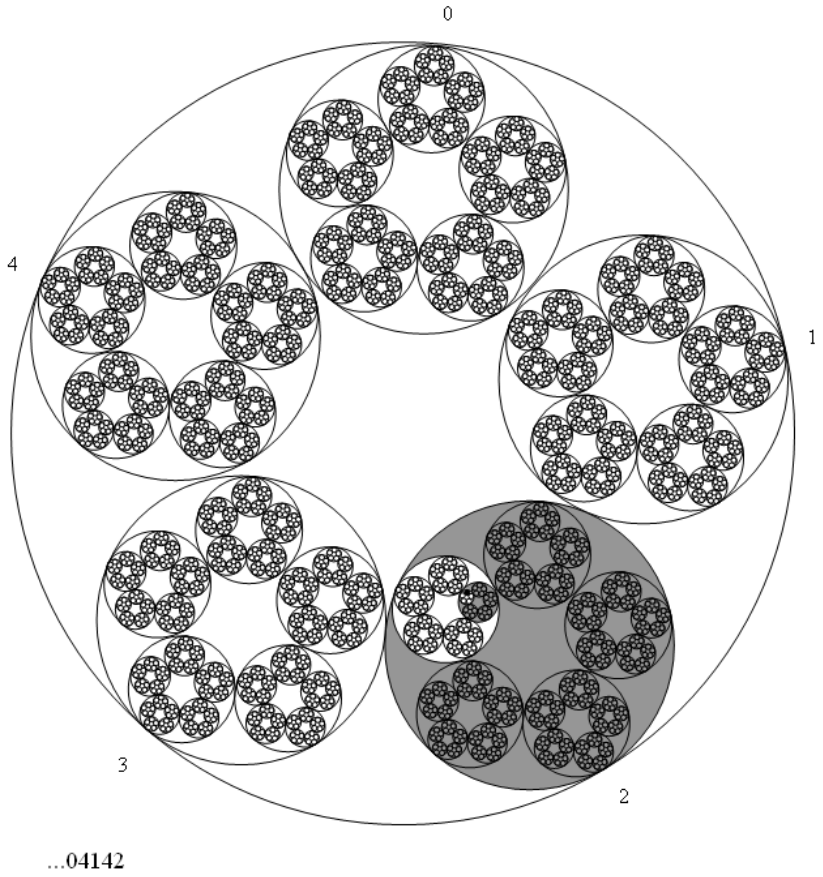
Introductie tot de p-adische getallen

Profielwerkstuk Junior College Utrecht

Lars van den Berg, Joep van den Hoven, Linda van der Spaa
Onder begeleiding van dr. R.W. Bruggeman

26 februari 2010[1]



[1]Laatst gewijzigd: 20 november 2011

Voorwoord

We zijn zo gewend om met de reële getallen te rekenen dat we er meestal niet bij stilstaan wat een getal eigenlijk is. Het begrip 'getal' heeft in de loop van de geschiedenis echter een grote ontwikkeling doorgemaakt. De oude Grieken bijvoorbeeld geloofden alleen in de rationale getallen (de 'breuken' a/b met a, b geheel), irrationale getallen als $\sqrt{2}$ en π bezorgden hen veel hoofdpijn en ruzies. Pas een paar honderd jaar geleden werden de negatieve getallen algemeen geaccepteerd in de westerse wiskunde. De ontdekking van de complexe getallen is erg moeizaam verlopen, en heeft uiteindelijk heel de wiskundige gedachtenwereld op z'n kop gezet. Hoe kon zoiets bestaan als een imaginair getal? Het duurde tot Gauss (rond 1830) voor de complexe getallen echt op een wiskundig bonafide manier werden bestudeerd. Wiskundigen begonnen steeds meer te beseffen dat de filosofische vraag 'bestaat het getal wel' niet zo veel zin heeft, een antwoord op de vragen 'hoe gedraagt het zich' en 'wat voor verbanden heeft het met andere wiskunde' geven veel meer inzicht. Dit is zeker het geval bij de p-adische getallen, die rond 1897 zijn ontdekt door Kurt Hensel. Voor beginners is het moeilijk je iets concreets bij deze getallen voor te stellen, en zeker je ervan te overtuigen dat ze bestaan: ze lijken ergens is de mist van het bovennatuurlijke te zweven, voor eeuwig onbereikbaar. Ze mogen dan wel zo ontastbaar zijn als de sterren, we kunnen ze in elk geval proberen te begrijpen, en de studie naar deze getallen is de afgelopen eeuw zeer vruchtbaar gebleken.

De p-adische getallen zijn in zekere zin precies het omgekeerde van de reële getallen. Bijvoorbeeld $65.7204851\ldots$ 'is' een reëel getal (hoewel de vraag open blijft hoe hij verder doorloopt); links van de komma mogen maar eindig veel cijfers staan, rechts heeft hij de vrijheid zich tot in het oneindige uit te strekken. We kunnen zo'n getal zien als limiet van een rij rationale getallen die hem steeds beter benadert maar nooit precies bereikt, bijvoorbeeld $60, 65, 65.7, 65.72, \ldots$ Een voorbeeld van een p-adisch getal is $\ldots 1584027.56$: we hebben het getal van daarnet omgeklapt. We kunnen het zien als limiet van de rij $0.06, 0.56, 7.56, 27.56, \ldots$ Maar bestaat deze limiet wel, en is dit getal niet oneindig groot? Dat hangt er vanaf hoe je het bekijkt. In de p-adische wereld worden de cijfers juist minder belangrijk naarmate ze verder naar links liggen. Als we de rij $0.06, 0.56, 7.56, 27.56, \ldots$ met een gewoon meetlint meten wordt het lint al snel te klein, maar als we ons p-adisch meetlint uit de kast halen komen de getallen wel degelijk steeds dichter bij elkaar te liggen en convergeert de rij naar een limiet. Volgens ons lint liggen dus bijvoorbeeld $\ldots 5227289$ en $\ldots 4227289$ heel dicht bij elkaar.

Met p-adische getallen kunnen we ook rekenen, dit gaat eigenlijk net zo als dat we

bij de reële getallen gewend zijn. Er blijken dan wel wonderlijke dingen te gebeuren. De p-adische getallen kennen bijvoorbeeld geen onderscheid tussen positieve en negatieve getallen. En als a groter is dan b, dan kan het zomaar zijn dat $a + c$ kleiner is dan $b + c$. Tussen de mystieke p-adisch getallen zitten zomaar getallen die we al lang kennen: alle rationale getallen komen ook voor tussen p-adische getallen. Ze zijn dan echter wel bijna onherkenbaar van gedaante veranderd.

Eerst moeten we leren rekenen met de getallen, dat is een belangrijke eerste stap om ze te begrijpen. Daarna nemen we een duik in de moderne algebra waar we hulpmiddelen zoeken om de p-adische getallen beter te bestuderen. Alles in de wiskunde hangt met elkaar samen, het zou kortzichtig zijn om wiskundige vragen te vermijden die op het eerste gezicht niet met p-adische getallen te maken hebben. We hopen dat je net zo veel plezier zult beleven aan het lezen hiervan als dat wij aan het schrijven hebben gehad.

Dat wij met plezier aan dit onderzoek hebben gewerkt was niet mogelijk geweest zonder de inspirerende gesprekken met Roelof Bruggeman. Hij heeft veel tijd besteed aan het begeleiden en in goede banen leiden van ons onderzoek. We hebben veel van hem geleerd, zowel zuivere wiskunde als het maken van een goed verslag, en we zijn hem veel dank verschuldigd. We ontvingen nuttig commentaar van Philip van Egmond, Corné Ruwaard, Erik Nonhebel en Marlien Sneller die het manuscript hebben doorgespit, we willen hen daar hartelijk voor danken.

Opmerking. Behalve dit voorwoord en het omslagplaatje hebben we vrijwel niets veranderd aan dit werkstuk. Het is daarom wiskundig van minder hoog niveau dan het werkstuk over de Laatste stelling van Fermat dat ook op mijn webpagina te vinden is, maar misschien daarom juist waardevoller voor vwo-leerlingen: er wordt minder voorkennis vereist. Toch wil ik graag kwijt dat de p-adische getallen veel en veel meer omvatten dan we in dit werkstuk konden behandelen of zelfs maar konden vermoeden. Ze zijn essentieel in de moderne getaltheorie, maar om te begrijpen waarom heb je min of meer drie jaar universitaire wiskunde nodig. De link met getaltheorie kunnen we als volgt zien: bijvoorbeeld de rij $6, 56, 756, 2756, \ldots$ met als grondtal het priemgetal p stelt het getal $\ldots 2756$ voor modulo $p, p^2, p^3, p^4, p^5 \ldots$. Rekenen modulo m is in zekere zin 'informatie vergeten' of 'minder nauwkeurig naar het getal kijken' zodat het getal eenvoudiger wordt, en hoe groter m, hoe groter de 'graad van nauwkeurigheid'. We zoomen dus steeds verder in, en als we dit tot in het oneindige herhalen hebben we het getal 'gelift' naar de p-adische wereld. Er zit veel getaltheoretische informatie in verstopt, maar daar blijft het niet bij: net als bij de reële getallen kunnen we de analyse inschakelen. Zo kunnen we bijvoorbeeld de afgeleide bekijken van een functie van een p-adische variabele, en we kunnen het hebben over e^x met x een p-adisch getal. Op deze manier wordt een brug gebouwd tussen twee ogenschijnlijk verschillende vakgebieden. Dit alles kunnen we hier helaas niet behandelen, maar toch ben ik ervan overtuigd dat er genoeg interessants overblijft om te inspireren tot verdere studie.

Alle correcties en suggesties voor verbetering kun je sturen naar lars.vd.berg@kpnmail.nl.

Lars van den Berg, november 2011

Inhoudsopgave

Hoofdstuk 1

Kennismaking met g-adische getallen

In de volgende hoofdstukken gaan we de g-adische getallen formeel definiëren en aan de hand daarvan een aantal stellingen bewijzen. Voordat we dit doen is het belangrijk dat we eerst een goed intuïtief beeld hebben van wat deze getallen voorstellen. Dat doen we in dit hoofdstuk: alles wat hier wordt besproken is nog puur informeel. Maak je daarom geen zorgen over 'vage' definities en formules, het meer precieze werk komt later.

Merk op dat we hier g-adisch schrijven in plaats van p-adisch. g of p is een *constante* en stelt het grondtal voor; zo hebben de 10-adische getallen als grondtal 10. Later zal blijken dat het speciale geval dat g een *priemgetal* is, een belangrijke rol speelt. Voortaan als we p-adisch schrijven is p een willekeurig priemgetal; als er g-adisch staat, is g een willekeurig natuurlijk getal[1] groter dan 1.

Door de tekst heen staan hier en daar oefeningen, die helpen je de stof beter te begrijpen. De antwoorden staan op pagina 61.

In dit werkstuk gebruiken we een decimale punt in plaats van een decimale komma, zoals in de wetenschappelijke literatuur gebruikelijk is.

1.1 Wat zijn g-adische getallen?

Voordat we de bizarre wereld van de g-adische getallen gaan verkennen, is het verhelderend om eerst de bekende getallen eens nader te bekijken. Dan kunnen we daarna de analogie met de g-adische getallen gemakkelijker inzien.

We zijn gewend om met reële getallen te werken, dat zijn getallen die als volgt kunnen worden geschreven (met eventueel een minteken ervoor).

$$a_n \dots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \dots \tag{1.1}$$

Hier zijn a_i de *cijfers*, niet-negatieve gehele getallen kleiner het grondtal[2] g. De reële getallen zijn dus alle getallen die, uitgeschreven in cijfers, links van de komma eindig

[1] De natuurlijke getallen zijn de niet-negatieve gehele getallen, dus $0, 1, 2, 3, \dots$

[2] Voor het gemak gaan we voorlopig uit van grondtal 10.

veel cijfers hebben, en rechts oneindig veel. Bijvoorbeeld $\frac{1}{4} = 0.25 = 0.25000\ldots$ is een reëel getal, net als $\pi = 3.141592654\ldots$ en $100\sqrt{2} = 141.42135\ldots$. In het bijzonder zijn alle gehele getallen, en alle breuken met gehele getallen in de teller en noemer[3], ook reële getallen. Andersom geldt het echter niet!

Het is van de meeste reële getallen onmogelijk om hun getalwaarde exact te bepalen: ze zijn immers oneindig lang en 'bijna' allemaal onregelmatig. Nu liggen de meeste mensen daar niet wakker van. Het is duidelijk dat elk reëel getal willekeurig dicht *benaderd* kan worden door een getal met eindig veel cijfers; bijvoorbeeld 3.141592 is voor de meeste toepassingen een voldoende nauwkeurige benadering van π. Immers, twee reële getallen die pas vanaf de zevende decimaal verschillen, liggen dicht bij elkaar, en nog dichter als ze pas vanaf de twintigste decimaal verschillen. Dit komt doordat in $\mathbb{R}$ de volgende limiet geldt:

$$\lim_{n\to\infty} g^{-n} = 0 \tag{1.2}$$

en $a_0.a_{-1}a_{-2}\ldots$ betekent niets anders dan $a_0g^0 + a_{-1}g^{-1} + a_{-2}g^{-2} + \ldots$ Hoe groter i, des te kleiner de invloed van $a_{-i}g^{-i}$ op de grootte van het getal.

In de volgende rij liggen twee opeenvolgende getallen steeds dichter bij elkaar. De rij *convergeert* naar een *limietwaarde*; die limietwaarde is een reëel getal.

300
310
314
314.1
314.15
314.159
314.1592
...

Het leuke is dat we met alleen deze kennis al een idee kunnen krijgen van wat g-adische getallen voorstellen. Het werkt namelijk net zo als bij de reële getallen, alleen dan precies andersom! De g-adische getallen zijn getallen van de vorm

$$\ldots a_3a_2a_1a_0.a_{-1}a_{-2}\ldots a_{-n} \tag{1.3}$$

waarbij a_i de *cijfers* zijn, niet-negatieve gehele getallen kleiner dan het grondtal g. Blijkbaar lopen de g-adische getallen *links* van de komma oneindig, en *rechts* eindig ver door. Je vraagt je misschien af wat deze getallen voor nut kunnen hebben: ze zijn immers allemaal oneindig groot! Toch blijkt dat aan g-adische getallen een bepaalde, eindige grootte kan worden toegekend. We kunnen namelijk het grondtal g als 'klein' beschouwen, zodat geldt:

$$\lim_{n\to\infty} g^{n} = 0 \tag{1.4}$$

Dit is wiskundig gezien natuurlijk onmogelijk omdat $g > 1$, maar omdat we nu nog informeel bezig zijn, maken we ons daar niet druk over. Ook stellen we: hoe verder een

[3]Dit worden ook wel de *rationale getallen* genoemd.

cijfer naar *links* ligt, hoe minder invloed het heeft op de grootte van het getal. Zo liggen de opeenvolgende rationale getallen in de volgende rij steeds dichter bij elkaar.

$$\begin{aligned} 0.003 \\ 0.013 \\ 0.413 \\ 1.413 \\ 51.413 \\ 951.413 \\ 2951.413 \\ \dots \end{aligned}$$

De rij *convergeert* 10-adisch gezien naar een *limietwaarde*; deze limietwaarde is een 10-adisch getal.

Met deze nogal vreemde beschouwing van 'grootte' kunnen we verwachten dat er ook vreemde dingen gebeuren. Bekijk bijvoorbeeld het volgende rijtje dat 10-adisch gezien steeds dichter naar -1 nadert.

$$\begin{aligned} 9 &= -1 + 10^1 \\ 99 &= -1 + 10^2 \\ 999 &= -1 + 10^3 \\ 9999 &= -1 + 10^4 \\ &\dots \end{aligned}$$

Volgens (1.4) is $\lim_{n\to\infty} 10^n = 0$, dus er moet wel gelden dat $\dots 99999 = -1$. Blijkbaar kunnen positieve g-adische getallen een negatief (geheel) getal voorstellen! Later zal blijken dat *alle* tegengestelden van g-adische getallen zonder minteken geschreven kunnen worden. Het heeft daarom geen zin om negatieve getallen als $-\dots a_2a_1a_0$ in te voeren, want die bestaan allemaal al onder de g-adische getallen.

Voor de reële getallen maakt het niet veel uit in welk grondtal je werkt; je kunt elk reëel getal in elk gewenst grondtal $g \in \mathbb{N}, g \geq 2$ schrijven. Bijvoorbeeld $1347 = 1024 + 256 + 64 + 2 + 1 = 10101000011$ in grondtal 10 resp. 2. Bij de g-adische getallen blijkt het grondtal wél uit te maken: je krijgt in sommige gevallen écht andere getallen als je op een ander grondtal overgaat.

In hoofdstuk 3 zullen we bewijzen dat er geen 'nuldelers' onder de g-adische getallen zijn, precies dan als g een priemgetal is. Nuldelers zijn getallen a en b ongelijk aan 0 waarvoor $ab = 0$, ofwel $a = \frac{0}{b}$ en $b = \frac{0}{a}$. Het blijkt belangrijk te zijn dat er geen nuldelers bestaan, daarom kijken we later alleen naar de situatie dat g priem is. Voorlopig is het voldoende dat g een natuurlijk getal groter dan 1 is.

Dan nog wat terminologie en afkortingen. Terloops hebben we de natuurlijke, de gehele, de rationale en de reële getallen genoemd. De verzamelingen die uit precies al deze getallen bestaan, duidt men aan met $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ resp. $\mathbb{R}$. Wellicht ken je ook $\mathbb{C}$, de verzameling complexe getallen. Later zullen we wat dieper ingaan op deze getalstelsels, evenals op het begrip verzameling.

De g-adische getallen die geen cijfers rechts van de komma hebben, noemen we de g-adische *gehele* getallen. Volgens (1.3) zijn dit de getallen van de vorm

$$\ldots a_4 a_3 a_2 a_1 a_0 \tag{1.5}$$

De verzameling van alle g-adische gehele getallen noemen we $\mathbb{Z}_g$. Let op: welke getallen deze verzameling bevat, hangt van het grondtal g af! Er blijken zelfs oneindig veel verzamelingen $\mathbb{Z}_g$ te zijn.

1.2 g-adisch rekenen

Het optellen en aftrekken in $\mathbb{Z}_g$ gaat ongeveer hetzelfde als in $\mathbb{R}$. We rekenen elementsgewijs en van rechts naar links, waarbij we naar links toe 'overlenen'. Voor optelling in $\mathbb{Z}_{10}$ bijvoorbeeld houdt dat in dat je cijfer voor cijfer optelt, en als de som groter is dan 10, bijvoorbeeld 17, leen je de 1 van 17 over naar links zodat je 7 overhoudt. Hieronder staan een paar voorbeelden van optellen en aftrekken in $\mathbb{Z}_{10}$.

$$\begin{array}{rr} \ldots 39142 & \\ \ldots 86951 & + \\ \hline \ldots 26093 & \end{array} \qquad \begin{array}{rr} \ldots 74801 & \\ \ldots 95236 & - \\ \hline \ldots 79565 & \end{array} \qquad \begin{array}{rr} \ldots 00000 & \\ \ldots 39802 & - \\ \hline \ldots 60198 & \end{array}$$

Je kunt op deze manier elk paar willekeurige g-adische gehele getallen a en b optellen of aftrekken. Op deze manier kun je van elke a de tegengestelde $-a$ berekenen door a van $0 = \ldots 00000$ af te trekken, zoals in het laatste voorbeeld is gedaan. Ter controle kun je daar snel berekenen dat inderdaad $a + (-a) = 0$.

Oefening 1.2.1.

a. Bereken exact de 10-adische uitkomst van $0 - 1$. Komt dit overeen met wat we op pagina 5 hebben geconstateerd over -1?
b. Benader in 5 decimalen nauwkeurig: $\ldots 41342 + \ldots 30243$, maar nu in grondtal 5.
c. Stel dat de twee getallen die je bij b hebt opgeteld in 10 decimalen nauwkeurig waren gegeven. Had dat invloed kunnen hebben op de 5 decimalen die je daar hebt berekend?

Het lijkt er dus op dat als g-adische getallen a en b in n decimalen nauwkeurig bepaald zijn, we ook $a+b$ ook in n decimalen nauwkeurig kunnen berekenen. Dat is handig, want als n naar oneindig gaat, weten we zeker dat $a+b$ naar een g-adisch getal convergeert. In $\mathbb{R}$ zitten daar wat haken en ogen aan. Neem bijvoorbeeld de reële getallen $a = 2.19635\ldots$ en $b = 3.23864\ldots$, een simpele berekening leert dat $a + b = 5.43499\ldots$. Liggen deze zes

Tabel 1.2: Vermenigvuldigen en delen in $\mathbb{Z}_{10}$

$$\begin{array}{rl} \ldots 22901 & \\ \ldots 37586 & \times \\ \hline \ldots 37406 & \\ \ldots 3208 & \\ \ldots 505 & \\ \ldots 07 & \\ \ldots 3 & + \\ \hline \ldots 56986 & \end{array} \qquad \begin{array}{l} 3 \, / \ldots 0000001 \setminus \ldots 6667 \\ \begin{array}{r} 21 \; - \\ \hline \ldots 9999980 \\ 180 \; - \\ \hline \ldots 9999800 \\ 1800 \; - \\ \hline \ldots 9998000 \\ 18000 \; - \\ \hline \ldots \end{array} \end{array}$$

cijfers nu vast? Nee, dat hoeft niet. Stel dat we a en b iets beter benaderen, we vinden bijvoorbeeld $a = 2.196358277\ldots$ en $b = 3.238643530\ldots$. Dan is $a+b = 5.435001807\ldots$; je ziet dat de eerste vijf decimalen niet allemaal overeenkomen met die van de eerder bepaalde waarde van $a+b$. In het algemeen is het zo dat tot en met de eerste decimaal van rechts die geen negen is, de cijfers onzeker zijn in een benadering in $\mathbb{R}$. In $\mathbb{Z}_g$ hebben we daar geen last van, omdat rechts altijd een eindig aantal decimalen staat.

We kunnen ook vermenigvuldigen in $\mathbb{Z}_g$, dit gaat net zoals in $\mathbb{R}$. Zie de linker som in Tabel 1.2.

Delen levert wat problemen op. Slechts in sommige gevallen kan dat met een staartdeling; bovendien is de methode daarvoor in $\mathbb{Z}_g$ even wennen. Een voorbeeld staat in Tabel 1.2 uitgewerkt naast de vermenigvuldiging, hier wordt $\frac{1}{3}$ in $\mathbb{Z}_{10}$ berekend. Je moet bij zo'n staartdeling sommige dingen net andersom doen dan je gewend bent, omdat de meest 'invloedrijke' cijfers rechts staan. Je wilt eerst het meest rechtse cijfer weg hebben, in dit geval een 1. Dat kan, want $3 \times 7 = 21$; we zetten dus een 7 bij de uitkomst. Nu berekenen we $1 - 21 = \ldots 9999980$ (ga maar na). Vervolgens willen we de 8 wegpoetsen, dit doen we met $3 \times 6 = 18$. We zetten daarom een 6 neer bij de uitkomst van het quotiënt, *links* van de 7 die er al stond. (Zie je waarom?) Aftrekken levert $\ldots 9999800$, weer hetzelfde getal als daarnet, maar nu met een nul erbij! De 8 kunnen we weer wegpoetsen met 3×6, dan krijgen we $\ldots 9998000$, etc. Bij het quotiënt komen er steeds meer zessen bij, terwijl bij de rest een steeds langere staart van nullen groeit; de rest wordt volgens de 10-adische beschouwing van grootte (zie vgl. (1.4)) steeds kleiner en nadert naar 0. Daarom is $\frac{1}{3} = \ldots 666667$ in $\mathbb{Z}_{10}$. En inderdaad, als we ter controle $3 \times \ldots 666667$ berekenen komt er 1 uit.

