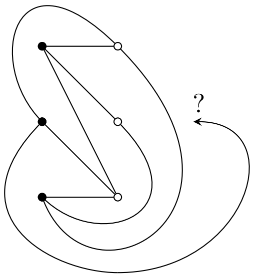
Caleidoscoop



door

dr.H.Finkelnberg

10 oktober 2013

Inhoudsopgave

1 Logica

Wie wiskunde wil leren moet naast de materie zelf zich ook de taal van de wiskunde eigen maken. In deze module worden twee fundamentele componenten van deze wiskundetaal behandeld: logica en kwantoren.

In de wiskunde spelen uitspraken een hoofdrol. Wiskunde is een wetenschap van uitspraken, waarbij getracht wordt de juistheid van deze uitspraken aan te tonen. Met de juistheid van een uitspraak wordt bedoeld of deze *waar* of *onwaar* is.

Voorbeelden van uitspraken:

- De zon is rond.
- Een week bestaat uit 5 dagen.
- Vijf is meer dan drie.
- $3 + 2 = 5$
- $8 - 2 = 11$

De eerste twee uitspraken, waarvan er één waar is en één onwaar, zijn niet erg wiskundig van aard, maar het zijn wel uitspraken. De derde is wel wiskundig, maar is taalkundig geformuleerd. De laatste twee uitspraken zijn zowel wiskundig van aard als ook wat notatie betreft.

Opmerking: De eerste drie uitspraken zijn zinnen. De laatste twee niet! Het '='-symbool in deze laatste twee uitspraken is dus géén gezegde, ook al wordt het uitgesproken als *is gelijk aan*. Gebruik dit '='-teken dan ook liever niet als een gezegde! Bijvoorbeeld:

- Fout: Als $a = 2$, dan is a even.
- Goed: Als geldt $a = 2$, dan is a even.

In de wiskunde worden veel symbolen gebruikt. Reden hiertoe is niet alleen de compacte en vooral ondubbelzinnige notatie, maar het maakt de formulering meer internationaal. In dit dictaat zullen bij *Kwantoren* twee heel bijzondere symbolen behandeld worden: de kwantoren.

In de wiskunde vindt ook zeer vaak het samenvoegen van uitspraken tot nieuwe uitspraken plaats. Dit is wat veel in bewijzen van stellingen gebeurt. Dit samenvoegen dient natuurlijk volkomen ondubbelzinnig te gebeuren. In dit dictaat zal bij *Logica* worden behandeld wat hier de spelregels zijn.

1.1 Logica

In de wiskunde gaan we er van uit dat een uitspraak *waar* of *onwaar* is. We geven dit aan door aan een uitspraak de waarde 1 toe te kennen als de uitspraak waar is en 0 als de uitspraak onwaar is. Om tot correcte bewijzen van wiskundige stellingen te komen, moeten uitspraken gecombineerd kunnen worden. In de wiskunde worden voornamelijk vier combinatieregels gebruikt om twee uitspraken te versmelten tot één uitspraak. Deze worden hier in eerste instantie formeel, zonder interpretatie, gedefinieerd als *binaire operatoren* op de *verzameling* $\{0, 1\}$:

- De *én-operator* met symbool $\wedge$.
- De *of-operator* met symbool $\vee$.
- De *implicatie-operator* met symbool $\Rightarrow$.
- De *equivalentie-operator* met symbool $\Leftrightarrow$.

Daarnaast kent men in de wiskunde ook nog de unaire *ontkennings-operator* met symbool $\neg$.

Definitie 1 *De operatoren $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ en $\neg$ worden als volgt gedefinieerd:*

A	B	$A \wedge B$ *A en B*	$A \vee B$ *A of B*	$A \Rightarrow B$ *A impliceert B*	$A \Leftrightarrow B$ *A is equivalent met B*	$\neg A$ *niet A*
0	0	0	0	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	0	0
1	1	1	1	1	1	0

De operatoren $\wedge$, $\vee$, $\Rightarrow$ en $\Leftrightarrow$ zijn *binaire operatoren*: aan ieder geordend tweetal elementen van de verzameling $\{0, 1\}$ wordt één element van deze verzameling toegekend. Zo is bijvoorbeeld de optelling een binaire operator op de verzameling der gehele getallen.

De operator $\neg$ is een *unaire operator*: deze voegt aan één element een ander (in principe niet noodzakelijkerwijs verschillend) element van de verzameling toe. Zo is bijvoorbeeld het min-teken een unaire operator op de verzameling der gehele getallen.

Een aantal opmerkingen:

- Vanaf nu zullen we de getallen 0 en 1 weer interpreteren als *onwaar* en *waar*. Vergeet echter niet dat de formele definitie van de operatoren plaats heeft gevonden zonder deze interpretatie!
- De of-operator $\vee$ is een zwakke of. De uitkomst is waar als minstens één van de componenten waar is; dus mogelijk ook beide.
- De implicatie is, ondanks zijn suggestieve naamgeving, niets anders dan een formele binaire operator waarvan de uitkomst volledig door bovenstaande tabel wordt vastgelegd. Het waar zijn van een implicatie, dat wil zeggen dat de uitkomst gelijk is aan 1, duidt niet op een oorzakelijk verband! Hetzelfde geldt voor de equivalentie. Zo zijn de volgende uitspraken allemaal waar:

  $2 < 3 \Rightarrow 7 = 7$

  $2 > 3 \Rightarrow 7 = 7$

  $2 > 3 \Rightarrow 23456789^{1234567} < 0$

  $3^{321} = 5 \Leftrightarrow \pi \in \mathbb{Q}$

  $3^{321} > 5 \Leftrightarrow$ de stelling van Fermat is waar
- Een veelgemaakte fout is dat de implicatiepijl wordt uitgesproken als *dus*. Dit is natuurlijk onjuist! De uitspraak $A \Rightarrow B$ zegt *niets* over de waarheid van A!.

1.1.1 Combinaties van drietallen

Deze logische operatoren zijn te vergelijken met de operatoren $+$, $\times$ en $-$ op de verzameling der gehele getallen. Eén eigenschap van de optelling beschouwen we nader. Als a, b en c drie getallen zijn, heeft niemand moeite met de expressie $a+b+c$. Toch zou het in eerste instantie de wenkbrauwen moeten doen fronzen. De optelling is immers een *binaire* operator en geen *ternaire*. Hoezo kan er dan gesproken worden over $a + b + c$? Dat is welgedefinieerd is (*wel* in de zin van *goed*, niet in de zin van *welles-nietes*), is een gevolg van een eigenschap van de optelling: *associativiteit*. Associativiteit wil zeggen dat het niet uitmaakt hoe de haakjes geplaatst worden en dat voor alle gehele a, b en c geldt:

$$(a + b) + c = a + (b + c)$$

Dit rechtvaardigt de notatie $a + b + c$ met als definitie:

$$a + b + c := (a + b) + c = a + (b + c)$$

De dubbele punt vóór het eerste =-teken geeft aan dat dit een definieërende = is.

1.1.2 Wat bedoelt men met $A \vee B \vee C$?

Als iemand de uitspraak $A \vee B \vee C$ formuleert, wordt er waarschijnlijk bedoeld dat minstens één van de drie componenten waar is. We controleren of dit formeel ook zo is. Hiertoe moeten we twee dingen nagaan:

- Is de operator $\vee$ wel associatief?
- Zo ja, komt de uitkomst van $(A \vee B) \vee C$ overeen met wat we er van verwachten: waar precies dan als minstens één van de drie componenten waar is?

Dat op beide vragen het antwoord *ja* is, wordt door onderstaande tabel aangetoond:

A	B	C	$A \vee B$	$B \vee C$	$(A \vee B) \vee C$	$=$	$A \vee (B \vee C)$	$=:$	$A \vee B \vee C$
0	0	0	0	0	0	=	0		0
0	0	1	0	1	1	=	1		1
0	1	0	1	1	1	=	1		1
0	1	1	1	1	1	=	1		1
1	0	0	1	0	1	=	1		1
1	0	1	1	1	1	=	1		1
1	1	0	1	1	1	=	1		1
1	1	1	1	1	1	=	1		1

1.1.3 Wat bedoelt men met $A \wedge B \wedge C$?

Als iemand de uitspraak $A \wedge B \wedge C$ formuleert, wordt er waarschijnlijk bedoeld dat alle drie de componenten waar zijn. We controleren of dit formeel ook zo is. Hiertoe moeten we twee dingen nagaan:

- Is de operator $\wedge$ wel associatief?
- Zo ja, komt de uitkomst van $(A \wedge B) \wedge C$ overeen met wat we er van verwachten: waar precies dan als ze alle drie waar zijn?

Dat op beide vragen het antwoord *ja* is, wordt door onderstaande tabel aangetoond:

A	B	C	$A \wedge B$	$B \wedge C$	$(A \wedge B) \wedge C$	$=$	$A \wedge (B \wedge C)$	$=:$	$A \wedge B \wedge C$
0	0	0	0	0	0	=	0		0
0	0	1	0	0	0	=	0		0
0	1	0	0	0	0	=	0		0
0	1	1	0	1	0	=	0		0
1	0	0	0	0	0	=	0		0
1	0	1	0	0	0	=	0		0
1	1	0	1	0	0	=	0		0
1	1	1	1	1	1	=	1		1

1.1.4 Wat bedoelt men met $A \Leftrightarrow B \Leftrightarrow C$?

Bij dit drietal lijkt er een probleem te ontstaan. In de praktijk bedoelt men met $A \Leftrightarrow B \Leftrightarrow C$, dat óf alle drie de uitspraken waar zijn óf juist alle drie onwaar. Oftewel, dat ze onderling equivalent zijn. We onderzoeken dit op dezelfde wijze als bij de *en* en de *of* en beschouwen de volgende tabel:

A	B	C	$A \Leftrightarrow B$	$B \Leftrightarrow C$	$(A \Leftrightarrow B) \Leftrightarrow C$	=	$A \Leftrightarrow (B \Leftrightarrow C)$
0	0	0	1	1	0	=	0
0	0	1	1	0	1	=	1
0	1	0	0	0	1	=	1
0	1	1	0	1	0	=	0
1	0	0	0	1	1	=	1
1	0	1	0	0	0	=	0
1	1	0	1	0	0	=	0
1	1	1	1	1	1	=	1

We zien dat de equivalentie inderdaad associatief is, maar dat de betekenis van $A \Leftrightarrow B \Leftrightarrow C$ in het licht van associatieve binaire operatoren *niet* overeenstemt met wat men er mee bedoelt:

A	B	C	$A \Leftrightarrow B \Leftrightarrow C$ als binaire operator	$A \Leftrightarrow B \Leftrightarrow C$ praktijk
0	0	0	0	1
0	0	1	1	0
0	1	0	1	0
0	1	1	0	0
1	0	0	1	0
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

Wat hier achter zit, is het volgende. Er kan op twee manieren naar *equivalentie* worden gekeken:

- als binaire operator op de verzameling $\{0, 1\}$, zoals hierboven gedefinieerd is;
- als transitieve relatie.

De term *transitieve relatie* zegt jullie in dit stadium nog niets, maar denk maar aan de ongelijkheid ($<$) of de gelijkheid ($=$). Als iemand opschrijft:

$$a = b < c,$$

dan wordt hiermee bedoeld:

$$(a = b) \wedge (b < c).$$

Zo is dat in de praktijk ook met de equivalentie. Waar men noteert $A \Leftrightarrow B \Leftrightarrow C$ wordt $\Leftrightarrow$ gebruikt als een transitieve relatie en bedoelt men $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)$. In het bijzonder geldt dan dus ook $A \Leftrightarrow C$.

1.2 Kwantoren

In de wiskunde komen uitspraken van de volgende vorm veelvuldig voor:

- Ieder kwadraat van een reëel getal is niet negatief.

- Ieder geheel getal is te ontbinden in priemfactoren.
- Er bestaat een reëel getal waarvan het kwadraat gelijk is aan 2.
- Voor ieder geheel getal bestaat er een groter geheel getal.
- Er bestaat een geheel getal dat kleiner is dan ieder positief geheel getal.

Deze uitspraken maken gebruik van twee bouwstenen:

- Voor ieder $\cdots$
- Er bestaat (bestaan) $\cdots$

Deze bouwstenen komen zo vaak voor in de wiskunde, dat ze hun eigen symbolen hebben gekregen: de *kwantoren*.

Definitie 2 (Universele kwantor) *Het symbool* $\forall$ *is de* universele kwantor *en staat voor* voor alle*.*

Definitie 3 (Existentiële kwantor) *Het symbool* $\exists$ *is de* existentiële kwantor *en staat voor* er bestaat *of* er bestaan*.*

De herkomst van deze symbolen is eenvoudiger dan men op het eerste gezicht zou denken:

- De universele kwantor $\forall$ is niets anders dan de vertikaal gespiegelde A in *for All* (horizontaal spiegelen had hier niet zo veel zin).
- De existentiële kwantor $\exists$ is niets anders dan de horizontaal gespiegelde E in *there Exists* (vertikaal spiegelen had hier niet zo veel zin).

Hieronder staan wat voorbeelden van het gebruik van kwantoren. Het symbool $\in$ staat voor *(is) element van de verzameling*.

- Ieder kwadraat van een reëel getal is niet negatief:
$$\forall a \in \mathbb{R} : a^2 \geq 0.$$
- Ieder geheel getal is te ontbinden in priemfactoren:

  $\forall a \in \mathbb{Z}\ \exists p_i \in \mathbb{Z}, i = 1, \cdots, n$ met p_i priem, zodanig dat: $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$.
- Er bestaat een reëel getal waarvan het kwadraat gelijk is aan 2:
$$\exists a \in \mathbb{R} : a^2 = 2.$$
- Voor ieder geheel getal bestaat er een groter geheel getal:
$$\forall a \in \mathbb{Z}\ \exists b \in \mathbb{Z} : b > a.$$
- Er bestaat een geheel getal dat kleiner is dan ieder positief geheel getal:
$$\exists a \in \mathbb{Z}\ \forall b \in \mathbb{Z}_{>0} : a < b.$$

1.2.1 Plaats van de kwantoren

Kwantoren dienen altijd aan het begin van de uitspraak te staan waar ze betrekking op hebben! De (taalkundig geformuleerde) uitspraak *7 is groter dan b voor ieder negatief geheel getal b* dient wiskundig dus niet zó :

$$7 > b \ \forall b \in \mathbb{Z}_{<0}$$

geformuleerd te worden, maar zó:

$$\forall b \in \mathbb{Z}_{<0} : \ 7 > b.$$

1.2.2 Volgorde van de kwantoren

De volgorde van de kwantoren, die dus altijd aan het begin moeten staan van de uitspraak, is relevant. We illustreren dit aan de hand van een voorbeeld::

- Beschouw de uitspraak: $\forall x \in \mathbb{R} \ \exists y \in \mathbb{R} : x + y = 5$.

  Deze uitspraak is waar. Er wordt namelijk gezegd dat bij ieder reëel getal x een reëel getal y bestaat met de eigenschap $x + y = 5$. Dit is juist, want voor y kunnen we nemen $5 - x$. De waarde van y is dus *afhankelijk* van de waarde van x. Dit wordt in de uitspraak $\forall x \in \mathbb{R} \ \exists y \in \mathbb{R} : x + y = 5$ tot uitdrukking gebracht door het feit dat $\exists y$ genoteerd is *na* $\forall x$.

- Beschouw nu de uitspraak: $\exists y \in \mathbb{R} \ \forall x \in \mathbb{R} : x + y = 5$.

  Deze uitspraak is onwaar! Doordat de volgorde van de kwantoren is omgedraaid, wordt er nu gezegd dat er een y bestaat, voor de rest van de uitspraak vast, met de eigenschap dat voor iédere x geldt $x + y = 5$.

In een uitspraak met kwantoren geldt voor iedere '$\cdots \exists x \cdots$' dat de x, waarvan dus de existentie wordt beweerd, *afhankelijk* is van de variabelen die vóór $\exists x$ in de uitspraak voorkomen.

Verwisseling van een existentiële en universele kwantor levert niet altijd een negatie van de uitspraak op. Beschouw bijvoorbeeld: $\forall x \in \mathbb{R} \ \exists y \in \mathbb{R} : xy = 0$. Deze is waar, maar de uitspraak $\exists y \in \mathbb{R} \ \forall x \in \mathbb{R} : xy = 0$ is óók waar: kies maar $y := 0$.

Twee opeenvolgende universele kwantoren mogen wel onderling verwisseld worden. Daarom wordt in de praktijk vaak niet genoteerd $\forall x \in \mathbb{R} \ \forall y \in \mathbb{R} : \cdots$, maar $\forall x, y \in \mathbb{R} : \cdots$.

1.2.3 Negatie van een uitspraak met kwantoren

De negatie van een uitspraak met kwantoren kan eenvoudig herschreven worden als een nieuwe uitspraak met kwantoren door het negatiesymbool 'naar binnen te drukken' en onderweg iedere universele kwantor om te zetten in een existentiële en omgekeerd. We illustreren dit aan de hand van een voorbeeld:

Beschouw de uitspraak:

$$\exists y \in \mathbb{R} \ \forall x \in \mathbb{R} : x + y = 5.$$

We hebben hierboven gezien dat deze uitspraak onwaar is. De uitspraak:

$$\neg[\exists y \in \mathbb{R}\ \ \forall x \in \mathbb{R} : x + y = 5]$$

is dus waar. In deze uitspraak drukken we het $\neg$-symbool naar binnen en veranderen onderweg de kwantoren.

Eerste stap:

$$\forall y \in \mathbb{R}\ \ \neg[\forall x \in \mathbb{R} : x + y = 5].$$

Tweede stap:

$$\forall y \in \mathbb{R}\ \ \exists x \in \mathbb{R} : \neg[x + y = 5].$$

Herschreven in standaardnotatie:

$$\forall y \in \mathbb{R}\ \ \exists x \in \mathbb{R} : x + y \neq 5.$$

Deze laatste uitspraak is inderdaad waar (net als de daaraanvoorafgaande, want ze zijn onderling equivalent): bij ieder reëel getal y is een reëel getal x te vinden z.d.d. geldt $x + y \neq 5$. Kies maar $x := 4 - y$.

