 2^k bevat geldt dat en van r, s of m een factor $2^{2(k-1)} = (2^{k-1})^2$ bevat.

3 Het eerste geval

In dit hoofdstuk veronderstellen we dat $\mathbb{Z}[\zeta]$ een UFD is, dit is zeker het geval voor $p < 23$. Later zullen we hier uitbreidingen voor zien, maar het bewijs zal ongeveer hetzelfde blijven.

Een algebraïsch getal α kunnen we schrijven als

$$\alpha = a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0.$$

Aangezien ζ^i met $0 \leq i \leq p-2$ een eenheid is, is het alleen deelbaar door een andere eenheid. Wanneer $p|\alpha$ moet⁴¹ ook gelden dat $p|a_i$, aangezien $p \nmid \zeta^i$.

We zullen een paar eigenschappen van modulo p rekenen in $\mathbb{Z}[\zeta]$ afleiden. Stel dat $\alpha \equiv \beta \pmod{p}$, dus modulo het ideaal $\langle p \rangle$ in $\mathbb{Z}[\zeta]$. Er geldt dan $\alpha = \beta + \gamma p$ voor een zekere $\gamma \in \mathbb{Z}[\zeta]$. Het monomorfisme

$$\sigma_{-1} : \mathbb{Z}[\zeta] \rightarrow \mathbb{Z}[\zeta] : \zeta \rightarrow \zeta^{-1} = \zeta^{p-1}$$

is de bekende complexe conjugatie op $\mathbb{Z}[\zeta] \subset \mathbb{C}$, en we zullen de complex geconjugeerde van een getal x , zoals gebruikelijk, noteren met \bar{x} . Er geldt

$$\bar{\alpha} = \overline{\beta + \gamma p} = \bar{\beta} + \bar{\gamma} p,$$

want $p \in \mathbb{Z}$ en dus $\bar{p} = p$, dit geeft ons:

$$\alpha \equiv \beta \pmod{p} \iff \bar{\alpha} \equiv \bar{\beta} \pmod{p}.$$

De uitdrukking $(\alpha + \beta)^p$ kunnen we schrijven als:

$$\binom{p}{0} \alpha^p \beta^0 + \binom{p}{1} \alpha^{p-1} \beta^1 + \dots + \binom{p}{p} \alpha^0 \beta^p$$

al de binominaalcoëfficiënten, behalve $\binom{p}{0} = \binom{p}{p} = 1$, zijn een veelvoud van p . De uitdrukking $(\alpha + \beta)^p$ is modulo p dus drastisch te vereenvoudigen:

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod{p}.$$

Dit is met volledige inductie uit te breiden tot sommen van willekeurige lengte: het geval $k = 2$ hebben we zojuist bewezen, stel dat de uitspraak waar is voor $k - 1$ dan ook voor k , aangezien

$$\begin{aligned} (\alpha_1 + \dots + \alpha_k)^p &\equiv ((\alpha_1 + \dots + \alpha_{k-1}) + \alpha_k)^p \\ &\equiv (\alpha_1 + \dots + \alpha_{k-1})^p + \alpha_k^p \\ &\equiv \alpha_1^p + \dots + \alpha_k^p \pmod{p}. \end{aligned}$$

Straks zullen we getallen van de vorm α^p tegenkomen, deze zijn met behulp van bovenstaande informatie te schrijven als:

$$\begin{aligned} \alpha^p &\equiv (a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0)^p \\ &\equiv a_{p-2}^p \zeta^{p(p-2)} + \dots + a_1^p \zeta^p + a_0^p \\ &\equiv a_{p-2}^p + \dots + a_1^p + a_0^p \pmod{p}, \end{aligned}$$

aangezien $\zeta^p = 1$. Wat belangrijk is is om op te merken dat $\alpha^p \equiv a \pmod{p}$ waarbij $a \in \mathbb{Z}$.

⁴¹Stel dat $p \mid a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0$ deelt, dan kunnen we schrijven, voor zekere b_i : $p(b_{p-2}\zeta^{p-2} + \dots + b_1\zeta + b_0) = a_{p-2}\zeta^{p-2} + \dots + a_1\zeta + a_0$ oftewel $a_i = pb_i$.

Lemma 3.1 *Stel dat u een eenheid is in $\mathbb{Z}[\zeta]$ en \bar{u} zijn complex geconjugeerde, dan is u/\bar{u} een macht van ζ .*

Bewijs: Stel dat u een eenheid is in $\mathbb{Z}[\zeta]$, dan is ook zijn complex geconjugeerde \bar{u} een eenheid, \bar{u} heeft als multiplicatieve inverse \bar{u}^{-1} aangezien $u\bar{u}^{-1} = \bar{1} = 1$. Als we schrijven $u = r(\zeta)$, voor een zeker polynoom r in $\mathbb{Z}[X]$, dan geldt dat

$$\bar{u} = r(\zeta^{-1}) = r(\zeta^{p-1}).$$

We construeren de eenheid $\mu = u/\bar{u}$, dat dit een eenheid is is goed in te zien als we opmerken dat \bar{u}/u zijn inverse is (dit is tevens de complex geconjugeerde van μ). Deze eenheid μ ligt in $\mathbb{Z}[\zeta]$, aangezien het een produkt is van u, \bar{u}^{-1} , die beide in $\mathbb{Z}[\zeta]$ liggen (en $\mathbb{Z}[\zeta]$ een ring is). We schrijven, net als Hellegouarch in [7] 1.8.2, wiens aanpak we vanaf hier zullen volgen:

$$\begin{aligned} \mu &= a_{p-1}\zeta^{p-1} + \dots + a_1\zeta + a_0 && \text{(Sic)} \\ &= E(\zeta) \end{aligned}$$

voor een zeker polynoom E in $\mathbb{Z}[X]$. Omdat we de inverse van μ kennen, namelijk zijn complex geconjugeerde en weten dat die inverse in $\mathbb{Z}[\zeta]$ ligt kunnen we schrijven:

$$\begin{aligned} \mu \cdot \bar{\mu} &= u/\bar{u} \cdot \bar{u}/u && (15) \\ &= E(\zeta)E(\zeta^{p-1}) \\ &= 1. \end{aligned}$$

De uitdrukking $E(\zeta)E(\zeta^{p-1})$ noteren we met:

$$E(\zeta)E(\zeta^{p-1}) = b_{p-1}\zeta^{p-1} + \dots + b_1\zeta + b_0, \quad E \in \mathbb{Z}[X]. \quad (16)$$

Wanneer we een wortel van $X^p - 1$ noteren met \tilde{X} en de restklasse modulo $\langle X^p - 1 \rangle$ van $f \in \mathbb{Z}[X]$ noteren als \hat{f} (om zo verwarring met de aanduiding voor complexe conjugatie \bar{f} te vermijden), kunnen we het evaluatie-in- \tilde{X} -isomorfisme⁴² in ogenschouw nemen:

$$\begin{aligned} ev_{\tilde{X}} &: \mathbb{Z}[X]/\langle X^p - 1 \rangle \rightarrow \mathbb{Z}[\tilde{X}] \\ ev_{\tilde{X}} &: \hat{f}(X) \rightarrow f(\tilde{X}). \end{aligned}$$

Wanneer we de notatie $\hat{E}(X)\hat{E}(X^{p-1})$ gebruiken om de restklasse van $E(X)E(X^{p-1})$ modulo $\langle X^p - 1 \rangle$ te noteren, verkrijgen we:

$$\begin{aligned} ev_{\tilde{X}}^{-1}\left(E(\zeta)E(\zeta^{p-1})\right) &= \hat{E}(X)\hat{E}(X^{p-1}) \\ &= E(X)E(X^{p-1}) + f(X)(X^p - 1), \end{aligned}$$

voor zekere $f(X) \in \mathbb{Z}[X]$. Dit kan, aangezien⁴³

$$E(\zeta)E(\zeta^{p-1}) \in \mathbb{Z}[\zeta] = \mathbb{Z}[\tilde{X}].$$

We concluderen, met behulp van het evaluatie-in-1-homomorfisme: ev_1 , dat immers het ene multiplicatieve eenheidselement naar de ander afbeeldt:

$$ev_1\left(\hat{E}(X)\hat{E}(X^{p-1})\right) = 1 \in \mathbb{Z}.$$

⁴²Dat dit een isomorfisme is volgt uit de eerste isomorfie stelling, zie hiervoor bijvoorbeeld [1], hoofdstuk 16

⁴³ $\tilde{X} \in \{\zeta^{p-1}, \dots, \zeta, 1\}$

Waarbij we opmerken dat $\widehat{E}(X)\widehat{E}(X^{p-1})$ wel het eenheidselement van $\mathbb{Z}[X]/\langle X^p - 1 \rangle$ moet zijn omdat dit het beeld is van $E(\zeta)E(\zeta^{p-1}) = 1$ onder het isomorfisme ev_ζ^{-1} .

Het evaluatie-in-1-homomorfisme geeft ons het volgende:

$$E(1)E(1) = (a_{p-1} + \dots + a_1 + a_0)^2 = b_{p-1} + \dots + b_1 + b_0. \quad (17)$$

We hebben al het bovenstaande ingevoerd om, met behulp van de vergelijkingen 15, 16 en 17, de volgende gelijkheid te verkrijgen:

$$\begin{aligned} 1 &= (a_{p-1} + \dots + a_1 + a_0)^2 & (18) \\ &= b_{p-1} + \dots + b_1 + b_0 \\ &= b_{p-1}\zeta^{p-1} + \dots + b_1\zeta + b_0. \end{aligned}$$

Aangezien alle b_i 's elementen van \mathbb{Z} zijn, en ζ^i niet, concluderen we dat alle b_i 's met $i \geq 1$ aan elkaar gelijk moeten zijn zodat we, met behulp van het minimaalpolynoom van ζ , kunnen afleiden dat geldt:

$$\begin{aligned} 1 &= b_0 + b_1(\zeta^{p-1} + \dots + \zeta) \\ &= b_0 - b_1 \quad (b_1 = b_2 = \dots = b_{p-1} = b_0 - 1). \end{aligned}$$

We concluderen dat als we schrijven $k = b_0 - 1$:

$$(a_{p-1} + \dots + a_1 + a_0)^2 = 1 + pk \equiv 1 \pmod{p}. \quad (19)$$

Aangezien p een priemgetal is⁴⁴ zijn ± 1 de enige elementen van orde 2 modulo p en dus:

$$a_{p-1} + \dots + a_1 + a_0 \equiv \pm 1 \pmod{p}.$$

Wanneer we vergelijking 16 uitwerken verkrijgen we:

$$\begin{aligned} E(\zeta)E(\zeta^{p-1}) &= (a_{p-1}\zeta^{p-1} + \dots + a_1\zeta + a_0)(a_{p-1}\zeta + \dots + a_1\zeta^{p-1} + a_0) \\ &= (a_{p-1}a_1)\zeta^{2(p-1)} + \dots + (a_{p-1}^2 + \dots + a_1^2 + a_0^2) \\ &= b_{p-1}\zeta^{p-1} + \dots + b_1\zeta + b_0. \end{aligned} \quad (20)$$

Omdat we de a_i 's lineair afhankelijk gekozen hebben, kunnen we ze zo kiezen dat geldt $k = 0$. Met behulp van voorgaande concluderen we:

$$b_0 = a_0^2 + a_1^2 + \dots + a_{p-1}^2 = 1.$$

Er is dus precies één a_k met $a_k^2 = 1$ de rest is 0, en we concluderen:

$$\begin{aligned} u/\bar{u} &= E(\zeta) \\ &= a_{p-1}\zeta^{p-1} + \dots + a_1\zeta + a_0 \\ &= a_k\zeta^k \\ &= \pm\zeta^k. \end{aligned}$$

⁴⁴Stel namelijk dat $n^2 \equiv 1 \pmod{p}$ voor $1 \leq n \leq p-1$ dan schrijven we $n^2 - 1 = (n-1)(n+1) = xp$ en aangezien p een priemgetal is geldt $p|(n+1)$ of $p|(n-1)$, en omdat $n \leq p-1$ concluderen we $p = n+1$ of $p = n-1$ en dus $n \equiv \pm 1 \pmod{p}$.