Bij het delen in $\mathbb{Z}_g$ kom je al snel in de problemen. Probeer in $\mathbb{Z}_{10}$ maar eens $\frac{1}{6}$ te berekenen met een staartdeling. Je wilt net zoals in het vorige voorbeeld allereerst het meest rechtse cijfer a_0 van het quotiënt zoeken waarmee je de 1 kan wegpoetsen. Dat is echter onmogelijk, want $a_0 \times 6$ is altijd even en kan dus nooit 1 zijn! We kunnen nog

wel andere dingen proberen, maar dat heeft geen zin. Immers, als $x = \frac{1}{6}$ is $6x = 1$; deze vergelijking is niet oplosbaar in $\mathbb{Z}_{10}$, want het meest rechtse cijfer in $6x$ is even en in 1 is het oneven.

Voor delingen onder de g-adische getallen blijkt het handig zijn om *kommagetallen* toe te staan, die we al gezien hebben bij vgl. (1.3). De verzameling van deze g-adische kommagetallen noemen we $\mathbb{Q}_g$. Eigenlijk is dat wiskundige niet helemaal correct, want $\mathbb{Q}_g$ heeft alleen 'zin' als g een priemgetal is. In hoofdstuk 4 zullen we zien waarom. Daar zullen we ons nu echter niet druk om maken.

In $\mathbb{Q}_{10}$ is de vergelijking $6x = 1$ wél oplosbaar. Omdat daar ook komma's zijn toegestaan, hoeft het meest rechtse cijfer van $6x$ niet hetzelfde te zijn als het meest rechtse cijfer van 1. Neem bijvoorbeeld $x = \ldots 33333.5$, dan is $2x = \ldots 66667.0$ en dat is $\frac{1}{3}$ zoals we gezien hebben. Dus $6x = 1$. Dit konden we doen doordat $5 \times 2 = 10 \equiv 0 \pmod{10}$.[4]

Het optellen en vermenigvuldigen in $\mathbb{Q}_g$ gaat hetzelfde als in $\mathbb{Z}_g$, waarbij je rekening moet houden met de plaats van de komma. Naar analogie van de voorbeelden op pagina 6 en 7 is bijvoorbeeld $\ldots 391.42 + \ldots 869.514 = \ldots 260.934$, en $\ldots 2290.1 \times \ldots 375.86 = \ldots 56.986$. Merk op dat het in $\mathbb{R}$ net zo gaat.

Delen door middel van een staartdeling in $\mathbb{Q}_g$ gaat echter mis als g geen priemgetal is. Dat komt doordat er dan nuldelers in $\mathbb{Z}_g$ zitten.

Oefening 1.2.2.

a. Bereken exact in $\mathbb{Z}_5$: (Let op: werk dus in grondtal 5.)

$$1421 \times \ldots 222222220413$$

Welk getal in $\mathbb{Z}$ stelt dit product voor (in grondtal 5)?

b. Bereken, indien mogelijk, $\frac{1}{7}$ in $\mathbb{Z}_{10}$. Heeft dit quotiënt een repeterende staart? Dezelfde opdracht voor $\frac{1}{8}$.

c. Had iemand anders een andere uitkomst voor $\frac{1}{7}$ in $\mathbb{Z}_{10}$ kunnen krijgen dan jij?[5] Met andere woorden, is er een paar getallen uit de tafel van 7 met hetzelfde rechtercijfer, zodat een bepaald cijfer dus op meerdere manieren kan worden weggepoetst? En hoe zit dat met de tafel van 8?

1.3 Er zitten breuken verstopt in $\mathbb{Q}_g$

We hebben al gezien dat niet alle getallen in $\mathbb{Q}_g$ per se als naar links oneindig doorlopende getallen hoeven te worden geschreven. Er bleken ook 'normale' getallen in te zitten, getallen die we al kenden. Bijvoorbeeld alle gehele getallen, en sommige rationale getallen zoals 15.3, $\frac{1}{3}$ en $\frac{1}{7}$. Dit zijn allemaal getallen die in de g-adische vorm een *repeterende*

[4] Maak je geen zorgen als je niet weet wat (mod 10) is, hier komen we in hoofdstuk 3 op terug.

[5] In de veronderstelling dat er geen rekenfouten zijn gemaakt.

staart hebben, namelijk $\ldots 00015.3$, $\ldots 6667$ en $\ldots 2857142857143$. Men kan bewijzen dat een getal a uit $\mathbb{Q}_g$ *precies dan* als getal in $\mathbb{Q}$ kan worden geschreven als a in de g-adische vorm een repeterende staart heeft. Er zijn natuurlijk heel veel onregelmatige g-adische getallen, deze kunnen dus niet als rationaal getal worden geschreven, en, zo kan men bewijzen, zelfs niet als reëel getal.

We focussen we ons nu op repeterende g-adische getallen. Hoe kunnen zij als rationaal getal worden geschreven? Dit lichten we toe aan de hand van een paar voorbeelden; het algemene geval gaat net zo.

Voorbeeld 1.3.1. *We nemen het* 10*-adische getal* $x = ...77777$ *en zijn benieuwd welk rationaal getal* x *voorstelt. Dat is niet moeilijk. Eerst berekenen* $10x = \ldots 77770$*. Vervolgens berekenen we*

$$-9x = x - 10x = \ldots 77777 - 77770 = \ldots 00007 = 7$$

waaruit volgt dat

$$x = \frac{-7}{9}$$

Wat we hier hebben gedaan was vrij intuïtief en informeel; we zullen eens nader beschouwen wat we allemaal gebruikt hebben. Het blijkt dat de somformule van de meetkundige reeks hier belangrijk is. Een meetkundige reeks heeft te maken met een oneindig lange getallenrij van de vorm $a_0, a_1, a_2, a_3, \ldots$ waarin de opeenvolgende elementen steeds met dezelfde factor worden vermenigvuldigd. Er geldt dus steeds dat $a_{i+1} = ka_i$ voor een zekere reële constante $k \neq 1$. Je kunt makkelijk inzien dat de getallenrij ook geschreven kan worden als $ak^0, ak^1, ak^2, ak^3, \ldots$ waarbij $a = a_0$.

We willen alle oneindig veel elementen van de rij bij elkaar optellen. Of daar een echt getal uitkomt of niet zien we later wel. Eerst beschouwen we een *benadering* van wat we willen berekenen, namelijk de som van de eerste $n+1$ elementen. Deze noemen we x_n. Dan berekenen we kx_n, en vervolgens trekken we de twee van elkaar af. Hierbij vallen op twee na alle termen tegen elkaar weg.

$$\begin{array}{lccccccc}
x_n = & ak^0 & + & ak^1 & + & ak^2 & + \ldots + & ak^n \\
kx_n = & & & ak^1 & + & ak^2 & + \ldots + & ak^n + ak^{n+1} \\
\hline
(1-k)x_n = & ak^0 & & & & & & - ak^{n+1}
\end{array}$$

Hieruit volgt dat

$$x_n = \frac{a(k^0 - k^{n+1})}{1-k} \tag{1.6}$$

Deze deling kunnen we uitvoeren omdat $k \neq 1$.

We zijn niet op zoek naar een benadering, maar naar de *exacte* waarde van $\lim_{n\to\infty} x_n = ak^0 + ak^1 + ak^2 + \ldots$ Om deze te bepalen laten we n in (1.6) naar oneindig gaan. Er zijn

dan twee[6] mogelijkheden. Als $|k| > 1$ gaat k^{n+1} naar (min) oneindig; dan divergeert x_n zodat x_∞ geen getal kan zijn. Als $-1 < k < 1$ gaat k^{n+1} naar 0; dan is dus

$$\lim_{n\to\infty} x_n = \frac{a(k^0 - 0)}{1-k} = \frac{a}{1-k} \tag{1.7}$$

Een som van oneindig veel termen kan dus een rationaal getal opleveren! Dat wisten we eigenlijk al, want bijvoorbeeld $0.33333\ldots$ in grondtal 10 is niets anders dan een meetkundige reeks met $a = 0.3$ en $k = 0.1$. Uit (1.7) volgt dat

$$0.33333\ldots = \frac{0.3}{1-0.1} = \frac{0.3}{0.9} = \frac{1}{3}$$

Nog een voorbeeld: $0.142857142857\ldots$ is een meetkundige reeks met $a = 0.142857$ en $k = 10^{-6}$ (ga dat na), dus

$$0.142857142857\ldots = \frac{0.142857}{1-10^{-6}} = \frac{0.142857}{0.999999} = \frac{1}{7}$$

Hierboven hebben we gesteld dat de som van de meetkundige reeks alleen oplosbaar is als $|k| < 1$, want alleen dan is $\lim_{n\to\infty} k^{n+1} = 0$. Bij g-adische getallen is het echter juist andersom, want volgens (1.4) gaat k^{n+1} naar 0 als $k > 1$! Daarom mogen we (1.7) ook op repeterende getallen van $\mathbb{Q}_g$ toepassen. Als voorbeeld nemen we weer $\ldots 77777$ in $\mathbb{Z}_{10}$, dit is een meetkundige reeks met $a = 7$ en $k = 10$.

$$\ldots 77777 = \frac{7}{1-10} = \frac{-7}{9}$$

Je ziet dat er een *negatieve* breuk uitkomt! Omdat altijd geldt dat $k > 1$ en $a > 0$ is dat voor alle g-adische getallen het geval. Uiteraard zitten er ook positieve breuken in $\mathbb{Q}_p$, je kunt namelijk met de methode van pagina 6 de tegengestelde van bijv. $\ldots 77777$ berekenen.

Alle g-adische getallen met repeterende staart zijn ook rationaal getal. Een voorbeeld laat zien hoe het algemene bewijs verloopt. We rekenen weer in $\mathbb{Q}_{10}$.

$$\ldots 2780527805139.46 = 10^3 \times \ldots 2780527805 + 139.46 = 10^3 \times \frac{27805}{1-10^5} + 139.46$$
$$= \frac{27805000 - 13945860.54}{-99999} = \frac{-1385913946}{9999900}$$

Men kan bewijzen dat *alle* rationale getallen als g-adisch getal te schrijven zijn, ofwel, $\mathbb{Q} \in \mathbb{Z}_g$ voor alle $g \in \mathbb{N}, g > 1$. Dat doen we hier echter niet.

[6] Eigenlijk is er nog een derde mogelijkheid, namelijk $k = -1$. Dit is een geval apart, we bespreken het hier niet.

Hoofdstuk 2

Algebraïsche structuren en getalsystemen

2.1 Algebra in een notendop

Voor veel mensen betekent algebra zoiets als 'rekenen met letters'. Algebra is echter veel meer dan dat. Heel globaal houdt de algebra zich bezig met het bestuderen van structuur, zoals symmetrieën van regelmatige veelvlakken en de structuur van de verzameling priemgetallen in andere getalstelsels. De basisobjecten waar we altijd van uitgaan zijn verzamelingen waar inwendige bewerkingen op zijn gedefinieerd.

Verzamelingen Informeel is een verzameling *het geheel van een aantal bij elkaar horende objecten*, een veelheid beschouwd als één.[1] Objecten die in een bepaalde verzameling niet op te delen zijn in kleinere objecten, worden *elementen* van die verzameling genoemd. Een object dat is opgebouwd uit meerdere elementen van een verzameling, wordt een *deelverzameling* daarvan genoemd. Deze is op zichzelf ook weer een verzameling.

We geven een voorbeeld. Alle mensen op aarde vormen een verzameling V. Alle Nederlanders vormen een deelverzameling W daarvan, en alle Nederlanders met blauwe ogen vormen daar weer een deelverzameling X van. Een willekeurige Nederlander met blauwe ogen is een element van X, en dus ook van W en van V. Natuurlijk weten wij dat een mens weer is opgebouwd uit achtereenvolgens organen, cellen, organellen, moleculen etc., maar wiskundig gezien wordt de mens in V, W en X als element beschouwd.

Een verzameling wordt vaak afgekort met een hoofdletter, en aangeduid met accolades waarbinnen een wiskundige omschrijving van de verzameling staat. Bijvoorbeeld $A = \{1, 3, 105\}$ is de verzameling bestaande uit de drie getallen 1, 3 en 105. De volgorde waarin de elementen staan maakt niet uit, dus $A = \{1, 3, 105\} = \{105, 1, 3\}$. Verzamelingen mogen oneindig veel elementen bevatten, denk bijvoorbeeld aan $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$. Het symbool $\in$ wordt uitgesproken als '$\ldots$ is een element van de

[1] Bron: [8]

verzameling ...', of kortweg als 'in'. Als gegeven is dat $x \in A$ weet je dus dat x één van de drie getallen 1, 3 en 105 is. Als $x \in \mathbb{N}$ is x een natuurlijk getal.

In het algemeen wordt een verzameling V als volgt aangeduid:

$$V = \{f(x) \mid \text{omschrijving van x}\}$$

Dit is de verzameling van precies alle elementen $f(x)$ waarvoor x aan de omschrijving rechts van de verticale streep voldoet. Bijvoorbeeld $\{2x + 1 \mid x \in \mathbb{N}\}$ is de verzameling van alle $2x + 1$ waarvoor x een natuurlijk getal is: de oneven natuurlijke getallen dus.

Met $V_{\geq k}$ bedoelen we de verzameling $W = \{x \in V \mid x \geq k\}$.

Operaties, samenstellingswetten en inwendigheid Laat V_1 en V_2 twee verzamelingen zijn. Een *operatie* of bewerking van V_1 naar V_2 is een functie waarmee een combinatie van elementen van V_1 wordt afgebeeld naar een element van V_2. Dit klinkt wat ingewikkeld, maar bijvoorbeeld optellen en vermenigvuldigen zijn operaties van $\mathbb{N}$ naar $\mathbb{N}$. Zo wordt $4 + 7$ afgebeeld naar 11. We noemen $+$ en $\times$ *binaire* operaties, omdat het altijd om een combinatie van *twee* elementen gaat.

We weten intuïtief dat de regel $a+b = b+a$ voor alle natuurlijke getallen a en b opgaat. Dit is een voorbeeld van een *samenstellingswet*. In §2.3 gaan we dieper op dergelijke wetten in. Al met enkele samenstellingswetten is het mogelijk om nieuwe wetten af te leiden. Dat is een van de mooiste eigenschappen van de wiskunde: uitgaande van een paar eenvoudige 'basisregels' kun je enorm veel, misschien wel oneindig veel nieuwe wetmatigheden ontdekken.

Er zit alleen een addertje onder het gras: samenstellingswetten mogen vaak alleen gecombineerd worden als ze *inwendig* zijn. Dat bijvoorbeeld $+$ en $\times$ inwendig zijn in $\mathbb{N}$, betekent dat $a + b \in \mathbb{N}$ resp. $a \times b \in \mathbb{N}$ voor alle $a, b \in \mathbb{N}$. Stel dat de operatie $\times$ niet inwendig was in $\mathbb{N}$, konden we er niet vanuit gaan dat ce een natuurlijk getal was, ook al waren c en e dat wel. Dit zou betekenen dat we niet zonder meer mochten beweren dat $ce+b = b+ce$. Gelukkig zijn $+$ en $\times$ wel inwendig in $\mathbb{N}$, zoals je gemakkelijk kunt nagaan. Daardoor zijn alle operaties samengesteld uit $+$ en $\times$, zoals $a(b + c)$, automatisch ook inwendig.

'Aftrekken' is een voorbeeld van een operatie die *niet* inwendig is in $\mathbb{N}$. Bijvoorbeeld $5 - 7 = -2$ is kleiner dan 0 en zit dus niet in $\mathbb{N}$.

Om dubbelzinnigheden te voorkomen, gebruiken we in formele gedeelten overal waar dat nodig is haakjes. Alleen als er echt geen verwarring kan ontstaan, laten we ze weg. Zo gaat vermenigvuldiging bij afspraak vóór optelling bij het ontbreken van haakjes. Verder laten we het $\times$-teken voor de overzichtelijkheid vaak weg, of schrijven we $\cdot$ ervoor in de plaats.

2.2 Symbolen

We zullen in dit werkstuk hier en daar gebruik maken van symbolen. Eén ervan zijn we al tegengekomen, namelijk $\in$. Er zijn nog veel meer symbolen met een vaste betekenis,

Tabel 2.1: Enkele belangrijke symbolen

Symbool	Lees dit als:
$\in$	... (is een element) van de verzameling ...
$\forall$	Voor alle ...
$\exists$	Er is een ...
:	... zodat geldt ...; *of:* ... geldt het volgende: ...
$\subset$	... is een deelverzameling van ...
:=	... is *per definitie* gelijk aan ...
$\Rightarrow$	... als ... dan ...
$\Leftrightarrow$	... dan en slechts dan als ...

degene die wij gebruiken (behalve de bekende zoals $\geq$) hebben we opgesomd in Tabel 2.1 op pagina 13. De symbolen op zichzelf betekenen eigenlijk niets; ze worden altijd gecombineerd met andere symbolen.
Een paar voorbeelden van wat we met deze symbolen kunnen uitdrukken, maken veel duidelijk.

- $\forall a \in A : a < 106$ betekent: 'Voor alle elementen a van de verzameling A geldt: a is kleiner dan 106.'
- $\exists x, y \in \mathbb{N} : \forall a \in V : (a > x \Rightarrow a > y)$ betekent: 'Er zijn natuurlijke getallen x, y zodat voor alle a in V geldt: als a groter is dan x, dan is a groter dan y.'

We doen een paar opmerkingen over Tabel 2.1.

- $A := B$ of $B =: A$ betekent: we kennen B al, en creëren nu een A die per definitie gelijk is aan B.
- $A \Rightarrow B$ betekent: *Als* bewering A waar is, *dan* volgt daaruit dat bewering B ook waar is. Het zegt dus niets over de waarheid van A.
- $A \Leftrightarrow B$ betekent dat A en B óf beide waar óf beide onwaar zijn. Dit wordt vaak uitgesproken als: A is waar *dan en sléchts dan* als B waar is.
- $V \subset W$ betekent dat V een deelverzameling is van W of gelijk is aan W. In symbolen: $\forall a \in V : a \in W$. Je kunt gemakkelijk inzien dat uit $V \subset W$ en $W \subset V$ volgt dat $V = W$.

Tabel 2.2: Enkele samenstellingswetten

Optelling

1) *Inwendigheid van de optelling.* Als $a, b \in V$, dan is ook $a + b \in V$.
2) *Associativiteit van de optelling.* $(a + b) + c = a + (b + c)$
3) *Nulelement.* Er is een $0 \in V$ zodat $a + 0 = 0 + a = a$.
4) *Tegengestelde.* Voor alle $a \in V$ is er een tegengestelde $-a \in V$, zodat $a + (-a) = (-a) + a = 0$.
5) *Commutativiteit van de optelling.* $a + b = b + a$

Vermenigvuldiging

1) *Inwendigheid van de vermenigvuldiging.* Als $a, b \in V$, dan is ook $a \times b \in V$.
2) *Associativiteit van de vermenigvuldiging.* $(a \times b) \times c = a \times (b \times c)$
3) *Eenheidselement.* Er is een $1 \in V$ zodat $a \times 1 = 1 \times a = a$.
4) *Inverse.* Voor alle $a \in V, a \neq 0$ is er een inverse $a^{-1} \in V$, zodat $a \times a^{-1} = a^{-1} \times a = 1$.
5) *Commutativiteit van de vermenigvuldiging.* $a \times b = b \times a$

Combinatie

6) *Distributiviteit.* $a(b+c) = ab+ac$ (links-distributiviteit), én $(a+b)c = ac+bc$ (rechts-distributiviteit).
7) *Nul keer iets is nul.* $a \times 0 = 0 \times a = 0$
8) *V bevat geen nuldelers.* Er kan alleen maar gelden dat $ab = 0$ als minstens één van beide a of b nul is.

2.3 Ringen en Lichamen

De ring en het lichaam zijn voorbeelden van *algebraïsche structuren.* Een algebraïsche structuur $(V, +, \times)$ is een verzameling V waarop twee binaire operaties $+$ en $\times$ zijn gedefinieerd, die aan bepaalde samenstellingswetten voldoen.[2] Hoewel $+$ en $\times$ niet per se overeen hoeven te komen met de bekende optelling en vermenigvuldiging, is dat in dit werkstuk wel altijd zo. Een voorbeeld van een algebraïsche structuur is $(\mathbb{N}, +, \times)$. Op pagina 12 hebben we al een paar samenstellingswetten voor $\mathbb{N}$ gezien. In Tabel 2.2 op pagina 14 staan er nog een aantal; deze gaan niet allemaal op voor $\mathbb{N}$. De wetten gelden steeds voor *alle* elementen a, b en c van een zekere verzameling V.

Ook 0 en 1 hoeven niet per se overeen te komen met de bekende nul en één. In de algebra stellen het zelfs geen getallen voor. In dit werkstuk komen ze daarmee echter wel altijd overeen.

We zien drie soorten rekenregels in Tabel 2.2. Vijf regels gaan over de optelling, vijf soortgelijke regels gaan over vermenigvuldiging. De laatste drie regels gaan over de

[2] Er zijn ook andere soorten algebraïsche structuren, maar die bestuderen we hier niet.

interactie tussen optellen en vermenigvuldigen.

Oefening 2.3.1.

a. Kunnen er algebraïsche structuren bestaan waarvoor wel de regels 7) en 8) gelden, maar niet 3) voor optelling?
b. Welke van de samenstellingswetten uit Tabel 2.2 gelden voor $V = \mathbb{N}$?
c. Dezelfde vraag voor $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$. Als je kunt rekenen met complexe getallen, kun je de vraag ook voor $\mathbb{C}$ beantwoorden.

Er zijn veel verschillende soorten algebraïsche structuren, afhankelijk van het aantal operaties en van de samenstellingswetten waaraan wordt voldaan. Veelgebruikte structuren hebben een naam gekregen; wij noemen er hier drie. De nummers verwijzen weer naar Tabel 2.2.

- Een algebraïsche structuur met een nulelement, waar optelling en vermenigvuldiging inwendig en associatief zijn en de optelling bovendien commutatief is, en waar de distributiviteit geldt, noemen we een *halfring*. Dit is dus een structuur die in elk geval voldoet aan 1), 2), 3) en 5) voor $+$, aan 1) en 2) voor $\times$, en aan 6).
- Een halfring waarin bovendien ieder element een tegengestelde heeft, wordt een *ring* genoemd. Dit is dus een halfring waar 4) geldt voor $+$.
- Een ring met een eenheidselement, waarin ieder element een inverse heeft en waarin bovendien vermenigvuldiging commutatief is, heet een *lichaam*. Dit is dus een ring waar 3), 4) en 5) gelden voor $\times$.

De begrippen ring en lichaam zullen we later nog vaak nodig hebben, daarom hebben we hun eigenschappen overzichtelijk in Tabel 2.4 gezet. Deze eigenschappen geleden in ieder geval, meer mag ook. Zo is elk lichaam automatisch ook een ring.

We kunnen bij de naam van een algebraïsche structuur de toevoegingen *commutatieve*, *met 1* en *zonder nuldelers* plaatsen om aan te geven dat de regels 5) en 3) voor $\times$, en regel 8) gelden.[3] Bijvoorbeeld een commutatieve ring met 1 waarvoor ook nog eens ieder element een inverse heeft, is hetzelfde als een lichaam.

Oefening 2.3.2.

a. Ga na dat uit je antwoord bij opgave 2.3.1.a. volgt dat $(\mathbb{N}, +, \times)$ een commutatieve halfring met 1 zonder nuldelers is.
b. Welke algebraïsche structuren zijn $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (en $\mathbb{C}$)?

Het leuke is dat met enkel en alleen de samenstellingswetten uit Tabel 2.2 heel veel

[3] Commutatieve gaat dan dus niet over optelling.

Tabel 2.4: Ring en Lichaam

Structuur	**Samenstellingswetten**
Ring	+: 1), 2), 3), 4), 5) ×: 1), 2); 6)
Lichaam	+: 1), 2), 3), 4), 5) ×: 1), 2), 3), 4), 5); 6)

(vaak zeer ingewikkelde) stellingen kunnen worden bewezen. Een aantal van de meest eenvoudige stellingen met bewijs kun je vinden in hoofdstuk 4 van [5]. Als bewezen is dat een stelling geldt voor bijvoorbeeld elke ring, mag deze op alle bekende ringen worden toegepast, bijvoorbeeld op $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. Dat is de kracht van de algebra.