1.2.4 Continuïteit: een voorbeeld

Een fraaie exercitie in het gebruik van kwantoren en de negatie is het bestuderen van de definitie van continuïteit. Zij f een functie van $\mathbb{R}$ naar $\mathbb{R}$. De functie f heet *continu in* $x = a$, als geldt:

$$\forall \varepsilon \in \mathbb{R}_{>0}\ \ \exists \delta \in \mathbb{R}_{>0} : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

De ervaring leert dat deze definitie bij de meeste studenten niet meteen glashelder maakt wat continuïteit in $x = a$ inhoudt. De definitie wordt echter een stuk helderder door te onderzoeken wat *discontinuïteit* betekent:

De functie f heet *discontinu* in $x = a$, als hij niet continu is in $x = a$. Met andere woorden, als geldt:

$$\neg[\forall \varepsilon \in \mathbb{R}_{>0}\ \ \exists \delta \in \mathbb{R}_{>0} : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon].$$

Deze laatste uitspraak werken we uit door het $\neg$-symbool naar binnen te werken:

Stap 1:

$$\exists \varepsilon \in \mathbb{R}_{>0}\ \ \neg[\exists \delta \in \mathbb{R}_{>0} : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon].$$

Stap 2:

$$\exists \varepsilon \in \mathbb{R}_{>0}\ \ \forall \delta \in \mathbb{R}_{>0} : \neg[|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon].$$

Om stap 3 te kunnen formuleren merken we op dat $|x-a| < \delta \Rightarrow |f(x)-f(a)| < \varepsilon$ ook geschreven kan worden als $\forall x \in (a - \delta, a + \delta) : |f(x) - f(a)| < \varepsilon$.

Stap 3:

$$\exists \varepsilon \in \mathbb{R}_{>0}\ \ \forall \delta \in \mathbb{R}_{>0} : \neg[\forall x \in (a - \delta, a + \delta) : |f(x) - f(a)| < \varepsilon].$$

Stap 4:

$$\exists \varepsilon \in \mathbb{R}_{>0}\ \forall \delta \in \mathbb{R}_{>0}\ \exists x \in (a-\delta, a+\delta) : \neg[|f(x)-f(a)| < \varepsilon].$$

In standaard notatie:

$$\exists \varepsilon \in \mathbb{R}_{>0}\ \forall \delta \in \mathbb{R}_{>0}\ \exists x \in (a-\delta, a+\delta) : |f(x)-f(a)| \geq \varepsilon.$$

Discontinuïteit in $x = a$ betekent dus dat er een *vaste* positieve ε bestaat met de eigenschap dat *willekeurig dicht bij* a functiewaarden worden aangenomen die méér dan ε verschillen van de functiewaarde in a zelf. Met andere woorden: er vindt geen convergentie plaats.

2 Volledige inductie

De ervaring leert dat studenten bewijsvoering met volledige inductie maar al te vaak slordig, onzorgvuldig of zelfs fout uitvoeren. We proberen hier weer te geven wat de structuur is van een stelling en het bewijs ingeval dit laatste er één is met volledige inductie.

2.1 De structuur van de stelling

Als een stelling bewezen kan worden *met volledige inductie naar* n, dan is deze stelling van de volgende vorm.

Stelling 1 *Voor zekere* $n_0 \in \mathbb{Z}$ *geldt:*

$$\forall n \in \mathbb{Z}_{\geq n_0} : A(n)$$

□

Hierin is $A(n)$ een uitspraak die afhangt van n.

Voorbeelden van deze structuur:

- De stelling: $\forall n \in \mathbb{Z}_{>0} : \sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$ is te bewijzen met volledige inductie naar n. Hierin geldt $n_0 = 1$, en $A(n)$ is de uitspraak

$$\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$$

.

- De stelling: *Iedere vlakke graaf is vijfkleurbaar* is te bewijzen met volledige inductie naar het aantal knopen. Hierin geldt $n_0 = 1$, en $A(n)$ is de uitspraak *'Zij G een vlakke graaf met n knopen. Dan is G vijfkleurbaar'*.

2.2 De structuur van het bewijs

Om een stelling te bewijzen met volledige inductie is het absoluut noodzakelijk éérst de hierboven gegeven structuur aan te geven. Dit gebeurt door aan te geven *waarnaar* de volledige inductie wordt uitgevoerd en wat de kleinste waarde is van die parameter. Het bewijs bestaat dan uit drie onderdelen:

- Stap 1: Bewijs $A(n_0)$.
- Stap 2: Zij gegeven $N \in \mathbb{Z}_{>n_0}$. Bewijs de volgende *implicatie*:
$$\big[\forall n \in \mathbb{Z}, n_0 \leq n < N : A(n)\big] \Rightarrow \big[A(N)\big]$$
- Stap 3: Uit de combinatie van stap 1 en stap 2 volgt
$$\forall n \in \mathbb{Z}_{\geq n_0} : A(n).$$

□

Definitie 4 *In stap 2 heet het stuk*

$$\forall n \in \mathbb{Z}, n_0 \leq n < N : A(n)$$

de inductievooronderstelling*.*

2.3 In woorden

Een stelling die bewezen kan worden met volledige inductie is dus in wezen een verzameling stellingen of uitspraken die geïndiceerd wordt door de gehele getallen groter gelijk een zekere gehele n_0. Deze n_0 is dus de kleinste index waarvoor een uitspraak gedaan wordt. Daarna staan er dus eigenlijk oneindig aftelbaar veel uitspraken met indices n_0, $n_0 + 1$, enz..

Het bewijs zelf bestaat uit drie delen:

- Stap 1: Bewijs de 'eerste' stelling. Met andere woorden, bewijs de stelling met index n_0.
- Stap 2: Fixeer éérst een indexwaarde N groter dan n_0. Dit fixeren is zeer wezenlijk en wordt vaak vergeten! Stap 2 dient te beginnen met: Zij $N \in \mathbb{Z}_{>n_0}$ willekeurig gegeven en neem aan dat (en dit is nu de *inductievooronderstelling*) de stellingen voor index-waarden kleiner dan N waar zijn. Laat vervolgens zien dat dít de waarheid van de stelling met index N impliceert. Na de fixatie van een waarde $N > n_0$ is stap 2 dus niets anders dan het bewijzen van een *implicatie*: de inductievooronderstelling impliceert de stelling met index N.
- Stap 3: Door het combineren van stap 1 en stap 2 volgt de waarheid van alle stellingen. Immers, de eerste stelling met index n_0 is waar (stap 1). We passen stap 2 toe met $N = n_0 + 1$. De inductievooronderstelling is nu waar: alle stellingen (dat is nu alleen de stelling met index n_0) met lagere

index zijn waar. We concluderen dat de stelling met index $n_0 + 1$ dus ook waar is. Door opnieuw stap 2 toe te passen, maar nu met $N = n_0+2$, en op te merken dat opnieuw de inductievooronderstelling waar is, concluderen we dat de stelling met index $n_0 + 2$ ook waar is. Zij nu $k \in \mathbb{Z}_{>0}$, dan wordt de stelling met index $n_0 + k$ bewezen door de in stap 2 bewezen implicatie k keer uit te voeren. Conclusie: de stellingen zijn waar voor alle indexwaarden en dus is de originele stelling waar.

Opmerking 1 *Hierboven is voor de inductievooronderstelling gekozen voor de versie waarin de waarheid van álle stellingen met lagere index dan N wordt aangenomen. Vaak is het voldoende voor het bewijzen van de implicatie alleen de waarheid van de stelling met index $N-1$ aan te nemen. Dit staat stap 3 niet in de weg. Vandaar dat men vaak ook deze vorm van de inductievooronderstelling tegenkomt.*

2.4 Voorbeeld

We geven hier een voorbeeld van een bewijs met volledige inductie.

Stelling 2 *Iedere volledige graaf met 5 of meer knopen is niet vlak.*

$\square$

We bewijzen deze stelling met volledige inductie. Vóórdat we met stap 1 kunnen beginnen, moeten we éérst aangeven *waarnaar* we de volledige inductie gaan uitvoeren: we voeren de inductie uit naar het aantal knopen in de graaf en $n_0 = 5$.

- Stap 1: Voor $n = 5$ is de stelling waar. De volledige graaf K_5 met 5 knopen is niet vlak. Dit werken we hier niet verder uit.
- Stap 2: Zij $N \in \mathbb{Z}_{>5}$ willekeurig gegeven en neem aan dat iedere volledige graaf met minstens 5 maar minder dan N knopen niet vlak is. Beschouw de volledige graaf K_N. Aan te tonen: K_N is niet vlak. Stel K_N is wel vlak. Kies dan een vlakke representatie van K_N. Door in deze vlakke representatie een willekeurige knoop en de $N-1$ takken naar deze knoop te verwijderen krijgen we een vlakke representatie van K_{N-1}. Echter, er geldt zowel $N-1 \geq 5$ als ook $N-1 < N$, dus we mogen de inductievooronderstelling toepassen die ons meldt dat K_{N-1} geen vlakke representatie heeft. Tegenspraak. We concluderen dat K_N niet vlak is.
- Stap 3: Uit stap 1 en stap 2 volgt dat iedere volledige graaf met minstens 5 knopen niet vlak is.

Opmerking 2 *In bovenstaande hebben we gewerkt met een inductievooronderstelling die betrekking heeft op indices kleiner dan N om van daaruit de situatie met index N te bestuderen. Vaak formuleert men de inductievooronderstelling ook wel voor situaties t/m index N om vervolgens de situatie met index $N+1$ te bestuderen. Dit maakt natuurlijk niets uit. Het enige dat dan anders is, is dat bij stap 2 bij de fixatie van deze N niet geldt $N > n_0$, maar $N \geq n_0$.*

Opmerking 3 *De meestgemaakte fout naast gewoon zeer slordig de dingen formuleren is die waarin in stap 2 niet wordt uitgegaan van de situatie met index N om van daaruit terug te werken naar een situatie met kleinere index, maar van de situatie met index $N-1$ om van daaruit óp te werken naar een situatie met index N. Het enige dat de auteur van het bewijs met déze werkwijze bewijst, is dat hij weinig van volledige inductie begrijpt.*

3 De verzameling der reële getallen

In dit hoofdstuk zullen we een definitie geven van de reële getallen met behulp van de zogenaamde *Cauchy-rijtjes*. Rijtjes spelen in deze module een belangrijke rol en om onnodig ingewikkelde formuleringen te vermijden, introduceren we de volgende notatie.

- Met *een rij* (a) wordt bedoeld een rij $\{a_i\}_{i=0}^{\infty}$. Als er bijvoorbeeld wordt gesproken over een *rij* (a) *van rationale getallen*, wordt bedoeld dat voor alle i geldt: $a_i \in \mathbb{Q}$.
- Als (a) en (b) twee rijen zijn en $\lambda \in \mathbb{Q}$, dan wordt bedoeld met:
  - $(a+b)$ de rij $\{a_i+b_i\}_{i=0}^{\infty}$.
  - (ab) de rij $\{a_i b_i\}_{i=0}^{\infty}$.
  - (λa) de rij $\{\lambda a_i\}_{i=0}^{\infty}$.

3.1 Cauchy-rijtjes

Definitie 5 *Een rij (a) van rationale getallen heet een* Cauchy-rij *als geldt:*

$$\forall \varepsilon \in \mathbb{Q}_{>0} : \exists N \in \mathbb{Z}_{\geq 0} : \forall i,j > N : |a_i - a_j| < \varepsilon$$

Stelling 3 *Cauchy-rijtjes zijn begrensd.*

□

Bewijs
Zij (a) een Cauchy-rijtje. Kies nu een $\exists N \in \mathbb{Z}_{\geq 0}$ (we kiezen $\varepsilon = 1$) met de eigenschap:

$$\forall i,j > N : |a_i - a_j| < 1.$$

In het bijzonder geldt dan:

$$\forall i > N : |a_{N+1} - a_i| < 1.$$

Hieruit volgt onmiddellijk dat de verzameling $\{a_{N+1}, a_{N+2}, \cdots\}$ begrensd is:

$$\{a_{N+1}, a_{N+2}, \cdots\} \subset B(a_{N+1}, 1).$$

Hierin is $B(a_{N+1}, 1)$ de open bol rond a_{N+1} met straal 1:

$$B(a_{N+1}, 1) = \{x \in \mathbb{Q} | |x - a_{N+1}| < 1\}.$$

Uit het feit dat $\{a_{N+1}, a_{N+2}, \cdots\}$ op eindig veel getallen na gelijk is aan de hele rij, volgt dat de rij zelf ook begrensd is:

$$\exists M_1, M_2 \in \mathbb{Q} : \forall i \in \mathbb{Z}_{\geq 0} : M_1 < a_i < M_2$$

□

Stelling 4 *Zij (a) en (b) twee Cauchy-rijtjes. Dan is de som $(a+b)$ ook een Cauchy-rij.*

□

Bewijs
Zij (a) en (b) twee Cauchy-rijtjes en zij $\varepsilon \in \mathbb{Q}_{>0}$. Te bewijzen:

$$\exists N \in \mathbb{Z}_{\geq 0} : \forall i, j > N : |(a_i + b_i) - (a_j + b_j)| < \varepsilon$$

Uit het feit dat zowel (a) als (b) Cauchy zijn, volgt:

- $\exists M_1 \in \mathbb{Z}_{\geq 0} : \forall i, j > M_1 : |a_i - a_j| < \frac{\varepsilon}{2}$,
- $\exists M_2 \in \mathbb{Z}_{\geq 0} : \forall i, j > M_2 : |b_i - b_j| < \frac{\varepsilon}{2}$.

We kiezen $N = max\{M_1, M_2\}$. Er geldt:

$$\begin{aligned} \forall i, j > N : |(a_i + b_i) - (a_j + b_j)| &= |(a_i - a_j) + (b_i - b_j)| \\ &\leq |(a_i - a_j)| + |(b_i - b_j)| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon. \end{aligned}$$

□

Stelling 5 *Zij (a) en (b) twee Cauchy-rijtjes. Dan is het verschil $(a-b)$ ook een Cauchy-rij.*

□

Bewijs
Dit volgt onmiddelijk uit stelling 4 door op te merken dat de rij $(-b)$ ook Cauchy is.

□

Stelling 6 *Zij (a) en (b) twee Cauchy-rijtjes. Dan is het produkt $(a \cdot b)$ ook een Cauchy-rij.*

□

Bewijs
Zij (a) en (b) twee Cauchy-rijtjes en zij $\varepsilon \in \mathbb{Q}_{>0}$. Te bewijzen:

$$\exists N \in \mathbb{Z}_{\geq 0} : \forall i, j > N : |(a_i \cdot b_i) - (a_j \cdot b_j)| < \varepsilon.$$

Uit de begrensdheid van (a) en (b) (stelling 3) volgt:

$$\exists p \in \mathbb{Q}_{>0} : \forall i \geq 0 : |a_i| < p \wedge |b_i| < p.$$

Uit het feit dat zowel (a) als (b) Cauchy zijn, volgt:

- $\exists M_1 \in \mathbb{Z}_{\geq 0} : \forall i, j > M_1 : |a_i - a_j| < \frac{\varepsilon}{2 \cdot p}$,
- $\exists M_2 \in \mathbb{Z}_{\geq 0} : \forall i, j > M_2 : |b_i - b_j| < \frac{\varepsilon}{2 \cdot p}$.

We kiezen $N = max\{M_1, M_2\}$. Er geldt:

$$\begin{aligned}
\forall i, j > N : |(a_i \cdot b_i) - (a_j \cdot b_j)| &= |(a_i \cdot b_i - a_j \cdot b_i) + (a_j \cdot b_i - a_j \cdot b_j)| \\
&\leq |(a_i \cdot b_i - a_j \cdot b_i)| + |(a_j \cdot b_i - a_j \cdot b_j)| \\
&= |b_i| \cdot |a_i - a_j| + |a_j| \cdot |b_i - b_j| \\
&\leq p \cdot |a_i - a_j| + p \cdot |b_i - b_j| \\
&< p \cdot \frac{\varepsilon}{2 \cdot p} + p \cdot \frac{\varepsilon}{2 \cdot p} \\
&= \varepsilon.
\end{aligned}$$

□

Stelling 7 *Zij (a) een binnen $\mathbb{Q}$ convergerende rij rationale getallen. Dan is de rij (a) Cauchy.*

□

Bewijs
Zij $\varepsilon > 0$ en zij b de limiet van de rij (a). Kies $N \in \mathbb{Z}_{>0}$ zo dat:

$$\forall i > N : |a_i - b| < \frac{\varepsilon}{2}.$$

Dit is mogelijk doordat b de limiet van de rij (a) is. Dan geldt echter ook:

$$\begin{aligned}
\forall i, j > N : |a_i - a_j| &= |(a_i - b) + (b - a_j)| \\
&\leq |a_i - b| + |b - a_j| \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\
&= \varepsilon.
\end{aligned}$$

□

Bovenstaande stelling zegt dat convergerende rijen Cauchy zijn. Gevoelsmatig zou de Cauchy-eigenschap ook voldoende kunnen zijn voor convergentie. Immers, wat kan er gebeuren als een rij divergeert? Hij kan 'naar oneindig' wegschieten. De Cauchy-eigenschap verhindert dit: Cauchy-rijen zijn immers begrensd. Als een divergente rij niet 'naar oneindig' wegschiet, moet hij heen en weer blijven stuiteren zonder 'tot rust' te komen. Het is precies de Cauchy-eigenschap die dit heen en weer blijven stuiteren zonder 'tot rust te komen' verhindert. Het is *precies* dit aspect waarom in de definitie van Cauchy-rijen staat:

$$\forall i,j > N : |a_i - a_j| < \varepsilon$$

en niét:

$$\forall i > N : |a_i - a_{i+1}| < \varepsilon.$$

Een voorbeeld van een rij (a) die voldoet aan:

$$\forall \varepsilon > 0 : \exists N \in \mathbb{Z}_{>0} : \forall i > N : |a_i - a_{i+1}| < \varepsilon,$$

en die niet 'tot rust komt' is de volgende:

$$a_1 = 0$$

$$a_2 = \frac{1}{2}$$

$$\forall i > 2 : a_i = \begin{cases} a_{i-1} + \frac{1}{i} & \text{, als } a_{i-1} < 0 \\ a_{i-1} - \frac{1}{i} & \text{, als } a_{i-1} > 1 \\ a_{i-1} + \frac{1}{i} & \text{, als } 0 \le a_{i-1} \le 1 \wedge a_{i-1} > a_{i-2} \\ a_{i-1} - \frac{1}{i} & \text{, als } 0 \le a_{i-1} \le 1 \wedge a_{i-1} < a_{i-2} \end{cases}$$

Uit de divergentie van de reeks $\sum_{i=1}^{\infty} \frac{1}{i}$ volgt dat er oneindig veel rijelementen groter-gelijk 1 zijn en tevens oneindig veel rijelementen kleiner-gelijk 0. Deze rij komt dus niet 'tot rust'.