Om aan te tonen dat het teken van $\pm\zeta^k$ positief is maken we gebruik van een bewijs uit het ongerijmde: Stel van niet dan is er een eenheid u zodanig dat:

$$u/\bar{u} = -\zeta^k.$$

Omdat net zoals $\{\zeta^{p-2}, \dots, 1\}$ ook $\{\zeta^{p-1}, \dots, \zeta\}$ een basis is voor $\mathbb{Z}[\zeta]$ is een willekeurig element $\alpha \in \mathbb{Z}[\zeta]$ te schrijven als:

$$\begin{aligned} \alpha &= c_{p-1}\zeta^{p-1} + \dots + c_2\zeta^2 + c_1\zeta \\ \alpha - \bar{\alpha} &= c_{p-1}(\zeta^{p-1} - \zeta^{-(p-1)}) + \dots + c_1(\zeta - \zeta^{p-1}) \\ &= (\zeta - \zeta^{p-1})(c_{p-1}\zeta^{p-2} + \dots + c_1). \end{aligned}$$

We concluderen dat $(\zeta - \zeta^{p-1}) | (\alpha - \bar{\alpha})$ voor willekeurige $\alpha \in \mathbb{Z}[\zeta]$. Uit de factorisatie:

$$\zeta - \zeta^{p-1} = \zeta^{p-1}(\zeta - 1)(\zeta + 1)$$

volgt dat ook $(\zeta - 1) | (\alpha - \bar{\alpha})$. Omdat we kunnen schrijven:

$$u/\bar{u} = \begin{cases} -\zeta^{k+p} & \text{als } k \text{ is oneven} \\ -\zeta^k & \text{als } k \text{ is even} \end{cases}$$

weten we dat:

$$u/\bar{u} = -\zeta^{2s}$$

voor zekere s . We construeren het algebraïsche getal:

$$\beta = u\zeta^{-s}.$$

Dit is zo gekozen dat geldt

$$\begin{aligned} \bar{\beta} &= \overline{u\zeta^{-s}} = -u\zeta^{-2s}\zeta^s = -u\zeta^{-s} \\ &= -\beta. \end{aligned}$$

We construeren $\beta - \bar{\beta} = 2\beta$, hiervoor geldt wegens voorgaande dat $(\zeta - 1) | 2u\zeta^{-s}$ en dus ook, wegens (11):

$$N(\zeta - 1) | N(2u\zeta^{-s}) \iff p | N(2)N(u)N(\zeta^{-s}) \iff p | 2^{p-1}.$$

Maar p is een oneven priemgetal en kan dus niet 2 delen, we hebben een tegenspraak en we concluderen dat het teken van $\pm\zeta^k$ niet negatief kan zijn. \square

Stelling 3.1 *Er bestaan geen oplossingen in \mathbb{Z} van $x^p + y^p = z^p$ met $xyz \neq 0$, $p \nmid xyz$ en $p > 3$.*

Bewijs: We zullen het equivalente probleem $x^p + y^p + z^p = 0$ oplossen, i.e. aantonen dat er geen oplossingen hiervan zijn. Dit probleem is equivalent omdat p een *oneven* priem is; een oplossing $\{x, y, z\}$ van de ene vergelijking geeft een oplossing $\{x, y, -z\}$ van de andere. We kunnen deze factoriseren, op dezelfde manier als (2), namelijk:

$$(x + y)(x + y\zeta)(x + y\zeta^2) \dots (x + y\zeta^{p-1}) = -z^p, \quad (21)$$

We gebruiken vergelijking (11) die zegt dat:

$$p = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{p-1}).$$

We zien dat al de factoren $x + y\zeta^i$ met $i > 1$ relatief priem met $x + y\zeta$ zijn. Zo niet dan zouden ze een priemfactor π gemeen hebben; $\pi | (x + y\zeta^i)$, $\pi | (x + y\zeta)$ en π deelt dus ook hun verschil:

$$(x + y\zeta^i) - (x + y\zeta) = y\zeta(1 - \zeta^{i-1}).$$

Dit is echter onmogelijk, want dat zou wegens het eerdere resultaat impliceren dat $\pi|yp$, dus $\pi|y$ of $\pi|p$. Verder deelt π ook z , maar x, y, z, p waren juist paarsgewijs priem verondersteld en y of p kan dus niet een factor gemeen hebben met z .⁴⁵

We concluderen dat, aangezien $x + y\zeta$ een p^{de} macht (namelijk $-z^p$) deelt, er moet gelden dat $x + y\zeta$ zelf een p^{de} macht is:

$$x + y\zeta = u\alpha^p \quad (22)$$

voor een zekere eenheid u en een $\alpha \in \mathbb{Z}[\zeta]$. Dit resultaat hebben we verkregen in een UFD, later zullen we dit uit kunnen breiden naar andere ringen, we zullen dan op een andere manier tot ditzelfde resultaat kunnen komen en vanaf hier dezelfde route volgen.

We zullen nu de eerder in deze paragraaf behandelde eigenschappen van modulo p rekenen gebruiken. Er geldt wegens (22)

$$x + y\zeta \equiv u\alpha^p \pmod{p}$$

en dus ook

$$\overline{x + y\zeta} \equiv \overline{u\alpha^p} \pmod{p},$$

dit (i.e. complexe conjugatie) is een erg handige afbeelding, omdat zoals opgemerkt $\bar{x} = x$ voor $x \in \mathbb{Z}$, met andere woorden: $\sigma_{-1}|_{\mathbb{Z}} = \text{id}$. We hebben dus

$$\begin{aligned} \overline{x + y\zeta} &\equiv \overline{x + y\bar{\zeta}} \\ &\equiv x + y\zeta^{-1} \pmod{p}, \end{aligned}$$

verder hebben we

$$\begin{aligned} \overline{u\alpha^p} &\equiv \overline{\bar{u}(a_0^p + \dots + a_{p-2}^p)} \\ &\equiv \bar{u}(a_0^p + \dots + a_{p-2}^p) \pmod{p}. \end{aligned}$$

We concluderen

$$x + y\zeta^{-1} \equiv \bar{u}a \pmod{p},$$

waarbij $a = a_0^p + \dots + a_{p-2}^p \in \mathbb{Z}$. Met behulp van lemma 3.1 schrijven we, modulo p :

$$\left. \begin{array}{l} x + y\zeta \equiv ua \\ x + y\zeta^{-1} \equiv \bar{u}a \end{array} \right\} \Rightarrow x + y\zeta \equiv (x + y\zeta^{-1})u/\bar{u} \iff x + y\zeta \equiv (x + y\zeta^{-1})\zeta^k.$$

We zien dat wanneer $k \neq 1$ we op een tegenspraak stuiten, we kunnen aan beide kanten machten van ζ verzamelen en deze zijn verschillend, dit kan niet. We concluderen $k = 1$ en dus:

$$x \equiv y \pmod{p}.$$

Als we (16) factoriseren als:

$$(x + z)(x + z\zeta)(x + z\zeta^2) \dots (x + z\zeta^{p-1}) = -y^p$$

verkrijgen we op dezelfde manier

$$x \equiv z \pmod{p}.$$

We concluderen:

$$3x^p \equiv x^p + y^p + z^p \equiv 0 \pmod{p}.$$

Met andere woorden: $p|x$ of $p|3$ in beide gevallen hebben we een tegenspraak, we concluderen dat er geen oplossingen van (1) bestaan voor n een oneven priem groter dan 3. \square

⁴⁵Zowieso zijn x, y, z paarsgewijs priem, zie hiervoor paragraaf 2.6, verder is aangenomen dat $p \nmid xyz$; het eerste geval.

4 Het tweede geval

Stelling 4.1 *Er bestaan geen oplossingen in \mathbb{Z} van $x^p + y^p = z^p$ met $xyz \neq 0$, $p|xyz$ en $p > 3$.*

Bewijs: Bij het tweede geval van FLT geldt dat $p|xyz$, we hebben al opgemerkt, in paragraaf 2.6, dat x, y en z paarsgewijs priem moeten zijn omdat we anders een gemeenschappelijke deler van x, y, z hebben. Er is dus precies 1 factor deelbaar door p , zonder beperking van algemeenheid nemen we aan dat $p|z$. Stel namelijk dat $p|y$ dan herschrijven we (1) als $x^p + (-z)^p = (-y)^p$ en kunnen we dezelfde aanpak volgen, idem bij $p|x$. We nemen dus vanaf nu aan dat x, y, z relatief priem zijn en dat $p|z$.

Als we, in dit tweede geval, vergelijking (1) factoriseren als:

$$\begin{aligned} x^p + y^p &= z^p \\ (x+y)(x+y\zeta)\dots(x+y\zeta^{p-1}) &= (p^n z_0)^p, \quad p \nmid z_0 \end{aligned} \quad (23)$$

moet gelden dat voor $i = 1, \dots, p-1$ de termen $(x+y\zeta^i)$ precies een keer deelbaar zijn door $\pi = \zeta - 1$.

- Stap 1: Als eerste zullen we laten zien dat alle termen $(x+y\zeta^i)$ precies een keer deelbaar zijn door π en dat ze naast π geen (priem)factor gemeenschappelijk hebben.

Om te laten zien dat iedere term minstens een keer deelbaar is door π schrijven we:

$$x^p + y^p \equiv (x+y)^p \equiv 0 \pmod{p}$$

omdat $p|z$. We concluderen:

$$x + y \equiv 0 \pmod{p}.$$

Aangezien $x + y$ deelbaar is door p is het ook zeker deelbaar door $\pi = \zeta - 1$ want $\pi|p$ in $\mathbb{Z}[\zeta]$.⁴⁶ Omdat we kunnen schrijven:

$$\begin{aligned} x + y\zeta &\equiv (x+y) + \pi y \equiv 0 \pmod{\pi} \\ x + y\zeta^2 &\equiv (x+y\zeta) + \pi y\zeta \equiv 0 \pmod{\pi} \\ &\vdots \end{aligned}$$

zien we dat elke term $(x+y\zeta^i)$ deelbaar is door π .