2.4 Enkele stellingen over algebraïsche structuren

In deze paragraaf bewijzen we drie stellingen die we later nog handig kunnen gebruiken. Bovendien geven de bewijzen een goed beeld van hoe je met algebraïsche structuren kunt werken. Als je algemene stellingen over bijvoorbeeld lichamen wilt bewijzen, kun je je niet beroepen op je intuïtie over de lichamen $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ die je al kent. Je wilt namelijk dat de stellingen gelden voor alle structuren die aan de eisen in Tabel 2.4 voldoen.

In dit werkstuk hebben we ervoor gekozen niet alle stellingen zo precies te bewijzen

als hier, dat zou veel te veel ruimte in beslag nemen en bovendien storend zijn voor het verhaal.

In de volgende stelling mag je voor $\circ$ zowel $+$ als $\times$ invullen. Als boven een $=$-teken bijvoorbeeld 2)$\circ$ staat, betekent dit dat deze stap volgt uit samenstellingswet 2) voor operatie $\circ$ uit Tabel 2.2.

Stelling 2.4.1. *Voor elke commutatieve ring* $(V, +, \times)$ *geldt:*

$$\forall a, b, c, d \in V : (a \circ b) \circ (c \circ d) = (a \circ d) \circ (c \circ b)$$

Bewijs. Voor willekeurige $a, b, c, d \in V$ geldt:

$$\begin{aligned}(a \circ b) \circ (c \circ d) &\overset{2)\circ}{=} a \circ \big(b \circ (c \circ d)\big) \overset{5)\circ}{=} a \circ \big((c \circ d) \circ b\big) \\ &\overset{5)\circ}{=} a \circ \big((d \circ c) \circ b\big) \overset{2)\circ}{=} a \circ \big(d \circ (c \circ b)\big) \overset{2)\circ}{=} (a \circ d) \circ (c \circ b)\end{aligned}$$

□

Dat stelling 2.4.1 geldt is intuïtief meteen duidelijk, maar het kost toch wat moeite om hem te bewijzen!

De volgende stelling voorkomt dat we verderop in dit werkstuk zowel de rechts- als de links-distributiviteit moeten bewijzen.

Stelling 2.4.2. *Voor elke commutatieve structuur* $(V, +, \times)$ *geldt: als de links-distributiviteit waar is, dan ook de rechts-distributiviteit.*

Bewijs. a, b en c zijn willekeurige elementen van V. Stel dat de links-distributiviteit geldt, zodat

$$a(b + c) = ab + ac \tag{2.1}$$

Hieruit volgt:

$$(b + c)a \overset{5)\times}{=} a(b + c) \overset{(2.1)}{=} ab + ac \overset{5)\times}{=} ba + ca$$

dus $(b+c)a = ba+ca$, de rechts-distributiviteit geldt dan dus ook. Hiermee is de stelling bewezen. □

De laatste stelling gaat over eigenschap 7) uit Tabel 2.2 die zegt dat nul keer iets altijd nul is. Dit blijkt namelijk in *elke* commutatieve ring te gelden.[4] In het bewijs laten we de verwijzingen boven de $=$-tekens weg; probeer zelf te achterhalen welke samenstellingswetten we gebruiken.

[4]Het geldt zelfs voor elke ring, ook voor niet-commutatieve ringen. Geheel analoog aan het bewijs hier kun je namelijk aantonen dat $0 = 0 \times a$. In dit werkstuk vormt het echter geen beperking als de ring commutatief is.

Stelling 2.4.3. *Voor elke commutatieve ring geldt:*

$$\forall a \in V : a \times 0 = 0 \times a = 0$$

Bewijs. Laat a een willekeurig element zijn van V. Er geldt:

$$\begin{aligned} 0 &= (a \times 0) + -(a \times 0) = \big((a(0+0)\big) + -(a \times 0) = \big(a \times 0 + a \times 0\big) + -(a \times 0) \\ &= a \times 0 + \big(a \times 0 + -(a \times 0)\big) = a \times 0 + 0 = a \times 0 \end{aligned}$$

dus $a \times 0 = 0$. Wegens de commutativiteit van $\times$ is dan ook $0 \times a = 0$, waarmee de stelling bewezen is. □

2.5 Getalsystemen als algebraïsche structuren

We hebben tot nu toe zeven verschillende getalsystemen genoemd, nu zullen we daar wat meer over zeggen. De volgorde waarin ze staan, namelijk $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$, is niet willekeurig gekozen. Behalve $\mathbb{Z}_p$ wordt elk van deze getalsystemen namelijk uit haar voorganger opgebouwd. Dat $\mathbb{R}$ wordt geconstrueerd vanuit $\mathbb{Q}$ is niet meteen duidelijk, maar in de wiskunde kunnen de reële getallen gedefinieerd worden als limieten van convergerende rijtjes rationale getallen. Zo is $\pi/4 = \arctan(1) = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$ Je kunt $\mathbb{R}$ ook construeren als oneindige decimale breuken, zoals we al hebben aangeduid in hoofdstuk 1. Dat heeft wel twee bezwaren. Ten eerste moet je soms verschillende decimale breuken identificeren. Zo is $1 = 0.99999\ldots$ Dat is lastig, maar niet onoverkomelijk. Ten tweede kun je je afvragen: "Als ik nu 8 vingers had, zou $\mathbb{R}$ er dan anders uit hebben gezien?" Gelukkig kan men bewijzen dat het voor de structuur van $\mathbb{R}$ niet belangrijk is welk grondtal je kiest.

Verder is elk hier genoemde getalstelsel deelverzameling van alle daaropvolgende stelsels (behalve $\mathbb{Z}_p$ en $\mathbb{Q}_p$), zoals je gemakkelijk intuïtief kunt inzien.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \qquad \begin{array}{ccc} \mathbb{Z} & \subset & \mathbb{Z}_p \\ \cap & & \cap \\ \mathbb{Q} & \subset & \mathbb{Q}_p \end{array}$$

In het rechter schema zien we dat $\mathbb{Z}$ deelverzameling is van $\mathbb{Z}_p$, $\mathbb{Q}$ en $\mathbb{Q}_p$, en dat $\mathbb{Q}_p$ de drie andere verzamelingen omvat. Maar bijvoorbeeld de inclusie $\mathbb{Q} \subset \mathbb{Z}_p$ is niet waar. Bijvoorbeeld $\frac{1}{p} \in \mathbb{Q}$ zit niet in $\mathbb{Z}_p$. Hier komen we in hoofdstuk 4 op terug.

$\mathbb{N}$ heeft in de volgorde die we aanhouden geen 'voorganger', maar je moet toch ergens beginnen. $\mathbb{N}$ wordt axiomatisch gedefinieerd en niet opgebouwd uit enig ander getalstelsel. Het staat aan de basis van alle ons bekende getalstelsels.

2.5.1 $\mathbb{N}$, de Natuurlijke getallen

$\mathbb{N}$ is de verzameling *natuurlijke* getallen $\{0, 1, 2, 3, \ldots\}$. Haar belangrijkste basiseigenschappen zijn dat er een *beginelement* is (dat we 0 noemen), en dat ieder natuurlijk

getal een unieke *opvolger* in $\mathbb{N}$ heeft. In oefening 2.3.1 heb je intuïtief ingezien dat $\mathbb{N}$ een commutatieve *halfring* met 1 zonder nuldelers is.

Op het eerste gezicht hebben de natuurlijke getallen niet veel met p-adische getallen te maken, maar uiteindelijk is ook $\mathbb{Z}_p$, net als alle andere getalsystemen, gebaseerd op $\mathbb{N}$.

2.5.2 $\mathbb{Z}$, de Gehele getallen

$\mathbb{Z}$ is de verzameling *gehele* getallen $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ bestaande uit de natuurlijke getallen, en voor elk natuurlijk getal zijn tegengestelde (0 is zijn eigen tegengestelde). Dat wil zeggen: $\mathbb{Z} = \{a, -a \mid a \in \mathbb{N}\}$.

Het grootste verschil tussen $\mathbb{N}$ en $\mathbb{Z}$ is dat $\mathbb{Z}$ geen beginelement heeft, en dat ieder getal een tegengestelde heeft. De gehele getallenlijn is als het ware symmetrisch ten opzichte van de 0.

We hebben $\mathbb{N}$ en $\mathbb{Z}$ formeel ingevoerd en bewezen dat ze een commutatieve halfring resp. ring met 1 zonder nuldelers vormen. Dit hebben we niet opgenomen in dit verslag. Men definieert $\mathbb{Z}$ op een heel andere manier dan $\mathbb{N}$, en stellingen worden op een heel andere manier bewezen. Dit komt doordat $\mathbb{N}$ 'uit het niets' wordt opgebouwd, terwijl $\mathbb{Z}$ kan worden geconstrueerd vanuit $\mathbb{N}$. De rekenregels die voor $\mathbb{N}$ bewezen zijn, kunnen handig worden gebruikt om stellingen over $\mathbb{Z}$ te bewijzen. Dit gaat voor de andere getalsystemen net zo.

In de uitbreiding van $\mathbb{N}$ naar $\mathbb{Z}$ hebben we geen eigenschappen gebruikt die specifiek zijn voor $\mathbb{N}$. Daarom kunnen we deze methode gebruiken om *elke* willekeurige commutatieve halfring met 1 uit te breiden naar een ring.

2.5.3 $\mathbb{Q}$, de Rationale getallen

$\mathbb{Q}$ is de verzameling *rationale* getallen, ofwel breuken $\frac{a}{b}$, met in de teller en noemer een geheel getal. Dat wil zeggen: $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}\}$.

In tegenstelling tot $\mathbb{Z}$ heeft een element in $\mathbb{Q}$ geen opvolger. Voor ieder paar $a, b \in \mathbb{Q}$ ligt er immers nog een breuk tussen a en b, bijvoorbeeld $\frac{a+b}{2}$. Er zitten dus geen 'gaten met positieve lengte' in de rationale getallenlijn.

In hoofdstuk 4 zullen we $\mathbb{Q}$ formeel construeren en bewijzen dat het een lichaam is.

2.5.4 $\mathbb{R}$, de Reële getallen

$\mathbb{R}$ is de verzameling *reële* getallen, dat zijn alle getallen op de getallenlijn. $\mathbb{R}$ komt overeen met de verzameling van alle naar *links* eindig en naar *rechts* oneindig doorlopende decimale breuken in een willekeurig grondtal $g \in \mathbb{N}_{\geq 2}$. Bijvoorbeeld $1.01100111000\ldots$ in grondtal 2, en $10^5\pi = 314159.2\ldots$ in grondtal 10 zijn reële getallen. Formeler: $\forall g \in \mathbb{N}_{\geq 2}$:

$$\mathbb{R} = \Big\{ \sum_{-\infty}^{i=k} a_i g^i \;\Big|\; k \in \mathbb{Z},\ \forall i \in \mathbb{Z} : (a_i \in \mathbb{N},\ 0 \leq a_i \leq g-1) \Big\}$$

Een reden om $\mathbb{N}$ uit te breiden naar $\mathbb{Z}$ en $\mathbb{Q}$ is omdat er zo een 'mooiere' algebraïsche structuur ontstaat die aan meer axioma's voldoet. Met $\mathbb{Q}$ is de mooiste structuur die we kennen (het lichaam) bereikt, dus we moeten andere redenen hebben om deze nog eens uit te breiden naar $\mathbb{R}$ en $\mathbb{C}$.

We hebben eerder beweerd dat er geen 'gaten' in de rationale getallenlijn zitten: elk getal op de getallenlijn kan oneindig dicht *benaderd* worden door rationale getallen. Maar voor veel toepassingen, bijvoorbeeld in de analyse, blijkt benaderen niet goed genoeg te zijn. Daar is het namelijk belangrijk dat je limieten kunt nemen. Bovendien blijken belangrijke reële getallen zoals $\sqrt{2}$, e en π niet rationaal te zijn.

2.5.5 $\mathbb{C}$, de Complexe getallen

De verzameling *complexe* getallen kan worden geschreven als $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. De constante i is een zogenaamd *imaginair* getal. Per definitie is $i^2 = -1$. Blijkbaar is i geen reëel getal, want in $\mathbb{R}$ zijn kwadraten altijd positief. Met i mag wel gerekend worden alsof het een reëel getal is.

De belangrijkste reden om $\mathbb{C}$ in te voeren is omdat zo een *algebraïsch gesloten* getalsysteem ontstaat. Dat wil zeggen dat er voor elke functie f van de vorm

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n \qquad (a_i \in \mathbb{C}, n \in \mathbb{N}_{\geq 1})$$

een $x \in \mathbb{C}$ is zodat $f(x) = 0$. Zo'n x heet een nulpunt van $f(x)$. Dat $\mathbb{R}$ niet algebraïsch gesloten is, is gemakkelijk in te zien: bijvoorbeeld $f(x) = x^2 + 3$ heeft geen nulpunt in $\mathbb{R}$. In $\mathbb{C}$ is bijvoorbeeld $i\sqrt{3}$ een nulpunt van deze functie.

Dat $\mathbb{C}$ algebraïsch gesloten is, bewijzen we hier niet. In hoofdstuk 8 van [5] staat een bewijs dat ook voor 6VWO-leerlingen te begrijpen is.

2.5.6 $\mathbb{Z}_p$ en $\mathbb{Q}_p$, de p-adische gehele en gebroken getallen

Wat $\mathbb{Z}_p$ en $\mathbb{Q}_p$ intuïtief inhouden hebben we uitgebreid besproken. In hoofdstuk 3 en 4 zullen we ze formeel definiëren.

In hoofdstuk 3 zullen we bewijzen dat $\mathbb{Z}_g$, voor elk geheel grondtal $g \geq 2$, een commutatieve ring met 1 is, en bovendien zonder nuldelers als g priem is. In hoofdstuk 4 bewijzen we dat $\mathbb{Q}_p$ voor elk priemgetal p een lichaam is. Dan blijkt dat we $\mathbb{Q}_p$ op een heel andere manier invoeren dan je misschien verwacht, namelijk als breuken $\frac{a}{b}$ met in de teller en noemer p-adische gehele getallen.

$$\forall p \in \mathbb{P}: \qquad \mathbb{Q}_p = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}_p,\ b \neq 0 \right\}$$

Hier is $\mathbb{P}$ de verzameling priemgetallen. Uiteindelijk bewijzen we dat alle elementen van $\mathbb{Q}_p$ geschreven kunnen worden als p-adische kommagetallen van de vorm

$$\ldots a_3a_2a_1a_0.a_{-1}a_{-2}\ldots a_{-n}$$

Bij deze schrijfwijze kunnen we ons tenminste iets voorstellen, en bovendien kunnen we op deze manier gemakkelijk met de getallen rekenen.

Hoofdstuk 3

Precieze invoering van de ring $\mathbb{Z}_g$

3.1 Voorbereiding

In dit hoofdstuk voeren we $\mathbb{Z}_g$ formeel in, waarna we bewijzen dat het een commutatieve ring met 1 is, en bovendien zonder nuldelers als g priem is. Voordat we dat doen, willen we eerste intuïtief inzien waarom dit zo is. Dat doen we in deze paragraaf. Let op: alle 'bewijzen' hier zijn nog informeel en niet strikt volgens wiskundige regels.

Een g-adisch geheel getal

$$\ldots a_3 a_2 a_1 a_0$$

betekent intuïtief hetzelfde als

$$\ldots + a_3 g^3 + a_2 g^2 + a_1 g^1 + a_0 g^0 \tag{3.1}$$

Dit korten we voortaan af als[1]

$$\sum_{i=0}^{\infty} a_i g^i \tag{3.2}$$

In §1.2 hebben we gezien dat twee g-adische getallen cijfer voor cijfer opgeteld worden, dus

$$\sum_{i=0}^{\infty} a_i g^i + \sum_{i=0}^{\infty} b_i g^i = \sum_{i=0}^{\infty} (a_i + b_i) g^i \tag{3.3}$$

Hier stuiten we echter op een probleem: de nieuwe cijfers $a_i + b_i$ kunnen groter zijn dan $g - 1$. We kunnen nu naar links 'overlenen' om er een echt g-adisch getal van te maken, maar dan hebben we geen simpele formule voor optelling meer. Het hangt immers van de specifieke waarden van alle a_i en b_i af of er overgeleend moet worden, en ook van alle vorige keren dat is overgeleend. Daarom nemen we voorlopig maar voor lief dat sommige cijfers te groot zijn.

[1] $\sum$ is het zogenaamde sommatie-teken. Lees formule (3.2) als: *de som van alle termen $a_i g^i$ waarbij de index i alle gehele getallen van 0 tot ∞ doorloopt.*

Het is nu makkelijk in te zien dat de optelling commutatief is. Alle a_i en b_i zijn namelijk natuurlijke getallen waarvoor de commutativiteit geldt, dus

$$\sum_{i=0}^{\infty} a_i g^i + \sum_{i=0}^{\infty} b_i g^i = \sum_{i=0}^{\infty} (a_i + b_i) g^i = \sum_{i=0}^{\infty} (b_i + a_i) g^i = \sum_{i=0}^{\infty} b_i g^i + \sum_{i=0}^{\infty} a_i g^i$$

Voor het gemak noteren we $\sum_{i=0}^{\infty} a_i g^i$ voortaan als $[a_i]$, analoog hieraan schrijven we $[b_i]$ en $[c_i]$. Zo stelt bijvoorbeeld $[0]$ een oneindige rij nullen voor.

Ook de associativiteit van de optelling is gemakkelijk in te zien.

$$\begin{aligned}\big([a_i] + [b_i]\big) + [c_i] = [a_i + b_i] + [c_i] &= \big[(a_i + b_i) + c_i\big] \\ &= \big[a_i + (b_i + c_i)\big] = [a_i] + [b_i + c_i] = [a_i] + \big([b_i] + [c_i]\big)\end{aligned}$$

Het bestaan van een nulelement is nóg eenvoudiger aan te tonen; immers,

$$[a_i] + [0] = [a_i + 0] = [a_i]$$

en wegens de commutativiteit van $+$ is ook $[0] + [a_i] = [a_i]$.

Om te bewijzen dat ieder getal een tegengestelde heeft, moeten we wat meer moeite doen. We willen dat de tegengestelde van een écht g-adisch getal $[a_i]$ (d.w.z. met cijfers tussen 0 en $g-1$) een écht g-adisch getal is. We kunnen daarom niet gewoon $[-a_i]$ nemen.

Oefening 3.1.1. Op pagina 6 hebben we van een g-adisch getal de tegengestelde berekend door het van 0 af te trekken. Wat is volgens deze methode in het algemeen de tegengestelde van $\ldots a_3 a_2 a_1 a_0$?

We vermoeden dus dat $[b_i]$ de tegengestelde is van $[a_i]$, waarbij $b_0 = g - a_0$ en $b_i = g - a_i - 1$ voor de overige i. Als we $[a_i] + [b_i]$ berekenen komt er $[c_i]$ uit, met $c_0 = g$ en $c_i = g - 1$ voor $i > 0$. Op het eerste gezicht lijkt dit niet veel op 0, maar we kunnen bewijzen dat wel degelijk $[c_i] = 0$. Hiervoor gebruiken we schrijfwijze (3.1) voor $[c_i]$.

$$\begin{aligned}[c_i] &= \ldots + (g-1)g^3 + (g-1)g^2 + (g-1)g^1 + (g)g^0 \\ &= \ldots + g^4 - g^3 + g^3 - g^2 + g^2 - g^1 + g^1 \\ &= \ldots + 0 + 0 + 0 + 0 \;\; = \;\; 0\end{aligned}$$

Gaan we vermenigvuldiging erbij betrekken, dan wordt de zaak ingewikkelder. Uit het voorbeeld van pagina 7 blijkt dat hoe verder een cijfer van het product naar links staat, hoe meer getallen bij elkaar opgeteld moesten worden om dit cijfer te verkrijgen. We willen een algemene formule vinden voor c_i in het product $[a_i] \times [b_i] = [c_i]$. Hiervoor schrijven we $[a_i]$ en $[b_i]$ weer zoals in vgl. (3.1).

$$[c_i] = (\ldots a_3 g^3 + a_2 g^2 + a_1 g^1 + a_0 g^0) \times (\ldots b_3 g^3 + b_2 g^2 + b_1 g^1 + b_0 g^0)$$

Als we deze vermenigvuldiging term voor term uitvoeren, krijgen we een som van $a_j b_k g^{j+k}$ voor alle mogelijke combinaties van j en k (ga dat na). Deze term hoort wegens de factor g^{j+k} bij het cijfer c_{j+k}. Op deze manier kunnen we inzien dat bijvoorbeeld

$$c_5 = a_0 b_5 + a_1 b_4 + a_2 b_3 + \ldots + a_5 b_0 = \sum_{k=0}^{5} a_k b_{5-k}$$

Dit is de som van alle $a_j b_k$ waarvoor $j + k = 5$. Voor andere cijfers c_i gaat het analoog. We concluderen:

$$[a_i] \times [b_i] = \Big[\sum_{k=0}^{i} a_k b_{i-k} \Big] \tag{3.4}$$

Deze formule is heel wat lastiger dan formule (3.3) voor de optelling! De bewijzen van de rekenregels van vermenigvuldiging zijn dan ook een stuk lastiger. Dat van de commutativiteit is nog wel te overzien; het komt er op neer dat je moet bewijzen dat

$$a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0 = b_0 a_i + b_1 a_{i-1} + \ldots + b_i a_0$$

Dat is een kwestie van de som in omgekeerde volgorde schrijven en vervolgens alle producten omdraaien.

Oefening 3.1.2. Ga na dat uit formule (3.4) volgt dat $[e_i]$ het eenheidselement van $\mathbb{Z}_g$ is, waarbij $e_0 = 1$ en $e_i = 0$ voor de overige i. Dat wil zeggen: bewijs dat $[e_i] \times [b_i] = [b_i]$ voor alle $[b_i]$.[2]

Het bewijs van de associativiteit voor $\times$ is een stuk lastiger, omdat daar drie elementen met elkaar vermenigvuldigd worden. Dit laten we daarom voorlopig achterwege, net als het bewijs van de distributiviteit.

3.1.1 Bezwaren tegen de $\sum$ methode

We hebben nu twee nadelen gezien van het schrijven van g-adische gehele getallen als een oneindige som. Ten eerste zijn de eigenschappen van vermenigvuldiging vrij moeilijk te bewijzen, zeker als je dat strikt volgens de regels van algebraïsche structuren wilt doen. Ten tweede kunnen cijfers groter zijn dan $g - 1$.

Wat misschien nog wel een belangrijker bezwaar is, is dat het niet wiskundig correct is om zomaar een oneindige som te nemen en daarmee te gaan rekenen zoals in (3.3) en (3.4). We zouden eerst moeten bewijzen dat deze sommen convergeren, en vervolgens dat (3.3) en (3.4) waar zijn. Daar hebben we te weinig voorkennis voor, daarom pakken we het anders aan. We definiëren g-adische getallen als abstracte rijtjes van 'cijfers', die op zichzelf niets voorstellen. Optelling en vermenigvuldiging worden vastgelegd met algoritmen (rekenvoorschriften). Het rekenvoorschrift voor optelling bijvoorbeeld doet

[2] Dat ook $[b_i] \times [e_i] = [b_i]$ hoef je niet te bewijzen, want dat volgt direct uit de commutativiteit van vermenigvuldiging in $\mathbb{Z}_g$.

eigenlijk niets anders dan stap voor stap 'onder elkaar staande' cijfers optellen, zoals we ook in §1.2 hebben gedaan. Het verschil is dat we eerst het overlenen laten zitten, we staan cijfers groter dan $g-1$ en kleiner dan 0 toe. Vervolgens laten we hier een algoritme op los dat kan overlenen, zodat een echt g-adisch getal ontstaat.

De verzameling van alle g-adisch-achtige getallen waar alle gehele getallen als cijfers zijn toegestaan, noemen we $\mathbb{Z}_g^*$. We zullen bewijzen dat dit een commutatieve ring met 1 is. Vervolgens beelden we de elementen van $\mathbb{Z}_g^*$ met het overleen-algoritme af naar $\mathbb{Z}_g$, en beredeneren dat $\mathbb{Z}_g$ ook een commutatieve ring met 1 moet zijn. Daarna laten we zien dan $\mathbb{Z}_g$ geen nuldelers heeft als g priem is, en kijken we waneer delen mogelijk is binnen $\mathbb{Z}_g$. Als toetje geven we uitleg bij een algoritme dat kan delen in $\mathbb{Z}_p$.

