CALEIDOSCOOP

VOORWOORD

In de Caleidoscoop geven we een kijk op verschillende onderdelen van de wiskunde en de onderlinge samenhang. Ook werken we met diverse hulpmiddelen, zoals bibliotheek en software pakketten. De basis daarvoor wordt gelegd in het college Inleiding tot de Wiskunde. In dit college word je verder vertrouwd gemaakt met de taal van de wiskunde, met axioma's, definities, stellingen, bewijzen en algoritmen, en wordt daarmee geoefend. Wiskundigen hebben een compacte manier van opschrijven die geleerd moet worden. De laatste hoofdstukken van het college bestaan uit een theoretische behandeling van de analyse.

Het college kent een veelzijdige *toetsing*. Deze bestaat uit:

- in te leveren huiswerk, elke week, totaal 4 studiepunten
  Er zijn elf vellen met huiswerkopgaven, voor elke week na de eerste één. Elk vel telt enkele vraagstukken, en een opgave om extra punten te verdienen. Ingeleverd huiswerk dat een cijfer lager dan 5 krijgt moet overgemaakt worden. Het tentamenbriefje wordt pas afgegeven als elf keer huiswerk is ingeleverd. (sept/dec)
- mondelinge presentatie van ongeveer 10 minuten, 1 studiepunt (dec)
- mondeling tentamen, 2 studiepunten (eerste helft 2003).
  Getoetst wordt of alle definities, stellingen, bewijzen, opmerkingen en opgaven (met uitzondering van de paragrafen met (AO)) uit Hoofdstukken 6 en 7 zowel goed begrepen zijn als vlot zonder dictaat geformuleerd/gegeven/gemaakt kunnen worden.
  Het mondeling tentamen kan worden afgelegd als ik beschikbaar ben. S.v.p. ruim een week van tevoren een afspraak maken.

Dit college kent dus geen schriftelijk tentamen, zoals bij de meeste andere vakken.

Er is een *dictaat* met vraagstukken en huiswerkopgaven.
Secties in het dictaat waarbij (AO) staat, betreffen geen basisstof die bij latere colleges bekend wordt verondersteld, maar algemene ontwikkeling.

Bij het college is een *werkgroep* die gegeven wordt door Szabolcs Tengely en ondergetekende. In de regel is het college op woensdag van 11.15 tot 13.00 uur, het werkcollege op donderdag van 14.45 tot 16.30 uur, terwijl het uur 13.45 tot 14.30 op donderdag vaak gebruikt zal worden voor voordrachten van docenten of het bespreken van het huiswerk.

Ik ken geen boek dat omvat wat tijdens dit college behandeld wordt. Per hoofdstuk zal ik relevante *literatuur* noemen.

R. Tijdeman
augustus 2002

1 HOOFDSTUK: GEHELE GETALLEN

1.1 De natuurlijke getallen.

De natuurlijke getallen vormen de bouwstenen van de wiskunde. Wat is vanzelfsprekend aan deze getallen en wat moet je nog bewijzen? Is $2+2=4$ vanzelfsprekend? $2 \times 2 = 4$? enz.

Wiskundigen, met name logici die aan grondslagenonderzoek van de wiskunde werken, streven ernaar een zo beperkt mogelijk aantal grondregels, zg. *axioma's*, op te stellen en dan alle andere eigenschappen daaruit af te leiden.

We beginnen met de grondregels voor de *natuurlijke getallen* $\mathbf{N} = \{1, 2, 3, ...\}$.

(i) Elk paar natuurlijke getallen a, b heeft een *som* $a + b \in \mathbf{N}$ zó dat $a + b = b + a$ voor alle $a, b \in \mathbf{N}$ (optelling is *commutatief*)
en $(a + b) + c = a + (b + c)$ voor alle $a, b, c \in \mathbf{N}$ (optelling is *associatief*).
(ii) Elk paar natuurlijke getallen a, b heeft een *product* $ab \in \mathbf{N}$
zó dat $ab = ba$ voor alle $a, b \in \mathbf{N}$ (vermenigvuldiging is commutatief) en $(ab)c = a(bc)$ voor alle $a, b, c \in \mathbf{N}$ (vermenigvuldiging is associatief).
(iii) Optelling en vermenigvuldiging zijn gekoppeld door de *distributiviteit*:

$$a(b + c) = ab + ac \text{ voor alle } a, b, c \in \mathbf{N}.$$

Bovenstaande eigenschappen zullen weinig weerstanden oproepen, maar zijn niet voldoende om de natuurlijke getallen te karakteriseren. Ook de gehele getallen en de reële getallen voldoen eraan, en nog vele andere verzamelingen. De natuurlijke getallen worden éénduidig vastgelegd door het volgende axioma:
(iv) Er is een natuurlijke getal 1 met de eigenschap dat $1 \times 1 = 1$;
elk natuurlijk getal wordt verkregen door 1 een aantal keren bij zichzelf op te tellen en elke keer als je er weer 1 bij optelt krijg je een nieuw getal.

De natuurlijke getallen zijn dus (vanwege eigenschap (i) hoeven we niet op de volgorde van optellen te letten):

$$1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1, ... \, .$$

Dat we deze getallen noteren met $1, 2, 3, 4, 5, ...$ is een afspraak. Sommige mensen beschouwen 0 ook als een natuurlijke getal, de lege som. Ook dit is louter een kwestie van afspraak. Als het begrip natuurlijke getallen gebruikt wordt, moet je even nagaan wat de schrijver ermee bedoelt. In dit college is 0 geen natuurlijk getal.

Als je het nu van de grond af wil opbouwen, moet je bijvoorbeeld bewijzen dat een getal niet verandert als je het met 1 vermenigvuldigt, dat je een ordening $<$ op de natuurlijke getallen kan invoeren met $1 < 2 < 3 < 4 < 5$... zó dat als $a < b$ en $b < c$, dan $a < c$, dat uit $a < b$ volgt dat $a = b - 1$ of $a < b - 1$, enz. Dat staat allemaal netjes uitgewerkt in boeken, bijv. in Van der Waerden I, p.5-8, maar zullen we hier niet doen. Ik zal zulke intuïtieve eigenschappen hier stilzwijgend gebruiken.

Wel zal ik een bewijsprincipe behandelen dat op axioma (iv) berust, het *principe van volledige inductie.*
Elk natuurlijk getal heeft eigenschap P als
(a) 1 eigenschap P heeft
(b) voor elk natuurlijk getal n geldt dat n eigenschap P heeft als elk kleiner natuurlijk getal eigenschap P heeft.

(a) noemen we de *beginvoorwaarde* , (b) de *inductiestap.*

Voorbeeld van een bewijs met volledige inductie:
Eigenschap $P : 1 + 3 + 5 + ... + (2n - 1) = n^2$
(de som van de eerste n oneven natuurlijke getallen is n^2).
Bewijs: (a) de som van het eerste oneven natuurlijke getal is $1^2 (= 1)$.
(b) Stel alle natuurlijke getallen kleiner dan m hebben eigenschap P.
Dan geldt, als $m > 1$, dat $1 + 3 + 5 + ... + (2m - 3) = (m - 1)^2$.
Hieruit volgt $1+3+5+...+(2m-3)+(2m-1) = (m-1)^2+(2m-1) = m^2$.
De inductiestap is voltooid. $\square$

Met een inductiebewijs hoef je dus niet elk van de oneindig vele natuurlijke getallen te controleren, maar volsta je met twee bewijsstappen.

De natuurlijke getallen zijn *gesloten* onder de optelling en vermenigvuldiging, d.w.z. dat de som en het product van natuurlijke getallen een natuurlijk getal is, maar niet onder aftrekking: $7 - 3 = 4 \in \mathbf{N}$, maar $3 - 7 \notin \mathbf{N}$. De kleinste uitbreiding van $\mathbf{N}$ die gesloten is onder aftrekking en aan (i)-(iii) voldoet, is de verzameling van de gehele getallen, $\mathbf{Z}$.
N.B. $3 - 7 = x$ betekent hetzelfde als $x + 7 = 3$.

1.2 De gehele getallen.

We kunnen $\mathbf{N}$ uitbreiden tot *de gehele getallen* (integers) $\mathbf{Z}$ via de volgende regels:
(+N) er is een getal $0 \in \mathbf{Z}$ zó dat $a + 0 = a$ voor alle $a \in \mathbf{Z}$
(+I) bij elke $a \in \mathbf{Z}$ bestaat een $x \in \mathbf{Z}$ met $a + x = 0$.

Door eigenschap (+N) wordt 0 toegevoegd, het *neutrale element* voor de optelling, door (+I) worden de negatieve getallen toegevoegd, de *inverse elementen* van de natuurlijke getallen voor de optelling. Bijv. bij 3 hoort -3 want $3 + (-3) = 0$.
Aftrekken is optellen van de inverse, *de tegengestelde*, bijv. $3 - 5 = 3 + (-5)$.
Er geldt $a - b = c - d$ als en alleen als $a + d = b + c$.

Voordat we verder gaan met de gehele getallen, laten we zien hoe de *rationale getallen* **Q** gedefinieerd worden. De gehele getallen zijn gesloten onder de optelling, aftrekking en vermenigvuldiging, maar niet onder deling: $7/3 \notin \mathbf{Z}$. Wel heeft **Z** een neutraal element voor de vermenigvuldiging:

(×N) $\qquad 1 \times a = a \quad$ voor alle a.

Voor **Q** eisen we nu het bestaan van een inverse t.o.v. vermenigvuldiging:

(×I) $\qquad$ bij elke $a \neq 0$ bestaat een x zodat $ax = 1$.

Het getal x heet het *omgekeerde* (of de multiplicatief inverse) van x, notatie a^{-1}. *Delen* is vermenigvuldigen met het omgekeerde: $a : b = a \times b^{-1}$. Er geldt $a : b = c : d$ als en alleen als $ad = bc$ en $bd \neq 0$. Merk op dat je wel elk geheel getal kan aftrekken, maar niet door elk geheel getal kan delen.
Als vervanger van deling hebben we in **Z** *deling met rest*:

Stelling 1.1. *Bij elk paar* $a, b \in \mathbf{Z}$ *met* $b > 0$ *bestaat precies één paar* $q, r \in \mathbf{Z}$ *met* $a = qb + r$ *en* $0 \leq r < b$.

q komt van quotient. Het getal r heet de rest bij deling van a door b.

Bewijs. Zij q het grootste gehele getal met $qb \leq a$. Dan is $(q + 1)b > a$. Definieer $r = a - qb$. Dan geldt $r \geq 0$ en $r < b$.
Zij q', r' een ander paar dat aan de eisen voldoet. Dan is $q'b \leq a$ en dus $q' \leq q$. Als $q' < q$, dan geldt $q' \leq q - 1$. Nu volgt: $r' = a - q'b \geq a - (q - 1)b = r + b \geq b$, d.w.z. $r' \geq b$. Tegenspraak. Als $q' = q$, dan is ook $r = a - qb = a - q'b = r'$. □

Opmerking. In bovenstaand "bewijs" hebben we gebruik gemaakt van allerlei eigenschappen die we niet uit de definities hebben afgeleid, met name eigenschappen van ongelijkheden.

De verzameling van getallen a die rest r geven bij deling door b noemen we de *restklasse* (residue class) r van b. De restklasse 0 verdient speciale aandacht. Als $a = qb$ met $q \in \mathbf{Z}$, dan heet b een *deler* (divisor) van a, en a een *veelvoud* (multiple) van b. Notatie $b|a$. Als b geen deler is, schrijven we $b \dagger a$.

Voor alle gehele getallen a, b, c, d geldt
(D1) $d|a$ en $d|b \Longrightarrow d|a+b$ en $d|a-b$
(D2) $a|b$ en $b|c \Longrightarrow a|c$
(D3) $d|a \Longrightarrow d|ab$ en $db|ab$.
(D4) $d|a$ en $a > 0 \Longrightarrow d \leq a$.

Uit (D4) zien we dat een getal $a > 0$ slechts eindig veel delers heeft.

Stel $a, b \in \mathbf{Z}$, niet beide 0. Onder de *grootste gemene deler* van a en b verstaan we het grootste gehele getal dat a èn b deelt, notatie (a, b) of $\mathrm{ggd}(a, b)$. Als $(a, b) = 1$, dan heten a en b *relatief priem* of *onderling ondeelbaar*. Het *kleinste gemene veelvoud* van a en b is het kleinste natuurlijke getal met a èn b als delers, notatie $[a, b]$ of $\mathrm{kgv}(a, b)$. Voor alle gehele getallen a, b en q geldt:

(D5) $$(a, b) = (a - qb, b).$$

Opgave 1.15 zegt dat voor alle natuurlijke getallen a, b geldt:

$$\mathrm{ggd}(a, b) \times \mathrm{kgv}(a, b) = ab.$$

Het algoritme van Euclides (omstreeks -300) is een snelle manier om de ggd uit te rekenen. Het berust op een combinatie van Stelling 1.1 en eigenschap (D5).

Voorbeeld. Neem $a = 842$ en $b = 356$. Pas Stelling 1.1. herhaaldelijk toe op b en r.

$$\begin{array}{rlrl}
842 & = 2 \times 356 + 130, & \text{dus } (842, 356) & = (356, 130) \\
356 & = 2 \times 130 + \ \ 96, & \text{dus } (356, 130) & = (130, 96) \\
130 & = 1 \times \ \ 96 + \ \ 34, & \text{dus } (130, 96) & = \ \ (96, 34) \\
96 & = 2 \times 34 + \ \ 28, & \text{dus } (96, 34) & = \ \ (34, 28) \\
34 & = 1 \times 28 + \ \ \ 6, & \text{dus } (34, 28) & \ \ (28, 6) \\
28 & = 4 \times 6 + \ \ \ 4, & \text{dus } (28, 6) & = \ \ (6, 4) \\
6 & = 1 \times 4 + \ \ \ 2, & \text{dus } (6, 4) & = \ \ (4, 2) \\
4 & = 2 \times 2, & \text{dus } (4, 2) & = \ \ 2.
\end{array}$$

De conclusie is dat $(842, 356) = 2$. Het proces eindigt omdat de resten steeds kleiner worden, dus (in dit geval na hoogstens 130 stappen) nul worden.

Het algoritme van Euclides stelt ons ook in staat om gehele getallen x en y te vinden zó dat $842x + 356y = 2$.

$$
\begin{array}{rrrc}
842 = & 1 \times 842 & +0 \times 356 & q \\
356 = & 0 \times 842 & +1 \times 356 & 2 \\
130 = & 1 \times 842 & -2 \times 356 & 2 \\
96 = & -2 \times 842 & +5 \times 356 & 1 \\
34 = & 3 \times 842 & -7 \times 356 & 2 \\
28 = & -8 \times 842 & +19 \times 356 & 1 \\
6 = & 11 \times 842 & -26 \times 356 & 4 \\
4 = & -52 \times 842 & +123 \times 356 & 1 \\
2 = & 63 \times 842 & -149 \times 356. &
\end{array}
$$

Elk volgend getal in de linkerkolom is door q keer aftrekken van de voorgaande rij van de daaraan voorafgaande rij te schrijven als lineaire combinatie van 842 en 356. Zo komen we na eindig veel stappen bij $(842, 356) = 2$ terecht.

Het algoritme van Euclides is toepasbaar voor elk paar $a \in \mathbf{Z}, \mathbf{b} \in \mathbf{N}$.
Het ziet er als volgt uit:

$$
\begin{array}{lll}
a = q_1 b + r_1, & q_1 \in \mathbf{Z}, \quad 0 \le r_1 < b, & r_1 = 1 \times a - q_1 \times b \\
b = q_2 r_1 + r_2, & q_2 \in \mathbf{Z}, \quad 0 \le r_2 < r_1, & r_2 = -q_2 a + (1 + q_2 q_1) b \\
r_1 = q_3 r_2 + r_3, & q_3 \in \mathbf{Z}, \quad 0 \le r_3 < r_2, & r_3 = (1 + q_3 q_2) a - ... b \\
\cdots\cdot \ \cdots\cdot \ \cdots\cdot \ \cdots\cdot & & \\
r_{k-2} = q_k r_{k-1} + r_k, & q_k \in \mathbf{Z}, \quad 0 \le r_k < r_{k-1} & r_k = ...a + ...b \\
r_{k-1} = q_{k+1} r_k & q_{k+1} \in \mathbf{Z}. &
\end{array}
$$

Omdat $b > r_1 > r_2 > ... > r_k > 0$, moet het algoritme na hoogstens b stappen afbreken (in de praktijk is het aantal stappen veel kleiner). Met volledige inductie bewijst men $(a, b) = r_k$, immers $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k$. Dat (a, b) te schrijven is als lineaire combinatie van a en b formuleren we als stelling.

Stelling 1.2. Stel $a, b \in \mathbf{Z}$, niet beide nul. Dan bestaan er gehele getallen x en y met $ax + by = (a, b)$.

Bewijs. We bewijzen met volledige inductie naar n dat er gehele getallen x_n en y_n bestaan met $r_n = x_n a + y_n b$.
Voor $n = 1$ is de bewering waar, want $r_1 = a - q_1 b$.
Voor $n = 2$ is de bewering waar, want $r_2 = -q_2 a + (q_1 q_2 + 1)b$.
Stel de bewering is juist voor $1, 2, ..., m-1$. Dan volgt

$$\begin{aligned} r_m &= r_{m-2} - q_m r_{m-1} \\ &= (x_{m-2}a + y_{m-2}b) - q_m(x_{m-1}a + y_{m-1}b) \\ &= (x_{m-2} - q_m x_{m-1})a + (y_{m-2} - q_m y_{m-1})b. \end{aligned}$$

Hiermee is de inductiestap voltooid.
De bewering is dus waar voor $n = 1, 2, ..., k$ en in het bijzonder geldt
$(a, b) = r_k = x_k a + y_k b$. □

Stelling 1.2. heeft enkele belangrijke gevolgen.

Gevolgen. Voor alle a, b, c in $\mathbf{Z}$ geldt
(G1) als $c|a$ en $c|b$, dan $c|(a, b)$,
(G2) als $a|c, b|c$ en $(a, b) = 1$, dan $ab|c$,
(G3) als $a|bc$ en $(a, b) = 1$, dan $a|c$,
(G4) als $c = (a, b)$ dan $(\frac{a}{c}, \frac{b}{c}) = 1$.

Bewijs. (G1) Er bestaan $x, y \in \mathbf{Z}$ met $xa + yb = (a, b)$. Volgens (D3) geldt $c|xa$ en $c|yb$ en volgens (D1) dan ook $c|xa + yb = (a, b)$.
(G2) Volgens Stelling 1.2. zijn er $x, y \in \mathbf{Z}$ met $xa + yb = (a, b) = 1$. Dus $acx + bcy = c$. Volgens (D3) geldt $ab|acx$ en $ab|bcy$ en uit (D1) volgt daaruit dat $ab|c$.
(G3) Kies $x, y \in \mathbf{Z}$ met $xa + yb = (a, b) = 1$. Dan $acx + bcy = c$. Er geldt $a|acx$ en $a|bcy$. Dus $a|c$.
(G4) Kies $x, y \in \mathbf{Z}$ met $xa + yb = c$. Dan volgt $x\frac{a}{c} + y\frac{b}{c} = 1$. Elke gemene deler van $\frac{a}{c}$ en $\frac{b}{c}$ deelt dus 1. □

Waarschuwing. Er hoeft niet te gelden dat $(\frac{a}{(a,b)}, b) = 1$.
Neem maar $a = 25, b = 10$.

1.3 Een algoritme voor een rekenapparaat (AO)

Op de rekenmachine is het algoritme van Euclides heel snel met de hand als volgt uit te voeren. Voer a/b in, trek het stuk voor de decimale punt af en druk op de x^{-1} knop, trek het stuk voor de decimale punt af en druk op de x^{-1} knop, ga zo door tot je een geheel getal krijgt. De getallen die je afgetrokken hebt zijn de q's. Vanwege afrondfouten werkt dit alleen voor niet al te grote a en b en moet je stoppen als je een getal vindt dat bijna geheel is.

Als je met gehele getallen (tussen 0 en 10^{10} of zo) werkt, heb je geen last van afrondfouten.

Op een programmeerbare rekenmachine is de berekening van $\mathrm{ggd}(a,b)$ en van oplossingen x, y van $ax+by=\mathrm{ggd}(a,b)$ in een klap uit te voeren. Daarbij is het wel nuttig te beschikken over een Int (naar beneden op een geheel getal afronden, zg. *entier* nemen) of Rnd (gewoon afronden) knop, verder over acht geheugenplaatsen en "als" optie. Noem die geheugenplaatsen a, b, q, r, x, y, u, v. Voer a en b in, kies $x=0, y=1, u=1, v=0$ en doe:

$$\begin{array}{lll} A: & q := \mathrm{Int}\frac{a}{b}(\text{of } \mathrm{Rnd}\frac{a}{b}); & a-qb=:r; \\ & u-qx=:a;\ x=:u; & a=:x; \\ & v-qy=:a;\ y=:v; & a=:y; \\ & b=:a;\ r=:b, & \text{als } |b|>.0001 \text{ ga naar } A; \end{array}$$

B : print (a), print (u); print (v); print (x); print (y).