We claimen dat, voor $i = 1, \dots, p-1$, deze termen niet door π^2 deelbaar zijn. Hiervoor moeten we eerst een tussenresultaat ophalen. In het bewijs van stelling 2.1 hebben we gezien, in vergelijking (11) en (12):

$$p = \pi^{p-1} (-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1}). \quad (24)$$

We zien dat

$$(-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1})$$

⁴⁶Herinner dat $N(\pi) = p$ en dus $p = \pi\sigma_2(\pi)\dots\sigma_{p-1}(\pi)$, dit is precies de strekking van vergelijking (11).

een eenheid is want zijn norm is 1. Er geldt namelijk:

$$\begin{aligned} N(p) &= N(\pi)^{p-1} N\left((-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1})\right) \\ p^{p-1} &= p^{p-1} N\left((-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1})\right) \\ 1 &= N\left((-1)^{p-1} \prod_{i=1}^{p-1} (1 + \dots + \zeta^{i-1})\right). \end{aligned}$$

Om in te zien dat een element met norm 1 een eenheid is kunnen we zijn inverse geven: zij $\alpha \in \mathbb{Z}[\zeta]$ een element van norm 1, dan kunnen we schrijven:

$$\frac{N(\alpha)}{\alpha} = \prod_{j=1}^{p-1} \sigma_j(\alpha) \in \mathbb{Z}[\zeta],$$

en er geldt:

$$\frac{N(\alpha)}{\alpha} \cdot \alpha = N(\alpha) = 1.$$

Andersom heeft een eenheid altijd norm ± 1 aangezien deze norm een eenheid in \mathbb{Z} moet zijn.

Op soortgelijke wijze leiden we af, aangezien $N(\pi) = N(\sigma_i(\pi)) = N(\zeta^i - 1)$ voor $i \neq 1$,⁴⁷ dat moet gelden voor zekere eenheid ϵ :

$$\pi = (\zeta - 1) = \epsilon(\zeta^i - 1)$$

Nu we deze resultaten hebben kunnen we laten zien dat de termen in het linkerlid van (18) geen factor π^2 gemeenschappelijk hebben, dit zullen we doen door een algemener resultaat te geven; namelijk dat de verschillende termen:

$$\frac{x + y\zeta^i}{\pi}, \quad i = 1, 2, \dots, p-1$$

paarsgewijs priem zijn. Hiervoor kunnen we dezelfde redenering als in het bewijs van stelling 3.1 gebruiken: Stel namelijk dat

$$\frac{x + y\zeta^i}{\pi}, \quad \frac{x + y\zeta^j}{\pi} \quad i \neq j$$

een priemfactor $\lambda \in \mathbb{Z}[\zeta]$ gemeen hebben, dan geldt:

$$\lambda \left| \left(\frac{x + y\zeta^i}{\pi} - \frac{x + y\zeta^j}{\pi} \right) \right|.$$

Wegens $\zeta^{i-j} - 1 = \epsilon\pi$ geldt, voor zekere eenheid ϵ :

$$\lambda \left| \frac{y\zeta^j(\zeta^{i-j} - 1)}{\pi} \right| \iff \lambda |y\zeta^j \epsilon| \iff \lambda |y|.$$

Oftewel λ deelt zowel y als z dit kan niet aangezien we deze relatief priem hebben verondersteld.

⁴⁷Met σ_i bedoelen we de afbeelding die wordt geïnduceerd door $\zeta \rightarrow \zeta^i$ zoals we die zijn tegengekomen in paragraaf 2.3.

- Stap 2: We zullen nu laten zien dat een oplossing $x, y, z \in \mathbb{Z}[\zeta]$ van (23) een oplossing $x, y, z_0 \in \mathbb{Z}[\zeta]$ van de vergelijking

$$x^p + y^p = e\pi^{pk}z_0^p,$$

induceert, voor een nog te definiëren k ⁴⁸. Daarna zullen we, bij de volgende stappen, aantonen dat deze laatste vergelijking geen oplossingen heeft, en hiermee het tweede geval van FLT bewijzen⁴⁹.

We zullen ook hier de aanpak van Hellegouarch volgen ([7] paragraaf 1.8.4). We hebben gezien dat termen $x + y\zeta^i$ met $i > 0$ precies een keer door π deelbaar zijn en dat de verschillende termen:

$$\frac{x + y\zeta^i}{\pi}, \quad i = 1, 2, \dots, p-1$$

paarsgewijs priem zijn. We kunnen, met behulp van onze oplossing x, y, z en vergelijking (22) schrijven:

$$\begin{cases} x + y\zeta & = \pi e_1 t_1^p \\ x + y\zeta^{p-1} & = \pi e_{p-1} t_{p-1}^p \\ x + y & = \pi e_0 \pi^{pk} t_0^p \end{cases}$$

voor zekere eenheden $e_{\pm 1}, e_0$. Waarbij $t_i \in \mathbb{Z}[\zeta]$ en $k = n(p-1) - 1$. Dit komt voort uit het feit dat we het rechterlid van het tweede deel van (23) kunnen herschrijven als:

$$(p^n z_0)^p = (\epsilon \pi^{p-1})^{pn} z_0^p.$$

We zien dus dat π beide kanten $pn(p-1)$ keer deelt, in het linkerlid van (23) hebben we dat π alle $p-1$ factoren $x + y\zeta^i$ precies een keer deelt en we houden dus over dat π de overgebleven factor $x + y$ precies

$$pn(p-1) - (p-1) = p(n(p-1) - 1) + 1 = pk + 1$$

keer moet delen.

We zien dat uit het paarsgewijs priem⁵⁰ zijn van de termen in het linkerstuk dit ook moet gelden voor de factoren $t_{\pm 1}, t_0$. Hieruit volgt ook dat ze, aangezien ze een p^{de} macht delen, zelf p^{de} machten moeten zijn. Met behulp van lineaire algebra en wanneer we opmerken dat $(\zeta^2 - 1) = \pi(\zeta + 1)$ ⁵¹ verkrijgen we:

$$\begin{aligned} x &= \pi e_1 t_1^p - y\zeta \\ y &= \zeta(\pi e_{p-1} t_{p-1}^p - \pi e_1 t_1^p + y\zeta) \\ (\zeta^2 - 1)y &= \zeta\pi(e_1 t_1^p - e_{p-1} t_{p-1}^p), \\ (\zeta + 1)y &= \zeta(e_1 t_1^p - e_{p-1} t_{p-1}^p). \end{aligned}$$

We concluderen:

$$\begin{aligned} x + y &= \pi e_0 \pi^{pk} t_0^p \\ &= \pi e_1 t_1^p - \pi y \\ &= \pi e_1 t_1^p - \pi(\zeta + 1)^{-1} \zeta (e_1 t_1^p - e_{p-1} t_{p-1}^p). \end{aligned}$$

⁴⁸Om verwarring te voorkomen is het goed om op te merken dat x, y, z_0 hier hergedefinieerd worden, ze hebben natuurlijk hun oorsprong in een oplossing van 23 maar betekenen hier wel echt wat anders; ze liggen bijvoorbeeld in $\mathbb{Z}[\zeta]$ in plaats van \mathbb{Z} . Later zullen we hieruit weer andere oplossingen construeren die we ook x, y, z_0 zullen noemen, ik hoop dat het uit de context duidelijk is wat we in welk geval bedoelen, maar uiteindelijk is vooral de vorm van de vergelijking belangrijk want dit zal namelijk met zich mee brengen dat er helemaal geen oplossingen bestaan.

⁴⁹i.e. aantonen dat er geen oplossingen zijn van de eerste vergelijking van (23) onder de aannames van "het tweede geval"

⁵⁰Tot op de factor π

⁵¹Merk op dat hieruit direct volgt dat $(\zeta + 1)$ een eenheid is.

Nu hebben we x, y uit het stelsel geëlimineerd en kunnen we de ontstane relatie vereenvoudigen:

$$\begin{aligned} e_0 \pi^{pk} t_0^p &= e_1 t_1^p - (\zeta + 1)^{-1} \zeta (e_1 t_1^p - e_{p-1} t_{p-1}^p) \\ (e_1 t_1^p - e_0 \pi^{pk} t_0^p)(\zeta + 1) &= \zeta (e_1 t_1^p - e_{p-1} t_{p-1}^p) \\ e_0 \pi^{pk} t_0^p (\zeta + 1) - e_1 t_1^p &= \zeta e_{p-1} t_{p-1}^p \\ t_1^p + \zeta \frac{e_{p-1}}{e_1} t_{p-1}^p &= e \pi^{pk} t_0^p \end{aligned}$$

Voor een zekere eenheid e . Merk op dat we hier gebruik gemaakt hebben van het feit dat $\zeta + 1$ een eenheid is. Wanneer we voorgaande relatie modulo p bekijken zien we:

$$t_1^p + \zeta \frac{e_{p-1}}{e_1} t_{p-1}^p \equiv 0 \pmod{p}.$$

De eenheid $\zeta \frac{e_{p-1}}{e_1}$ moet dus een geheel in \mathbb{Z} zijn, modulo p^{52} . De enige mogelijkheid is $\zeta \frac{e_{p-1}}{e_1} = 1$, en we verkrijgen:

$$t_1^p + t_{p-1}^p = e \pi^{pk} t_0^p$$

oftewel een vergelijking van de vorm:

$$x^p + y^p = e \pi^{pk} z_0^p, \quad (25)$$

waarbij $x, y, z_0 \in \mathbb{Z}[\zeta]$.

- Stap 3: We zullen in de volgende stappen aantonen dat bovenstaande vergelijking geen oplossingen heeft. Dit zullen we doen door Fermat's methode van "descent" te gebruiken; we zullen als eerste laten zien dat $k > 1$. Daarna zullen we bij stap 4 laten zien dat een oplossing van bovenstaande vergelijking een oplossing induceert van dezelfde vergelijking met een strikt kleinere k .

Stel nu dat we een oplossing x, y, z_0 van (25) hebben, er geldt dan $x, y, z_0 \in \mathbb{Z}[\zeta]$ paarsgewijs priem en:

$$xy z_0 \not\equiv 0 \pmod{\pi}.$$

De getallen $\{\pi^{p-2}, \dots, \pi^2, \pi, 1\}$ vormen net als $\{\zeta^{p-2}, \dots, \zeta, 1\}$ een basis voor $\mathbb{Z}[\zeta]$. Dit is goed in te zien doordat de elementen van de een op een unieke manier in die van de ander uit te drukken zijn en vica versa.⁵³ We kunnen hierdoor de elementen $x, y \in \mathbb{Z}[\zeta]$ schrijven als:

$$\begin{aligned} x &= a_{p-2} \pi^{p-2} + \dots + a_1 \pi + a_0 \\ y &= b_{p-2} \pi^{p-2} + \dots + b_1 \pi + b_0. \end{aligned}$$

Wanneer we dit modulo π^2 bekijken verkrijgen we:

$$\begin{aligned} x &\equiv a_1 \pi + a_0 \pmod{\pi^2} \\ y &\equiv b_1 \pi + b_0 \pmod{\pi^2}. \end{aligned}$$

Met behulp van de relatie

$$\begin{aligned} \zeta^j &= (\pi + 1)^j = \pi^j + \binom{j}{1} \pi^{j-1} + \dots + \binom{j}{j-1} \pi + 1 \\ &\equiv j \pi + 1 \pmod{\pi^2} \end{aligned}$$

⁵²Herinner dat een p -de macht van een algebraïsche geheel een geheel in \mathbb{Z} is, modulo p , zie pagina 22, de congruentievergelijking is dus louter een vergelijking in \mathbb{Z} .