De volgende alternatieve definitie van Cauchy-rijen illustreert het 'tot rust komen' van Cauchy-rijen veel beter dan de klassieke definitie die hierboven gehanteerd is.

Definitie 6 *Een rij (a) van rationale getallen heet een* Cauchy-rij *als geldt:*

$$\forall \varepsilon \in \mathbb{Q}_{>0} : \exists N \in \mathbb{Z}_{\ge 0} : \forall i > N : a_i \in B(a_N, \varepsilon).$$

Hierin is $B(a_N, \varepsilon)$ de open bol *rond a_N met straal ε:*

$$B(a_N, \varepsilon) := \{x \in \mathbb{Q} : |a_N - x| < \varepsilon\}.$$

Het is een aardige oefening in de driehoeksongelijkheid na te gaan dat deze definitie inderdaad equivalent is met de klassieke.

Cauchy-rijen zijn dus rijen die zich convergerend gedragen (zeker in het licht van de alternatieve definitie), hetgeen leidt tot de vraag of Cauchy-rijen altijd convergent zijn. De volgende stelling geeft hier een negatief antwoord op.

Stelling 8 *Er bestaat een Cauchy-rij van rationale getallen die niet in $\mathbb{Q}$ convergeert.*

□

Bewijs
Het volstaat een voorbeeld te geven: definieer de rij (a) als volgt:

$$\forall i \in \mathbb{Z}_{>0} : a_i := \sum_{j=0}^{i} 10^{-j^2}.$$

De rij begint als volgt:

$$\begin{aligned} a_1 &= 1,1 \\ a_2 &= 1,1001 \\ a_3 &= 1,100100001 \end{aligned}$$

Ga zelf na dat het hier een Cauchyrij betreft. Het aantal nullen tussen de laatste twee énen in de decimale ontwikkeling van de partiële sommen neemt telkens met twee toe. Stel dat de limiet binnen $\mathbb{Q}$ bestaat. Dan bestaat er een geheel getal b met de volgende eigenschap:

$$\sum_{j=0}^{\infty} b10^{-j^2} \in \mathbb{Z}.$$

Dat dit onmogelijk is, is in te zien door op te merken dat vanaf een zeker punt in de reeks bepaalde decimalen van de partiële sommen niet meer veranderen. Stel namelijk dat b uit n cijfers bestaat. Kies dan een index N zodanig dat het aantal nullen tussen de laatste twee énen in de decimale ontwikkeling van a_N groter is dan n. Vanaf deze index N wordt de decimale ontwikkeling van a_i, $i > N$, afgesloten met de n cijfers van b met daarna enkel nullen.

□

De vooruit denkende lezer zou nu kunnen vermoeden dat de Cauchy-rijtjes per definitie reële getallen zullen zijn. Dat is bijna goed, maar er moet nog iets gebeuren. Een Cauchy-rijtje 'wijst' iets aan dat we een reëel getal willen noemen, maar twee verschillende Cauchy-rijtjes kunnen hetzelfde 'getal' aanwijzen. Waar we te maken hebben met niet-convergerende Cauchy-rijtjes is de terminologie 'aanwijzen' erg vaag en zeker wiskundig niet sterk gefundeerd, maar bij convergerende Cauchy-rijtjes wordt er gewoon de limiet mee bedoeld. In dat geval is goed in te zien dat twee verschillende Cauchy-rijtjes hetzelfde getal aan kunnen wijzen c.q. dezelfde limiet hebben. Beschouw bijvoorbeeld de twee Cauchy-rijen $\left\{-\frac{1}{i}\right\}_{i=1}^{\infty}$ en $\left\{\frac{1}{i}\right\}_{i=1}^{\infty}$. Ze zijn beslist verschillend, maar er geldt:

$$\lim_{i\to\infty}\left(-\frac{1}{i}\right) = 0 = \lim_{i\to\infty}\left(\frac{1}{i}\right).$$

We moeten aangeven wanneer we twee Cauchy-rijen equivalent beschouwen:

Definitie 7 *Zij* (a) *en* (b) *twee Cauchy-rijen. De rijen* (a) *en* (b) *heten* equivalent *als geldt:*

$$\forall \varepsilon \in \mathbb{Q}_{>0} : \exists N \in \mathbb{Z}_{\geq 0} \forall i > N : |a_i - b_i| < \varepsilon.$$

Notatie: $(a) \sim (b)$.

We lopen kort na dat deze relatie inderdaad een equivalentierelatie is (we nemen hiermee alvast een voorschotje op de theorie der equivalentierelaties verderop in dit dictaat):

- Reflexiviteit: Volgt uit het feit dat $\forall \varepsilon > 0 : |a_i - a_i| = 0 < \varepsilon$.
- Symmetrie: Volgt uit het feit dat $|a_i - b_i| = |b_i - a_i|$.
- Transitiviteit: Volgt uit de driehoeksongelijkheid.

Verdere uitwerking hiervan laten we aan de lezer over.

Door uit te delen naar deze equivalentierelatie krijgen we wat we willen:

Definitie 8 *Zij C de verzameling van alle Cauchy-rijtjes van rationale getallen en zij $\sim$ de relatie die hierboven gedefinieerd is. De verzameling $\mathbb{R}$ der reële getallen wordt gedefinieerd door:*

$$\mathbb{R} := C/\sim$$

Een manier waarop we informeel tegen deze definitie aan kunnen kijken is de volgende. Cauchy-rijtjes zijn op te vatten als *aanwijsstokjes* die soms iets aanwijzen dat in $\mathbb{Q}$ aanwezig is (de convergerende rijtjes) en soms iets aanwijzen dat *niet* in $\mathbb{Q}$ aanwezig is. Twee rijtjes wijzen hetzelfde aan precies dan als ze equivalent zijn. Door zulke rijtjes bij elkaar te nemen zijn de klassen van equivalente rijtjes te identificeren met hetgeen dat ze aanwijzen. Dit is nu precies wat er in de definitie van $\mathbb{R}$ gebeurt.

Cauchy-rijtjes worden door veel mensen, ook niet-wiskundigen, gebruikt zonder dat men zich er van bewust is. De decimale ontwikkeling van reële getallen is een voorbeeld van een Cauchy-rij. Door bijvoorbeeld van het getal π het begin van de decimale ontwikkeling te geven:

$$\pi = 3,141592653589\cdots,$$

geeft men eigenlijk het begin van een representant (a) van π aan:

$$\begin{aligned} a_0 &= 3 \\ a_1 &= 3,1 \\ a_2 &= 3,14 \\ a_3 &= 3,141 \\ a_4 &= 3,1415 \\ a_5 &= 3,14159 \end{aligned}$$

enzovoort. En er geldt:

$$\overline{(a)} = \pi.$$

In dit licht is goed in te zien dat geldt:

$$0,99999\cdots = 1,00000\cdots.$$

De twee bijbehorende Cauchy-rijtjes zijn namelijk equivalent (opgave voor de lezer) en dus zijn hun klassen gelijk.

3.2 Een ordening op $\mathbb{R}$

Op de verzameling der rationale getallen kennen we als standaard ordening de 'kleiner gelijk relatie', aangegeven met het symbool $\leq$. In deze paragraaf zullen we deze ordening op kompatibele wijze uitbreiden naar de reële getallen. Om deze laatste zin zinvol te laten zijn, identificeren we $\mathbb{Q}$ met een deelverzameling van $\mathbb{R}$ via de injectieve afbeelding $i : \mathbb{Q} \to \mathbb{R}$, gedefinieerd door:

$$i(x) := \overline{x}.$$

Hierin is $\overline{x}$ de klasse van de Cauchyrij met constante waarde x.

Om in te kunnen zien op welke wijze we zinvol een $\leq$-relatie op $\mathbb{R}$ kunnen definiëren, analyseren we de situatie waarin twee reële getallen *ongelijk* zijn aan elkaar.

Zij a en b twee reële getallen die *ongelijk* zijn aan elkaar:

$$a \neq b.$$

Laat $\{a_i\}$ resp. $\{b_i\}$ representanten zijn van a resp. b. Als de twee getallen *gelijk* zouden zijn, had dat betekend dat het volgende geldt:

$$\forall \varepsilon \in \mathbb{Q}_{>0} \exists N \in \mathbb{Z}_{\geq 0} \forall i > N : |a_i - b_i| < \varepsilon.$$

Echter, ze zijn niet gelijk aan elkaar, hetgeen betekent:

$$\neg[\forall \varepsilon \in \mathbb{Q}_{>0} \exists N \in \mathbb{Z}_{\geq 0} \forall i > N : |a_i - b_i| < \varepsilon].$$

Uitwerking hiervan levert:

$$\exists \varepsilon \in \mathbb{Q}_{>0} \forall N \in \mathbb{Z}_{\geq 0} \exists i > N : |a_i - b_i| \geq \varepsilon.$$

We kiezen zo'n ε en noemen deze ε_0. Er geldt dus:

$$\forall N \in \mathbb{Z}_{\geq 0} \exists i > N : |a_i - b_i| \geq \varepsilon_0.$$

Gegeven is dat de rijen $\{a_i\}$ en $\{b_i\}$ Cauchy zijn. Dit houdt in dat er indices N_a en N_b bestaan z.d.d.:

$$\forall i \geq N_a : |a_{N_a} - a_i| < \frac{\varepsilon_0}{10},$$

$$\forall i \geq N_b : |b_{N_b} - b_i| < \frac{\varepsilon_0}{10}.$$

Zij $M = max\{N_a, N_b\}$.

Er geldt:

$$\Big(a_M - \frac{\varepsilon_0}{10}, a_M + \frac{\varepsilon_0}{10}\Big) \cap \Big(b_M - \frac{\varepsilon_0}{10}, b_M + \frac{\varepsilon_0}{10}\Big) = \emptyset,$$

waarin dit intervallen in $\mathbb{Q}$ zijn. Stel namelijk dat dit niet het geval is. Kies dan een getal x in deze doorsnede en kies een index $i_0 > M$ waarvoor geldt:

$$|a_{i_0} - b_{i_0}| \geq \varepsilon_0.$$

Echter, vanaf M ligt de *gehele* staart van de rij $\{a_i\}$ in $(a_M - \frac{\varepsilon_0}{10}, a_M + \frac{\varepsilon_0}{10})$ en de *gehele* staart van de rij $\{b_i\}$ in $(b_M - \frac{\varepsilon_0}{10}, b_M + \frac{\varepsilon_0}{10})$. In het bijzonder, omdat $i_0 > M$, geldt dus:

$$a_{i_0} \in \left(a_M - \frac{\varepsilon_0}{10}, a_M + \frac{\varepsilon_0}{10}\right),$$

en ook:

$$b_{i_0} \in \left(b_M - \frac{\varepsilon_0}{10}, b_M + \frac{\varepsilon_0}{10}\right).$$

Door nu de driehoeksongelijkheid toe te passen op de drie getallen a_{i_0}, b_{i_0} en x vinden we tegenspraak:

$$\varepsilon_0 \leq |a_{i_0} - b_{i_0}| = |(a_{i_0} - x) + (x - b_{i_0})| \leq |a_{i_0} - x| + |x - b_{i_0}| < \frac{\varepsilon_0}{10} + \frac{\varepsilon_0}{10} = \frac{\varepsilon_0}{5} < \varepsilon_0,$$

waar uit volgt:

$$\varepsilon_0 < \varepsilon_0.$$

Conclusie:

$$\left(a_M - \frac{\varepsilon_0}{10}, a_M + \frac{\varepsilon_0}{10}\right) \cap \left(b_M - \frac{\varepsilon_0}{10}, b_M + \frac{\varepsilon_0}{10}\right) = \emptyset.$$

In het bijzonder geldt dus dat $a_M \neq b_M$ en zonder de algemeenheid te schaden mogen we aannemen dat $a_M < b_M$. Dit betekent dat het gehele interval $(a_M - \frac{\varepsilon_0}{10}, a_M + \frac{\varepsilon_0}{10})$ op de rationale getallenrechte $\mathbb{Q}$ links van het interval $(b_M - \frac{\varepsilon_0}{10}, b_M + \frac{\varepsilon_0}{10})$ ligt.

We vinden dus dat ingeval twee reële getallen a en b ongelijk zijn aan elkaar, uiteindelijk het staartstuk van een representant van het éne getal geheel vóór of ná het staartstuk van een representant van het andere getal ligt. Ga zelf na, dat deze relatieve positie onafhankelijk is van de gekozen representant. Afhankelijk van de relatieve positie noteren we dan $a < b$ of $a > b$. In de situatie hierboven geldt dus $a < b$.

Definitie 9 *Op de verzameling* $\mathbb{R}$ *der reële getallen definiëren we de* kleiner dan relatie *(notatie <) aan de hand van de observatie hierboven.*

Definitie 10 *Op de verzameling* $\mathbb{R}$ *der reële getallen definiëren we de* kleiner-gelijk *(notatie $\leq$) door: $a \leq b \Leftrightarrow [a < b \vee a = b]$.*

Hierboven gaan we een beetje kort door de bocht en zijn we niet helemaal volledig. Ga zelf aan de keukentafel na dat het volgende geldt:

- De standaard kleiner-dan-relatie op $\mathbb{Q}$ is compatibel met de kleiner-dan-relatie op $\mathbb{R}$.
- De kleiner-gelijk-relatie op $\mathbb{R}$ is *reflexief.*
- De kleiner-gelijk-relatie op $\mathbb{R}$ is *anti-symmetrisch.*
- De kleiner-gelijk-relatie op $\mathbb{R}$ is *transitief.*
- De kleiner-gelijk-relatie op $\mathbb{R}$ is *lineair*, dat wil zeggen dat *ieder* tweetal reële getallen te vergelijken is.

- Bij het definiëren van Cauchyrijtjes van reële getallen maakt het niet uit of ε in $\mathbb{Q}$ of $\mathbb{R}$ ligt.

Nu we een kleiner-dan-relatie op $\mathbb{R}$ hebben, kunnen we praten over positieve ε-en en absolute waarden en dús over reële Cauchy-rijen die als eigenschap hebben dat bij iedere positieve *reële* ε er een index bestaat zodanig dat enz. enz.. Dit zou kunnen betekenen, dat we het hele Cauchy-bouwwerk dat we hiervoor hebben opgericht op de fundering $\mathbb{Q}$ om tot een grotere verzameling te komen die de gaten opvult, ook weer op $\mathbb{R}$ kunnen bouwen. De volgende stelling zegt echter, dat dit niet kan.

Stelling 9 *Iedere Cauchy-rij in* $\mathbb{R}$ *convergeert. Men zegt ook wel, dat* $\mathbb{R}$ volledig *is.*

$\square$

Het bewijs van deze stelling volgt uit een zorgvuldige observatie van een reële Cauchy-rij. Het recept waarmee bij zo'n rij een limiet wordt gevonden is als volgt. Kies bij een Cauchy-rij bij ieder element een representant. Dit levert een rij representanten op die elk rationale Cauchy-rijen zijn. Een eerste kandidaat voor de representant van de limiet van deze rij reële getallen zou kunnen zijn de diagonaalrij die we hier aantreffen. Het is echter in het algemeen niet waar dat deze rij überhaupt Cauchy is. Geef zelf eens een tegenvoorbeeld hiervan. We laten het als een opgave voor de lezer zelf een representant van de limiet aan te wijzen.

3.3 Supremum en Infimum

Definitie 11 *Zij* $X \subset \mathbb{R}$ *een verzameling reële getallen. Een getal* $a \in \mathbb{R}$ *heet een* bovengrens van X*, als geldt:*

$$\forall x \in X : x \leq a.$$

Een analoge definitie geldt voor ondergrens*.*

Definitie 12 *Een verzameling* $X \subset \mathbb{R}$ *van reële getallen heet* naar boven (beneden) begrensd*, als deze een bovengrens (ondergrens) heeft.*

Merk op dat voor deze twee definities alleen gebruik wordt gemaakt van het feit dat we op de omhullende verzameling (in dit geval $\mathbb{R}$) een ordening hebben. In het bijzonder kunnen we dus ook binnen $\mathbb{Q}$ praten over onder- en bovengrenzen van deelverzamelingen.

Definitie 13 *Zij* X *een naar boven begrensde deelverzameling van* $\mathbb{Q}$ *of* $\mathbb{R}$*. Een bovengrens* $s \in \mathbb{Q}$ *(of* $\mathbb{R}$*) van* X *heet een* supremum*, als voor iedere bovengrens* a *van* X *geldt:* $s \leq a$*. Met andere woorden: een supremum is een kleinste bovengrens. Op analoge wijze wordt een* infimum *gedefinieerd als een grootste ondergrens.*

Merk op dat een begrensde verzameling ten hoogste één supremum kan hebben en ten hoogste één infimum. Bovendien geldt dat als X een supremum heeft en deze bovendien een element is van X, dat deze dan het maximum is van X, en omgekeerd. Eenzelfde opmerking geldt voor infimum/minimum.

Aan de hand van een aantal voorbeelden laten we zien dat verschillende situaties mogelijk zijn. We beschouwen de volgende verzamelingen binnen $\mathbb{Q}$:

- $X = [0, 1]$: Het infimum is 0, het supremum is 1 en X bevat beide. Dit zijn dus het minimum en maximum van X.
- $X = [0, 1)$: Het infimum is 0, het supremum is 1 en X bevat alleen zijn infimum.
- $X = (0, 1)$: Het infimum is 0, het supremum is 1 en X bevat geen van beide.
- $X = \{x \in \mathbb{Q} | x > 0 \wedge x^2 < 2\}$: Het infimum is 0 en X heeft geen supremum. We kijken immers binnen $\mathbb{Q}$!
- $X = \{2^i | i \in \mathbb{Z}\}$: Het infimum is 0 en X heeft geen supremum, omdat X niet naar boven begrensd is.