Het eerst geprinte getal is $\mathrm{ggd}(a,b)$, het tweede en derde geprinte getal is x resp. y met $ax+by=\mathrm{ggd}(a,b)$, de absolute waarden van het vierde en vijfde geprinte getal zijn de noemer resp. teller van de vereenvoudige breuk van $|a/b|$.

Opgave: Ga na dat de geprinte getallen inderdaad de genoemde waarden aangeven; vergelijk automaatberekeningen met enkele berekeningen met de hand (en hoofd).

1.4 Representatie van getallen in het g-tallig stelsel.

We zijn gewend getallen 'tientallig' of 'decimaal' te schrijven. Met 3507 bedoelen we $3\times10^3+5\times10^2+0\times10^1+7\times10^0$. Mogelijke cijfers zijn $0, 1, ..., 9$ en de plaats van het cijfer bepaalt de waarde. Het idee om de plaats van een cijfer de waarde te laten bepalen en daarbij nullen te gebruiken danken we aan de Arabieren. Het is veel handiger dan de systemen gebruikt door de oude Egyptenaren, Grieken en Romeinen. De keuze van het getal 10 is vrij willekeurig. Het positiesysteem kun je voor elk natuurlijk getal $g>1$ toepassen. Het getal g heet dan de *basis*. Computers werken vaak met een basis die een macht van 2 is. De 2-adische getallen worden *binaire getallen* genoemd.

Stelling 1.3. Stel $g \in \mathbf{N}, g \geq 2$. Bij elk natuurlijk getal n bestaat een $t \in \mathbf{Z}, t \geq 0$ en cijfers $a_0, a_1, ..., a_t \in \mathbf{Z}$ met $0 \leq a_j < g$ voor alle j en $a_t \neq 0$ zó dat

$$n = a_t g^t + a_{t-1} g^{t-1} + ... + a_0.$$

De cijfers $a_t, a_{t-1}, ..., a_0$ zijn éénduidig bepaald.

We noemen $(a_t, a_{t-1}, ..., a_0)_g$ de *g-tallige schrijfwijze* van n.

Bewijs. Door deling met rest herhaaldelijk toe te passen krijgen we

$$\begin{array}{ll} n = A_1 g + a_0, & 0 \leq a_0 < g, \quad A_1 > 0, \\ A_1 = A_2 g + a_1, & 0 \leq a_1 < g, \quad A_2 > 0, \\ A_2 = A_3 g + a_2, & 0 \leq a_2 < g, \quad A_3 > 0, \\ \dots\dots\dots\dots\dots\dots & \\ A_t = A_{t+1} g + a_t, & 0 \leq a_t < g. \end{array}$$

Omdat $g \geq 2$, geldt $n > A_1 > A_2 > ... \geq 0$ en moet er een t komen met $A_{t+1} = 0$. Dan volgt

$$n = a_0 + a_1 g + a_2 g^2 + ... + a_t g^t.$$

We tonen nu aan dat de schrijfwijze uniek is.
Stel dat ook $n = b_0 + b_1 g + b_2 g^2 + ... + b_s g^s$ met $b_j \in \{0, 1, ..., g-1\}$ voor alle j. Kies de kleinste k met $a_k \neq b_k$. Dan volgt door aftrekken:

$$(b_k - a_k) g^k = (a_{k+1} - b_{k+1}) g^{k+1} + (a_{k+2} - b_{k+2}) g^{k+2} + ... \text{ met } 0 < |b_k - a_k| < g.$$

Het rechterlid is deelbaar door g^{k+1}, het linkerlid dus ook. Dus $b_k - a_k$ is deelbaar door g, in tegenspraak met $0 < |b_k - a_k| < g$. $\square$

Voorbeeld. Schrijf 500 in het drietallig stelsel.

$$\begin{array}{rcl} 500 & = & 166 \times 3 + 2 \\ 166 & = & 55 \times 3 + 1 \\ 55 & = & 18 \times 3 + 1 \\ 18 & = & 6 \times 3 + 0 \\ 6 & = & 2 \times 3 + 0 \\ 2 & = & 0 \times 3 + 2 \end{array}$$

Dus $500 = (200212)_3$.

Voorbeeld. Vermenigvuldig $(2475)_8$ en $(6023)_8$.

```
    2475
    6023
    7667
   5172
17556
17637607
```

Het antwoord is dus $(17637607)_8$.

Optellen, aftrekken en vermenigvuldigen gaat analoog aan het decimale stelsel, zelfs deling met rest:

Voorbeeld. Pas deling met rest toe op $(24013)_5$ en $(1234)_5$.

```
1234/24013\14
     1234
     11123
     11101
        22
```

Dus $(24013)_5 = (14)_5 \times (1234)_5 + (22)_5$.

1.5 Priemgetallen.

Een *priemgetal* is een natuurlijk getal > 1 dat alleen 1 en zichzelf als positieve delers heeft. Een natuurlijk getal > 1 dat niet priem is, heet *samengesteld*.

In de volgende stelling en elders spreken we af dat het lege product gelijk is aan 1, en het product van één getal aan het getal zelf.

Stelling 1.4. Elk natuurlijk getal is het product van priemgetallen.

Bewijs. Met volledige inductie.
(a) Het getal 1 is het lege product.
(b) Stel de bewering is waar voor de natuurlijke getallen kleiner dan n. Als n priem is, is n het product van één priemgetal, n zelf. Als n samengesteld is, heeft n een deler d met $1 < d < n$ wegens (D4). Zij $e = n/d$. Dan ook $1 < e < n$. Volgens de inductieveronderstelling zijn d èn e producten van priemgetallen, en dan dus ook $n = de$. $\square$

Een opmerkelijk feit is dat op volgorde na de priemontbinding van een natuurlijk getal uniek is.

Stelling 1.5. Elk natuurlijk getal kan, op volgorde na, maar op één manier geschreven worden als product van priemgetallen.

Bewijs. Stel de bewering is onjuist. Dan is er een natuurlijk getal met (tenminste) twee verschillende priemontbindingen. Wegens axioma (iv) is er een kleinste getal met deze eigenschap, $n(>1)$. Stel $n = p_1p_2...p_s = q_1q_2...q_t$ met $p_1, ..., p_s, q_1, ..., q_t$ priemgetallen en $q_1, q_2, ..., q_t$ geen "permutatie" van $p_1, p_2, ..., p_s$. Als een priemgetal p in beide ontbindingen voorkomt, kunnen we p overal uitdelen en vinden we het kleinere getal $\frac{n}{p}$ met twee echt verschillende ontbindingen: $\frac{n}{p} = p_1p_2... * ...p_s = q_1q_2... * ...q_t$. ($*$ betekent dat een factor p is weggelaten).
We concluderen dat $p_1, p_2, ..., p_s$ en $q_1, q_2, ..., q_t$ geen priemgetal gemeen hebben. Dit houdt in dat $\text{ggd}(p_1, q_j) = 1$ voor $j = 1, ..., t$. We passen nu eigenschap (G3) herhaaldelijk toe: Er geldt $p_1|q_1(q_2...q_t)$ en $(p_1, q_1) = 1$. Dus $p_1|q_2...q_t$. Omdat $(p_1, q_2) = 1$, geldt dan $p_1|q_3(q_4...q_t)$. Na $t-1$ keer vinden we $p_1|q_t$. Dit is een tegenspraak met $(p_1, q_t) = 1$. □

Euclides bewees al dat er oneindig veel priemgetallen bestaan:

Stelling 1.6. Er bestaan oneindig veel priemgetallen.

Bewijs. Stel er zijn maar eindig veel priemgetallen, $p_1, p_2, ..., p_r$. Beschouw het getal $p_1p_2...p_r + 1 =: N$.
Uit (D1) volgt dat N niet deelbaar is door $p_1, p_2, ..., p_{r-1}$ of p_r, want $N - p_1p_2...p_r = 1$. Omdat $N > 1$, is dit in tegenspraak met Stelling 1.4. □

1.6 Meer over priemgetallen (AO)

Stelling 1.4 heeft een analogon voor vele andere verzamelingen, in tegenstelling tot Stelling 1.5. Beschouw bijv. de rij $1, 5, 9, 13, 17, 21, ...$ van getallen > 0 die rest 1 bij deling door 4 hebben. Je kunt het bewijs van Stelling 1.4 toepassen. Hierbij zijn $1, 5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, ...$ priemen. De priemontbinding is echter niet eenduidig, want $441 = 9 \times 49 = 21 \times 21$ heeft twee verschillende ontbindingen in priemen.

De "Laatste stelling van Fermat" zegt dat er geen natuurlijke getallen $n \geq 3, x, y, z$ bestaan met $x^n + y^n = z^n$. Deze bewering werd door Fermat (1601-1665) in een boek geschreven met de aantekening dat hij een bewijs had dat niet in de marge paste. Het boek werd na Fermat's dood gevonden en niemand kon een bewijs voor de bewering vinden. Euler (1707-1783) bewees vele uitspraken van Fermat, maar niet deze. In de 18de en 19de eeuw claimden verschillende mensen een bewijs te hebben, waarbij soms hun fout bleek te zijn dat ze dachten dat Stelling 1.5 waar is voor algebraïsche getallenlichamen. Uiteindelijk heeft A. Wiles (1953 -) in samenwerking met R. Taylor (1962 -) in 1995 een bewijs gevonden dat van diepe algebra, getaltheorie en meetkunde gebruikt maakt en meer dan 100 blz. omvat. Een bewijs dat in de marge van een blad van een boek past is nog niet gevonden. Een open vermoeden is dat er geen natuurlijke getallen l, m, n alle ≥ 3 en x, y, z met $\text{ggd}(x, y, z) = 1$ bestaan zó dat $x^l + y^m = z^n$. Dit heeft Fermat's laatste stelling als speciaal geval $l = m = n$. Een ander speciaal geval is dat er geen machten y^m, z^n met $m \geq 3, n \geq 3$ bestaan die 1 verschillen (vermoeden van Catalan, 1842) (neem $x = 1, l = 3$).

Veel vragen over priemgetallen zijn nog onbeantwoord, *open*, bijv.

1. (Priemgetaltweelingen.) Bestaan er oneindig veel priemgetallen p zó dat $p + 2$ een priemgetal is ? (Voorbeelden: $p = 5, 17, 101$.)
2. Bestaan er oneindig veel priemgetallen zó dat $p - 1$ een kwadraat is? (Voorbeelden: $p = 5, 17, 101$.)
3. (Mersennepriemgetallen, naar Mersenne (1588-1648)). Bestaan er oneindig veel priemgetallen p zó dat $p + 1$ een macht van 2 is? (Voorbeelden: $p = 3, 7, 127, 2^{3021377} - 1$).
4. (Goldbach, 1690-1764) Is elk even getal groter dan 2 de som van twee priemgetallen?

Literatuur bij dit hoofdstuk:

F. Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, Utrecht, 1999.

L.K. Hua, *Introduction to the Theory of Numbers*, Springer-Verlag.

G.H. Hardy & E.M. Wright, *Introduction to the Theory of Numbers*, Clarendon Press, Oxford 1938.

O. Ore, *Number Theory and its History*, Dover, 1988.

L. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag, 1979, Part I.

Opgaven bij Hoofdstuk 1. Gehele getallen.

1.1 Bewijs met volledige inductie dat

a) $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{1}{6}n(n+1)(2n+1)$

b) $1^3 + 2^3 + 3^3 + ... + n^3 = (\frac{1}{2}n(n+1))^2$.

1.2. Bewijs met volledige inductie dat voor $a \neq 1$

$$1 + a + a^2 + ... + a^n \;=\; \frac{a^{n+1}-1}{a-1}.$$

1.3. De binomiaalcoëfficiënt $\binom{n}{k}$ is gedefinieerd als

$$\frac{n!}{k!(n-k)!} \quad \text{waarbij} \quad n! \;=\; 1 \times 2 \cdots \times n$$

als n en k gehele getallen zijn met $0 \leq k \leq n$; als $k < 0$ of $k > n$ is de binomiaalcoëfficiënt gelijk aan 0.

a) Ga na dat

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

voor alle gehele getallen n en k.

b Bewijs met volledige inductie dat $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

1.4 a) Bewijs (D2) and (D3).

b) Bewijs voor $a, b \in \mathbf{Z}$ en $d, q \in \mathbf{N}$ dat als d een deler is van a en b, d ook een deler is van $a - qb$ en van $a + qb$.

c) Bewijs (D5).

1.5. Bereken (a, b) en schrijf deze als lineaire combinatie van a en b voor de volgende paren (a, b):

(i) $(681, 361)$, (ii) $(2047, 3649)$, (iii) $(12345, 54321)$.

1.6. Bewijs: $ax + by = c$ heeft een oplossing $x, y \Longleftrightarrow (a, b)|c$.

1.7. Bewijs: als $a|c$ en $b|c$, dan $\text{kgv}(a, b)|c$.

1.8. Bepaal a) ggd $(2^{250}-1, 2^{100}-1)$.
b) ggd $(3^{48}-1, 3^{32}-1)$.

1.9.a) Schrijf 500 uit in het tweetallig, vijftalig en zeventallig stelsel.

b) Schrijf de volgende getallen uit in het decimale stelsel:

$(17538)_9, (24ADE)_{16} \quad (A=10, B=11, C=12, D=13, E=14, F=15)$

1.10. Voer de volgende berekeningen uit in het negentallig stelsel:

$$(1357)_9 \times (7531)_9, \quad (857)_9 : (77)_9.$$

1.11. Voer de volgende berekeningen uit in het dertientallig stelsel:
$(A=10, B=11, C=12)$
$(7BC)_{13} + (CBA8)_{13}, \qquad (ABCAB)_{13} \times (BCA)_{13}$.

1.12. Laat zien dat er oneindig veel priemgetallen zijn die bij deling door 4 rest 3 geven.

1.13a) Laat zien: als $a^n - 1$ een priemgetal is en $n > 1$, dan is a gelijk aan 2 en n zelf een priemgetal.

b) Zoek een priemgetal p zó dat $2^p - 1$ niet priem is.

1.14. Bepaal het enige priemgetal p zó dat $p+2$ en $p+4$ ook priem zijn; laat zien dat p uniek is.

1.15. Stel $a = p_1^{k_1} \ldots p_r^{k_r}$ en $b = p_1^{l_1} \ldots p_r^{l_r}$ met $p_1 < p_2 \ldots < p_r$ priemgetallen en $k_1, \ldots, k_r, l_1, \ldots, l_r \in \mathbf{Z}_{\geq 0}$.

a) Druk (a,b) uit in $p_1, \ldots, p_r, k_1, \ldots, k_r, l_1, \ldots, l_r$.

b) Druk $[a,b]$ uit in $p_1, \ldots, p_r, k_1, \ldots, k_r, l_1, \ldots, l_r$.

c) Bewijs m.b.v. a) en b) dat $(a,b) \times [a,b] = ab$.

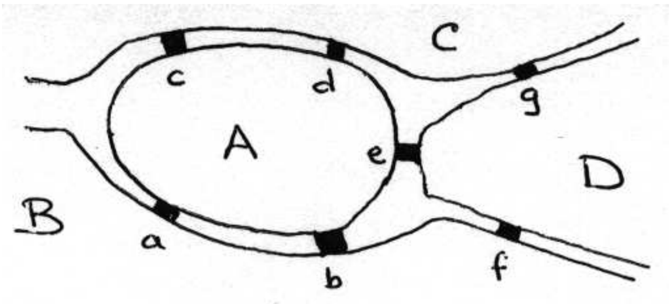
2 HOOFDSTUK: GRAFENTHEORIE

2.1 Inleiding.

Een *graaf* bestaat uit een aantal *(knoop)punten* en een aantal verbindingen tussen twee knooppunten, zg. *takken*. Een tak wordt aangegeven met de twee knooppunten die ze verbindt; de verdere ligging speelt geen rol.

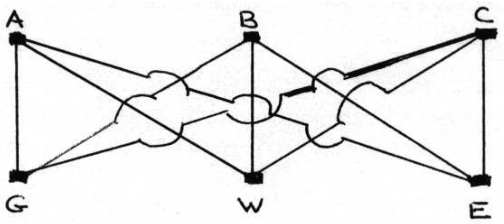
Sommige problemen kunnen op natuurlijke wijze in termen van grafen gesteld worden. Ik geef enkele voorbeelden.

Voorbeeld 1: Het Bruggenprobleem van Euler (1736)
Door de plaats Königsbergen stroomt de rivier de Pregel. Deze rivier splitst zich waardoor een eiland ontstaat. De vier delen van de stad zijn verbonden door bruggen. In 1736 vroeg de beroemde wiskundige Leonard Euler zich af of het mogelijk was om een wandeling te maken, waarbij iedere brug precies éénmaal wordt gepasseerd. (Je mag zelf kiezen waar je begint en eindigt).

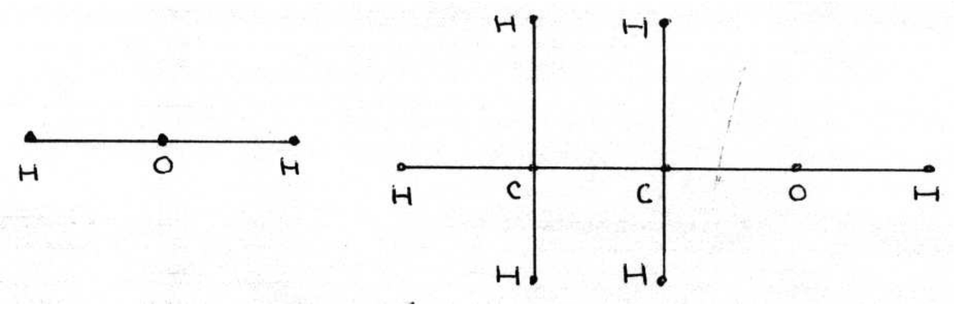


Hoofdletters voor stadsdelen, kleine letters voor bruggen.

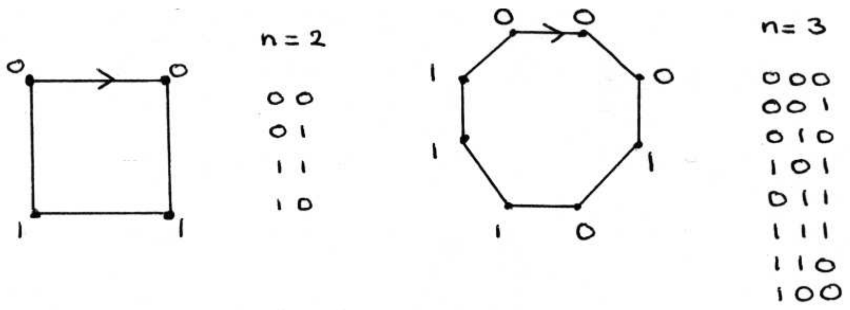
Voorbeeld 2: Het $(3,3)$-probleem.
Drie huizen (A, B, C) moeten verbonden worden met drie nutsbedrijven (G,W,E). Is het mogelijk de huizen zo aan te sluiten dat de verbindingen elkaar niet snijden?



Voorbeeld 3: Moleculen.
Een molecuul bestaat uit een aantal atomen verbonden door chemische bindingen.Dit kunnen we voorstellen door een graaf. Hieronder staan de grafen voor water (H_2O)en voor ethanol (C_2H_5OH). Elke C heeft vier takken, elke O twee en elke H één. Hoeveel verschillende grafen zijn mogelijk met twee atomen C, zes atomen H en één atoom O?



Voorbeeld 4: Kring van binaire getallen.
Bestaat er een kring van 2^n nullen en enen zó dat er 2^n verschillende getallen van n bits ontstaan als je op alle mogelijke plaatsen start met lezen in een bepaalde richting?



Voorbeeld 5: Vierkleurenprobleem (1852)
In een landkaart wordt elk land begrensd door aaneengesloten lijnstukken (geen enclaves e.d.). Is het mogelijk de kaart zo met vier kleuren te kleuren dat elk paar landen met een gemeenschappelijke grens verschillende kleuren hebben?

Dit probleem is in 1976 met grafentheorie en uitgebreid computergebruik opgelost door Appel en Haken.

