Voorwoord

Deze cursusnota's horen bij het opleidingsonderdeel *Relaties en structuren* uit de eerste Bachelor wiskunde. Alles wat aan bod zal komen tijdens de theorielessen, is bevat in deze nota's. De student kan dus steeds op deze nota's terugvallen indien er onduidelijkheden zijn. Naast de theorielessen zijn er ook praktische oefeningen onder begeleiding voorzien. Het materiaal dat in de oefeningenlessen aan bod komt, zal via het elektronisch leerplatform aangeboden worden.

De bachelor wiskunde beheerst de basiselementen van de wiskunde, kan zelfstandig nieuwe vakkennis verwerven en ze integreren in reeds opgedane kennis en vaardigheden. Dit is één van de eindcompetenties in de bacheloropleiding wiskunde. Willen we deze competentie bereiken, dan moeten we, vanaf dag één in de opleiding, de wiskunde onderwijzen zoals ze is: als een abstracte wetenschap waarin een uitspraak slechts een stelling genoemd wordt als ze bewezen is. Wiskunde is dus geen kookboek, het is niet een lijst met recepten om bepaalde problemen, die vandaag toevallig hip zijn, op te lossen. Wiskunde biedt echter zeer veel inzicht in structuren die model kunnen staan voor de omgeving waarin een probleem omschreven wordt, en aldus kan de wiskundige voor specifieke problemen een oplossing bedenken. Dit feit ligt trouwens aan de basis van de eeuwenlange, uiterst succesvolle wisselwerking tussen wiskunde en natuurkunde, en ook andere wetenschappen.

We merken dat de instromende studenten minder beschikken over abstracte kennis, terwijl er in de cursussen zoals Analyse en Lineaire algebra en analytische meetkunde, soms een zekere (abstracte) voorkennis verondersteld wordt. Om de voorkennis van de instromende studenten op hetzelfde peil te brengen, werd enkele jaren geleden deze cursus ingevoerd in het programma. Voor deze cursus veronderstellen we eigenlijk geen voorkennis. Een aantal *algebraïsche structuren* die steeds terugkeren in de opleiding, komt aan bod. Daarnaast hebben we aandacht voor een aantal combinatorische technieken, en bevat deze cursus ook een zeer korte inleiding tot de grafentheorie. We behandelen alles op een strikt wiskundige manier. Alle eigenschappen waarvan we vinden dat de student ze na het volgen van deze cursus moet beheersen, worden *bewezen*. Stelling en bewijs spelen dus een belangrijke rol.

Eerstebachelorstudenten moeten heel wat nieuwe kennis verwerven. Het pleidooi voor een abstracte aanpak sluit niet uit dat we meestal met concrete structuren zullen werken. De visie is immers dat als we studenten abstracte theorieën willen aanleren over structuren, ze op zijn minst een aantal verschillende voorbeelden van een specifieke structuur moeten kennen en goed begrijpen, voor ze een abstractieniveau verder gaan. Het is bijvoorbeeld heel moeilijk om een theorie over velduitbreidingen geven (in een cursus Algebra bijvoorbeeld), als de studenten alleen maar de reële getallen als voorbeeld van een veld kennen.

Deze cursusnota's zijn gebaseerd op de cursusnota's die bij de invoering van dit vak door Fank De Clerck geschreven werden. Op basis van onze ervaringen in het academiejaar 2012–2013, en na lange pleidooien van Bert Seghers, werd besloten om enkele ingrijpende wijzigingen aan te brengen in de versie voor het academiejaar 2013–2014. Zo werden de hoofdstukken logica en verzamelingenleer grondig herwerkt door Bert Seghers, waarvoor ik hem zeer erkentelijk ben. De hoofdstukken getaltheorie en modulair rekenen werden samengevoegd, zodat enkele belangrijke stellingen een eleganter (en vooral korter) bewijs kregen; de hoofdstukken groepentheorie en algebra werden samengevoegd tot één hoofdstuk "algebra", en een aantal fouten in het hoofdstuk grafentheorie werd rechtgezet.

Met dank aan Frank De Clerck, die op 1 oktober 2012 met pensioen ging, voor het beschikbaar stellen van de LaTeX-bestanden van zijn nota's, aan Tom De Medts voor het beschikbaar stellen van het LaTeX-stylebestand die de hoofdingen van de hoofdstukken vormgeeft, en aan Karsten Naert, Bert Seghers, Geert Vernaeve en Bart De Bruyn voor het kritisch nalezen van deze nota's.

Jan De Beule
september 2013

Leidraad

Moet er in een studie wiskunde *van buiten geleerd worden*? Dit is een zeer interessante vraag. In het voorwoord verwezen we reeds naar één van de eindcompetenties van de bachelor wiskunde: *De bachelor wiskunde beheerst de basiselementen van de wiskunde, kan zelfstandig nieuwe vakkennis verwerven en ze integreren in reeds opgedane kennis en vaardigheden.* Het vak Relaties en Structuren is bij uitstek een vak over basiselementen van de wiskunde. Er mag dus verwacht worden dat de student, na het volgen van dit vak, en na het gedurende enige tijd studeren van dit vak, de in de cursus aanwezige basiselementen beheerst. Hoeveel uren er *precies* gestudeerd moeten worden, is van student tot student verschillend, en daarop kan deze leidraad geen antwoord geven.

Deze nota's bevatten heel wat informatie. Een gedeelte daarvan is essentieel. Dat wil zeggen dat er verwacht wordt dat de student deze essentiële informatie *vlot beheerst*. Definities, lemma's, stellingen en gevolgen zijn allemaal essentieel, en hebben een opvallende vormgeving meegekregen:

Definitie 0.1

Dit is een definitie van een bepaalde *structuur*.

Lemma 0.2

Zonder dit lemma, kan de volgende stelling niet bewezen worden.

Stelling 0.3

Dit is een belangrijke stelling.

Gevolg 0.4

Dit is een gevolg van de vorige stelling.

Er wordt verwacht dat de student essentiële informatie kan reproduceren. Dit betekent, in zekere zin, dat deze informatie van buiten geleerd kan worden. Beter nog probeert de student eerst voldoende inzicht te verwerven in de materie, onder andere door een aantal praktische oefeningen te maken. Nadien zal de student inderdaad voldoende studietijd moeten investeren om de essentiële informatie te memoriseren. Dank zij het verworven inzicht kan dit systematisch gebeuren, en is er geen sprake meer van *van buiten leren*. Zo goed als alle lemma's, stellingen en gevolgen worden *bewezen*. Naast de parate kennis van de lemma's, stellingen en gevolgen, wordt er uiteraard verwacht dat de student de bewijzen kan reproduceren. Ook hier geldt dat hoe beter het inzicht in het bewijs is, des te gemakkelijker dit gememoriseerd kan worden. Bewijzen die correct zijn, maar anders dan in de cursus, worden onvoorwaardelijk goed gerekend. Elk bewijs is in de tekst duidelijk gemarkeerd. Het begin van een bewijs wordt toepasselijk aangegeven door *Bewijs.*, het einde door de *halmos*: $\square$, welke de traditionele afkorting *QED* vervangt.

Op sommige plaatsen in de nota's is er nogal wat bijkomende informatie te vinden. Deze dient in de eerste plaats om de essentiële informatie te verduidelijken, onder andere door middel van voorbeelden. Er wordt niet verwacht dat de student alle voorbeelden kan reproduceren. Eerder kunnen er vragen gesteld worden over de voorbeelden. In elk geval zal er ten gepaste tijde een volledig overzicht gegeven worden van de materie die als te kennen beschouwd wordt, en de materie waar er op het examen geen vragen over gesteld zullen worden.

Tijdens het mondeling examen wordt er dus van de student verwacht dat er vlot antwoord gegeven kan worden op de gestelde vragen. Dit mondeling examen geschiedt echter met een grondige schriftelijke voorbereiding, waarvoor er voldoende tijd gegeven wordt. De bedoeling van het mondeling examen is om in te pikken op de schriftelijke voorbereiding, en kleine, bijkomende vragen te stellen, om aldus te peilen naar het inzicht in de materie, én om de student de kans te geven om onvolkomenheden of fouten recht te zetten.

Een gedeelte van de lestijden wordt ingevuld door oefeningenlessen onder begeleiding. Ook voor dit gedeelte is er een examen voorzien, dat volledig schriftelijk afgenomen wordt. Ook voor dit schriftelijk examen wordt de student verondersteld om de essentiële materie voldoende te beheersen. Het oefeningenexamen is dus eveneens onder gesloten boek.

Inhoudsopgave

Hoofdstuk

1 Logica

Logica is de wetenschap van het redeneren. Wiskundigen leiden waarheid af door zorgvuldig te redeneren. Daarom is basiskennis van logica onontbeerlijk in elke opleiding wiskunde, al was het maar om de spelregels van het spel der wiskunde duidelijk te stellen, die bijna alle wiskundige disciplines vandaag gebruiken. Een dergelijke introductie is het voornaamste wat dit hoofdstuk wil bereiken en we proberen dan ook een precieze, maar voldoende intuïtieve aanpak te hanteren.

In dit logicahoofdstuk zullen we op papier zetten wat de regels zijn om correct gevormde wiskundige uitspraken te maken (de syntax van de wiskundige taal) en de betekenis van belangrijke woorden en symbolen ondubbelzinnig vastleggen (de semantiek van de wiskundige taal). Dit doen we eerst voor *en*, *of*, ... en daarna voor de *kwantoren*. Dit zal ons de eerste twintig pagina's bezighouden.

De reden van deze oppervlakkige studie van propositie- en predikaatlogica is dat we daarmee expliciet de wiskundige denkprocessen blootleggen. Ontdaan van alle concrete invulling bestuderen we de wetmatigheden waaraan het menselijk redeneren, en in het bijzonder het wiskundig redeneren, voldoet. De verdienste daarvan is dat we zo voeling kunnen krijgen met hoe correcte argumenten in een redenering (lees: bewijs) eruit kunnen zien. We staan dan ook stil bij de consequenties van onze uiteenzetting voor de praktijk van het *bewijzen*. Hoewel het mogelijk is om "al doende" wiskundige redeneringen te leren opbouwen, dus wiskunde te doen zonder vooraf de logica zo expliciet te maken als wij hier zullen doen, hopen we dat deze introductie beginnende wiskundigen sterker zal maken, en hen in staat zal stellen om op elk moment beter te beseffen waarmee ze bezig zijn.

Dat ze dus het elementaire begin is voor elke wiskundige neemt niet weg dat de wiskundige logica vandaag één van de grote en bloeiende gebieden binnen de wiskunde is geworden, waar vooral in de twintigste eeuw theorieën zijn ontwikkeld waarin vandaag heel wat interessant onderzoek gebeurt. Om een glimp op te vangen van de totaliteit van dit domein, zal de beginnende wiskundestudent nog moeten wachten tot *Wiskundige logica* (3de bachelorjaar wiskunde), maar we lichten al een tipje van de sluier in paragraaf 1.5.

1.1 Propositielogica

1.1.1 Proposities

Wiskunde is een discipline die ideeën behandelt die uitgedrukt worden in zinnen. Dit kan in een symbolische taal, maar doorgaans gebruiken we de Nederlandse (of soms een andere) taal.

Taal — bijvoorbeeld het Nederlands — is een opmerkelijk efficiënt communicatiemiddel. Dat is voor een groot deel te danken aan wat linguisten *indexicaliteit* noemen. Dat is de manier waarop de betekenis van wat we schrijven of zeggen afhangt van de context waarin we het schrijven of zeggen en de context waarin het gehoord of gelezen wordt. Woorden als *ik*, *zomermaanden* of *klein* hebben bijvoorbeeld geen universele, maar een contextafhankelijke betekenis. Indexicaliteit stelt ons in staat om met relatief weinig woorden te spreken over een veel grotere reeks onderwerpen en is dus van onvoorstelbaar nut in dagdagelijkse communicatie.

Helaas kan indexicaliteit van de taal problematisch zijn wanneer het aankomt op spreken of schrijven over wiskunde. Wiskundige ideeën die we in Nederlandse zinnen uitdrukken, worden verondersteld niet dubbelzinnig of vaag te zijn; ze moeten duidelijke, precieze en unieke betekenissen hebben, onafhankelijk van de context. We zullen ons ervan verzekeren dat dit zo is door onze studie te *beperken* tot enkel díe zinnen die geschikt zijn voor wiskundige doeleinden, als volgt.

Met een **propositie** of **uitspraak** bedoelen we voortaan een stellende zin die ondubbelzinnig hetzij waar, hetzij onwaar is.

Als een propositie waar is, zeggen we dat ze de **waarheidswaarde** *waar* heeft. Als dat niet zo is, zeggen we dat de waarheidswaarde *onwaar* of *vals* is. Een kenmerk van uitspraken is dat elke twee redelijke en geïnformeerde personen het zouden eens zijn over de waarheidswaarde van een uitspraak.

De volgende zinnen zijn proposities:

- Twee plus drie is vijf.
- David Hilbert is geboren in Königsberg.
- Alle reële functies op $[0, 1]$ zijn afleidbaar op $]0, 1[$.
- Gent is de enige Vlaamse universiteitsstad.
- Als 32 een priemgetal is of 32 geen priemgetal is, dan is $\pi \in \mathbb{Q}$.

- Euclides was een Griek of een wiskundige.
- Elk even getal groter dan drie is te schrijven als de som van twee priemgetallen.

Het kan mogelijk zijn om te bepalen of een zin een propositie is, zonder de waarheidswaarde te weten of na te gaan. Dit is het geval bij het laatste voorbeeld: deze propositie staat bekend als het vermoeden van Goldbach.

De uitspraak $xy = z$ is bijvoorbeeld geen propositie, want er wordt niet gespecifieerd wat x, y en z zijn.

1.1.2 Connectieven

Woorden zoals *en*, *of* en *niet* kunnen proposities wijzigen of combineren om complexere beweringen te maken. Ze worden **logische connectieven** genoemd en combineren één of meer proposities tot samengestelde proposities. Proposities die niet samengesteld zijn d.m.v. connectieven worden atomaire proposities genoemd.

Om alle dubbelzinnigheid uit te sluiten, hebben wiskundigen vastgelegd welke van de mogelijke betekenissen precies bedoeld wordt met elk van deze connectieven — veel hiervan was al gedaan door de oude Grieken. Dit zullen we ook in dit hoofdstuk doen.

Conjunctie

Het woord

$$en$$

stelt ons in staat om te beweren dat twee gebeurtenissen zich simultaan voordoen. In symbolische uitdrukkingen kunnen we dit woord afkorten met een symbool, de meest gebruikelijke zijn

$$\wedge \qquad , \qquad \&$$

zodat de uitdrukking

$$(\pi > 3) \wedge (\pi < 4)$$

zegt:

$$\pi \text{ is groter dan } 3 \textit{ en } \pi \text{ is kleiner dan } 4,$$

of dus dat π tussen 3 en 4 ligt. Voor twee wiskundige uitspraken ϕ en ψ noemen we de bewering $\phi \wedge \psi$ de **conjunctie** van ϕ en ψ. We zullen ook verderop deze Griekse letters gebruiken als *propositievariabelen*.

In wiskundige context is *en* onafhankelijk van de volgorde: $\phi \wedge \psi$ betekent hetzelfde als $\phi \wedge \psi$. In de Nederlandse taal kan er soms een nuance of tijdsaspect meespelen: vergelijk bijvoorbeeld "hij reed weg en raakte een voetganger" met "hij raakte een voetganger en reed weg".

Disjunctie

Het woord

$$of$$

zullen we gebruiken om aan te geven dat een gebeurtenis A *of* een gebeurtenis B zich voordoet. Het gebruik van *of* in de volgende uitspraken

$$a > 0 \qquad of \qquad \text{de vergelijking } x^2 + a = 0 \text{ heeft een reële wortel}$$
$$ab = 0 \qquad \text{als} \qquad a = 0 \ of \ b = 0$$

zou kunnen verschillend geïnterpreteerd worden, omdat er in het eerste geval geen mogelijkheid is dat beide gebeurtenissen zich tegelijk voordoen, terwijl in het tweede geval wordt bedoeld dat ook $a = 0$ en $b = 0$ beide mogen waar zijn. De wiskunde kent geen plaats voor mogelijke dubbelzinnigheid in de betekenis van een woord als *of*, dus kiezen we hier voor één van beide betekenissen. Het blijkt dat het geschikter is om met het woord *of* te bedoelen dat één van beide, *of beide* voorvalt. We zullen dus altijd de *inclusieve of* bedoelen wanneer we *of* schrijven en gebruiken daarvoor het volgende symbool.[1]

$$\vee$$

De uitspraak

$$\phi \vee \psi$$

betekent dat *ten minste één van* ϕ, ψ waar is en wordt de **disjunctie** genoemd van ϕ en ψ. De volgende (eerder zielige) bewering is bijvoorbeeld betekenisvol en bovendien waar:

$$(3 < 5) \vee (1 = 0)$$

[1]Het Latijn kent de distinctie tusen de inclusieve of (*vel*) en de exclusieve of (*aut*) — het symbool $\vee$ komt van *vel*.

Negatie

We willen ook uitspraken kunnen ontkennen, dus leggen we de betekenis van het woord

$$\textit{niet}$$

vast. Als ψ een bewering is, dan is *niet* ψ de bewering dat ψ vals is. Dus als ψ een ware uitspraak is, dan is *niet* ψ een valse uitspraak. Als ψ een valse uitspraak is, dan is *niet* ψ een ware uitspraak. Het symbool dat tegenwoordig standaard is, is

$$\neg$$

en de uitspraak $\neg\phi$ wordt de **negatie** of (logische) **ontkenning** genoemd van ϕ. De uitspraak

$$\neg(\pi < 3)$$

betekent bijvoorbeeld $\pi \geq 3$, wat hetzelfde is als $(\pi = 3) \vee (\pi > 3)$.

Implicatie en de conditionele propositie

In wiskunde gebruiken we vaak een uitdrukking van de vorm

$$\text{Als } \phi\text{, dan } \psi.$$

Het is van groot belang om vast te leggen wat de betekenis is van een samengestelde propositie van deze vorm. Hoewel het niet is wat we zullen doen, zou het niet onredelijk zijn om die deze betekenis te geven: *Als ϕ waar is, kan men hieruit afleiden dat ψ ook waar moet zijn.* Maar neem voor ϕ de ware uitspraak "$\sqrt{2}$ is irrationaal" en voor ψ de ware uitspaak "$0 < 1$". Is de implicatie dan waar? Volgt uit de irrationaliteit van $\sqrt{2}$ dat 0 kleiner is dan 1?

Natuurlijk niet. Er is geen echt verband tussen ϕ en ψ in dit geval. Om nog niet te spreken van implicaties als

$$\text{(Julius Caesar is dood) } \textit{impliceert } (1 + 1 = 2).$$

Het probleem is dat het concept van implicatie in onze taal niet alleen betrekking heeft op waarheid (zoals *en*, *of* en *niet*), maar ook op *causaliteit*. Wanneer mensen zeggen "ϕ impliceert ψ", wordt bedoeld dat ϕ er op één of andere oorzakelijke manier voor zorgt dat ψ waar is. Dat heeft als gevolg dat de waarheid van ψ volgt uit de waarheid van ϕ, maar waarheid alleen kan niet helemaal vatten wat er gebeurt.

Voor onze doeleinden, het preciseren van ons wiskundig taalgebruik, is de complexe zaak van causaliteit iets wat we niet wensen te beschouwen. Daarom zullen we de notie van implicatie uiteentrekken in een waarheidsgedeelte en een causaliteitsgedeelte, en het laatste bannen. Het waarheidsgedeelte zullen we noteren met $\Rightarrow$ en een samengestelde uitspraak

$$\phi \Rightarrow \psi$$

noemen we een **conditionele propositie**. De uitspraak ϕ is hierin het **antecedent**, de **voorwaarde** of de **hypothese** en ψ het **consequens**, het **gevolg** of de **conclusie**. De waarheid van een conditionele uitspraak zal volledig in functie van de waarheid van het antecedent en het consequens gedefinieerd worden[2]. Het is precies dit feit, dat een conditionele uitspraak altijd een goed gedefinieerde waarheidswaarde heeft, wat deze notie zo belangrijk maakt in de wiskunde — in de wiskunde kan men zich immers geen uitspraken met ongedefinieerde waarheidswaarde veroorloven. Zo'n definitie, die een betekenisvol deel van de gebruikelijke implicatie onder de mat veegt, kan tot contraintuïtieve of soms absurde waarheden leiden, zoals (Julius Caesar is dood) $\Rightarrow (1 + 1 = 2)$. Maar gelukkig zal, telkens wanneer er *wel* een betekenisvol verband is tussen ϕ en ψ, de waarheidswaarde van de conditionele uitspraak overeenstemmen met die van de betekenisvolle implicatie ϕ *impliceert* ψ.

Wanneer zal de conditionele propositie $\phi \Rightarrow \psi$ nu waar zijn? Als het antecedent ϕ waar is, ligt het voor de hand dat $\phi \Rightarrow \psi$ waar moet zijn als ook ψ waar is, en vals als ψ vals is. Om de waarheidswaarde vast te leggen wanneer ϕ vals is, kijken we naar de negatie van de implicatie. Noteer het causaliteitsvrije waarheidsgedeelte van de uitspraak "ϕ impliceert ψ niet" met $\phi \not\Rightarrow \psi$. Welnu, ϕ zal ψ *niet* impliceren als het zo is dat *hoewel* ϕ waar is, ψ *toch* vals is. Daarom zullen we definiëren dat $\phi \not\Rightarrow \psi$ waar is precies wanneer ϕ waar is *en* ψ vals. Door hiervan de logische ontkenning te bekijken, bekomen we de waarheidswaarde van $\phi \Rightarrow \psi$: deze zal waar zijn in de gevallen waar $\phi \not\Rightarrow \psi$ vals is. Dus $\phi \Rightarrow \psi$ zal waar zijn in de volgende gevallen:

- ϕ en ψ zijn beide waar.
- ϕ en ψ zijn beide vals.
- ϕ is vals en ψ is waar.

[2] *Relevantielogica* is een tak van de logica, ontstaan in 1928, die de implicatie pas waar definieert wanneer er *wel* een betekenisvol verband is tussen antecedent en consequens. Deze komt niet aan bod in de opleiding wiskunde.

We onthouden: dat we met de conditionele uitspraak een notie gedefinieerd hebben die slechts een deel vat van wat de implicatie betekent; dat we de definitie enkel gebaseerd hebben op de waarheidswaarde van antecedent en consequens; en dat deze in alle betekenisvolle gevallen overeenstemt met de waarheidswaarde van de echte implicatie.

Equivalentie

Nauw verwant aan de notie van de implicatie is die van equivalentie. Twee uitspraken zijn *logisch equivalent* als elk ervan de andere impliceert. Het formele waarheidsgedeelte ervan is de **biconditionele propositie**, die we schrijven als

$$\phi \Leftrightarrow \psi.$$

Ze is gedefinieerd als een afkorting voor

$$(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi).$$

Terugkijkend naar de definitie van de conditionele propositie, stellen we vast dat $\phi \Leftrightarrow \psi$ zal waar zijn in het geval waar ϕ en ψ beide waar zijn, en in het geval beide vals zijn (en vals in de andere gevallen). Dus twee uitspraken zijn equivalent als ze dezelfde waarheidswaarde hebben.

Ondanks het betoog dat een implicatie over het algemeen meer inhoudt dan enkel een conditionele waarheidsuitspraak, zal men in de wiskunde toch vaak spreken over *implicatie* en *equivalentie*, hoewel strikt genomen de (bi)conditionele propositie bedoeld wordt. Dit komt omdat (bi)conditionele uitspraken slechts verschillen van echte implicatie en equivalentie in situaties die niet voortspruiten uit de gangbare wiskundige praktijk. In bijna elke wiskundige context *is* de conditionele uitspraak een implicatie en *is* de biconditionele uitspraak een equivalentie, *met* een achterliggende suggestie van een betekenisvol verband.

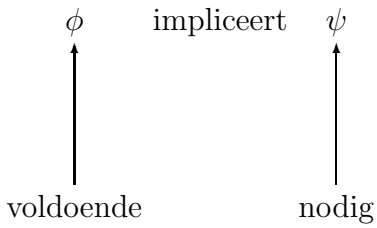
Formuleringen van implicatie en equivalentie

Er zijn heel wat termen om een implicatie te formuleren:

- ϕ impliceert ψ
- Als ϕ, dan ψ
- Uit ϕ volgt ψ
- ϕ is voldoende voor ψ
- ψ als ϕ
- ψ wanneer ϕ

- ψ zodra ϕ
- ψ is noodzakelijk voor ϕ

De terminologie van *nodige* en *voldoende voorwaarde*n wordt ook nog gebruikt. Echter, zorgvuldigheid is geboden om verwarring te vermijden. Zeggen dat ψ noodzakelijk is voor ϕ betekent niet dat ψ alleen genoeg is om ϕ te garanderen. Het betekent eerder dat ψ zal moeten waar zijn, eer er sprake kan zijn van ϕ. Antecedent en consequens worden af en toe ook de **voldoende voorwaarde** en **nodige voorwaarde** genoemd:



Omdat equivalentie zich herleidt tot implicatie in beide richtingen, volgt uit het bovenstaande dat de volgende uitspraken hetzelfde betekenen:

- ϕ is equivalent met ψ
- ϕ als en slechts als ψ
- ϕ is nodig en voldoende voor ψ
- ϕ dan en slechts dan als ψ

In Engelstalige wiskundeteksten wordt *if and only if* soms afgekort tot *iff*.

1.1.3 Ontkenning van samengestelde proposities

De eerste observatie is eenvoudig: de dubbele negatie

$$\neg(\neg\phi)$$

is equivalent met ϕ. In de Nederlandse taal is dit principe niet noodzakelijk geldig: wie zegt niet ontevreden te zijn, bedoelt zeker niet helemaal tevreden te zijn!

De conjunctie $\phi \wedge \psi$ betekent dat ϕ en ψ beiden waar zijn, dus

$$\neg(\phi \wedge \psi)$$

betekent dat het niet het geval is dat ze beiden waar zijn. In dat geval moet minstens één van de twee vals zijn. Zeggen dat ten minste één van ϕ en ψ

vals is, is hetzelfde als zeggen dat ten minste één van $\neg\phi$ en $\neg\psi$ waar is. Door de gedefinieerde betekenis van *of* kan dit dus uitgedrukt worden als $(\neg\phi) \vee (\neg\psi)$. Dus ontkenning heeft het effect dat het $\wedge$ verandert in $\vee$ en op dezelfde manier kan men nagaan dat het $\vee$ verandert in $\wedge$. Deze identiteiten staan bekend als de **wetten van De Morgan**:

Wetten van De Morgan

$$\begin{aligned} \neg(\phi \wedge \psi) &\iff (\neg\phi) \vee (\neg\psi) \\ \neg(\phi \vee \psi) &\iff (\neg\phi) \wedge (\neg\psi) \end{aligned}$$

Het effect van de negatie op conditionele uitspraken wordt bepaald door onze definitie van de conditionele propositie op basis van haar negatie. Door deze definitie hebben we de equivalentie

$$\neg(\phi \Rightarrow \psi) \iff \phi \wedge (\neg\psi).$$

We besluiten dus dat de negatie van "als ϕ, dan ψ" niets anders is dan "ϕ is waar en ψ is vals". Door bovenstaande equivalentie lid aan lid te ontkennen, vinden we middels de wetten van De Morgan:

$$\phi \Rightarrow \psi \iff (\neg\phi) \vee \psi$$

Vaak noteren we korter

$$\begin{aligned} & \phi \not\Rightarrow \psi \quad \text{i.p.v.} \quad \neg(\phi \Rightarrow \psi) \\ \text{en} \quad & x \neq y \quad \text{i.p.v.} \quad \neg(x = y) \end{aligned}$$

1.1.4 Waarheidstabellen

Omdat de logische connectieven gedefinieerd zijn in termen van waarheidswaarde alleen, en bovendien volledig bepaald worden door de waarheidswaarde van de samenstellende proposities, kunnen we elk connectief volledig voorstellen aan de hand van een zogenaamde *waarheidstabel*. Alle mogelijke combinaties van waarheidswaarden van de atomaire proposities krijgen een regel in de tabel. Met de notatie 1 voor waar en 0 voor vals, krijgen we de volgende waarheidstabellen:

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Waarheidstabellen kunnen opgesteld worden voor ingewikkelder uitspraken, die samengesteld zijn uit meerdere (voorkomens van) proposities. Ze kunnen gebruikt worden om na te gaan dat twee complexer samengestelde proposities equivalent zijn. Door de definitie van equivalentie zullen twee uitspraken equivalent zijn als ze dezelfde waarheidstabel hebben. Bij wijze van voorbeeld bewijst de volgende tabel een wet van De Morgan.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Omdat de middelste en laatste kolom een gelijke invulling hebben, moeten we besluiten dat ze altijd dezelfde waarheidswaarde hebben, ongeacht wat de waarheidswaarden van ϕ en ψ zijn. En dat was wat logische equivalentie van proposities betekende.

1.1.5 Contrapositie

Als $\phi \Rightarrow \psi$ een implicatie is, dan wordt de propositie $\psi \Rightarrow \phi$ de **omgekeerde implicatie** (converse) genoemd. Er is in het algemeen geen verband tussen de waarheidswaarde van een implicatie en die van zijn omgekeerde. Merk wel op dat twee uitspraken equivalent zijn precies wanneer zowel de implicatie als de omgekeerde implicatie waar zijn.

De **contrapositieve** van de implicatie $\phi \Rightarrow \psi$ is de propositie $(\neg\psi) \Rightarrow (\neg\phi)$. Bijvoorbeeld, voor de implicatie

$$\textit{Als } 2^n - 1 \textit{ een priemgetal is, dan is } n \textit{ een priemgetal.} \tag{1.1}$$

is de contrapositieve

Als n een samengesteld getal is, dan is $2^n - 1$ ook samengesteld.

Stelling 1.1

Elke implicatie is equivalent met zijn contrapositieve.

Bewijs.

p	q	$p \to q$	$\neg p$	$\neg q$	$(\neg q) \to (\neg p)$
1	1	1	0	0	1
1	0	0	0	1	0
0	1	1	1	0	1
0	0	1	1	1	1

□

Dit resultaat is de logische basis voor het wiskundige concept van een bewijs door contrapositie, waar een uitspraak bewezen wordt door de contrapositie ervan te bewijzen. Krachtens deze stelling zou het bijvoorbeeld, om de waarheid van uitspraak 1.2.2 te vestigen, volstaan om te bewijzen dat als n samengesteld is, dan ook $2^n - 1$ samengesteld is.

1.1.6 Tautologie en contradictie

Het **falsum** is de atomaire propositie die altijd vals is. Het wordt genoteerd met $\bot$. De atomaire propositie die altijd waar is wordt genoteerd met $\top$ en is dus equivalent met $\neg\bot$.

Een propositionele formule wordt een **tautologie** genoemd als ze waar is voor elke mogelijke combinatie van waarheidswaarden van de atomaire proposities waaruit ze samengesteld is. Een propositionele formule die altijd vals is wordt een **contradictie** genoemd.

Anders gezegd, een tautologie is een propositionele formule die equivalent is met $\top$ en een contradictie is er één die equivalent is met $\bot$. De proposities $\top$ en $\bot$ worden soms ook gedefinieerd als *een willekeurige tautologie* of *een willekeurige contradictie*.

De volgende formules zijn tautologieën:

$P \Rightarrow (P \vee Q)$	Constructie van de disjunctie
$(P \wedge Q) \Rightarrow P$	Decompositie van de conjunctie
$(P \vee P) \Leftrightarrow P$	Vereenvoudiging
$(P \wedge P) \Leftrightarrow P$	Vereenvoudiging
$P \vee \neg P$	Tertium non datur
$(\neg P \Rightarrow \bot) \Rightarrow P$	Reductio ad absurdum
$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$	Contrapositie
$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$	Modus ponens
$(\neg Q \wedge (P \Rightarrow Q)) \Rightarrow \neg P$	Modus tollens
$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$	Hypothetisch syllogisme
$((P \vee Q) \wedge \neg P) \Rightarrow Q$	Disjunctief syllogisme
$[(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R)] \Rightarrow R$	Gevalsonderscheid (proof by cases)
$[(P \wedge Q) \Rightarrow R] \Leftrightarrow [P \Rightarrow (Q \Rightarrow R)]$	Exportatie
$[(P \Rightarrow Q) \wedge (R \Rightarrow S) \wedge (P \vee R)] \Rightarrow Q \vee S$	Constructief dilemma
$(P \Rightarrow Q) \Rightarrow (P \Rightarrow (P \wedge Q))$	Absorptie
$(P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$	Associativiteit van disjunctie
$(P \wedge (Q \wedge R)) \Leftrightarrow ((P \wedge Q) \wedge R)$	Associativiteit van conjunctie
$(P \vee Q) \Leftrightarrow (Q \vee P)$	Commutativiteit van disjunctie
$(P \wedge Q) \Leftrightarrow (Q \wedge P)$	Commutativiteit van conjunctie
$(P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$	Distributiviteit
$(P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$	Distributiviteit

1.2 Predikaatlogica

1.2.1 Predikaten

De propositielogica is niet voldoende als instrument om wiskundige objecten te bestuderen. Over uitdrukkingen zoals "x is een positief reëel getal" of "voor elk natuurlijk getal n is n^2 niet-negatief", kan de propositielogica niet echt iets zeggen. De eerste uitdrukking is zelfs geen uitspraak, want de waarde van x is niet gegeven.

Dergelijke uitdrukkingen, zoals "is een positief reëel getal" of "studeert wiskunde aan de UGent", worden **predikaten** genoemd. Het zijn geen proposities omdat men nog een onderwerp moet invullen. Men gebruikt soms ook de term **propositionele functie** voor predikaten, omdat men ze kan opvatten als een functie die een object uit een bepaald domein afbeeldt op een propositie — of gewoon op een waarheidswaarde, één van *waar, vals*.

Bij predikaten houdt men steeds een **universum** in gedachten: dit is de

onderliggende verzameling waaruit objecten mogen ingevuld worden in het predikaat om het een zinvolle betekenis en waarheidswaarde te kunnen geven. Voor "is een positief reëel getal" zouden dat de reële of complexe getallen kunnen zijn, voor "studeert wiskunde aan de UGent" misschien alle UGent-studenten of zelfs alle personen ter wereld.

Zoals we deden met proposities, kunnen we ook predikaten voorstellen door letters. Noteren we P voor het predikaat "is strikt groter dan nul", of nog $P(x)$ voor het predikaat "$x > 0$", dan noemen we x een *objectvariabele* en P de *predikaatvariabele*.

Een predikaat kan afhangen van verschillende **argumenten** of **parameters**. Noteren we bijvoorbeeld met $R(x, y)$ het predikaat $x + y = 3$. Het aantal argumenten van een predikaat wordt de **ariteit** of *plaatsigheid* genoemd. Uit het bovenstaand voorbeeld heeft P ariteit 1 en het is dus een *unair* predikaat. Het predikaat R is dan *binair* of *tweeplaatsig*, maar men maakt gemakkelijk *ternaire*, *quaternaire* en meerplaatsige predikaten. Proposities kunnen we opvatten als predikaten met ariteit 0.

De eenvoudigste manier om van een predikaat een propositie te maken, is door het *invullen* van een object uit het universum in het predikaat. Zo krijgt men een uitspraak met betekenis, die waar of vals kan zijn. Bijvoorbeeld, de proposities $R(-1, 4)$, $R(\pi, 3 - \pi)$ en $P(\frac{1}{2})$ zijn waar, terwijl de propositie $P(0)$ vals is.

Er is nog een andere manier om een predikaat te bewerken tot een propositie, namelijk door de toevoeging van *kwantoren*.

1.2.2 De existentiële en universele kwantor

De **existentiële kwantor** is het symbool

$$\exists x$$

dat we lezen als

Er bestaat een x zodanig dat ...

Voor een unair predikaat P is de uitdrukking

$$\exists x : P(x)$$

een *propositie* die de *existentiële kwantificatie* van P genoemd wordt. Ze heeft de betekenis "Er bestaat een element x in het universum waarvoor geldt dat $P(x)$ waar is".

De **universele kwantor** is het symbool

$$\forall x$$

waarmee bedoeld wordt

$$\text{Voor alle } x \text{ geldt dat } \ldots$$

Voor een unair predikaat P is de uitdrukking

$$\forall x : P(x)$$

een *propositie* die de *universele kwantificatie* van P genoemd wordt. Ze heeft de betekenis "$P(x)$ is waar voor alle waarden van x in het universum".

Hoe de kwantor en het predikaat waarop ze toegepast wordt, notationeel gescheiden worden, kan variëren van auteur tot auteur. De volgende drie notaties komen vaak voor.

$$\forall x : P(x) \qquad (\forall x)(P(x)) \qquad \forall x P(x)$$

De meeste uitspraken in de wiskunde hebben combinaties van beide soorten kwantoren. Men zal snel kunnen vaststellen dat de volgorde waarin kwantoren voorkomen van het grootste belang is!

Bereik van een kwantor

Het **bereik** van een kwantor is de kwantor zelf en dat deel van de zin waarop hij van toepassing is. In de voorbeelden hieronder is het bereik van de kwantoren onderlijnd en stellen de hoofdletters predikaten voor.

$$\underline{\forall x[P(x) \Rightarrow Q(x)]} \wedge (R(x) \Rightarrow S(y))$$
$$\underline{\exists x \left[\underline{\forall y[(P(x) \wedge Q(y)) \Rightarrow R(y)]} \wedge S(x)\right]}$$

1.2.3 Kwantificatiedomein

In de wiskunde doet men vaak uitspraken die geschreven kunnen worden met kwantoren, zoals

$$\text{De vergelijking } x^2 + 2x + 1 = 0 \text{ heeft een reële wortel.}$$
$$\sqrt{2} \text{ is een rationaal getal.}$$

We kunnen deze proposities herschrijven zodat hun aard duidelijker wordt:

$$\textit{Er bestaat} \text{ een reëel getal } x \text{ zodat } x^2 + 2x + 1 = 0.$$
$$\textit{Er bestaan} \text{ gehele getallen } p \text{ en } q \text{ zodat } \sqrt{2} = p/q.$$

Dit wordt dan, in symbolen

$$(\exists x)(x^2 + 2x + 1 = 0)$$
$$(\exists p)(\exists q)(\sqrt{2} = p/q)$$

Door enkel $(\exists x)$ te noteren, zouden we de specificatie van het soort objecten dat bestaat (een reëel getal, gehele getallen) verliezen, dus vaak wordt de kwantornotatie aangepast om de aard van het object te specifiëren. De bovenstaande voorbeelden vertalen zich dan als

$$(\exists x \in \mathbb{R})(x^2 + 2x + 1 = 0)$$
$$(\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})(\sqrt{2} = p/q)$$

Deze bijvoegingen $\mathbb{R}$ en $\mathbb{Z}$ zijn verzamelingen, waarover de kwantor *loopt*. Deze verzameling waarover gekwantificeerd wordt, wordt het *kwantificatiedomein* genoemd. Met een kwantor is *altijd* een kwantificatiedomein geassocieerd. Staat die niet expliciet aangegeven, dan wordt verstaan dat die duidelijk is uit de context — in de reële analyse is dat meestal $\mathbb{R}$, in de getaltheorie vaak $\mathbb{Z}$. Om te illustreren hoe belangrijk het kan zijn om het kwantificatiedomein te vermelden, beschouw de volgende uitspraken.

$$(\forall x : x > 2) \qquad \text{en} \qquad (\forall x : x \geq 3)$$

Deze beweringen zijn equivalent als het kwantificatiedomein $\mathbb{Z}$ is, maar helemaal niet als het domein $\mathbb{R}$ is.

Een herhaling van gelijke kwantoren wordt meestal afgekort, zoals de laatste tot $(\exists p, q \in \mathbb{Z})$.

Kwantificatie over deeldomeinen

Vaak willen we in de loop van een redenering een kwantor beperken tot een bepaalde deelverzameling. We zullen in zo'n geval de kwantornotatie wijzigen tot

$$(\forall x \in A)(P(x)) \qquad \text{en} \qquad (\exists x \in A)(P(x)),$$

waarbij A een *deelverzameling* is van het domein. We zullen deze symbolische uitdrukkingen gebruiken als een afkorting voor de uitspraken

$$(\forall x)(A(x) \Rightarrow P(x)) \qquad \text{en} \qquad (\exists x)(A(x) \wedge P(x))$$

waarbij $A(x)$ het predikaat is dat zegt dat x tot de collectie A behoort. In de praktijk zullen we dit schrijven als $x \in A$, maar meer hierover in hoofdstuk 2.

Om dat te plausibiliseren, neem bijvoorbeeld als domein de collectie van alle dieren. Zij $L(x)$ het predikaat "x is een luipaard" en $V(x)$ het predikaat "x heeft vlekken". Dan kan de zin "Alle luipaarden hebben vlekken" geschreven worden als

$$(\forall x)(L(x) \Rightarrow V(x))$$

Inderdaad, "Voor alle dieren geldt dat, als het een luipaard is, dan heeft het vlekken" is een eerder plompe uitdrukking die equivalent is met de bewering dat alle luipaarden gevlekt zijn. Als $P(x)$ het predikaat "x is een paard" is, dan is de zin "Er bestaat een paard met vlekken" equivalent met

$$(\exists x)(P(x) \wedge V(x))$$

Inderdaad: "Er is een dier met de eigenschap dat het een paard is *en* dat het vlekken heeft".

Men merke op dat kwantificatie over deeldomeinen naargelang de kwantor dus een ander connectief vergt. Vergelijk bovenstaande (ware) uitspraken maar eens met de uitspraken

$$(\forall x)(L(x) \wedge V(x)) \qquad \text{en} \qquad (\exists x)(P(x) \Rightarrow V(x)).$$

De eerste zegt dat voor alle dieren x, x zowel een luipaard is als vlekken heeft. Dit is duidelijk vals, om te beginnen zijn al niet alle dieren luipaarden. De tweede zin zegt dat er een dier bestaat zodat, als het een paard is, het dan vlekken heeft. Dit zegt al niet veel interessants, en al zeker niet dat er een gevlekt paard bestaat.

1.2.4 Eigenschappen en taalgebruik bij kwantoren

Negatie van kwantoren

In analyse en andere delen van de wiskunde is het vaak belangrijk om uitspraken met kwantoren te kunnen ontkennen. Dat kan natuurlijk door een

$\neg$ ervoor te zetten, maar als negatie van een uitspraak willen we meestal een *positieve* uitspraak, waarbij geen negatiesymbool meer voorkomt of waarin de negatiesymbolen zo ver mogelijk *in* de uitspraak zitten.

We onderzoeken wat de logische ontkenning is van de uitspraak $\forall x A(x)$, voor een predikaat $A(x)$.

Stel eerst dat

$$\neg(\forall x A(x))$$

geldt. Dan, als het niet het geval is dat alle x voldoen aan $A(x)$, dan moet er minstens één x zijn die niet voldoet aan $A(x)$, dus

$$\exists x(\neg A(x)).$$

Omgekeerd, als dit laatste waar is, en er dus een x bestaat waarvoor $A(x)$ misloopt, dan kan mag het niet waar zijn dat, voor alle $x : A(x)$ geldt, of dus $\neg(\forall x A(x))$.

We vinden dus dat de negatie van proposities met kwantoren voldoet aan de volgende logische equivalenties — de tweede equivalentie is een oefening, analoog aan de voorgaande.

$$\begin{aligned} \neg\ \forall x P(x) &\iff \exists x[\neg P(x)] \\ \neg\ \exists x P(x) &\iff \forall x[\neg P(x)] \\ \text{en dus ook } \neg\ (\forall x \exists y \forall z A(x,y,z)) &\iff \exists x \forall y \exists z[\neg A(x,y,z)]. \end{aligned}$$

Kwantoren, conjuncties en disjuncties

Oplettendheid is geboden wanneer kwantoren met *en* en *of* in contact komen. De kwantificatie van een conjunctie is over het algemeen *niet equivalent* met de conjunctie van de gekwantificeerde uitspraken. We illustreren dit met een voorbeeld. Zij $E(x)$ het predikaat "x is even" en $O(x)$ het predikaat "x is oneven". Welke van de volgende uitspraken, met kwantificatiedomein $\mathbb{Z}$, zijn dan waar en welke vals?

$$\begin{array}{ll} \forall x\ (E(x) \vee O(x)) & \exists x\ (E(x) \wedge O(x)) \\ (\forall x E(x))\ \vee\ (\forall x O(x)) & (\exists x E(x))\ \wedge\ (\exists x O(x)) \end{array}$$

Indien het universum een eindige verzameling $\{x_1, x_2, \ldots, x_n\}$ is, dan gelden de volgende logische equivalenties.

$$\begin{aligned} (\forall x)(P(x)) &\Leftrightarrow P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n) \\ (\exists x)(P(x)) &\Leftrightarrow P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n). \end{aligned} \tag{1.2}$$

Unieke existentie

Een kwantor die verder vaak nuttig is, is de *kwantor voor unieke existentie*, die genoteerd wordt als

$$\exists!$$

en gelezen als "Er bestaat een *unieke* x zodat ...". Deze kwantor kan gedefinieerd worden in termen van de andere, door

$$\exists!\, x \ : \ P(x)$$

te nemen als een afkorting voor

$$\exists x \ [P(x) \ \wedge \ \forall y(P(y) \Rightarrow y = x)]\,.$$

Impliciete kwantificatie

Op gevaar van verwarring af moeten we nog toegeven dat in de wiskundige praktijk de melding van universele kwantificatie soms weggelaten wordt. Uitspraken als

$$x \geq 0 \Rightarrow \sqrt{x} \geq 0$$

moeten dan begrepen worden als

$$(\forall x \in \mathbb{R})(x \geq 0 \Rightarrow \sqrt{x} \geq 0).$$

Dit staat bekend als *impliciete kwantificatie* en wordt enkel gebruikt indien de context duidelijk maakt dat de algebraïsche identiteit inderdaad dient gelezen te worden als *universeel gesloten*.

Triviaal voldaan

Soms is een implicatie $\phi \Rightarrow \psi$ zodanig dat het antecedent ϕ altijd vals is. In dat geval is $\phi \Rightarrow \psi$ dus sowieso waar, en we zeggen dat de implicatie **triviaal voldaan** is, of we spreken van een *ledige implicatie*.

Een uitspraak als

$$\forall x \in A : P(x), \quad \text{ of dus } \quad \forall x : x \in A \Rightarrow P(x)$$

zal dan ook triviaal voldaan zijn als de verzameling A ledig is, want dan is voor alle objecten x uit het universum het antecedent $x \in A$ vals, wat de implicatie voor elke x ledig maakt.

In het Engels wordt dit fenomeen *vacuous truth* genoemd, een uitspraak is dan *vacuously true*.

1.2.5 Vrije en gebonden variabelen

In de predikaatlogica worden *variabelen* gebruikt, doorgaans voorgesteld door letters uit het einde van het alfabet. Het zijn symbolen die willekeurige objecten kunnen vertegenwoordigen en die zelf geen informatie in zich dragen. Er is echter een belangrijk onderscheid in het voorkomen van variabelen.

In zinnen zoals $x^2 - 1 = (x-1)(+1)$ of "x studeert wiskunde aan de UGent" komt een variabele x voor, met de eigenschap dat als we x vervangen door een object uit het domein, we dan een (ware of valse) propositie krijgen, zoals $8^2 - 1 = (8-1)(8+1)$. Deze x is dus een notatie die de plaats(en) in de uitdrukking specifieert waar men iets kan invullen, als ware het een wildcard die staat voor een ongespecifieerd object. In zo'n geval noemen we x een **vrije variabele**.

In de zin $(\exists x \in \mathbb{N})(x > 25)$ komt de variabele x niet vrij voor. Immers, de tekenreeks $(\exists 5 \in \mathbb{N})(5 > 25)$ is zelfs geen uitdrukking waaraan we betekenis zouden kunnen geven. We zeggen dat de variabele x hier een **gebonden variabele** is, omdat ze gebonden wordt door de kwantor $\exists x$.

Kwantoren zijn niet de enige symbolen die variabelen kunnen binden. In de volgende vijf uitdrukkingen komen de letters i, j, k, x, y, z en c gebonden voor, terwijl n, a en b vrij voorkomen.

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

$$\int_0^{\sqrt{3}} ax^2 dx = \sqrt{3}a$$

$$\{x \in \mathbb{R} \mid x + 1 = x\} = \varnothing$$

$$\forall y \in \mathbb{R}, \exists z \in \mathbb{R} : \prod_{j=0}^{\infty} \left(1 + \frac{z}{j}\right) > y$$

$$\forall k \in \mathbb{N}, \forall c \in \mathbb{N} : k > 2 \Rightarrow a^k + b^k \neq c^k$$

De precieze letters van de gebonden variabelen spelen geen rol van betekenis in de uitspraak. Het zijn *dummyvariabelen*, die je even goed door een andere, in die context nog niet gebruikte letter zou kunnen vervangen zonder de

waarheidswaarde van de uitspraak te veranderen. Bijvoorbeeld:

$$\sum_{i=0}^{n} 2^i = \sum_{k=0}^{n} 2^k$$

$$\forall y \in \mathbb{R}, \exists z \in \mathbb{R} : \prod_{j=0}^{\infty} \left(1 + \frac{z}{j}\right) > y \Leftrightarrow \forall z \in \mathbb{R}, \exists x \in \mathbb{R} : \prod_{m=0}^{\infty} \left(1 + \frac{x}{m}\right) > z$$

Gebonden variabelen lopen over een domein, een verzameling waarin ze verondersteld worden waarden te kunnen aannemen — het kwantificatiedomein voor kwantoren is hier een specifiek geval van. Bijvoorbeeld, in de eerste lijn hierboven loopt i over de verzameling $\{0, \ldots, n\}$. Dit fenomeen laat ons toe om substituties te doen in de gebonden variabelen. Stellen we bijvoorbeeld $j = i + 1$, dan is $i = j - 1$. Als $i = 0$, dan is $j = 1$. Als $i = n$, dan is $j = n + 1$. Zo kunnen we deze som herschrijven:

$$\sum_{i=0}^{n} 2^i = \sum_{j=1}^{n+1} 2^{j-1}.$$

Substitutie in de integratieveranderlijke is op hetzelfde principe gebaseerd.

Hoewel het a priori is toegelaten om elke letter te gebruiken voor een substitutie, is er een wiskundige folklore waar letters als i, j, k, l, m, n meestal gebruikt worden als gebonden variabelen om natuurlijke getallen voor te stellen en x, y, z om reële getallen mee voor te stellen.

Een grondiger discussie over vrije en gebonden variabelen stellen we uit tot *Wiskundige logica I*.

1.3 Bewijzen

Hoewel de wiskundige logica een interessante discipline is op zichzelf, is dat niet de reden waarom ze in deze cursus staat. Dat is omdat logica ten grondslag ligt aan één van de meest fundamentele aspecten van de wiskunde: *bewijzen*.

In tegenstelling tot empirische wetenschappen, leidt de wiskunde geen waarheden af door het experiment of door zintuiglijke vaststelling. Ze leidt nieuwe waarheden uit oude waarheden af door logische redeneringen. De logisch geldige argumentatie die de waarheid vestigt van een bepaalde uitspraak, wordt een *bewijs* genoemd en die bewezen uitspraak wordt dan een *stelling*. Een

uitspraak die geloofd wordt waar te zijn, maar waarvan nog geen bewijs werd gevonden, wordt een *vermoeden* genoemd. Sinds de tijd van Euclides vormen stellingen en hun bewijzen het format waarin de wiskunde overgeleverd wordt, als waren het getuigen van redeneringen.

Redeneren is wat wiskundigen doen. Het begrijpen, verifiëren en zelf bedenken van nieuwe bewijzen is dan ook een belangrijke competentie voor elke wiskundige. Dat neemt niet weg dat het opstellen van een goed onderbouwde en overtuigende bewijsvoering best moeilijk kan zijn.

Een bewijs is een correcte toepassing van de logische principes uit de propositie- en predikaatlogica op wiskundige uitspraken. Formeel gezien is een bewijs een eindige rij van zinnen, waarvan elke zin ofwel een axioma of definitie is, ofwel volgt uit de vorige zinnen door toepassingen van een logische afleidingsregel. In de praktijk wordt elke leesbare tekst, die door wiskundigen aanvaard wordt als een voldoende argumentatie voor een bepaalde uitspraak, aanzien als een bewijs. Het is niet nodig om een bewijs neer te pennen als zo'n rij van symbolische zinnen — het is voldoende dat het *in principe* mogelijk zou zijn om de tekst zonder moeite om te zetten in een *formeel bewijs*. In de *bewijstheorie*, een tak van de wiskundige logica, worden deze formele bewijzen als wiskundige objecten bestudeerd en *zelf* geanalyseerd door middel van wiskundige technieken.

Er zijn vele soorten bewijzen. Het doel hier is om er enkele van te vermelden en te zien hoe ze gerechtvaardigd worden door tautologieën uit de logica.

1.3.1 Een implicatie rechtstreeks bewijzen

Stel dat we de waarheid willen vestigen van een implicatie $\phi \Rightarrow \psi$. Daar die zeker zal voldaan zijn wanneer ϕ vals is, moeten we enkel het geval beschouwen waarin ϕ waar is. We mogen dus ϕ *veronderstellen* in de redenering die de waarheid van ψ aantoont. Een voorbeeld:

Lemma 1.2

Als p even is, dan is p^2 ook even.

Bewijs. Als p even is, dan bestaat er een q zodat $p = 2q$. Dan is $p^2 = 4q^2 = 2 \cdot (2q^2)$, wat ook een even getal is. □

1.3.2 Bewijs door contrapositie

Omdat we de logische equivalentie tussen een implicatie en zijn contrapositieve

$$(\phi \Rightarrow \psi) \quad \Longleftrightarrow \quad (\neg\psi \Rightarrow \neg\phi)$$

hebben, kunnen we een implicatie ook bewijzen door zijn contrapositieve aan te tonen. In dat geval vertrekt men van de veronderstelling dat ψ niet waar is, dus van $\neg\psi$, en bewijst men dat dit impliceert dat ϕ niet waar is, dus $\neg\phi$. Dit heet een **bewijs door contrapositie**.

Lemma 1.3

Als p^2 even is, dan is p ook even.

Bewijs. Om deze implicatie te bewijzen, zullen we haar contrapositieve

als p oneven is, dan is p^2 ook oneven

bewijzen: als $p = 2k + 1$, dan is $p^2 = 4k^2 + 4k + 1$, wat een oneven getal is. □

1.3.3 Bewijs uit het ongerijmde

Eén van de meest gebruikte bewijstechnieken is het zogenaamde *bewijs uit het ongerijmde*, ofte *reductio ad absurdum*. Dit soort bewijs steunt op de logische equivalentie

$$\psi \quad \Longleftrightarrow \quad (\neg\psi \Rightarrow \bot).$$

Om een uitspraak ϕ te bewijzen wordt eerst *verondersteld* dat ϕ niet waar is en vervolgens door logische redeneringen een duidelijk onware uitspraak afgeleid. Daar de conclusie vals is, moet de fout wel liggen bij onze aanname $\neg\phi$, maar als $\neg\phi$ vals is, moet ϕ waar zijn.

Bij het bewijzen van een implicatie mogen volgens hetzelfde idee zowel de hypothesen van de implicatie, als de negatie van de conclusie gebruikt worden om een strijdigheid af te leiden. Dit steunt op de logische equivalentie

$$(\phi \Rightarrow \psi) \quad \Longleftrightarrow \quad (\phi \wedge \neg\psi) \Rightarrow \bot.$$

Deze bewijstechniek wordt vaak gebruikt als men niet goed weet waar te beginnen, omdat dan meer veronderstellingen beschikbaar worden. Bewijst

men uiteindelijk toch ψ (wellicht zonder $\neg\psi$ te gebruiken), dan heeft men de implicatie eigenlijk rechtstreeks aangetoond; bewijst men uiteindelijk $\neg\phi$, dan heeft men eigenlijk een bewijs door contrapositie gegeven, maar beiden kunnen ook opgevat worden als een bewijs uit het ongerijmde, daar zowel ψ als $\neg\phi$ uitkomsten zijn die in strijd zijn met de assumpties.

Het schoolvoorbeeld van het bewijs uit het ongerijmde is het volgende resultaat

Stelling 1.4

$\sqrt{2}$ is irrationaal.

Bewijs. Veronderstel, uit het ongerijmde, dat $\sqrt{2}$ een rationaal getal is. Dan bestaan er natuurlijke getallen p en q, onderling ondeelbaar, zodat

$$\sqrt{2} = p/q.$$

Kwadrateren we beide leden en herschikken we, dan krijgen we

$$p^2 = 2q^2.$$

Dat betekent dat p^2 even is en bijgevolg ook p even moet zijn wegens Lemma 1.3. Dus er bestaat een geheel getal r met $p = 2r$. Substitueren we dit in bovenstaande uitdrukking, dan vinden we

$$4r^2 = 2q^2$$

of dus

$$2r^2 = q^2.$$

Bijgevolg is q^2 even. Dit kan wederom enkel als q zelf even is. Maar ook p is even en p en q waren onderling ondeelbaar. Dit is een strijdigheid. Bijgevolg moet onze aanname dat $\sqrt{2}$ rationaal was, vals zijn. Met andere woorden, $\sqrt{2}$ is irrationaal, en dat is wat we moesten bewijzen. □

1.3.4 Existentiële uitspraken bewijzen

Om de existentiële uitspraak

$$\exists x : A(x)$$

te bewijzen, is het genoeg om één bijzondere x te vinden waarvoor $A(x)$ waar is. Als we bijvoorbeeld willen bewijzen

Er bestaat een irrationaal getal

dan volstaat het om bovenstaande stelling aan te halen. Niet alleen vertelt dit ons dat irrationale getallen bestaan, het verschaft ons meteen een concreet voorbeeld, dat een *existentiële getuige* genoemd wordt van de existentiële uitspraak.

Niettemin is het niet nodig dat een existentiebewijs altijd een speciaal object identificeert dat dienstdoet als existentiële getuige. Er zijn vele gevallen in de wiskunde waar men weet dat een reëel getal dat aan een voorwaarde voldoet, bestaat, zonder te weten hoe x eruit ziet, of zelfs zonder te weten of x positief of negatief is. Hier een klassiek voorbeeld.

Stelling 1.5

Er bestaan irrationale getallen a en b zodat a^b rationaal is.

Bewijs. Door stelling 1.4 weten we dat $\sqrt{2}$ irrationaal is. Beschouw nu het getal $r = \sqrt{2}^{\sqrt{2}}$. Als r rationaal is, dan kunnen we $a = \sqrt{2}$ en $b = \sqrt{2}$ nemen en we zijn klaar. Als echter r irrationaal is, dan kunnen we $a = r$ en $b = \sqrt{2}$ nemen, want

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2.$$

□

Opmerkelijk aan dit bewijs is dat het ons niet zegt welk koppel getallen a, b voldoet aan de eisen van de stelling.[3]

In dit geval weten we wel dat het daadwerkelijke paar één van deze twee paren is. Maar vele bewijzen van stellingen in meer geavanceerde wiskundegebieden geven niet eens een eindige lijst van mogelijke existentiële getuigen: ze leveren enkel de conclusie dat een object met een bepaalde eigenschap bestaat. Dergelijke bewijzen worden *niet-constructieve* bewijzen genoemd. Heel vaak zijn het bewijzen uit het ongerijmde.

[3]Een aanzienlijk geraffineerder bewijs zou aantonen dat het getal $r = \sqrt{2}^{\sqrt{2}}$ inderdaad irrationaal is, dus het tweede getallenkoppel voldoet aan de eisen. Maar het bewijs hier toont dit niet aan.

1.3.5 Universele uitspraken bewijzen

Tot slot kijken we hoe we een uitspraak van de vorm

$$\forall x : A(x)$$

kunnen bewijzen. De meest rechtstreekse manier is om een *willekeurige* x te beschouwen en aan te tonen dat die moet voldoen aan $A(x)$. Stel bijvoorbeeld dat we de uitspraak

$$\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : m > n^2$$

willen bewijzen. We kunnen dit als volgt doen:

Bewijs. Zij n een willekeurig natuurlijk getal. Dan is ook n^2 een natuurlijk getal. En ook $n^2 + 1$ is dan een natuurlijk getal. Daar $m = n^2 + 1 > n^2$, hebben we dat

$$\exists m \in \mathbb{N} : m > n^2.$$

Omdat onze n willekeurig was, is de uitspraak bewezen. □

Dit bewijs is geldig, omdat de oorspronkelijke n, die we hebben beschouwd, *willekeurig* was. We hebben niets gezegd of verondersteld over n — het kon elk natuurlijk getal zijn. Om die reden is onze redenering geldig *voor alle* n in $\mathbb{N}$ en bewijst het de universele uitspraak.

Dit is niet hetzelfde als het *kiezen* van een *specifieke* n. Als we op een random manier pakweg $n = 37$ hadden gekozen, dan zou ons bewijs niet geldig geweest zijn, hoe willekeurig we die n ook hadden gekozen. Veronderstel bijvoorbeeld dat we willen bewijzen

$$\forall n \in \mathbb{N} : n^2 = 81.$$

Door willekeurig een specifieke n te kiezen, zouden we toevallig $n = 9$ kunnen kiezen. Dat bewijst natuurlijk de uitspraak niet, want onze keuze was een *willekeurige keuze* voor een *specifieke* n en niet voor een *willekeurige* n.

In de praktijk betekent dit dat, telkens als we een bewijs starten met "Zij n willekeurig", we het symbool n dan doorheen het ganse bewijs kunnen gebruiken en onderstellen dat de waarde van n constant blijft doorheen het bewijs, maar we maken absoluut geen restrictie op wat de waarde van n is.

Er zijn andere mogelijkheden om universele uitspraken $\forall x : A(x)$ te bewijzen. Als alle andere aanpakken falen, kan men proberen bij wijze van contradictie te vertrekken van de onderstelling $\neg\forall x : A(x)$, of dus $\exists x : \neg A(x)$. Nu heb je een vertrekpunt. De moeilijkheid is echter het eindpunt vinden (de tegenspraak).

1.3.6 Bewijs door inductie

Om een bewering van de vorm

$$\forall n \in \mathbb{N} : A(n)$$

te bewijzen, waarbij de kwantificatie over alle natuurlijke getallen loopt, is het mogelijk om de volgende twee uitspraken te bewijzen:

- $A(0)$, dat wil zeggen, de bewering is waar voor $n = 0$
- $\forall n \in \mathbb{N} : (A(n) \Rightarrow A(n+1))$, dat wil zeggen, voor een willekeurige n: als de bewering waar is voor n, dan ook voor $n + 1$

Dat daaruit de geldigheid volgt van $\forall n \in \mathbb{N} : A(n)$, kan men als volgt beredeneren: de geldigheid van $A(0)$ wordt expliciet bewezen. Uit het bijzonder geval $A(0) \Rightarrow A(1)$ volgt nu ook $A(1)$. Door $A(1) \Rightarrow A(2)$ is ook $A(2)$ geldig, enzovoort doorheen de natuurlijke getallen. Voor elk natuurlijk getal n wordt de geldigheid van $A(n)$ gevestigd door een eindig aantal toepassingen van $A(i) \Rightarrow A(i+1)$. De uitspraak dat $\forall n \in \mathbb{N} : A(n)$ uit deze twee beweringen volgt, m.a.w. dat

$$[A(0) \wedge \forall n \in \mathbb{N}\,(A(n) \Rightarrow A(n+1))] \quad \Rightarrow \quad \forall n \in \mathbb{N} : A(n) \tag{1.3}$$

staat bekend als het **principe van wiskundige inductie**. Men vergelijkt dit principe soms met het domino-effect. Elke dominosteen die omvalt laat z'n opvolger omvallen. Valt de eerste steen om, dan zullen alle stenen omvallen.

Het inductieprincipe is een zeer belangrijk principe, omdat het kan gebruikt worden voor bewijzen. Een bewijs dat steunt op het inductieprincipe, is dan een *inductiebewijs* of een **bewijs door inductie**. Het wordt gekenmerkt door de volgende drie onderdelen:

- Er wordt duidelijk gezegd dat de methode van inductie gebruikt wordt (op welke variabele).
- Er wordt bewezen dat de bewering is waar voor $n = 0$ (**inductiebasis**).
- Er wordt bewezen voor een willekeurige n: als de bewering waar is voor n, dan ook voor $n + 1$ (**inductiestap**). Dit is doorgaans het moeilijke deel.

De inductiestap is een implicatie. In het bewijs ervan mag dus, om $A(n+1)$ te bewijzen, het antecedent $A(n)$ als assumptie gebruikt worden. Deze $A(n)$ wordt de **inductiehypothese** genoemd.

Inductiebewijzen voor uitspraken van de vorm $\forall n \in \mathbb{N} : A(n)$ zijn meestal eenvoudiger dan rechtstreekse bewijzen (zij n willekeurig, ...). Bij een inductiebewijs kan men namelijk gebruik maken van het vorige geval van n, wat toelaat om $A(n)$ te *reduceren* tot $A(n-1)$. Dit is doorgaans gemakkelijker dan $A(n)$ uit het niets bewijzen. Inductiebewijzen komen vaak voor, bijvoorbeeld in het geval dat n een dimensie van een bepaalde algebraïsche of meetkundige structuur is.

Het is mogelijk dat de uitspraak $A(n)$ zinloos of vals is voor $n = 0$, of erger, voor alle $n < n_0$ voor een zekere $n_0 \in \mathbb{N} \setminus \{0\}$. In dat geval is de uitspraak die men wenst te bewijzen van de vorm

$$\forall n \geq n_0 : A(n)$$

Hier bestaat de inductiebasis uit het bewijzen van $A(n_0)$, en de inductiestap uit het bewijzen van

$$\forall n \geq n_0 : (A(n) \Rightarrow A(n+1))$$

We gebruiken deze bewijsmethode voor een eenvoudig voorbeeld. We bewijzen dat de volgende formule geldt voor alle $n \in \mathbb{N} \setminus \{0\}$:

$$\sum_{i=1}^{n} (2i-1) = n^2.$$

Bewijs. We bewijzen dit door inductie op n. De formule is zeker correct voor $n = 1$, aangezien $\sum_{i=1}^{1}(2-1) = 1^2$. Zij nu k een willekeurig natuurlijk getal groter dan of gelijk aan 1 en veronderstel dat de formule correct is voor k, met andere woorden dat

$$\sum_{i=1}^{k} (2i-1) = k^2.$$

Dan is de formule ook correct voor $k+1$, want

$$\begin{aligned}\sum_{i=1}^{k+1} (2i-1) &= \sum_{i=1}^{k} (2i-1) + 2k + 1 \\ &\overset{\text{IH}}{=} k^2 + 2k + 1 \\ &= (k+1)^2,\end{aligned}$$

waarbij we in de middelste gelijkheid de inductiehypothese hebben gebruikt. Dus wegens het principe van inductie is $\sum_{i=1}^{n}(2i-1) = n^2$ geldig voor alle $n \in \mathbb{N} \setminus \{0\}$. □

1.3.7 Bewijs door sterke inductie

Een andere variant op het bewijs door inductie is deze, waarbij als inductiehypothese niet wordt aangenomen dat de uitdrukking waar is voor enkel *de vorige waarde van n*, maar voor *alle waarden kleiner dan n*. Men spreekt dan over een bewijs door **sterke inductie**. Het wordt gerechtvaardigd door het *sterk inductieprincipe*:

$$[A(0) \wedge \forall n \in \mathbb{N}\,((\forall m < n : A(m)) \Rightarrow A(n+1))] \quad \Rightarrow \quad \forall n \in \mathbb{N} : A(n)$$

De vorige bewijsmethodes hebben we gerechtvaardigd door tautologieën in de propositielogica of redeneringen in de predikaatlogica. Een echt bewijs van correctheid van de bewijstechniek "bewijs door inductie" stellen we nog even uit tot hoofdstuk 2, in Gevolg 2.31.

1.4 De axiomatische methode

De notie van *waarheid* er is er één die vele generaties filosofen heeft bezig-gehouden en dat allicht zal blijven doen. Het is niet de bedoeling om de filosofische toer op te gaan, maar we moeten wel eens stilstaan bij wat een wiskundige bedoelt met de bewering dat een bepaalde wiskundige uitspraak *waar* is (of onwaar). Dit vergt enige vertrouwdheid met de historische ontwikkeling van de wiskunde.

Wiskundige concepten vinden hun oorsprong in de alledaagse wereld rondom ons: de natuurlijke getallen spruiten voort uit onze wens om collecties objecten te kunnen tellen, meetkunde en driehoeksmeetkunde werd gemotiveerd door de nood aan correcte navigatie, enzovoort. *Waar* betekende in het beginstadium gewoon *experimenteel vaststelbaar*. De waarheid van de uitspraak

$$2 + 1 = 3$$

kon worden aangetoond door twee appels en een meloen te nemen en vast te stellen dat dit drie objecten in totaal waren. Maar wat met de volgende uitspraak?

$$1\,000\,000\,000 + 5 = 1\,000\,000\,005$$

We kunnen het erover eens zijn dat deze even waar is als de vorige, maar het is niet aan de orde om dit te verifiëren door te tellen. Waarom stemmen we er dan zo snel mee in dat dit deze gelijkheid geldig is?

Hoewel de concepten van natuurlijke getallen en hun optelling voortvloeien uit de alledaagse ervaring, zijn het enkel geïdealiseerde, abstracte concepten, die leven in onze verbeelding. Hun eigenschappen en gedrag zijn *gepostuleerd* (door ons) zodat ze zouden overeenkomen met de ervaring in de natuur. De gelijkheid $1\,000\,000\,000+5 = 1\,000\,000\,005$ is *waar* omdat ze een gevolg is van de eigenschappen die we aangenomen hebben voor de natuurlijke getallen. Optelling van natuurlijke getallen is misschien zo vertrouwd dat het raar is om er op deze manier over te denken, maar hetzelfde gebeurt voor pakweg de complexe getallen. De gelijkheid

$$(1+i)^2 = 2i$$

is *waar* omdat men kan deduceren dat ze een gevolg is van de eigenschappen van de complexe getallen die, in feite net zoals de natuurlijke getallen, abstracte concepten zijn.

Dit brengt ons tot de ware aard van zuivere wiskunde. In elke discipline, van de optelling van natuurlijke getallen tot de theorie van lineair algebraïsche groepen, starten we in principe met een collectie *postulaten* of *axioma's*, die de eigenschappen beschrijven die de objecten die we wensen te bestuderen, zouden moeten hebben. Deze axioma's kunnen gemotiveerd zijn door observatie of ervaring of door ons af te vragen welke eigenschappen onze structuur behoort te hebben. Eens de axioma's zijn vastgelegd, betekent *waar* simpelweg *bewijsbaar van de axioma's*. De zuivere wiskunde begint pas hier: het afleiden van nieuwe waarheden uit de axioma's, op een onweerlegbare manier. Dat neemt niet weg dat het een zinvolle competentie is voor de wiskundige expert van een bepaalde wiskundige theorie, om te begrijpen hoe de axioma's zijn geënt op de realiteit en hun beperkingen te kennen in het modelleren van die realiteit. Bij het voorspellen op basis van statistische methodes, het modelleren van ecologische populaties of het prijzen van complexe financiële producten is dat soms zelfs van levensbelang!

In bijvoorbeeld *Lineaire Algebra en Analytische Meetkunde I*, eerste jaar bachelor wiskunde, worden de axioma's van een vectorruimte gepostuleerd en wordt de hele lineaire algebra, de studie van vectorruimten, opgebouwd vanuit enkel deze eigenschappen (en vele definities). Het is soms wat wennen aan deze manier van werken maar er zullen zonder twijfel nog vele vakken volgen met een axiomatische aanpak, van *Algebra* tot *Kwantummechanica*. In veel gevallen worden de axioma's echter niet uitdrukkelijk vermeld, zoals

bij de natuurlijke getallen (deze cursus) of zelfs in de reële analyse (Analyse I).

De kennis van de onderliggende axioma's is niet (altijd) nodig om een correct bewijs op te stellen. We herhalen dat een *bewijs* van een feit gewoon een logisch argument is *dat ons ervan overtuigt dat het feit waar is*. Het eerdere bewijs dat $\sqrt{2}$ irrationaal is, is geldig in deze zin. Toegegeven, het gebruikte verschillende eigenschappen van de natuurlijke getallen, die technisch gesproken enkel waar zijn omdat ze uit de axioma's volgen, maar die we allemaal kennen, dus het is niet nodig om terug te gaan naar de axioma's om dit na te gaan. Als vuistregel: laat je gezond verstand bepalen wat een bewijs is en wat niet. Na een tijd zou je geen problemen meer mogen hebben om uit te maken wat je wel of niet mag veronderstellen in een bepaald geval.

1.5 Wiskundige logica

Logica is de wetenschap van het redeneren. Wiskundige logica is de wetenschap van het wiskundig redeneren. Dit gebied van de wiskunde is eigenlijk pas in de twintigste eeuw echt ontstaan en is tegenwoordig één van de grotere deeldisciplines binnen de wiskunde geworden. Hier worden de toepassingen van formele logica in de wiskunde onderzocht en het gebied heeft nauwe verbanden met theoretische informatica, metawiskunde en filosofie. De wiskundige logica heeft bijgedragen tot en vindt haar motivatie in de studie van de grondslagen van de wiskunde, die begon aan het einde van de 19de eeuw met de ontwikkeling van axiomatische kaders voor meetkunde, rekenkunde en analyse.

In dit korte paragraafje proberen we een glimp van dit gebied te tonen, door de vier gebieden te schetsen waarin de wiskundige logica vandaag wordt onderverdeeld, door de intuïtief geïntroduceerde logica wat formeler in te voeren en door een blik te werpen op de stellingen van Gödel.

1.5.1 De vier deelgebieden van wiskundige logica

Over **verzamelingenleer** lees je alvast meer in het volgende hoofdstuk. Het is de plaats in de wiskunde waar vragen over oneindigheid gesteld worden. Het is een rijke theorie, geaxiomatiseerd door de axioma's van Zermelo en Fraenkel, samen met het keuzeaxioma, over o.a. kardinaalgetallen, welordeningen en ordinalen. De vraag welke kardinaalgetallen aanleiding geven tot

consistente wiskundige universa, is vandaag een belangrijk onderzoeksonderwerp. Zie ook het vak *Logica I*, derde jaar bachelor wiskunde.

Modeltheorie is de studie van wiskundige structuren (zoals groepen, vectorruimten, grafen...) door gebruik te maken van wiskundige logica. Modellen zijn structuren die voldoen aan bepaalde logische zinnen of axioma's, die dan samen een *theorie* vormen. Belangrijke resultaten zijn de compactheidsstelling, de stellingen van Löwenheim en Skolem, de eigenschap van kwantoreliminatie en de stelling van Morley.[4] Deze komen ook aan bod in het vak *Logica I*.

