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, on-the-fly, 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 hoofdzakelijk gebaseerd op de cursusnota's die bij de invoering van dit vak door prof. dr. Fank De Clerck geschreven werden. In samenspraak met lesgevers van andere vakken uit het eerste semester, werd, ten opzichte van de versie voor het academiejaar 2011–2012, de volgorde van de hoofdstukken aangepast, en hier en daar werden enkele zaken toegevoegd. Prof. dr. Frank De Clerck, die op 1 oktober 2012 met pensioen ging, ben ik zeer erkentelijk voor het beschikbaar stellen van de LaTeX-bestanden van zijn nota's. Prof. dr. Tom De Medts ben ik zeer erkentelijk voor het beschikbaar stellen van het LaTeX-stylebestand die de hoofdingen van de hoofdstukken vormgeeft. Ten slotte bedank ik Karsten Naert, Bert Seghers en Geert Vernaeve voor het kritisch nalezen van deze nota's.

Jan De Beule
september 2012

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

Lijst van figuren

Hoofdstuk 1

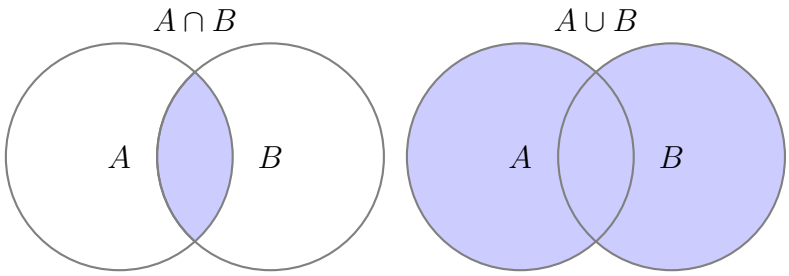
Elementen van de verzamelingenleer

1.1 De basisnotaties

Het begrip *verzameling* heb je zeker al in allerlei omstandigheden, binnen of buiten cursussen wiskunde, ontmoet. In de gewone spreektaal worden hiervoor heel wat synoniemen gebruikt. Volgende uitdrukkingen zijn je dus zeker niet vreemd: een *kudde* schapen, een *collectie* postzegels, een *regiment* soldaten, een *school* vissen, een *stapel* boeken, een *bende* schavuiten, een *stel* kookpotten, een *groep* studenten, ...

Al die uitdrukkingen wijzen erop dat sommige dingen samen beschouwd worden. Dit wordt dan aangeduid door het gebruik van woorden zoals kudde, collectie, regiment, ... verzameling. Binnen de wiskunde wordt het begrip *verzameling* gebruikt om te vertolken dat **verschillende** en **duidelijk gedefinieerde** dingen, die we dan *elementen* van de verzameling noemen, samen moeten worden beschouwd. Indien we de eis "verschillend" laten vallen, dan spreken we eerder van een *familie* van elementen, soms wordt in dat geval ook gesproken van een *multiverzameling*. De eis dat de elementen duidelijk gedefinieerd zijn is ook belangrijk. Zo kan je moeilijk spreken van de verzameling van de belangrijkste vakken in het eerste bachelorjaar wiskunde, omdat dit zeer subjectief is en dus niet duidelijk gedefinieerd. Je kan het wel hebben over de verzameling van al de vakken uit het eerste bachelorjaar, wat een eindige verzameling is. De elementen van een eindige verzameling kan je in principe dus expliciet opschrijven, maar indien de verzameling zeer veel elementen bezit is dit wat onhandig. Meer nog, voor een niet-eindige verzameling is dat gewoon niet mogelijk. In deze gevallen behelpen we ons met een omschrijving. Overigens, bij opsomming van de elementen in een verzameling speelt de volgorde geen rol. Een verzameling met één element wordt een *singleton* genoemd, terwijl een verzameling met twee elementen een *paar* genoemd wordt; niet te verwarren met een koppel (x, y) van twee elementen, ook wel een *geordend paar* genoemd.

Vanaf nu is een verzameling dus een wiskundig object, waar we een zeker intuïtief begrip van hebben. Er zijn essentieel twee verschillende mogelijkheden om een verzameling op te schrijven. We kunnen een verzameling *door middel van opsomming* definiëren of *door middel van voorschrift*. Beide bena-



Figuur 1.1: Venndiagram voor $A \cap B$ en $A \cup B$

mingen maken het verschil reeds duidelijk. Bekijk bijvoorbeeld de volgende definities: $A := \{1, 2, 3, 6, 12, 15, 30\}$ en $B := \{x \| x \in \mathbb{N} \text{ en } x \mid 30\}$.

Wanneer een verzameling gegeven wordt door middel van voorschrift, moet de kenmerkende voorwaarde eenduidig geïnterpreteerd kunnen worden. Beschouw het volgende voorbeeld: $A := \{x \| x > 1\}$. Deze omschrijving bepaalt de verzameling A eenduidig, als $x > 1$ met behulp van de context eenduidig geïnterpreteerd kan worden. In een een cursus reële analyse bijvoorbeeld zou x doorgaans een reëel getal kunnen zijn, waarmee $x > 1$ onmiddellijk duidelijk is. Maar de uitspraak $x > 1$ kan ook volkomen betekenisloos kan zijn, bijvoorbeeld als uit de context blijkt dat x een element is van een verzameling of structuur waarop er geen orde relatie $>$ kan bestaan.

Als voor een gegeven verzameling A, de uitspraak $x \in A$ vals is voor elk object x, dan is de verzameling A *ledig*. We noteren de ledige verzameling ook als $\emptyset$.

We definiëren nu de twee operatoren "doorsnede" en "unie".

Definitie 1.1

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

We kunnen doorsnede en unie van twee verzamelingen ook definiëren als een verzameling door middel van omschrijving:

$$A \cap B := \{x \| x \in A \text{ en } x \in B\} \text{ en } A \cup B := \{x \| x \in A \text{ of } x \in B\}.$$

We noemen twee verzamelingen A en B *disjunct* als en slechts als $A \cap B = \emptyset$. De uitspraak $x \in A$, voor x een willekeurig object en A een willekeurige

verzameling is waar of vals, en heeft steeds betekenis. Dit wil niet zeggen dat we kunnen beslissen of de uitspraak waar is of niet, maar essentieel is hier dat de verzameling $A \cap B$ en $A \cup B$ wel steeds gedefinieerd is, voor elke twee willekeurige verzamelingen A en B. Figuur 1.1 illustreert de doorsnede- en unie-operatoren op een grafische wijze. Dergelijke diagrammen heten *Venn-diagrammen* en worden dikwijls gebruikt om stellingen over verzamelingen te illustreren.

Definitie 1.2

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

Als $A \subset B$ kan de verzameling A dus ook samenvallen met B. Naar analogie met de notatie voor *kleiner dan of gelijk aan* bij de getallen wordt ook soms de notatie $A \subseteq B$ gebruikt en de verzamelingen zijn dan gelijk als $A \subseteq B$ en $B \subseteq A$. Indien A een deelverzameling is van B en de mogelijkheid $A = B$ expliciet wordt uitgesloten, dan wordt dit soms genoteerd als $A \subsetneq B$. We zullen in deze cursus echter de notatie $A \subset B$ veralgemeend gebruiken en (tenzij het uitdrukkelijk vermeld wordt) kan A dus gelijk zijn aan B. De verzameling van alle deelverzamelingen van een gegeven verzameling A wordt genoteerd als $\mathcal{P}(A)$. Er geldt dus dat $\{\emptyset, A\} \subset \mathcal{P}(A)$.

De verschiloperator is enkel afhankelijk van het al dan niet behoren tot een verzameling en kan dus eveneens eenvoudig gedefinieerd worden. Meteen kan ook het symmetrisch verschil van twee verzamelingen gedefinieerd worden.

Definitie 1.3

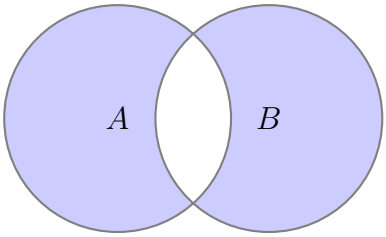
- Het *verschil van twee verzamelingen* A en B is de verzameling van alle elementen die bevat zijn in A maar niet in B.
- Het *symmetrisch verschil* van twee verzamelingen A en B is de verzameling van alle elementen die bevat zijn in $A \cup B$ maar niet in $A \cap B$.

Opnieuw kunnen we het verschil en symmetrisch verschil van twee verzamelingen definiëren als een verzameling door middel van omschrijving.

$$A \setminus B := \{x \| x \in A \,\text{en}\, x \notin B\},$$

en

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



Figuur 1.2: Venndiagram voor $A \triangle B$

Notatie	**Omschrijving**
$\{a, b, c\}$	verzameling met als elementen a, b en c
$\{a, b, c, \ldots\}$	verzameling met als elementen a, b en c, enz.
$\{x \mid\mid \ldots\}$	verzameling van alle elementen zodanig dat ...
$\emptyset$	de ledige verzameling
$\in$	is element van (behoort tot)
$\notin$	is geen element van (behoort niet tot)
$\subset$	is deelverzameling van
$\not\subset$	is geen deelverzameling van
$A \cap B$	A doorsnede B
$A \cup B$	A unie B
$A \setminus B$	verschil van A en B
$A \triangle B$	symmetrisch verschil van A en B wat gelijk is aan $(A \cup B) \setminus (A \cap B)$

Tabel 1.1: Notaties voor verzamelingen

De meeste notaties zijn wereldwijd vastgelegd en zijn doorgaans goed gekend. Waar de notatie voor doorsnede, unie en verschil van twee verzamelingen vrij standaardnotaties zijn (al wordt i.p.v. $A \setminus B$ ook wel $A - B$ gebruikt), is er geen algemeen aanvaarde notatie voor het symmetrisch verschil dat ook wel eens als $A \ominus B$ of zelfs als $A + B$ genoteerd wordt. Ten slotte zullen we soms de symbolen uit de verzamelingenleer in zijn symmetrische vorm gebruiken zoals $A \ni a$, $A \supset B$, ... Een overzicht wordt gegeven in Tabel 1.1. Indien nodig zullen aanvullende notaties in de loop van de cursus worden ingevoerd.

De ledige verzameling is de verzameling die geen enkele element bevat. Aan de andere kant van het spectrum, vooral van belang bij de theoretische behandeling van verzamelingenleer, zullen we het hebben over het *universum* of de *universele verzameling* die dan bestaat uit de verzameling van alle

elementen die we op dat moment beschouwen. Dus de context is hier relevant. In tegenstelling tot de notatie voor de ledige verzameling bestaat hiervoor geen "universele" notatie, we zullen meestal Ω gebruiken.

Veronderstel dat A een deelverzameling is van een verzameling B, dan noemen we het *complement* van A, de verzameling van alle elementen van B die niet in A gelegen zijn. Indien een verzameling A kan beschouwd worden als deelverzameling van een universele verzameling Ω, dan definiëren we het complement van A als $A^c = \Omega \backslash A$. Het is eenvoudig na te gaan dat $(A^c)^c = A$; $A \cap A^c = \emptyset$ en $A \cup A^c = \Omega$.

Merk op dat voor een gegeven verzameling A er niet noodzakelijk een unieke universele verzameling is. Beschouw bijvoorbeeld $A = \{1, 2, 3\}$. Dan is $A \subset \mathbb{N}$, maar ook $A \subset \mathbb{R}$. Voor deze twee mogelijk universele verzamelingen is het duidelijk dat het complement van A verschillend is.

Nu we de notaties hebben vastgelegd, kunnen we al een eerste reeks eigenschappen opsommen, die we hier in de vorm van een eerste stelling formuleren. Het bewijs is een eenvoudige oefening.

Stelling 1.4

Als A, B en C verzamelingen zijn, dan gelden de volgende eigenschappen.

1. **Commutatieve eigenschap**
   (a) $A \cap B = B \cap A$.
   (b) $A \cup B = B \cup A$.
2. **Associatieve eigenschap**
   (a) $A \cap (B \cap C) = (A \cap B) \cap C$ (en noteren daarom $A \cap B \cap C$).
   (b) $A \cup (B \cup C) = (A \cup B) \cup C$ (en noteren daarom $A \cup B \cup C$).
3. **Distributieve eigenschap**
   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
4. **Wetten van De Morgan**
   (a) $(A \cup B)^c = A^c \cap B^c$.
   (b) $(A \cap B)^c = A^c \cup B^c$.

De paradox van Russell

De *naïeve verzamelingenleer* zoals we ze hier gebruiken, bevat eigenlijk heel wat verborgen veronderstellingen. Sommige daarvan leiden tot eigenaardigheden. Het meest bekend is de zogenaamde *Paradox van Russell* (Bertrand Russell, 1872 - 1970).

> Veronderstel dat R de verzameling is van alle verzamelingen die geen element zijn van zichzelf. Dan is R noch een element van zichzelf noch geen element van zichzelf.

Met de notaties die we tot hiertoe hebben gezien, betekent dit dus dat als $R = \{x \| x \notin x\}$ dan is $R \in R$ gelijkwaardig met $R \notin R$.

Een paradox die zijn eigen leven is gaan leiden. Hoe komen we hieruit? De paradox ontstaat doordat we ons intuïtief begrip van verzamelingen op een foutieve wijze abstraheren. Meer bepaald leidt onder andere het feit dat de *uitspraak* $R \in R$ (of de ontkenning ervan, $R \notin R$) voor een willekeurig verzamelingen R gedefinieerd is, tot deze paradox. Een diepgaande behandeling van deze paradox, en de oplossing op dit probleem te vermijden, valt (ver) buiten het bestek van deze cursus. We gaan dan ook niet in op een axiomasysteem voor een verzamelingenleer, maar we gebruiken verzamelingen op een intuïtieve manier.

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

Van Leopold Kronecker (1823 –1891) is geweten dat hij eens uitriep:

> *God schiep de natuurlijke getallen en de rest is het werk van de mens.*

Het is zonder meer duidelijk dat de natuurlijke getallen ons van kindsaf zijn ingelepeld, allemaal hebben wij moeten leren *tellen*, meestal op de vingers, en dan klonk het 1, 2, 3, 4, 5, ... De naam *natuurlijke getallen* is dan ook niet verkeerd gekozen. Alleen, wij willen meer doen met deze getallen. Wij willen ze bv. optellen, wij willen ze ordenen en nog meer dergelijke zaken. Strikt gesproken moeten wij hier een definitie geven van *tellen* en *optellen*. Het is echter niet onze bedoeling om hier nu op in te gaan; wij nemen derhalve aan dat deze begrippen *primitieve* begrippen zijn. Ook hier gebruiken we onze intuïtieve kennis, eerder dan een axiomatische opbouw.

Terug naar de *verzameling van de natuurlijke getallen*. Indien wij enige structuur op deze verzameling willen leggen, dan is het al vlug duidelijk dat wij een notatie moeten hebben voor *niets*. Dit is de aanleiding geweest om een extra element, genoteerd door 0, bij te voegen. Men kan nu discussiëren over het feit of 0 al dan niet een natuurlijk getal is. Internationaal zijn hierover geen afspraken gemaakt. Voor de ene is het getal (of moeten wij zeggen symbool) 0 geen natuurlijk getal, voor anderen wel. Indien wij het over telproblemen hebben, is het meer logisch om te starten van het getal 1, maar als we het later hebben over de algebraïsche structuur van de natuurlijke getallen, dan zal vlug blijken dat we er alle belang bij hebben om 0 wel degelijk als natuurlijk getal te beschouwen. Wij gebruiken de volgende notaties.

$$\begin{aligned} \mathbb{N} &= \{0, 1, 2, 3, \ldots\} \\ \mathbb{N}^* &= \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\} \end{aligned}$$

Misschien ben je gewoon om de notatie $\mathbb{N}_0$ te gebruiken voor $\mathbb{N}^*$, maar dit doen we liever niet om verwarring met gelijkaardige notaties die een totaal andere betekenis hebben, te vermijden.

Eens we kunnen optellen, willen wij ook de inverse bewerking (die wij dus *aftrekken* noemen) uitvoeren. Uiteraard willen wij binnen onze verzameling van de natuurlijke getallen blijven, maar dit kan echter niet altijd. Wij zijn dus verplicht de verzameling van de natuurlijke getallen uit te breiden met nieuwe getallen, de zogenaamde *negatieve gehele getallen*. Voegen wij hier de natuurlijke getallen bij, die we dus ook de *niet-negatieve gehele getallen* kunnen noemen, dan ontstaat de verzameling van de gehele getallen

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Alhoewel de notatie $\mathbb{Z}$ voor de verzameling van de gehele getallen een internationale standaardnotatie is (komt van het Duits *Zahl*), geldt dit niet voor de notatie en benaming van de verzameling van de negatieve gehele getallen en andere deelverzamelingen van $\mathbb{Z}$. Wij noteren (bewust van enige inconsequenties)

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

Merk op dat 0 noch positief noch negatief is, de benaming *strikt positieve getallen* voor $\mathbb{N}^*$ is dus niet zinvol, we spreken daarom liever van de natuurlijke getallen zonder 0 of van de positieve gehele getallen. Om dezelfde reden

noemen we $\mathbb{Z}^-$ de verzameling van de *negatieve gehele getallen samen met 0* maar het is korter om te spreken over de *niet-positieve gehele getallen*.

We voeren ten slotte nog een laatste notatie in, die weliswaar terug niet standaard is, en waarbij we veronderstellen dat $a \leq b$:

$$\mathbb{N}[a, b] = \{a, a + 1, a + 2, \ldots, b - 1, b\} \subset \mathbb{N}.$$

Een analoge notatie zal gebruikt worden voor deelverzamelingen van de andere getallenverzamelingen.

De gehele getallen werden ingevoerd om de inverse bewerking van de optelling steeds mogelijk te maken. Er is echter nog een tweede bewerking die ons van kindsbeen af werd bijgebracht, met name de vermenigvuldiging. Indien wij hiervan de inverse bewerking willen uitvoeren, dan blijkt al vlug dat wij terug nieuwe getallen moeten invoeren, met name de (eigenlijke) *breuken*. Samen met de gehele getallen vormen zij de verzameling van de *rationale getallen*, die door $\mathbb{Q}$ voorgesteld wordt (komt van *quotiënt*). Deze verzameling wordt dan nog uitgebreid met de zogenaamde *irrationale getallen*, om dan de verzameling $\mathbb{R}$ van de *reële getallen* te vormen. Deze verzameling wordt dan op haar beurt nog uitgebreid tot de verzameling $\mathbb{C}$ van de *complexe getallen*. De structuur van deze verzamelingen ten opzichte van de "natuurlijke" bewerkingen, optelling (en aftrekking) en vermenigvuldiging (en deling) komt nog aan bod in Hoofdstuk 6

1.3 Relaties

Wanneer we twee verzamelingen A en B beschouwen (niet noodzakelijk verschillend), dan kunnen we uit elke verzameling een element kiezen, stel $a \in A$ en $b \in B$, en daarmee een nieuw object maken: het koppel (a, b). Merk op dat de volgorde wel degelijk belangrijk is. Alle mogelijke koppels bij gegeven verzamelingen A en B vormen opnieuw een verzameling.

1.3.1 Basisdefinities

Definitie 1.5

Het *cartesisch product* van twee verzamelingen A en B, ook nog *productverzameling* genoemd, is de verzameling

$$A \times B = \{(a, b) \| a \in A, b \in B\}.$$

Het is dus duidelijk dat voor twee verschillende verzamelingen A en B, $A \times B \neq B \times A$. Meer algemeen wordt het cartesisch product van k verzamelingen $A_1, A_2 \dots A_k$ gedefinieerd als de verzameling

$$A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, \dots, a_k) || a_i \in A_i, i = 1, 2, \dots, k\}.$$

De elementen van deze verzamelingen worden *geordende k-tallen* genoemd. Indien $A_i = A$ voor alle $i \in \{1, 2, \dots, k\}$ dan noteren we het cartesisch product als A^k. Als $A = \emptyset$ of $B = \emptyset$, dan is $A \times B = \emptyset$.

Definitie 1.6

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

Een relatie is dus een verzameling $\Re$ van koppels met eerste element (begin van het koppel) in A en tweede element in B (einde van het koppel). We noemen A de *beginverzameling* en B de *eindverzameling*. Als $(a, b) \in \Re$, dan wordt b een *beeld* genoemd van a onder de relatie $\Re$, en soms wordt dit genoteerd als $a \Re b$ (denk bv. aan $a \leq b$), maar ook (bv. in de analyse) als $b = \Re(a)$. Een relatie kan voorgesteld worden door middel van pijlen van de verzameling A naar de verzameling B, of kan voorgesteld worden als punten in het vlak met coördinaatassen A en B. Indien $A = B$ dan spreken we eerder van een relatie in A.

Voorbeeld 1.7. Deelbaarheid in $\mathbb{N}$ is een relatie $\mathcal{D} \subset \mathbb{N} \setminus \{0\} \times \mathbb{N}$ gedefinieerd door

$$(a, b) \in \mathcal{D} \Longleftrightarrow \exists q \in \mathbb{N} : b = a \cdot q.$$

De notatie $(a, b) \in \mathcal{D}$ betekent dus "a is een deler van b", of nog, "b is deelbaar door a". Deelbaarheid is een vertrouwd begrip. We kunnen in feite snel enkele eigenschappen van $\mathcal{D}$ opschrijven.

- Elk natuurlijk getal is deelbaar door zichzelf en door 1 dus $(x, x) \in \mathcal{D}$ voor alle $x \in \mathbb{N} \setminus \{0\}$ en $(1, x) \in \mathcal{D}$ voor alle $x \in \mathbb{N}$
- Elk getal verschillend van nul is een deler van nul. Dus $(x, 0) \in \mathcal{D}$ voor alle $x \in \mathbb{N} \setminus \{0\}$.
- Voor alle $x, y \in \mathbb{N} \setminus \{0\}$ geldt er dat $(x, y) \in \mathcal{D}$ en $(y, x) \in \mathcal{D}$ impliceert dat $x = y$.

Veronderstel dat X een willekeurige verzameling is. "Is deelverzameling van" $(\subset)$ is een relatie in $\mathcal{P}(X)$. Ook van deze relatie kunnen we snel enkele eigenschappen opsommen.