Op natuurlijke wijze kom je ertoe te vragen wat het kleinste aantal kleuren is waarmee knooppunten van een graaf zo gekleurd kunnen worden dat knooppunten die door een tak verbonden zijn verschillende kleuren hebben. We noemen dat getal het *kleurgetal* van een graaf.

Voorbeeld 6:Het handelsreizigersprobleem ($\leq$ 1832).
Er zijn n steden met bekende afstand tussen elk paar steden. Het probleem is een rondreis langs alle steden te maken zó dat de totale reisafstand minimaal is.

In 1954 kon men dit oplossen voor 20 steden, in 1984 is een voorbeeld opgelost van 318 steden. In 1997 is er een probleem van 3038 steden opgelost. (Het laatste probleem kwam uit een technisch probleem om met een laser gaatjes op een printplaat te maken en de totale verplaatsing te minimaliseren.) De verbetering is te danken aan sterk verbeterde wiskundige technieken en sterk verbeterde computerapparatuur.

Als we deze uiteenlopende voorbeelden vergelijken, zien we allereerst dat we *gemodelleerd* hebben. We hebben geen rekening gehouden met de vorm van de bruggen in Königsbergen, de grootte van de huizen in voorbeeld 2, het gewicht van de atomen in voorbeeld 3, enz., omdat die voor de probleemstelling niet ter zake deden. We hebben een *wiskundig model* gemaakt waarbij in alle gevallen grafen betrokken waren en geen essentiële informatie verloren is gegaan.

We kunnen grafentheorie toepassen om de problemen op te lossen. Daarbij blijken voorbeelden 1 en 4 tot een verwant probleem te leiden, terwijl ook 2 en 5 met elkaar te maken hebben. Het tweedejaarscollege Discrete Wiskunde, voor elke wiskundestudent verplicht, bevat een inleiding in de grafentheorie. Een grondige behandeling volgt in het niet-verplichte derde/vierdejaarscollege Grafentheorie. Wat wel duidelijk is, is dat vraagstellingen soms verschillende behandelingen vereisen. Voorbeeld 2 vereist een *bewijs* dat iets niet kan. 'Ik kan het niet vinden' of 'Dat zie je toch zo' is niet genoeg. Verlangd wordt een sluitende redenering te geven die niemand redelijkerwijs kan tegenspreken. Ook voorbeelden 4 en 5 vragen om een bewijs. We zullen in secties 2 en 3 zulke bewijsmethoden behandelen.

Bij voorbeeld 6 is het duidelijk dat er een kleinste afstand is. Het gaat erom die te vinden. Ook bij voorbeeld 5 is het interessant te weten hoe je met vier kleuren kan kleuren, en bij voorbeeld 4 hoe je de kring van cijfers construeert. Daarvoor heb je *een algoritme* nodig, een rij regels volgens welke je (eventueel met een computer) de gezochte oplossing vindt.

Wij zullen nu niet een algoritme geven om het handelsreizigersprobleem op te lossen, maar wel een om een redelijk goede benadering te vinden, een zg. *heuristiek*.

Invoegheuristiek voor het handelsreizigersprobleem.

[stap 1] Kies een beginstad uit. Noem die S, de andere steden T.
[stap 2] Zoek de kortste verbinding tussen een stad uit S en één uit T, zeg stad x.
[stap 3] Haal x uit T weg en voeg x aan S toe. Voeg x zo zuinig mogelijk in de reeds gevonden route in en bereken de nieuwe reisafstand.
[stap 4] Ga naar stap 2 als T nog steden bevat. Stop anders.

Voorbeeld.

	A	B	C	D	E	F
A	–	35	43	23	33	19
B	35	–	47	42	21	26
C	43	47	–	36	31	30
D	23	42	36	–	50	17
E	33	21	31	50	–	45
F	19	26	30	17	45	–

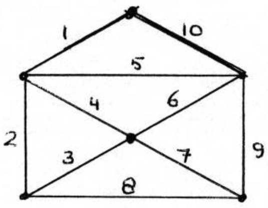
$S = (a, b, c)$ betekent route $a \to b \to c \to a$

1) Neem A.
2) $x = F$ 3) $S = (A, F)$, met afstand = 38
2) $x = D$ 3) $S = (A, F, D)$, met afstand = 59
2) $x = B$ 3) $S = (A, B, F, D)$, met afstand = 101
2) $x = E$ 3) $S = (A, E, B, F, D)$ met afstand = 120
2) $x = C$ 3) $S = (A, C, E, B, F, D)$, met afstand = 161

2.2 Eulerse kringen.

We zullen een stelling bewijzen die ons in staat stelt om voor elke stad te bepalen of het bruggenprobleem voor die stad oplosbaar is. In het bewijs wordt een variant van volledige inductie gebruikt, nl. dat elke verzameling van natuurlijke getallen een kleinste heeft. Zij G een graaf met knooppunten $v_1, ..., v_n$ en takken $e_1, ..., e_m$ waarbij elke e_i staat voor een paar knooppunten (v_k, v_l). Een *keten* is een rijtje onderling verschillende takken $d_1, ..., d_s \in \{e_1, ..., e_m\}$ waarbij een knooppunt van d_1 gelijk is aan een knooppunt van d_2, het andere knooppunt van d_2 gelijk is aan een knooppunt van $d_3, ...,$ het andere knooppunt van d_{s-1} gelijk is aan een knooppunt van d_s. Als bovendien het andere knooppunt van d_s gelijk is aan het andere knooppunt van d_1, heet de keten een *kring*. Een graaf heet *samenhangend* als elk paar knooppunten verbonden is door een keten. Een keten of kring heet *eulers* als elke tak van G erin voorkomt.

Voorbeeld



G is samenhangend. Kringen worden gegeven door $2, 3, 4$ en $2, 8, 9, 6, 4, 5, 10, 1$, maar deze kringen zijn niet eulers. Er is wel een eulerse keten: $2, 1, 10, 5, 4, 6, 9, 7, 3, 8$.

Stelling 2.1. (Euler) *Een samenhangende graaf heeft een eulerse kring als en alleen als in elk knooppunt een even aantal takken uitkomt.*

We zeggen dat de *graad* van het knooppunt even moet zijn.

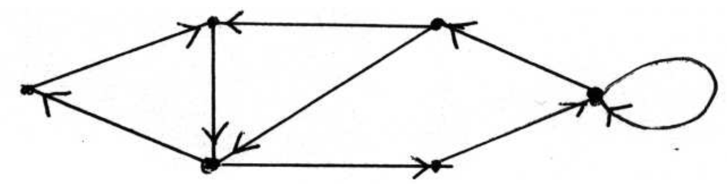
Bewijs. Enerzijds: bij een kring is elk knooppunt even vaak het eindpunt van een tak als het beginpunt. Omdat alle doorlopen takken verschillend zijn, moet het aantal keren dat een knooppunt als grenspunt van een tak fungeert even zijn.
Anderzijds: Beschouw alle mogelijke kringen en tel voor elk het aantal niet doorlopen takken. Dat is een natuurlijk getal of 0. Als het 0 is, heb je een eulerse kring en ben je klaar. Anders heb je een verzameling natuurlijke getallen en kies je het kleinste met bijbehorende kring. Die kring is dus de kring met de meeste takken.

Stel de kring begint in v_1 en tak $e_m = (v_i, v_j)$ wordt niet doorlopen. Vanwege de samenhang is er een keten beginnend in v_1 en eindigend in v_i. Doorloop de keten zolang je takken tegenkomt die ook tot de langste kring behoren. Noem het eindpunt van deze keten v. Je kunt even goed de kring doorlopen beginnend in v (en dan ook eindigend in v). Maar nu kun je een tak verder lopen langs een nog niet belopen tak. Zolang als deze tak niet in v eindigt, maar bijvoorbeeld in knooppunt w, kun je verder wandelen langs een nog ongebruikte tak, omdat elk knooppunt een even aantal keren grenspunt van een tak is en w een oneven aantal keren in de verlengde keten is opgetreden. Omdat het aantal takken eindig is, moet hier een einde aan komen en dat kan alleen doordat je in v uitkomt. Op dat moment heb je echter een langere kring gevonden dan de maximale en dat is een tegenspraak. $\square$

2.3 Gerichte grafen.

Tot nog toe hebben we zg. ongerichte grafen bestudeerd. In deze sectie zullen we gerichte grafen (directed graphs) bespreken. Bij een *gerichte graaf* heeft elke tak een richting waardoor een uiteinde van de tak *beginpunt* en het andere *eindpunt* wordt. Bij een *keten* in een gerichte graaf wordt geeist dat het eindpunt van de vorige tak gelijk is aan het beginpunt van de volgende tak en ook weer dat geen enkele tak meer dan eens doorlopen wordt. Takken mogen dus niet in de verkeerde richting doorlopen worden. Een *kring* in een gerichte graaf is een keten waarvan het allereerste beginpunt gelijk is aan het allerlaatste eindpunt. Een gerichte graaf heet *samenhangend* als je van elk punt naar elk ander punt kunt lopen langs een keten. Een keten of kring in een gerichte graaf heet *eulers* als elke tak erin voorkomt.

Voorbeeld.



Deze gerichte graaf is samenhangend, maar niet eulers.

Stelling 2.2. (Euler) *Een samenhangende graaf heeft een eulerse kring als en alleen als elk knooppunt evenvaak beginpunt als eindpunt is.*

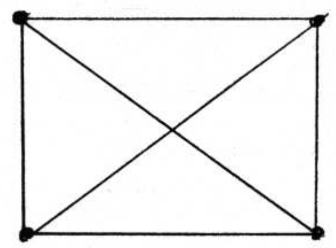
Bewijs. Analoog aan het bewijs van Stelling 2.1. Opgave.

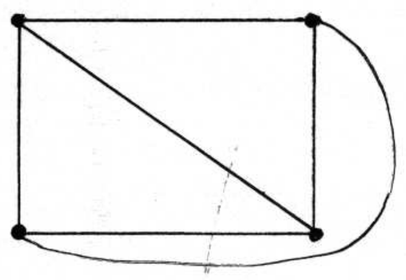
Door Stelling 2.2 toe te passen kun je bewijzen dat het antwoord op de vraag uit Voorbeeld 4 voor elk natuurlijk getal bevestigend is.

2.4.Vlakke grafen.

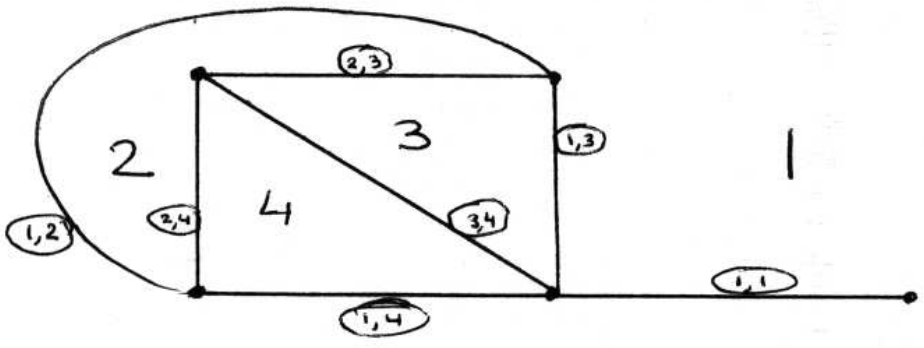
Een (ongerichte) graaf G met verzameling V van knooppunten en takken E heet *vlak* (planar) als G in het platte vlak getekend kan worden zó dat de takken elkaar niet snijden. (Ze mogen wel eindpunten gemeen hebben.)

Dus onderstaande graaf G is vlak, want hij heeft een vlakke representatie (vgl. rechts)





Een vlakke representatie van een graaf noemen we plat (plane). Een platte graaf verdeelt het platte vlak in gebieden, het buitengebied meegeteld. Elke tak is grenslijn van twee gebieden. Het kan gebeuren dat die twee gebieden hetzelfde zijn.



Euler (1707-1783) bewees een formule voor veelvlakken die we later zullen tegenkomen en die het volgende analogon heeft voor grafen:

Stelling 2.3. Een platte, samenhangende graaf met n knooppunten, m takken en r gebieden voldoet aan

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

Bewijs. Stel er is een kring in de graaf. Laat dan één tak uit de kring weg. Dan worden m en r één kleiner en verandert de waarde $n - m + r$ dus niet. (In feite is het $n - (m - 1) + (r - 1)$.) Als er nog een kring is in de nieuwe graaf, herhaal je het procédé. Uiteindelijk krijg je een samenhangende graaf zonder kringen, een zg. *boom*. Voor die boom geldt $r = 1$ en $m = n - 1$, zoals gemakkelijk met volledige inductie naar n is na te gaan. Hieruit volgt $n - m + r = n - (n-1) + 1 = 2$. Voor de oorspronkelijke graaf geldt dus ook $n - m + r = 2$. □

Toepassing. Probleem 2 is niet oplosbaar.
Stel nl. dat er wel een oplossing is. Dan heb je een platte graaf met $n = 6$ en $m = 9$. Uit de stelling volgt dat $r = 5$. In dit geval hebben we een zogenaamde *bipartiete graaf*, d.w.z. dat de knooppunten in twee verzamelingen uiteenvallen die onderling niet verbonden zijn. Er zijn dan geen gebieden met drie grenstakken. Ieder gebied heeft dan minstens vier grenstakken. Dus het aantal takken, dubbel geteld, is tenminste 20. Dan volgt $m \geq 10$, terwijl $m = 9$. □

Bij het tweedejaarscollege Discrete Wiskunde wordt een kriterium gegeven om te beslissen of een gegeven graaf vlak is of niet.

Literatuur

[1] R.J. Wilson, *Introduction to Graph Theory*, Longman, 1985

[2] R.J. Wilson & J.J. Watson, *Graphs, an Introductory Approach*, Wiley, 1990

Opgaven bij Hoofdstuk 2. Grafentheorie.

2.1a) Maak een graaf met knooppunten A, B, C, D die de essentie van het bruggenprobleem van Euler weergeeft;

b) Ga na of er een oplossing is.

2.2. Laat zien dat er bij vier huizen en twee nutsbedrijven wel een kruisingsloze wijze is om de leidingen te leggen.

2.3. Er bestaan twee verschillende moleculen met formule C_4H_{10} (zg. isomeren). Geef voor beide een graafrepresentatie. Beargumenteer dat de grafen essentieel verschillend zijn.

2.4a) Laat zien dat in een graaf het aantal knooppunten met oneven graad even is.

b) Bewijs: een samenhangende graaf heeft een eulerse keten als en alleen als er ten hoogste twee knooppunten met oneven graad zijn.

2.5a) Geef een oplossing van het kringenprobleem voor $N = 4$.

b) Formuleer het probleem in grafentaal (rijtjes van n worden knooppunten, rijtjes van $n + 1$ worden takken)

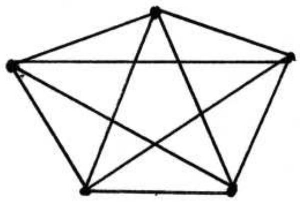
c) Bewijs Stelling 2.2.

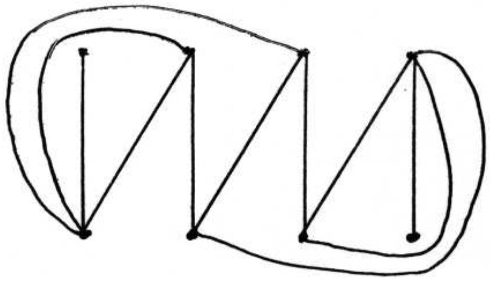
2.6. Een dominospel bestaat uit stenen met aan beide zijden een getal uit $\{0, 1, 2, 3, 4, 5, 6\}$ waarbij elke combinatie één keer voorkomt.

a) Hoeveel stenen telt het dominospel?

b) De stenen worden zo op een rij geplaatst dat alleen gelijke getallen tegen elkaar gelegd worden. Bewijs dat het mogelijk is om alle stenen zo op een rij te leggen en dat in dat geval de waarden aan de uiteinden aan elkaar gelijk zijn.

2.7. Bepaal de kleurgetallen van de volgende grafen:





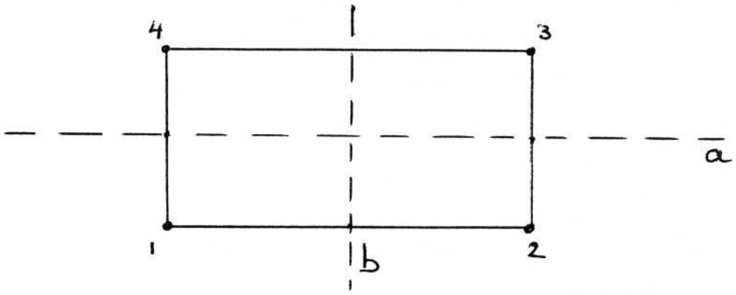
2.8. Pas de invoegheuristiek toe op de volgende afstandstabel:

	A	B	C	D	E	F
A	–	35	43	12	33	39
B	35	–	47	42	41	26
C	43	47	–	36	31	30
D	12	42	36	–	30	27
E	33	41	31	30	–	43
F	39	26	30	27	43	–

3 HOOFDSTUK: PERMUTATIES

3.1 Isometrieën.

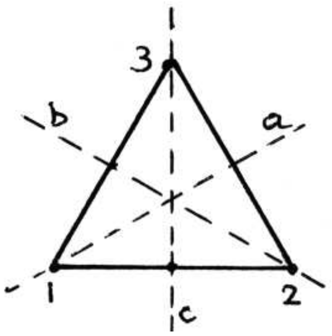
Beschouw een rechthoek die geen vierkant is.



Er zijn vier manieren om de figuur op zichzelf af te beelden zó dat de afstanden gelijk blijven, namelijk spiegelen om de assen a en b, draaien over 180° en niets doen. We kunnen deze afbeeldingen noteren door te zeggen wat er met de hoekpunten gebeurt:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

Zo'n afbeelding noemen we een *isometrie*. Bij een gelijkzijdige driehoek, vinden we zes isometrieën.



$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$
identieke afb.

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$
draaiing over 120°

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
draaiing over 240°

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$
spiegeling om c

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$
om a

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$
om b

We voeren de cykelnotatie in om isometrieën korter te kunnen noteren.
(abc) betekent $a \to b \to c \to a$, dus

$$\begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix}.$$

Voor de gelijkzijdige driehoek vinden we in dezelfde volgorde $\begin{array}{ccc} (1) & (123) & (132) \\ (12) & (23) & (13). \end{array}$
We laten bijna steeds onveranderde elementen ongenoemd. Bij de rechthoek krijgen we in cykelnotatie:

(1) (14)(23) (12)(34) (13)(24)

We noemen $(a_1 a_2 \ldots a_k)$ een cykel van *lengte* k.

Voorbeelden van isometrieën in de $\mathbf{R}^n$ zijn spiegelingen, *rotaties* (draaiingen) en *translaties* (verschuivingen). Elke figuur heeft de identieke afbeelding als isometrie, notatie (1) of e. Hoe symmetrischer een figuur, des te meer isometrieën.

Beschouw een veelhoek of veelvlak met hoekpunten $1, 2, \ldots, n$. We vatten de isometrie op als een functie op de verzameling $\{1, 2, \ldots, n\}$. We noemen de functie *injectief* omdat elk paar hoekpunten verschillende beelden heeft, en *surjectief* omdat elk hoekpunt in het beeld voorkomt. Afbeeldingen die injectief èn surjectief zijn heten *bijectief*. Elke isometrie is dus een bijectie.

De samenstelling van twee isometrieën σ en τ krijgen we door eerst σ toe te passen en dan τ, notatie $\tau \circ \sigma$. Is bijvoorbeeld $\sigma = (12)(34)$ en $\tau = (14)(23)$, dan vinden we $\tau \circ \sigma = (13)(24)$, immers

$$[1\ 2\ 3\ 4] \xrightarrow{\sigma} [2\ 1\ 4\ 3] \xrightarrow{\tau} [3\ 4\ 1\ 2].$$

De volgorde is van belang. Immers als $\sigma = (12)$ en $\tau = (123)$, dan geldt $\tau \circ \sigma = (13)$, maar $\sigma \circ \tau = (23)$. Voor elke isometrie σ geldt: $\sigma \circ e = e \circ \sigma = \sigma$. Ook heeft elke isometrie σ een *inverse* σ^{-1} met de eigenschap

$$\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = e.$$

Je vindt σ^{-1} door in de "rechte haken notatie" bovenste en onderste rij te verwisselen. Je kunt een samenstellingstabel maken die aangeeft wat het effect van $\circ$ is. Bij de rechthoek vinden we bijvoorbeeld als $e = (1)$, $a = (14)(23)$, $b = (12)(34)$, $d = (13)(24)$

$$\begin{array}{c|cccc} \tau & & & & \\ \sigma & e & a & b & d \\ \hline e & e & a & b & d \\ a & a & e & d & b \\ b & b & d & e & a \\ d & d & b & a & e \end{array}$$

3.2 Permutaties.

Elke isometrie is een permutatie. We gaan nu over het abstracte begrip permutatie praten en houden daarbij isometrieën als voorbeelden in gedachten.