Berekenbaarheidstheorie of **recursietheorie** bestudeert de definieerbaarheid en berekenbaarheid van functies. Je kunt denken over berekenbaarheid van een functie op de natuurlijke getallen als *implementeerbaar op een computer*. In het bijzonder wordt de hiërarchische structuur van onberekenbare functies in graden van onberekenbaarheid bestudeerd. Zie ook de vakken *Logica II* en *Berekenbaarheid en complexiteit*.

Bewijstheorie is de studie van bewijzen als wiskundige objecten. Bewijstheoristen onderzoeken specifieke bewijzen en hun structuur, bijvoorbeeld als bewijsbomen, maar ook de bewijskracht van formele bewijssystemen. Zie ook de vakken *Bewijstheorie* en *Fasenovergangen in logica en combinatoriek*, master wiskunde.

1.5.2 Formele logica van eerste orde

In de voorbije paragrafen hebben we logica op een intuïtieve manier ingevoerd. Om logica meer formeel te introduceren, hebben we de notie nodig van een *formeel systeem*. Dat is een viertal, bestaande uit een *alfabet*, een *grammatica*, een verzameling *axioma's* en een verzameling *afleidingsregels*. Het alfabet is een eindige verzamelingen symbolen die aaneengezet kunnen worden om *formules* te vormen — dit zijn eindige rijen van symbolen. De grammatica bepaalt de *syntax* van de taal: het voorziet een procedure om uit te maken welke formules *goed gevormd* zijn en zegt hoe *goed gevormde formules* kunnen gemaakt worden uit symbolen uit het alfabet of kleinere goed gevormde formules. De axioma's vormen een verzameling van goed gevormde formules en de afleidingsregels zorgen dat van goed gevormde formules kan bepaald worden of ze kunnen gededuceerd worden uit de axioma's.

[4] Een theorie is κ-categorisch als elke twee modellen ervan van kardinaliteit κ isomorf zijn. De stelling van Morley (1965) zegt dat als een theorie categorisch is voor *een* overaftelbare kardinaliteit, dat ze dan categorisch is voor *alle* overaftelbare kardinaliteiten.

In een formeel systeem is er dus een notie van *bewijsbaarheid*. Alle bewijsbare formules vormen de *theorie* van het systeem. Als zowel een uitspraak en haar negatie bewijsbaar zijn, wordt het systeem *inconsistent* genoemd en *consistent* anders. Een theorie is *compleet* als ze van elke zin de zin zelf of haar negatie bevat. Een consistente theorie kan uitgebreid worden tot een complete theorie.

Een *logisch systeem* of *logica* is een formeel systeem, samen met een semantiek, die waarheidswaarden toekent aan goed gevormde zinnen uit het formeel systeem die geen vrije variabelen bevatten (*proposities*). Meestal heeft deze semantiek de vorm van een modeltheoretische interpretatiefunctie, waaraan een concrete wiskundige structuur (*model*) ten gronde ligt: uitspraken krijgen dan een waarheidswaarde naargelang hun betekenisvolle interpretatie in het model waar of vals is. In een logica is dus een notie van *waarheid* (namelijk: waar in de interpretatie). Een formeel systeem heet *vervulbaar* (satisfiable) als ze een model heeft, m.a.w. als er een interpretatie bestaat waaronder alle formules in de theorie waar zijn. Een uitspraak is *geldig* als ze waar is in elk model van de logica.

Een logica is *correct* als alle bewijsbare zinnen ook waar zijn. Een logica is *volledig* als alle ware zinnen ook bewijsbaar zijn. Als voor een bepaalde logica de definities van consistent en vervulbaar samenvallen, dan is deze logica volledig.

1.5.3 De stellingen van Gödel

Sinds 1931, door Kurt Gödel, weten we

- De propositielogica (nulde-ordelogica) is correct en volledig.
- De predikaatlogica (eerste-ordelogica) is correct en volledig. Equivalent, een eerste-ordetheorie is vervulbaar als en slechts als ze consistent is.
- Elk logisch systeem dat sterk genoeg is om de natuurlijke getallen te bevatten (noodzakelijk tweede-ordelogica), is niet compleet: er zijn altijd ware proposities die niet bewijsbaar zijn.
- Elk consistent logisch systeem dat sterk genoeg is om de natuurlijke getallen te bevatten, is niet in staat zijn eigen consistentie te bewijzen, m.a.w. de ware propositie *deze theorie is consistent* is zo'n onbewijsbare propositie.

De tweede stelling staat bekend als *Gödels volledigheidsstelling*. Ze wordt bewezen in *Logica I*. De derde en vierde stelling staan bekend als *Gödels onvolledigheidsstellingen*. Beide worden bewezen in *Berekenbaarheid en complexiteit*. Een beschouwing hierover vindt men op `http://prime.ugent.be/top10/1`.

Gödels onvolledigheidsstellingen zijn van groot belang in de logica en doen een uitspraak over hele omvang van de wiskunde. Ten eerste zullen er altijd uitspraken zijn over de natuurlijke getallen die niet kunnen bewezen worden. Ten tweede is het onmogelijk om de consistentie van een theorie te bewijzen vanuit zijn eigen axioma's. Dit betekent onder andere dat we niet in staat zijn om te bewijzen dat de grondslagen waarop de wiskunde gevest is, zoals de ZFC-verzamelingenleer, consistent zijn, *binnen dat systeem zelf*. Erger nog, niet alleen ZFC heeft deze onwenselijke eigenschap, ook elk ander systeem dat als grondslag van de wiskunde genomen wordt, moet ze hebben.

De consistentie van ZFC kan wel aangetoond worden als een oneindig ordinaalgetal bestaat, maar dat leeft zelf weer in een groter systeem, waarvoor een consistentiebewijs een nóg groter ordinaalgetal nodig heeft. Niettemin zijn bijna alle wiskundigen ervan overtuigd dat ZFC consistent is: mocht er een tegenspraak kunnen afgeleid worden, dan zou die al lang gevonden zijn door het werk van de vele wiskundigen die wereldwijd elke dag nieuwe wiskunde ontwikkelen.

Hoofdstuk

2 Verzamelingenleer

Verzamelingenleer is de wiskundige wetenschap van het oneindige. Ze bestudeert eigenschappen van verzamelingen, abstracte objecten waarvan het geheel van de moderne wiskunde doordrongen is. De taal van de verzamelingenleer is eenvoudig en voldoende universeel om bijna alle wiskundige concepten te formaliseren. Uit het vorige hoofdstuk leerden we logica, waardoor we kunnen werken met proposities en via logische gevolgtrekkingen stellingen uit axioma's bewijzen. We hadden echter nog geen universum van objecten waarover de kwantoren kunnen lopen of waarop de predikaten slaan. Die wereld van wiskundige objecten wordt ons gegeven door de verzamelingenleer. In die hoedanigheid vormen verzamelingenleer en predikaatlogica samen de ware grondslagen van de wiskunde.

In de opbouw van de verzamelingenleer zullen we een intuïtieve aanpak hanteren. Het voordeel is de begrijpelijkheid, die ons toelaat de nadruk te leggen op het ontwikkelen van een intuïtie over verzamelingen, die onmisbaar is voor een wiskundige. Deze aanpak is geschikt voor didactische doeleinden en wordt altijd gevolgd in introductorische bronnen over wiskunde — ze heeft dan ook een naam, namelijk *naïeve verzamelingenleer*.

Ondanks onze intuïtieve aanpak moet de wiskundige weten (eigenlijk: erop vertrouwen) dat haar redeneringen over verzamelingen in principe zouden kunnen geformaliseerd worden binnen een axiomatische theorie. Men kan namelijk de verzamelingenleer zien als een logisch systeem, dat buiten de taal en regels van de predikaatlogica beschikt over een extra symbool, namelijk "$\in$", en dat voldoet aan een lijst axioma's. Af en toe zullen we een knipoogje geven naar het meest gebruikte axiomasysteem van de verzamelingenleer, namelijk dat van Zermelo en Fraenkel, met het keuzeaxioma (**ZFC**).

Er wordt verwacht dat de lezer in dit hoofdstuk vertrouwd is met een basis wiskundige logica en bewijzen. Vele constructies in verzamelingenleer zijn immers herformuleringen van constructies in de logica. Bovendien begint het vaardig worden in bewijzen onvermijdelijk in de verzamelingenleer, de wereld van o.a. injecties en surjecties.

2.1 Verzamelingen

Centraal in de verzamelingenleer staat het begrip *verzameling*. Deze notie is zo primitief en basaal dat we ze niet zullen definiëren, maar enkel een informele beschrijving zullen geven: een **verzameling** is een goedgedefinieerde collectie van objecten. Verzamelingen kunnen objecten van uiteenlopende aard bevatten: mensen, fysieke objecten, getallen, ideeën ... of zelfs verzamelingen. De verzameling van π en jouw linkeroor is bijvoorbeeld een verzameling.

De objecten die *behoren tot* een verzameling noemen we **elementen**. We schrijven symbolisch

$$x \in A$$

om aan te duiden dat het object x een element is van de verzameling A en $x \notin A$ om aan te duiden dat dat niet zo is. De zin $x \in A$, voor een bepaald object x en een bepaalde verzameling A, is steeds een propositie: het is een uitspraak met betekenis, die eenduidig waar of vals is — wat niet wil zeggen dat we ook kunnen beslissen of de uitspraak waar is of niet. Dit maakt dat alle volgende definities, die steunen op deze "$\in$", betekenis zullen hebben.

2.1.1 Gelijkheid van verzamelingen, deelverzameling

Axioma van extensionaliteit

Twee verzamelingen zijn gelijk als ze dezelfde elementen hebben. Voor twee verzamelingen A en B geldt dus

$$A = B \iff \forall x\, (x \in A \Leftrightarrow x \in B)$$

Dit is het eerste axioma van ZFC en meteen de definitie van *gelijkheid* van verzamelingen. De definitie reflecteert de aard van een verzameling als een (ordeloze) collectie van objecten.

Definitie 2.1

De verzameling A is een **deelverzameling** van de verzameling B, genoteerd $A \subseteq B$, als elk element van A tot B behoort. Symbolisch

$$A \subseteq B \iff \forall x\, (x \in A \Rightarrow x \in B)$$

Uit deze twee definities volgt dat verzamelingen gelijk zijn als de één een deelverzameling is van de ander en vice versa:

$$A = B \quad \Longleftrightarrow \quad A \subseteq B \ \wedge B \subseteq A.$$

Als A een deelverzameling is van B, kan het gebeuren dat A en B samenvallen (en dus gelijk zijn wegens extensionaliteit). Als men wil stellen dat A een deelverzameling is van B en de mogelijkheid $A = B$ expliciet moet worden uitgesloten, zegt men dat A een *eigenlijke* of *strikte* of *echte* deelverzameling is van B en men noteert $A \subsetneq B$ of $A \subsetneqq B$ of zelfs $A \subsetneqq B$. Vaak wordt ook de notatie $\subset$ gebruikt, maar het gebruik daarvan is niet gestandaardiseerd: doorgaans wordt $\subsetneq$ bedoeld (naar analogie met $<$ voor getallen), maar afhankelijk van de auteur kan soms ook $\subseteq$ bedoeld worden (veralgemeend gebruik).

Soms zullen we symbolen uit de verzamelingenleer in hun gespiegelde vorm gebruiken zoals $A \ni x$ en $A \supseteq B$.

2.1.2 Opschrijven van verzamelingen

Er zijn essentieel twee verschillende mogelijkheden om een nieuwe verzameling op te schrijven. Als een verzameling weinig elementen heeft, kunnen we die oplijsten, door ze, gescheiden door komma's en omsloten door *accolades*, neer te schrijven, zoals bijvoorbeeld:

$$A = \{1, 2, 3, 6, 12, 15, 30\}$$

Door gebruik te maken van een beletselteken kunnen we die notatie uitbreiden tot grotere en zelfs oneindige verzamelingen, zoals

$$\{1, 2, 3, \ldots, n\} \qquad \text{of} \qquad \{2, 4, 6, \ldots, 2n, \ldots\}$$

waarbij men wel moeten opletten dat het duidelijk is hoe de auteur bedoelt dat de weggelaten elementen moeten aangevuld worden. Dit heet een definitie van een verzameling *door middel van opsomming*.

Over het algemeen worden verzamelingen echter best beschreven door de eigenschap die de verzameling definieert. De volgende verzameling is gedefinieerd *door middel van voorschrift*.

$$A = \{x \in \mathbb{N} : x \text{ is een deler van } 30\}$$

Het is natuurlijk belangrijk dat het kenmerkende predikaat eenduidig kan geïnterpreteerd worden en dit verkrijgen we door te eisen dat we enkel kijken

naar de objecten die aan de voorwaarde voldoen *en die al element zijn van een bepaalde verzameling*. Waarom dit erg belangrijk is, leggen we uit in paragraaf 2.9, op pagina 98.

Deze constructie is één van de vele mogelijkheden om uit een verzameling een nieuwe verzameling te maken. Het is het tweede van de negen axioma's van ZFC.

Axioma van specificatie / Axioma van separatie

Als A een verzameling is en P is een goed gedefinieerd predikaat op A, dan is de collectie van elementen van A waarvoor P waar is, ook een verzameling, die we noteren als

$$\{x \in A : P(x)\}$$

2.1.3 De ledige verzameling

Als we uitgaan van het bestaan van ten minste één verzameling, volgt uit de eerste twee axioma's het bestaan van een verzameling die geen elementen bevat.

Stelling 2.2

Er bestaat een unieke verzameling zonder elementen.

Bewijs. Er bestaat ten minste een verzameling A (bijvoorbeeld door het axioma van oneindigheid, zie Appendix B). Beschouw nu een predikaat P dat vals is voor alle elementen van A (zoals $x \neq x$), dan is $L = \{x \in A : P(x)\}$ een verzameling wegens het axioma van separatie. Bovendien bevat L geen elementen.

Stel nu dat L en E twee ledige verzamelingen zijn. Voor elk object z, zijn de uitspraken $z \in L$ en $z \in E$ beiden vals, en dus logisch equivalent. Dus $L = E$ door het axioma van extensionaliteit. □

Deze unieke verzameling zonder elementen noemen we *de ledige verzameling* en we noteren die met de Scandinavische[1] letter

$$\varnothing.$$

[1] De letter ø uit o.a. het Deense en Noorse alfabet is waarschijnlijk ontstaan als versie van de ligatuur Œ, waarbij het streepje van de E doorheen de O werd geschreven.

Merk op dat $\varnothing$ en $\{\varnothing\}$ verschillende verzamelingen zijn. De eerste heeft geen elementen, de tweede heeft er precies één — het feit dat dit unieke element toevallig het symbool is voor de lege verzameling, is irrelevant.

2.1.4 De machtsverzameling

De collectie van alle deelverzamelingen van een verzameling A is weer een verzameling. Dit is het vijfde axioma van ZFC. Deze wordt de **machtsverzameling** van A genoemd en genoteerd als $\mathcal{P}(A)$, soms ook als 2^A:

$$\mathcal{P}(A) = \{D : D \subseteq A\} = \{D : \forall x(x \in D \Rightarrow x \in A)\}$$

Een voorbeeld:

$$\mathcal{P}\left(\{1,2,3\}\right) \;=\; \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Er geldt voor elke verzameling A dat $\{\varnothing, A\} \subseteq \mathcal{P}(A)$.

2.1.5 Singletons, paren en koppels

Een verzameling met precies één element wordt een **singleton** genoemd. Een verzameling met precies twee elementen wordt een *paar* genoemd. Het bestaan van paren wordt gegarandeerd door het ZFC-axioma van paren, dat stelt dat als A en B verzamelingen zijn, dan ook $\{A, B\}$. Het is een oefening in het toepassen van extensionaliteit, om te bewijzen dat $\{a, b\} = \{b, a\}$ en dat $\{a, a\} = \{a\}$. Door dit laatste verzekert het axioma van paren ook het bestaan van singletons.

We willen nu definiëren wat een koppel (a, b) is. Het zou een object moeten zijn, geconstrueerd uit twee elementen a en b, dat de eigenschap moet hebben dat

$$(a, b) = (\alpha, \beta) \quad \Leftrightarrow \quad a = \alpha \text{ en } b = \beta$$

Het paar $\{a, b\}$ heeft deze eigenschap niet, daar de elementen van een paar niet geordend zijn. Enige schranderheid is vereist om de juiste constructie te vinden. Maar éénmaal ze gevonden is, zijn de details niet meer nodig; enkel bovenstaande eigenschap wordt gebruikt.

Definieer het **koppel** of *geordend paar* (a, b) als de verzameling met als elementen het ongeordend paar en het singleton bestaande uit het eerste element.

$$(a, b) \;=\; \{\{a\}, \{a, b\}\}$$

Bemerk dat door deze definitie het *identieke koppel* (a, a) gelijk is aan $\{\{a\}\}$.

Stelling 2.3

Er geldt $(a, b) = (\alpha, \beta)$ als en slechts als $a = \alpha$ en $b = \beta$.

Bewijs. De implicatie van rechts naar links is duidelijk. Onderstel nu dat $(a, b) = (\alpha, \beta)$, dus

$$\{\{a\}, \{a, b\}\} = \{\{\alpha\}, \{\alpha, \beta\}\}$$

De verzameling links heeft twee elementen (die mogelijks gelijk zijn), namelijk $\{a\}$ en $\{a, b\}$ en evenzo voor de verzameling rechts. Het axioma van extensionaliteit geeft dat *ofwel*

$$\{a\} = \{\alpha\} \quad \text{en } \{a, b\} = \{\alpha, \beta\}$$

ofwel

$$\{a\} = \{\alpha, \beta\} \quad \text{en } \{a, b\} = \{\alpha\}.$$

In het eerste geval hebben we (weer door extensionaliteit) dat $a = \alpha$ en hetzij $a = \alpha$ en $b = \beta$, hetzij $b = \alpha$ en $a = \beta$. In het eerste deelgeval hebben we de gewenste conclusie. In het tweede deelgeval hebben we $\beta = a = \alpha = b$, dus zijn we weer klaar. In het tweede geval hebben we $\alpha = a = \beta$ en $a = \alpha = b$, dus ook hier volgt dat $a = \alpha$ en $b = \beta$. □

2.2 Operaties op verzamelingen

Universele verzameling

Zelden worden in de wiskunde arbitraire verzamelingen beschouwd. We kunnen bijvoorbeeld geïnteresseerd zijn in verzamelingen reële getallen. In dat geval leggen we de verzameling $\mathbb{R}$ vast als **universele verzameling**. Dat betekent dat elke verzameling waarvan sprake in de discussie op dat ogenblik, *verondersteld* wordt een deelverzameling van $\mathbb{R}$ te zijn. Er is niet één universele verzameling; we kunnen er één vastleggen binnen elke context waarin het gepast is om alle andere mogelijkheden te negeren dan diegene die we beschouwen. Sommige operaties op verzamelingen vereisen dat een universele verzameling vastgelegd is. In het vervolg zullen we impliciet veronderstellen dat een universele verzameling vastgelegd is, indien noodzakelijk voor de context.

2.2.1 Unie, doorsnede, verschil en complement

De volgende vier operaties op verzamelingen zijn natuurlijk om te beschouwen. Het complement van een verzameling kunnen we enkel definiëren ten opzichte van een universele verzameling Ω.

Definitie 2.4

De **unie** of *vereniging* van twee verzamelingen A en B is de verzameling van alle elementen die in A *of* in B bevat zijn.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

De **doorsnede** van twee verzamelingen A en B is de verzameling van alle elementen die in A *en* in B bevat zijn.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Het **verschil** van twee verzamelingen A en B is de verzameling van alle elementen die bevat zijn in A maar niet in B.

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

Het **complement** van een verzameling A (ten opzichte van een universele verzameling Ω) is de verzameling van alle elementen van Ω die *niet* in A bevat zijn.

$$A^c = \{x \in \Omega \mid x \notin A\} = \Omega \setminus A$$

Dat de doorsnede en het verschil van twee verzamelingen weer een verzameling is, volgt uit het axioma van separatie. Voor de unie is dat niet zo: dat unies weer verzamelingen zijn, is de inhoud van het derde axioma van ZFC.

De symbolen $\cap, \cup$ en $\setminus$ zijn wereldwijd vastgelegde standaardsymbolen, al wordt soms ook wel eens $A - B$ gebruikt i.p.v. $A \setminus B$ en A', $\overline{A}$ of $\mathrm{comp}(A)$ i.p.v. A^c.

We noemen twee verzamelingen A en B **disjunct** als hun doorsnede leeg is, dus als

$$A \cap B = \varnothing.$$

Om een unie van A en B te noteren, waarbij bovendien wordt benadrukt dat A en B disjunct zijn, wordt soms $A \uplus B$ genoteerd, of $A \sqcup B$.

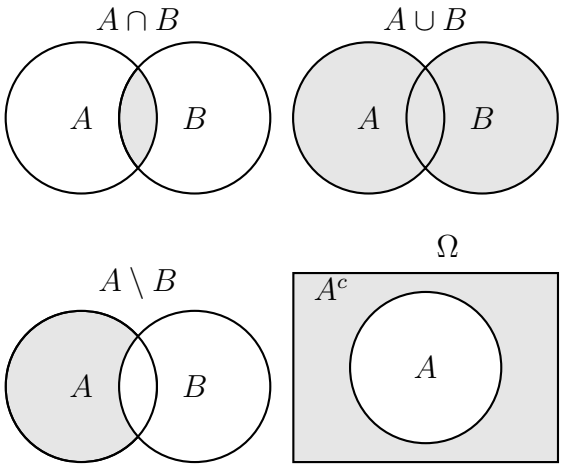
Minder voorkomend is de notie van het *symmetrisch verschil* van verzamelingen. Dit is de verzameling van alle elementen die bevat zijn in A of in B maar niet in beiden. Deze notie kunnen we op verschillende manieren definiëren in functie van de vorige operaties op verzamelingen:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \ \cup \ (B \setminus A)$$

Er is geen standaardnotatie voor het symmetrisch verschil, dat naast $A \triangle B$ ook wel eens als $A \ominus B$ of zelfs als $A + B$ genoteerd wordt.

2.2.2 Venndiagrammen

Het is gebruikelijk om verzamelingen diagrammatisch weer te geven, bijna altijd als begrijpelijke visualisering ter ondersteuning van een bewijs of situatie. Verzamelingen worden voorgesteld door ellipsen. De elementen van de verzameling worden voorgesteld door punten binnen deze ellips. Mogelijks is een universele verzameling Ω vastgelegd. Deze wordt weergegeven als een rechthoek en de punten erin stellen de elementen van Ω voor. Deelverzamelingen van Ω worden voorgesteld door regio's binnen Ω te omcirkelen met ellipsen. Een dergelijk schema wordt een venndiagram genoemd, naar de Britse logicus John Venn.



Figuur 2.1: Venndiagram voor de vier operaties uit Definitie 2.4

2.2.3 Eigenschappen van de basisoperaties

De volgende stelling somt de basisfeiten op over hoe de drie operaties unie, doorsnede en complement met elkaar interageren. Het zijn gevolgen van het gedrag van disjunctie, conjunctie en negatie van proposities van de vorm $x \in A$. Zoals eerder vermeld veronderstellen we dat de verzamelingen in kwestie deelverzameling zijn van een bepaalde universele verzameling indien nodig.

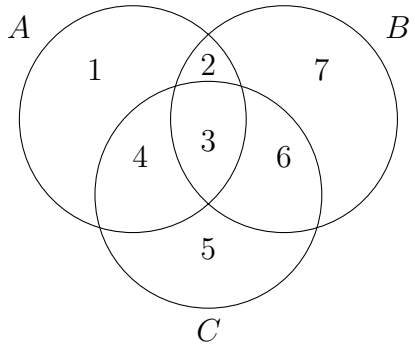
Stelling 2.5

Zij A, B en C verzamelingen.

1. *Associatieve wet*
   (a) $A \cup (B \cup C) = (A \cup B) \cup C$
   (b) $A \cap (B \cap C) = (A \cap B) \cap C$
2. *Commutatieve wet*
   (a) $A \cup B = B \cup A$.
   (b) $A \cap B = B \cap A$.
3. *Distributieve wet*
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. *Wetten van De Morgan*
   (a) $(A \cup B)^c = A^c \cap B^c$
   (b) $(A \cap B)^c = A^c \cup B^c$
5. *Complementwetten*
   (a) $A \cup A^c = \Omega$
   (b) $A \cap A^c = \varnothing$
6. *Zelfinversieve wet*
   (a) $(A^c)^c = A$

Bewijs. Om de rek op het concept *bewijs* te illustreren, zullen we 3a aantonen met een venndiagrambewijs en 3b en 4b bewijzen met een logisch argument. De andere delen van de stelling laten we over als oefening.

We kunnen de situatie van geval 3a voorstellen door middel van een venndiagram. Het meest algemene geval is getekend, waarbij alle verzamelingen



elementen kunnen gemeenschappelijk hebben met de andere verzamelingen. De verzameling A wordt voorgesteld door de regio's met nummers 1, 2, 3 en 4. De doorsnede $B \cap C$ wordt voorgesteld door 3 en 6, dus $A \cup (B \cap C)$ wordt voorgesteld door 1, 2, 3, 4 en 6. Wederom, $(A \cup B)$ komt overeen met nummers 1, 2, 3, 4, 6 en 7 en $(A \cup C)$ komt overeen met 1, 2, 3, 4, 5 en 6, dus $(A \cup B) \cap (A \cup C)$ komt overeen met 1, 2, 3, 4 en 6. Maar dat is dezelfde als $A \cup (B \cap C)$, dus ze bevat dezelfde elementen.

Om geval 3b logisch te bewijzen, introduceer de afkortingen

$$D = A \cap (B \cup C) \quad \text{en} \quad E = (A \cap B) \cup (A \cap C)$$

We bewijzen eerst dat $D \subseteq E$. Zij $x \in D$ willekeurig. Dan is $x \in A$ en $x \in B \cup C$. Wegens dat laatste is ofwel $x \in B$ of $x \in C$ (of zelfs beiden). In het geval dat $x \in B$, hebben we dat $x \in A$ en $x \in B$, dus $x \in A \cap B$. Als $x \notin B$, moet wel $x \in C$, zodat $x \in A \cap C$. In beide gevallen is $x \in (A \cap B) \cup (A \cap C) = E$, dus omdat x willekeurig was, is $D \subseteq E$.

Om te bewijzen dat $E \subseteq D$, neem x willekeurig in E. Er zijn twee gevallen. Stel eerst dat $x \in A \cap B$. Dan is $x \in A$ en $x \in B$, dus $x \in A$ en $x \in B \cup C$, waaruit $x \in D$. Als $x \notin A \cap B$, dan moet wel $x \in A \cap C$, dus we vinden weer dat $x \in A$ en $x \in B \cup C$, en dus $x \in D$. Vandaar dat $E \subseteq D$. Bijgevolg hebben we $D \subseteq E$ en $E \subseteq D$, wat bewijst dat $D = E$.

We presenteren een logisch argument waarbij we een wet van De Morgan uit de verzamelingenleer terugbrengen naar die uit de logica. We hebben

namelijk

$$\begin{aligned} x \in (A \cap B)^c &\Leftrightarrow \neg\, x \in (A \cap B) \\ &\Leftrightarrow \neg(x \in A \ \wedge \ x \in B) \\ &\Leftrightarrow (\neg\, x \in A) \ \vee \ (\neg\, x \in B) \\ &\Leftrightarrow (x \in A^c) \ \vee \ (x \in B^c) \\ &\Leftrightarrow x \in A^c \cup B^c \end{aligned}$$

Dit bewijst 4b. □

2.2.4 Willekeurige unie en doorsnede

De associatieve wetten laten ons toe om ondubbelzinnig $A \cap B \cap C$ en $A \cup B \cup C$ te schrijven, en zelfs willekeurig grote (maar eindige) intersecties en unies te beschouwen, bijvoorbeeld:

$$A_1 \cup A_2 \cup \cdots \cup A_n = (\ldots (A_1 \cup A_2) \cup \ldots) \cup A_n$$

In de wiskunde moeten we echter vaak unies en doorsnedes beschouwen van *oneindige* collecties verzamelingen. Die kunnen we niet definiëren a.d.h.v. de notie van unie en doorsnede van twee verzamelingen.

Als met elk element i van een bepaalde niet-ledige verzameling I een verzameling A_i correspondeert, dan verwijzen we naar de niet-ledige collectie

$$\{A_i \mid i \in I\}$$

als een *familie* verzamelingen, *geïndexeerd door* de verzameling I die we de *indexverzameling* noemen. Op de indexverzameling liggen bijna geen restricties: ze moet bijvoorbeeld niet noodzakelijk geordend zijn, of aftelbaar, maar meestal eisen we wel dat ze niet ledig is (zie later).

Definitie 2.6

De **unie** van een familie verzamelingen $\{A_i \mid i \in I\}$ is de verzameling van alle elementen die bevat zijn in *één of meerdere* verzamelingen A_i uit de familie.

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I : x \in A_i\}$$

De **doorsnede** van een familie verzamelingen $\{A_i \mid i \in I\}$ is de verzameling van alle elementen die bevat zijn in *alle* verzamelingen A_i uit de familie.

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I : x \in A_i\}$$

Merk eerst op dat in het geval dat de indexverzameling $I = \{1, 2\}$ uit slechts twee elementen bestaat, we de eindige unie en doorsnede krijgen:

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \qquad \text{en} \qquad \bigcap_{i \in I} A_i = A_1 \cap A_2$$

Deze definitie is dus een echte veralgemening van de unie en doorsnede van twee verzamelingen.

Merk verder op dat we de definitie van willekeurige unie en doorsnede terugvoeren tot de existentiële resp. universele kwantor, op dezelfde manier als we de unie en doorsnede van *twee* verzamelingen hebben teruggevoerd tot een conjunctie resp. disjunctie. Vergelijk met de identiteiten 1.2, waar de kwantoren overeenkomen met con- en disjuncties in het geval het universum maar twee elementen heeft.

We maken melding van de volgende eigenschappen en hun bewijzen, omdat ze mooi illustreren op welke manier willekeurige unies en doorsneden gehanteerd worden. Nergens wordt verondersteld dat de indexverzameling een bepaalde grootte of ordening heeft.

Stelling 2.7

Zij $\{A_i \mid i \in I\}$ een geïndexeerde familie verzamelingen. Zij B een willekeurige verzameling (deelverzameling van een universele verzameling).

1. Voor elke $i_0 \in I$ geldt: $\bigcap_{i\in I} A_i \subseteq A_{i_0} \subseteq \bigcup_{i\in I} A_i$
2. $B \cup \bigcup_{i\in I} A_i = \bigcup_{i\in I}(B \cup A_i)$
3. $B \cap \bigcap_{i\in I} A_i = \bigcap_{i\in I}(B \cap A_i)$
4. $B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(B \cap A_i)$
5. $B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I}(B \cup A_i)$
6. $\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c$
7. $\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c$

Bewijs. We bewijzen enkel de eerste, middelste en laatste eigenschap en laten de rest als oefening.

1. Stel dat $x \in \bigcap_{i\in I} A_i$. Dan is, $\forall i \in I : x \in A_i$. In het bijzonder is $x \in A_{i_0}$. Dit bewijst de eerste inclusie. Neem nu $x \in A_{i_0}$. Dan geldt zeker $\exists i \in I : x \in A_i$ (i_0 is de existentiële getuige), dus $x \in \bigcup_{i\in I}$. Dit bewijst de tweede inclusie.

4. Stel dat $x \in B \cap \bigcup_{i\in I} A_i$. Dan is $x \in B$ en voor een bepaalde i_0 is $x \in A_{i_0}$. Dus $x \in B \cap A_{i_0}$ en er volgt dat $x \in \bigcup_{i\in I}(B \cap A_i)$. Omgekeerd, stel dat $x \in \bigcup_{i\in I}(B \cap A_i)$. Dan is er een i_0 zodat $x \in B \cap A_{i_0}$. Dus $x \in B$ en $x \in A_{i_0} \subseteq \bigcup_{i\in I} A_i$, en bijgevolg $x \in B \cap \bigcup_{i\in I} A_i$.

7. Zij x een willekeurig element van de universele verzameling. Dan is

$$\begin{aligned} x \in \Big(\bigcap_{i\in I} A_i\Big)^c &\Leftrightarrow \neg x \in \Big(\bigcap_{i\in I} A_i\Big) \\ &\Leftrightarrow \neg \forall i \in I : x \in A_i \\ &\Leftrightarrow \exists i \in I : \neg\, x \in A_i \\ &\Leftrightarrow \exists i \in I : x \in A_i^c \\ &\Leftrightarrow x \in \bigcup_{i\in I} A_i^c \end{aligned}$$

□

In het geval dat de indexverzameling de natuurlijke getallen zijn, wordt ook wel genoteerd

$$\bigcup_{i=0}^{\infty} A_i \text{ i.p.v. } \bigcup_{i\in\mathbb{N}} A_i \qquad \text{en} \qquad \bigcap_{i=0}^{\infty} A_i \text{ i.p.v. } \bigcap_{i\in\mathbb{N}} A_i$$

Als $\mathcal{F}$ een bepaalde collectie van verzamelingen is, kunnen unie en doorsnede ook genoteerd worden zonder melding te maken van een indexverzameling:

$$\bigcup \mathcal{F} = \{x \mid \exists A \in \mathcal{F} : x \in A\} \qquad \text{en} \qquad \bigcap \mathcal{F} = \{x \mid \forall A \in \mathcal{F} : x \in A\}$$

In het geval $\mathcal{F} = \{A_i \mid i \in I\}$ een geïndexeerde familie is, herleiden deze definities zich:

$$\bigcup \mathcal{F} = \bigcup_{i\in I} A_i \qquad \text{en} \qquad \bigcap \mathcal{F} = \bigcap_{i\in I} A_i$$

Er is een probleem met de ledige verzameling hier. De unie $\bigcup \varnothing$ is gewoon de ledige verzameling, want er zijn geen element-verzamelingen in $\varnothing$ waarvan de elementen in $\bigcup \varnothing$ zouden kunnen zitten — de conditie $\exists A \in \varnothing : x \in A$ is altijd vals. Maar $\bigcap \varnothing$ zou uit het hele universum moeten bestaan: gegeven een willekeurige x is de conditie $\forall A \in \varnothing : x \in A$ triviaal voldaan — er is geen A in $\varnothing$ om een restrictie te bepalen. Om dit uit te sluiten stellen we dat de unie $\bigcap \mathcal{F}$ enkel gedefinieerd is als $\mathcal{F} \neq \varnothing$.

2.2.5 Partitie

Met de notie van unie van een familie verzamelingen kunnen we het belangrijke concept *partitie* invoeren. Het is een opdeling van een verzameling in disjuncte deelverzamelingen, die de hele verzameling bedekken.

Definitie 2.8

Een **partitie** van een verzameling A is een familie $\mathcal{F}$ van deelverzamelingen van A, **klassen** genoemd, met de volgende eigenschappen.

1. Geen enkele klasse is ledig, m.a.w.

$$\forall S \in \mathcal{F} \ : \ S \neq \varnothing.$$

2. De unie van alle klassen is heel A, m.a.w.

$$\bigcup_{S \in \mathcal{F}} S = A$$

3. De klassen zijn onderling disjunct, m.a.w.

$$\forall S_1 \neq S_2 \in \mathcal{F} \ : \ S_1 \cap S_2 = \varnothing$$

We zeggen dat de klassen de verzameling A *partitioneren*. We geven drie voorbeelden.

$$\{\{1\}, \{2,3\}, \{4\}\} \text{ is een partitie van } \{1,2,3,4\}.$$
$$\{\{2n \mid n \in \mathbb{Z}\}, \{2n+1 \mid n \in \mathbb{Z}\}\} \text{ is een partitie van } \mathbb{Z}.$$

Zij R een verzameling mensen. Beschouw de deelverzamelingen $S(p) = \{q \in R \mid p \text{ en } q \text{ hebben hetzelfde geboortejaar}\}$. Dan is $\{S(p) \mid p \in R\}$ een partitie van R.

2.2.6 Cartesisch product

Er rest ons nog een laatste operatie te introduceren, die van twee verzamelingen een nieuwe verzameling maakt: het cartesisch product. Het cartesisch product van verzamelingen veralgemeent de ideeën van het Euclidische vlak en het cartesiaans coördinatensysteem in de vlakke meetkunde, vandaar de naam, die teruggaat op René Descartes (Cartesius).

Definitie 2.9

Het **cartesisch product** van een verzameling A met een verzameling B is de verzameling van alle koppels (a, b), met $a \in A$ en $b \in B$.

$$A \times B \ = \ \{(a,b) \mid a \in A \wedge b \in B\}$$

Het cartesisch product van verzamelingen is niet commutatief. Hoewel er een betekenisvolle correspondentie bestaat tussen $A \times B$ en $B \times A$, zijn de verzamelingen niet *gelijk*, zoals blijkt uit een eenvoudig voorbeeld, met $A = \{1, 2\}$ en $B = \{2, 3, 4\}$. Dan is

$$A \times B = \{(1,2), (1,3), (1,4), (2,2), (2,3), (2,4)\}$$
$$B \times A = \{(2,1), (2,2), (3,1), (3,2), (4,1), (4,2)\}$$

Stelling 2.10

Zijn A, B, C en D verzamelingen. Dan is

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
3. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
4. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

Bewijs. We bewijzen enkel 3 en laten de rest als oefening.

$$\begin{aligned}(x,y) \in (A \times B) \cap (C \times D) &\Leftrightarrow (x,y) \in A \times B \text{ en } (x,y) \in C \times D \\ &\Leftrightarrow x \in A \text{ en } y \in B \text{ en } x \in C \text{ en } y \in D \\ &\Leftrightarrow x \in A \cap C \text{ en } y \in B \cap D \\ &\Leftrightarrow (x,y) \in (A \cap C) \times (B \cap D)\end{aligned}$$

2.3 Relaties

De notie van een *relatie* is vertrouwd: een relatie tussen een verzameling A en een verzameling B *verbindt* bepaalde elementen van A met bepaalde elementen van B. Een voorbeeld van een relatie tussen de verzameling van alle personen en die van alle objecten, is de relatie *eigendom*, waarbij een persoon p *gerelateerd is met* een object a als p het object a *bezit*.

Vele voorbeelden uit de wiskunde zijn relaties die elementen van eenzelfde verzameling A met elkaar verbinden. Die noemen we dan *relaties op* A en A is dan de *onderliggende verzameling*. Bijvoorbeeld, $<$, $\leq$ en $=$ zijn allen relaties

op de verzameling $\mathbb{N}$. Voor natuurlijke getallen m en n wordt $m < n$ een propositie die een betekenisvol verband uitdrukt tussen m en n. Verder zijn het getrouwd zijn van personen, de delingsrelatie op $\mathbb{N}$, het loodrecht staan van rechten in het Euclidisch vlak of het disjunct zijn van verzamelingen allemaal voorbeelden van relaties.

We gaan het begrip relatie nu formeel invoeren als verzameling.

2.3.1 Relaties als deelverzameling van het cartesisch product

Definitie 2.11

Een **relatie** tussen een verzameling A en een verzameling B is een deelverzameling van de productverzameling $A \times B$.

We vatten een relatie dus op als een verzameling R van geordende paren. Het **complement van een relatie** R is dus de verzameling van koppels die niet tot de relatie R behoren — zo is bijvoorbeeld $<$ het complement van $\geq$ op de reële getallen. De unie en doorsnede van relaties zijn eveneens goed gedefinieerd. Nog een operatie op relaties, is het *beperken* van een relatie $R \subseteq A \times B$ tot een deelverzameling $C \times D$, met $C \subseteq A$ en $D \subseteq B$.

Definitie 2.12

Als R een relatie is tussen A en B en $C \subseteq A$ en $D \subseteq B$, dan is de **restrictie** of **beperking** van R tot $C \times D$ de relatie op $C \times D$ bestaande uit die R-koppels die in $C \times D$ liggen, m.a.w.

$$R_{|C \times D} = R \cap (C \times D).$$

Tot slot kunnen we een binaire relatie ook *omkeren*, door de volgorde van de elementen in de koppels om te wisselen.

Definitie 2.13

Als $R \subseteq A \times B$ een relatie is tussen A en B, dan is de **omgekeerde relatie** of **inverse relatie** de verzameling van de *omgekeerde koppels*, d.w.z.

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

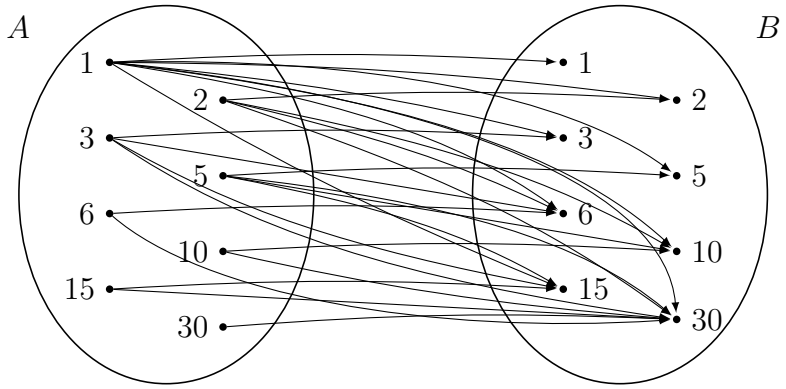
Bijvoorbeeld, de relaties "is kind van" en "is ouder van" zijn elkaars omgekeerde.

Een bijzondere relatie die bestaat op elke verzameling A, wordt geïnduceerd door de gekende *gelijkheid* "=". Het is de *identiteitsrelatie*, bestaande uit enkel de identieke koppels.

$$I_A = \{(a, a) \mid a \in A\}$$

2.3.2 Voorstellen van relaties

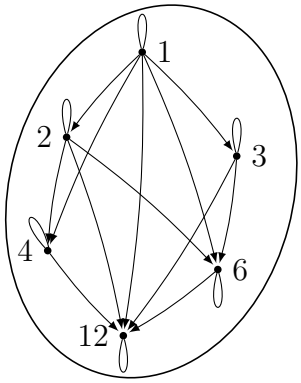
Een relatie kan voorgesteld worden door middel van pijlen van A naar B, voorgesteld als venndiagrammen.



Figuur 2.2: Deelbaarheidsrelatie op $\{1, 2, 3, 5, 6, 10, 15, 30\}$

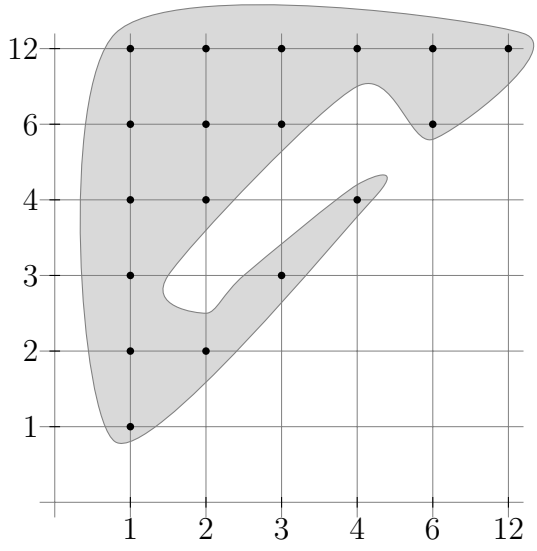
Een relatie R op één verzameling A kan voorgesteld worden met een pijlenvoorstelling binnen A, waarbij een pijl getekend wordt van a naar b als $(a, b) \in R$. In de pijlenvoorstelling wordt een identiek koppel voorgesteld door een lus (zonder pijl).

Wordt het cartesisch product $A \times B$ voorgesteld als een vlak met coördinaatassen A en B, dan kan een relatie gevisualiseerd worden door de punten die



Figuur 2.3: Deelbaarheidsrelatie op $\{1, 2, 3, 4, 6, 12\}$

corresponderen met de koppels van de relatie, aan te duiden. De identiteitsrelatie wordt bijvoorbeeld voorgesteld door de eerste bissectrice (de rechte $y = x$). Om de duidelijkheid te vergroten, kan men daarenboven ook de punten die de relatie voorstellen in een Venndiagram tekenen.



Figuur 2.4: "Cartesiaanse" voorstelling van een relatie

2.3.3 Kenmerken van relaties

Vele vertrouwde concepten, zoals ordeningen, bewerkingen en functies zijn eigenlijk relaties, die aan bepaalde eigenschappen voldoen. We lijsten hieronder de belangrijkste eigenschappen op waaraan een relatie kan voldoen. We geven de definities voor relaties op één verzameling A, maar sommige definities kunnen zonder moeite uitgebreid worden voor deelverzamelingen van $A \times B$.

We gebruiken voor de leesbaarheid hier de lichte infixnotatie $a\ R\ b$ (zoals $>$ en $\subseteq$) i.p.v. de zwaardere notatie $(a, b) \in R$.

Definitie 2.14

- Een relatie $R \subseteq A \times A$ is **reflexief** als alle identieke koppels tot R behoren, dus als
$$\forall a \in A : a\ R\ a$$
Een relatie $R \subseteq A \times A$ is **antireflexief** als geen enkel identiek koppel ertoe behoort, dus als
$$\forall a \in A : \neg\ a\ R\ a$$

- Een relatie $R \subseteq A \times A$ is **symmetrisch** als
$$\forall a, b \in A : a\ R\ b \Rightarrow b\ R\ a$$
Een relatie $R \subseteq A \times A$ is **asymmetrisch** als
$$\forall a, b \in A : a\ R\ b \Rightarrow \neg b\ R\ a$$
Een relatie $R \subseteq A \times A$ is **antisymmetrisch** als
$$\forall a \neq b \in A : a\ R\ b \Rightarrow \neg b\ R\ a$$
of, equivalent, als
$$\forall a, b \in A : (a\ R\ b \wedge b\ R\ a) \Rightarrow a = b$$

- Een relatie $R \subseteq A \times A$ is **transitief** als
$$\forall a, b, c \in A : a\ R\ b \wedge b\ R\ c \Rightarrow a\ R\ c$$

Men mag zeker niet denken dat elke relatie aan één van de definities onder elk puntje moet voldoen. Als bijvoorbeeld een relatie *niet reflexief* is, bevat ze niet alle identieke koppels. Dat betekent natuurlijk niet dat ze dan geen enkel identiek koppel bevat, m.a.w. *antireflexief* is. Relaties die sommige identieke koppels bevatten en sommige niet, zijn gewoon niet reflexief en niet antireflexief. Op eenzelfde manier zijn er ook vele relaties die noch symmetrisch, noch antisymmetrisch, noch asymmetrisch zijn.

Met betrekking tot deze eigenschappen kan men de "sluiting" beschouwen, als een operatie om van een bepaalde relatie een nieuwe relatie te maken die *wel* aan een eigenschap voldoet. Zo is de *reflexieve sluiting* van een relatie $R \subseteq A \times A$ degene die ontstaat door alle identieke koppels bij te voegen:

$$\text{Reflexieve sluiting van } R = R \cup \{(x, x) \in A \times A \mid x \in A\}$$

De *symmetrische sluiting* van een relatie $R \subseteq A \times A$ ontstaat analoog:

$$\text{Symmetrische sluiting van } R = R \cup \{(x, y) \in A \times A \mid y \; R \; x\}$$

De *transitieve sluiting* van een relatie $R \subseteq A \times A$ tot slot is de relatie

$$R \cup \{(x, y) \in A \times A \mid \exists z_1, \ldots, z_n : x \; R \; z_1 \wedge z_1 \; R \; z_2 \wedge \cdots \wedge z_n \; R \; y\}$$

De transitieve (reflexieve, symmetrische) sluiting van een relatie is de kleinste transitieve (reflexieve, symmetrische) relatie die R bevat. Hier moet "kleinste" geïnterpreteerd worden met betrekking tot verzamelingtheoretische inclusie $\subseteq$. Dit zijn vaak nuttige concepten. Een voorbeeldje uit het reisleven: als de relatie R op de verzameling van alle luchthavens ter wereld zo is dat $x \; R \; y$ betekent "er is een rechtstreekse vlucht van x naar y", dan is de transitieve sluiting van R de relatie "het is mogelijk om van x naar y te vliegen in één of meer vluchten.

2.3.4 Equivalentierelaties

Definitie 2.15

Een relatie $R \subseteq A \times A$ is een **equivalentierelatie** als R reflexief, symmetrisch en transitief is.

Elementen a en b die gerelateerd zijn onder een equivalentierelatie R (dus $(a, b) \in R$) noemen we soms *equivalent*. Voor equivalentierelaties worden vaak symbolen als $\sim$ of $\equiv$ gebruikt. Men kan nagaan dat de volgende relaties equivalentierelaties zijn (door drie condities te verifiëren).

- zelfde geboortejaar hebben (op een verzameling mensen)
- parallellisme (op de rechtenverzameling van het Euclidisch vlak)
- de identiteitsrelatie "=" (op elke verzameling)
- de relatie R op $\mathbb{Z}$ met: $a\ R\ b \Leftrightarrow a - b$ is even
- de relatie R op $\mathbb{N} \times \mathbb{N}$ met: $(m, n)\ R\ (p, q) \Leftrightarrow mq = np$

Definitie 2.16

Als $\sim$ een equivalentierelatie is op A en a een element van A, dan is de **equivalentieklasse van** a (ook wel "a modulo $\sim$" genoemd) de verzameling van alle elementen van A die equivalent zijn met a.

$$[a] = \{x \in A \mid x \sim a\}$$

Het element a is een *representant* van deze equivalentieklasse.

Omwille van de drie eigenschappen waaraan een equivalentierelatie voldoet, staan alle elementen van een equivalentieklasse onderling in relatie tot elkaar en zichzelf.

Bijvoorbeeld, beschouwen we de relatie R op $\mathbb{Z}$ gedefinieerd door $a\ R\ b \Leftrightarrow a - b$ is even, dan is

$$[1] = \{n \in \mathbb{Z} \mid 1\ R\ n\} = \{n \in \mathbb{Z} \mid 1 - n \text{ is even}\} = \{n \in \mathbb{Z} \mid n \text{ is oneven}\}$$
$$[2] = \{n \in \mathbb{Z} \mid 2\ R\ n\} = \{n \in \mathbb{Z} \mid 2 - n \text{ is even}\} = \{n \in \mathbb{Z} \mid n \text{ is even}\}$$

Als we zo verder gaan, zien we dat $[1] = [3] = [5] = \ldots$ allemaal dezelfde verzameling zijn, namelijk die van de oneven getallen (en $[2] = [4] = [6] = \ldots$ die van de even getallen). In dit geval zijn er dus maar twee equivalentieklassen, dus $\mathbb{Z}$ wordt door de equivalentierelatie R opgedeeld in twee disjuncte stukken, die dus een partitie vormen van $\mathbb{Z}$. Dit is een speciaal geval van een meer algemeen fenomeen.

Lemma 2.17

Zij $\sim$ een equivalentierelatie op A.

- $x \sim y \Rightarrow [x] = [y]$
- $x \not\sim y \Rightarrow [x] \cap [y] = \varnothing$

Bewijs.

- Stel dat $x \sim y$. We bewijzen eerst dat $[x] \subseteq [y]$, dus neem willekeurig $z \in [x]$. Dus $z \sim x$. Wegens de transitiviteit van $\sim$ is ook $z \sim y$, dus $z \in [y]$. Dit bewijst $[x] \subseteq [y]$. Voor de omgekeerde inclusie, neem $z \in [y]$, dan is $z \sim y$ en wegens de symmetrie van $\sim$ ook $y \sim z$. Door transitiviteit is $x \sim z$ en door symmetrie $z \sim x$, dus $z \in [x]$. Dit bewijst beide inclusies.

- Stel dat $x \not\sim y$. Als $[x] \cap [y]$ niet-ledig zou zijn, neem dan $z \in [x] \cap [y]$. Dan is $[x] = [z] = [y]$, maar $x \in [x] = [y]$, wat betekent dat $x \sim y$, in strijd met de onderstelling. □

Stelling 2.18

- Zij $\sim$ een equivalentierelatie op A. De equivalentieklassen van $\sim$

$$\mathcal{F}_\sim = \{[x] \mid x \in A\}$$

  vormen een partitie van A.

- Zij $\mathcal{F}$ een partitie van A. Dan is de relatie "zit in dezelfde partitieklasse als", d.w.z. $\sim_\mathcal{F}$ gedefinieerd door

$$x \sim_\mathcal{F} y \Leftrightarrow \exists T \in \mathcal{F} : x \in T \wedge y \in T$$

  een equivalentierelatie op A. De equivalentieklassen van deze relatie zijn precies de verzamelingen in $\mathcal{F}$.

Bewijs. Stel dat $\sim$ een equivalentierelatie is op A. Het vorige lemma bewijst dat de equivalentieklassen disjunct zijn. Geen enkele equivalentieklasse $[a]$ is ledig, want ze bevat a. De unie van de klassen is heel A, want een willekeurige a is bevat in de klasse $[a]$.

Stel nu dat $\mathcal{F}$ een partitie is van A. Neem $a \in A$. Omdat $\bigcup_{T \in \mathcal{F}} T = A$, bestaat er een T zodat $a \in T$, dus $a \sim_\mathcal{F} a$, wat de reflexiviteit bewijst. Voor de symmetrie, stel dat $a \sim_\mathcal{F} b$, dan bestaat er een $T \in \mathcal{F}$ met $a \in T \wedge b \in T$, waaruit volgt dat ook $b \sim_\mathcal{F} a$. Voor de transitiviteit, stel dat $a \sim_\mathcal{F} b$ en $b \sim_\mathcal{F} c$. Dan bestaan er klassen S en T in $\mathcal{F}$ met $a \in S, b \in S, b \in T$ en $c \in T$. Omdat verschillende klassen van een partitie disjunct zijn, moet wel $S = T$, anders zou b in de doorsnede van twee verschillende partitieklassen liggen. We hebben nu dat $a \in S = T$ en $c \in T$, waaruit $a \sim_\mathcal{F} c$.

We bewijzen tot slot dat de verzamelingen T in $\mathcal{F}$ de equivalentieklassen $[x]_\mathcal{F}$ van $\sim_\mathcal{F}$ zijn. Neem een $T \in \mathcal{F}$. Deze is niet-ledig, dus neem $x \in T$. We zullen bewijzen dat $[x]_\mathcal{F} = T$. Voor elke $y \in T$ geldt dat $x \sim_\mathcal{F} y$ per definitie van $\sim_\mathcal{F}$ en dus $y \sim_\mathcal{F} x$ ofwel $y \in [x]_\mathcal{F}$, wat $T \subseteq [x]_\mathcal{F}$ bewijst. Stel omgekeerd dat $y \in [x]_\mathcal{F}$, dan is $y \sim_\mathcal{F} x$. Dat betekent dat er een $S \in \mathcal{F}$ is zodat $x, y \in S$. Maar $x \in S \cap T$, dus $S = T$. Dat bewijst $[x]_\mathcal{F} \subseteq T$ en dus de gelijkheid. □

Deze stelling vertelt dat equivalentierelaties en partities verschijningsvormen zijn van eenzelfde idee, waarmee we vertrouwd zijn: het classificeren of categoriseren. Zowel in wiskunde als in het dagelijkse leven klasseren we vaak dingen naargelang een bepaald criterium. Het ligt voor de hand om de klassen of categorieën nu zelf al elementen van een verzameling te gaan bekijken, wat aanleiding geeft tot het vruchtbare concept van de *quotiëntverzameling*.

2.3.5 Quotiëntstructuren

Als een equivalentierelatie gedefinieerd is op een verzameling A, dan heeft deze verzameling A een elegante structuur krachtens stelling 2.18. Die structuur laat ons toe om de klassen als objecten op zich te bekijken, door bij wijze van spreken te vergeten dat ze nog uit verschillende elementen bestaan.

Definitie 2.19

Zij A een verzameling en $\sim$ een equivalentierelatie op A. De **quotiëntverzameling** $A/\sim$ is de verzameling van equivalentieklassen

$$A/\sim = \{[x]_\sim \mid x \in A\}$$

De quotiëntverzameling kan men zien als de verzameling A waarvan alle equivalente elementen worden geïdentificeerd tot één element. Deze verandering van perspectief, van de verzameling A met al haar elementen naar de kleinere equivalentieklassenstructuur met haar klassen als objecten, noemen wiskundigen *uitdelen*. De quotiëntverzameling $A/\sim$ wordt dan genoemd A *uitgedeeld naar* $\sim$, of A *modulo* $\sim$. De naam is afkomstig van het *opdelen* van de originelen in A volgens de equivalentierelatie, en van de volgende observatie: als A een eindige verzameling is en alle equivalentieklassen hebben evenveel elementen, dan wordt de grootte van de quotiëntverzameling bepaald door het aantal elementen van A te *delen* door het aantal elementen in elke klasse.

In vele takken van de wiskunde en in het bijzonder de algebra, zal dit een nuttig gereedschap zijn om algebraïsche structuren beter te begrijpen. Als de verzameling A voorzien is van een algebraïsche bewerking of andere structuur, kan er vaak (d.i. bij een logische keuze van equivalentierelatie) eenzelfde structuur gedefinieerd worden op de quotiëntverzameling. Zo kunnen groepen aanleiding geven tot quotiëntgroepen (zie hoofdstuk 5 en *Algebra I*) en vectorruimten tot quotiëntruimten (zie *LAAM I*).

Aan een quotiëntstructuur is steeds een *projectieafbeelding* of *canonische projectie* geassocieerd, zie daarvoor pagina 67.

2.4 Afbeeldingen

Zonder twijfel een heel belangrijk concept in de wiskunde is dat van een *afbeelding* — in nagenoeg elke tak van de wiskunde blijken afbeeldingen het centrale onderzoeksonderwerp te zijn. Het is dan ook niet verrassend dat het concept *afbeelding* er één is van grote algemeenheid. De term *functie* wordt gebruikt als synoniem voor *afbeelding*, al is *functie* vooral gebruikelijk in contexten waarbij de beelden van de functie getallen uit een veld zijn — de analyse bestudeert bijvoorbeeld reële functies (van $\mathbb{R}$ naar $\mathbb{R}$).

2.4.1 Concept en notaties

Men kan denken over een afbeelding van een niet-ledige verzameling A naar een niet-ledige verzameling B als een algemene *regel* die met elk element van A een uniek element van B associeert. Er zijn geen restricties op het soort regel; de enige cruciale punten zijn:

- de regel wijst een element van B toe aan *elk* element van A
- het element van B dat we associëren met een gegeven a in A moet *uniek bepaald* zijn voor deze a.

We schrijven

$$f : A \to B$$

om aan te duiden dat het object f een functie is *van* de verzameling A *naar* de verzameling B. Hierbij wordt A het *domein* of *definitiegebied* genoemd

en B het *codomein*. Als $a \in A$, dan noteren we het unieke element van B dat de functie toekent aan a als

$$f(a)$$

(maar vele andere notaties zijn in omloop, afhankelijk van de context) en we noemen a hierin het *argument* en $f(a)$ het *beeld van a onder f* of ook de *(functie)waarde* van a.

Bijvoorbeeld, de regel die aan elke $x \in \mathbb{R}$ het reëel getal $x^2 + x + 1$ toekent, kan men opvatten als een afbeelding van $\mathbb{R}$ naar $\mathbb{R}$. We kunnen die dan opschrijven als

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f(x) = x^2 + x + 1 \end{aligned}$$

Om de intuïtie over afbeeldingen aan te scherpen, is het instructief om het begrip *afbeelding* op te vatten als een soort "black box", die een inputlade en een outputlade heeft. In de inputlade kunnen we elk mogelijk element van A in de machine steken, waarop de black box onze invoer verwerkt en één enkel beeld produceert, dat altijd in de verzameling B zal zitten. Domein A en codomein B zijn integrale onderdelen van de afbeelding.

In de aanloop naar een precieze definitie van afbeelding leggen we vast wat het betekent voor twee afbeeldingen om gelijk te zijn. Beschouw de volgende twee definities van functies

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ n &\mapsto f(n) = n^2 - 2n + 1 \\ g : \mathbb{Z} &\to \mathbb{Z} \\ n &\mapsto g(n) = (n-1)^2 \end{aligned}$$

Deze afbeeldingen hebben hetzelfde domein en codomein, maar duidelijk andere *regels* om een beeld toe te wijzen aan een origineel: de eerste gebruikt een kwadratering, een verdubbeling, een aftrekking en een optelling, terwijl de tweede enkel uit een aftrekking en een kwadratering bestaat. Iedereen weet echter dat f en g aanleiding zullen geven tot dezelfde beelden, voor elk mogelijk argument.

Dat $f(n) = g(n), \forall n \in \mathbb{Z}$, is voldoende motivatie om de afbeeldingen f en g ook echt als gelijk te beschouwen. Dat betekent dat een afbeelding niet zozeer een *regel* is om elementen uit A af te beelden op elementen uit B, maar eerder de *argument-naar-beeld-toewijzing zelf* die door die regel bepaald wordt. Dit idee gebruiken we om een formele definitie van afbeelding te geven.

2.4.2 Afbeeldingen als relaties

Definitie 2.20

Een **afbeelding** of **functie** van een verzameling A naar een verzameling B is een relatie R tussen A en B waarbij elk element van A juist één keer voorkomt als eerste lid van een koppel in de relatie, d.w.z. als

$$\forall a \in A : \exists! \, b \in B : (a, b) \in R$$

Een **partiële afbeelding** of **partiële functie** van A naar B is een relatie R tussen A en B waarbij elk element van A ten hoogste één keer voorkomt als eerste lid van een koppel in de relatie, d.w.z. als

$$\forall a \in A : \forall b, c \in B : ((a, b) \in R \wedge (a, c) \in R) \Rightarrow b = c$$

Deze definitie vat een afbeelding op als een verzameling koppels, waarbij de koppels alle argumenten van A, als eerste lid van een koppel, associëren met hun beelden in B, als tweede lid van het koppel. Een afbeelding f zoals intuïtief geïntroduceerd in de vorige paragraaf, is dus formeel gezien de verzameling koppels

$$R_f = \{(a, b) \in A \times B \mid f(a) = b\}$$

Deze definitie is aangewezen voor de verzamelingtheoretische opbouw van de wiskunde, en drukt uit dat het concept *afbeelding* kan gemodelleerd worden door een verzameling geordende paren. Niettemin is de intuïtie bij wiskundigen over afbeeldingen die van input-outputmachines, en niet die van deelverzamelingen van het cartesisch product. We zullen voortaan dan ook schrijven

$$f(a) = b \qquad \text{i.p.v.} \qquad (a, b) \in R_f$$

Het is voor een partiële afbeelding mogelijk dat elementen uit A geen beeld hebben. Dat is in het algemeen slechts van geringe, formele betekenis, aangezien men in praktische gevallen voornamelijk geïnteresseerd is in de argumenten waarvoor wel een beeld bestaat. Men moet alleen opletten niet een functiewaarde te willen berekenen voor een argument waarvoor de afbeelding niet gedefinieerd is.

Vaak komt men afbeeldingen tegen die niet één argument nodig hebben om hun resultaat te bepalen, maar n elementen als invoer nemen. Die kunnen we

gewoon opvatten als afbeeldingen waarvan het domein een cartesisch product is. Op die manier worden meerplaatsige afbeeldingen speciale gevallen van afbeeldingen in het algemeen, zodat we ze niet apart moeten behandelen. Onderstaand voorbeeld illustreert hoe we dit noteren.

$$\begin{aligned} f : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \times \mathbb{R}^+ &\to \mathbb{R} \\ (a, b, \sigma) &\mapsto f(a, b, \sigma) = \frac{1}{\sigma\sqrt{2\pi}} \int_a^b e^{-\frac{x^2}{2\sigma^2}} dx \end{aligned}$$

We kunnen afbeeldingen *beperken* tot een deel van hun domein.

Definitie 2.21

Als $f : A \to B$ een afbeelding is en $E \subseteq A$ een deelverzameling van het domein van f, dan is de **beperking** of **restrictie** van f tot E afbeelding die dezelfde beelden oplevert, maar enkel gedefinieerd op E:

$$\begin{aligned} f_{|E} : E &\to B \\ x &\mapsto f_{|E}(x) = f(x) \end{aligned}$$

De verzameling van alle functies van A naar B wordt genoteerd met B^A.

2.4.3 Injecties en surjecties

De voorwaarde om een functie te zijn, namelijk dat elk argument exact één beeld produceert, mag niet verward worden met de mogelijkheid dat verschillende argumenten *dezelfde* functiewaarde opleveren. Dit gebeurt namelijk vaak, dat bij een afbeelding f van A naar B, twee verschillende argumenten a_1 en a_2 afgebeeld worden op eenzelfde element van B, dus $f(a_1) = f(a_2)$. Als deze situatie nooit voorkomt, dus als verschillende originelen ook verschillende beelden produceren, zullen we de functie *injectief* noemen.

In het codomein B leven alle *mogelijke* waarden die functiewaarden kunnen aannemen. Het is echter mogelijk dat niet alle mogelijke waarden ook effectief bereikt worden door de elementen uit het domein A als origineel te geven voor de afbeelding. Als elk element van B wel degelijk het beeld is van één of ander element uit het domein, zullen we de functie *surjectief* noemen.

Definitie 2.22

- Een afbeelding $f : A \to B$ is **injectief** als elk element van B het beeld is van hoogstens één element van A, d.w.z. als

$$\forall a_1, a_2 \in A\,(f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$$

- Een afbeelding $f : A \to B$ is **surjectief** als elk element van B het beeld is van minstens één element van A, d.w.z. als

$$\forall b \in B : \exists a \in A : f(a) = b$$

- Een afbeelding $f : A \to B$ is **bijectief** als ze injectief en surjectief is, m.a.w. als elk element van B het beeld is van precies één element van A, d.w.z. als

$$\forall b \in B : \exists! a \in A : f(a) = b$$

  Een bijectie van een verzameling A op zichzelf wordt een **permutatie** genoemd.

Merk op dat injectiviteit en surjectiviteit sterk afhangen van het domein. De functie $x \mapsto x^2$ is bijvoorbeeld injectief als het domein $\mathbb{R}^+$ is, maar niet als het domein $\mathbb{R}$ is. Als functie van $\mathbb{R}^+$ naar $\mathbb{R}^+$ is ze surjectief, maar niet als functie van $\mathbb{N}$ naar $\mathbb{N}$.

In de wiskundige taal wordt een bijzondere aandacht besteed aan het voorzetselgebruik, zowel in het Nederlands als in het Engels. Een injectieve afbeelding van A naar B wordt een *injectie van A **in** B* genoemd. Een surjectieve afbeelding van A naar B wordt een *surjectie van A **op** B* genoemd.[2] Als men niet wil suggereren dat een afbeelding in- of surjectief is, gebruikt men het neutrale **naar**.

Een **origineel** van een element $b \in B$ voor een functie $f : A \to B$ is *een* element $a \in A$ waarvoor $f(a) = b$. De verzameling van alle originelen van een element $b \in B$ wordt de **vezel** van b onder f genoemd, en genoteerd als

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

[2] In het Engels worden surjecties *onto* genoemd, naar het voorzetsel dat naar/op betekent, eigenlijk *naar een positie op het oppervlak van*, zoals in "He threw his plate onto the floor" of "The band climbed onto the stage".

Deze vezel kan voor een algemene afbeelding één, meer of zelfs geen elementen bevatten. Als een afbeelding injectief is, dan heeft elke b ten hoogste één origineel. Als ze surjectief is, dan heeft elke b ten minste één origineel. Bij een bijectie bestaat er voor elk element uit het codomein een origineel dat bovendien uniek is.

Als $f : A \to B$ een afbeelding is en $X \subseteq A$, dan noemen we de verzameling beelden van elementen uit X, d.w.z. de verzameling

$$f[X] = \{b \in B \mid \exists x \in X : f(x) = b\} = \{f(x) \mid x \in X\}$$

het *beeld van X (onder f)*. Het *beeld van f* of het *bereik van f* is het beeld van zijn volledige domein, dit is

$$\mathrm{im}(f) = f[A] = \{b \in B \mid \exists a \in A : f(a) = b\} = \{f(a) \mid a \in A\}$$

Een afbeelding is een surjectie als codomein en beeld samenvallen.

Goed om weten is dat de samenstelling van injecties weer een injectie is, en de samenstelling van surjecties weer een surjectie. Hiervoor moeten we eerst definiëren wat de samenstelling van functies is.

2.4.4 Samenstelling en inverse

Als $f : A \to B$ en $g : B \to C$ afbeeldingen zijn, kunnen we een afbeelding definiëren die een $a \in A$ als origineel neemt, f gebruikt om $b = f(a)$ te bepalen en daarna g om $g(b)$ te bepalen *voor deze gevonden b*, dus $g(b) = g(f(a))$. Deze *samenstelling* van afbeeldingen kan algemener gedefinieerd worden, namelijk wanneer $g(b)$ goedgedefinieerd is voor alle b in het beeld van f, dus waarbij het domein van g het beeld $f[A]$ omvat.

Definitie 2.23

- Als $f : A \to B$ en $g : E \to C$ afbeeldingen zijn met $\text{im}(f) \subseteq E$, dan is de **compositie** of **samenstelling van** f **en** g de functie $g \circ f$, gedefinieerd door

$$\begin{aligned} g \circ f : A &\to C \\ x &\mapsto g \circ f\ (x) = g(f(x)) \end{aligned}$$

- Een afbeelding $f : A \to B$ wordt **inverteerbaar** genoemd als er een afbeelding $g : B \to A$ bestaat waarvoor

$$\forall a \in A, \forall b \in B : f(a) = b \ \Leftrightarrow\ g(b) = a$$

  Deze afbeelding g wordt een **inverse** van f genoemd en genoteerd als f^{-1}.

De samenstelling van functies (indien gedefinieerd) is associatief: $h \circ (g \circ f) = (h \circ g) \circ f$, maar over het algemeen niet commutatief: $f \circ g \neq g \circ f$. Men kan meer algemeen ook de samenstelling van relaties definiëren, maar dat laten we hier achterwege. Dat het begrip *inverse* voor afbeeldingen overeenstemt met het begrip *inverse relatie*, laten we als oefening. Ook een zinvolle oefening is het om te bewijzen dat een afbeelding $f : A \to B$ inverteerbaar als en slechts als er een $g : B \to A$ bestaat waarvoor

$$\forall a \in A : g \circ f(a) = a \qquad \text{en} \qquad \forall b \in B : f \circ g(b) = (b).$$

Stelling 2.24

Zij $f : A \to B$ een afbeelding. Dan is f inverteerbaar als en slechts als f een bijectie is. Bovendien, als f inverteerbaar is, dan is de inverse uniek.

Bewijs. Stel dat f inverteerbaar is, dan bestaat er een $g : B \to A$. Voor de injectiviteit van f, stel dat $f(a_1) = f(a_2) = b$. Daar g de inverse afbeelding is, is $g(b) = a_1$ en ook $g(b) = a_2$, dus $a_1 = a_2$. Voor de surjectiviteit, neem willekeurig $b \in B$. We moeten aantonen dat b bereikt wordt door f. Beschouw $a = g(b)$. Dan is $f(a) = f(g(b)) = b$, dus b is inderdaad het beeld van een $a \in A$. We besluiten dat f een bijectie is.

Stel nu dat f een bijectie is. We construeren nu een inverse afbeelding. Zij $b \in B$. Omdat f surjectief is, bestaat er een $a \in A$ zodat $f(a) = b$. Omdat f

injectief is, is deze a uniek. We kunnen dus een functie $g : B \to A$ definiëren, door het voorschrift: voor een $b \in B$, neem voor $g(b)$ het unieke element a van A waarvoor $f(a) = b$. Dit is duidelijk een inverse voor f.

Het bovenstaande bewijs vestigt ook de uniciteit van de inverse, want voor elke $b \in B$ is er maar één mogelijke $a \in A$ om te nemen als $g(b)$. □

Stelling 2.25

- De samenstelling van injecties is een injectie.
- De samenstelling van surjecties is een surjectie.
- De samenstelling van bijecties is een bijectie.

Bewijs.

- Zij f en g injecties. Stel dat $g \circ f\ (x) = g \circ f\ (y)$, of dus $g(f(x)) = g(f(y))$. Door injectiviteit van g is dan $f(x) = f(y)$ en door injectiviteit van f is $x = y$.
- Zij $f : A \to B$ en $g : B \to C$ surjecties. Zij $c \in C$ willekeurig. Dan is er een $b \in B$ zodat $g(b) = c$ wegens surjectiviteit van g. Door surjectiviteit van f is er een $a \in A$ waarvoor $f(a) = b$. Voor deze a geldt dat $g \circ f\ (a) = g(f(a)) = g(b) = c$.
- Combinatie van de vorige. □

2.4.5 Enkele veelvoorkomende afbeeldingen

We geven enkele voorbeelden van afbeeldingen die in verschillende takken van de wiskunde voorkomen, van mechanica tot statistiek.

De *identieke afbeelding* op een verzameling A is een afbeelding die altijd dezelfde waarde weergeeft als deze die gebruikt is als argument.

$$\begin{aligned} \mathbf{id}_A : A &\to A \\ a &\mapsto a \end{aligned}$$

Het is de meest eenvoudige bijectie (eigenlijk permutatie) die op elke verzameling leeft. Hoewel deze afbeelding er zielig uitziet, zal ze van belang zijn om inverse afbeeldingen te definiëren.

Nauw verwant is de *canonische injectie* of *inclusie* van een verzameling A in een verzameling B, waarvoor al geldt dat $A \subseteq B$. Deze is gewoon

$$\begin{aligned} i : A &\hookrightarrow B \\ a &\mapsto a \end{aligned}$$

Ze wordt *canonisch* genoemd omdat ze de meest natuurlijke injectie is die men kan bedenken van $A \subseteq B$ naar B. Voor inclusies en meer algemeen, injecties, wordt in de definitie af en toe het symbool $\hookrightarrow$ gebruikt i.p.v. $\to$, om duidelijk te maken dat het over een injectie gaat.

Als $A \subseteq B$, dan is de *karakteristieke functie* of *indicator* van A de afbeelding die lidmaatschap van de deelverzameling A aangeeft

$$\begin{aligned} \mathbf{1}_A : B &\to \{0,1\} \\ a &\mapsto \begin{cases} 1 & \text{als } x \in A, \\ 0 & \text{als } x \notin A. \end{cases} \end{aligned}$$

De indicator van de identiteitsrelatie in een cartesisch product is de bruikbare *Kronecker delta*, een tweewaardige functie die afhangt van twee elementen (meestal natuurlijke getallen die gebruikt worden als indices).

$$\begin{aligned} \delta : A \times A &\to \{0,1\} \\ (i,j) &\mapsto \delta(i,j) = \delta_{ij} = \begin{cases} 0 & \text{als } i \neq j \\ 1 & \text{als } i = j \end{cases} \end{aligned}$$

Als op een verzameling een equivalentierelatie $\sim$ gedefinieerd is, dan wordt met de *projectieafbeelding* of de *canonische projectie* de afbeelding

$$\begin{aligned} \pi : A &\twoheadrightarrow A/\!\sim \\ a &\mapsto \pi(a) = [a] \end{aligned}$$

bedoeld. Voor projecties en meer algemeen, surjecties, wordt in de definitie soms het symbool $\twoheadrightarrow$ gebruikt i.p.v. $\to$.