- Elke deelverzameling $A \in \mathcal{P}(X)$ is bevat in zichzelf, $A \subset A$.
- Voor alle $A, B \in \mathcal{P}(X)$ geldt, als $A \subset B$ en $B \subset A$, dan is $A = B$
- Voor alle $A, B, C \in \mathcal{P}(X)$ geldt, als $A \subset B$ en $B \subset C$, dan is $A \subset C$.
- Als $X \neq \emptyset$ en X is geen singleton, kunnen er steeds $A, B \in \mathcal{P}(X)$ gevonden worden waarvoor $A \not\subset B$ en $B \not\subset A$.

Definitie 1.8

Als $\Re \subset A \times B$ een relatie is, dan is de *omgekeerde* of *inverse relatie* de verzameling $\Re^{-1}$ van de omgekeerde koppels, formeel

$$\Re^{-1} = \{(b, a) \| (a, b) \in \Re\}.$$

Als (a, b) en (b, c) twee koppels zijn, die dus het kenmerk vertonen dat het einde van het eerste koppel precies het begin is van het tweede koppel, dan zeggen we dat het koppel (b, c) volgt op het koppel (a, b) of nog, dat de koppels (a, b) en (b, c) opeenvolgende koppels zijn. Twee opeenvolgende koppels kunnen samengesteld worden.

Definitie 1.9

De *samenstelling* van twee opeenvolgende koppels $(a, b) \in A \times B$ en $(b, c) \in B \times C$ is het koppel $(a, c) \in A \times C$.

De samenstelling van alle koppels van twee gegeven relaties is uiteraard opnieuw een relatie. We leggen de definitie van een samengestelde relatie vast.

Definitie 1.10

Voor de relaties $\Re_1 \subset A \times B$ en $\Re_2 \subset B \times C$ is de de *samengestelde relatie* van $\Re_1$ en $\Re_2$ de verzameling

$$\Re_2 \circ \Re_1 := \{(a, c) \| \text{er bestaat een } b \in B \text{ zodat } (a, b) \in \Re_1 \text{ en } (b, c) \in \Re_2\}.$$

De notatie $\Re_2 \circ \Re_1$ wordt gelezen als "$\Re_2$ na $\Re_1$". Het is duidelijk dat $\Re_2 \circ \Re_1 \subset A \times C$. Deze notatie is zinvol want als $(a, b) \in \Re_1$ en $(b, c) \in \Re_2$, dan is $\Re_2 \circ \Re_1(a) = \Re_2(\Re_1(a)) = \Re_2(b) = c$.

Merk op dat twee willekeurige relaties niet noodzakelijk samengesteld kunnen worden. De samenstelling van relaties (indien gedefinieerd) is associatief, $(\Re_3 \circ (\Re_2 \circ \Re_1) = (\Re_3 \circ \Re_2) \circ \Re_1)$, maar niet commutatief $(\Re_1 \circ \Re_2 \neq \Re_2 \circ \Re_1)$.

Verder is duidelijk dat de omgekeerde van een samengestelde relatie de samenstelling is van de omgekeerde relaties maar dan wel in de omgekeerde volgorde.

$$(\Re_2 \circ \Re_1)^{-1} = \Re_1^{-1} \circ \Re_2^{-1}.$$

We kunnen een gegeven relatie $\Re \subset A \times B$ beperken tot een deelverzameling $C \times D$, met $C \subset A$ en $D \subset B$.

Definitie 1.11

Stel $\Re$ is een relatie van A naar B en $C \subset A$ en $D \subset B$. De verzameling $\Re' := \Re \cap (C \times D)$ is een relatie en wordt de *beperking van* $\Re$ *tot* $C \times D$ genoemd, genoteerd $\Re_{|C \times D}$.

Opmerking

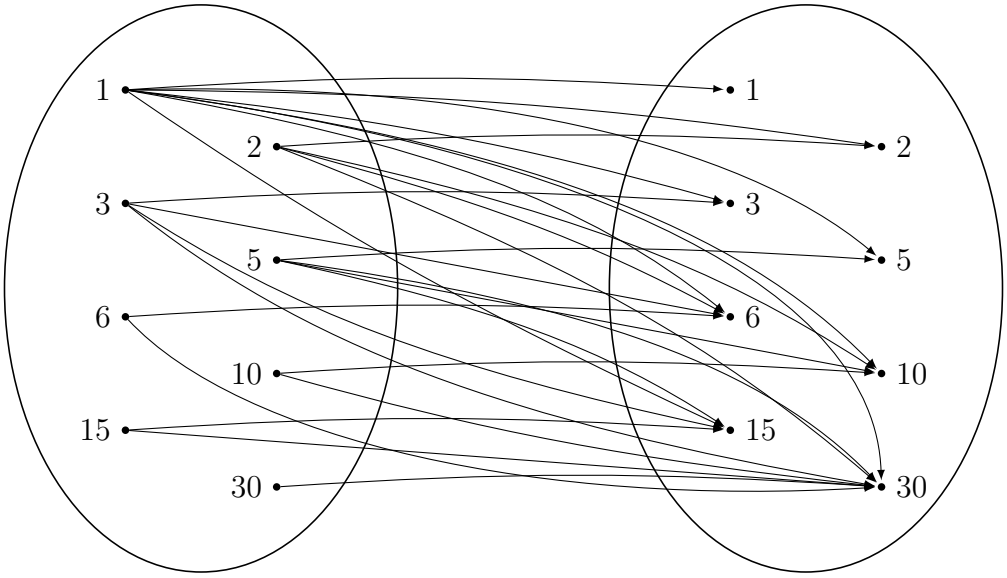
Wat de notatievoorwaarden van een relatie betreft, wordt ook wel de zogenaamde exponentiële notatie gebruikt. Als $(a, b) \in \Re_1$ dan schrijven we $b = a^{\Re_1}$. Dit heeft dan wel als gevolg dat wat de samenstelling betreft, voor $(a, b) \in \Re_1$ en $(b, c) \in \Re_2$, we de samenstelling anders zullen noteren, namelijk als $\Re_1 \Re_2$, wat dan weer zinvol is, want $a^{\Re_1 \Re_2} = (a^{\Re_1})^{\Re_2} = b^{\Re_2} = c$.

1.3.2 Bijzondere relaties

Bij de definitie van een relatie van een verzameling A naar een verzameling B hebben we geen restricties gelegd op het bestaan van de beelden: een element van A kan meerdere, één of geen enkel beeld hebben. Naargelang het aantal beelden dat de elementen van A hebben, willen we nu een voorlopige classificatie opmaken van de soorten relaties van A naar B.

Definitie 1.12

Een *functie* van A naar B is een relatie van A naar B waarbij elk element van A hoogstens één beeld heeft.



Figuur 1.3: $\mathcal{D}_{|\{1,2,3,5,6,10,15,30\}\times\{1,2,3,5,6,10,15,30\}}$

Definitie 1.13

Een *afbeelding* van A naar B is een relatie van A naar B waarbij elk element van A juist één beeld heeft.

Relaties kunnen grafisch voorgesteld worden met een zogenaamde pijlenvoorstelling. Figuur 1.3.2 is de pijlenvoorstelling van de beperking van $\mathcal{D}$ tot $\{1, 2, 3, 5, 6, 10, 15, 30\} \times \{1, 2, 3, 5, 6, 10, 15, 30\}$.

In de pijlenvoorstelling van een functie van A naar B vertrekt in elk element van A ten hoogste één pijl. In de pijlenvoorstelling van een afbeelding van A naar B vertrekt in elk element van A juist één pijl. Indien $A = B$ dan spreken we soms van een *transformatie in* A in plaats van afbeelding van A naar A.

Elke afbeelding is dus een functie, maar niet omgekeerd. Overigens is het duidelijk dat het omgekeerde van een afbeelding (in het bijzonder van een functie) niet noodzakelijk een afbeelding is.

Opmerking

We kunnen een eerder filosofische discussie opstarten rond de verschillen tussen een functie en een afbeelding, in het bijzonder wat de benaming van de

beginverzameling A betreft. In de theorie van de functies wordt de deelverzameling van A waar de pijlen vertrekken, en dus de functie gedefinieerd is, meestal de *definitieverzameling* of het *definitiegebied* genoemd. Een afbeelding is dan in deze context een functie waarbij het definitiegebied samenvalt met de beginverzameling. Een analoog onderscheid kan overigens gemaakt worden naar de beeldenverzameling toe, die dus een (al dan niet eigenlijke) deelverzameling is van de eindverzameling B. In de analyse wordt eerder gesproken over A-B-functies. Anderzijds wordt daar ook gesproken over *reële functies*, waarbij eigenlijk alleen bedoeld wordt dat de begin- en eindverzameling een deelverzameling is van de verzameling $\mathbb{R}$ van de reële getallen.

Ook de begrippen *domein* voor beginverzameling en *codomein* voor eindverzameling komen voor, maar om de verwarring nog groter te maken, zal in vele handboeken analyse (en ook in de cursus analyse) de term *domein* gebruikt worden als een synoniem voor *definitiegebied* eerder dan voor de term *beginverzameling*. De context zal moeten duidelijk maken wat bedoeld wordt.

Definitie 1.14

(i) Een relatie $\Re \subset A \times B$ is *injectief* als en slechts als elk element van B het beeld is van hoogstens één element van A.

(ii) Een relatie $\Re \subset A \times B$ is *surjectief* als en slechts als elk element van B het beeld is van minstens één element van A.

(iii) Een relatie $\Re \subset A \times B$ is *bijectief* als en slechts als $\Re$ injectief en surjectief is.

Een alternatieve manier om een de injectiviteit te omschrijven is als volgt. Een relatie $\Re \subset A \times B$ is injectief als en slechts als de volgende implicatie waar is:

$$(x, b) \in \Re \,\text{en}\, (y, b) \in \Re \Longrightarrow x = y$$

Een injectieve afbeelding van A naar B wordt ook kortweg een *injectie van A in B* genoemd. Een surjectieve afbeelding van A naar B wordt ook kortweg een *surjectie van A op B* genoemd.

Een bijectieve afbeelding van A naar B wordt ook kortweg een *bijectie van A op B* genoemd. Elk element van B is dus het beeld van juist één element van A, en omdat een bijectie een afbeelding is, heeft elk element van A ook juist één element van B als beeld. Als $\Re$ dus een bijectie is, dan is de omgekeerde relatie $\Re^{-1}$ dus ook een afbeelding, en noodzakelijk bijectief. Wanneer er een bijectie bestaat van A naar B (en dus ook van B in A) dan zeggen we dat beide verzamelingen *gelijkmachtig* zijn. Voor

eindige verzamelingen betekent dit eigenlijk dat deze verzamelingen evenveel elementen bezitten. Een bijectie van een verzameling A op zichzelf wordt een *permutatie* genoemd. Voor een eindige verzameling correspondeert dit begrip inderdaad met ons intuïtief begrip van permuteren van een aantal elementen, in de betekenis van verwisselen van volgorde van deze elementen, hierover meer in Hoofdstuk 7.

- Het is duidelijk dat $\mathcal{D}$ surjectief is, elk element $b \in \mathbb{N}$ heeft minstens één deler (zelfs twee als $b \neq 1$), maar $\mathcal{D}$ is niet injectief.
- De functie $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is noch injectief noch surjectief. De beperking van f tot $\mathbb{R}^+ \times \mathbb{R}^+$ is bijectief

1.3.3 Bijzondere relaties in één verzameling

We bespreken in deze paragraaf enkele bijzondere relaties van een verzameling naar zichzelf. Daartoe definiëren we eerst formeel enkele eigenschappen waar dergelijke relaties aan kunnen voldoen. We noemen een koppel (a, a), $a \in A$, een *identiek koppel in* A^2.

Definitie 1.15

Een relatie $\Re \subset A^2$ is *reflexief* als en slechts als alle identieke koppels in A^2 tot $\Re$ behoren. Een relatie $\Re \subset A$ is *antireflexief* als geen enkel identiek koppel in A^2 tot $\Re$ behoort.

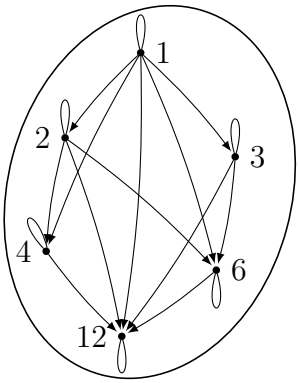
We kunnen deze definities ook zeer formeel noteren. Een relatie $\Re \subset A^2$ is reflexief als en slechts als

$$\{(x, x) \| x \in A\} \subset \Re\,.$$

Een relatie $\Re \subset A^2$ is antireflexief als en slechts als

$$\{(x, x) \| x \in A\} \cap \Re = \emptyset\,.$$

Een *niet-reflexieve* relatie is een relatie die niet alle identieke koppels bevat, en is dus niet noodzakelijk een antireflexieve relatie. In de pijlenvoorstelling op één verzameling van een relatie, wordt een identiek koppel voorgesteld door een lus (zonder pijl). In een reflexieve relatie komen in de pijlenvoorstelling alle lussen voor. In een niet-reflexieve relatie komen sommige lussen niet voor. In een antireflexieve relatie komen nooit lussen voor. Figuur 1.3.3 is de pijlenvoorstelling van de beperking van $\mathcal{D}$ tot $\{1, 2, 3, 4, 6, 12\} \times \{1, 2, 3, 4, 6, 12\}$.



Figuur 1.4: pijlenvoorstelling van $\mathcal{D}_{\{1,2,3,4,6,12\}\times\{1,2,3,4,6,12\}}$

Definitie 1.16

Een relatie $\Re \subset A^2$ is *symmetrisch* als en slechts als voor alle $x, y \in A$ de volgende implicatie waar is:

$$(x, y) \in \Re \Longrightarrow (y, x) \in \Re$$

Een relatie $\Re \subset A$ is *antisymmetrisch* als en slechts als voor alle $x, y \in A$ met $x \neq y$ de volgende implicatie waar is:

$$(x, y) \in \Re \Longrightarrow (y, x) \notin \Re$$

De definitie van de antisymmetrische eigenschap is equivalent met de volgende: $\Re$ is antisymmetrisch als en slechts als voor alle $x, y \in A$, $(x, y) \in \Re$ en $(y, x) \in \Re$ impliceert dat $x = y$. Een niet-symmetrische relatie is een relatie die niet aan de symmetrische eigenschap voldoet. Dit is dus niet noodzakelijk een antisymmetrische relatie.

Definitie 1.17

Een relatie $\Re \subset A^2$ is *transitief* als en slechts als voor alle $x, y, z \in A$ de volgende implicatie waar is:

$$(x, y) \in \Re \,\text{en}\, (y, z) \in \Re \Longrightarrow (x, z) \in \Re$$

Definitie 1.18

(i) Een relatie $\Re \subset A^2$ is een *partiële orderelatie* als en slechts als $\Re$ reflexief, antisymmetrisch en transitief is.

(ii) Een orderelatie $\Re \subset A^2$ is *totaal* als en slechts als voor alle $x, y \in A$ $(x, y) \in \Re$ of $(y, x) \in \Re$.

Een orderelatie $\Re \subset A^2$ wordt soms ook als $\preceq$ genoteerd.

Voorbeeld 1.19.

- Het standaardvoorbeeld van een totale orderelatie is $\leq$ in $\mathbb{R}$. Ook in de getallenverzamelingen $\mathbb{N}$, $\mathbb{Z}$ en $\mathbb{Q}$ is $\leq$ een totale orderelatie.
- Voor een gegeven verzameling A, is $\subset$ een partiële orderelatie in $\mathcal{P}(A)$.
- De deelbaarheidsrelatie $\mathcal{D}$ is een partiële orderelatie in $\mathbb{N} \setminus \{0\}$. Merk op dat we hier stilzwijgend de *beperking van* $\mathcal{D}$ tot $\mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\}$ beschouwen.

Definitie 1.20

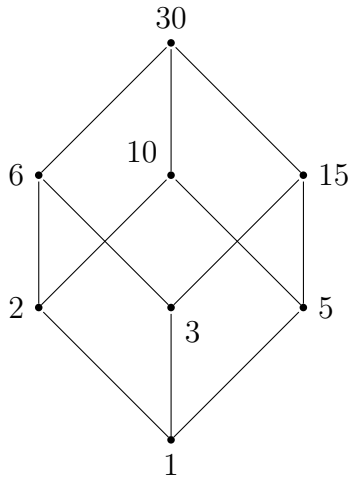
Een relatie $\Re \subset A^2$ is een *strikt-orderelatie* als en slechts als $\Re$ antireflexief en transitief is.

Het is duidelijk dat $<$ en $>$ in de getallenverzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ voorbeelden van strikt-orderelaties zijn.

Een verzameling A en een partiële orderelatie $\preceq$ kunnen we grafisch voorstellen door een zogenaamd *Hassediagram*. Een ketting van opeenvolgende koppels (a_1, a_2), (a_2, a_3), ..., (a_{n-1}, a_n) in $\preceq$ wordt voorgesteld door de opeenvolgende elementen a_i en a_{i+1} met elkaar te verbinden. Indien A eindig is en elke ketting een kleinste en grootste element heeft met betrekking tot $\preceq$, dan illustreert een Hassediagram $\preceq$ volledig. Figuur 1.3.3 is het Hassediagram van de beperking van $\mathcal{D}$ tot $\{1, 2, 3, 5, 6, 10, 15, 30\} \times \{1, 2, 3, 5, 6, 10, 15, 30\}$. Merk op dat uit de context duidelijk is dat bv. $(1, 2) \in \mathcal{D}$ en niet $(2, 1) \in \mathcal{D}$. Een Hassediagram maakt normaal gezien geen gebruik van pijlen om dit aan te geven, de context zal echter steeds duidelijkheid verschaffen.

Definitie 1.21

Een relatie $\Re \subset A^2$ is een *equivalentierelatie* als en slechts als $\Re$ reflexief, symmetrisch en transitief is.



Figuur 1.5: Hassediagram van $\mathcal{D}_{\{1,2,3,5,6,10,15,30\}\times\{1,2,3,5,6,10,15,30\}}$

Eenvoudige voorbeelden van equivalentierelaties zijn

- "zelfde leeftijd hebben" (in bijvoorbeeld de verzameling van alle studenten van het eerste bachelorjaar wiskunde);
- "parallellisme van rechten (in bijvoorbeeld het Euclidisch vlak);
- "zelfde rest bezitten na deling door een natuurlijk getal m (in de verzameling van de gehele getallen)".

Stel dat $\equiv$ een equivalentierelatie is over A. Gegeven een element $a \in A$, dan kunnen we alle elementen $b \in A$ beschouwen die equivalent zijn met a. Deze elementen vormen een deelverzameling B van A, en omwille van de drie eigenschappen waaraan een equivalentierelatie voldoet, staan alle elementen van B onderling in relatie tot elkaar en zichzelf. We noemen de verzameling B een *equivalentieklasse* van de equivalentierelatie $\Re$. We zullen voorlopig de equivalentieklasse die het element a bevat noteren door $[a]$ en noemen a een *representant* van deze klasse. Merk overigens op dat als $b \equiv a$, uiteraard $[b] = [a]$, of nog dat elk element van $[a]$ als representant van deze klasse kan genomen worden. Uit de definitie volgt onmiddellijk dat geen enkele equivalentieklasse ledig kan zijn, dat twee verschillende equivalentieklassen altijd een ledige doorsnede hebben en dat bovendien de unie van alle equivalentieklassen de volledige verzameling A is. In de verzamelingenleer wordt elke verzameling van deelverzamelingen van A die de eigenschap bezit dat geen enkele deelverzameling ledig is en zodanig dat elk element van A tot juist

één dergelijke deelverzameling behoort, een *partitie* genoemd van A. Het is nu duidelijk dat elke equivalentierelatie in een verzameling A aanleiding geeft tot een partitie van A, maar ook omgekeerd dat elke partitie van A aanleiding geeft tot een equivalentierelatie van A. Met andere woorden de begrippen *equivalentierelatie* en *partitie* zijn "equivalente" of gelijkwaardige begrippen. Wanneer $\Re$ een equivalentierelatie is over de verzameling A, dan noteren we de verzameling van equivalentieklassen ook soms als $A/\Re$.

1.3.4 Het axioma van de goede ordening

Naast de natuurlijke ordening in $\mathbb{Z}$, moeten we ook nog aandacht besteden aan een andere wetmatigheid. Noem X een willekeurige deelverzameling van $\mathbb{Z}$, dan zeggen we dat het geheel getal b een *benedengrens* is voor X als $b \leq x$, $\forall x \in X$. Een benedengrens voor een verzameling X, die eveneens tot deze verzameling behoort, wordt *het kleinste element* van X genoemd.

De volgende wetmatigheid of *axioma* is gekend onder de naam *het axioma van de goede ordening* of het *well–ordening axioma*.

axioma van de goede ordening in $\mathbb{Z}$

Als X een deelverzameling is van $\mathbb{Z}$, verschillend van de ledige deelverzameling, die een benedengrens heeft, dan bezit X een kleinste element.

Dat dit een eigenschap is die geldt voor de gehele getallen mag duidelijk zijn, maar deze eigenschap geldt niet meer in de verzameling van de rationale getallen. Zo zal bijvoorbeeld de verzameling $X = \{\frac{1}{n} \| n \in \mathbb{N}^*\}$ wel degelijk een benedengrens bezitten in $\mathbb{Q}$ (bv. 0), maar X bezit geen kleinste element.

1.4 Recursieve definities

Als X een deelverzameling is van $\mathbb{N}$ of van $\mathbb{N}^*$, dan heeft het automatisch een benedengrens. Bijgevolg zal het axioma van de goede ordening hier de volgende vorm aannemen.

axioma van de goede ordening in $\mathbb{N}$

Als X een niet-ledige deelverzameling is van $\mathbb{N}$ of $\mathbb{N}^*$, dan bezit X een kleinste element.