3.2 Formele definitie van $\mathbb{Z}_g^*$ en $\mathbb{Z}_g$

We zullen $\mathbb{Z}_g^*$ en $\mathbb{Z}_g$ nu formeel definiëren. Met $(a_i) : i \in \mathbb{N}$ bedoelen we een geordende rij van de vorm $(a_0, a_1, a_2, a_3, \cdots)$. Deze rij is een abstract ding: voordat we er de operaties optellen en vermenigvuldigen op gedefinieerd hebben, heeft de rij strikt gezien geen enkele betekenis. Toch houden we in ons achterhoofd wat we eigenlijk bedoelen met zo'n rij, namelijk een g-adisch geheel getal van de vorm

$$\ldots a_3 a_2 a_1 a_0$$

Zo wordt het veel gemakkelijker om intuïtief in te zien wat in de bewijzen nou eigenlijk gedaan wordt. We zullen in de rest van dit hoofdstuk (a_i) vaak afkorten tot a, analoog voor andere letters dan a. Als iets anders bedoeld wordt met zo'n letter, wordt dat expliciet vermeld.

Definitie 3.2.1. *We definiëren de verzameling $\mathbb{Z}_g^*$ als volgt.*

$$\forall g \in \mathbb{N}_{\geq 2} : \qquad \mathbb{Z}_g^* := \{(a_i) \mid i \in \mathbb{N},\ a_i \in \mathbb{Z}\}$$

Optelling en vermenigvuldiging in $\mathbb{Z}_g^*$ zijn zo gedefiniëerd als in algoritme 1 resp. 2, zie §3.3.1 en §3.3.2. Dat wil zeggen: $\forall a, b \in \mathbb{Z}_g^*$ is

$$a + b = add(a, b) \qquad en \qquad a \times b = mult(a, b)$$

Definitie 3.2.2. *$\mathbb{Z}_g$ is de deelverzameling van $\mathbb{Z}_g^*$ waarvoor alle a_i tussen 0 en $g-1$ liggen.*

$$\forall g \in \mathbb{N}_{\geq 2} : \qquad \mathbb{Z}_g := \{(a_i) \mid i \in \mathbb{N},\ a_i \in \mathbb{Z},\ 0 \leq a_i \leq g-1\}$$

Hoewel dit een deelverzameling van $\mathbb{Z}_g^*$ is, zijn optelling en vermenigvuldiging anders gedefinieerd.[3] *Nadat algoritme 1 of 2 is toegepast, laten we op de uitkomst namelijk ook nog algoritme 3 los, zie §3.4. Dat wil zeggen: $\forall a, b \in \mathbb{Z}_g$ is*

$$a + b = \mathrm{norm}\big(\mathrm{add}(a, b)\big) \qquad en \qquad a \times b = \mathrm{norm}\big(\mathrm{mult}(a, b)\big)$$

[3] Strikt gezien zijn het dan ook andere operaties.

3.3 Algoritmes voor $\mathbb{Z}_g^*$

We hebben de bewerkingen in $\mathbb{Z}_g$ en $\mathbb{Z}_g^*$ dus gedefiniëerd met algoritmen.[4] Het is alsof je een hypersnelle computer programmeert die bij twee oneindige rijtjes een nieuw oneindig rijtje oplevert. Natuurlijk bestaan zulke computers alleen in gedachten.

Hoewel onze hersenen niet als een computer werken, kunnen we toch inzien hoe zo'n algoritme werkt, en daarmee kunnen we bepaalde rekenregels bewijzen.

3.3.1 Optelling

Algorithm 1 Add

```
1: function add(a, b ∈ Z_g^*) ∈ Z_g^*
2: c ∈ Z_g^*
3: begin
4: for i := 0 to ∞ do
5:     c_i := a_i + b_i
6: result := c
7: end
```

Met algoritme 1 kan de som c van twee elementen a en b uit $\mathbb{Z}_g^*$ worden berekend. Bij dit eerste algoritme zullen we uitleggen hoe je het kunt lezen.

Regel 1 vertelt de computer dat de functie die tussen **begin** en **end** staat afgekort wordt als add(a, b). De functie heeft als domein $\mathbb{Z}_g^*$ en als bereik ook $\mathbb{Z}_g^*$. Op regel 2 wordt c in het geheugen van de computer geschreven, met de informatie dat c element van $\mathbb{Z}_g^*$ is. Dat heeft een computer nou eenmaal nodig, anders zou hij niet weten wat hij met regel 6 aanmoest.

Bij de regels 4 t/m 6 wordt de daadwerkelijke berekening uitgevoerd. Hierbij moeten we vermelden dat a gelijk is aan $(a_0, a_1, a_2, \cdots)$, analoog zijn ook b en c zulke rijtjes.[5] De *for-lus* in regel 4 vertelt dat het volgende gedeelte moet worden uitgevoerd voor $i = 0$ tot $i = \infty$. In regel 5 worden de afzonderlijke elementen (de 'cijfers') van (a_i) en (b_i) bij elkaar opgeteld; het resultaat (c_i) wordt in regel 6 opgeslagen als c.

Wat het algoritme doet kan worden samengevat als

$$(a_i) + (b_i) = (a_i + b_i) \tag{3.5}$$

zoals je gemakkelijk kunt nagaan. De inwendigheid van $+$ in $\mathbb{Z}_g^*$ is wel duidelijk, optelling is immers ook inwendig in $\mathbb{Z}$ (bedenk dat $a_i, b_i \in \mathbb{Z}$). Ook de associativiteit van optelling is makkelijk te bewijzen.

$$\begin{aligned}\big((a_i) + (b_i)\big) + (c_i) = (a_i + b_i) + (c_i) &= \big((a_i + b_i) + c_i\big) \\ &= \big(a_i + (b_i + c_i)\big) = (a_i) + (b_i + c_i) = (a_i) + \big((b_i) + (c_i)\big)\end{aligned}$$

[4] De taal waarin de algoritmen geschreven zijn is afgeleid van Pascal.

[5] Natuurlijk moet de computer dat ook weten, maar voor de overzichtelijkheid hebben we dit uit het algoritme weggelaten.

Maar dit bewijs lijkt wel heel veel op dat van pagina 22! Het enige verschil is dat de vierkante haakjes [ ] vervangen zijn door ronde haakjes ( ), maar dat is slechts een kwestie van notatie. En natuurlijk is de interpretatie van het bewijs anders, $[a_i]$ stelde immers een oneindige som voor terwijl (a_i) 'slechts' een abstracte rij getallen is. Dat maakt algebraïsch echter niet uit, de manier van bewijzen blijft hetzelfde. Verder is hier $a_i \in \mathbb{Z}$, terwijl we in de voorbereiding met $a_i \in \mathbb{N}$ werkten. Ook dat is niet erg, want in $\mathbb{Z}$ gelden alle samenstellingswetten van $\mathbb{N}$ ook.

Voor de bewijzen van de andere samenstellingswetten voor optelling in $\mathbb{Z}_g^*$ gaat dit ook op. Dat komt doordat de optelling op pagina 21 hetzelfde is 'gedefinieerd' als hier, namelijk als $[a_i] + [b_i] = [a_i + b_i]$. Daarmee zijn de commutativiteit en de associativiteit van $+$, het bestaan van een nulelement, en het bestaan van een tegengestelde voor elk element bewezen; dit hebben we immers allemaal in §3.1 gedaan. Voor de tegengestelde van (a_i) mogen we nu zelfs $(-a_i)$ nemen, omdat we met $a_i \in \mathbb{Z}$ werken.

3.3.2 Vermenigvuldiging

Algorithm 2 Mult

```
1:  function mult(a, b ∈ Z_g^*) ∈ Z_g^*
2:  c ∈ Z_g^*
3:  begin
4:  c := (0, 0, 0, ···)
5:  for i := 0 to ∞ do
6:      begin
7:      for z := 0 to i do
8:          c_i := c_i + a_z · b_{i−z}
9:      end
10: result := c
11: end
```

Ook algoritme 2 komt op hetzelfde neer als de formule voor vermenigvuldiging zoals we die in §3.1 hebben afgeleid, namelijk vgl. (3.4). Dit zullen we beredeneren nadat we wat uitleg bij het algoritme hebben gegeven.

In regel 4 wordt c opgeslagen als een rij nullen: we beginnen met een schone lei. In regel 5 begint een oneindige lus, die op zijn beurt een *eindige* lus bevat, namelijk die van regel 7. Regel 8 ziet er wat vreemd uit, je zou zeggen dat dit alleen kan als $a_z \cdot b_{i-z} = 0$. Dat hoeft echter niet, want in computertaal betekent $c_i := c_i + a_z \cdot b_{i-z}$ iets anders dan in de wiskunde. De rechter c_i is het getal dat al in het geheugen van de computer stond (in het begin dus 0), die wordt vervangen door de linker c_i. Eigenlijk betekent regel 8 dus: *tel* $a_z \cdot b_{i-z}$ *op bij* c_i.

Wat wordt hier nu eigenlijk gedaan? We berekenen $(a_i) \cdot (b_i) = (c_i)$. Elk 'cijfer' c_i

wordt samengesteld uit de som van alle $a_z \cdot b_{i-z}$ waarvoor $0 \leq z \leq i$. Dat wil zeggen:

$$(a_i) \cdot (b_i) = \Big(\sum_{z=0}^{i} a_z b_{i-z} \Big) \tag{3.6}$$

en dat is precies dezelfde formule als (3.4).[6] Omdat we in §3.1 de commutativiteit van $\times$ en het bestaan van een eenheidselement hebben bewezen, zijn we daar klaar mee. De inwendigheid is duidelijk. Blijft over de associativiteit en de distributiviteit.[7]

Stelling 3.3.1. *De vermenigvuldiging is associatief in* $\mathbb{Z}_g^*$.

Bewijs. We willen bewijzen dat $(ab)c = a(bc)$ voor alle $a, b, c \in \mathbb{Z}_g^*$. Hiervoor voegen we twee mult-algoritmes[8] samen tot één. Het begin en eind van het algoritme dat alleen voor de computer van belang is laten we voor het gemak weg. De uitkomst van $a \cdot b$ noemen we q; vervolgens berekenen we de uitkomst $k = q \cdot c$ van het algoritme. Het algoritme berekent dus $(ab)c$.

for $i := 0$ **to** ∞ **do**
begin
for $z := 0$ **to** i **do**
$q_i := q_i + a_z \cdot b_{i-z}$; (a) {Hier wordt $q = a \cdot b$ berekend zoals in algoritme 2.}
for $z := 0$ **to** i **do**
$k_i := k_i + q_z \cdot c_{i-z}$; (b) {Hier wordt $k = qc = (ab)c$ berekend.}
end

In for-lus (b) is q_z gelijk aan de bij (a) berekende som van i termen, dus we kunnen het algoritme als volgt korter opschrijven.

for $i := 0$ **to** ∞ **do**
begin
for $y := 0$ **to** i **do**
for $z := 0$ **to** $i - y$ **do**
$k_i := k_i + a_z \cdot b_{i-y-z} \cdot c_y$ {Let op: z vervult hier een andere functie dan in for-lus (a).}
end

Hier wordt elk 'cijfer' k_i berekend als de som van alle $a_p b_q c_r$ waarvoor $p + q + r = i$. Immers, $z + (i - y - z) + y = i$, en omdat z, $i - y - z$ en y niet kleiner dan nul mogen zijn is het voldoende om y van 0 tot i te laten lopen en z van 0 tot $i - y$. Omdat dit een eindige som is in $\mathbb{Z}$, doet de volgorde van de optelling er niet toe. Zolang we maar alle

[6] Dat k vervangen is door z en [ ] door ( ) is slechts een kwestie van notatie.
[7] Het bestaan van een invers element is een geval apart, dit komt in een andere paragraaf aan de orde.
[8] d.i. algoritme 2

combinaties van $a_p b_q c_r$ waarvoor $p+q+r=i$ een keer optellen bij k_i, komt er dezelfde k uit. We kunnen het algoritme dus ook als volgt schrijven.

for $i := 0$ **to** ∞ **do**
  begin
  for $y := 0$ **to** i **do**
    for $z := 0$ **to** $i - y$ **do**
      $k_i := k_i + a_y \cdot b_z \cdot c_{i-y-z}$
  end

Wegens de commutativiteit van vermenigvuldiging in $\mathbb{Z}$ mogen we in het laatste algoritme ook schrijven: $k_i := k_i + b_z \cdot c_{i-y-z} \cdot a_y$. Als we dat doen, hebben we precies het tweede algoritme van dit bewijs teruggekregen, alleen nu met a, b en c omgewisseld. De uitkomst van dit algoritme is dus gelijk aan $(bc)a$ en dat is $a(bc)$. Maar we begonnen met een algoritme dat $(ab)c$ berekende, en omdat de algoritmes steeds zo zijn omgeschreven dat de uitkomst gelijk blijft, mogen we concluderen dat $(ab)c = a(bc)$. □

Nu bewijzen we de distributiviteit.

Stelling 3.3.2. *De vermenigvuldiging is distributief over optelling in $\mathbb{Z}_g^*$.*

Bewijs. We willen bewijzen dat $a(b+c) = ab + ac$ en dat $(a+b)c = ac + bc$ voor alle $a, b, c \in \mathbb{Z}_g^*$. Hiervoor voegen we weer twee functies samen, dit keer de add-functie en de mult-functie (algoritme 1 en 2). Dit samengestelde algoritme berekent, zoals je gemakkelijk kunt nagaan, $a(b+c)$.

for $i := 0$ **to** ∞ **do**
  begin
  $q_i := b_i + c_i$; (a) {Hier wordt $q = \text{add}(b, c)$ berekend.}
  for $z := 0$ **to** i **do**
    $k_i := k_i + a_z \cdot q_{i-z}$; (b) {Hier wordt $k = \text{mult}(a, q)$ berekend.}
  end

Volgens (a) is $q_i = b_i + c_i$, dus (b) kunnen we schrijven als $k_i := k_i + a_z(b_{i-z} + c_{i-z})$, en dat is wegens de distributiviteit in $\mathbb{Z}$ gelijk aan $k_i + a_z b_{i-z} + a_z c_{i-z}$. We kunnen dit algoritme dus schrijven als

for $i := 0$ **to** ∞ **do**
  begin
  for $z := 0$ **to** i **do**
    $k_i + a_z b_{i-z} + a_z c_{i-z}$ (a)
  end

We kunnen (a) in tweeën splitsen, zodat we het volgende algoritme krijgen:

for $i := 0$ **to** ∞ **do**
  for $z := 0$ **to** i **do**
    begin
    $k_i := k_i + a_z \cdot b_{i-z}$; (a)
    $k_i := k_i + a_z \cdot c_{i-z}$;
    end

In dit laatste algoritme kunnen we (a) als het ware buiten haakjes halen door deze berekening als eerst uit te voeren. De uitkomst noemen we q; die tellen we aan het eind bij k_i op. Ga voor jezelf na dat het volgende algoritme echt dezelfde uitkomst zal geven als het vorige.

for $i := 0$ **to** ∞ **do**
  begin
  for $z := 0$ **to** i **do**
    $q_i := q_i + a_z \cdot b_{i-z}$; (a)
  for $z := 0$ **to** i **do**
    $k_i := k_i + a_z \cdot c_{i-z}$; (b)
  $k_i := q_i + k_i$; (c)
  end

Bij (a) wordt ab berekend, bij (b) wordt ac berekend, en bij (c) worden de uitkomsten daarvan bij elkaar opgeteld. De uitkomst k van het algoritme is dus gelijk aan $ab + ac$, en omdat het algoritme waarmee we begonnen $a(b + c)$ berekende, hebben we bewezen dat $a(b+c) = ab+ac$, dat is de links-distributiviteit. Omdat de commutativiteit van $\times$ al is bewezen, geldt volgens stelling 2.4.2 ook de rechts-distributiviteit. Hiermee stelling 3.3.2 bewezen. □

We hebben in deze paragraaf bewezen dat voor $\mathbb{Z}_g^*$ de volgende samenstellingswetten uit Tabel 2.2 gelden. Voor + gelden 1), 2), 3), 4) en 5); voor $\times$ gelden 1), 2), 3) en 5); verder geldt ook 6). Met Tabel 2.4 volgt hieruit dat $\mathbb{Z}_g^*$ een *commutatieve ring met* 1 is.

3.4 Normalisatie

We hebben nu bewezen dat $\mathbb{Z}_g^*$ een ring vormt, maar dat willen we uiteindelijk natuurlijk bewijzen voor $\mathbb{Z}_g$. Om dit te bereiken komen we terug op het idee dat een element a van $\mathbb{Z}_g^*$ te schrijven is als een oneindige som van de vorm

$$a = \sum_{i=0}^{\infty} a_i g^i, \qquad a_i \in \mathbb{Z} \tag{3.7}$$

Algorithm 3 Norm

```
1: function norm(a ∈ Z_g^*) ∈ Z_g
2: d_{-1} := 0          {Dit is nodig omdat de computer anders bij 6 in de knoop komt.}
3: begin
4: for i := 0 to ∞ do
5:     begin
6:     a_i := a_i + d_{i-1}          {Hier wordt als het ware overgeleend van a_{i-1}.}
7:     d_i := a_i div g              {a div b geeft het quotiënt bij de restdeling a/b.}
8:     a_i := a_i − g · d_i          {Dit is de rest bij die deling.}
9:     end
10: result := a
11: end
```

Nu gaan we de volgende zeer fundamentele stelling gebruiken. Voor een bewijs verwijzen we naar §2.2 van [1].

Stelling 3.4.1. (Deling met rest) *Stel $a, b \in \mathbb{Z}$ en $b > 0$. Dan zijn er gehele getallen q en r zó dat*

$$a = bq + r, \qquad 0 \leq r < b$$

We noemen q het *quotiënt* en r de *rest* van de restdeling $\frac{a}{b}$. De stelling zegt dus niets anders dan dat deze restdeling altijd kan worden uitgevoerd (mits $b \neq 0$), waarbij een positieve rest kleiner dan b ontstaat.

We kunnen volgens stelling 3.4.1 restdeling van de 'cijfers' a_i van a (zie formule 3.7) door g uitvoeren. Het quotiënt noemen we d_i en de rest c_i. We krijgen:

$$a_i g^i = (d_i g + c_i) g^i = d_i g^{i+1} + c_i g^i, \qquad 0 \leq c_i < g$$

c_i wordt het nieuwe cijfer van a op positie i; we tellen d_i wegens de factor g^{i+1} op bij het cijfer op positie $i+1$, dit wordt de nieuwe a_{i+1}. Nu kunnen we restdeling op a_{i+1} toepassen, hierbij blijft c_i onveranderd. Als we op deze manier vanaf a_0 restdeling toepassen, krijgen we

$$a = \sum_{i=0}^{\infty} a_i g^i = \sum_{i=0}^{\infty} c_i g^i, \qquad c_i \in \mathbb{Z},\ 0 \leq c_i < g.$$

We hebben een getal $a \in \mathbb{Z}_g^*$ omgevormd tot een een getal uit $\mathbb{Z}_g$; immers, de cijfers c_i liggen tussen 0 en $g-1$. Dit is precies wat algoritme 3 (zie pagina 30) doet, het komt eigenlijk op hetzelfde neer als het 'overlenen' zoals we in §1.2 hebben gedaan.

Met algoritme 3 kunnen we $\mathbb{Z}_g^*$ afbeelden naar $\mathbb{Z}_g$. We zullen in deze paragraaf de volgende stelling bewijzen.

Stelling 3.4.2. *Voor alle $g \in \mathbb{N}_{\geq 2}$ is $\mathbb{Z}_g$ een commutatieve ring met* 1.

Allereerst voeren we een notatie in.

Definitie 3.4.3. *Voor alle $(a_i) \in \mathbb{Z}_g^*$ definiëren we voor alle $i > 0$:*

$$a'_i := a_{i-1} \qquad en \qquad a'_0 := 0$$

Verder duiden we (a'_i) aan met $(a_i)'$ ofwel a'.

Het is intuïtief duidelijk dat a' overeenkomt met $g \times a$. Alle cijfers van a schuiven immers één positie naar links op, en de lege plek wordt opgevuld met een 0. Deze bewering zullen we in het volgende hoofdstuk nodig hebben, daarom geven we een bewijs. In plaats van g schrijven we $y = \ldots 00010$ ofwel $(0, 1, 0, 0, 0, \cdots)$; het is duidelijk dat $y = \text{norm}(g)$.

Stelling 3.4.4. *De afbeelding $a \mapsto a'$ in $\mathbb{Z}_g$ komt overeen met vermenigvuldiging van a met $(y_i) = (0, 1, 0, 0, 0, \cdots)$. Informeel komt deze stelling neer op $a' = a \times g$.*

Bewijs. We hebben eerder gezien dat de mult-functie van algoritme 2 dezelfde uitkomst geeft als formule (3.6) op pagina 27. In deze formule vullen we voor b het getal (y_i) in, zo krijgen we de volgende formule voor $(a_i) \times (y_i)$.

$$\Big(\sum_{z=0}^{i} a_z y_{i-z} \Big) \tag{3.8}$$

Als $z = i - 1$ is $y_{i-z} = y_1 = 1$, dan is $a_z y_{i-z}$ dus gelijk aan $a_{i-1} \times 1 = a_{i-1}$. Voor de overige z is $y_{i-z} \neq y_1$, dan is $y_z = 0$. We concluderen dat de uitkomst van (3.8) alleen bepaald wordt door $z = i-1$, dus de uitkomst is (a_{i-1}),[9] ofwel (a'_i), ofwel $(a_i)'$. Hiermee is bewezen dat $a' = a \times (y_i)$. □

Om stelling 3.4.2 te bewijzen, hebben we eerst een paar lemma's (hulpstellingen) nodig.

3.4.1 Lemma's

Lemma 3.4.5. *Voor alle $a \in \mathbb{Z}_g^*$ is er een $d \in \mathbb{Z}_g^*$ zodat* $\text{norm}(a) = a + d' - gd$*, waarbij bovendien $d_i = a_i + d_{i-1}$ **div** g voor alle $i \geq 0$.*

Bewijs. Beschouw algoritme 3. In regel 6 wordt d_{i-1} bij a_i opgeteld; in regel 8 wordt vervolgens g maal de in regel 7 berekende waarde van d_i, van a_i afgetrokken. Dit betekent dat het genormaliseerde cijfer a_i gelijk is aan $a_i + d_{i-1} - gd_i$, en omdat bovendien $d_{-1} := 0$ is dat gelijk aan $a_i + d'_i - gd_i$. We concluderen dat $\text{norm}(a) = (a_i + d'_i - gd_i)$, en met behulp van vgl. (3.5) volgt hieruit dat

$$\text{norm}(a) = (a_i + d'_i + -gd_i) = (a_i) + (d'_i) + (-gd_i) = a + d' - gd$$

Bovendien blijkt uit regel 6 en 7 dat $d_i = a_i + d_{i-1}$ **div** g. □

[9] en het eerste cijfer is $a_0 y_0 = 0$

Lemma 3.4.6.

$$\forall b, e \in \mathbb{Z}_g^* : \qquad \text{norm}(b) = \text{norm}(b + e' - ge)$$

Bewijs. Volgens lemma 3.4.5 is er een $z \in \mathbb{Z}_g^*$ zodat

$$\text{norm}(b) = b + z' - gz \tag{3.9}$$

$$z_i = b_i + z_{i-1} \textbf{ div } g \tag{3.10}$$

We gaan norm$(b + e' - ge)$ voor een willekeurige $e \in \mathbb{Z}_g^*$ berekenen, en willen bewijzen dat dat dit gelijk is aan norm(b). We doorlopen de norm-functie voor $a = b + e' - ge$. Eerst bereken we het nulde cijfer a_0. In regel 6 van algoritme 3 gebeurt er nog niets van belang, want $d_{-1} = 0$. Regel 7 geeft vervolgens:

$$\begin{aligned} d_0 = a_0 \textbf{ div } g &= b_0 + e'_0 - ge_0 \textbf{ div } g = b_0 - ge_0 \textbf{ div } g = -e_0 + (b_0 \textbf{ div } g) \\ &= -e_0 + (b_0 + z_{-1} \textbf{ div } g) \overset{(3.10)}{=} -e_0 + z_0 \end{aligned} \tag{3.11}$$

Regel 8 berekent:

$$a_0 := a_0 - gd_0 = (b_0 + e'_0 - ge_0) - g(-e_0 + z_0) = b_0 - ge_0 + ge_0 - gz_0 = b_0 - gz_0$$

en dat is volgens vgl. (3.9) gelijk aan het nulde cijfer van norm(b), want $z'_0 = 0$.