2.4.6 Eerste isomorfiestelling

We vermelden nog dit belangrijk resultaat, dat voor zich zou moeten spreken, maar waarvan het instructief is om het bewijs eens precies neer te schrijven. De stelling geeft een soort van constructie om een willekeurige afbeelding om te vormen tot een bijectie.

Stelling 2.26

Zij $f : X \to Y$ een afbeelding. Dan is

$$\mathrm{Ker}(f) = \{(x_1, x_2) \in X \times X \mid f(x_1) = f(x_2)\}$$

een equivalentierelatie. Bovendien induceert f een bijectie

$$\hat{f} : X/\mathrm{Ker}(f) \to \mathrm{im}(f)$$

Bewijs. Oefening. □

In verschillende takken van de algebra zal men een resultaat vinden dat bekend staat als *de eerste isomorfiestelling*. Dit komt omdat algebraïsche structuren, doorgaans verzamelingen met extra *structuur*, aanleiding geven tot een meer bijzonder begrip dan bijectie, namelijk *isomorfisme*: een bijectie die de structuur *bewaart*. Als f dan een soort projectieafbeelding t.o.v. een deelstructuur is, dan is het vaak mogelijk om een dergelijke structuurbewarende bijectie te leggen. Meer hierover in *Algebra I*.

2.4.7 Keuzefuncties en willekeurige cartesische producten

Nu we het concept *afbeelding* hebben, zijn we in staat om het cartesisch product te definiëren voor een familie van verzamelingen. Gegeven een familie verzamelingen $\{F_i \mid i \in I\}$, definiëren we een *keuzefunctie* voor $\{F_i \mid i \in I\}$ als een afbeelding

$$f : I \to \cup_{i \in I} F_i$$

die elke index $i \in I$ (of dus elke verzameling F_i) afbeeldt op *een* element $f(i) \in F_i$ (dus als het ware in elke F een element *kiest*). Het **cartesisch product**

$$\prod_{i \in I} F_i$$

is de verzameling van alle keuzefuncties voor de familie $\{F_i \mid i \in I\}$.

Bijvoorbeeld, als $I = \{1, 2\}$, en $\{F_i \mid i \in I\}$ een familie verzamelingen is, door I geïndexeerd, dan kiest een keuzefunctie een element $x_1 \in F_1$ en een element $x_2 \in F_2$, dus die kan voorgesteld worden als een koppel (x_1, x_2), een

element van $F_1 \times F_2$. Dus in dit geval is $\prod_{i\in\{1,2\}} F_i$ in essentie hetzelfde als $F_1 \times F_2$.

Zo hebben we meteen het cartesisch product van een eindig aantal verzamelingen $A_1 \times \cdots \times A_n$ gedefinieerd: het is de verzameling van alle keuzefuncties

$$f : \{1, 2, \ldots, n\} \to \bigcup_{i=1}^{n} A_i$$

met de eigenschap dat voor elke i, $f(i) \in A_i$. Zo'n keuzefunctie noemen we ook wel een geordende n-tal en noteren we als

$$(a_1, \ldots, a_{n-1}, a_n).$$

Net zoals we koppels hebben gedefinieerd, hebben zij ook de eigenschap dat

$$(a_1, \ldots a_n) = (\alpha_1, \ldots, \alpha_n) \quad \text{als en slechts als} \quad a_1 = \alpha_1, \ldots, a_n = \alpha_n.$$

Indien de factoren dezelfde zijn ($A_i = A$ voor alle $i \leq n$) dan noteren we het cartesisch product als A^n. Als één van de verzamelingen F_i ledig is, dan is het cartesisch product ook leeg: een keuzefunctie kan niet bestaan. Voor de omgekeerde implicatie is het nog even wachten tot paragraaf 2.5.3.

2.4.8 Het functieconcept in historisch perspectief

Aan de basis van het moderne concept *functie* ligt het werk van twee wiskundigen, de Fransman Joseph Fourier (1768–1830) en de Duitser met Belgische roots Lejeune Dirichlet (1805–1859). De wiskundige methoden die Fourier gebruikte in zijn groots werk over hitteoverdracht, zijn nu onmisbaar in vele takken van de wiskunde, fysica en ingenieurswetenschappen, maar veroorzaakten controverse in zijn tijd. Fourier ontwikkelde functies als oneindige goniometrische reeksen en verlegde daarmee de grenzen van hoe men toen aankeek tegen functies, namelijk als berekeningsprocessen. Dirichlet ging erop verder en zette de hele theorie van Fourier op stevige grondvesten, waardoor hij beschouwd wordt als de vader van de fourieranalyse. Zijn ideeën waren het die ons het moderne functieconcept hebben gegeven.

De belangrijkste les hieruit voor de beginnende wiskundige is dat de hoge abstractiegraad in de wiskunde, waarvan het functieconcept slechts een voorbeeld is, er niet gemakkelijk gekomen is, noch zonder reden. Wanneer we bedenken dat het werk van Fourier en Dirichlet, dat wiskundigen dwong hun

notie van functie te herconceptualiseren, aan het hart ligt van moderne synthesizers, internetprotocollen, het MP3-formaat en een rist andere toepassingen, waaronder de originele vraagstukken omtrent hitteoverdracht die Fourier oorspronkelijk motiveerden, dan realiseren we ons dat deze abstractie het resultaat was van beslist praktische toepassingen. Dit is een verschijningsvorm van de sterkte van wiskunde, haar abstractie.

2.5 Ordes

Het idee dat we hebben bij het concept "ordening" wordt geformaliseerd in het wiskundige begrip *orderelatie*.

2.5.1 Orderelaties

Definitie 2.27

- Een relatie $\preceq \subseteq A \times A$ is een **orderelatie** of **partiële orderelatie** als $\preceq$ reflexief, antisymmetrisch en transitief is.
- Een **(partiële) orde**, **(partieel) geordende verzameling** of **poset** is een verzameling, voorzien van een partiële orderelatie. Meer specifiek is het een koppel $(A, \preceq)$, met A een verzameling en $\preceq$ een partiële orderelatie op A.
- Een orde $(A, \preceq)$ is **totaal** of **lineair** als elke twee elementen vergelijkbaar zijn, d.w.z. als

  $$\forall a, b \in A : a \preceq b \vee b \preceq a$$

  Een totaal geordende deelverzameling van A wordt een **keten** (chain) genoemd.

Een relatie die enkel reflexief en transitief is, wordt een *pre-orderelatie* genoemd. Een relatie die irreflexief, antisymmetrisch en transitief is, heet *strikt-orderelatie*.

Enkele voorbeelden van ordes:

- De natuurlijke ordeningen $\leq$ op de getallenverzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ zijn totaal.

- Voor elke verzameling A, is $\subseteq$ een partiële orderelatie op $\mathcal{P}(A)$.
- De deelbaarheidsrelatie is een partiële orderelatie in $\mathbb{N} \setminus \{0\}$.
- De deelruimten van een vectorruimte zijn geordend door inclusie.

Als we kunnen spreken van "groter dan", dan kunnen we ook spreken van "grootste" en "kleinste". Omdat niet alle ordeningen totaal zijn, zijn er verschillende begrippen voor verschillende definities.

Definitie 2.28

Zij $(A, \preceq)$ een orderelatie.

- Als $S \subseteq A$, dan wordt $x \in S$ een **kleinste element van** S genoemd als alle andere groter of gelijk zijn, m.a.w. als

  $$\forall y \in S : x \preceq y$$

  en x is een **grootste element** als $\forall y \in S : y \preceq x$.
- Een element m is een **minimaal element** als er geen kleiner bestaat, m.a.w. als

  $$\neg\exists a \in A \setminus \{m\} : a \preceq m$$

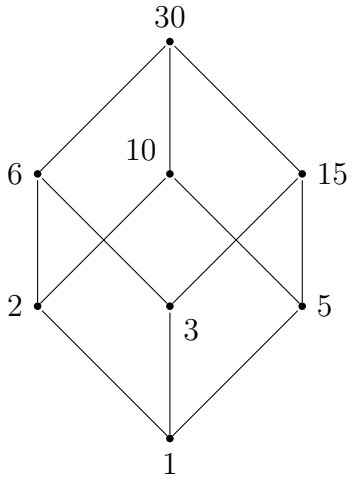
  Een element m is **maximaal** als $\neg\exists a \in A \setminus \{m\} : m \preceq a$.
- Als $S \subseteq A$, dan wordt $x \in A$ een **ondergrens voor** S genoemd als alle elementen van S groter of gelijk zijn, m.a.w. als

  $$\forall y \in S : x \preceq y$$

  en x is een **bovengrens voor** S als $\forall y \in S : y \preceq x$. Onder- en bovengrenzen moeten niet tot de verzameling S zelf behoren.

Kleinste en grootste elementen bestaan niet altijd. Als A een oneindige verzameling is, dan is $(\mathcal{P}(A), \subseteq)$ een orde waarvoor de deelverzameling van alle eindige deelverzamelingen van A geen grootste element heeft. Ordes kunnen één, geen of verschillende minimale of maximale elementen hebben, en zelfs elementen die tegelijk minimaal en maximaal zijn.

Een verzameling A en een partiële orderelatie $\preceq$ kunnen we grafisch voorstellen door een zogenaamd **Hassediagram**. Een keten $a_1 \preceq a_2 \preceq \ldots \preceq a_n$ wordt voorgesteld door de opeenvolgende elementen a_i en a_{i+1} met elkaar te



Figuur 2.5: Hassediagram van de delingsrelatie op $\{1, 2, 3, 5, 6, 10, 15, 30\}$

verbinden, waarbij *kleinere* elementen op de figuur *onder* de *grotere* elementen getekend worden. Er komen dus geen horizontale lijnen voor in een Hassediagram. Indien A eindig is en elke keten een kleinste en grootste element heeft met betrekking tot $\preceq$, dan illustreert een Hassediagram $\preceq$ volledig.

2.5.2 Welordeningen en het welordeningsprincipe

Definitie 2.29

Een **welorderelatie** op een verzameling A is een totale orderelatie $\preceq$ op A met de eigenschap dat elke niet-ledige deelverzameling van A een kleinste element heeft, m.a.w. zodat

$$\forall S \in \mathcal{P}(A) : \exists x \in S : \forall s \in S : x \preceq s$$

Een verzameling met daarop een welorderelatie gedefinieerd wordt een *welgeordende* verzameling genoemd, of kort een *welordening*.

Intuïtief kan men begrijpen dat de verzameling van de natuurlijke getallen $\mathbb{N}$ welgeordend wordt door $\leq$.

Welordeningsprincipe

Elke deelverzameling van $\mathbb{N}$ heeft een kleinste element.

Toch is het niet mogelijk om, in een logisch systeem zoals de Peanorekenkunde (zie Appendix A) zonder wiskundige inductie te bewijzen dat dit principe geldig is. Met inductie bedoelen we één van de volgende principes.

Inductieprincipe over $\mathbb{N}$

Zij $S \subseteq \mathbb{N}$, met de eigenschap dat als $n \in S$, dan ook $n + 1 \in S$. Als $1 \in S$, dan is $S = \mathbb{N}$.

Sterk inductieprincipe over $\mathbb{N}$

Zij $S \subseteq \mathbb{N}$, met de eigenschap dat als voor alle $m < n : m \in S$, dan ook $n \in S$. Als $1 \in S$, dan is $S = \mathbb{N}$.

Het inductieprincipe volgt uit het welordeningsprincipe. Eigenlijk is zelfs meer waar:

Stelling 2.30

Uit elk van de volgende kun je de andere twee met elementaire methoden bewijzen.

- Het welordeningsprincipe
- Het inductieprincipe
- Het sterke inductieprincipe

Bewijs. We zullen hier enkel bewijzen dat het inductieprincipe volgt uit het welordeningsprincipe en laten de rest als oefening.

Zij $S \subseteq \mathbb{N}$, met de eigenschap dat als $n \in S$, dan ook $n + 1 \in S$ en met $1 \in S$. Indien $S \neq \mathbb{N}$, dan zou het complement van S ten opzichte van $\mathbb{N}$, namelijk $S^c = \{r \in \mathbb{N} \mid r \notin S\}$ een niet-ledige deelverzameling van $\mathbb{N}$. Door het welordeningsprincipe bezit S^c een kleinste element m. Aangezien echter $1 \in S$, zal $m \neq 1$. Bijgevolg is $m - 1 \in \mathbb{N}$, maar aangezien m het kleinste

element is van S^c, zal $m-1 \in S$. Stel nu $n = m-1$ in de karakteriserende eigenschap van S, dan volgt hieruit dat $m \in S$, een tegenstrijdigheid. Dus we mogen besluiten dat $S = \mathbb{N}$. □

Gevolg 2.31

Het bewijs door (sterke) inductie is een geldige bewijstechniek.

Bewijs. Dat, voor een predikaat P op $\mathbb{N}$, de waarheid van $\forall n \in \mathbb{N} : P(n)$ volgt uit de inductiebasis en (sterke) inductiestap, krijgen we door toepassing van het (sterke) inductieprincipe op de verzameling $S = \{n \in \mathbb{N} \mid P(n)\}$. □

Dat het bewijs door (sterke) inductie geldig is, werd hier voorgesteld als een gevolg. We herhalen dat dit waar is op voorwaarde dat we het weloreningsprincipe als axioma aannemen. De Peanorekenkunde is een beperkt logisch systeem, dat bedoeld is om de natuurlijke getallen te beschrijven. Hierbinnen is één van de drie uitspraken uit Stelling 2.30 nodig als axioma of als bewijsregel — het welordeningsprincipe volgt niet uit de standaardaxioma's van de natuurlijke getallen. In de Peanorekenkunde is gekozen om als negende en laatste axioma het inductieprincipe toe te voegen: dit is uitspraak 2.2.5, universeel gekwantificeerd *over alle predikaten* A. Door deze kwantificatie over predikaten wordt het het enige tweede-orde-axioma, waardoor de onvolledigheidsstellingen van Gödel (zie paragraaf 1.5.3) van toepassing zijn op de Peanorekenkunde.

In de ZFC-verzamelingenleer, die niet alleen de natuurlijke getallen maar de hele wiskunde wil beschrijven, zit de subtiliteit van het welordeningsprincipe in de definitie van $\mathbb{N}$ als de kleinste inductieve verzameling, waarvan het bestaan wordt gegarandeerd door het axioma van oneindigheid. Een schets van het bewijs van het welordeningsprincipe binnen ZFC geven we op pagina 92.

2.5.3 Keuzeaxioma

De definities uit deze paragraaf over ordening, samen met het begrip van willekeurige cartesische producten via keuzefuncties (zie pagina 68), zijn voldoende achtergrond om enkele beruchte uitspraken te formuleren.

Keuzeaxioma (Zermelo, 1904)

Het cartesisch product van niet-ledige verzamelingen is niet-ledig. Of: elke familie verzamelingen laat een keuzefunctie toe.

Het keuzeaxioma zegt ruwweg dat het *wiskundig mogelijk* is om gegeven een collectie verzamelingen, uit elke verzameling één element te kiezen (tegelijk). In veel gevallen kan een dergelijke selectie worden gemaakt zonder een beroep te doen op het keuzeaxioma. Dit is zo als er maar een eindig aantal verzamelingen zijn of als er een onderscheidende eigenschap bestaat die maar voor één element in elk van de verzamelingen geldt, bijvoorbeeld als de elementen ervan genummerd zijn met natuurlijke getallen. Om dat te verduidelijken: als men een oneindige verzameling van paren schoenen heeft, is het mogelijk om uit elk paar één schoen te kiezen, zonder het keuzeaxioma aan te roepen (neem bijvoorbeeld telkens de rechterschoen). Maar voor een oneindige verzameling van paren sokken, kan men een dergelijke selectie enkel realiseren met behulp van het keuzeaxioma. Dit voorbeeld komt van Bertrand Russell zelf, één van de protagonisten in de grondslagencrisis (zie 2.9).

Het keuzeaxioma lijkt vanzelfsprekend, maar blijkt niet te volgen uit alle andere axioma's van ZFC.

Lemma van Zorn

Zij $(A, \preceq)$ een partieel geordende verzameling. Als elke keten in A een bovengrens heeft, dan heeft A een maximaal element.

Welordeningsstelling

Elke verzameling kan welgeordend worden.

Deze drie uitspraken blijken equivalent te zijn met elkaar, in de zin dat elk ervan, samen met de axioma's van Zermelo-Fraenkel, voldoende is om de andere te bewijzen. Het bewijs van hun equivalentie komt aan bod in *Logica I*.

Heel wat belangrijke stellingen gebruiken het keuzeaxioma in hun bewijs, in de vorm van het lemma van Zorn. Voorbeelden zijn de stelling van Hahn-Banach in functionaalanalyse (zie *Wiskundige Analyse IV*), de stelling dat elk veld een algebraïsche sluiting heeft (zie verder of zie *Algebra II*), de stelling

dat elke nietnulring een maximaal ideaal heeft, de stelling dat elke partiële orde kan uitgebreid worden tot een lineaire orde, of de stelling van Tychonoff in de topologie. Het lemma van Zorn is een handige en bruikbare vorm van het keuzeaxioma, misschien wel de vorm waarin het keuzeaxioma het meest toegepast wordt. Bepaalde cursussen in de opleiding wiskunde zullen het ook gebruiken, zoals in het bewijs van de stelling dat elke vectorruimte een basis heeft (zie *LAAM I*). Soms wordt het keuzeaxioma impliciet gebruikt, in zinnen als *Kies nu in elk van deze verzamelingen een element.*

In het begin van de twintigste eeuw was het gebruik van het keuzeaxioma omstreden, omdat het tot contra-intuïtieve resultaten leidde, zoals de Banach-Tarskiparadox. Tegenwoordig wordt het door bijna alle wiskundigen zonder terughoudendheid gebruikt.

2.6 Kardinaliteiten

Er zijn archeologische aanwijzingen dat mensen al ten minste 50 000 jaar *tellen*: dit werd door antieke culturen voornamelijk gebruikt om sociale en economische data bij te houden, zoals de grootte van mensengroepen, prooidieren, bezit of schulden. De geschiedenis van het *tellen* gaat dus veel verder terug dan die van de *getallen*, of de eerste talstelsels, de oudst bekende daterend van 5 000 jaar geleden.

Antieke beschavingen registreerden hoeveel objecten eigendom waren, door te *turven*. Om pakweg de grootte van een schapenkudde bij te houden, werd een hoopje steentjes of stokjes bijgehouden, evenveel als schapen. Bij het binnenhalen van de kudde werd dan een steentje opzijgelegd per schaap dat binnenkwam, zodat men zich ervan kon verzekeren dat de hele kudde binnen was. Als de eigenaar gevraagd werd hoeveel schapen hij had, zou die de collectie steentjes tonen: *zo veel*. Voor zo'n doeleinden is een universeel systeem van abstracte getallen niet nodig, het is voldoende om de notie van een *één-één-correspondentie* te hebben, hetgeen we vandaag *bijectie* noemen. Dit fundamentele en oeroude concept, dat we nu wel precies hebben gedefinieerd, leidt ons tot de eerste definitie.

2.6.1 Gelijkmachtigheid

Definitie 2.32

Twee verzamelingen A en B zijn **gelijkmachtig** of **hebben dezelfde kardinaliteit** als er een bijectie bestaat van A naar B. In dat geval schrijven we

$$|A| = |B|$$

We hebben nog niet gezegd wat *kardinaliteit* is of wat het symbool $|A|$ betekent — dat is eigenlijk ook niet nodig, maar we komen erop terug op pagina 86. We kunnen alvast het volgende bewijzen.

Stelling 2.33

Voor verzamelingen A, B en C geldt:

(i) $|A| = |A|$

(ii) $|A| = |B| \quad \Rightarrow \quad |B| = |A|$

(iii) $|A| = |B| \ \wedge \ |B| = |C| \quad \Rightarrow \quad |A| = |C|$

Bewijs. (i) Gebruik de bijectie $\mathbf{id}_A$.

(ii) Wegens stelling 2.24 is de bijectie $f : A \to B$ inverteerbaar. Gebruik f^{-1}.

(iii) Gebruik de samenstelling der bijecties, weer een bijectie wegens stelling 2.25. □

We zeggen dat een verzameling A een *kleinere kardinaliteit* heeft dan B, als er een injectie bestaat van A in B, en we schrijven $|A| \leq |B|$. Als er bovendien geen bijectie bestaat, dan heeft A een *strikt kleinere kardinaliteit* dan B en we noteren $|A| < |B|$.

2.6.2 Stellingen over kardinaliteiten

Verrassend genoeg zijn er vele beweringen die duidelijk lijken, maar die niet kunnen bewezen worden zonder het keuzeaxioma. De volgende stellingen zijn

belangrijk en interessant, maar voor sommige bewijzen is het wachten tot het derde jaar bachelor wiskunde.

Stelling 2.34 — Principe van kardinaliteitenvergelijkbaarheid

Elke twee verzamelingen zijn vergelijkbaar, m.a.w. voor elke twee verzamelingen A en B is $|A| \leq |B|$ of $|B| \leq |A|$.

Bewijs. Zie *Logica I*. Eigenlijk is deze stelling equivalent met het keuzeaxioma. □

Stelling 2.35

Zijn $A \neq \varnothing$ en B verzamelingen. Er bestaat een injectie van A in B als en slechts als er een surjectie van B naar A bestaat.

Bewijs. De richting $\Leftarrow$ maakt gebruik van het keuzeaxioma en wordt bewezen in *Logica I*. De implicatie $\Rightarrow$ kunnen we zonder bewijzen. Zij $f : A \to B$ een injectie en zij a een willekeurig element van A. Definieer nu de functie

$$g : B \to A$$
$$y \mapsto \begin{cases} x & \text{als } f(x) = y \\ a & \text{als geen zo'n } x \text{ bestaat} \end{cases}$$

Omdat f injectief is, is x uniek bepaald (als x bestaat), dus g is goed gedefinieerd. Omdat elke $x \in A$ bereikt wordt door een $y = f(x)$, is g surjectief. □

Stelling 2.36 — Cantor – Schröder – Bernstein

Als er tussen twee verzamelingen A en B injecties $f : A \to B$ en $g : B \to A$ bestaan, dan bestaat er ook een bijectie $h : A \to B$, m.a.w.

$$|A| \leq |B| \ \wedge \ |B| \leq |A| \quad \Rightarrow \quad |A| = |B|$$

Bewijs. Zie *Logica I*. □

Het rechtstreeks uitsluiten van het bestaan van bijecties tussen verzamelingen is meestal moeilijk. In één geval, opgemerkt door Cantor, kunnen we dat wel. De stelling van Cantor gebruikt zijn fameuze *diagonaalargument*.

Stelling 2.37 — Stelling van Cantor

Er bestaat een injectie maar geen bijectie van een verzameling naar zijn machtsverzameling. D.w.z, voor elke verzameling A geldt

$$|A| < |\mathcal{P}(A)|.$$

Bewijs. Een injectie is eenvoudig, neem bijvoorbeeld

$$\begin{aligned} f : X &\to \mathcal{P}(X) \\ x &\mapsto \{x\}, \end{aligned}$$

wat een injectie definieert wegens het axioma van extensionaliteit.

Stel nu uit het ongerijmde dat er een bijectie $h : X \to \mathcal{P}(X)$ bestaat. Beschouw de verzameling

$$Y = \{x \in X \mid x \notin h(x)\}.$$

Daar h een bijectie is, is er een unieke $y \in X$ waarvoor $h(y) = Y \in \mathcal{P}(X)$. Maar dan is

$$y \notin h(y) \quad \Leftrightarrow \quad y \in Y \quad \Leftrightarrow \quad y \in h(y),$$

een strijdigheid. □

2.6.3 De natuurlijke getallen

Voor vele voorbeelden tot hier toe, als indexverzameling en bij het welordenings- en inductieprincipe hebben we subtiel de verzameling $\mathbb{N}$ van de natuurlijke getallen *gebruikt*. Dat is niet verwonderlijk, het is de meest natuurlijke niet-triviale verzameling die men beschouwt als men wiskunde of een andere wetenschap wil bedrijven. Van Leopold Kronecker (1823–1891) is geweten dat hij eens uitriep:

> *Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.*

De naam *natuurlijke getallen* is dan ook niet verkeerd gekozen: ze zijn ons van kindsbeen af ingelepeld, wanneer we leerden tellen. Laat dat precies de reden zijn waarvoor we ze hier zullen nodig hebben.

Hoe de natuurlijke getallen precies gedefinieerd worden, of beter, gemodelleerd worden in de verzamelingenleer, beschrijven we in paragraaf 2.7. Middels die wegomlegging kunnen we weer verdergaan op het rigoureuze pad. Het volstaat voor de doeleinden van deze paragraaf om zich de natuurlijke getallen voor te stellen als de verzameling

$$\mathbb{N} = \{0, 1, 2, 3, \ldots, n, \ldots\}.$$

Voor een natuurlijk getal n noteren[3] we de verzameling van alle natuurlijke getallen kleiner dan n met $\mathbb{N}_{<n}$:

$$\mathbb{N}_{<n} = \{0, 1, \ldots, n-1\}.$$

Bij wijze van afspraak leggen we ook de volgende notaties vast.

$$\begin{aligned} \mathbb{N}^* &= \{1, 2, 3, \ldots, n, \ldots\} \\ \mathbb{Z} &= \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}. \end{aligned}$$

De notatie $\mathbb{Z}$ voor de verzameling van de gehele getallen is een internationale standaardnotatie, afkomstig van het Duitse *Zahl*.

Men kan een semantische discussie opstarten over de natuurlijkheid van het getal 0. Internationaal zijn hierover geen afspraken gemaakt. In de verzamelingenleer, informatica en algebra zijn er goede redenen om te opteren voor 0 als natuurlijk getal, dus deze conventie zullen we hier aanhouden.

We zullen de natuurlijke getallen nodig hebben voor de definities van eindigheid en aftelbaarheid.

2.6.4 Eindige verzamelingen

Definitie 2.38

- Een verzameling A is een **eindige verzameling** als er een $n \in \mathbb{N}$ bestaat zodat er een bijectie is van $\mathbb{N}_{<n}$ naar A.
- Een **oneindige verzameling** is een verzameling die niet eindig is.

[3] Deze notatie is geïnspireerd op een richtlijn van Terence Tao. Ze heeft talloze voordelen, niet in het minst dat van de duidelijkheid.

Als A in bijectie is met $\mathbb{N}_{<n}$ schrijven we $|A| = n$.

Dit is de meest gebruikelijke definitie voor eindigheid, en wordt soms Peano-eindigheid genoemd. Men kan ook de volgende definities hanteren: een verzameling A is Dedekind-oneindig als er een bijectie bestaat tussen A en een *echte* deelverzameling van A, en Dedekind-eindig als dat niet zo is. De volgende stelling heeft geen moeilijk bewijs, maar het gebruikt noodzakelijk wel het keuzeaxioma.

Stelling 2.39

Een verzameling is Peano-eindig als en slechts als ze Dedekind-eindig is.

Bewijs. Zie oefeningenles. □

De studie van eindige verzamelingen is de *combinatoriek*. In het volgende hoofdstuk zullen we dan ook de kardinaliteiten bepalen van de verzamelingen van deelverzamelingen, functies, injecties, surjecties, ... van eindige verzamelingen. Ook telprincipes, zoals de dubbele telling, het inclusie-exclusieprincipe en het duivenhokprincipe behoren tot dit domein, dat aangeraakt wordt in Hoofdstuk 3.

2.6.5 Aftelbaarheid

Definitie 2.40

- Een verzameling A is een **aftelbare verzameling** als er een surjectie bestaat van $\mathbb{N}$ op A.
- Een **overaftelbare verzameling** is een verzameling die niet aftelbaar is.
- Een verzameling A is **aftelbaar oneindig** als er een bijectie bestaat van $\mathbb{N}$ naar A.

Hoewel dit de meest gangbare benamingen zijn, gebruiken sommige auteurs het woord *aftelbaar* voor *aftelbaar oneindig* en spreken ze over *ten hoogste aftelbaar* voor *aftelbaar*.

Een bijectie $f : \mathbb{N} \to A$ die voor de aftelbare oneindigheid van de verzameling A getuigt, *telt* letterlijk de elementen van A af: de rij $f(0), f(1), f(2), \ldots$ zal

precies de verzameling A zijn, omdat f een bijectie is. Noemen we $f(i) = a_i \in A$, dan is

$$A = \{a_0, a_1, a_2, \dots\}.$$

Aftelbaar oneindige verzamelingen A en B hebben dezelfde kardinaliteit: $|A| = |B|$, wegens stelling 2.33 en de definitie van aftelbaar oneindig die $|\mathbb{N}| = |A|$ en $|\mathbb{N}| = |B|$ betekent.

Van veel verzamelingen kan men eenvoudig zien dat ze aftelbaar zijn. De verzamelingen $\mathbb{N}$ zelf, die van de even getallen, de verzameling $\{1/n \mid n \in \mathbb{N}\}$ of $\mathbb{Z}_{<0}$ zijn aftelbaar oneindig.

We zullen nu van de belangrijkste getallenverzamelingen, namelijk $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$, bewijzen of ze aftelbaar zijn of niet. We doen dat ook voor het cartesisch product $\mathbb{N} \times \mathbb{N}$.

Stelling 2.41

$\mathbb{Z}$ is aftelbaar.

Bewijs. De afbeelding

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto f(n) = \begin{cases} \frac{n}{2} & \text{als } n \text{ even is} \\ -\frac{n+1}{2} & \text{als } n \text{ oneven is.} \end{cases} \end{aligned}$$

is een bijectie. □

De aftelling van $\mathbb{Z}$ die deze bijectie oplevert, is

$$0, -1, 1, -2, 2, -3, 3, \dots$$

Stelling 2.42

$\mathbb{Q}$ is aftelbaar.

Bewijs. Beschouw voor elk rationaal getal, verschillend van 0, zijn vorm als onvereenvoudigbare breuk a/b met $a \neq 0$ en dat $b > 0$. Noem het *niveau* van een niet-nul-breuk a/b het natuurlijk getal $\max(|a|, b)$, en stel het niveau van 0 gelijk aan 0.

Rangschik nu alle rationale getallen volgens hun niveau en rangschik *per niveau* alle rationale getallen op dit niveau volgens de natuurlijke ordening $<$ op $\mathbb{Q}$. Zo ontstaat de volgende opsomming van $\mathbb{Q}$.

niveau								
0	0							
1	-1	1						
2	-2	$-1/2$	$1/2$	2				
3	-3	$-3/2$	$-2/3$	$-1/3$	$1/3$	$2/3$	$3/2$	3
4	-4	$-4/3$	$-3/4$	$-1/4$	$1/4$	$3/4$	$4/3$	4
$\vdots$	$\vdots$							

Voor elk natuurlijk getal n is er maar een eindig aantal rationale getallen van niveau n. Elk rationaal getal komt juist één maal voor in deze lijst. Doorlopen we de lijst per niveau, en binnen een niveau van links naar rechts, dan tellen we zo alle rationale getallen af. De bijectie beeldt een $n \in \mathbb{N}$ dan af op het n-de rationaal getal in deze lijst. Dus $\mathbb{Q}$ is aftelbaar. □

Stelling 2.43

$\mathbb{N} \times \mathbb{N}$ is aftelbaar.

Bewijs. Splits $\mathbb{N} \times \mathbb{N}$ op in eindige maar langer wordende nevendiagonalen

$$S_k = \{(i, j) \in \mathbb{N} \times \mathbb{N} \mid i + j = k\}.$$

Zo'n verzameling S_k bevat $k + 1$ paren, namelijk

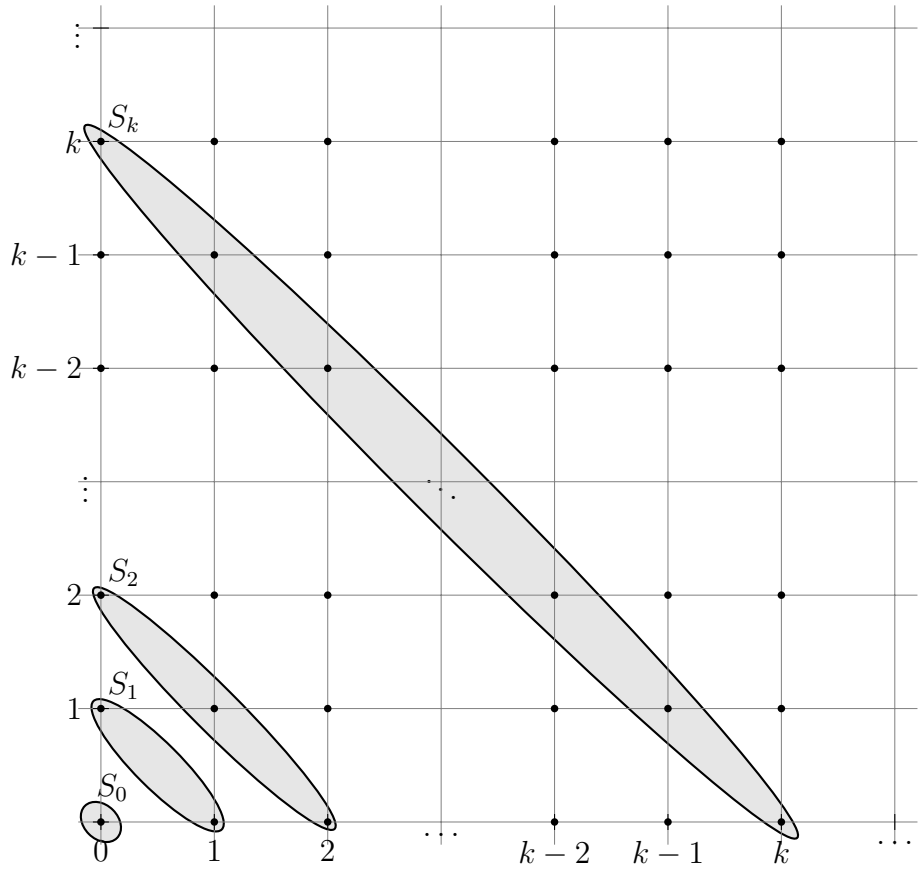
$$S_k = \{(0, k), (1, k - 1), \ldots, (k, 0)\}.$$

Schrijf nu $\mathbb{N} \times \mathbb{N}$ als een rij door eerst het element van S_0 te geven, daarna de twee elementen van S_1, daarna de drie elementen van S_2, enzovoort.

We kunnen hiervoor een expliciete bijectie opschrijven. Het koppel (i, j) is het $(j + 1)$-ste element van S_{i+j} en wordt dus voorafgegaan door j andere elementen in S_{i+j}, samen met alle elementen in $S_0 \cup S_1 \cup \ldots \cup S_{i+j-1}$ (in aantal $1 + 2 + \cdots + (i + j) = (i + j)(i + j + 1)/2$. Dus de afbeelding

$$\begin{aligned} \pi : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (i, j) &\mapsto \pi(i, j) = \frac{(i + j)(i + j + 1)}{2} + j \end{aligned}$$

is een bijectie. □



Figuur 2.6: De indeling van $\mathbb{N} \times \mathbb{N}$

Dit bewijs is niet het kortste, maar is instructief in de zin dat het de lezer in staat stelt te *begrijpen* waarom een "vlak" van koppels natuurlijke getallen "evenveel" elementen bevat als de natuurlijke getallen zelf. Een ander eenvoudig bewijs verkrijgt men met de meer getaltheoretische bijectie $(m, n) \mapsto 2^m(2n + 1)$ van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}^*$.

Dat $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ stelt ons in staat om een eenvoudiger bewijs te geven voor de aftelbaarheid van $\mathbb{Q}$.

Alternatief bewijs voor stelling 2.42. Zij π de bijectie uit stelling 2.43, f de bijectie uit stelling 2.41, p de bijectie $p : \mathbb{N} \to \mathbb{N}^* : n \mapsto n + 1$, met als cartesisch product de afbeelding

$$\begin{aligned} f \times p : \mathbb{N} \times \mathbb{N} &\to \mathbb{Z} \times \mathbb{N}^* \\ (m, n) &\mapsto (f(m), p(n)) \end{aligned}$$

en q de surjectie

$$\begin{aligned} q : \mathbb{N} \times \mathbb{N} &\twoheadrightarrow \mathbb{Q} \\ (a, b) &\mapsto a/b \end{aligned}$$

Dan is de samenstelling van de surjecties

$$\mathbb{N} \xrightarrow{\pi} \mathbb{N} \times \mathbb{N} \xrightarrow{f \times p} \mathbb{Z} \times \mathbb{N}^* \xrightarrow{q} \mathbb{Q}$$

een surjectie die de aftelbaarheid van $\mathbb{Q}$ vestigt. □

Er zal blijken (zie *Logica I*) dat de aftelbare unie en aftelbare cartesische producten van aftelbare verzamelingen weer aftelbaar zijn. Inderdaad, de meeste elementaire operaties op aftelbare verzamelingen leveren weer een aftelbare verzameling.

2.6.6 Overaftelbaarheid

Er bestaan ook overaftelbare verzamelingen: wegens de stelling van Cantor weten we dat de machtsverzameling van een aftelbare verzameling overaftelbaar moet zijn. Hier volgt nog een belangrijk resultaat.

Stelling 2.44

$\mathbb{R}$ is overaftelbaar.

Bewijs. Stel dat $\mathbb{R}$ wel aftelbaar is, dan is $\mathbb{R} \cap]0,1[$ zeker aftelbaar. Zij $f : \mathbb{N} \to]0,1[$ een surjectie, die ons een aftelling van $]0,1[$ oplevert:

$$]0,1[= \{r_0, r_1, r_2, \dots\}$$

Elk reëel getal in $]0,1[$ kan op een unieke manier geschreven worden als een niet-eindigend decimaal getal, d.w.z. een kommagetal dat oneindig veel niet-nuldecimalen heeft. (In het geval van rationale getallen met een eindige decimale voorstelling, bestaat er een alternatieve decimale ontwikkeling die oneindig is: verlaag de laatste decimaal met 1 en voeg een oneindige rij negens toe, bv. $0.45 = 0.44999\dots$)

Dus de decimale ontwikkeling van de getallen in de lijst levert cijfers $x_{ij} \in \{0, 1, \dots, 9\}$ zodat

$$r_i = 0.x_{i0}\, x_{i1}\, x_{i2}\, \dots$$

We produceren nu een reëel getal tussen 0 en 1 dat niet in de lijst kan voorkomen. Definieer

$$y = 0, y_0 y_1 y_2 \dots$$

waarbij

$$y_i = \begin{cases} 7 & \text{als } x_{ii} \neq 7 \\ 3 & \text{als } x_{ii} = 7 \end{cases}$$

Dan moet voor alle i, het getal y verschillen van r_i, want hun unieke decimale ontwikkeling verschilt op de i-de plaats. Dus y wordt niet bereikt door de surjectie f, een strijdigheid. □

2.6.7 Kardinaalgetallen

De kardinaliteit van een verzameling is een maat voor het aantal elementen in die verzameling, die wordt genoteerd met $|A|$ of $\#A$.

Wiskundig gezien zijn er twee benadering om kardinaliteiten precies in te voeren. De eerste is als vergelijkend criterium dat injecties en bijecties gebruikt — dat was onze aanpak, startend met de definitie van gelijkmachtig. Het is niet nodig om precies te definiëren wat *kardinaliteit* betekent, of welke betekenis het symbool $|A|$ heeft: de zinsnede *heeft dezelfde / kleinere kardinaliteit als* en haar symbolische evenknieën $|A| = |B|$ en $|A| \leq |B|$ zijn voldoende om alles te beschrijven wat men over de omvang van verzamelingen wil uitdrukken.

De tweede benadering is die van *kardinaalgetallen*, die een echte betekenis geven aan het symbool $|A|$ voor een verzameling A. Kardinaalgetallen moeten

dus een uitbreiding vormen van de natuurlijke getallen. Er zijn verschillende pistes om die te definiëren, bijvoorbeeld aan de hand van ordinaalgetallen, of als equivalentieklassen in de *klasse* van alle verzamelingen (niet de verzameling van alle verzamelingen, zie 2.9.5). We verwijzen de geïnteresseerde lezer voor precieze definities graag naar de literatuur of naar *Logica I*.

ℵ, ב en de continuümhypothese

Het kleinste kardinaalgetal dat alle eindige kardinaalgetallen overstijgt, is de kardinaliteit van $\mathbb{N}$ zelf. Deze wordt genoteerd[4] met $\aleph_0$. De kardinaalgetallen zijn welgeordend, dus men kan telkens "het volgende" kardinaalgetal beschouwen, dat dan een volgende index krijgt. De kardinaalgetallen vormen zo de rij

$$0, 1, 2, 3, \ldots, n, \ldots; \aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\alpha, \ldots$$

die alle kardinaalgetallen doorloopt als het keuzeaxioma wordt aangenomen. Hier moet wel opgemerkt worden dat de indices zelf niet alleen natuurlijke getallen zijn, maar verder lopen tot ordinaalgetallen.

Een andere manier om een stijgende keten kardinaalgetallen te maken, is door het nemen van de machtsverzameling. Zo krijgen we de ב-getallen.[5]

$$\begin{aligned}
\beth_0 &= \aleph_0 = |\mathbb{N}| \\
\beth_1 &= |\mathcal{P}(\mathbb{N})| \\
\beth_2 &= |\mathcal{P}(\mathcal{P}(\mathbb{N}))| \\
&\vdots \\
\beth_i &= |\underbrace{\mathcal{P}(\ldots\mathcal{P}(}_{i \text{ keer}}\mathbb{N})\ldots)|
\end{aligned}$$

Dat deze kardinaalgetallen verschillend zijn, volgt uit de stelling van Cantor, stelling 2.37.

Verzamelingen met kardinaliteit $\beth_1 = |\mathcal{P}(\mathbb{N})|$ zijn welbekend, zoals $\mathbb{R}$ en $\mathbb{R}^n$. Deze kardinaliteit wordt de *kardinaliteit van het continuüm* genoemd en zelfs vaker genoteerd met $|\mathbb{R}|$ of met $\mathfrak{c}$ dan met $\beth_1$. Andere verzamelingen met kardinaliteit van het continuüm zijn $\mathbb{Z}^\mathbb{N}$, de verzameling van alle rijen gehele getallen, of zelfs $\mathbb{R}^\mathbb{N}$, die van alle rijen reële getallen, of $\mathcal{C}(\mathbb{R}, \mathbb{R})$, de verzameling van alle continue functies van $\mathbb{R}$ naar $\mathbb{R}$.

[4] ℵ is de eerste letter van het Hebreeuwse alfabet, de alef.
[5] ב is de tweede letter van het Hebreeuwse alfabet, de beet.

Een natuurlijke vraag om te stellen is of $\beth_1 = \aleph_1$, m.a.w. is $|\mathbb{R}|$ de eerstvolgende kardinaliteit na $|\mathbb{N}|$, of is de kardinaliteit van het continuüm de kleinste overaftelbare kardinaliteit? De uitspraak dat dit zo is, staat bekend als de continuümhypothese:

Continuümhypothese

Er bestaat geen verzameling A met

$$|\mathbb{N}| < A < |\mathbb{R}|.$$

De continuümhypothese werd in 1877 al door Cantor vermoed. De waar- of onwaarheid ervan bewijzen was het eerste van Hilberts 23 problemen. Intussen weten we dat, als ZFC consistent is, de continuümhypothese niet kan weerlegd worden (Gödel, 1940), maar ook niet kan bewezen worden (Cohen, 1963) uit de axioma's van ZFC. De continuümhypothese is dus *onafhankelijk* van ZFC. Dat betekent dat de continuümhypothese zou kunnen toegevoegd worden aan de ZFC-axioma's om een axiomastelsel te krijgen dat consistent is als ZFC dat is, en hetzelfde geldt voor haar negatie.

De *veralgemeende continuümhypothese* zegt dat voor elke oneindige verzameling X, er geen kardinaalgetallen liggen tussen $|X|$ en $2^{|X|}$.

Rekenkunde der kardinaalgetallen

Men kan rekenen met kardinaalgetallen, op zo'n manier dat de rekenkunde der kardinaalgetallen die deze van de natuurlijke getallen uitbreidt. Zo zullen de volgende gelijkheden gelden bij het rekenen met kardinaalgetallen — zoals je hier ziet zijn verschillende notaties van verzamelingconcepten geïnspireerd op hoe hun kardinaliteiten zich gedragen.

$$\begin{aligned} |X \cup Y| &= |X| + |Y| \quad \text{disjuncte unie van } X \text{ en } Y \\ |X \times Y| &= |X| \cdot |Y| \quad \text{cartesisch product van } X \text{ en } Y \\ |Y^X| &= |Y|^{|X|} \quad \text{verzameling van alle afbeeldingen van } X \text{ naar } Y \\ |\mathcal{P}(X)| = |2^X| &= 2^{|X|} \quad \text{verzameling van alle deelverzamelingen van } X \end{aligned}$$

Dit betekent dat bijvoorbeeld de schrappingswet over het algemeen niet zal gelden. Immers, wegens $|\mathbb{N}^*| = |\mathbb{N}|$ geldt er dat

$$\aleph_0 = |\mathbb{N}| = |\mathbb{N}^* \cup \{0\}| = |\mathbb{N}^*| + |\{0\}| = |\mathbb{N}| + 1 = \aleph_0 + 1$$

Ook vele andere vertrouwde rekenregels zullen zich niet veralgemenen tot kardinaalgetallen.

Bemerk tot slot de oorsprong van de 2^X voor $\mathcal{P}(X)$. Met 2 als notatie voor $\{0,1\}$ (zie 2.8), hebben we de volgende bijectie tussen de verzameling van alle deelverzamelingen van X en de verzameling van alle functies van X naar $\{0,1\}$.

$$\begin{aligned} \beta : \mathcal{P}(X) &\to \{0,1\}^X = 2^X \\ A &\mapsto \mathbf{1}_A \end{aligned}$$

2.7 Verzamelingen als fundament van de wiskunde

Tot de negentiende eeuw hebben wiskundigen gerekend, stellingen bewezen, kortom wiskunde bedreven gebaseerd op een intuïtieve notie van de basisconcepten, zoals verzamelingen. Pas met het contra-intuïtieve werk van Cantor en de paradoxen van Russell is het onderzoek naar de grondslagen van de wiskunde in een stroomversnelling geraakt. Eén van de grote figuren in dit verhaal is David Hilbert, wiens werk *Grundlagen der Mathematik* invloedrijk geweest is. Over de historiek hiervan lees je meer in de volgende paragraaf.

In het grondslagenonderzoek speelt de axiomatische opbouw een zeer belangrijke rol, en de verzamelingenleer, in het bijzonder die met het ZFC-axiomastelsel, vormt zowat het fundament van de wiskunde. Een belangrijk gevolg van deze beslissing is dat we accepteren dat alles wat we binnen de wiskunde, dat betekent, binnen de ZFC-verzamelingenleer zullen beschouwen, een verzameling is. Men zou dit als een "doctrine" kunnen bestempelen: *Alles is een verzameling.*

Alles wat we tot nu toe gedefinieerd hebben, is een verzameling, van deelverzameling tot equivalentierelatie. We kunnen zo een tijdje doorgaan: heel veel objecten binnen de wiskunde kunnen gedefinieerd worden als één of andere *verzameling*. In die hoedanigheid bestudeert de verzamelingenleer een rijke collectie van *wiskundige objecten*, van de simpelste tot de meest complexe: het getal 27, de groep van rotaties van het regelmatig twaalfvlak, de Hilbertruimte $L^2[0,1]$, enz.

Bijvoorbeeld, een *binaire bewerking*, zoals $+$ of $\times$, op een verzameling A, is eigenlijk een afbeelding van $A \times A \to A$, die aan vele eisen kan voldoen. Verzamelingen met structuur in de vorm van één of meer bewerkingen, zoals

groepen, ringen, velden, vectorruimten en algebra's, vormen op die manier een koppel of n-tal van verzamelingen en dus ook verzamelingen. Verzamelingen, voorzien van een collectie deelverzamelingen, zoals maatruimten, topologische ruimten of projectieve ruimten, worden op voor de hand liggende wijze gemodelleerd door verzamelingen. Al deze structuren kunnen we modelleren door verzamelingen, precies omdat het krachtige concept verzameling ons in staat stelt de extra *structuur* te *vatten* als verzameling.

Maar hoe, gegeven een verzameling S, kunnen we herkennen dat het een Hilbertruimte is? Wel, een Hilbertruimte is een koppel (V, i), dus conform de constructie van koppel (zie pagina 40) moeten we kijken of S van de vorm $\{\{a\}, \{a, b\}\}$ is. Als dat het geval is, kunnen we kijken of a een viertal $(V, \mathbb{K}, +, \cdot)$ is en of b een afbeelding $V \times V \to \mathbb{K}$ zou kunnen zijn, dus een deelverzameling van $V \times V \times \mathbb{K}$, enzovoort. Uiteraard is dit allemaal niet nodig in de gangbare wiskundige praktijk. De doorsnee wiskundige hoeft (gelukkig) niet wakker te liggen van de grondslagen van de wiskunde. Daarenboven zijn er ook alternatieven mogelijk. Als verzamelingen basisobjecten zijn, dan kunnen we functies als basisprocessen beschouwen. In plaats van functies als verzamelingen te definiëren, kunnen we functies als fundamentele objecten beschouwen. Met dit als uitgangspunt levert *Categorietheorie* een mogelijke ontwikkeling van de fundamenten van de wiskunde.

Er zijn drie mogelijkheden om categorietheorie op te bouwen. De eerste mogelijkheid is de naïeve categorietheorie, met een opbouw vergelijkbaar aan die van de naïeve verzamelingenleer (en met hetzelfde soort beperkingen). De verzamelingenleer zelf is dus noodzakelijk in deze opbouw. De tweede mogelijkheid, met als pionier Alexander Grothendieck, is een axiomatische opbouw vergelijkbaar met de axiomatische opbouw van de verzamelingenleer, dewelke zelf een sterke rol blijft spelen in de opbouw van de categorietheorie. Ook hier is de verzamelingenleer dus noodzakelijk. De derde mogelijkheid tenslotte gooit de volledige verzamelingenleer overboord. Alle wiskundige objecten worden dan opgebouwd vanuit een aantal axioma's die de fundamenten vormen van de categorietheorie. De verzamelingen verschijnen dan als een categorie Set. De pionier in deze opbouw is Lawvere.

In elk geval is het duidelijk dat de verzamelingenleer alleen niet het fundament is van de volledige hedendaagse wiskunde. Het is immers duidelijk dat de categorie van de verzamelingen zelf geen verzameling kan zijn. Wel is het zo dat we binnen de verzamelingenleer heel veel interessante objecten kunnen definiëren. Ook in deze cursus zullen we nog een aantal objecten als verzameling construeren.

Er zijn nog heel wat alternatieven mogelijk, die er ook uitzien als verzame-

lingenleer, maar dan met gewijzigde axioma's. Sommige verzamelingenleren laten in hun axioma's zogenaamde *urelementen* toe: atomaire objecten die element kunnen zijn van een verzameling, maar zelf geen verzameling zijn. Meest vermeldenswaardig hier is misschien de axiomatische verzamelingenleer *New Foundations* van Quine (1908-2000), een vereenvoudiging van de typentheorie in de *Principa Mathematica* van Whitehead en Russell.

Historisch gezien moet men eigenlijk ook de *meetkunde* als alternatieve fundering van de wiskunde beschouwen. Duizenden jaren werd (Euclidische) meetkunde gezien als de basis van alle wiskunde. Getallen werden beschouwd als lengtes van lijnstukken, kwadratische vergelijkingen waren uitdrukkingen van relaties van oppervlakten van bepaalde figuren. Hoewel er problemen waren met deze aanpak, was alle wiskunde in dat historisch perspectief, meetkundig van aard.

2.8 De getallenverzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$

De natuurlijke getallen

Als dan alles een verzameling is, hoe zien de natuurlijke getallen er dan uit? Dat hebben we in paragraaf 2.6.3 uitgesteld, maar hier zullen we de natuurlijke getallen definiëren in de verzamelingenleer. Stel $0 = \varnothing$ en definieer inductief $n + 1 = n \cup \{n\}$. Dat wil zeggen

$$
\begin{aligned}
0 &= \varnothing \\
1 &= \{\varnothing\} = \{0\} \\
2 &= \{\varnothing, \{\varnothing\}\} = \{0, 1\} \\
3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\} \\
4 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} = \{0, 1, 2, 3\} \\
&\vdots
\end{aligned}
$$

Op deze manier is $n = \{0, 1, \ldots, n-1\}$, het is een soort standaardverzameling met n elementen. Dit maakt het eenvoudig om te tellen: zeggen dat een verzameling kardinaliteit n heeft, is zeggen dat er een bijectie bestaat tussen A en $\ldots$ n zelf!

Dat deze natuurlijke getallen als verzameling bestaan, binnen de theorie van de ZFC-verzamelingenleer, volgt uit het axioma van oneindigheid, dat stelt dat er een verzameling moet bestaan met oneindig veel elementen.

Axioma van oneindigheid

Er bestaat een verzameling, die de ledige verzameling bevat en waarvoor, zodra x erin zit, dan ook de verzameling gevormd door de unie te nemen van x met singleton $\{x\}$, erin zit, m.a.w.

$$\exists I\ (\varnothing \in I\ \wedge\ \forall x \in I\ [x \cup \{x\} \in I]).$$

Een verzameling die gesloten is onder "het bevatten van de opvolger", heet een *inductieve verzameling*. Dat verklaart ook de letter I in het axioma.

Men kan aantonen dat er een unieke *kleinste* inductieve verzameling moet bestaan. De verzameling van natuurlijke getallen $\mathbb{N}$ wordt dan *gedefinieerd* als deze unieke kleinste verzameling. Haar elementen, de natuurlijke getallen, zijn dan ook ter beschikking als verzamelingen!

Men kan middels de axioma's van ZFC ook aantonen dat de verzameling natuurlijke getallen n waarvoor $\{0, \ldots, n\}$ welgeordend is, een inductieve verzameling vormt, die bijgevolg alle natuurlijke getallen moet bevatten. Daaruit volgt dat $\mathbb{N}$ zelf welgeordend is, m.a.w. het welordeningsprincipe is bewijsbaar in ZFC.

Het heeft heel wat voeten in de aarde om te komen tot een goede definitie van de natuurlijke getallen, in elk systeem dat kan dienen als fundamenten vooor de wiskunde, zoals ZFC-verzamelingenleer. Al deze problemen om getallen te definiëren verdwijnen echter, als men het concept *natuurlijk getal* als basaal en atomair veronderstelde, zoals Poincaré deed. Vanuit zo'n standpunt komt getaltheorie wel degelijk vóór verzamelingenleer.

De gehele getallen

Stel dat we de structuur $(\mathbb{N}, +, \cdot, \leq)$ hebben, waarbij $\mathbb{N}$ de hierboven beschreven verzameling is, $+$ en $\cdot$ binaire bewerkingen op $\mathbb{N}$ (dat zijn afbeeldingen $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, dus deelverzamelingen van $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$), en $\leq$ een relatie op $\mathbb{N}$, die bovendien voldoen aan wat we weten over de natuurlijke getallen. Zo moeten optelling en vermenigvuldiging associatief en commutatief zijn, moet 0 een eenheidselement voor optelling en 1 een eenheidselement voor vermenigvuldiging zijn, moeten de schrappingswetten gelden voor optelling en vermenigvuldiging, en moet gelden dat als $a \leq b$, dan $a + c \leq b + c$ en $ac \leq bc$.

Als we de getallenverzameling $\mathbb{N}$ willen uitbreiden zodat aftrekking gedefinieerd is, willen we uitdrukken dat elke vergelijking van de vorm $a + x = b$

een oplossing heeft. Elk koppel (a, b) moet precies één nieuwe x bepalen, dus we zullen x gewoon *voorstellen* door het koppel (a, b). Verschillende koppels kunnen eenzelfde x bepalen, dus eigenlijk moeten x voorgesteld worden door een equivalentieklasse van geordende paren. Definieer dus een relatie $\sim$ op $\mathbb{N} \times \mathbb{N}$ door de regel

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = b + c$$

en bewijs als oefening dat dit een equivalentierelatie definieert. Definieer nu de gehele getallen als de quotiëntverzameling (in de betekenis van op pagina 58)

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$$

en noteer met $[a, b]$ de equivalentieklasse met representant (a, b). Definieer nu optelling, vermenigvuldiging en ordening als volgt:

$$\begin{aligned} [a, b] + [c, d] &= [a + c, b + d] \\ [a, b] \cdot [c, d] &= [ac + bd, ad + bc] \\ [a, b] \leq [c, d] &\Leftrightarrow a + d \leq b + c \end{aligned}$$

Deze definities komen uit onze bedoelde interpretatie van een equivalentieklasse $[a, b]$ als het geheel getal $a - b$, bijvoorbeeld: $(a - b) \cdot (c - d) = (ac + bd) - (ad + bc)$. We moeten eerst aantonen dat dit goede definities zijn, d.w.z. dat verschillende keuzes van representanten van de equivalentieklassen het gedefinieerde object niet zouden veranderen. Bijvoorbeeld, stel dat $(a, b) \sim (a', b')$ en $(c, d) \sim (c', d')$. Een korte berekening toont aan dat $(a + c, b + d) = (a' + c', b' + d')$ en $(ac + bd, ad + bc) = (a'c' + b'd', a'd' + b'c')$.

Verder kan men aantonen dat de gebruikelijke rekenkundige eigenschappen van $\mathbb{Z}$ voldaan zijn. Bovendien is de afbeelding die a afbeeldt op $[a, 0]$ een injectie van $\mathbb{N}$ in $\mathbb{Z}$ die optelling, vermenigvuldiging en orde bewaart. Dat betekent dat eens we $\mathbb{Z}$ hebben, we onze definitie van $\mathbb{N}$ kunnen vergeten en de natuurlijke getallen kunnen zien als een bijzonder soort gehele getallen.

De rationale, reële en complexe getallen

We zullen ook de rationale getallen construeren als quotiëntverzameling. Maar we zullen dit in een iets algemenere context doen, en daarom stellen we de constructie uit tot Hoofdstuk 5. Voor de reële getallen zijn er verschillende mogelijkheden. Opnieuw is een verzamelingtheoretische opbouw mogelijk, maar een algemener algebraïsch kader is nuttig om beter te begrijpen wat er achter de eerder steriele verzamelingtheoretische constructie zit. Dit geldt a fortiori voor de constructie van de complexe getallen.

2.9 De grondslagencrisis

We maken even een historiografische uitstap aan het einde van dit hoofdstuk, om een bijzondere periode in de geschiedenis van de moderne wiskunde te belichten.

We bevinden ons in Europa, in de tweede helft van de negentiende eeuw, in de tweede golf van de industriële revolutie. Onder andere de ontwikkeling van de fysica maakt een groei van de wiskunde nodig. De ontwikkeling van de wiskunde nam een vaart en werd georganiseerder, getuige de geboorte van vele Mathematical Societies en wiskundige tijdschriften aan het einde van de negentiende eeuw. Eén van de meest notoire wiskundige in de negentiende eeuw was Carl Friedrich Gauß (1777–1855), die in bijna alle bestaande takken van de wiskunde belangrijke bijdragen had geleverd.

2.9.1 De verzamelingenleer van Cantor

Het is in die periode dat Georg Cantor (1845–1918) een originele theorie ontwikkelde waarin hij het oneindige op een nieuwe manier behandelde. Hij kwam tot bijzondere resultaten omtrent de groottes van oneindige getallenverzamelingen en bouwde daaruit zijn verzamelingenleer op, voortbouwend op het werk van zijn voorloper Bernard Bolzano (1781–1848). Het begon in 1873 toen Cantor in een brief aan Richard Dedekind (1831–1916) met behulp van geneste intervallen bewees dat de reële rechte méér dan aftelbaar veel punten bevatte. Tot dan toe had bijna niemand met de mogelijkheid rekening gehouden dat er verschillende groottes oneindigheden waren. Het werd al paradoxaal genoeg gevonden dat oneindige verzamelingen echte deelverzamelingen konden hebben die even groot waren, één van de subtiliteiten die Bolzano ervan weerhield een verzamelingenleer te ontwikkelen. Het bestaan van overaftelbare verzamelingen en in het bijzonder de overaftelbaarheid der reëlen was de grootste controverse in de theorie van Cantor.

Een vraag uit die tijd was die naar de zeldzaamheid van transcendente getallen, waarvan er zonet een aantal ontdekt waren. Cantor bewees dat transcendente getallen overvloedig aanwezig waren op de reële rechte, in een veel grotere overvloed dan algebraïsche getallen. In zijn bewijs definieerde hij aftelbaar en bewees dat de algebraïsche getallen aftelbaar zijn en de reële niet. Het ganse bewijs construeert echter op geen enkele wijze een transcendent getal en steunt op de bovenvermelde resultaten van Cantor: het definiëren van verschillende graden oneindigheid.

Er kwam een hevige reactie van ongeloof op Cantors ideeën. De ergste kwamen van Leopold Kronecker (1823–1891), die uitriep dat hij niet wist of er meer filosofie of theologie domineerde in Cantors theorie, maar dat hij zeker was dat er geen wiskunde in te vinden was! Kronecker had tot zijn dertigste zijn agriculturele familiebedrijf geleid en beoefende sinds zijn bijzonder vroegtijdig pensioen zijn hobby, wiskunde. Hij hield zich bezig met het storen van zijn medewiskundigen door de soliditeit van hun moderne wiskunde in vraag te stellen. Kronecker was virulent en persoonlijk in zijn aanvallen op de mannen wiens wiskunde hij afkeurde. De voorname oude Weierstraß werd tot tranen gebracht bij Kroneckers opmerkingen over "de onjuistheid van al die conclusies waarmee de zogenaamde analyse tegenwoordig werkt". De gespannen en gevoelige Cantor was, als gevolg van Kroneckers aanvallen op zijn verzamelingenleer, volledig ingestort en moest onderkomen zoeken in een psychiatrische instelling.

Hoewel het verhaal van de verzamelingenleer pas goed begint met Cantor, kan men al stellen dat na Cantor wiskunde nooit meer hetzelfde geweest is.

2.9.2 Het probleem van Gordan

Cantors diagonaalargument was wiskundig correct en is zelfs in deze cursus opgenomen als Stelling 2.44. Het probleem was dat het bestaan van verschillende oneindigheden niet strookte met de intuïtie van de wiskundigen. Men zou niet meer weten wat te geloven, als deze contra-intuïtieve resultaten tot de wiskunde zouden behoren...

Invariantenkoning Paul Gordan (1837–1912), de latere promotor van Emmy Noether, was bekend als een rekenwonder sinds zijn kindertijd. Zijn publicaties bestonden niet zelden uit twintig pagina's tekstloze formules.

Nu de interne structuur van invariante vormen vrij goed gekend werd, kwam de vraag of er een basis bestond, een eindige collectie invarianten waaruit alle — oneindig vele — invarianten konden worden opgebouwd. Na lang en ondoorzichtig rekenwerk had Gordan een basis geconstrueerd voor de eenvoudigste, de binaire vormen. De algemene vraag was een gesofistikeerd wiskundig probleem dat bekend stond als het probleem van Gordan.

Niemand was voorbereid op de oplossing van het oude probleem, temeer omdat elke poging bestond uit lang rekenwerk en variabelentransformaties. Toen David Hilbert (1862–1943) in december 1888 een verrassend eenvoudig bewijs publiceerde, was de eerste reactie dan ook ongeloof. Zijn sensationele existentiebewijs steunde op wat we vandaag kennen als Hilberts basisstelling

(zie *Algebra II*). Hierin construeert hij geen eindige basis, maar bewijst hij dat het niet bestaan ervan tot een contradictie leidt.

Hoewel sommigen, zoals Felix Klein, het bewijs aanvaardden, vonden de meesten de gedachtengang obscuur. Cayley had twee uitlegbrieven van Hilbert nodig voor hij het begreep, Kronecker haalde scherp uit naar deze onzin en Gordan schreeuwde: *Das ist nicht Mathematik. Das ist Theologie!*

De vijf volgende jaren, waarin Kronecker stierf, verdween de georganiseerde tegenstand. Hilbert bewees kort daarna zijn fundamentele en welbekende Nullstellensatz en was in 1892 in staat om steunend op dit resultaat een constructiemethode te beschrijven voor de basis waarvan hij het bestaan bewezen had. Elke verzet tegen zijn existentiebewijs moest nu wel als sneeuw voor de zon smelten. Gordan moest eindelijk toegeven dat hij inzag dat "theologie ook zijn verdiensten kan hebben".

2.9.3 Grundlagen der Geometrie

Hilbert bestudeert de grondslagen van de meetkunde en presenteerde in 1899 een geheel nieuw axiomasysteem voor Euclidische meetkunde, in *Grundlagen der Geometrie*. Eenentwintig formele axioma's vervingen de traditionele axioma's van Euclides en Hilbert analyseerde hun belang en rol voor de meetkunde.

Hij wilde ook de consistentie van de meetkunde aantonen, d.i. de consistentie van de axioma's waarop ze gebaseerd is. Dit deed hij door de constructie van modellen, meer bepaald als volgt: laat koppels of vectoren reële getallen de rol van punten spelen, eerstegraadsvergelijkingen die van rechten in het vlak en bijgevolg corresponderen oplossingen van stelsels dergelijke vergelijkingen met snijpunten van rechten. Zo krijgen we de analytische meetkunde naar het idee van René Descartes (1596–1650). Deze interpretatie van punten en rechten voldoet aan de axioma's. Als de axioma's inconsistent zijn kan er een tegenspraak uit afgeleid worden. Omdat logische implicatie onafhankelijk is van de specifieke woorden punt en rechte, zullen de axioma's ook een contradictie impliceren onder hun cartesische herinterpretatie. Maar dat betekent een tegenspraak in de theorie van de reële getallen, dus ook deze is inconsistent. Hilbert kon dus bewijzen dat de meetkunde consistent was als de theorie van de reële rechte consistent was. En die kon op haar beurt teruggebracht worden tot de consistentie van de Peano-rekenkunde (zie Appendix A), en Hilbert werkte op die laatste tot 1905.

Hilbert toont zich met dit boek ook de eerste die zich beweegt op een hoger metamathematisch niveau. Eigenlijk is het niet zozeer meetkunde die het

belang van dit werk uitmaakte, maar de aandacht voor de grondslagen en de metabeschouwingen. Onderzoek naar de fundamenten vond Hilbert een organisch deel van de groei van een wiskundige discipline. De fundamenten vormen het beginpunt van de rigoureuze opbouw van een theorie, maar niet het beginpunt in de historische ontwikkeling: pas wanneer een theorie een volwassen stadium bereikt, begint men zich af te vragen of de leest waarop ze geschoeid is, goed in elkaar zit.

De meetkunde was de eerste en grootste wiskundige theorie die op deze manier werd geaxiomatiseerd. Grundlagen der Geometrie was onmiskenbaar het startschot van de axiomatische revolutie. Dit boek bleef verschijnen in nieuwe edities en was van de grootste invloed op de verspreiding van de axiomatische methode in de wiskunde, die een belangrijke rol zou gaan spelen in de rest van de twintigste eeuw en waarschijnlijk nog lang erna.

2.9.4 Aandacht voor grondslagen

De contra-intuïtieve resultaten van Cantor en de tegenstand op Hilberts oplossing van het probleem van Gordan wezen op de noodzaak om de grondslagen waarop de wiskunde gebouwd werd, ondubbelzinnig vast te leggen. Het is in dit kader dat Hilberts *Grundlagen der Geometrie* (1899) en later *Grundlagen der Mathematik* (1934–1939) van Bernays en Hilbert, moet gezien worden.

In 1900 kreeg Hilbert de kans om te spreken voor het tweede International Congress of Mathematicians in Parijs. Hij had in de vier grote wiskundegebieden (algebra, getaltheorie, meetkunde en analyse) gewerkt en had een goed zicht op de ontwikkeling en stand van zaken van de hele wiskunde aan de eeuwwisseling. Hij besloot te spreken over de betekenis en de relevantie van individuele problemen en zou een lijst geven van 23 problemen die hij als de meest vruchtbare voor de wiskunde van de volgende eeuw zag. Hoewel de meeste van deze concrete wiskundeproblemen er waren uit de analyse, meetkunde en getaltheorie (zoals de Riemannhypothese), besteedde hij hier ook aandacht aan het grondslagenonderzoek. Het eerste probleem was de continuümhypothese, het tweede de consistentie van de rekenkunde en het zesde de axiomatisatie van de statistiek en mechanica. Hilberts 23 problemen zijn inderdaad belangrijk gebleven en doorheen de twintigste eeuw meegenomen. Vele problemen hebben nieuwe takken van de wiskunde doen ontstaan en tot op heden zijn vele ervan de basis van verder onderzoek.

2.9.5 De paradox van Russell

Toen Russell (1872–1970) in 1901 probeerde een fout te ontdekken in een bewijs van Cantor, stootte hij op zijn bekende paradox, die hij publiceerde in 1903. Vrij vertaald:

> Beschouw de verzameling R van alle verzamelingen die geen element zijn van zichzelf. R is element van R als en slechts als dat niet zo is.

Russells paradox was een rampzalige ontdekking. Uit een tegenspraak kan men elke bewering afleiden, en uit verzamelingenleer kon men sinds Russells paradox een tegenspraak halen. Daar de wiskunde min of meer gebaseerd was op verzamelingenleer, rees de mogelijkheid dat alles bewijsbaar was en dus geen enkel wiskundig bewijs nog kon vertrouwd worden. De paradox bracht de hele wiskunde aan het wankelen en de grondslagencrisis was compleet. De grote werkers in de fundamenten van de wiskunde zoals Frege en Dedekind haakten af, hun nederlaag toegevend.

Ernst Zermelo (1871–1953) was naar Göttingen gekomen in 1897 om zijn doctoraat in de wiskundige natuurkunde af te werken, maar raakte geïnteresseerd in de fundamenten van de rekenkunde en verzamelingenleer. Onafhankelijk van Russell kwam ook Zermelo tot dezelfde paradox. Hij werkte op de open problemen in de verzamelingenleer, zoals een mogelijke welordening van de reële getallen, de continumhypothese en een goede oplossing voor Russells paradox. In 1904 bewees Zermelo de stelling dat elke verzameling welgeordend kan worden (zie pagina 73), origineel Wohlordnungssatz genoemd. Zijn resultaat werd massaal bekritiseerd door zijn collega's. Het feit dat de reëlen een welordening toelaten, is namelijk intuïtief onwaarschijnlijk. Bovendien waren er geen axioma's voor de verzamelingenleer, waarop zijn bewijs kon rusten. Gegeven dit axiomatisatiegebrek, dat hij onder invloed stond van zijn medeprofessor Hilbert en dat er een paradox moest opgelost worden, is het niet moeilijk te raden wat Zermelo's volgende stap was.

2.9.6 Axiomatisatie van de verzamelingenleer

Zermelo publiceerde zijn axiomatisatie van de verzamelingenleer in 1908, hoewel hij er niet in geslaagd was om de consistentie van zijn axioma's aan te tonen, wat Hilberts stokpaardje was.

Zijn origineel axiomasysteem had zeven begrijpelijke axioma's en bevatte al het keuzeaxioma. Het systeem werd verbeterd door Abraham Fraenkel

(1891–1965) en onafhankelijk door Thoralf Skolem (1987–1963), tot wat we nu kennen als Zermelo-Fraenkel verzamelingenleer met keuzeaxioma (ZFC). Hij publiceert meteen ook een nieuw bewijs van zijn welordeningsstelling, dat de kritieken van vier jaar eerder weerlegde en veel breder geaccepteerd werd.

Zermelo steunde daarbij op zijn piepjonge keuzeaxioma, dat hij als onweerlegbaar beschouwt. Het keuzeaxioma kende tegenstand van verschillende kanten, omdat het zoals de controverses rond Cantor vanaf 1873 en Hilbert in 1888 het bestaan postuleert van iets wat niet kan geconstrueerd worden. Hadamard en Hilbert hadden geen probleem met de aanvaarding ermee, Poincaré en Borel al beduidend meer.

Het nieuwe axiomasysteem voor de verzamelingenleer lost de paradox van Russell op, door de notie van *verzameling* op de juiste manier te beperken, namelijk door het axioma van separatie. Niet *elke* collectie objecten die men kan bepalen door een voorschrift, is een verzameling, maar enkel die objecten *binnen een bepaalde verzameling* die aan een voorschrift voldoen, vormen een nieuwe verzameling. In Zermelo's axiomasysteem zijn de verzameling van alle verzamelingen en de Russellverzameling niet construeerbaar met de methodes aangereikt door de axioma's, en bijgevolg zijn het dus geen verzamelingen.

2.9.7 Intuïtionisme

Aan het einde van de eerste wereldoorlog was er een nieuwe machtsgreep naar de volledige omvang van wiskunde, door een groep onder leiding van L.E.J. Brouwer (1881–1966) die met zijn fixpuntstellingen bekend geraakt was als de grootste topoloog. In drie artikelen, samen minder dan zeventien pagina's lang, stelde Brouwer een drastisch programma voor om de fundamentencrisis te beëindigen die ingeluid werd door de paradox van Russell — hoewel intussen verschillend opgelost door Russell zelf, met zijn typentheorie, en Zermelo. Brouwer geloofde niet dat de wetten van de klassieke logica een absolute waarheid hadden, onafhankelijk van het onderwerp waarin ze worden toegepast. De nieuwe aanpak die voorstelde, was om de wiskunde te baseren op de intuïtie van de menselijke geest en zijn filosofische stroming wordt dan ook *intuïtionisme* genoemd.

Brouwer beschouwde de wiskunde als louter het resultaat van de constructieve mentale activiteit van de mens in plaats van de geldende opvatting van wiskunde als de ontdekking van de fundamentele principes in een objectieve werkelijkheid. Logica en wiskunde ontstaan door toepassing van methoden in de menselijke geest, die noodzakelijk consistent zijn, los van één of andere objectieve realiteit.

Brouwer verwierp onder andere de wet van de uitgesloten derde (*tertium non datur*) voor oneindige verzamelingen, terwijl hij het accepteerde voor eindige verzamelingen. Hij redeneerde namelijk dat om de waarheid te achterhalen van "er bestaat een element in een oneindige verzameling S dat een eigenschap P heeft", het voldoende was om alle elementen in S af te lopen en er één te vinden dat aan P voldoet. Maar als men er geen zou vinden, zijn er verschillende mogelijkheden: dat er werkelijk geen zijn, of dat men niet lang genoeg gezocht heeft. Voor uitspraken over eindige verzamelingen accepteerde Brouwer wel de wet van de uitgesloten derde, en in eindige contexten bleef veel van de klassieke wiskunde overeind.

2.9.8 Hilberts programma

Brouwers voorstel werd bij Hilbert onthaald op een besliste woede: hij vond Brouwer een gevaar voor de wiskunde. Hilbert somde een grote lijst schatten op die zouden verloren gaan mocht het intuïtionistische programma uitgevoerd worden en weigerde de wiskunde een dergelijke verminking te laten ondergaan. Hij zag echter een manier waarop de wiskundige objectiviteit die Brouwer vroeg, zou kunnen teruggehaald worden zonder offers te doen.