Dit axioma van de goede ordening geeft ons de gelegenheid om een veel gebruikte procedure te rechtvaardigen. We komen immers geregeld functies

tegen zoals

$$\begin{array}{rccc} u: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & 3n+2 \end{array}$$

Het is dan geen probleem om voor een specifieke waarde van n het getal $u(n)$ uit te rekenen. Een andere methode om een functie te definiëren is de *recursie* of *recursieve definitie*. In dit geval wordt de functie u met behulp van een uitdrukking geformuleerd die zelf u weer bevat (een dergelijke uitdrukking wordt een *recurrente betrekking* genoemd), zoals in het volgende voorbeeld, waarbij de zogenaamde *Fibonacci getallen* gedefinieerd worden.

$$u(1) := 1, \quad u(2) := 1, \quad u(n) := u(n-1) + u(n-2) \ \ (n \geq 3).$$

Wij hebben dan geen enkel probleem om de **opeenvolgende** waarden van $u(n)$ te berekenen. Het is de gewoonte de waarden $u(n)$ als u_n te noteren. De rij van de waarden, geordend volgens stijgende waarden van n, wordt genoteerd als $(u_n)_{n\in\mathbb{N}}$.

Alhoewel dit op het eerste zicht triviaal lijkt, hebben wij het axioma van de goede ordening nodig om aan te tonen dat er voor elke n een unieke u_n is gedefinieerd. Inderdaad veronderstel dat er een natuurlijk getal n bestaat waarvoor u_n niet uniek bepaald is. Als gevolg van het axioma van de goede ordening, bestaat er een kleinste positief getal m met deze eigenschap. Aangezien u_1 en u_2 expliciet gegeven zijn, moet $n \geq 3$ en zal dus $u_m = u_{m-1} + u_{m-2}$. Wegens de definitie van m echter, zijn u_{m-1} en u_{m-2} uniek bepaald, zodat de som van deze getallen, met name het getal u_m uniek bepaald is, hetgeen tegen de veronderstelling is. Bijgevolg is elke u_n uniek gedefinieerd.

Een ander voorbeeld van een recursieve definitie, is de volgende

$$s_1 = 1, \quad s_n = s_{n-1} + (2n-1) \ \ (n \geq 2).$$

Dergelijke recursieve definitie kan verkort voorgesteld worden door

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

en is dus, als gevolg van het axioma van de goede ordening, een geldige definitie in $\mathbb{N}^*$. Merk echter op dat voor de effectieve berekening, bvb met de computer, de recursieve definitie $s_1 = 1,\ s_n = s_{n-1} + (2n-1)$ $(n \geq 2)$ gebruikt moet worden.

Een ander voorbeeld van verkorte schrijfwijze van een recursieve definitie vinden wij bij producten. Zo weten wij dat

$$n! := \prod_{i=1}^{n} i,$$

Soms zullen we ook de notatie $a_1 + \cdots + a_n$ gebruiken ipv. $\sum_{i=1}^{n} a_i$ en $a_1 \cdots a_n$ voor $\prod_{i=1}^{n} a_i$.

1.5 Het inductieprincipe

Veronderstel dat er gevraagd wordt om de volgende formule te bewijzen

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

Met andere woorden, er wordt gevraagd te bewijzen dat de recursief gedefinieerde uitdrukking in het linkerlid gelijk is aan de formule in het rechterlid, en dit voor alle waarden van n.

Om dit te bewijzen, kunnen we als volgt te werk gaan. De formule is zeker correct voor $n = 1$, aangezien $1 = 1^2$. Veronderstel dat de formule correct is voor een specifieke waarde k, met andere woorden

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

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

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \sum_{i=1}^{k}(2i-1) + 2k + 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2.\end{aligned}$$

Aangezien we reeds hebben opgemerkt dat de formule correct is voor $n = 1$, is zij bijgevolg ook correct voor $n = 2$, en om dezelfde reden is zij dan geldig voor elke andere waarde van n.

Een dergelijke bewijsvoering steunt op het *inductieprincipe*. Het is een zeer eenvoudige, maar uitermate bruikbare techniek. Het is terug een gevolg van het axioma van de goede ordening in $\mathbb{N}$ (of $\mathbb{N}^*$) dat een dergelijke bewijsvoering correct is, zoals mag blijken uit de volgende stelling.

Stelling 1.22

Veronderstel dat S een deelverzameling van $\mathbb{N}^*$ is waarvoor een bepaalde uitdrukking waar is en dat S aan de volgende voorwaarden voldoet.

1. $1 \in S$.
2. Voor elke $k \in \mathbb{N}^*$ geldt: $k \in S$ impliceert dat $k+1 \in S$.

Dan is $S = \mathbb{N}^*$.

Bewijs. Indien de conclusie niet waar zou zijn, en bijgevolg $S \neq \mathbb{N}^*$, dan is het complement van S ten opzichte van $\mathbb{N}^*$, maw $S^c = \{r \in \mathbb{N}^* \| r \notin S\}$ een niet-ledige deelverzameling van $\mathbb{N}^*$. Als gevolg van het axioma van de goede ordening, 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 $k = m-1$ in de 2de voorwaarde van de stelling, dan volgt hieruit dat $m \in S$, bijgevolg een tegenstrijdigheid. Dus we mogen besluiten dat $S = \mathbb{N}^*$. □

Opmerking

Het feit dat het resultaat waar is voor $n = 1$ wordt soms de *inductiebasis* genoemd, terwijl de veronderstelling dat de uitdrukking waar is voor $n = k$ de *inductiehypothese* wordt genoemd. We merken ook op dat wij ook als inductiebasis $n = 0$ hadden kunnen nemen. In feite kan *elke* waarde als inductiebasis dienen. Natuurlijk moet men erop toezien dat er wel degelijk een bewijs geleverd wordt voor alle mogelijke waarden van n. Neemt men bijvoorbeeld $n = 5$ als inductiebasis, dan dienen de waarden $k < 5$ doorgaans afzonderlijk behandeld te worden, tenzij natuurlijk 5 de eerste zinvolle waarde is voor n. Daarenboven wordt soms als inductiehypothese aangenomen dat een uitdrukking waar is voor alle waarden kleiner dan k. Men spreekt dan soms van het *sterk inductieprincipe*.

Het inductieprincipe is een zeer belangrijk principe dat kan gebruikt worden voor bewijsvoeringen door middel van inductie.

1.6 Het ladenprincipe van Dirichlet

ladenprincipe van Dirichlet

Indien m objecten verdeeld moeten worden over n laden, dan zal minstens 1 lade meer dan 1 object bevatten indien er meer objecten zijn dan laden.

Dit zeer eenvoudig principe, wordt het *ladenprincipe* genoemd, maar is ook onder verschillende andere namen gekend zoals het *duivenhokprincipe*, in het Engels wordt dit principe het *pigeonhole principle* genoemd.

Voorbeelden

Alhoewel dit een zeer 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 $\mathbb{N}[0, m-1]$. Om het ladenprincipe te kunnen toepassen, moeten we echter nog bewijzen dat het waardegebied een eigenlijke deelverzameling is van $\mathbb{N}[0, m-1]$. 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 $\mathbb{N}[0, m-1]$ 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.

1.7 Eindige en oneindige verzamelingen

Bij de basisdefinities van de verzamelingenleer hebben we het reeds gehad over eindige verzamelingen als verzamelingen met een eindig aantal elementen. We kunnen dit nu wat meer wiskundig formuleren.

Definitie 1.23

Een verzameling X, zodanig dat er een bijectie bestaat van de verzameling $\mathbb{N}[1, n]$ naar X, wordt een *eindige* verzameling genoemd. We noemen n de *orde* van X. Elke verzameling die niet eindig is wordt een *oneindige* verzameling genoemd.

Alhoewel de volgende stelling op het eerste gezicht triviaal lijkt, is het toch de moeite hierop in te gaan.

Stelling 1.24

Een niet-ledige verzameling X is een oneindige verzameling dan en slechts dan als er een injectie bestaat van $\mathbb{N}^*$ naar X.

Bewijs. Veronderstel dat X een oneindige verzameling is. Dan kunnen wij steeds op de volgende recursieve manier een functie f van $\mathbb{N}^*$ naar X definiëren. Noem $f(1)$ een willekeurig element van X; indien $f(1), \ldots, f(k)$ gedefinieerd zijn, dan kiezen wij voor $f(k+1)$ een willekeurig element van X verschillend van $f(1), \ldots, f(k)$. Bijgevolg is f een injectie. Bovendien is $f(k+1)$ steeds gedefinieerd, want anders zou $X = \{f(1), f(2), \ldots, f(k)\}$ zodat f een bijectie zou zijn van X naar $\mathbb{N}[1, k]$, maar dit is tegen de veronderstelling dat X een oneindige verzameling is.

Veronderstel nu omgekeerd dat er een injectie f bestaat van $\mathbb{N}^*$ naar X. Indien X eindig zou zijn, dan zou er een bijectie β van $\mathbb{N}[1, n]$ naar X bestaan voor een zekere n. Bijgevolg bestaat de volgende ketting van injecties:

$$\mathbb{N}[1, n+1] \xrightarrow{i} \mathbb{N}^* \xrightarrow{f} X \xrightarrow{\beta^{-1}} \mathbb{N}[1, n].$$

Hierbij is i de zogenaamde *inclusie-injectie* ($i(k) = k$). De samenstelling van al deze injecties, is terug een injectie α van $\mathbb{N}[1, n+1]$ naar $\mathbb{N}[1, n]$, maar dit is onmogelijk wegens het ladenprincipe. Bijgevolg moet X een oneindige verzameling zijn. □

Merk op dat de injectie f, waarvan sprake is in het bewijs van de bovenstaande stelling, niet noodzakelijk een bijectie is.

Definitie 1.25

Een oneindige verzameling X wordt *aftelbaar* genoemd, als er een bijectie bestaat van $\mathbb{N}$ (of $\mathbb{N}^*$) op X. Indien dit niet het geval is, dan noemen we X een *niet-aftelbare* verzameling.

Bijgevolg kunnen we onder de oneindige verzamelingen nog een onderscheid maken tussen de aftelbare en de niet-aftelbare verzamelingen. Het ligt voor de hand dat we eindige verzamelingen eveneens als aftelbare verzamelingen beschouwen. Een niet-aftelbare verzamelingwordt ook een *over-aftelbare* verzameling genoemd. De theorie met betrekking tot de aftelbare verzamelingen zou men kunnen beschouwen als het domein van de discrete wiskunde, dit in tegenstelling tot de theorie met betrekking tot de niet-aftelbare verzamelingen (zoals $\mathbb{R}$, zie later) die tot het domein van de analyse behoort.

Merk op dat de oneindige verzamelingen eigenlijke deelverzamelingen kunnen bezitten die zelf oneindige verzamelingen zijn. Zo is bijvoorbeeld de verzameling van de even natuurlijke getallen een eigenlijke deelverzameling van $\mathbb{N}$.

1.7.1 Aftelbaarheid en niet-aftelbaarheid van enkele getallenverzamelingen

Stelling 1.26

De verzameling van de gehele getallen is aftelbaar.

Bewijs. Beschouw de afbeelding f van $\mathbb{N}$ naar $\mathbb{Z}$ gedefinieerd door

$$f(n) = \begin{cases} \frac{n}{2} & \text{als } n \text{ even is} \\ -\frac{n+1}{2} & \text{als } n \text{ oneven is.} \end{cases}$$

Deze afbeelding is inderdaad een bijectie en de (strikt-geordende) waardeverzameling van f, of de *rij* van de waarden is $(0, -1, 1, -2, 2, -3, 3, \ldots)$.□

Stelling 1.27

De verzameling $\mathbb{Q}$ van de rationale getallen is aftelbaar.

Bewijs. We beschrijven een bijectie f van $\mathbb{N}$ op $\mathbb{Q}$ waarvan de rij van waarden er als volgt uitziet:

$$(0, -1, 1, -2, -1/2, 1/2, 2, -3, -3/2, -2/3, -1/3, 1/3, 2/3, 3/2, 3, \ldots).$$

Om de plaats van a/b in deze rij te bepalen, gaan we als volgt te werk. We bepalen eerst zogenaamde *niveaus*. Op niveau 0 komt enkel het getal 0. Voor het bepalen van de andere niveau's veronderstellen wij dat de breuk een niet-vereenvoudigbare breuk is met $a \neq 0$ en dat $b > 0$. Wij noemen $n = \max(|a|, b)$ (met $|a|$ de absolute waarde van a) het niveau van de breuk a/b. Per niveau worden alle rationale getallen op dit niveau gerangschikt volgens de orderelatie $<$ van $\mathbb{Q}$. Op die manier ontstaat een lijst van de volgende gedaante.

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
$\vdots$	$\vdots$							

Elk rationaal getal komt op die manier juist één maal voor in deze lijst. Aangezien er nu voor elk natuurlijk getal n slechts een eindig aantal rationale getallen a/b bestaan van niveau $n = \max(|a|, b)$, volgt hieruit dat $\mathbb{Q}$ inderdaad aftelbaar is. □

Stelling 1.28

De verzameling $\mathbb{R}$ is een niet-aftelbare verzameling.

Bewijs. We bewijzen de stelling door aan te tonen dat het interval $[0, 1[$ van $\mathbb{R}$ een niet-aftelbare verzameling is. Veronderstel het tegendeel. Dan is er, wegens de definitie van aftelbaarheid, een bijectie f van $\mathbb{N}$ op het interval $[0, 1[$, en ontstaan de volgende waarden:

$$\begin{aligned} f(0) &= 0, a_0 b_0 c_0 d_0 \ldots \\ f(1) &= 0, a_1 b_1 c_1 d_1 \ldots \\ f(2) &= 0, a_2 b_2 c_2 d_2 \ldots \\ f(3) &= 0, a_3 b_3 c_3 d_3 \ldots \\ \vdots &\quad \vdots \end{aligned}$$

Hierbij staan $a_i, b_i, \ldots$ voor één van de cijfers 0 tot en met 9.

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

$$x = 0, x_1 x_2 x_3 x_4 \ldots$$

waarbij

$$\begin{array}{rcl} x_1 & = & \begin{cases} a_0 + 1 & \text{als } a_0 \leq 7 \\ a_0 - 1 & \text{als } a_0 \geq 8 \end{cases} \\ x_2 & = & \begin{cases} b_1 + 1 & \text{als } b_1 \leq 7 \\ b_1 - 1 & \text{als } b_1 \geq 8 \end{cases} \\ x_3 & = & \begin{cases} c_2 + 1 & \text{als } c_2 \leq 7 \\ c_2 - 1 & \text{als } c_2 \geq 8 \end{cases} \\ \vdots & & \vdots \end{array}$$

Als bijvoorbeeld de lijst vanwaar wij vertrekken op de volgende manier begint:

$$\begin{array}{rcl} f(0) & = & 0,772563\ldots \\ f(1) & = & 0,092971\ldots \\ f(2) & = & 0,000000\ldots \\ f(3) & = & 0,000722\ldots \\ f(4) & = & 0,000998\ldots \\ f(5) & = & 0,227354\ldots \\ & \vdots & \end{array}$$

Dan zal het getal x beginnen als $0,881885\ldots$. De juiste definitie van x doet er niet toe, het is alleen belangrijk om te bewijzen dat x niet in de lijst getallen waarvan wij vertrokken zijn, kan voorkomen. Inderdaad, voor $n = 0, 1, 2, \ldots$ zal het getal x met het getal $f(n)$ verschillen op de $(n+1)$de plaats na de komma. Bijgevolg zal het interval $[0, 1[$ en dus ook de verzameling $\mathbb{R}$ niet aftelbaar zijn. □

Opmerking

Het feit dat $\mathbb{Q}$ aftelbaar is, kan misschien meer verwonderlijk schijnen dan voor $\mathbb{Z}$ aangezien er tussen elke 2 rationale getallen oneindig veel andere rationale getallen gelegen zijn. Het bewijs steunt echter op een volledige andere strikt-ordening dan de natuurlijke strikt-ordening $<$ van de rationale getallen.

1.7.2 Kardinaalgetallen

We herhalen de volgende definitie.

Definitie 1.29

Twee verzamelingen A en B zijn *gelijkmachtig* als en slechts als er een bijectie bestaat van A naar B.

Een eindige verzameling A is dus bijectief met de verzameling $\mathbb{N}[1, n]$ voor een zeker natuurlijk getal n. Dit getal is uiteraard gewoon gelijk aan het aantal elementen in de gegeven verzameling. We noemen in dit geval n ook het *kardinaalgetal van* A. De uitbreiding van dit begrip voor oneindige verzamelingen is echter geen eenvoudige opgave, alhoewel ze dat misschien intuïtief wel lijkt.

Men zou kunnen gebruik maken van het begrip gelijkmachtigheid om een definitie te geven, door in de klasse van gelijkmachtige verzamelingen een representant te kiezen en deze het kardinaalgetal van alle verzamelingen uit deze klasse te noemen. Dit vereist dat we gelijkmachtigheid als een relatie tussen verzamelingen gaan beschouwen, hetgeen, volgens onze definitie van relatie, dus betekent dat we een deelverzameling van $U \times U$ beschouwen met U de verzameling van ... alle verzamelingen! We hebben echter op het einde van paragraaf 1.1 gezien dat het veronderstellen dat deze verzameling bestaat, leidt tot de paradox van Russell.

Het enige wat we momenteel kunnen doen is de gekende oneindige verzamelingen met elkaar vergelijken en ze al dan niet hetzelfde kardinaalgetal toekennen. We kunnen hier geen definitie geven van het kardinaalgetal van een oneindige verzameling, maar we beperken ons tot het opschrijven van enkele eigenschappen waarvan we intuïtief denken dat ze gelden voor kardinaalgetallen. Het kardinaalgetal van een verzameling X noteren we als $|X|$.

Het kardinaalgetal van een oneindige, aftelbare verzameling noteren we als $\aleph_0$ (aleph-nul). Beschouw nu de afbeelding f gedefinieerd door $f(n) = n+1$, $\forall n \in \mathbb{N}$. Dan is f een bijectie van $\mathbb{N}$ op $\mathbb{N}^*$, en bijgevolg is $|\mathbb{N}^*| = |\mathbb{N}| = \aleph_0$. Anderzijds is

$$\mathbb{N} = \mathbb{N}^* \cup \{0\},$$

zodat, indien we de optelling van eindige kardinaalgetallen tot de oneindige kardinaalgetallen willen uitbreiden,

$$\aleph_0 = \aleph_0 + 1.$$

Dit betekent bijvoorbeeld dat bij het rekenen met oneindige kardinaalgetallen de schrappingswet niet geldt, want anders zou $0 = 1$. De ogenschijnlijke paradox is het gevolg van het feit dat er bijecties bestaan van de verzameling $\mathbb{N}$ naar eigenlijke deelverzamelingen van $\mathbb{N}$.

Door Stellingen 1.26 en 1.27 geldt dat $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

Het is wel degelijk de bedoeling om met kardinaalgetallen te *rekenen*. In die zin vormen de kardinaalgetallen een uitbreiding van de natuurlijke getallen. De volgende regels gelden dus.

$$|X| + |Y| = |X \cup Y|, \text{ als } X \text{ en } Y \text{ disjuncte verzamelingen zijn.}$$

$|X|^{|Y|} = |X^Y|$, met X^Y de verzameling van alle afbeeldingen van X naar Y.

De tweede rekenregel stelt ons in staat om $2^{|X|}$, het kardinaalgetal van de verzameling van alle deelverzamelingen van een gegeven verzameling X te *berekenen*. Definiëren we $g : \mathcal{P}(X) \to X^{\{0,1\}} : A \mapsto f$, met $f : A \to \{0, 1\}$: $f(a) = 0 \iff a \notin A$ en $f(a) = 1 \iff a \in A$, dan is g een bijectie van $\mathcal{P}(X)$ naar $X^{\{0,1\}}$ en dus $2^{|X|} = |\mathcal{P}(X)|$. Hieruit volgt ook dat $2^{\aleph_0}$ het kardinaalgetal is van $\mathbb{R}$. De *continuumhypothese* stelt dat er geen kardinaalgetal ζ bestaat waarvoor $\aleph_0 < \zeta < 2^{\aleph_0}$.

1.8 Het somprincipe

Dit principe is evenals het ladenprincipe elementair. We formuleren het als een stelling.

Stelling 1.30

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. Oefening. Bewijs dit principe door te steunen op het inductieprincipe. □

Dit principe geeft ons de mogelijkheid om het ladenprincipe in een meer algemene vorm te formuleren.

ladenprincipe (algemene vorm)

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.

1.9 Noten

- Het is duidelijk dat de term "cartesisch product" afkomstig is van het begrip "cartesisch assenstelsel" waarbij bvb voor elk punt van de driedimensionale ruimte met coördinaten in de verzameling $\mathbb{R}$ van de reële getallen, elk punt uniek bepaald is door zijn coördinaat (x, y, z). Op zijn beurt verwijst cartesisch naar de Franse filosoof René Descartes (1596 – 1650), die in zijn werk *La géométrie*, de toepassing beschrijft van de algebra in de studie van de meetkunde, hetgeen dan geleid heeft tot de term cartesisch of cartesiaans assenstelsel.

- Venndiagrammen werden geïntroduceerd door John Venn, 1834 – 1923, Engels wiskundige en logicus. Hij deed dit ter ondersteuning van zijn onderzoek naar de uitbreiding van Boole's wiskundige logica.

- August De Morgan (1806 – 1871) was de eerste professor in wiskunde aan het University College London. Een belangrijk element in het werk van De Morgan is de behandeling van algebra als een pure symbolisch-logische discipline. Hij deed verder voornamelijk onderzoek in wiskundige logica, en zijn wetten (Stelling 1.4 (4)) zijn in deze context ontstaan.

- Het symmetrisch verschil in de wiskunde is de exclusieve of in de informatica.

- De eerste 10 termen uit de rij van Fibonacci zijn gelijk aan: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55. Deze rij komt in veel situaties voor. Fibonacci (in feite de bijnaam van Leonardo van Pisa (1180 – 1250)) zou de rij als volgt hebben gedefinieerd. Een konijnenpaar krijgt iedere maand een paar jongen. Ieder nieuw paar krijgt vanaf de tweede maand ook weer steeds een paar jongen. Hoeveel konijnenparen zijn er aan het eind van iedere maand? In de literatuur is er heel wat te vinden over Fibonacci en bijvoorbeeld over het verband met de gulden snede.

- De theorie van de oneindige kardinaalgetallen werd ontwikkeld door Georg Cantor (1845–1918). David Hilbert kon Cantor's werk wel appreciëren, getuige daarvan zijn uitspraak "Aus dem Paradies, das Cantor uns geschaffen hat, soll uns niemand vertreiben können" (1925).