Nu kijken we naar het algemene geval. Stel dat we voor een zekere $i > 0$ weten dat

$$d_{i-1} = -e_{i-1} + z_{i-1} \tag{3.12}$$

Regel 6 geeft dan

$$\begin{aligned} a_i := a_i + d_{i-1} &= (b_i + e'_i - ge_i) + (-e_{i-1} + z_{i-1}) \\ &= b_i + e_{i-1} - ge_i - e_{i-1} + z_{i-1} = b_i - ge_i + z_{i-1} \end{aligned} \tag{3.13}$$

Regel 7 berekent

$$\begin{aligned} d_i := a_i \textbf{ div } g &\overset{(3.13)}{=} (b_i - ge_i + z_{i-1}) \textbf{ div } g \\ &= -e_i + \big((b_i + z_{i-1}) \textbf{ div } g\big) \overset{(3.10)}{=} -e_i + z_i \end{aligned} \tag{3.14}$$

Regel 8 geeft vervolgens:

$$\begin{aligned} a_i := a_i - gd_i &\overset{(3.13)}{=} (b_i - ge_i + z_{i-1}) - gd_i \overset{(3.14)}{=} (b_i - ge_i + z_{i-1}) - g(-e_i + z_i) \\ &= b_i - ge_i + ge_i + z_{i-1} - gz_i = b_i + z'_i - gz_i \end{aligned}$$

en dat is volgens vgl. (3.9) precies gelijk aan het i-de cijfer van norm(b). Bovendien blijkt uit (3.14) dat opnieuw de gelijkheid in (3.12) geldt, alleen nu met i eentje opgehoogd. We kunnen het hele verhaal dus opnieuw toepassen voor $i+1$, dan voor $i+2$, etc; telkens blijkt dat a_i, het i-de cijfer van norm$(b+e'-ge)$, gelijk is aan het i-de cijfer van norm(b). Volgens (3.11) mogen we de redenering beginnen bij $i = 1$.[10] Bovendien zagen we eerder al dat ook de nulde cijfers aan elkaar gelijk zijn. We concluderen dat *alle* cijfers van norm$(b + e' - ge)$ en norm(b) overeenkomen, waarmee de stelling bewezen is. □

[10] Bedenk dat er $i - 1$ staat bij vgl. (3.12).

Lemma 3.4.7.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad a' + b' = (a + b)'$$

Bewijs. In formule (3.5) hebben we gezien dat $(a_i) + (b_i) = (a_i + b_i)$. Als we het i-de cijfer van $(a_i) + (b_i)$ voor het gemak $(a + b)_i$ noemen, volgt hieruit dat $(a + b)_i = a_i + b_i$. Nu zien we dat voor alle $i > 0$ geldt:

$$(a + b)'_i = (a + b)_{i-1} = a_{i-1} + b_{i-1} = a'_i + b'_i = (a' + b')_i$$

Nu moeten we de stelling alleen nog maar bewijzen voor $i = 0$. Dat is zo gedaan:

$$(a + b)'_0 = 0 = 0 + 0 = a'_0 + b'_0 = (a' + b')_0$$

Hiermee is bewezen dat $(a + b)'_i = (a' + b')_i$ voor alle i, dus alle cijfers van $(a + b)'$ en $a' + b'$ komen met elkaar overeen, deze getallen zijn dus gelijk. Hiermee is de stelling bewezen. □

Lemma 3.4.8.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad a' \times b = (a \times b)'$$

Bewijs. Volgens formule (3.6) geldt voor de cijfers a_i en b_i van de getallen (a_i) en (b_i):

$$a_i \times b_i = \sum_{z=0}^{i} a_z b_{i-z}$$

Hieruit volgt dat voor alle $i > 0$:[11]

$$(ab)'_i = (ab)_{i-1} = \sum_{z=0}^{i-1} a_z b_{i-1-z} = \sum_{k=1}^{i} a_{k-1} b_{i-k} = \sum_{k=1}^{i} a'_k b_{i-k} = (a'b)_i$$

We kunnen gemakkelijk aantonen dat bovenstaande gelijkheid ook geldt voor $i = 0$.

$$(ab)'_0 = 0 = 0 \times b_0 = a'_0 b_0 = \sum_{z=0}^{0} a'_0 b_0 = (a'b)_0$$

Conclusie: voor alle i is $(ab)'_i = (a'b)_i$, dus de getallen $(ab)'$ en $(a'b)$ zijn aan elkaar gelijk. □

Lemma 3.4.9.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad \mathrm{norm}\big(\mathrm{norm}(a) + b\big) = \mathrm{norm}(a + b)$$

Bewijs. Volgens lemma 3.4.5 kunnen we $\mathrm{norm}(a)$ schrijven als $a + d' - gd$ voor een zekere $d \in \mathbb{Z}_g^*$. Nu kunnen we afleiden:[12]

$$\mathrm{norm}\big(\mathrm{norm}(a) + b\big) = \mathrm{norm}\big((a + d' - gd) + b\big) = \mathrm{norm}((a + b) + d' - gd) \overset{3.4.6}{=} \mathrm{norm}(a + b)$$

□

[11] In de derde stap wordt k gesubstitueerd voor $z + 1$.

[12] een nummer boven een =-tekens verwijst naar het lemma dat bij die stap gebruikt wordt.

Lemma 3.4.10.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad \text{norm}\big(\text{norm}(a) \cdot b\big) = \text{norm}(a \cdot b)$$

Bewijs. We kunnen norm(a) schrijven als $a + d' - gd$ voor een $d \in \mathbb{Z}_g^*$.

$$\begin{aligned}\text{norm}\big(\text{norm}(a) \cdot b\big) &= \text{norm}\big((a + d' - gd)b\big) = \text{norm}(ab + d'b - gdb) \\ &\overset{3.4.8}{=} \text{norm}\big(ab + (db)' - g(db)\big) \overset{3.4.6}{=} \text{norm}(ab)\end{aligned}$$

□

3.4.2 Bewijs: $\mathbb{Z}_g$ is een commutatieve ring met 1

Om stelling 3.4.2 te bewijzen, hebben we nog twee belangrijke maar eenvoudig te bewijzen stellingen nodig.

Stelling 3.4.11.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad \text{norm}(a + b) = \text{norm}\big(\text{norm}(a) + \text{norm}(b)\big)$$

Bewijs. De eerste gelijkheid volgt met behulp van het feit dat norm$(b) \in \mathbb{Z}_g^*$, de tweede met de commutativiteit van optelling in $\mathbb{Z}_g^*$.

$$\text{norm}\big(\text{norm}(a) + \text{norm}(b)\big) \overset{3.4.9}{=} \text{norm}\big(a + \text{norm}(b)\big) \overset{3.4.9}{=} \text{norm}(a + b)$$

□

Stelling 3.4.12.

$$\forall a, b \in \mathbb{Z}_g^* : \qquad \text{norm}(a \cdot b) = \text{norm}\big(\text{norm}(a) \cdot \text{norm}(b)\big)$$

Bewijs. Dit gaat geheel analoog aan dat van de vorige stelling.

$$\text{norm}\big(\text{norm}(a) \cdot \text{norm}(b)\big) \overset{3.4.10}{=} \text{norm}\big(a \cdot \text{norm}(b)\big) \overset{3.4.10}{=} \text{norm}(a \cdot b)$$

□

Nu hebben we genoeg gereedschap om te bewijzen dat $\mathbb{Z}_g$ een commutatieve ring met 1 is.

Laat a, b, c elementen zijn van $\mathbb{Z}_g$. Omdat $\mathbb{Z}_g \subset \mathbb{Z}_g^*$ is ook $a, b, c \in \mathbb{Z}_g^*$, dus op a, b en c mogen we de regels van een commutatieve ring met 1 al toepassen.

De optelling en vermenigvuldiging in $\mathbb{Z}_g$ zijn anders gedefiniëerd dan in $\mathbb{Z}_g^*$, zie definitie 3.2.2 op pagina 24. Om onderscheid tussen de operaties te maken, duiden we optelling en vermenigvuldiging in $\mathbb{Z}_g$ aan met $\oplus$ resp. $\otimes$, in $\mathbb{Z}_g^*$ schrijven we gewoon $+$ en $\times$. Volgens definitie 3.2.2 geldt:

$$a \oplus b = \text{norm}(a + b), \qquad a \otimes b = \text{norm}(a \times b).$$

Verder geldt voor alle $z \in \mathbb{Z}_g$ natuurlijk dat

$$\text{norm}(z) = z \tag{3.15}$$

Immers, alle cijfers z_i van z liggen tussen 0 en $g-1$, dus in algoritme 3 geldt voor alle i dat $d_i = z_i \textbf{ div } g = 0$. Hierdoor blijven alle z_i onveranderd.

Als eerste bewijzen we de *inwendigheid* van $\oplus$ en $\otimes$ in $\mathbb{Z}_g$. Dat is zo gedaan. Immers, $a \oplus b = \text{norm}(a+b)$, en omdat $+$ inwendig is in $\mathbb{Z}_g^*$, is dit de norm-functie toegepast op een element van $\mathbb{Z}_g^*$. Volgens definitie 3.2.2 is het resultaat weer een element van $\mathbb{Z}_g$. Voor vermenigvuldiging gaat het analoog: vervang overal $\oplus$ door $\otimes$ en $+$ door $\times$, en je bent er.

Nu bewijzen we de *commutativiteit* van $\oplus$ en $\otimes$ in $\mathbb{Z}_g$. Ook dat is eenvoudig:

$$a \oplus b = \text{norm}(a+b) = \text{norm}(b+a) = b \oplus a$$

Voor vermenigvuldiging gaat het weer analoog.

Voor de *associativiteit* moeten we wat meer moeite doen, omdat we met drie elementen te maken hebben. Het bewijs voor $\oplus$ gaat als volgt.[13] We korten norm af tot $\mathbf{n}$.

$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus \mathbf{n}(b+c) = \mathbf{n}\big(a + \mathbf{n}(b+c)\big) \overset{(3.15)}{=} \mathbf{n}\big(\mathbf{n}(a) + \mathbf{n}(b+c)\big) \\ &\overset{3.4.11}{=} \mathbf{n}\big(a + (b+c)\big) = \mathbf{n}\big((a+b)+c\big) = \mathbf{n}\big(\mathbf{n}(a+b) + \mathbf{n}(c)\big) \\ &= \mathbf{n}\big(\mathbf{n}(a+b) + c\big) = \mathbf{n}(a+b) \oplus c = (a \oplus b) \oplus c \end{aligned}$$

Het bestaan van een nulelement en een eenheidselement in $\mathbb{Z}_g$ is gemakkelijk te bewijzen: het zijn dezelfde 0 en 1 als in $\mathbb{Z}_g^*$. Voor $\oplus$ 0 hebben we het bewijs uitgewerkt, voor $\otimes$ 1 gaat het analoog.

$$a \oplus 0 = \mathbf{n}(a+0) = \mathbf{n}(a) = a$$

Omdat we de commutativiteit voor $\oplus$ en $\otimes$ al hebben bewezen, is ook $0 \oplus a = a$ en $1 \otimes a = a$, waarmee is aangetoond dat 0 en 1 inderdaad de gezochte elementen zijn.

Het bestaan van een *tegengestelde* van elke $(a_i) \in \mathbb{Z}_g$ is makkelijk aan te tonen, het is vergelijkbaar met de manier waarop we de tegengestelde op pagina 6 hebben berekend. De kleinste i waarvoor $a_i \neq 0$ noemen we k. We nemen het getal $(b_i) \in \mathbb{Z}_g$ waarbij $b_i = 0$ voor alle $i < k$, $b_k = g - a_k$ en $b_i = g - a_i - 1$ voor alle $i > k$. Ga na dat inderdaad $(b_i) \in \mathbb{Z}_g$. Algoritme 1 berekent:

$$(a_i) + (b_i) = (0, 0, \cdots, 0, g, g-1, g-1, g-1, \cdots) := (c_i)$$

Nu berekenen we $(a_i) \oplus (b_i) = \text{norm}(c_i)$. Alle cijfers c_i met $i < k$ blijven natuurlijk 0. Dan wordt $d_k = g \textbf{ div } g = 1$ berekent, daarna $c_k = g - g \cdot 1 = 0$. Dan wordt d_k bij c_{k+1} opgeteld zodat dit g wordt, deze wordt weer 0 waarbij weer 1 wordt overgeleend, etc. Zo wordt $(c_i) = 0$, dus (b_i) is de tegengestelde van (a_i).

[13] Opnieuw gaat het voor $\otimes$ analoog, maar nu moet wel stelling 3.4.11 vervangen worden door 3.4.12.

Het bestaan van een inverse bespreken we in de volgende paragraaf, evenals het (niet) bestaan van nuldelers.

Tot slot bewijzen we de *distributiviteit*.

$$a \otimes (b \oplus c) = a \otimes \mathbf{n}(b+c) = \mathbf{n}\big(a \cdot \mathbf{n}(b+c)\big) \overset{3.4.10}{=} \mathbf{n}\big(a(b+c)\big)$$
$$= \mathbf{n}(ab+ac) \overset{3.4.12}{=} \mathbf{n}\big(\mathbf{n}(ab)+\mathbf{n}(ac)\big) = \mathbf{n}(a \otimes b + a \otimes c) = a \otimes b \oplus a \otimes c$$

Nu hebben we de eigenschappen 1), 2), 3), 4) en 5) voor optelling bewezen, zie Tabel 2.2. We hebben 1), 2), 3) en 5) voor vermenigvuldiging en bovendien 6) bewezen. Volgens Tabel 2.4 is hiermee stelling 3.4.2 bewezen: $\mathbb{Z}_g$ is een commutatieve ring met 1.

In het vervolg werken we vooral met $\mathbb{Z}_g$. Daarom schrijven we gewoon weer $+$ en $\times$ in plaats van $\oplus$ en $\otimes$, tenzij anders vermeld.

3.5 Deelbaarheid in $\mathbb{Z}_g$

Wanneer is delen mogelijk in $\mathbb{Z}_g$? En in welke gevallen zijn er nuldelers? Daarover gaat deze paragraaf.

3.5.1 Nuldelers

Laten we met die laatste vraag beginnen. Zoals al eerder is gezegd, zijn nuldelers getallen a, b ongelijk aan 0 waarvoor $a \times b = 0$. In de getalsystemen waarmee we bekend zijn bestaan geen nuldelers, maar we zullen laten zien dat deze er in $\mathbb{Z}_g$ wél zijn voor bepaalde grondtallen g.

Hiervoor hebben we eerst wat basiskennis nodig over modulorekenen[14], ook wel klokrekenen genoemd. Iedereen leert als kind rekenen met de klok van twaalf. Als het nu 8 uur is, is het 7 uur later natuurlijk 3 uur. Dit noteren[15] we als $8+7 = 15 \equiv 3 \pmod{12}$. In het algemeen is $a \equiv b \pmod{g}$ precies dan als a en b dezelfde *rest* hebben bij deling door g.

Met $b \bmod g$ bedoelen we het kleinste positieve getal a waarvoor $a \equiv b \pmod{g}$. Je kunt makkelijk inzien dat $b \bmod g$ de rest is van de restdeling van b door g. Hierdoor is altijd $0 \leq b \bmod g < g$.

Maar wat heeft modulorekenen nou met g-adische getallen te maken? Bij het optellen of vermenigvuldigen van twee (g-adische) getallen gebruik je, wellicht zonder dat je het door hebt, modulorekenen. Bereken bijvoorbeeld $13 \cdot 8$ in grondtal 10. Het eerste cijfer 4 van het product heb je berekend met $3 \cdot 8 = 24 \equiv 4 \pmod{10}$, ofwel, door $2 \cdot 10$ naar links over te lenen. Bij g-adische getallen werkt het net zo. Als $\ldots a_2 a_1 a_0 \times \ldots b_2 b_1 b_0 = \ldots c_2 c_1 c_0$, dan is $c_0 = a_0 b_0 \bmod g$.

Nu gaan we laten zien dat Z_{10} nuldelers heeft. We zoeken hiervoor een $x \in \mathbb{Z}_{10}$ ongelijk aan 0 of 1 met de op het eerste gezicht absurde eigenschap $x^2 = x$. Zo'n getal

[14] Zie ook [10] voor meer uitleg hierover.

[15] Spreek uit: 'vijftien en drie zijn congruent modulo twaalf'.

blijkt echt te bestaan. We beginnen met het vaststellen van het eerste cijfer:

$$x_0 = 5.$$

Dan is ook het nulde cijfer van x^2 gelijk aan $5^2 = 25 = 5 \bmod 10$; dit cijfer voldoet dus aan de eis. Nu blijkt dat alle volgende cijfers vastliggen; we laten zien hoe we ze stap voor stap kunnen construeren.

Stel dat we in de k-de stap het cijfer x_k willen bepalen zodat aan de eis wordt voldaan.[16] In de vorige stappen hebben we dus als benadering $x = \ldots x_{k-1}x_{k-2}\ldots x_0$ gevonden, waarbij $x^2 = \ldots x_{k-1}x_{k-2}\ldots x_0$. Deze k cijfers kunnen niet meer beïnvloed worden door volgende cijfers, deze zijn dus in elk geval goed.

Dit alles schrijven we iets duidelijker op. We weten dat

$$(x_{k-1}\ldots x_2x_1x_0)^2 \equiv x_{k-1}\ldots x_2x_1x_0 \pmod{10^k}$$

en we zoeken x_k zodat

$$(x_k\ldots x_2x_1x_0)^2 \equiv x_k\ldots x_2x_1x_0 \pmod{10^{k+1}}$$

We moeten modulo een macht van 10 rekenen omdat de volgende cijfers nog niet bekend zijn. Bedenk dat hoe groter k, hoe kleiner de invloed is van 10^k, dus x wordt steeds nauwkeuriger bepaald.

Als we het i-de cijfer van x^2 aanduiden met a_i, dan volgt uit vgl. (3.6) en de norm-functie dat

$$a_k = \sum_{z=0}^{k} x_z x_{k-z} + d_{k-1} = x_0x_k + \sum_{z=1}^{k-1}(x_z x_{k-z}) + x_kx_0 + d_{k-1} = y_{k-1} + 2x_0x_k \mod 10$$

waarbij $y_{k-1} = \sum_{z=1}^{k-1}(x_z x_{k-z}) + d_{k-1}$. Omdat d_{k-1} met overlenen te berekenen is, en er verder alleen termen met x_i in voorkomen waarbij $0 < i < k$, is y_{k-1} een bekend (geheel) getal. Omdat $x^2 = x$ moeten alle i-de cijfers van x en x^2 overeenkomen, dus

$$\begin{aligned} & x_k = a_k \equiv 2x_0x_k + y_{k-1} \pmod{10} \\ \Rightarrow\ & x_k \equiv 2\cdot 5\cdot x_k + y_{k-1} \pmod{10} \\ \Rightarrow\ & -9x_k \equiv 1y_{k-1} \equiv 81y_{k-1} = 9^2y_{k-1} \pmod{10} \\ \Rightarrow\ & x_k = -9y_{k-1} \mod 10 \end{aligned} \tag{3.16}$$

Hiermee hebben we de gevraagde waarde van x_k gevonden.[17]

Door steeds de waarde van y_{k-1} te bepalen om vervolgens x_k te berekenen met vgl. (3.16), kun je het getal x construeren; voor de eerste vijf decimalen vinden we $x = \ldots 90625$. Met een vermenigvuldiging kun je controleren dat inderdaad $x^2 = x$ op een veelvoud van 10^6 na.

[16] De nulde stap is dus het vaststellen van $x_0 = 5$.

[17] In vgl. (3.16) mogen we $\bmod 10$ schrijven in plaats van $\pmod{10}$, want omdat x_k een cijfer is weten we dat $0 \le x_k < 10$.

Nu berekenen we het getal $y = 1 - x = \ldots 09376$. Als we dit met zichzelf vermenigvuldigen, rijst het vermoeden op dat ook $y^2 = y$. En inderdaad,

$$y^2 = (1-x)^2 = 1^2 - 2x + x^2 = 1 - 2x + x = 1 - x = y.$$

Er geldt:

$$xy = x(1-x) = x - x^2 = x - x = 0$$

dus x en y zijn nuldelers in $\mathbb{Z}_{10}$.

In dit voorbeeld hebben we gebruik gemaakt van speciale eigenschappen van het begincijfer 5 van x, bijvoorbeeld bij de aanloop naar vgl. (3.16). Het is daarom niet meteen duidelijk of we deze methode ook bij andere grondtallen dan 10 kunnen toepassen, en zo ja, hoe. Het lijkt daarom een onbegonnen werk om te zoeken naar een g waarvoor de ring $\mathbb{Z}_g$ geen nuldelers heeft. Toch blijkt dat heel gemakkelijk te zijn als we handig gebruik maken van eigenschappen van priemgetallen.[18]

Stelling 3.5.1. *Voor alle $p \in \mathbb{P}$ bevat $\mathbb{Z}_p$ geen nuldelers.*

Bewijs. Beschouw twee p-adische getallen a en b ongelijk aan 0, waarbij $p \in \mathbb{P}$. We schrijven $a = \ldots a_2 a_1 a_0$ en $b = \ldots b_2 b_1 b_0$. Omdat $a, b \neq 0$ is er een kleinste a_i en een kleinste b_i die niet nul zijn, zeg a_r en b_s.

We berekenen $ab = c$ door achtereenvolgens de mult-functie en de norm-functie toe te passen. Volgens formule (3.6) is het door de mult-functie berekende cijfer c_{r+s} gelijk aan

$$\sum_{z=0}^{r+s} a_z b_{(r+s)-z}$$

Als $z < r$ is $a_z = 0$, deze termen vallen dus weg. Als $z > r$ is $(r+s) - z < s$ zodat $b_{(r+s)-z} = 0$, ook deze termen vallen weg. Het enige wat overblijft is de situatie $z = r$, dus

$$c_{r+s} = a_r b_s \tag{3.17}$$

Op dezelfde manier kun je gemakkelijk inzien dat $c_i = 0$ voor alle $i < r + s$. Bij het berekenen van $a \otimes b = \text{norm}(ab)$ wordt er vóór c_{r+s} dus niet overgeleend. c_{r+s} zelf kan wél groter zijn dan $p-1$, van dit cijfer kan dus een deel worden overgeleend. Kan het zijn dat c_{r+s} daardoor nul wordt? Dat zou betekenen dat c_{r+s} veelvoud van p is.[19] Maar a_r en b_s zijn cijfers tussen 1 en $p-1$, dus $c_{r+s} = a_r b_s$ is niet nul en haar priemfactorontbinding kan nooit p bevatten, tegenspraak! We concluderen dat c_{r+s} niet 0 kan zijn, ook niet nadat de norm-functie is toegepast. Daardoor kan $ab = c$ niet 0 zijn, dus $\mathbb{Z}_p$ heeft geen nuldelers. □

In dit bewijs zie je ook waarom het voor samengestelde grondtallen mis kan gaan.

In hoofdstuk 4 zal blijken dat het van belang is dat $\mathbb{Z}_g$ geen nuldelers heeft, daarom zullen we daar alleen kijken naar $\mathbb{Z}_p$ met p priem.

[18] $\mathbb{P}$ is de verzameling priemgetallen.

[19] Dit volgt uit regel 7 en 8 van algoritme 3.