Definitie. *Een permutatie σ is een bijectieve afbeelding van $\{1, 2, \ldots, n\}$ naar $\{1, 2, \ldots, n\}$. Notatie*

$$\begin{bmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{bmatrix}.$$

Stelling 3.1. Er zijn $n!$ permutaties van $1, 2, \ldots, n$.

Bewijs. Voor $\sigma(1)$ hebben we n mogelijkheden, waarvan er één benut wordt. Voor $\sigma(2)$ hebben we nog $n-1$ mogelijkheden, waarvan er weer één benut wordt. Zo doorgaande vinden we dat het totale aantal mogelijkheden gelijk is aan
$n(n-1)(n-2)\ldots 2 \cdot 1 = n!$ $\square$

Het is gemakkelijk na te gaan dat $n! > 2^n$ voor $n > 3$.

De verzameling van alle permutaties op $\{1, 2, \ldots, n\}$ noteren we met S_n. We kunnen twee permutaties σ en τ *samenstellen* door eerst σ toe te passen en dan τ, notatie $\tau \circ \sigma$. Het resultaat is een permutatie.
Bijvoorbeeld: als $\sigma = (1\ 2\ 3)(4\ 5)$ en $\tau = (1\ 4)(2\ 5)$, dan is $\tau \circ \sigma = (1\ 5)(2\ 3\ 4)$ en $\sigma \circ \tau = (1\ 5\ 3)(2\ 4)$.
De volgorde van samenstellen is dus van belang. Dit geldt natuurlijk alleen als eenzelfde element in verschillende cykels optreedt. Cykels heten *disjunct* als er geen getal is dat in beide voorkomt. Bij disjuncte cykels is de volgorde niet van belang.

Voor de identieke permutatie $e = (1)$ geldt dat elke $\sigma \in S_n$ voldoet aan

$$\sigma \circ e = e \circ \sigma = \sigma.$$

Verder heeft elke permutatie $\sigma \in S_n$ een *inverse permutatie* $\sigma^{-1} \in S_n$, d.w.z. dat

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e.$$

De inverse van de cykel $(a_1 a_2 \ldots a_k)$ is de cykel $(a_k a_{k-1} \ldots a_2 a_1)$. Als bij de isometrieën kan men een samenstellingstabel van S_n maken waarbij in elke rij en elke kolom elk element van S_n precies eenmaal voorkomt.

De volgende ontbindingsstelling lijkt op Stelling 1.5 waarbij (paarsgewijs disjuncte) cykels van lengte groter dan 1 de rol van de priemgetallen vervullen.

Herhalingen komen hier echter niet voor. We vatten (1) op als het lege product van cykels.

Stelling 3.2. Elke permutatie van $\{1, 2, \ldots, n\}$ kan geschreven worden als product van paarsgewijs disjuncte cykels van lengte > 1. Op volgorde na is de schrijfwijze éénduidig.

Voorbeeld. Zij $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 10 & 1 & 5 & 3 & 7 & 9 & 8 & 6 & 2 \end{bmatrix}$.

Er geldt $\sigma = (1\ 4\ 5\ 3)(2\ 10)(6\ 7\ 9)$.

'Op volgorde na' slaat zowel op de volgorde van de cykels als op de volgorde binnen de cykels. We beschouwen $(1\ 4\ 5\ 3)$, $(4\ 5\ 3\ 1)$, $(5\ 3\ 1\ 4)$ en $(3\ 1\ 4\ 5)$ als dezelfde cykel, maar deze zijn ongelijk aan $(1\ 5\ 3\ 4)$.

Bewijs van Stelling 3.2. Neem een element a_1. Schrijf $a_2 := \sigma(a_1)$, $a_3 := \sigma(a_2)$,..., totdat je een element tegenkomt dat al eerder opgetreden is. (Dit gebeurt omdat n eindig is.) Stel k is het kleinste getal met $\sigma(a_k) \in \{a_1, a_2, \ldots, a_k\}$. Als $\sigma(a_k) = a_j$ met $j > 1$, dan is $\sigma(a_k) = \sigma(a_{j-1})$ en is σ niet surjectief. Dus $\sigma(a_k) = a_1$ en we hebben een cykel $(a_1 a_2 \ldots a_k)$. Ga nu verder met de resterende elementen tot alle elementen in cykels ondergebracht zijn. Uit de constructie volgt dat de cykels disjunct zijn, dat daarom de volgorde van de cykels onbelangrijk is en dat σ gelijk is aan de samenstelling van de cykels. Laat nu cykels ter lengte 1 weg.
Stel σ heeft nog een andere schrijfwijze van het beschreven type. Als deze niet slechts in de volgorde verschilt, is er een cykel die in de ene representatie optreedt en in de andere niet. Dan moet er een element zijn dat in de ene representatie door een ander element gevolgd wordt dan in de andere representatie. Dan zijn de beelden van dat element en dus de gerepresenteerde permutaties verschillend. $\square$

Men kan permutaties ook op zichzelf toepassen. De notatie σ^k betekent σ k keer toegepast. Het kleinste positieve gehele getal k met $\sigma^k = e$ heet de *orde* van σ. Elke permutatie heeft een orde. De orde van de cykel $(a_1 \ldots a_k)$ is k. Immers, $\sigma^l(a_1) = a_{l+1}$ voor $l < k$ en $\sigma^k(a_j) = a_j$ voor elke j. Algemeen geldt:

Stelling 3.3. De orde van een permutatie is het kleinste gemene veelvoud van de lengtes van de cykels in zijn disjuncte-cykel-representatie.

Bewijs. Stel de permutatie is geschreven in zijn disjuncte-cykel-representatie. Als er een cykel is van lengte k, dan worden de betrokken elementen op zichzelf afgebeeld door σ^l als l door k deelbaar is en anders niet. De orde van σ is dus een veelvoud van alle cykellengtes, en elk gemeenschappelijk veelvoud van alle cykellengtes voldoet. Het kleinste gemene veelvoud is dus de orde van σ. $\square$

Voorbeeld. De orde van (1 4 5 3)(2 10)(6 7 9) is 12.

3.3 Het inversiegetal van een permutatie.

Het *inversiegetal* van een permutatie $\sigma \in S_n$ is het aantal paren i, j met $i < j$ en $\sigma(i) > \sigma(j)$. Voorbeeld: Het inversiegetal van $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{bmatrix}$ is 5.
In de lineaire algebra is het voor het berekenen van determinanten belangrijk te weten of het inversiegetal van een permutatie even of oneven is. Hier behandelen we een methode om dat snel te bepalen.

Een *paarwisseling* is een cykel van twee elementen. Elke cykel is te schrijven als product van paarwisselingen, want

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-2} a_{k-1})(a_{k-1} a_k).$$

Volgens Stelling 3.2 is dus ook elke permutatie het product van paarwisselingen. De schrijfwijze is niet éénduidig, want (1 2 5 4 3) = (1 2)(2 5)(5 4)(4 3) = (1 3)(1 4)(1 5)(1 2) = (2 3)(2 1)(1 4)(3 5)(2 3)(1 5). Zelfs het aantal paarwisselingen kan dus variëren. We zullen aantonen dat het aantal paarwisselingen van σ dezelfde *pariteit* heeft (d.w.z. tegelijk even/oneven is) als het inversiegetal van σ. Als het even is, noemen we σ *even*, anders noemen we σ *oneven*. Dus (1 2 5 4 3) is een even permutatie.

Stelling 3.4. Het inversiegetal van een permutatie heeft dezelfde pariteit als het aantal cykels in een schrijfwijze van de permutatie als product van paarcykels.

Bewijs. Het is voldoende aan te tonen dat het toevoegen van een paarwisseling de pariteit van het inversiegetal verandert. Elke paarwisseling is het product van een oneven aantal buurwisselingen. Bijvoorbeeld, als $a < b$, dan is $(b\ a) = (a\ b) = (b\ b-1)(b-1\ b-2) \dots (a+2\ a+1)(a+1\ a)(a+1\ a+2) \dots (b-2\ b-1)(b-1\ b)$. Het is dus voldoende te laten zien dat elke buurwisseling $(a\ a+1)$ de pariteit van het inversiegetal verandert.
Als je in een permutatie a en $a+1$ verwisselt, dan verandert er niets aan de paren waar a noch $a+1$ in voorkomt, verandert er niets aan het inversiegetal door paren waarin een $i \neq a, a+1$ voorkomt, omdat (i, a) en $(i, a+1)$

elkaars rol overnemen, en resteert dus alleen het paar $(a, a+1)$. Door de verwisseling verandert het inversiegetal met 1. Dus verandert de pariteit door de buurwisseling. $\square$

Voorbeeld. $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{bmatrix}$ heeft inversiegetal 4, en is dus even. Verwisselen we 4 en 5, dan krijgen we in plaats van de verkeerde paren $(2,1), (4,1), (4,3), (5,3)$ de verkeerde paren $(2,1), (5,1), (5,3), (4,3)$ en $(5,4)$. Het inversiegetal wordt dus 5, oneven.

Gevolg van Stelling 3.4. Het inversiegetal van een permutatie heeft dezelfde pariteit als het aantal cykels van even lengte in haar disjuncte-cykel-notatie.

Bewijs. Uit $(a_1a_2 \ldots a_k) = (a_1a_2)(a_2a_3) \ldots (a_{k-1}a_k)$ volgt dat een cykel van even lengte oneven is en omgekeerd. Een cykel van even lengte doet de pariteit dus omklappen; een cykel van oneven lengte heeft geen effect op de pariteit. $\square$

Met $|S|$ geven we het aantal elementen van de verzameling S aan. De deelverzameling van even permutaties van S_n noteren we met A_n. In S_n zijn er voor $n > 1$ evenveel even als oneven permutaties:

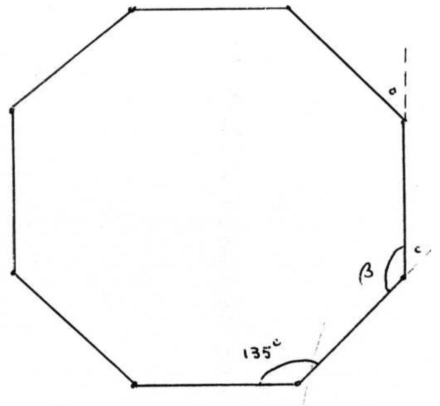
Stelling 3.5. $|A_n| = \frac{n!}{2}$ voor $n > 1$.

Bewijs. We weten dat $|S_n| = n!$. Beschouw $f : S_n \to S_n$ gegeven door $f(\sigma) = (1\ 2)\sigma$. Volgens het bovenstaande beeldt deze f even permutaties af op oneven permutaties en omgekeerd. Verder geldt $f(f(\sigma)) = \sigma$ voor alle $\sigma \in S_n$. Dus f deelt S_n op in paren bestaande uit een even en een oneven permutatie. Dus zijn er evenveel even als oneven permutaties in S_n. $\square$

3.4 Regelmatige figuren. (AO)

Een *regelmatige p-hoek* (polygon) is een p-hoek met p gelijke hoeken en gelijke zijden. De p hoekpunten liggen op een cirkel. De hoek β voldoet aan $p(180^0 - \beta) = 360^0$. Hieruit volgt dus $\beta = 180^0 - \frac{360^0}{p}$.

Regelmatige achthoek



Een klassieke vraag is voor welke p je het vlak kan verdelen in regelmatige p-hoeken. Als in een hoekpunt q regelmatige p-hoeken samenkomen, geldt $\beta = \frac{360^0}{q}$. Zo vinden we als eis

$$180^0 - \frac{360^0}{p} = \frac{360^0}{q},$$

dus $\frac{2}{p} + \frac{2}{q} = 1$. Omdat $p \geq 3$, geldt $\frac{2}{q} \geq \frac{1}{3}$, ofwel $q \leq 6$. Voor $q = 3$ vinden we $p = 6$, voor $q = 4$ is $p = 4$, voor $q = 5$ is er geen gehele p, voor $q = 6$ vinden we $p = 3$.
De enige regelmatige p-hoeken die voldoen zijn dus driehoeken, vierhoeken en zeshoeken.

Het equivalent van een regelmatige n-hoek in de ruimte is een figuur met gelijke hoeken, ribben en zijvlakken. Een voorbeeld is een kubus, een ander de regelmatige pyramide met gelijkzijdige driehoek als basis. Hier is een klassieke vraag welke regelmatige figuren er bestaan.
Stel dat de zijvlakken bestaan uit regelmatige p-hoeken en dat er in elk hoekpunt van de figuur q zijvlakken samenkomen. Dus voor de kubus $p = 4, q = 3$. De q zijvlakken die in een hoekpunt samenkomen hebben een gezamenlijke openingshoek kleiner dan 360^0, d.w.z. $q\beta < 360^0$.
Vullen we $\beta = 180^0 - \frac{360^0}{p}$ in, dan krijgen we na vereenvoudiging $1 < \frac{2}{p} + \frac{2}{q}$ waarbij natuurlijk $p > 2$ en $q > 2$.

Er geldt dus

$$pq - 2p - 2q < 0,$$

ofwel

$$(p-2)(q-2) < 4.$$

Dit heeft als enige oplossingen $(p,q) = (3,3), (3,4), (4,3), (3,5)$ en $(5,3)$. De vijf figuren bestaan inderdaad en worden “de vijf platonische lichamen” genoemd. Het zijn resp. de tetraëder, de oktaëder, de hexaëder (= kubus), de dodecaëder en de icosaëder, ofwel het regelmatige viervlak, achtvlak, zesvlak, twaalfvlak en twintigvlak.
In het algemeen wordt een figuur in de driedimensionale ruimte bestaande uit hoekpunten, ribben en zijvlakken een *veelvlak* (polytope) genoemd. De platonische lichamen zijn de regelmatige veelvlakken.

3.5 Eulers veelvlakformule. (AO)

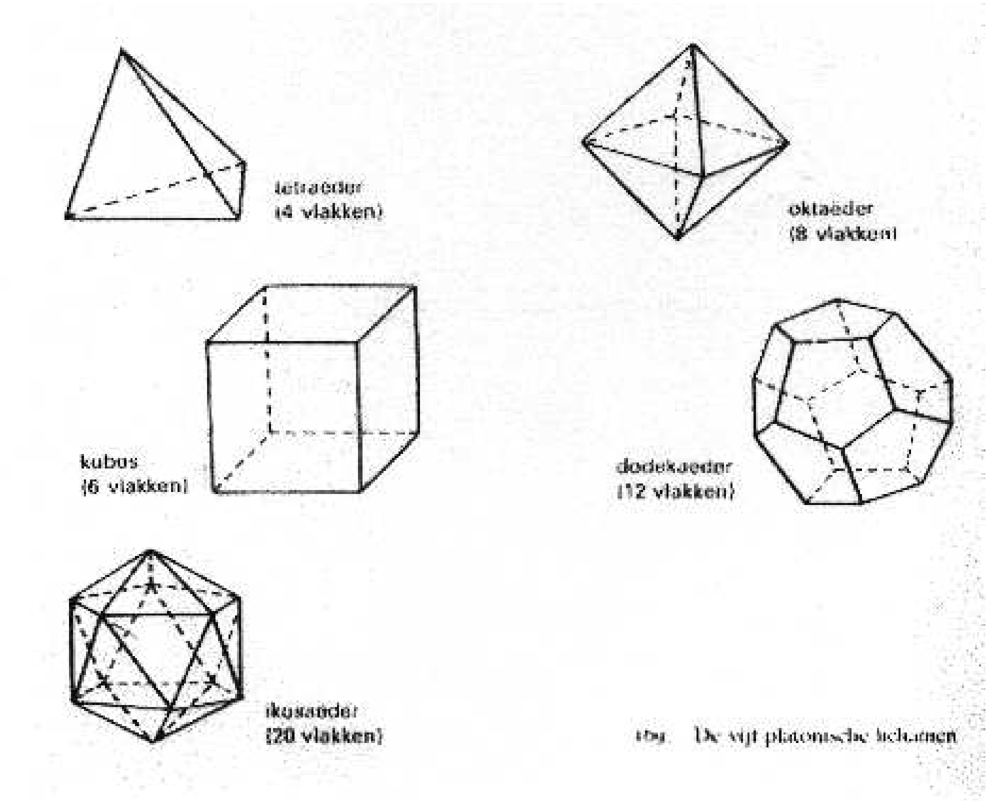
We tellen het aantal hoekpunten n, het aantal ribben m en het aantal vlakken r van de vijf platonische lichamen.

	n	m	r
tetraeder	4	6	4
kubus	8	12	6
octaeder	6	12	8
dodekaeder	20	30	12
ikosaeder	12	30	20

Er is op het eerste gezicht niet zo veel verband tussen n, m en r, maar in alle 5 gevallen geldt $n - m + r = 2$. Dit volgt uit *Euler's veelvlakformule* (vgl. Stelling 2.2.):

Stelling 3.6. Als alle hoekpunten van een veelvlak op een bol liggen, dan geldt $n - m + r = 2$ waarbij n het aantal hoekpunten, m het aantal ribben en r het aantal vlakken is.

Het bewijs gaat analoog aan dat van Stelling 2.3, waarbij in plaats van naar gebieden naar boldelen gekeken wordt, en in plaats van ribben naar verbindingslijnen op de bol.



De vijf platonische Lichamen.
(Uit : 'De toverspiegel van M. C. Escher')

Literatuur bij dit hoofdstuk

J.B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, 1967, Part I, Sections 4 and 5.

J.W. Archbold, *Algebra*, Pitmann, 1970, Ch. 16-18.
Bij 3.4:

H.S.M. Coxeter, *Regular Polytopes*, Dover, 1973.

Opgaven bij Hoofdstuk 3. Permutaties.

3.1. Bepaal alle isometrieën van een a) parallelogram, b) ruit, c) vierkant, d) regelmatig tetraëder.

3.2 Hoeveel isometreën heeft een
a) cirkel, b) rechthoekig blok met 3 verschillende zijden, c) kubus?

3.3 Maak de samenstellingstabel van een gelijkzijdige driehoek.

3.4 Bewijs dat in elke rij en in elke kolom van een samenstellingstabel elke isometrie precies éénmaal voorkomt.

3.5a) Hoeveel mogelijkheden heeft een handelsreiziger in principe als hij n steden moet bezoeken alvorens terug te keren?

b) Bewijs dat $n! > 2^n$ voor $n > 3$.

3.6. Schrijf de volgende permutaties als product van disjuncte cykels:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 2 & 4 & 1 & 8 & 5 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 3 & 2 & 8 & 5 & 4 & 7 & 9 \end{bmatrix}.$$

3.7. In S_5 beschouwen we de permutaties $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{bmatrix}$,
$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{bmatrix}, \delta = \sigma\tau\sigma^3$ en $\theta = \delta\tau\delta^{-1}$.

a) Schrijf σ, τ, δ en θ in disjuncte cykelnotatie

b) Bereken de ordes van σ, τ, δ en θ.

c) Ga na welke van σ, τ, δ en τ even zijn.

3.8. Bepaal σ^{103} voor $\sigma = (134)(257)(6\ 10\ 9\ 8)$.

3.9 Geef in S_{10} een permutatie van orde 20 aan.

3.10. Schrijf A_3 en A_4 uit.

3.11. Los de volgende vergelijkingen op:

a) $(132)\sigma(341) = (234)$ in S_4,

b) $\sigma^2 = (123)$ in S_3,

c) $\sigma^3 = (123)$ in S_4.

4 HOOFDSTUK: POLYNOMEN

4.1 Basiseigenschappen.

Een *polynoom* (of veelterm) is een functie $P : \mathbf{R} \to \mathbf{R}$ die aan $x \in \mathbf{R}$ het getal $a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ toevoegt, waarbij $a_n, a_{n-1}, ..., a_0 \in \mathbf{R}$ vast zijn en $a_n \neq 0$ als $n > 0$.
Als $a_n \neq 0$, dan heet n de *graad* (degree) van P en a_n de *kopcoëfficiënt* van P. Als $a_n = 1$, noemen we P *monisch.* We schrijven $\mathrm{gr}(P) = n$. De coëfficiënt a_0 noemen we de constante term van P. Als $n = 0$, schrijven we $P = a_0$ en noemen we P *constant.* Als $P = 0$, definiëren we $\mathrm{gr}(P) = -\infty$.