- Het inductieprincipe is één van de axioma's die Giuseppe Peano (1858 – 1932) heeft opgesteld met het oog op de axiomatische opbouw van de natuurlijke getallen.

Hoofdstuk 2

Elementaire logica en waarheidstabellen

2.1 Propositielogica

Een van de meest moeilijke taken van een wiskundige is de opdracht om een goed onderbouwde en overtuigende bewijsvoering op te stellen. De algemene opinie die de man in de straat heeft over wiskunde, stelt wiskunde gelijk met rekenen en de daaruit volgende overtuiging dat wiskunde als wetenschap "af" is. De wiskundigen weten wel beter en iedereen binnen het vakgebied zal akkoord gaan dat wiskunde voor het grootste deel bestaat uit het opbouwen van een perfecte redenering. Het is dan ook de taak van de wiskundigen om anderen te overtuigen met gesproken en geschreven argumenten die op hun waarheid kunnen getest worden. We zouden kunnen stellen dat wiskunde een zwart-wit wetenschap is, er is weinig plaats voor een grijze zone. Wat het werk van de wiskundigen onderscheidt van het werk van anderen is dat zij kunnen *bewijzen dat ze gelijk hebben*. Er is geen ruimte voor discussie, maar dat kan natuurlijk alleen maar indien we de juiste logische regels gebruiken.

De bedoeling van dit hoofdstuk is de wiskundige grondslag te leggen voor het formuleren van precieze wiskundige uitspraken door middel van het gebruik van de juiste argumenten of regels. Hiermee stappen we in het domein van de logica.

We zullen het in het vervolg veelal hebben over *uitspraken*, een al dan niet wiskundig geformuleerde *bewering*. Dergelijke uitspraak kan *waar*, *vals* of *twijfelachtig* zijn. Het woord *twijfelachtig* op zich houdt reeds een waardeoordeel in, misschien moeten we daarom eerder hebben over *niet gedefinieerd*. Zo is bijvoorbeeld de uitspraak "Wiskunde is een mooie wetenschap" voor jou misschien een ware uitspraak, maar misschien ook een niet-ware uitspraak. Het is in elk geval als uitspraak niet goed gedefinieerd, want subjectief. In hetgeen volgt zullen we ons dus beperken tot enkel goed gedefinieerde uitspraken, waarbij we dan bedoelen dat de uitspraken die we behandelen ofwel waar ofwel niet waar zullen zijn. In de plaats van *niet-ware uitspraken* spreken we in deze logica, die we de *tweewaardige logica* noemen, ook van *valse uitspraken*. In wiskundige termen kunnen we dan aan de ware uitspraken de *waarheidswaarde* 1 toekennen, terwijl we aan de valse uitspraken de waarheidswaarde of kortweg waarde 0 toekennen, daarom wordt ook wel eens

gesproken van *binaire logica*. In de veronderstelling dat we een derde opinie aanvaardbaar achten, zoals bvb twijfelachtig, of niet-bepaald, dan kunnen we spreken van driewaardige logica. We kunnen nog verder gaan, als jij op een zomerse avond bijvoorbeeld zou beweren dat het warm is, dan kan dit misschien wel opgaan voor jezelf, maar wat is de exacte definitie van warm? Iedereen heeft zo zijn gevoel van wat dit betekent, het is dus een eerder vaag gedefinieerd begrip en de logica die hierop gebouwd is wordt de vage logica (in het Engels "fuzzy logic") genoemd. In verscheidene cursussen later in de bachelor- en masteropleiding komt zowel meerwaardige logica als vage logica aan bod. Het is in dit inleidend hoofdstuk echter enkel de bedoeling om een basis van de tweewaardige logica te leggen, die dan als basis kan gebruikt worden voor verder wiskundige behandeling maar ook voor uitbreiding naar de andere logicabenaderingen.

In formeel logische termen gaan we uit van een verzameling van **uitspraken met betekenis**, ook *proposities* genoemd, die ofwel *waar* of *vals* zijn. Zo is de uitspraak "Gent is een Vlaamse universiteitsstad" een ware propositie, maar de uitspraak "Gent is de enige Vlaamse universiteitsstad" is een valse propositie. De uitspraak $xy = z$ is geen propositie, want we weten niet wat x, y en z zijn. We zullen hier dus wat specifieker moeten zijn.

Op dezelfde manier zoals we in de verzamelingenleer nieuwe verzamelingen construeren uit bestaande verzamelingen (zoals $A \cap B, A \setminus B, \ldots$), zullen we dit ook doen met proposities. We zullen uit bestaande proposities, nieuwe proposities maken, die we dan *samengestelde proposities* noemen. Eigenlijk kan een volledige analogie gelegd worden met de verzamelingenleer. Zo is bvb de *negatie* van een propositie p een propositie die vals is als p waar is. Deze propositie, genoteerd als $\neg p$ (lees "niet p") is eigenlijk het equivalent van het begrip complementaire verzameling van een gegeven verzameling.

Aangezien de negatie als operatie op een enkelvoudige propositie wordt uitgevoerd, zoals ook complement nemen van een verzameling ook maar op één verzameling is betrokken, spreken we van een *unaire* operatie. Maar de meeste operatoren in de verzamelingenleer zoals $\cap, \cup, \triangle$ zijn evenals de bewerkingen in de getallenverzamelingen zoals $+, -, \times$, *binaire* operatoren.

Als p en q twee proposities zijn, dan wordt de *conjunctie* van p en q, genoteerd als $p \wedge q$ (lees "p en q"), gedefinieerd als de propositie die waar is als en alleen dan als zowel p als q waar zijn. De conjuctie neemt dus de rol over van de operator "doorsnede" in de verzamelingenleer. Analoog, wordt de *disjunctie* van p en q, genoteerd als $p \vee q$ (lees " p of q") gedefinieerd als de propositie die waar is wanneer ten minste één van de uitspraken p of q waar zijn. Deze operator is dus equivalent met de operator "unie" in de verzamelingenleer. Tot slot, de *exclusieve of* van p en q, genoteerd $p \ominus q$ (lees

"ofwel p ofwel q") is de propositie die waar is als en alleen dan als juist één van de proposities p of q waar is. Het correspondeert dus met het begrip symmetrisch verschil van twee verzamelingen (en overigens is dat de reden waarom de notatie voor het symmetrisch verschil van de verzamelingen A en B soms ook $A \ominus B$ is).

Het ligt nu voor de hand om deze operatoren te combineren en het zal je wel niet verwonderen dat we dus ook kunnen spreken van de wetten van De Morgan in deze binaire logica (ook wel propositielogica genoemd). Overigens, De Morgan heeft zijn wetten eerst geformuleerd binnen de logica en later werd een verband gelegd met wat men de *Boole algebra* is gaan noemen, naar zijn leeftijdsgenoot en vriend George Boole (1815–1864) met wie De Morgan veel heeft samengewerkt.

In de symbolische taal die we hierboven hebben ingevoerd, lezen de wetten van De Morgan als volgt.

$$\neg(p \wedge q) = (\neg p) \vee (\neg q),$$

en

$$\neg(p \vee q) = (\neg p) \wedge (\neg q).$$

Eigenlijk gebruiken we hier al een gelijkheid van twee (samengestelde) uitspraken, terwijl we strikt gesproken nog moeten definiëren wat we bedoelen met "gelijk" of beter "logisch equivalent", maar dit mag geen probleem zijn.

2.2 Waarheidstabellen

De *waarheidswaarde* van een samengestelde propositie is volledig bepaald door de waarheidswaarde van de samenstellende proposities. Dit verband wordt dan meestal in tabelvorm weergegeven, hetgeen we de *waarheidstabellen* noemen.

Hier zijn de waarheidstabellen voor de samengestelde proposities die we tot hiertoe hebben gedefinieerd.

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	$p \ominus q$
1	1	0
1	0	1
0	1	1
0	0	0

Het is nu misschien tijd om even dieper in te gaan op het logisch begrip dat gelijkwaardig is met de gelijkheid van de verzamelingen. We zeggen dat twee proposities *logisch equivalent* zijn als en alleen dan als beide proposities dezelfde waarheidstabellen hebben (eventueel op een permutatie van de rijen na). We zullen dit noteren als $p \iff q$.

Als voorbeeld kunnen we de wetten van De Morgan bewijzen.

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

Indien we de beide kolommen voor $\neg(p \wedge q)$ en $(\neg p) \vee (\neg q)$ vergelijken, dan zien we dat deze gelijk zijn en dus mogen we besluiten dat $\neg(p \wedge q) \iff (\neg p) \vee (\neg q)$. De andere wet van De Morgan wordt op dezelfde manier bewezen.

De *implicatie* $p \to q$ van twee proposities p en q is de propositie die vals is wanneer p waar is en q vals (in de andere gevallen is de implicatie waar). De propositie p wordt dan de *hypothese* of het *antecedent* genoemd terwijl de propositie q de *conclusie* of het *consequent* genoemd wordt. Vergeet niet dat indien de propositie p vals is, dan de implicatie $p \to q$ waar is, onafhankelijk van de waarde van q. Er bestaan een ganse rist manieren om een implicatie in woorden te formuleren: "als p dan q", "q als p", "uit p volgt q", "p impliceert q". Maar ook de volgende eerder oubollige terminologie wordt veel gebruikt in een wiskundige context, "p is voldoende voor q" of "q is nodig voor p".

De waarheidstabel voor de implicatie ziet er als volgt uit.

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Voorbeeld

De volgende uitspraak die niet door iedereen in dank wordt afgenomen is wel bekend (wie heeft dit gezegd?) "Het regent dus dit is België". Vraag is nu, wat is de negatie van deze uitspraak? We beweren dat het is "Het regent en dit is niet België".

In termen van de propositielogica kunnen we de uitspraak vertalen met $p =$ "Het regent" en $q =$ "Dit is België" als $p \to q$. We bewijzen nu met behulp van de waarheidstabellen dat

$$\neg(p \to q) \iff p \wedge (\neg q).$$

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

We besluiten dus dat de negatie van "uit p volgt q" niet anders is dan "p is waar en q is vals".

Het *omgekeerde* van de implicatie $p \to q$ is de implicatie $q \to p$, terwijl de *contrapositieve* (ook wel *contrapositie* genoemd) van de implicatie $p \to q$ de implicatie $(\neg q) \to (\neg p)$ is.

De waarheidstabellen zien er als volgt uit.

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

Aangezien de kolom $(\neg q) \to (\neg p)$ gelijk is aan deze van $p \to q$, mogen we besluiten dat een implicatie en zijn contrapositieve logisch equivalent zijn, terwijl de implicatie en zijn omgekeerde duidelijk niet logisch equivalent zijn. Dit zal belangrijke consequenties hebben wanneer we het later hebben over de bewijsmethodes. Willen we namelijk de waarheid van een implicatie bewijzen, dan kunnen we even goed de waarheid van de contrapositieve van de implicatie bewijzen, wat soms gemakkelijker is, zoals zal blijken.

Op dit principe steunt eigenlijk de bewijsmethode beter gekend als *bewijs door contrapositie*. Wil men een implicatie $p \to q$ bewijzen, dan vertrekt men van de veronderstelling dat q niet waar is, dus van $(\neg q)$ en bewijst men dat

dit impliceert dat p niet waar is (dus $(\neg p)$), wat tegen de "veronderstelling" was. Met deze methode wordt dus $(\neg q) \to (\neg p)$ in plaats van $p \to q$, die echter, zoals gezegd logisch equivalent zijn.

Voorbeeld

Het omgekeerde van de implicatie "Het regent dus dit is België" is "Als dit België is, dan moet het regenen", terwijl de contrapositieve van dezelfde implicatie luidt "Als dit Belgë niet is dan regent het niet".

Tot slot, als p en q proposities zijn, dan noemen we de *biconditionele propositie van p en q*, de propositie $p \leftrightarrow q$ die precies waar is wanneer p en q dezelfde waarde hebben. In woorden wordt de biconditionele propositie uitgedrukt als "p als en alleen dan als q" of " p is een nodige en voldoende voorwaarde voor q". De waarheidstabel voor $p \leftrightarrow q$ ziet er als volgt uit.

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Het is dus duidelijk dat

$$(p \leftrightarrow q) \Longleftrightarrow (p \to q) \wedge (q \to p).$$

Dus, om de waarheid van $p \leftrightarrow q$ te bewijzen moeten we dus de waarheid bewijzen van de implicatie $p \to q$ en de waarheid van zijn omgekeerde $q \to p$.

2.3 Predicatenlogica

Zoals we in de sectie over propositielogica hebben aangegeven, zijn uitspraken zoals $x + y = 3$ of $x > 0$ geen proposities, omdat we niet weten wat bedoelen met x, of y, het zijn uitspraken zonder betekenis. Dergelijke uitspraken worden *propositionele functies* of *predicaten* in één of meerdere variabelen genoemd. We noteren bvb met $P(x, y)$ het predicaat $x + y = 3$ en met $Q(x)$ het predicaat $x > 0$. Indien we nu een *universum* aangeven voor de variabelen, dit wil zeggen indien we zeggen tot welke verzameling deze variabelen moeten behoren, dan wordt het predicaat een uitspraak met betekenis en dus een propositie, die waar of vals kan zijn, indien we de variabele vervangen door een element van het universum. Bijvoorbeeld, indien het universum

de verzameling $\mathbb{R}$ van de reële getallen is, dan zijn de proposities $P(-1,4)$, $P(\pi, 3-\pi)$ en $Q(\frac{1}{2})$ waar, terwijl de propositie $Q(0)$ vals is.

Om van een predicaat een propositie te maken, kan men ook werken met zogenaamde *kwantoren*.

Als $P(x)$ een predicaat is met één variabele x, dan wordt de propositie "$P(x)$ is waar voor alle waarden van x in het universum" de *universele kwantificatie* van $P(x)$ genoemd en we noteren dit als volgt.

$$\forall x[P(x)]$$

We lezen dit als "voor alle x (geldt) $P(x)$". Het symbool $\forall$, (voor alle), wordt de *universele kwantor* genoemd.

De propositie "Er bestaat een element x uit het universum zodanig dat $P(x)$ waar is" wordt de *existentiële kwantificatie* van $P(x)$ genoemd en we noteren dit als volgt.

$$\exists x[P(x)]$$

We lezen dit als "er bestaat een x zodanig dat $P(x)$ (geldt)".

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

$$\begin{aligned} \forall x[P(x)] &\iff P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n) \\ \exists x[P(x)] &\iff P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n). \end{aligned}$$

Voorbeelden

1. Als $P(x)$ het volgende predicaat voorstelt "x kreeg 10 op 20 voor het examen over het vak *Relaties en Structuren*". Dan is er een groot verschil tussen $\forall x[P(x)]$ en $\exists x[P(x)]$.

2. Als $P(x)$ het predicaat $x^2 \geq x$ voorstelt, met universum $\mathbb{R}$ dan zeggen we kortweg " $\forall x \in \mathbb{R}[P(x)]$ is vals".

Van zodra een variabele een waarde heeft gekregen, of van zodra we één van de kwantoren toevoegen, dan spreken we van een *gebonden variabele*. Een predicaat in één of meerdere variabelen wordt dus een propositie van zodra alle variabelen gebonden zijn. Bij predicaten van meerdere variabelen en gebruik van verschillende kwantoren, is de volgorde van gebruik van kwantoren zeer belangrijk. Zo is $\forall x \exists y[P(x,y)]$ niet logisch equivalent met $\exists y \forall x[P(x,y)]$. In het eerste geval wordt er gezegd dat voor elke x een y kan gevonden worden, in het tweede geval bestaat er een y zodanig dat voor elke x $P(x,y)$.

Tot slot nog iets over de negatie van proposities met kwantoren. Volgende logische equivalenties zouden duidelijk moeten zijn.

$$\begin{aligned} \neg(\forall x[P(x)]) &\iff \exists x[\neg P(x)]; \\ \neg(\exists x[P(x)]) &\iff \forall x[\neg P(x)]; \\ \neg(\forall x \exists y[P(x,y)]) &\iff \exists x \forall y[\neg P(x,y)]. \end{aligned}$$

Hoofdstuk

3 Getaltheorie

In dit hoofdstuk gaan we dieper in op de *algebraïsche* structuur van de verzameling $\mathbb{Z}$ voorzien van de optelling en de vermenigvuldiging.

3.1 Deelbaarheid en grootste gemene deler

We hebben deelbaarheid in $\mathbb{N}$ gezien in Hoofdstuk 1, Voorbeeld 1.7. De uitbreiding naar $\mathbb{Z}$ ligt voor de hand.

Definitie 3.1

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 3.2

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 3.3

Veronderstel $a \mid b$ en $a \mid c$. Dan zal voor alle gehele getallen x en y gelden dat $a \mid (bx + cy)$

Lemma 3.4

De deelbaarheidsrelatie beperkt tot $(\mathbb{Z} \times \mathbb{Z}) \setminus \{(0,0)\}$ is reflexief en transitief.

Bovenstaand lemma formuleert welgekende eigenschappen van deelbaarheid in $\mathbb{Z}$ en behoeft daarom geen bewijs meer. Merk op dat $\mathcal{D}$ over $\mathbb{Z}$ niet antisymmetrisch is, terwijl ze dat over $\mathbb{N}$ wel is. Immers $(x, -x)$ en $(-x, x)$ zijn steeds twee koppels in $\mathcal{D}$ voor alle $x \neq 0$. Vanaf nu zullen we met $\mathcal{D}$ steeds de deelbaarheidsrelatie over $\mathbb{Z}$ bedoelen, tenzij anders vermeld. Een relatie die reflexief en transitief is wordt ook een *pre-orderelatie* genoemd.

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. Merk op dat dus 1 een deler is van elk geheel getal, en dat elk geheel getal verschillend van 0, deler is van 0. In plaats van $2|b$ zeggen we meestal dat b even is, terwijl $2 \nmid b$ betekent dat b oneven is.

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 3.5

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 axioma van de goede ordening 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 $r \in \mathbb{N}[0, a - 1]$.

(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 $r_1, r_2 \in \mathbb{N}[0, a-1]$. Als $q_1 > q_2$, dan geldt $r_2 = a \cdot (q_1 - q_2) + r_1 \geq a + r_1 \geq a$, een tegenstrijdigheid. Bijgevolg geldt $q_2 \geq q_1$. We kunnen nu de rol van q_1 en q_2 omkeren, waaruit dan volgt dat $q_1 \geq q_2$, zodat we mogen besluiten dat $q_1 = q_2$ en $r_1 = r_2$. □

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 $\mathbb{N}[0, t - 1]$ behoren. Indien we immers de voorgaande stelling

herhaalde malen toepassen, dan verkrijgen we:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ \dots &\quad \dots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Hierbij zal elke rest r_i tot $\mathbb{N}[0, t-1]$ 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, $r_i \in \mathbb{N}[0, 9]$) en $t = 2$ (binair getallenstelsel, $r_i \in \mathbb{N}[0, 1]$). 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 3.6

Stel $a, b \in \mathbb{Z}$ niet beide nul. Een getal $c \in \mathbb{Z}$ 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 3.7

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 3.8

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 wijst *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 3.9

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 3.3. 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 3.3. 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 3.10. 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 bij deling van a door b als $\text{rem}(a, b)$.

Algoritme 3.1 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 3.10 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 $a = \text{quo}(a, b)q + \text{rem}(a, b)$.

Algoritme 3.2 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 3.11

Veronderstel dat a en b gehele getallen zijn (niet beide nul), en dat $d = \text{ggd}(a, b)$, dan bepaalt Algoritme 3.2 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

$$r_{k-1} = r_{k-3} - r_{k-2} q_{k-1}.$$

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 3.11 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

$$ma + nb = (m - kb)a + (n + ka)b, \quad \forall k \in \mathbb{Z}.$$

We gebruiken nu Stelling 3.11 om twee gekende eigenschappen zeer kort te bewijzen.

Gevolg 3.12

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 3.11 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 3.13

Veronderstel dat $a \mid m$, $b \mid m$ en $\text{ggd}(a, b) = 1$. Dan geldt $a \cdot b \mid m$.

Bewijs. Uit Stelling 3.11 volgt het bestaan van $x, y \in \mathbb{Z}$ met $ax + by = 1$, dus $max + mby = m$. Uit de veronderstellingen 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*.

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 3.14

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.

Heel wat meer eigenschappen van de grootste gemene deler en het kleinste gemeen veelvoud kunnen bewezen worden. Wij vatten deze eigenschappen in de volgende stelling samen, we laten het bewijs als oefening.

Stelling 3.15

1. Als a, b en c natuurlijke getallen zijn, en ac en bc niet beide nul zijn, dan is $\text{ggd}(ca, cb) = c\,\text{ggd}(a, b)$.
2. Als a, b, c getallen zijn (a en b niet beide nul), zodanig dat c deelbaar is door a en b, dan is c deelbaar door $\dfrac{ab}{\text{ggd}(a, b)}$.
3. Als a en b natuurlijke getallen zijn, niet beide nul, dan is $\text{kgv}(a, b) \cdot \text{ggd}(a, b) = ab$.
4. Als a, b en c 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 dan en slechts dan als zowel a en c als b en c onderling ondeelbaar zijn.
5. Veronderstel dat $a, b \in \mathbb{Z}$ en dat er gehele getallen x, y bestaan zodat $ax + by = c$. Dan is $\text{ggd}(a, b) \mid c$.

Bewijs. Oefening. □

Opmerking

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 historische informatie vindt men in [9, pp. 22–24].

3.2 Priemgetallen

Definitie 3.16

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 $m_i \in \mathbb{N}[2, m-1]$ (m_1 kan gelijk zijn aan m_2). We noemen daarom elk dergelijk getal m een *samengesteld getal* .

De lijst van de priemgetallen kleiner dan 50 is eenvoudig op te schrijven:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

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. Wij zullen in dit hoofdstuk enkele technieken bespreken om deze 2 problemen aan te pakken.

Merk vooreerst op dat er oneindig veel priemgetallen bestaan. Dit is een stelling die toegeschreven is aan Euclides.

Stelling 3.17 — Euclides

De verzameling van de priemgetallen is een oneindige verzameling.

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. □

[1] Dit algoritme is het oudste niet-triviale algoritme dat nog steeds onvervangbaar is, [5, §4.5.2]

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. Deze eigenschap is echter een gevolg van het axioma van de goede ordening. Om de uniciteit van deze ontbinding te bewijzen, hebben we het volgende lemma nodig.