⁵³ $\pi + 1 = \zeta$, $(\pi + 1)^2 = \zeta^2, \dots$ en $\zeta - 1 = \pi$, $(\zeta - 1)^2 = \pi^2, \dots$

leiden we af:

$$\begin{aligned} x + y\zeta^j &\equiv (a_0 + a_1\pi) + (\pi + 1)^j(b_0 + b_1\pi) \\ &\equiv (a_0 + b_0) + (a_1 + b_1 + jb_0)\pi \pmod{\pi^2}. \end{aligned} \quad (26)$$

De vergelijking $a_1 + b_1 + jb_0 \equiv 0 \pmod{p}$ heeft precies een oplossing voor $j \in \{0, 1, \dots, p-1\}$, waarbij we natuurlijk a_i en b_i in \mathbb{Z} hebben aangenomen. Aangezien al deze verschillende j een ander resultaat opleveren en er ook precies $p-1$ restklassen modulo p zijn, er moet dus een j de restklasse 0 modulo p geven. Hierbij moet dan opgemerkt worden dat b_0 natuurlijk niet 0 kan zijn, aangezien dan y deelbaar door π zou zijn en dat kan niet. We weten dat π de vergelijking

$$(x + y)(x + y\zeta) \dots (x + y\zeta^{p-1}) \equiv (a_0 + b_0)^p \pmod{\pi} \quad (27)$$

deelt, zie bijvoorbeeld (23) en (26). Hieruit concluderen we:

$$(a_0 + b_0)^p \equiv 0 \pmod{\pi}$$

oftewel $\pi | (a_0 + b_0)^p$ en we concluderen $p = N(\pi) | (a_0 + b_0)^{p(p-1)}$ en, aangezien p een priem in \mathbb{Z} is: $p | (a_0 + b_0)$. Aangezien $\pi^2 | p$ hebben een term in het linkerlid van (27) waarvoor geldt:

$$x + y\zeta^j \equiv 0 \pmod{\pi^2}.$$

Dit kan alleen $x + y$ zijn aangezien dit de enige term is die meer dan een keer door π deelbaar kan zijn, zie hiervoor de redenering aan het begin van deze paragraaf.

Wanneer we aan beide kanten in vergelijking (23) factoren π verzamelen zien we dat we in het linkerlid in ieder geval: $2 + (p-1)$ factoren hebben; twee van de term $x + y$ en van elk van de overige $p-1$ termen precies een. We concluderen dus dat de exponent k in het rechterlid strikt groter dan 1 moet zijn.

- Stap 4: In het volgende gedeelte zullen we laten zien dat een oplossing van vergelijking (25), met zekere k een andere oplossing induceert van dezelfde vergelijking met strikt kleinere k .

Op precies dezelfde manier als in het begin van het bewijs, kunnen we van onze oplossing een volgende afleiden; we verkrijgen, op dezelfde manier:

$$\begin{cases} x + y\zeta &= \pi e_1 t_1^p \\ x + y\zeta^{p-1} &= \pi e_{p-1} t_{p-1}^p \\ x + y &= \pi e_0 \pi^{pk_1} t_0^p \end{cases} .$$

Door naar de factoren π aan beide kanten van

$$(x + y)(x + y\zeta) \dots (x + y\zeta^{p-1}) = e\pi^{pk} z_0^p$$

te kijken zien we dat moet gelden dat $pk_1 + 1 + (p-1) = pk$. De eerste term in het linkerlid is precies $pk_1 + 1$ keer deelbaar door π terwijl de overige termen precies een keer gedeeld worden. We concluderen:

$$k_1 = k - 1.$$

- Stap 5: Conclusie:

Stel dat we een oplossing hebben van vergelijking (25) dan induceert dit dus een oplossing van dezelfde vergelijking met $k_1 = k - 1$, we krijgen dus een strikt dalende rij van oplossingen⁵⁴ die op een gegeven moment een oplossing moet geven van:

$$x^p + y^p = e\pi^{pk_n} z_0^p, \quad k_n \leq 1.$$

Maar dit is onmogelijk, aangezien we hadden bewezen dat k strikt *groter* dan 1 moet zijn. We concluderen dat er geen oplossing kan bestaan van vergelijking (25) en het tweede geval van FLT bewezen is. \square

⁵⁴Dalend in de zin dat de bijbehorende $k \in \mathbb{Z}$ strikt kleiner wordt.

5 Dedekind-ring en unieke factorisatie in idealen

5.1 inleiding

In de vorige hoofdstukken hebben we FLT bewezen onder de aanname dat $\mathbb{Z}[\zeta]$ een UFD is. Dit is niet voor alle p zo. Bijvoorbeeld voor $p = 23$ gaat het mis, Kummer heeft aangetoond dat de bijbehorende ring $\mathbb{Z}[\zeta]$ geen UFD is. We hebben de unieke factorisatie eigenschap nodig gehad om te concluderen dat wanneer een priem een p^{de} macht deelt hij deze p keer deelt. We zullen in dit hoofdstuk dit op een andere manier afleiden, en zo de stelling (FLT) algemenere geldigheid geven. We zullen dit doen door naar de idealen van $\mathbb{Z}[\zeta]$ te kijken. Er zal blijken dat voor een groot aantal gevallen een getal in $\mathbb{Z}[\zeta]$ dan wel niet uniek factoriseert in priemgetallen maar wel op een unieke manier te schrijven is als produkt van idealen. Deze aanpak is bedacht door E. Kummer. In dit hoofdstuk zal ik veel gebruiken van de aanpak uit [14] en delen uit [2], lecture 7. Een andere meer uitgebreider en formelere aanpak is te vinden in [4].⁵⁵

Wanneer we over getallen in \mathbb{Z} praten, of algebraïsche gehelen in $\mathbb{Z}[\zeta]$, en met name over deelbaarheidseigenschappen van die elementen, zoals bijvoorbeeld factorisatie in priemen, dan is het om het even of we over elementen praten met de gebruikelijke vermenigvulging in \mathbb{Z} of $\mathbb{Z}[\zeta]$ of dat we over de hoofdidealen van bijbehorende ring praten met de volgende vermenigvuldigingsregel:

$$\langle a \rangle \langle b \rangle = \langle ab \rangle.$$

Dit is precies de gebruikelijke vermenigvuldiging van idealen in het geval van hoofdidealen, in het algemeen is het produkt van 2 idealen namelijk gedefinieerd als:

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}. \quad (28)$$

De sommatie is hier altijd eindig. Merk op dat dit produkt commutatief is.

Een ideaal \mathfrak{a} in een ring R heet *maximaal* als er geen ander ideaal $\mathfrak{b} \subset R$ bestaat, met $\mathfrak{b} \neq \mathfrak{a}, R$ zodanig dat $\mathfrak{a} \subset \mathfrak{b} \subset R$. Een ideaal \mathfrak{a} heet *priem* als $ab \in \mathfrak{a}$, met a, b niet nul of één, impliceert dat $a \in \mathfrak{a}$ of $b \in \mathfrak{a}$. We noemen een ideaal \mathfrak{a} deelbaar door \mathfrak{b} als er een ideaal \mathfrak{c} bestaat zodanig dat $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. In het geval dat $\mathfrak{a}, \mathfrak{b}$ en \mathfrak{c} hoofdidealen zijn met als voortbrengers respectievelijk a, b en c , hebben we:⁵⁶

$$\mathfrak{a} | \mathfrak{b} \Leftrightarrow a | b \Leftrightarrow \mathfrak{a} \supseteq \mathfrak{b}.$$

In het geval van hoofdidealen is delen hetzelfde als omvatten. Wanneer we dit weten kunnen we de benaming van priemideaal ook verduidelijken, we zouden de verzameling van hoofdidealen van een getallenlichaam graag als een groep willen zien⁵⁷ en zullen dit in de volgende paragraaf ook echt zo gaan construeren, we zouden een hoofdideaal \mathfrak{p} priem willen noemen wanneer geldt $\mathfrak{p} | \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} | \mathfrak{a}$ of $\mathfrak{p} | \mathfrak{b}$. We zien:

$$ab \in \mathfrak{p} \Leftrightarrow \langle ab \rangle \subseteq \mathfrak{p} \Leftrightarrow \mathfrak{p} | \langle ab \rangle = \langle a \rangle \langle b \rangle,$$

per definitie van een priemideaal geldt ook het volgende:

$$a \text{ of } b \in \mathfrak{p} \Leftrightarrow \langle a \rangle \text{ of } \langle b \rangle \subseteq \mathfrak{p} \Leftrightarrow \mathfrak{p} | \langle a \rangle \text{ of } \mathfrak{p} | \langle b \rangle.$$

⁵⁵Ik zal deze aanpak in dit hoofdstuk niet volgen, aangezien dit veel minder toegespitst en (dus) langer is, het zou voor grote delen buiten het blikveld van deze scriptie vallen. Het is, voor sommige onderdelen, wel de moeite waard.

⁵⁶We maken hier gebruik van het feit dat de voortbrenger van een hoofdideaal op eenheid na uniek is.

⁵⁷Die groep idealen zal dan isomorf zijn met de ring der gehelen uitgedeeld naar eenheden.