3.5.2 Wanneer kun je delen in $\mathbb{Z}_g$?

Deze vraag moeten we wat nauwkeuriger formuleren. Stel $a, b \in \mathbb{Z}_g$. Zijn er grondtallen g waarvoor we precies kunnen zeggen voor welke a en b geldt dat $\frac{a}{b} \in \mathbb{Z}_g$?

Allereerst merken we op dat er geen enkele g is waarvoor *elke* $\frac{a}{b}$ weer element is van $\mathbb{Z}_g$; geen enkele ring $\mathbb{Z}_g$ is dus een lichaam.[20] Stel namelijk dat $x = \frac{a}{g}$, dan is $a = gx$ zodat het eerste cijfer a_0 van a gelijk is aan nul.[21] In bijvoorbeeld $\mathbb{Z}_{10}$ is dus voor minstens 90% van alle a deze deling niet mogelijk. In het algemeen doet dit probleem zich voor bij $\frac{a}{b}$ waarbij $\text{ggd}(b, g) > 1$.

In §1.2 hebben we al gezien dat delen in $\mathbb{Z}_{10}$ lang niet altijd mogelijk is, ook als b niet deelbaar is door 10. Op pagina 8 constateerden we dat bijvoorbeeld $x = \frac{a}{b}$ nooit element van $\mathbb{Z}_{10}$ kan zijn als a 'oneven' is en b 'even'.[22] Dit komt doordat als b even is, ook $a = bx$ altijd even is; dit heeft te maken met het feit dat $\text{ggd}(b_0, 10) = 2$. In het algemeen is $\frac{a}{b}$ geen element van $\mathbb{Z}_g$ als $\text{ggd}(b_0, g) = d$ en bovendien d geen deler is van a_0.

Als g priem is, is dat geen enkel probleem. Dan is $\text{ggd}(b_0, g) = 1$ voor alle b met $b_0 \neq 0$, en dat 1 deler is van a_0 vormt zeker geen beperking. We kunnen zelfs de volgende stelling bewijzen.

Stelling 3.5.2. *Stel $p \in \mathbb{P}$ en $a, c \in \mathbb{Z}_p$. Als het eerste cijfer c_0 van c ongelijk is aan 0, dan is $\frac{a}{c} \in \mathbb{Z}_p$.*

Om dit te kunnen bewijzen, hebben we de volgende stelling nodig. Hierbij maken we weer gebruik van modulorekenen.

Stelling 3.5.3. *Stel $c, s \in \mathbb{Z}$ en $g \in \mathbb{N}_{\geq 2}$. De verzameling $\{0, 1, 2, \ldots, g-1\}$ noemen we A_g. We laten de variabele b alle elementen van A_g precies één keer doorlopen. Dan doorloopt ook $bc + s \bmod g$ alle elementen a van A_g precies één keer, dan en slechts dan als $\text{ggd}(c, g) = 1$. Dit komt op hetzelfde neer als*

$$\forall a \in A_g : \exists b \in A_g : (bc + s) \bmod g = a \qquad \Leftrightarrow \qquad \text{ggd}(c, g) = 1$$

Bewijs. We onderscheiden twee gevallen.

Stel dat $\text{ggd}(c, g) = d \neq 1$. Dan zijn bc en g beide deelbaar door d, en daardoor is ook $bc \bmod g$ deelbaar door d. Er is dus geen $b \in A_g$ zodat $bc \bmod g = 1$, want 1 is deelbaar door geen enkel getal groter dan 1. Het element $1 + s \bmod g$ van A_g wordt dus niet bezocht door $bc + s \bmod g$.

[20] In een lichaam bestaat immers voor alle b een element $\frac{1}{b}$, en wegens de inwendigheid van vermenigvuldiging bestaan ook alle $\frac{a}{b}$.

[21] Dit is intuïtief al duidelijk, maar we hebben het ook bewezen, namelijk in stelling 3.4.3. Daar concludeerden we dat $ga = a'$ en per definitie is $a'_0 = 0$.

[22] Met even en oneven bedoelen we, ook in $\mathbb{Z}_g$, dat het meest rechtse cijfer (niet) deelbaar is door 2.

Dan nu het tweede geval, waarin $\text{ggd}(c, g) = 1$. Optelling en vermenigvuldiging volgens het modulorekenen zijn inwendig in A_g, dus alle $bc + s \bmod g$ zijn element van A_g. Omdat b precies g elementen van A_g doorloopt, doet $bc+s \bmod g$ dat ook, waarvan er nog een aantal gelijk kunnen zijn. *Aanname: Stel* dat er twee gelijk zijn, zodat $b_1c + s \equiv b_2c + s \pmod g$ en $b_1 \neq b_2$. Hieruit volgt dat $(b_1 - b_2)c \equiv 0 \pmod g$, dus $(b_1 - b_2)c$ is een veelvoud van g. Omdat c en g geen priemfactoren gemeenschappelijk hebben en $c \neq 0$,[23] moet $(b_1 - b_2)$ een veelvoud zijn van g, en omdat $b_1, b_2 \in A_g$ weten we ook dat $0 \leq b_1, b_2 \leq g - 1$. Hieruit volgt dat $|b_1 - b_2| \leq g - 1$. Dan kan alleen $(b_1 - b_2) = 0$, zodat $b_1 = b_2$, tegenspraak! Dus alle g getallen $bc + s \bmod g$ zijn verschillend. En omdat A_g maar g elementen geeft, moeten alle elementen van A_g worden bezocht door $bc + s \bmod g$.

Met deze twee gevallen hebben we bewezen dat $bc + s \bmod g$ alle elementen van A_g doorloopt, dan en slechts dan als $\text{ggd}(c, g) = 1$. Hiermee is de stelling bewezen. □

Met dit resultaat is het een kleine moeite om stelling 3.5.2 te bewijzen. Dit zullen we nu doen.

Bewijs. Laat p een priemgetal zijn, en $a, c \in \mathbb{Z}_p$. We willen bewijzen dat $\frac{a}{c} \in \mathbb{Z}_p$ als $c_0 \neq 0$.

We berekenen het product a van twee getallen $b, c \in \mathbb{Z}_p$ door er achtereenvolgens de mult- en de norm-functie op los te laten. Het tussenproduct $\text{mult}(b, c)$ duiden we aan met k.

$$a = \text{norm}(k) = \text{norm}\big(\text{mult}(b, c)\big)$$

Omdat $\mathbb{Z}_p \subset \mathbb{Z}_p^*$ geldt ook dat $b, c \in \mathbb{Z}_p^*$. We schrijven b, c en k uit in cijfers, bijvoorbeeld $b = \ldots b_2b_1b_0 = (b_i)$. Uit vgl. (3.6) volgt dat elk cijfer k_i van k te schrijven is als

$$k_i = \sum_{z=0}^{i} b_z c_{i-z}$$

Nu berekenen we $a = \text{norm}(k)$. Als we nog eens naar algoritme 3 kijken, zien we dat in de regels 6 t/m 8 elk berekende cijfer a_i gelijk is aan $k_i + d_{i-1} \bmod 10$. In de regels 7 en 8 wordt namelijk als het ware restdeling van $k_i + d_{i-1}$ door p uitgevoerd; het quotiënt wordt d_i genoemd, de rest wordt de nieuwe a_i. Er geldt dus:

$$a_i = k_i + d_{i-1} = \sum_{z=0}^{i} b_z c_{i-z} + d_{i-1} = \sum_{z=0}^{i-1} (b_z c_{i-z}) + b_i c_0 + d_{i-1} = b_i c_0 + s \mod p$$

Hier is $s = \sum_{z=0}^{i-1} (b_z c_{i-z}) + d_{i-1}$; omdat dit een eindige som in $\mathbb{Z}$ is, is s een geheel getal, net als b_i en c_0. En omdat p priem is en $c_0 \neq 0$, is $\text{ggd}(c_i, p) = 1$. Hierdoor is er volgens stelling 3.5.3 voor *alle* mogelijke $a_i \in A_p$ een geschikte $b_i \in A_p$ te vinden zodat $a_i = b_i c_0 + s \bmod g$. Omdat A_p de verzameling is van alle mogelijke cijfers van

[23] want als $c = 0$ is $\text{ggd}(c, g) = g \neq 1$

elementen van $\mathbb{Z}_p$, is er voor elk mogelijk cijfer a_i een geschikt cijfer b_i te vinden.[24]We concluderen dat voor alle $a, c \in \mathbb{Z}_p$, $c_0 \neq 0$ de vergelijking $bc = a$ oplosbaar naar b is in $\mathbb{Z}_p$. Met andere woorden, voor alle $a, c \in \mathbb{Z}_p$ waarbij c niet eindigt op het cijfer 0, is $b = \frac{a}{c} \in \mathbb{Z}_p$. □

In hoofdstuk 4 zal blijken dat we handig gebruik kunnen maken van deze stelling.

3.6 Algoritme voor deling

Als afsluiting van dit hoofdstuk geven we een algoritme dat kan delen in $\mathbb{Z}_g$. Dit algoritme is gebaseerd op de staartdeling zoals we die in §1.2 hebben uitgevoerd. Laten we de werking van zo'n staartdeling eens nauwkeuriger bekijken. Als voorbeeld nemen we weer de berekening van $\frac{1}{3}$ in $\mathbb{Z}_{10}$ die op pagina 7 staat uitgewerkt. De uitkomst van deze deling duiden we aan met $c = \ldots c_2c_1c_0$, dit is dus gelijk aan $\ldots 667$.

Om c te construeren, zochten we stap voor stap cijfers c_i zó dat het meest rechtse cijfer van $3c_i$ gelijk was aan a_i; hiermee kon a_i worden weggepoetst.[25] Met andere woorden, we zochten c_i zodat $3c_i \equiv a_i \pmod{10}$. Zo vonden we bijvoorbeeld $c_0 = 7$, want $3 \cdot 7 = 21 \equiv 1 \pmod{10}$. Hierna trokken we 21 af van a om een nieuw tussentijds product a te vinden.

In het algemeen gaat het net zo. Als we voor $a, b \in \mathbb{Z}_g$ de getalwaarde van $c = \frac{a}{b} \in \mathbb{Z}_g$ willen bepalen (voor zover c bestaat natuurlijk), moeten we de vergelijking $c_ib_0 \equiv a_i \pmod{g}$ oplossen naar c_i. Merk op dat hier alleen het meest rechtse cijfer van b een rol speelt.

We lossen deze vergelijking op met behulp van het zogenaamde 'uitgebreide algoritme van Euclides'. Dat is een algoritme dat voor ieder paar *gehele* getallen a, b de vergelijking $ax + by = \text{ggd}(a, b)$ oplost naar x, y. Hoe en vooral waarom het algoritme werkt kunnen we hier niet in detail uitleggen; hiervoor verwijzen we naar §3.4 van [1] of hoofdstuk 1 van [5]. Het uitgebreide algoritme van Euclides hebben we (in computertaal) opgenomen als algoritme 4.

Algorithm 4 Uitgebreid algoritme van Euclides

```
function eucl(a, b ∈ ℤ) : (x, y) ∈ ℤ
begin
if a mod b = 0 then
    result := (0, 1)
else
    (x, y) := eucl(b, a mod b)
result := (y, x − y · (a div b))
end
```

[24]Bedenk dat alle cijfers van getallen in $\mathbb{Z}_p$ tussen 0 en $p - 1$ liggen.

[25]$a = \ldots a_2a_1a_0$ is hier het 'tussentijdse product' dat in het begin $\ldots 0001$ was, vervolgens $\ldots 9998$, et cetera.

Met dit algoritme kun je voor elke $b_0, g \in \mathbb{Z}$ de vergelijking $b_0x+gy = \text{ggd}(b_0, g)$ oplossen. Als bovendien $\text{ggd}(b_0, g) = 1$, dan is $b_0x + gy = 1$ waaruit volgt dat $b_0x \equiv 1 \pmod{g}$. Volgens een regel van het modulorekenen geldt dan dat $b_0xa_i \equiv a_i \pmod{g}$. Hiermee hebben we een mogelijkheid gevonden voor het gezochte cijfer c_i dat moest voldoen aan $c_ib_0 \equiv a_i \pmod{g}$, namelijk $c_i = xa_i \bmod g$.

Het mooie van dit algoritme is dat het je precies vertelt *hoe* je c_i kunt construeren als $\text{ggd}(b_0, g) = 1$. In de praktijk is het voor kleine g natuurlijk handiger om gewoon de tafel van b_0 op te schrijven met grondtal g, en de c_i te kiezen waarvoor het laatste cijfer van c_ib_0 gelijk is aan a_i. Voor grote waarden van g is het algoritme van Euclides echter véél sneller.

Aan de hand van het uitgebreide algoritme van Euclides creëren we de functie divide(a, b), zie algoritme 5.

Algorithm 5 Divide

```
 1: function divide(a, b ∈ Z_g) ∈ Z_g
 2: c := (0, 0, 0, ···)
 3: begin
 4: (x, y) := eucl(b_0, g)
 5: for i = 0 to ∞ do
 6:     begin
 7:     c_i := x a_i mod g
 8:     a := norm(a − cb)
 9:     end
10: end
11: Result := c
```

Dit algoritme voert als het ware een staartdeling uit. In regel 7 wordt c_i berekend met behulp van 4, waarna in regel 8 de waarde van het nieuwe tussenproduct a wordt bepaald.

Dit werkt alleen als $\text{ggd}(b_0, g) = 1$, anders geeft $\text{eucl}(b_0, g)$ de verkeerde uitkomst. Het gaat dus in ieder geval goed als g priem is en b_0 ongelijk aan nul. Dit is in overeenstemmingen met wat we eerder gezien hebben in §3.5.2.

Hoofdstuk 4

Formele invoering van het lichaam $\mathbb{Q}_p$

In §1.2 hebben we laten zien dat het bij deling handig is om g-adische kommagetallen toe te staan, getallen van de vorm $\ldots a_2a_1a_0.a_{-1}a_{-2}\ldots a_{-n}$. We zeiden toen dat we de verzameling van al deze kommagetallen $\mathbb{Q}_g$ noemen, en dat deze verzameling eigenlijk alleen 'zin' heeft als g een priemgetal is. Waarom dat zo is, zal in dit hoofdstuk duidelijk worden. We veronderstellen vanaf nu dat p priem is. We definiëren $\mathbb{Q}_p$ heel anders dan je zou verwachten, namelijk niet als kommagetallen maar als breuken met in de teller en noemer elementen van $\mathbb{Z}_p$. Later zal blijken dat deze twee 'definities' overeenkomen, dus al die breuken zijn als kommagetallen te schrijven.

Behalve dat $\mathbb{Q}_p$ in sommige gevallen voordeel heeft bij het uitvoeren van delingen, heeft het een nog veel belangrijker voordeel ten opzichte van $\mathbb{Z}_p$. We kunnen namelijk bewijzen dat $(\mathbb{Q}_p, +, \times)$ een *lichaam* is. In lichamen gaat alles erg mooi, omdat je altijd kunt delen. Daardoor kunnen veel stellingen voor lichamen worden bewezen die voor ringen niet altijd opgaan.[1] Daar gaan we hier verder niet op in; we verwijzen naar hoofdstuk 4 van [5] voor een aantal eenvoudige stellingen over ringen en lichamen.

Met de methode die we gebruiken, kun je elke willekeurige commutatieve ring met 1 zonder nuldelers (laten we deze ring Ξ noemen) uitbreiden naar een lichaam $\mathbb{L}$. Dat is handig, want zo hebben we ook gelijk een formele invoering van $\mathbb{Q}$ vanuit $\mathbb{Z}$. In dit hoofdstuk zullen we vooral in ons achterhoofd houden dat Ξ staat voor $\mathbb{Z}_p$ en $\mathbb{L}$ voor $\mathbb{Q}_p$.

4.1 Definitie van $\mathbb{L}$

We definiëren nu de algebraïsche structuur $(\mathbb{L}, +, \times)$, lees $(\mathbb{Q}_p, +, \times)$

Definitie 4.1.1.

$$\mathbb{L} = \left\{ \frac{a}{b} \mid a, b \in \Xi,\ b \neq 0 \right\}$$

[1] Dit betekent niet dat lichamen per se rijkere structuren zijn dan ringen. In ringen kan delen soms wel en soms niet. Dat levert, voor een geschikte klasse van ringen, de mogelijkheid om iets in de trant van priemgetallen te definiëren en te bestuderen.

Twee 'breuken' $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{L}$ *worden als gelijk beschouwd volgens de regel:*

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = a_2 b_1 \tag{4.1}$$

Op alle elementen $\frac{a}{b} \in \mathbb{L}$ *definiëren we de operaties optelling en vermenigvuldiging als volgt.*

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} := \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \tag{4.2}$$

$$\frac{a_1}{b_1} \times \frac{a_2}{b_2} := \frac{a_1 a_2}{b_1 b_2} \tag{4.3}$$

Voordat we van deze definitie uit mogen gaan, willen we eerst aantonen dat ze wel zinvol is. In dit geval komt het erop neer dat we twee stellingen moeten bewijzen.

1. De optelling en vermenigvuldiging zijn inwendig in $\mathbb{L}$.

   Bewijs. Wegens de inwendigheid van $+$ en $\times$ in Ξ geldt dat $a_1 b_2 + a_2 b_1 \in \Xi$, dat $a_1 a_2 \in \Xi$ en dat $b_1 b_2 \in \Xi$. Bovendien heeft Ξ geen nuldelers, dus $b_1 b_2 \neq 0$. Hierdoor zijn $\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$ en $\frac{a_1 a_2}{b_1 b_2}$ elementen van $\mathbb{L}$, dus $+$ en $\times$ zijn inwendig in $\mathbb{L}$. □

2. De definitie van de som en het product zijn ondubbelzinnig. Dit houdt in dat als $\frac{a_1}{b_1}$ en $\frac{a_2}{b_2}$ vervangen worden door andere elementen van Ξ die hieraan volgens (4.1) gelijk zijn, de uitkomsten van de som en het product niet veranderen. Eerst bewijzen we dit voor de optelling.

   Bewijs. Stel dat voor de volgende vier elementen van $\mathbb{L}$ geldt:

   $$\frac{a_1}{b_1} = \frac{c_1}{d_1} \qquad \text{en} \qquad \frac{a_2}{b_2} = \frac{c_2}{d_2} \tag{4.4}$$

   We willen dus het volgende aantonen:

   $$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{c_1}{d_1} + \frac{c_2}{d_2} \tag{4.5}$$

   Dit is volgens (4.2) gelijkwaardig met:

   $$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{c_1 d_2 + c_2 d_1}{d_1 d_2} \tag{4.6}$$

   Volgens (4.1) is dit bewezen als we hebben aangetoond dat

   $$(a_1 b_2 + a_2 b_1)(d_1 d_2) = (c_1 d_2 + c_2 d_1)(b_1 b_2) \tag{4.7}$$

   Uit (4.4) volgt bovendien met behulp van (4.1) dat

   $$a_1 d_1 = c_1 b_1 \qquad \text{en} \qquad a_2 d_2 = c_2 b_2 \tag{4.8}$$

Nu hebben we genoeg gegevens verzameld om te bewijzen dat vgl. (4.5) waar is.[2]

$$(a_1b_2 + a_2b_1)(d_1d_2) \overset{6)}{=} (a_1b_2)(d_1d_2) + (a_2b_1)(d_1d_2) \overset{5)\times}{=} (d_1d_2)(a_1b_2) + (a_2b_1)(d_1d_2)$$
$$\overset{5)\times}{=} (d_1d_2)(b_2a_1) + (a_2b_1)(d_1d_2) \overset{2.4.1}{=} (d_1a_1)(b_2d_2) + (a_2d_2)(d_1b_1)$$
$$\overset{5)\times}{=} (a_1d_1)(b_2d_2) + (a_2d_2)(d_1b_1) \overset{(4.8)}{=} (c_1b_1)(b_2d_2) + (c_2b_2)(d_1b_1)$$
$$\overset{5)\times}{=} (b_1c_1)(d_2b_2) + (b_2c_2)(d_1b_1) \overset{2.4.1}{=} (b_1b_2)(d_2c_1) + (b_2b_1)(d_1c_2)$$
$$\overset{5)\times}{=} (b_1b_2)(c_1d_2) + (b_1b_2)(c_2d_1) \overset{6)}{=} (b_1b_2)(c_1d_2 + c_2d_1) \overset{5)\times}{=} (c_1d_2 + c_2d_1)(b_1b_2)$$

Hiermee hebben we de geldigheid van (4.7) aangetoond, en daarmee ook die van (4.6) en (4.5). Dat laatste is precies wat we wilden bewijzen. □

Nu bewijzen we de stelling voor vermenigvuldiging.

Bewijs. We gaan weer uit van de situatie in vgl. (4.4); daardoor geldt automatisch ook vgl. (4.8). We willen nu het volgende aantonen:

$$\frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{c_1}{d_1} \times \frac{c_2}{d_2} \tag{4.9}$$

Dit komt volgens (4.3) op hetzelfde neer als:

$$\frac{a_1a_2}{b_1b_2} = \frac{c_1c_2}{d_1d_2} \tag{4.10}$$

Volgens (4.1) is dit bewezen als we hebben aangetoond dat

$$(a_1a_2)(d_1d_2) = (c_1c_2)(b_1b_2) \tag{4.11}$$

Nu hebben we genoeg gereedschap om de stelling te bewijzen.

$$(a_1a_2)(d_1d_2) \overset{5)\times}{=} (a_1a_2)(d_2d_1) \overset{2.4.1}{=} (a_1d_1)(d_2a_2) \overset{5)\times}{=} (a_1d_1)(a_2d_2)$$
$$\overset{(4.8)}{=} (c_1b_1)(c_2b_2) \overset{5)\times}{=} (c_1b_1)(b_2c_2) \overset{2.4.1}{=} (c_1c_2)(b_2b_1) \overset{5)\times}{=} (c_1c_2)(b_1b_2)$$

Hiermee hebben we de geldigheid van (4.11) aangetoond, en daarmee ook die van (4.10) en (4.9). En laat dat laatste nou juist ons doel zijn. □

Samenvattend komt het er op neer dat we nu de algebraïsche structuur $(\mathbb{L}, +, \times)$ formeel hebben gedefinieerd, en bovendien bewezen dat de definities van $+$ en $\times$ zinvol zijn.

[2]Nummers met één haakje rechts verwijzen naar een eigenschap uit Tabel 2.2 *die geldt voor* Ξ. Bijvoorbeeld 5)$\times$ boven een $=$-teken betekent dat eigenschap 5), de commutativiteit, geldt voor de vermenigvuldiging. Nummers met twee haakjes verwijzen naar een vergelijking, nummers zonder haakjes naar een stelling.

4.2 Lemma's

Om te bewijzen dat $\mathbb{L}$ een lichaam is, hebben we twee lemma's (hulpstellingen) nodig.

Lemma 4.2.1.

$$\forall a, b, c \in \Xi, \;\; b, c \neq 0 : \qquad \frac{ca}{cb} = \frac{a}{b}$$

Bewijs. Uit de associativiteit en commutativiteit van vermenigvuldiging in Ξ volgt dat

$$(ca)b = (ac)b = a(cb),$$

dus $(ca)b = a(cb)$. Hieruit volgt met (4.1) dat $\frac{ca}{cb} = \frac{a}{b}$. □

Overigens geldt het lemma niet andersom. Niet voor elk paar gelijkwaardige breuken $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{L}$ is er een $c \in \Xi$ te vinden zodat

$$ca_1 = a_2 \qquad \text{en} \qquad cb_1 = b_2$$

Als we bijvoorbeeld naar $\Xi = \mathbb{Z}$ en $\mathbb{L} = \mathbb{Q}$ kijken, zien we dat $\frac{3}{9} = \frac{4}{12}$. Natuurlijk is

$$\frac{\frac{4}{3} \times 3}{\frac{4}{3} \times 9} = \frac{4}{12},$$

maar $\frac{4}{3}$ is geen element van $\mathbb{Z}$.