Lemma 3.18

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 3.12 volgt dat $p \mid b$. □

Gevolg 3.19

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 ($i \in \mathbb{N}[1, n]$).

Bewijs. Door volledige inductie, en met behulp van Lemma 3.18. □

Stelling 3.20 — 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 $m = m_1 m_2,\ m_i \in \mathbb{N}[2, m-1]$. 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 3.18 geldt $p_i \mid q_j$ 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. □

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 $\mathbb{Z}$

We hebben een priemgetal gedefinieerd als een natuurlijk getal. De natuurlijke vraag stelt zich of we priemgetallen in $\mathbb{Z}$ moeten herdefiniëren, en zo ja, hoe. We bekijken eerst hoe we bepaalde eigenschappen kunnen vertalen naar $\mathbb{Z}$, alvorens een strikte definitie te geven. Een samengesteld getal $m \in N$ blijft uiteraard samengesteld in $\mathbb{Z}$. Omgekeerd, stel dat $p \in \mathbb{N}$ een

priemgetal is, en dat $p = a \cdot b$, $a, b \in \mathbb{Z}$. Dan is noodzakelijk $0 > a$ en $0 > b$, maar dan is $(-a) \cdot (-b) = p$ in $\mathbb{N}$ een ontbinding van p, een tegenstrijdigheid. Omgekeerd, stel dat $p \in \mathbb{Z} \setminus \mathbb{N}$ samengesteld is, en dat $-p \in \mathbb{N}$ een priemgetal is. Omdat $p = a \cdot b$, zal $-p = -a \cdot b$ en dus p kan geen priemgetal zijn, tenzij $a = -1$ of $b = -1$. Hieruit zou men kunnen afleiden dat er, op een minteken na, geen verschil is wat betreft priemgetallen in $\mathbb{N}$ en $\mathbb{Z}$. Dit is analoog aan de observatie over de grootste gemene delers en het teken. We houden vast aan het feit dat een priemgetal steeds een natuurlijk getal is, en we definiëren een veralgemening in $\mathbb{Z}$.

Definitie 3.21

Een *priemelement* in $\mathbb{Z}$ is ofwel een priemgetal ofwel een priemgetal vermenigvuldigd met -1.

Het is onze bedoeling de hoofdstelling van de rekenkunde te herformuleren in $\mathbb{Z}$. Het is ondertussen duidelijk dat we enkel rekening moeten houden met verschil in teken. Voor $a \in \mathbb{Z} \setminus \{0\}$ definiëren we het *teken van* a, als $\text{sign}(a) = |a|/a$, en $\text{sign}(0) = 1$.

Stelling 3.22

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 priemfactoren 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

$$d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}, \quad x_i \in \mathbb{N}[0, e_i], i = 1, \dots, k.$$

Het aantal delers van n is bijgevolg gelijk aan het aantal k-tallen $(x_1, x_2, \dots, x_k)$ met $x_i \in \mathbb{N}[0, e_i]$ 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.

Stelling 3.23

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

$$a_0 (p/q)^n + a_1 (p/q)^{n-1} + \dots + a_{n-1}(p/q) + a_n = 0.$$

Vermenigvuldiging met q^n levert

$$a_0 p^n + a_1 p^{n-1} q + \dots + a_{n-1} p q^{n-1} + a_n q^n = 0.$$

Hieruit volgt dat

$$p(a_0 p^{n-1} + a_1 p^{n-2} q + \dots + a_{n-1} q^{n-1}) = -a_n q^n,$$

zodat p een deler is van $a_n q^n$. 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. □

3.3 De Eulerfunctie

Veronderstel dat n een positief natuurlijk getal is, dan noteren we met $\varphi(n)$ het aantal natuurlijke getallen uit $\mathbb{N}[1, n]$ dat copriem is met n; per definitie is $\varphi(1) = 1$. De functie φ wordt de *Eulerfunctie* ook wel *indicator van Euler* of *Eulertotiënt* genoemd naar Leonhard Euler (1707–1783). Indien $n = p$ een priemgetal is, dan is duidelijk

$$\varphi(p) = p - 1.$$

Het is onze bedoeling om een expliciete formule voor $\varphi(n)$ in het algemeen geval te bepalen. Daartoe bewijzen we eerst twee lemma's.

Lemma 3.24

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 het interval $\mathbb{N}[1, p^e]$ is de verzameling $\{c \cdot p \| c = 1 \dots p^{e-1}\}$. Er zijn m.a.w. juist p^{e-1} veelvouden van p, dit zijn de enige getallen in $\mathbb{N}[1, p^e]$ die niet onderling ondeelbaar zijn met p^e. Dus $\varphi(p^e) = p^{e-1}(p-1)$. □

Lemma 3.25

Veronderstel dat de natuurlijke getallen m en n onderling ondeelbaar zijn. Dan is $\varphi(mn) = \varphi(m)\varphi(n)$.

Bewijs. Stel dat voor $a \in \mathbb{N}[1, mn]$ geldt dat $\text{ggd}(a, mn) = 1$. Door Stelling 3.11 bestaan er gehele getallen x, y waarvoor $ax + mny = 1$. Door Stelling 3.15 (5) tweemaal toe te passen vinden we onmiddellijk dat $\text{ggd}(a, m) = 1$ en $\text{ggd}(a, n) = 1$.

Omgekeerd, stel dat voor $a \in \mathbb{N}[1, mn]$ geldt dat $\text{ggd}(a, m) = 1$ en $\text{ggd}(a, n) = 1$. Passen we Stelling 3.11 (4) toe, dan vinden we onmiddellijk dat $\text{ggd}(a, mn) = \text{ggd}(a, m) \cdot \text{ggd}(a, n) = 1$.

Dus $\text{ggd}(a, mn) = 1 \iff \text{ggd}(a, m) = 1$ en $\text{ggd}(a, n) = 1$. We definiëren nu twee verzamelingen:

$$A_m := \{x \in \mathbb{N}[1, nm] \| \text{ggd}(x, m) \neq 1\}$$
$$A_n := \{x \in \mathbb{N}[1, nm] \| \text{ggd}(x, n) \neq 1\}$$

Stel nu $x \in \mathbb{N}[1,m]$ en $\text{ggd}(x,m) \neq 1$ en $y \in \mathbb{N}[1,n]$, en $\text{ggd}(y,n) \neq 1$. Dan is $z := x \cdot y \in \mathbb{N}[1,nm]$ en $\text{ggd}(z,nm) \neq 1$. Uiteraard geldt ook dat $\text{ggd}(z,m) \neq 1$ en $\text{ggd}(z,n) \neq 1$. We mogen besluiten dat $z \in A_m \cap A_n$. Omgekeerd, stel dat $z \in A_m \cap A_n$. Er geldt dat $c := \text{ggd}(z,m) \neq 1$ en $d := \text{ggd}(z,n) \neq 1$. Omdat $\text{ggd}(m,n) = 1$, geldt $cd = \text{ggd}(z,mn)$, Dus $cd \mid z$, of nog, $z = c \cdot d \cdot e$ voor een zekere $e \in \mathbb{N}$, en $e < z$. Dus vinden we nu gemakkelijk de elementen x en y waarvoor $x \in \mathbb{N}[1,m]$ en $\text{ggd}(x,m) \neq 1$ en $y \in \mathbb{N}[1,n]$, en $\text{ggd}(y,n) \neq 1$ en $z = x \cdot y$. We mogen besluiten dat $|A_m \cap A_n| = (m - \varphi(m))(n - \varphi(n))$.

Er rest ons nu nog $|A_m|$ en $|A_n|$ te bepalen. Er zijn in $\mathbb{N}[1,m]$ juist $m - \varphi(m)$ elementen x met $\text{ggd}(x,mn) \neq 1$, namelijk diegenen waarvoor $\text{ggd}(x,m) \neq 1$. Elk veelvoud van zo'n x komt n keer voor in het interval $\mathbb{N}[1,mn] \supset A_m$. Dus $|A_m| = n(m - \varphi(m))$. Analoog vinden we $|A_n| = m(n - \varphi(n))$. Nu gebruiken we het feit dat voor de eindige verzamelingen A_m en A_n geldt dat $|A_m \cup A_n| = |A_m| + |A_n| - |A_m \cap A_n|$. We kunnen nu alle elementen $z \in \mathbb{N}[1,mn]$ waarvoor $\text{ggd}(z,mn) = 1$ tellen.

$$\begin{aligned}\varphi(mn) &= mn - |A_m \cup A_n| \\ &= mn - m(n - \varphi(n)) - n(m - \varphi(m)) + (m - \varphi(m))(n - \varphi(n)) \\ &= \varphi(m)\varphi(n)\,.\end{aligned}$$

Daarmee is het gestelde aangetoond. □

Stelling 3.26

Veronderstel dat $n \geq 2$ een natuurlijk getal is met priemfactorontbinding $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Dan is

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \tag{3.1}$$

$$= p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1)\dots p_k^{e_k-1}(p_k - 1)\,. \tag{3.2}$$

Bewijs. Voor de priemgetallen p_i in de ontbinding van n geldt uiteraard dat $\text{ggd}(p_i^{e_i}, p_j^{e_j}) = 1$. Inductieve toepassing van Lemma's 3.24 en 3.25 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 3.27

Voor elk natuurlijk getal n geldt dat $\sum_{d|n} \varphi(d) = n$. Hierbij wordt gesommeerd over al de 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

$$\begin{aligned}
\sum_{d|mp^e} \varphi(d) &= \sum_{d|m} \varphi(d) + \sum_{d|m} \varphi(dp) + \cdots + \sum_{d|m} \varphi(dp^e) \\
&= m + m\varphi(p) + \cdots + m\varphi(p^e) \\
&= m(1 + \varphi(p) + \cdots + \varphi(p^e)) \\
&= m(1 + (p-1) + \cdots + p^{e-1}(p-1)) \\
&= mp^e = n\,.
\end{aligned}$$

3.4 Noten

- Het bekijken waard is zeker `http://eulerarchive.maa.org/`, het *Eulerarchief*.
- Hoofdstuk 1 van [1] bevat zes verschillende bewijzen van Stelling 3.17, waaronder het elementaire bewijs van Euclides zelf. In Hoofdstuk 2 van het boek vindt men een "elementair" bewijs van het *postulaat van Bertrand*: voor elke $n \geq 1$ bestaat er steeds een priemgetal p waarvoor $n < p \leq 2n$.

Hoofdstuk

4 Modulair rekenen

4.1 Congruenties

Definitie 4.1

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 4.2

De relatie congruent modulo m is een equivalentierelatie

Bewijs. Oefening. □

De equivalentieklassen worden de *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 $\mathbb{Z}_m$. Indien we uit elke restklasse de kleinste natuurlijke representant

kiezen, dan ontstaat de verzameling $\mathbb{N}[0, m-1]$. Er bestaat m.a.w. een bijectie tussen de verzamelingen $\mathbb{Z}_m$ en $\mathbb{N}[0, m-1]$.

Stelling 4.3

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 $x_1 y_1$ en $x_2 y_2$ congruent modulo m. □

Bovenstaande stelling toont in feite aan dat we over een goed gedefinieerde *optelling en vermenigvuldiging* beschikken in de verzameling $\mathbb{Z}_m$. Merk op dat we optelling en vermenigvuldiging hier zien als een abstracte binaire operatie die aan bepaalde vereisten voldoet. In Hoofdstuk 6 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 4.4

Veronderstel dat $(x_n x_{n-1} \dots x_2 x_1 x_0)_{10}$ *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 4.3

$$\theta(x)\theta(y) \equiv xy \pmod 9.$$

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 $\theta(xy) \equiv \theta(x)\theta(y) \equiv 3 \pmod 9$.

4.2 Optelling en vermenigvuldiging in $\mathbb{Z}_m$

We zullen nu in de verzameling $\mathbb{Z}_m$ 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 4.3.

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) $\forall [a]_m, [b]_m \in \mathbb{Z}_m$: $[a]_m \oplus [b]_m \in \mathbb{Z}_m$ en $[a]_m \otimes [b]_m \in \mathbb{Z}_m$.

(A2) $\forall [a]_m, [b]_m \in \mathbb{Z}_m$: $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$ en $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$.

(A3) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$: $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$ en $([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$.

(A4) $\forall [a]_m \in \mathbb{Z}_m$: $[a]_m \oplus [0]_m = [a]_m$ en $[a]_m \otimes [1]_m = [a]_m$.

(A5) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$: $[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m)$.

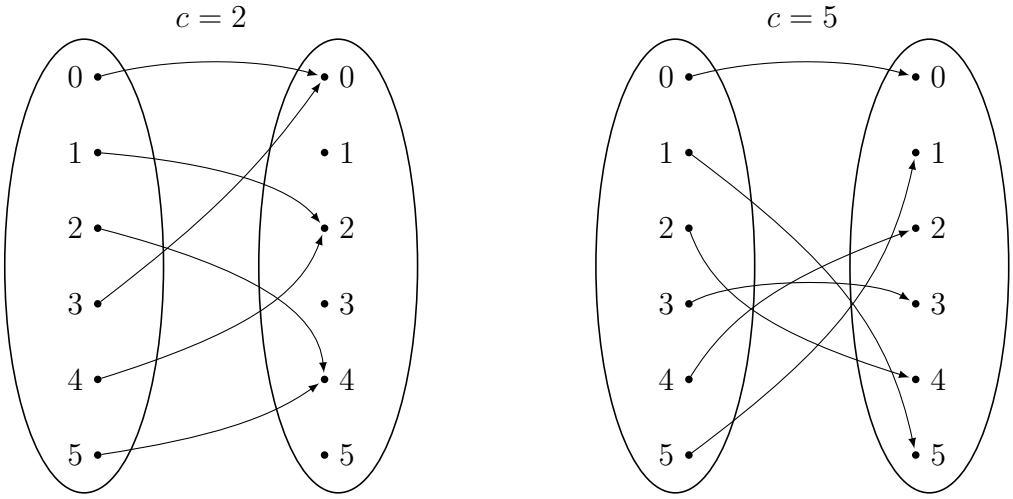
(A6) $\forall [a]_m \in \mathbb{Z}_m, \exists - [a]_m = [-a]_m \in \mathbb{Z}_m : [a]_m \oplus (-[a]_m) = [0]_m$.

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 $\mathbb{Z}_m, \oplus, \otimes$ een *ring* is. In Hoofdstuk 6 komen we hierop terug.

Merk echter op dat de schrappingswet voor de vermenigvuldiging in $\mathbb{Z}_m$ niet geldt. Zo is bijvoorbeeld in $\mathbb{Z}_6$,

$$[3]_6 \otimes [1]_6 = [3]_6 \otimes [5]_6,$$

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 $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, $x \mapsto c \cdot x$, 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 $\mathbb{Z}_6$,

$$[2]_6 \otimes [3]_6 = [0]_6 \,,$$

Men zegt daarom dat de klassen $[a]_m$ met a een echte deler van m, *nuldelers* zijn in $\mathbb{Z}_m$. Indien $m = p$ een priemgetal is, dan bezit $\mathbb{Z}_p$ dus geen nuldelers door Lemma 3.18.

Opmerking

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.

4.3 Inverteerbare elementen in $\mathbb{Z}_m$

Een geheel getal r ($r \neq \pm 1$) bezit geen invers element in $\mathbb{Z}$ voor de vermenigvuldiging. In $\mathbb{Z}_m$ is de situatie enigszins anders. We gaan na wanneer een element van $\mathbb{Z}_m$ een invers element in $\mathbb{Z}_m$ bezit.

Definitie 4.5

Een element $r \in \mathbb{Z}_m$ wordt *inverteerbaar* genoemd als er een element x in $\mathbb{Z}_m$ bestaat, zodanig dat $rx = 1$ in $\mathbb{Z}_m$, met andere woorden indien $rx \equiv 1 \pmod{m}$. We noteren het *invers element* x van r als r^{-1}.

Stelling 4.6

Een element r in $\mathbb{Z}_m$ is inverteerbaar dan en slechts dan als r en m onderling ondeelbaar zijn. In het bijzonder is in $\mathbb{Z}_p$, 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 Stelling 3.15 (5) 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 3.11), hetgeen gelijkwaardig is met $xr \equiv 1 \pmod{m}$. □

Gevolgen

In Paragraaf 3.3 hebben we $\varphi(m)$ gedefinieerd hebben als het aantal gehele getallen $r \in \mathbb{N}[1, m]$, die copriem zijn met m. Het aantal inverteerbare elementen in $\mathbb{Z}_m$ is bijgevolg gelijk aan $\varphi(m)$.

De volgende stelling is één van de klassiekers in de elementaire getaltheorie en heeft een groot aantal toepassingen.

Stelling 4.7 — 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 $\mathbb{Z}_m$. Noem U_m de verzameling van de inverteerbare elementen in $\mathbb{Z}_m$, 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 $\mathbb{Z}_m$ eveneens inverteerbaar is, kunnen we de schrappingswet toepassen, zodat $y^{\varphi(m)} \equiv 1 \pmod m$. □

Gevolg 4.8 — 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. □

In het bijzonder geval dat $m = p$ een priemgetal is, en dus $\varphi(p) = p - 1$, wordt de stelling van Euler,

$$\text{als } p \nmid y, \text{ dan is } y^{p-1} \equiv 1 \pmod p.$$

Gevolg 4.9

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. □

4.4 Lineaire congruenties

Na de definitie van congruentie te hebben gegeven, is het logisch dat we proberen vergelijkingen op te lossen in $\mathbb{Z}_m$. 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 $\mathbb{Z}_m$, wordt een *lineaire congruentie* genoemd. Het oplossen van een dergelijke lineaire congruentie is gelijkwaardig met het zoeken naar een koppel $(x, t), x \in \mathbb{N}[0, m-1], t \in \mathbb{Z}$, 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 4.10

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 $r \in \mathbb{N}[0, m-1]$.

Bewijs.

1. Veronderstel dat $\text{ggd}(a, m) = d > 1$ geen deler is van b. Indien $r \in \mathbb{N}[0, m-1]$ 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 4.6, a inverteerbaar in $\mathbb{Z}_m$. Bijgevolg bestaat er een element $a^{-1} \in \mathbb{Z}_m$ zodanig dat $aa^{-1} \equiv 1 \pmod{m}$, zodat $a^{-1}(ax) \equiv (a^{-1}b) \pmod{m}$ of dus $x \equiv (a^{-1}b)$

(mod 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 $\mathbb{N}[0, \frac{m}{d} - 1]$. Alle oplossingen van $ax \equiv b \pmod{m}$ zijn bijgevolg van de gedaante $r + t\frac{m}{d}, t \in \mathbb{N}[0, d-1]$. 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 3.11), 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 $\dfrac{b + tm}{a} \pmod{m}$.

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 $\mathbb{N}[0, 32]$. 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 4.11. *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.

$$\begin{array}{lrcl} \text{bv.} & 16y & \equiv & 35 \pmod{9} \\ \iff & 7y & \equiv & 35 \pmod{9} \\ \iff & y & \equiv & 5 \pmod{9} \\ \iff & y & = & 5 + 9t, \quad t \in \mathbb{Z}. \end{array}$$

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.

4.5 De stelling van Wilson en toepassingen

Stelling 4.12 — 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 $\mathbb{Z}_p \setminus \{0\}$. 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 $a \in \mathbb{N}[1, p-1]$, volgt hieruit dat ofwel $a = 1$ ofwel $a = p - 1$. Bijgevolg is

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (1)^{\frac{p-3}{2}} \equiv -1 \pmod{p}. \qquad \square$$

Stelling 4.13

Veronderstel dat p een oneven priemgetal is, dan bestaat er een $a \in \mathbb{Z}_p$ waarvoor $a^2 \equiv -1 \pmod{p}$ dan en slechts dan als $p \equiv 1 \pmod{4}$.

Bewijs. Merk op dat

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\
&\equiv [1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(-\frac{p-1}{2}) \cdot (-\frac{p-3}{2}) \cdots (-1)] \pmod{p} \\
&\equiv [1 \cdot 2 \cdots \frac{p-1}{2}]^2 \cdot (-1)^{\frac{p-1}{2}} \pmod{p}
\end{aligned}$$

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

$$(p-1)! \equiv [1 \cdot 2 \cdots \frac{p-1}{2}]^2 \equiv -1 \pmod{p}.$$

Met andere woorden, $a = \frac{p-1}{2}!$ heeft de eigenschap dat $a^2 \equiv -1 \pmod{p}$ als $p \equiv 1 \pmod{4}$.

Veronderstel nu omgekeerd dat er een a bestaat zodanig dat $a^2 \equiv -1 \pmod{p}$, dan zal eveneens $(-a)^2 \equiv -1 \pmod{p}$. Merk bovendien op dat uit $a^2 \equiv b^2 \pmod{p}$ eenvoudig volgt dat $a \equiv \pm b \pmod{p}$, zodat $x = a$ en $x = -a$ de enige waarden zijn waarvoor $x^2 \equiv -1 \pmod{p}$. Met elk element $t \in \mathbb{Z}_p \setminus \{0, a, -a\}$ correspondeert juist één element $t' \in \mathbb{Z}_p \setminus \{0, a, -a\}$, $t \neq t'$, zodanig dat $tt' \equiv -1 \pmod{p}$. Hieruit volgt dat

$$\begin{aligned} (p-1)! &\equiv -1 \pmod{p} \\ &\equiv (-1)^{\frac{p-3}{2}} \cdot a \cdot (-a) \pmod{p} \\ &\equiv (-1)^{\frac{p-3}{2}} \pmod{p}. \end{aligned}$$

Aangezien wegens de stelling van Wilson, $(p-1)! \equiv -1 \pmod{p}$, volgt hieruit dat $\frac{p-3}{2}$ oneven is, bv. $\frac{p-3}{2} = 2k-1$, zodat $p = 4k+1$. □

4.6 Stelsels lineaire congruenties

We beschouwen nu een stelsel van lineaire congruenties, met andere woorden een stelsel van de gedaante

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k \quad \gcd(a_i, m_i) | b_i.$$

Merk op dat we er steeds voor kunnen zorgen dat de vergelijkingen in dit stelsel van de vorm $x \equiv b_i \pmod{m_i}$ met $b_i \in \mathbb{N}[0, m_i - 1]$ zijn (zie oplossen van lineaire congruenties). We zullen ons daarom beperken tot de stelsels van de vorm

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1], i = 1, \ldots, k.$$

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 $x \equiv 52 \pmod{105}$. □

Opmerking

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 4.14 — Chinese reststelling

Het stelsel lineaire congruenties

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1], i = 1, \ldots, k$$

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. Met elk natuurlijk getal $t \in \mathbb{N}[0, M - 1]$ laten we het geordend k-tal $(r_1(t), r_2(t), \ldots, r_k(t))$ corresponderen met

$$r_i(t) \equiv t \pmod{m_i}, \quad r_i(t) \in \mathbb{N}[0, m_i - 1].$$

Met andere woorden $r_i(t)$ is de rest na deling van t door m_i. Twee verschillende getallen t en t' uit de verzameling $\mathbb{N}[0, M - 1]$ definiëren verschillende k-tallen $(r_1(t), r_2(t), \ldots, r_k(t))$ en $(r_1(t'), r_2(t'), \ldots, r_k(t'))$. Indien immers voor elke $i = 1, \ldots, k$, zou gelden dat $r_i(t) = r_i(t')$, dan betekent dit dat $t \equiv t' \pmod{m_i}$ voor elke $i = 1, \ldots, k$, en dus ook dat $t \equiv t' \pmod M$.