Voorbeelden van polynomen zijn $x^2 + 1, x^3 - 2x - 4, x^{100}$. We kunnen polynomen optellen en vermenigvuldigen, bijv.

$$(x^2 + 1) + (x^3 - 2x - 4) = x^3 + x^2 - 2x - 3,$$

$$(x^2 + 1)(x^3 - 2x - 4) = x^5 - x^3 - 4x^2 - 2x - 4.$$

We definiëren de *som* van twee polynomen $P(x) = a_0 + a_1 x + ... + a_n x^n (a_n \neq 0)$ en $Q(x) = b_0 + b_1 x + ... + b_m x^m (b_m \neq 0)$ als het polynoom

$$(P + Q)(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ...$$

waarbij $a_k = 0$ voor $k > n, b_l = 0$ voor $l > m$ en we ophouden als er alleen nog coëfficiënten 0 volgen. Dus $\mathrm{gr}(P + Q) \leq \max(\mathrm{gr}(P), \mathrm{gr}(Q))$ en $\mathrm{gr}(P+Q) = \max(\mathrm{gr}(P), \mathrm{gr}(Q))$ als $\mathrm{gr}(P) \neq \mathrm{gr}(Q)$. (Met $\max(a, b)$ bedoelen we de grootste van a en b.) Het *product* van $P(x)$ en $Q(x)$ wordt gedefinieerd door

$$(PQ)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + ...$$

met dezelfde conventie als bij de som. De coëfficiënt van x^k is dus $a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k$. Dit soort uitdrukkingen wordt vaak verkort opgeschreven met de $\sum$-notatie, in dit geval

$$\sum_{j=0}^{k} a_{k-j} b_j.$$

Merk op dat PQ graad $n + m$ heeft en kopcoëfficiënt $a_n b_m$.

We kunnen de polynomen opvatten als een verzameling functies die gesloten is onder optelling en vermenigvuldiging. Deze verzameling noteren we als $\mathbf{R}[x]$. De polynomen hebben een aantal eigenschappen die overeenkomen met basiseigenschappen van $\mathbf{Z}$.

(+C) $P+Q=Q+P$ voor alle P, Q
(+A) $(P+Q)+R=P+(Q+R)$ voor alle P, Q, R
(×C) $PQ=QP$ voor alle P, Q
(×A) $(PQ)R=P(QR)$ voor alle P, Q, R
(D) $P(Q+R)=PQ+PR$ voor alle P, Q, R.

(+N) $P+0=P$ voor alle P
(+I) bij elke P bestaat een Q met $P+Q=0$, notatie $Q=-P$
(×N) $P.1=P$ voor alle P

De verzameling $\mathbf{R}[x]$ heeft *niet* eigenschap (×I), dat er bij elke P een Q bestaat met $PQ=1$. Zo'n Q is er alleen als $\mathrm{gr}(P)=0$, want als $\mathrm{gr}(P)>0$ of $\mathrm{gr}(P)=-\infty$, dan is $\mathrm{gr}(PQ)>0$ of $\mathrm{gr}(PQ)=-\infty$, terwijl $\mathrm{gr}(1)=0$.
De kleinste uitbreiding van $\mathbf{R}[x]$ die gesloten is onder deling is de verzameling van *rationale functies* $\frac{P(x)}{Q(x)}$ met $P, Q \in \mathbf{R}[x], Q \neq 0$. Net als bij de rationale getallen geldt $\frac{P_1}{Q_1}=\frac{P_2}{Q_2}$ als en alleen als $P_1Q_2=P_2Q_1, Q_1Q_2 \neq 0$.

De structuur van $\mathbf{Z}$ heeft dus opmerkelijke overeenkomsten met die van $\mathbf{R}[x]$. Er zijn natuurlijk ook essentiële verschillen. In $\mathbf{Z}$ hebben we volledige inductie, in $\mathbf{R}[x]$ niet (eventueel wel naar de graad); in $\mathbf{Z}$ kunnen we niet differentiëren, $\mathbf{R}[x]$ is gesloten onder differentiatie:

$$\frac{d}{dx}(a_nx^n+a_{n-1}x^{n-1}+...+a_0)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+...+a_1.$$

Differentiatie en integratie worden behandeld in Analyse 1. Hier werken we de analogie van $\mathbf{Z}$ en $\mathbf{R}[x]$ verder uit.

Ook in $\mathbf{R}[x]$ hebben we *deling met rest*, waarbij de graad als maatstaf voor grootte genomen wordt.

Stelling 4.1. Stel $A, B \in \mathbf{R}[x]$ en $B \neq 0$. Dan bestaat er precies één paar $Q, R \in \mathbf{R}[x]$ zó dat $A=QB+R$ en $\mathrm{gr}(R)<\mathrm{gr}(B)$.

De Q en R zijn, net als bij $\mathbf{Z}$, te bepalen door middel van een staartdeling. Stel $A(x) = x^4 + x^3 - 3x^2 - x + 2$ en $B(x) = 2x^2 - 1$. Dan vinden we

$$
\begin{array}{cccccccccccc}
2x^2-1 & / & x^4 & + & x^3 & - & 3x^2 & - & x & + & 2 & \backslash \quad \frac{1}{2}x^2 + \frac{1}{2}x - \frac{5}{4} \\
 & & x^4 & & & - & \frac{1}{2}x^2 & & & & & \\
 & & & & x^3 & - & \frac{5}{2}x^2 & & & & & \\
 & & & & x^3 & & & - & \frac{1}{2}x & & & \\
 & & & & & - & \frac{5}{2}x^2 & - & \frac{1}{2}x & + & 2 & \\
 & & & & & - & \frac{5}{2}x^2 & & & + & \frac{5}{4} & \\
 & & & & & & & - & \frac{1}{2}x & + & \frac{3}{4} &
\end{array}
$$

d.w.z. $Q(x) = \frac{1}{2}x^2 + \frac{1}{2}x - \frac{5}{4}$ en $R(x) = -\frac{1}{2}x + \frac{3}{4}$. Voor deze Q en R geldt $A = QB + R$ en $\mathrm{gr}(R) < \mathrm{gr}(B)$.

Bewijs van Stelling 4.1. Zij R een polynoom van minimale graad waarvoor een Q bestaat met $A = QB + R$. Veronderstel dat $\mathrm{gr}(R) \geq \mathrm{gr}(B)$. Schrijf $R(x) = r_n x^n + r_{n-1}x^{n-1} + \ldots + r_0$ en $B(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$. Dan is $n \geq m$. Verder heeft

$$R_1(x) = R(x) - \frac{r_n}{b_m} B(x) x^{n-m} = (r_{n-1}x^{n-1} + \ldots + r_0) - \frac{r_n}{b_m}(b_{m-1}x^{n-1} + \ldots + b_0)$$

graad kleiner dan n. Er geldt

$$A(x) = Q(x)B(x) + R(x) = (Q(x) + \frac{r_n}{b_m}x^{n-m})B(x) + R_1(x)$$

met $\mathrm{gr}(R_1) < \mathrm{gr}(R)$ in tegenspraak met de keuze van R.

Stel er is nog een paar Q_1, R_1 dat voldoet.
Door aftrekken vinden we $0 = A - A = (Q - Q_1)B + R - R_1$, d.w.z. $(Q - Q_1)B = R_1 - R$. Hieruit volgt $\mathrm{gr}(Q - Q_1) + \mathrm{gr}(B) \leq \max(\mathrm{gr}(R_1), \mathrm{gr}(R)) < \mathrm{gr}(B)$, ofwel $\mathrm{gr}(Q - Q_1) < 0$. Dus $Q = Q_1$. Dan volgt $R = A - QB = A - Q_1 B = R_1$. $\square$

De verzameling van polynomen A die rest R geven bij deling door B noemen we de *restklasse* R van B. De restklasse 0 verdient speciale aandacht. Als $A = QB$, dan heet B *een deler* van A en A een *veelvoud* van B. Notatie $B|A$.

Voor $A, B, C, D \in \mathbf{R}[x]$ geldt
(D1) Als D een deler is van A en B, is D ook een deler van $A + B$ en van $A - B$.
(D2) Als A een deler van B is, en B van C, dan is A een deler van C.
(D3) Als D een deler van A is, is AB een veelvoud van D en ook van BD.
(D4) Als D een deler is van A en $A \neq 0$, dan geldt $\mathrm{gr}(D) \leq \mathrm{gr}(A)$.
Uit (D4) kunnen we **nog niet** concluderen dat A met $A \neq 0$ maar eindig veel monische delers heeft!

Geheel analoog aan $\mathbf{Z}$ hebben we in $\mathbf{R}[x]$ het algoritme van Euclides, door herhaald deling met rest toe te passen. Startend met polynomen A, B, niet beide 0, vinden we zo een polynoom D met $D|A$ en $D|B$ en anderzijds met de eigenschap: als $C|A$ en $C|B$, dan $C|D$. Het monische polynoom dat we krijgen door D door zijn kopcoëfficiënt te delen noemen we de *grootste gemene deler* van A en B, notatie $\mathrm{ggd}(A, B)$.

Voorbeeld: Zij $A(x) = x^4 + 4$ en $B(x) = \frac{1}{2}x^3 + \frac{1}{2}x^2 - 1$.
Dan geeft het algoritme van Euclides:

$$x^4 + 4 = (2x - 2)(\frac{1}{2}x^3 + \frac{1}{2}x^2 - 1) + x^2 + 2x + 2$$

$$\frac{1}{2}x^3 + \frac{1}{2}x^2 - 1 = (\frac{1}{2}x - \frac{1}{2})(x^2 + 2x + 2).$$

We vinden $D(x) = x^2 + 2x + 2$. Omdat D al monisch is, is $D = \mathrm{ggd}(A, B)$.

Net als in het vorige hoofdstuk vinden we door de corresponderende lineaire combinaties van A en B uit te rekenen uiteindelijk polynomen P en Q zódat $AP + BQ = \mathrm{ggd}(A, B)$.

Voorbeeld. Zij $A(x) = x^4 + 4$ en $B(x) = \frac{1}{2}x^3 + \frac{1}{2}x^2 - 1$. We vinden direct uit de derde regel van het vorige voorbeeld:

$$x^2 + 2x + 2 = 1 \times (x^4 + 4) - (2x - 2)(\frac{1}{2}x^3 + \frac{1}{2}x^2 - 1).$$

Dus $P(x) = 1, Q(x) = -2x + 2.$

Stelling 4.2. Stel $A, B \in \mathbf{R}[x]$, niet beide nul. Dan bestaan er $P, Q \in \mathbf{R}[x]$ zó dat $AP + BQ = \text{ggd}(A, B)$.

Het bewijs gaat geheel analoog aan dat voor $\mathbf{Z}$. (Ga na). Wel zullen we het volgende afleiden:

Gevolg. Stel A, B en C zijn polynomen, A en B niet beide 0. Er zijn polynomen P, Q met $AP + BQ = C \iff \text{ggd}(A, B)|C$.

Bewijs. $\Longrightarrow$ $\text{ggd}(A, B)$ deelt A en B, dus volgens (D3) ook AP en BQ, dan volgens (D1) ook $AP + BQ = C$.
$\Longleftarrow$ Volgens Stelling 4.2 zijn er polynomen P_1 en Q_1 met $AP_1 + BQ_1 = \text{ggd}(A, B)$. Omdat $\text{ggd}(A, B)|C$, is er een polynoom D zó dat $C = D \times \text{ggd}(A, B)$. Nu volgt $A(DP_1) + B(DQ_1) = C$. We kunnen dus $P = DP_1, Q = DQ_1$ kiezen. $\square$

Voor alle A, B, C in $\mathbf{R}[x]$ geldt:
(G1) Als $C|A$ en $C|B$, dan $C|\text{ggd}(A, B)$
(G2) Als $A|C, B|C$ en $\text{ggd}(A, B) = 1$, dan $AB|C$.
(G3) Als $A|BC$ en $\text{ggd}(A, B) = 1$, dan $A|C$.
(G4) Als $C = \text{ggd}(A, B)$, dan is $\text{ggd}(\frac{A}{C}, \frac{B}{C}) = 1$.

Elk polynoom P is deelbaar door a en door aP voor elke $a \in \mathbf{R}$ met $a \neq 0$. We noemen dit de *triviale delers* van P. Analoog aan het begrip priemgetal noemen we een polynoom P met $\text{gr}(P) > 0$ *irreducibel* als P alleen triviale delers heeft, en anders *reducibel*. Een reducibel polynoom is dus te schrijven als product van twee polynomen, beide van lagere graad.

Stelling 4.3. Elk polynoom van positieve graad is het product van irreducibele polynomen.

Bewijs. Met inductie naar de graad.
Als $\text{gr}(P) = 1$, dan is P irreducibel en voldoet P. Stel de bewering is waar voor polynomen van graad kleiner dan n. Als $\text{gr}(P) = n$ en P is irreducibel, dan voldoet P. Als $\text{gr}(P) = n$ en P is reducibel, dan kunnen we $P = QR$ schrijven met $0 < \text{gr}(Q) < n, 0 < \text{gr}(R) < n$. Omdat volgens de inductiehypothese Q en R producten van irreducibele polynomen zijn, is $P = QR$ dat ook. $\square$

In Algebra 1 zullen we zien dat elk polynoom op volgorde en constanten na op precies één manier te schrijven is als product van irreducibele polynomen. Hieruit volgt dat elk polynoom $\neq 0$ maar eindig veel monische delers heeft.

4.2 Breuksplitsing.

Stelling 4.2 ligt ten grondslag aan de breuksplitsing waarmee in de Analyse 1 integralen uitgerekend worden.

Voorbeeld. We zoeken polynomen $P, Q \in \mathbf{R}[x]$ zó dat

$$\frac{1}{(x^2+1)(x^2+x+1)} = \frac{P(x)}{x^2+1} + \frac{Q(x)}{x^2+x+1}.$$

Door links en rechts met de noemer te vermenigvuldigen, vinden we

$$1 = (x^2+x+1)P(x) + (x^2+1)Q(x).$$

Volgens het Gevolg is dit oplosbaar omdat $\mathrm{ggd}(x^2+1, x^2+x+1) = 1$. Met het euclidisch algoritme vinden we $P(x) = -x, Q(x) = x+1$. Uit deze redenering volgt dat $\frac{C(x)}{A(x)B(x)}$ alleen geschreven kan worden als $\frac{P(x)}{A(x)} + \frac{Q(x)}{B(x)}$ als $\mathrm{ggd}(A, B)|C$. Het kan dus zeker als A en B onderling ondeelbaar zijn.

4.3 Fibonaccigetallen en genererende functies. (AO)

Polynomen spelen een fundamentele rol in de Algebra. In feite is algebra de theorie waarin de gemeenschappelijke eigenschappen van gehele getallen, rationale getallen, reële getallen, polynomen en permutaties worden geabstraheerd tot begrippen als groep, ring en lichaam. Dit gebeurt in colleges Algebra 1, 2, 3. Daarbij blijven polynomen, vanwege het eigen specifieke karakter, een belangrijke rol spelen in de Algebra en ook in de Meetkunde. Polynomen en de in Analyse 1 behandelde generalisatie Machtreeken spelen eveneens een belangrijke rol in de Combinatoriek en de Kansrekening. Ik wil dat hier illustreren aan de hand van het gebruik van *genererende functies.*

Ik laat zien hoe genererende functies helpen bij de bestudering van de Fibonaccirij $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ gedefinieerd door $F_1 = 1, F_2 = 1, F_n = F_{n-1} + F_{n-2}$ voor $n \geq 3$. Beschouw de genererende functie $F(x) = \sum_{n=1}^{\infty} F_n x^n$. Uit $F_n = F_{n-1} + F_{n-2}$ volgt

$$\sum_{n=3}^{\infty} F_n x^n = \sum_{n=3}^{\infty} F_{n-1} x^n + \sum_{n=3}^{\infty} F_{n-2} x^n = x \sum_{n=2}^{\infty} F_n x^n + x^2 \sum_{n=1}^{\infty} F_n x^n.$$

Dus $F(x) - x - x^2 = x(F(x) - x) + x^2 F(x)$.

We lossen $F(x)$ op:

$$F(x) = \frac{x}{1-x-x^2}.$$

Door breuksplitsen vinden we, omdat $1-x-x^2 = (1-\alpha_1 x)(1-\alpha_2 x)$ met $\alpha_{1,2} = \frac{1}{2} \pm \frac{1}{2}\sqrt{5}$,

$$F(x) = \frac{1}{\sqrt{5}}\frac{1}{1-\alpha_1 x} - \frac{1}{\sqrt{5}}\frac{1}{1-\alpha_2 x}.$$

Er geldt $\frac{1}{1-\alpha x} = 1 + \alpha x + (\alpha x)^2 + (\alpha x)^3 + ...$, en dus

$$F(x) = \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}(\alpha_1 x)^n - \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}(\alpha_2 x)^n.$$

Door links en rechts coëfficiënten van x^n gelijk te stellen vinden we

$$F_n = \frac{1}{\sqrt{5}}(\frac{1}{2} + \frac{1}{2}\sqrt{5})^n - \frac{1}{\sqrt{5}}(\frac{1}{2} - \frac{1}{2}\sqrt{5})^n \tag{2}$$

Omdat de tweede term pijlsnel naar 0 gaat, is de eerste term een heel goede benadering van F_n. Er geldt bijv.

$$\frac{1}{\sqrt{5}}(\frac{1}{2} + \frac{1}{2}\sqrt{5})^{20} = 15126,99999 \text{ en } F_{20} = 15127.$$

Het getal $\frac{1}{2} + \frac{1}{2}\sqrt{5}(= 1,6180339)$ heet het *getal van de gulden snede*.

Literatuur bij dit hoofdstuk:

L. Childs, *A concrete Introduction to Higher Algebra*, Springer-Verlag, 1979, Part II.

J.R. Durbin, *Modern Algebra*, Wiley, 1979, Ch XI.

Voor Sectie 4.3

C.L. Liu, *Introduction to Combinatorial Mathematics*, McGraw Hill, 1968,
Ch. 1-2.

Opgaven bij Hoofdstuk 4. Polynomen.

4.1. Pas deling met rest toe op $A(x) = x^4 - x^3 + 3$ en $B(x) = x^2 - 2$ en op $A(x) = 2x^3 - x + 1$ en $B(x) = 3x^2 + 2x + 1$.

4.2. Bewijs (D2) en (D3).

4.3. a) Bewijs (D5).

b) Ga na dat met behulp van het algoritme van Euclides de grootste gemene deler van twee polynomen gevonden wordt.

4.4 Bepaal de ggd van

a) $x^5 - 2x - 4$ en $x^3 + x^2 - 2$.

b) $x^3 - 2x^2 + 2x - 1$ en $x^3 - 3x^2 + 3x + 1$.

4.5. Bepaal $P, Q \in \mathbf{R}[X]$ zó dat

a) $(x^3 - 2x^2 + 3x - 2)P(x) + (x^3 + x^2 - 2)Q(x) = x - 1$.

b) $(x^3 - 2x^2 + 3x - 2)P(x) + (x^3 + x^2 - 2)Q(x) = x^2 - 1$.

4.6. a) Bewijs (G2) en (G4).

b) Bewijs dat er maar één ggd van twee polynomen is.

4.7.a) Bewijs: $x^n - 1 = (x - 1)\sum_{j=0}^{n-1} x^j$ voor $n \in \mathbf{N}$.

b) Bewijs: $x^d - 1 | x^n - 1 \Longleftrightarrow d|n$.

c) Bepaal ggd $(x^m - 1, x^n - 1)$.

d) Voor welke n is $x^n + 1$ deelbaar door $x + 1$? Wat is in die gevallen het quotiënt?

4.8. Bepaal polynomen P en Q zó dat
a) $\frac{x+1}{x^4-1} = \frac{P(x)}{x^2-1} + \frac{Q(x)}{x^2+1}$ $\quad (\mathrm{gr}(P), \mathrm{gr}(Q) < 2)$.
b) $\frac{x}{x^2-2} = \frac{P(x)}{x-\sqrt{2}} + \frac{Q(x)}{x+\sqrt{2}}$ $\quad (\mathrm{gr}(P), \mathrm{gr}(Q) < 1)$.

4.9. Zij $P(x) = (2x^2 - 7x + 6)^{2002}$.
Wat is de som van de coëfficiënten van P?

5 HOOFDSTUK: LOGICA EN VERZAMELINGENLEER

5.1 Logica.

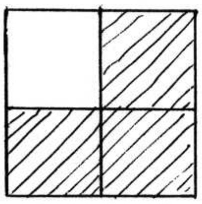
In de wiskunde kiezen we een aantal uitgangspunten, zg. *axioma's*. Daaruit proberen we andere eigenschappen af te leiden. Die eigenschappen worden vaak in de vorm van stellingen geformuleerd. Die stellingen worden uitgedrukt in een nogal beperkt jargon. Er komen begrippen voor waarvan de definitie bekend verondersteld wordt, zoals 'graaf', 'samenhangend', 'natuurlijk getal', 'priemgetal'. Verder komen er
woorden in voor als: 'voor alle geldt', 'er bestaat een'. Vaak zijn er twee beweringen die verbonden worden door 'als ... dan ... ', '... impliceert ... ', '... is equivalent met ... ', '... of ... ', '... en ... '. Ik geef hier een korte verhandeling over de betekenis van deze begrippen.