Als we niet binnen $\mathbb{Q}$ maar binnen $\mathbb{R}$ kijken, leveren deze voorbeelden het volgende op:

- $X = [0, 1]$: Het infimum is 0, het supremum is 1 en X bevat beide. Dit zijn dus het minimum en maximum van X.
- $X = [0, 1)$: Het infimum is 0, het supremum is 1 en X bevat alleen zijn infimum.
- $X = (0, 1)$: Het infimum is 0, het supremum is 1 en X bevat geen van beide.
- $X = \{x \in \mathbb{Q} | x > 0 \wedge x^2 < 2\}$: Het infimum is 0 en het supremum is $\sqrt{2}$.
- $X = \{2^i | i \in \mathbb{Z}\}$: Het infimum is 0 en X heeft geen supremum, omdat X niet naar boven begrensd is.

Deze voorbeelden doen het volgende vermoeden:

a) Waar een begrensde verzameling binnen $\mathbb{Q}$ reeds een supremum of infimum heeft (het doet er niet toe of deze bevat zijn in de verzameling of niet) blijven deze dezelfde als we binnen $\mathbb{R}$ gaan kijken.

b) Waar een naar boven begrensde verzameling binnen $\mathbb{Q}$ geen supremum heeft, heeft deze binnen $\mathbb{R}$ wel een supremum.

Het eerste vermoeden laten we liggen voor de keukentafel.

Het tweede vermoeden bevestigen we met de volgende fundamentele stelling:

Stelling 10 *Binnen $\mathbb{R}$ heeft iedere niet lege naar boven resp. beneden begrensde verzameling een supremum resp. infimum. Men zegt ook wel dat $\mathbb{R}$ de* supremumeigenschap *heeft.*

□

Het bewijs is dankzij de volledigheid van $\mathbb{R}$ verrassend simpel:

Zij X een niet lege naar boven begrensde deelverzameling van $\mathbb{R}$ zijn. Zij $x \in X$ en zij b een bovengrens van X. We definiëren twee rijen $\{x_i\}$ en $\{b_i\}$ als volgt:

- $x_1 := x$ en $b_i := b$.
- Voor $i \in \mathbb{Z}_{>1}$ definiëren we $\{x_i\}$ en $\{b_i\}$ recursief. Zij $i \in \mathbb{Z}_{>1}$ en neem aan dat x_{i-1} en b_{i-1} reeds gedefinieerd zijn. We beschouwen het gemiddelde:

$$m := \frac{x_{i-1} + b_{i-1}}{2}.$$

We definiëren:

$$(x_i, b_i) := \begin{cases} (x_{i-1}, m) & \text{, als } m \text{ een bovengrens is van } X, \\ (m, b_{i-1}) & \text{, als } m \text{ geen bovengrens is van } X. \end{cases}$$

Nu geldt dat de rijen $\{x_i\}$ en $\{b_i\}$ twee equivalente Cauchy-rijtjes zijn. Aangezien $\mathbb{R}$ volledig is, bestaat er dus (bij beide rijen dezelfde) limiet s van deze rijen. Er geldt:

- De limiet s is een bovengrens van X.
- Er bestaat geen kleinere bovengrens van X.

Het is een fraaie opgave voor de keukentafel deze twee feiten na te gaan.

Conclusie: deze limiet s is het supremum van X en dus heeft X een supremum, hetgeen te bewijzen was.

Op analoge wijze kan het bestaan van een infimum bewezen worden. Het is een fraaie opgave voor de keukentafel de existentie van infima af te leiden uit de universele existentie van suprema voor naar boven begrensde verzamelingen. Hint: bij een niet lege naar beneden begrensde verzameling is de verzameling der ondergrenzen een niet lege naar boven begrensde verzameling...

4 Grafentheorie

4.1 Definities

Definitie 14 *Een* graaf *G is een eindige en niet-lege verzameling punten,* knopen *genoemd, met tussen ieder tweetal (niet noodzakelijkerwijs verschillende) knopen* 0 *of meer (wel eindig veel) verbindingen, de* takken *genoemd. Een tak tussen een knoop en zichzelf wordt een* lus *genoemd.*

Opmerking 4 *Grafen kunnen met een rijkere structuur worden voorzien. Zo kunnen takken gericht zijn of van een waarde voorzien. In dit dictaat laten we dit soort grafen buiten beschouwing.*

Definitie 15 *Een* enkelvoudige graaf *is een graaf zonder lussen en met tussen ieder tweetal knopen ten hoogste 1 tak.*

Definitie 16 *Zij* $n \in \mathbb{Z}_{>0}$. *De* volledige graaf K_n *is de enkelvoudige graaf met* n *knopen waarbij ieder tweetal verschillende knopen verbonden is door een tak.*

Definitie 17 *Een* bipartiete graaf G *is een enkelvoudige graaf waarbij de verzameling knopen uitéén valt in twee niet-lege verzamelingen* A *en* B *zodanig dat iedere tak uit* G *een knoop uit* A *verbindt met een knoop uit* B. *Als iédere knoop uit* A *verbonden is met iédere knoop uit* B, *heet* G *de* volledige bipartiete graaf $K_{n,m}$. *Hierin is* n *het aantal knopen in* A *en* m *het aantal knopen in* B.

Grafentheorie is een gebied in de wiskunde dat goed toegankelijk is aan het begin van je wiskundestudie en waar je veel van kunt leren. Niet alleen vakinhoudelijk, maar ook wat betreft zaken als:

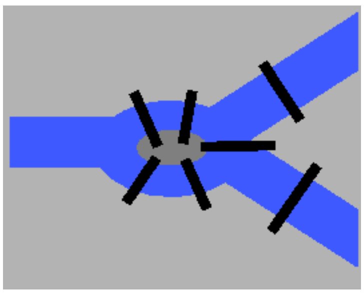
1. Standaard bewijstechnieken
2. Structuur van wiskundetheorie
3. Hoe wiskunde te studeren

We bestuderen drie klassieke problemen:

1. Het Konigsberger Bruggenprobleem van Euler (1736)
2. Het Gas-Water-Licht probleem
3. De Vijfkleurbaarheid van vlakke grafen

4.2 Het Konigsberger Bruggenprobleem

Door het stadje Königsberg stroomt de rivier De Pregel. In de rivier ligt een eilandje en bovendien splitst de rivier zich in Königsberg. Er zijn in totaal 7 bruggen die de verschillende delen van Königsberg met elkaar verbinden:



Het probleem waar de beroemde wiskundige Euler zich in 1736 mee bezig hield, was het volgende. Is het mogelijk een wandeling door Königsberg te maken waarbij iedere brug precies één keer wordt overgestoken? Het maakt niet uit waar je begint of waar je eindigt.

De oplossing van dit probleem wordt gegeven door de grafentheorie. Voordat we dit echter kunnen behandelen, hebben we eerst meer theorie nodig.

Definitie 18 *Zij G een graaf met knopen $v_1, v_2, \cdots, v_n$ en takken $t_1, t_2, \cdots, t_m$. Een* keten *is een rijtje takken $t_{i_1}, t_{i_2}, \cdots, t_{i_k}$ met de volgende eigenschappen:*

1. *De takken t_{i_j} zijn onderling verschillend*
2. *Eén van de eindpunten van t_{i_1} is tevens eindpunt van t_{i_2}. Het ándere eindpunt van t_{i_2} is tevens eindpunt van t_{i_3}. Enzovoort.*

Zij in de situatie van definitie 18 Q het niet-gebruikte eindpunt van t_{i_k} en P het niet-gebruikte beginpunt van t_{i_1}. Men zegt dan wel dat deze keten de knopen P en Q met elkaar verbindt.

Definitie 19 *Als in de situatie van definitie 18 het niet-gebruikte eindpunt van t_{i_k} gelijk is aan het niet-gebruikte beginpunt van t_{i_1}, heet de keten een* kring.

Definitie 20 *Een graaf heet* samenhangend *als tussen ieder tweetal knopen een keten bestaat.*

Definitie 21 *Een keten in een graaf G heet* eulers *als hij alle takken van G bevat.*

Definitie 22 *Een samenhangende graaf heet* eulers *als hij een eulerse kring bevat.*

Definitie 23 *De* graad *van een knoop in een graaf is het aantal takken waar deze knoop begin-/eindpunt van is, waarbij een lus met multipliciteit 2 wordt geteld.*

Stelling 11 *Zij G een samenhangende graaf. Dan geldt: G is eulers d.e.s.d.a. (dan en slechts dan als) iedere knoop heeft even graad.*

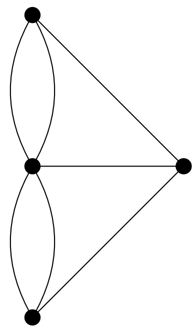
□

Een kleine variatie op deze stelling is de volgende.

Stelling 12 *Zij G een samenhangende graaf. Dan geldt: G heeft een eulerse keten d.e.s.d.a. óf alle knopen hebben even graad óf er zijn precies twéé knopen met oneven graad.*

□

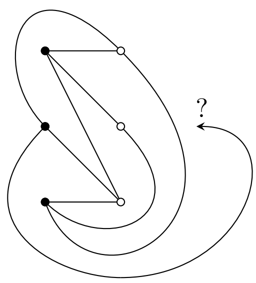
Nu kunnen we het bruggenprobleem oplossen. Door goed te kijken, zien we dat het bruggenprobleem zich laat reduceren tot de vraag of deze graaf:



een eulerketen heeft. Stelling 12 geeft ontkennend antwoord op deze vraag. Er zijn 4 knopen met oneven graad, dus deze graaf bevat geen eulerketen.

4.3 Het Gas-Water-Licht probleem

Het *Het Gas-Water-Licht probleem* is een bekend puzzeltje onder kinderen. Zij gegeven drie huisjes en drie nutsbedrijven voor gas, water en licht. Is het mogelijk ieder huisje met ieder nutsbedrijf te verbinden op zó'n manier dat geen enkele leiding, van boven af gezien, een andere leiding kruist/snijdt? Hoe je het ook probeert, het lukt je niet:



Dat het tekenen telkens niet lukt te hanteren als bewijs voor het feit dat het onmogelijk is, zou getuigen van stevige arrogantie en in de meeste gevallen van zelfoverschatting. Ook hier wordt de oplossing gegeven door grafentheorie.

Definitie 24 *Zij G een graaf. G heet* planair *of* vlak *als hij zó in het platte vlak getekend kan worden dat de takken geen contact met elkaar maken buiten de knopen. Een tekening van G die aan deze voorwaarde voldoet heet een* vlakke representatie *van G.*

Euler heeft een formule voor veelvlakken bewezen die het volgende analogon heeft voor vlakke grafen.

Stelling 13 *Zij G een vlakke samenhangende graaf met n knopen en m takken. Een vlakke representatie van G verdeelt het vlak in r gebieden. Merk hierbij op dat op dit punt de waarde van r in principe afhangt van de gekozen vlakke representatie. Dan geldt:*

$$n - m + r = 2$$

In het bijzonder betekent dit dat de waarde van r niét afhangt van de gekozen vlakke representatie.

□

Om deze stelling te kunnen bewijzen, hebben we de volgende stelling nodig:

Stelling 14 *Zij G een samenhangende graaf zonder kring. Als G meer dan 1 knoop bevat, bevat G een knoop met graad 1.*

□

Bewijs
Zij G een samenhangende graaf met n knopen met $n \geq 2$. Kies een knoop P. De graad van P kan niet 0 zijn, want dan zou de graaf niet samenhangend zijn. Als de graad van P gelijk is aan 1, zijn we klaar. Stel de graad van P is groter dan 1. Dan 'wandelen' we over één van de takken die in P uitkomen naar een volgende knoop. Deze volgende knoop heeft graad 1 of een hogere graad. Als deze knoop graad 1 heeft, zijn we klaar: de graaf bevat dan klaarblijkelijk een knoop van graad 1. Is de graad van deze knoop groter dan 1, dan kiezen we een willekeurige tak die op deze knoop uitkomt (niet de tak waar we net over zijn binnengekomen) en wandelen naar een volgende knoop. Dit proces herhalen we. Merk op dat iedere nieuw bereikte knoop niet eerder bereikt kan zijn, daar de graaf geen kring bevat. Dit in combinatie met het feit dat er slechts eindig veel knopen zijn, brengt met zich mee dat dit proces noodzakelijkerwijs stopt. De enige manier waarop dit mogelijk is, is dat we in een knoop aankomen met graad 1. Conclusie: iedere samenhangende graaf zonder kring bevat een knoop van graad 1.

□

We kunnen nu de stelling van Euler bewijzen. We doen dit met volledige inductie naar het aantal takken.

Stap 1: Zij G een vlakke samenhangende graaf met 0 takken. In dat geval bestaat G uit slechts één knoop. Een vlakke representatie is niets anders dan een stip op het vlak. Dan geldt dus:

$$n - m + r = 1 - 0 + 1 = 2.$$

Dit bewijst de stelling voor alle samenhangende vlakke grafen met 0 takken.

Stap 2: Zij $M \in \mathbb{Z}_{>0}$ en stel dat de stelling geldt voor alle vlakke grafen met minder dan M takken. Zij G een vlakke graaf met M takken. Kies een vlakke representatie van G. Zij n het aantal knopen van G en r het aantal gebieden bij de gekozen vlakke representatie. Te bewijzen:

$$n - M + r = 2$$

Er zijn twee situaties mogelijk:

1. G bevat een kring: kies in dat geval een kring en maak een nieuwe graaf $\widetilde{G}$ door in deze kring een tak te verwijderen. Als vlakke representatie van $\widetilde{G}$ kiezen we die van G met daarin deze tak verwijderd. Het aantal knopen in $\widetilde{G}$ is $\widetilde{n}$, het aantal takken $\widetilde{m}$ en het aantal gebieden van de vlakke representatie is $\widetilde{r}$. Er geldt:

$$\widetilde{n} = n$$

$$\widetilde{m} = M - 1$$

$$\widetilde{r} = r - 1$$

   Dit laatste geldt doordat verwijdering van een tak in een kring in een vlakke representatie een binnengebied laat versmelten met een gebied buiten de kring, waardoor het aantal gebieden met één afneemt. Op dit punt is het dus van belang dat de vlakke representatie van $\widetilde{G}$ gebaseerd is op die van G! De graaf $\widetilde{G}$ is een vlakke en nog steeds samenhangende (waarom?) graaf met minder dan M takken. Per inductievooronderstelling geldt dus:

$$\widetilde{n} - \widetilde{m} + \widetilde{r} = 2.$$

   Er geldt echter ook:

$$\widetilde{n} - \widetilde{m} + \widetilde{r} = n - (M - 1) + (r - 1) = n - M + r$$

   Conclusie:

$$n - m + r = 2$$

2. G bevat geen kring. In dat geval bevat G een knoop van graad 1. Net als in het geval dat er wel een kring bestaat, maken we een nieuwe graaf door deze knoop en de tak naar deze knoop te verwijderen. We laten het aan de lezer over dit onderdeel van het bewijs af te maken.

Conclusie: $n - m + r = 2$.

Stap 3: De combinatie van stap 1 en stap 2 levert dat de stelling geldt voor alle vlakke samenhangende grafen.

□

De stelling van Euler levert de oplossing voor het gas, water en licht probleem. Het probleem komt neer op de vraag of de volledige bipartiete graaf $K_{3,3}$ vlak is. Het antwoord wordt gegeven door de volgende stelling:

Stelling 15 *De volledige bipartite graaf $K_{3,3}$ is niet vlak.*

□

Bewijs
Uit het ongerijmde: Stel $K_{3,3}$ is vlak. Dan is de stelling van Euler van toepassing. Voor $K_{3,3}$ geldt dat $n = 6$ en $m = 9$ en dus:

$$6 - 9 + r = 2$$

waar uit volgt:

$$r = 5$$

Aangezien ieder gebied begrensd wordt door minstens 4 takken (waarom eigenlijk?) tellen we, door bij ieder gebied het aantal begrenzende takken te tellen, minstens $4 \times 5 = 20$ takken. Bij deze telling is iedere tak echter mogelijk dubbel geteld. Dit betekent dat er dus minstens $\frac{20}{2} = 10$ takken zijn, hetgeen in tegenspraak is met $m = 9$. Conclusie: $K_{3,3}$ is niet vlak.

□

4.4 De Vijfkleurbaarheid van vlakke grafen

Definitie 25 *Zij G een graaf. Een* n-kleuring *van G is een afbeelding*[1] *van de verzameling knopen naar de verzameling $\{1, 2, \cdots, n\}$ z.d.d. ieder tweetal verbonden knopen twee verschillende beelden heeft.*

Als een graaf G n knopen heeft, is er altijd een n-kleuring mogelijk. Geef iedere knoop immers een ander beeld (een andere kleur). Wat is echter bij een graaf het minimale aantal kleuren dat gebruikt kan worden? In het algemeen is dit een lastige vraag. De volgende stelling is in 1976 met de hulp van veel computerwerk bewezen:

Stelling 16 *Iedere vlakke graaf is 4-kleurbaar.*

□

Het bewijs van deze stelling is te lastig voor dit college. Wat niet te lastig is, is de iets zwakkere versie:

Stelling 17 *Iedere vlakke graaf is 5-kleurbaar.*

□

Voor het bewijs van deze stelling hebben we eerst nog wat lemma's en een andere stelling nodig.

Lemma 1 *De volledige graaf K_5 is niet vlak.*

Bewijs
Uit het ongerijmde: Stel K_5 is vlak. Dan is de stelling van Euler van toepassing. De volledige graaf K_5 heeft 5 knopen en 10 takken en dus geldt:

$$n - m + r = 5 - 10 + r = 2.$$

Hieruit volgt $r = 7$. Daar K_5 enkelvoudig is, wordt ieder gebied in een vlakke representatie begrensd door minstens 3 takken. Zo tellen we minstens $3 \times 7 = 21$ takken, waarbij iedere tak mogelijk 2 keer (maar niet meer) geteld wordt. Hieruit volgt dat er dus minstens 11 takken moeten zijn, hetgeen in strijd is met het feit dat er 10 zijn. Conclusie: K_5 is niet vlak.

[1] Dit begrip *afbeelding* wordt elders in dit college correct gedefinieerd. Voor dit moment kan je het beschouwen als een soort functie.