Vica versa volgt ook dat elk priemelement in de "groep" van hoofdidealen een priemideaal moet zijn. We zien dus steeds meer de nauwe samenhang tussen (hoofd)idealen van een lichaam en het lichaam zelf; elk priemelement correspondeert met een priemideaal. In de "groep" van hoofdidealen hebben we als eenheidselement het ideaal voortgebracht door het eenheidselement van bijbehorende ring der gehelen, namelijk 1, dit eenheidsideaal is dus $\langle 1 \rangle = \mathcal{O}$.⁵⁸

Lemma 5.1 *In een Noethers domein wordt elk hoofdideaal dat priem is voortgebracht door een priemelement.*

Bewijs: Stel van niet, stel dat $\mathfrak{a} = \langle ab \rangle$ een priemideaal is, en a, b geen eenheden. Er moet gelden, aangezien \mathfrak{a} een priemideaal is dat $a \in \mathfrak{a}$ of $b \in \mathfrak{a}$. Beide mogelijkheden zijn onmogelijk, aangezien $a \in \mathfrak{a}$ (idem b) zou betekenen dat $\langle a \rangle \subseteq \mathfrak{a}$ maar er geldt $\mathfrak{a} = \langle a \rangle \langle b \rangle$ en geen van de idealen is het eenheidsideaal, we concluderen $\langle a \rangle \mathfrak{a} \Leftrightarrow \langle a \rangle \subseteq \mathfrak{a}$ en gelijkheid is onmogelijk, we hebben een tegenspraak en concluderen dat wanneer de voortbrenger van een priemideaal te schrijven is als ab , één van de termen wel een eenheid moet zijn. Oftewel de voortbrenger is een priemelement. \square

Wanneer we in een unieke factorisatie domein een factorisatie in priemelementen hebben is dit equivalent, op eenheden na, met een factorisatie in bijbehorende hoofdidealen:

$$x = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m} \Leftrightarrow \langle x \rangle = \langle p_1 \rangle^{n_1} \langle p_2 \rangle^{n_2} \dots \langle p_m \rangle^{n_m}.$$

Stel bijvoorbeeld dat $x = ab$ een factorisatie van een element x is, dan is

$$\begin{aligned} \langle a \rangle \langle b \rangle &= \left\{ \sum a_i b_i \mid a_i \in \langle a \rangle, b_i \in \langle b \rangle \right\} \\ &= \left\{ \sum ab \cdot c_i \right\} \\ &= \langle x \rangle. \end{aligned}$$

Anderzijds volgt uit bovenstaande dat $ab = ux$ voor zekere eenheid u . We kunnen dus evengoed over een factorisatie in (hoofd)idealen praten als over een factorisatie in priemelementen. De aanpak met idealen is zelfs lichtelijk beter omdat het de ambivalentie met betrekking tot de eenheden wegneemt: er geldt namelijk $\langle a \rangle = \langle ua \rangle$ als u een eenheid is. Was de factorisatie in priemelementen nog uniek op eenheden en volgorde na, de factorisatie in idealen is uniek tot op volgorde. Wat belangrijk is, is dat bij de pijl terug, dat wil zeggen dat de factorisatie in priemelementen volgt uit een factorisatie in hoofdidealen, het wel van belang is dat we inderdaad praten over hoofdidealen. Aan een hoofdideaal kunnen we immers een, op eenheden na uniek element, namelijk zijn voortbrenger, koppelen.

We kunnen in dit licht nu nog eens het voorbeeld uit hoofdstuk 1 paragraaf 2 bekijken. Hier hadden we 2 factorisaties van 10 namelijk

$$10 = 2 \cdot 5 = (5 + \sqrt{15}) \cdot (5 - \sqrt{15})$$

in de ring der gehelen $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ van het getallenlichaam $\mathbb{Q}(\sqrt{15})$. Er zijn natuurlijk uitbreidingen van $\mathbb{Q}(\sqrt{15})$ te bedenken die de meervoudigheid teniet doen door een verdere factorisatie van de huidige factoren, zoals dat al in hoofdstuk 1 beschreven is. Een voorbeeld zou $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ zijn met $\mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{5})}$. wanneer we definiëren:

$$\begin{aligned} \wp_1 &= \sqrt{5} + \sqrt{3}, & \wp_3 &= \sqrt{5}, \\ \wp_2 &= \sqrt{5} - \sqrt{3}, & \wp_4 &= \sqrt{5}, \end{aligned}$$

⁵⁸Een eenheidselement is altijd uniek, stel dat e en e' beide eenheidselementen zijn dan geldt: $e = ee' = e'$.

dan kunnen we schrijven:

$$\begin{aligned} 10 &= 2 \cdot 5 &= (5 + \sqrt{15}) \cdot (5 - \sqrt{15}) \\ &= \wp_1 \wp_2 \cdot \wp_3 \wp_4 &= \wp_1 \wp_3 \cdot \wp_2 \wp_4 \end{aligned}$$

en we zien dat de meervoudigheid van factorisaties teniet wordt gedaan, natuurlijk zou je dan moeten controleren dat er ook in deze uitbreiding niet meerdere factorisaties bestaan. Dit kun je doen door te bewijzen dat de nieuwe factoren priemem in $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ zijn, aangezien een factorisatie in priemelementen (in een domein) uniek is⁵⁹ maar dat zullen we in dit voorbeeld voorbij laten gaan (maar *wel* aannemen dat de factorisatie uniek is).

Wanneer we nu naar bijbehorende factorisatie in idealen kijken verkrijgen we wanneer we schrijven $\langle \wp_i \rangle = \mathfrak{p}_i$:

$$\langle 10 \rangle = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4.$$

Waarbij de betreffende idealen in de ring der gehelen $\mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{5})}$ van $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ liggen. Het idee is nu om naar de idealen $\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ te kijken, dit zijn immers idealen in $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ en we hebben reden om aan te nemen dat we hiermee $\langle 10 \rangle$ kunnen factoriseren.

Stel namelijk dat L en K twee getallenlichamen zijn, zodanig dat $L \supseteq K$, en $\mathcal{O}_L \supseteq \mathcal{O}_K$ hun bijbehorende ringen der gehelen. Stel verder dat $\langle a \rangle$ en $\langle b \rangle$ twee idealen in \mathcal{O}_L zijn. Dan geldt

$$\left(\langle a \rangle \cap \mathcal{O}_K \right) \left(\langle b \rangle \cap \mathcal{O}_K \right) = \langle a \rangle \langle b \rangle \cap \mathcal{O}_K.$$

We kunnen $\left(\langle a \rangle \cap \mathcal{O}_K \right) \left(\langle b \rangle \cap \mathcal{O}_K \right)$ namelijk schrijven als:

$$\begin{aligned} \left\{ \sum a_i b_i \mid a_i \in \langle a \rangle \cap \mathcal{O}_K, b_i \in \langle b \rangle \cap \mathcal{O}_K \right\} &= \left\{ ab \sum c_i \mid c_i \in \mathcal{O}_L, ab \sum c_i \in \mathcal{O}_K \right\} \\ &= \left\{ ab \cdot d_i \mid d_i \in \mathcal{O}_L, ab \cdot d_i \in \mathcal{O}_K \right\} \\ &= \langle ab \rangle \cap \mathcal{O}_K \end{aligned}$$

en dit is per definitie gelijk aan $\langle a \rangle \langle b \rangle \cap \mathcal{O}_K$. Wanneer we dit, zoals aangekondigd, gebruiken om $\langle 10 \rangle$ te factoriseren in idealen uit $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ in tegenstelling tot idealen uit $\mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{5})}$, verkrijgen we:

$$\begin{aligned} \langle 10 \rangle \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})} &= \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})} \\ &= \prod_{i=1}^4 \left(\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})} \right). \end{aligned}$$

Aangezien $\langle 10 \rangle$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ ligt krijgen we een factorisatie van het ideaal $\langle 10 \rangle$ in idealen uit $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ van de vorm $\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})}$.

Het punt waarop de factorisatie in *elementen* van $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ misgaat is dat de idealen $\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ geen hoofdidealten hoeven te zijn; we kunnen dus niet aan deze factorisatie in idealen een equivalente factorisatie in elementen van $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ verbinden. Dit is dan ook de betekenis van de "uitbreiding door middel van ideale getallen zodanig dat unieke factorisatie behouden blijft"; je gaat niet-hoofd-idealten gebruiken om idealen te factoriseren. Kummer probeerde hier nog daadwerkelijk *getallen* te vinden om factorisatie te behouden, Dedekind heeft later ingezien dat we hier idealen nodig hebben, en heeft dit geformaliseerd tot het ideaalbegrip zoals we dat nu kennen.

⁵⁹Dis is precies lemma 2.6

5.2 Dedekind-ring

Na vorige paragraaf zouden we ons graag in een omgeving bevinden waarin elk ideaal uniek factoriseert in priemidealen. Hiertoe is het begrip *Dedekind-ring* ingevoerd, we definiëren: Zij A een domein met de eigenschappen dat

- A is Noethers
- A is zijn eigen integrale afsluiting
- elk priemideaal ongelijk 0 in A is maximaal

dan noemen we A een *Dedekind-ring*.

We zullen in deze paragraaf bewijzen dat de ring der gehelen $\mathbb{Z}[\zeta]$ een Dedekind-ring is, hiertoe zullen we eerst een aantal resultaten moeten behandelen.

Lemma 5.2 *Als R een ring is en \mathfrak{a} een ideaal dan is \mathfrak{a} maximaal dan en slechts dan als R/\mathfrak{a} een lichaam is.*

Bewijs: We noteren de restklassen modulo \mathfrak{a} als \bar{x} en een representant als x . Het feit dat R/\mathfrak{a} een lichaam is impliceert dat elk element \bar{x} een inverse \bar{x}^{-1} heeft. Stel nu dat het ideaal \mathfrak{a} niet maximaal is, dan bestaat er een ideaal \mathfrak{b} ongelijk R en strikt groter dan \mathfrak{a} , we kiezen een element $x \in \mathfrak{b}$ met $x \notin \mathfrak{a}$, er geldt:

$$\begin{aligned} \bar{x} \cdot \bar{x}^{-1} &\equiv 1 \pmod{\mathfrak{a}} \\ (x + \mathfrak{a})(x^{-1} + \mathfrak{a}) &= xx^{-1} + \mathfrak{a} \\ &= 1 + \mathfrak{a} \end{aligned}$$

we verkrijgen, aangezien $xx^{-1} \in \mathfrak{b}$ dat $1 + \mathfrak{a} \subseteq \mathfrak{b}$, dit geeft op zijn beurt dat $1 \in \mathfrak{b}$ en hieruit volgt $\langle 1 \rangle \subseteq \mathfrak{b}$ en concluderen $\mathfrak{b} = R$; een tegenspraak. We concluderen dus dat \mathfrak{a} wel maximaal moet zijn. Andersom volgt uit het feit dat \mathfrak{a} maximaal is dat voor een willekeurig element $x \notin \mathfrak{a}$ dat

$$\mathfrak{a} + Rx = R = \langle 1 \rangle.$$

Aangezien $\mathfrak{a} + Rx$ een ideaal is strikt groter dan \mathfrak{a} . Omdat $1 \in \mathfrak{a} + Rx$ moet er een element $x^{-1} \in R$ zijn zodanig dat

$$\mathfrak{a} + x^{-1}x = (\mathfrak{a} + x^{-1})(\mathfrak{a} + x) = \langle 1 \rangle.$$

Er moet dus een element in R/\mathfrak{a} zijn, die we \bar{x}^{-1} zullen noemen zodanig dat $\bar{x}\bar{x}^{-1} = 1$. We concluderen dat R/\mathfrak{a} een lichaam is. \square

Lemma 5.3 *Stel dat A en B domeinen zijn met $A \supseteq B$ en dat A algebraïsch is over B , dan is A een lichaam dan en slechts dan als B dat is.*

Bewijs:⁶⁰ Stel $x \in A$ dan bestaat er een monisch polynoom in $B[X]$, waarvan x een wortel is, we kiezen degene met minimale graad. Merk op dat we het polynoom monisch kunnen veronderstellen omdat B een lichaam is en we door de eerste coëfficiënt kunnen delen. We hebben dus:

$$f(x) = x^n + \dots + a_{n-1}x + a_n, \quad a_i \in A$$

en we claimen dat $a_n \neq 0$. Stel namelijk dat a_n wel nul is, dat schrijven we $f(x)$ als

$$f(x) = x(x^{n-1} + \dots + a_{n-1}) = 0.$$

⁶⁰Dit bewijs komt uit [2] lecture 6.