Allereerst beperken we ons tot beweringen die 'waar' of 'niet waar' zijn. Als A een bewering is, geven we met $\neg A$ (niet A) de tegengestelde bewering aan. Is A waar, dan is $\neg A$ niet waar; is A niet waar, dan is $\neg A$ waar. Het zal duidelijk zijn dat $\neg(\neg A) = A$.

In de volgende waarheidstabellen geven we de betekenis van bepaalde uitdrukkingen weer, waarbij we onware beweringen arceren.

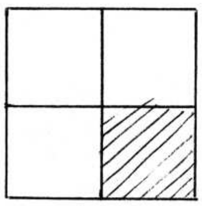
Notatie

A en B

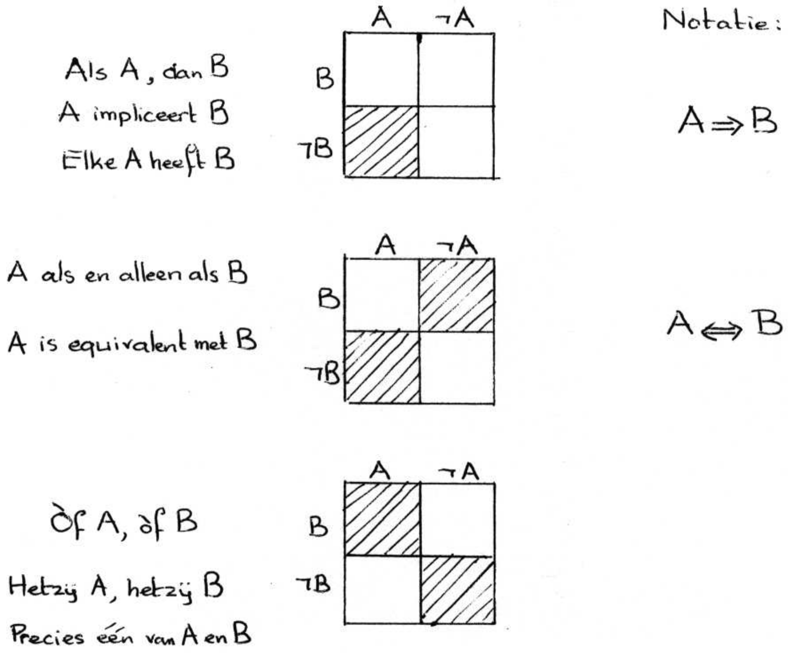


$A \wedge B$

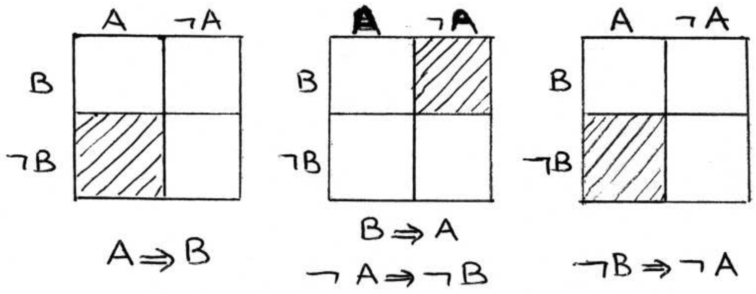
A of B



$A \vee B$



Bij gebruik van het woordje 'of' wordt dus *niet* naar een keuze gevraagd. Het woord 'als' wordt dus *niet* gebruikt in de betekenis van 'op voorwaarde dat'. In het dagelijks taalgebruik hebben 'of' en 'als' dus vaak een andere betekenis. We beschouwen de waardheidstabellen bij $A \Longrightarrow B$, $\neg A \Longrightarrow \neg B$ en $\neg B \Longrightarrow \neg A$.



We zien dat de tabel van $A \Longrightarrow B$ anders is dan van $B \Longrightarrow A$, maar dat de waarheidstabellen van $A \Longrightarrow B$ en $\neg B \Longrightarrow \neg A$ overeenkomen. In plaats van $A \Longrightarrow B$ kunnen we dus evengoed $\neg B \Longrightarrow \neg A$ bewijzen. Een variant die vaak gebruikt wordt is een *bewijs uit het ongerijmde.* Om $A \Longrightarrow B$ te bewijzen nemen we aan dat A en $\neg B$ waar zijn en leiden dan af dat $\neg A$ waar is. Deze tegenspraak bewijst dat $A \Longrightarrow B$.

De notatie $\Longrightarrow$ wordt door studenten vaak verkeerd gebruikt, nl. in de zin van 'dus' '$A \Longrightarrow B$' betekent niet dat B waar is, maar alleen dat B waar is als A waar is. Als A niet waar is, is de implicatie waar, ook als B niet waar is.

Het gebruik van 'voor alle' of 'er bestaat' verwijst altijd naar welgedefinieerde verzamelingen, bijv. $\mathbf{Z}, \mathbf{R}$, S_n, $\mathbf{R}$[x]. We kunnen bijvoorbeeld beweren dat voor alle natuurlijke getallen x geldt dat $x \geq 1$, notatie $\forall x \in \mathbf{N}$: $x^2 \geq 1$, en dit is een ware bewering. De bewering $\forall x \in \mathbf{Z}$: $x^2 \geq 1$ is onwaar. Het hangt dus van de verzameling X af of '$\forall x \in X$: $x^2 \geq 1$' waar is.

De negatie van deze bewering verkrijgen we in stappen:
$\neg(\forall$x$\in$X: $x^2 \geq 1)$
$\exists x \in X$: $\neg(x^2 \geq 1)$ ($\exists$: er bestaat een)
$\exists x \in X : x^2 < 1$.
Een negatie van een 'er bestaat een' bewering leidt tot een bewering met 'alle':
$\neg(\exists x \in X : \quad x^2 = 2)$
$\forall x \in X : \quad \neg(x^2 = 2)$
$\forall x \in X : \quad x^2 \neq 2$
We noemen $\forall$ een universele quantificator en $\exists$ een existentiële. We hebben al beweringen gezien met twee en drie universele quantificatoren:
(+C) $\forall A, \forall B \quad A + B = B + A$
(+A) $\forall A, \forall B, \forall C \quad (A + B) + C = A + (B + C)$
Hier doet de volgorde van de quantificatoren er niet toe. Dat is anders als het om quantificatoren van verschillend type gaat:
$\forall A \;\; \exists B: \qquad A + B = 0,$
$\exists B \;\; \forall A: \qquad A + B = 0.$
Dit zijn twee verschillende beweringen. In $\mathbf{Z}$ is de eerste bewering wel waar, de tweede niet. Ook nu maakt de schrijfwijze het gemakkelijk om de negatie in stappen te vinden:
$\neg(\forall A \;\; \exists B : \quad A + B = 0)$
$\exists A \;\; \neg(\exists B : \quad A + B = 0)$
$\exists A \;\; \forall B : \quad \neg(A + B = 0)$
$\exists A \;\; \forall B : \quad A + B \neq 0$

5.2 Verzamelingen.

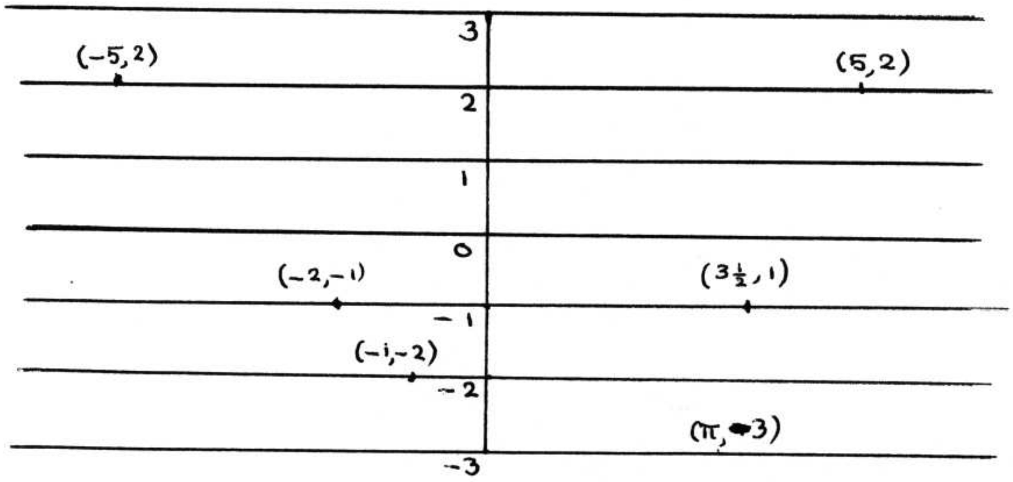
Een *verzameling* V bestaat uit elementen (Engels: 'set'). Als v een element van V is, schrijven we $v \in V$. Als v geen element van V is schrijven we $v \notin V$. Dus $3 \in \mathbf{Z}$, $0 \in \mathbf{Z}$, $-5 \in \mathbf{Z}$, $\sqrt{2} \notin \mathbf{Z}$. Als V geen elementen bevat, heet V *leeg*. Notatie: $V = \emptyset$.

Stel we hebben twee verzamelingen, V en W. De *vereniging* (union) $V \cup W$ van V en W bestaat uit alle elementen v met $v \in V$ of $v \in W$. De *doorsnede* (intersection) $V \cap W$ van V en W bestaat uit alle v met $v \in V$ en $v \in W$. De verzamelingen V en W heten *disjunct* als $V \cap W = \emptyset$.

Een verzameling W heet een *deelverzameling* (subset) van een verzameling V als elk element van W ook een element van V is, notatie $W \subseteq V$. Als $W \subseteq V$ en $V \subseteq W$, dan schrijven we $V = W$. Als $W \subseteq V$, maar niet $V \subseteq W$, dan is W een *echte deelverzameling* (proper subset) van V, notatie $W \subset V$. Bijv. $\mathbf{Z} \subset \mathbf{Q}$, $\mathbf{Q} \subset \mathbf{R}$.
Opmerking: In de plaats van $\subseteq$ gebruikt men vaak $\subset$ en in plaats van $\subset$ vaak $\subset$.

Als V een deelverzameling van W is, wordt het *complement* van V in W gedefinieerd door $\{w \in W | w \notin V\}$, notatie V^c. Zo vormen de oneven getallen het complement van de even getallen in $\mathbf{Z}$.

Als je twee verzamelingen V en W hebt, kun je een nieuwe verzameling $V \times W$ maken bestaande uit alle geordende paren (v, w) met $v \in V$ en $w \in W$. Deze verzameling heet het *Carthesisch produkt* van V en W (genoemd naar de Franse wiskundige en filosoof René Descartes (1596–1650), de grondlegger van de analytische meetkunde). Als $V = W$, dan schrijven we wel V^2 in plaats van $V \times V$. Dus $(-7, -3) \in \mathbf{Z}^2, (-3, -7) \in \mathbf{Z}^2, (-7, -3) \neq (-3, -7)$. We kunnen $V \times W$ voorstellen met behulp van een Carthesisch assenstelsel waarbij V met de horizontale en W met de verticale as correspondeert.



$\mathbb{R} \times \mathbb{Z}$

Een *relatie* R op een verzameling V is een deelverzameling van $V \times V$.
Als $v \in V, w \in V$ en $(v, w) \in R$, schrijven we $v \sim w$.

Een relatie heet een *equivalentierelatie* als aan de volgende drie eisen voldaan is:
1) reflexiviteit: $v \sim v$ voor alle $v \in V$.
2) symmetrie: $v \sim w \Rightarrow w \sim v$ voor alle $v, w \in V$.
3) transitiviteit: $u \sim v, v \sim w \Rightarrow u \sim w$ voor alle $u, v, w \in V$.

Voorbeelden: Zij $V = \mathbf{Z}$.
De relatie $v \leq w$ is reflexief, niet symmetrisch, wel transitief.
De relatie $|v - w| \leq 1$ is reflexief, symmetrisch, niet transitief.
De relatie $v \neq w$ is niet reflexief, wel symmetrisch, niet transitief.
De relatie $v = w$ is een equivalentierelatie.
De relatie' $v - w$ is door 10 deelbaar' is ook een equivalentierelatie.

Een equivalentierelatie op V splitst V op in disjuncte klassen, zg. *equivalentieklassen*, waarbij $a, b \in V$ tot dezelfde klasse behoren als en alleen als $a \sim b$ (Ga na). Een *volledig representantensysteem* is een verzameling met uit elke klasse precies één element. In het laatstgenoemde voorbeeld is $\{0, 1, 2, \ldots, 9\}$ een volledig stel representanten, maar ook

$$\{-37, -14, -11, -9, -2, 4, 10, 22, 107, 525\}$$

(Volgens het zg. keuzeaxioma kun je altijd een volledig stel representanten kiezen.)

5.3 Functies.

Een *functie* (of *afbeelding*) f van V naar W is een voorschrift dat aan elk element van V precies één element van W toekent. Notatie: $f : V \to W$. Een functie komt dus overeen met een deelverzameling van $V \times W$ waarbij bij elk element v van V er precies één element w van W is zodat (v, w) tot de deelverzameling behoort. Die deelverzameling noemen we wel de *grafiek* van f.

Stel $f : V \to W$. Als aan $v \in V$ het element $w \in W$ wordt toegekend, heet w het *beeld* van v onder f en v een *origineel* van w , notatie $f(v) = w$ of $v \longmapsto w$. Een element $w \in W$ kan meerdere originelen hebben. De verzameling $\{v \in V | f(v) = w\}$ heet het *origineel* van w onder f, (Engels: inverse image), notatie $f^{-1}(w)$. De verzameling $f(V) := \{f(v) | v \in V\}$ heet het beeld van V onder f. Dus $f(V) \subseteq W$.

De functie $f : V \to W$ heet *surjectief* als $f(V) = W$, d.w.z. dat elke $w \in W$ een origineel heeft. (Ook wel 'afbeelding op'.) Verder heet $f : V \to W$

injectief (of 1-1-duidig) als elk paar verschillende elementen van V onder f verschillende beelden heeft, m.a.w.

$$f(v) = f(w) \Rightarrow v = w.$$

De functie $f : V \to W$ heet *bijectief* als f zowel injectief als surjectief is.

Voorbeelden:

- De functie $f : \mathbf{Z} \to \mathbf{Z}$ gegeven door $x \longmapsto -x$ is bijectief.
- De functie $f : \mathbf{Z} \to \mathbf{Z}$ gegeven door $x \longmapsto x^2$ is niet injectief en niet surjectief.
- De functie $f : \mathbf{Z} \to \mathbf{Z}$ gegeven door $f(x) = |x|$ is niet injectief en niet surjectief.
- De functie $f : \mathbf{N} \to \mathbf{Z}$ gegeven door $f(x) = |x|$ is injectief.
- De functie $f : \mathbf{N} \to \mathbf{N}$ gegeven door $f(x) = |x|$ is bijectief.

Merk op dat injectief, surjectief, bijectief niet alleen van f afhangt, maar ook van de keuze van V en W. De functie $f : V \to V$ gegeven door $f(x) = x$ voor alle $x \in V$ heet de *identieke afbeelding* op V. Een functie $f : V \to W$ met $f(v) = a$ voor elke $v \in V$ heet een *constante* functie. (Elke v heeft dus hetzelfde beeld.) Als $f : V \to W$ bijectief is, heeft elke $w \in W$ precies één origineel in V. Dit induceert een functie $g : W \to V$ waarbij $g(w) = v \Longleftrightarrow f(v) = w$. Deze functie heet de *inverse functie* van f, notatie f^{-1}. Voorbeelden:

- $f : \mathbf{Z} \to \mathbf{Z}$ gegeven door $f(x) = -x$ heeft zichzelf als inverse functie.
- $f : \mathbf{R}^+ \to \mathbf{R}^+$ gegeven door $f(x) = x^2$ is een bijectieve functie met als inverse $f^{-1} : \mathbf{R}^+ \to \mathbf{R}^+$ gegeven door $f^{-1}(x) = \sqrt{x}$.
- De functie e^x van $\mathbf{R}$ naar $\mathbf{R}^+$ heeft als inverse de functie $\ln x$ van $\mathbf{R}^+$ naar $\mathbf{R}$. (Wiskundigen schrijven meestal log in plaats van ln.)

Stel U, V en W zijn verzamelingen en $f : U \to V$ en $g : V \to W$ functies. Dan heet $g \circ f : U \to W$ gedefinieerd door $g \circ f(u) = g(f(u))$ de *samenstelling* (of *compositie*) van f en g.

Stelling 5.1. Als $f : U \to V$ en $g : V \to W$ injectief/surjectief/bijectief is, is $g \circ f : U \to W$ dat ook.

Bewijs.
a) Stel f en g zijn injectief. Stel $g \circ f(u_1) = g \circ f(u_2)$. Dan is dus $g(f(u_1)) = g(f(u_2))$. Omdat g injectief is, volgt $f(u_1) = f(u_2)$. Omdat f injectief is, krijgen we $u_1 = u_2$. We concluderen dat $g \circ f$ injectief is.
b) Stel f en g zijn surjectief. Dan is $W = g(V) = g(f(U)) = g \circ f(U)$. Dus is $g \circ f$ surjectief.
c) Combineer a) en b).

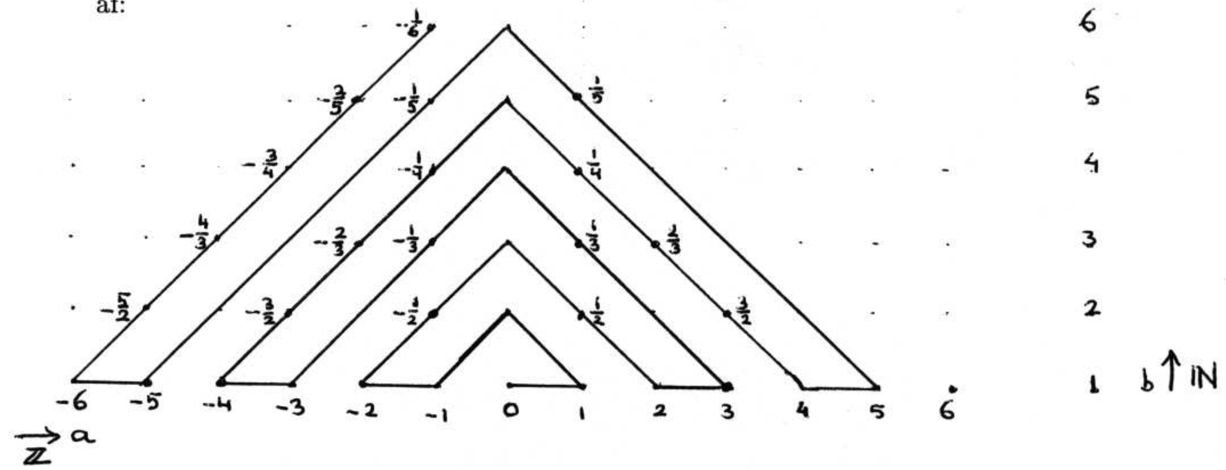
5.4 Aantal

We zeggen dat de verzamelingen V en W *evenveel elementen* (dezelfde *kardinaliteit*) hebben als er een bijectie van V naar W bestaat. Notatie: $|V| = |W|$. De verzameling heet *eindig* als $|V| = |\{1, 2, \ldots, n\}|$ voor een natuurlijk getal n of $V = \emptyset$. We schrijven dan $|V| = n$ resp. $|V| = 0$. Verder heet V *aftelbaar oneindig* als $|V| = |\mathbf{N}|$ en *overaftelbaar* als V niet eindig en niet aftelbaar oneindig is.
Dezelfde kardinaliteit hebben is een equivalentierelatie:
reflexiviteit: de identieke afbeelding op V is een bijectie.
symmetrie: er is een bijectie van V op W als en alleen als er een bijectie is van W op V. (Opgave)
transitiviteit: uit bovenstaande stelling volgt dat de samenstelling van twee bijecties een bijectie is.

Voor de bepaling van de kardinaliteit van een verzameling V is het dus voldoende een bijectie te vinden van V op een verzameling met reeds bekende kardinaliteit. We onderzoeken de kardinaliteit van $\mathbf{Z}$, $\mathbf{Q}$ en $\mathbf{R}$.