Dit betekent dat M een deler is van $t - t'$. Aangezien echter t en t' tot $\mathbb{N}[0, M-1]$ behoren, volgt hieruit dat $t = t'$. De afbeelding θ die met elke getal t uit $\mathbb{N}[0, M-1]$ het k-tal $(r_1(t), r_2(t), \ldots, r_k(t))$ van resten na deling door m_i laat corresponderen is bijgevolg een injectie. Nu hebben de verzamelingen $\mathbb{N}[0, M-1]$ en $\mathbb{N}[0, m_1 - 1] \times \mathbb{N}[0, m_2 - 1] \times \cdots \times \mathbb{N}[0, m_k - 1]$ beide evenveel elementen, namelijk $M = m_1 \cdot m_2 \cdots m_k$. Zou een bepaald k-tal uit $\mathbb{N}[0, m_1 - 1] \times \mathbb{N}[0, m_2 - 1] \times \cdots \times \mathbb{N}[0, m_k - 1]$ niet voorkomen als beeld onder θ, dan volgt uit het ladenprincipe dat een ander k-tal uit $\mathbb{N}[0, m_1 - 1] \times \mathbb{N}[0, m_2 - 1] \times \cdots \times \mathbb{N}[0, m_k - 1]$ tenminste 2 maal moet voorkomen als beeld onder θ, wat in tegenstrijd is met de injectiviteit van θ. Bijgevolg wordt elk k-tal uit $\mathbb{N}[0, m_1 - 1] \times \mathbb{N}[0, m_2 - 1] \times \cdots \times \mathbb{N}[0, m_k - 1]$ bereikt door θ, zodat θ surjectief is. De afbeelding θ is bijgevolg een bijectie. Met andere woorden, er bestaat juist één getal $t \in \mathbb{N}[0, M-1]$ zodanig dat $t \equiv b_i \pmod{m_i}$, $i = 1, \ldots, k$. □

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

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1], i = 1, \ldots, k$$

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

$$1 \equiv y_i m^{(i)} \pmod{m_i}, \quad y_i \in \mathbb{N}[0, m_i - 1], i = 1, \ldots, k.$$

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 Primitieve wortels

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 4.7) is

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Definitie 4.15

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

Indien we de opeenvolgende machten van de 10 elementen uit $\mathbb{Z}_{11} \setminus \{0\}$ uitrekenen, dan verkrijgen we de volgende tabel.

	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

$a^n \pmod{11}$

Uit de tabel blijkt onder andere dat $2, 6, 7, 8$ de orde 10 hebben. Anderzijds hebben $3, 4, 5, 9$ de orde 5 en heeft 10 de orde 2. Het is niet toevallig dat de mogelijke ordes allemaal delers zijn van $10 = \varphi(11)$.

Stelling 4.16

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 $r \in \mathbb{N}[0, t-1]$. Hieruit volgt dat

$$a^n \equiv a^{qt+r} \pmod{m}$$

zodat

$$1 \equiv a^r \pmod{m}.$$

Aangezien echter $r \in \mathbb{N}[0, t-1]$, 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 4.17

(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

$$a^r \equiv a^s \pmod{m} \Longleftrightarrow a^{r-s} \equiv 1 \pmod{m} \Longleftrightarrow r - s \equiv 0 \pmod{t}.$$

□

Definitie 4.18

Een *primitieve wortel van* m is een element $a \in \mathbb{Z}_m$, $\text{ggd}(a, m) = 1$, en waarvan de orde van a gelijk is aan $\varphi(m)$.

Voorbeeld 4.19. $2, 6, 7$ 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 4.20

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 $\mathbb{N}[1, m-1]$ 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

In $\mathbb{Z}_9$ is 2 een primitieve wortel (oefening). 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 4.21

Veronderstel dat a de orde t heeft modulo m ($\text{ggd}(a, m) = 1$). Dan zal a^k eveneens de orde t modulo m hebben dan en slechts dan 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 $\mathbb{Z}_{11}$ dat dit niet het geval is. Dit is eveneens het gevolg van de volgende stelling die we zonder bewijs aannemen.

Stelling 4.22

Elk priemgetal p bezit juist $\varphi(p-1)$ primitieve wortels. Indien g een primitieve wortel is van p, dan is de verzameling $\{g^k \pmod{p} \| \text{ggd}(k, p-1) = 1\}$, de verzameling van de primitieve wortels van p.

4.8 Kwadratische congruenties

In deze sectie zullen we steeds veronderstellen dat p een oneven priemgetal is. Een *kwadratische congruentie* in $\mathbb{Z}_p$ is een vergelijking van de vorm

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{4.2}$$

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 $\mathbb{Z}_p$. Bijgevolg is de kwadratische congruentie (4.2) gelijkwaardig met

$$x^2 + a^{-1}bx + a^{-1}c \equiv 0 \pmod{p}. \tag{4.3}$$

Aangezien p een oneven priemgetal is, geldt dus dat $\text{ggd}(2, p) = 1$, zodat 2 inverteerbaar is in $\mathbb{Z}_p$ (zie Stelling 4.6). Bijgevolg is (4.3) gelijkwaardig met

$$(x + \frac{a^{-1}b}{2})^2 \equiv \frac{b^2 - 4ac}{4a^2} \pmod{p},$$

dus ook met

$$y^2 \equiv \frac{\delta}{4a^2} \pmod{p} \quad \text{met } \delta = b^2 - 4ac \text{ en } y = x + \frac{a^{-1}b}{2}. \tag{4.4}$$

Het bestaan van een oplossing van de kwadratische congruentie (4.2) is dus herleid tot het bepalen van een oplossing van (4.4). 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 4.23

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 4.24

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 $p \not| r$, $p = 2$, 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 $\mathbb{Z}_{11}$ 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 $\mathbb{Z}_p \setminus \{0\}$ met p een oneven priemgetal bezit juist $(p-1)/2$ kwadratische resten en juist $(p-1)/2$ kwadratische niet-resten. Merk op dat indien $a \in \mathbb{Z}_p$ 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 4.25 — 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 $g^k \equiv a \pmod{p}$. 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

$$a^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}. \tag{4.5}$$

Veronderstel dat k even is, dan volgt uit (4.5) 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 4.26

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 4.27. 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.

4.9 Het Legendre symbool

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 zeer handig 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 4.28

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 4.16 volgt dat $p - 1 \mid (r - 2n)$, waaruit volgt dat r even is. □

Stelling 4.29

Het Legendre symbool $\left[\frac{a}{p}\right]$ 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 4.28 volgt het gestelde. □

Het belang van het Legendre symbool ligt vooral in het feit dat als gevolg van de bovenstaande eigenschappen, de berekeningen soms zeer sterk vereenvoudigd kunnen worden. Er is echter nog een andere zeer belangrijke stelling, de zogenaamde *kwadratische wederkerigheidsstelling*, die het rekenen met Legendre symbolen vereenvoudigt. Er bestaat een elementair (maar nogal lang) bewijs van deze stelling. Elementair betekent hier geen diepe kennis vereist is, maar omdat het bewijs te langdradig is laten we het hier weg. Een bewijs kan gevonden worden in [7].

Stelling 4.30 — Kwadratische wederkerigheidsstelling

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

$$\left[\frac{p}{q}\right] = \left[\frac{q}{p}\right].$$

Oefening 4.31. *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 Legendre symbolen

$$\left[\frac{5}{97}\right] \text{ en } \left[\frac{17}{97}\right].$$

Aangezien $17 \equiv 97 \equiv 1 \pmod 4$ en rekening houdende met de eigenschappen

kunnen we het Legendre symbool $\left[\frac{17}{97}\right]$ als volgt eenvoudig berekenen.

$$\begin{aligned}
\left[\frac{17}{97}\right] &= \left[\frac{97}{17}\right] \\
&= \left[\frac{12}{17}\right] \\
&= \left[\frac{4}{17}\right] \cdot \left[\frac{3}{17}\right] \\
&= \left[\frac{3}{17}\right] \\
&= \left[\frac{17}{3}\right] \\
&= \left[\frac{2}{3}\right]
\end{aligned}$$

Aangezien $2 \equiv -1 \pmod 3$ volgt hieruit dat $\left[\frac{17}{97}\right] = -1$.
Het andere Legendre symbool 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 Legendre symbool steeds herleid wordt tot het berekenen van de Legendre symbolen $\left[\frac{-1}{p}\right]$ en $\left[\frac{2}{p}\right]$. Voor deze Legendre symbolen gelden de volgende rekenregels:

1. (zie stelling 4.13)

$$\left[\frac{-1}{p}\right] = +1 \Longleftrightarrow -1 \equiv a^2 \pmod p \Longleftrightarrow p \equiv 1 \pmod 4$$

$$\left[\frac{-1}{p}\right] = -1 \Longleftrightarrow -1 \not\equiv a^2 \pmod{p} \Longleftrightarrow p \equiv 3 \pmod{4}.$$

2.

$$\left[\frac{2}{p}\right] = +1 \Longleftrightarrow p \equiv 1 \pmod{8} \text{ of } p \equiv 7 \pmod{8}$$

$$\left[\frac{2}{p}\right] = -1 \Longleftrightarrow p \equiv 3 \pmod{8} \text{ of } p \equiv 5 \pmod{8}.$$

4.10 Noten

- Gevolg 4.8 is ook gekend onder de naam *stelling van Fermat voor congruenties*. Het is opmerkelijk dat Fermat dit resultaat zonder bewijs publiceerde in 1640, terwijl het maar pas rond 1760 als bijzonder geval door Euler werd bewezen.
- Een zeer belangrijke toepassing van de Stelling van Euler is het cryptografisch systeem RSA, opgesteld door Ron Rivest, Adi Shamir and Leonard Adleman in 1977.
- Er bestaat ook een "niet elementair" bewijs van de kwadratische reciprociteitswet, door te redeneren in zogenaamde cyclotomische velden. Dit zijn velduitbreidingen van $\mathbb{Q}$ met wortels van cyclotomische polynomen, dit zijn de minimaalpolynomen van primitieve n-de eenheidswortels (hetgeen complexe getallen zijn).

Hoofdstuk 5

Inleiding tot de groepentheorie

5.1 Definities

In Hoofdstuk 1 en Hoofdstuk 4 hebben we de rekenregels opgesomd voor de optelling en de vermenigvuldiging in $\mathbb{Z}$ en in $\mathbb{Z}_m$. Het wordt tijd dat we deze regels wat formaliseren. Met andere woorden, we willen de structuur bepaald door een verzameling en een bewerking formeel beschrijven.

Heel wat van de definities zijn herhalingen van hetgeen in het secundair onderwijs ingevoerd werd, en eveneens in andere cursussen aan bod komen. We zullen ons beperken tot de meest belangrijke definities.

Definitie 5.1

Een *binaire bewerking* op een verzameling V is een afbeelding van de gedaante

$$f : V \times V \to V; (a, b) \longmapsto f(a, b).$$

Merk dus op dat een binaire bewerking steeds als een gesloten bewerking beschouwd wordt. Naar analogie met de getallenverzamelingen zullen we voor $f(a, b)$ meestal de additieve notatie $(a + b)$ of de multiplicatieve notatie (ab) gebruiken. Er is trouwens geen bezwaar om als voorbeeld steeds de optelling of vermenigvuldiging van (reële) getallen in gedachten te houden. Nochtans moeten we er de aandacht op vestigen dat er heel wat andere structuren met bewerkingen in aanmerking komen, zoals we later zullen zien.

De structuren die we beschrijven bestaan steeds uit een verzameling en een binaire bewerking. Zonder enige context noteren we dit 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, $a, b \in G$.

Definitie 5.2

Een *groep* is een koppel $(G, \cdot)$, waarbij G een verzameling is en $\cdot$ een binaire bewerking die aan 3 bijkomende voorwaarden voldoet.

(A) $\forall a, b, c \in G : \ a(bc) = (ab)c$ (associatieve wet);

(N) $\exists e \in G \parallel \forall a \in G, \ ae = ea = a$ (identiteitswet);

(I) $\forall a \in G, \ \exists a^{-1} \in G \parallel aa^{-1} = a^{-1}a = e$ (inversieve wet).

Dus in deze definitie is de notatie $\cdot$ niet relevant, we hadden net zo goed $+$ kunnen gebruiken, of f voor een binaire afbeelding.

Definitie 5.3

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 5.4

Een groep $G, \cdot$ is *abels* of *commutatief* als en slechts als de volgende voorwaarde voldaan is.

(C) $\forall a, b \in G, \ ab = ba$ (commutatieve wet).

Een eerste reeks voorbeelden wordt gegeven door de getallenverzamelingen en één van de standaardbewerkingen.

Voorbeeld 5.5.

- $\mathbb{Z}, +; \mathbb{Q}, +; \mathbb{R}, +; \mathbb{C}, +$ 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 5.6. 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 5.7. We hebben in Hoofdstuk 4 de verzamelingen $\mathbb{Z}_m$ ingevoerd, met bijhorende bewerkingen. Deze leveren interessante groepen.

- $\mathbb{Z}_m, \oplus$ is een abelse groep voor alle $m \in \mathbb{N} \setminus \{0, 1\}$.
- $\mathbb{Z}_m \setminus \{0\}, \otimes$ is een abelse groep als en slechts als m een priemgetal is. Dit is het volgende Lemma.

Lemma 5.8

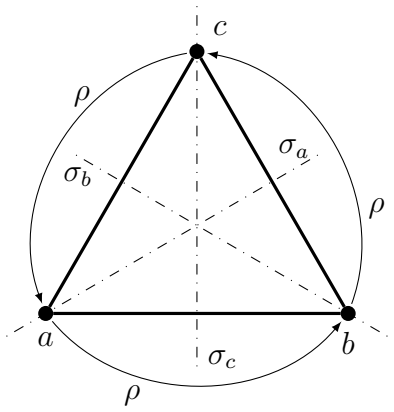
$\mathbb{Z}_m \setminus \{0\}, \otimes$ is een abelse groep als en slechts als m een priemgetal is.

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 4.6 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 5.9

De *orde* van een groep is het aantal elementen van de verzameling.



Figuur 5.1: Enkele symmetrieën van een gelijkzijdige driehoek

Voorbeeld 5.10. 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 rotaties: ρ en ρ^2, over respectievelijk 120° en 240° (in tegenwijzerzin); en de triviale symmetrie e; zie Figuur 5.10.

Het is eenvoudig om na te gaan dat het product van deze symmetrieën gegeven wordt door de volgende Cayley tabel.

$\bullet$	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_b	σ_c	σ_a
ρ^2	ρ^2	e	ρ	σ_c	σ_a	σ_b
σ_a	σ_a	σ_c	σ_b	e	ρ^2	ρ
σ_b	σ_b	σ_a	σ_c	ρ	e	ρ^2
σ_c	σ_c	σ_b	σ_a	ρ^2	ρ	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 5.11. 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).

5.2 Enkele eenvoudige eigenschappen

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 5.12

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 $ax = b$. □

5.3 Groepmorfismen

Definitie 5.13

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 5.14.

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 $\mathbb{Z}_4, \oplus$ is isomorf met de groep $\{e, a, b, c\}, \cdot$ waarbij de bewerking $\cdot$ door middel van de volgende Cayley tabel gedefinieerd wordt.

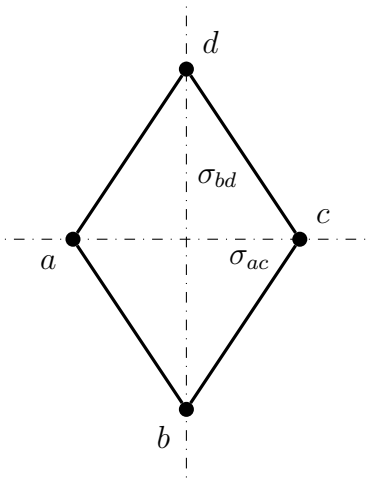
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

6. $\theta : \mathbb{Z} \to \mathbb{Z}, a \longmapsto -a$ is een automorfisme van $\mathbb{Z}, +$.

Stelling 5.15

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 5.12 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 5.12 vinden we dat $b = \theta(a^{-1})$. □

Voorbeeld 5.16. 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 5.3. 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 $\theta : V \to G$, $\theta(e) = e$, $\theta(\sigma_{ac}) = a$, $\theta(\sigma_{bd}) = b$, en $\theta(\varrho) = c$ een isomorfisme is tussen $V, \cdot$ en $G, \circ$. We hebben in Voorbeeld 5.14 (5) gezien dat $\mathbb{Z}_4, \oplus$ isomorf is met V; dus beide groepen zijn isomorf met de symmetriegroep van een ruit.

5.4 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 1. 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 5.17

Veronderstel dat $G, \cdot$ een groep is en $G' \subset G$ 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 5.18.

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 5.19.

1. Beschouw de viergroep van Klein zoals gedefinieerd in Voorbeeld 5.6. De groepen $\{e, a\}, \bullet$ (resp. $\{e, b\}, \bullet$ en $\{e, c\}, \bullet$) zijn deelgroepen van de viergroep van Klein, terwijl $\{e, a, b\}, \bullet$ geen deelgroep van de viergroep van Klein is.

2. De groep $\{e = \rho^3, \rho, \rho^2\}, \bullet$ is een deelgroep van D_6, die enkel de rotaties bevat. De orde van de deelgroep is 3.

Stelling 5.20 — 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 5.21

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 5.20 □

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 5.20 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 5.20.

Ook homomorfismen kunnen interessante voorbeelden van deelverzamelingen opleveren.

Definitie 5.22

Stel dat θ een homomorfisme is van $G, \cdot$ in $G', \times$. Het *beeld van* θ, genoteerd $\text{im}(\theta)$, is de verzamling $\{\theta(x) l x \in G\}$. De *kern van* θ, genoteerd $\ker(\theta)$, is de verzameling $\{x \in G \| \theta(x) = e'\}$ (het eenheidselement in G').

Stelling 5.23

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 5.20 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 5.14

Voorbeeld 5.24.

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 $\ker(\theta) = \{2x \| x \in \mathbb{Z}\}$.

5.5 Nevenklassen van een deelgroep

Definitie 5.25

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 5.26. De verzameling van de oneven gehele getallen is een nevenklasse van de additieve deelgroep van de even gehele getallen in $\mathbb{Z}, +$.

Stelling 5.27

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 5.28 — 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 5.29

Stel dat $H \leqslant G$. Het getal $\dfrac{|G|}{|H|}$ noemt men de *index van H in G* en wordt ook genoteerd als $[G : H]$.

5.6 Cyclische groepen

Definitie 5.30

Stel dat $G, \cdot$ een groep is en dat $D \subset G$. 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 5.31

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 5.31, 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 5.28 volgt dat de orde van een element van een groep steeds een deler is van de orde van de groep.

Stelling 5.32

Elke eindige cyclische groep van de orde m is isomorf met $\mathbb{Z}_m, \oplus$. 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 $r \equiv s \pmod{m}$. De afbeelding θ

$$\theta : G \to \mathbb{Z}_m; g^s \longmapsto [s]_m$$

is bijgevolg een isomorfisme van de eindige cyclische groep G van de orde m op de groep $\mathbb{Z}_m, \oplus$. □

Gevolg 5.33

Elke twee cyclische groepen van dezelfde orde zijn isomorf.

Alhoewel we voor een cyclische groep van de orde m mogen denken aan de groep $\mathbb{Z}_m, \oplus$, zullen we meestal de notatie C_m gebruiken omdat we gewoonlijk de bewerking multiplicatief en niet additief zullen noteren.

Stelling 5.34

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 5.35

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 5.36

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 7.30 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. □

5.7 Het direct product van groepen

Definitie 5.37

Veronderstel dat $A, *$ en $B, \bullet$ 2 groepen zijn. Beschouw $A \times B$ en definieer een bewerking $\cdot$ op $A \times B$ als volgt

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \bullet b_2).$$

We noemen $A \times B, \cdot$ *direct product* of het *cartesisch product* van de groepen A en B.

Op een volledige analoge manier kan het direct product van h groepen $A_1, A_2, \ldots, A_h$ gegeven worden.

Voorbeeld 5.38. De groep $C_2 \times C_3$ is isomorf met C_6. Inderdaad veronderstel dat $C_2 = \langle x \rangle = \{1, x\}$ en dat $C_3 = \langle y \rangle = \{1, y, y^2\}$. Dan bezit de groep $C_2 \times C_3$ de volgende 6 elementen:

$$(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2).$$

Indien we nu $z = (x, y)$ stellen, dan blijkt dat

$$\begin{aligned} z^2 &= (1, y^2) \\ z^3 &= (x, 1) \\ z^4 &= (1, y) \\ z^5 &= (x, y^2) \\ z^6 &= (1, 1). \end{aligned}$$

Hieruit volgt dat $C_2 \times C_3$ een cyclische groep is van de orde 6.

Het zou echter verkeerd zijn te denken dat het direct product van twee cyclische groepen steeds een cyclische groep is. Zo is bijvoorbeeld de viergroep van Klein geen cyclische groep maar wel isomorf met $C_2 \times C_2$.