Het was Hilberts doel om de ideeën van Brouwer te bevechten met zijn eigen wapen, namelijk eindigheid. Maar dan wel met een andere opvatting van wiskunde. Wat resulteerde staat bekend als Hilberts programma (jaren 1920). Het is een oproep om alle wiskunde te formaliseren in een axiomatische vorm, en een metatheorie te ontwikkelen die een bewijs van consistentie kon leveren. Hij liet eisen dat de consistentiebewijzen en metatheorie met strikt finitistische methoden zouden tewerk gaan, teneinde Brouwer gelukkig te stemmen.

Het studieobject in Hilberts programma zijn de sequenties van symbolen, zoals formules en geformaliseerde bewijzen. Deze kunnen syntactisch worden gemanipuleerd, en daarvoor kunnen logicaloze regels opgesteld worden.

Wiskunde zelf, echter, werkt met abstracte maar inhoudsvolle begrippen zoals oneindige verzamelingen en functies, en maakt gebruik van logische gevolgtrekking op basis van wiskundige inductie of tertium non datur, die door Brouwer bekritiseerd werden omdat ze oneindige verzamelingen als gegeven veronderstellen. Hilbert wilde hun gebruik rechtvaardigen, door erop te wijzen dat ze geformaliseerd konden worden in axiomatische systemen.

Op deze manier transformeren wiskundige stellingen en bewijzen tot formules, symboolsequenties en afleidingen vanuit axioma's die geschieden volgens strikt omschreven afleidingsregels, die verder niets met logica te maken

hebben. Daar de formules en bewijzen zelf niet meer zijn dan eindige opeenvolgingen van karakters, zijn de methoden die gebruikt worden om ze te manipuleren eveneens eindig en moeten critici tevreden zijn. Wiskunde wordt zo een inventaris van bewijsbare formules, waarin wiskundige bewijzen onderworpen worden aan metamathematisch onderzoek. Het doel van Hilberts programma is dan om een inhoudelijk, metamathematisch bewijs te vinden dat er geen formele afleiding kan bestaan van een formule A en haar ontkenning $\neg A$. Hij was zelf optimistisch dat een dergelijk consistentiebewijs vlug zou gevonden worden.

Formalisme

Er kwam kritiek tegen Hilberts programma, die stelde dat de wetenschap getransformeerd werd in een betekenisloos spel met betekenisloze symbolen op papier. Maar voor al wie vertrouwd was met Hilberts werk, was deze kritiek ongeldig. Men kon onmogelijk stellen dat Hilbert, de meest productieve en belangrijkste wiskunde van zijn tijd, de betekenis en echtheid van de wiskunde ontkende. Zijn programma was enkel bedoeld om de grondslagencrisis te bezweren en de consistentie van de wiskunde te vestigen, maar was helemaal geen filosofische overtuiging dat zo'n symbolenspel de ware aard van de wiskunde was, en al zeker geen oproep om de wiskunde voortaan *enkel* in een geformaliseerd format te ontwikkelen.

Toch wordt formalisme soms op dezelfde hoogte geplaatst wordt als platonisme, intuïtionisme, logicisme, cantorisme en andere filosofische stromingen die hun oplossing voor de grondslagencrisis wel als geloofwaardige visie op de wiskunde poneren. Felix Hausdorff (1868–1942) was bijvoorbeeld, in tegenstelling tot Hilbert, een echtere formalist in de hierboven beschreven zin. Hij werd sterk beïnvloed door de Grundlagen der Geometrie, in een richting die Hilbert zelf nooit bedoeld had. Hij postuleerde de meetkunde als autonome discipline, losstaand van elke ervaring of empirische basis, zoals hij ook de hele wiskunde als vrij, autonoom en betekenisloos zag. Wanneer wiskundige objecten betekenis krijgen, spreekt hij van toegepaste wiskunde. Intuïtie speelt volgens Hausdorff een heuristische en pedagogische rol, maar is voor de rest inexact, beperkt, misleidend en variabel, in tegenstelling tot wiskunde.

2.9.9 Logicisme

Rond de eeuwwisseling had Gottlob Frege (1848–1925) gewerkt om logica te rechtvaardigen als grondvesten van de wiskunde, maar Russell had ont-

dekt dat zijn aanpak contradictorische verzamelingen toeliet: de naar hem genoemde paradox. Alfred North Whitehead en Bertrand Russell gaan op dit pad verder en willen de wiskunde helemaal funderen op (enkel) de logica, een stroming die bekend staat als *logicisme*.

In de jaren 1910 publiceerden deze auteurs hun *Principa Mathematica*, een ambitieus boek in drie volumes. Daarin beschrijven ze axioma's en afleidingsregels in symbolische logica, waaruit volgens hen alle wiskundige waarheden in principe zouden moeten kunnen bewezen worden. In hun opbouw vermijden ze problemen zoals Russells paradox door de notie van verzameling (gedefinieerd in functie van logica) te beperken, op een andere manier als Zermelo deed in zijn axiomatisatie. Ze gebruikten een *hiërarchie* van verzamelingen van verschillende *types*, waarbij een bepaald type verzameling enkel verzamelingen van een lager type mag bevatten.

Op pagina 379 van het eerste volume van de Principa Mathematica wordt een stelling bewezen met als onderschrift: "From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$." Het bewijs daarvan wordt pas voltooid in het tweede volume, pagina 86, vergezeld van het commentaar "The above proposition is occasionally useful."

2.9.10 Uitdoven van de grondslagencrisis

In het begin van de twintigste eeuw zijn verschillende suggesties gekomen om de grondslagencrisis, die ingeluid werd door Cantors verzamelingenleer en Russells paradox, op te lossen. De initieel goedbedoelde oplossingssuggesties groeiden vanaf hun origine echter uit tot filosofische overtuigingen over de ware toedracht van de wiskunde. In navolging van Cantor wil het cantorisme de wiskunde grondvesten op de verzamelingenleer. Naar model van Frege, Russell en Whitehead wil het logicisme de wiskunde opbouwen vanuit (enkel) de logica. De intuïtionisten willen de wiskunde funderen op de menselijke intuïtie en de formalisten willen als reactie de wiskunde zien als een formeel symbolenspel. De platonisten zien wiskunde als een ontdekking van noodzakelijke waarheden die bestaan in een fictieve realiteit — de technische oplossing van de grondslagencrisis is voor hen geen prioriteit: als er problemen zouden ontstaan, zullen die wel opgelost worden. Doordat de discussie precies over de grondslagen van de wiskunde ging, hebben al deze stromingen gelijk in hun eigen wiskunde. Het vooropstellen van een voorkeursovertuiging behoort niet tot de wiskunde, maar tot de filosofie.

Gödel

De vijfentwintigjare Kurt Gödel (1906–1978), die sterk beïnvloed was door het programma van Hilbert en wiens werk erdoor gemotiveerd was, publiceerde in zijn doctoraatsthesis met de grootste finaliteit drie belangrijke stellingen, namelijk de correct- en compleetheid van de predikaatcalculus, de onvolledigheid van de geformaliseerde getaltheorie, en de onmogelijkheid van de formele rekenkunde om haar eigen consistentie te bewijzen.

Hilbert heeft altijd geloofd in een consistentiebewijs voor de rekenkunde, en was ervan overtuigd dat elk probleem een oplossing had, dat wiskundigen konden vinden. De onvolledigheidsstellingen van Gödel doorprikten die droom op de meest expliciete wijze, hoewel een reactie van Hilbert hierop niet terug te vinden is in de literatuur. De exacte formulering van Gödel sloot echter niet uit dat er finitistische bewijzen van de consistentie van de Peano-rekenkunde mogelijk waren die niet formaliseerbaar waren in de Peano-rekenkunde zelf. Het staat open voor discussie in welke mate deze dan nog finitistisch kunnen genoemd worden.

Het vervolg van dit verhaal, de gevolgen van Gödels stellingen op het programma van Hilbert en de zoektocht naar een aanvaardbaar consistentiebewijs is complex. Er is bijzonder veel werk op uitgevoerd in de rest van de twintigste eeuw, onder andere door Bernays, Ackermann en John von Neumann. Startend vanuit het werk van Gerhard Gentzen (1909–1945) uit de jaren dertig, is het werk op de zogenaamde gerelativeerde Hilbertprogramma's centraal geweest in de ontwikkeling van hedendaagse bewijstheorie. We mogen stellen dat Hilberts programma gedeeltelijk is voltooid, in de mate waarin het mogelijk gebleken is.

Verzachting van de filosofische stromingen

Nog vóór de publicatie van Gödels doctoraatsthesis, vervaagde het enthousiasme van de brede wiskundige gemeenschap voor de intuïtionisten. Het gevoel van vele wiskundigen werd verwoord door een wiskundige, als repliek op Brouwer wanneer hij een lezing gaf in Göttingen: "Als we zoveel resultaten verliezen en door zo'n moeilijke hel moeten gaan om tot dezelfde resultaten te komen, wie zal wiskunde dan nog leuk vinden? Het blijft een menselijke activiteit... Zodra we contradicties tegenkomen zal de wiskunde ze oplossen, maar zolang Brouwer geen contradicties vindt in de klassieke wiskunde, zal niemand hem geloven."

Na Gödel werden ook het logicisme en formalisme slechts in verzachte mate verdergezet. Zowel de Principa Mathematica als Hilberts programma had-

den als doel om een systeem voor te stellen waarin alle wiskundige waarheden zouden kunnen bewezen worden. De onvolledigheidsstellingen van Gödel bewezen definitief dat deze pogingen dit ijdel doel nooit zouden kunnen bereiken.

Vanaf 1935 publiceerde een groep Franse wiskundigen onder de naam Bourbaki een reeks boeken om vele gebieden van de wiskunde te formaliseren op het nieuwe fundament van de verzamelingenleer. Van de Bourbakigroep stammen de woorden *injectie, surjectie* en vele andere.

Vandaag

Vandaag zijn er vele mogelijke varianten van verzamelingenleer bekend die verschillen in bewijskracht, waarbij de sterkere systemen telkens formele bewijzen bevatten van zwakkere versies, maar geen zijn eigen consistentie kan bewijzen.

In de praktijk formaliseren wiskundigen hun werk niet in axiomatische systemen, en als ze dat doen, maken ze zich geen zorgen over mogelijke inconsistentie van ZFC. De onvolledigheidsstellingen en paradoxen van de onderliggende formele theorieën hebben nooit een actieve rol gespeeld in de meeste takken van de wiskunde. De meeste wiskundigen hebben dan ook geen uitgesproken filosofische overtuigingen. Ruw gezegd moet het de wiskundige niet kunnen schelen wat de eventuele problemen aan de grondslagen zijn, om succesvol wiskunde te bedrijven.

In die takken waar die subtiliteiten wel van belang zijn, zoals de wiskundige logica en categorietheorie, worden ze zorgvuldig en gepast behandeld. We kunnen stellen dat wiskunde een duidelijke en afdoende basis heeft gevonden in de verzamelingenleer en modeltheorie. Beide kan men duidelijk definieren en ze zijn de juiste grondslagen voor elkaar. Hedendaags onderzoek in verzamelingenleer is divers, maar altijd gericht op het uiteindelijke doel van de theorie: de structuur van het wiskundige universum te beschrijven.

Hoofdstuk

3 Combinatoriek

De kardinaliteit van een eindige verzameling is een natuurlijk getal. Combinatoriek kan men zien als de studie van aritmetische verbanden tussen de kardinaliteiten van eindige verzamelingen.

3.1 Elementaire principes

Ladenprincipe van Dirichlet, duivenhokprincipe

Als $n+1$ objecten verdeeld moeten worden over n laden, dan zal minstens één lade meer dan één object bevatten.

Alhoewel dit een eenvoudig principe is, zijn er heel wat toepassingen te bedenken van dit principe.

1. In elke verzameling van ten minste 13 mensen, zijn er ten minste 2 die verjaren in dezelfde maand.

2. In elke groep mensen zijn er steeds 2 mensen te vinden die evenveel vrienden in de groep hebben. (We veronderstellen wel dat de vriendschap wederkerig (dus symmetrisch) is en antireflexief.)

Dit tweede voorbeeld is, in tegenstelling tot het eerste, niet triviaal. Inderdaad, noem X de groep mensen, en noem f een afbeelding van X naar $\mathbb{N}$, zodanig dat $f(x)$ het aantal vrienden van $x \in X$ is. Als $|X| = m$, dan kan $f(x)$ de waarden $0, 1, \ldots, m-1$ aannemen. Met andere woorden, het waardegebied van f is een deelverzameling van $\mathbb{N}_{<m}$. Om het ladenprincipe te kunnen toepassen, moeten we echter nog bewijzen dat het waardegebied een eigenlijke deelverzameling is van $\mathbb{N}_{<m}$. Merk echter op dat, indien er een persoon a is die $m-1$ vrienden heeft (met andere woorden alle personen uit X zijn vrienden van a), dan is er geen enkel persoon uit X zonder vrienden,

dus in dit geval is 0 geen element van de waardeverzameling van f, en omgekeerd als 0 tot de waardeverzameling behoort, dan zal $m-1$ er niet toe behoren. Bijgevolg is de waardeverzameling een echte deelverzameling van $\mathbb{N}_{<m}$ en heeft dus ten hoogste $m-1$ elementen. Nu kunnen wij het ladenprincipe toepassen en er zijn dus ten minste 2 mensen a en b uit de groep waarvoor geldt dat $f(a) = f(b)$. Daarmee is de uitspraak aangetoond.

Het somprincipe

Dit principe is evenals het ladenprincipe elementair. We formuleren het als een stelling.

Stelling 3.1

Als A_i $(i = 1, \ldots, k)$ k twee aan twee disjuncte, eindige verzamelingen zijn, dan is

$$|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{i=1}^{k} |A_i|.$$

Bewijs. Dit principe kan eenvoudig bewezen worden door te steunen op het inductieprincipe. □

Het somprincipe geeft ons de mogelijkheid om het ladenprincipe in een meer algemene vorm te formuleren.

Veralgemeend ladenprincipe

Indien m objecten over n laden moeten verdeeld worden waarbij $m > nr$, dan is er ten minste één lade die meer dan r objecten bevat.

3.2 Het principe van de dubbele telling

Veronderstel dat X en Y twee eindige verzamelingen zijn met $|X| = n$ en $|Y| = m$ en S een willekeurige deelverzameling van $X \times Y$. Indien we nu de kardinaliteit van deze eindige verzameling S willen bepalen, dan kunnen wij

op twee manieren te werk gaan. Men kan met name eerst alle koppels tellen die een welbepaalde x als eerste element bevatten. Noem $r_x(S)$ het aantal koppels in S die x als eerste element bevatten. Dan is

$$|S| = \sum_{x \in X} r_x(S).$$

Noem anderzijds $k_y(S)$ het aantal koppels in S die y als tweede element bevatten. Dan is

$$|S| = \sum_{y \in Y} k_y(S).$$

Deze telmethode, het principe van de dubbele telling genoemd, is op het eerste zicht zeer eenvoudig, maar heeft heel wat toepassingen. Wij vatten deze methode in de volgende stelling samen.

Stelling 3.2

Indien X en Y twee eindige niet-ledige verzamelingen zijn, en indien S een deelverzameling is van $X \times Y$, dan gelden volgende eigenschappen.

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} k_y(S).$$

Gevolg 3.3

Stel $S \subset X \times Y$, X en Y twee eindige niet-ledige verzamelingen.

1. Indien $r_x(S)$ een constante r is, onafhankelijk van de keuze van $x \in X$, en indien $k_y(S)$ een constante k is, onafhankelijk van de keuze van $y \in Y$, dan is

$$r|X| = k|Y|.$$

2. De orde van $X \times Y$ wordt gegeven door

$$|X \times Y| = |X| \cdot |Y|.$$

3.3 Het eenvoudig inclusie–exclusie principe

Dit principe is een uitbreiding van het somprincipe. In zijn eenvoudigste versie kan men dit principe als volgt formuleren:

Eenvoudig inclusie-exclusie principe

Als A en B twee eindige verzamelingen zijn, dan vindt men het kardinaalgetal van de unie van A en B als de som van de kardinaalgetallen van A en van B waarvan men het aantal elementen van de doorsnede van beide verzamelingen aftrekt

$$|A \cup B| = |A| + |B| - |A \cap B| \,.$$

We komen later terug op een algemene versie van dit principe.

Oefening 3.4. *Hoeveel natuurlijke getallen van* 1 *tot* 1000 *zijn niet deelbaar door* 3 *of* 7*?*

Oplossing. Noteer V_3 en V_7 voor de verzamelingen van de drievouden, resp. de zevenvouden, kleiner dan of gelijk aan 1000. Het antwoord op de vraag wordt gegeven door

$$1000 - |V_3 \cup V_7|$$

(ook al een inclusie/exclusie toepassing). Blijft nu het bepalen van $|V_3 \cup V_7|$. Het is duidelijk dat $|V_3| = 333$ en dat $|V_7| = 142$. Verder geldt eveneens $V_3 \cap V_7 = V_{21}$ (de verzameling van de 21-vouden) en $|V_{21}| = 47$. Het antwoord op de vraag vinden we dus als

$$1000 - (333 + 142 - 47) = 572.$$

■

3.4 Combinatieleer

Traditioneel wordt onder *combinatieleer* het tellen van al dan niet geordende k-tallen verstaan. Hierbij kunnen in deze k-tallen al dan niet herhalingen optreden. We geven hier een kort overzicht van deze theorie.

3.4.1 Variaties

Voorbeeld 3.5. Een voetbaltoernooi wordt door 4 ploegen gespeeld (we noemen ze a, b, c, d). Telkens wordt een thuis– en een uitwedstrijd gespeeld. Veronderstel dat we met ab noteren dat de ploeg a als thuisploeg speelt tegen de ploeg b (als uitploeg). Hoeveel wedstrijden moeten er dan gespeeld worden?

Er wordt dus gevraagd naar het aantal koppels bestaande uit verschillende elementen, die we kunnen maken uit de verzameling $X = \{a, b, c, d\}$. In dit geval zijn deze koppels eenvoudig uit te schrijven. Het zijn er 12, met name

$$\begin{array}{cccc} ab & ba & ca & da \\ ac & bc & cb & db \\ ad & bd & cd & dc \end{array}$$

Definitie 3.6

Een *variatie van n elementen in groepen van k* is een **geordend** k–tal van k **verschillende** elementen gekozen uit een gegeven **verzameling** van n elementen.

Het totaal aantal variaties van n elementen in groepen van k noteren we door V_n^k of nog door $P(n, k)$.

Opmerkingen

1. Het is duidelijk dat $k \leq n$; $k \in \mathbb{N}$ en $n \in \mathbb{N}$. Hierbij veronderstellen we stilzwijgend dat indien $k = 0$, $V_n^0 = 1$.
2. Twee verschillende variaties van n elementen in groepen van k kunnen dus verschillend zijn
   - door de opgenomen elementen;
   - door de volgorde van de elementen.

Stelling 3.7

Er geldt $V_n^k = n(n-1)\cdots(n-(k-1))$.

Bewijs. Aangezien de volgorde van belang is, en aangezien een element geen 2 maal in een variatie kan voorkomen, kunnen we als volgt te werk gaan. We kiezen eerst het eerste element, dat kan op n verschillende manieren, eens het eerste element gekozen, blijven er nog $n-1$ manieren over om het tweede element te kiezen, waarna er nog $n-2$ manieren zijn om het derde element te kiezen. Indien wij zo verder gaan, zullen er voor de laatste keuze (met name de $k$de keuze) nog $n-(k-1)$ kandidaten overblijven. In het totaal zijn er dus $n(n-1)\cdots(n-(k-1))$ mogelijke variaties van n elementen in groepen van k. □

3.4.2 Permutaties

Definitie 3.8

Een variatie van n elementen in groepen van n, wordt een *permutatie* genoemd.

Met andere woorden, een permutatie is een geordend n-tal van n verschillende elementen. Twee permutaties van n elementen zijn dus verschillend door de **volgorde** van de elementen. Het is duidelijk dat het aantal permutaties van n elementen gelijk is aan

$$P(n,n) = n(n-1)(n-2)\ldots 4\cdot 3\cdot 2.$$

Zoals we reeds vroeger gezien hebben, wordt dit aantal kort voorgesteld door $n!$ (n faculteit).

Opmerkingen

1. We spreken af dat 0!=1.
2. Uit de formule van het aantal variaties van n elementen in groepen van k volgt duidelijk dat dit kan geschreven worden als

   $$V_n^k = \frac{n!}{(n-k)!}.$$

   Merk terloops op dat, indien we $k=0$ stellen in de bovenstaande formule, $V_n^0 = \frac{n!}{n!} = 1$, hetgeen de eerdere afspraak rechtvaardigt. Anderzijds is $0! = 1$ in overeenstemming met

   $$V_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!.$$

3. Het woord permutatie is uiteraard goed gekozen. Inderdaad, een permutatie van n elementen is niets anders dan een bijectie van een verzameling met n elementen op zichzelf. De verzameling van alle permutaties van een verzameling met n elementen stellen we voor door S_n.

3.4.3 Combinaties

Voorbeeld 3.9. Veronderstel dat bij het voetbaltoernooi tussen de 4 ploegen a, b, c, d telkens slechts 1 wedstrijd (op neutraal terrein) wordt gespeeld. In dit geval speelt de volgorde dus geen rol. We zoeken in dit geval nu naar het aantal **paren** uit de verzameling van 4 elementen. Dit aantal is uiteraard 6.

Definitie 3.10

Een *combinatie van n elementen in groepen van k* is een **deelverzameling** met k elementen uit een gegeven verzameling van n elementen.

Het aantal combinaties van n elementen in groepen van k stellen we voor door $\binom{n}{k}$ of $C(n,k)$. Deze getallen worden ook nog de *binomiaalgetallen* of de *binomiaalcoëfficiënten* genoemd.

Stelling 3.11

Er geldt $V_n^k = \binom{n}{k} \cdot k! \quad (n, k \in \mathbb{N},\ k \leq n)$.

Bewijs. Een willekeurige variatie van n elementen in groepen van k ontstaat door eerst een deelverzameling met k elementen uit de verzameling van deze n elementen te nemen, en dit kan op $\binom{n}{k}$ manieren, en daarna de volgorde van de k elementen in deze deelverzameling vast te leggen. We kunnen deze k elementen op $k!$ manieren permuteren, m.a.w. we kunnen deze k elementen op $k!$ manieren ordenen. In het totaal kunnen we dus op die manier $\binom{n}{k}k!$ variaties construeren. □

Gevolg 3.12

Er geldt $\binom{n}{k} = \dfrac{V_n^k}{k!} = \dfrac{n!}{(n-k)!k!}$.

Enkele belangrijke eigenschappen formuleren we in de volgende lemma's en een stelling.

Lemma 3.13

Er geldt $\binom{n}{k} = \binom{n}{n-k}$.

Bewijs. Dit volgt onmiddellijk uit de bovenstaande formule, maar kan ook onmiddellijk uit de definitie afgeleid worden. □

Lemma 3.14

Er geldt $\binom{n}{k+1} = \binom{n}{k} \cdot \frac{n-k}{k+1}$.

Bewijs.

$$\begin{aligned}\binom{n}{k+1} &= \frac{n!}{(k+1)!(n-(k+1))!} \\ &= \frac{n!}{k!(n-k)!} \cdot \frac{n-k}{k+1} \\ &= \frac{n-k}{k+1} \cdot \binom{n}{k}.\end{aligned}$$

□

Stelling 3.15 — Formule van Stifel–Pascal

Er geldt $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ $(n, k \in \mathbb{N}^*,\ k < n)$.

Bewijs. Inderdaad, indien we uit de verzameling van n elementen één element a fixeren, dan kunnen al de mogelijke combinaties van de n elementen in groepen van k ingedeeld worden in twee disjuncte verzamelingen. Enerzijds zijn er de combinaties die a bevatten. Een dergelijke combinatie vormen we door uit de $n-1$ overblijvende elementen $k-1$ andere elementen te kiezen. Het aantal is $\binom{n-1}{k-1}$. Anderzijds zijn er de combinaties die a niet bevatten, zo een combinatie vormen we door uit de $n-1$ overblijvende elementen er juist k uit te kiezen, hun aantal is $\binom{n-1}{k}$. Hieruit volgt de formule. □

De driehoek van Pascal

Uit de definitie en de eigenschappen van de combinaties kunnen we afleiden dat

$$\begin{array}{lcll} \binom{n}{0} & = & \binom{n}{n} & = 1 \\ \binom{n}{1} & = & \binom{n}{n-1} & = n \\ \binom{n}{2} & = & \binom{n}{n-2} & = \dfrac{n(n-1)}{2} \\ \ldots & & \ldots & \ldots \end{array}$$

Uit de formule $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ $(n, k \in \mathbb{N}^*,\ k < n)$, volgt een recursieve methode om de binomiaalgetallen $\binom{n}{k}$ te berekenen, indien de binomiaalgetallen $\binom{n-1}{k}$, $0 \leq k \leq n-1$, gekend zijn. De getallen worden veelal in een driehoek gerangschikt. Deze driehoek wordt soms de driehoek van Pascal genoemd, naar Blaise Pascal (1623–1662).

1												
1	1											
1	2	1										
1	3	3	1									
1	4	6	4	1								
1	5	10	10	5	1							
1	6	15	20	15	6	1						
1	7	21	35	35	21	7	1					
1	8	28	56	70	56	28	8	1				
1	9	36	84	126	126	84	36	9	1			
1	10	45	120	210	252	210	120	45	10	1		
1	11	55	165	330	462	462	330	165	55	11	1	
1	12	66	220	495	792	924	792	495	220	66	12	1

3.4.4 Herhalingsvariaties

Zoals het woord het zelf zegt, zal in dit geval een element in een geordend k-tal meerdere malen mogen voorkomen. De definitie luidt dus als volgt.

Definitie 3.16

Een *herhalingsvariatie van n elementen in groepen van k* is een **geordend** k-tal elementen uit een verzameling van n elementen.

Het aantal herhalingsvariaties van n elementen in groepen van k noteren we door $\overline{V_n^k}$ of $\overline{P(n,k)}$.

Stelling 3.17

Er geldt $\overline{V_n^k} = n^k$.

Bewijs. Dit is onmiddellijk duidelijk, aangezien bij elke nieuwe keuze, al de elementen uit de verzameling van n elementen gekozen mogen worden. □

Opmerking

Het is duidelijk dat hier in tegenstelling tot het geval van de variaties zonder herhaling, k kleiner dan, gelijk aan of groter dan n kan zijn.

3.4.5 Herhalingscombinaties

Definitie 3.18

Een *herhalingscombinatie van n elementen in groepen van k* is een **niet-geordend** k-tal elementen, gekozen uit een verzameling van n elementen.

Het aantal dergelijke herhalingscombinaties wordt voorgesteld door $\overline{\binom{n}{k}}$ of nog door $\overline{C(n,k)}$.

Een herhalingscombinatie ontstaat dus door uit een voorraad van n voorwerpen, bvb. a_1, a_2, ... ,a_n, precies k voorwerpen uit te kiezen. Herhaling is mogelijk maar de volgorde is niet van belang. In het algemeen zal zo'n keuze er dus als volgt uitzien: men heeft bijvoorbeeld r_1 keer het voorwerp a_1 gekozen, r_2 keer het voorwerp a_2, ..., r_n keer het voorwerp a_n. Vermits in totaal k voorwerpen gekozen werden, geldt uiteraard dat $r_1 + r_2 + r_3 + \cdots + r_n = k$. We kunnen dus stellen

> Het aantal herhalingscombinaties van n elementen in groepen van k is gelijk aan het aantal manieren waarop we een natuurlijk getal k kunnen schrijven als de som van n natuurlijke getallen r_1, r_2, ... r_n.

Stelling 3.19

Er geldt $\overline{\binom{n}{k}} = \binom{n+k-1}{k}$.

Bewijs. Aangezien de volgorde geen belang heeft kunnen we dus in elk k-tal al de elementen van dezelfde soort samen plaatsen. We maken ons hiervan nu de volgende voorstelling. We beschikken over n hokjes waarover we k stippen verdelen. Indien we de hokjes afscheiden door middel van een schot (rechte streep), dan hebben we hiervoor $n-1$ schotten nodig. Het probleem is dus herleid tot het opvullen van $n-1+k$ plaatsen met k stippen en $n-1$ rechte strepen. Indien we eerst de k stippen plaatsen, dan moeten de overige $n-1$ plaatsen ingenomen worden door strepen. Bijgevolg is het voldoende om na te gaan op hoeveel manieren we $n-1+k$ plaatsen kunnen opvullen met k stippen (of gelijkwaardig hiermee: op hoeveel manieren we $n-1+k$ plaatsen kunnen opvullen met $n-1$ strepen). Met andere woorden, het probleem is herleid tot de vraag op hoeveel manieren we uit een verzameling van $n-1+k$ plaatsen er k kunnen selecteren. Dit is uiteraard het aantal combinaties van $n-1+k$ elementen in groepen van k (of gelijkwaardig: in groepen van $n-1$). □

Samenvatting

De verschillende tellingen die we hier besproken hebben, hangen af van de manier van kiezen van de elementen; met name

- met of zonder terugplaatsen van de gekozen elementen,
- met of zonder rekening te houden met de volgorde.

Tabel 3.1 vat de resultaten samen.

3.5 Toepassingen op combinatieleer

3.5.1 De binomiale kansverdeling

Combinatorische tellingen van bovenstaande aard komen zeer veel voor in de theorie van de kansrekening. We beperken ons hier tot één basisvoorbeeld.

	zonder terugplaatsen	met terugplaatsen
ongeordend	$\binom{n}{k}$	$\binom{n+k-1}{k}$
geordend	$n(n-1)\cdots(n-k+1)$	n^k

Tabel 3.1: Overzicht (herhalings)variaties en (herhalings)combinaties

Gegeven is een voorraad van a blauwe letters en van b rode letters. Alle letters zijn verschillend. Hoeveel woorden (eventueel zonder betekenis) van n letters (met herhaling van letters toegestaan) kunnen hieruit gevormd worden? Dat is eenvoudig: $(a+b)^n$. Hoeveel van die mogelijke woorden bevatten juist k blauwe (en dus $n-k$ rode) letters? Daarvoor gaan we eerst na op hoeveel manieren we van n plaatsen er k kunnen blauw kleuren (en de rest dus rood). Dit is het aantal combinaties van n elementen in groepen van k, met andere woorden $\binom{n}{k}$. Op hoeveel manieren kunnen we nu de blauwe plaatsen invullen met een blauwe letter? Dit is duidelijk op a^k manieren (herhalingsvariatie). Analoog kunnen de rode plaatsen op b^{n-k} manieren opgevuld worden met rode letters. Het totaal aantal woorden met k blauwe en $n-k$ rode letters is bijgevolg gelijk aan

$$\binom{n}{k} a^k b^{n-k}.$$

Gesteld dat we dus de kans willen bepalen opdat bij de keuze van 1 woord uit de $(a+b)^n$ woorden we een woord kiezen met juist k blauwe letters en $n-k$ rode letters, dan wordt deze kans gegeven door:

$$\frac{1}{(a+b)^n}\binom{n}{k} a^k b^{n-k}.$$

Merk op dat $a/(a+b) = p$ de kans is dat we uit de $a+b$ letters er 1 blauwe uitnemen, en dat $b/(a+b) = q$ de kans is dat we uit de $a+b$ letters er 1 rode uitnemen (merk op dat er slechts één van de 2 mogelijkheden kan optreden, zodat $p+q=1$). We kunnen dan de bovenstaande formule als volgt herschrijven:

$$\begin{aligned} \frac{1}{(a+b)^n}\binom{n}{k} a^k b^{n-k} &= \binom{n}{k}\left(\frac{a}{a+b}\right)^k \left(\frac{b}{a+b}\right)^{n-k} \\ &= \binom{n}{k} p^k q^{n-k} \end{aligned}$$

Dergelijk model wordt de *binomiale* kansverdeling genoemd. Een gelijkwaardige formulering van dit model is als volgt.

> *Wat is de kans dat we uit een verzameling van n voorwerpen waarvan er n_1 de eigenschap s_1 en n_2 de eigenschap s_2 hebben ($n_1 + n_2 = n$), er juist k elementen uitnemen met de eigenschap s_1, waarbij het gekozen voorwerp telkens teruggeplaatst wordt.*

3.5.2 Het aantal deelverzamelingen van een verzameling

Stelling 3.20

Een verzameling X van n elementen bezit 2^n deelverzamelingen.

Bewijs. Noem $X = \{x_1, x_2, \ldots, x_n\}$ en beschouw de verzameling $Y = \{0, 1\}$. Met elke deelverzameling S van X kunnen we nu een functie f_S van X naar Y laten corresponderen, die als volgt gedefinieerd wordt.

$$f_S(x_i) = \begin{cases} 0 & \text{als} \quad x_i \notin S \\ 1 & \text{als} \quad x_i \in S. \end{cases}$$

Het aantal deelverzamelingen van X is bijgevolg gelijk aan het aantal manieren waarop we uit een verzameling Y met 2 elementen geordende n-tallen kunnen kiezen. Dit is bijgevolg gelijk aan het aantal herhalingsvariaties van 2 elementen in groepen van n, dus aan 2^n. □

3.5.3 Het binomium van Newton

De volgende formules maken deel uit van de zogenaamde reeks merkwaardige producten

$$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2 \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3. \end{aligned}$$

Deze formules zijn bijzondere gevallen van het zogenaamde *binomium van Newton*.

Stelling 3.21

Veronderstel dat n een positief natuurlijk getal is, dan geldt voor elke 2 (reële) getallen a en b, dat

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Bewijs. Het bewijs van deze stelling is zeer eenvoudig. De formule volgt eigenlijk uit de manier waarop we het product met n factoren $(a+b)(a+b)\cdots(a+b)$ uitrekenen. De coëfficiënt van $a^k b^{n-k}$ is het aantal manieren om uit de n factoren $(a+b)$, k maal a te kiezen (en dus $n-k$ maal b). Dit is het aantal combinaties van n elementen in groepen van k, dus $\binom{n}{k}$. □

Opmerking

1. Het doet er niet toe of a en b reële getallen zijn, we hebben enkel gesteund op de commutativiteit van de vermenigvuldiging.

2. Volgende vormen zijn allemaal equivalente vormen van het binomium van Newton (bewijs als oefening)

$$\begin{aligned}
(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= \sum_{k=0}^{n} \binom{n}{n-k} a^{n-k} b^k.
\end{aligned}$$

3.5.4 Het (veralgemeend) inclusie–exclusieprincipe

We hebben in het vereenvoudigd inclusieprincipe gezien dat voor de kardinaliteit van de unie van 2 verzamelingen A_1 en A_2 geldt:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Beschouwen we 3 verzamelingen A_1, A_2 en A_3, dan moeten we naast de orde van de doorsneden $A_1 \cap A_2$, $A_1 \cap A_3$, $A_2 \cap A_3$, ook rekening houden met de orde van de doorsnede $A_1 \cap A_2 \cap A_3$ en dan geldt:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Deze formules kunnen we nu samenvatten in het zogenaamde (veralgemeend) *inclusie–exclusieprincipe*.

Stelling 3.22 — Inclusie-exclusieprincipe

Als $A_1, A_2, \ldots, A_n$ eindige verzamelingen zijn, dan is

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n.$$

Hierbij is α_i de notatie voor de som van de kardinaalgetallen van al de mogelijke doorsneden die men kan vormen met i dergelijke verzamelingen A_i.

Bewijs. We bewijzen dat elk element x uit de unie inderdaad slechts 1 maal wordt geteld in het rechterlid. Veronderstel dat x tot juist k verzamelingen behoort. Dan zal x een bijdrage k leveren in $\alpha_1 = \sum_{i=1}^{n} |A_i|$. In de som $\alpha_2 = \sum_{i,j=1}^{n} |A_i \cap A_j|$ $(i \neq j)$ zal de bijdrage 1 zijn dan en slechts dan als A_i en A_j zich onder de k verzamelingen bevinden die x bevatten. Er zijn $\binom{k}{2}$ dergelijke paren verzamelingen $\{A_i, A_j\}$, bijgevolg is $\binom{k}{2}$ de bijdrage van x tot α_2. Algemeen is $\binom{k}{i}$ de bijdrage van x in α_i. De totale bijdrage van x in het rechterlid is bijgevolg

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{k-1}\binom{k}{k}.$$

Aangezien echter (zie oefeningen)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

volgt hieruit dat de bijdrage van x tot het rechterlid juist 1 is. □

3.5.5 Permutaties zonder fixelementen

Een weinig efficiënte secretaresse moet n brieven in n omslagen doen. Op hoeveel manieren kan ze erin slagen om alle brieven in verkeerde omslagen te doen?

We vragen dus in feite het aantal permutaties van de verzameling $\{1, \ldots, n\}$ die geen enkel fixelement bezitten. Volgens het inclusie-exclusie principe is het totaal aantal permutaties zonder fixelementen d_n van $\{1, \ldots, n\}$ gelijk aan

$$d_n = n! - \alpha_1 + \alpha_2 - \cdots + (-1)^n \alpha_n,$$

waarbij α_i het aantal permutaties is van $\{1, \ldots, n\}$ die minstens i elementen fixeren voor alle mogelijke keuzes van i uit $\{1, \ldots, n\}$. Er zijn nu $\binom{n}{i}$ manieren om i elementen te kiezen uit $\{1, \ldots, n\}$, en het aantal permutaties van $\{1, \ldots, n\}$ die deze i elementen (elementgewijze) fixeren is het aantal permutaties op de $n - i$ overige elementen, met andere woorden $(n - i)!$. Bijgevolg is

$$\alpha_i = \binom{n}{i} \times (n - i)! = \frac{n!}{i!}.$$

Zodat het totaal aantal permutaties zonder fixelementen gelijk is aan

$$d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

Willen we echter een recursieve definitie van het getal d_n vinden, dan kunnen we als volgt te werk gaan. Aangezien geen enkel element van $\{1, \ldots, n\}$ gefixeerd wordt, is het beeld van 1 onder een bepaalde wanorde f het getal $f(1) = k_1$ met $k_1 \neq 1$. We fixeren nu k_1. Er kunnen nu 2 gevallen optreden: ofwel is $f(k_1) = 1$ (maw. $f^2(1) = 1$)) ofwel is $f(k_1) \neq 1$. We tellen nu beide soorten van permutaties zonder fixelementen.

Indien $f(k_1) = 1$, dan zal f een permutatie zonder fixelementen definiëren op de verzameling $\{1, \ldots, n\} \setminus \{1, k_1\}$. Het aantal dergelijke permutaties is per definitie gelijk aan d_{n-2}. Merk op dat elke permutatie zonder fixelementen op $\{1, \ldots, n\} \setminus \{1, k_1\}$ aanleiding geeft tot juist 1 permutatie zonder fixelementen op $\{1, \ldots, n\}$ door de definitie $f(1) = k_1;\ f(k_1) = 1$.

Veronderstel nu dat f een permutatie zonder fixelementen is waarvoor geldt dat $f(k_1) \neq 1$, dan bestaat er een $k_0 \in \{1, \ldots, n\} \setminus \{1, k_1\}$ zodanig dat $f(k_0) = 1$. We definiëren nu een nieuwe permutatie g in $\{2, \ldots, n\}$ door $g(k_0) = k_1$ en $g(k) = f(k)\ \forall k \neq k_0$. Dan is g eveneens een permutatie zonder fixelementen, maar nu op de verzameling $\{2, \ldots, n\}$, en zo zijn er

d_{n-1}. Aangezien we weten dat 1 het beeld is onder f van k_0 en dat k_1 het beeld is onder f van 1, kunnen we op een unieke manier g uitbreiden tot de permutatie f waarvan we waren vertrokken.

Bijgevolg het aantal permutaties zonder fixelementen f waarvoor geldt dat $f(1) = k_1 \in \{2, \ldots, n\}$ (met k_1 een vast gekozen getal) is gelijk aan $d_{n-1} + d_{n-2}$. Aangezien er nu $n-1$ mogelijke keuzes zijn voor k_1, zal

$$d_n = (n-1)(d_{n-1} + d_{n-2}).$$

Merk op dat $d_1 = 0$ terwijl $d_2 = 1$, zodat we op die manier een recursieve definitie gegeven hebben van het aantal permutaties zonder fixelementen op een verzameling van n elementen.

Deze recursieve definitie geeft de volgende waarden van d_n voor $n \leq 8$

n	1	2	3	4	5	6	7	8
d_n	0	1	2	9	44	265	1854	14833

3.6 De Stirlinggetallen

Definitie 3.23

Het *Stirlinggetal* $S(n,k)$ (van de tweede soort) is per definitie het aantal mogelijkheden waarop men een verzameling X met n elementen kan schrijven als een disjuncte unie van k niet-ledige deelverzamelingen.

Stelling 3.24

Het Stirlinggetal $S(n,k)$ met $1 \leq k \leq n$ wordt recursief gedefinieerd door

$$\begin{aligned} S(n,1) &= 1 \\ S(n,k) &= S(n-1,k-1) + kS(n-1,k) \quad (2 \leq k \leq n-1) \\ S(n,n) &= 1. \end{aligned}$$

Bewijs. Het is duidelijk dat $S(n,1) = S(n,n) = 1$. Veronderstel nu dat $2 \leq k \leq n-1$. Noem z een willekeurig element van X. Indien we al de mogelijke partities van X in k klassen beschouwen, dan zal ofwel (i) het singleton $\{z\}$

een klasse van de partitie zijn ofwel (ii) zal $\{z\}$ een eigenlijke deelverzameling zijn van één klasse. Indien we in het eerste geval $\{z\}$ wegnemen uit de partitie, dan ontstaat een partitie van de verzameling $X \setminus \{z\}$ in $k-1$ klassen. Het aantal dergelijke partities is $S(n-1, k-1)$. Omgekeerd zal elke partitie $\mathcal{P}$ van $X \setminus \{z\}$ in $k-1$ klassen, op unieke manier een partitie van X in k klassen definiëren door aan $\mathcal{P}$ het singleton $\{z\}$ toe te voegen. Indien we echter in het tweede geval z wegnemen uit de partitie, dan ontstaat een partitie van de verzameling $X \setminus \{z\}$ in k klassen. Omgekeerd, beschouw een partitie $\mathcal{P}$ van de verzameling $X \setminus \{z\}$ in k klassen. Dan kunnen we hieruit k verschillende partities in k klassen van de verzameling X construeren door het element z achtereenvolgens toe te voegen aan elke klasse van $\mathcal{P}$. Hieruit mogen we besluiten dat er $k \cdot S(n-1, k)$ partities van de tweede soort zijn.

Het totaal aantal partities van een verzameling van n elementen in k klassen is bijgevolg gelijk aan

$$S(n, k) = S(n-1, k-1) + kS(n-1, k) \quad (2 \leq k \leq n-1). \qquad \square$$

Voorbeeld

Naar analogie met de driehoek van Pascal voor binomiaalgetallen kan er ook een driehoek voor de Stirlinggetallen van de tweede soort opgesteld worden.

1						
1	1					
1	3	1				
1	7	6	1			
1	15	25	10	1		
1	31	90	65	15	1	
1	63	301	350	140	21	1

Gevolg 3.25

Het aantal surjecties van een verzameling X ($|X| = n$) naar een verzameling Y ($|Y| = k$) is gelijk aan $k!S(n, k)$.

Bewijs. Bewijs dit gevolg als oefening. $\square$

De kritische lezer vraagt zich misschien af waar de Stirlinggetallen van de *eerste* soort gebleven zijn. In [12, Sectie 3.4] vindt men een prima omschrijving van de *beide* soorten Stirlinggetallen en het verband ertussen.

3.7 De multinomiaalgetallen

Het aantal functies van een verzameling X met n elementen op een verzameling $Y = \{y_1, y_2, \ldots, y_k\}$, zodanig dat y_i het beeld is van n_i elementen uit X ($\sum_{i=1}^{k} n_i = n$), wordt het *multinomiaalgetal* genoemd en genoteerd als:

$$\begin{pmatrix} n \\ n_1, n_2, \ldots, n_k \end{pmatrix}.$$

Merk op dat

$$\binom{n}{n_1, n_2} = \binom{n}{n_1},$$

vandaar de benaming multinomiaalgetallen als veralgemening van de binomiaalgetallen.

Stelling 3.26

Voor elke verzameling positieve natuurlijke getallen $n, n_1, \ldots n_k$ waarvoor $\sum_{i=1}^{k} n_i = n$ is

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

Bewijs. We mogen veronderstellen dat elk element y_i minstens één maal wordt bereikt, maw. alle $n_i > 0$. Merk echter op dat in de definitie $n_i = 0$ toegelaten is, maar als gevolg van de afspraak $0! = 1$ levert dit toch geen bijdrage tot het multinomiaalgetal. Met andere woorden we mogen veronderstellen dat we het aantal surjecties f van X op $Y = \{y_1, y_2, \ldots, y_k\}$ tellen zodanig dat y_i het beeld is van n_i elementen uit X. Elke surjectie definieert een partitie van X in k klassen X_i met $|X_i| = n_i$. Indien we de n_i elementen uit de klasse X_i onderling permuteren, ontstaat een permutatie van de verzameling X. Gegeven f ontstaan op die manier $n_1! n_2! \cdots n_k!$ permutaties. Indien we al de mogelijke surjecties van X op $Y = \{y_1, y_2, \ldots, y_k\}$, zodanig dat y_i beeld is van n_i elementen uit X beschouwen, en zo zijn er dus

$$\binom{n}{n_1, n_2, \ldots, n_k}$$

en telkens de elementen van al de klassen X_i permuteren, en zo zijn er dus $n_1! n_2! \cdots n_k!$, dan hebben we al de mogelijke permutaties van X geconstrueerd, en dit zijn er $n!$. Hieruit volgt het gestelde. □

Aangezien de multinomiaalgetallen de veralgemening zijn van de binomiaalgetallen, is het niet verwonderlijk dat er een veralgemening bestaat van het binomium van Newton, met name de *multinomiaalstelling*.

Stelling 3.27

Voor elke 2 positieve natuurlijke getallen n en k geldt dat

$$(\sum_{i=1}^{k} a_i)^n = \sum \binom{n}{n_1, n_2, \cdots, n_k} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}.$$

Hierbij wordt de som in het rechterlid genomen over al de mogelijke k-tallen van natuurlijke getallen $(n_1, n_2, \ldots, n_k)$ waarvoor $\sum_{i=1}^{k} n_i = n$.

Bewijs. De coëfficiënt van $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ in de ontwikkeling is het aantal keer dat we uit de n factoren $(a_1 + a_2 + \cdots + a_k)$, de term a_1 nemen uit n_1 van de factoren, de term a_2 nemen uit n_2 van de factoren, $\ldots$, de term a_k nemen uit n_k van de factoren. Dit is juist de definitie van de multinomiaalgetallen. Hieruit volgt het gestelde. □

Hoofdstuk

4 Getaltheorie

4.1 Deelbaarheid en grootste gemene deler

Definitie 4.1

Deelbaarheid in $\mathbb{Z}$ is een relatie $\mathcal{D} \subset \mathbb{Z} \setminus \{0\} \times \mathbb{Z}$ gedefinieerd door

$$(a, b) \in \mathcal{D} \iff \exists q \in \mathbb{Z} : b = a \cdot q.$$

We noemen $\mathcal{D}$ ook de *deelbaarheidsrelatie* en we zeggen dat a *een deler is van* b of dat b *een* a*-voud* is, of b *is deelbaar door* a of nog dat a *een factor is van* b. Indien $(a, b) \in \mathcal{D}$, dan noteren we dit kort als $a \mid b$, terwijl $a \nmid b$ een verkorte notatie is voor $(a, b) \notin \mathcal{D}$.

Enkele eigenschappen liggen voor de hand. We formuleren ze in opeenvolgende lemma's.

Lemma 4.2

Voor $a, b, c, m, n \in \mathbb{Z}$ geldt

(i) $a \mid b$ en $a \mid c \implies a \mid (b + c)$.

(ii) $a \mid b \implies a \mid bc$.

(iii) $a \mid m$ en $b \mid n \implies ab \mid mn$.

Bewijs. (i) Uit de veronderstelling volgt dat er gehele getallen d, e bestaan waarvoor $a \cdot d = b$ en $a \cdot e = c$. Dus $a(d + e) = b + c$, dus $a \mid (b + c)$.

(ii) Uit $a \mid b$ volgt dat $a \cdot d = b$ voor een zekere $d \in \mathbb{Z}$. Dus $a \cdot d \cdot c = b \cdot c$, dus $a \mid bc$.

(iii) Analoog aan (ii). □

Gevolg 4.3

Veronderstel $a \mid b$ en $a \mid c$. Dan zal voor alle gehele getallen x en y gelden dat $a \mid (bx + cy)$

Lemma 4.4

De deelbaarheidsrelatie beperkt tot $\mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\}$ is reflexief en transitief.

Lemma 4.4 formuleert welgekende eigenschappen van deelbaarheid in $\mathbb{Z}$ en het bewijs laten we over als oefening. De deelbaarheidsrelatie $\mathcal{D}$ is niet antisymmetrisch, $(x, -x)$ en $(-x, x)$ zijn steeds twee koppels in $\mathcal{D}$ voor alle $x \neq 0$. Haar beperking tot $\mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\}$ is dat echter wel.

Elk geheel getal $b \neq 0$ is uiteraard deelbaar door $1, -1, b$ en $-b$. We noemen deze soms de *onechte delers* van het getal. Al de andere delers worden de *echte delers* van het getal genoemd. Dus 1 is een deler is van elk geheel getal, en elk geheel getal verschillend van 0 is een deler van 0. Het getal b is *even* als $2 \mid b$ en *oneven* als $2 \nmid b$.

Voor twee gegeven gehele getallen a en $b \neq 0$, kunnen we steeds nagaan *hoeveel keer b in a past*. Indien dit een geheel aantal keer is, dan is $b \mid a$. Indien $b \nmid a$, dan zal deze deling een *rest* opleveren. De *staartdeling* of *Euclidische deling* om dit uit te voeren, is een welbekend algoritme. Beschouwen we bijvoorbeeld de getallen 126 en 35, dan vinden we dat $126 = 35 \cdot 3 + 21$. Uiteraard geldt ook dat $126 = 35 \cdot 4 - 14$. Bekijken we -126 en 35, dan zien we dat $-126 = -3 \cdot 35 - 21$, en ook $-126 = -4 \cdot 35 + 14$. Zo kunnen we ook nog 126 en -35 en -126 en -35 bekijken. Telkens zien we twee mogelijkheden, maar telkens zien we ook dat de *absolute waarde* van de rest kleiner is dan de absolute waarde van de deler. De *absolute waarde* van een geheel getal $a \in \mathbb{Z}$ is a zelf als $a \in \mathbb{N}$ en $-a$ als $a \in \mathbb{Z} \setminus \mathbb{N}$. De absolute waarde van a wordt genoteerd als $|a|$. De volgende stelling verschaft duidelijkheid.

Stelling 4.5

Voor elke 2 getallen $a \in \mathbb{Z} \setminus \{0\}$ en $b \in \mathbb{Z}$ bestaan er unieke gehele getallen q (quotiënt) en r (rest) zodanig dat

$$b = a \cdot q + r \text{ en } 0 \leq r < |a|$$

Bewijs. (a) We tonen eerst aan dat er dergelijke getallen q en r bestaan. We passen het welordeningsprincipe toe op de volgende verzameling R:

$$R = \{x \in \mathbb{N} || b = a \cdot y + x \text{ voor een } y \in \mathbb{Z}\}.$$

We bewijzen eerst dat R niet ledig is. Als $b \geq 0$, dan volgt uit $b = a \cdot 0 + b$ dat $b \in R$. Als $b < 0$, dan geldt $b = |a| \cdot b + (1 - |a|) \cdot b$. Aangezien $(1 - |a|) \cdot b \geq 0$ zal $(1 - |a|) \cdot b \in R$. De verzameling R is dus niet ledig en bezit bijgevolg een kleinste element r. We hebben $b = a \cdot q + r$ voor een zekere $q \in \mathbb{Z}$. Als $0 < a \leq r$, dan hebben we eveneens dat $b = a \cdot (q + 1) + (r - a)$ met $r > r - a \geq 0$, in tegenstrijd met de definitie van r. Als $-r \leq a < 0$, dan hebben we eveneens dat $b = a \cdot (q - 1) + (r + a)$, met $r > r + a \geq 0$, in tegenstrijd met de definitie van r. Bijgevolg geldt $r \in \mathbb{N}_{<|a|}$.

(b) We tonen de uniciteit van q en r aan. Onderstel dat $b = a \cdot q_1 + r_1 = a \cdot q_2 + r_2$ voor zekere $q_1, q_2 \in \mathbb{Z}$ en zekere $r_1, r_2 \in \mathbb{N}_{<|a|}$. Als $q_1 \neq q_2$, dan mogen we zonder verlies van algemeenheid veronderstellen dat $a \cdot (q_1 - q_2) > 0$. Dan geldt $r_2 = a \cdot (q_1 - q_2) + r_1 \geq |a| + r_1 \geq |a|$, een tegenstrijdigheid. Bijgevolg geldt $q_1 = q_2$ en daaruit volgt dan ook dat $r_1 = r_2$. □

Opmerking

Een belangrijk gevolg van deze stelling is, dat voor elk gegeven natuurlijk getal $t \geq 2$, een willekeurig positief geheel getal geschreven kan worden als een lineaire combinatie van machten van t waarbij de coëfficiënten tot de verzameling $\mathbb{N}_{<t}$ behoren. Indien we immers de voorgaande stelling herhaalde malen toepassen, dan verkrijgen we:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ \cdots &\quad \cdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Hierbij zal elke rest r_i tot $\mathbb{N}_{<t}$ behoren en zal de deling stoppen van zodra $q_n = 0$. Indien we nu de quotiënten q_i elimineren, dan verkrijgen we

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0.$$

We schrijven verkort $x = (r_n r_{n-1} \dots r_0)_t$ en we noemen dit de *ontwikkeling van x in basis t*. De meest gebruikte basissen zijn $t = 10$ (tiendelig getallenstelsel, $r_i \in \mathbb{N}_{<10}$) en $t = 2$ (binair getallenstelsel, $r_i \in \{0, 1\}$). Men kan bv. eenvoudig narekenen dat $(1992)_{10} = (11111001000)_2$.

Voor elke 2 gehele getallen a, b noemen we een geheel getal d dat zowel a als b deelt, een *gemene deler* van a en b.

Definitie 4.6

Stel $a, b \in \mathbb{Z}$ niet beide nul. Een gemene deler c van a en b is een *grootste gemene deler* van a en b als en slechts als elke gemene deler van a en b een deler is van c.

De terminologie *grootste* is dus niet gerelateerd aan de natuurlijke orderelatie op $\mathbb{Z}$, maar aan de pre-orderelatie $\mathcal{D}$. We bekijken een voorbeeld. Stel $a = 30$ en $b = 75$. De gemene delers van a en b zijn $\{-15, -5, -3, -1, 1, 3, 5, 15\}$. Elke gemene deler deelt -15 en 15. Dus -15 en 15 zijn twee verschillende grootste gemene delers van a en b. Men kan zich afvragen of er meer dan twee grootste gemene delers zijn in $\mathbb{Z}$. Het antwoord volgt uit het volgende lemma.

Lemma 4.7

Als a en b twee grootste gemene delers zijn van twee gehele getallen, dan geldt $a = b$ of $a = -b$.

Bewijs. Uit het feit dat a en b twee grootste gemene delers zijn, volgt $a \mid b$ en $b \mid a$. Er bestaan dus getallen $c, d \in \mathbb{Z}$ zodat $a \cdot c = b$ en $b \cdot d = a$. Dus $a \cdot c \cdot d = a$, dus er geldt noodzakelijk dat $c \cdot d = 1$. Met andere woorden, c en d zijn elkaars inverse in $\mathbb{Z}$, dus $c = d = 1$ of $c = d = -1$, waaruit het lemma volgt. □

Het is duidelijk dat in $\mathbb{Z}$ er steeds twee grootste gemene delers zijn, een positieve en een negatieve. We maken de keuze om de positieve gemene deler te kiezen als *de* grootste gemene deler.

Definitie 4.8

Stel $a, b \in \mathbb{Z}$ niet beide nul. *De grootste gemene deler* van a en b is de unieke positieve onder de grootste gemene delers van a en b.

Vanaf nu slaat *de grootste gemene deler* dus steeds op de unieke positieve grootste gemene deler. We noteren de grootste gemene deler van a en b als $\text{ggd}(a, b)$.

Alhoewel de *Elementen* van Euclides hoofdzakelijk over meetkunde gaan, worden in Boeken 7, 8 en 9 aritmetische problemen beschreven. Propositie 2 in Boek 7 beschrijft een algoritme om de grootste gemene deler van 2 gehele getallen te berekenen. Dit algoritme is zeer efficiënt, en staat algemeen bekend als het **algoritme van Euclides**. Het algoritme steunt op het volgende lemma.

Lemma 4.9

Stel $a, b, q, r \in \mathbb{Z}$, met $a = bq + r$. Dan geldt $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs. Stel $c = \text{ggd}(a, b)$. Dan is $c \mid a - bq = r$ door Gevolg 4.3. Dus c is een gemene deler van b en r, en bijgevolg geldt $\text{ggd}(a, b) \mid \text{ggd}(b, r)$. Stel $d = \text{ggd}(b, r)$. Dan is $d \mid bq + r = a$, opnieuw door Gevolg 4.3. Dus d is een gemene deler van a en b, en bijgevolg geldt $\text{ggd}(b, r) \mid \text{ggd}(a, b)$. Omdat beide positief zijn, besluiten we dat $\text{ggd}(a, b) = \text{ggd}(b, r)$. □

Voorbeeld 4.10. We passen het lemma toe om een grootste gemene deler van 126 en 35 te bepalen. Omdat $\text{ggd}(a, 0) = |a|$ voor alle $a \in \mathbb{Z} \setminus \{0\}$, kennen we een grootste gemene deler van zodra de deling opgaat.

$$\begin{aligned} 126 &= 3 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 \end{aligned}$$

Dus $\text{ggd}(126, 35) = 7$. De keuze van de quotiënten en resten bepaalt uiteraard niet het eindresultaat, maar wel de uitvoering van het algoritme:

$$\begin{aligned} 126 &= 4 \cdot 35 - 14 \\ 35 &= -3 \cdot (-14) - 7 \\ -14 &= -2 \cdot 7 \end{aligned}$$

Het is duidelijk dat de laatste niet-nul rest *een* grootste gemene deler is. Zijn absolute waarde is steeds de grootste gemene deler. Omdat we zeker weten dat de resten in absolute waarde steeds kleiner worden, zal dit algoritme

eindigen. We noteren de unieke positieve rest (Stelling 4.5) bij deling van a door b als $\text{rem}(a, b)$.

Algoritme 4.1 Algoritme van Euclides

input: $a, b \in \mathbb{Z} \setminus \{0\}$.
output: de grootste gemene deler van a en b.
1 $r_0 \leftarrow a$, $r_1 \leftarrow b$
2 $i \leftarrow 1$
3 **while** $r_i \neq 0$
4 **do** $r_{i+1} \leftarrow \text{rem}(r_{i-1}, r_i)$
5 $i \leftarrow i + 1$
6 **return** r_{i-1}

Voorbeeld 4.10 toont aan dat de bekomen grootste gemene deler kan geschreven worden als een lineaire combinatie van de elementen 126 en 35:

$$7 = 21 - 1 \cdot 14 = 21 - (35 - 1 \cdot 21) = 2 \cdot (126 - 3 \cdot 35) - 35 = 2 \cdot 126 - 7 \cdot 35$$

Dit principe kunnen we onmiddellijk vertalen naar een aanpassing van het algoritme van Euclides. Voor $a, b \in \mathbb{Z}$ noteren we het uniek quotiënt horend bij $\text{rem}(a, b)$ als $\text{quo}(a, b)$. Er geldt dus steeds dat $a = \text{quo}(a, b)b + \text{rem}(a, b)$.

Algoritme 4.2 Uitgebreid algoritme van Euclides

input: $a, b \in \mathbb{Z} \setminus \{0\}$.
output: r, s, t, met $r = \gcd(a, b) = sa + tb$.
1 $r_0 \leftarrow a$, $s_0 \leftarrow 1$, $t_0 \leftarrow 0$.
2 $r_1 \leftarrow b$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$.
3 $i \leftarrow 1$.
4 **while** $r_i \neq 0$
5 **do** $q_i \leftarrow \text{quo}(r_{i-1}, r_i)$
6 $r_{i+1} \leftarrow (r_{i-1} - q_i r_i)$
7 $s_{i+1} \leftarrow (s_{i-1} - q_i s_i)$
8 $t_{i+1} \leftarrow (t_{i-1} - q_i t_i)$
9 $i \leftarrow i + 1$
10 $l \leftarrow i - 1$
11 **return** r_l, s_l, t_l

De volgende stelling toont de correctheid van het uitgebreid algoritme van Euclides aan.

Stelling 4.11

Veronderstel dat a en b gehele getallen zijn (niet beide nul), en dat $d = \text{ggd}(a, b)$, dan bepaalt Algoritme 4.2 gehele getallen m, n zodanig dat $am + bn = d$, tenzij $b \mid a$.

Bewijs. Als $b \mid a$, dan geeft het algoritme b terug. Indien $b < 0$, dan is $-b = \text{ggd}(a, b)$. Het is duidelijk dat $b \mid a \iff r_2 = 0$.

Noem $k > 2$ de kleinste natuurlijke k waarvoor $r_k = 0$. Dan is $r_{k-1} = \text{ggd}(a, b) =: d$. Dus kan de voorlaatste vergelijking herschreven worden als

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-2}.$$

Bijgevolg kan d geschreven worden in de vorm

$$m'r_{k-2} + n'r_{k-3},$$

waarbij $m' = -q_{k-1}$ en $n' = 1$. Indien we nu r_{k-2} substitueren als een lineaire combinatie van r_{k-3} en r_{k-4} dan verkrijgen we

$$d = m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3},$$

hetgeen in de vorm $m''r_{k-3} + n''r_{k-4}$ gebracht kan worden met $m'' = n' - m'q_{k-2}$ en $n'' = m'$. Op die manier zal na opeenvolgende substituties uiteindelijk d in de gewenste vorm gebracht worden. □

De getallen m en n worden ook wel de *Bézout-coëfficiënten* genoemd. Merk op dat deze niet uniek zijn. Stelling 4.11 is vooral belangrijk in het geval $\text{ggd}(a, b) = 1$, aangezien er dan gehele getallen m en n gevonden kunnen worden zodat $ma + nb = 1$. Merk wel op dat de getallen m en n niet noodzakelijk uniek bepaald zijn, immers

$$ma + nb = (m - kb)a + (n + ka)b, \quad \forall k \in \mathbb{Z}.$$

Het (uitgebreid) algoritme van Euclides is wel degelijk efficiënt in de computationele zin. Men kan aantonen dat de complexiteit voor $\mathbb{Z}$ kwadratisch is in de woordlengte van de getallen, hetgeen goed genoeg is om als basisalgoritme te dienen. Het uitgebreid algoritme van Euclides maakt daarenboven

efficiënte modulaire berekeningen mogelijk, hetgeen de hoeksteen is van vele belangrijke algoritmen in de computeralgebra. Elk computeralgebrasysteem bevat dan ook een implementatie van dit algoritme[1]. Meer informatie vindt men in [17, pp. 22–24].

Een aantal elementaire eigenschappen van de grootste gemene deler zijn nuttig in de verdere opbouw. Het bewijs steunt al dan niet op Stelling 4.11.

Gevolg 4.12

Er geldt dat $\text{ggd}(a, b) \mid ax + by$ voor alle $x, y \in \mathbb{Z}$.

Bewijs. Dit volgt onmiddellijk uit Gevolg 4.3 □

Gevolg 4.13

Veronderstel dat $a, b, c \in \mathbb{Z}$, en $\text{ggd}(a, b) = 1$. Dan geldt $a \mid b \cdot c \Longrightarrow a \mid c$.

Bewijs. Uit $a \mid bc$ volgt dat $a \cdot z = bc$, voor een $z \in \mathbb{Z}$. Door Stelling 4.11 en de veronderstelling dat $\text{ggd}(a, b) = 1$ volgt het bestaan van gehele getallen x, y met $ax + by = \text{ggd}(a, b) = 1$. Vermenigvuldigen we beide leden met c, dan zien we onmiddellijk dat $c = cax + cby = a(cx + zy)$, dus $a \mid c$. □

Gevolg 4.14

Veronderstel dat $a \mid m$, $b \mid m$ en $\text{ggd}(a, b) = 1$. Dan geldt $a \cdot b \mid m$.

Bewijs. Uit Stelling 4.11 volgt het bestaan van $x, y \in \mathbb{Z}$ met $ax + by = 1$, dus $max + mby = m$. Uit de veronderstellingen $a \mid m$ en $b \mid m$ volgt ook dat $ab \mid max$ en $ab \mid mby$, dus $ab \mid m$. □

Getallen a en b met $\text{ggd}(a, b) = 1$ noemen we *onderling ondeelbaar*.

Lemma 4.15

Veronderstel dat de gehele getallen a en b onderling ondeelbaar zijn. Dan geldt voor alle $c \in \mathbb{Z}$ dat $\text{ggd}(\text{ggd}(a, c), \text{ggd}(b, c)) = 1$.

[1] Dit algoritme is het oudste niet-triviale algoritme dat nog steeds onvervangbaar is, [11, §4.5.2]

Bewijs. Noem $g = \text{ggd}(a, c)$ en $h = \text{ggd}(b, c)$. Dan geldt $g \mid a$, $g \mid c$ en $h \mid b$ $h \mid c$, dus $\text{ggd}(g, h)$ is een deler van a, b en c. Maar $\text{ggd}(a, b) = 1$, dus $\text{ggd}(g, h) = 1$. □

Lemma 4.16

Als a, b en c natuurlijke getallen zijn, en ac en bc niet beide nul zijn, dan is $\text{ggd}(ca, cb) = c\,\text{ggd}(a, b)$.

Bewijs. Stel $h = \text{ggd}(ca, cb)$ en $g = \text{ggd}(a, b)$. Er geldt dat $g \mid a$ en $g \mid b$, dus $cg \mid ca$ en $cg \mid cb$, dus $cg \mid \text{ggd}(ca, cb)$. Er geldt ook dat $h \mid ca$ en $h \mid cb$, dus $h \mid xca + ycb$ voor willekeurige gehele getallen x en y. Er bestaan welbepaalde gehele getallen m en n waarvoor $\text{ggd}(a, b) = ma + nb$ (Stelling 4.11), dus $h \mid c(ma + nb) = c\,\text{ggd}(a, b)$. We besluiten dat $\text{ggd}(ca, cb) = c\,\text{ggd}(a, b)$. □

Lemma 4.17

Als a, b en c gehele getallen zijn met hetzij a en b, hetzij a en c, hetzij b en c onderling ondeelbaar, dan geldt $\text{ggd}(a, c) \cdot \text{ggd}(b, c) = \text{ggd}(ab, c)$. Bijgevolg zijn ab en c onderling ondeelbaar als en slechts als als zowel a en c als b en c onderling ondeelbaar zijn.

Bewijs. (i) We tonen eerst aan dat $\text{ggd}(ab, c) \mid \text{ggd}(a, c)\,\text{ggd}(b, c)$. Wegens Stelling 4.11 bestaan er gehele getallen r, s, t en u zodat $\text{ggd}(a, c) = ra + sc$ en $\text{ggd}(b, c) = tb + uc$. Dus $\text{ggd}(a, c)\,\text{ggd}(b, c) = rtab + c(stb + rua + suc)$, een lineaire combinatie van ab en c. Door Gevolg 4.12 geldt nu dat $\text{ggd}(ab, c) \mid \text{ggd}(a, c)\,\text{ggd}(b, c)$.

(ii) We veronderstellen nu dat $\text{ggd}(a, b) = 1$. Er geldt dat $\text{ggd}(a, c) \mid \text{ggd}(ab, c)$ en $\text{ggd}(b, c) \mid \text{ggd}(ab, c)$, en $\text{ggd}(\text{ggd}(a, c), \text{ggd}(b, c)) = 1$ door Lemma 4.15. Door Gevolg 4.14 geldt dat $\text{ggd}(a, c)\,\text{ggd}(b, c) \mid \text{ggd}(ab, c)$. Door (i) mogen we nu besluiten dat $\text{ggd}(ab, c) = \text{ggd}(a, c)\,\text{ggd}(b, c)$.

(iii) We veronderstellen nu dat $\text{ggd}(a, c) = 1$. Samen met (i) geldt nu dat $\text{ggd}(ab, c) \mid \text{ggd}(b, c)$. Omdat $\text{ggd}(b, c) \mid \text{ggd}(ab, c)$ volgt nu dat $\text{ggd}(ab, c) = \text{ggd}(b, c)$.

(iv) Volledig analoog als in (iii) leidt de veronderstelling $\text{ggd}(b, c) = 1$ tot $\text{ggd}(ab, c) = \text{ggd}(a, c)$. □

Voor elke 2 gehele getallen a, b noemen we een geheel getal v waarvoor zowel $a \mid v$ als $b \mid v$ een *gemeen veelvoud* van a en b. Volkomen analoog aan de definitie van grootste gemene deler, komen we tot de volgende definitie van kleinste gemeen veelvoud.

Definitie 4.18

Stel $a, b \in \mathbb{Z}$ beide niet nul. Een getal $c \in \mathbb{Z}$ is een *kleinste gemeen veelvoud* van a en b als en slechts als elk gemeen veelvoud van a en b een veelvoud is van c. *Het kleinste gemeen veelvoud* van a en b is het unieke positieve onder de kleinste gemene veelvouden van a en b.

Op vergelijkbare wijze zoals voor de grootste gemene deler, kunnen heel wat eigenschappen van het kleinste gemeen veelvoud bewezen worden.

4.2 Priemgetallen

Definitie 4.19

Een positief geheel getal p wordt een *priemgetal* genoemd als p juist 2 positieve delers bezit (1 en zichzelf).

Met deze definitie is dus 1 geen priemgetal. Elk getal $m \in \mathbb{N} \setminus \{0, 1\}$ dat geen priemgetal is, kan dus geschreven worden als een product $m_1 m_2$ met $m_i \in \{2, \ldots, m-1\}$ (m_1 kan gelijk zijn aan m_2). We noemen daarom elk dergelijk getal m een *samengesteld getal*.

De priemgetallen kleiner dan 50 zijn:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Nochtans is het voor grotere getallen niet altijd zo eenvoudig om snel te bepalen of een getal een priemgetal is. Het probleem om al de priemgetallen kleiner dan een gegeven positief geheel getal op te sommen is een ander probleem.

Merk vooreerst op dat er oneindig veel priemgetallen bestaan. Dit is een stelling die toegeschreven is aan Euclides.

Stelling 4.20 — Euclides

Er zijn oneindig veel priemgetallen.

Bewijs. Veronderstel dat de verzameling van de priemgetallen een eindige verzameling $\{p_1, p_2, \ldots, p_n\}$ zou zijn. Stel $m = \prod_{i=1}^{n} p_i$, dan is $m + 1$ dus geen priemgetal en dus bezit $m + 1$ eigenlijke delers. Noem q de kleinste eigenlijke positieve deler van $m + 1$. Dan is q een priemgetal en dus ook een deler van m. Bijgevolg is q een deler van $(m + 1) - m = 1$. Dit is een tegenstrijdigheid. Bijgevolg is de verzameling van de priemgetallen een oneindige verzameling. □

Priemgetallen spelen een fundamentele rol in de algebraïsche structuur van de gehele getallen. Wij zijn vertrouwd met de idee dat elk natuurlijk getal (verschillend van 0 en 1) geschreven kan worden als een product van priemfactoren, of m.a.w. ontbonden kan worden in priemfactoren, en dat die ontbinding uniek is, op de volgorde van de factoren na. Om de uniciteit van de ontbinding aan te tonen, zullen we gebruik maken van het volgende lemma (en zijn gevolg).

Lemma 4.21

Stel dat p een priemgetal is en dat $p \mid ab$ voor twee gehele getallen $a, b \in \mathbb{Z}$. Dan geldt $p \mid a$ of $p \mid b$.

Bewijs. Veronderstel dat $p \nmid a$. Dan is $\text{ggd}(a, p) = 1$. Uit Gevolg 4.13 volgt dat $p \mid b$. □

Gevolg 4.22

Indien p een priemgetal is en indien $x_1, x_2, \ldots, x_n$ gehele getallen zijn zodanig dat

$$p \Big| \prod_{i=1}^{n} x_i,$$

dan is p een deler van ten minste één x_i ($i \in \{1, \ldots, n\}$).

Bewijs. Door volledige inductie, en met behulp van Lemma 4.21. □

Het *bestaan* van een ontbinding steunt in het bewijs dat we hier geven op het welordeningsprincipe. Het is niet verwonderlijk dat dit ook kan aangetoond worden door volledige inductie.

Stelling 4.23 — Hoofdstelling van de rekenkunde (Euclides)

Elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ is te schrijven als een product van priemfactoren. Op de volgorde na is deze ontbinding uniek.

Bewijs. Noem B de verzameling van de natuurlijke getallen $n \geq 2$ die niet te schrijven zijn als een product van priemfactoren. Veronderstel dat $B \neq \emptyset$, dan bezit B als gevolg van het axioma van de goede ordening een kleinste element m. Aangezien m dan geen priemgetal kan zijn, moet m samengesteld zijn: stel $m = m_1 m_2,\ m_i \in \{2, \ldots, m-1\}$. Aangezien echter m als kleinste element uit B gekozen was, bezitten zowel m_1 als m_2 een ontbinding in priemfactoren. Het product $m = m_1 m_2$ bezit dan echter eveneens een ontbinding in priemfactoren, en dit is tegen de onderstelling dat m tot B behoort. Bijgevolg is B de ledige verzameling.

Veronderstel nu dat voor een natuurlijk getal $n \in \mathbb{N} \setminus \{0, 1\}$ er twee ontbindingen gevonden kunnen worden.

$$\begin{aligned} n &= p_1 \cdot p_2 \cdots p_k \\ &= q_1 \cdot q_2 \cdots q_r \end{aligned}$$

Alle getallen p_i en q_i zijn priemgetallen. Door Gevolg 4.21 geldt $p_1 \mid q_j$ voor een zekere j. We mogen $j = 1$ stellen. Omdat q_1 en p_1 priemgetallen zijn, geldt $p_1 = q_1$. na wegdelen van $p_1 = q_1$ in beide zijden van de vergelijking, blijft er de gelijkheid

$$p_2 \cdots p_k = q_2 \cdots q_r$$

over. We kunnen bovenstaande redenering inductief verder toepasen, en vinden dan dat noodzakelijk $p_i = q_i$ na eventuele wijzigingen van de volgorde, en $k = r$. Hiermee is de uniciteit aangetoond. □

Zoals gezegd is het ook mogelijk om het bestaan van een ontbinding in priemfactoren te bewijzen door volledige inductie. Daartoe gebruiken we als inductiehypothese de volgende uitspraak:

> $A(n)$: elk natuurlijk getal $m \in \mathbb{N}_{<n+1}$ is ofwel een priemgetal ofwel het product van priemgetallen.