□

Lemma 2 *Zij G een enkelvoudige samenhangende vlakke graaf met n knopen, m takken ($m \geq 2$) en r gebieden. (De waarde van r is onafhankelijk van de vlakke representatie!) Dan geldt:*

$$r \leq \frac{2}{3}m$$

en tevens:

$$m \leq 3n - 6$$

Bewijs
Zij G als in de stelling. Het eerste deel verlangt geen samenhang en is als volgt in te zien. Daar G enkelvoudig is, wordt ieder gebied begrensd door minstens 3 takken. Door per gebied 3 takken te tellen en hierbij rekening houden dat elke tak mogelijk 2 keer geteld is, vinden we een ondergrens voor het aantal takken:

$$m \geq \frac{3r}{2},$$

hetgeen zich direkt laat herschrijven tot

$$r \leq \frac{2}{3}m.$$

Het tweede deel volgt door de ongelijkheid $r \leq \frac{2}{3}m$ in te vullen in de gelijkheid van Euler. De graaf G is vlak en samenhangend, zodat geldt:

$$n - m + r = 2,$$

en dus ook:

$$r = 2 - n + m.$$

Substitutie van $r \leq \frac{2}{3}m$ hierin levert op:

$$2 - n + m \leq \frac{2}{3}m.$$

Dit laat zich onmiddelijk herschrijven tot:

$$m \leq 3n - 6.$$

□

Lemma 3 *Zij G een graaf met n knopen en m takken en zij $k \in \mathbb{N}$ z.d.d. iedere knoop minstens graad k heeft. Dan geldt:*

$$m \geq \frac{1}{2}kn$$

Bewijs
Per knoop geldt dat er minstens k takken in uitkomen. Dat betekent dat er minstens kn uiteinden van takken zijn. Daar iedere tak twee uiteinden heeft, zijn er dus minstens $\frac{1}{2}kn$ takken. Met andere woorden:

$$m \geq \frac{1}{2}kn.$$

□

Stelling 18 *Iedere enkelvoudige vlakke graaf heeft een knoop met graad* ≤ 5.

□

Bewijs
Uit het ongerijmde: Stel G is een enkelvoudige vlakke graaf met de eigenschap dat de minimale graad van een knoop gelijk is aan 6. Zonder beperking der algemeenheid mag worden aangenomen dat G samenhangend is. De getallen n, m en r zijn zoals gebruikelijk. Daar G enkelvoudige en vlak is, geldt:

$$m \leq 3n - 6 \wedge m \geq \frac{1}{2}6n = 3n.$$

Hieruit volgt direkt:

$$3n \leq 3n - 6,$$

en dus:

$$0 \leq -6.$$

Dit laatste is ongegerijmd. Conclusie: iedere enkelvoudige vlakke graaf heeft een knoop met graad ≤ 5.

□

Nu hebben we genoeg gereedschap om de vijfkleurbaarheidsstelling voor vlakke grafen te bewijzen.

We bewijzen de stelling met volledige inductie naar het aantal knopen.

Stap 1: Dat de stelling correct is voor alle grafen met één knoop, is juist.

Stap 2: Zij $N \in \mathbb{Z}_{>1}$ en neem aan dat de stelling correct is voor alle vlakke grafen met minder dan N knopen. Zij G een vlakke graaf met N knopen.

We mogen aannemen dat G samenhangend is. Immers, als G dat niet is, bestaat G uit twee of meer samenhangscomponenten die elk minder dan N knopen bevatten en die elk vlak zijn. Door de inductievooronderstelling toe te passen, vinden we dan meteen dat deze componenten en dus ook G zelf vijfkleurbaar zijn/is. Daarnaast mogen we ook aannemen dat G enkelvoudig is, daar het bij kleurbaarheid er alleen maar om gaat of twee knopen verbonden zijn of niet. Bovendien spelen lussen bij kleurbaarheid helemaal geen rol.

De graaf G is vlak en bevat dus een knoop P met graad hoogstens 5. Kies een vlakke representatie van G. We maken een nieuwe graaf $\tilde{G}$ door uit G de knoop P en alle daarmee verbonden takken te verwijderen. Als vlakke representatie van $\tilde{G}$ kiezen we die van G met daaruit P en de contact makende takken te verwijderen. De graaf $\tilde{G}$ is vlak en bevat minder dan N knopen. Door de inductievooronderstelling toe te passen vinden we dat $\tilde{G}$ vijfkleurbaar is. Kies een vijf-kleuring van $\tilde{G}$ en laat d de graad van P in G zijn. Er zijn nu drie verschillende situaties mogelijk:

- $d < 5$: De kleuring van $\tilde{G}$ levert nu meteen een vijf-kleuring van G op.
- $d = 5$ en de vijf buren van P zijn in $\tilde{G}$ met minder dan vijf verschillende kleuren gekleurd. Ook nu levert de kleuring van $\tilde{G}$ meteen een vijf-kleuring van G op.
- $d = 5$ en de vijf buren van P zijn in $\tilde{G}$ met exact vijf verschillende kleuren gekleurd. Het lijkt er op dat we nu een probleem hebben, maar het niet vlak zijn van K_5 redt het bewijs. Van de vijf buren van P zijn er minstens twee niet met elkaar verbonden, omdat K_5 niet vlak is. Kies er twee en noem deze Q_1 en Q_2. Via de locatie van de twee verwijderde verbindende takken met P zijn Q_1 en Q_2 aan elkaar te lijmen zonder de rest van $\tilde{G}$ te veranderen. We verkrijgen zo een nieuwe graaf $\tilde{\tilde{G}}$ met $N - 2$ knopen waarin Q_1 en Q_2 als het ware met elkaar geïdentificeerd zijn. Ook deze graaf is dankzij de inductievooronderstelling te kleuren met ten hoogste vijf kleuren. Voorzie deze graaf met zo'n kleuring. Door de versmolten knopen Q_1 en Q_2 weer los te maken, levert dit ons een vijfkleuring op van $\tilde{G}$ waarin de vijf buren van P met hoogstens 4 kleuren gekleurd zijn. Deze kleuring van $\tilde{G}$ levert de gewenste kleuring van G op.

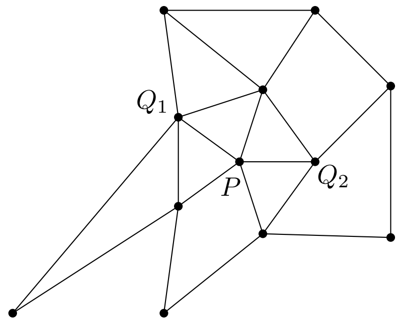
Conclusie: G is vijfkleurbaar.

Stap 3: Uit stap 1 en 2 volgt dat iedere vlakke graaf vijfkleurbaar is, hetgeen bewezen moest worden.

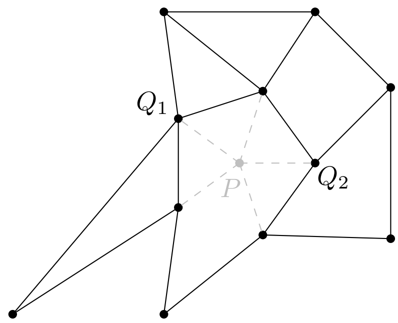
□

4.5 Visualisatie van het laatste deel van het bewijs

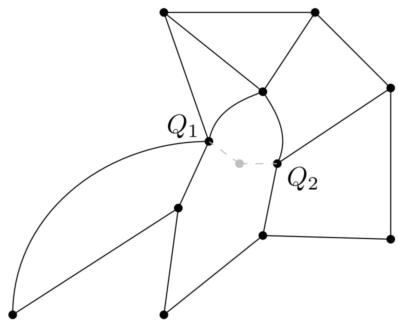
We gaan uit van een graaf G met een knoop P van graad 5. In dit voorbeeld bestaan ook knopen met lagere graad dan 5, maar het zou het plaatje onnodig ingewikkeld maken als we een voorbeeld zouden forceren waarin de minimale graad precies 5 is. We visualiseren de constructie uit het laatste deel van het bewijs van de 5-kleurbaarheid.



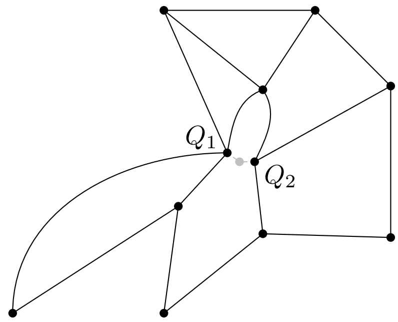
Figuur 1: De voorbeeldgraaf.



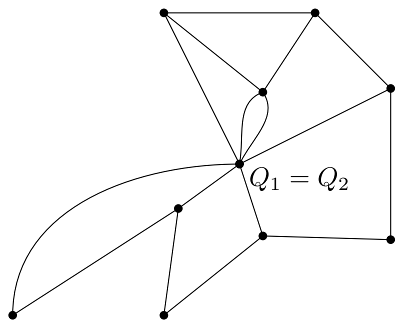
Figuur 2: De knoop van graad 5 wordt verwijderd.



Figuur 3: Twee buurknopen Q_1 en Q_2 die in G niet verbonden waren, worden over de oude takken naar P naar elkaar toegeschoven. De takken die nog steeds aansluiten op Q_1 of Q_2 worden mee naar binnen getrokken.



Figuur 4: De knopen Q_1 en Q_2 worden naar elkaar toegedrukt.

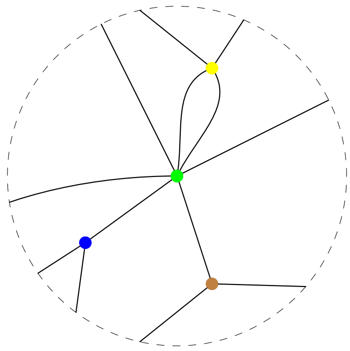


Figuur 5: Tot ze uiteindelijk 'versmelten' op de oude plek van P.

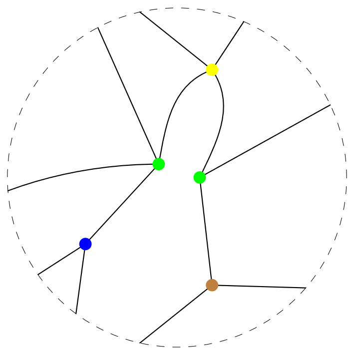
De graaf in 5 is volgens de inductievooronderstelling 5-kleurbaar en we voorzien hem van een 5-kleuring met de kleuren:

- Blauw: •
- Rood: •
- Geel: •
- Groen: •
- Bruin: •

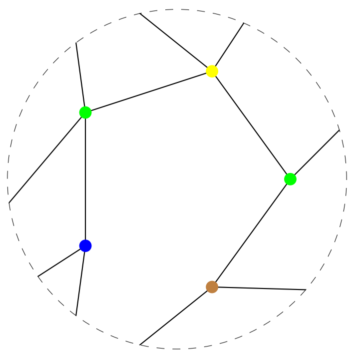
Vanaf nu focussen we ons geheel op het centrale deel van de constructie, namelijk de situatie rondom de twee samengesmolten knopen en de overige 3 oude buren van P:



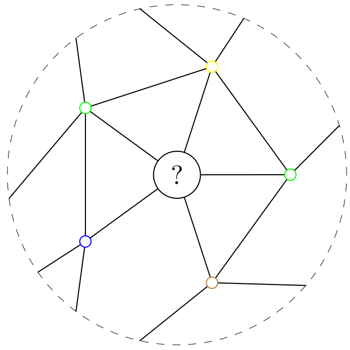
Figuur 6: De centrale plek 'where it all happens'.



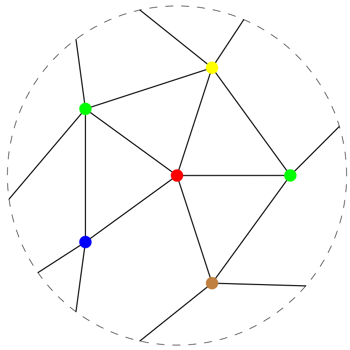
Figuur 7: De samengesmolten punten worden weer losgeknipt.



Figuur 8: Ze worden weer op hun oude plaats teruggezet.



Figuur 9: We zetten P met de 5 takken terug en gaan op zoek naar een kleur.



Figuur 10: Per constructie hebben we nog een kleur in de aanbieding: rood.

5 De verzameling der complexe getallen

In de wiskunde kennen we de volgende getallenverzamelingen die via de inclusierelatie geordend zijn.

- $\mathbb{N}$: De niet-negatieve gehelen of de positieve gehelen. Of het getal 0 er bij hoort, varieert van boek tot boek. In de praktijk is het verstandig het symbool $\mathbb{N}$ te vermijden en te praten over $\mathbb{Z}_{>0}$ of $\mathbb{Z}_{\geq 0}$.
- $\mathbb{Z}$: De gehelen. Deze verzameling heeft een rijkere structuur dan $\mathbb{N}$ (het is een ring, zie later het college Algebra). In het bijzonder is in $\mathbb{Z}$ iedere vergelijking van de vorm $x + a = b$, met $a, b \in \mathbb{N}$, oplosbaar. Sterker nog: iéder geheel getal is de oplossing van zo'n vergelijking.
- $\mathbb{Q}$: De breuken. Deze verzameling heeft weer een rijkere structuur dan $\mathbb{Z}$ (het is een lichaam, zie wederom later het college Algebra). In het bijzonder is in $\mathbb{Q}$ iedere vergelijking van de vorm $ax+b = c$, met $a, b, c \in \mathbb{Z}$ en $a \neq 0$, oplosbaar. Sterker nog: iédere breuk is de oplossing van zo'n vergelijking.

- $\mathbb{R}$: De reëele getallen. Waar de uitbreidingen van $\mathbb{N}$ naar $\mathbb{Z}$ naar $\mathbb{Q}$ nogal eenvoudig te beschrijven waren, is de uitbreiding van $\mathbb{Q}$ naar $\mathbb{R}$ veel ingewikkelder. Dit hebben we gezien bij de definitie van $\mathbb{R}$ met behulp van Cauchyrijtjes. De winst van deze uitbreiding zit hem voornamelijk in de volledigheid van $\mathbb{R}$ en de supremumeigenschap. De algebraïsche kwaliteit van de uitbreiding ten opzichte van $\mathbb{Q}$ is matig. Lineaire vergelijkingen over $\mathbb{R}$ zijn altijd oplosbaar (als de coëfficiënt van de variabele niet 0 is, natuurlijk), dus algebraïsche winst in $\mathbb{R}$ als uitbreiding van $\mathbb{Q}$ moeten we zoeken in oplosbaarheid van hogeregraads vergelijkingen. Hier vinden we dat vele wél, maar vele ook niét oplosbaar zijn. Bijvoorbeeld: $x^2 = 5$ is in $\mathbb{R}$ oplosbaar, maar $x^2 = -1$ is dat niet.

In deze module zullen we de 'laatste' uitbreiding in dit rijtje behandelen: die van de complexe getallen $\mathbb{C}$. Let wel, het adjectief *laatste* hoort enkel en alleen bij *in dit rijtje*! De *algebra* leert ons dat er wat getalachtige structuren betreft, 'iets' meer onder de zon is dan het rijtje $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$.

5.1 De strategie

Er zijn vele manieren om tot een definitie van de complexe getallen te komen. Hier volgen we een strategie die vergelijkbaar is met de wijze waarop we de reële getallen met behulp van Cauchyrijtjes hebben gedefinieerd:

1. We beschouwen een specifieke verzameling X.
2. Op X definiëren we een optelling en vermenigvuldiging.
3. We laten (deels) zien dat deze twee bewerkingen de eigenschappen hebben die we er van verwachten.
4. We laten zien dat $\mathbb{R}$ op te vatten is als deelverzameling van deze X (die onderwijl $\mathbb{C}$ is gaan heten), en wel zó dat de optelling en vermenigvuldiging op $\mathbb{R}$ overeenkomt met die op $\mathbb{C}$.
5. We behandelen enkele fraaie eigenschappen van $\mathbb{C}$ (meer verklappen we hier nog niet).

5.2 Aan de slag!

We beschouwen de verzameling $\mathbb{R}^2$ (dit is de verzameling X van hierboven). Op $\mathbb{R}^2$ definiëren we een optelling (som) en een vermenigvuldiging (produkt) als volgt:

Definitie 26 (Som) *Laat (a, b) en (c, d) twee elementen van $\mathbb{R}^2$ zijn. De* som *$(a, b) + (c, d)$ wordt gedefinieerd door:*

$$(a, b) + (c, d) := (a + c, b + d).$$

Definitie 27 (Produkt) *Laat (a, b) en (c, d) twee elementen van $\mathbb{R}^2$ zijn. Het* produkt *$(a, b) \cdot (c, d)$ wordt gedefinieerd door:*

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Nu we $\mathbb{R}^2$ hebben voorzien van een optel- en vermenigvuldigingsstructuur, zullen we het beestje maar meteen zijn naampje geven:

Definitie 28 (De verzameling der complexe getallen) *Het tripel* $(\mathbb{R}^2, +, \cdot)$ *heet de verzameling der complexe getallen. Notatie:* $\mathbb{C}$. *De elementen van* $\mathbb{C}$ *noemen we* complexe getallen. *Complexe getallen op de* y*-as, ongelijk aan de oorsprong, noemen we* zuiver imaginair *en die op de* x*-as noemen we* reëel.

We zullen later zien waarom deze naamgeving zo gekozen is.

Zoals we voor reële getallen zeer vaak het symbool x gebruiken als variabele of onbekende, zo is het gebruikelijk voor complexe variabelen of onbekenden het symbool z te gebruiken. Daarnaast geldt bij afspraak (die we nu dus formuleren), dat de vermenigvuldiging 'voorrang' heeft op de optelling. Dat wil zeggen, met $z_1 + z_2 \cdot z_3$ wordt $z_1 + (z_2 \cdot z_3)$ bedoeld en niet $(z_1 + z_2) \cdot z_3$. Dit is in overeenstemming met de voorrangsregels voor optellen en vermenigvuldigen die in $\mathbb{R}$ gelden.

Merk op dat we op dit moment in principe twee verschillende soorten *reële getallen* hebben: complexe getallen op de x-as en elementen van $\mathbb{R}$. Dit wordt afgevangen door de volgende afspraak. Via de injectieve afbeelding:

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{C} \\ x & \to & (x, 0) \end{array}$$

zullen we $\mathbb{R}$ beschouwen als een deelverzameling van $\mathbb{C}$. We hebben nu wel mogelijk een probleem. Een hoofdrol in dit hele verhaal vormen de optelling en de vermenigvuldiging. Doordat we $\mathbb{R}$ nu beschouwen als een deelverzameling van $\mathbb{C}$ hebben we op $\mathbb{R}$ nu in principe twee verschillende optellingen en twee verschillende vermenigvuldigingen. We zullen verifiëren dat dit gelukkig niet het geval is. Voor deze verificatie, en ook alleen voor deze verificatie, zullen we de symbolen labelen met $\mathbb{R}$ en $\mathbb{C}$ als index om aan te geven wélke optelling of vermenigvuldiging we bedoelen.