Uit het feit dat A een domein is volgt dat of $x = 0$ of $x^{n-1} + \dots + a_{n-1} = 0$, in beide gevallen hebben we tegenspraak in het eerste geval met het feit dat we aangenomen hebben dat x ongelijk nul is, in het tweede geval met de minimaliteit van de graad van $f(x)$. We concluderen $a_n \neq 0$ en constureren:

$$x \cdot a_n^{-1}(-x^{n-1} + \dots - a_{n-1}) = 1.$$

We hebben dus een multiplicatieve inverse van x gevonden en we concluderen dat A een lichaam is.

Andersom, als we aanemen dat A een lichaam is en $x \in B$ een element ongelijk 0, geldt er dat $x^{-1} \in A$ en omdat A algebraïsch is over B bestaat er een monisch polynoom $g(X) \in B[X]$ met:

$$g(x^{-1}) = (x^{-1})^m + \dots + b_{m-1}x^{-1} + b_m = 0, \quad b_i \in B.$$

Wanneer we vermenigvuldigen met x^{m-1} verkrijgen we:

$$\begin{aligned} x^{-1} + b_1 + \dots + b_m x^{m-1} &= 0 \\ x^{-1} &= -(b_1 + \dots + b_m x^{m-1}) \in B. \end{aligned}$$

We hebben dus een multiplicatieve inverse van x in B en we concluderen dat B een lichaam is. \square

Lemma 5.4 *De ring der gehelen $\mathbb{Z}[\zeta]$ is een Dedekind-ring.*

Bewijs: We weten dat $\mathbb{Z}[\zeta]$ een domein is en we hebben aangenomen dat $\mathbb{Z}[\zeta]$ Noethers is (zie eventueel voetnoot 26).

Om te zien dat $\mathbb{Z}[\zeta]$ zijn eigen integrale afsluiting is⁶¹ is het genoeg om te herinneren dat $\mathbb{Z}[\zeta]$ de ring der gehelen is en dat elk element daarin te schrijven is als wortel van een monisch polynoom in \mathbb{Z} (dus $\mathbb{Z}[\zeta]$ is zelfs algebraïsch over \mathbb{Z} dan ook zeker over $\mathbb{Z}[\zeta]$).

Als laatste moeten we bewijzen dat elk priemideaal ongelijk nul ook maximaal is. Ik zal hiervoor de aanpak van [2], lecture 6 gebruiken, die gebruik maakt van het feit dat wanneer je een ring deelt door een maximaal ideaal, je een lichaam verkrijgt. Zij \mathfrak{p} een priemideaal in $\mathbb{Z}[\zeta]$, we zullen bewijzen dat $\mathbb{Z}[\zeta]/\mathfrak{p}$ een lichaam is. Omdat $\mathbb{Z} \subset \mathbb{Z}[\zeta]$ geldt ook dat:

$$\mathbb{Z}[\zeta]/\mathfrak{p} \supseteq \mathbb{Z}/(\mathbb{Z} \cap \mathfrak{p}).$$

Omdat $\mathbb{Z} \cap \mathfrak{p}$ een priemideaal in \mathbb{Z} is wordt hij voortgebracht door een priemgetal, zeg p , we schrijven dus $\mathbb{Z} \cap \mathfrak{p} = \langle p \rangle$. We weten dat $\mathbb{Z}/\langle p \rangle$ een lichaam is. Wanneer we kunnen bewijzen dat $\mathbb{Z}[\zeta]/\mathfrak{p}$ algebraïsch over $\mathbb{Z}/\langle p \rangle$ is, kunnen we met behulp van lemma 5.2 concluderen dat ook $\mathbb{Z}[\zeta]/\mathfrak{p}$ een lichaam is en verder, met behulp van lemma 5.1, dat het priemideaal \mathfrak{p} maximaal is.

Stel dat \bar{x} een element van $\mathbb{Z}[\zeta]/\mathfrak{p}$ is en x een representant van de restklasse \bar{x} . Aangezien x een element is van $\mathbb{Z}[\zeta]$ is het de wortel van een monisch polynoom in \mathbb{Z} , want $\mathbb{Z}[\zeta]$ is algebraïsch over \mathbb{Z} . We schrijven:

$$f(x) = x^n + \dots + a_{n-1}x + a_n = 0, \quad a_i \in \mathbb{Z}$$

wanneer we deze vergelijking modulo \mathfrak{p} bekijken, verkrijgen we:

$$\overline{f(x)} = \bar{x}^n + \dots + \bar{a}_{n-1}\bar{x} + \bar{a}_n = \bar{0},$$

⁶¹Men noemt dit ook wel algebraïsch gesloten.

waarbij \bar{a}_i de restklassen van a_i zijn modulo $\mathbb{Z} \cap \mathfrak{p} = \langle p \rangle$, oftewel $\bar{a}_i \in \mathbb{Z}/\langle p \rangle$ en we zien dat $\overline{f(x)} \in \mathbb{Z}_p[X]$ en concluderen dat $\mathbb{Z}[\zeta]/\mathfrak{p}$ algebraïsch is over $\mathbb{Z}/\langle p \rangle$ en hieruit volgt dat $\mathbb{Z}[\zeta]$ een Dedekind-ring is. \square

Zoals we in paragraaf 5.1 al gezien hebben hebben we soms meer idealen nodig dan alleen de hoofdidealen van een ring, we zouden ook van deze verzameling idealen graag een groep maken.⁶² Hiertoe moet elk ideaal een inverse hebben, dit zal voor de idealen van de ring der gehelen van een getallenlichaam in het algemeen niet mogelijk zijn, we zullen daartoe de idealen ingebed zien in een grotere structuur waarin we wel een groep kunnen construeren.

We kunnen de idealen in de ring der gehelen \mathcal{O}_K van K zien als *modulen*⁶³ over \mathcal{O}_K , een ideaal, of beter gezegd zijn elementen, kunnen immers op de ring \mathcal{O}_K werken door middel van het produkt op \mathcal{O}_K . Equivalent hiermee, maar misschien inzichtelijker is te zeggen dat een ideaal een \mathcal{O}_K -deelmoduul is van \mathcal{O}_K .⁶⁴

De uitbreiding bestaat nu hierin dat we niet alleen naar \mathcal{O}_K -deelmodulen van \mathcal{O}_K kijken maar ook naar \mathcal{O}_K -deelmodulen van het quotientlichaam⁶⁵ van \mathcal{O}_K .

Een \mathcal{O}_K -deelmoduul \mathfrak{a} van het quotientlichaam van \mathcal{O}_K noemen we een *gebroken ideaal* van \mathcal{O}_K als we kunnen schrijven $c\mathfrak{a} \subseteq \mathcal{O}_K$ voor zekere $c \in \mathcal{O}_K$. Dit betekent dat $c\mathfrak{a}$ een \mathcal{O}_K -deelmoduul is van \mathcal{O}_K en dus een ideaal van \mathcal{O}_K , zie voetnoot 64. We noteren $\mathfrak{b} = c\mathfrak{a}$ en we zien dat elk gebroken ideaal van de vorm $\mathfrak{a} = c^{-1}\mathfrak{b}$ is, waarbij c^{-1} in het quotientlichaam van \mathcal{O}_K ligt. We zijn nu al veel dichter bij een definitie van een inverse van een ideaal, in het geval van een hoofdideaal kunnen we al een inverse definiëren, immers zij $\langle a \rangle$ een ideaal in \mathcal{O}_K , dan geldt voor het gebroken ideaal $a^{-1}\mathcal{O}_K$ dat:

$$\langle a \rangle a^{-1} \mathcal{O}_K = \langle aa^{-1} \rangle = \mathcal{O}_K$$

we kunnen dus met recht $a^{-1}\mathcal{O}_K$ als $\langle a \rangle^{-1}$ definiëren.⁶⁶ Merk op, dat \mathcal{O}_K een eenheid is, aangezien het alle idealen van zichzelf bevat, en daarom al die idealen ook deelt. Voor het gemak zullen we het quotientlichaam van \mathcal{O}_K noteren als \mathcal{Q}_K . Voor een algemeen ideaal \mathfrak{a} in \mathcal{O}_K definiëren we, in overeenstemming met voorgaande:

$$\mathfrak{a}^{-1} = \{x \in \mathcal{Q}_K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

Uit de definitie van (deel)moduul volgt direct dat dit een \mathcal{O}_K -deelmoduul van \mathcal{Q}_K is. We zullen bewijzen dat dit de inverse van \mathfrak{a} is. Hiertoe moeten we eerst nog een tweetal tussenresultaten behandelen.

Lemma 5.5 *In een Dedekind-ring R geldt voor een ideaal \mathfrak{i} ongelijk nul dat er priemidealen \mathfrak{p}_i bestaan zodanig dat $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n \subseteq \mathfrak{i}$.*

Bewijs: Stel van niet, stel dat Σ de verzameling idealen is waarvoor dit niet geldt, dan is Σ niet leeg en heeft een maximaal element, zie eventueel voetnoot 29. We noemen dit element \mathfrak{m} , dit kan niet een priemideaal zijn en we kunnen hierdoor

⁶²In de volgende paragraaf zullen we veel uitgebreider op deze groep ingaan.

⁶³Voor een korte inleiding over (deel)modulen zie [10], hoofdstuk 5 paragraaf 4

⁶⁴Er geldt zelfs dat elk \mathcal{O}_K -deelmoduul van \mathcal{O}_K een ideaal in \mathcal{O}_K is, dit volgt rechtstreeks uit de definitie van deelmoduul en ideaal.

⁶⁵Voor een duidelijke korte inleiding op quotientlichamen, zie [10] hoofdstuk 3 paragraaf 4

⁶⁶Het is belangrijk te zien dat we het nu niet meer over idealen in \mathcal{O}_K hebben maar over \mathcal{O}_K -submodulen van het quotientlichaam van \mathcal{O}_K , a^{-1} is namelijk een element van het quotientlichaam en niet van \mathcal{O}_K , wanneer we dit onthouden kunnen we bovenstaande operaties zien als operaties op \mathcal{O}_K -submodulen en blijven ze betekenis houden.

dus een element $ab \in \mathfrak{m}$ vinden zodanig dat $a, b \notin \mathfrak{m}$. We construeren de idealen⁶⁷ $\mathfrak{a} = \langle \mathfrak{m}, a \rangle$ en $\mathfrak{b} = \langle \mathfrak{m}, b \rangle$, deze zijn beide strikt groter dan \mathfrak{m} aangezien ze elementen bevatten die niet in \mathfrak{m} liggen. Deze idealen kunnen niet in Σ liggen en hebben zodoende een factorisatie in priemidealen:

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n, \quad \mathfrak{b} = \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Voor hun produkt $\mathfrak{a}\mathfrak{b}$ geldt de volgende factorisatie:

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

De elementen van $\mathfrak{a}\mathfrak{b}$ hebben de volgende vorm: $c \cdot am$, $c \cdot bm$, $c \cdot m^2$, $c \cdot ab$ of eindige sommaties hiervan, waarbij $c \in R$ en $m \in \mathfrak{m}$. We concluderen dat alle elementen van $\mathfrak{a}\mathfrak{b}$ in \mathfrak{m} liggen en zodoende dat $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{m}$, oftewel $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_m \subseteq \mathfrak{m}$ en dit levert een tegenspraak op aangezien we hadden aangenomen dat \mathfrak{m} juist niet aan de voorwaarde voldeed. \square

Lemma 5.6 *Zij \mathcal{O}_K een Dedekind-ring en \mathfrak{p} een priemideaal in \mathcal{O}_K ongelijk nul, dan geldt $\mathfrak{p}^{-1} \neq \mathcal{O}_K$*

Bewijs: Als eerste merken we op dat $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$ aangezien voor elk element $x \in \mathcal{O}_K$ geldt $x\mathfrak{p} \subseteq \mathfrak{p} \subseteq \mathcal{O}_K$.