Het is nu een eenvoudige oefening om een alternatief bewijs op te stellen.

De zeef van Eratosthenes

Een elementaire manier om alle priemgetallen te vinden die kleiner zijn dan een gegeven getal n staat bekend als de *Zeef van Eratosthenes*. Deze methode gaat als volgt. Het getal 2 is een priemgetal, en al de andere even getallen zijn uiteraard geen priemgetallen. We kunnen ons dus beperken tot de oneven getallen, kleiner dan n. We rangschikken deze getallen van klein naar groot. Het eerste getal in de rij is 3, een priemgetal, maar alle 3-vouden mogen we schrappen. Het volgende getal is het priemgetal 5, de 5-vouden worden geschrapt, daarna komt 7 en worden al de 7-vouden geschrapt. Merk op dat 9 reeds geschrapt was als 3-voud, zodat het volgende priemgetal 11 zal zijn, ... Telkens we een getal tegenkomen dat nog niet geschrapt is, weten we dat het geen eigenlijke delers bezit en dus een priemgetal is. We schrappen telkens de veelvouden van dit getal (sommige van deze getallen kunnen al eerder geschrapt zijn).

Priemelenten in $\mathbb{Z}$

Priemgetallen spelen een essentiële rol in de algebra van de gehele getallen. Desondanks hebben we priemgetallen als natuurlijke getallen gedefinieerd.

Definitie 4.24

Een getal $x \in \mathbb{Z}$ is een *priemelement* als $|x| \in \mathbb{N}$ een priemgetal is.

In Hoofdstuk 5 zullen we zien dat de getallen -1 en 1 een bijzondere rol spelen in $\mathbb{Z}$. De formulering van de hoofdstelling van de rekenkunde in $\mathbb{Z}$ is de volgende stelling.

Stelling 4.25

Elk getal $z \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is te schrijven als het product van priemelementen. Op de volgorde en het teken van deze priemelementen na, is deze ontbinding uniek.

In een cursus algebra zal bovenstaande stelling in nog een abstracter kader herhaald worden.

Aangezien we afgesproken hebben om 1 niet als priemgetal te beschouwen, kunnen we ook zeggen dat $\text{ggd}(a, b) = 1$ betekent dat a en b geen priemfac-

toren gemeen hebben. Daarom worden in dit geval ook a en b *relatief priem*, soms ook wel *copriem* genoemd.

Gevolgen

1. Het aantal positieve delers van een natuurlijk getal n kan op de volgende manier berekend worden. Veronderstel dat de ontbinding van n in priemfactoren er als volgt uitziet:
$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$
Elke deler d van n is dan van de vorm
$$d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}, \quad x_i \in \mathbb{N}_{<e_i+1}, i = 1, \dots, k.$$
Het aantal delers van n is bijgevolg gelijk aan het aantal k-tallen $(x_1, x_2, \dots, x_k)$ met $x_i \in \mathbb{N}_{<e_i+1}$ en is bijgevolg gelijk aan $\prod_{i=1}^{k}(e_i + 1)$.

2. De grootste gemene deler van twee natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i een gemene deler is van a en van b, en waarbij e_i het minimum is van de exponent van p_i in de priemfactorontbindingen van a en b.

3. Het kleinste gemeen veelvoud van 2 natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i ten minste één maal voorkomt in de priemfactorontbinding van a of van b, en waarbij e_i het maximum is van de exponent van p_i in deze priemfactorontbindingen van a en b.

4. Als a en b natuurlijke getallen zijn, niet beide nul, dan is $\text{kgv}(a, b) \cdot \text{ggd}(a, b) = ab$.

Stelling 4.26

Laat n een positief natuurlijk getal zijn, en $a_0, \dots, a_n$ gehele getallen, met $a_0 \neq 0$ en $a_n \neq 0$. Dan geldt voor elke rationale oplossing x_0 van de vergelijking
$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0$$
dat $x_0 = p/q$, voor een zekere p die deler is van a_n, en voor een zekere q die deler is van a_0. In het bijzonder, als $a_0 = 1$, dan zijn de rationale oplossingen ook geheel.

Bewijs. Laten we een rationale oplossing x_0 schrijven als een onvereenvoudigbare breuk, dus $x_0 = p/q,\ \text{ggd}(p,q) = 1$. Dan geldt

$$a_0(p/q)^n + a_1(p/q)^{n-1} + \cdots + a_{n-1}(p/q) + a_n = 0.$$

Vermenigvuldiging met q^n levert

$$a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n = 0.$$

Hieruit volgt dat

$$p(a_0p^{n-1} + a_1p^{n-2}q + \cdots + a_{n-1}q^{n-1}) = -a_nq^n,$$

zodat p een deler is van a_nq^n. Aangezien echter p en q relatief priem zijn, moet p een deler zijn van a_n. Op dezelfde manier bewijzen we dat q een deler is van a_0. □

4.3 Congruenties

Definitie 4.27

Veronderstel dat x_1 en x_2 gehele getallen zijn en dat m een positief natuurlijk getal is. We noemen dan x_1 en x_2 *congruent modulo* m dan en slechts dan als $x_1 - x_2$ deelbaar is door m. We noteren dit als

$$x_1 \equiv x_2 \pmod{m}.$$

Twee gehele getallen zijn congruent modulo m dan en slechts dan als ze dezelfde rest opleveren na deling door m. Met andere woorden x_1 en x_2 zijn congruent modulo m dan en slechts dan als er een geheel getal t bestaat zodanig dat

$$x_1 = x_2 + mt.$$

Het volgende lemma is eenvoudig te bewijzen.

Lemma 4.28

De relatie congruent modulo m is een equivalentierelatie.

Bewijs. Oefening. □

De equivalentieklassen worden *congruentieklassen modulo m* genoemd. We zeggen ook soms dat x_1 en x_2 *equivalent zijn modulo m*. De congruentieklassen modulo m worden daarom ook nog *de restklassen modulo m* genoemd, en de klasse met representant r, wordt soms genoteerd door $[r]_m$ of kortweg door $[r]$ indien er geen verwarring mogelijk is. De verzameling van de restklassen modulo m (met andere woorden de quotiëntverzameling van $\mathbb{Z}$ met betrekking tot de equivalentierelatie congruent modulo m) wordt genoteerd door $\mathbb{Z}/m\mathbb{Z}$. Indien we uit elke restklasse de kleinste natuurlijke representant kiezen, dan ontstaat de verzameling $\mathbb{N}_{<m}$. Er bestaat m.a.w. een bijectie tussen de verzamelingen $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{N}_{<m}$.

Stelling 4.29

Veronderstel dat m een positief natuurlijk getal is en dat x_1, x_2, y_1, y_2 gehele getallen zijn zodanig dat

$$x_1 \equiv x_2 \pmod{m}, \quad y_1 \equiv y_2 \pmod{m}.$$

Dan gelden volgende eigenschappen

1. $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,
2. $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.

Bewijs. 1. Uit het gegeven volgt dat er gehele getallen t en t' bestaan zodanig dat

$$x_1 - x_2 = mt, \qquad y_1 - y_2 = mt'.$$

Bijgevolg geldt

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= mt + mt' \\ &= m(t + t').\end{aligned}$$

Bijgevolg zijn $x_1 + y_1$ en $x_2 + y_2$ congruent modulo m.

2. Merk op dat

$$\begin{aligned}x_1 y_1 - x_2 y_2 &= (x_1 - x_2)y_1 + x_2(y_1 - y_2) \\ &= mty_1 + x_2 mt' \\ &= m(y_1 t + x_2 t').\end{aligned}$$

Bijgevolg zijn x_1y_1 en x_2y_2 congruent modulo m. □

Bovenstaande stelling toont in feite aan dat we over een goed gedefinieerde *optelling en vermenigvuldiging* beschikken in de verzameling $\mathbb{Z}/m\mathbb{Z}$. Merk op dat we optelling en vermenigvuldiging hier zien als een abstracte binaire operatie die aan bepaalde vereisten voldoet. In Hoofdstuk 5 zullen we dieper ingaan op deze vereisten.

We bespreken eerst een kleine toepassing. De *negenproef* is een werkwijze die in de lagere school aangeleerd wordt om na te gaan of een gemaakte vermenigvuldiging al dan niet fout is. Deze werkwijze is gebaseerd op het volgende eenvoudige lemma.

Lemma 4.30

Veronderstel dat $(x_nx_{n-1}\dots x_2x_1x_0)_{10}$ *de voorstelling is van het getal* x *in basis* 10*. Dan geldt*

$$x \equiv \sum_{i=0}^{n} x_i \pmod 9.$$

Bewijs. Uit de definitie van de voorstelling van een getal in basis 10, volgt dat

$$\begin{aligned} x - (\sum_{i=0}^{n} x_i) &= \sum_{i=0}^{n} x_i(10)^i - \sum_{i=0}^{n} x_i \\ &= \sum_{i=1}^{n} ((10)^i - 1)x_i. \end{aligned}$$

Aangezien nu voor elk natuurlijk getal $i \geq 0$ geldt dat $((10)^i - 1)$ deelbaar is door 9, volgt hieruit de gevraagde congruentie. □

Indien we nu kort $\theta(x)$ schrijven voor $\sum_{i=0}^{n} x_i$, dan hebben we dus aangetoond dat $\theta(x) \equiv x \pmod 9$. Bijgevolg geldt wegens stelling 4.29

$$\theta(x)\theta(y) \equiv xy \pmod 9.$$

We hebben eveneens dat

$$\theta(xy) \equiv xy \pmod 9,$$

zodat

$$\theta(xy) \equiv \theta(x)\theta(y) \pmod 9.$$

Dit is de gekende *negenproef* voor de vermenigvuldiging van gehele getallen. B.v. als $x = 12$ en $y = 13$, is $\theta(x) = 3$, $\theta(y) = 4$, $\theta(x)\theta(y) = 12$, $xy = 156$ en $\theta(xy) = 12$. We hebben nu dat $\theta(xy) \equiv \theta(x)\theta(y) \equiv 3 \pmod 9$.

4.4 Optelling en vermenigvuldiging in $\mathbb{Z}/m\mathbb{Z}$

We zullen nu in de verzameling $\mathbb{Z}/m\mathbb{Z}$ een optelling $\oplus$ en een vermenigvuldiging $\otimes$ definiëren.

$$[x]_m \oplus [y]_m = [x + y]_m$$

$$[x]_m \otimes [y]_m = [x \times y]_m.$$

Merk op dat de bewerkingen $+$ en $\times$ de optelling en de vermenigvuldiging zijn van gehele getallen, terwijl $\oplus$ en $\otimes$ bewerkingen definiëren met deelverzamelingen van gehele getallen. Opdat de definitie zinvol zou zijn, moeten we er ons van vergewissen dat deze definitie onafhankelijk is van de keuze van de representanten x en y uit de klassen $[x]_m$ en $[y]_m$. Met andere woorden, als $[x]_m$ en $[x']_m$ dezelfde klasse voorstellen en als $[y]_m$ en $[y']_m$ dezelfde klasse voorstellen, dan moeten ook $[x]_m \oplus [y]_m$ en $[x']_m \oplus [y']_m$ dezelfde klasse voorstellen, analoog moet dit ook gelden voor de vermenigvuldiging. Dat dit wel degelijk het geval is, volgt onmiddellijk uit stelling 4.29.

De eigenschappen die voor de optelling en de vermenigvuldiging van restklassen modulo m gelden, zijn dan ook een onmiddellijk gevolg van de eigenschappen voor de optelling en de vermenigvuldiging van de gehele getallen. We geven hier een kort overzicht.

(A1) $\forall [a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [b]_m \in \mathbb{Z}/m\mathbb{Z}$ en $[a]_m \otimes [b]_m \in \mathbb{Z}/m\mathbb{Z}$.

(A2) $\forall [a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$ en $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$.

(A3) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$: $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$ en $([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$.

(A4) $\forall [a]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [0]_m = [a]_m$ en $[a]_m \otimes [1]_m = [a]_m$.

(A5) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m)$.

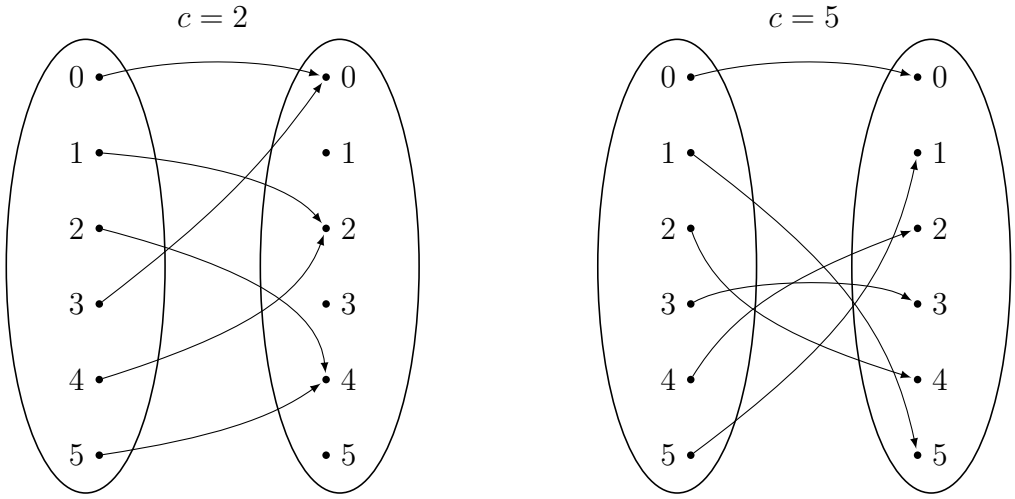
(A6) $\forall [a]_m \in \mathbb{Z}/m\mathbb{Z}, \exists - [a]_m = [-a]_m \in \mathbb{Z}/m\mathbb{Z} : [a]_m \oplus (-[a]_m) = [0]_m$.

Bekijken we de optelling $\oplus$ afzonderlijk, dan is deze inwendig, commutatief, associatief, en bestaat er steeds een neutraal element. Voor de vermenigvuldiging $\otimes$ gelden dezelfde eigenschappen. De optelling heeft echter als extra eigenschap dat er steeds een invers element bestaat. Ten slotte is er nog de distributiviteit van de vermenigvuldiging ten opzichte van de optelling. Deze eigenschappen maken dat $\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes$ een *ring* is. In Hoofdstuk 5 komen we hierop terug.

Merk echter op dat de schrappingswet voor de vermenigvuldiging in $\mathbb{Z}/m\mathbb{Z}$ niet geldt. Zo is bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}$,

$$[3]_6 \otimes [1]_6 = [3]_6 \otimes [5]_6,$$

en alhoewel $[3]_6 \neq [0]_6$ mogen we de klasse $[3]_6$ niet schrappen, want $[1]_6 \neq [5]_6$. Het zelfde geldt voor de $[2]_6$, maar niet voor $[5]_6$. Bekijken we de afbeelding $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $x \mapsto c \cdot x$, voor $c = 2$, en $c = 5$, dan wordt onmiddellijk duidelijk waarom.



Figuur 4.1: De afbeelding f voor $c = 2$ en $c = 5$

We observeren eveneens dat het kan voorkomen dat $[a]_m \otimes [b]_m = [0]_m$ terwijl nochtans $[a]_m \neq [0]_m$ en $[b]_m \neq [0]_m$, dergelijk geval doet zich onder andere

voor indien m een deler is van ab. Zo is bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}$,

$$[2]_6 \otimes [3]_6 = [0]_6 \,,$$

Men zegt daarom dat de klassen $[a]_m$ met a een echte deler van m, *nuldelers* zijn in $\mathbb{Z}/m\mathbb{Z}$. Indien $m = p$ een priemgetal is, dan bezit $\mathbb{Z}/p\mathbb{Z}$ dus geen nuldelers door Lemma 4.21.

Indien er geen verwarring mogelijk is, zullen we in het vervolg de klassen $[r]_m$ meestal voorstellen door een representant $r+tm$ en zullen we voor de optelling van twee klassen in plaats van $[a]_m \oplus [b]_m$, de notatie $a+b \pmod m$ gebruiken. Analoog zal voor de vermenigvuldiging van twee klassen $[a]_m \otimes [b]_m$ de notatie $a \times b \pmod m$ of kortweg $ab \pmod m$ of $a \cdot b \pmod m$gebruikt worden.

Een geheel getal r ($r \neq \pm 1$) bezit geen invers element in $\mathbb{Z}$ voor de vermenigvuldiging. In $\mathbb{Z}/m\mathbb{Z}$ is de situatie enigszins anders. We gaan na wanneer een element van $\mathbb{Z}/m\mathbb{Z}$ een invers element in $\mathbb{Z}/m\mathbb{Z}$ bezit.

Definitie 4.31

Een element $r \in \mathbb{Z}/m\mathbb{Z}$ wordt *inverteerbaar* genoemd als er een element x in $\mathbb{Z}/m\mathbb{Z}$ bestaat, zodanig dat $rx = 1$ in $\mathbb{Z}/m\mathbb{Z}$, met andere woorden indien $rx \equiv 1 \pmod m$. We noteren het *invers element* x van r als r^{-1}.

Stelling 4.32

Een element r in $\mathbb{Z}/m\mathbb{Z}$ is inverteerbaar dan en slechts dan als r en m onderling ondeelbaar zijn. In het bijzonder is in $\mathbb{Z}/p\mathbb{Z}$, p een priemgetal, elk element verschillend van 0 inverteerbaar.

Bewijs. Veronderstel dat r inverteerbaar is, dan bestaat er een geheel getal x, zodanig dat $rx \equiv 1 \pmod m$. Bijgevolg bestaat er een $k \in \mathbb{Z}$ zodanig dat $rx - 1 = km$, of

$$rx - km = 1.$$

Uit Gevolg 4.12 volgt dat $\text{ggd}(r, m) = 1$.

Omgekeerd, veronderstel dat r en m onderling ondeelbaar zijn, dan bestaan er gehele getallen x en y, zodanig dat $rx + my = 1$ (Stelling 4.11), hetgeen gelijkwaardig is met $xr \equiv 1 \pmod m$. □

Stelling 4.33 — Stelling van Wilson

Als p een priemgetal is, dan geldt

$$(p-1)! \equiv -1 \pmod{p}.$$

Bewijs. We merken vooreerst op dat de stelling triviaal voldaan is voor $p = 2$. Veronderstel daarom nu dat p een oneven priemgetal is. We beschouwen de verzameling $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Aangezien p een priemgetal is, zal elk element a van deze verzameling inverteerbaar zijn en het invers element a^{-1} behoort eveneens tot deze verzameling. Bijgevolg kunnen we bij de berekening van $(p-1)!$ modulo p telkens een element a samennemen met zijn invers element a^{-1}, (en $aa^{-1} \equiv 1 \pmod{p}$) op voorwaarde dat $a \not\equiv a^{-1} \pmod{p}$. Maar $a \equiv a^{-1} \pmod{p}$ dan en slechts dan als $(a^2 - 1) \equiv 0 \pmod{p}$, zodat dus p een deler is van $a^2 - 1 = (a+1)(a-1)$. Aangezien p een priemgetal is, volgt hieruit dat p ofwel een deler is van $a - 1$ of van $a + 1$. Aangezien $a \in \{1, \ldots, p-1\}$, volgt hieruit dat ofwel $a = 1$ ofwel $a = p - 1$. Bijgevolg is

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (1)^{\frac{p-3}{2}} \equiv -1 \pmod{p}. \qquad \square$$

4.5 Lineaire congruenties

We beschikken over de bewerkingen $+$ en $\cdot$ in $\mathbb{Z}/m\mathbb{Z}$. Het is dus vanzelfsprekend dat we proberen om vergelijkingen op te lossen in $\mathbb{Z}/m\mathbb{Z}$. We zullen ons beperken tot de lineaire en de kwadratische vergelijkingen.

Een vergelijking van de vorm $ax \equiv b \pmod{m}$ met a en b gegeven gehele getallen, en x een onbekende in $\mathbb{Z}/m\mathbb{Z}$, wordt een *lineaire congruentie* genoemd. Het oplossen van een dergelijke lineaire congruentie is gelijkwaardig met het zoeken naar een koppel $(x, t), x \in \mathbb{N}_{<m}, t \in \mathbb{Z}$, zodanig dat $ax = b + mt$.

Merk op dat $ax \equiv b \pmod{m}$ in feite een verkorte schrijfwijze is voor $[a]_m \otimes [x]_m = [b]_m$. Een oplossing van deze vergelijking tussen congruentieklassen modulo m is dus zelf een congruentieklasse modulo m. We zullen echter ook nu weer spreken van de oplossing r i.p.v. $[r]_m$. Met deze afspraken zijn twee oplossingen r_1 en r_2 van eenzelfde lineaire congruentie verschillend dan en slechts dan als $[r_1]_m \neq [r_2]_m$.

Stelling 4.34

1. Als $d = \text{ggd}(a, m) \nmid b$, dan bezit $ax \equiv b \pmod{m}$ geen oplossing.
2. Als $d = \text{ggd}(a, m) \mid b$, dan bezit $ax \equiv b \pmod{m}$ juist d oplossingen r waarbij $r \in \mathbb{N}_{<m}$.

Bewijs. 1. Veronderstel dat $\text{ggd}(a, m) = d > 1$ geen deler is van b. Indien $r \in \mathbb{N}_{<m}$ een oplossing is van de lineaire congruentie $ax \equiv b \pmod{m}$, dan bestaat er een geheel getal k zodanig dat $ar - b = km$ of dus zodanig dat $ar - km = b$. Hieruit zou volgen dat d een deler is van b. Een tegenstrijdigheid.

2. Veronderstel dat $\text{ggd}(a, m) = 1$, dan is, wegens stelling 4.32, a inverteerbaar in $\mathbb{Z}/m\mathbb{Z}$. Bijgevolg bestaat er een element $a^{-1} \in \mathbb{Z}/m\mathbb{Z}$ zodanig dat $aa^{-1} \equiv 1 \pmod{m}$, zodat $a^{-1}(ax) \equiv (a^{-1}b) \pmod{m}$ of dus $x \equiv (a^{-1}b) \pmod{m}$. Bovendien kan men eenvoudig bewijzen dat elke oplossing van deze vorm is (oefening). Veronderstel nu dat $\text{ggd}(a, m) = d > 1$ en dat $d|b$. We kunnen dan de beide leden van de lineaire congruentie delen door d en we bekomen dan

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \quad \text{ggd}(\frac{a}{d}, \frac{m}{d}) = 1.$$

Deze laatste lineaire congruentie bezit juist één oplossing r in $\mathbb{N}_{<\frac{m}{d}}$. Alle oplossingen van $ax \equiv b \pmod{m}$ zijn bijgevolg van de gedaante $r + t\frac{m}{d}, t \in \mathbb{N}_{<d}$. Er zijn dus juist d oplossingen. □

Opmerkingen

1. Veronderstel dat $\text{ggd}(a, m) = 1$, dan bezit $ax \equiv b \pmod{m}$ juist één oplossing. Wegens het algoritme van Euclides (zie stelling 4.11), weten we dat er gehele getallen r en s bestaan zodanig dat $ar + ms = 1$, en bijgevolg is dan $a(rb) + m(sb) = b$ of $a(rb) \equiv b \pmod{m}$. Hieruit volgt dat $rb \pmod{m}$ een oplossing is van de gegeven lineaire congruentie.

2. In de praktijk kunnen we de oplossing het gemakkelijkst op de volgende manier vinden. We controleren eerst of $d = \text{ggd}(a, m)$ een deler is van b die groter is dan 1. Indien dit het geval is, dan moeten we eerst d wegdelen in de congruentie. Veronderstel dat dit gebeurd is,

dan schrijven we de lineaire congruentie $ax \equiv b \pmod{m}$ in de vorm $ax \equiv (b + tm) \pmod{m}$ met $b + tm$ een veelvoud van a. De oplossing van de lineaire congruentie is dan van de vorm $\frac{b+tm}{a} \pmod{m}$.

Voorbeelden

Zoek de oplossing(en) van de volgende lineaire congruenties.

1. $4x \equiv 1 \pmod{15}$. Dit is gelijkwaardig met $4x \equiv 16 \pmod{15}$ en bijgevolg is $x \equiv 4 \pmod{15}$.

2. $14x \equiv 27 \pmod{31}$. Dit is gelijkwaardig met $14x \equiv 58 \pmod{31}$ en dus met $7x \equiv 29 \pmod{31}$, hetgeen op zijn beurt gelijkwaardig is met $7x \equiv 91 \pmod{31}$, zodat $x \equiv 13 \pmod{31}$.

3. $6x \equiv 15 \pmod{33}$. Aangezien $\text{ggd}(6, 33) = 3$ en 3 een deler is van 15, zijn er 3 oplossingen in $\mathbb{N}_{<33}$. We delen de congruentie door 3, en we zoeken de oplossing van $2x \equiv 5 \pmod{11}$. Dit is gelijkwaardig met $2x \equiv 16 \pmod{11}$ of met $x \equiv 8 \pmod{11}$. Alle oplossingen modulo 33, zijn dus van de gedaante $8 + 11t,\ t \in \{0, 1, 2\}$. Bijgevolg is x congruent met $8, 19, 30$ modulo 33.

Oefening 4.35. *Zoek de oplossingen* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *van* $9x + 16y = 35$.

Oplossing. De vergelijking $9x + 16y = 35$ impliceert dat x en y oplossingen zijn van het stelsel lineaire congruenties

$$\begin{cases} 9x &\equiv 35 \pmod{16} \\ 16y &\equiv 35 \pmod{9}. \end{cases}$$

We lossen één van de congruenties op en substitueren de oplossing dan in de andere lineaire congruentie.

$$\begin{aligned} & 16y \equiv 35 \pmod{9} \\ \iff \quad & 7y \equiv 35 \pmod{9} \\ \iff \quad & y \equiv 5 \pmod{9} \\ \iff \quad & y = 5 + 9t, \quad t \in \mathbb{Z}. \end{aligned}$$

Indien we deze oplossing nu substitueren in de gegeven vergelijking, dan bekomen we $9x + 16(5 + 9t) = 35$ hetgeen impliceert dat $x = -5 - 16t$. ■

Opmerkingen

1. In plaats van de oplossing $y = 5+9t$ van de lineaire congruentie $16y \equiv 35 \pmod 9$ te substitueren in $9x + 16y = 35$ en dan op te lossen naar x, hadden we ook de andere lineaire congruentie $9x \equiv 35 \pmod{16}$ onafhankelijk kunnen oplossen. Deze congruentie heeft als oplossing $x \equiv -5 \pmod{16}$, bijgevolg bestaat $t' \in \mathbb{Z}$ zodanig dat $x = -5 + 16t'$. De substitutie van $y = 5+9t$ en $x = -5+16t'$ in de gegeven vergelijking levert dan $t = -t'$. Deze werkwijze heeft als voordeel dat we de twee lineaire congruenties parallel kunnen uitrekenen.

2. Elke vergelijking $ax + by = c$ in $\mathbb{Z}$ (a, b en c gehele getallen), wordt *een lineaire diophantische vergelijking met 2 onbekenden* genoemd.

4.6 Stelsels lineaire congruenties

We beschouwen nu een stelsel van lineaire congruenties, met andere woorden een stelsel van de gedaante

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k \quad \text{ggd}(a_i, m_i) | b_i.$$

We kunnen er steeds voor zorgen dat de vergelijkingen in dit stelsel van de vorm $x \equiv b_i \pmod{m_i}$ met $b_i \in \mathbb{N}_{<m_i}$ zijn (zie Paragraaf 4.5). We zullen ons daarom beperken tot de stelsels van de vorm

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}_{<m_i}, i = 1, \ldots, k.$$

Voorbeeld

Zoek een oplossing van het volgende stelsel lineaire congruenties

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

Oplossing.

Uit de eerste lineaire congruentie volgt dat $x = 1 + 3k_1$. Indien we dit substitueren in de tweede lineaire congruentie, dan is $1 + 3k_1 \equiv 2 \pmod 5$ hetgeen impliceert dat $3k_1 \equiv 1 \pmod 5$ of dat $k_1 \equiv 2 \pmod 5$. Bijgevolg

is $k_1 = 2 + 5k_2$, zodat $x = 7 + 15k_2$. We substitueren dit nu in de derde lineaire congruentie: $7+15k_2 \equiv 3 \pmod 7$, of dus $15k_2 \equiv -4 \pmod 7$, hetgeen gelijkwaardig is met $15k_2 \equiv 3 \pmod 7$. Hieruit volgt dat $5k_2 \equiv 1 \pmod 7$ of dus $k_2 \equiv 3 \pmod 7$. Elke oplossing x van het stelsel is met andere woorden van de vorm $x = 7 + 15(3 + 7k_3) = 52 + 105k_3$, zodat $x \equiv 52 \pmod{105}$. □

Het zoeken van de oplossing is volgens de bovenstaande methode vrij omslachtig. Het wordt vooral veel rekenwerk indien er meerdere congruenties in het stelsel voorkomen. Merk op dat dit stelsel een unieke oplossing bezit modulo 105, omdat 3, 5 en 7 onderling ondeelbaar zijn. In de volgende stelling zullen we dit algemeen bewijzen. We zullen bovendien een veel sneller algoritme opstellen om dergelijke stelsels van lineaire congruenties op te lossen. De stelling wordt gemeenzaam de *Chinese reststelling* genoemd omdat het voorbeeld van hierboven reeds in een Chinees wiskundeboek uit de 4de eeuw besproken werd.

Stelling 4.36 — Chinese reststelling

Het stelsel lineaire congruenties

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}_{<m_i}, i = 1, \ldots, k$$

met $\text{ggd}(m_i, m_j) = 1$ als $i \neq j$, bezit juist 1 oplossing modulo $M = \prod_{i=1}^{k} m_i$.

Bewijs. We bewijzen de steling door volledige inductie. We veronderstellen eerst dat $k = 2$. Door Stelling 4.11 weten we dat er getallen $s, t \in \mathbb{Z}$ bestaan waarvoor $sm_1 + tm_2 = \text{ggd}(m_1, m_2) = 1$. Definieer

$$x = b_2 s m_1 + b_1 t m_2 \,,$$

dan geldt $x \equiv b_1 t m_2 \pmod{m_1} \equiv b_1 \pmod{m_1}$, want t is net de inverse voor $m_2 \pmod{m_1}$. Analoog geldt $x \equiv b_2 \pmod{m_2}$. We veronderstellen nu dat $k > 2$ en dat de stelling bewezen is voor $2, \ldots, k-1$. Uit de inductiehypothese volgt het bestaan van een getal $y \in \mathbb{Z}$ waarvoor

$$y \equiv b_i \pmod{m_i}, \qquad i = 1, \ldots, k-1.$$

Met dezelfde redenering als in het geval $k = 2$, construeren we nu een $x \in Z$ waarvoor

$$\begin{aligned} x &\equiv y \pmod{m_1 m_2 \ldots m_{k-1}} \\ x &\equiv b_k \pmod{m_k}. \end{aligned}$$

Veronderstel nu dat $x_1, x_2 \in \mathbb{Z}$ twee verschillende oplossingen zijn van het stelsel congruenties. Dan geldt $x_1 \equiv x_2 \pmod{m_i}$, dus $m_i \mid (x_1 - x_2)$ voor $i = 1, \ldots, k$. Omdat $\text{ggd}(m_i, m_j) = 1$ als $i \neq j$ leert Gevolg 4.14 dat $m_1 m_2 \ldots m_k \mid x_1 - x_2$, dus $x_1 \equiv x_2 \pmod{m_1 m_2 \ldots m_k}$. □

Gevolg 4.37

Veronderstel dat $n, m \in \mathbb{N}$ onderling ondeelbaar zijn. Dan is de afbeelding

$$\begin{aligned} \theta : \quad & \mathbb{N}_{<mn} \to \mathbb{N}_{<n} \times \mathbb{N}_{<m} \\ & x \mapsto \theta(x) = (x \pmod{n}, x \pmod{m}) \end{aligned}$$

een bijectie.

Bewijs. De stelling is een rechtstreeks gevolg van Stelling 4.36. □

Het algoritme

We leggen het algoritme eerst uit aan de hand van ons voorbeeld.

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7}. \end{cases}$$

We zoeken een oplossing van de volgende vorm

$$x = 1 \cdot y_1 \cdot (5 \cdot 7) + 2 \cdot y_2 \cdot (3 \cdot 7) + 3 \cdot y_3 \cdot (3 \cdot 5). \tag{4.1}$$

De getallen tussen haakjes achter y_i zijn de producten van al de moduli uitgezonderd de modulus m_i uit de i-de congruentie. De coëfficiënt van y_i is b_i. Indien we nu deze gedaante van x invullen in de achtereenvolgende congruenties, dan ontstaat een stelsel van congruenties in y_i, namelijk:

$$\begin{cases} 35y_1 \equiv 1 \pmod{3} \\ 21y_2 \equiv 1 \pmod{5} \\ 15y_3 \equiv 1 \pmod{7}. \end{cases}$$

Deze drie congruenties kunnen nu elk afzonderlijk opgelost worden, eventueel met het algoritme van Euclides. We vinden hier echter onmiddellijk de

oplossing

$$\begin{cases} y_1 \equiv 2 \pmod 3 \\ y_2 \equiv 1 \pmod 5 \\ y_3 \equiv 1 \pmod 7. \end{cases}$$

Substitueren we de waarden $y_1 = 2, y_2 = 1, y_3 = 1$ in (4.1), dan bekomen we $x = 157$, hetgeen dan modulo $105 = (3 \cdot 5 \cdot 7)$ congruent is met 52.

Algemeen bestaat het algoritme voor het oplossen van het stelsel

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}_{<m_i}, i = 1, \ldots, k$$

erin van een oplossing te zoeken van de vorm

$$x = \sum_{i=1}^{k} b_i m^{(i)} y_i, \qquad \text{met } m^{(i)} = \frac{\prod_{j=1}^{k} m_j}{m_i}.$$

Het stelsel herleidt zich dan tot een stelsel van de vorm

$$1 \equiv y_i m^{(i)} \pmod{m_i}, \quad y_i \in \mathbb{N}_{<m_i}, i = 1, \ldots, k.$$

Elk van deze lineaire congruenties uit het stelsel kan door middel van het algoritme van Euclides opgelost worden. Na substitutie vinden we de waarde van x.

Opmerking

Indien het stelsel slechts uit 2 congruenties bestaat, dan is $x = b_1 m_2 y_1 + b_2 m_1 y_2$.

4.7 Eulers totiëntfunctie

Veronderstel dat n een positief natuurlijk getal is, dan noteren we met $\varphi(n)$ het aantal natuurlijke getallen uit $\{1, \ldots, n\}$ dat copriem is met n; per definitie is $\varphi(1) = 1$. De functie φ wordt de *Eulerfunctie* ook wel *indicator van Euler* of *Eulers totiëntfunctie* genoemd naar Leonhard Euler (1707–1783). Gelet op Stelling 4.32 is $\varphi(n)$ ook gelijk aan het aantal inverteerbare elementen in $\mathbb{Z}/n\mathbb{Z}$.

Indien $n = p$ een priemgetal is, dan is duidelijk

$$\varphi(p) = p - 1.$$

We willen echter een formule voor $\varphi(n)$ voor alle $n \in \mathbb{N} \setminus \{0\}$.

Lemma 4.38

Veronderstel dat de natuurlijke getallen m en n onderling ondeelbaar zijn. Dan is $\varphi(mn) = \varphi(m)\varphi(n)$.

Bewijs. Omdat $\gcd(m, n) = 1$ geldt door Lemma 4.17 geldt dat $\gcd(a, mn) = \gcd(a, m)\gcd(a, n)$. Dus $\gcd(a, mn) = 1 \iff \gcd(a, m) = \gcd(a, n) = 1$.

Beschouw nu een element $a \in \{1, \ldots, mn-1\}$ dat inverteerbaar is modulo mn. Dus $\gcd(a, m) = \gcd(a, n) = 1$. Als $a \equiv r \pmod{m}$, dan volgt uit Lemma 4.9 dat $\gcd(r, m) = 1$, analoog is $\gcd(s, n) = 1$ als $a \equiv s \pmod{n}$. Maar de reductie modulo m en n bepaalt juist de bijectie uit Gevolg 4.37. Dus het aantal elementen in $\{1, \ldots, mn-1\}$ dat inverteerbaar is modulo mn is gelijk aan het aantal koppels $(r, s) \in \{1, \ldots, m-1\} \times \{1, \ldots, n-1\}$ met r en s inverteerbaar modulo m, respectievelijk, modulo n. □

Lemma 4.39

Veronderstel dat p een priemgetal is en $e \geq 1$. Dan geldt $\varphi(p^e) = p^{e-1}(p-1)$.

Bewijs. De verzameling van de veelvouden van p in de verzameling $\{1, \ldots, p^e\}$ is de verzameling $\{c \cdot p : c = 1 \ldots p^{e-1}\}$. Er zijn m.a.w. juist p^{e-1} veelvouden van p, dit zijn de enige getallen in $\{1, \ldots, p^e\}$ die niet onderling ondeelbaar zijn met p^e. Dus $\varphi(p^e) = p^{e-1}(p-1)$. □

Stelling 4.40

Veronderstel dat $n \geq 2$ een natuurlijk getal is met priemfactorontbinding $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. Dan is

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \tag{4.2}$$

$$= p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\ldots p_k^{e_k-1}(p_k-1)\,. \tag{4.3}$$

Bewijs. Voor de priemgetallen p_i in de ontbinding van n geldt uiteraard dat $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$. Inductieve toepassing van Lemma's 4.39 en 4.38 levert het gestelde. □

Opmerking

Van zodra we de priemfactorontbinding van n hebben opgesteld kunnen we vrij vlug $\varphi(n)$ bepalen. Zo is bijvoorbeeld

$$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 2 \cdot 4 = 32$$

en

$$\varphi(1680) = \varphi(2^4 \cdot 3 \cdot 5 \cdot 7) = 2^3 \cdot 2 \cdot 4 \cdot 6 = 384.$$

Stelling 4.41

Voor elk natuurlijk getal n geldt dat $\sum_{d|n} \varphi(d) = n$. Hierbij wordt gesommeerd over alle mogelijke delers van het getal n.

Bewijs. We bewijzen de stelling door middel van inductie. Voor $n = 1$ is de stelling triviaal. Stel dus $n = mp^e$, p een priemgetal, $e \geq 1$, $\text{ggd}(m, p) = 1$, en veronderstel dat de stelling waar is voor $m < n$. Elke deler van mp^e is van de vorm dp^i, $d \mid m$, $1 \leq i \leq e$. Er volgt dus

$$\begin{aligned}
\sum_{d|mp^e} \varphi(d) &= \sum_{d|m} \varphi(d) + \sum_{d|m} \varphi(dp) + \cdots + \sum_{d|m} \varphi(dp^e) \\
&= m + m\varphi(p) + \cdots + m\varphi(p^e) \\
&= m(1 + \varphi(p) + \cdots + \varphi(p^e)) \\
&= m(1 + (p-1) + \cdots + p^{e-1}(p-1)) \\
&= mp^e = n\,.
\end{aligned}$$

De volgende stelling is één van de klassiekers in de elementaire getaltheorie en heeft een groot aantal toepassingen.

Stelling 4.42 — Stelling van Euler

Als $\text{ggd}(y, m) = 1$, dan geldt

$$y^{\varphi(m)} \equiv 1 \pmod{m}.$$

Bewijs. Aangezien $\text{ggd}(y, m) = 1$, is y inverteerbaar in $\mathbb{Z}/m\mathbb{Z}$. Noem U_m de verzameling van de inverteerbare elementen in $\mathbb{Z}/m\mathbb{Z}$, bijgevolg is $y \in U_m$. Definieer

$$yU_m := \{yu_i \pmod m : u_i \in U_m\}.$$

Dan is yU_m gelijk is aan U_m, want het product van twee inverteerbare elementen is terug inverteerbaar, (zodat $yU_m \subseteq U_m$) en elk element u_i van U_m kan geschreven worden als $u_i = y(y^{-1}u_i) \pmod m \in yU_m$, (zodat $U_m \subseteq yU_m$).

We noemen u het product modulo m van alle elementen uit U_m, maw.

$$u \equiv \prod_{i=1}^{\varphi(m)} u_i \pmod m.$$

Aangezien $yU_m = U_m = \{yu_1, yu_2, \ldots, yu_{\varphi(m)}\}$ (modulo m) is

$$u \equiv \prod_{i=1}^{\varphi(m)} u_i \equiv \prod_{i=1}^{\varphi(m)} yu_i \equiv y^{\varphi(m)}u \pmod m.$$

Aangezien u als product van al de inverteerbare elementen in $\mathbb{Z}/m\mathbb{Z}$ eveneens inverteerbaar is, kunnen we de schrappingswet toepassen, zodat $y^{\varphi(m)} \equiv 1 \pmod m$. □

Gevolg 4.43 — Kleine stelling van Fermat

Stel p een priemgetal en $p \nmid y$. Dan is

$$y^{p-1} \equiv 1 \pmod p.$$

Bewijs. Voor een priemgetal p is $\varphi(p) = p - 1$. De uitspraak volgt dus onmiddellijk uit voorgaande stelling. □

Gevolg 4.44

Voor elk positief natuurlijk getal n en elk priemgetal p geldt $n^p \equiv n \pmod p$. Hieruit volgt dat n en n^5 steeds op hetzelfde cijfer eindigen.

Bewijs. Indien $p \nmid n$, dan volgt uit de stelling van Fermat dat $n^{p-1} \equiv 1 \pmod{p}$ en dus dat $n^p \equiv n \pmod{p}$. Anderzijds, indien $p \mid n$, dan zijn zowel n als n^p veelvouden van p.

Indien we nu dit resultaat toepassen in het geval $p = 5$, dan volgt hieruit dat $n^5 - n$ deelbaar is door 5. Anderzijds is $n^5 - n = n(n-1)(n^3+n^2+n+1)$ en dus ook even. Hieruit volgt dat $n^5 - n$ deelbaar is door 5 en door 2, bijgevolg door 10, zodat n en n^5 op hetzelfde cijfer eindigen. □

De combinatie van de stelling van Wilson en de kleine stelling van Fermat tenslotte geeft het volgende resultaat over het al dan niet een kwadraat zijn van $-1 \in \mathbb{Z}/p\mathbb{Z}$, p priem.

Stelling 4.45

Veronderstel dat p een oneven priemgetal is, dan is $-1 \in \mathbb{Z}/p\mathbb{Z}$ een kwadraat als en slechts als als $p \equiv 1 \pmod{4}$.

Tekst

Bewijs. Merk op dat

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\ &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \cdot \left((-\frac{p-1}{2}) \cdot (-\frac{p-3}{2}) \cdots (-1)\right) \pmod{p} \\ &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \cdot (-1)^{\frac{p-1}{2}} \pmod{p}\end{aligned}$$

Deze congruentie is verkregen door van elk van de factoren van $\frac{p+1}{2}$ tot $p-1$ (zo zijn er $\frac{p-1}{2}$) telkens p af te trekken.

Anderzijds is wegens de stelling van Wilson, $(p-1)! \equiv -1 \pmod{p}$. Indien $\frac{p-1}{2}$ even is, bv. $\frac{p-1}{2} = 2k$, zodat $p = 4k+1$, dan is

$$(p-1)! \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \equiv -1 \pmod{p}.$$

Met andere woorden, $a = \left(\frac{p-1}{2}\right)!$ heeft de eigenschap dat $a^2 \equiv -1 \pmod{p}$ als $p \equiv 1 \pmod{4}$.

Als we nu veronderstellen dat $a^2 \equiv -1 \pmod{p}$ dan geldt: $a \neq 0 \pmod{p}$ en omdat p bovendien een priemgetal is, geldt $\text{ggd}(a,p) = 1$. Door de kleine stelling van Fermat is $a^{p-1} \equiv 1 \pmod{p}$ en dan geldt:

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

en dus moet $\frac{p-1}{2}$ even zijn, of nog, $p = 4m+1$ of nog $p \equiv 1 \pmod{4}$. □

4.8 Multiplicatieve functies

Aritmetische functies zijn functies van $\mathbb{N} \setminus \{0\}$ naar $\mathbb{C}$. In geavanceerde getaltheorie spelen ze een belangrijke rol. We beschrijven hier enkele basiseigenschappen.

Definitie 4.46

Een *multiplicatieve functie* is een functie $f : \mathbb{N} \setminus \{0\} \to \mathbb{C}$ waarvoor $f(mn) = f(m)f(n)$ als $\text{ggd}(m, n) = 1$. Een multiplicatieve functie is *totaal multiplicatief* als $f(mn) = f(m)f(n)$ voor alle $m, n \in \mathbb{N}$.

Voorbeeld 4.47.

- De functie $\mathbf{1} : \mathbb{N} \setminus \{0\} \to \mathbb{C}; x \mapsto 1$ en de functie $\mathbf{id} : \mathbb{N} \to \mathbb{C}; x \mapsto x$ zijn totaal multiplicatief.
- Eulers totiëntfunctie is multiplicatief.
- De functie $\epsilon : \mathbb{N} \setminus \{0\} \to \mathbb{C}; \epsilon(1) = 1$ en $\epsilon(x) = 0$ voor alle $x \in \mathbb{N} \setminus \{0, 1\}$ is multiplicatief.

De volgende eigenschap is een elementair gevolg van de hoofdstelling van de rekenkunde.

Lemma 4.48

Een multiplicatieve functie is volledig gekend als haar warden gekend zijn voor alle priemmachten. Twee multplicatieve functies zijn gelijk als ze gelijk zijn voor alle priemmachten.

Het convolutieproduct is in de complexe analyse een integraaltransformatie van het product van twee functies. Er bestaat echter ook een discrete versie van het principe. Het discreet convolutieproduct (en zijn varianten) heeft vergelijkbare eigenschappen en is niet alleen van theoretische belang, maar heeft ook toepassingen in de computationele wiskunde, bijvoorbeeld bij algoritmen om grote gehele getallen op een snelle en efficiënte wijze te vermenigvuldigen.

Definitie 4.49

Het *Dirichlet-convolutieproduct* van twee aritmetische functies f en g is de functie $f * g : \mathbb{N} \setminus \{0\} \to \mathbb{C}$;

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) ,$$

waarbij gesommeerd wordt over de natuurlijke delers van n.

Het Dirichlet-convolutieproduct wordt bruikbaar als we enkele eigenschappen aantonend.

Lemma 4.50

Het Dirichlet-convolutieproduct van twee multiplicatieve functies is een multiplicatieve functie.

Bewijs. Beschouw de getallen $m, n \in \mathbb{N}$ met $\text{ggd}(m, n) = 1$ en veronderstel dat f en g twee multiplicatieve functies zijn. Omdat $\text{ggd}(m, n) = 1$, is een deler van mn ofwel een deler van m ofwel een deler van n. De verzameling van alle delers van mn is dus de verzameling $\{ab \in \mathbb{N} : a \mid m, b \mid n\}$. Nu kunnen we eenvoudig $(f * g)(mn)$ berekenen uit de definitie:

$$\begin{aligned}
(f * g)(mn) = & \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{a|m} \sum_{b|n} f(ab) g\left(\frac{mn}{ab}\right) \\
= & \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right) \\
= & (f * g)(m)(f * g)(n) .
\end{aligned}$$

Lemma 4.51

Het Dirichlet-convolutieproduct is commutatief.

Bewijs. Beschouw een getal $n \in \mathbb{N}$ en de verzameling S van alle delers van n. Dan is het duidelijk dat ook $S = \{\frac{n}{d} : d \mid n\}$. Dus:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = (g * f)(n) .$$

□

Lemma 4.52

Het Dirichlet-convolutieproduct is associatief.

Bewijs. We passen de definitie toe van het Dirichlet-convolutieproduct:

$$\begin{aligned}((f*g)*h)(n) &= \sum_{d|n}(f*g)(d)h\left(\frac{n}{d}\right) = \sum_{d|n}\left(\sum_{e|d}f(e)g\left(\frac{d}{e}\right)\right)h\left(\frac{n}{d}\right)\\ &= \sum_{d|n}\sum_{e|d}f(e)g\left(\frac{d}{e}\right)h\left(\frac{n}{d}\right). \qquad (4.4)\\ (f*(g*h))(n) &= \sum_{d|n}f(d)(g*h)\left(\frac{n}{d}\right) = \sum_{d|n}f(d)\sum_{e|\frac{n}{d}}g(e)h\left(\frac{n}{de}\right)\\ &= \sum_{d|n}\sum_{e|\frac{n}{d}}f(d)g(e)h\left(\frac{n}{de}\right). \qquad (4.5)\end{aligned}$$

Beschouw nu de verzamelingen van tripels $S_1 = \{(d, e, \frac{n}{de}) : d \mid n, e \mid \frac{n}{d}\}$ en $S_2 = \{(e, d, \frac{n}{d}) : d \mid n, e \mid d\}$. Het is eenvoudig in te zien dat zowel S_1 als S_2 beide gelijk zijn aan de verzameling $S = \{(a, b, c) : abc = n\}$. Dus de uitdrukkingen (4.4) en (4.5) zijn gelijk aan elkaar. □

Lemma 4.53

Voor elke multiplicatieve functie f geldt $\epsilon * f = f$.

Bewijs. Het volstaat om de definities toe te passen. □

De *Möbiusfunctie* μ, naar August Ferdinand Möbius (1790–1868), is een functie van $\mathbb{N} \setminus \{0\}$ naar de verzameling $\{-1, 0, +1\}$ die als volgt gedefinieerd wordt:

$$\mu(d) = \begin{cases} 1 & \text{als } d = 1\\ (-1)^r & \text{als } d \text{ een product is van } r \text{ verschillende priemgetallen}\\ 0 & \text{als } d \text{ een meervoudige priemfactor bezit.}\end{cases}$$

Het is duidelijk dat de Möbiusfunctie een multiplicatieve functie is.

Lemma 4.54

Er geldt $\mu * \mathbf{1} = \epsilon$.

Bewijs. Zowel $\mu * \mathbf{1}$ als ϵ zijn multiplicatieve functies (de eerste wegens Lemma 4.50). Het volstaat dus te verifiëren dat beide functies samenvallen voor priemmachten. Nu geldt voor $n \geq 1$ en p een priemgetal, wegens de definities van μ, $\mathbf{1}$ en ϵ, dat $(\mu * \mathbf{1})(p^n) = \sum_{i=0}^{n} \mu(p^i)\mathbf{1}(p^{n-i})) = 1-1+0+\ldots+0 = 0 = \epsilon(p^n)$. Tenslotte geldt ook $(\mu * \mathbf{1})(1) = \epsilon(1) = 1$, wegens de definities. Dit bewijst het lemma. □

Een alternatieve formulering van Stelling 4.41 is als volgt: $\varphi * \mathbf{1} = \mathbf{id}$. Om deze te bewijzen kan men opnieuw de gelijkheid van beide leden op de priemmachten nagaan, en moet dezelfde berekening zoals in het bewijs van Stelling 4.41 gemaakt worden.

Gevolg 4.55

Voor elk natuurlijk getal $n \geq 2$ geldt

$$\sum_{d|n} \mu(d) = 0$$

Bewijs. We gebruiken Lemma 4.54 en vinden voor een natuurlijk getal $n \geq 2$:

$$(\mu * \mathbf{1})(n) = \sum_{d|n} \mu(d)\mathbf{1}\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \epsilon(n) = 0\,.$$

□

Gevolg 4.56

De functies die, respectievelijk, een natuurlijk getal afbeeldt op de som van zijn delers en op het aantal delers, zijn multiplicatief.

Bewijs. De vermelde functies zijn niets anders dan $\mathbf{1} * \mathbf{id}$ en $\mathbf{1} * \mathbf{1}$ respectievelijk. □

Stelling 4.57 — Möbiusinversie

Voor twee aritmetische functies f en g geldt $g = \mu * f \iff f = \mathbf{1} * g$. Indien $g = \mu * f$, dan is bijgevolg g multiplicatief als en slechts als f multiplicatief is.

Bewijs. Stel dat $g = \mu * f$. Dan geldt, gelet op Lemmas 4.52 ,4.52, 4.54 en 4.53:

$$\mathbf{1} * g = (\mathbf{1} * \mu) * f = \epsilon * f = f\,.$$

Stel nu dat $f = \mathbf{1} * g$. Dan geldt, gelet op Lemmas 4.52 , 4.54 en 4.53:

$$\mu * f = \mu * (\mathbf{1} * g) = (\mu * \mathbf{1}) * g = \epsilon * g = g\,. \qquad \square$$

De zogenaamde *Möbius-inversieformule* is niets anders dan een formulering van de Möbiusinversie zonder het Dirichlet-convolutieproduct te gebruiken.

Stelling 4.58 — Möbius-inversieformule

Veronderstel dat g een aritmetische functie is en dat f een functie is die uit g verkregen wordt door de regel:

$$f(n) = \sum_{d|n} g(d).$$

Dan kan g omgekeerd verkregen worden uit f door de regel:

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Gevolg 4.59

Voor alle $n \in \mathbb{N} \setminus \{0\}$ geldt

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}\,.$$

Bewijs. Stelling 4.41 is gelijkwaardig met $\varphi * \mathbf{1} = \mathbf{id}$. Uit de Möbiusinversie (Stelling 4.57) volgt dat $\varphi = \mu * id$, hetgeen net de gestelde formule is. $\square$

4.9 Polynoomcongruenties

Definitie 4.60

Een *veelterm* of *polynoom* over $\mathbb{Z}$ is elke uitdrukking van de gedaante

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

met $a_i \in \mathbb{Z}$.

Hierbij noemt men x een *onbepaalde variabele* en noemt men de elementen $a_i, i \in \mathbb{Z}$, de *coëfficiënten* van de veelterm.

De *graad van een veelterm* is het natuurlijk getal $\max\{i \in \mathbb{N} : a_i \neq 0\}$. De veeltermen van de vorm (a_0) worden *constante veeltermen* genoemd en kunnen geïdentificeerd worden met de elementen van $\mathbb{Z}$. De *nulveelterm* is per definitie de constante veelterm (0) en heeft graad $-\infty$.

Een veelterm f over $\mathbb{Z}$ is dus een $n+1$-tupel van elementen in $\mathbb{Z}$ waarmee een afbeelding van $\mathbb{Z}$ naar $\mathbb{Z}$ geassocieerd kan worden die een element $b \in \mathbb{Z}$ afbeeldt op $f(b)$. De specifieke aard van een veelterm laat echter toe veeltermen op te tellen en te vermenigvuldigen, waarbij we uiteraard opnieuw een veelterm bekomen.

In het vervolg zullen wij soms de veeltermen noteren in dalende volgorde van de exponenten van x:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

De coëfficiënt van $a_n(\neq 0)$ wordt soms de *leidende coëfficiënt* genoemd. Indien $a_n = 1$, dan noemen we de veelterm een *monische veelterm*. Merk op dat indien we de verkorte (rij)notatie gebruiken, we steeds de coëfficiënten in stijgende volgorde van de exponenten zullen schrijven.

Veronderstel dat

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n \quad \text{en} \quad b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_mx^m$$

twee veeltermen zijn over $\mathbb{Z}$ met respectievelijke graad n en m. We zullen deze veeltermen verkort noteren door $a(x)$, respectievelijk $b(x)$. Zonder de algemeenheid te schaden, mogen wij veronderstellen dat $n \geq m$. Indien $n > m$, dan stellen we $b_{m+1} = b_{m+2} = \ldots = b_n = 0$. We kunnen nu de *som*

$a(x) + b(x)$ en het *product* $a(x)b(x)$ van de veeltermen als volgt definiëren.

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots \\ &\qquad \cdots + a_nb_mx^{n+m}. \end{aligned}$$

Met andere woorden, de veelterm $s(x) = a(x)+b(x)$ is de veelterm $(s_0, s_1, \ldots, s_n)$ met

$$s_i = a_i + b_i \quad (0 \leq i \leq n),$$

terwijl $p(x) = a(x)b(x)$ de veelterm $(p_0, p_1, \ldots, p_{n+m})$ is met

$$p_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (0 \leq i \leq n+m) \quad (a_k = 0, \forall k > n; b_k = 0, \forall k > m).$$

Definitie 4.61

Veronderstel dat $m \in \mathbb{Z} \setminus \{0\}$. Twee polynomen $f, g \in \mathbb{Z}[x]$ zijn *congruent modulo* m als m een deler is van alle coëfficiënten van het polynoom $f - g$.

Als $f, g \in \mathbb{Z}[x]$ congruent modulo m zijn, dan noteren we $f \equiv g \mod m$.

Het volgende lemma is vergelijkbaar met Stelling 4.29.

Lemma 4.62

Veronderstel dat $m \in \mathbb{Z}\setminus\{0\}$ en dat $f_1 \equiv f_2 \mod m$ en $g_1 \equiv g_2 \mod m$. Dan geldt

$$\begin{aligned} f_1 + f_2 &\equiv g_1 + g_2 \mod m \\ f_1f_2 &\equiv g_1g_2 \mod m \end{aligned}$$

Bewijs. Oefening. □

Veronderstel dat $f \in \mathbb{Z}[x]$. We noemen een element $b \in \mathbb{Z}$ een *nulpunt* van f als $f(b) = 0$. We noemen een element $a \in \mathbb{Z}$ een *nulpunt modulo* m als $f(a) \equiv 0 \mod m$.

Lemma 4.63

Veronderstel dat $f \in \mathbb{Z}[x]$ een veelterm is van graad $n > 0$ en $a \in \mathbb{Z}$ is een nulpunt modulo m van f. Dan bestaat er een polynoom $f_1 \in \mathbb{Z}[x]$ van graad $n-1$ waarvoor $f \equiv f_1(x-a) \mod m$.

Bewijs. Veronderstel dat $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Definieer $h_1 = a_n x^{n-1}$ en $g_1 = f - h_1(x-a)$. Dan is g_1 een polynoom van graad hoogstens $n-1$ en $g_1(a) \equiv 0 \mod m$, en dus $f = h_1(x-a) + g_1$. Tenzij g_1 een constant polynoom is, kunnen we deze procedure herhalen. Na een eindig aantal stappen vinden we dus $g_m = h_{m+1}(x-a) + g_{m+1}$, met g_{m+1} een constant polynoom waarvoor a een nulpunt modulo m is. Dus $g_{m+1} = b \in \mathbb{Z}$ en $m \mid b$. Stellen we $f_1 = h_1 + \ldots + h_{m+1}$, dan geldt

$$f = f_1(x-a) + b \equiv f_1(x-a) \mod m\,. \qquad \square$$

Als $a \in \mathbb{Z}$ een nulpunt van f modulo m is, dan is elk getal $b \in \mathbb{Z}$ waarvoor $b \equiv a \mod m$ ook een nulpunt van f modulo m. Om dit in te zien hoeven we enkel de aritmetische eigenschappen van $\mathbb{Z}/m\mathbb{Z}$ toe te passen, Stelling 4.29. Het is dus zinvol om van nulpunten in $\mathbb{Z}/m\mathbb{Z}$ te spreken. Het aantal elementen in $\mathbb{Z}/m\mathbb{Z}$ dat een nulpunt is van f modulo m kan groter zijn dan de graad van f. Beschouw als voorbeeld het polynoom $x^2 - 1$ modulo 8. Het is duidelijk dat $1, 3, 5, 7$ nulpunten van f modulo 8 zijn. De volgende stelling geeft duidelijkheid als m priem is.

Stelling 4.64

Veronderstel dat $p \in \mathbb{N}$ priem is en dat $f \in \mathbb{Z}[x]$ een polynoom van graad $n > 0$ is waarvoor geldt dat niet alle coëfficiënten door p deelbaar zijn. Dan heeft f hoogstens n nulpunten modulo p.

Bewijs. Veronderstel dat f $n+1$ verschillende nulpunten $b_1, \ldots, b_{n+1}$ modulo p heeft. Wegens Lemma 4.63 vinden we, rekening houdend met de eerste n nulpunten van f modulo p dat

$$f \equiv c(x-b_1)(x-b_2)\cdots(x-b_n) \mod p\,.$$

Er geldt dus

$$0 \equiv f(b_{n+1}) \equiv c \cdot (b_{n+1}-b_1)\cdots(b_{n+1}-b_n) \mod p\,.$$

Omdat alle b_i verschillend zijn modulo p geldt $(b_{n+1} - b_i) \not\equiv 0 \mod p$, waaruit volgt dat $p \mid c$, hetgeen impliceert dat alle coëfficiënten deelbaar zijn door p, een contradictie. Dus f heeft hoogstens n verschillende nulpunten modulo p. □

4.10 Primitive wortels modulo m

Veronderstel dat $a \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{N} \setminus \{0\}$ en dat $\text{ggd}(a, m) = 1$. De verzameling $T := \{s \in \mathbb{N}^* | a^s \equiv 1 (\text{mod } m)\}$ is niet ledig, want wegens de stelling van Euler (stelling 4.42) is

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Definitie 4.65

De *orde van a modulo m* is het kleinste natuurlijk getal t waarvoor $a^t \equiv 1 \pmod{m}$.

Merk op dat 1 dus altijd de orde 1 heeft.

Voorbeeld

We berekenen de opeenvolgende machten van de $n-1$ elementen uit $\mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, $n \in \{4, 6, 11\}$.

	a^2	a^3
1	1	1
2	0	0
3	1	3

$a^n \pmod 4$

	a^2	a^3	a^4	a^5
1	1	1	1	1
2	4	2	4	2
3	3	3	3	3
4	4	4	4	4
5	1	5	1	5

$a^n \pmod 6$

	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

$a^n \pmod{11}$

- Indien de orde bestaat, dan is ze een deler van $\varphi(n)$.
- De voorwaarde $\text{ggd}(a, m) = 1$ is niet overbodig in de definitie van orde.
- Het is nu ook duidelijk dat alle niet nul elementen modulo p, p priem, een orde hebben.

Stelling 4.66

Veronderstel dat $\text{ggd}(a, m) = 1$ en dat a de orde t bezit modulo m. Dan is $a^n \equiv 1 \pmod{m}$ dan en slechts dan als n een veelvoud is van t.

Bewijs. Veronderstel dat n een veelvoud is van t, stel $n = qt$. Dan geldt dat

$$a^n = a^{qt} = (a^t)^q \equiv 1^q \pmod{m} \equiv 1 \pmod{m}.$$

Veronderstel omgekeerd dat $a^n \equiv 1 \pmod{m}$. Aangezien t de kleinste positieve exponent is waarvoor geldt dat $a^t \equiv 1 \pmod{m}$ moet $n \geq t$. Bijgevolg is $n = qt + r$ met $r \in \mathbb{N}_{<t}$. Hieruit volgt dat

$$a^n \equiv a^{qt+r} \pmod{m}$$

zodat

$$1 \equiv a^r \pmod{m}.$$

Aangezien echter $r \in \mathbb{N}_{<t}$, en t de kleinste positieve exponent was zodanig dat $a^t \equiv 1 \pmod{m}$, volgt hieruit dat $r = 0$, zodat $n = qt$ en dus n een veelvoud is van t. □

Gevolg 4.67

(1) Als $\text{ggd}(a, m) = 1$ en als a de orde t heeft modulo m, dan moet t een deler zijn van $\varphi(m)$.

(2) Als $\text{ggd}(a, m) = 1$ en als a de orde t heeft modulo m, dan geldt

$$a^r \equiv a^s \pmod{m} \Longleftrightarrow r \equiv s \pmod{t}.$$

Bewijs. (1) Onmiddellijk.

(2) Veronderstel dat $r > s$. Dan geldt

$$a^r \equiv a^s \pmod{m} \Longleftrightarrow a^{r-s} \equiv 1 \pmod{m} \Longleftrightarrow r - s \equiv 0 \pmod{t}.$$

□

Voorbeeld

We bekijken nog enkele voorbeelden van ordes van enkele elementen, nu modulo 8 en modulo 9. In de tabellen beperken we ons nu tot elementen a waarvoor $\text{ggd}(a, m) = 1$.

	a^2	a^3	a^4	a^5	a^6	a^7
1	1	1	1	1	1	1
3	1	3	1	3	1	3
5	1	5	1	5	1	5
7	1	7	1	7	1	7

$a^n \pmod 8$

	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
7	4	1	7	4	1	7	4

$a^n \pmod 9$

Voor $m = 4, 6, 9$ en 11 zien we dat er inderdaad minstens één element is dat orde $\varphi(m)$ heeft, terwijl er voor $m = 8$ geen elementen zijn met orde $\varphi(8) = 4$.

Definitie 4.68

Een *primitieve wortel van* m is een element $a \in \mathbb{Z}/m\mathbb{Z}$, $\text{ggd}(a, m) = 1$, en waarvan de orde van a gelijk is aan $\varphi(m)$.

De elementen $2, 6, 7$ en 8 zijn de primitieve wortels van 11. Niet elk natuurlijk getal m bezit primitieve wortels. Zo zijn $1, 3, 5$ en 7 de $\varphi(8) = 4$ getallen die copriem zijn met 8. Maar $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

Stelling 4.69

Als g een primitieve wortel is van m, dan zijn de resten modulo m van $g, g^2, \ldots, g^{\varphi(m)}$ de $\varphi(m)$ natuurlijke getallen uit $\mathbb{N}_{<m}\backslash\{0\}$ die copriem zijn met m.

Bewijs. Aangezien $\text{ggd}(g, m) = 1$, is ook $\text{ggd}(g^k, m) = 1$, $k = 1, \ldots, \varphi(m)$. Bovendien zijn al deze getallen verschillend, want $g^j \equiv g^k \pmod m$ is gelijkwaardig met $j \equiv k \pmod{\varphi(m)}$. □

Voorbeeld

We hebben gezien in een bovenstaand voorbeeld dat $2 \in \mathbb{Z}/9\mathbb{Z}$ een primitieve wortel is. Aangezien $\varphi(9) = 6$ zal de verzameling $\{2, 2^2, 2^3, 2^4, 2^5, 2^6\}$

modulo 9, de verzameling zijn van de getallen die copriem zijn met 9. Deze verzameling is inderdaad gelijk aan $\{2, 4, 8, 7, 5, 1\}$.

Stelling 4.70

Veronderstel dat $\text{ggd}(a, m) = 1$ en dat a de orde t heeft modulo m. Dan zal a^k ook de orde t modulo m hebben als en slechts als $\text{ggd}(k, t) = 1$.

Bewijs. Veronderstel dat $\text{ggd}(k, t) = 1$. We merken op dat $(a^k)^t \equiv (a^t)^k \equiv 1 \pmod{m}$, zodat voor de orde s van a^k geldt dat $s \leq t$. Merk echter op dat $(a^k)^s \equiv 1 \pmod{m} \equiv (a^k)^t$ zodat s een deler is van t. Anderzijds geldt dat $a^{(ks)} \equiv 1 \pmod{m}$ zodat t een deler is van ks. Aangezien echter $\text{ggd}(k, t) = 1$ volgt hieruit dat t een deler is van s. Bijgevolg is $s = t$.

Veronderstel omgekeerd dat a en a^k beide de orde t bezitten en dat $\text{ggd}(k, t) = r$. Dan geldt

$$1 \equiv a^t \equiv (a^t)^{\frac{k}{r}} \equiv (a^k)^{\frac{t}{r}} \pmod{m}.$$

Hieruit volgt dat $r = 1$. □

Voorbeeld

We hebben reeds gezien dat het getal 2 de orde 10 bezit, dus een primitieve wortel is van 11. Hieruit volgt dat 2^k met $\text{ggd}(k, 10) = 1$ eveneens primitieve wortels van 11 zijn. Nu is $\text{ggd}(k, 10) = 1 \iff k = 1, 3, 7, 9$ en $2^3 \equiv 8 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$ en $2^9 \equiv 6 \pmod{11}$, zodat 2, 6, 7 en 8 primitieve wortels zijn van 11. We kunnen ons natuurlijk de vraag stellen of er eventueel nog andere primitieve wortels bestaan van 11. We weten uit de vermenigvuldigingstabel van $\mathbb{Z}/11\mathbb{Z}$ dat dit niet het geval is.

Lemma 4.71

Veronderstel dat p een priemgetal is en dat $d \mid p - 1$. Dan zijn er ofwel geen ofwel juist $\varphi(d)$ verschillende restklassen modulo p van orde d.

Bewijs. Veronderstel dat $a \in \mathbb{Z}/p\mathbb{Z}$ orde d heeft. Dan is a een nulpunt van $f = x^d - 1$ modulo p. Omdat a orde d heeft, zijn de elementen $a, a^2, \ldots, a^d$ allemaal verschillend, en daarenboven zijn dit d verschillende nulpunten van f modulo p. Door Stelling 4.64 zijn dit dus alle d verschillende nulpunten van f modulo p. Omdat elk element van orde d een nulpunt is van f, geldt dus

dat elk element van orde d te schrijven is als a^i, $1 \leq i \leq d$. Uit Stelling 4.70 volgt dat een element a^i orde d heeft als en slechts als $\text{ggd}(i, d) = 1$. Dit bewijst het gestelde. □

Stelling 4.72 — Gauß

Veronderstel dat p een priemgetal is en dat $d \mid p - 1$. Dan zijn er juist $\varphi(d)$ verschillende elementen in $\mathbb{Z}/p\mathbb{Z}$ van orde d. In het bijzonder zijn er dus $\varphi(p - 1)$ primitieve wortels van p.

Bewijs. Noem $A(d)$ het aantal elementen in $\mathbb{Z}/p\mathbb{Z}$ van orde $d \mid p-1$. O mdat p priem is, heeft elk element uit $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ een orde (door de kleine stelling van Fermat). Er geldt dus

$$\sum_{d|p-1} A(d) = p - 1\,.$$

Maar wegens Lemma 4.71 geldt $A(d) \leq \varphi(d)$. Samen met Stelling 4.41 geeft dit

$$\sum_{d|p-1} A(d) \leq \sum_{d|p-1} \varphi(d) = p - 1\,.$$

Noodzakelijkerwijs geldt dus dat $A(d) = \varphi(d)$ voor alle $d \mid p - 1$. Dit bewijst het gestelde. □

Gevolg 4.73

Veronderstel dat a een primitieve wortel van p is. Dan is de verzameling $\{a^i : 1 \leq i \leq p - 1\}$ gelijk aan de verzameling $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, of nog, elk element van $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ kan geschreven worden als a^i, voor een uniek bepaalde macht i, $1 \leq i \leq p - 1$.

Bewijs. Omdat a een primitieve wortel van p is, zijn de elementen $a, a^2, \ldots, a^{p-1}$ alle verschillend. Het gestelde is nu aangetoond omdat $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ juist $p-1$ elementen bevat. □

De discussie over het bestaan van primitieve wortels modulo m, m niet priem, is heel wat ingewikkelder, en valt buiten het bereik van deze cursus. We

vermelden de volgende stelling zonder bewijs. Vergelijk de opgave van de stelling met de bovenstaande observaties over het al dan niet voorkomen van primitieve wortels modulo m, $m \in \{4, 6, 8, 9, 11\}$.

Stelling 4.74

Er bestaat een primitieve wortel modulo m als en slechts als $m = p^k$, of $m = 2p^k$, p een oneven priemgetal, of $m \in \{2, 4\}$.

4.11 Kwadratische congruenties

In deze sectie zullen we steeds veronderstellen dat p een oneven priemgetal is. Een *kwadratische congruentie* in $\mathbb{Z}/p\mathbb{Z}$ is een vergelijking van de vorm

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{4.6}$$

Hierbij zijn a, b en c gehele getallen en is x de onbekende variabele in $\mathbb{Z}_p$. We veronderstellen dat $a \not\equiv 0 \pmod{p}$ (anders hebben we te maken met lineaire congruenties). Aangezien p een priemgetal is, zal $\text{ggd}(a, p) = 1$, zodat a inverteerbaar is in $\mathbb{Z}/p\mathbb{Z}$. Bijgevolg is de kwadratische congruentie (4.6) gelijkwaardig met

$$x^2 + a^{-1}bx + a^{-1}c \equiv 0 \pmod{p}. \tag{4.7}$$

Aangezien p een oneven priemgetal is, geldt dus dat $\text{ggd}(2, p) = 1$, zodat 2 inverteerbaar is in $\mathbb{Z}_p$ (zie Stelling 4.32). Bijgevolg is (4.7) gelijkwaardig met

$$(x + \frac{a^{-1}b}{2})^2 \equiv \frac{b^2 - 4ac}{4a^2} \pmod{p},$$

dus ook met

$$y^2 \equiv \frac{\delta}{4a^2} \pmod{p} \quad \text{met } \delta = b^2 - 4ac \text{ en } y = x + \frac{a^{-1}b}{2}. \tag{4.8}$$

Het bestaan van een oplossing van de kwadratische congruentie (4.6) is dus herleid tot het bepalen van een oplossing van (4.8). Een oplossing hiervan zal dus afhangen van de waarde van δ. Indien $\delta \equiv 0 \pmod{p}$, dan is uiteraard $y \equiv 0 \pmod{p}$ de enige oplossing. Indien $\delta \not\equiv 0 \pmod{p}$, dan zal de oplossing

afhangen van het feit of δ al dan niet een kwadraat is modulo p. We zullen daarom de oplossing bespreken van de kwadratische congruenties van de vorm

$$x^2 \equiv a \pmod{p}.$$

Definitie 4.75

Als $x^2 \equiv a \pmod{p}$ een oplossing bezit, dan wordt *a een kwadratische rest modulo p* genoemd. Als $x^2 \equiv a \pmod{p}$ geen oplossing bezit, dan wordt *a een kwadratische niet-rest modulo p* genoemd.

De volgende stelling beschrijft het aantal oplossingen van een kwadratische congruentie modulo p, p een oneven priemgetal.

Stelling 4.76

Veronderstel dat p een oneven priemgetal is en dat $a \not\equiv 0 \pmod{p}$. Dan bezit $x^2 \equiv a \pmod{p}$ juist 2 of geen oplossingen.

Bewijs. Veronderstel dat r een oplossing is van $x^2 \equiv a \pmod{p}$. Dan is $-r \equiv p - r \pmod{p}$ eveneens een oplossing. Bovendien is $p - r \not\equiv r \pmod{p}$, want anders zou $2r \equiv 0 \pmod{p}$ zodat aangezien $p \nmid r$, $p = 2$, een tegenstrijdigheid aangezien we p oneven ondersteld hebben. Indien er dus een oplossing r is, dan zijn er ten minste 2 oplossingen modulo p. Veronderstel dat s eveneens een oplossing is modulo p van $x^2 \equiv a \pmod{p}$. Dan is $r^2 \equiv s^2 \pmod{p}$ zodat p een deler is van $r^2 - s^2 = (r - s)(r + s)$. Bijgevolg is p een deler van $r - s$ en dus $s \equiv r \pmod{p}$ of is p een deler van $r + s$ en dus $s \equiv p - r \pmod{p}$. Bijgevolg, indien $x^2 \equiv a \pmod{p}$ een oplossing bezit modulo p, dan bestaan er juist 2 oplossingen modulo p. □

Opmerkingen

Deze stelling geldt niet voor elk getal p. Zo heeft de kwadratische congruentie $x^2 \equiv 1 \pmod{8}$ precies 4 oplossingen, met name $x = 1, 3, 5$ en 7.