Verificatie dat de 'oude' optelling en vermenigvuldiging op $\mathbb{R}$ overeenkomt met die op $\mathbb{C}$ beperkt tot de reële x-as via de hierboven gedefinieerde 'identificatie-afbeelding' f:

Optelling: Zij $a, b \in \mathbb{R} \subset \mathbb{C}$. We moeten laten zien dat geldt: $f(a +_{\mathbb{R}} b) = f(a) +_{\mathbb{C}} f(b)$. We vinden dit door uitschrijven:

$$f(a +_{\mathbb{R}} b) := (a +_{\mathbb{R}} b, 0) =: (a, 0) +_{\mathbb{C}} (b, 0) =: f(a) +_{\mathbb{C}} f(b).$$

Vermenigvuldiging: Zij $a, b \in \mathbb{R} \subset \mathbb{C}$. We moeten laten zien dat geldt: $f(a \cdot_{\mathbb{R}} b) = f(a) \cdot_{\mathbb{C}} f(b)$. We vinden dit door uitschrijven, maar deze keer beginnen we aan de andere kant:

$$f(a) \cdot_{\mathbb{C}} f(b) := (a, 0) \cdot_{\mathbb{C}} (b, 0) := (a \cdot_{\mathbb{R}} b -_{\mathbb{R}} 0 \cdot_{\mathbb{R}} 0, a \cdot_{\mathbb{R}} 0 +_{\mathbb{R}} 0 \cdot_{\mathbb{R}} b) =$$

$$(ab, 0) =: f(ab) = f(a \cdot_{\mathbb{R}} b).$$

Om meteen over te kunnen gaan op de standaard schrijfwijze van complexe getallen maken we de volgende afspraken:

- Complexe getallen $(a, 0)$ op de x-as noteren we als a en niet als $f(a)$. Dit strookt met de afspraak dat we complexe getallen op de x-as *reëel* noemen.
- Vanaf nu zullen we de afbeelding f niet meer noemen. Deze afbeelding was nodig om $\mathbb{R}$ te kunnen beschouwen als een deelverzameling van $\mathbb{C}$ en bovenstaande verficatie uit te kunnen schrijven.
- Het complexe getal $(0, 1)$ noteren we als i.
- Het symbool $\cdot$ voor de vermenigvuldiging van complexe getallen wordt vaak weggelaten.

De belangrijkste afspraak noemen we even apart: Vanaf nu zullen we de notatie (a, b) voor een complex getal niet meer gebruiken. In plaats van (a, b) schrijven we $a + bi$. Let wel, de *afspraak* betreft het niet meer gebruiken van de notatie (a, b) en *niet* de '$a + bi$'. De expressie '$a + bi$' heeft namelijk betekenis, en wel die van (a, b):

$$a+bi = (a, 0)+(b, 0)\cdot(0, 1) = (a, 0)+(b\cdot 0-0\cdot 1, b\cdot 1+0\cdot 0) = (a, 0)+(0, b) = (a, b).$$

Wie het leuk vindt, kan nu alvast het kwadraat van i uitrekenen. De uitwerking in dit dictaat laten we even rusten tot we een beter meetkundig zicht hebben op de vermenigvuldiging van complexe getallen.

5.2.1 Pas op de plaats

Hierboven is gedefinieerd het rekenkundige systeem der complexe getallen als uitbreiding van de reële getallen. Het is belangrijk nu eerst precies op een rijtje te zetten wat we wél en wat we (nog) niét weten/kunnen. De terminologie en symbolen ($+$ en $\cdot$) die we bij $\mathbb{C}$ gebruiken is namelijk nogal suggestief. Om precies te kunnen doen wat we hier moeten doen, moeten we vage kreten als *rekenkundige systemen* vermijden. Daarom geven we hier de definitie waar het bij $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ om gaat:

Definitie 29 (Lichaam) *Zij K een verzameling met twee binaire operatoren $+$ en $\cdot$. Het vijftal $(K, +, \cdot, 0, 1)$, met $0 \in K$ en $1 \in K$, heet een* lichaam *als geldt:*

1. $\forall a, b, c \in K : a + (b + c) = (a + b) + c$ *en* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. *Met andere woorden: de optelling en vermenigvuldiging zijn associatief.*
2. $\forall a, b \in K : a + b = b + a$ *en* $a \cdot b = b \cdot a$. *Met andere woorden: de optelling en vermenigvuldiging zijn commutatief.*
3. $\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c$. *Met andere woorden: de vermenigvuldiging is distributief ten opzichte van de optelling.*
4. $\forall x \in K : x + 0 = 0 + x = x$. *Dit element* 0 *heet het* neutrale element voor de optelling.
5. $\forall x \in K : \exists y \in K : x + y = y + x = 0$. *Dit element y wordt genoteerd als $-x$ en heet de* additieve inverse van x *of* tegengestelde van x. *Dus:* $\forall x \in K : x + (-x) = (-x) + x = 0$.

6. $\forall x \in K : 1 \cdot x = x \cdot 1 = x$. *Dit element* 1 *heet het* neutrale element voor de vermenigvuldiging.

7. $\forall x \in K$ *met* $x \neq 0 : \exists y \in K : x \cdot y = y \cdot x = 1$. *Dit element* y *heet de* multiplicatieve inverse van x *en wordt genoteerd als* x^{-1}. *Dus:* $\forall x \in K : x \cdot x^{-1} = x^{-1} \cdot x = 1$.

8. $0 \neq 1$.

Lichamen en andere algebraïsche structuren als *groepen*, *ringen* worden in de *algebra* bestudeerd. Het is voor de lezer misschien wel een aardige opgave de volgende punten te verifiëren:

- Het 0-element in een lichaam is uniek. Dat wil zeggen, in een lichaam is er maar één element dat neutraal is t.o.v. de optelling.
- Het 1-element in een lichaam is uniek. Dat wil zeggen, in een lichaam is er maar één element dat neutraal is t.o.v. de vermenigvuldiging.
- De laatste voorwaarde ($0 \neq 1$) is een wezenlijke en volgt niet uit de voorgaande.

De twee meest bekende voorbeelden van lichamen zijn $\mathbb{Q}$ en $\mathbb{R}$. Omdat geldt $\mathbb{Q} \subset \mathbb{R}$ en de optelling en vermenigvuldiging van $\mathbb{Q}$ compatibel is met die van $\mathbb{R}$, heet $\mathbb{R}$ een *lichaamsuitbreiding* van $\mathbb{Q}$.

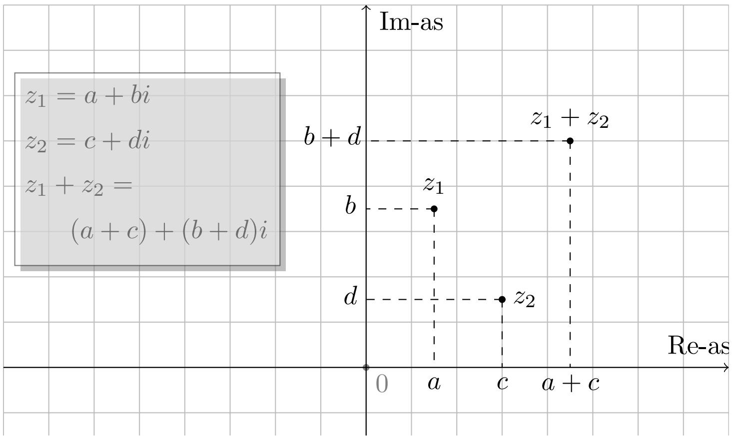
Hoe zit het nu met $\mathbb{C}$? We weten het volgende:

- Op $\mathbb{C}$ is een optelling en een vermenigvuldiging gedefinieerd.
- Er geldt $\mathbb{R} \subset \mathbb{C}$.
- De optelling en vermenigvuldiging op $\mathbb{R}$ is compatibel met die van $\mathbb{C}$.
- De verzameling $\mathbb{R}$ (met $+$ en $\cdot$) is een lichaam.

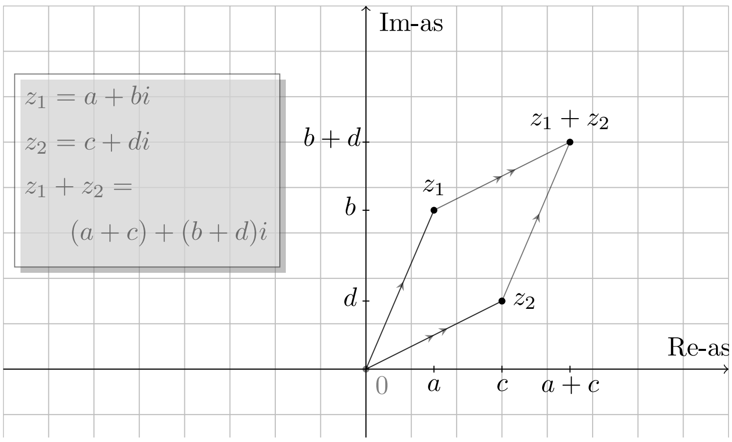
Wat we echter nog *niet* weten, is of $\mathbb{C}$ (met de gedefinieerde optelling en vermenigvuldiging) een lichaam is! Met andere woorden: we weten nog niet of $\mathbb{C}$ een lichaamsuitbreiding van $\mathbb{R}$ is. Om deze vraag te kunnen beantwoorden beschouwen we de optelling en en in het bijzonder de vermenigvuldiging op $\mathbb{C}$ eerst eens wat nader.

5.2.2 De optelling nader beschouwd

De optelling op $\mathbb{R}^2$ is waarschijnlijk een bekende operatie. Het is in wezen niets anders dan de optelling waarbij we de elementen van $\mathbb{R}^2$ beschouwen als vectoren. De volgende twee figuren maken dit visueel.



Figuur 11: Het optellen van complexe getallen m.b.v. reëel en imaginair deel.



Figuur 12: Het optellen van complexe getallen 'als vectoren'.

We zouden nu al enkele punten in de definitie van een lichaam kunnen controleren, maar om alles in één keer te kunnen doen, beschouwen we eerst de vermenigvuldiging.

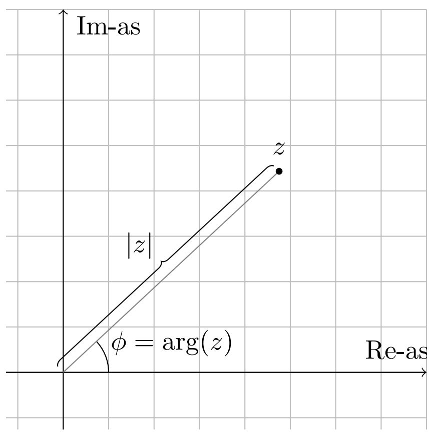
5.2.3 De vermenigvuldiging nader beschouwd

De vermenigvuldiging van complexe getallen oogt op het eerste gezicht misschien wat vreemd, maar als we de vermenigvuldiging in termen van poolcoördinaten beschrijven, wordt het een stuk helderder. Eerst hebben we echter een paar begrippen nodig.

Definitie 30 *Zij* $z \in \mathbb{C} \backslash \{0\}$. *Dan bestaan er* $r \in \mathbb{R}_{>0}$ *en* $\phi \in [0, 2\pi\rangle$ *zodanig dat* $z = r\cos(\phi) + ir\sin(\phi)$. *Hierin heet* r *de* modulus *en* ϕ *het* argument *van* z. *Notatie:*

- $|z|$ *is de modulus van* z,
- $\arg(z)$ *is het argument van* z.

De modulus $|z|$ *wordt ook wel de* absolute waarde *van* z *genoemd.*



Figuur 13: Argument en modulus van een complex getal

Merk op dat de modulus en het argument van een complex getal z uniek zijn. De modulus is immers de afstand in $\mathbb{R}^2$ van z tot de oorsprong en het argument de hoek die de vector z maakt met het positieve deel van de x-as. Door de hoek in $[0, 2\pi\rangle$ te nemen, is ook deze uniek. Voor complexe getallen ongelijk aan nul zijn modulus en argument niets anders dan de poolcoördinaten van deze getallen opgevat als punten in $\mathbb{R}^2$.

Als we de vermenigvuldiging op $\mathbb{C}$ in poolcoördinaten uitschrijven, zien we wat deze bewerking meetkundig inhoudt:

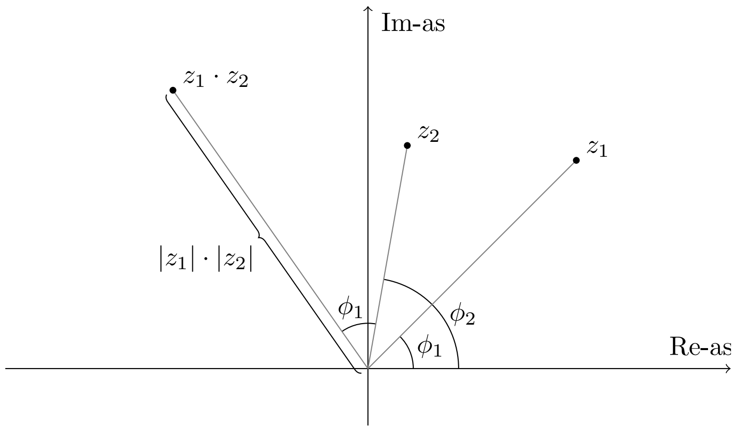
Zij $z_1 = r_1\cos(\phi_1) + ir_1\sin(\phi_1)$ en $z_2 = r_2\cos(\phi_2) + ir_2\sin(\phi_2)$ twee complexe getallen ongelijk aan nul. Dan geldt voor het produkt:

$$
\begin{aligned}
z_1 \cdot z_2 &= (r_1\cos(\phi_1) + ir_1\sin(\phi_1)) \cdot (r_2\cos(\phi_2) + ir_2\sin(\phi_2)) \\
&= (r_1\cos(\phi_1), r_1\sin(\phi_1)) \cdot (r_2\cos(\phi_2), r_2\sin(\phi_2)) \\
&= (r_1\cos(\phi_1)r_2\cos(\phi_2) - r_1\sin(\phi_1)r_2\sin(\phi_2), \\
&\quad\; r_1\cos(\phi_1)r_2\sin(\phi_2) + r_1\sin(\phi_1)r_2\cos(\phi_2)) \\
&= (r_1r_2\cos(\phi_1 + \phi_2), r_1r_2\sin(\phi_1 + \phi_2))
\end{aligned}
$$

We vinden dus:

- $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$,
- $\arg(z_1 \cdot z_2) = \arg(z_1) + \arg(z_2)$.

Met andere woorden: het vermenigvuldigen van complexe getallen (ongelijk aan nul) komt neer op het optellen van argumenten en vermenigvuldigen van moduli:



Figuur 14: Het produkt van twee complexe getallen

Een fraai feit vinden we, als we het kwadraat van i uitrekenen. De modulus van i is 1 en het argument is $\frac{1}{2}\pi$, dus de modulus van i^2 is ook 1 en het argument is π. Oftewel:

$$i^2 = -1,$$

en natuurlijk ook:

$$(-i)^2 = -1.$$

5.2.4 $\mathbb{C}$ is inderdaad een lichaam

We hebben nu genoeg inzicht in handen om te verifiëren dat $\mathbb{C}$ inderdaad een lichaam is. Een aantal onderdelen had al meteen na de definitie van $\mathbb{C}$ gecontroleerd kunnen worden, maar het is wel zo netjes alle verificaties in één keer te doen.

Associativiteit: Dit kan gecontroleerd worden door saai uitschrijven van de definities, hetgeen we graag aan de lezer overlaten. Mooier zijn de volgende twee argumenten. De optelling is dezelfde als die in $\mathbb{R}^2$ opgevat als vectorruimte en deze optelling is associatief, dus ook die van $\mathbb{C}$. Vermenigvuldiging is voor getallen ongelijk aan 0 niets anders dan een combinatie van twee onderling onafhankelijk en elk associatieve bewerkingen: optellen van argumenten en vermenigvuldigen van moduli. Zodra het getal 0 als één de factoren voorkomt, is het eindantwoord van de vermenigvuldiging altijd 0, dus dat geval gooit geen roet in het eten. Derhalve is de vermenigvuldiging op $\mathbb{C}$ associatief.

Commutativiteit: Dit kan wederom gecontroleerd worden door saai uitschrijven van de definities, hetgeen we ook deze keer graag aan de lezer overlaten. Mooier zijn de volgende twee argumenten. De optelling is nog steeds dezelfde als die in $\mathbb{R}^2$ opgevat als vectorruimte en deze optelling is commutatief, dus ook die van $\mathbb{C}$. Vermenigvuldiging is voor getallen ongelijk aan 0 niets anders dan een combinatie van twee onderling onafhankelijk en elk commutatieve bewerkingen: optellen van argumenten en vermenigvuldigen van moduli. Zodra het getal 0 als één de factoren voorkomt, is het eindantwoord van de vermenigvuldiging altijd 0, dus dat geval gooit geen roet in het eten. Derhalve is de vermenigvuldiging op $\mathbb{C}$ commutatief.

Distributiviteit: Ook hier is saai uitschrijven een opgave voor de lezer, maar ook hier is er een mooier argument. Vermenigvuldiging met een complex getal $z = a+bi$ met $a, b \in \mathbb{R}$ is voor $\mathbb{C}$ beschouwd als de reële vectorruimte $\mathbb{R}^2$ een lineaire afbeelding van $\mathbb{R}^2$ naar zichzelf. De matrix M van deze afbeelding ten opzichte van de standaardbasis van $\mathbb{R}^2$ is:

$$M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Lineaire afbeeldingen zijn per definitie 'distributief' over de optelling. Derhalve is in $\mathbb{C}$ de vermenigvuldiging distributief over de optelling.

Het nulelement: Deze is snel gevonden: het getal $0 \in \mathbb{C}$ is neutraal ten opzichte van de optelling.