We zijn dus op zoek naar een element x uit het quotientlichaam \mathcal{Q}_K van \mathcal{O}_K zodanig dat $x \in \mathfrak{p}^{-1}$ en $x \notin \mathcal{O}_K$. We zullen dit doen door x te schrijven als $x = a^{-1}b$ voor zekere $a, b \in \mathcal{O}_K$. Dit is altijd mogelijk aangezien \mathcal{Q}_K een lichaam is. De twee eigenschappen van x vertalen zich respectievelijk als $b\mathfrak{p} \subseteq \langle a \rangle$ en $b \notin \langle a \rangle$. Dit komt voort uit het feit dat

$$a^{-1}b \in \mathfrak{p}^{-1} \iff a^{-1}b\mathfrak{p} \subseteq \mathcal{O}_K \iff b\mathfrak{p} \subseteq a\mathcal{O}_K = \langle a \rangle$$

en het feit dat

$$a^{-1}b \notin \mathcal{O}_K \iff b \neq c \cdot a \ \forall c \in \mathcal{O}_K \iff b \notin \langle a \rangle.$$

Zij a een element van \mathfrak{p} ongelijk nul, naar aanleiding van lemma 5.5 zijn er priemidealen \mathfrak{p}_i te vinden zodanig dat $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq \langle a \rangle$, en we kiezen r minimaal. Uit het feit dat $a \in \mathfrak{p}$ volgt dat $\langle a \rangle \subseteq \mathfrak{p}$ oftewel $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq \mathfrak{p}$. Dit geeft ons:

$$\mathfrak{p} | \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \iff \exists_i \mathfrak{p} | \mathfrak{p}_i \iff \exists_i \mathfrak{p}_i \subseteq \mathfrak{p}.$$

Omdat \mathcal{O}_K een Dedekind-ring is is elk priemideaal ongelijk nul maximaal, dus we concluderen $\mathfrak{p}_i = \mathfrak{p}$. (vanaf nu $\mathfrak{p}_i = \mathfrak{p}_1$)

Wanneer nu $r = 1$ dan verkrijgen we $\mathfrak{p} = \langle a \rangle$ en we concluderen $\mathfrak{p} \neq \mathcal{O}_K$, we kunnen dus aannemen dat $r > 1$. Omdat r minimaal gekozen is kan niet gelden dat $\mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq \langle a \rangle$, anders zouden we $\tilde{r} = r - 1$ kunnen kiezen. Er is dus een $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ zodanig dat $b \notin \langle a \rangle$. We zien dat voor $b\mathfrak{p}$ geldt:

$$b\mathfrak{p} = b\mathfrak{p}_i \subseteq \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq \langle a \rangle.$$

We hebben dus een b geconstrueerd die voldoet, dit geeft ons een $x \in \mathfrak{p}$ met $x \notin \mathcal{O}_K$ en we concluderen $\mathfrak{p} \neq \mathcal{O}_K$. \square

⁶⁷Deze zijn gedefinieerd als de kleinste idealen die \mathfrak{m} en a of b bevatten, respectievelijk, en zijn zodoende bona fide idealen.

Lemma 5.7 *Zij \mathcal{O}_K een Dedekind-ring en \mathfrak{p} een priemideaal in \mathcal{O}_K , dan is \mathfrak{p}^{-1} een gebroken ideaal van \mathcal{O}_K waarvoor geldt: $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.*

Bewijs: Wegens de definitie van \mathfrak{p}^{-1} geldt voor alle $x \in \mathfrak{p}^{-1}$ dat $x\mathfrak{p} \subseteq \mathcal{O}_K$, dus we zien dat \mathfrak{p}^{-1} een gebroken ideaal van \mathcal{O}_K is, aangezien $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K \forall \mathfrak{p} \in \mathfrak{p}$.

Aangezien $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$ (zie lemma 5.6) geldt $\mathfrak{p} = \mathcal{O}_K\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. Omdat \mathcal{O}_K een Dedekind-ring is is elk priemideaal maximaal, er moet dus gelden: $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ of $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$. Het eerste geval zou betekenen dat \mathfrak{p}^{-1} het eenheidsideaal is, en we hebben gezien (zie voetnoot 58) dat dit eenheidsideaal uniek en \mathcal{O}_K zelf is, we zouden dus verkrijgen $\mathfrak{p}^{-1} = \mathcal{O}_K$, wat onmogelijk is wegens lemma 5.6. We concluderen $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. \square

Stelling 5.1 *In een Dedekind-ring R factoriseert elk ideaal, ongelijk $\langle 0 \rangle$ of $\langle 1 \rangle$, op een unieke manier als produkt van priemidealen.*

Bewijs: We zullen als eerste bewijzen dat een mogelijke factorisatie in priemidealen uniek is. Stel dat

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_m \quad (29)$$

waarbij allen priemidealen zijn. aangezien het priemideaal \mathfrak{p}_1 het linkerlid van bovenstaande uitdrukking deelt, hebben we voor zekere i dat $\mathfrak{p}_1|\mathfrak{q}_i$. Zonder beperking van algemeenheid nemen we aan dat $\mathfrak{q}_i = \mathfrak{q}_1$ en concluderen $\mathfrak{p}_1 = \mathfrak{q}_1$. We kunnen nu beide kanten in vergelijking 29 vermenigvuldigen met \mathfrak{p}_1^{-1} en verkrijgen:

$$\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_n = \mathfrak{q}_2\mathfrak{q}_3 \dots \mathfrak{q}_m.$$

Wanneer we deze procedure herhalen, zal het op een gegeven moment moeten stoppen⁶⁸ waarnaar we concluderen $\mathfrak{p}_i = \mathfrak{q}_i$ voor alle i . We concluderen dat factorisatie in priemidealen uniek is.

Zij Σ de verzameling van idealen, naast $\langle 0 \rangle$ en $\langle 1 \rangle$, die *niet* te schrijven zijn als produkt van priemidealen. We nemen aan dat deze verzameling niet leeg is en dus een maximaal element heeft dat we zullen aanduiden met \mathfrak{m} (zie eventueel voetnoot 29). Dit ideaal moet bevat zijn in een zeker maximaal ideaal dat we \mathfrak{p} zullen noemen⁶⁹. Wegens de inclusies $R \subseteq \mathfrak{p}^{-1}$ en $\mathfrak{m} \subseteq \mathfrak{p}$ verkrijgen we:

$$\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R. \quad (30)$$

We construeren het gebroken ideaal $\mathfrak{m}\mathfrak{p}^{-1}$ hiervoor geldt $\mathfrak{m}\mathfrak{p}^{-1} \neq \mathfrak{m}$, wegens de opmerking in het bewijs van lemma 5.7 en met vergelijking 30 concluderen we dat $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1}$. Zodoende moet $\mathfrak{m}\mathfrak{p}^{-1}$ wel een priemfactorisatie bezitten (herinner dat \mathfrak{m} maximaal was gekozen). We vermenigvuldigen beide kanten met \mathfrak{p} en verkrijgen:

$$\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n\mathfrak{p}$$

een tegenspraak, we concluderen dat Σ leeg is en dat zodoende ieder ideaal van R uniek te schrijven is als produkt van priemidealen. \square

⁶⁸Hier nemen we dus impliciet aan dat elk ideaal maar eindig veel delers heeft, wat in een Noethers domein natuurlijk niet zo een gekke aanneme is, we zullen dat hier echter niet bewijzen.

⁶⁹Dit volgt uit Zorn's lemma, waarbij we als inductieve geordende verzameling de idealen $\mathfrak{a} \supseteq \mathfrak{m}$ met $\mathfrak{a} \neq R$ nemen met als ordening " \supseteq ", deze verzameling heeft als bovengrens het ideaal R en is dus daadwerkelijk een inductief geordende verzameling en heeft wegens Zorn's lemma een maximaal element. Voor Zorn's lemma zie [10] hoofdstuk 10 paragraaf 2.

5.3 De ideaalklassengroep

In deze paragraaf zullen we de verzameling idealen ook daadwerkelijk tot een groep maken, en hier een belangrijke eigenschap uit afleiden. Het is misschien goed om te herinneren dat we in dit hoofdstuk een voortzetting van het bewijs van FLT zoeken, daarvoor hebben we nodig dat de p -de macht van een hoofdideaal weer een hoofdideaal is. We zullen dit in onze, te construeren, groep afleiden door groeptheoretische overwegingen.

Lemma 5.8 *De verzameling van gebroken idealen van de ring der gehelen $\mathbb{Z}[\zeta]$ is een groep.*

Bewijs: Elk gebroken ideaal \mathfrak{a} in $\mathbb{Z}[\zeta]$ is te schrijven als $\mathfrak{a} = c^{-1}\mathfrak{b}$, waarbij $c \in \mathbb{Z}[\zeta]$ en \mathfrak{b} een ideaal van $\mathbb{Z}[\zeta]$ is. Omdat \mathfrak{b} een ideaal in $\mathbb{Z}[\zeta]$ is, is het te schrijven als produkt van priemidealen: $\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$. We definiëren, in overeenstemming met het voorgaande:

$$\mathfrak{b}^{-1} = c\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \dots \mathfrak{p}_n^{-1}$$

Hiervoor geldt:

$$\mathfrak{b}^{-1}\mathfrak{b} = \mathfrak{b}\mathfrak{b}^{-1} = c^{-1}c \cdot \mathfrak{p}_1^{-1}\mathfrak{p}_1\mathfrak{p}_2^{-1}\mathfrak{p}_2 \dots \mathfrak{p}_n^{-1}\mathfrak{p}_n = \mathbb{Z}[\zeta]$$

elk element heeft dus een inverse. Het eenheidselement \mathfrak{e} is zoals gezegd $\mathbb{Z}[\zeta]$ we zien dat de verzameling van gebroken idealen gesloten is onder vermenigvuldiging, we hebben dus een multiplicatieve (abelse) groep. \square

We zullen deze groep \mathfrak{G} noemen. Het is goed om op te merken dat de gebruikelijke optelling van idealen (door alle elementen van beide idealen op te tellen) ook op deze groep blijft gedefiniëerd, we zullen dit later nog nodig hebben, vooralsnog echter zijn de groepeigenschappen belangrijker.