Lemma 4.2.2.

$$\forall a_1, a_2, b \in \Xi : \qquad \frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 + a_2}{b}$$

Bewijs. Uit (4.2), Lemma 4.2.1 en de distributiviteit in Ξ volgt:

$$\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 b + a_2 b}{b^2} = \frac{(a_1 + a_2)b}{b^2} = \frac{a_1 + a_2}{b}$$

□

4.3 Bewijs: $\mathbb{L}$ is een lichaam

We gaan nu bewijzen dat $(\mathbb{L}, +, \times)$ een lichaam is. Hierbij maken we onder meer gebruik van de formules (4.1) t/m (4.3), van de twee lemma's en van het feit dat $(\Xi, +, \times)$ een commutatieve ring met 1 zonder nuldelers is.

4.3.1 Bewijzen van de eigenschappen van optelling

Als je niet meer weet wat de eigenschappen die we hier bewijzen inhouden, kun je altijd terugblikken naar Tabel 2.2.

We laten vanaf nu de verwijzingen boven de =-tekens weg, het is aan jou om te achterhalen welke eigenschappen worden toegepast. Bijna overal wordt de inwendigheid van $+$ en $\times$ in Ξ en $\mathbb{L}$, gebruikt, net als het niet bestaan van nuldelers in Ξ.

Inwendigheid. Dit hebben we al bewezen in §4.1.

Commutativiteit.

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2} = \frac{a_2b_1 + a_1b_2}{b_2b_1} = \frac{a_2}{b_2} + \frac{a_1}{b_1}$$

Associativiteit.

$$\begin{aligned}
&(\frac{a_1}{b_1} + \frac{a_2}{b_2}) + \frac{a_3}{b_3} = \frac{a_1b_2 + a_2b_1}{b_1b_2} + \frac{a_3}{b_3} \\
&= \frac{(a_1b_2 + a_2b_1)b_3 + a_3(b_1b_2)}{(b_1b_2)b_3} = \frac{(a_1b_2)b_3 + (a_2b_1)b_3 + a_3(b_1b_2)}{(b_1b_2)b_3} \\
&= \frac{a_1(b_2b_3) + (a_2b_1)b_3 + (a_3b_1)b_2}{(b_1b_2)b_3} = \frac{a_1(b_2b_3) + b_3(a_2b_1) + b_2(a_3b_1)}{(b_1b_2)b_3} \\
&= \frac{a_1(b_2b_3) + (b_3a_2)b_1 + (b_2a_3)b_1}{b_1(b_2b_3)} = \frac{a_1(b_2b_3) + (b_3a_2 + b_2a_3)b_1}{b_1(b_2b_3)} \\
&= \frac{a_1}{b_1} + \frac{b_3a_2 + b_2a_3}{b_2b_3} = \frac{a_1}{b_1} + \frac{a_2b_3 + a_3b_2}{b_2b_3} = \frac{a_1}{b_1} + (\frac{a_2}{b_2} + \frac{a_3}{b_3})
\end{aligned}$$

Nulelement van $\mathbb{L}$. We duiden het nulelement van Ξ aan met 0, en het eenheidselement met 1. Hieruit leiden we af:[3]

$$\frac{a}{b} = \frac{a+0}{b\times 1} = \frac{a\times 1 + 0\times b}{b\times 1} = \frac{a}{b} + \frac{0}{1}$$

Wegens de commutativiteit van $+$ in $\mathbb{L}$ geldt ook dat $\frac{0}{1} + \frac{a}{b} = \frac{a}{b}$. Hiermee is bewezen dat $\frac{0}{1}$ het nulelement is van $\mathbb{L}$.

Tegengestelde. Voor alle $a \in \Xi$ is er ook een $-a \in \Xi$ zodat $a + -a = 0$. Nu leiden we af:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a + -a}{b} = \frac{0}{b} = \frac{0\times b}{b} = \frac{0\times b}{1\times b} = \frac{0}{1}$$

Wegens de commutativiteit van $+$ in $\mathbb{L}$ geldt ook dat $\frac{-a}{b} + \frac{a}{b} = \frac{0}{1}$. En omdat $\frac{0}{1}$ het nulelement is van $\mathbb{L}$, is hiermee aangetoond dat elk element $\frac{a}{b} \in \mathbb{L}$ een tegengestelde $\frac{-a}{b} \in \mathbb{L}$ heeft.

[3] Bij het bewijs van deze en de volgende stelling wordt stelling 2.4.3 gebruikt.

4.3.2 Bewijzen van de eigenschappen van vermenigvuldiging

Inwendigheid. Dit is al bewezen in §4.1.

Commutativiteit.

$$\frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} = \frac{a_2 a_1}{b_2 b_1} = \frac{a_2}{b_2} \times \frac{a_1}{b_1}$$

Associativiteit.

$$(\frac{a_1}{b_1} \times \frac{a_2}{b_2}) \times \frac{a_3}{b_3} = \frac{a_1 a_2}{b_1 b_2} \times \frac{a_3}{b_3} = \frac{(a_1 a_2) a_3}{(b_1 b_2) b_3} = \frac{a_1 (a_2 a_3)}{b_1 (b_2 b_3)} = \frac{a_1}{b_1} \times \frac{a_2 a_3}{b_2 b_3} = \frac{a_1}{b_1} \times (\frac{a_2}{b_2} \times \frac{a_3}{b_3})$$

Eenheidselement van $\mathbb{L}$. We duiden het eenheidselement van Ξ weer aan met 1.

$$\frac{a}{b} = \frac{a \times 1}{b \times 1} = \frac{a}{b} \times \frac{1}{1}$$

Wegens de commutativiteit van $\times$ in $\mathbb{L}$ geldt ook dat $\frac{1}{1} \times \frac{a}{b} = \frac{a}{b}$. We concluderen dat $\frac{1}{1}$ het eenheidselement van $\mathbb{L}$ is.

Inverse. We willen bewijzen dat elke $\frac{a}{b} \in \mathbb{L}$ ongelijk aan het nulelement $\frac{0}{1}$ van $\mathbb{L}$, een inverse heeft in $\mathbb{L}$. Uit Lemma 4.2.1 volgt dat

$$\frac{0}{1} = \frac{0 \times b}{1 \times b} = \frac{0}{b}$$

voor alle $b \in \Xi$. We zijn dus klaar als we hebben bewezen dat er voor elke $\frac{a}{b} \in \mathbb{L}$ met $a \neq 0$ een inverse is. Dat is niet moeilijk. Omdat $a \neq 0$ is namelijk $\frac{b}{a} \in \mathbb{L}$.

$$\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ba} = \frac{1 \times (ab)}{1 \times (ab)} = \frac{1}{1}$$

Omdat vermenigvuldiging commutatief is in $\mathbb{L}$, is ook $\frac{b}{a} \times \frac{a}{b} = \frac{1}{1}$, het eenheidselement van $\mathbb{L}$. Hiermee is bewezen dat elk element $\frac{a}{b} \in \mathbb{L}$ ongelijk aan $\frac{0}{1}$ een inverse $\frac{b}{a}$ heeft.

4.3.3 Bewijs van de distributiviteit

Distributiviteit. We bewijzen eerst de links-distributiviteit:

$$\begin{aligned}
&\frac{a_1}{b_1} \times (\frac{a_2}{b_2} + \frac{a_3}{b_3}) = \frac{a_1}{b_1} \times \frac{a_2 b_3 + a_3 b_2}{b_2 b_2} = \frac{a_1 (a_2 b_3 + a_3 b_2)}{b_1 (b_2 b_3)} \\
&= \frac{a_1 (a_2 b_3) + a_1 (a_3 b_2)}{b_1 (b_2 b_3)} = \frac{(a_1 a_2) b_3 + (a_1 a_3) b_2}{(b_1 b_2) b_3} = \frac{(a_1 a_2) b_3}{(b_1 b_2) b_3} + \frac{(a_1 a_3) b_2}{(b_1 b_2) b_3} \\
&= \frac{(a_1 a_2) b_3}{(b_1 b_2) b_3} + \frac{(a_1 a_3) b_2}{b_3 (b_1 b_2)} = \frac{(a_1 a_2) b_3}{(b_1 b_2) b_3} + \frac{(a_1 a_3) b_2}{(b_3 b_1) b_2} = \frac{a_1 a_2}{b_1 b_2} + \frac{a_1 a_3}{b_3 b_1} \\
&= \frac{a_1 a_2}{b_1 b_2} + \frac{a_1 a_3}{b_1 b_3} = \frac{a_1}{b_1} \times \frac{a_2}{b_2} + \frac{a_1}{b_1} \times \frac{a_3}{b_3}
\end{aligned}$$

Omdat $\times$ commutatief is in $\mathbb{L}$, mogen we stelling 2.4.2 toepassen. De rechts-distributiviteit geldt daarom ook.

Met dit alles hebben we bewezen dat $\mathbb{L}$ een lichaam is. In het bijzonder zijn dus $\mathbb{Q}$ en $\mathbb{Q}_p$ lichamen. Dit zetten we tot slot nog even overzichtelijk in een tabel.

	Commutatieve ring met 1 zonder nuldelers	Daaruit geconstrueerd lichaam
Algemeen	Ξ	$\mathbb{L}$
Voorbeelden	$\mathbb{Z}$	$\mathbb{Q}$
	$\mathbb{Z}_p$	$\mathbb{Q}_p$

4.4 Koppeling tussen Ξ en 𝕃

We weten intuïtief dat Ξ een deelverzameling is van $\mathbb{L}$. Immers, voor alle $a \in \Xi$ is $a/1 \in \mathbb{L}$, en voor ons gevoel is $a = a/1$. Hoe logisch dat ook lijkt, het is niet echt te bewijzen. Dat komt doordat we de operaties in $\mathbb{L}$ heel anders gedefinieerd hebben dan in Ξ, en je kunt in de wiskunde geen appels met peren vergelijken.

Wel kunnen we laten zien dat ons idee om a en $a/1$ als gelijk te beschouwen, 'zinvol' is. Hiervoor creëren we een 'afbeeldingsfunctie' f, die elk element $a \in \Xi$ aan het element $a/1 \in \mathbb{L}$ koppelt.

Definitie 4.4.1.

$$\forall a \in \Xi : \qquad f(a) := \frac{a}{1}$$

Het nagaan dat het zin heeft om a aan $a/1$ (ofwel $f(a)$) te koppelen, komt in dit geval hierop neer. We bewijzen drie dingen, namelijk dat $f(a)+f(b) = f(a+b)$, dat $f(a)f(b) = f(ab)$, en dat uit $a \neq b$ volgt dat $f(a) \neq f(b)$. Dat zijn drie vereisten die natuurlijk in elk geval zouden moeten gelden als $f(a)$ op te vatten is als a. Als hieraan voldaan wordt, zegt men ook wel dat f de bewerkingen $+$ en $\times$ in Ξ en $\mathbb{L}$ 'respecteert'.

Stelling 4.4.2. *De som van de afbeeldingen is gelijk aan de afbeelding van de som.*

$$\forall a, b \in \Xi : \qquad f(a) + f(b) = f(a + b)$$

Bewijs.

$$f(a) + f(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \times 1 + b \times 1}{1 \times 1} = \frac{a+b}{1} = f(a+b)$$

□

Stelling 4.4.3. *Het product van de afbeeldingen is gelijk aan de afbeelding van het product.*

$$\forall a, b \in \Xi : \qquad f(a) \times f(b) = f(ab)$$

Bewijs.

$$f(a) \times f(b) = \frac{a}{1} \times \frac{b}{1} = \frac{a \times b}{1 \times 1} = \frac{ab}{1} = f(ab)$$

□

Stelling 4.4.4. *Verschillende elementen hebben verschillende afbeeldingen.*

$$\forall a, b \in \Xi : \qquad a \neq b \Rightarrow f(a) \neq f(b)$$

Bewijs. Laat a ongelijk zijn aan b. *Aanname: Stel* dat $f(a) = f(b)$. Hieruit volgt:

$$f(a) = f(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a \times 1 = b \times 1 \Rightarrow a = b$$

Maar we hadden gesteld dat $a \neq b$, tegenspraak! We concluderen dat de aanname onjuist is, dus de stelling is juist. □

We hebben nu aangetoond dat f de bewerkingen van Ξ en $\mathbb{L}$ respecteert. Nu heeft het zin om de verzameling Ξ als deelverzameling van $\mathbb{L}$ op te vatten, waarbij a en $a/1$ als gelijk worden beschouwd. Gelukkig maar dat we konden bewijzen dat dat 'zin' heeft, anders was er iets vreemds aan de hand!

4.5 Komen verschillende definities van $\mathbb{Q}_p$ overeen?

We hebben tot nu toe twee ideeën van $\mathbb{Q}_p$ door elkaar heen gebruikt. In de informele beschouwing van hoofdstuk 1 kwam ons beeld van $\mathbb{Q}_p$ hierop neer:

$$\forall p \in \mathbb{P} : \quad \mathbb{Q}_p = \{\ldots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \ldots a_{-n} \mid a_i \in \mathbb{N},\ 0 \leq a_i < p\} \tag{4.12}$$

In de formele definitie van $\mathbb{Q}_p$ in §4.1 hebben we juist gesteld dat

$$\forall p \in \mathbb{P} : \quad \mathbb{Q}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}_p,\ b \neq 0 \right\} \tag{4.13}$$

In deze paragraaf bewijzen we dat beide definities van $\mathbb{Q}_p$ op hetzelfde neerkomen. Bovendien bewijzen we dat er nog een derde definitie mogelijk is die ook op hetzelfde neerkomt.

4.5.1 Plan van aanpak

We gaan uit van de *formele* definitie van $\mathbb{Q}_p$, dus van (4.13) en niet van (4.12).

We definiëren de deelverzameling V_p van $\mathbb{Q}_p$ als de verzameling van breuken die geschreven worden als $\frac{a}{p^n}$ met $a \in \mathbb{Z}_p$ en $n \in \mathbb{N}$. Dit is duidelijk een deelverzameling van $\mathbb{Q}_p$, want omdat $\mathbb{Z} \subset \mathbb{Z}_p$ is ook $p^n \in \mathbb{Z}_p$; bovendien is p^n nooit nul.

$$V_p := \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z}_p, n \in \mathbb{N} \right\} \tag{4.14}$$

Op een soortgelijke manier definiëren we de deelverzameling W_p van $\mathbb{Q}_p$ als de verzameling van breuken die geschreven worden als $\frac{a}{d}$ met $a \in \mathbb{Z}_p$ en $d \in \mathbb{Z}_{\geq 1}$.

$$W_p := \left\{ \frac{a}{d} \mid a \in \mathbb{Z}_p;\ d \in \mathbb{Z}_{\geq 1} \right\} \tag{4.15}$$

Omdat $p^n \in \mathbb{Z}_{\geq 1}$ is bovendien V_p een deelverzameling van W_p, zodat

$$V_p \subset W_p \subset \mathbb{Q}_p \tag{4.16}$$

Hierdoor gelden ook voor elementen uit V_p en W_p de vergelijkingen (4.1), (4.2) en (4.3). We willen de volgende stelling bewijzen.

Stelling 4.5.1.

$$V_p = W_p = \mathbb{Q}_p$$

Je vraagt je misschien af wat dit te maken heeft met wat bovenaan §4.5 staat, namelijk dat we bewijzen dat de verzamelingen bij (4.12) en (4.13) overeenkomen. Toch komt het bewijzen van stelling 4.5.1 op hetzelfde neer, zoals later zal blijken. V_p komt namelijk overeen met de verzameling bij (4.12).[4] De verzameling W_p is de derde mogelijke definitie van $\mathbb{Q}_p$.

We bewijzen de stelling door aan te tonen dat $\mathbb{Q}_p \subset V_p$. Omdat $V_p \subset \mathbb{Q}_p$ volgt daaruit[5] dat $V_p = \mathbb{Q}_p$. Uit (4.16) volgt dan natuurlijk ook dat $V_p = W_p = \mathbb{Q}_p$, waarmee de stelling bewezen is.

Om de stelling te bewijzen hebben we een lemma nodig.

4.5.2 Lemma: goochelen met nullen

Lemma 4.5.2 is een uitbreiding van stelling 3.4.4 (zie pagina 31). Voor elk p-adisch getal a, is pa volgens stelling 3.4.4 gelijk aan a met een nul erachter geplakt.

$$p \times \ldots a_2 a_1 a_0 = \ldots a_2 a_1 a_0 0$$

[4] Behalve dat we nu nog niet mogen beweren dat verzameling (4.12) gelijk is aan $\mathbb{Q}_p$, want dat willen we juist bewijzen.

[5] zie pagina 13

Vermenigvuldigen met p^n kan worden opgevat als het n keer herhaald vermenigvuldigen met p. Dus $p^n a$ is gelijk aan a met n nullen erachter geplakt.

Een eigenschap van *deling* in $\mathbb{Q}_p$ is dat het vermenigvuldiging ongedaan maakt. Immers,

$$\frac{a \times b}{b} = \frac{(a \times 1) \times b}{1 \times b} = \frac{a \times 1}{1} = \frac{a}{1} = a \tag{4.17}$$

Daarom moet deling door p^n in $\mathbb{Z}_p$ op hetzelfde neerkomen als een verschuiving van alle cijfers n plaatsen naar *rechts*, waarbij een rij van n nullen waar a op eindigt, wordt verwijderd. Deze nullen moeten er natuurlijk wel zijn, anders is het resultaat geen element van $\mathbb{Z}_p$. We mogen eventuele andere cijfers dan nullen niet "achter de komma" plaatsen en zeggen dat dit een element van $\mathbb{Q}_p$ is, want we hebben de elementen van $\mathbb{Q}_p$ niet gedefinieerd als rijtjes van cijfers. Dus als a eindigt op z nullen (waarbij z ook 0 kan zijn), moet gelden dat $n \leq z$ willen we kunnen delen door p^n binnen $\mathbb{Z}_p$.

Lemma 4.5.2. *Voor alle $a = \ldots a_2 a_1 a_0 \in \mathbb{Z}_p$ en $n \in \mathbb{N}$ komt* vermenigvuldiging *met p^n op hetzelfde neer als n nullen achter a plakken.*

$$p^n \times \ldots a_2 a_1 a_0 = \ldots a_2 a_1 a_0 \overbrace{000\ldots0}^{n \text{ nullen}}$$

Als $a_i = 0$ voor alle $i \leq z$, en bovendien $z \geq n$, dan komt deling *door p^n op hetzelfde neer als een rij van n nullen achter a schrappen.*

$$\frac{\ldots a_2 a_1 a_0}{p^n} = \ldots a_{n+2} a_{n+1} a_n$$

4.5.3 Bewijs: $V_p = W_p = \mathbb{Q}_p$

Allereerste een verkorte notatie. De verzameling $\{x \mid x \in \mathbb{N},\ x \leq p-1\}$, dat zijn alle mogelijke *cijfers* van getallen in $\mathbb{Z}_p$, noemen we weer A_p.

We beschouwen een element $c = \frac{a}{b} \in \mathbb{Q}_p$. De p-adische gehele getallen a, b en c schrijven we als $\ldots a_3 a_2 a_1 a_0$, $\ldots b_3 b_2 b_1 b_0$ resp. $\ldots c_3 c_2 c_1 c_0$ waarbij $a_i, b_i, c_i \in A_p$. De kleinste i waarvoor $b_i \neq 0$ noemen we z. Het is makkelijk na te gaan dat z het aantal nullen is waar b op eindigt.

We onderscheiden 2 gevallen.

i. $z = 0$, dus $b_0 \neq 0$. Omdat bovendien p priem is, volgt uit stelling 3.5.2 dat $\frac{a}{b} \in \mathbb{Z}_p$. Omdat[6] $\mathbb{Z}_p \subset V_p$ is ook $\frac{a}{b} \in V_p$.

ii. $z \neq 0$, dus $b_0 = 0$. Stelling 3.5.2 mogen we nu niet toepassen, want die geldt alleen als $b_0 \neq 0$. Wat we wel kunnen doen, is b delen door p^z. Dit komt op hetzelfde neer als bij b direct links van de komma z nullen verwijderen, zie Lemma 4.5.2. En

[6] Immers, als $n = 0$ is $\frac{a}{p^n} = \frac{a}{1} = a$, een vrij te kiezen element uit $\mathbb{Z}_p$.

omdat b op precies z nullen eindigt, is het eerste cijfer van b/p^z ongelijk aan nul. Nu mogen we stelling 3.5.2 wél gebruiken, dus

$$\frac{a}{b/p^z} =: y \in \mathbb{Z}_p \tag{4.18}$$

Omdat $V_p \subset \mathbb{Q}_p$ mogen we de rekenregels voor $\mathbb{Q}_p$ natuurlijk ook toepassen op V_p. Daarvan zullen we nu gebruik maken. De derde gelijkheid volgt uit vgl. (4.17).

$$y = \frac{a}{b/p^z} = \frac{a \times p^z}{(b/p^z) \times p^z} = \frac{a \times p^z}{b} = \frac{a \times p^z}{b \times 1} = \frac{a}{b} \times \frac{p^z}{1} = \frac{a}{b} \times p^z$$

Hieruit volgt:

$$\frac{y}{p^z} = \frac{a}{b}$$

Volgens vgl. (4.18) is $y \in \mathbb{Z}_p$, dus $y/p^z \in V_p$.[7] Hieruit blijkt dat $\frac{a}{b} \in V_p$.

In beide gevallen i en ii, dus voor alle $\frac{a}{b} \in \mathbb{Q}_p$,[8] is $\frac{a}{b} \in V_p$. We concluderen dat $\mathbb{Q}_p \subset V_p$. Uit vgl. (4.16) volgt dat

$$V_p = W_p = \mathbb{Q}_p \tag{4.19}$$

Hiermee is stelling 4.5.1 bewezen.

4.5.4 $\mathbb{Q}_p$ beschouwd als rijtjes van cijfers

Met dit resultaat kunnen we $\mathbb{Q}_p$ voortaan beschouwen als V_p, zodat elk element van $\mathbb{Q}_p$ kan worden opgevat als een p-adisch geheel getal gedeeld door een macht van het grondtal p. In $\mathbb{Z}_p$ hebben we gezien dat a/p^n overeenkomt met een verschuiving van alle cijfers n plaatsen naar rechts, mits a eindigt op minstens n nullen. We kunnen dit idee uitbreiden naar $\mathbb{Q}_p$. Hiervoor voeren we in $\mathbb{Z}_p$ een decimale punt in rechts van elk getal, zo kunnen we bijvoorbeeld $a = \ldots k_3k_2k_1k_0.$ schrijven. Deling door p^n kunnen we weer opvatten als een verschuiving van alle cijfers n plaatsen naar rechts, waarbij cijfers ook rechts van de komma mogen staan. Zodoende kunnen we elk element $a/p^n \in \mathbb{Q}_p$ opvatten als een rij cijfers $\ldots k_{n+3}k_{n+2}k_{n+1}k_n.k_{n-1}k_{n-2}\ldots k_0$. Voor $m \in \mathbb{N}$, $m \leq n$ komt vermenigvuldiging met p^m overeen met een verschuiving van alle cijfers m plaatsen naar links, want

$$\ldots k_{n+1}k_n.k_{n-1}\ldots k_0 \times p^m = \frac{a}{p^n} \times \frac{p^m}{1} = \frac{a \times p^m}{p^n \times 1} = \frac{a \times p^m}{(p^{n-m} \times p^m) \times 1}$$
$$= \frac{a \times p^m}{p^{n-m} \times p^m} = \frac{a}{p^{n-m}} = \ldots k_{n-m+1}k_{n-m}.k_{n-m-1}\ldots k_0$$

Dit kan ook worden opgevat als een verschuiving van de *komma* m plaatsen naar *rechts*. Deling door p^m in $\mathbb{Q}_p$ kan dan worden opgevat als een verschuiving van de komma m

[7] Immers, z is het aantal nullen is waarop b eindigt, dus $z \in \mathbb{N}$.

[8] want als i niet geldt, dan geldt ii en andersom

plaatsen naar *links*. Een eventuele rij nullen aan het eind van het getal rechts van de komma mag worden weggedacht.