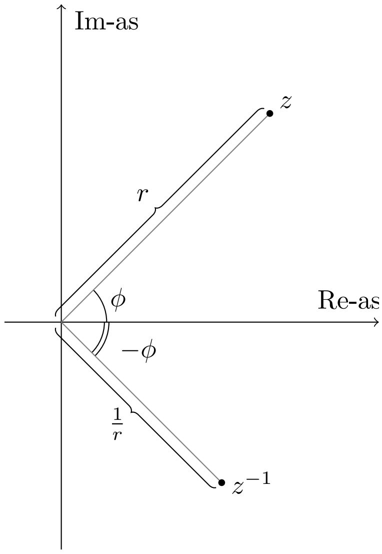
De additieve inverse: Ook deze is snel gevonden: de additieve inverse van $z = a + bi$ is $(-a) + (-b)i$, hetgeen genoteerd wordt als $-a - bi$.

Het eenheidselement : Het getal 1 is het eenheidselement.

De multiplicatieve inverse: Hier wordt het interessant. Het zou mogelijk zijn het volgende te doen. Zij $z = a + bi \in \mathbb{C}^*$. Dan is $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$ de inverse van z. Bewijs: reken maar na. Dit zou natuurlijk de existentie van de multiplicatieve inverse bewijzen, maar enig inzicht levert dit niet op. Veel fraaier is het de situatie te beschouwen in termen van poolcoördinaten. Zij $z = a+bi \in \mathbb{C}^*$ met modulus r en argument ϕ, dan is de multiplicatieve inverse van z het getal met modulus $\frac{1}{r}$ en argument $-\phi(+2\pi)$. De 2π moet bij $-\phi$ worden opgeteld als ϕ ongelijk is aan 0 om het argument weer in $[0, 2\pi\rangle$ te krijgen. Het produkt van z met deze geclaimde inverse heeft dan als argument $\phi + (-\phi + 2\pi) \equiv 0 \mod 2\pi$ en modulus $r \cdot \frac{1}{r} = 1$. Dit produkt is dus 1, hetgeen bewijst dat we inderdaad de inverse van z te pakken hebben.

Nul en één zijn verschillend: Dit volgt uit het feit dat in $\mathbb{R}^2$ geldt:

$$(0, 0) \neq (1, 0).$$



Figuur 15: De inverse van een complex getal

Gevolg: $\mathbb{C}$ is een lichaam en dus een lichaamsuitbreiding van $\mathbb{R}$.

Dat $\mathbb{C}$ een lichaam is, heeft onder andere tot gevolg dat je een heleboel vertrouwde rekenregels ook voor complexe getallen gebruikt mogen worden. We geven een voorbeeld:

Zij $a, b \in \mathbb{C}$. Dan geldt: $(a+b)^2 = a^2+2ab+b^2$. Zo op het oog lijkt dit misschien flauw, maar we hebben wel degelijk een aantal lichaamseigenschappen nodig om dit te kunnen bewijzen:

$$\begin{aligned}
(a+b)^2 &= (a+b)\cdot(a+b) \\
&= (a+b)\cdot a + (a+b)\cdot b && (1)\\
&= a\cdot(a+b) + b\cdot(a+b) && (2)\\
&= a\cdot a + a\cdot b + b\cdot a + b\cdot b && (3)\\
&= a^2 + ab + ba + b^2 \\
&= a^2 + ab + ab + b^2 && (4)\\
&= a^2 + ab(1+1) + b^2 && (5)\\
&= a^2 + ab\cdot 2 + b^2 && (6)\\
&= a^2 + 2ab + b^2
\end{aligned}$$

Toelichting:

(1) Distributiviteit,

(2) commutativiteit van de vermenigvuldiging,

(3) distributiviteit,

(4) commutativiteit van de vermenigvuldiging,

(5) distributiviteit,

(6) gebruiken dat in $\mathbb{C}$ geldt $1 + 1 = 2$.

Over $\mathbb{C}$ is erg veel te zeggen, maar wij zullen ons hier beperken tot drie bijzondere zaken:

- De Stelling van De Moivre
- De functie $z \to e^z$
- De Hoofdstelling van de algebra

5.3 De Stelling van De Moivre

Kwadrateren van een complex getal z komt meetkundig neer op het verdubbelen van het argument en het kwadraat nemen van de modulus. Een interessante situatie is die waarin de modulus van het z gelijk is aan 1. Met andere woorden, als geldt:

$$z = \cos(\phi) + i\sin(\phi).$$

Hierin is ϕ het argument van z.

We kunnen nu op twee manieren z^2 uitrekenen: gebruik maken van de meetkundige interpretatie of het uitwerken van $(\cos(\phi) + i\sin(\phi))^2$.

Via de meetkundige interpretatie vinden we onmiddellijk:

$$z^2 = \cos(2\phi) + i\sin(2\phi).$$

Via haakjes wegwerken[2] vinden we:

$$\begin{aligned} z^2 &= (\cos(\phi) + i\sin(\phi))^2 \\ &= (\cos(\phi))^2 + 2\cos(\phi)i\sin(\phi) + (i\sin(\phi))^2 \\ &= (\cos^2(\phi) - \sin^2(\phi)) + i(2\cos(\phi)\sin(\phi)) \end{aligned}$$

Deze twee resultaten combinerend vinden we dus:

$$\cos(2\phi) + i\sin(2\phi) = (\cos^2(\phi) - \sin^2(\phi)) + i(2\cos(\phi)\sin(\phi)).$$

Aangezien twee complexe getallen aan elkaar gelijk zijn d.e.s.d.a. als zowel het reële én het imaginaire deel gelijk zijn, vinden we twee bekende goniometrieformules:

$$\begin{aligned} \cos(2\phi) &= \cos^2(\phi) - \sin^2(\phi), \\ \sin(2\phi) &= 2\cos(\phi)\sin(\phi). \end{aligned}$$

[2] Dit gaat als 'vanouds', omdat $\mathbb{C}$ een lichaam is!

Dit lijkt een beetje flauw, want deze formules waren al eerder gebruikt. Bovenstaande bevestigt deze formules dus alleen maar. Echt nieuwe resultaten kunnen echter worden gevonden door derde en hogere machten uit te werken. Zo kunnen alle formules gevonden worden voor $\cos(n\phi)$ en $\sin(n\phi)$, met $n \in \mathbb{Z}_{>1}$. Dit fraaie resultaat wordt samengevat in de stelling van De Moivre:

Stelling 19 (De Moivre) *Zij $n \in \mathbb{Z}_{>0}$. Dan geldt:*

$$\forall \phi \in \mathbb{R} : (\cos(\phi) + i\sin(\phi))^n = \cos(n\phi) + i\sin(n\phi)$$

$\square$

Met behulp van de stelling van De Moivre kunnen voor iedere $n \in \mathbb{Z}_{>0}$ zowel $\sin(n\phi)$ als ook $\cos(n\phi)$ uitgedrukt worden in $\cos(\phi)$ en $\sin(\phi)$.

5.4 De functie $z \to e^z$

Complexe getallen spelen onder andere een belangrijke rol in de analyse; met name in de zogenaamde *complexe analyse*. In de *reële analyse* speelt de functie

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \to & e^x \end{array}$$

een belangrijke rol.

Het is hier nu de wens op $\mathbb{C}$ een complexe functie 'e^z' te definiëren die beperkt tot $\mathbb{R}$ de functie e^x is en die verder vergelijkbare eigenschappen heeft als de reële functie $x \to e^x$:

- $\forall n \in \mathbb{Z}_{>0} : \forall z \in \mathbb{C} : (e^z)^n = e^{nz}$
- $\forall z_1, z_2 \in \mathbb{C} : e^{z_1} \cdot e^{z_2} = e^{z_1+z_2}$

In beginsel is het helemaal niet duidelijk dat zo'n functie bestaat! Áls hij bestaat, geldt in ieder geval het volgende. Zij $z = a + bi$, met $a, b \in \mathbb{R}$. Dan moet gelden:

$$e^z = e^{a+bi} = e^a \cdot e^{bi}.$$

De eerste factor e^a ligt vast daar a een reëel getal is. We moeten dus op zoek naar een zinvolle definitie voor e^{bi}. Deze wordt ons op een zilveren dienblad aangereikt door de voorgaande beschouwingen rondom de stelling van De Moivre:

Definitie 31 *De* exponentiële functie e^z *op $\mathbb{C}$ wordt gedefinieerd door:*

$$e^{a+bi} := e^a(\cos(b) + i\sin(b)).$$

We controleren of deze inderdaad aan de eisen voldoet:

- De beperking van e^z tot $\mathbb{R}$ is inderdaad de 'oude' e^x:

$$e^{a+0\cdot i} = e^a(\cos(0) + i\sin(0)) = e^a(1 + i \cdot 0) = e^a$$

- Zij $n \in \mathbb{Z}_{>0}$. Dan geldt:

$$\begin{aligned}
(e^z)^n &= \left(e^{a+bi}\right)^n \\
&= (e^a(\cos(b) + i\sin(b)))^n \\
&= e^{na}(\cos(b) + i\sin(b))^n \\
&= e^{na}(\cos(nb) + i\sin(nb)) \text{ [De Moivre]} \\
&= e^{na+inb} \\
&= e^{nz}
\end{aligned}$$

- Zij $z_1, z_2 \in \mathbb{C}$. Dan geldt:

$$\begin{aligned}
e^{z_1} \cdot e^{z_2} &= e^{a_1+ib_1} \cdot e^{a_2+ib_2} \\
&= e^{a_1}(\cos(b_1) + i\sin(b_1)) \cdot e^{a_2}(\cos(b_2) + i\sin(b_2)) \\
&= e^{a_1+a_2}(\cos(b_1) + i\sin(b_1)) \cdot (\cos(b_2) + i\sin(b_2)) \\
&= e^{a_1+a_2}(\cos(b_1 + b_2) + i\sin(b_1 + b_2)) \\
&= e^{(a_1+a_2)+i(b_1+b_2)} \\
&= e^{(a_1+ib_1)+(a_2+ib_2)} \\
&= e^{z_1+z_2}
\end{aligned}$$

Klaar!

5.5 De Hoofdstelling van de algebra

Bij elke uitbreiding/vergroting van getallenverzamelingen die we tot nu toe gezien hebben, werden meer polynomiale vergelijkingen oplosbaar. Bijvoorbeeld:

- $\mathbb{N}$: '$x + 3 = 7$' is oplosbaar, maar '$x + 5 = 3$' niet.
- $\mathbb{Z}$: '$x + 5 = 3$' is oplosbaar, maar '$3x + 5 = 3$' niet.
- $\mathbb{Q}$: '$3x + 5 = 3$' is oplosbaar, maar '$x^2 = 3$' niet.
- $\mathbb{R}$: '$x^2 = 3$' is oplosbaar, maar '$x^2 + 1 = 0$' niet.
- $\mathbb{C}$: '$x^2 + 1 = 0$' is oplosbaar (met i en $-i$ als oplossingen), maar $\cdots$ niet?

De vraag is nu of er op de stippeltje nog een polynomiale vergelijking moet staan. De hoofdstelling uit de algebra geeft hier antwoord op.

Stelling 20 *Zij $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ een polynoom in z over $\mathbb{C}$ van positieve graad n. Dat wil zeggen: $\forall i \in \{0, \cdots, n\} : a_i \in \mathbb{C}$, $a_n \neq 0$ en $n \in \mathbb{Z}_{>0}$. Dan heeft de vergelijking*

$$P(z) = 0$$

minstens één oplossing in $\mathbb{C}$.

□

Een toepassing van het euclidisch algoritme op polynoomringen leert dan dat zo'n vergelijking $P(z) = 0$ uit de stelling dan exact n (mogelijk meervoudige) oplossingen heeft. Zie hiervoor het college algebra.

We zullen de stelling hier niet bewijzen. Voor het sluitend maken van een bewijs is namelijk wezenlijk meer wiskunde nodig dan we hier op dit moment voorhanden hebben. We zullen echter wel aannemelijk en vooral inzichtelijk proberen te maken dat de stelling geldt. Hiervoor zijn enkele observaties nodig.

Zij $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ een willekeurig polynoom in z over $\mathbb{C}$ van positieve graad n.

We beschouwen P als een afbeelding (functie) van $\mathbb{C}$ naar $\mathbb{C}$ en met name de restrictie tot cirkels met middelpunt 0. Zij $M \in \mathbb{R}_{>0}$ en S_M de cirkel met middelpunt 0 en straal M. Het beeld van S_M onder P is nu nog even iets te lastig, maar het beeld onder het polynoom $z^j, j \in \{1, \cdots, n\}$, is goed te zien. Het beeld van S_M is dan een cirkel met straal M^j. Dit is het beste in te zien door S_M te beschouwen als een geparametriseerde kromme met domein $[0, 2\pi\rangle$:

$$t \to (M\cos(t), M\sin(t)).$$

Het beeld onder z^j is dan de volgende parameterkromme:

$$t \to (M^j\cos(jt), M^j\sin(jt)).$$

Het beeld van deze parameterkromme is een cirkel met straal M^j die exact j keer wordt doorlopen, als t het interval $[0, 2\pi\rangle$ doorloopt.

Als we dit spel spelen met $a_j z^j, a_j \neq 0$, in plaats van z^j, vinden we als beeld een cirkel die nog steeds j keer wordt doorlopen, maar die straal $|a_j|^j M^j$ heeft.

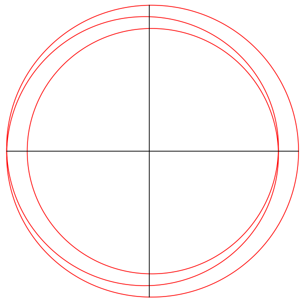
Als we dit spel gaan spelen met $a_j z^j + a_k z^k, k \in \{1, \cdots, \hat{j}, \cdots, n\}$, vinden we als beeld van S_M een *cycloïde*, een samenstelling van twee draaibewegingen[3].

Zonder de algemeenheid te schaden mogen we aannemen dat geldt $j > k$. Cruciaal is de volgende opmerking: Als we M groot maken, zal vanaf zekere waarde gelden:

$$|a_k M^k| < \frac{|a_j M^j|}{100}.$$

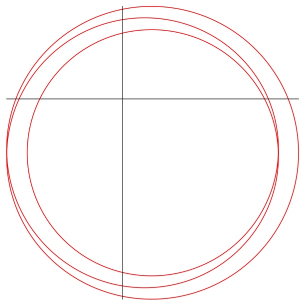
Met andere woorden: de cycloïde die het beeld is van S_M onder $a_j z^j + a_k z^k$ is in wezen de baan van een punt dat j keer om de oorsprong draait op basisafstand $|a_j M^j|$ en die bij die beweging telkens een storing ondergaat waarbij het punt minder dan een honderdste deel van de basisafstand wordt verschoven. Losjes gezegd: deze cycloïde is de tekening van iemand die met niet al te vaste hand een j-voudige cirkel om de oorsprong probeert te tekenen met redelijk grote straal. In figuur 16 wordt dit duidelijk geïllustreerd.

[3]Cycloïden zijn op de kermis erg populair bij personen die graag betalen om misselijk te worden.



Figuur 16: Een cycloïde met $j = 3$ en $k = 2$ en M groot genoeg.

De idee van een bewijs van de hoofdstelling is nu deze redenatie door te trekken naar het beeld van S_M, waarbij we M een eindig aantal keren 'groot genoeg' moeten maken, onder het polynoom $\tilde{P}(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z$. Voor M groot genoeg lijkt de bijbehorende cycloïde op een slordig getekende n-voudige cirkel met straal M om 0. Het beeld onder het oorspronkelijke polynoom is een verschuiving van deze cycloïde over het getal/de vector a_0. Als we echter M veel groter kiezen dan $|a_0|$, ligt het 'binnengebied' van de cycloïde over 0 heen. Dit wordt geïllustreerd in figuur 17



Figuur 17: Het beeld onder het oorspronkelijke polynoom.

Het binnengebied van de cycloïde wordt via P bedekt door het binnengebied van S_M. In het binnengebied van de cycloïde ligt ook 0. Ook dit getal is dus het beeld onder P van een getal a in het binnengebied van S_M. Maar dat betekent precies dat geldt:

$$P(a) = 0,$$

hetgeen betekent dat het polynoom P een nulpunt in $\mathbb{C}$ heeft. Dit 'bewijst' de hoofdstelling van de algebra.

Klaar!

6 Verzamelingenleer

Dit hoofdstuk gaat over over *verzamelingenleer*. Wat een verzameling precies is, is niet zo eenvoudig te definiëren. Op dit punt moet er in een stuk dat handelt over verzamelingenleer een keuze worden gemaakt, namelijk die tussen de axiomatische en de naïeve verzamelingenleer. In de axiomatische verzamelingenleer wordt de theorie opgebouwd vanuit een stelsels axioma's. Met name het axiomastelsel van Zermelo en Fraenkel mag hier niet onvermeld blijven. In de naïeve verzamelingenleer wordt er niet gewerkt op basis van een axiomastelsel, maar gaan we uit van een naïef / intuïtief verzamelingenbegrip: een verzameling is een soort container die *objecten*, de *elementen*, bevat en die volledig door deze elementen (niet voorzien van een volgorde) wordt bepaald.

De keuze die hier in dezen wordt gemaakt, is die voor de naïeve verzamelingenleer. De motivatie hiertoe is gelegen in de grotere toegankelijkheid hiervan voor eerstejaars studenten.

Opmerking 5 *Het is soms nodig het begrip* klasse *te gebruiken op plaatsen waar men mogelijk geneigd zou kunnen zijn het begrip* verzameling *te gebruiken. Een* klasse *is, net als een verzameling, een soort container die* objecten*, de* elementen*, bevat en die volledig door deze elementen (niet voorzien van een volgorde) wordt bepaald. De noodzaak van dit begrip komt in zicht, als we kijken naar* alle verzamelingen*. Dit is gevoelsmatig toch een container met elementen, namelijk de verzamelingen. Als we deze container echter een* verzameling *willen noemen, komen we in de problemen met de Russell paradox: Zij A gedefinieerd door:*

$$A = \{V | V \notin V\}.$$

In woorden: A bevat precies die verzamelingen die geen element van zichzelf zijn.