Uit de volgende stelling blijkt dat $C_2 \times C_3$ isomorf is met C_6 omdat 2 en 3 copriem zijn.

Stelling 5.39

Als m en n copriem zijn, dan is

$$C_m \times C_n \cong C_{mn}.$$

Bewijs. Veronderstel dat $C_m = \langle x \rangle$ en dat $C_n = \langle y \rangle$. Noem z het element (x, y) van $C_m \times C_n$. Veronderstel dat z de orde r bezit. We bewijzen nu dat $r = mn$. Merk op dat het eenheidselement van de groep $C_m \times C_n$ het element $(1, 1)$ is. Aangezien z de orde r bezit, zal dus $1 = z^r = (x^r, y^r) = (1, 1)$. Bijgevolg is $x^r = 1$ in C_m en is $y^r = 1$ in C_n. Aangezien x de orde m bezit en aangezien y de orde n bezit, zal r een veelvoud zijn van m en van n. Bovendien is r de orde van z en dus het kleinste positief natuurlijk getal waarvoor $z^r = 1$, zodat $r = \text{kgv}(m, n)$. Aangezien m en n copriem zijn, zal $\text{kgv}(m, n) = mn$. Bijgevolg is z een element van de orde mn in de groep $C_m \times C_n$ van de orde mn, zodat $C_m \times C_n$ een cyclische groep is van de orde mn. □

5.8 Permutatiegroepen

We beschouwen een verzameling X van n elementen. Zonder de algemeenheid te schaden, mogen we veronderstellen dat $X = \{1, 2, \ldots, n\} = \mathbb{N}[1, n]$. 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 $f(i) = j \in \mathbb{N}[1, n]$ 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 $\mathbb{N}[1, 5]$.

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 $\mathbb{N}[1,n]$ (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 $\mathbb{N}[1,n]$ opgenomen hebben. Indien een element van $\mathbb{N}[1,n]$ 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

$$(1)(2)(3), \quad (1\ 2\ 3), \quad (1\ 3\ 2), \quad (1)(2\ 3), \quad (2)(1\ 3), \quad (3)(1\ 2).$$

We bekijken opnieuw de symmetriegroep van een gelijkzijdige driehoek uit Voorbeeld 5.10. 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. Nummeren we 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 $\mathbb{N}[1, 3]$.

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 5.40

Een permutatie van $\mathbb{N}[1, n]$ die 2 elementen verwisselt en de andere elementen fixeert, noemen we een *transpositie* van $\mathbb{N}[1, n]$.

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):

$$(x_1\ x_2\ \ldots\ x_{r-1}\ x_r) = (x_1\ x_r) \circ (x_1\ x_{r-1}) \circ \cdots \circ (x_1\ x_3) \circ (x_1\ x_2).$$

Bijgevolg kan elke permutatie geschreven worden als een samenstelling van een aantal transposities. Zo is bijvoorbeeld

$$(12)(579)(68) = (12) \circ (59) \circ (57) \circ (68).$$

Merk echter op dat de *ontbinding* van een permutatie als samenstelling van transposities niet uniek is. Zo is bijvoorbeeld in $\mathbb{N}[1, 7]$ (we laten hier voor de eenvoud het bewerkingsteken $\circ$ weg)

$$\begin{aligned}(1\ 5)(3\ 5)(3\ 6)(5\ 7)(1\ 4)(2\ 7)(1\ 2) &= (1\ 3\ 6)(2\ 4\ 5\ 7)\\ &= (1\ 6)(1\ 3)(2\ 7)(2\ 5)(2\ 4).\end{aligned}$$

Belangrijk en enigszins merkwaardig is wel dat de pariteit van het aantal transposities voor elke permutatie vast ligt, maw., 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 5.41

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. Om deze stelling te bewijzen, is het in feite voldoende van na te gaan wat er gebeurt met het aantal cykels indien we een permutatie samenstellen met een transpositie. We gaan dit na aan de hand van een voorbeeld.

Beschouw de permutatie

$$(1\ 2\ 3)(4\ 5)$$

van $\mathbb{N}[1,5]$. Dan geldt enerzijds dat

$$(1\ 2\ 3)(4\ 5) \circ (1\ 2) = (1\ 3)(2)(4\ 5),$$

en anderzijds dat

$$(1\ 2\ 3)(4\ 5) \circ (1\ 4) = (1\ 5\ 4\ 2\ 3).$$

In het eerste geval was het paar $\{1,2\}$ een deelverzameling van de cykel $(1\ 2\ 3)$ en werd daardoor het aantal cykels met 1 vermeerderd. In het tweede geval was het paar $\{1,4\}$ geen deelverzameling van een cykel en werd het aantal cykels in de samenstelling daardoor met 1 verminderd. Men kan nagaan dat dit een algemene regel is (oefening).

Veronderstel nu dat de permutatie α ontbonden is als samenstelling van r transposities:

$$\alpha = \sigma_r \sigma_{r-1} \ldots \sigma_2 \sigma_1.$$

De transpositie σ_1 bezit één cykel van lengte 2 en $n-2$ cykels van lengte 1. Indien we het aantal cykels van een permutatie f voorstellen door $c(f)$, dan is dus $c(\sigma_1) = n-1$. Indien we σ_1 samenstellen met de transpositie σ_2, zal $c(\sigma_2\sigma_1)$ ofwel met 1 verminderen of ofwel met 1 vermeerderen. In elke volgende stap van de uitwerking van de samenstelling gebeurt hetzelfde. We moeten in totaal $r-1$ samenstellingen uitrekenen. Veronderstel dat g keer het aantal cykels met 1 vermeerderd wordt en dat h keer het aantal cykels met 1 verminderd wordt. Dan is dus $g+h = r-1$ en bovendien is

$$c(\alpha) = c(\sigma_1) + g - h = n - 1 + g - h.$$

Hieruit volgt dat

$$r = 1 + g + h = 1 + g + n - 1 + g - c(\alpha) = n + 2g - c(\alpha).$$

Veronderstel nu dat α geschreven wordt als een samenstelling van r' transposities, dan geldt volledig analoog dat

$$r' = n + 2g' - c(\alpha).$$

Hieruit volgt dat

$$r - r' = 2(g - g').$$

Dit betekent dat r en r' dezelfde pariteit bezitten. □

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.

Hoofdstuk

6 Ringen, lichamen en velden

In het vorige hoofdstuk zijn we uitvoerig ingegaan op de groepen. Daarbij speelt één binaire bewerking een rol. De getallenverzamelingen leveren voorbeelden van groepen, maar we hebben heel wat andere voorbeelden gevonden die aan de axioma's van een groep voldoen. We hadden hierbij niet alleen de optelling en de vermenigvuldiging van getallen voor ogen. Wanneer we echter terugkeren naar de vertrouwde bewerkingen van optelling en vermenigvuldiging van de getallen, dan moeten we vaststellen dat het concept van een groep niet voldoende is om deze bewerkingen volledig te beschrijven. Zo geldt bijvoorbeeld ook nog de distributiviteit van de vermenigvuldiging ten opzichte van de optelling. In dit hoofdstuk gaan we dieper in op een axiomatische beschrijving en enkele eigenschappen van algebraïsche structuren waar twee binaire bewerkingen een rol spelen. In de beschrijving van deze structuren spelen groepen wel een prominente rol.

6.1 Ringen

De gehele getallen, voorzien van de optelling en vermenigvuldiging, vormen een standaardvoorbeeld dat we abstraheren in de volgende definitie.

Definitie 6.1

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 5.12 (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 6.2

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 $\mathbb{Z}_m, +, \cdot$.

Voorbeeld 6.3.

1. $\mathbb{Q}, +, \cdot; \mathbb{R}, +, \cdot; \mathbb{Z}, +, \cdot$ zijn (commutatieve) ringen voor de gewone optelling en vermenigvuldiging en bezitten geen nuldelers.

2. $\mathbb{Z}_m, \oplus, \otimes$ 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 $\mathbb{Z}_6$ 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. Bedie 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 6.4

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 5.12 (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 $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ en $U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$.

Stelling 6.5

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. □

Opmerkingen

In stelling 4.6 hebben we bewezen dat een element r in $\mathbb{Z}_m$ inverteerbaar is dan en slechts dan als r en m onderling ondeelbaar zijn. Bijgevolg is $U(\mathbb{Z}_m), \cdot$ in dit geval een groep van de orde $\varphi(m)$. Zo zal bijvoorbeeld $U(\mathbb{Z}_8), \cdot$ isomorf zijn met de viergroep van Klein (bewijs als oefening). Zoals we echter verder zullen zien, zal de groep $U(\mathbb{Z}_p), \cdot$ met p een priemgetal steeds een cyclische groep van de orde $\Phi(p) = p - 1$ zijn. Zo is bijvoorbeeld $U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$ een cyclische groep C_6 met voortbrengend element 3, want

$$3^2 \equiv 2 \pmod 7, \quad 3^3 \equiv 6 \pmod 7, \quad 3^4 \equiv 4 \pmod 7,$$

$$3^5 \equiv 5 \pmod 7, \quad 3^6 \equiv 1 \pmod 7.$$

Oefening 6.6. Toon aan dat de groep $U(\mathbb{Z}_8)$ is isomorf met de viergroep van Klein.

Oplossing. Men kan eenvoudig nagaan dat $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$. 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 $\theta : \mathbb{Z}_8 \to V$, $\theta(3) = a$, $\theta(5) = b$, $\theta(7) = c$ (en uiteraard $\theta(1) = e$) is dus een isomorfisme van $\mathbb{Z}_8, \otimes$ naar $V, \cdot$. ■

6.2 Lichamen en velden

Definitie 6.7

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 6.8

Een *veld* 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 abelse 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 veld is dus een lichaam F waarvoor de vermenigvuldiging commutatief is. Typische voorbeelden van velden zij $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. Uit Stelling 4.6 voldt dat $\mathbb{Z}_p$ een veld is als en slechts als p een priemgetal is. Dit is een voorbeeld van een *eindig veld*. Eén van de belangrijkste doelstellingen van dit hoofdstuk is de beschrijving van (andere) velden. We besteden in deze algemene sectie ook aandacht aan lichamen en enkele algemene eigenschappen. De volgende stelling is een mooie illustratie van hoe combinatorische eigenschappen algebraïsche eigenschappen kunnen induceren.

Stelling 6.9

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 6.10

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 6.11 — stelling van Wedderburn

Een eindig lichaam is een veld.

In Hoofdstuk 1 hebben we kort de getallenverzamelingen besproken. We bespreken nu een expliciete constructie voor $\mathbb{Q}$ en $\mathbb{R}$. De constructie van $\mathbb{Q}$ is intuïtief duidelijk. We kunnen dit echter in een abstracter kader beschrijven.

Veronderstel dat $R, +, \cdot$ een integriteitsgebied is, dus een commutatief domein. 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 *inbedding* 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 6.12

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.

De volgende stelling is een klassieker

Stelling 6.13

De vergelijking $x^2 = 2$ heeft geen oplossingen in $\mathbb{Q}$.

Bewijs. Zie cursus Analyse I. □

We beschouwen nu het veld $\mathbb{Q}$. 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. Er zijn echter meer sneden dan rationale getallen. De verzameling $B := \{x \in \mathbb{Q} \| x^2 < 2\}$ is een snede, maar door Stelling 6.13 bestaat er geen rationaal getal dat groter is dan alle elementen van B. Definieer $\mathbb{R}$ als de verzameling van alle sneden van $\mathbb{Q}$. Veronderstel dat A en B twee elementen uit $\mathbb{R}$ zijn, dan definiëren we de optelling $+_{\mathbb{R}}$ en $\cdot_{\mathbb{R}}$ als volgt.

$$A +_{\mathbb{R}} B := \{a + b \| a \in A, b \in B\}$$

$$A \cdot_{\mathbb{R}} B := \{x \in \mathbb{Q} \| \exists 0 \leq a \in A, \exists 0 \leq b \in B, x < ab\}$$

Het is niet ingewikkeld (maar vraagt wat schrijfwerk) om na te gaan dat $A +_{\mathbb{R}} B$ en $A \cdot_{\mathbb{R}} B$ sneden zijn. Het is ook niet moeilijk om een elk rationaal getal te beschrijven als een snede. De ordening $\leq_{\mathbb{R}}$ tenslotte is eenvoudig te definiëren als

$$A \leq_{\mathbb{R}} B \iff A \subset B\,.$$

Daarmee is al snel duidelijk dat $\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}$ een geordend veld is, dat $\mathbb{Q}$ bevat. We kunnen dus opnieuw de notatie $+$ en $\cdot$ behouden in $\mathbb{R}$, 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. De reële getallen voldoen aan het *supremumprincipe*: voor elke naar boven begrensde deelverzameling van $\mathbb{R}$ bestaat er een kleinste bovengrens. Merk op dat deze eigenschap inderdaad niet geldt in $\mathbb{Q}$.

6.3 Veeltermringen

We hebben formeel de velden $\mathbb{Q}$ en $\mathbb{R}$ geconstrueerd, en gezien dat $\mathbb{Q} \subset \mathbb{R}$. Informeel kunnen we zeggen dat $\mathbb{R}$ een uitbreiding is van het veld $\mathbb{Q}$. Dit is algemeen, aan aan veld F kunnen we proberen om elementen toe te voegen en zo F uit te breiden. 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. Wel zullen we enkele velduitbreidingen concreet beschrijven. Daartoe bestuderen we eerst een klasse van specifieke ringen, namelijk veeltermringen.

Definitie 6.14

Een *veelterm* of *polynoom* over een ring R is elke uitdrukking van de gedaante

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

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:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

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 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.

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots \\ &\qquad \cdots + a_nb_mx^{n+m}. \end{aligned}$$

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

$$p_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 \quad (0 \leq i \leq n+m) \quad (a_k = 0, \forall k > n; b_k = 0, \forall k > m).$$

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 $\mathbb{Z}_3[x]$ 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 $\mathbb{Z}_6[x]$ 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 $\mathbb{Z}_6$ 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.

6.3.1 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 6.15

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

$$\bar{a}(x) = a(x) - a_{m+k}b_m^{-1}x^k b(x).$$

De coëfficiënt van x^{m+k} in $\bar{a}(x)$ is

$$a_{m+k} - (a_{m+k}b_m^{-1})b_m = 0.$$

Bijgevolg is de graad van $\bar{a}(x)$ kleiner dan de graad van $a(x)$. Wegens de inductiehypothese weten we dat er veeltermen $\bar{q}(x)$ en $r(x)$ bestaan zodanig dat

$$\bar{a}(x) = b(x)\bar{q}(x) + r(x),$$

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

$$q(x) = \bar{q}(x) + a_{m+k}b_m^{-1}x^k.$$

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 3.6 kan, mutatis mutandis, overgenomen worden.

Definitie 6.16

Stel $a, b \in \mathbb{F}[x]$ niet beide nul. Een veelterm $c \in \mathbb{F}[x]$ 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 3.7 kan eenvoudig aangepast worden.

Lemma 6.17

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 6.18

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 3.11 opgesteld.

Stelling 6.19

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 6.20. *Zoek een grootste gemene deler $d(x)$ van $a(x) = x^3 + 2x^2 + x + 1$ en $b(x) = x^2 + 5$ in $\mathbb{Z}_7[x]$ 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 $\mathbb{Z}_7$ 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 $\mathbb{Z}_7[x]$ 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 $\mu(x) = 6x + 5$. ■

6.3.2 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 6.21

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 6.22

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 [9] is heel veel toegankelijke 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 6.23

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 6.24

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 6.25. *Zoek de irreducibele factoren van* $x^4 + 1$ *in* $\mathbb{Z}_3[x]$.

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 $a, b, c, d \in \mathbb{Z}_3$. 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 $\mathbb{Z}_3$.

$$\begin{cases} a + c &= 0 \\ b + d + ac &= 0 \\ ad + bc &= 0 \\ bd &= 1. \end{cases}$$

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 $\mathbb{Z}_3[x]$, 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 $\mathbb{Z}_p[x]$ (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, $\mathbb{Z}_p$ een veld is. De essentiële reden is het bestaan van

Bézoutcoëfficiënten, waarmee we een inverse konden bepalen van a modulo p. Maar, Stelling 6.19 biedt alle noodzakelijke ingrediënten om dit ook in $\mathbb{F}[x]$ mogelijk te maken.

We zullen deze manier van werken uitleggen aan de hand van een voorbeeld, om een al te formele beschrijven, die in elk geval wel gegeven wordt in de cursus Algebra, te vermijden. We kiezen $\mathbb{F} = \mathbb{R}$, 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, $x^2 = -1$. We hebben dus een formele constructie van het veld der complexe getallen via modulair rekenen in $\mathbb{R}[x]$.

In principe kunnen we nu polynomen in $\mathbb{C}[x]$ beschouwen, en bovenstaand principe herhalen. Dit levert ons echter geen groter veld, vanwege de volgende stelling. Een bewijs wordt doorgaans in een cursus Analyse gegeven. Er bestaat ook een zuiver algebraïsch bewijs, dat gebruik maakt van Galoistheorie.

Stelling 6.26 — 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. Het veld der complexe getallen is echter geen geordend veld.

Stelling 6.27

Er bestaat geen orderelatie in $\mathbb{C}$ die voldoet aan de voorwaarden van Definitie 6.12.

Bewijs. Veronderstel dat $\preceq$ een totale orderelatie is over $\mathbb{C}$ die voldoet aan de voorwaarden van Definitie 6.12. 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. □

6.4 Deelvelden en veldisomorfismen

Definitie 6.28

Stel $K, +, \cdot$ is een veld. Een verzameling $F \subset K$ 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.

Beschouw $\mathbb{R}, +, \cdot$. Het is duidelijk dat $\mathbb{Q}$ een deelveld is van $\mathbb{R}$. Uit de constructie van $\mathbb{C}$ hebben we ook geleerd dat $\mathbb{C}$ een twee dimensionale vectorruimte over $\mathbb{R}$ is. Algemeen is het heel eenvoudig om het volgende lemma aan te tonen.

Lemma 6.29

Stel K is een veld en $F \subset K$ is een deelveeld. Dan is K een F-vectorruimte.

Definitie 6.30

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. In deze cursus zullen we slechts op één plaats van veldisomorfismen gebruik maken.

6.5 Eindige velden

Definitie 6.31

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 5.6, opmerking op pagina 94).

Definitie 6.32

De *karakteristiek* p van een eindig veld is de orde van de additieve deelgroep voortgebracht door het element 1.

Lemma 6.33

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 6.34

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 6.35

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 $\psi : \mathbb{N} \to F$, $\psi(n) = n \cdot 1 := \underbrace{1 + \cdots + 1}_{n \text{ keer}}$. We kunnen deze afbeelding ψ beperken tot $\mathbb{Z}_p$, omdat we de elementen van $\mathbb{Z}_p$ kunnen identificeren met de elementen $0, 1, \ldots, p-1$. Men kan eenvoudig nagaan dat ψ een isomorfisme is tussen de velden $\mathbb{Z}_p$ en $\{\psi(x) \| x \in \mathbb{Z}_p\} \subset F$. Er bestaat dus een deelveld van F van orde p. 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. □

In eerste instantie bespreken we de constructie van eindige velden in detail, waarna we enkele eigenschappen zullen observeren. Een aantal daarvan wordt bewezen in Hoofdstuk 7.

6.5.1 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 $\mathbb{Z}_p$. Veronderstel nu dat $h > 1$. Een eindig veld van de orde $q = p^h$ wordt als volgt geconstrueerd.

1. Zoek een veelterm $f(t) \in \mathbb{Z}_p[t]$ van de graad h die irreducibel is over $\mathbb{Z}_p$.
2. Beschouw de restklassering $\mathbb{Z}_p[t]/\langle f(t) \rangle$. We hebben gezien dat deze bestaat uit de verzameling

$$K = \{a_0 + a_1 t + a_2 t^2 + \cdots + a_{h-1} t^{h-1} \| a_i \in \mathbb{Z}_p\}.$$

We kennen de optelling en vermenigvuldiging, deze zijn namelijk overgenomen uit $\mathbb{Z}_p[t]$ 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 6.15 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 6.3.2 dat deze constructie een veld is als $f(t)$ irreducibel is. Het volgende lemma vermelden we zonder bewijs.

Lemma 6.36

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 6.37

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 $\mathbb{Z}_p$. 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 $\mathbb{Z}_p[t]$ we gebruiken. We noteren een eindig veld van orde q als $\mathbb{F}_q$.

In Hoofdstuk 7 zullen we aantonen dat de multiplicatieve groep van $\mathbb{F}_q$ een cyclische groep van orde $q - 1$ is. 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 $\mathbb{Z}_p$ 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.

6.5.2 Voorbeelden van eindige velden

$\mathbb{F}_4$

1. We zoeken een veelterm $f(t) \in \mathbb{Z}_2[t]$ van de graad 2 die irreducibel is over $\mathbb{Z}_2$. De veelterm $f(t) = t^2 + t + 1$ voldoet hieraan.
2. $K = \mathbb{F}_4 = \{a_0 + a_1 t \| a_i \in \mathbb{Z}_2\} = \{0, 1, t, 1 + t\}$.
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 $\mathbb{Z}_2$. 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 $\mathbb{Z}_3$.

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 6.38. *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 6.39.

   (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) $\mathbb{F}_9 = \{0, \pm 1, \pm\alpha, \pm\alpha^2, \pm\alpha^3 \| 3 = \alpha^3 + \alpha - 1 = \alpha^2 - \alpha - 1 = \alpha^3 + \alpha^2 + 1 = \alpha^4 + 1 = 0\}$.

   Het komt er dus op aan om bij gebruik van de multiplicatieve notatie, volgende functie θ te kennen:

$$\begin{aligned}
\theta : \ \{0, 1, 2, \cdots, q-2, \dagger\} &\longrightarrow \{0, 1, 2, \cdots, q-2, \dagger\} \\
i &\longmapsto j \Longleftrightarrow \alpha^j = \alpha^i + 1.
\end{aligned}$$

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	$\dagger$
1	3
2	6
3	1
4	5
5	4
6	2
$\dagger$	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).