$\mathbf{Z}$. De gehele getallen zijn aftelbaar oneindig. Een bijectie f wordt gegeven door $f(1) = 0, f(2) = -1, f(3) = 1, f(4) = -2, f(5) = 2$, enz. Dus de aftelling $0, -1, 1, -2, 2, -3, 3, \ldots$
$\mathbf{Q}$. De rationale getallen zijn aftelbaar oneindig. Elk rationaal getal is van de vorm $\frac{a}{b}$ met $a \in \mathbf{Z}, b \in \mathbf{N}$.

Beschouw het Carthesisch produkt $\mathbf{Z} \times \mathbf{N}$ en tel volgens onderstaand schema af:



Zo komt elk paar (a, b) met een $a \in \mathbf{Z}$, $b \in \mathbf{N}$ aan de beurt, dus ook elke breuk a/b. Als een breuk al eerder voorgekomen is, slaan we hem over. Zo krijgen we een aftelling van $\mathbf{Q}$: $0, 1, -1, -2, -\frac{1}{2}, \frac{1}{2}, 2, 3, \frac{1}{3}, -\frac{1}{3}, -3, -4, -\frac{3}{2}, -\frac{2}{3}, -\frac{1}{4}, \ldots$

$\mathbf{Q}$ heeft dus evenveel elementen als $\mathbf{N}$.

$\mathbf{R}$. Cantor toonde in 1874 aan dat de reële getallen niet aftelbaar zijn. Dat is als volgt in te zien met behulp van decimale ontwikkelingen. Als $\mathbf{R}$ aftelbaar is, zijn de reële getallen x met $0 < x < 1$ dat ook. (Waarom?)
Schrijf zo'n aftelling op:
$x_1 = 0,3672958325311111\ldots$
$x_2 = 0,7248830001472583 2\ldots$
$x_3 = 0,3141592654183795 6\ldots$
$x_4 = 0,1414213562815370 2\ldots$
$x_5 = 0,6931471883951426 6\ldots$
$x_6 = 0,7777777124356789 0\ldots$
$x_7 = \ldots$
We construeren nu een getal y dat niet in de aftelling kan voorkomen. We nemen 4 voor de i-de decimaal van y als de i-de decimaal van x_i 7 is, en anders 7. In bovenstaand voorbeeld vinden we $y = 0,777774\ldots$ Dit rationale getal kan niet in de aftelling voorkomen. (Waarom niet?).

5.5 Bewijzen.

Veel beweringen zijn van de vorm: als A, dan B. Vaak is de formulering anders. Zo kun je de bewerking: 'elke a heeft b' ook formuleren als 'als je a hebt, heb je b'.

Het bewijzen van $A \Rightarrow B$ maakt vaak gebruik van de transitiveit van de implicatie: als $A \Rightarrow C$, $C \Rightarrow D$, $D \Rightarrow E$,..., $P \Rightarrow Q$ en $Q \Rightarrow B$, dan is $A \Rightarrow B$. De juistheid van deze redenering wordt duidelijk als je $A \Rightarrow B$ leest als: de verzameling van objecten met eigenschap A is een deelverzameling van de objecten met eigenschap B.

Het is belangrijk je te realiseren dat $A \Rightarrow B$ niet betekent dat B waar is. Als je wilt bewijzen dat B waar is, is het niet genoeg $A \Rightarrow B$ te bewijzen, maar zul je tevens moeten aantonen dat A waar is.

Bewijzen van equivalenties $A \Leftrightarrow B$ worden vaak gegeven door aan te tonen dat zowel $A \Rightarrow B$ als $B \Rightarrow A$ geldt.

Een bewijs uit het ongerijmde dat $A \Rightarrow B$ waar is, berust op het feit dat $A \Rightarrow B$ hetzelfde is als $\neg(A \wedge \neg B)$. Het komt erop neer dat je laat zien dat de veronderstelling $A \wedge \neg B$ tot een tegenspraak leidt.

Als je $A \Rightarrow B$ moet bewijzen, is het fundamenteel onjuist om met B te beginnen. Je begint dan aan te nemen wat je moet bewijzen. Toch kan het voor de analyse van het probleem wel nuttig zijn. Bij het opschrijven van het bewijs wordt zo'n kreeftengang niet geaccepteerd. Je kunt wel met $\neg B$ beginnen en aantonen dat $\neg A$ volgt.

Een bruikbaar principe bij bewijzen is het '*ladenprincipe*' (box principle): als je $n + 1$ ballen in n laden stopt, bevat één van de laden (tenminste) 2 ballen.

5.6 Axioma's. (AO)

De meeste axioma's zijn onomstreden. Dat geldt bijv. voor de definities van de natuurlijke getallen en de gehele getallen. Alleen beperkte richtingen in het grondslagenonderzoek, het intuïtionisme en het constructivisme, vinden dat de axioma's te veel toelaten. Er zijn echter een paar axioma's die tot veel discussies onder wiskundigen hebben geleid.
De meeste wiskundigen vinden het gebruik van het keuzeaxioma toegestaan, maar sommigen vinden dat onjuist. Het *keuzeaxioma* zegt het volgende: het Carthesisch product van willekeurig veel niet-lege verzamelingen is niet leeg. Als het gaat om eindig veel verzamelingen, is er geen probleem en is de kardinaliteit van het product gelijk aan het product van de kardinaliteiten: (eindig($\neq 0$)$\times$ aftelbaar oneindig = aftelbaar oneindig $\times$ aftelbaar oneindig = aftelbaar oneindig; eindig $\times$ overaftelbaar = overaftelbaar, enz.) Als er aftelbaar oneindig veel verzamelingen in het geding zijn, is er nog geen echt probleem. Maar het probleem schuilt vooral in het Carthesisch product van overaftelbaar veel niet-lege verzamelingen.

Het andere omstreden axioma is de zg. continuumhypothese. Ter inleiding bewijs ik dat voor elke verzameling V geldt dat de kardinaliteit van de verzameling van deelverzamelingen van V (echt) groter is dan $|V|$, notatie $2^{|V|} > |V|$. Er is dus wel een injectie van V naar de deelverzamelingen van V, nl. $v \to \{v\}$, maar geen surjectie. Stel er is een surjectie $f : V \to 2^V$. Beschouw dan $W = \{v \in V | v \notin f(v)\}$. Dit is een deelverzameling van V, dus het beeld van een element $w \in V$ onder de surjectie f.

Als $w \in W$, dan is $w \notin f(w) = W$.
Als $w \notin W$, dan is w per definitie een element van $f(w) = W$.

De tegenspraak bewijst dat er geen surjectie is.

Het aantal deelverzamelingen van $\mathbf{N}$ is gelijk aan het aantal aftelbare rijtjes van nullen en enen; immers je beslist van elk natuurlijk getal of het wel (1) of niet (0) tot de deelverzameling behoort. Dus $2^{|\mathbf{N}|} = |\mathbf{R}|$. Cantor opperde de zg. *continuumhypothese* dat er geen kardinaalgetallen tussen $|\mathbf{N}|$ en $|\mathbf{R}|$ liggen. De *algemene continuumhypothese* zegt dat er geen kardinaalgetallen liggen tussen $|\mathbf{N}|$, $|\mathbf{R}|$, $2^{|\mathbf{R}|}$, $2^{2^{|\mathbf{R}|}}$, enz. Gödel (1906-1978) bewees in de dertiger jaren dat je een consistente (=tegenspraakvrije) wiskunde krijgt als je de continuumhypothese als axioma accepteert. P.J. Cohen (1934-) bewees in de zestiger jaren dat je ook een consistente wiskunde kunt construeren met kardinaalgetallen tussen $|\mathbf{N}|$ en $|\mathbf{R}|$.

In het begin van deze eeuw veroorzaakte de Britse filosoof Bertrand Russell (1872-1970) verwarring met de volgende paradox: 'Beschouw de verzameling V van alle verzamelingen die zichzelf niet bevatten. Als V zichzelf bevat, bevat V zichzelf niet. Als V niet zichzelf bevat, bevat V zichzelf wel.'

Om uit deze draaikolk te blijven, is het niet geaccepteerd om over de 'verzameling van alle verzamelingen' te praten. Ook kan een verzameling zichzelf niet bevatten. Een verzameling kan wel element zijn van een hoger soort verzamelingen zijn. Dit verklaart het onderscheid tussen $\in$ en $\subset$.

Literatuur bij dit hoofdstuk:

P.R. Halmos, *Naive Set Theory*, Springer-Verlag, 1974.

Opgaven bij Hoofdstuk 5. Logica en verzamelingenleer.

5.1 Gegeven zijn de beweringen: $A : 3 \leq 3$, $B : 3 \leq 4$, $C : 3^{3^3} < 10^6$.
Welke van de volgende beweringen zijn waar?
(i) B en C, (ii) A of B, (iii) als A, dan C (iv) als C, dan A, (v) $\neg A \Longleftrightarrow \neg B$.

5.2 Werk de negaties uit van de volgende beweringen:

a) $\forall x : A(x) \wedge B(x)$,

b) $\forall x \exists y : x > y + 1$,

c) $\forall x \exists y \forall z : A(x, y) \Longrightarrow B(z)$.

5.3 Welke van de volgende beweringen zijn waar, als $x, y, z \in \mathbf{R}$?

a) $\forall x \exists y \forall z : x = yz$,

b) $\exists x \forall y \exists z : x = yz$,

c) $\forall x \forall y \exists z : x = yz$.

5.4 Formuleer de negaties van de volgende beweringen:

a) elk even getal > 2 is de som van twee priemgetallen,

b) als $a + b$ priem is, is a of b oneven,

c) a is rood als en alleen als b rood is.

5.5. Gegeven is dat U, V, W deelverzamelingen zijn van X.
Bewijs a) $(V \cap W)^c = V^c \cup W^c$, b) $U \cap (V \cup W) = (U \cap V) \cup (U \cap W)$.

5.6 Teken in $\mathbf{R}^2$ de relatie a) $\{(x, y) | x^2 \leq -y^2\}$, b) $\{(x, y) | x^2 \leq y^2\}$.

5.7 Zijn de volgende relaties tussen a en b (i) reflexief, (ii) symmetrisch, (iii) transitief?

a) $a + b$ is even $(a, b \in \mathbf{Z})$

b) a is een deler van b $(a, b \in \mathbf{Z})$

c) $a - b$ is deelbaar door 7 $(a, b \in \mathbf{Z})$

d) $a + b \in \mathbf{Z}$ $(a, b \in \mathbf{R})$

e) $a - b \in \mathbf{Z}$ $(a, b \in \mathbf{R})$

5.8 Geef bij elke equivalentierelatie onder 5.7 een volledig stel representanten.

5.9 Ga na of de volgende functies (i) injectief, (ii) surjectief zijn.

a) $f : \mathbf{R} \to \mathbf{R}, f(0) = 0, f(x) = \frac{1}{x}$ voor $x \neq 0$,

b) $f : \mathbf{R}^2 \to \mathbf{R}^2, f(x, y) = (y, -x)$,

c) $f : \mathbf{R} \to \mathbf{R}, f(x) = 13x$,

d) $f : \mathbf{Z} \to \mathbf{Z}, f(x) = 13x$.

5.10 Bepaal van de bijectieve functies uit 5.9 de inverse.

5.11 Zij $f : V \to W$ bijectief met inverse functie g. Bewijs:

a) $g \circ f : V \to V$ gegeven door $g \circ f(v) = g(f(v))$ is de identieke afbeelding op V.

b) $f \circ g : W \to W$ is de identieke afbeelding op W.

c) g is bijectief met f als inverse functie.

5.12. Als er een injectie $f : A \to B$ bestaat, schrijven we dat $|A| \leq |B|$.

a) Stel $f : A \to B$ is surjectief. Bewijs dat dan $|B| \leq |A|$.

b) Bewijs: Als $|A| \leq |B|$ en $|B| \leq |A|$ zijn, dan hebben A en B dezelfde kardinaliteit.

5.13. a) Toon aan dat $\mathbf{Z}^2$ aftelbaar is.

b) Laat zien dat de oneindige rijtjes van nullen en enen dezelfde kardinaliteit als $\mathbf{R}$ hebben.

5.14. a) Als je 11 gehele getallen hebt, zijn er twee waarvan het verschil door 10 deelbaar is.

b) Als je 11 getallen uit $\{1, ..., 20\}$ kiest, is één een veelvoud van een ander uit die 11.

5.15 Kun je uit $A \Longrightarrow B$ en $\neg A$ concluderen dat B niet waar is?

5.16 Wat is fout in de volgende redenering?
We bepalen x zó dat $\sqrt{x + \sqrt{x + \sqrt{x + ...}}} = 1$.
Kwadrateren geeft $x + \sqrt{x + \sqrt{x + ...}} = 1$.
Dus $x + 1 = 1$. Hieruit volgt $x = 0$.

6 HOOFDSTUK: DE REËLE GETALLEN

6.1 Axioma's voor R.

Het was al in de tijd van de klassieke oudheid duidelijk dat niet alle reële getallen rationaal zijn. Het is gemakkelijk om bij gegeven lengte 1 een lijnstuk ter lengte $\sqrt{2}$ te construeren en de Grieken wisten dat dit getal niet rationaal was. Pas in de tweede helft van de negentiende eeuw werden bevredigende definities van **R** gegeven, en wel drie verschillende door Karl Weierstrass (1815-1897), Georg Cantor (1845-1918) en Richard Dedekind (1831-1916). In 1889 stelde Guiseppe Peano (1858-1932) axioma's op voor de natuurlijke getallen (en daarmee voor de rationale getallen) en deze axioma's tezamen met Dedekind's theorie verschaft een solide en geaccepteerd fundament voor de reële getallen. Daarbij worden de reële getallen gedefinieerd als de kleinste uitbreiding van de rationale getallen die nog aan het volledigheidsaxioma voldoet.
Voordat we dit axioma formuleren, voeren we enkele begrippen in.

Stel we hebben een verzameling K met de volgende eigenschappen:
Aan elk paar getallen $x,\ y \in K$ wordt een som $x + y \in K$ en een product $xy \in K$ toegekend zó dat voor alle $x, y, z \in K$ geldt:

- (commutativiteit) $x + y = y + x$, $xy = yx$
- (associativiteit) $x + (y + z) = (x + y) + z$, $x(yz) = (xy)z$
- (distributiviteit) $x(y + z) = xy + xz$
- (bestaan neutrale elementen) Er bestaan getallen 0 en 1 in K zó dat voor elke x in K geldt dat $x + 0 = x$ en $1 \cdot x = x$
- (bestaan inversen) Bij elke $x \in K$ bestaat een $y \in K$ met $x + y = 0$; bij elke $x \in K$, $x \neq 0$ bestaat een $y \in K$ met $xy = 1$

We schrijven $-x$ voor de eerste y en x^{-1} voor de tweede.

Vanwege bovenstaande eigenschappen noemen we K een *lichaam*. De volgende extra eisen maken van K een *geordend lichaam*.
Er bestaat een deelverzameling K^+ van K, de zg. *positieve getallen*, zo dat

- voor elke $x,\ y \in K^+$ geldt $x + y \in K^+$ en $xy \in K^+$
- voor elke $x \in K$, $x \neq 0$ geldt òf $x \in K^+$ òf $-x \in K^+$
- $0 \notin K^+$.

Merk op dat zowel **Q** als **R** bovenstaande eigenschappen bezitten. De laatste drie stellen ons in staat de elementen van K naar grootte te ordenen. Daartoe definiëren we

$$x < y \iff y > x \iff y - x \in K^+$$

$$x \leq y \iff y \geq x \iff \{x < y \ \text{ of } \ x = y\}.$$

Hieruit volgt direct dat voor elk paar $x, y \in K$ geldt $x < y$ òf $x = y$ òf $x > y$.

We schrijven $x < y \leq z$ in plaats van $\{x < y$ en $y \leq z\}$, enz.

Stel $Y \subset K$. Als er een $b \in K$ is met $y \leq b$ voor alle $y \in Y$, dan heet b een *bovengrens* voor Y en heet Y *naar boven begrensd.* Als b een bovengrens is voor Y, is elk getal groter dan b dat ook. Soms is er een kleinste bovengrens, bijvoorbeeld voor alle getallen $y \in K$ met $y \leq 1$. Soms is er geen kleinste bovengrens. Er is geen kleinste bovengrens als $Y = \emptyset$. Verder is er bijv. geen kleinste bovengrens als $X = \mathbf{Q}$ en $Y = \{y \mid y^2 < 2\}$. Immers een rationaal getal q met $q^2 < 2$ is geen bovengrens en een rationaal getal q met $q^2 > 2$ is wel een bovengrens, maar niet de kleinste.
Een geordend lichaam K heet *volledig* als elke niet-lege, naar boven begrensde verzameling Y een kleinste bovengrens in K heeft.

Volledigheidsaxioma: *De reële getallen*, $\mathbf{R}$, vormen het kleinste volledige geordende lichaam dat $\mathbf{Q}$ bevat.

Men kan bewijzen dat $\mathbf{R}$ uniek bepaald is. Als Y een niet-lege naar boven begrensde deelverzameling van $\mathbf{R}$ is, heeft Y dus een kleinste bovengrens of *supremum*, notatie sup Y. Zo schrijven we voor $Y = \{y \in \mathbf{R} \mid y^2 < 2\}$ dat sup $Y = \sqrt{2}$. Als het supremum tot Y hoort, noemen we dit het *maximum* van Y, notatie max Y. Dus als $Y = \{ y \in \mathbf{R}, y \leq 1\}$, dan is sup Y = max $Y = 1$.
We definiëren analoog dat $l \in X$ een *ondergrens* is voor $Y \subseteq K$ als $l \leq y$ voor alle $y \in Y$, en dat Y*naar beneden begrensd* is als Y een ondergrens heeft. Door het volledigheidsaxioma op $-Y$ toe te passen vinden we dat elke niet-lege, naar beneden begrensde deelverzameling Y van $\mathbf{R}$ een *grootste ondergrens* of *infimum* heeft, notatie inf Y. Als dit getal een element van Y is, spreken we over het *minimum* van Y, notatie min Y.

Voorbeelden. 1. inf $\mathbf{R}^+ = 0$ en sup $\mathbf{R}^+$ is niet gedefinieerd. Vaak schrijven we sup $Y = \infty$ voor een niet naar boven begrensde verzameling en inf $Y = -\infty$ voor een niet naar beneden begrensde verzameling; dus sup $\mathbf{R} = \infty$, inf $\mathbf{R} = -\infty$.
2. Als $Y = \{ y \mid 0 \leq y < 1\}$, dan is inf Y = min $Y = 0$, sup $Y = 1$.

Stel dat een supremum geen maximum is. Dan wordt het willekeurig dicht benaderd door elementen uit de verzameling. Zij $Y \subseteq \mathbf{R}$. Stel sup $Y = b$. Als $b \in Y$, dan is b = max Y. Als $b \notin Y$, dan is voor elk getal $\epsilon > 0$ het getal $b - \epsilon$ geen bovengrens. Dus is er een $y \in Y$ met $y > b - \epsilon$. In het bijzonder is er voor elk natuurlijk getal n een $y_n \in Y$ met $b - \frac{1}{n} < y_n < b$. We zeggen dat de rij $y_1, y_2, ...$ naar b *convergeert.* (Als sup $Y = \infty$, dan kun je voor elke $n \in \mathbf{N}$ een $y_n \in Y$ vinden met $y_n > n$; we zeggen dat $y_1, y_2, ...$ *naar* ∞ *gaat.*)

Stelling 6.1. (Archimedische eigenschap van $\mathbf{R}$).
Als $a, b \in \mathbf{R}^+$, dan bestaat een natuurlijk getal n met $na > b$.

Bewijs. Beschouw $Y := \{ \ y \mid y \leq ba^{-1}\}$. Dit is een naar boven begrensde verzameling met maximum ba^{-1}. Omdat $\sup \mathbf{N} = \infty$, moet er een $n \in \mathbf{N}$ zijn met $n \notin Y$. Dan geldt dus $n \ > \ ba^{-1}$, ofwel $na > b$. $\square$

De archimedische eigenschap hebben we al bij Stelling 1.1 (deling met rest) voor natuurlijke getallen toegepast. We gebruiken het nu voor de *insluitingsstelling.*
Stelling 6.2. Als reële getallen a, b en x voldoen aan

$$a - \frac{b}{n} \ < \ x \ < \ a + \frac{b}{n},$$

voor elk natuurlijk getal n, dan is $x = a$.