We zien dat de verzameling van gebroken hoofdidealen een (normale) ondergroep is, dit is al ter sprake gekomen in vorige paragraaf, we zullen deze groep aanduiden met \mathfrak{H} . Uit deze beide groepen construeren we de *ideaalklassengroep* van $\mathbb{Z}[\zeta]$:

$$\mathfrak{Cl} = \frac{\mathfrak{G}}{\mathfrak{H}}.$$

Omdat deze groep uit equivalentieklassen bestaat noteren we een element van deze groep als $[\mathfrak{a}]$ waarbij \mathfrak{a} een representant is van zijn equivalentieklasse. Twee gebroken idealen \mathfrak{a} en \mathfrak{b} behoren tot dezelfde equivalentieklasse als:

$$\mathfrak{a} \equiv \mathfrak{b} \pmod{\mathfrak{H}} \iff \mathfrak{a} = \langle c \rangle \mathfrak{b}$$

voor zekere $c \in \mathbb{Z}[\zeta]$. Het produkt van 2 zulke equivalentieklassen is:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{ab}].$$

Het klassegetal van $\mathbb{Z}[\zeta]$ is gedefiniëerd als de orde van de ideaalklassengroep van $\mathbb{Z}[\zeta]$, dit is een functie van p , herinner dat ζ een p -de eenheidswortel is. We noteren dit getal met $h(p)$. Dit getal is eindig⁷⁰.

Omdat de ideaalklassengroep eindig is, met orde h geldt voor elk element $[\mathfrak{a}]^h = [\mathfrak{a}^h] = [e]$ wegens Langrange's Stelling⁷¹, dit betekent dat \mathfrak{a}^h congruent \mathfrak{e} modulo

⁷⁰We zullen dat niet bewijzen, maar een bewijs is te vinden in [4] hoofdstuk 3 paragraaf 7 Satz 2 of in [14] hoofdstuk 9 paragraaf 3 theorem 9.7.

⁷¹Zie bijvoorbeeld [1] hoofdstuk 11.

\mathfrak{h} is, oftewel \mathfrak{a}^h is een hoofdideaal. Stel nu dat p niet $h(p)$ deelt dan noemen we p *regulier*. Wanneer p een reguliere priem is, geldt dat zijn grootste gemene deler met $h(p)$ 1 is en we kunnen dus u en v in \mathbb{Z} vinden zodanig dat geldt: $up + vh(p) = 1$. Stel nu dat \mathfrak{a}^p een hoofdideaal is dan verkrijgen we dat ook \mathfrak{a} een hoofdideaal is. Er geldt immers:

$$[\mathfrak{a}] = [\mathfrak{a}^{up+vh(p)}] = [\mathfrak{a}^p]^u \cdot [\mathfrak{a}^{h(p)}]^v = [\mathfrak{a}^p]^u = [e].$$

Wegens de vermenigvuldingsregel op de groep van (hoofd)idealen concluderen we dat wanneer $\mathfrak{a} = \langle a \rangle$ dan $\langle a \rangle^p = \langle b \rangle$ en $b = u \cdot a^p$ voor een zekere eenheid u in $\mathbb{Z}[\zeta]$.

5.4 Uitbreiding voor FLT naar reguliere priemen

De klasse van reguliere priemen is veel groter dan de klasse van priemen die een UFD oplevert, wanneer $\mathbb{Z}[\zeta]$ een PID is is zijn klassegroep triviaal, elk ideaal is immers een hoofdideaal, en het klassegetal (1) is niet deelbaar door p . Anderzijds zijn er wel veel priemen die regulier zijn en toch geen UFD (of equivalent PID) opleveren. Bijvoorbeeld voor $p = 23$ gaat het voor het eerst mis, terwijl alle priemen onder de 37 regulier zijn. Ik heb achterin een tabel opgenomen, uit [4], met alle priemgetallen onder de 100 met hun bijbehorende klassegetal. We zullen in deze paragraaf het bewijs van FLT uitbreiden naar de gevallen waarin p regulier is en zodoende de stelling een veel grotere geldigheid geven. Wanneer we naar de bewijzen van het eerste en tweede geval kijken valt op dat we maar op een paar plaatsen gebruik hebben gemaakt van unieke factorisatie eigenschappen, deze zullen we nu behandelen.

Bij het eerste geval van FLT verkrijgen we factorisatie

$$(x + y)(x + y\zeta)(x + y\zeta^2) \dots (x + y\zeta^{p-1}) = -z^p, \quad (31)$$

hieruit leiden we een equivalente factorisatie van idealen af:

$$\langle x + y \rangle \langle x + y\zeta \rangle \langle x + y\zeta^2 \rangle \dots \langle x + y\zeta^{p-1} \rangle = \langle -z^p \rangle. \quad (32)$$

We zullen aantonen dat deze idealen relatief priem zijn, stel namelijk van niet dan hebben ze een ideaaldeler \mathfrak{d} gemeenschappelijk, stel voor het gemak dat het om de eerst twee termen gaat dan geldt:

$$\mathfrak{d} | \langle x + y \rangle \text{ en } \mathfrak{d} | \langle x + y\zeta \rangle \Rightarrow \mathfrak{d} | \langle x + y \rangle - \langle x + y\zeta \rangle = \langle (\zeta - 1)y \rangle,$$

idem $\mathfrak{d} | \langle (\zeta - 1)x \rangle$. Nu zien we ook dat de aanname dat het om de eerste twee termen gaat geen beperking van algemeenheid is aangezien we in een ander geval hoogstens een eenheid ζ^s zouden verschillen en dit dezelfde idealen oplevert. We verkrijgen dus,

$$\begin{cases} (\zeta - 1)y \in \mathfrak{d}, \\ (\zeta - 1)x \in \mathfrak{d}. \end{cases}$$

Omdat x en y relatief priem zijn in \mathbb{Z} zijn er u en v te vinden zodanig dat $ux + vy = 1$ we verkrijgen dat dus ook het element $u(\zeta - 1)x + v(\zeta - 1)y = (\zeta - 1)$ in \mathfrak{d} ligt. Hierdoor ligt ook p , dat immers een veelvoud van $(\zeta - 1)$ is in \mathfrak{d} . Maar $\langle p \rangle$ is een priemideaal, uit $ab \in \langle p \rangle$ volgt immers $p | ab$ en in \mathbb{Z} betekent dat $p | a$ of $p | b$ oftewel $a \in \langle p \rangle$ of $b \in \langle p \rangle$. We hebben dus een priemideaal \mathfrak{d} die een ander priemideaal $\langle p \rangle$ deelt, we concluderen $\mathfrak{d} = \langle p \rangle$ en uit de factorisatie van $-z^p$, vergelijking 31, verkrijgen we:

$$\langle p \rangle | \langle x + y \rangle \iff p | x + y \iff p | z$$

en we hebben een tegenspraak, want we bevinden ons in het eerste geval, waarbij $p \nmid xyz$. We hebben dus een factorisatie (namelijk vergelijking 5.4) in idealen die allen

paarsgewijs priem zijn. Voor elke factor in vergelijking geldt dat zijn priemdelers een p -de macht delen, en dus zelf als p -de machten voorkomen, elk ideaal in vergelijking heeft dus de vorm \mathfrak{a}^p . Omdat p regulier is volgt uit de vergelijking $\langle x + y\zeta \rangle = \mathfrak{a}^p$ dat \mathfrak{a} een hoofdideaal moet zijn, \mathfrak{a}^p is het immers ook. We schrijven $\mathfrak{a} = \langle \alpha \rangle$ en concluderen

$$x + y\zeta = u\alpha^p$$

waarna we verder kunnen met het bewijs zoals het is gegeven in hoofdstuk 3.

In het tweede geval kunnen precies hetzelfde doen, voor de factorisatie

$$\left(\frac{x+y}{\pi}\right)\left(\frac{x+y\zeta}{\pi}\right)\dots\left(\frac{x+y\zeta^{p-1}}{\pi}\right) = \left(\frac{-\pi^{pk+p}z_0^p}{\pi^p}\right).$$

Waar we wederom een factorisatie in idealen aan kunnen koppelen:

$$\left\langle \frac{x+y}{\pi} \right\rangle \left\langle \frac{x+y\zeta}{\pi} \right\rangle \dots \left\langle \frac{x+y\zeta^{p-1}}{\pi} \right\rangle = \left\langle -\pi^{pk}z_0^p \right\rangle.$$

Al deze idealen zijn paarsgewijs priem en dus p -de machten:

$$\left\langle \frac{x+y\zeta}{\pi} \right\rangle = \mathfrak{a}^p \iff \frac{x+y\zeta^1}{\pi} = e_1 t_1^p,$$

voor zekere eenheid e_1 en algebraïsch geheel t_1 . Hiernaar kunnen we verder met het bewijs zoals het gegeven is in hoofdstuk 4.

We zien dus dat beide gevallen van FLT uit te breiden zijn naar reguliere priem-exponenten, en dus een veel bredere geldigheid hebben verkregen.

Referenties

- [1] M.A.Armstrong, Groups and symmetry, Springer-Verlag (1988)
- [2] M. Baker, Algebraic Number Theory course notes (2002)
<http://www.math.uga.edu/~mbaker/papers.html>.
- [3] F.Beukers, Dictaat, Elementaire getaltheorie (2001).
- [4] S.Borewicz & I.R.Safarevic, Zahlentheorie, Birkhäuser Verlag (1966)
- [5] G.Cornelissen, Dictaat, Galoistheorie (2003)
- [6] G.H Hardy & E.M Wright, An introduction to the theory of numbers (4th ed.) Oxford University Press (1938, 1975)
- [7] Hellegouarch, Invitation aux mathématiques de Fermat-Wiles, Dunod (2001)
- [8] V.J.Katz, A history of mathematics, 2nd edition, Addison-Wesley (1998), p.650-661
- [9] E.Kummer, De numeris complexis, qui radicibus unitatus et numeris integris constant, Journal de mathématiques pures et appliquées 12 (1847) p.185-212, also reprinted in his Collected Papers, Springer-Verlag (1975), vol. 1, p.165-192, p.182
- [10] S.Lang, Undergraduate Algebra, 2nd edition, Springer-Verlag (1987,1990).
- [11] D.A.Marcus, Number Fields, Springer-Verlag (1977)
- [12] J.S.Milne, Algebraic Number Theory (1998)
<http://www.jmilne.org/math/index.html>.
- [13] J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag (1992).
- [14] Stewart and Tall, Algebraic number theory, Chapman and Hall (1979).
- [15] D.R.Wilkins, Hilary Term (2002) Introduction to Galois theory (part 3).

6 Appendix

p	$h(p)$	commentaar
3	1	
5	1	
7	1	
11	1	
13	1	
17	1	
19	1	
23	3	Het eerste priemgetal waarvoor $\mathbb{Z}[\zeta]$ geen UFD is.
29	2^3	
31	3^2	
37	37	Het eerste irreguliere priemgetal.
41	11^2	
43	211	
47	5·139	
53	4 889	
59	3·59·233	Het tweede irreguliere priemgetal.
61	41·1 861	
67	67·12 739	Het derde irreguliere priemgetal.
71	7^2 ·79 241	
73	89·134 353	
79	5·53·377 911	
83	3·279 405 653	
89	113·118 401 449	
97	577·3 457·206 209	