In het geval van $\mathbb{Z}/11\mathbb{Z}$ hebben we de volgende tabel.

x	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

Er zijn dus 5 kwadratische resten verschillend van 0, die telkens kwadraten modulo 11 zijn van 2 getallen. Dit is een algemene eigenschap die een gevolg is van de voorgaande stelling. De verzameling $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ met p een oneven priemgetal bezit juist $(p-1)/2$ kwadratische resten en juist $(p-1)/2$ kwadratische niet-resten. Merk op dat indien $a \in \mathbb{Z}/p\mathbb{Z}$ en $a \not\equiv 0 \pmod{p}$ dat $a^{\Phi(p)} = a^{p-1} \equiv 1 \pmod{p}$. Bijgevolg is $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Het criterium van Euler maakt van deze eigenschap gebruik.

Stelling 4.77 — Criterium van Euler

Als p een oneven priemgetal is en $p \nmid a$, dan bezit $x^2 \equiv a \pmod{p}$ 2 oplossingen als $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ en geen oplossing als $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Bewijs. Veronderstel dat g een primitieve wortel is modulo p. Dan bestaat er een natuurlijk getal k zodanig dat $g^k \equiv a \pmod{p}$ (Gevolg 4.73). Bijgevolg is dan

$$a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \pmod{p} \equiv (g^{\frac{p-1}{2}})^k \pmod{p}.$$

Aangezien echter g een primitieve wortel is, zal $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hieruit volgt dat

$$a^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}. \tag{4.9}$$

Veronderstel dat k even is, dan volgt uit (4.9) dat $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ en dat $x \equiv g^{\frac{k}{2}} \pmod{p}$ een oplossing is.

Veronderstel dat k oneven is, dan is met andere woorden $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We bewijzen nu dat $x^2 \equiv a \pmod{p}$ geen oplossingen bezit.

Veronderstel dat r een oplossing is. Aangezien p geen deler is van r kunnen we de stelling van Fermat toepassen en zal dus

$$r^{p-1} \equiv 1 \pmod{p}.$$

Anderzijds is echter $r^{p-1} \equiv (r^2)^{\frac{p-1}{2}} \pmod{p} \equiv (a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, een tegenstrijdigheid. Bijgevolg zal in dit geval $x^2 \equiv a \pmod{p}$ geen oplossing bezitten. □

De volgende stelling besluit het bovenstaande.

Stelling 4.78

De kwadratische congruentie $x^2 \equiv a \pmod{p}$ met $\text{ggd}(a,p) = 1$ bezit geen oplossing indien $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ en bezit juist 2 oplossingen indien $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. In dit laatste geval zijn de oplossingen van de gedaante $x \equiv g^m$ en $x \equiv p - g^m \pmod{p}$, met g een primitieve wortel en $a \equiv g^{2m} \pmod{p}$.

Voorbeeld 4.79. We bepalen of 7 een kwadratische rest modulo 31 is. Hiervoor moeten we $7^{15} \pmod{31}$ berekenen. Er geldt achtereenvolgens

$$\begin{array}{lllllll} 7^2 & \equiv & 49 \pmod{31} & \equiv & 18 \pmod{31} & & \\ 7^4 & \equiv & (18)^2 \pmod{31} & \equiv & 324 \pmod{31} & \equiv & 14 \pmod{31} \\ 7^8 & \equiv & (14)^2 \pmod{31} & \equiv & 196 \pmod{31} & \equiv & 10 \pmod{31} \\ 7^{16} & \equiv & (10)^2 \pmod{31} & \equiv & 100 \pmod{31} & \equiv & 7 \pmod{31}. \end{array}$$

Hieruit volgt dat $7^{15} \equiv 1 \pmod{31}$. Zodat 7 een kwadratische rest modulo 31 is. Merk op dat $x^2 \equiv 7 \equiv 100 \equiv (10)^2 \pmod{31}$ is. Bijgevolg zijn $x \equiv 10 \pmod{31}$ en $x \equiv 21 \pmod{31}$ de twee oplossingen van de gegeven kwadratische congruentie.

4.12 Het Legendresymbool

Het criterium van Euler heeft het nadeel dat het niet altijd eenvoudig is om $a^{\frac{p-1}{2}} \pmod{p}$ uit te rekenen. Er bestaat echter een hulpmiddel, namelijk het zogenaamde Legendre symbool dat als volgt gedefinieerd wordt.

$$\left[\frac{a}{p}\right] = \begin{cases} 1 & \text{als } a \text{ een kwadratische rest modulo } p \text{ is.} \\ 0 & \text{als } p \mid a \\ -1 & \text{als } a \text{ een kwadratische niet-rest modulo } p \text{ is} \end{cases}$$

Merk op dat we hier nog altijd veronderstellen dat p een oneven priemgetal is.

Zo zal bijvoorbeeld $\left[\frac{3}{5}\right] = -1$ aangezien $3^2 \equiv -1 \pmod{5}$.

Een aantal eigenschappen zijn kort te bewijzen.

Lemma 4.80

Veronderstel dat g een primitieve wortel modulo p is, p een oneven priemgetal. Dan geldt

$$\left[\frac{g^r}{p}\right] = (-1)^r .$$

Bewijs. We moeten aantonen dat g^r een kwadratische rest modulo p is als en slechts als r even is. Als r even is, dan is $g^r = (g^{\frac{r}{2}})^2$, dus g^r is een kwadratische rest modulo p. Als g^r een kwadratische rest modulo p is, dan is $g^r \equiv h^2 \pmod{p}$. Maar g is een primitieve wortel, dus $h \equiv g^n \pmod{p}$, voor een zekere $n \in \mathbb{N}$. Dus $g^r \equiv g^{2n} \pmod{p}$. Uit Stelling 4.66 volgt dat $p - 1 \mid (r - 2n)$, waaruit volgt dat r even is. □

Stelling 4.81

Het Legendresymbool $\left[\frac{a}{p}\right]$ bezit de volgende eigenschappen.

(1) Als $a \equiv b \pmod{p}$, dan is $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

(2) $\left[\frac{a^2}{p}\right] = \left[\frac{a}{p}\right]^2$.

(3) $\left[\frac{ab}{p}\right] = \left[\frac{a}{p}\right] \cdot \left[\frac{b}{p}\right]$.

Bewijs. Eigenschappen (1) en (2) volgen vrijwel onmiddellijk uit de definitie.

Veronderstel eerst dat $p \mid ab$. Dan geldt $p \mid a$ of $p \mid b$. Dus het rechterlid is nul als en slechts als het linkerlid nul is. Veronderstel nu dat $p \nmid ab$ en noem g een primitieve wortel modulo p. Dan bestaan er natuurlijke getallen r, s met $a \equiv g^r \pmod{p}$ en $b \equiv g^s \pmod{p}$. Uit Lemma 4.80 volgt het gestelde. □

Stelling 4.82 — Kwadratische wederkerigheid

Als p en q oneven priemgetallen zijn, dan is

$$\left[\frac{q}{p}\right] \cdot \left[\frac{p}{q}\right] = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Of gelijkwaardig hiermee:
Als $p \equiv q \equiv 3 \pmod 4$, dan is

$$\left[\frac{p}{q}\right] = -\left[\frac{q}{p}\right].$$

In al de andere gevallen is

$$\left[\frac{p}{q}\right] = \left[\frac{q}{p}\right].$$

Het belang van het Legendresymbool ligt vooral in het feit dat als gevolg van de bovenstaande eigenschappen, de berekeningen soms zeer sterk vereenvoudigd kunnen worden. Er bestaat een elementair (maar nogal lang) bewijs van de kwadratische wederkerigheid. Elementair betekent hier geen diepe kennis vereist is, maar omdat het bewijs te langdradig is laten we het hier weg. Een elementair bewijs kan gevonden worden in [14].

Oefening 4.83. *Ga na of* 85 *een kwadratische rest is modulo* 97*.*

Oplossing. We berekenen

$$\left[\frac{85}{97}\right] = \left[\frac{5 \cdot 17}{97}\right] = \left[\frac{5}{97}\right] \cdot \left[\frac{17}{97}\right].$$

Het vraagstuk is dus herleid tot het berekenen van de twee Legendresymbolen $\left[\frac{5}{97}\right]$ en $\left[\frac{17}{97}\right]$. Aangezien $17 \equiv 97 \equiv 1 \pmod 4$ en rekening houdende met de eigenschappen kunnen we het Legendresymbool $\left[\frac{17}{97}\right]$ als volgt eenvoudig berekenen:

$$\left[\frac{17}{97}\right] = \left[\frac{97}{17}\right] = \left[\frac{12}{17}\right] = \left[\frac{4}{17}\right] \cdot \left[\frac{3}{17}\right] = \left[\frac{3}{17}\right] = \left[\frac{17}{3}\right] = \left[\frac{2}{3}\right].$$

Aangezien $2 \equiv -1 \pmod 3$ volgt hieruit dat $\left[\frac{17}{97}\right] = -1$.

Het andere Legendresymbool is eveneens eenvoudig uit te rekenen:

$$\left[\frac{5}{97}\right] = \left[\frac{97}{5}\right] = \left[\frac{2}{5}\right].$$

Aangezien $2^2 \pmod 5 = -1$ volgt hieruit dat $\left[\frac{5}{97}\right] = -1$. Bijgevolg is

$$\left[\frac{85}{97}\right] = 1,$$

de kwadratische congruentie $x^2 \equiv 85 \pmod{97}$ bezit dus twee oplossingen.

Voor het vinden van de oplossingen zelf is er geen eenvoudige procedure. Aangezien $85 \pmod{97} \equiv 85 + 20 \cdot (97) \pmod{97} \equiv 2025 \pmod{97} \equiv (45)^2 \pmod{97}$ zullen $x \equiv 45 \pmod{97}$ en $x \equiv 52 \pmod{97}$ de twee oplossingen zijn van de gegeven kwadratische congruentie. ■

Opmerking

Men kan bewijzen dat het berekenen van een willekeurig Legendresymbool steeds herleid wordt tot het berekenen van de Legendresymbolen $\left[\frac{-1}{p}\right]$ en $\left[\frac{2}{p}\right]$. Voor deze Legendresymbolen gelden de volgende rekenregels:

1. (zie stelling 4.45)

$$\left[\frac{-1}{p}\right] = +1 \Longleftrightarrow -1 \equiv a^2 \pmod p \Longleftrightarrow p \equiv 1 \pmod 4$$

$$\left[\frac{-1}{p}\right] = -1 \Longleftrightarrow -1 \not\equiv a^2 \pmod p \Longleftrightarrow p \equiv 3 \pmod 4.$$

2.

$$\left[\frac{2}{p}\right] = +1 \Longleftrightarrow p \equiv 1 \pmod 8 \text{ of } p \equiv 7 \pmod 8$$

$$\left[\frac{2}{p}\right] = -1 \Longleftrightarrow p \equiv 3 \pmod 8 \text{ of } p \equiv 5 \pmod 8.$$

Hoofdstuk

5 Algebra

5.1 Binaire bewerkingen

We beginnen met de formalisering van de rekenregels voor de optelling en de vermenigvuldiging in $\mathbb{Z}$ en $\mathbb{Z}/m\mathbb{Z}$ uit Hoofdstuk 4.

Definitie 5.1

Een *(binaire) bewerking* of *operatie* op een verzameling S is een afbeelding van $S \times S$ naar S, dus van de gedaante

$$f : S \times S \to S; (a, b) \mapsto f(a, b)$$

Definitie 5.2

Zij $(S, *)$ een verzameling S met een binaire bewerking $*$.

(A) $(S, *)$ is *associatief* als

$$\forall a, b, c \in S : a * (b * c) = (a * b) * c\,.$$

(C) $(S, *)$ is *commutatief* als

$$\forall a, b \in S : a * b = b * a\,.$$

(N) $(S, *)$ heeft een *eenheidselement* als

$$\exists e \in S : \forall a \in S : a * e = a = e * a\,.$$

(I) $(S, *)$ (met eenheidselement) voldoet aan de *inversieve wet* als

$$\forall a \in S : \exists b \in S : a * b = b * a = e\,.$$

Via deze formalisering willen we een een algemene theorie opbouwen over *ringen* (zoals $\mathbb{Z}$) en *velden* (zoals $\mathbb{Z}/p\mathbb{Z}$, p priem).

Een bewerking op een verzameling is dus een operatie die gegeven twee elementen van S, een nieuw element van S oplevert. We zeggen ook dat de bewerking *intern*, of ook *gesloten* is, waarmee we bedoelen dat de bewerking altijd terug in S uitkomt (en niet in pakweg een grotere verzameling). Zo is de deling $|$ geen interne bewerking op $\mathbb{Z}$.

De vertrouwde optelling en vermenigvuldiging van natuurlijke, gehele, rationale, reële of complexe getallen zijn binaire bewerkingen. Naar analogie zullen we het resultaat van een binaire bewerking $f(a, b)$ vaak noteren met $a+b$, of $a \cdot b$, $a*b$ of kortweg ab. De gekende bewerkingen $+$ en $\cdot$ in de gekende verzamelingen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc. voldoen aan bepaalde eigenschappen. In de algebra staat net de studie van abstracte structuren die aan deze eigenschappen voldoen centraal. Daarom geven we de volgende definitie.

Zonder enige context noteren we een een structuur met een binaire bewerking soms als een koppel (V, f). Voor getallenverzamelingen bijvoorbeeld noteren we de binaire bijwerking op de gebruikelijke wijze. De bewerkingen zelf worden dan ook op de gebruikelijke wijze genoteerd, bv. $1 + 2$ in $\mathbb{Z}$ in plaats van $f(1, 2)$, met f de optelling in $\mathbb{Z}$; of $3 \cdot 4$, of ab, in plaats van $f(2, 3)$ of $f(a, b)$, met f nu de vermenigvuldiging in $\mathbb{Z}$. We noemen algemeen de notatie $a \cdot b$ of ab de multiplicatieve notatie, terwijl we $a + b$ de additieve notatie noemen. Wanneer we spreken over een verzameling G met een bewerking $\cdot$, dan zullen we vaak de multiplicatieve notatie ab gebruiken, $a, b \in G$. Structuren met twee binaire bewerkingen worden dikwijls genoteerd als $S, +, \cdot$. Een van de best gekende voorbeelden is het veld der rationale getallen: $\mathbb{Q}, +, \cdot$

5.2 Groepen

5.2.1 Definitie en voorbeelden

Definitie 5.3

Een *groep* is een koppel $(G, \cdot)$, waarbij G een verzameling is en $\cdot$ een binaire bewerking op G die aan eigenschappen **(A)**, **(N)** en **(I)** (Definitie 5.2) voldoet.

Dus in deze definitie is de notatie $\cdot$ niet relevant, we hadden net zo goed $+$ kunnen gebruiken, of f voor een binaire afbeelding.

Definitie 5.4

Het element e uit voorwaarde **(N)** noemt met het *eenheidselement* voor de bewerking $\cdot$. Het element a^{-1} uit voorwaarde **(I)** noemt men het *invers element van* a.

Indien de additieve notatie gebruikt wordt, dan noteren we het eenheidselement vaak door 0, het invers element vaak door $-a$, en noemen we $-a$ soms ook het *tegengesteld element van* a. Indien de multiplicatieve notatie gebruikt wordt, noteren we het eenheidselement vaak door 1.

Definitie 5.5

Een groep $G, \cdot$ is *abels* of *commutatief* als de binaire bewerking $\cdot$ aan eigenschap **(C)** (Definitie 5.2) voldoet.

Een eerste reeks voorbeelden wordt gegeven door de getallenverzamelingen en één van de standaardbewerkingen.

Voorbeeld 5.6.

- $\mathbb{Z}, +; \mathbb{Q}, +; \mathbb{R}, +; \mathbb{C}, +$ zijn abelse groepen. $\mathbb{N}, +$ is duidelijk **geen** groep.
- $\mathbb{Q}^*, \cdot; \mathbb{R}^*, \cdot; \mathbb{C}^*, \cdot$ zijn abelse groepen. $\mathbb{N}^*, \cdot$ en $\mathbb{Z}^*, \cdot$ zijn duidelijk **geen** groepen. Merk op dat $\mathbb{Q}, \cdot$ eveneens *geen groep* is, omdat 0 geen invers element heeft voor $\cdot$. Analoog uiteraard voor de andere getallenverzamelingen.

Net zoals verzamelingen, kunnen groepen in zekere zin ook door een expliciete omschrijving gegeven worden. Meer bepaald volstaat het om van alle koppels $(a, b) \in G$ het resultaat $f(a, b)$ vast te leggen, met f die binaire bewerking die met G een groep moet worden. Dit kan gebeuren met behulp van een *bewerkingstabel* (ook *Cayley tabel* genaamd). Het volgende voorbeeld maakt dit duidelijk.

Voorbeeld 5.7. Stel $G = \{e, a, b, c\}$. We definiëren een binaire bewerking $\bullet$ in G aan de hand van de volgende *bewerkingstabel* of *Cayley tabel*:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

De axioma's voor een groep kunnen eenvoudig gecontroleerd worden. Deze groep wordt de *viergroep van Klein* genoemd. Deze groep wordt soms genoteerd als V In de praktijk moet slechts een gedeelte van de bewerkingstabel gegeven worden en is de rest een gevolg van de gegeven bewerkingen. Anderzijds is niet elke tabel zomaar een Cayleytabel van een groep.

Voorbeeld 5.8. We hebben in Hoofdstuk 4 de verzamelingen $\mathbb{Z}/m\mathbb{Z}$ ingevoerd, met bijhorende bewerkingen. Deze leveren interessante groepen.

- $\mathbb{Z}/m\mathbb{Z}, \oplus$ is een abelse groep voor alle $m \in \mathbb{N} \setminus \{0\}$.
- $\mathbb{Z}/m\mathbb{Z} \setminus \{0\}, \otimes$ is een abelse groep als en slechts als m een priemgetal is. Dit is het volgende Lemma.

Lemma 5.9

$\mathbb{Z}/m\mathbb{Z} \setminus \{0\}, \otimes$ is een abelse groep als en slechts als m een priemgetal is.

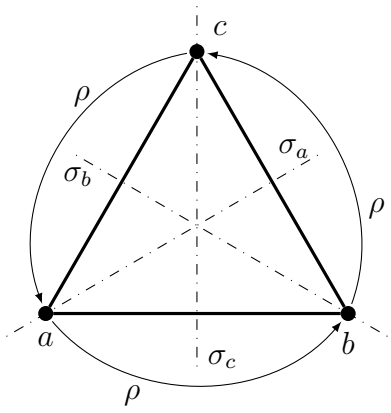
Bewijs. Stel dat m een samengesteld getal is. Dan is $m = ab$, dus $[a]_m \otimes [b]_m = [0]_m$, dus $\otimes$ is geen inwendige binaire bewerking.

Stel dat m een priemgetal is. Door Stelling 4.32 weten we dat voorwaarde **(I)** voldaan is, en dat er geen nuldelers zijn. Dus $\otimes$ is inwendig. De voorwaarden **(A)**, **(C)** en **(N)** zijn duidelijk voldaan. □

Definitie 5.10

De *orde* van een groep is het aantal elementen van de verzameling.

Voorbeeld 5.11. Symmetrieën van (meetkundige) structuren geven doorgaans ook interessante voorbeelden van groepen. Bekijken we in het Euclidisch vlak een gelijkzijdige driehoek abc. Er zijn 6 symmetrieën: 3 spiegelingen σ_a, σ_b en σ_c, rond de respectievelijke hoogtelijnen door a, b en c; twee



Figuur 5.1: Enkele symmetrieën van een gelijkzijdige driehoek

rotaties: ρ en ρ^2, over respectievelijk 120° en 240° (in tegenwijzerzin); en de triviale symmetrie e; zie Figuur 5.11.

Het is eenvoudig om na te gaan dat het product van deze symmetrieën gegeven wordt door de volgende Cayley tabel.

$\circ$	e	ρ	ρ^2	σ_a	σ_b	σ_c
e	e	ρ	ρ^2	σ_a	σ_b	σ_c
ρ	ρ	ρ^2	e	σ_c	σ_a	σ_b
ρ^2	ρ^2	e	ρ	σ_b	σ_c	σ_a
σ_a	σ_a	σ_b	σ_c	e	ρ	ρ^2
σ_b	σ_b	σ_c	σ_a	ρ^2	e	ρ
σ_c	σ_c	σ_a	σ_b	ρ	ρ^2	e

De groep van alle symmetrieën van een regelmatige n hoek wordt genoteerd als D_n of soms ook als D_{2n}. In elk geval heeft een regelmatige n hoek steeds $2n$ symmetrieën. De *diëdergroep* van orde $2n$ is dus de symmetriegroep van een regelmatige $2n$-hoek.

Voorbeeld 5.12. De verzameling van de niet-singuliere $(n \times n)$-matrices over $\mathbb{C}$ vormt een groep voor de matrixvermenigvuldiging. Deze groep wordt meestal genoteerd als $\mathrm{GL}(n, \mathbb{C}), \cdot$ (zie cursus Lineaire algebra en analytische meetkunde).

Als gevolg van de gegeven axioma's voor een groep, kunnen enkele eenvoudige eigenschappen bewezen worden. We vatten deze in de volgende stelling samen.

Stelling 5.13

1. In een groep $G, \cdot$ geldt de linkse en de rechtse schrappingswet; d.w.z. uit $ac = ad$ (resp. $ca = da$) volgt $c = d$.

2. Elke groep $G, \cdot$ heeft slechts één enkel neutraal element e. Elk element a van een groep heeft juist één invers element a^{-1}.

3. In een groep $G, \cdot$ heeft de vergelijking $xa = b$ (resp. $ax = b$) met onbekende x, juist één oplossing voor elke a en b, nl. $x = ba^{-1}$ (resp. $x = a^{-1}b$).

Bewijs. 1. Stel dat er twee elementen e en e' zijn waarvoor $a \cdot e = a \cdot e' = a$ en $e \cdot a = e' \cdot a = a$ voor alle $a \in G$. Maar dan gaat geldt eigenschap ook voor $e, e' \in G$ zelf, dus $ee' = e$ en $ee' = e'$, waaruit $e = e'$. Het neutraal element is dus uniek.

2. Stel dat $a \in G$ twee inverses b en b' heeft. Dan geldt $a \cdot b = e = a \cdot b'$. Links vermenigvuldigen van deze vergelijkingen levert $b = b'$. Dus de inverse van een element is uniek bepaald.

3. Beschouw de vergelijking $xa = b$. Beide leden links vermenigvuldigen met de inverse van a levert $x = ba^{-1}$. Aangezien a^{-1} uniek is, is x uniek bepaald. Dezelfde redenering gaat op voor de vergelijking $ax = b$. □

5.2.2 Deelgroepen

Beschouw een groep $G, \cdot = (G, f)$. Veronderstel dat G' een deelverzameling is van G en dat f' de beperking van f tot $G' \times G'$ is (dus $f' : G' \times G' \to G; (a, b) \longmapsto f'(a, b) = f(a, b) = a \cdot b$). Aangezien f een relatie is van $G \times G$ naar G, kunnen we de notatie $f_{|G' \times G'}$ gebruiken, zoals in Hoofdstuk 2. Omdat er geen verwarring mogelijk is als G' gegeven is, zal de notatie (G', f) impliciet verwijzen naar de beperking van f tot G'.

Definitie 5.14

Veronderstel dat $G, \cdot$ een groep is en $G' \subseteq G$ een deelverzameling van G. Dan is $G', \cdot$ een *deelgroep van* $G, \cdot$, genoteerd $G' \leqslant G$, als en slechts als $G', \cdot$ een groep is.

Met deze definitie is G zelf een deelgroep van G, evenals $\{e\}, \cdot$. Deze laatste groep wordt ook de *triviale deelgroep* genoemd. De deelgroepen van $G, \cdot$ verschillend van de groep G zelf en de triviale deelgroep, worden de *eigenlijke deelgroepen* genoemd.

Voorbeeld 5.15.

1. $\mathbb{Q}, +$ is een deelgroep van $\mathbb{R}, +$ die op zijn beurt eveneens een deelgroep is van $\mathbb{C}, +$. Anderzijds is $\mathbb{Z}, +$ een deelgroep van $\mathbb{Q}, +$ en dus ook van $\mathbb{R}, +$ en van $\mathbb{C}, +$.

2. $\mathbb{Q}^*, \cdot$ is een deelgroep van $\mathbb{R}^*, \cdot$, die op zijn beurt een deelgroep is van $\mathbb{C}^*, \cdot$.

3. De groep $\mathrm{SL}(n, \mathbb{C}), \cdot$ van de $(n \times n)$-matrices met determinant 1 over de complexe getallen, is een deelgroep van $\mathrm{GL}(n, \mathbb{C}), \cdot$.

Voorbeeld 5.16.

1. Beschouw de viergroep van Klein zoals gedefinieerd in Voorbeeld 5.7. De groepen $\{e, a\}, \cdot$ (resp. $\{e, b\}, \cdot$ en $\{e, c\}, \cdot$) zijn deelgroepen van de viergroep van Klein, terwijl $\{e, a, b\}, \cdot$ geen deelgroep van de viergroep van Klein is.

2. De groep $\{e = \rho^3, \rho, \rho^2\}, \circ$ is een deelgroep van D_6, die enkel de rotaties bevat. De orde van de deelgroep is 3.

Stelling 5.17 — Criterium voor deelgroepen

Veronderstel dat $G, \cdot$ een groep is en dat G' een niet ledige deelverzameling is van G. Dan is $G', \cdot$ een deelgroep van $G, \cdot$ als en slechts als $ab^{-1} \in G'$ voor alle $a, b \in G'$.

Bewijs. Als $G', \cdot$ een deelgroep is, dan is de voorwaarde waar. Veronderstel nu omgekeerd dat de voorwaarde waar is. Veronderstel dat $a, b \in G'$. Omdat de voorwaarde waar is, geldt $e = aa^{-1} \in G'$. Dus is ook $a^{-1} \in G'$. Hetzelfde geldt voor b, dus ook $b^{-1} \in G'$. Daaruit volgt tenslotte dat $ab = a(b^{-1})^{-1} \in G'$. Dus $G', \cdot$ is een deelgroep. □

Lemma 5.18

De doorsnede van twee deelgroepen $G', \cdot$ en $G'', \cdot$ van een groep $G, \cdot$ is terug een deelgroep van $G, \cdot$

Bewijs. Dit volgt onmiddellijk uit Stelling 5.17 □

De unie van $G', \cdot$ en $G'', \cdot$ is in het algemeen geen deelgroep van $G, \cdot$.

Opmerking

De associativiteitswet is in principe voor een willekeurige groep het moeilijkst te controleren omdat hier telkens de bewerking tussen 3 willekeurige elementen berekend moet worden. Dergelijke berekening is niet onmiddellijk uit bv. de Cayley tabel van de groep af te lezen, dit in tegenstelling tot de identiteitswet en de inversieve wet. Indien echter deze associativiteitswet geldt voor de groep G, dan geldt die automatisch ook voor elke deelgroep. Merk op dat het eenheidselement van de groep G automatisch ook het eenheidselement van elke deelgroep is. De voorwaarde uit Stellingn 5.17 is wel heel eenvoudig te controleren. Het is dan ook meestal nuttig, indien men wil nagaan of een structuur een groep is, te bewijzen dat de structuur een deelgroep is van een gekende groep aan de hand van de voorwaarde uit Stelling 5.17.

Definitie 5.19

Als $H, \cdot$ een deelgroep is van een groep $G, \cdot$ en $a \in G$, dan worden de verzamelingen $aH = \{ah \| h \in H\}$ en $Ha = \{ha \| h \in H\}$ respectievelijk *linkse* en *rechtse nevenklassen* van H in G genoemd.

Voorbeeld 5.20. De verzameling van de oneven gehele getallen is een nevenklasse van de additieve deelgroep van de even gehele getallen in $\mathbb{Z}, +$.

Stelling 5.21

De linkse (resp. rechtse) nevenklassen van een deelgroep H van G vormen een partitie van G.

Bewijs. Voor elke $x \in G$ is $x \in xH$. Bijgevolg is geen enkele (linkse) nevenklasse ledig en bovendien is de unie van alle nevenklassen de ganse groep G.

Veronderstel nu dat $xH \cap yH \neq \emptyset \ \ (x \neq y)$. Dan bestaat er een $z \in G$ zodanig dat $z \in xH \cap yH$. Dit betekent dat er elementen $h_1 \in H$ en $h_2 \in H$ bestaan, zodanig dat $z = xh_1 = yh_2$. Hieruit volgt dat $x = yh_2h_1^{-1}$, of dat $x \in yH$, hetgeen impliceert dat $xH \subseteq yH$. Volledig analoog kunnen we bewijzen dat $yH \subseteq xH$, bijgevolg is $xH = yH$. □

Stelling 5.22 — Stelling van Lagrange

Als H een deelgroep is van een eindige groep G, dan is de orde van H een deler van de orde van G.

Bewijs. De afbeelding $f_x : H \to xH,\ h \longmapsto xh$ is een bijectie. Bijgevolg is $|H| = |xH|,\ \forall x \in G$. Aangezien de (linkse) nevenklassen een partitie vormen van G, is $|G| = k|H|$, met k het aantal nevenklassen van H. □

Definitie 5.23

Stel dat $H \leqslant G$. Het getal $\dfrac{|G|}{|H|}$ noemt men de *index van H in G* en wordt ook genoteerd als $[G : H]$.

5.2.3 Groepmorfismen

Definitie 5.24

Beschouw twee groepen $G, \cdot$ en $G', \times$. Een *(homo)morfisme* van $G, \cdot$ in $G', \times$ is een afbeelding θ van G in G' zodanig dat $\theta(a.b) = \theta(a) \times \theta(b),\ \forall a, b \in G$.

Is het (homo)morfisme θ injectief, dan noemen we θ een *monomorfisme*. Is het surjectief, dan spreken we van een *epimorfisme*. Is θ bijectief, dan spreken

we van een *isomorfisme*. Een isomorfisme van $G, \cdot$ op $G, \cdot$ noemen we een *automorfisme* van $G, \cdot$.

Voorbeeld 5.25.

1. $\theta : \mathbb{Z} \to \mathbb{Q}, a \longmapsto a$ is een monomorfisme van $\mathbb{Z}, +$ in $\mathbb{Q}, +$.
2. $\theta : \mathbb{Z} \to \mathbb{Z}, a \longmapsto na \quad (n \in \mathbb{Z} \setminus \{0\})$ is een monomorfisme van $\mathbb{Z}, +$ in zichzelf.
3. Beschouw de viergroep van Klein. Stel $\theta(e) = e, \theta(a) = b, \theta(b) = a$ en $\theta(c) = c$. Dan is θ een automorfisme van de viergroep van Klein.
4. Beschouw de groepen $\mathbb{Z}, +$ en $\{-1, 1\}, \cdot$. Definieer θ als volgt:

$$\begin{cases} \theta(a) = 1 & \text{als } a \text{ even is} \\ \theta(a) = -1 & \text{als } a \text{ oneven is.} \end{cases}$$

   Dan is θ een epimorfisme van $\mathbb{Z}, +$ op $\{-1, 1\}, \cdot$
5. De groep $\mathbb{Z}/4\mathbb{Z}, \oplus$ is isomorf met de groep $\{e, a, b, c\}, \cdot$ waarbij de bewerking $\cdot$ door middel van de volgende Cayley tabel gedefinieerd wordt.

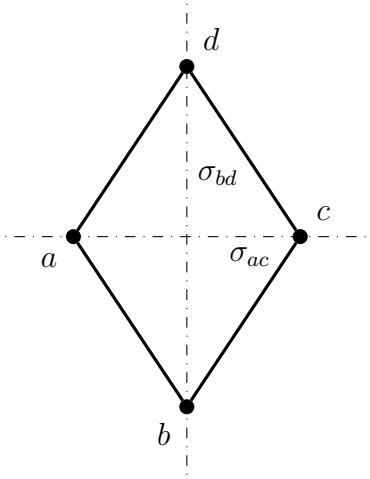
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

   Uit deze tabel wordt duidelijk dat $\mathbb{Z}/4\mathbb{Z}, \oplus$ niet isomorf is met de viergroep van Klein.
6. $\theta : \mathbb{Z} \to \mathbb{Z}, a \longmapsto -a$ is een automorfisme van $\mathbb{Z}, +$.

Stelling 5.26

Als θ een homomorfisme van $G, \cdot$ in $G', \times$ is, dan is $\theta(e)$ het neutraal element van $G', \times$ en dan is $\theta(a^{-1})$ het invers element van $\theta(a)$ in $G', \times$.

Bewijs. (i) Voor elk element $a \in G$ geldt $\theta(a) = \theta(e \cdot a) = \theta(e) \times \theta(a) = \theta(a)$, $\theta(e)$ is dus het neutraal element voor $\theta(a) \in G'$. Maar door Stelling 5.13 weten we dat het neutraal element uniek is.



Figuur 5.2: Enkele symmetrieën van een ruit

(ii) Kies een willekeurige $a \in G$ en beschouw $\theta(a) \in G'$. Stel $b := (\theta(a)^{-1})$. Dan geldt $\theta(e) = \theta(a \cdot a^{-1}) = \theta(a) \times \theta(a^{-1})$, maar ook $\theta(a) \times b = \theta(e)$. Opnieuw door Stelling 5.13 vinden we dat $b = \theta(a^{-1})$. □

Voorbeeld 5.27. Een ruit *abcd* heeft drie niet triviale symmetrieën: twee spiegelingen ten opzichte van de assen *ac* en *bd*, genoteerd respectievelijk σ_{ac} en σ_{bd}, en een puntspiegeling, genoteerd ϱ, zie Figuur 5.2.3. Het is duidelijk dat $\varrho = \sigma_{ac} \circ \sigma_{bd} = \sigma_{bd} \circ \sigma_{ac}$. Doordat alle spiegelingen orde 2 hebben, kunnen we onmiddelijk de Cayleytabel opstellen. Noteer $G := \{e, \sigma_{ac}, \sigma_{bd}, \varrho\}$.

$\circ$	e	σ_{ac}	σ_{bd}	ϱ
e	e	σ_{ac}	σ_{bd}	ϱ
σ_{ac}	σ_{ac}	e	ϱ	σ_{bd}
σ_{bd}	σ_{bd}	ϱ	e	σ_{ac}
ϱ	ϱ	σ_{bd}	σ_{ac}	e

Het is duidelijk dat de afbeelding $\theta : G \to V$, $\theta(e) = e$, $\theta(\sigma_{ac}) = a$, $\theta(\sigma_{bd}) = b$, en $\theta(\varrho) = c$ een isomorfisme is tussen $G, \circ$ en $V, \cdot$.

Homorfismen kunnen interessante deelgroepen opleveren.

Definitie 5.28

Stel dat θ een homomorfisme is van $G, \cdot$ in $G', \times$. Het *beeld van* θ, genoteerd $\mathrm{im}(\theta)$, is de verzamling $\{\theta(x) : x \in G\}$. De *kern van* θ, genoteerd $\ker(\theta)$, is de verzameling $\{x \in G : \theta(x) = e'\}$ (het eenheidselement in G').

Stelling 5.29

Onderstel dat θ een homomorfisme is van $G, \cdot$ in $G', \times$. Dan is $\text{im}(\theta) \leqslant G'$ en $\ker(\theta) \leqslant G$.

Bewijs. We gebruiken Stelling 5.17 om na te gaan dat $\ker(\theta) \leqslant G$ en $\text{im}(\theta) \leqslant G'$.

Stel $a = \theta(x)$, $b = \theta(y)$ en $a, b \in G'$. Dan geldt $a \times b^{-1} = \theta(x) \times \theta(y)^{-1} = \theta(x) \times \theta(y^{-1}) = \theta(x \cdot y^{-1}) \in G'$. Dus $\text{im}(\theta) \leqslant G'$.

Stel $x, y \in \ker(\theta)$. Dan is $\theta(x \cdot y^{-1}) = \theta(x) \times \theta(y)^{-1} = e'^{-1} = e'$, dus $x \cdot y^{-1} \in \ker(\theta)$. □

We hernemen Voorbeeld 5.25

Voorbeeld 5.30.

1. $\theta : \mathbb{Z}, + \to \mathbb{Q}, +, a \longmapsto a$: $\ker(\theta) = \{0\}$, $\text{im}(\theta) = \mathbb{Z}$.
2. $\theta : \mathbb{Z}, + \to \mathbb{Z}, +, a \longmapsto na \quad (n \in \mathbb{Z} \setminus \{0\})$: $\ker(\theta) = \{0\}$, $\text{im}(\theta) = \{nxlx \in \mathbb{Z}\}$, dus de veelvouden van n.
3. Beschouw de viergroep van Klein. Stel $\theta(e) = e, \theta(a) = b, \theta(b) = a$ en $\theta(c) = c$. Dan is θ een automorfisme van de viergroep van Klein. Noodzakelijkerwijs is $\ker(\theta) = \{e\}$.
4. Beschouw de groepen $\mathbb{Z}, +$ en $\{-1, 1\}, \cdot$. Definieer θ als volgt:

$$\begin{cases} \theta(a) = 1 & \text{als } a \text{ even is} \\ \theta(a) = -1 & \text{als } a \text{ oneven is.} \end{cases}$$

   Dan is θ een epimorfisme van $\mathbb{Z}, +$ op $\{-1, 1\}, \cdot$ en $\ker(\theta) = \{2x \| x \in \mathbb{Z}\}$.

De volgende stelling zal van toepassing zijn in de studie van eindige velden.

Stelling 5.31

Stel G is een eindige groep en $A \subset G$, $B \subset G$ en $|A| + |B| \geq G$. Dan geldt $G = AB$, i.e. voor element $g \in G$ bestaan er elementen $a \in A$ en $b \in B$ zodanig dat $g = ab$.

Bewijs. Kies een element $g \in G$ en beschouw de verzameling $B_g := \{gb^{-1} : b \in B\}$. Het is duidelijk dat $|B_g| = |B|$. Aangezien $|A \cap B_g| = |A| + |B_g| - |A \cup B_g|$ (het inclusie-exclusieprincipe, zie pagina 108), is $|A \cap B_g| > 0$, want $|A| + |B_g| > |G|$, en $|A \cup B_g| \leq |G|$. Dus er bestaat een element $a \in A \cap B_g$, dus er bestaat een element $b \in B$ waarvoor $a = gb^{-1}$, of nog, $g = ab$. □

5.2.4 Cyclische groepen

Definitie 5.32

Stel dat $G, \cdot$ een groep is en dat $D \subseteq G$. Kan elk element van G geschreven worden als het product van elementen en hun inverses uit D, dan noemen we de elementen van D de *generatoren* of *voortbrengers* van G.

Als D een verzameling generatoren is voor G, dan noteren we soms $G = \langle D \rangle$, of ook nog $G = \langle x_1, \ldots, x_r \rangle$ als $D = \{x_1, \ldots, x_r\}$.

Definitie 5.33

Een groep G wordt een *cyclische groep* genoemd als G voortgebracht wordt door één element.

Als G een cyclische groep is, dan bestaat er dus een $x \in G$ waarvoor $G = \langle x \rangle$. We zeggen dat x een *voortbrengend element* is van de groep G. Uit de definitie van generatoren van een groep volgt dat machten met negatieve exponenten of exponent gelijk aan 0 toegelaten zijn: $x^0 := 1$ en $x^{-n} := (x^{-1})^n$, $n \in \mathbb{N} \setminus \{0\}$.

Indien er een $m \in \mathbb{N} \setminus \{0\}$ bestaat zodanig dat $x^m = e$, het eenheidselement van de groep, en indien m het kleinste positief natuurlijk getal is met deze eigenschap, dan zal voor elk natuurlijk getal $k > m$ gelden dat $k = mq + r$ met $r \in \mathbb{N}[0, m-1]$, zodat $x^k = x^{mq+r} = x^r$. Bijgevolg bezit de cyclische groep voortgebracht door x in dit geval juist m elementen en is dus met andere woorden een groep van de orde m, meer nog

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{m-1}\}.$$

Indien er echter geen dergelijk natuurlijk getal m bestaat, dan is $\langle x \rangle$ een oneindige groep. Deze groep wordt soms genoteerd als C_∞.

Gebruiken we de additieve notatie dan is een groep G een *cyclische groep* als en slechts als het een element x bevat, zodanig elk element van G geschreven kan worden als een veelvoud van x. Dit is uiteraard niet in tegenspraak met Definitie 5.33, want het product in deze definitie slaat op de samenstelling van elementen, hetgeen in de additieve notatie de optelling is. In de additieve notatie is elk element van G dus te schrijven als $n \cdot x := \underbrace{x + x + \cdots + x}_{n \text{ keer}}$, $n \in \mathbb{N} \setminus \{0\}$, waarbij ook de veelvouden $0 \cdot x := 0$ en de veelvouden $(-n) \cdot x := n \cdot (-x)$ toegelaten worden. Zo brengt het element 1 in $\mathbb{Z}$ de volledige groep $\mathbb{Z}, +$ voort.

Veronderstel dat G een willekeurige groep is. Als x een element is van deze groep, dan brengt x een cyclische groep voort die een deelgroep is van G. De orde van $\langle x \rangle$ wordt de orde van het element x genoemd. Uit stelling 5.22 volgt dat de orde van een element van een groep steeds een deler is van de orde van de groep.

Stelling 5.34

Elke eindige cyclische groep van de orde m is isomorf met $\mathbb{Z}/m\mathbb{Z}, \oplus$. Elke oneindige cyclische groep is isomorf met $\mathbb{Z}, +$.

Bewijs. Veronderstel dat de cyclische groep G voortgebracht wordt door g. Dan geldt

$$g^r = g^s \Longleftrightarrow g^{r-s} = e.$$

Hierbij zijn r en s gehele getallen en is e het eenheidselement van de groep G. Als G een oneindige cyclische groep is, dan is $g^{r-s} \neq e$ voor $r \neq s$. Bijgevolg is $g^r \neq g^s$ voor $r \neq s$. Aangezien nu $g^r g^s = g^{r+s}$ volgt hieruit dat de afbeelding θ

$$\theta : G \to \mathbb{Z}; g^s \longmapsto s$$

een isomorfisme is van de oneindige cyclische groep G op de groep $\mathbb{Z}, +$.

Veronderstel nu dat G een eindige cyclische groep is van de orde m. Dan is de groep $G = \{g, g^2, \ldots, g^{m-1}, g^m = e\}$. Bovendien is voor elke $s > m$, $s = mq + r$, zodat $g^s = g^r$. Met andere woorden $g^r = g^s$ dan en slechts dan als $r \equiv s \,(\text{mod } m)$. De afbeelding θ

$$\theta : G \to \mathbb{Z}/m\mathbb{Z}; g^s \longmapsto [s]_m$$

is bijgevolg een isomorfisme van de eindige cyclische groep G van de orde m op de groep $\mathbb{Z}/m\mathbb{Z}, \oplus$. □

Gevolg 5.35

Elke twee cyclische groepen van dezelfde orde zijn isomorf.

Alhoewel we voor een cyclische groep van de orde m mogen denken aan de groep $\mathbb{Z}/m\mathbb{Z}, \oplus$, zullen we meestal de notatie C_m gebruiken omdat we gewoonlijk de bewerking multiplicatief en niet additief zullen noteren.

Stelling 5.36

Elke eindige groep G waarvan de orde een priemgetal is, is een cyclische groep.

Bewijs. Beschouw een element $g \neq 1$ van de groep en beschouw de cyclische groep $\langle g \rangle$ voortgebracht door g. De orde van g is dan een deler van $|G| = p$, en dus gelijk aan p. Bijgevolg is $G = \langle g \rangle$. □

Stelling 5.37

Er bestaan op een isomorfisme na juist 2 groepen van de orde 4.

Bewijs. Veronderstel dat $G = \{1, a, b, c\}$. De orde van a is ofwel 2 ofwel 4. Als a de orde 4 heeft, dan is $G = \langle a \rangle$, m.a.w. G is cyclisch en $b = a^2$ en $c = a^3$ (b heeft dan de orde 2 en c heeft de orde 4) of omgekeerd. Veronderstel nu dat a, b en c van de orde 2 zijn, m.a.w. $a^2 = b^2 = c^2 = 1$. Dan moet $ab = c$. Inderdaad, uit $ab = 1$ zou volgen dat $a^2b = a$ en dus dat $b = a$; uit $ab = a$ zou volgen dat $b = 1$; en tenslotte uit $ab = b$ zou volgen dat $a = 1$. Op dezelfde manier bewijzen we dat $ba = c, ac = ca = b, bc = cb = a$. Hieruit volgt dat G de viergroep van Klein is. □

Stelling 5.38

Een cyclische groep $C_n = \langle g \rangle$ van de orde n bezit voor elke deler d van n juist één deelgroep van de orde d, bovendien is deze deelgroep een cyclische groep voortgebracht door g^k met $n = kd$.

Bewijs. Wegens de stelling van Lagrange is de orde d van een willekeurige deelgroep H van de cyclische groep $C_n = \langle g \rangle$ een deler van n. Elk element h van H heeft de eigenschap dat $h^d = 1$. We hebben in stelling 5.39 gezien dat er juist d elementen van C_n deze eigenschap hebben, namelijk de elementen $1, g^k, \ldots, g^{(d-1)k}$, met $dk = n$. Bijgevolg moet H juist deze elementen bevatten. Hieruit volgt dat H uniek bepaald is en bovendien een cyclische groep is. □

Stelling 5.39

Veronderstel dat $G, \cdot$ een eindige groep is van de orde $n \geq 2$. Dan zijn de volgende eigenschappen gelijkwaardig.

(i) $G, \cdot$ is een cyclische groep.

(ii) Als d een deler is van n, dan bezit $x^d = 1$ precies d oplossingen in $G, \cdot$.

(iii) Als d een deler is van n, dan bezit $G, \cdot$ juist $\varphi(d)$ elementen van de orde d.

Bewijs. We zullen bewijzen dat uit de eigenschap (i) de eigenschap (ii) volgt, dat die op zijn beurt de eigenschap (iii) impliceert, en dat tenslotte de eigenschap (iii) de eigenschap (i) impliceert.

(i) $\Longrightarrow$ (ii)

Veronderstel dat G een cyclische groep is van de orde n die door een element g voortgebracht wordt. Als d een willekeurige deler is van n, dan stellen we $n = dk$. De elementen

$$1, g^k, g^{2k}, \ldots, g^{(d-1)k}$$

zijn allemaal verschillende elementen. Elk van deze elementen is bovendien oplossing van de vergelijking $x^d = 1$ want

$$(g^{ik})^d = (g^{kd})^i = (g^n)^i = 1^i = 1.$$

We hebben dus reeds d oplossingen van de vergelijking $x^d = 1$. We moeten nog bewijzen dat er geen andere zijn. Veronderstel dat y een willekeurig element van G is waarvoor geldt dat $y^d = 1$. Aangezien echter G een cyclische groep is die voortgebracht wordt door g, bestaat er een exponent j zodanig dat $y = g^j$ en bijgevolg is

$$g^{jd} = (g^j)^d = y^d = 1.$$

Aangezien de orde van g gelijk is aan n volgt hieruit dat jd een veelvoud is van n, stel $jd = ln$. Aangezien echter $n = dk$ volgt hieruit dat $j = lk$, zodat $y = g^j = g^{lk}$, hetgeen betekent dat y tot de verzameling van de d oplossingen van de vorm g^{ik}, $0 \leq i \leq d-1$, behoort. Bijgevolg bezit de vergelijking $x^d = 1$ juist d oplossingen in G.

(ii) $\Longrightarrow$ (iii)

Een element x van de orde c zal voldoen aan de vergelijking $x^d = 1$ dan en slechts dan als c een deler is van d. Indien er bijgevolg $\alpha(c)$ dergelijke elementen van de orde c zijn en rekening houdend met het feit dat $x^d = 1$ juist d oplossingen heeft, moet

$$d = \sum_{c|d} \alpha(c).$$

Wegens de Möbiusinversieformule (Gevolg 4.58) is

$$\alpha(d) = \sum_{c|d} \mu(c)\frac{d}{c} = \varphi(d).$$

(iii) $\Longrightarrow$ (i)

Indien eigenschap (iii) geldt, dan weten wij in het bijzonder dat er $\varphi(n)$ elementen van de orde n bestaan. Nu is $\varphi(n) \geq 1$ zodat G tenminste één element van de orde n bevat. Dit element zal de ganse groep G voortbrengen, m.a.w. G is een cyclische groep van de orde n. □

Gevolg 5.40

Als C_n een cyclische groep is die voortgebracht wordt door g, dan wordt C_n eveneens voortgebracht door g^k met $\text{ggd}(k, n) = 1$.

Voorbeeld 5.41. Beschouw bijvoorbeeld de cyclische groep C_{12} van de orde 12 met als voortbrengend element z, maw. $C_{12} = \langle z \rangle = \{z, z^2, \ldots, z^{11}, z^{12} = 1\}$. De verzameling van de delers van 12 is $\{1, 2, 3, 4, 6, 12\}$. Voor elk van deze 6 delers bestaat er juist één deelgroep van die orde en telkens is de groep

cyclisch. Deze groepen zien er als volgt uit:

$$
\begin{aligned}
C_1 &= \langle 1 \rangle = \{1\} \\
C_2 &= \langle z^6 \rangle = \{1, z^6\} \\
C_3 &= \langle z^4 \rangle = \langle z^8 \rangle = \{1, z^4, z^8\} \\
C_4 &= \langle z^3 \rangle = \langle z^9 \rangle = \{1, z^3, z^6, z^9\} \\
C_6 &= \langle z^2 \rangle = \langle z^{10} \rangle = \{1, z^2, z^4, z^6, z^8, z^{10}\} \\
C_{12} &= \langle z \rangle = \langle z^5 \rangle = \langle z^7 \rangle = \langle z^{11} \rangle = \{z, z^2, \ldots, z^{11}, z^{12} = 1\}.
\end{aligned}
$$

Voorbeeld 5.42. We hebben in Gevolg 4.73 gezien dat de elementen van $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, p priem, allemaal te schrijven zijn als a^i, met a een primitieve wortel modulo p. De verzameling $\mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ samen met de vermenigvuldiging is dus een cyclische groep van orde $p - 1$.

Gevolg 5.43

Als er een primitieve wortel modulo m bestaat, dan bestaan er precies $\varphi(m - 1)$ primitieve wortels modulo m.

Bewijs. Als er een primitieve wortel modulo m bestaat, dan is $\mathbb{Z}/m\mathbb{Z} \setminus \{0\}, \cdot$ een cyclische groep van orde $m - 1$. Stelling 5.39 bewijst nu het gestelde. □

5.3 Ringen

De gehele getallen, voorzien van de optelling en vermenigvuldiging, vormen een standaardvoorbeeld dat we abstraheren in de volgende definitie.

Definitie 5.44

Een *ring* is een verzameling R, voorzien van twee binaire bewerkingen $+$ en $\cdot$, waarvoor geldt dat

(1) $R, +$ is een abelse groep, met eenheidselement 0;

(2) de vermenigvuldiging is associatief (voorwaarde **(A)** uit Definitie 5.2);

(3) de vermenigvuldiging is *distributief* ten opzichte van de optelling, i.e. $\forall a, b, c \in R$:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c\,, \\ (a + b) \cdot c &= a \cdot c + b \cdot c\,. \end{aligned}$$

Bovenstaande definitie is vrij algemeen, behalve $\mathbb{Z}, +, \cdot$ zijn er nog zeer veel andere algebraïsche structuren die aan de voorwaarden voldoen. Als $R, +, \cdot$ een ring is, en de context maakt duidelijk welke de twee binaire bewerkingen zijn, dan worden deze ook weggelaten in de notatie, en dan veronderstellen we ook dat 0 het eenheidselement is voor de optelling en 1 het eenheidselement voor de vermenigvuldiging.

Opmerkingen

We veronderstellen dat $R, +, \cdot$ een ring is.

1. Als $R \setminus \{0\}, \cdot$ aan voorwaarde **(N)** voldoet (er bestaat een neutraal element e voor de vermenigvuldiging), dan wordt R een *ring met neutraal element* of een *ring met eenheidselement* genoemd. Het bewijs van Stelling 5.13 (1) kan overgenomen worden om aan te tonen dat het neutraal element uniek is. Soms zullen we dit neutraal element ook gewoon voorstellen door 1.

2. Als $R \setminus \{0\}, \cdot$ aan voorwaarde **(C)** voldoet (de vermenigvuldiging is commutatief), dan zegt men dat $R, +, \cdot$ een *commutatieve* of *abelse* ring is.

3. De orde van een ring R is per definitie de orde van de verzameling R.

4. Uit de definitie van een ring kan men niet besluiten dat de linkse of rechtse schrappingswet geldt. Het is ook mogelijk dat in een ring,

elementen a en b bestaan die verschillend zijn van 0, maar waarvoor hun product 0 is. De volgende definitie houdt hiermee verband.

Definitie 5.45

Stel R een ring. Elementen $a, b \in R \setminus \{0\}$ worden *nuldelers* genoemd als $ab = 0$.

Een ring zonder nuldelers wordt een *domein* genoemd, een commutatieve ring met eenheidselement en zonder nuldelers wordt een *integriteitsgebied* genoemd. Zo is de ring $\mathbb{Z}, +, \cdot$ een integriteitsgebied, maar is dit niet altijd waar voor de ring $\mathbb{Z}/m\mathbb{Z}, +, \cdot$.

Voorbeeld 5.46.

1. $\mathbb{Q}, +, \cdot; \mathbb{R}, +, \cdot; \mathbb{Z}, +, \cdot$ zijn (commutatieve) ringen voor de gewone optelling en vermenigvuldiging en bezitten geen nuldelers.

2. $\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes$ is de ring der gehele getallen modulo m, waarbij de optelling en vermenigvuldiging gedefinieerd worden modulo m, zoals in hoofdstuk 4 ingevoerd werd. Deze ring is een voorbeeld van een eindige commutatieve ring van de orde m. Indien m geen priemgetal is, dan bezit deze ring nuldelers. Zo is bijvoorbeeld $[3]_6 \otimes [2]_6 = [0]_6$. De schrappingswet geldt niet want $[3]_6 \otimes [5]_6 = [3]_6 \otimes [1]_6$, maar nochtans is $[1]_6 \neq [5]_6$. Ondertussen weten wij dat dit een gevolg is van het feit dat in $\mathbb{Z}/6\mathbb{Z}$ het element $[3]_6$ geen invers element bezit.

3. $M_n(\mathbb{R}), +, \times$ is de ring van de $n \times n$ matrices over de reële getallen voor de matrixoptelling en de matrixvermenigvuldiging. Deze ring is geen commutatieve ring. Ook hier geldt niet zomaar de linkse of rechtse schrappingswet en zijn de singuliere matrices (maw. de matrices waarvan de determinant gelijk is aan 0) de nuldelers van de ring (zie cursus lineaire algebra).

We hebben gezien dat -1 en 1 een speciale rol spelen in de ring $\mathbb{Z}$. Zo zijn alle grootste gemene delers van twee gehele getallen gelijk aan elkaar op het teken na, dus het product met -1 of 1, en geldt de ontbinding van een geheel in priemelementen op het teken na. Beide elementen -1 en 1 hebben verder ook nog gemeen dat ze de enige elementen in $\mathbb{Z}$ zijn die een inverse hebben voor de vermenigvuldiging. Deze observatie zetten we om in een definitie.

Definitie 5.47

Stel $R, +, \cdot$ is een ring. Een element $u \in R$ is een *eenheid* als het het inverteerbaar element is voor de vermenigvuldiging, i.e. er bestaat een element $v \in R$ waarvoor $u \cdot v = v \cdot u = 1$.

Indien $u \in R$ een eenheid is, dan is zijn inverse uniek bepaald. Opnieuw kan het argument van Stelling 5.13 (2) gebruikt worden om dit aan te tonen. Ook is duidelijk dat indien u een eenheid is, ook u^{-1} dat is. De verzameling van de eenheden van een ring noteren we als $U(R)$. Enkele eenvoudige voorbeelden zijn $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\}$ en $U(\mathbb{Z}/7\mathbb{Z}) = \{1, 2, 3, 4, 5, 6\}$.

Stelling 5.48

De verzameling $U(R)$ van de inverteerbare elementen van een ring R vormen een groep voor de (restrictie van de) vermenigvuldiging.

Bewijs. Veronderstel dat x en y inverteerbaar zijn en noem x^{-1} en y^{-1} hun respectievelijke inversen. Dan geldt

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= 1\\ (y^{-1}x^{-1})(xy) &= 1.\end{aligned}$$

Bijgevolg is $(xy)^{-1} = y^{-1}x^{-1}$ het invers element van xy. De verzameling $U(R)$ is dus gesloten voor de vermenigvuldiging. Aangezien uit de definitie van $U(R)$ volgt dat voor elk element x van $U(R)$ het invers element x^{-1} eveneens tot $U(R)$ behoort, volgt hieruit dat $U(R)$ een groep is voor de vermenigvuldiging. □

In stelling 4.32 hebben we bewezen dat een element r in $\mathbb{Z}/m\mathbb{Z}$ inverteerbaar is dan en slechts dan als r en m onderling ondeelbaar zijn. Bijgevolg is $U(\mathbb{Z}/m\mathbb{Z}), \cdot$ in dit geval een groep van de orde $\varphi(m)$. Zo zal bijvoorbeeld $U(\mathbb{Z}/8\mathbb{Z}), \cdot$ isomorf zijn met de viergroep van Klein (bewijs als oefening). Daarenboven betekent Stelling 4.72 in deze context niets anders dan dat $U(\mathbb{Z}/p\mathbb{Z}), \cdot$; p een priemgetal, een cyclische groep van de orde $\varphi(p) = p - 1$ is. Zo is bijvoorbeeld $U(\mathbb{Z}/7\mathbb{Z}) = \{1, 2, 3, 4, 5, 6\}$ een cyclische groep C_6 met voortbrengend element 3, want de orde van 3 modulo 7 is 6.

Oefening 5.49. Toon aan dat de groep $U(\mathbb{Z}/8\mathbb{Z})$ is isomorf met de viergroep van Klein.

Oplossing. Men kan eenvoudig nagaan dat $U(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\}$. Men rekent eenvoudig na dat $[3]_8 \otimes [5]_8 = [7]_8$, $[3]_8 \otimes [7]_8 = [5]_8$, en $[5]_8 \otimes [7]_8 = [3]_8$. De afbeelding $\theta : \mathbb{Z}/8\mathbb{Z} \to V$, $\theta(3) = a$, $\theta(5) = b$, $\theta(7) = c$ (en uiteraard $\theta(1) = e$) is dus een isomorfisme van $\mathbb{Z}/8\mathbb{Z}, \otimes$ naar $V, \cdot$. ■

5.4 Lichamen en velden

Definitie 5.50

Een *lichaam* is een verzameling F, voorzien van twee binaire bewerkingen $+$ en $\cdot$, waarvoor geldt dat

(1) $F, +$ is een abelse groep, met eenheidselement 0;

(2) $F \setminus \{0\}, \cdot$ is een groep;

(3) de vermenigvuldiging is *distributief* ten opzichte van de optelling, i.e. $\forall a, b, c \in R$:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c\,, \\ (a + b) \cdot c &= a \cdot c + b \cdot c\,. \end{aligned}$$

Een lichaam is dus een ring F waarvoor $U(F) = F \setminus \{0\}$.

Definitie 5.51

Een *veld* is een lichaam waarvoor bovendien geldt dat de vermenigvuldiging commutatief is.

Typische voorbeelden van velden zijn $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. Uit Stelling 4.32 volgt dat $\mathbb{Z}/p\mathbb{Z}$ een veld is als en slechts als p een priemgetal is. Dit is een voorbeeld van een *eindig veld*. Eén van de doelstellingen in dit hoofdstuk is de constructie en beschrijving van velden. We beginnen met enkele algemeenheden.

Stelling 5.52

Een eindig domein is een lichaam.

Bewijs. Stel dat R een eindig domein is. Dan zijn er in R geen nuldelers. Kies een willekeurige $a \in R\setminus\{0\}$ en beschouw de afbeelding $f_a : R\setminus\{0\} \to R\setminus\{0\}$, $x \mapsto xa$. Stel $f_a(x) = f_a(y)$, dan is $ax = ay$ of $a(x-y) = 0$, wegens de distributiviteit. Aangezien $a \neq 0$ en er in R geen nuldelers zijn, moet $x - y = 0$, of $x = y$. De afbeelding f_a is dus injectief. Een injectieve afbeelding van een eindige verzameling naar zichzelf is ook surjectief. Dus er bestaat een $x \in R \setminus \{0\}$ waarvoor $xa = 1$, of nog, er bestaat een inverse voor a. Omdat a willekeurig was, besluiten we dat elk element van $R \setminus \{0\}$ inverteerbaar is, dus R is een lichaam. □

Gevolg 5.53

Een eindig integriteitsgebied is een veld.

De volgende stelling maakt de zoektocht naar eindige lichamen die geen veld zijn, overbodig. Het bewijs is niet ingewikkeld maar vereist nog een klein beetje extra groepentheorie dan wat er in deze cursus staat. In de cursus Algebra I wordt deze stelling bewezen.

Stelling 5.54 — stelling van Wedderburn

Een eindig lichaam is een veld.

De constructie van $\mathbb{Q}$ als breukenveld van $\mathbb{Z}$ is duidelijk. We beschrijven deze constructie algemener.

Veronderstel dat $R, +, \cdot$ een integriteitsgebied is. Op de verzameling $R \times R \setminus \{0\}$ definiëren we een equivalentierelatie $\sim$: $(a,b) \sim (c,d) \iff ad = bc$. Noem Q_R de verzameling van equivalentieklassen, en noteer de klasse die het element (a,b) bevat als $\frac{a}{b}$.

We definiëren een optelling $+_Q$ en een vermenigvuldiging $\cdot_Q$ op de verzameling Q_R als volgt:

$$\frac{a}{b} +_Q \frac{c}{d} := \frac{ad+cb}{bd} \text{ en } \frac{a}{b} \cdot_Q \frac{c}{d} := \frac{a \cdot c}{b \cdot d}$$

Het is eenvoudig na te gaan dat $Q_R, +_Q, \cdot_Q$ een veld is. Daarenboven kan men R *inbedden* in Q_R. De afbeelding $\theta : R \to Q_R$, $\theta(x) := \frac{x}{1}$ is een afbeelding tussen de twee ringen R en Q_R die de structuur bewaart. Als met $R = \mathbb{Z}$ stelt, dan is Q_R niets anders dan de vertrouwde verzameling van de rationale

getallen. Omdat R ingebed is in Q_R, kunnen we $+_Q$ en $\cdot_Q$ blijven noteren als $+$ en $\cdot$. Tenslotte wordt $Q_R, +, \cdot$ ook nog het *breukenveld* van R genoemd.

Is $R = \mathbb{Z}$, dan kiezen we de representant van de klasse $\frac{a}{b}$ zodanig dat $\text{ggd}(a, b) = 1$ en $b > 0$. Daarmee kunnen we ook de orderelatie $\leq$ op $\mathbb{Z}$ uitbreiden naar een orderelatie $\leq_Q$ op Q_R: $\frac{a}{b} \leq_Q \frac{c}{d} \iff ad \leq bc$. Ook de notatie $\leq$ zullen we gebruiken voor $\leq_Q$. Daarmee is de uitbreiding van $\mathbb{Z}$ naar $\mathbb{Q}$ formeel beschreven, en kan deze ook uitgevoerd worden voor andere integriteitsgebieden (en zelfs domeinen) dan $\mathbb{Z}$.

Definitie 5.55

Een geordend veld is een veld $\mathbb{F}, +, \cdot$, samen met een totale orderelatie $\preceq$ op $\mathbb{F}$ die voldoet aan de volgende eigenschappen:

$$x \preceq y \Longrightarrow x + z \preceq y + z \ \forall z \in \mathbb{F}$$
$$0 \preceq x \text{ en } 0 \preceq y \Longrightarrow 0 \preceq xy$$

Het is eenvoudig om na te gaan dat $\mathbb{Q}$ een geordend veld is. De verzameling $\mathbb{Q}$ is ook *dicht* ten opzichte van $\leq$. Tussen elke twee verschillende rationale getallen kan men (eenvoudig) een derde rationaal getal construeren verschillend van de eerste twee, een daardoor oneindig veel. Een veld wordt *dicht* genoemd als deze eigenschap geldig is. Het supremumprincipe (geformuleerd in de cursus Analyse I), geldt echter niet in het veld der rationale getallen.

5.5 De reële getallen

Decimale ontwikkelingen

Een *decimale ontwikkeling* is een rij $a = (a_i)$, $a_i \in \{0, \ldots, 9\}$, waarvoor er steeds een $m \in \mathbb{N}$ bestaat zodat we de rij kunnen indexeren als volgt: $a_m, a_{m-1}, \ldots, a_1, a_0, a_{-1}, a_{-2}, \ldots$. We noteren deze verzameling als D, de optelling $+_D$ en vermenigvuldiging $\cdot_D$ kunnen heel gemakkelijk gedefinieerd worden, evenals de ordening $\leq_D$. Het is eenvoudig te controleren dat elk rationaal getal een decimale ontwikkeling heeft, indien gewenst zelfs een oneindige decimale ontwikkeling. Deze eigenschap hebben we al gebruikt in het bewijs van Stelling 2.44. De verzameling D *bevat* dus de rationale getallen $\mathbb{Q}$, preciezer: er bestaat een injectieve afbeelding f van $\mathbb{Q}$ naar D die elk element

van $\mathbb{Q}$ afbeeldt op een element van D en zodanig dat f *de bewerkingen respecteert*, en zodanig dat de beperking van $\leq_D$ overeenkomt met de ordening op $\mathbb{Q}$. We zullen dit verderop preciezer omschrijven. In de cursus Analyse I wordt aangetoond dat de verzameling D aan het supremumprincipe voldoet

De sneden van Dedekind

Een *snede* is een deelverzameling $A \subset \mathbb{Q}$ die voldoet aan de volgende eigenschappen:

(i) $A \neq \emptyset$ en $A \neq \mathbb{Q}$,

(ii) Als $x \in A$, en $y \leq x$, dan is $y \in A$,

(iii) A bevat geen grootste element.

Eigenschap (iii) voor een snede houdt in dat als $x \in A$, er een $y > x$ bestaan waarvoor $y \in A$. Kiezen we een willekeurig element van $\mathbb{Q}$, dan is de verzameling $\{x \in \mathbb{Q} : x < b\}$ een voorbeeld van een snede, omdat $\mathbb{Q}$ dicht is. Er zijn echter meer sneden dan rationale getallen. De verzameling $B := \{x \in \mathbb{Q} : x^2 < 2\}$ is een snede, maar door Stelling 1.4 bestaat er geen rationaal getal dat groter is dan alle elementen van B. Definieer R als de verzameling van alle sneden van $\mathbb{Q}$. Veronderstel dat A en B twee elementen uit R zijn, dan definiëren we de optelling $+_R$ en $\cdot_R$ als volgt.

$$A +_R B := \{a + b : a \in A, b \in B\}$$

$$A \cdot_R B := \{x \in \mathbb{Q} : \exists 0 \leq a \in A, \exists 0 \leq b \in B, x < ab\}$$

Het is niet ingewikkeld (maar vraagt wat schrijfwerk) om na te gaan dat $A +_R B$ en $A \cdot_R B$ sneden zijn. Het is ook niet moeilijk om een elk rationaal getal te beschrijven als een snede. De ordening $\leq_R$ tenslotte is eenvoudig te definiëren als

$$A \leq_R B \iff A \subseteq B\,.$$

Daarmee is al snel duidelijk dat $R, +_R, \cdot_R$ een geordend veld is, dat $\mathbb{Q}$ bevat. We kunnen dus opnieuw de notatie $+$ en $\cdot$ behouden in D, evenals de notatie $\leq$. Er is verder enig werk nodig om aan te tonen dat deze constructie de reële getallen oplevert zoals wij ze kennen, namelijk de verzameling van alle mogelijke (inclusief oneindige) decimale ontwikkelingen. Het is nu eenvoudig in te zien dat het supremumprincipe geldt in de geordende verzameling R.

Deelvelden en veldisomorfismen

We hebben twee modellen voor de reële getallen als *uitbreiding* van de rationale getallen beschreven. De volgende definities laten ons toe dit preciezer te omschrijven.

Definitie 5.56

Stel $K, +, \cdot$ is een veld. Een verzameling $F \subseteq K$ is een *deelveld* van K als en slechts als $K, +, \cdot$ een veld is.

Bovenstaande definitie zegt niets anders dan dat een deelverzameling van een veld een deelveld is, als de bewerkingen, beperkt tot de deelverzameling, opnieuw een veldstructuur geven aan de deelverzameling. Het is onmiddellijk duidelijk dat een deelveld hetzelfde eenheidselement voor de vermenigvuldiging en optelling moet hebben. Een deelverzameling die beide elementen niet bevat, kan dus nooit een deelveld zijn.

Definitie 5.57

Een geordend veld $K, \leq_K$ is een deelveld van het geordend veld $F, \leq_F$ als K een deelveld is van F en als de beperking van $\leq_F$ tot K gelijk is aan $\leq_K$.

Lemma 5.58

Stel K is een veld en $F \subset K$ is een deelveeld. Dan is K een F-vectorruimte.

Het is duidelijk dat $\mathbb{C}$ een 2-dimensionale vectorruimte over $\mathbb{R}$ is.

Definitie 5.59

Twee velden F en K zijn *isomorf* als en slechts als er een bijectieve afbeelding $\phi : F \to K$ bestaat zodat $\phi : F, + \to K, +$ een isomorfisme is tussen de beide additieve groepen en $\phi : F, \cdot \to K, \cdot$ een isomorfisme is tussen de beide multiplicatieve groepen

In principe kunnen we ook ringisomorfismen definiëren, en aldus deze definitie in een algemener kader geven.

Zeggen dat $\mathbb{Q}$ een deelveld is van bijvoorbeeld het hierboven beschreven veld D (of R), betekent dus heel precies dat er een deelverzameling $Q \subseteq D$ (of $Q \subseteq R$) bestaat, en een isomorfisme tussen $\mathbb{Q}$ en Q.

De volgende stelling laat ons toe naar believen constructies te bedenken voor de reële getallen, zonder dat we ons zorgen moeten maken over welke constructie we nu moeten kiezen.

Stelling 5.60

Er bestaat op isomorfisme na slechts één geordend veld $F, +, \cdot, \leq$ dat $\mathbb{Q}$ als deelveld bevat waarin het supremumprincipe geldt.

Vanaf nu gebruiken we opnieuw de notatie $\mathbb{R}$ voor (elk model van) de reële getallen.

Completering via Caucy-rijen

Noteer $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$.

Definitie 5.61

Veronderstel dat $\mathbb{K}$ een veld is. Een absolute waarde op $\mathbb{K}$ is een afbeelding $a : \mathbb{K} \to \mathbb{R}^+$ die voldoet aan de volgende drie eigenschappen:

(i) $a(x) = 0 \iff x = 0$

(ii) $a(xy) = a(x)a(y)$

(iii) $a(x + y) \leq a(x) + a(y)$.

Een gekend voorbeeld van een veld met absolute waarde is $\mathbb{K} = \mathbb{Q}$ en $a = |\ |$, met $|x| = x$ als $x \geq 0$ en $|x| = -x$ als $x < 0$. Met behulp van een absolute waarde kan een *afstand* gedefinieerd worden tussen elementen: $d(x, y) := a(x-y)$. Deze afstand maakt van $\mathbb{K}$ een *metrische ruimte*, en allerlei gekende concepten uit de Analyse kunnen nu gedefinieerd worden, zoals bijvoorbeeld een open bal rond een element x met straal $\epsilon > 0$.

Veronderstel nu dat $\mathbb{K}$ een veld is met bijhorende absolute waarde $|\ |_{\mathbb{K}}$. Een rij $(x_n)_{n\in\mathbb{N}}$, $x_n \in \mathbb{K}$, convergeert naar een limiet $L \in \mathbb{K}$ als $\forall \epsilon \in \mathbb{R}^+ \backslash \{0\}, \exists N \in \mathbb{N} : n \geq N \Rightarrow |x_n - L|_{\mathbb{K}} < \epsilon$.

Definitie 5.62

Een rij (x_n) is een *Cauchy-rij* in $\mathbb{K}$ ten opzichte van $|\ |_{\mathbb{K}}$ als

$$\forall \epsilon \in \mathbb{R}^+ \setminus \{0\}, \exists N \in \mathbb{N} : n, m \geq N \Rightarrow |x_n - x_m|_{\mathbb{K}} < \epsilon$$

Een convergente rij is steeds een Cauchy-rij (gebruik eigenschap (iii) van de absolute waarde), we noemen $\mathbb{K}$ compleet (ten opzichte van $|\ |_{\mathbb{K}}$) als het omgekeerde waar is. Het veld $\mathbb{Q}$ is niet compleet (ten opzichte van $|\ |$). De decimale ontwikkeling van $\sqrt{2}$ levert een Cauchy-rij die naar $\sqrt{2} \notin \mathbb{Q}$ convergeert. Deze observatie ligt aan de basis van het idee om het veld $\mathbb{Q}$ uit te breiden met behulp van Cauchy-rijen, en dit kan in een algemene context gebeuren.

Noteer de verzameling van alle Cauchy-rijen in $\mathbb{K}$ als $\mathcal{C}(\mathbb{K})$. De optelling en vermenigvuldiging op $\mathbb{K}$ worden puntsgewijze overgedragen op $\mathcal{C}(\mathbb{K})$:

$$(x_n) + (y_n) := (x_n + y_n)$$
$$(x_n) \cdot (y_n) := (x_n \cdot y_n)$$

Definieer $\mathcal{N} \subseteq \mathcal{C}(\mathbb{K})$ als de verzameling van de nulrijen, i.e. de rijen die als limiet $0 \in \mathbb{K}$ hebben, en we definiëren de relatie $\sim$ op $\mathcal{C}(\mathbb{K})$ als volgt: $(x_n) \sim (y_n) \iff (x_n - y_n) \in \mathcal{N}$. Men kan eenvoudig nagaan dat $\sim$ een equivalentierelatie is. Zoals gebruikelijk worden de bewerkingen op $\mathcal{C}(\mathbb{K})$ overgedragen op de quotiëntstructuur $\mathcal{C}(\mathbb{K})/\sim$. Dan is er wat werk nodig om aan te tonen dat de quotiëntstructuur, samen met de bewerkingen, een veld is. Het bewijs dat er voor elk niet-nul element een inverse voor de vermenigvuldiging bestaat, vergt het meeste schrijfwerk, maar is elementair en steunt op de kenmerkende eigenschappen van de absolute waarde. Deze procedure noemen we een completering van het veld $\mathbb{K}$ ten opzichte van $|\ |_{\mathbb{K}}$. Noteer het bekomen veld als $\mathbb{F}$. Het is duidelijk dat $i : \mathbb{K} \to \mathcal{C}(\mathbb{K}), x \mapsto (x)_{n \in \mathbb{N}}$ een injectie van $\mathbb{K}$ in $\mathcal{C}(\mathbb{K})$ is die een isomorfisme tussen $\mathbb{K}$ en een deelveld van $\mathbb{F}$ induceert. De volgende eigenschappen kunnen dan aangetoond worden.