Als $m \in \mathbb{N}$, $m \geq n$ is

$$\ldots k_{n+1}k_n.k_{n-1}\ldots k_0 \times p^m = \frac{a}{p^n} \times \frac{p^m}{1} = \frac{a \times p^m}{p^n \times 1} = \frac{a \times (p^{m-n} \times p^n)}{1 \times p^n}$$

$$= \frac{(a \times p^{m-n}) \times p^n}{1 \times p^n} = \frac{a \times p^{m-n}}{1} = a \times p^{m-n} = \ldots k_3k_2k_1k_0 \overbrace{0000\ldots0}^{m-n \text{ nullen}}$$

Dit komt overeen met een verschuiving van de komma m plaatsen naar rechts, waarbij de $m - n$ lege plaatsen van een nul worden voorzien.

De gevonden resultaten ordenen we in formules. Laat $c \in \mathbb{Q}_p$, $q \in \mathbb{N}$. We schrijven c uit in cijfers als $\ldots k_3k_2k_1k_0.k_{-1}k_{-2}\ldots k_{-n}$. Let op: het laatste cijfer is nu k_{-n} en niet k_0, zoals hiervoor steeds het geval was.

$$c \times p^q = \begin{cases} \ldots k_{-n+3}k_{-n+2}k_{-n+1}k_{-n} \overbrace{000\ldots0}^{q-n \text{ nullen}} & \text{als } n < q \\ \ldots k_{-n+3}k_{-n+2}k_{-n+1}k_{-n} & \text{als } n = q \\ \ldots k_{-q+2}k_{-q+1}k_{-q}.k_{-q-1}k_{-q-2}\ldots k_{-n} & \text{als } n > q \end{cases}$$

Voor deling door p^q in $\mathbb{Q}_p$ gelden de volgende formules. Het is mogelijk dat $n = 0$ zodat $c \in \mathbb{Z}_p$, dan is dus $c = \ldots k_3k_2k_1k_0$. Als in dat geval c bovendien rechts eindigt op z nullen, dan mogen de nullen achter de komma natuurlijk weggedacht worden in c/p^q. In formule:

$$\frac{c}{p^q} = \begin{cases} \ldots k_{z+3}k_{z+2}k_{z+1}k_z \overbrace{000\ldots0}^{z-q \text{ nullen}} & \text{als } n = 0, z > q \\ \ldots k_{q+3}k_{q+2}k_{q+1}k_q & \text{als } n = 0, z = q \\ \ldots k_{q+2}k_{q+1}k_q.k_{q-1}k_{q-2}\ldots k_z & \text{als } n = 0,\ 0 \leq z < q \\ \ldots k_{q+2}k_{q+1}k_q.k_{q-1}k_{q-2}\ldots k_{-n} & \text{als } n \neq 0 \end{cases}$$

Dat laatste geval, $n \neq 0$, is natuurlijk het meest voorkomend. De eerste drie gevallen zijn uitzonderingen.

Een voordeel van getallen uit $\mathbb{Q}_p$ voorstellen als rijtjes van cijfers

$$\ldots k_3k_2k_1k_0.k_{-1}k_{-2}\ldots k_{-n}$$

is dat er gemakkelijk mee kan worden gerekend. Stel dat we twee willekeurige p-adische getallen a_1/p^{n_1} en a_2/p^{n_2} bij elkaar willen optellen. Zoals we weten geldt:

$$\frac{a_1}{p^{n_1}} + \frac{a_2}{p^{n_2}} = \frac{a_1p^{n_2} + a_2p^{n_1}}{p^{n_1+n_2}}$$

$a_1p^{n_2}$ en $a_2p^{n_1}$ zijn de oorspronkelijke p-adische getallen waarbij de komma $n_1 + n_2$ plaatsen naar links geschoven is, en de n_2 resp. n_1 lege plekken met nullen zijn opgevuld.

Deze p-adische gehele getallen tellen we op volgens het optel-algoritme, en vervolgens "delen" we door $p^{n_1+n_2}$, ofwel we plaatsen de komma $n_1 + n_2$ stappen naar links. Nu hebben we de gevraagde som berekend.

Deze optelling klinkt misschien ingewikkeld, maar het gaat eigenlijk net zo als we bij (afgeronde) reële getallen gewend zijn. Op pagina 8 hebben we zelfs al zo'n optelling uitgevoerd.

Ook vermenigvuldigen is makkelijk als elementen $a/p^n \in \mathbb{Q}_p$ als rijtjes voorgesteld worden. We weten namelijk:

$$\frac{a_1}{p^{n_1}} \times \frac{a_2}{p^{n_2}} = \frac{a_1 a_2}{p^{n_1} p^{n_2}}$$

a_1 en a_2 zijn de oorspronkelijke p-adische getallen waarbij "de komma weggedacht wordt". We berekenen $a_1 a_2$ met het vermenigvuldig-algoritme en plaatsen de komma links van het $(n_1 + n_2)$-de cijfer, waarmee het gevraagde product gevonden is. Ook dit gaat eigenlijk net zo als vermenigvuldiging van (afgeronde) reële getallen.

Hoofdstuk 5

Weergave van g-adische getallen

Hoe kun je $\mathbb{Z}_g$ of $\mathbb{Q}_p$ grafisch weergeven? En welke problemen treden daarbij op? Daarover gaat dit hoofdstuk.

5.1 Chaos

De verzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ kunnen we afbeelden op een getallenlijn. In principe kunnen we dit ook met $\mathbb{C}$ doen, we zouden bijvoorbeeld $523.7104\ldots+8.9076\ldots i$ kunnen afbeelden naar het punt $502038.79100746\ldots$ van de reële getallenlijn. In het algemeen zouden we $\mathbb{C}$ kunnen afbeelden naar $\mathbb{R}$ met de afbeeldingsfunctie

$$a_n \ldots a_0.a_{-1} \ldots \; + \; b_n \ldots b_0.b_{-1} \ldots i \qquad \mapsto \qquad a_n b_n \ldots a_0 b_0.a_{-1} b_{-1} \ldots$$

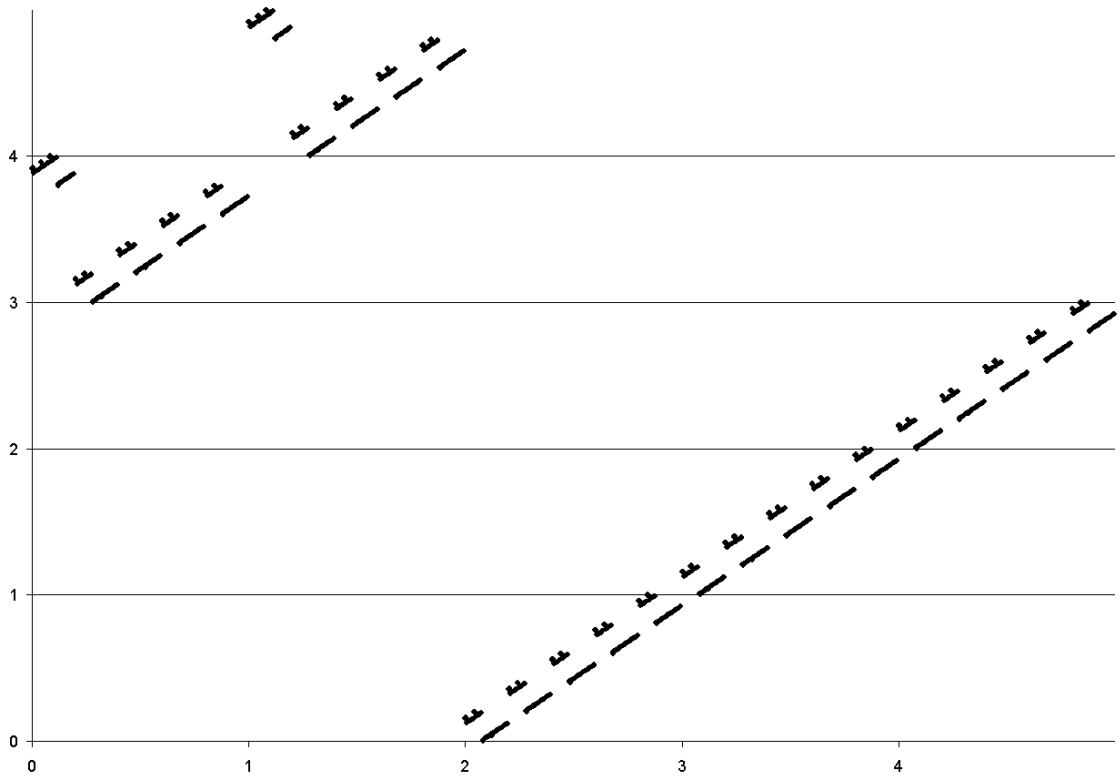
Op deze manier stelt elk punt op de reële getallenlijn precies één complex getal voor. De vraag is alleen wat deze afbeelding voor zin heeft. Het blijkt veel waardevoller te zijn om $\mathbb{C}$ af te beelden naar een getallenvlak door een imaginaire as loodrecht op de reële as toe te voegen.

Iets dergelijks doet zich voor bij de p-adische getallen. We zouden simpelweg een afbeeldingsfunctie $f : \mathbb{Q}_p \to \mathbb{R}$ kunnen definiëren die elk getal omkeert.

$$f : \qquad \ldots a_2 a_1 a_0.a_{-1} \ldots a_{-n} \qquad \mapsto \qquad a_{-n} \ldots a_{-1}.a_0 a_1 a_2 \ldots$$

Dit hebben we eens uitgeprobeerd met $\mathbb{Q}_5$, voor het gemak hebben we alleen naar de deelverzameling $\mathbb{Z}_5$ daarvan gekeken. Met Microsoft Excel hebben we voor alle elementen $x \in \mathbb{Z}_5$, afgerond op 5 decimalen, de waarde van $f(x)$ berekend en die op de getallenlijn uitgezet. Vervolgens lieten we een grafiek van de functie $g(x) = x + b$ tekenen, waarbij b een constant 5-adisch geheel getal was. Dit is een lineaire functie; als je deze grafiek voor $x, b \in \mathbb{R}$ zou tekenen, zou er een rechte lijn ontstaan. In $\mathbb{Z}_g$ blijkt dat niet het geval te zijn, zie Figuur 5.1 op pagina 57. De x-as is de reële getallenlijn op het interval $[0, 1)$ in grondtal 5, voor de y-as geldt hetzelfde. Voor b hebben we hier $\ldots 42424244$ genomen. Op het eerste gezicht ziet dit er best ordelijk uit, hoewel minder dan een rechte lijn. Toch heeft elk schuin 'streepje' op zijn beurt ook weer een grillige structuur.

Figuur 5.1: Grafiek van $g(x) = x + b$ met $x, b \in \mathbb{Z}_5$

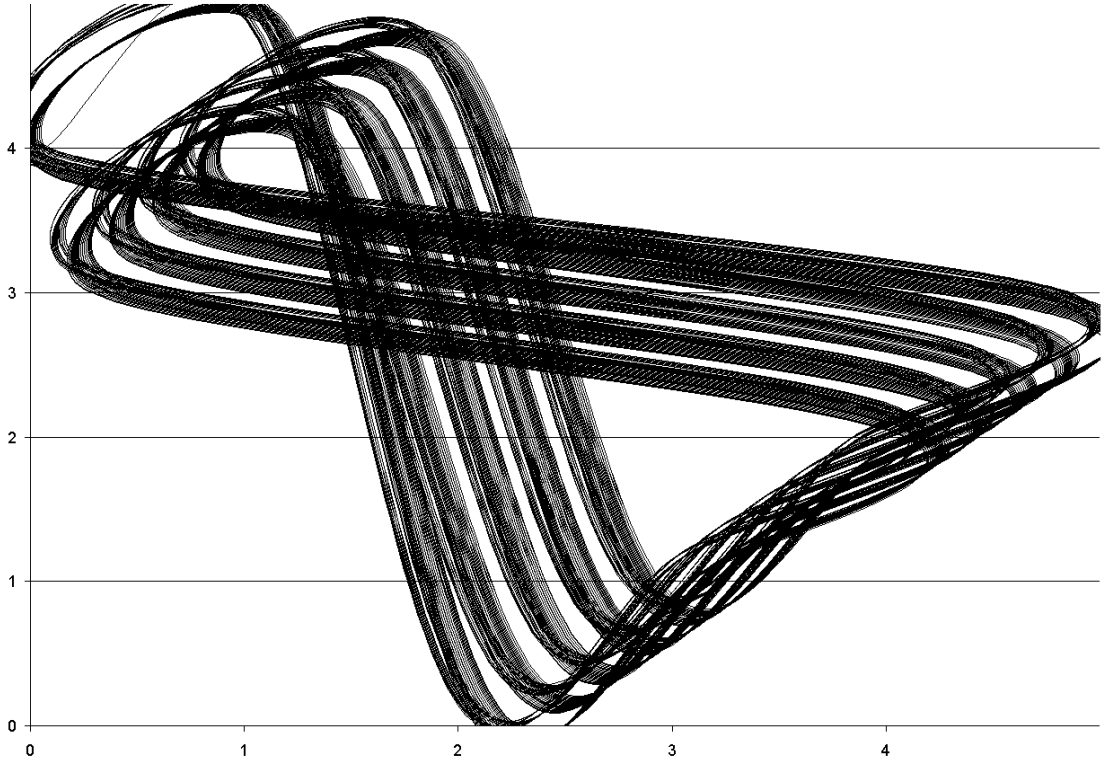


Ook blijkt dat op hoe meer decimalen nauwkeurig je de getallen benadert, hoe grilliger deze structuur is. Als je op één streepje van de grafiek inzoomt, lijkt dit heel veel op de grafiek zelf. We vermoeden dat het plaatje een fractal is als je de getallen met oneindige nauwkeurigheid zou benaderen.

Vervolgens hebben we de punten van Figuur 5.1 laten verbinden door een vloeiende lijn. Hierbij werd de volgorde $x = \ldots 001,\ \ldots 002,\ \ldots 003,\ \ldots 010,\ \cdots$ aangehouden. Op deze manier is Figuur 5.2 ontstaan, zie pagina 58. Het is een prachtig en bizar plaatje, maar het is niet duidelijk wat de betekenis ervan is. In ieder geval ziet het er chaotisch uit, het is bepaald geen rechte lijn zoals bij de reële getallen het geval zou zijn. De afbeelding doet denken aan de zogenaamde *Lorenz-attractor*, een oplossing van een bepaalde differentiaalvergelijking die oorspronkelijk is opgesteld om een natuurkundig verschijnsel te modelleren. De Lorenz-attractor blijkt een fractal te zijn.[1] Of dit werkelijk iets met de afbeelding van p-adische getallen te maken heeft weten we niet; misschien heeft het vooral te maken met de vreemde volgorde van het verbinden van punten, en met de manier waarop Excel vloeiende lijnen tekent.

[1] Bron: [2], hoofdstuk 20

Figuur 5.2: Opnieuw de grafiek van $g(x) = x + b$, nu verbonden door een lijn.



5.2 Het g-adische getallenvlak

We hebben gezien dat een poging om 5-adische getallen op een getallenlijn uit te zetten, absurde resultaten oplevert. Uit Figuur 5.1 blijkt bijvoorbeeld dat er problemen ontstaan als we een bepaalde grootte aan een 5-adisch getal willen toekennen. Het is voor de hand liggend om af te spreken dat het meest rechtse cijfer het meeste invloed heeft op de grootte van het getal, gevolgd door het cijfer links daarvan, et cetera. Dan is bijvoorbeeld $\ldots 13 > \ldots 11$ en $\ldots 29 > \ldots 31$. Maar ook geldt:

$$\ldots 13 + \ldots 18 = \ldots 31 < \ldots 29 = \ldots 11 + \ldots 18$$

Blijkbaar gaat, volgens deze definitie van de relatie $>$, de regel $a > b \Rightarrow a + c > b + c$ niet altijd op. Dit verschijnsel wordt goed geïllustreerd door Figuur 5.1.

Voor een beter begrip van g-adische getallen is het afbeelden op een getallenlijn dan ook geen goed idee, het schept alleen maar verwarring. Daarom pakken we het anders aan. In plaats van een getallenlijn tekenen we een getallenvlak.

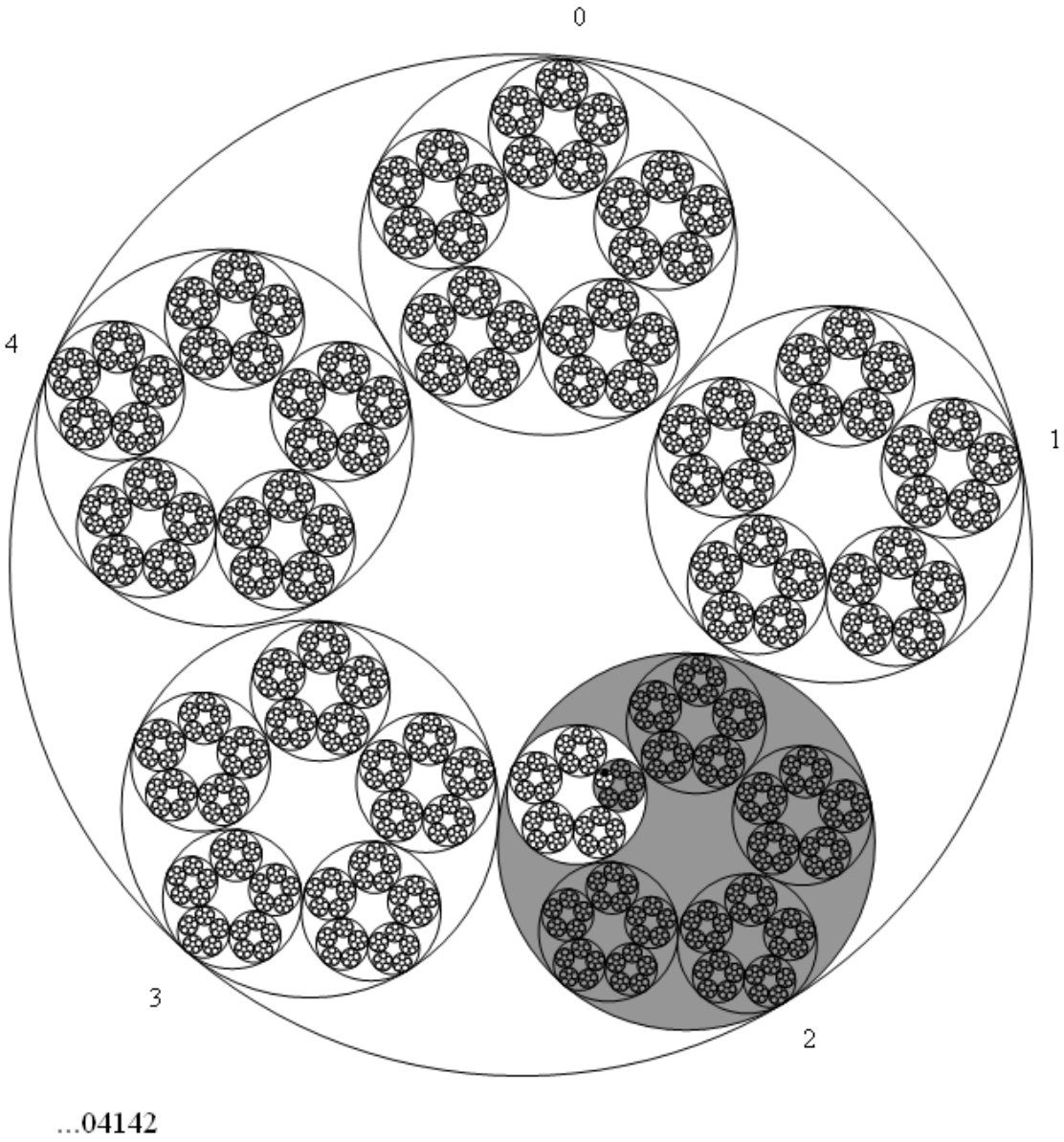
We werken weer in $\mathbb{Z}_5$, voor andere $\mathbb{Z}_g$ en voor $\mathbb{Q}_p$ gaat het analoog. Allereerst tekenen we een grote cirkel, hierin bevinden zich alle elementen van $\mathbb{Z}_5$. Deze cirkel delen we op in vijf kleinere cirkels, zie Figuur 5.3. Deze vijf cirkels stellen de mogelijkheden voor van a_0 waarbij $a = \ldots a_2 a_1 a_0$ een willekeurig element van $\mathbb{Z}_5$ is. Voor het gemak nummeren we de cirkels met

$0, 1, \ldots, 4$.

Laten we bijvoorbeeld $a_0 = 2$ kiezen. Binnen cirkel 2 tekenen we weer vijf cirkels, zij geven de mogelijkheden van a_1 weer. Hieruit kiezen we weer een cirkel en delen deze ook op. Zo kunnen we in theorie oneindig lang doorgaan. Met ieder cijfer wordt a beter benaderd, evenals de plaats van het getal in het 5-adische getallenvlak.

We zien nu grafisch weergegeven dat hoe verder een cijfer van een g-adisch getal naar links staat, hoe minder invloed het heeft op (de plaats van) het getal. Opnieuw is het resultaat een prachtig plaatje, dit keer is het duidelijk dat het een fractal is. Het behoeft geen uitleg hoe het g-adische getallenvlak er in het algemeen uitziet voor andere g.

Figuur 5.3: Het 5-adische getallenvlak



Antwoorden

1.2.1 a. $\ldots 99999$, dit is inderdaad wat we op blz. 5 gezien hebben. **b.** $\ldots 22140$ **c.** Nee. Het overlenen gebeurt van rechts naar links, dit kan daarom geen invloed hebben op cijfers die je eerder hebt berekend.

1.2.2 a. $\ldots 00001423423 = 1423423$ in grondtal 5 in $\mathbb{Z}$. **b.** $\frac{1}{7} = \ldots 2857142857143$, dit heeft 285714 als repeterende staart. $\frac{1}{8}$ is niet te berekenen in $\mathbb{Z}_{10}$, het eerste cijfer 1 van $\ldots 00001$ is namelijk niet weg te poetsen met een getal uit de tafel van 8. **c.** In de tafel van 7 heeft ieder getal in grondtal 10 een ander rechtercijfer; elk rechtercijfer komt precies 1 keer voor. Daardoor is elk cijfer op precies één manier weg te poetsen in een deling. In de tafel van 8 komt elk even rechtercijfer twee keer voor, en elk oneven rechtercijfer nul keer. Dit alles heeft te maken met het feit dat $\text{ggd}(7, 10) = 1$ en $\text{ggd}(8, 10) = 2 \neq 1$.

2.3.1 a. Nee. 7) en 8) zijn geen zinvolle beweringen als er geen nulelement is vastgelegd. **b.** Allemaal behalve 4) voor optelling en 4) voor vermenigvuldiging. **c.** $\mathbb{Z}$: allemaal behalve 4) voor vermenigvuldiging. Voor $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ gelden alle regels.

2.3.2 b. $\mathbb{Z}$ is een commutatieve ring met 1 zonder nuldelers. $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ zijn lichamen.

3.1.1 $\ldots b_3 b_2 b_1 b_0$ waarbij $b_0 = g - a_0$, en $b_i = g - a_i - 1$ voor alle $i > 0$.

3.1.2 Er geldt: $[e_i] \times [b_i] = [\sum_{k=0}^{i} e_k b_{i-k}] = [e_0 b_{i-0}] = [1 b_i] = [b_i]$, want als $k > 0$ is $e_k = 0$ en dan is ook $e_k b_{i-k} = 0$.

Bibliografie

[1] Frits Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven 2008

[2] Jan van de Craats, *Vervolgboek Wiskunde*, Pearson Education 2009

[3] David A. Madore, *A first introduction to p-adic numbers*, 2000

[4] Fernando Quadros Gouvêa, *p-adic Numbers: An Introduction*, Springer-Verlag 2003

[5] M. Riemersma, *Algebra*, Epsilon Uitgaven 2003

[6] http://en.wikipedia.org/wiki/P-adic_number

[7] http://en.wikipedia.org/wiki/Algebraic_structure

[8] http://nl.wikipedia.org/wiki/Verzameling_%28wiskunde%29

[9] http://nl.wikipedia.org/wiki/Polynoom

[10] http://en.wikipedia.org/wiki/Modular_arithmatic#The_congruence_relation

(Zie de genoemde pagina's van Wikipedia voor de primaire bronnen.)