Als we de container met alle verzamelingen een verzameling willen noemen, moet A een deelverzameling zijn van die verzameling van alle verzamelingen en dus een verzameling. De paradox openbaart zich, als we de vraag willen beantwoorden of A zichzelf als element bevat of niet. Er geldt echter:

$$A \in A \Leftrightarrow A \notin A.$$

Derhalve praten we niet over de verzameling *van alle verzamelingen, maar over de* klasse *van alle verzamelingen. In principe worden in dit dictaat alleen verzamelingen besproken.* Equivalentierelaties *echter worden ook voor klassen gedefinieerd. Dit hebben we later in het dictaat nodig bij het definiëren van kardinaalgetallen.*

Als een object x bevat is in een verzameling A wordt dit genoteerd als:

$$x \in A.$$

Als een object x niet bevat is in een verzameling A, geldt dus:

$$\neg\{x \in A\}.$$

Dit wordt in de regel genoteerd als:

$$x \notin A.$$

Verzamelingen worden bepaald door hun elementen. Dit leidt tot de volgende definitie.

Definitie 32 (Gelijkheid van twee verzamelingen) *Zij A en B twee verzamelingen. Dan wordt de gelijkheid van A en B gedefinieerd door:*

$$A = B \Leftrightarrow [\forall x : x \in A \Leftrightarrow x \in B].$$

Definitie 33 *Zij A en B twee verzamelingen. A heet een* deelverzameling *van B (notatie $A \subset B$), als geldt:*

$$\forall x : x \in A \Rightarrow x \in B.$$

Een verzameling wordt bepaald door zijn elementen. Een bijzondere situatie is die waarin een verzameling juist géén elementen bevat.

Definitie 34 *Een* lege verzameling $\emptyset$ *is een verzameling zonder elementen:*

$$\forall x : x \notin \emptyset.$$

Opmerking 6 *Merk op dat een lege verzameling deelverzameling is van iedere verzameling. Zij A een verzameling. Omdat geldt: $\forall x : x \notin \emptyset$, volgt uit de logica:*

$$\forall x : x \in \emptyset \Rightarrow x \in A,$$

hetgeen betekent $\emptyset \subset A$.

Stelling 21 *Als de lege verzameling bestaat, is deze uniek.*

□

Bewijs
Stel dat $\emptyset_1$ en $\emptyset_2$ beide voldoen aan de definitie voor de lege verzameling. Dan geldt volgends de definitie van gelijkheid van verzamelingen:

$$\emptyset_1 = \emptyset_2 \Leftrightarrow [\forall x : x \in \emptyset_1 \Leftrightarrow x \in \emptyset_2].$$

Volgens de definitie van lege verzameling is de rechter uitspraak in deze equivalentie

$$\forall x : x \in \emptyset_1 \Leftrightarrow x \in \emptyset_2$$

hetzelfde als:

$$\forall x : false \Leftrightarrow false,$$

hetgeen een ware uitspraak is. Derhalve geldt dus ook

$$\emptyset_1 = \emptyset_2.$$

□

Het bestaan van een, en dus dé lege verzameling moet bewezen worden. Hiervoor hebben we een willekeurige verzameling X nodig. Beschouw dan de verzameling:

$$\{x \in X | x \neq x\}.$$

Deze verzameling is leeg.

Definitie 35 (machtsverzameling) *Zij A een verzameling. De* machtsverzameling $\wp(A)$ *is de verzameling van alle deelverzamelingen van A:*

$$\wp(A) = \{U | U \subset A\}$$

Voorbeeld 1 *Merk bij de volgende drie verzamelingen op dat van de eerste twee de machtsverzameling meer elementen bevat dan de basisverzameling. Is dat altijd zo? Hoe zit dat bij het laatste voorbeeld? Hier komen we verderop uitgebreid op terug.*

- $A = \emptyset : \wp(\emptyset) = \{\emptyset\}$
- $A = \{a, b\} : \wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $A = \mathbb{N} : \wp(\mathbb{N}) = \cdots$ *?*

6.1 Relaties

Definitie 36 *Een* geordend paar *is een geordend tweetal objecten. Als het eerste object a is en het tweede b, wordt het geordend paar genoteerd als (a, b). Hierin heet a de* x-coördinaat *en b de* y-coördinaat.

Definitie 37 *Een* relatie *is een verzameling geordende paren.*

Als R een relatie is en $(a, b) \in R$ is een element van R, dan wordt dit ook wel genoteerd als aRb.

Definitie 38 (domein en bereik) *Zij R een relatie.*

- *Het* domein *van R is* $D_R := \{x | \exists y : (x, y) \in R\}$
- *Het* bereik *van R is* $B_R := \{y | \exists x : (x, y) \in R\}$

Definitie 39 *Zij A en B twee verzamelingen. Een relatie R heet een* relatie van A naar B *als geldt:*

$$D_R \subset A \wedge B_R \subset B$$

Definitie 40 *Zij A en B twee verzamelingen. Het* cartesisch produkt $A \times B$ *van A en B is:*

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

Opmerking 7 *Een relatie van A naar B had dus ook gedefinieerd kunnen worden als* een deelverzameling van $A \times B$.

Definitie 41 *Een* relatie op A *is een deelverzameling van $A \times A$. Dit is hetzelfde als een relatie van A naar A.*

6.2 Equivalentierelaties

Definitie 42 *Een relatie R op een verzameling of een klasse A ($A \neq \emptyset$) heet een* equivalentierelatie op A *als aan de volgende drie voorwaarden is voldaan:*

- *reflexiviteit:* $\forall a \in A : aRa$
- *symmetrie:* $aRb \Leftrightarrow bRa$
- *transitiviteit:* $[aRb \wedge bRc] \Rightarrow aRc$

Als R een equivalentierelatie is op een verzameling, wordt aRb vaak genoteerd als $a \sim b$.

Definitie 43 *Zij A een verzameling. Een deelverzameling $P \subset \wp(A)$ heet een* partitie *van A als geldt:*

1. $\emptyset \notin P$
2. $[U \in P \wedge V \in P] \Rightarrow [U = V \vee U \cap V = \emptyset]$
3. $\forall x \in A : \exists U \in P : x \in U$

Definitie 44 *Zij $\sim$ een equivalentierelatie op een niet lege verzameling A en zij $x \in A$. De verzameling*

$$\overline{x} := \{a \in A | x \sim a\}$$

heet de equivalentieklasse *van x.*

Merk op dat geldt:

- De equivalentieklassen vormen een partitie van de onderliggende verzameling.
- Ieder element is bevat in zijn eigen equivalentieklasse.
- Zij A een niet lege verzameling. Dan bestaat er een kanonieke bijectie tussen de verzameling van partities van A en de verzameling van equivalentierelaties op A.

Definitie 45 *Zij $\sim$ een equivalentierelatie op een niet lege verzameling A en zij $x \in A$. De verzameling*

$$A/\sim := \{\overline{x} | x \in A\}$$

van alle equivalentieklassen heet de quotiëntruimte *van A onder $\sim$.*

Definitie 46 (rationale getallen) *Zij X de verzameling $\mathbb{Z} \times \mathbb{Z}^*$[4]. Op X wordt de equivalentierelatie $\sim$ gedefinieerd door:*

$$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0$$

De quotiëntruimte van X onder $\sim$ heet de verzameling der rationale getallen, *notatie: $\mathbb{Q}$.*

[4] $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$

6.3 Afbeeldingen

Definitie 47 *Een* afbeelding *is een relatie f met de volgende eigenschap:*

$$[(x, y_1) \in f \wedge (x, y_2) \in f] \Rightarrow y_1 = y_2$$

Definitie 48 *Zij A en B twee verzamelingen. Een* afbeelding f van A naar B *is een afbeelding met de eigenschap:*

$$D_f = A \wedge B_f \subset B$$

Notatie: $f : A \to B$.

Definitie 49 *Een afbeelding f van A naar B heet:*

- injectief*, als geldt:* $[(x_1, y) \in f \wedge (x_2, y) \in f] \Rightarrow x_1 = x_2$
- surjectief*, als geldt:* $B_f = B$.
- bijectief*, als f zowel injectief als surjectief is.*

Een injectieve afbeelding f van A naar B wordt ook wel een *injectie* genoemd.

Een surjectieve afbeelding f van A naar B wordt ook wel een *surjectie* genoemd.

Definitie 50 *Twee verzamelingen A en B heten* gelijkmachtig *of* equipotent*, als er een bijectie bestaat van A naar B.*

Als twee verzamelingen A en B equipotent zijn, wordt dit ook wel genoteerd als: $A \sim B$.

Stelling 22 *Equipotentie is een equivalentierelatie op de klasse van verzamelingen.*

□

Bewijs

We lopen de drie eisen na:

- Reflexiviteit: Zij X een verzameling. De identiteit $id_X : X \to X$ is een bijectie. Dit geeft $X \sim X$.
- Symmetrie: Zij X en Y twee verzamelingen met $X \sim Y$. Zij $f : X \to Y$ een bijectie. Dan is $f^{-1} : Y \to X$ ook een bijectie. Dit geeft $Y \sim X$.
- Transitiviteit: Zij X, Y en Z drie verzamelingen z.d.d. $X \sim Y$ en $Y \sim Z$. Zij $f : X \to Y$ en $g : Y \to Z$ twee bijecties. Dan is $g \circ f : X \to Z$ ook een bijectie. Dit geeft $X \sim Z$.

□

Definitie 51 *Een equivalentieklasse onder equipotentie heet een* kardinaalgetal.

Stelling 23 *Zij A een verzameling. Dan zijn A en $\wp(A)$ niet equipotent.*

$\square$

Bewijs
Zij A een verzameling en zij $f : A \to \wp(A)$ een willekeurige afbeelding. Beschouw $W \subset A$ gedefinieerd door:

$$W = \{x \in A | x \notin f(x)\}.$$

Er geldt $W \notin B_f$. Immers, als wel zou gelden $W \in B_f$, dan geldt voor zekere $p \in A$: $W = f(p)$. Dit leidt echter direct tot de volgende tegenspraak:

$$p \in W \Leftrightarrow p \notin W.$$

Conclusie: iedere afbeelding $f : A \to \wp(A)$ is niet surjectief en dus zijn A en $\wp(A)$ niet equipotent.

$\square$

Stelling 24 (Cantor-Bernstein) *Zij A en B twee verzamelingen en stel:*

$$\exists f : A \to B \wedge \exists g : B \to A$$

met f en g injectief, dan geldt: $A \sim B$.

$\square$

Stelling 25 (Cantor-Bernstein, alternatieve formulering) *Zij $A \subset B$ en stel: $\exists f : B \to A$ met f injectief. Dan geldt: $A \sim B$.*

$\square$

Bewijs
De essentie van dit bewijs zal zijn dat we de inbedding $i : A \hookrightarrow B$ die natuurlijk van nature al injectief is, gaan verbouwen tot een surjectie zonder de injectiviteit aan te tasten. Door dit te doen, wordt de stelling natuurlijk bewezen. Definieer C_0 door:

$$C_0 = B \setminus A$$

Als geldt $C_0 = \emptyset$, is de inbedding $i : A \hookrightarrow B$ reeds surjectief en zijn we klaar. Stel dus dat geldt $C_0 \neq \emptyset$. Definieer nu voor $t \in \mathbb{Z}_{>0}$:

$$C_t = f(C_{t-1})$$

Deze C_t's zijn onderling disjunct:

$$\forall s, t \in \mathbb{Z}_{\geq 0} : s \neq t \Rightarrow C_s \cap C_t = \emptyset$$

Het is een leuke opgave voor de student dit zelf aan te tonen.

Een direkt gevolg hiervan is dat voor de restrictie van f tot deze C_t's geldt dat

$$f : \bigcup_{t=0}^{\infty} C_t \to \bigcup_{t=1}^{\infty} C_t$$

een bijectie is. De inverse van deze afbeelding levert ons de mogelijkheid de inbedding $i : A \hookrightarrow B$ te 'verbouwen' tot een bijectie. We definiëren $g : A \to B$ als volgt:

$$g(x) = \begin{cases} f^{-1}(x) & \text{als } x \in \bigcup_{t=1}^{\infty} C_t \\ \\ x & \text{als } x \notin \bigcup_{t=1}^{\infty} C_t \end{cases}$$

Buiten $\bigcup_{t=1}^{\infty} C_t$ is g de oorspronkelijke inbedding en (letterlijk en figuurlijk) daarnaast geldt dat

$$g : \bigcup_{t=1}^{\infty} C_t \to \bigcup_{t=0}^{\infty} C_t$$

een bijectie is. Gevolg: g is bijectief.

$\square$

Definitie 52 *Zij A een verzameling.*

- *Als geldt $A \sim \mathbb{N}$, dan heet A* (oneindig) aftelbaar*.*
- *Als A eindig is, heet A* eindig aftelbaar*.*
- *Als A oneindig is, maar niet aftelbaar, heet A* overaftelbaar*.*

Stelling 26

$$\mathbb{R} \sim \wp(\mathbb{N})$$

$\square$

De verzameling $\mathbb{R}$ is dus overaftelbaar.

6.4 Ordeningen

Definitie 53 *Zij A een verzameling. Een relatie R op A heet een* (partiële) ordening *als geldt:*

- $\forall x \in A : (x, x) \in R$ *(reflexiviteit)*
- $\forall x, y \in A : [(x, y) \in R \wedge (y, x) \in R] \Rightarrow x = y$ *(antisymmetrie)*
- $\forall x, y, z \in A : [(x, y) \in R \wedge (y, z) \in R] \Rightarrow (x, z) \in R$ *(transitiviteit)*

Gebruikelijke symbolen voor partiële ordeningen zijn:

- $\leq$

- $\preceq$
- $\subseteq$
- $\sqsubseteq$

Door in de definitie van partiële ordeningen zo'n symbool te gebruiken, wordt meteen duidelijk dat een partiële ordening niets anders is dan de abstrahering van de 'kleiner-gelijk' relatie:

- $\forall x \in A : x \preceq x$
- $\forall x, y \in A : [x \preceq y \wedge y \preceq x] \Rightarrow x = y$
- $\forall x, y, z \in A : [x \preceq y \wedge y \preceq z] \Rightarrow x \preceq z$

Voorbeeld 2 *Belangrijke voorbeelden van ordeningen zijn:*

- *De standaard ordening op (deelverzamelingen van) de reële getallen.*
- *De inclusie-ordening op een machtsverzameling.*
- *De volgende ordening op kardinaalgetallen. Zij* $\overline{K}$ *en* $\overline{L}$ *twee kardinaalgetallen. Dan wordt* $\overline{K} \preceq \overline{L}$ *gedefinieerd door:* $\exists B \subset L : B \sim K$*. Merk hierbij op dat reflexiviteit en transitiviteit zijn in te zien door recht-toe-recht-aan de definities na te lopen, maar dat de anti-symmetrie gegeven wordt door de stelling van Cantor-Bernstein.*

Definitie 54 *Een partiële ordening* $\preceq$ *op een verzameling* A *heet een* lineaire *of* totale *ordening als geldt:*

$$\forall x, y \in A : x \preceq y \vee y \preceq x$$

Interessante vraag: Worden kardinaalgetallen door de hierboven gedefinieerde ordening (voortaan ook wel de standaard ordening op kardinaalgetallen genoemd) *lineair* geordend?

Deze vraag komt neer op: *Gegeven twee verzamelingen; geldt dan altijd dat er in minstens één van beide richtingen een inclusie bestaat?* Intuïtief zullen de meesten deze vraag bevestigend beantwoorden. Echter, voor het bevestigende antwoord op deze vraag is extra gereedschap nodig: *het keuzeaxioma.* Het keuzeaxioma (dat hieronder wordt geformuleerd) is één van de belangrijkste en meest intrigerende axioma's uit de verzamelingenleer. Het voert echter te ver dit in deze module uit te werken.

Axioma 1 (Het Keuzeaxioma (=AC)) *Zij* A *een niet-lege verzameling. Dan geldt:*

$$\exists k : \wp(A)^* \to A : \forall U \in \wp(A)^* : k(U) \in U$$

Zo'n afbeelding k *wordt een* keuzeafbeelding *genoemd.*

Het keuzeaxioma stelt dus dat het bij iedere niet-lege verzameling mogelijk is *op voorhand* bij iedere niet-lege deelverzameling een element uit die deelverzameling te kiezen.

Stelling 27 (AC) *Iedere verzameling van kardinaalgetallen wordt door de standaard ordening lineair geordend.*

□

Definitie 55 (welordening) *Een lineaire ordening op een verzameling A heet een* welordening, *als iedere niet lege deelverzameling van A een kleinste element heeft.*

Voorbeeld 3 *Twee voorbeelden:*

- *De standaard ordening op de natuurlijke getallen is een welordening.*
- *De standaard ordening op de reële getallen is* geen *welordening.*

Stelling 28 ***AC*** *Iedere verzameling van kardinaalgetallen wordt door de standaard ordening welgeordend.*

□

Interessante vraag: De reële getallen worden niet welgeordend door de standaard ordening. Bestaat er eigenlijk wel een welordening op $\mathbb{R}$? Het antwoord op deze vraag wordt gegeven door:

Stelling 29 (Welordeningsstelling van Zermelo, AC) *Iedere verzameling is te voorzien van een welordening.*

□

Wat in deze context beslist niet onvermeld mag blijven is het lemma van Zorn. Eerst een paar definities.

Definitie 56 (bovengrens) *Zij A een door $\preceq$ partieel geordende verzameling en zij $B \subset A$. Een element $x \in A$ heet een* bovengrens *van B als geldt:*

$$\forall a \in B : a \preceq x$$

Definitie 57 (maximaal element) *Zij A een door $\preceq$ partieel geordende verzameling. Een element $m \in A$ heet een* maximaal element *van A als geldt:*

$$\forall x \in A : x = M \vee \neg(m \preceq x)$$

Definitie 58 (keten) *Zij A een door $\preceq$ partieel geordende verzameling. Een* keten *K is een deelverzameling $K \subset A$ die door $\preceq$ lineair geordend wordt.*

Stelling 30 (Lemma van Zorn, AC) *Zij A een partieel geordende verzameling. Als iedere keten in A een bovengrens heeft, heeft A een maximaal element.*

□

Dit beroemde lemma zal je bij Algebra hard nodig hebben voor de existentie van maximale idealen. Deze termen zeggen je hier nog niets, maar het kan geen kwaad dit alvast een keer gehoord te hebben. Dit dictaat wordt afgesloten met het verband tussen het keuzeaxioma, het lemma van Zorn en de welordeningsstelling van Zermelo:

Stelling 31 *De volgende drie uitspraken zijn onderling equivalent:*

- *Het keuzeaxioma*
- *Het lemma van Zorn*
- *De welordeningsstelling van Zermelo*

$\square$