Stelling 5.63

(i) Er bestaat een unieke absolute waarde $|\ |_{\mathbb{F}}$ zodanig dat $|x|_{\mathbb{F}} = |x|_{\mathbb{K}}$ voor alle $x \in \mathbb{K}$.

(ii) $\mathbb{F}$ is compleet ten opzichte van $|\ |_{\mathbb{F}}$

(iii) $\mathbb{K}$ is dicht in $\mathbb{F}$, i.e. elke open bal rond een element van $\mathbb{F}$ bevat een element van $\mathbb{K}$.

De completering van $\mathbb{Q}$ ten opzichte $|\ |$, levert $\mathbb{R}$ (met dezelfde absolute waarde). Het completeringsproces maakt gebruik van een absolute waarde, en dus impliciet van het veld $\mathbb{R}$. Omdat $\mathbb{Q}$ een geordend veld is, kan men echter de absolute waarde definiëren als een afbeelding van $\mathbb{Q}$ naar zichzelf (op de gebruikelijke wijze). De definitie van convergente rij en Cauchy-rij blijft ongewijzigd (maar men gebruikt nu $\mathbb{Q}^+$ in plaats van $\mathbb{R}^+$). Het completeringsproces blijft ongewijzigd en levert ook dan de reële getallen $\mathbb{R}$, met alle bijhorende eigenschappen. Het gebruik van een absolute waarde met als waardegebied de reële getallen, maakt het echter mogelijk om het completeringsproces ook uit te voeren op ongeordende velden of ten opzichte van alternatieve absolute waarden.

De p-adische getallen

Kies een getal $r \in \mathbb{Q}\backslash\{0\}$ en kies een priemgetal $p \in \mathbb{N}$. Dan bestaan er steeds getallen $a, b, n \in \mathbb{Z}$ zodat $r = \frac{a}{b}p^n$ en $\text{ggd}(a, b) = \text{ggd}(a, p) = \text{ggd}(b, p) = 1$. Het getal $n =: v_p(r)$ definiëren we als de *p-adische valuatie* van r. Bij definitie geldt $v_p(0) = \infty$. We definiëren we $|r|_p := p^{-v_p(r)}$. Men kan eenvoudig aantonen dat $|\ |_p$ een absolute waarde is op $\mathbb{Q}$, die bovendien voldoet aan

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}\,,$$

hetgeen sterker is dan de driehoeksongelijkheid (eigenschap (iii) uit Definitie 5.61). Een absolute waarde die aan deze sterkere eigenschap voldoet wordt een *niet-Archimedische absolute waarde* genoemd.

Het completeringsproces kan nu ook uitgevoerd worden ten opzichte van de absolute waarde $|\ |_p$. Dit proces levert het zogenaamde *veld der p-adische getallen* op, genoteerd $\mathbb{Q}_p$. Stelling 5.63 blijft (uiteraard) geldig, maar er zijn enkele extra's: $\mathbb{Q}_p$ kan niet geordend worden en de geïnduceerde absolute waarde op $\mathbb{Q}_p$ is niet-Archimedisch en heeft hetzelfde bereik als $|\ |_p$.

De p-adische getallen spelen een belangrijke rol in getaltheorie. In zekere zin vormen ze de brug tussen *discrete* concepten zoals deelbaarheid, en analytische methoden om deze concepten te bestuderen, net omdat deelbaarheidseigenschappen uitgedrukt worden in een valuatie (de functie v_p) en de bijhorende absolute waarde, en de daaruit voortvloeiende topologische eigenschappen waarvan analytische methoden gebruik maken.

Net zoals reële getallen kunnen p-adische getallen voorgesteld worden door een soort ontwikkeling, nu geen decimale, maar een p-adische. Men kan

aantonen dat

$$\mathbb{Q}_p = \{ \sum_{n=-m}^{\infty} a_i p^i : m \in \mathbb{N}, a_i \in \{0, \ldots p-1\}\} .$$

Meteen is ook duidelijk dat $\mathbb{Q} \subseteq \mathbb{Q}_p$. Tenslotte bekijken we de volgende verzameling

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} .$$

Gelet op de voorstelling van de elementen uit $\mathbb{Q}_p$ is het duidelijk dat

$$\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_i p^i : a_i \in \{0, \ldots p-1\}\} .$$

Meteen zien we dat $\mathbb{Z} \subseteq \mathbb{Z}_p$ (zie de opmerking op pagina 127), de verzameling $\mathbb{Z}_p$ wordt de verzameling van de *p-adische gehele getallen* genoemd. Zoals in de gehele getallen kunnen we modulair rekenen, stel $p\mathbb{Z}_p = \{px : x \in \mathbb{Z}_p\}$, en $x \equiv y \mod p\mathbb{Z}_p \iff x - y \in p\mathbb{Z}_p$. De quotiëntstructuur $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorf met het eindig veld $\mathbb{Z}/p\mathbb{Z}$. Zonder in te gaan op de details vermelden we nog dat er een belangrijk verband is tussen modulair rekenen modulo opeenvolgende machten van p en de p-adische getallen, en dat dit verband tevens aan de grondslag ligt van enkele efficiënte algoritmen die factorisatie van polynomen over de gehelen getallen (en dus ook de rationale getallen), mogelijk maken. Voor de praktijk verwijzen we naar de cursus Computeralgebra.

5.6 Veeltermringen

Velduitbreidingen kunnen ook geschieden op een louter algebraïsche wijze. We zullen enkele velduitbreidingen concreet beschrijven. Daartoe bestuderen we eerst een klasse van specifieke ringen, namelijk veeltermringen. In deze cursus is het niet de bedoeling om een theorie van velduitbreidingen te ontwikkelen, dit is één van de onderwerpen die aan bod komen in de cursus Algebra I.

Definitie 5.64

Een *veelterm* of *polynoom* over een ring R is elke uitdrukking van de gedaante

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$$

met $a_i \in R$.

Hierbij noemt men x een *onbepaalde variabele* en noemt men de elementen $a_i, i \in \mathbb{N}[0,n]$, de *coëfficiënten* van de veelterm. Indien $a_n \neq 0$, dan noemen we n de graad van de veelterm. Een veelterm is niets meer dan een afbeelding van R naar zichzelf. De specifieke aard van een veelterm laat echter toe veeltermen op te tellen en te vermenigvuldigen, waarbij we uiteraard opnieuw een veelterm bekomen. Ook scalaire vermenigvuldiging met elementen van R is mogelijk. Dit alles maakt dat de verzameling van de veeltermen over een veld F, in feite een oneindigdimensionale vectorruimte over F is, waarbij er ook een vermenigvuldiging tussen de vectoren gedefinieerd is. Dergelijke structuren beschrijven we verderop ook nog formeel.

De verzameling van al de veeltermen met coëfficiënten in de ring R wordt genoteerd door $R[x]$. De veeltermen van de vorm (a_0) worden *constante veeltermen* genoemd en kunnen geïdentificeerd worden met de elementen van R. De *nulveelterm* is per definitie de constante veelterm (0). In het vervolg zullen we de constante veeltermen (a_0) kortweg als a_0 noteren.

In het vervolg zullen wij soms de veeltermen noteren in dalende volgorde van de exponenten van x:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

De coëfficiënt van $a_n (\neq 0)$ wordt soms de *leidende coëfficiënt* genoemd. Indien $a_n = 1$, dan noemen we de veelterm een *monische veelterm*. Merk op dat indien we de verkorte (rij)notatie gebruiken, we steeds de coëfficiënten in stijgende volgorde van de exponenten zullen schrijven.

Veronderstel dat

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \quad \text{en} \quad b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots + b_m x^m$$

twee veeltermen zijn over R met respectievelijke graad n en m. We zullen deze veeltermen verkort noteren door $a(x)$, respectievelijk $b(x)$. Zonder de algemeenheid te schaden, mogen wij veronderstellen dat $n \geq m$. Indien $n > m$, dan stellen we $b_{m+1} = b_{m+2} = \ldots = b_n = 0$. We kunnen nu de *som* $a(x) + b(x)$ en het *product* $a(x)b(x)$ van de veeltermen als volgt definiëren.

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots \\ &\qquad \cdots + a_n b_m x^{n+m}. \end{aligned}$$

Met andere woorden, de veelterm $s(x) = a(x) + b(x)$ is de veelterm $(s_0, s_1, \ldots, s_n)$ met

$$s_i = a_i + b_i \quad (0 \leq i \leq n),$$

terwijl $p(x) = a(x)b(x)$ de veelterm $(p_0, p_1, \ldots, p_{n+m})$ is met

$$p_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (0 \leq i \leq n+m) \quad (a_k = 0, \forall k > n; b_k = 0, \forall k > m).$$

De optelling en de vermenigvuldiging van elementen in $R[x]$ worden dus gedefinieerd aan de hand van de optelling en vermenigvuldiging in R. We hebben daarom bewust geen andere notatie ingevoerd voor de optelling en de vermenigvuldiging in $R[x]$. Uit de definitie van een ring volgt dat indien de coëfficiënten van $a(x)$ en van $b(x)$ tot een ring R behoren, de coëfficiënten van hun som en hun product eveneens tot deze ring R behoren. Men kan eenvoudig (maar vrij omslachtig) bewijzen dat $R[x]$ voor de gedefinieerde optelling en vermenigvuldiging een commutatieve ring is, op voorwaarde dat R zelf een commutatieve ring is. Merk echter op dat de graad van de som $a(x) + b(x)$ van twee veeltermen $a(x)$ en $b(x)$ strikt kleiner kan zijn dan de graad van $a(x)$ en van $b(x)$. Zo zal bijvoorbeeld in $\mathbb{Z}/3\mathbb{Z}[x]$ de som van de veeltermen $(1, 1, 1)$ en $(1, 1, 2)$ die beide van de graad 2 zijn, gelijk zijn aan de veelterm $(2, 2)$ van de graad 1. Bovendien kan de graad van het product van twee veeltermen $a(x)$ en $b(x)$ strikt kleiner zijn dan de som van de graden van $a(x)$ en $b(x)$. Zo zal bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}[x]$ het product van de veelterm $(4, 1, 2)$ van de graad 2 en de veelterm $(1, 3)$ van de graad 1 gelijk zijn aan de veelterm $(4, 1, 5)$ van de graad 2, want in $\mathbb{Z}/6\mathbb{Z}$ is $3 \cdot 2 = 0$. Algemeen zal de graad van het product van twee veeltermen $a(x)$ en $b(x)$ kleiner zijn dan de som van de graden van deze veeltermen als de leidende coëfficiënten van $a(x)$ en $b(x)$ nuldelers van de ring zijn en als het product van deze leidende coëfficiënten gelijk is aan 0.

5.6.1 Veeltermringen over een veld

Vanaf nu veronderstellen we dat de veeltermcoëfficiënten elementen zijn van een veld $\mathbb{F}$. Dit betekent echter hoegenaamd niet dat de ring $\mathbb{F}[x]$ een veld zal zijn. Naar analogie met de ring van de gehele getallen bestaat ook voor de veeltermring $\mathbb{F}[x]$ een stelling over deelbaarheid van veeltermen.

Stelling 5.65

Veronderstel dat $\mathbb{F}$ een veld is en dat $a(x)$ en $b(x)$ veeltermen zijn in $\mathbb{F}[x]$ waarbij $b(x) \neq 0$. Dan bestaan er unieke veeltermen $q(x)$ en $r(x)$ in $\mathbb{F}[x]$ zodanig dat

$$a(x) = b(x)q(x) + r(x),$$

waarbij de graad van $r(x)$ kleiner is dan de graad van $b(x)$ of waarbij $r(x)$ de nulveelterm is.

Bewijs. We zullen inductie toepassen op de graad van de veelterm $a(x)$. Indien de graad van $a(x)$ kleiner is dan de graad van $b(x)$, dan is aan de stelling voldaan door $q(x)$ gelijk te stellen aan de nulveelterm en $r(x) = a(x)$ te nemen. We veronderstellen nu dat de graad van $b(x)$ gelijk is aan m en dat de graad van $a(x)$ gelijk is aan $n = m + k$ met $k \in \mathbb{N}$.

Stel

$$a(x) = a_{m+k}x^{m+k} + \cdots + a_0, \quad \text{en} \quad b(x) = b_m x^m + \cdots + b_0,$$

met $a_{m+k} \neq 0,\ b_m \neq 0$. Als inductiehypothese veronderstellen we dat de stelling waar is voor elke veelterm waarvan de graad kleiner is dan n.

Stel

$$\overline{a}(x) = a(x) - a_{m+k}b_m^{-1}x^k b(x).$$

De coëfficiënt van x^{m+k} in $\overline{a}(x)$ is

$$a_{m+k} - (a_{m+k}b_m^{-1})b_m = 0.$$

Bijgevolg is de graad van $\overline{a}(x)$ kleiner dan de graad van $a(x)$. Wegens de inductiehypothese weten we dat er veeltermen $\overline{q}(x)$ en $r(x)$ bestaan zodanig dat

$$\overline{a}(x) = b(x)\overline{q}(x) + r(x),$$

waarbij $r(x)$ ofwel de nulveelterm is of waarbij de graad van $r(x)$ kleiner is dan de graad van $b(x)$. We stellen nu

$$q(x) = \overline{q}(x) + a_{m+k}b_m^{-1}x^k.$$

Dan volgt hieruit dat

$$a(x) = b(x)q(x) + r(x),$$

waarbij $r(x)$ aan de gestelde voorwaarden voldoet.

We moeten nu nog enkel bewijzen dat $q(x)$ en $r(x)$ uniek bepaald zijn. Veronderstel dat

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x),$$

met $r_i(x)$ $(i = 1, 2)$ ofwel de nulveelterm ofwel is de graad van $r_i(x)$ $(i = 1, 2)$ kleiner dan de graad van $b(x)$. Dan geldt

$$b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

De veelterm in het linkerlid is ofwel de nulveelterm (en dan is $q_1(x) = q_2(x)$) ofwel is de graad ten minste gelijk aan de graad van $b(x)$ (merk op dat we veeltermen over een veld $\mathbb{F}$ beschouwen). Anderzijds is de veelterm in het rechterlid ofwel de nulveelterm (en dan is $r_1(x) = r_2(x)$) ofwel is de graad ervan strikt kleiner dan de graad van $b(x)$. Bijgevolg moeten de veeltermen in beide leden de nulveelterm zijn en zal dus $q_1(x) = q_2(x)$ en $r_1(x) = r_2(x)$.□

Een eerste analogie tussen de ring $\mathbb{Z}$ en de ring $F[x]$ laat zich opmerken. Een Euclidische deling kan in beide ringen uitgevoerd worden. De absolute waarde in $\mathbb{Z}$ wordt daarbij vervangen door de graad van de veeltermen in het delingsalgoritme.

Naar analogie met de gehele getallen kunnen we nu ook definities geven en stellingen bewijzen over deelbaarheid van veeltermen. We noemen $g(x)$ een *deler* of *factor* van een veelterm $f(x)$ in $\mathbb{F}[x]$ als er een veelterm $h(x)$ bestaat in $\mathbb{F}[x]$ zodanig dat

$$f(x) = g(x)h(x).$$

Definitie 4.6 kan, mutatis mutandis, overgenomen worden.

Definitie 5.66

Stel $a, b \in \mathbb{F}[x]$ niet beide nul. Een gemene deler $c \in \mathbb{F}[x]$ van a en b is een *grootste gemene deler* van a en b als en slechts als elke gemene deler van a en b een deler is van c.

Ook Lemma 4.7 kan eenvoudig aangepast worden.

Lemma 5.67

Als a en b twee grootste gemene delers zijn van twee elementen in $\mathbb{F}[x]$, dan geldt $a = u \cdot b$, met $u \in \mathbb{F} \setminus \{0\}$.

We kunnen dus steeds een grootste gemene deler vermenigvuldigen met de inverse van zijn leidende coëfficiënt, want $\mathbb{F}$ is een veld, en dus kunnen we een keuze maken over wat we precies bedoelen met *de* grootste gemene deler.

Definitie 5.68

Stel $a, b \in \mathbb{Z}$ niet beide nul. *De grootste gemene deler* van a en b is de unieke monische onder de grootste gemene delers van a en b.

Om nu de ggd$((a(x), b(x))$ in $\mathbb{F}[x]$ te berekenen herhalen we het argument zoals voor de gehele getallen, hetgeen nu aanleiding geeft tot het *(uitgebreid) algoritme van Euclides voor veeltermen over* $\mathbb{F}$. We kunnen dus de volgende opeenvolgende delingen uitvoeren.

$$\begin{aligned} a(x) &= b(x)q_0(x) + r_0(x) \\ b(x) &= r_0(x)q_1(x) + r_1(x) \\ r_0(x) &= r_1(x)q_2(x) + r_2(x) \\ \vdots &\quad \vdots \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x). \end{aligned}$$

Uit de laatste vergelijking volgt dat $r_n(x)$ een deler is van $r_{n-1}(x)$. Indien we de vergelijkingen in omgekeerde volgorde doorlopen, dan volgt hieruit dat $r_n(x)$ een deler is van $r_{n-3}(x)$ enz., zodat $r_n(x)$ eveneens deler is van $a(x)$ en van $b(x)$. Door de achtereenvolgende substituties uit te voeren, kunnen we dus $r_n(x)$ schrijven in de vorm

$$\lambda(x)a(x) + \mu(x)b(x),$$

waarbij $\lambda(x)$ en $\mu(x)$ veeltermen zijn in $\mathbb{F}[x]$. Op die manier hebben we een analogon voor de stelling 4.11 opgesteld.

Stelling 5.69

Veronderstel dat $\mathbb{F}$ een veld is en noem $d(x)$ een grootste gemene deler van de veeltermen $a(x)$ en $b(x)$ in $\mathbb{F}[x]$. Dan bestaan er veeltermen $\lambda(x)$ en $\mu(x)$ in $\mathbb{F}[x]$ zodanig dat

$$d(x) = \lambda(x)a(x) + \mu(x)b(x).$$

Oefening 5.70. *Zoek een grootste gemene deler $d(x)$ van $a(x) = x^3 + 2x^2 + x + 1$ en $b(x) = x^2 + 5$ in $\mathbb{Z}/7\mathbb{Z}[x]$ en schrijf $d(x)$ in de vorm $d(x) = \lambda(x)a(x) + \mu(x)b(x)$.*

Oplossing. We moeten dus de deling van de polynomen $a(x)$ en $b(x)$ uitvoeren. Dit gebeurt op dezelfde manier als we gewoon zijn voor de veeltermen over bijvoorbeeld de reële getallen, alleen moeten we nu de coëfficiënten als elementen van $\mathbb{Z}/7\mathbb{Z}$ beschouwen. We bekomen

$$x^3 + 2x^2 + x + 1 = (x^2 + 5)(x + 2) + (3x + 5).$$

Als volgende stap moeten we de deling van $x^2 + 5$ door $3x + 5$ uitvoeren. Merk op dat in $\mathbb{Z}/7\mathbb{Z}[x]$ geldt dat $x^2 + 5 = 15x^2 + 5$. Hieruit volgt dat

$$x^2 + 5 = (3x + 5)(5x + 1).$$

Bijgevolg is $3x + 5$ een grootste gemene deler van de gegeven veeltermen. Aangezien we maar weinig delingen hebben uitgevoerd om $d(x)$ te bepalen, zijn de veeltermen $\lambda(x)$ en $\mu(x)$ vrij vlug te bepalen. We bekomen

$$\begin{aligned} 3x + 5 &= (x^3 + 2x^2 + x + 1) - (x + 2)(x^2 + 5) \\ &= (x^3 + 2x^2 + x + 1) + (6x + 5)(x^2 + 5). \end{aligned}$$

Bijgevolg is $\lambda(x) = 1$ en $\mu(x) = 6x + 5$. ■

5.6.2 Irreducibele factoren en modulair rekenen

In hoofdstuk 4 hebben we bewezen dat elk geheel getal op het teken na op een unieke manier te ontbinden is in een product van priemgetallen. Aangezien we tot hiertoe de theorie van de veeltermen over een veld volledig naar analogie met de theorie van de gehele getallen hebben opgebouwd, kunnen we ons de vraag stellen of er ook een analogon voor priemgetallen bestaat.

Merk eerst en vooral op dat een constante veelterm verschillend van de nulveelterm altijd een deler is van een willekeurige veelterm $f(x)$ in $\mathbb{F}[x]$. Dit is niet verwonderlijk, aangezien de elementen van F de eenheden zijn van de ring $\mathbb{F}[x]$.

Definitie 5.71

Een veelterm $f(x)$ in $\mathbb{F}[x]$ wordt *irreducibel* genoemd dan en slechts dan als $f(x)$ geen constante veelterm is en als $f(x) = g(x)h(x)$ in $\mathbb{F}[x]$ impliceert dat ofwel $g(x)$ ofwel $h(x)$ constante veeltermen zijn.

Deze irreducibele veeltermen van $\mathbb{F}[x]$ zullen nu de rol overnemen van de priemelementen in $\mathbb{Z}$. Er geldt dan ook de volgende stelling, waarvan we echter het (eenvoudig) bewijs achterwege laten.

Stelling 5.72

Indien $f(x)$ een veelterm is in $\mathbb{F}[x]$ die geen constante veelterm is, dan kan $f(x)$ geschreven worden als een product van irreducibele veeltermen. Indien

$$f(x) = g_1(x)g_2(x)\dots g_r(x) = h_1(x)h_2(x)\dots h_s(x),$$

dan is $r = s$ en bovendien bestaat er voor elke $g_i(x)$ $(i = 1, \dots, r)$ juist één $h_j(x)$ $(j = 1, \dots, r)$ zodanig dat $g_i(x) = \alpha_j h_j(x)$ met $\alpha_j \in \mathbb{F}^*$.

Deze stelling zegt echter niet hoe we nu de ontbinding of factorisatie moeten vinden. Dit is in het algemeen, i.e. voor $\mathbb{F}$ een willekeurig veld, een zeer moeilijk probleem. Voor $\mathbb{F} = \mathbb{Q}$ bestaan er echter efficiënte algoritmes. Dit is meteen in scherp contrast met het factorisatie probleem over $\mathbb{Z}$. Hoewel we tot hiertoe veel analogieën gezien hebben tussen $\mathbb{Z}$ en $\mathbb{F}[x]$, en zeker wanneer $\mathbb{F} = \mathbb{Q}$, is het factorisatieprobleem over $\mathbb{Z}$ computationieel gezien vele malen moeilijker dan over $\mathbb{Q}[x]$. In de master cursus Computeralgebra is de studie van efficiënte algoritmen voor de factorisatie in $\mathbb{Q}[x]$ een klassiek hoofdstuk. In [17] is veel informatie te vinden.

Er bestaat in elk geval wel een vrij eenvoudig algoritme om na te gaan of een veelterm een lineaire factor, dwz. van de vorm $g(x) = a_1x + a_0$ $(a_1 \neq 0)$, bezit. Aangezien $a_1 \neq 0$ kunnen we de lineaire veelterm steeds in de vorm $x - \alpha$ brengen. Indien $f(x) = f_nx^n + f_{n-1}x^{n-1} + \dots + f_0$, dan zal voor elke α van $\mathbb{F}$, $f(\alpha) = f_n\alpha^n + f_{n-1}\alpha^{n-1} + \dots + f_0$ een element zijn van $\mathbb{F}$. Nu geldt de volgende zogenaamde *factorisatiestelling*.

Stelling 5.73

Veronderstel dat $\mathbb{F}$ een veld is en veronderstel dat $f(x)$ een veelterm is in $\mathbb{F}[x]$ dan is $x - \alpha$ een factor van $f(x)$ in $\mathbb{F}[x]$, dan en slechts dan als $f(\alpha) = 0$ in $\mathbb{F}$.

Bewijs. Veronderstel dat $x - \alpha$ een deler is van $f(x)$, dan is

$$f(x) = (x - \alpha)g(x).$$

Hieruit volgt echter dat

$$f(\alpha) = (x - \alpha)g(\alpha) = 0 \cdot g(\alpha) = 0.$$

Omgekeerd, veronderstel dat $f(\alpha) = 0$ in $\mathbb{F}$. Er bestaan veeltermen $q(x)$ en $r(x)$ in $\mathbb{F}[x]$ zodanig dat

$$f(x) = (x - \alpha)q(x) + r(x),$$

waarbij $r(x)$ een constante veelterm moet zijn. Aangezien echter

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha),$$

volgt hieruit dat $r(x)$ de nulveelterm is. Bijgevolg is $x - \alpha$ een deler van $f(x)$. □

Voor elke veelterm $f(x)$ van $\mathbb{F}[x]$ worden de elementen α van $\mathbb{F}$ waarvoor geldt dat $f(\alpha) = 0$, de *wortels* genoemd van de vergelijking $f(x) = 0$.

Stelling 5.74

Indien $\mathbb{F}$ een veld is en indien $f(x)$ een veelterm is van de graad n ($n \geq 1$) in $\mathbb{F}[x]$, dan bezit de vergelijking $f(x) = 0$ ten hoogste n wortels in $\mathbb{F}$.

Bewijs. Veronderstel dat de vergelijking m wortels $\alpha_1, \alpha_2, \ldots, \alpha_m$ bezit. Dan zal wegens de factorisatiestelling

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)g(x),$$

voor een zekere $g(x)$ in $\mathbb{F}[x]$. Aangezien de coëfficiënten tot een veld behoren, zal de graad van het product in het rechterlid de som van de graden van de factoren zijn. Hieruit volgt dat de graad van $f(x)$ ten minste m is, of gelijkwaardig hiermee dat het aantal wortels van $f(x) = 0$ ten hoogste n is. □

Zoals het bij de gehele getallen niet steeds eenvoudig is om een gegeven getal in priemfactoren te ontbinden, is het hier niet steeds eenvoudig om een gegeven veelterm handmatig te ontbinden in irreducibele factoren. Om de eventuele lineaire factoren van een veelterm $f(x)$ in $\mathbb{F}[x]$ te vinden, weten we dat we gewoon $f(\alpha)$ moeten uitrekenen waarbij α het veld $\mathbb{F}$ zal doorlopen. Indien dit veld een eindig aantal elementen bezit, dan hebben we op die manier een bruikbaar algoritme. Misschien heeft de veelterm $f(x)$ geen lineaire

factoren, in dit geval hebben we dus al de berekeningen voor niets gedaan. Niemand zegt echter dat er eventueel geen factoren van hogere graad kunnen optreden.

Oefening 5.75. *Zoek de irreducibele factoren van* $x^4 + 1$ *in* $\mathbb{Z}/3\mathbb{Z}[x]$.

Oplossing. We zoeken eerst de eventuele lineaire factoren. Stel $x^4 + 1 = f(x)$, dan is

$$f(0) = 1 \quad \text{en} \quad f(1) = f(2) = 2.$$

Er zijn bijgevolg geen lineaire factoren. Indien de veelterm dus reduciebel is, dan moet hij noodzakelijk het product zijn van twee irreducibele kwadratische veeltermen.

Bijgevolg geldt dan

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

met $a, b, c, d \in \mathbb{Z}/3\mathbb{Z}$. Aangezien

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd,$$

moeten a, b, c, d oplossingen zijn van het volgende stelsel over $\mathbb{Z}/3\mathbb{Z}$.

$$\begin{cases} a + c &= 0 \\ b + d + ac &= 0 \\ ad + bc &= 0 \\ bd &= 1. \end{cases}$$

Men vindt eenvoudig de volgende oplossingen $a = 1$ en $b = c = d = 2$ of $c = 1$ en $a = b = d = 2$(oefening). Beide oplossingen leiden tot dezelfde ontbinding in $\mathbb{Z}/3\mathbb{Z}[x]$, namelijk:

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2).$$

■

Opmerking

Alhoewel het zoeken naar een irreducibele veelterm in $\mathbb{F}[x]$ dus niet steeds eenvoudig is, kan men bewijzen dat in $\mathbb{Z}/p\mathbb{Z}[x]$ (p een priemgetal) steeds een irreducibele veelterm te vinden is voor elke graad n. Deze veeltermen zullen de bouwstenen vormen voor de constructie van de eindige velden.

Beschouw nu een willekeurig niet constant polynoom $m(x) \in F[x]$. Er is niets wat ons nog belet om aan modulaire aritmetiek te doen in de ring $\mathbb{F}[x]$. Alle definities uit Hoofdstuk 4 kunnen, mutatis mutandis, overgenomen worden. Vertrekkende van de veeltermring $\mathbb{F}[x]$ en $m(x)$, kunnen we nu opnieuw een ring construeren, namelijk de ring van alle polynomen modulo m. Wat zijn nu de eigenschappen van deze ring? We hebben gezien dat als p een priemgetal is, $\mathbb{Z}/p\mathbb{Z}$ een veld is. De essentiële reden is het bestaan van Bézoutcoëfficiënten, waarmee we een inverse konden bepalen van a modulo p. Maar, Stelling 5.69 biedt alle noodzakelijke ingrediënten om dit ook in $\mathbb{F}[x]$ mogelijk te maken.

De complexe getallen

We zullen deze manier van werken uitleggen aan de hand van een voorbeeld. De volledige theorie wordt uitgewerkt in een cursus Algebra. Stel $\mathbb{F} = \mathbb{R}$ en $m(x) = x^2+1$. De relatie modulo m is een equivalentierelatie. We noteren de verzameling van representanten van de equivalentieklassen als $\mathbb{R}[x]/\langle x^2+1\rangle$. In elke klasse kan een representant gekozen worden van de vorm $ax + b$, $a, b \in \mathbb{R}$, omdat de graad van de rest bij deling door $x^2 + 1$ hoogstens 1 is. Dus $\mathbb{R}[x]/\langle x^2 + 1\rangle = \{a + bx \| a, b \in \mathbb{R}\}$. De optelling en vermenigvuldiging in deze verzameling zijn op de gebruikelijke wijze gedefinieerd, in elk geval is onmiddellijk duidelijk dat $\mathbb{R}[x]/\langle x^2 + 1\rangle$ een commutatieve ring is.

Het is duidelijk dat $m(x)$ irreducibel is over $\mathbb{R}$. Stel $f \in \mathbb{R}[x] \setminus \{0\}$ is een willekeurig polynoom, dan geldt $\text{ggd}(f, m) = 1$. Er bestaan dus polynomen $a, b \in \mathbb{R}[x]$ waarvoor

$$a(x)f(x) + b(x)(x^2 + 1) = 1\,,$$

of nog, modulo $a(x)f(x) \pmod m = 1$. Met andere woorden, we vinden een element in $\mathbb{R}[x]/\langle x^2 + 1\rangle$ dat de inverse is van $f(x)$. Elk polynoom (behalve 0) heeft dus een inverse. M.a.w. deze structuur is niets anders dan een veld. Ook geldt dat $x^2 + 1 = 0 \pmod{x^2 + 1}$, of nog, $x^2 = -1$, dus we bekomen het veld der complexe getallen. De volgende stelling toont aan de $\mathbb{C}$ op deze wijze niet verder uitgebreid kan worden. Een bewijs wordt doorgaans in een cursus Analyse gegeven. Er bestaat ook een zuiver algebraïsch bewijs, dat gebruik maakt van Galoistheorie.

Stelling 5.76 — hoofdstelling van de algebra

Elke veelterm van graad $n \geq 1$ over $\mathbb{C}$ kan ontbonden worden in precies n lineaire factoren.

Een veld waarin deze eigenschap geldt, wordt *algebraïsch afgesloten* genoemd. Een *algebraïsche sluiting* van een veld $\mathbb{F}$ is een veld $\mathbb{K}$ zodat $\mathbb{F} \subseteq \mathbb{K}$ en $\mathbb{K}$ is algebraïsch gesloten. Ook de volgende stelling vermelden we zonder bewijs

Stelling 5.77

Voor elk veld bestaat er een algebraïsche sluiting.

Het veld der complexe getallen is echter geen geordend veld.

Stelling 5.78

Er bestaat geen orderelatie in $\mathbb{C}$ die voldoet aan de voorwaarden van Definitie 5.55.

Bewijs. Veronderstel dat $\preceq$ een totale orderelatie is over $\mathbb{C}$ die voldoet aan de voorwaarden van Definitie 5.55. Dan geldt $0 \preceq i$ of $i \preceq 0$. Veronderstel eerst dat $0 \preceq i$. Maar dan moet $0 \preceq i^2 = -1$, door de tweede voorwaarde, en door dezelfde voorwaarde geldt na vermenigvuldiging met -1, $0 \preceq 1$. Tellen we nu bij beide leden -1 op, dan volgt door de eerste voorwaarde $-1 \preceq 0$, een contradictie met het eerder gevonden $0 \preceq -1$. De veronderstelling $i \preceq 0$ leidt op analoge wijze tot een contradictie. □

5.7 Eindige velden

Definitie 5.79

Een *eindig veld* is een veld van eindige orde

Veronderstel dat $\mathbb{F}$ een veld is. Als $m \in \mathbb{Z}$ and $x \in \mathbb{F}$, dan kunnen we $m \cdot x$ gaan definiëren (zie sectie 5.2.4, opmerking op pagina 189).

Definitie 5.80

De *karakteristiek* p van een eindig veld is de orde van de additieve deelgroep voortgebracht door het element 1.

Lemma 5.81

Stel $\mathbb{F}$ is een eindig veld. Dan is de karakteristiek een priemgetal

Bewijs. Noteer p de karakteristiek van $\mathbb{F}$. Indien p geen priemgetal zou zijn, dan geldt $p = m_1 \cdot m_2$ met $2 \leq m_1$ en $2 \leq m_2$. We hebben dan dat

$$0 = p \cdot 1 = \underbrace{1 + \cdots + 1}_{p \text{ keer}} = (\underbrace{1 + \cdots + 1}_{m_1 \text{ keer}}) \cdot (\underbrace{1 + \cdots + 1}_{m_2 \text{ keer}}) \neq 0,$$

een tegenstrijdigheid. Bijgevolg is de karakteristiek van een eindig veld steeds een priemgetal. □

Lemma 5.82

De karakteristiek van een eindig veld $\mathbb{F}$ is het kleinste positief geheel getal p waarvoor geldt dat $p \cdot x = 0$, $\forall x \in \mathbb{F}$.

Bewijs. Voor elke $x \in \mathbb{F}$ en elke $m \in \mathbb{N}^*$ hebben we

$$m \cdot x = \underbrace{x + \cdots + x}_{m \text{ keer}} = (\underbrace{1 + \cdots + 1}_{m \text{ keer}}) \cdot x.$$

□

Voor $\mathbb{R}, +, \cdot$ en $\mathbb{C}, +, \cdot$ geldt dat:

$$m \cdot 1 = 1 \cdot m = 0 \Longleftrightarrow m = 0.$$

Van de lichamen en velden met deze eigenschap zegt men dat ze *karakteristiek* 0 bezitten. Ze hebben dan noodzakelijk een oneindige orde. Merk op dat er lichamen en velden van oneindige orde bestaan met een karakteristiek verschillend van 0. Dergelijke structuren komen in deze cursus niet aan bod.

Lemma 5.83

Een eindig veld heeft steeds orde p^h, p een priemgetal, $h \geq 1$.

Bewijs. Veronderstel dat F een eindig veld is. Dan heeft het karakteristiek p voor een zeker priemgetal p. We construeren een deelveld in F van orde p als volgt. Beschouw 1 in F en definieer $\psi : \mathbb{N} \to F$, $\psi(n) = n \cdot 1 := \underbrace{1 + \cdots + 1}_{n \text{ keer}}$. Omdat F karakteristiek p heeft, is $\psi(p) = 0$, dus $\text{im}(\psi) = \{\psi(k) : k \in \{0, 1, \ldots, p-1\}\}$. Men kan eenvoudig nagaan dat $\psi(x+y) = \psi(z) \iff x+y \equiv z \mod p$ en $\psi(xy) = \psi(z) \iff xy \equiv z \mod p$. Dus ψ induceert een isomorfisme van het veld $\mathbb{Z}/p\mathbb{Z}$ naar $\text{im}(\psi), +, \cdot$, met $+$ en $\cdot$ de bewerkingen in F. Het veld F is een G-vectorruimte en aangezien F eindig is, heeft het een eindige dimensie over G, stel $h \geq 1$. Het aantal elementen in F is het aantal elementen van F als vectorruimte over G en is dus gelijk aan p^h. □

Stelling 5.84 — Freshman's dream

In een veld F van karakteristiek p geldt voor alle elementen $a, b \in F$

$$(a+b)^p = a^p + b^p \,.$$

Bewijs. Het binomium van Newton levert de gekende uitdrukking $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. Beschouw nu $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Als $1 \leq i < p$ is $p - i \nmid p$ en $i \nmid p$ omdat p priem is. Dus $p \mid \binom{p}{i}$ omdat de teller $p!$ wel de factor p bevat. Dus $\binom{p}{i} = 0$ in F als $1 \leq i < p-1$, hetgeen het gestelde bewijst. □

5.7.1 Constructie van eindige velden

Stel $q = p^h$ met p een priemgetal, $h \geq 1$. Het is de bedoeling om voor elke dergelijke q een eindig veld van orde q te construeren, genoteerd als $\mathbb{F}_q$. Als $h = 1$, dan is het veld $\mathbb{F}_p$ per definitie $\mathbb{Z}/p\mathbb{Z}$. Veronderstel nu dat $h > 1$. Een eindig veld van de orde $q = p^h$ wordt als volgt geconstrueerd.

1. Zoek een veelterm $f(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ van de graad h die irreducibel is over $\mathbb{Z}/p\mathbb{Z}$.

2. Beschouw de restklassering $\mathbb{Z}/p\mathbb{Z}[t]/\langle f(t) \rangle$. We hebben gezien dat deze bestaat uit de verzameling

$$K = \{a_0 + a_1 t + a_2 t^2 + \cdots + a_{h-1} t^{h-1} \| a_i \in \mathbb{Z}/p\mathbb{Z}\}.$$

We kennen de optelling en vermenigvuldiging, deze zijn namelijk overgenomen uit $\mathbb{Z}/p\mathbb{Z}[t]$ en worden in K enkel modulo $f(t)$ uitgevoerd, m.a.w.

$$(a_0 + a_1 t + a_2 t^2 + \cdots + a_{h-1} t^{h-1}) + (b_0 + b_1 t + b_2 t^2 + \cdots + b_{h-1} t^{h-1}) = (a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2 + \cdots + (a_{h-1} + b_{h-1})t^{h-1}.$$

En voor de vermenigvuldiging geldt dat indien $a(t)$ en $b(t)$ elementen zijn van K, dan is $a(t)b(t)$ in K het element $r(t)$ zodanig dat

$$a(t)b(t) = f(t)q(t) + r(t).$$

Wegens stelling 5.65 is $r(t)$ uniek bepaald.

De elementen van K kunnen dus ook voorgesteld worden als h tupels $(a_0, a_1, \ldots, a_{h-1})$ zodat K inderdaad p^h elementen bevat. We hebben gezien in Sectie 5.6.2 dat deze constructie een veld is als $f(t)$ irreducibel is. Het volgende lemma vermelden we zonder bewijs.

Lemma 5.85

Stel dat F een eindig veld is van orde q. Voor elke gegeven $h \geq 1$ bestaat er steeds een irreducibel polynoom $f(t)$ over F van graad h.

Voor een gegeven $q = p^h$, kunnen we dus steeds een veld van orde q construeren. Maar bovenstaand lemma garandeert ook dat we een veld van orde q steeds kunnen uitbreiden naar een veld van orde q^h. We hoeven dus niet steeds van een veld van priemorde te starten.

De volgende stelling vermelden we ook zonder bewijs.

Stelling 5.86

Stel $q = p^h$, p een priemgetal, $h \geq 1$. Op isomorfisme na bestaat er slechts één veld van de orde q.

De constructie maakt gebruik van een irreducibele veelterm $f(t)$ over $\mathbb{Z}/p\mathbb{Z}$. Aangezien we weten dat er op een isomorfisme na slechts één eindig veld van de orde $q = p^h$ bestaat, zal het geen belang hebben welke irreducibele polynoom $f(t)$ van de graad h in $\mathbb{Z}/p\mathbb{Z}[t]$ we gebruiken. We noteren een eindig veld van orde q als $\mathbb{F}_q$.

Merk op dat t steeds element is van $\mathbb{F}_q$, maar niet noodzakelijk een primitief element. Elke veelterm $f(t)$ van de graad h die irreducibel is over $\mathbb{Z}/p\mathbb{Z}$ en zodanig dat t primitief element is van het veld van de orde p^h dat door middel van $f(t)$ wordt geconstrueerd, noemen we een *primitieve* veelterm.

Stelling 5.87

Indien $\mathbb{F}_q$ een eindig veld is met karakteristiek p, dan is de groep $\mathbb{F}_q^*, \cdot$ een cyclische groep van de orde $q-1$.

Bewijs. De multiplicatieve groep $\mathbb{F}_q^*$ is dus van de orde $q-1$ zodat voor een willekeurig element f van deze groep geldt dat $f^{q-1}=1$. Bijgevolg bezit de vergelijking $x^{q-1}-1=0$ juist $q-1$ wortels in $\mathbb{F}_q^*$. We bewijzen nu dat deze groep aan de karakterisatiestelling 5.39 voor cyclische groepen voldoet. In het bijzonder zullen we bewijzen dat er voor elke deler d van $q-1$ juist d elementen f bestaan in $\mathbb{F}_q^*$ waarvoor $f^d=1$.

Veronderstel dat $q-1=dk$, dan geldt in $\mathbb{F}_q[x]$:

$$x^{q-1}-1=(x^d-1)(x^{d(k-1)}+x^{d(k-2)}+\cdots+x^d+1).$$

Stel

$$g(x)=x^{d(k-1)}+x^{d(k-2)}+\cdots+x^d+1.$$

Aangezien $g(x)$ een veelterm is van de graad $d(k-1)$ bezit de vergelijking $g(x)=0$ ten hoogste $d(k-1)$ wortels in $\mathbb{F}_q^*$. Analoog bezit de vergelijking $x^d-1=0$ ten hoogste d wortels in $\mathbb{F}_q^*$. Aangezien echter $x^{q-1}-1=0$ juist $q-1$ wortels bezit in $\mathbb{F}_q^*$ en aangezien $d(k-1)+d=q-1$ volgt hieruit dat $x^d-1=0$ juist d wortels bezit. Dit is wegens stelling 5.39 voldoende om te besluiten dat $\mathbb{F}_q^*$ een cyclische groep is van de orde $q-1$. □

5.7.2 Voorbeelden van eindige velden

$\mathbb{F}_4$

1. We zoeken een veelterm $f(t)\in\mathbb{Z}/2\mathbb{Z}[t]$ van de graad 2 die irreducibel is over $\mathbb{Z}/2\mathbb{Z}$. De veelterm $f(t)=t^2+t+1$ voldoet hieraan.
2. $K=\mathbb{F}_4=\{a_0+a_1t \| a_i\in\mathbb{Z}/2\mathbb{Z}\}=\{0,1,t,1+t\}$.
3. De multiplicatieve groep is $\{1,t,t+1\},\cdot$. Omdat $t^2=t+1$, is t inderdaad een generator van deze groep.

De Cayley tabellen voor de optelling en de vermenigvuldiging zien er als volgt uit:

$+$	0	1	t	$1+t$
0	0	1	t	$1+t$
1	1	0	$1+t$	t
t	t	$1+t$	0	1
$1+t$	$1+t$	t	1	0

$\cdot$	1	t	$1+t$
1	1	t	$1+t$
t	t	$1+t$	1
$1+t$	$1+t$	1	t

$\mathbb{F}_8$

De veelterm t^3+t+1 is van de graad 3 en irreducibel over $\mathbb{Z}/2\mathbb{Z}$. Deze veelterm kan dus gebruikt worden om $\mathbb{F}_8$ te construeren.

Bijgevolg is $\mathbb{F}_8 = \{0, 1, t, 1+t, t^2, 1+t^2, t+t^2, 1+t+t^2\}$.

De Cayley tabellen voor de optelling en de vermenigvuldiging zijn respectievelijk:

$+$	0	1	t	$1+t$	t^2	$1+t^2$	$t+t^2$	$1+t+t^2$
0	0	1	t	$1+t$	t^2	$1+t^2$	$t+t^2$	$1+t+t^2$
1	1	0	$1+t$	t	$1+t^2$	t^2	$1+t+t^2$	$t+t^2$
t	t	$1+t$	0	1	$t+t^2$	$1+t+t^2$	t^2	$1+t^2$
$1+t$	$1+t$	t	1	0	$1+t+t^2$	$t+t^2$	$1+t^2$	t^2
t^2	t^2	$1+t^2$	$t+t^2$	$1+t+t^2$	0	1	t	$1+t$
$1+t^2$	$1+t^2$	t^2	$1+t+t^2$	$t+t^2$	1	0	$1+t$	t
$t+t^2$	$t+t^2$	$1+t+t^2$	t^2	$1+t^2$	t	$1+t$	0	1
$1+t+t^2$	$1+t+t^2$	$t+t^2$	$1+t^2$	t^2	$1+t$	t	1	0

$\cdot$	1	t	$1+t$	t^2	$1+t^2$	$t+t^2$	$1+t+t^2$
1	1	t	$1+t$	t^2	$1+t^2$	$t+t^2$	$1+t+t^2$
t	t	t^2	$t+t^2$	$1+t$	1	$1+t+t^2$	$1+t^2$
$1+t$	$1+t$	$t+t^2$	$1+t^2$	$1+t+t^2$	t^2	1	t
t^2	t^2	$1+t$	$1+t+t^2$	$t+t^2$	t	$1+t^2$	1
$1+t^2$	$1+t^2$	1	t^2	t	$1+t+t^2$	$1+t$	$t+t^2$
$t+t^2$	$t+t^2$	$1+t+t^2$	1	$1+t^2$	$1+t$	t	t^2
$1+t+t^2$	$1+t+t^2$	$1+t^2$	t	1	$t+t^2$	t^2	$1+t$

Opmerking

Aangezien de orde van de multiplicatieve groep (C_7) een priemgetal is, is elk element (verschillend van 0 en 1) van $\mathbb{F}_8$ een primitief element.

$\mathbb{F}_9$

De veelterm t^2+1 is van de graad 2 en irreducibel over $\mathbb{Z}/3\mathbb{Z}$.

Dus $\mathbb{F}_9 = \{0, 1, -1, t, -t, 1+t, 1-t, -1+t, -1-t\}$. De Cayley tabel voor de optelling laten we hier voor de eenvoud weg. Deze voor de vermenigvuldiging is:

$\cdot$	1	-1	t	$-t$	$1+t$	$1-t$	$-1+t$	$-1-t$
1	1	-1	t	$-t$	$1+t$	$1-t$	$-1+t$	$-1-t$
-1	-1	1	$-t$	t	$-1-t$	$-1+t$	$1-t$	$1+t$
t	t	$-t$	-1	1	$-1+t$	$1+t$	$-1-t$	$1-t$
$-t$	$-t$	t	1	-1	$1-t$	$-1-t$	$1+t$	$-1+t$
$1+t$	$1+t$	$-1-t$	$-1+t$	$1-t$	$-t$	-1	1	t
$1-t$	$1-t$	$-1+t$	$1+t$	$-1-t$	-1	t	$-t$	1
$-1+t$	$-1+t$	$1-t$	$-1-t$	$1+t$	1	$-t$	t	-1
$-1-t$	$-1-t$	$1+t$	$1-t$	$-1+t$	t	1	-1	$-t$

Oefening 5.88. *Gegeven zijn de 2 veeltermen in de onbepaalde variabele x in het veld $\mathbb{F}_9$:*

$$f(x) = x^3 + tx^2 - x - 1 - t \qquad en \qquad g(x) = tx^2 + x - t.$$

We berekenen het product $f(x) \cdot g(x)$ door gebruik te maken van de bewerkingstabellen van $\mathbb{F}_9$.

Oplossing.

$$\begin{aligned} f(x)\cdot g(x) &= (x^3 + tx^2 - x - 1 - t)\cdot(tx^2 + x - t) \\ &= tx^5 + (1+t^2)x^4 + (-t+t-t)x^3 + (-t^2 - 1 + t(-1-t))x^2 \\ &\qquad +(-t-1+t)x - t(-1-t) \\ &= tx^5 - tx^3 + (-t+1)x^2 - x + t - 1. \end{aligned}$$

■

Opmerkingen

1. De gekozen veelterm $f(t) = t^2 + 1$ is geen primitieve veelterm want $t^4 = 1$ zodat t de cyclische deelgroep van de orde 4 voortbrengt ipv. de

ganse groep. Het element $t+1$ is wel een primitief element, want stel $1+t=\alpha$, dan volgt onmiddellijk dat

$$\begin{aligned}
\alpha^2 &= -t \\
\alpha^3 &= 1-t \\
\alpha^4 &= -1 \\
\alpha^5 &= -1-t \\
\alpha^6 &= t \\
\alpha^7 &= -1+t \\
\alpha^8 &= 1.
\end{aligned}$$

2. Veronderstel dat $a_0+a_1t+a_2t^2+\cdots+a_{h-1}t^{h-1}$, of kortweg $(a_0,a_1,a_2,\cdots,a_{h-1})$, een willekeurig element is van het veld $\mathbb{F}_{p^h}$. Deze voorstelling is handig aangezien de optelling in $\mathbb{F}_q$, precies de optelling van vectoren is. Deze voorstelling is echter niet handig voor de multiplicatieve bewerking. Anderzijds weten we dat de multiplikatieve groep van $\mathbb{F}_q$ een cyclische groep is, en dat dus elk element verschillend van 0 kan voorgesteld worden in de vorm α^i, met α een primitief element van $\mathbb{F}_q$. Deze voorstelling is handig voor de multiplicatieve bewerking, maar is op zijn beurt nadelig voor de additieve bewerking. Daarom kan men steeds bij gebruik van de multiplicatieve notatie een aantal definiërende relaties meegeven die de bewerkingen vereenvoudigen.

Voorbeeld 5.89.

(a) $\mathbb{F}_4=\{0,1,\alpha,\alpha^2\|2=\alpha^2+\alpha+1=\alpha^3+1=0\}$.

(b) $\mathbb{F}_8=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\|2=\alpha^3+\alpha^2+1=\alpha^5+\alpha+1=\alpha^6+\alpha^4+1=\alpha^7+1=0\}$.

(c) $\mathbb{F}_9=\{0,\pm1,\pm\alpha,\pm\alpha^2,\pm\alpha^3\|3=\alpha^3+\alpha-1=\alpha^2-\alpha-1=\alpha^3+\alpha^2+1=\alpha^4+1=0\}$.

Het komt er dus op aan om bij gebruik van de multiplicatieve notatie, volgende functie θ te kennen:

$$\begin{array}{rccl}
\theta: & \{0,1,2,\cdots,q-2,\dagger\} & \longrightarrow & \{0,1,2,\cdots,q-2,\dagger\} \\
 & i & \longmapsto & j \Longleftrightarrow \alpha^j=\alpha^i+1.
\end{array}$$

Met de afspraak dat $\alpha^\dagger=0$. Men kan dan gebruik maken van de volgende formule:

$$\begin{aligned}
\alpha^a+\alpha^b &= \alpha^b(\alpha^{(a-b)}+1) \\
&= \alpha^b\cdot\alpha^{\theta(a-b)} \\
&= \alpha^{\theta(a-b)+b}.
\end{aligned}$$

De functie θ wordt soms de Zech log-functie of kortweg de log-functie van het veld $\mathbb{F}_q$ genoemd, zo is bvb. voor $\mathbb{F}_8$ met $\alpha^3 = \alpha + 1$ de log-functie af te lezen uit de volgende tabel:

i	$\theta(i)$
0	†
1	3
2	6
3	1
4	5
5	4
6	2
†	0

Merk op dat inderdaad $\alpha^0 + 1 = 0$. Merk ook op dat voor velden van even karakteristiek, deze log-functie een involutie is (dwz. $\theta^2 = 1$), zodat slechts de helft van de log-tabel dient opgegeven te worden. Ook als de karakteristiek oneven is, moeten niet alle beelden onder de Zech-log-functie berekend worden (zie oefeningen).

5.7.3 Enkele belangrijke stellingen

Stelling 5.90

Elk element van $\mathbb{F}^*_{2^h}$ is een kwadraat, terwijl juist de helft van het aantal elementen van $\mathbb{F}^*_{p^h}$, met $p \neq 2$, een kwadraat is.

Bewijs. Veronderstel dat α een primitief element is van $\mathbb{F}_q$. Elk element van de vorm α^{2m} is uiteraard een kwadraat. Veronderstel dat q even is, dan is

$$\alpha^{2m+1} = \alpha^{2m+1}\alpha^{q-1} = \alpha^{2m+q}.$$

Aangezien $2m+q$ in dit geval even is, zullen ook de elementen α^{2m+1} kwadraten zijn. Bijgevolg, indien q even is, zullen al de elementen van $\mathbb{F}_q$ verschillend van 0 een kwadraat zijn.

Veronderstel dat q oneven is en dat een element α^{2m+1} een kwadraat is. Stel bijvoorbeeld dat $\alpha^{2m+1} = \beta^2$. Aangezien echter α een primitief element is, bestaat er een natuurlijk getal k zodanig dat $\beta = \alpha^k$. Bijgevolg is

$$\alpha^{2(m-k)+1} = \alpha^{2m+1}\alpha^{-2k} = \alpha^{2m+1}(\beta^2)^{-1} = 1.$$

Aangezien de orde van de multiplicatieve groep gelijk is aan $q-1$, moet dus $2(m-k)+1$ een veelvoud zijn van $q-1$. Dit is onmogelijk als q oneven is. Indien q oneven is, dan zijn er dus $(q-1)/2$ kwadraten verschillend van nul. □

Opmerking

Deze stelling is zeer eenvoudig te controleren in de bovenstaande vermenigvuldigingstabellen.

We zien dat inderdaad voor $\mathbb{F}_4^*$ en $\mathbb{F}_8^*$ elk element juist 1 maal voorkomt op de diagonaal.

Anderzijds blijkt uit de vermenigvuldigingstabel van $\mathbb{F}_9^*$, dat ± 1 en $\pm t$ de 4 kwadraten zijn van de multiplicatieve groep.

Merk op dat in dit veld -1 een kwadraat is. We hebben in stelling 4.45 gezien dat -1 een kwadraat is in $\mathbb{Z}/p\mathbb{Z}$, p oneven, dan en slechts dan als $p \equiv 1 \pmod 4$. Deze eigenschap kan veralgemeend worden voor een algemeen eindig veld $\mathbb{F}_q$, q oneven.

Stelling 5.91

In $\mathbb{F}_q$, q oneven, is -1 een kwadraat dan en slechts dan als $q \equiv 1 \pmod 4$.

Bewijs. We bewijzen eerst dat

$$\alpha^{\frac{q-1}{2}} = -1$$

met α een primitief element van $\mathbb{F}_q$. Merk eerst op dat de vergelijking $x^2 = 1$ juist 2 oplossingen bezit in $\mathbb{F}_q$ want $\mathbb{F}_q^*$ is een cyclische groep van even orde $q-1$ en wegens stelling 5.39 bezit een vergelijking $x^d = 1$,voor elke deler d van $q-1$, juist d oplossingen. De oplossingen van de vergelijking $x^2 = 1$ zijn uiteraard 1 en -1. Aangezien echter α de orde $q-1$ bezit, zal $\alpha^{q-1} = 1$ en moet dus $\alpha^{\frac{q-1}{2}} = -1$. Aangezien echter -1 een kwadraat is, moet $\frac{q-1}{2}$ even zijn, dus moet $\frac{q-1}{2} = 2m$ of $q = 4m+1$. □

Stelling 5.92

In $\mathbb{F}_q$, q oneven, is elk element te schrijven als de som van 2 kwadraten

Bewijs. Beschouw de verzameling K van de elementen in $\mathbb{F}_q$ die een kwadraat zijn, inclusief 0. Dan is $|K| = \frac{q+1}{2}$, wegens Stelling 5.90. We beschouwen nu de additieve groep $\mathbb{F}_q, +$. Wegens Stelling 5.31 geldt $\mathbb{F}_q = K + K$, m.a.w. elk element is te schrijven als de som van twee elementen uit K. □

5.7.4 Kwadratische vergelijkingen

Uit de eigenschappen van een veld volgt onmiddellijk dat elke lineaire vergelijking van de vorm $ax = b$, met a en b elementen van een (eindig) veld en x de onbepaalde, juist 1 oplossing bezit, namelijk $x = a^{-1}b$. Het oplossen van lineaire vergelijkingen levert met andere woorden voor eindige velden geen extra moeilijkheden op. Anders is het gesteld met het oplossen van kwadratische vergelijkingen. Hier moet duidelijk een onderscheid gemaakt worden tussen even en oneven karakteristiek. Merk eerst en vooral op dat de kwadratische vergelijking $ax^2 + bx + c = 0$ ten hoogste 2 oplossingen bezit.

1. Veronderstel dat de karakteristiek p van het eindig veld oneven is. In dit geval gebeuren de berekeningen zoals voor het veld van de reële getallen.

   Met andere woorden, we noemen $\Delta = b^2 - 4ac$ de discriminant van de kwadratische vergelijking $ax^2 + bx + c = 0$ ($a \neq 0$).

   Als $\Delta = 0$, dan heeft de vergelijking juist 1 oplossing, namelijk

   $$x = -\frac{b}{2a}.$$

   Als $\Delta \neq 0$ en geen kwadraat is, dan heeft de kwadratische vergelijking geen enkele oplossing.

   Als $\Delta = d^2$ ($d \in \mathbb{F}_q^*$), dan heeft de kwadratische vergelijking juist 2 oplossingen

   $$\frac{-b \pm d}{2a}.$$

2. Veronderstel dat de karakteristiek p van het veld 2 is. Stel $q = 2^h$. We mogen veronderstellen dat $a \neq 0$ en dat $c \neq 0$.

   Als $b = 0$, dan heeft de vergelijking $ax^2 + c = 0$ als enige oplossing

   $$x = \sqrt{\frac{c}{a}}$$

(merk op dat $\dfrac{c}{a}$ steeds een kwadraat is).

Veronderstel $b \neq 0$, stel

$$y = \frac{ax}{b} \qquad \text{en} \qquad \delta = \frac{ac}{b^2},$$

dan herleidt de vergelijking $ax^2 + bx + c = 0$ zich tot $y^2 + y + \delta = 0$ die we de gereduceerde vergelijking zullen noemen. Met elke oplossing van de ene correspondeert juist 1 oplossing van de andere. Het is onmiddellijk duidelijk dat we nu niet meer op dezelfde manier zoals voor de oneven karakteristiek, de discriminant kunnen definiëren. Aangezien bovendien in dit geval elk element een kwadraat is, moet een andere bespreking gebruikt worden.

Merk vooreerst op dat als s een oplossing is van de vergelijking $y^2 + y + \delta = 0$, dan $s + 1$ eveneens een oplossing is van deze vergelijking.

Definieer nu

$$\mathrm{Tr}(z) = z + z^2 + z^4 + \cdots + z^{2^{h-1}}.$$

We noemen $\mathrm{Tr}(z)$ het *spoor* (in het Engels *trace*) van het element z. Dan is

$$\mathrm{Tr}(z)^2 + \mathrm{Tr}(z) = 0, \quad \forall z \in \mathbb{F}_q.$$

Bijgevolg is in het bijzonder $\mathrm{Tr}(\delta) = 0$ of $\mathrm{Tr}(\delta) = 1$.

Veronderstel dat $\mathrm{Tr}(\delta) = 0$ en dat k een element is van $\mathbb{F}_q$ waarvoor $\mathrm{Tr}(k) = 1$. Dan heeft de vergelijking $y^2 + y + \delta = 0$ de volgende oplossing:

$$s = k\delta^2 + (k + k^2)\delta^4 + \cdots + (k + k^2 + k^4 + \cdots + k^{2^{h-2}})\delta^{2^{h-1}}.$$

Inderdaad:

$$\begin{aligned} s^2 \;=\; & k^2\delta^4 + (k^2 + k^4)\delta^8 + \cdots + (k^2 + k^4 + \cdots + k^{2^{h-2}})\delta^{2^{h-1}} \\ & + (k^2 + k^4 + \cdots + k^{2^{h-1}})\delta^{2^h}. \end{aligned}$$

Aangezien

$$\mathrm{Tr}(k) = k + k^2 + k^4 + \cdots + k^{2^{h-1}} = 1 \quad \text{en} \quad \delta^{2^h} = \delta,$$

is

$$(k^2 + k^4 + \cdots + k^{2^{h-1}})\delta^{2^h} = (1 + k)\delta,$$

zodat

$$s^2 = (1 + k)\delta + k^2\delta^4 + (k^2 + k^4)\delta^8 + \cdots + (k^2 + k^4 + \cdots k^{2^{h-2}})\delta^{2^{h-1}}.$$

Dus,

$$\begin{aligned} s + s^2 &= (1+k)\delta + k\delta^2 + k\delta^4 + \cdots + k\delta^{2^{h-1}} \\ &= \delta + k(\delta + \delta^2 + \delta^4 + \cdots + \delta^{2^{h-1}}) \\ &= \delta + k\mathrm{Tr}(\delta) \\ &= \delta. \end{aligned}$$

Bijgevolg als $\mathrm{Tr}(\delta) = 0$, dan heeft $y^2 + y + \delta = 0$ twee verschillende oplossingen (s en $s+1$).

Omgekeerd, veronderstel dat s, en dus ook $s+1$, een oplossing is van de vergelijking $y^2 + y + \delta = 0$.

Dan geldt maw. dat $s + s^2 = \delta$. En dan is

$$\begin{aligned} \mathrm{Tr}(\delta) &= s + s^2 + (s+s^2)^2 + (s+s^2)^4 + \cdots + (s+s^2)^{2^{h-1}} \\ &= s + s^2 + s^2 + s^4 + s^4 + s^8 + s^8 + \cdots + s^{2^{h-1}} + s^{2^{h-1}} + s^{2^h} \\ &= s + s^{2^h} \\ &= 0. \end{aligned}$$

Bijgevolg mogen we besluiten dat de kwadratische vergelijking $ax^2 + bx + c = 0$ juist twee verschillende oplossingen bezit dan en slechts dan als

$$\mathrm{Tr}(\frac{ac}{b^2}) = 0.$$

Opmerkingen

1. Veronderstel dat q even is, dan is $\mathbb{F}_q = \mathcal{C}_0 \cup \mathcal{C}_1$ waarbij

$$\mathcal{C}_0 = \{t \in \mathbb{F}_q \| \mathrm{Tr}(t) = 0\}$$

en

$$\mathcal{C}_1 = \{t \in \mathbb{F}_q \| \mathrm{Tr}(t) = 1\}.$$

De elementen van $\mathcal{C}_0$ worden de elementen van categorie 0 genoemd, terwijl de elementen van $\mathcal{C}_1$ de elementen van categorie 1 genoemd worden.

Men toont dan eenvoudig aan dat

(a) $0 \in \mathcal{C}_0$

(b) $q = 2^{2m} \Longrightarrow 1 \in \mathcal{C}_0$

(c) $q = 2^{2m+1} \Longrightarrow 1 \in \mathcal{C}_1$

(d) $s \in \mathcal{C}_i,\ t \in \mathcal{C}_j \quad (i,j \in \{0,1\}) \Longrightarrow \begin{cases} s+t \in \mathcal{C}_0 & \text{als} \quad i = j \\ s+t \in \mathcal{C}_1 & \text{als} \quad i \neq j \end{cases}$

(e) $|\mathcal{C}_0| = |\mathcal{C}_1| = \frac{q}{2}$.

2. Als $q = 2^{2m+1}$, dan is $1 \in \mathcal{C}_1$ en bijgevolg heeft de vergelijking $y^2 + y + \delta = 0$, in de veronderstelling dat $\mathrm{Tr}(\delta) = 0$, als oplossing (stel $k = 1$):

$$\begin{aligned} s &= \delta^2 + \delta^{2^3} + \cdots + \delta^{2^{2m-1}} \\ &= s + \mathrm{Tr}(\delta) \\ &= \delta + \delta^{2^2} + \delta^{2^4} + \cdots + \delta^{2^{2m}}. \end{aligned}$$

Voorbeeld 5.93. We lossen de volgende kwadratische vergelijking op in $\mathbb{F}_8$.

$$tx^2 + (t^2 + t + 1)x + t + 1 = 0.$$

We brengen deze vergelijking eerst in de gereduceerde gedaante. Daartoe vermenigvuldigen we met t, delen we door $(t^2 + t + 1)^2$ en stellen we

$$\frac{tx}{t^2 + t + 1} = y.$$

Op die manier verkrijgen we de vergelijking:

$$y^2 + y + \frac{t(t+1)}{(t^2 + t + 1)^2} = 0.$$

Bijgevolg is

$$\delta = \frac{t(t+1)}{(t^2 + t + 1)^2} = \frac{t(t+1)}{t+1} = t.$$

We berekenen nu $\mathrm{Tr}(\delta) = \mathrm{Tr}(t)$.

$$\begin{aligned} \mathrm{Tr}(t) &= t + t^2 + t^4 \\ &= t + t^2 + t + t^2 \\ &= 0. \end{aligned}$$

Bijgevolg heeft de gegeven vergelijking juist 2 verschillende oplossingen. Aangezien $8 = 2^3$, is 1 een element uit $\mathcal{C}_1$ en is een oplossing van de gereduceerde vergelijking gegeven door

$$s = \delta^2 = t^2.$$

De gereduceerde vergelijking bezit met andere woorden de 2 oplossingen $y_1 = s = t^2$ en $y_2 = s + 1 = t^2 + 1$. De beide oplossingen van de oorspronkelijke vergelijking zijn dan:

$$\begin{aligned} x_1 &= \frac{(t^2+t+1)y_1}{t} = \frac{(t^2+t+1)t^2}{t} = (t^2+t+1)t = 1+t^2 \\ x_2 &= \frac{(t^2+t+1)y_2}{t} = \frac{(t^2+t+1)(t^2+1)}{t} = (t^2+t+1)(t^2+1)(t^2+1) \\ &= (t^2+t+1)(t^2+t+1) = t+1. \end{aligned}$$

De veelterm $tx^2 + (t^2+t+1)x + t + 1$ is bijgevolg reducibel over $\mathbb{F}_8$ en te schrijven als $t(x+t^2+1)(x+t+1)$.

5.8 Permutatiegroepen

We beschouwen een verzameling X van n elementen. Zonder de algemeenheid te schaden, mogen we veronderstellen dat $X = \{1, 2, \ldots, n\}$. Een *permutatie* van X is een bijectie van X op zichzelf. Uit deze definitie volgt onmiddellijk dat de samenstelling van twee permutaties dus weer een permutatie is. Dus als S_n de verzameling van alle permutaties van X voorstelt, dan is $S_n, \circ$, met $\circ$ de samenstelling, een groep. In het vervolg laten we de groepsbewerking vallen in de notatie, dus S_n is de groep van alle permutaties op n elementen. Elke deelgroep van S_m wordt ook een *permutatiegroep* genoemd. Een deelgroep van S_n van de orde m wordt een *permutatiegroep van de orde m* genoemd.

Elk element f van S_n kan dus beschreven worden door een stelsel van n betrekkingen van de vorm $f(i) = j \in \{1, 2, \ldots, n\}$ met $f(i_1) \neq f(i_2) \iff i_1 \neq i_2$. Zo is bijvoorbeeld de permutatie f gedefinieerd door

$$f(1) = 2, \quad f(2) = 4, \quad f(3) = 5, \quad f(4) = 1, \quad f(5) = 3,$$

een permutatie van $\{1, 2, 3, 4, 5\}$.

Het is gebruikelijk om een kortere notatie voor dergelijke permutaties te gebruiken. Zo zal in ons voorbeeld de permutatie f het element 1 afbeelden op 2, 2 afbeelden op 4 en 4 terug afbeelden op 1. We zeggen daarom dat 1,2 en 4 een *cykel van lengte* 3 definiëren. Aangezien anderzijds 3 op 5 afgebeeld wordt en 5 terug op 3, kunnen we zeggen dat 3 en 5 een cykel van lengte 2 definiëren. We kunnen daarom f verkort noteren in de zogenaamde *cykelvoorstelling*:

$$f = (1\ 2\ 4)(3\ 5).$$

Algemeen zal een element f van S_n op de volgende manier in cykelvoorstelling geschreven kunnen worden.

> We beginnen met een willekeurig element van $\{1, 2, \ldots, n\}$ (bijvoorbeeld het element 1, maar de keuze is vrij). We schrijven na dit element het beeld onder f en vervolgens het beeld van dit element onder f, en zo verder tot we terug bij het eerste element (hier 1) terugkomen. Op die manier hebben we een cykel van lengte k_1. Indien nog niet al de elementen in de cykel opgenomen zijn, dan kiezen we een willekeurig element dat we nog niet hebben opgenomen en we herhalen de procedure, op die manier ontstaat een tweede cykel van lengte k_2. We herhalen deze procedure tot wanneer we al de elementen van $\{1, 2, \ldots, n\}$ opgenomen hebben. Indien een element van $\{1, 2, \ldots, n\}$ door f gefixeerd wordt, dan schrijven we dit als een cykel van lengte 1.

Zo zullen bijvoorbeeld de 6 elementen van S_3 de volgende cykelvoorstelling bezitten

$$(1)(2)(3), \quad (1\ 2\ 3), \quad (1\ 3\ 2), \quad (1)(2\ 3), \quad (2)(1\ 3), \quad (3)(1\ 2).$$

Definitie 5.94

Beschouw een cykel $\sigma = (x_1\ x_2\ \ldots\ x_r) \in S_n$. De *baan* van σ is de verzameling $\{x_1, x_2, \ldots, x_r\}$. Twee cykels zijn *disjunct* als hun banen disjuncte verzamelingen zijn.

In feite hebben we het volgende lemma bewezen in de uitwerking van de cykelnotatie voor permutaties.

Lemma 5.95

Elke permutatie kan geschreven worden als de samenstelling van disjuncte cykels. Op de volgorde van de cykels en de notatie van de cykels na, is deze samenstelling uniek.

De samenstelling in S_n wordt vaak ook op multiplicatieve wijze genoteerd, met weglating van $\cdot$. De actie van een permutatie op een element wordt

vaak exponentieel genoteerd: $1^{(1\,2)} = 2$. Gebruiken we de exponentiële notatie in combinatie met de multiplicatieve, dan ligt de interpretatie van de volgorde voor de hand. Stel bijvoorbeeld dat $f, g \in S_n$, dan is $1^{fg} = (1^f)^g$, dus fg is de permutatie die ontstaat door **eerst** f uit te voeren en dan g. Met andere woorden: $fg = g \circ f$. Het gebruik van $\circ$ in trouwens volledig in overeenstemming met de functionele notatie: $g \circ f(1) = g(f(1))$. De samenstelling/vermenigvuldiging in S_n is niet commutatief, er bestaan echter wel permutaties die commuteren, i.e. $ab = ba$. Bekijken we bijvoorbeeld de permutaties (1 2) en (3 4) dan is duidelijk (1 2)(3 4) = (3 4)(1 2).

We bekijken opnieuw de symmetriegroep van een gelijkzijdige driehoek uit Voorbeeld 5.11. Elke symmetrie is volledig bepaald als we weten welk hoekpunt op welk hoekpunt afgebeeld wordt. Aldus is een symmetrie ook voor te stellen als een permutatie op drie elementen. We nummeren a, b en c als respectievelijk 1, 2 en 3,

We hebben S_3 bij de voorbeelden van groepen reeds beschreven als de groep van de symmetrieën van de gelijkzijdige driehoek abc. Het is duidelijk dat θ, zoals hieronder gedefinieerd, een isomorfisme is tussen de beide voorstellingen van dezelfde groep S_3.

$$\begin{aligned}
\theta(e) &= (1)(2)(3) \\
\theta(\rho) &= (1\ 2\ 3) \\
\theta(\rho^2) &= (1\ 3\ 2) \\
\theta(\sigma_a) &= (1)(2\ 3) \\
\theta(\sigma_b) &= (2)(1\ 3) \\
\theta(\sigma_c) &= (3)(1\ 2).
\end{aligned}$$

Merk op dat de volgorde van de cykels in een cykelvoorstelling van een permutatie geen rol speelt, bovendien hebben we voor elke cykel de keuze van het eerste element (nadien ligt alles vast). In ons voorbeeld van S_3 is bijvoorbeeld

$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2) \quad \text{maar} \quad (1\ 2\ 3) \neq (1\ 3\ 2).$$

Bovendien is

$$(1)(2\ 3) = (2\ 3)(1).$$

Soms worden de cykels van lengte 1 wel eens weggelaten, maar in dit geval moet wel steeds duidelijk vermeld worden over welke verzameling de permutatie beschouwd wordt. Zo kunnen we de permutatie (1)(2 3) ook voorstellen door de permutatie (2 3) die werkt op de verzameling $\{1, 2, 3\}$.

Merk op dat voor de samenstelling $\circ$ van permutaties, de gewone rekenregels voor de samenstelling van relaties gelden. In het bijzonder moet $f_1 \circ f_2$

gelezen worden als "f_1 na f_2" (de samenstelling moet dus van rechts naar links uitgevoerd worden). Zo zal de permutatie (1 2 3) het element 1 afbeelden op 2 en zal de permutatie (1)(2 3) het element 2 afbeelden op 3, zodat in de samenstelling (1)(2 3) $\circ$ (1 2 3) het element 1 afgebeeld wordt op 3.

Bijgevolg zal in S_3 gelden dat

$$(1)(2\ 3) \circ (1\ 2\ 3) = (1\ 3)(2).$$

Definitie 5.96

Een permutatie van $\{1, 2, \ldots, n\}$ die 2 elementen verwisselt en de andere elementen fixeert, noemen we een *transpositie* van $\{1, 2, \ldots, n\}$.