6.5.3 Enkele belangrijke stellingen

Stelling 6.40

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 4.13 gezien dat -1 een kwadraat is in $\mathbb{Z}_p$, 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 6.41

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 7.30 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 $q = 4m+1$. □

6.5.4 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 $\frac{c}{a}$ 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:

$$\begin{aligned} s^2 &= k^2\delta^4 + (k^2 + k^4)\delta^8 + \cdots + (k^2 + k^4 + \cdots + k^{2^{h-2}})\delta^{2^{h-1}} \\ &\quad + (k^2 + k^4 + \cdots + k^{2^{h-1}})\delta^{2^h}. \end{aligned}$$

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 6.42. 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 $t(x + t^2 + 1)(x + t + 1)$.

6.6 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 $H \subset M_2(\mathbb{C})$, 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 $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ als $\mathbb{R}$-algebra's, en als lichamen. De vermenigvuldiging in $\mathbb{H}$ wordt dan

$$(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) =$$
$$(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i$$
$$+(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2) j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2) k.$$

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.

Noten

- Evariste Galois (1812–1832) is één van de grondleggers van de theorie van de eindige velden, en daarom worden zij ook wel eens Galoisvelden van de orde q genoemd, en soms worden ze dan ook genoteerd door $\mathrm{GF}(q)$. Galois heeft deze *veldentheorie* ontwikkeld met de bedoeling om een klaar inzicht te krijgen in de stelling van Niels Abel uit 1826 waarin deze bewees dat de algemene oplossingen van een vergelijking van de 5de graad of hoger in 1 onbekende niet uitgedrukt kunnen worden in *radicalen* over $\mathbb{Q}$. Anders gezegd, in tegenstelling tot vierkantsvergelijkingen, derde graadsvergelijkingen en vierde graadsvergelijkingen met algemene coëfficiënten, kan er voor een vijfde graadsvergelijking geen formule opgesteld worden die de oplossingen weergeeft. Het is meer dan vermeldenswaardig dat Galois in zijn werk over veldentheorie en velduitbreidingen ook het abstracte principe van symmetrie opstelt, en aldus de basis legt van de moderne groepentheorie. Het is dan ook niet verwonderlijk dat het moderne bewijs van Abel's stelling en haar veralgemening een gevolg is van een eigenschap van de alternerende groepen A_n, $n \geq 5$. Eveneens vermeldenswaardig is het feit dat Galois, allemaal in het kader van bovenvermeld werk, reeds bepaalde matrixgroepen bestudeerde die de groep van bepaalde collineaties van de projectieve rechte voorstellen. Dit verklaart ook meteen de naam *Galoismeetkunde*, wat tegenwoordig de naam is voor het vakgebied dat zich bezig houdt met de studie van projectieve meetkunde over eindige velden. Een zeer interessant en uitstekend geschreven vulgariserend werk waar Galois en zijn werk aan bod komt is [3] – origineel in het Engels, [2].

- William Rowan Hamilton (1805-1865), Iers wiskundige, is de bedenker van het principe $i^2 = j^2 = k^2 = ijk = -1$. Tijdens een wandeling in Dublin zag hij het licht, en kerfde dit principe in een brug.

- Joseph Wedderburn was de eerste om zijn stelling te bewijzen. Sommige bronnen vermelden echter een gat in zijn bewijs. Het bewijs dat heden gebruikelijk gegeven wordt, is toe te schrijven aan Ernst Witt (1911 – 1991).
- In Nederland heet een lichaam een *scheeflichaam*, en een veld een *lichaam*.

Hoofdstuk

7 Combinatoriek

7.1 Het principe van de dubbele telling

Veronderstel dat X en Y 2 eindige verzamelingen zijn met $|X| = n$ en $|Y| = m$. een willekeurige deelverzameling $S \subset X \times Y$. 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 7.1

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 7.2

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
$$|X \times Y| = |X| \cdot |Y|.$$

7.2 Het eenvoudig inclusie–exclusie principe

Dit principe is een uitbreiding van het vereenvoudigd 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 7.3. *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

$$1000 - (333 + 142 - 47) = 572.$$

■

7.3 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.

7.3.1 Variaties

Voorbeeld 7.4. 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 7.5

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 7.6

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. □

7.3.2 Permutaties

Definitie 7.7

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.

7.3.3 Combinaties

Voorbeeld 7.8. 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 7.9

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 7.10

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, maw. 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 7.11

Er geldt $\binom{n}{k} = \frac{V_n^k}{k!} = \frac{n!}{(n-k)!k!}$.

Enkele belangrijke eigenschappen formuleren we in de volgende lemma's en een stelling.

Lemma 7.12

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 7.13

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 7.14 — 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

$$\begin{array}{lllll} \binom{n}{0} & = & \binom{n}{n} & = & 1 \\ \binom{n}{1} & = & \binom{n}{n-1} & = & n \\ \binom{n}{2} & = & \binom{n}{n-2} & = & \dfrac{n(n-1)}{2} \\ \ldots & & \ldots & & \ldots \end{array}$$

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

7.3.4 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 7.15

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 7.16

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.

7.3.5 Herhalingscombinaties

Definitie 7.17

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 herhalingskombinaties 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 7.18

Er gedlt $\overline{\binom{n}{k}} = \binom{n+k-1}{k}$.

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

	zonder terugplaatsen	met terugplaatsen
ongeordend	$\binom{n}{k}$	$\binom{n+k-1}{k}$
geordend	$n(n-1)\cdots(n-k+1)$	n^k

Tabel 7.1: Overzicht (herhalings)variaties en (herhalings)combinaties

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 7.1 vat de resultaten samen.

7.4 Toepassingen op combinatieleer

7.4.1 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. 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.*

7.4.2 Het aantal deelverzamelingen van een verzameling

Stelling 7.19

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. □

7.4.3 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 7.20

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)

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=0}^{n} \binom{n}{n-k} a^{n-k} b^k.\end{aligned}$$

7.4.4 Het (veralgemeend) inclusie–exclusie principe

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–exclusie principe* of *zeefprincipe*.

Stelling 7.21 — inclusie-exclusie- of zeefprincipe

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. □

7.4.5 Permutaties zonder fixelementen: wanorde

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 $\mathbb{N}[1, n]$ die geen enkel fixelement bezitten. Een dergelijke permutatie wordt een *wanorde* genoemd. Volgens het inclusie-exclusie principe is het totaal aantal wanordes d_n van $\mathbb{N}[1, n]$ gelijk aan

$$d_n = n! - \alpha_1 + \alpha_2 - \cdots + (-1)^n\alpha_n,$$

waarbij α_i het aantal permutaties is van $\mathbb{N}[1, n]$ die minstens i elementen fixeren voor alle mogelijke keuzes van i uit $\mathbb{N}[1, n]$. Er zijn nu $\binom{n}{i}$ manieren om i elementen te kiezen uit $\mathbb{N}[1, n]$, en het aantal permutaties van $\mathbb{N}[1, n]$ 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 wanordes 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 $\mathbb{N}[1,n]$ 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 wanordes.

Indien $f(k_1) = 1$, dan zal f een wanorde definiëren op de verzameling $\mathbb{N}[1,n] \setminus \{1, k_1\}$. Het aantal dergelijke wanordes is per definitie gelijk aan d_{n-2}. Merk op dat elke wanorde op $\mathbb{N}[1,n] \setminus \{1, k_1\}$ aanleiding geeft tot juist 1 wanorde op $\mathbb{N}[1,n]$ door de definitie $f(1) = k_1;\ f(k_1) = 1$.

Veronderstel nu dat f een wanorde is waarvoor geldt dat $f(k_1) \neq 1$, dan bestaat er een $k_0 \in \mathbb{N}[1,n] \setminus \{1, k_1\}$ zodanig dat $f(k_0) = 1$. We definiëren nu een nieuwe permutatie g in $\mathbb{N}[2,n]$ door $g(k_0) = k_1$ en $g(k) = f(k)\ \forall k \neq k_0$. Dan is g eveneens een wanorde, maar nu op de verzameling $\mathbb{N}[2,n]$, 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 wanorde f waarvan we waren vertrokken.

Bijgevolg het aantal wanordes f waarvoor geldt dat $f(1) = k_1 \in \mathbb{N}[2,n]$ (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 wanordes 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

7.5 De Stirling getallen

Definitie 7.22

Het *Stirling getal* $S(n,k)$ (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 7.23

Het Stirling getal $S(n,k)$ 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 Stirling getallen 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 7.24

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. □

De kritische lezer vraagt zich misschien af waar de Stirling getallen van de *eerste* soort gebleven zijn. In [6, Sectie 3.4] vindt men een prima omschrijving van de *beide* soorten Stirling getallen en het verband ertussen.

7.6 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:

$$\left(\begin{array}{c} n \\ n_1, n_2, \ldots, n_k \end{array} \right).$$

Merk op dat

$$\binom{n}{n_1, n_2} = \binom{n}{n_1},$$

vandaar de benaming multinomiaalgetallen als veralgemening van de binomiaalgetallen.

Stelling 7.25

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 7.26

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, ..., de term a_k nemen uit n_k van de factoren. Dit is juist de definitie van de multinomiaalgetallen. Hieruit volgt het gestelde. □

7.7 Enkele toepassingen in de algebra

7.7.1 De Möbiusfunctie

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:

$$\mu(d) = \begin{cases} 1 & \text{als } d = 1 \\ (-1)^r & \text{als } d \text{ een product is van } r \text{ verschillende priemgetallen} \\ 0 & \text{als } d \text{ een meervoudige priemfactor bezit.} \end{cases}$$

Stelling 7.27

Voor elk natuurlijk getal $n \geq 2$ zal de som van de waarden $\mu(d)$, genomen over alle delers van n, gelijk zijn aan 0, m.a.w.

$$\sum_{d|n} \mu(d) = 0.$$

Bewijs. Veronderstel dat $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Elke deler d is dan van de vorm $d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$ met $0 \leq x_i \leq e_i$. Bovendien is $\mu(d) = 0$ tenzij elk van de x_i $(1 \leq i \leq k)$ gelijk is aan 0 of 1. Bijgevolg zal elke deler d waarvoor $\mu(d) \neq 0$, corresponderen met een deelverzameling van $\{p_1, p_2, \dots, p_k\}$ bestaande uit de priemgetallen p_i met $x_i = 1$. Het aantal dergelijke deelverzamelingen van de orde r is $\binom{k}{r}$ en voor elke deler d die het product is van r verschillende priemfactoren geldt dat $\mu(d) = (-1)^r$. Bijgevolg is

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k} = 0.$$

□

Stelling 7.28

Veronderstel dat g een functie is met definitiegebied (een deelverzameling van) $\mathbb{N} \setminus \{0\}$ 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:

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Bewijs.

$$\begin{aligned}\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right) &= \sum_{d|n}\mu(d)\left(\sum_{c|(n/d)}g(c)\right)\\ &= \sum\sum\mu(d)g(c).\end{aligned}$$

Hierbij wordt de dubbele sommatie genomen over de verzameling S van alle koppels (c,d) waarvoor geldt dat $d|n$ en $c|(n/d)$. Maar dit is eveneens de verzameling van de koppels (c,d) waarvoor geldt dat $c|n$ en $d|(n/c)$, zodat we de sommatie als volgt kunnen schrijven:

$$\sum_{c|n}g(c)\left(\sum_{d|n/c}\mu(d)\right).$$

Wegens bovenstaande stelling is de som tussen de haken gelijk aan 0 van zodra $n/c \geq 2$. Bijgevolg wordt de bovenstaande uitdrukking

$$g(n)\sum_{d|1}\mu(d) = g(n)\mu(1) = g(n),$$

wat te bewijzen was. □

Gevolg 7.29

Aangezien $\sum_{d|n}\varphi(d) = n$ zal als gevolg van de Möbius inversieformule

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}.$$

Deze formule is echter niets anders dan een verkorte schrijfwijze van de volgende formule die uit (3.2) kan afgeleid worden.

$$\begin{aligned}\varphi(n) &= n - \left(\frac{n}{p_1}+\frac{n}{p_2}+\cdots+\frac{n}{p_k}\right)+\left(\frac{n}{p_1p_2}+\frac{n}{p_1p_3}+\cdots+\frac{n}{p_{k-1}p_k}\right)-\cdots\\ &\quad\cdots+(-1)^k\left(\frac{n}{p_1p_2\cdots p_k}\right).\end{aligned}$$

Ook voor de Möbius functie geldt de formule

$$\mu(mn) = \mu(m)\mu(n) \quad \forall(m,n); \text{ggd}(m,n) = 1.$$

7.7.2 Groepen

Stelling 7.30

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 Möbius inversieformule en haar Gevolg 7.29 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, maw. G is een cyclische groep van de orde n. □

Gevolg 7.31

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 7.32. 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:

$$\begin{aligned}
C_1 &= \langle 1 \rangle = \{1\} \\
C_2 &= \langle z^6 \rangle = \{1, z^6\} \\
C_3 &= \langle z^4 \rangle = \langle z^8 \rangle = \{1, z^4, z^8\} \\
C_4 &= \langle z^3 \rangle = \langle z^9 \rangle = \{1, z^3, z^6, z^9\} \\
C_6 &= \langle z^2 \rangle = \langle z^{10} \rangle = \{1, z^2, z^4, z^6, z^8, z^{10}\} \\
C_{12} &= \langle z \rangle = \langle z^5 \rangle = \langle z^7 \rangle = \langle z^{11} \rangle = \{z, z^2, \ldots, z^{11}, z^{12} = 1\}.
\end{aligned}$$

7.7.3 Eindige velden

Stelling 7.33

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 7.30 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 7.30 voldoende om te besluiten dat $\mathbb{F}_q^*$ een cyclische groep is van de orde $q-1$. □

Hoofdstuk 8

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.

8.1 Ongerichte grafen

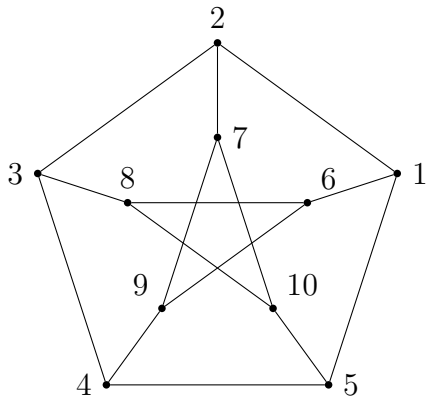
Heel eenvoudig gezegd is een graaf een verzameling van toppen, samen met een verzameling van verbindingen tussen twee toppen. Soms speelt de richting van deze verbinding een rol, soms zijn er meerdere verbindingen tussen twee punten mogelijk, en soms zijn er lussen. We starten met een formele definitie van een van de eenvoudigste gevallen.

Definitie 8.1

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.

We kunnen een graaf definiëren door opsomming. Beschouw bijvoorbeeld



Figuur 8.1: Petersen graaf

het Petersen graaf (Figuur 8.1). Dan is

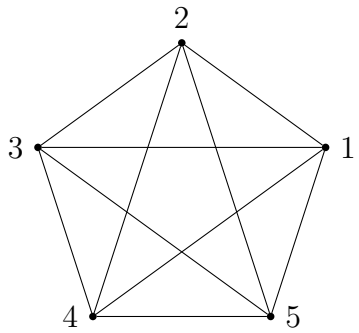
$$
\begin{aligned}
T(\Gamma) =& \{1,2,3,4,5,6,7,8,9,10\} \\
E(\Gamma) =& \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\} \\
\sigma =& \{(1,(1,2)),(2,(1,5)),(3,(1,6)),(4,(2,3)),(5,(2,7)),(6,(3,4)),(7,(3,8)), \\
& (8,(4,5)),(9,(4,9)),(10,(5,10)),(11,(6,8)),(12,(7,9)),(13,(8,10)), \\
& (14,(9,6)),(15,(10,7))\}
\end{aligned}
$$

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 8.2 toont het compleet graaf op 5 toppen. Algemeen is het compleet graaf op n toppen snel omschreven: $T(\Gamma) := \mathbb{N}[1 \ldots n]$, $E(\Gamma) :=$



Figuur 8.2: Compleet graaf op 5 toppen

$\{\{x, y\} \| x, y \in T, x \neq y\}$. 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 8.2

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 8.3

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, hoeveel bogen kan Γ bevatten? Merk op dat het Petersen graaf bijvoorbeeld geen 3-clique bevat.

Stelling 8.4

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

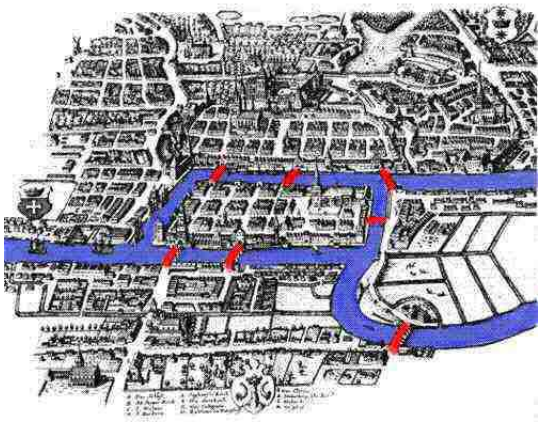
$$e_{A,B} \leq (p-2)(n-p+1)\,.$$

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 $B(\Gamma_2)$.

Als $\Gamma_1 = \Gamma_2$, dan spreken we van een automorfisme Γ_1.



Figuur 8.3: De zeven bruggen van Koningsbergen

Stelling 8.5

De automorfismegroep van het Petersengraaf is S_5.

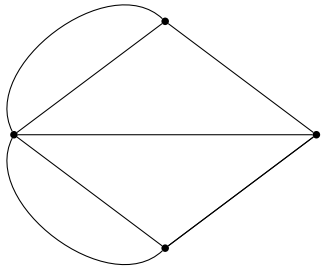
Bewijs. Oefening. □

8.2 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 8.3

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 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

[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 8.4: De zeven bruggen in een graaf

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 8.6

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 8.7 — 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. □

8.3 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 8.8

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 8.9 — 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

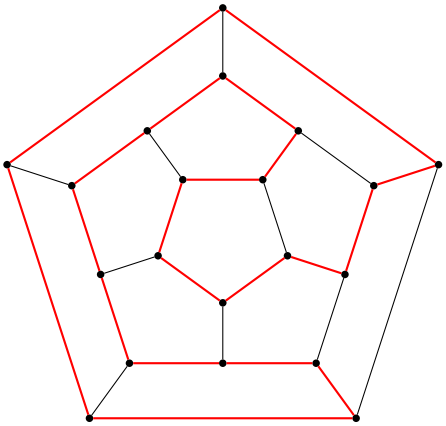
Het zou verkeerd zijn te denken dat een graaf waarbij één of meerdere toppen een graad bezit die kleiner is dan de helft van de orde nooit Hamiltoniaans kan zijn. Het is uiteraard voldoende om hiervan een tegenvoorbeeld te geven. Een standaardvoorbeeld voor Hamiltoniaanse grafen is de dodecaëder graaf. 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 8.5 maakt duidelijk dat de graaf inderdaad Hamiltoniaans is.

8.4 Planaire grafen

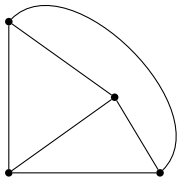
Definitie 8.10

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



Figuur 8.5: Hamiltoniaans pad (rood)



Figuur 8.6: Compleet graaf op 4 toppen

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 8.2). 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 8.6), 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

Stelling 8.11 — 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 8.12

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 $E := \{\{x, y\} \| x \in Uenv \in V\}$, $T := U \cup V$. 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 8.13 — 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 8.12 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 8.1), 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 8.14 — 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. □

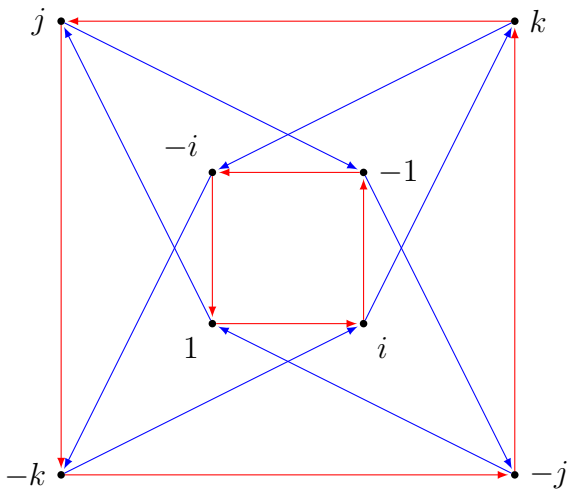
Ongeveer op het einde van de negentiende eeuw werd de conjectuur geformuleerd dat 4 kleuren volstaan om een planair graaf te kleuren. Het duurde tot 1976 eer een bewijs gegeven werd. Dit bewijs herleidde het probleem tot 1936 subgevallen, die met behulp van de computer afgehandeld werden. Hadwiger's 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.

8.5 gekleurde grafen

We kunnen definitie 8.6 uitbreiden tot gerichte grafen.

Definitie 8.15

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.



Figuur 8.7: Cayleygraaf van Q_8

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 8.7 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

$$1 \overset{i}{\to} i \overset{j}{\to} k \overset{i^{-1}}{\to} -j \overset{j^{-1}}{\to} -1\,.$$

Bekijken we het pad

$$1 \overset{i}{\to} i \overset{j}{\to} k \overset{i^{-1}}{\to} -j \overset{j^{-1}}{\to} -1 \overset{i}{\to} -i \overset{j}{\to} -k \overset{i^{-1}}{\to} j \overset{j^{-1}}{\to} 1\,,$$

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 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, [4]), samen met de extensie GRAPE ([8]). 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.

8.6 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 adjacentiematric 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 8.16

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) $\implies$ (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) $\implies$ (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 8.4, 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.

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] M. du Sautoy, *Finding Moonshine*, Harper Perennial, 2009. ISBN: 978-0-00-721462-4.

[3] ——, *Het Symmetriemonster*, Uitgeverij Nieuwezijds, 2010. ISBN: 978 90 5712 286 6.

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.5*, 2012.

[5] D. E. Knuth, *The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[6] M. E. Larsen, *Summa summarum*, CMS Treatises in Mathematics, Canadian Mathematical Society, Ottawa, ON, 2007.

[7] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer-Verlag, 2009.

[8] L. H. Soicher, *The GRAPE package for GAP*, 2012.

[9] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, second ed., 2003.

Index