Elke transpositie bezit dus een cykelvoorstelling met één cykel van lengte 2 en al de andere cykels van lengte 1. Het is nu onmiddellijk duidelijk dat elke cykel van lengte r geschreven kan worden als een samenstelling van transposities (we laten hier de cykels van lengte 1 weg):

$$\begin{aligned}(x_1\ x_2\ \ldots\ x_{r-1}\ x_r) &= (x_1\ x_r) \circ (x_1\ x_{r-1}) \circ \cdots \circ (x_1\ x_3) \circ (x_1\ x_2) \\ &= (x_1\ x_2)(x_1\ x_3) \cdots (x_1\ x_{r-1})(x_1\ x_r)\end{aligned}$$

Bijgevolg kan elke permutatie geschreven worden als een samenstelling van een aantal transposities. Zo is bijvoorbeeld

$$(6\ 8)(5\ 7\ 9)(1\ 2) = (6\ 8)(5\ 7)(5\ 9)(1\ 2)$$

Merk echter op dat de *ontbinding* van een permutatie als samenstelling van transposities niet uniek is. Zo is bijvoorbeeld in $\{1, 2, 3, 4, 5, 6, 7\}$

$$\begin{aligned}(1\ 2)(2\ 7)(1\ 4)(5\ 7)(3\ 6)(3\ 5)(1\ 5) &= (1\ 3\ 6)(2\ 4\ 5\ 7) \\ &= (2\ 4)(2\ 5)(2\ 7)(1\ 3)(1\ 6)\,.\end{aligned}$$

Belangrijk en enigszins merkwaardig is wel dat de pariteit van het aantal transposities voor elke permutatie vast ligt, m.a.w., indien we een permutatie bijvoorbeeld kunnen ontbinden in een oneven aantal transposities dan kunnen we deze nooit ontbinden als een even aantal transposities. Dit wordt in de volgende stelling bewezen.

Stelling 5.97

Veronderstel dat een permutatie α van S_n geschreven kan worden als een samenstelling van r transposities en eveneens als een samenstelling van r' transposities. Dan zijn ofwel r en r' beide even ofwel beide oneven.

Bewijs. Veronderstel dat σ een willekeurige permutatie is. Dan kan σ geschreven worden als de samenstelling van disjunctie cykels $c_1, \ldots, c_k$. Noem de banen van deze cykels $B_1, B_2, \ldots, B_k$. De verzamelingen B_i zijn twee aan twee disjunct. Beschouw een transpositie $\tau = (x_1\ x_2)$.

Ofwel behoren x_1 en x_2 tot dezelfde baan B_j. De samenstelling van τ en c_j zal dan gelijk zijn aan twee cykels d_1 en d_2. De samenstelling van σ en τ is dan gelijk aan de samenstelling van de cykels c_i, $i \neq j$ en de cykels d_1 en d_2. Het aantal banen van $\sigma\tau$ is dus één meer dan het aantal banen van σ.

Ofwel behoren x_1 en x_2 tot verschillende banen B_i en B_j. De samenstelling van τ, c_i en c_j is dan gelijk aan juist één cykel d, de samenstelling van σ en τ is dan de samenstelling van de cykels c_l, $i \neq l \neq j$, en de cykel d. Het aantal banen van $\sigma\tau$ is dus één minder dan het aantal banen van σ.

Beschouw nu de identieke permutatie. Indien we deze herhaaldelijk samenstellen met een transpositie, dan verandert bij elke samenstelling het aantal banen (één minder of één meer). De samenstelling van een oneven aantal transposities kan dus niet dezelfde permutatie voorstellen als de samenstelling van een even aantal permutaties, want de pariteit van het aantal banen van beide samenstellingen is ongelijk. □

Met behulp van zogenaamde *permutatiematrices* kunnen we bovenstaande stelling op een alternatieve manier bewijzen.

Definitie 5.98

Stel dat $\sigma \in S_n$. Dan is de permutatiematrix M^σ de $n \times n$ matrix (m_{ij}) met

$$\begin{cases} m_{ij} = 1 & \iff \sigma(i) = j \\ m_{ij} = 0 & \text{in alle andere gevallen} \end{cases}$$

Beschouw de transpositie $\tau = (12) \in S_2$, dan is dus $M^\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Beschouw de permutaties $\sigma_1 = (23)$, $\sigma_2 = (12)$. Dan is $\sigma_3 := \sigma_1\sigma_2 = (1\ 2\ 3)$, $M^{\sigma_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $M^{\sigma_2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, en $M^{\sigma_1}M^{\sigma_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = M^{\sigma_3}$.

Lemma 5.99

Indien $\tau \in S_n$ een transpositie is, dan is $\det(M^\tau) = -1$.

Bewijs. Ontwikkeling van de determinant volgens de rijen, levert onmiddellijk het gestelde. □

Stelling 5.100

Veronderstel dat een permutatie α van S_n geschreven kan worden als een samenstelling van r transposities en eveneens als een samenstelling van r' transposities. Dan zijn ofwel r en r' beide even ofwel beide oneven.

Bewijs. Aangezien de samenstelling van permutaties, en dus ook van transposities, overeenkomt met matrixvermenigvuldiging, zal de determinant van M^σ, met $\sigma \in S_n$, gelijk zijn aan $(-1)^r$, met r het aantal transposities. Voor twee verschillende ontbindingen geldt dus dat $(-1)^r = (-1)^{r'}$, hetgeen de stelling bewijst. □

Gevolg

Een permutatie wordt een *even* permutatie genoemd dan en slechts dan als deze geschreven kan worden als een samenstelling van een even aantal transposities en wordt een *oneven* permutatie genoemd dan en slechts dan als deze geschreven kan worden als een samenstelling van een oneven aantal transposities.

Merk op dat de samenstelling van 2 even permutaties terug een even permutatie is. Hieruit volgt dat de deelverzameling van de even permutaties van S_n een deelgroep vormen voor de samenstelling. Deze deelgroep wordt de *alternerende groep* genoemd en wordt genoteerd als A_n of $\mathrm{Alt}(n)$. Indien we een willekeurige oneven permutatie σ beschouwen, dan is de nevenklasse σA_n de verzameling van de oneven permutaties. Bijgevolg is $S_n = A_n \cup \sigma A_n$ en bezit S_n evenveel even als oneven permutaties. De alternerende groep A_n is bijgevolg een permutatiegroep van de orde $\frac{n!}{2}$.

Opmerking

De afbeelding θ van $S_n, \circ$ op $\{1, -1\}, \cdot$ die de elementen van A_n afbeeldt op 1 en de oneven permutaties afbeeldt op -1, is een epimorfisme. De groep A_n is de kern van dit epimorfisme. Deze afbeelding wordt soms de *sign* afbeelding genoemd.

5.9 Epiloog

De p-adische (complexe) getallen

Het veld der p-adische getallen kan eveneens op algebraïsche wijze uitgebreid worden. Men kan aantonen dat een algebraïsche uitbreiding van een veld $\mathbb{K}$ met absolute waarde een absolute waarde op het uitgebreid veld induceert die samenvalt met de absolute waarde op $\mathbb{K}$, en dat het uitgebreid veld compleet is ten opzichte van de nieuwe absolute waarde. Dit blijft gelden na een eindig aantal algebraïsche uitbreidingen.

Als L een algebraïsche uitbreiding is van $\mathbb{Q}_p$, met absolute waarde $|\ |_L$, dan kunnen we de verzamelingen $\mathcal{O}_L := \{x \in L : |x|_L \leq 1\}$ en $\mathfrak{B} := \{x \in L : |x|_L < 1\}$ beschouwen . Opnieuw kunnen we "modulair rekenen": $x \equiv y \mod \mathfrak{B} \iff x - y \in \mathfrak{B}$. De quotiëntstructuur $\mathcal{O}_L/\mathfrak{B}$ is isomorf met het eindig veld $\mathbb{F}_{p^h}$ met $1 \leq h \leq n$ en n de dimensie van L als $\mathbb{Q}_p$ vectorruimte. Er treedt *ramificatie* op als $h < n$. Men kan aantonen dat er voor elke $h > 1$, algebraïsche uitbreidingen van $\mathbb{Q}_p$ bestaan die *niet geramificeerd* zijn, i.e. $n = h$, in feite komt het er op aan een geschikt irreduciebel polynoom te kiezen over $\mathbb{Q}_p$.

Veronderstel dat $\overline{\mathbb{Q}}_p$ een algebraïsche sluiting is van $\mathbb{Q}_p$. Men kan aantonen dat $\overline{\mathbb{Q}}_p$ niet bekomen wordt door door een eindig aantal algebraïsche uitbreidingen van $\mathbb{Q}_p$. Dit is in scherp contrast met de complexe getallen, die bekomen werden door juist één algebraïsche uitbreiding van $\mathbb{R}$. Men kan ook aantonen dat elke constructie van $\overline{\mathbb{Q}}_p$ een absolute waarde $|\ |_{\overline{\mathbb{Q}}_p}$ induceert die samenvalt met $|\ |_p$ op $\mathbb{Q}_p$, maar dat $\overline{\mathbb{Q}}_p$ **niet** compleet is ten opzichte van $|\ |_{\overline{\mathbb{Q}}_p}$. Het completeringsproces kan nu uitgevoerd worden op $\overline{\mathbb{Q}}_p$ en levert het veld $\mathbb{C}_p$, met bijhorende absolute waarde $|\ |_{\mathbb{C}_p}$, die samenvalt met $|\ |_{\overline{\mathbb{Q}}_p}$. Men toont dan aan dat het veld $\mathbb{C}_p$ algebraïsch afgesloten is. Tenslotte kan men aantonen dat $|x|_{\mathbb{C}_p} := p^{v_p(x)}$ een *discrete valuatie definieert* op $\mathbb{C}_p \setminus \{0\}$, i.e. v_p is een homomorfisme van $\mathbb{C}_p \setminus \{0\}, \cdot$ naar $\mathbb{Q}, +$. Zoals gebruikelijk stellen we $v_p(0) = \infty$ (omdat $|0|_{\mathbb{C}_p} = 0$).

We kunnen zoals gebruikelijk de verzamelingen $\mathcal{O} := \{x \in \mathbb{C}_p : |x|_L \leq 1\}$ en $\mathfrak{B} := \{x \in \mathbb{C}_p : |x|_L < 1\}$ beschouwen. In dit geval is $\mathcal{O}/\mathfrak{B}$ een algebraïsche sluiting van het eindig veld $\mathbb{F}_p$. Dat de eindige uitbreidingen van $\mathbb{F}_p$ niet meer te voorschijn komen, heeft te maken met ramificatie. Men kan immers aantonen dat de maximale niet geramificeerde uitbreiding van $\mathbb{Q}_p$ een echt deelveld is van $\overline{\mathbb{Q}}_p$, en dat een aantal van de geramificeerde uitbreidingen die nodig zijn om $\overline{\mathbb{Q}}_p$ te bekomen, steeds *totaal geramificeerd* zijn, i.e. $h = 1$.

In de algebraïsche zin zijn $\mathbb{C}$ en $\mathbb{C}_p$ hetzelfde veld. Men kan aantonen dat er een isomorfisme tussen beiden bestaat. De topologische eigenschappen zijn echter totaal verschillend, en worden volkomen bepaald door de verschillende absolute waarden $|\ |$ en $|\ |_p$.

Het lichaam der quaternionen

We hebben $\mathbb{C}$ geconstrueerd als velduitbreiding van $\mathbb{R}$. We hebben eveneens gezien dat $\mathbb{C}$ ook een tweedimensionale vectorruimte over $\mathbb{R}$ is, en dat $\mathbb{C}$ niet verder uitgebreid kan worden door nulpunten van polynomen toe te voegen, eenvoudigweg omdat elk polynoom van graad n over $\mathbb{C}$ juist n oplossingen over $\mathbb{C}$ heeft. Toch is het mogelijk om $\mathbb{C}$ uit te breiden, maar dan tot een *lichaam* dat $\mathbb{C}$ bevat.

Beschouw de volgende vier matrices over $\mathbb{C}$: $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Definieer de verzameling

$$H = \{aE + bI + cJ + dK \| a, b, c, d \in \mathbb{R}\}\,.$$

Aangeizen $H \subseteq M_2(\mathbb{C})$, kunnen we gewoon de optelling en vermenigvuldiging van matrices beschouwen als optelling en vermenigvuldiging in H. Het is ook duidelijk dat H een vectorruimte over $\mathbb{R}$ is. Een dergelijke structuur, i.e. een vectorruimte V over een veld K, waarbij er ook een vermenigvuldiging bestaat in V, wordt een *K-algebra* genoemd.

Bekijken we opnieuw $\mathbb{C}$, dan is het duidelijk dat $\mathbb{C}$ een $\mathbb{R}$-algebra is. Noteren we de elementen van $\mathbb{C}$ als koppels (a, b), dan geldt voor de vermenigvuldiging $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Bekijken we nu de verzameling H, dan is het duidelijk dat H een vierdimensionale vectorruimte over $\mathbb{R}$ is. Voor de elementen I, J en K geldt dat $I^2 = J^2 = K^2 = IJK = -E$. Als we de elementen van H noteren als tupels (a, b, c, d), dan geldt voor de vermenigvuldiging

$$\begin{aligned}(a_1, b_1, c_1, d_1) \cdot (a_2, b_2, c_2, d_2) = \\ (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, \\ a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\,,\end{aligned}$$

Noteren we zoals gebruikelijk $\mathbb{C} = \{a + ib \| a, b \in \mathbb{R}, i^2 = -1\}$, en $\mathbb{H} = \{a + ib + jc + kd \| a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$, dan is duidelijk dat $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ als $\mathbb{R}$-algebra's, en als lichamen. De vermenigvuldiging in $\mathbb{H}$ wordt dan

$$
\begin{aligned}
&(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) = \\
&\quad (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\
&\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k.
\end{aligned}
$$

Onder bepaalde voorwaarden, met name het beschikbaar zijn van een bepaalde norm, kan men alle $\mathbb{R}$-algebra's klasseren. Er blijken maar 4 mogelijkheden te zijn wat betreft hun dimensie: $1, 2, 4$ en 8. De eerste drie mogelijkheden hebben we gezien: $\mathbb{R}$, $\mathbb{C}$ en $\mathbb{H}$. De quaternionen $\mathbb{H}$ kunnen uitgebreid worden tot een 8-dimensionale $\mathbb{R}$-algebra, waar de vermenigvuldiging niet commutatief, en ook niet meer associatief is.

Hoofdstuk

6 Inleiding tot de grafentheorie

Alhoewel Euler beschouwd wordt als de vader van de grafentheorie en deze theorie dus dateert uit de 2de helft van de 18de eeuw, wordt deze toch algemeen als een vrij jonge theorie binnen de discrete wiskunde beschouwd. Grafentheorie heeft zowel combinatorische als algebraïsche aspecten, een heeft heel wat (praktische) toepassingen.

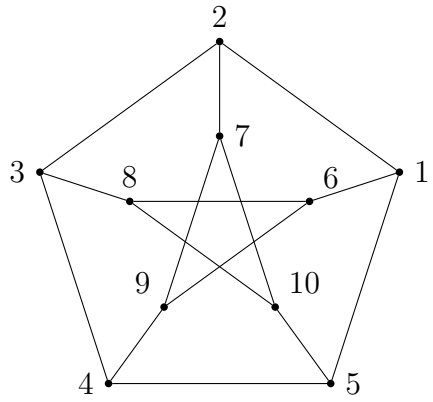
6.1 Ongerichte grafen

Heel eenvoudig gezegd is een graaf een verzameling van toppen, samen met een verzameling van verbindingen tussen twee toppen. Soms speelt de richting van deze verbinding een rol, soms zijn er meerdere verbindingen tussen twee punten mogelijk, en soms zijn er lussen. We starten met een formele definitie van een van de eenvoudigste gevallen.

Definitie 6.1

Een *graaf* (of ook *ongericht graaf*) Γ is een tupel (T, E, σ), T een niet-ledige verzameling van *toppen*, E een verzameling van *bogen*, en σ een injectieve relatie $E \to T \times T$, die met elke boog $e \in E$ een koppel (x, y) laat corresponderen, en waarbij elk koppel van de vorm (x, y) geïdentificeerd wordt met het koppel (y, x).

Een *lus* is een boog e waarvoor $\sigma(e) = (x, x)$. Als $\sigma(e) = (x, y)$, dan worden x en y de *eindtoppen* van de boog e genoemd. We eisen in de definitie dat σ injectief is, en omdat $(x, y) \equiv (y, x)$, is er dus tussen elk paar toppen hoogstens één boog mogelijk. Een graaf zonder lussen wordt ook *enkelvoudig* genoemd. Twee toppen die tot een boog behoren, worden *adjacent* genoemd. Als $\sigma(e) = (x, y)$, dan zeggen we ook dat de toppen x en y *incident* zijn met de boog e. Een top wordt *geïsoleerd* genoemd als hij met geen enkele boog incident is. Het aantal toppen van een graaf wordt de *orde* van de graaf genoemd. We geven een eenvoudig voorbeeld van een graaf.



Figuur 6.1: Petersen graaf

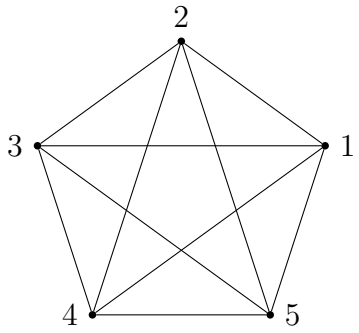
We kunnen een graaf definiëren door opsomming. Beschouw bijvoorbeeld het Petersen graaf (Figuur 6.1). Dan is

$$
\begin{aligned}
T(\Gamma) =& \{1,2,3,4,5,6,7,8,9,10\} \\
E(\Gamma) =& \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\} \\
\sigma =& \{(1,(1,2)),(2,(1,5)),(3,(1,6)),(4,(2,3)),(5,(2,7)),(6,(3,4)),(7,(3,8)), \\
& (8,(4,5)),(9,(4,9)),(10,(5,10)),(11,(6,8)),(12,(7,9)),(13,(8,10)), \\
& (14,(9,6)),(15,(10,7))\}
\end{aligned}
$$

De nummering van de bogen is in dit voorbeeld (en vele andere) niet belangrijk. Dus kunnen we net zo goed $E(\Gamma)$ identificeren met de beeldenverzameling van σ. Het Petersen graaf is een ongericht graaf. Dus een boog $(1,2) = (2,1)$. Aangezien er geen lussen zijn, kunnen we dus net zo goed $E(\Gamma)$ omschrijven als

$$
\begin{aligned}
E(\Gamma) =& \{\{1,2\},\{1,5\},\{1,6\},\{2,3\},\{2,7\},\{3,4\},\{3,8\},\{4,5\},\{4,9\}, \\
& \{5,10\},\{6,8\},\{7,9\},\{8,10\},\{9,6\},\{10,7\}\}
\end{aligned}
$$

Het is duidelijk dat een omschrijving door de verzamelingen T en E expliciet op te schrijven, nogal omslachtig is. Als ook σ volledig omschreven moet worden, is het al snel duidelijk dat deze voorstellingswijze omslachtig is.



Figuur 6.2: Compleet graaf op 5 toppen

Figuur 6.2 toont het compleet graaf op 5 toppen. Algemeen is het compleet graaf op n toppen snel omschreven: $T(\Gamma) := \mathbb{N}[1 \ldots n]$, $E(\Gamma) := \{\{x, y\} \| x, y \in T, x \neq y\}$. We noteren het compleet graaf op n toppen als K_n. Het is onmiddellijk duidelijk dat $|T(K_n)| = n$ en $|E(K_n)| = \binom{n}{2}$.

Een graaf bevat heel veel deelgrafen, elke deelverzameling van de toppen geeft in feite onmiddellijk aanleiding tot een deelgraaf, door enkel deze deelverzameling te beschouwen en alle bogen met beide eindtoppen in deze deelverzameling. We formaliseren dit in de volgende definitie

Definitie 6.2

Veronderstel dat $\Gamma = (T, E, \sigma)$ een graaf is, en dat $T' \subset T$. Dan induceert T' het deelgraaf $(T', E', \sigma_{|E' \times (T' \times T')})$, met $E' \subset E$ de verzameling van alle bogen e waarvoor $\sigma(e) \in T' \times T'$.

Definitie 6.3

Veronderstel dat Γ een graaf is. Een p-clique in Γ is een compleet deelgraaf op p toppen van Γ.

Eén van de standaard technieken om grafentheoretische vragen te behandelen, is combinatoriek. De volgende vraag werd door Pál Turán, een Hongaars wiskundige, opgelost in 1941: gegeven een enkelvoudig graaf dat geen p-clique bevat, hoveel bogen kan Γ bevatten? Merk op dat het Petersen graaf bijvoorbeeld geen 3-clique bevat.

Stelling 6.4

Veronderstel dat het graaf Γ van orde n geen p-clique bevat. Dan geldt

$$|E| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$$

Bewijs. We bewijzen de stelling door middel van inductie op n. Voor $n = 1$ is de stelling triviaal. Veronderstel dus dat $n > 1$. We zijn op zoek naar een bovengrens voor het aantal bogen van Γ. We veronderstellen dat deze bovengrens M is, en dat Γ M bogen bevat. We mogen veronderstellen dat Γ een $(p-1)$-clique bevat. Immers, indien dit niet het geval zou zijn, dan konden we aan Γ minstens één boog toevoegen, een contradictie met het feit dat M het maximaal aantal bogen is dat Γ kan bevatten. Noteer de toppenverzameling van de $(p-1)$-clique als A, en stel $B := T(\Gamma) \setminus A$.

De verzameling A induceert een compleet deelgraaf K_{p-1} in Γ. Dus er zijn $\binom{p-1}{2}$ bogen met beide eindtoppen in A. Noem e_B het aantal bogen met beide eindtoppen in B en $e_{A,B}$ het aantal bogen met een eindtop in A en een eindtop in B. Merk op dat B een deelgraaf van orde $n-p+1$ induceert in Γ, en door de veronderstelling geen p-clique bevat. Door de inductiehypothese geldt dus dat

$$e_B \leq \left(1 - \frac{1}{p-1}\right) \frac{(n-p+1)^2}{2}\,.$$

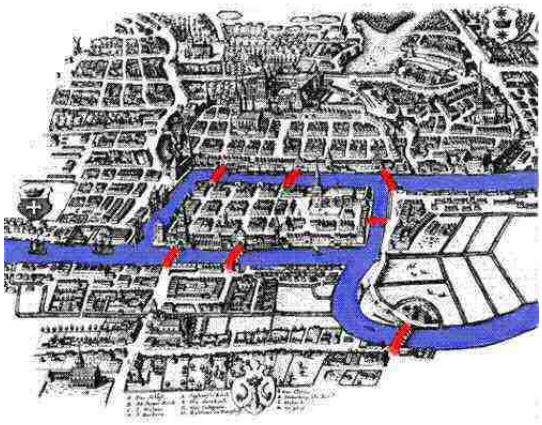
Aangezien Γ geen p-clique bevat, kan een top $v \in B$ adjacent zijn met ten hoogste $p-2$ toppen in A. Het tegendeel zou anders onmiddellijk aanleiding geven tot een p-clique, omdat A een compleet deelgraaf op $p-1$ toppen induceert. We besluiten dus dat

$$e_{A,B} \leq (p-2)(n-p+1)\,.$$

Gebruiken we de bovengrenzen voor e_B en $E_{A,B}$, en $|E| = \binom{p-1}{2} + e_B + e_{A,B}$, dan vinden we precies de gestelde formule □

Isomorfismen van grafen

We noemen twee enkelvoudige grafen Γ_1 en Γ_2 *isomorf* als er een bijectie bestaat van $T(\Gamma_1)$ naar $T(\Gamma_2)$ die een bijectie induceert van $B(\Gamma_1)$ naar $B(\Gamma_2)$.



Figuur 6.3: De zeven bruggen van Koningsbergen

Als $\Gamma_1 = \Gamma_2$, dan spreken we van een automorfisme Γ_1.

Stelling 6.5

De automorfismegroep van het Petersengraaf is S_5.

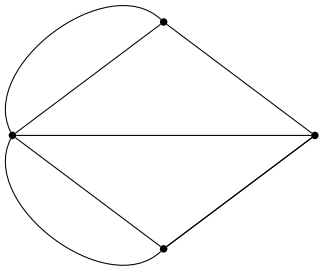
Bewijs. Oefening. □

6.2 Euleriaanse grafen

In een inleiding tot grafentheorie mag het verhaal over het probleem van de 7 bruggen van Koningsbergen (Duits: Königsberg) niet ontbreken. De rivier Pregel stroomt door deze oud-Pruissische stad[1] en verdeelde het grondgebied in 4 delen. In het midden van de rivier lag het eiland Kneiphof. De rivier splitste zich verder stroomafwaarts in 2 delen. Er lagen 7 bruggen over de rivier zoals in Figuur 6.3

Leonhard Euler beweerde in 1736 in één van zijn artikelen dat de volgende vraag moeilijk was. *Is het mogelijk om een wandeling te maken door de stad, zodanig dat elke brug juist één maal wordt gebruikt en zodanig dat de eindtop van de wandeling samenvalt met de begintop?* Zoals we zullen zien is

[1]Na WOII werd Oost-Pruisen verdeeld onder Polen en de Sovjet-Unie. Königsberg, nu Kaliningrad, ligt in het noordelijke Sovjet deel, hetgeen na het uiteenvallen van de Sovjet-Unie een exclave van Rusland werd.



Figuur 6.4: De zeven bruggen in een graaf

deze vraag hoegenaamd niet moeilijk. In elk geval wordt het bewuste artikel door iedereen beschouwd als het eerste artikel in de grafentheorie en wordt Euler de grondlegger van deze theorie genoemd. Indien we de 4 landengtes schematisch voorstellen als de 4 toppen A, B, C, D van een graaf en de bruggen door bogen tussen de betreffende toppen dan ontstaat de onderstaande multigraaf. We geven eerst de formele definitie van een multigraaf.

Definitie 6.6

Een *multigraaf* (of ook *gekleurd graaf*) Γ is een tupel (T, E, K, σ), T een niet-ledige verzameling van *toppen*, E een verzameling van *bogen*, K een verzameling van kleuren en σ een injectieve relatie $E \to (T \times T) \times K$, die met elke boog $e \in E$ een tupel $((x, y), k)$ laat corresponderen, en waarbij elk tuppel van de vorm $((x, y), k)$ geïdentificeerd wordt met het tuppel $((y, x), k)$.

Het spreekt voor zich dat een graaf ook een multigraaf is, met $|K| = 1$, waardoor K overbodig wordt. Daardoor echter zijn de meeste definities die we voor veralgemeningen van grafen geven, uiteraard ook geldig voor de minder algemene versie. Vanaf nu gebruiken we steeds stilzwijgend dit principe wanneer we bepaalde concepten gebruiken voor minder algemene grafen, of zelfs omgekeerd als er geen verwarring mogelijk is. Wanneer we het hebben over een *graaf*, dan zal de context ook duidelijk maken of we het over een multigraaf of een graaf hebben, of andere veralgemeningen.

Veronderstel dat Γ een multigraaf is. Het aantal bogen incident met een top x wordt de *graad* of *valentie* van de top genoemd en wordt soms genoteerd als $grd(x)$. Een lus levert een bijdrage 2 aan de graad van de top. Indien al

de toppen van een graaf dezelfde graad hebben dan noemen we deze graaf *regulier*.

Een *wandeling* in een graaf Γ bestaat uit een alternerende rij

$$x_0, e_1, x_1, e_2, x_2, \ldots, x_{k-1}, e_k, x_k$$

van toppen x_i (niet noodzakelijk verschillend) en bogen e_i zodanig dat de uiteinden van e_i de toppen x_{i-1} en x_i zijn, $i = 1, 2 \ldots, k$. Indien de graaf enkelvoudig is, wordt een wandeling volledig bepaald door de rij van opeenvolgende adjacente toppen $x_0, x_1, x_2, \ldots, x_{k-1}, x_k$; men noemt in dit geval k de *lengte* van de wandeling.

Indien de bogen $e_1, e_1, \ldots, e_k$ allemaal verschillend zijn, dan wordt de wandeling een *pad* genoemd. Indien $x_0 = x_k$ wordt de wandeling of het pad *gesloten* genoemd. Een *enkelvoudig pad* is er een waarbij al de toppen uit dit pad verschillend zijn. De *lengte van het pad* is het aantal bogen dat in het pad voorkomt.

Indien er voor elke keuze van x en y in $T(G)$ een pad van x naar y bestaat, dan noemen we de graaf G *samenhangend*. Indien dit niet het geval is bestaat G uit een aantal *samenhangende componenten* waartussen onderling geen bogen bestaan.

Een Eulerpad in een (multi)graaf Γ is een pad dat elke boog van Γ precies één maal bevat. Een samenhangende graaf die een gesloten Eulerpad bevat wordt een *Euleriaanse graaf* of *Eulergraaf* genoemd.

Stelling 6.7 — Euler

Zij Γ een samenhangende multigraaf. Dan is Γ een Eulergraaf dan en slechts dan als alle toppen van G een even graad hebben.

Bewijs. We gaan er eerst van uit dat Γ een gesloten Eulerpad bezit. Neem een willekeurige top v van Γ. Bij het doorlopen van het gesloten Eulerpad in Γ passeren we een aantal malen deze top v. Elke passage gebruikt twee bogen, één om in v te komen en één om v weer te verlaten. Bij het doorlopen van het Eulerpad worden alle bogen incident met v precies één maal doorlopen. Dus de graad van v is tweemaal het aantal passages door v, hetgeen een even getal is.

Veronderstel nu dat alle graden in Γ even zijn. We willen in Γ een gesloten Eulerpad construeren. We doen dit als volgt. We nemen een top u en beginnen vanuit u bogen te doorlopen, waarbij we nooit een boog voor een

tweede keer gebruiken. We stoppen pas als we weer terug in u zijn. We zullen niet voortijdig vastlopen. Stel namelijk dat we aankomen in een top v verschillend van u. Dan hebben we een oneven aantal bogen incident met v doorlopen, want bij elke passage door v gebruiken we twee bogen en we gebruiken een boog om in v aan te komen. Er is dus nog minstens een ongebruikte boog incident met v waarlangs we v kunnen verlaten. We hebben zo een gesloten pad P geconstrueerd met begin- en eindtop u, die geen boog twee keer gebruikt.

Als P alle bogen van Γ bevat, dan is P een gesloten Eulerpad en zijn we klaar. Stel dus dat P niet alle bogen van Γ bevat. We gaan P uitbreiden tot een groter pad dat geen enkele boog tweemaal gebruikt. Omdat Γ samenhangend is, is er een top u' op P, dat incident is met minstens één boog die nog niet doorlopen is. We laten nu alle bogen van P uit Γ weg, hetgeen resulteert in een graaf G'. De graden van de toppen in G' zijn natuurlijk nog steeds even. We beschouwen nu de component van G' waar u' in ligt (dat we niet G' zelf nemen maar een component van G' komt omdat G' onsamenhangend kan zijn).

Op dezelfde manier als we het pad P in Γ vanuit u hebben gemaakt, kunnen we nu in G' een gesloten pad P' maken beginnend in u' en eindigend in u', waarbij we geen enkele boog in G' tweemaal gebruiken. Natuurlijk is P' ook een pad in Γ, en wel eentje die geen enkele boog gemeen heeft met P. Nu combineren we P en P' tot één pad: we beginnen in u, wandelen langs P tot we in u' aankomen, wandelen dan eerst heel P' langs, dus tot we weer in u' terug zijn, en wandelen dan pas langs P verder tot we weer in u terug zijn. Dit nieuw gesloten pad begint en eindigt in u, bevat geen enkele boog tweemaal en bevat alle bogen van P en P'. Het is dus langer dan P. Als dit nieuw pad nog niet alle bogen bevat, dan kunnen we het uitbreidingsprocédé herhalen en nog een langer pad maken. Zo doorgaand hebben we dan uiteindelijk een gesloten pad geconstrueerd dat elke boog van Γ precies één maal bevat. We hebben dus een gesloten Eulerpad geconstrueerd. □

6.3 Hamiltoniaanse grafen

Een *polygon* is een eindige samenhangende graaf die regulier is met valentie 2. Het is duidelijk dat er op een isomorfisme na voor elke n juist één polygon P_n bestaat van de orde n. Een polygon P_n van de orde n die een deelgraaf is van een graaf G wordt een *cykel van lengte* n genoemd.

Zij Γ een graaf. Een pad in Γ dat alle toppen bevat, heet een *Hamiltoniaans pad*. Een cykel in Γ die alle toppen bevat, heet een *Hamiltoncykel*.

Indien Γ een Hamiltoncykel heeft, dan wordt G een *Hamiltoniaanse graaf* of *Hamiltongraaf* genoemd.

De vraag ligt nu voor de hand. Gegeven een willekeurige graaf, is deze graaf al dan niet Hamiltoniaans. De vraag is vrij analoog met deze voor Euleriaanse grafen. In beide gevallen gaat het eigenlijk om een globale eigenschap van de gegeven graaf, dwz. alle toppen of bogen van de graaf zijn erbij betrokken. Vreemd genoeg is de Eulervoorwaarde voor het bestaan van een gesloten Eulerpad een lokaal criterium.

Voor het onderzoeken of een gegeven graaf Hamiltoniaans is, zijn er echter geen voorwaarden bekend met een lokaal karakter. Er is zelfs geen enkel criterium bekend dat een efficiënt algoritme oplevert om na te gaan of een gegeven graaf een Hamiltoncykel bevat. Dit is één van de nog belangrijke onopgeloste problemen in de grafentheorie. Er zijn echter wel enkele stellingen gekend die ofwel alleen voldoende voorwaarden ofwel alleen nodige voorwaarden geven. We geven hiervan een voorbeeld.

Stelling 6.8

Als G een Hamiltongraaf is, en uit G worden k toppen (met aangrenzende bogen) verwijderd, dan valt G in hooguit k componenten uiteen.

Bewijs. Zij H een Hamiltoncykel in G. Noem de deelgrafen die uit G en H ontstaan door verwijdering van de k toppen, G' respectievelijk H'. Voor H is de bewering uit de stelling zonder meer waar, omdat H een cykel is. Dat wil zeggen dat H' uit hooguit k componenten bestaat. Maar G' bevat H' als deelgraaf en heeft dezelfde toppenverzameling als H'. Het aantal componenten van G' kan dus niet groter zijn dan dat van H'. Dus G' bestaat uit hooguit k componenten. □

Stelling 6.9 — Dirac, 1952

Als G een graaf is met n toppen ($n \geq 3$) en alle graden zijn tenminste $n/2$, dan is G een Hamiltongraaf.

Bewijs. We geven een bewijs uit het ongerijmde. Neem dus aan dat de bewering uit de stelling onwaar is; er moet dan minstens één tegenvoorbeeld bestaan: een graaf met n toppen, waarvoor wel geldt dat $grd(v) \geq n/2$ voor alle toppen v van de graaf, maar die geen Hamiltoncykel bevat. Voeg aan deze

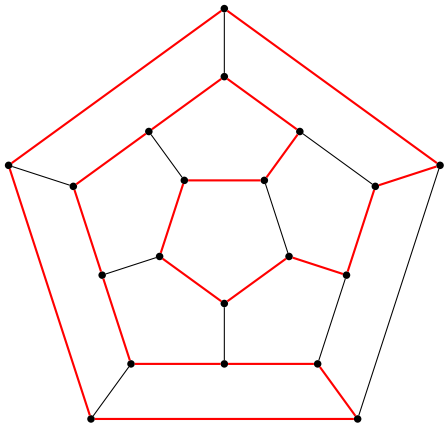
graaf zoveel mogelijk bogen toe (door niet adjacente toppen te verbinden) zonder daarbij Hamiltoncykels te creëren. De aldus verkregen graaf noemen we G. In G is geen Hamiltoncykel, dus kan G niet de complete graaf zijn. Stel v en w zijn twee niet adjacente toppen van G. Vanwege de constructie van G doet toevoegen van de boog $e = vw$ een Hamiltoncykel ontstaan. Dus bevat G een Hamiltonpad $v = v_1 \to v_2 \to \ldots \to v_n = w$. We zullen nu laten zien hoe we hieruit in het algemeen een Hamiltoncykel kunnen construeren.

We kijken naar twee verzamelingen van toppen op het pad, en bewijzen dat die een top gemeenschappelijk hebben. De eerste verzameling is die van de buren van de top v, kortweg de verzameling v-buren. Hiervan zijn er minstens $n/2$. De tweede verzameling is die van de toppen die op het pad de opvolger zijn van een w-buur. Daarvan zijn er eveneens minstens $n/2$. De som van hun aantallen is dus minstens n. Beide verzamelingen zijn echter deelverzamelingen van $\{v_2, \ldots, v_n\}$, met $n-1$ elementen. De verzamelingen moeten dus minstens één top gemeenschappelijk hebben.

Er is dus een v_j die zowel v-buur als opvolger van een w-buur is. Dan is de voorganger van v_j, dat is dus v_{j-1}, dus een w-buur. Maar dan is $v = v_1 \to v_j \to \ldots \to v_n \to v_{j-1} \to \ldots \to v_1 = v$ een Hamiltoncykel. De graaf G heeft dus een Hamiltoncykel terwijl we aangenomen hadden dat hij die niet had. Dit is een ongerijmdheid zoals we zochten. □

opmerking

Het zou verkeerd zijn te denken dat een graaf waarbij één of meerdere toppen een graad bezit die kleiner is dan de helft van de orde nooit Hamiltoniaans kan zijn. Het is uiteraard voldoende om hiervan een tegenvoorbeeld te geven. Een standaardvoorbeeld voor Hamiltoniaanse grafen is de dodecaëder graaf. Het is de graaf met toppenverzameling de 20 punten van de dodecaëder (of regelmatig twaalfvlak) en met bogenverzameling de 30 ribben van dit oppervlak. Het is duidelijk dat beide onderstaande voorstellingen isomorfe voorstellingen zijn. Het was Hamilton zelf die de vraag stelde of het mogelijk was om op deze graaf een gesloten pad te vinden die elke top juist één maal zou aandoen. Figuur 6.5 maakt duidelijk dat de graaf inderdaad Hamiltoniaans is.



Figuur 6.5: Hamiltoniaans pad (rood)

6.4 Planaire grafen

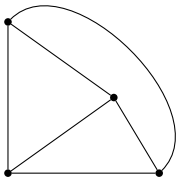
Definitie 6.10

Een graaf is *planair* als het in het Euclidisch vlak getekend kan worden zodanig dat geen twee bogen elkaar snijden.

Formeel moeten we zeggen wat we precies bedoelen met *tekenen*. Wiskundig gezien spreken we van een *inbedding*, d.i. een afbeelding die met de bogen begrensde krommen laat corresponderen en met de toppen de eindpunten van deze krommen. Een graaf is dus planair als er een inbedding kan gevonden worden met de eigenschap dat de krommen elkaar enkel in het beeld van een top snijden. De intuïtie is hier duidelijk. Het concept *inbedding* is echter heel belangrijk in vakgebieden als topologie en meetkunde.

Het is duidelijk dat K_3 en K_4 planair zijn, terwijl K_5 (zie Figuur 6.2). Ook het Petersengraaf is niet planair. Veronderstel dat Γ een planair graaf is, en beschouw de inbedding van Γ in het Euclidisch vlak. Een *gebied* is een deelvlak dat begrensd is door een eindig aantal krommen die het beeld zijn van een boog. We rekenen het vlak zelf minus alle gebieden die het graaf definieert, ook als één gebied. Beschouwen we K_4 (Figuur 6.6), dan zien we dat er 4 gebieden zijn.

Er zijn uiteraard $v = 4$ toppen, $e = 6$ bogen, en dus ook $f = 4$ gebieden. Er geldt dus $e + 2 = v + f$. Dit blijkt algemeen waar te zijn voor planaire grafen, zoals we bewijzen in de volgende stelling



Figuur 6.6: Compleet graaf op 4 toppen

Stelling 6.11 — de formule van Euler

Veronderstel dat Γ een planair graaf is op v toppen, met e bogen, en f gebieden. Dan geldt $v + f = e + 2$.

Bewijs. We bewijzen de formule per inductie of e. Voor $e = 1$ de formule correct is. Veronderstel dat de formule waar is voor planaire grafen met ten hoogste $e - 1$ bogen voor een zekere $e > 1$ en beschouw een planair graaf Γ met e bogen. Mogelijks bevat Γ geen enkele cykel. Dan is er een top t met graad 1. Verwijderen we de unieke boog b door t en t zelf, dan is het nieuwe graaf zeker planair, bevat het precies $e-1$ bogen en $v-1$ toppen, en definieert het hetzelfde aantal gebieden als Γ. Dus er geldt $v-1+f = e-1+2$ omwille van de inductiehypothese. Maar dan geldt de formule dus ook voor Γ. Veronderstel nu dat Γ een cykel bevat. Verwijderen we juist één boog b uit de cykel en behouden we de eindtoppen van b, dan ontstaat er een nieuw graaf met $e - 1$ bogen, v toppen en $f - 1$ gebieden. Wegens de inductiehypothese geldt er dus dat $v + f - 1 = e - 1 + 2$. Dus opnieuw geldt de formule ook voor Γ □

Een graaf is *samenhangend* als en slechts als er tussen elke twee toppen een pad bestaat. Een graaf Γ is *bipartiet* als en slechts als $T(\Gamma) = U \cap V$, en deze unie is disjunct, én elke boog verbind één top uit U met één top uit V.

Gevolg 6.12

In een eindig, samenhangend, enkelvoudig graaf Γ geldt $e \leq 3v - 6$. Als Γ bipartiet is, dan geldt $e \leq 2v - 4$.

Bewijs. Omdat Γ enkelvoudig is, zijn er minstens drie bogen per gebied nodig. Anderzijds is elke boog de grens tussen twee gebieden. Dus $3f \leq 2e$.

Dus $e+2 = v+f \leq v+\frac{2e}{3}$, of $3e+6 \leq 3v+2e$, of nog, $e \leq 3v-6$. Als Γ bipartiet is, dan is elk gebied begrensd door minstens 4 bogen. In dit geval is $4f \leq 2e$, en $e \leq 2v-4$ volgt. □

Het compleet graaf op 5 toppen, K_5, heeft 10 bogen, en $3v-6 = 9$, dus K_5 kan niet planair zijn. Veronderstel nu dat U en V twee disjuncte verzamelingen zijn van grootte u en v, respectievelijk. Definieer $E := \{\{x,y\} \| x \in U env \in V\}$, $T := U \cup V$. Dan zijn T en E de toppen, respectievelijk bogen van het compleet bipartiet graaf $K_{u,v}$. Beschouw $K_{3,3}$, dit graaf heeft $3^2 = 9$ bogen en 6 toppen, en $2v-4 = 2$. Dus $K_{3,3}$ kan niet planair zijn. Men kan vrij eenvoudig nagaan dat $K_{2,n}$, $n \in \mathbb{N}$ wel planair is. Vreemd genoeg zijn $K_{3,3}$ en/of K_5 steeds aanwezig in een graaf dat niet planair is.

Beschouw een willekeurig graaf Γ. Beschouw een boog $e \in E(\Gamma)$. Een *boog-contractie* is het identificeren van de eindtoppen van e en het verwijderen van e. Door een boog-contractie uit te voeren ontstaat een nieuw graaf. Een *minor* van Γ is een graaf dat uit Γ ontstaat door één of meerdere contracties.

Stelling 6.13 — stelling van Robertson-Seymour

Een eindig graaf Γ is planair als en slechts als geen enkele minor van Γ K_5 of $K_{3,3}$ is.

Bewijs. Zonder bewijs. □

Merk op dat het Petersengraaf niet planair is. Gevolg 6.12 is niet krachtig genoeg om te besluiten dat het Petersengraaf niet planair is, maar contractie van de bogen $\{1,6\}$, $\{2,7\}$, $\{3,8\}$, $\{4,9\}$, en $\{5,10\}$ levert K_5 op (zie Figuur 6.1), zodat de Stelling van Wagner kan toegepast worden.

Het vierkleurenprobleem is een ander historisch probleem dat verwant is met grafentheorie. Het probleem bestaat erin om een landkaart in te kleuren zodanig dat landen die een lijnstuk als grens delen, verschillend gekleurd worden. De vraag is of dit steeds, voor een willekeurige landkaart, met vier kleuren mogelijk is. Met een landkaart kunnen we een planair graaf associëren. De toppen zijn de landen, en twee toppen zijn adjacent als en slechts als ze een grens delen. Eén enkel punt als gedeelde grens volstaat dus niet. Een kleuring van een graaf Γ is niets meer dan een afbeelding $\kappa : T(\Gamma) \to K$, $\kappa(x) \neq \kappa(y)$ als $x \not\sim y$. Een kleuring met hoogstens vijf kleuren is steeds mogelijk.

Stelling 6.14 — Vijfkleurenstelling

Voor een planair graaf Γ bestaat er steeds een kleuring met ten hoogste vijf kleuren.

Bewijs. We bewijzen de stelling door inductie. Noteer het aantal toppen van Γ door v en het aantal bogen door e. Voor $v = 3$ is de stelling triviaal. Veronderstel dat $v > 3$. Omdat Γ planair is, geldt $e \leq 3v - 6$. Een boog is incident met twee toppen, dus als g de gemiddelde graad voorstelt, dan geldt $g = \frac{2e}{v} \leq \frac{6v-12}{v} < 6$. Er bestaat dus minstens één top t met graad ten hoogste 5. Beschouwen we het deelgraaf Γ' geïnduceerd door $T(\Gamma)\backslash\{t\}$, dan bestaat er wegens de inductiehypothese een kleuring van Γ' met hoogstens vijf kleuren. Als de graad van t hoogstens vier is, of als er hoogstens vier kleuren nodig zijn om de buren van t te kleuren, dan kan dus t gekleurd worden met de vijfde kleur. Veronderstel dus dat de graad van t vijf is, en dat de vijf buren x_i, $i = 1 \ldots 5$ van t in Γ door de vijf kleuren i, $i = 1 \ldots 5$, respectievelijk, gekleurd zijn. Kies twee kleuren i en j, en beschouw het deelgraaf $\Gamma'(i, j)$ dat bestaat uit de toppen x_i en x_j en alle daarmee verbonden toppen met kleur i of j. Als x_i en x_j niet in dezelfde component van $\Gamma'(i, j)$ voorkomen, dan kan in één van deze componenten kleuren i en j omgewisseld worden. Dus krijgt t twee buren met eenzelfde kleur, en blijft er een vijfde kleur over om aan t te geven. Dus veronderstel dat voor elke twee kleuren i en j de toppen x_i en x_j voorkomen in dezelfde component van de graaf $\Gamma'(i, j)$. De inbedding van Γ zorgt ervoor dat als we bv. kleuren $i = 1$ en $j = 3$ beschouwen, en een pad P van x_1 naar x_3 in $\Gamma'(i, j)$, en de kleuren $i = 2$ en $j = 4$, en een pad Q van x_2 naar x_4 in $\Gamma'(i, j)$, beide paden elkaar moeten snijden, dus noodzakelijk in een top, omdat Γ planair is. Maar dan moet deze top zowel kleur 1 of 3 én kleur 2 of 4 hebben, een contradictie. Dus deze situatie is niet mogelijk, en we mogen de stelling besluiten. □

Ongeveer op het einde van de negentiende eeuw werd de conjectuur geformuleerd dat 4 kleuren volstaan om een planair graaf te kleuren. Het duurde tot 1976 eer een bewijs gegeven werd. Dit bewijs herleidde het probleem tot 1936 subgevallen, die met behulp van de computer afgehandeld werden. Hadwiger's conjectuur is een sterke veralgemening van het origniele vierkleurenprobleem, en stelt dat als er voor elke kleuring van een planair graaf minstens k kleuren nodig zijn, men k disjuncte deelgrafen kan vinden met de eigenschap dat elk deelgraaf via een top met elk ander deelgraaf verbonden is.

6.5 gekleurde grafen

We kunnen definitie 6.6 uitbreiden tot gerichte grafen.

Definitie 6.15

Een *gekleurd en gericht graaf* is een tupel (T, E, K, σ), T een niet-ledige verzameling van *toppen*, E een verzameling van *bogen*, K een verzameling *kleuren* en σ een relatie $E \to (T \times T) \times K$, die met elke boog $e \in E$ een tupel $((x, y), k)$ laat corresponderen.

Wanneer we spreken van een *gekleurd graaf*, dan bedoelen we een *gekleurd, ongericht* graaf. Veronderstel nu dat $G, \cdot$ een groep is, voortgebracht door een verzameling X van generatoren. Het *Cayleygraaf* van de groep G ten opzichte van X, genoteerd $\Gamma_X(G)$ is een gekleurd en gericht graaf, met $T(\Gamma_X(G)) = G$, en

$$E(\Gamma_X(G)) = \{((g, h), x_i) \| g \cdot x_i = h\}\,.$$

Het is duidelijk hoe σ gedefinieerd is. Als e een boog is met $\sigma(e) = ((g, h), x_i)$, dan noemen we x_i het *kleur* van e. Beschouw nu de elementen $i, j, k \in \mathbb{H}$, het is duidelijk dat $Q_8 := \{-1, 1, -i, i, -j, j, -k, k\}, \cdot$ een groep is. Deze groep wordt voortgebracht door $X = \{i, j\}$. Figuur 6.7 stelt $\Gamma_X(Q_8)$ voor. Een blauwe pijl correspondeert met rechtse vermenigvuldiging met j, een rode pijl met rechtse vermenigvuldiging met i.

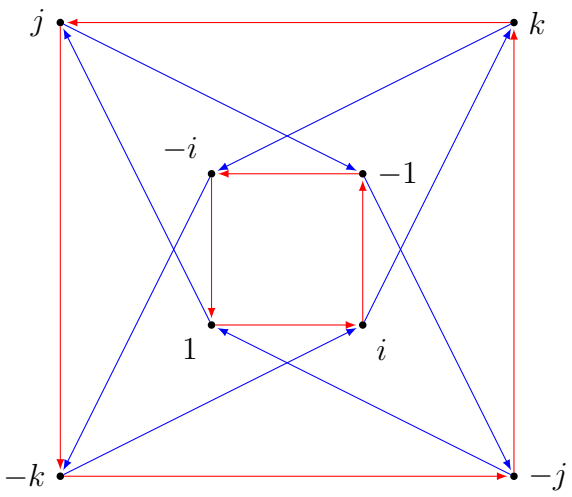
Een pad in een Cayleygraaf correspondeert met een *woord* in de elementen uit X. Een dergelijk woord is uiteraard niets meer dan een element uit de groep G. Als we een boog in tegengestelde richting gebruiken, dan vermenigvuldigen we met de inverse van het corresponderend element uit x. Bekijken we het woord $i \cdot j \cdot i^{-1} \cdot j^{-1}$ in Q_8, dan zien we in het Cayleygraaf dat dit gelijk is aan -1. Dit woord correspondeert met het pad

$$1 \xrightarrow{i} i \xrightarrow{j} k \xrightarrow{i^{-1}} -j \xrightarrow{j^{-1}} -1\,.$$

Bekijken we het pad

$$1 \xrightarrow{i} i \xrightarrow{j} k \xrightarrow{i^{-1}} -j \xrightarrow{j^{-1}} -1 \xrightarrow{i} -i \xrightarrow{j} -k \xrightarrow{i^{-1}} j \xrightarrow{j^{-1}} 1\,,$$

dan zien we onmiddellijk dat dit een cykel is in het Cayleygraaf. De cykels in het Cayleygraaf spelen een belangrijke rol, want deze corresponderen met woorden in de elementen van X (en hun inverse) die altijd gelijk zijn aan het



Figuur 6.7: Cayleygraaf van Q_8

eenheidselement van de groep. We noemen een dergelijk woord een *relatie* in de groep. Nu kan men elke groep ook op een abstracte manier beschrijven door middel van generatoren en relaties. De details vallen buiten het bereik van de cursus, maar het principe komt kort gezegd erop neer dat een verzameling generatoren (voorgesteld door letters), en hun inverses, en waarvoor er van een gegeven verzameling woorden geëist wordt dat ze het eenheidselement voorstellen, een volledige beschrijving van de groep kan zijn. Voor een gegeven groep is het computationieel gezien verre van triviaal om een dergelijke beschrijving te berekenen. Een elementair algoritme, het zogenaamde *colouring algorithm*, maakt echter dankbaar gebruik van het Cayleygraaf van een groep.

De *diameter* van een graaf is het kleinste natuurlijk getal N waarvoor geldt dat er tussen elke twee toppen steeds een pad van lengte N kan gevonden worden. Het is afhankelijk van de context of het toegelaten is dat bogen in tegengestelde richting gebruikt worden. In deze context, omdat we inverses van de groepselementen toelaten, is het duidelijk dat we dit toelaten. Hiermee is het eenvoudig om na te gaan dat de diameter van het Cayleygraaf van Q_8 gelijk is aan 2.

We kunnen ons ook laten bijstaan door het onvolprezen softwarepakket GAP (Groups, Algorithms and Programming, [8]), samen met de extensie GRAPE ([15]). De volgende output laat een GAP-sessie zien waarin de diameter van het Cayleygraaf van Q_8 bepaald wordt.

```
GAP4, Version: 4.4.12 of 17-Dec-2008, i686-apple-darwin10.8.0-gcc
Components:  small 2.1, small2 2.0, small3 2.0, small4 1.0, small5 1.0,
             small6 1.0, small7 1.0, small8 1.0, small9 1.0, small10 0.2,
             id2 3.0, id3 2.1, id4 1.0, id5 1.0, id6 1.0, id9 1.0, id10 0.1,
             trans 1.0, prim 2.1  loaded.
Packages:    GAPDoc 1.3, IO 3.3, TomLib 1.1.4  loaded.
gap> q := QuaternionAlgebra(Rationals);
<algebra-with-one of dimension 4 over Rationals>
gap> gens := GeneratorsOfAlgebraWithOne(q);
[ e, i, j, k ]
gap> g := Group(gens);
#I  default 'IsGeneratorsOfMagmaWithInverses' method returns 'true' for
[ e, i, j, k ]
<group with 4 generators>
gap> Order(g);
8
gap> LoadPackage("grape");

Loading  GRAPE 4.3  (GRaph Algorithms using PErmutation groups),
by L.H.Soicher@qmul.ac.uk.

true
gap> gamma := CayleyGraph(g);
rec( isGraph := true, order := 8,
  group := Group([ (), (1,2,8,7)(3,5,6,4), (1,3,8,6)(2,4,7,5),
      (1,4,8,5)(2,6,7,3) ]), schreierVector := [ -1, 2, 3, 4, 2, 4, 3, 2 ],
  adjacencies := [ [ 1, 2, 3, 4, 5, 6, 7 ] ], representatives := [ 1 ],
  names := [ (-1)*e, (-1)*i, (-1)*j, (-1)*k, k, j, i, e ], isSimple := false )
gap> Diameter(gamma);
2
```

Er zijn andere interessante groepen om de diameter van het Cayleygraaf te kennen. Nemen we bijvoorbeeld de groep van de Rubik's kubus, dan willen we graag weten in hoeveel bewegingen we zeker de puzzel vanuit elke mogelijke stand kunnen oplossen. Dit is niets anders dan de diameter van het Cayleygraaf. Onderstaande output behandelt de $2 \times 2 \times 2$ kubus. De rekentijd om de diameter te bepalen bedraagt ongeveer 10 minuten.

```
GAP4, Version: 4.4.12 of 17-Dec-2008, i686-apple-darwin10.8.0-gcc
Components:  small 2.1, small2 2.0, small3 2.0, small4 1.0, small5 1.0,
             small6 1.0, small7 1.0, small8 1.0, small9 1.0, small10 0.2,
             id2 3.0, id3 2.1, id4 1.0, id5 1.0, id6 1.0, id9 1.0,
             id10 0.1, trans 1.0, prim 2.1  loaded.
```

```
Packages:    GAPDoc 1.3, IO 3.3, TomLib 1.1.4  loaded.
gap> b := (17,18,19,20)(4,8,22,11)(3,7,21,12);
(3,7,21,12)(4,8,22,11)(17,18,19,20)
gap> l := (9,10,12,11)(13,1,17,21)(15,4,20,24);
(1,17,21,13)(4,20,24,15)(9,10,12,11)
gap> a := (21,22,23,24)(7,14,9,20)(6,13,11,19);
(6,13,11,19)(7,14,9,20)(21,22,23,24)
gap> cube := Group([b,l,a]);
Group([ (3,7,21,12)(4,8,22,11)(17,18,19,20),
   (1,17,21,13)(4,20,24,15)(9,10,12,11),
   (6,13,11,19)(7,14,9,20)(21,22,23,24) ])
gap> Order(cube);
3674160
gap> LoadPackage("grape");

Loading  GRAPE 4.3  (GRaph Algorithms using PErmutation groups),
by L.H.Soicher@qmul.ac.uk.

true
gap> Gamma := CayleyGraph(cube);;
gap> Diameter(Gamma);
14
gap> time;
618072
```

Computationieel geizen is het bepalen van de diameter van het Cayleygraaf van een groep een zeer complex probleem. Op `http://www.cube20.org/` vindt men een interessant overzicht van de bepaling van de diameter van het Caylyegraaf van de groep van de $3 \times 3 \times 3$ kubus, deze blijkt 20 te zijn.

6.6 Algebraïsche grafentheorie

Grafen kunnen ook voorgesteld worden door matrices. Hierbij worden de toppen van een graaf van de orde n op willekeurige wijze genummerd door middel van getallen uit $\mathbb{N}[1, n]$. Men vormt dan een matrix A, de zogenaamde *adjacentiematrix* waarbij A_{ij} het aantal bogen met begintop i en eindtop j aangeeft. Indien de graaf niet gericht is, zal deze matrix een symmetrische matrix zijn, bovendien zal een enkelvoudige graaf aanleiding geven tot een adjacentiematrix met op de diagonaal steeds 0 en hierbij zal A_{ij} voor $i \neq j$ gelijk zijn aan 1 dan en slechts dan als i en j adjacent zijn.

We geven in deze inleiding een voorsmaakje. Een *sterk regulier graaf met parameters* v, k, λ, μ is een enkelvoudig, ongericht graaf van orde v waarvoor

1. Elke top is adjacent met k andere toppen,
2. voor elk paar adjacente toppen x en y, $x \neq y$, zijn er juist λ toppen adjacent met x én y,
3. voor elk paar niet-adjacente toppen x en y, zijn er juist μ toppen adjacent met x én y

Een vijfhoek is een sterk regulier graaf met $v = 5$, $k = 2$, $\lambda = 0$, $\mu = 1$. We noemen een graaf dat aan voorwaarde (1) voldoet *k-regulier*. We bekijken nu de adjacentiematrix A van een k-regulier graaf Γ. Dit is een $v \times v$ matrix. Beschouw de "all-one" vector in $V(k, \mathbb{R})$, $\mathbf{j} = \underbrace{(1, 1, \ldots, 1)}_{v}$. Omdat Γ k-regulier is, komen er in elke rij juist k enen voor en $v - k$ nullen. Het inproduct van een rij met $\mathbf{j}$ is dus altijd gelijk aan k. De vector $\mathbf{j}$ is dus een eigenvector met eigenwaarde k. Maar ook het omgekeerde is waar, als $\mathbf{j}$ een eigenvector is met eigenwaarde k, dan is Γ k-regulier.

We noemen een eigenwaarde e van A *beperkt* als de corresponderende eigenvector orthogonaal is met $\mathbf{j}$. De volgende stelling heeft een kort bewijs en legt de fundamenten bloot. Met I bedoelen we de $v \times v$ eenheidsmatrix, met J bedoelen we de $v \times v$ "all-one" matrix.

Stelling 6.16

Voor een sterk regulier graaf Γ, met parameters v, k, λ, μ, adjacentiematrix A, dat niet compleet of leeg is, gelden de volgende uitspraken.

(i) De eigenwaarden van A zijn k, r en s, met $r \geq 0$ en $s \leq -1$ de oplossingen van de kwadratische vergelijking

$$x^2 + (\mu - \lambda)x + (\mu - k) = 0 \tag{6.1}$$

Bewijs. Noem $(b_{ij}) = B = A^2$. We onderscheiden drie gevallen.

(a) Elk getal b_{ii} is het aantal toppen adjacent met x_i, dus $b_{ii} = k$.

(b) Stel dat $i \neq j$ en $x_i \sim x_j$, dus $a_{ij} = 1$. Dan is $b_{ij} = \lambda$, het aantal toppen adjacent met twee adjacente toppen. Dus $b_{ij} = \lambda a_{ij}$ in dit geval

(c) Stel dat $i \neq j$ en $x_i \not\sim x_j$, dus $a_{ij} = 0$. Dan is $b_{ij} = \mu$, het aantal toppen adjacent met twee niet-adjacente toppen. Dus $b_{ij} = \mu(1 - a_{ij})$.

Het is duidelijk dat

$$B = A^2 = kI + \lambda A + \mu(J - I - A)\,,$$

of, gelijkwaardig

$$A^2 + (\mu - \lambda)A + (\mu - k)I = \mu J\,.$$

Stel nu dat θ een eigenwaarde is van A, met bijhorende eigenvector $\mathbf{e} = (e_1, e_2, \ldots, e_v)$. Vermenigvuldigen we $\mathbf{e}$ met beide leden van bovenstaande vergelijking, dan kunnen we besluiten dat

$$\theta^2 + (\mu - \lambda)\theta + (\mu - k) = \mu \sum_{i=1}^{v} e_i\,,$$

en $\mathbf{e}$ is ook een eigenvector van μJ. Als $\mu \sum_{i=1}^{v} e_i \neq 0$, dan zijn alle e_i gelijk (anders is $\mathbf{e}$ zeker geen eigenvector van μJ. Aangezien $A\mathbf{1} = kI$, volgt dat $\theta = k$.

Als $\mu \sum_{i=1}^{v} e_i = 0$, dan voldoet θ aan vergelijking (6.1). Aangezien $k > 0$ een positieve eigenwaarde is, $\mathrm{tr}A = 0$, de term $\mu - l \leq 0$, zijn er juist twee oplossingen, $r \geq 0$ en $s < 0$.

Dan is $b_{ij} = \sum_{k=1}^{v} a_{ik}a_{kj}$. Dus als $i \neq j$ dan is b_{ij} gelijk aan het aantal toppen adjacent met top x_i en top x_j. Dus als $x_i \sim x_j$, m.a.w als $a_{ij} = 1$, dan is $b_{ij} = \lambda a_{ij}$. Als $i = j$, dan is b_{ij} gelijk aan het aantal toppen adjacent met top x_i, dus $b_{ii} = k$, en als $i \neq j$ en $x_i \not\sim x_j$, dan is $b_{ij} = \mu$. Maar dan is $a_{ij} = 0$, of nog, $1 - a_{ij} = 1$. □

Stelling 6.17

Voor een eindig enkelvoudig graaf, niet compleet of leeg, van orde v, zijn de volgende uitspraken gelijkwaardig

(i) Γ is een sterk regulier graaf met parameters v, k, λ, μ

(ii) $A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$

(iii) A heeft juist twee verschillende beperkte eigenwaarden

Bewijs. De vergelijking in (ii) voor A^2 kan herschreven worden als

$$A^2 = kI + \lambda A + \mu(J - I - A)\,.$$

Noem $(b_{ij}) = B = A^2$. Dan is $b_{ij} = \sum_{k=1}^{v} a_{ik}a_{kj}$. Dus als $i \neq j$ dan is b_{ij} gelijk aan het aantal toppen adjacent met top x_i en top x_j. Dus als $x_i \sim x_j$, m.a.w als $a_{ij} = 1$, dan is $b_{ij} = \lambda a_{ij}$. Als $i = j$, dan is b_{ij} gelijk aan het aantal toppen adjacent met top x_i, dus $b_{ii} = k$, en als $i \neq j$ en $x_i \not\sim x_j$, dan is $b_{ij} = \mu$. Maar dan is $a_{ij} = 0$, of nog, $1 - a_{ij} = 1$. Hiermee is (i) $\iff$ (ii) duidelijk.

(ii) $\Longrightarrow$ (iii). Veronderstel dat ρ een beperkte eigenwaarde is van A, met bijhorende eigenvector $\mathbf{u}$. Vermenigvuldigen we de vergelijking voor A met $\mathbf{u}$, dan vinden we $\rho^2 = (\lambda - \mu)\rho + (k - \mu)$. Deze vergelijking heeft altijd precies twee oplossingen omdat $\mu \leq k$ en $\lambda \leq k - 1$.

(iii) $\Longrightarrow$ (ii). Veronderstel dat r en s de twee beperkte eigenwaarden zijn. Dan geldt $(A - rI)(A - sI) = \alpha J$, met $\alpha \in \mathbb{R}$. Dus A^2 is een lineaire combinatie van A, I en J. □

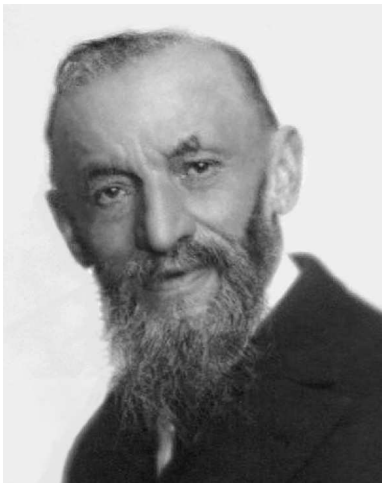
Er bestaat een uitgewerkte theorie waarin de algebraïsche eigenschappen van adjacentiematrix in verband gebracht worden met de combinatorische eigenschappen van de graaf. Het bewijs van combinatorische eigenschappen van bepaalde klassen van grafen wordt vaak eenvoudiger als er gebruik gemaakt kan worden van de algebraïsche vertaling. Aldus worden ook combinatorische problemen uit andere gebieden, bijvoorbeeld de eindige meetkunde, codeertheorie, en designtheorie verbonden met de algebra. Deze connectie levert nog steeds verrassende resultaten op.

Noten

- Bekijken we Figuur 6.4, dan is onmiddellijk duidelijk wat het antwoord op Euler's vraag is. Met de stelling van Euler in de hand hebben we een eenvoudig criterium om vast te stellen of een graaf Euleriaans is of niet. Maar daarmee hebben we in een Eulergraaf nog geen gesloten Eulerpad gevonden. Het *algoritme van Fleury* kan hiervoor gebruikt worden.
- De formule van Euler is niet zo verrassend. Ze is immers exact dezelfde voor toppen, zijden en vlakken van een veelvlak. Stereografische projectie van een veelvlak levert een planair graaf.

Hoofdstuk A

De Peanorekenkunde



Figuur A.1: Giuseppe Peano

Giuseppe Peano (1858-1932) was een Turijnse pionier in de logica, axiomatiek en rigueur. Hij had al een samenvatting van 4200 wiskundige stellingen in symboolschrift opgetekend in zijn werk *Formulario Matematico*. Volgend op werk van Peirce en Dedekind die de rekenkunde al probeerden te axiomatiseren, publiceerde Peano in 1889 een preciezer geformuleerde versie van hun werk, in zijn boek *De principes van de rekenkunde, gepresenteerd via een nieuwe methode* (*Arithmetices principia, nova methodo exposita*).

De Peanorekenkunde is een formeel systeem $(\mathcal{L}, \Gamma, \mathcal{A}, \mathcal{I})$, waarbij $\mathcal{L}$ de taal is bestaande uit $=$, 0, S, $+$, $\cdot$, samen met de symbolen uit de propositie- en predikaatlogica en de variabelen $x_1, x_2, \ldots$ De grammatica Γ drukt uit dat zinnen goed gevormd zijn (het behelst de goedgevormdheidsregels van de propositie- en predikaatlogica en komt erop neer dat 0 een constante is, $=$ een relatiesymbool, S een functiesymbool en $+$ en $\cdot$ binaire bewerkingen). De afleidingsregels $\mathcal{I}$ zijn deze uit de propositie- en predikaatlogica.

De axioma's van de Peanorekenkunde zijn de volgende (soms samen met die axioma's die uitdrukken dat $=$ een equivalentierelatie is).

1. $\forall x : S(x) \neq 0$
2. $\forall x, y(S(x) = S(y) \Rightarrow x = y)$
3. $\forall x : x + 0 = x$
4. $\forall x, y : x + S(y) = S(x + y))$
5. $\forall x : x \cdot 0 = 0$
6. $\forall x, yx \cdot S(y) = x \cdot y + x$
7. $\forall \phi : \forall y_1, \ldots, y_n(\phi(x \mid 0) \wedge \forall x(\phi \Rightarrow \phi(x \mid S(x)) \Rightarrow \forall x \phi$

Het laatste axioma is een tweede-orde-formulering van het beginsel van wiskundige inductie over de natuurlijke getallen. De eerste kwantificatie loopt over alle mogelijke predikaten ϕ waarvan de vrije vrije variabelen een deelverzameling zijn van $\{x, y_1, \ldots, y_n\}$. We hebben hier substitutienotatie gebruikt: $\phi(x|0)$ is de notatie voor het resultaat van het vervangen van alle vrije voorkomens van x in ϕ door 0.

Een zwakker, eerste-orde-systeem wordt verkregen door het vervangen van het inductieaxioma door een oneindige lijst van instantiaties, voor alle mogelijke predikaten ϕ.

Hoofdstuk

B Het axiomasysteem ZFC

Ernst Zermelo formuleerde een lijst axioma's in 1908, die onafhankelijk door Thoralf Skolem en Abraham Fraenkel geoptimaliseerd werd. De axioma's die tegenwoordig tot ZFC gerekend worden, zijn:

1. Axioma van extensionaliteit. Als twee verzamelingen dezelfde elementen hebben, dan zijn ze gelijk.

   $$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y]$$

   De omgekeerde implicatie volgt uit de de substitutie-eigenschap voor gelijkheid. Als de achterliggende logica de gelijkheid $=$ niet bevat, dan kan $x = y$ gedefinieerd worden als de formule

   $$\forall z [z \in x \Leftrightarrow z \in y] \wedge \forall w [x \in w \Leftrightarrow y \in w].$$

   In dat geval wordt het axioma van extensionaliteit

   $$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow \forall w (x \in w \Leftrightarrow y \in w)],$$

   wat uitdrukt dat als x en y dezelfde elementen hebben, ze dan ook tot dezelfde verzamelingen moeten behoren.

2. Axiomaschema van separatie / specificatie / beperkte comprehensie. De elementen van een gegeven verzameling die aan een goed gedefinieerde eigenschap voldoen, vormen een verzameling. In symbolen, er is een axioma van de volgende vorm, voor elke goed gevormde formule ϕ met vrije variabelen in $\{x, z, w_1, \ldots, w_n\}$:

   $$\forall z \forall w_1 \forall w_2 \ldots \forall w_n \exists y \forall x [x \in y \Leftrightarrow (x \in z \wedge \phi)].$$

   Het axioma laat niet toe om verzamelingen van de vorm $\{x : \phi(x)\}$ te construeren, wat de paradox van Russell uitsluit. In sommige axiomatisaties van ZF volgt dit axioma uit dat van substitutie, wat onafhankelijk voorgesteld werd door Skolem en Fraenkel.

3. Axioma van paren. Als x en y verzamelingen zijn, dan ook een verzameling die x en y als elementen bevat.

   $$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

Om de verzameling met *precies* deze twee elementen te construeren als verzameling, moet men het axioma van specificatie gebruiken; eenzelfde opmerking geldt voor de volgende twee axioma's.

4. Axioma van unie. Voor elke verzameling $\mathbb{F}$ bestaat er een verzameling die elke verzameling bevat die een element is van *een element van* $\mathbb{F}$.

$$\forall \mathcal{F}\, \exists A\, \forall Y\, \forall x[(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow x \in A]$$

5. Axioma van de machtsverzameling. Voor elke verzameling bestaat er een verzameling die alle deelverzamelingen ervan bevat.

$$\forall x \exists y \forall z[z \subseteq x \Rightarrow z \in y]$$

6. Axioma van oneindigheid. Er bestaat een inductieve verzameling.

$$\exists X\, [\varnothing \in X \wedge \forall y(y \in X \Rightarrow y \cup \{y\} \in X)]$$

   Voor meer over dit axioma, zie pagina 91.

7. Axiomaschema van substitutie. Als het domein van een functie een verzameling is, dan ook het beeld. In symbolen, ZFC bevat een axioma van de volgende vorm, voor elke goed gevormde formule ϕ met vrije variabelen in $\{x, y, A, w_1, \ldots, w_n\}$:

$$\forall A \forall w_1 \forall w_2 \ldots \forall w_n \big[\forall x(x \in A \Rightarrow \exists! y\, \phi) \Rightarrow \exists B\ \forall x\big(x \in A \Rightarrow \exists y(y \in B \wedge \phi)\big)\big]$$

8. Axioma van regulariteit / fundering. Elke niet-ledige verzameling x bevat een element dat disjunct is met x.

$$\forall x[\exists a(a \in x) \Rightarrow \exists y(y \in x \wedge \neg \exists z(z \in y \wedge z \in x))]$$

   Dit is een ietwat mysterieus axioma dat de onbedoelde mogelijkheden $a \in a$ of $a \in b \in a$ uitsluit.

9. Axioma van keuze. Voor elke verzameling $\mathcal{F}$ van niet-ledige, disjuncte verzamelingen bestaat er een verzameling waarvan de doorsnede met elk van de verzamelingen in $\mathcal{F}$ een singleton is.

$$\begin{aligned} \forall \mathcal{F} : \forall x \in \mathcal{F}(x \neq \varnothing \wedge \forall y \in \mathcal{F} : x \neq y \Rightarrow x \cup y = \varnothing) \Rightarrow \\ \exists C : \forall x \in \mathcal{F} : \exists! y : y \in x \wedge x \in C \end{aligned}$$

   Men kan dit uitschrijven door symbolen als $\varnothing$, $\cup$ en $\exists!$ te vervangen door de uitdrukkingen in de taal van ZFC, waarvoor ze afkortingen zijn, maar dat hindert de leesbaarheid.

   Voor een meer uitgebreide behandeling van het keuzeaxioma, zie pagina 74 en vooral de cursus *Wiskundige logica I*.

Bibliografie

[1] M. Aigner and G. M. Ziegler, *Proofs from The Book*, Springer-Verlag, Berlin, 1999. Including illustrations by Karl H. Hofmann, Corrected reprint of the 1998 original.

[2] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984.

[3] N. L. Biggs, *Discrete mathematics*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1985.

[4] P. J. Cameron, *Sets, logic and categories*, Springer Undergraduate Mathematics Series, Springer-Verlag London Ltd., London, 1999.

[5] K. Devlin, *Sets, functions, and logic*, Chapman & Hall/CRC Mathematics, Chapman & Hall/CRC, Boca Raton, FL, third ed., 2004. An introduction to abstract mathematics.

[6] M. du Sautoy, *Finding Moonshine*, Harper Perennial, 2009. ISBN: 978-0-00-721462-4.

[7] ———, *Het Symmetriemonster*, Uitgeverij Nieuwezijds, 2010. ISBN: 978 90 5712 286 6.

[8] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.5*, 2012.

[9] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, Reading, MA, second ed., 1994. A foundation for computer science.

[10] K. E. Hummel, *Introductory concepts for abstract mathematics*, Chapman & Hall/CRC, Boca Raton, FL, 2000.

[11] D. E. Knuth, *The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[12] M. E. Larsen, *Summa summarum*, CMS Treatises in Mathematics, Canadian Mathematical Society, Ottawa, ON, 2007.

[13] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Reading, MA, fourth ed., 2000.

[14] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer-Verlag, 2009.

[15] L. H. Soicher, *The GRAPE package for GAP*, 2012.

[16] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge University Press, Cambridge, second ed., 2001.

[17] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, second ed., 2003.