Bewijs. Stel $x > a$. Kies met behulp van Stelling 6.1 een natuurlijk getal n zó dat $n(x-a) \ > \ b$. Voor deze n geldt $x \ > \ a + \frac{b}{n}$. Tegenspraak. De veronderstelling $x < a$ leidt evenzo tot een tegenspraak. $\square$

6.2 Metrische ruimten.

In deze paragraaf worden topologische eigenschappen behandeld. In de *topologie* spelen de begrippen open, gesloten en volledig een belangrijke rol. We beginnen met het invoeren van een afstandsbegrip.
Laat X een willekeurige verzameling zijn. De elementen noemen we *punten.*
Definitie. Een functie $d : X \times X \to \mathbf{R}$ heet een *metriek* op X als

$$(i) \quad \forall x, y \in X : \quad d(x,y) \geq 0 \ \text{ en } \ d(x,y) = 0 \Longleftrightarrow x = y.$$

$$(ii) \quad \forall x, y \in X : \qquad d(x,y) = d(y,x).$$

$$(iii) \ \forall x, y, z \in X : d(x,z) \leq d(x,y) + d(y,z) \ \ \text{(driehoeksongelijkheid)}.$$

Als $d : X \times X \to \mathbf{R}$ een metriek is, dan heet het paar (X, d) een *metrische ruimte.*

Het is duidelijk dat op een verzameling X meerdere metrieken kunnen zijn gedefinieerd. Toch spreekt men vaak over de metrische ruimte X i.p.v. over de metrische ruimte (X, d). Aangenomen is dan dat over de stilzwijgend gemaakte keuze van de metriek d geen misverstand bestaat. In het vervolg is X nu steeds een metrische ruimte met metriek d.

Voorbeeld. $X = \mathbf{R}$ is de verzameling van de reële getallen met $d(x,y) = |x - y|$. Tenzij anders vermeld is dit de gebruikte metriek van $\mathbf{R}$.

Opmerking. Iedere deelverzameling van een metrische ruimte is met dezelfde metriek weer een metrische ruimte.

Definities. Laat $A \subseteq X$.
(i) Een punt $a \in A$ heet een *inwendig punt* van A als

$$\exists \delta > 0 : B_\delta(a) := \{x \in X : d(x,a) < \delta\} \subseteq A.$$

De verzameling $B_\delta(a)$ heet de *open bol* met straal δ en middelpunt a.
(ii) Een punt $a \in A$ heet een *geïsoleerd punt* van A als

$$\exists \delta > 0 : \ B_\delta(a) \cap A = \{a\}.$$

(iii) Een punt $a \in X$ heet een *ophopingspunt* van A als

$$\forall \delta > 0 \ \exists p \in A : \quad p \neq a \quad \text{en} \quad d(a,p) < \delta.$$

(iv) Als elk punt van A een inwendig punt van A is, dan heet A een *open deelverzameling* van X.
(v) Als het *complement* van A,

$$A^c := X - A := \{x \in X : x \notin A\},$$

open is, dan heet A een *gesloten deelverzameling* van X.

In het vervolg zullen we kortweg zeggen dat A open (gesloten) is als A een open (gesloten) deelverzameling van X is.
(vi) Een punt $a \in X$ heet een *randpunt* van A als elke open bol met middelpunt a zowel een punt van A als een punt van A^c bevat.
(vii) Een punt $a \in X$ heet een *uitwendig punt* van A als er een open bol om a is die geheel tot A^c behoort.

Stelling 6.3. (i) Iedere open bol is een open verzameling.
(ii) Een verzameling A in X is open dan en slechts dan als A een vereniging van open bollen is.

Bewijs: Opgave.

Stelling 6.4. (i) X is open; de lege verzameling is open.
(ii) De vereniging van elke collectie open deelverzamelingen is open.
(iii) De doorsnede van elk eindig aantal open deelverzamelingen is open.

Bewijs: (i) Neem een punt van X. Neem een bol met straal 1 om dat punt. Omdat elk punt tot X behoort, ligt die bol in X. Dus elk punt van X is

inwendig punt van X. Hieruit volgt dat X open is. Omdat $\emptyset$ geen punten bevat, is elk punt inwendig punt. Dus $\emptyset$ is open.
(ii) Zij $\cup_\alpha \mathcal{O}_\alpha$ de vereniging van open verzamelingen $\mathcal{O}_\alpha$. Stel $a \in \cup_\alpha \mathcal{O}_\alpha$. Dan $a \in \mathcal{O}_\alpha$ voor zekere α. Omdat $\mathcal{O}_\alpha$ open is, is er een bol $B_\delta(a)$ die helemaal in $\mathcal{O}_\alpha$, en dus ook in $\cup_\alpha \mathcal{O}_\alpha$ ligt. Dus a is inwendig punt van $\cup_\alpha \mathcal{O}_\alpha$. Hieruit volgt dat $\cup_\alpha \mathcal{O}_\alpha$ open is .
(iii) Zij $\cap_{i=1}^n \mathcal{O}_i$ de eindige doorsnede van open verzamelingen $\mathcal{O}_i$. Zij $a \in \cap_{i=1}^n \mathcal{O}_i$. Dan is $a \in \mathcal{O}_i$ voor $i = 1, ..., n$. Omdat elke $\mathcal{O}_i$ open is, is er voor elke i een $\delta_i > 0$ met $B_{\delta_i}(a) \subseteq \mathcal{O}_i$. Kies $\delta = \min_{i=1,...,n} \delta_i$. Dan $\delta > 0$ en $B_\delta(a) \subseteq \mathcal{O}_i$ voor $i = 1, ..., n$. Dus $B_\delta(a) \subseteq \cap_{i=1}^n \mathcal{O}_i$. Nu blijkt dat a inwendig punt is van $\cap_{i=1}^n \mathcal{O}_i$. Dus $\cap_{i=1}^n \mathcal{O}_i$ is open . $\Box$

Stelling 6.5. (i) X is gesloten, de lege verzameling is gesloten.
(ii) De doorsnede van elke collectie gesloten deelverzamelingen is gesloten.
(iii) De vereniging van elk eindig aantal gesloten verzamelingen is gesloten.

Bewijs. Opgave.

Stelling 6.6. Laat $A \subseteq X$. Dan is A gesloten dan en slechts dan als A al zijn ophopingspunten bevat.

Bewijs. Neem eerst aan dat A gesloten is en laat p een ophopingspunt zijn van A. We moeten laten zien dat $p \in A$. Stel niet. Dan $p \in A^c$. Maar A^c is open, dus p is een inwendig punt van A^c. Zodoende is er een $\delta > 0$ waarvoor $B_\delta(p) \subseteq A^c$, in tegenspraak met de veronderstelling dat p een ophopingspunt is van A. Dus p ligt wel in A.
Neem vervolgens aan dat A een verzameling is die al zijn ophopingspunten bevat. We tonen aan dat A gesloten is door te bewijzen dat A^c open is. Zij $p \in A^c$. Dan is p geen ophopingspunt van A, dus er is een $\delta > 0$ zo dat $B_\delta(p)$ geen punten van $A - \{p\} := \{x \in A : x \neq p\}$ bevat, en wegens $p \in A^c$ betekent dit dat $B_\delta(p) \subseteq A^c$, m.a.w. p is een inwendig punt van A^c. Dit geldt voor elke $p \in A^c$, en dus is A^c open. $\Box$

Definitie. Een rij $(x_n)_{n=1}^\infty$ in X heet *convergent* als er een $x_0 \in X$ is zo dat

$$\forall \epsilon > 0 \ \exists n_\epsilon \in \mathbf{N} : n \geq n_\epsilon \Longrightarrow d(x_n, x_0) < \epsilon.$$

Het punt x_0 heet de *limiet* van de rij.

Stelling 6.7. Als de rij $(x_n)_{n=1}^\infty$ in X convergent is, dan is de limiet x_0 eenduidig bepaald.

Notatie $\lim_{n\to\infty} x_n = x_0$ of $x_n \to x_0$.

Bewijs. Neem aan dat de rij twee verschillende limieten heeft, zeg x_0 en x_0'. Omdat $x_0 \neq x_0'$, is $d(x_0, x_0') > 0$. Kies $0 < \epsilon < \frac{1}{2}d(x_0, x_0')$. Dan is er een n_ϵ zo dat $d(x_n, x_0) < \epsilon$ voor alle $n \geq n_\epsilon$. Evenzo is er een n_ϵ' zo dat $d(x_n, x_0') < \epsilon$ voor alle $n \geq n_\epsilon'$. Met behulp van de driehoeksongelijkheid volgt nu

$$d(x_0, x_0') \leq d(x_0, x_n) + d(x_n, x_0') < \epsilon + \epsilon < d(x_0, x_0')$$

voor $n \geq \max(n_\epsilon, n_\epsilon')$, tegenspraak. □

In plaats van de rij $(x_n)_{n=1}^\infty$ is convergent, zegt men ook wel dat $\lim_{n\to\infty} x_n$ bestaat en eindig is.

Stelling 6.8. Als de rij $(x_n)_{n=1}^\infty$ in X convergent is, dan is de rij begrensd, d.w.z. bevat in een (open) bol $B_\delta(a)$ voor zekere $a \in X, \delta \in \mathbf{R}_{>0}$.

Bewijs. Omdat $(x_n)_{n=1}^\infty$ convergeert, is er een $x_0 \in X$ zó dat er een n_1 bestaat met $n \geq n_1 \Longrightarrow d(x_n, x_0) < 1$. Kies

$$M = \max(d(x_1, x_0), d(x_2, x_0), ..., d(x_{n_1 - 1}, x_0), 1).$$

Dan is $d(x_n, x_0) \leq M$ voor alle n . □

Stelling 6.9. Laat $A \subseteq X$ gesloten zijn. Als de rij $(x_n)_{n=1}^\infty$ in A convergent is in X, dan ligt de limiet in A.

Bewijs. Opgave.

Stelling 6.10. Laat $A \subseteq X$ en $p \in X$. De volgende drie uitspraken zijn equivalent:
(i) p is een ophopingspunt van A.
(ii) Er bestaat een rij $(a_n)_{n=1}^\infty$ in $A - \{p\}$ die convergent is met p als limiet.
(iii) Iedere (niet-lege) open bol met middelpunt p bevat oneindig veel punten van A.

Bewijs. (i) $\Longrightarrow$ (ii). Neem aan dat p een ophopingspunt van A is. We construeren de rij $(a_n)_{n=1}^\infty$ in A. Kies voor elk natuurlijk getal n een $a_n \in A - \{p\}$ met $d(a_n, p) < 2^{-n}$. Dan is $(a_n)_{n=1}^\infty$ een rij in $A - \{p\}$ die convergeert naar p.
(ii) $\Longrightarrow$ (iii) Stel (ii) geldt en $\mathcal{O}_1$ is een open bol met middelpunt p en straal r. Dan is p een inwendig punt van $\mathcal{O}_1$. Omdat $(a_n)_{n=1}^\infty$ naar p convergeert, is er een n_1 met $a_{n_1} \in \mathcal{O}_1$. Zij $\mathcal{O}_2$ de open bol met middelpunt p en straal

$d(a_{n_1}, p)/2$. Dan is de straal positief en kiezen we een $n_2 > n_1$ met $a_{n_2} \in \mathcal{O}_2$. Zo doorgaande krijgen we een oneindige rij van onderling verschillende punten die alle in $\mathcal{O}_1$ bevat zijn.
(iii) $\Longrightarrow$ (i) volgt direct uit de definitie van ophopingspunt. $\square$

6.3 Rijkompakte verzamelingen.

We definiëren verzamelingen A met de eigenschap dat elke rij in A een deelrij heeft die in A convergeert.
Definitie. Laat $(x_n)_{n=1}^{\infty}$ een rij zijn in X.
(i) Als $(n_k)_{k=1}^{\infty}$ een strict stijgende rij natuurlijke getallen is, dan heet de rij $(x_{n_k})_{k=1}^{\infty}$ een *deelrij* van $(x_n)_{n=1}^{\infty}$.
(ii) Als $x_0 \in X$ de limiet is van een convergente deelrij van $(x_n)_{n=1}^{\infty}$, dan heet x_0 een *limietpunt* (ook wel: rijophopingspunt) van $(x_n)_{n=1}^{\infty}$.

Stelling 6.11. Een rij $(x_n)_{n=1}^{\infty}$ in X heeft een convergente deelrij met limiet x_0 dan en slechts dan als

$$\forall \epsilon > 0 \ \forall n \ \exists k \geq n : \quad d(x_k, x_0) < \epsilon.$$

Bewijs. Opgave.

Definitie. Laat $A \subseteq X$. Dan heet A *rijkompakt* als iedere rij in A een deelrij heeft die convergent is met limiet in A.

Stelling 6.12. A is rijkompakt dan en slechts dan als iedere rij in A een limietpunt in A heeft.

Bewijs. Opgave.

Er is nog een andere definitie van kompaktheid. Deze is in termen van open verzamelingen in plaats van rijen. In paragraaf 6.6 wordt deze definitie gegeven en aangetoond dat beide definities in metrische ruimten equivalent zijn.

Stelling 6.13. Gesloten deelverzamelingen G van rijkompakte verzamelingen zijn weer rijkompakt.

Bewijs. Stel dat $(a_n)_{n=1}^{\infty}$ een rij is in G. Omdat A rijkompakt is, bestaat er een convergente deelrij met limiet in A. Daar G gesloten is, ligt de limiet in G volgens Stelling 6.9. Conclusie: elke rij in G heeft een convergente deelrij met limiet in G. $\square$

Stelling 6.14. Laat A een rijkompakte deelverzameling zijn van X. Dan is A gesloten en begrensd.

Bewijs. Opgave.

6.4 Volledigheid.

Definitie. Een rij $(x_n)_{n=1}^{\infty}$ in X heet een Cauchyrij als

$$\forall \epsilon > 0 \; \exists n_\epsilon : m, n \geq n_\epsilon \Longrightarrow d(x_m, x_n) < \epsilon.$$

Stelling 6.15. Iedere convergente rij is een Cauchyrij.

Bewijs. Zij $(x_n)_{n=1}^{\infty}$ een convergente deelrij met limiet x_0. Laat $\epsilon > 0$, en gebruik de definitie van convergentie met $\frac{1}{2}\epsilon$. Dan

$$\forall m, n \geq n_{\frac{1}{2}\epsilon} : \; d(x_m, x_n) \leq d(x_m, x_0) + d(x_0, x_n) < \frac{1}{2}\epsilon + \frac{1}{2}\epsilon = \epsilon.$$

$\epsilon > 0$ was willekeurig. Dus is de rij een Cauchyrij. □

Stelling 6.16. Iedere Cauchyrij is begrensd.

Bewijs. Opgave.

Stelling 6.17. Als een Cauchyrij een limietpunt heeft, dan is de Cauchyrij convergent.

Bewijs. Laat $(x_n)_{n=1}^{\infty}$ een Cauchyrij zijn die een convergente deelrij heeft. Laat $\epsilon > 0$ en gebruik de definitie van Cauchyrij. Dus

$$\forall m, n \geq n_\epsilon : \; d(x_m, x_n) < \frac{1}{2}\epsilon.$$

Anderzijds, omdat de rij een convergente deelrij heeft, zeg met limiet x_0, bestaat er een $k_\epsilon > n_\epsilon$ zodat

$$d(x_{k_\epsilon}, x_0) < \frac{1}{2}\epsilon.$$

Beide ongelijkheden combinerend vinden we

$$\forall n \geq n_\epsilon : \ d(x_n, x_0) \leq d(x_n, x_{k_\epsilon}) + d(x_{k_\epsilon}, x_0) < \frac{1}{2}\epsilon + \frac{1}{2}\epsilon = \epsilon.$$

□

We geven nu een definitie van volledigheid die ook opgaat voor metrische ruimten die niet geordend zijn, dit in tegenstelling met sectie 6.1.

Definitie. Als iedere Cauchyrij in X convergent is, dan heet X *volledig*.

Om na te gaan of een rij $(x_n)_{n=1}^\infty$ in een volledige metrische ruimte X convergent is, hoeft men slechts na te gaan dat de rij een Cauchyrij is. Daarbij is het niet nodig om a priori de limietwaarde te kennen. Het bewijs van een belangrijke stelling in de analyse, de Banach contractiestelling, berust op dit principe. Zie paragraaf 7.

De volgende stelling geeft op een andere manier weer wat de essentie is van het volledig zijn van X.

Stelling 6.18. (Cantor) Een metrische ruimte X is volledig dan en slechts dan als voor elke dalende rij niet-lege gesloten deelverzamelingen

$$F_1 \supseteq F_2 \supseteq F_3 ...,$$

met de eigenschap dat

$$\mathrm{diam}(F_n) := \sup_{x,y \in F_n} d(x,y) \to 0 \ \text{ als } \quad n \to \infty,$$

geldt dat de doorsnede $\cap_{n=1}^\infty F_n$ precies één punt bevat.

Bewijs. Stel X is volledig. Kies voor elk natuurlijk getal n een punt x_n uit F_n. Dan is $(x_n)_{n=1}^\infty$ een rij in F_1. Bij elke $\epsilon > 0$ bestaat een n_ϵ zó dat $d(x,y) < \epsilon$ als $x, y \in F_{n_\epsilon}$. In het bijzonder geldt $d(x_m, x_n) < \epsilon$ als $m, n \geq n_\epsilon$. Dus $(x_n)_{n=1}^\infty$ is een Cauchyrij. Omdat X volledig is, heeft $(x_n)_{n=1}^\infty$ een limiet x_0. Merk op dat $(x_n)_{n=m}^\infty$ een rij in F_m is voor $m \in \mathbf{N}$. Omdat F_m gesloten is, is dan ook $x_0 \in F_m$ voor $m \in \mathbf{N}$. Dus $x_0 \in \cap_{m=1}^\infty F_m$. De doorsnede bevat dus tenminste één punt.
Stel er is nog een ander punt x_0' in de doorsnede. Dan is $d(x_0, x_0') =: \epsilon > 0$. Er geldt $d(x_0, x_0') < \epsilon$ als $x_0, x_0' \in F_{n_\epsilon}$. Deze tegenspraak bewijst dat er niet nog een ander punt dan x_0 in de doorsnede zit.
Stel aan de voorwaarde van Stelling 6.18 is voldaan. Om te bewijzen dat X volledig is, beschouwen we een Cauchyrij $(x_n)_{n=1}^\infty$ in X. Defineer F_m

als de verzameling $\{x_m, x_{m+1}, ...\}$ verenigd met al haar randpunten. Dan voldoet $(F_m)_{m=1}^{\infty}$ aan de voorwaarde van de stelling (ga na). Nu volgt dat $\cap_{m=1}^{\infty} F_m = \{x_0\}$ voor zekere x_0. Dus $x_n, x_0 \in F_n$ en $d(x_n, x_0) \to 0$ als $n \to \infty$. Dit zegt dat $(x_n)_{n=1}^{\infty}$ naar x_0 convergeert. Dus X is volledig. $\square$

6.5 Het geval $X = \mathbf{R}$.

We hebben gezien dat rijkompakte deelverzamelingen van een metrische ruimte X gesloten en begrensd zijn. Als $X = \mathbf{R}$, geldt ook het omgekeerde. We laten dit eerst zien voor een gesloten begrensd interval.

Stelling 6.19. (Heine-Borel) Laat $a, b \in \mathbf{R}$. Dan is het gesloten begrensde interval

$$[a, b] = \{x \in \mathbf{R} : a \leq x \leq b\}$$

rijkompakt.

Bewijs. Laat $(x_n)_{n=1}^{\infty}$ een rij zijn in $[a, b]$. We moeten bewijzen dat deze rij een convergente deelrij heeft met limiet in $[a, b]$. We delen hiertoe het interval in twee gelijke stukken, d.w.z. in

$$[a, \frac{a+b}{2}] \quad \text{en} \quad [\frac{a+b}{2}, b].$$

Dan bevat tenminste één van deze twee intervallen voor oneindig veel waarden van n het rijelement x_n. Als we dit interval $[a_1, b_1]$ noemen, kunnen we dus een deelrij van $(x_n)_{n=1}^{\infty}$ kiezen die volledig bevat is in $[a_1, b_1]$. Noteer deze rij als $(x_n^1)_{n=1}^{\infty}$. Dit argument herhalende, krijgen we een dalende rij intervallen

$$[a, b] \supset [a_1, b_1] \supset [a_2, b_2] \supset [a_3 b_3] \supset ...,$$

en bijbehorende steeds verdere deelrijen, genoteerd als $(x_n^j)_{n=1}^{\infty}$, met de eigenschap dat de deelrij $(x_n^j)_{n=1}^{\infty}$ volledig bevat is in $[a_j, b_j]$.
Vervolgens nemen we de zogenaamde diagonaalrij, dat is de rij $(x_n^n)_{n=1}^{\infty}$. Dit is zelf weer een deelrij van de oorspronkelijke rij $(x_n)_{n=1}^{\infty}$, en er geldt dat $x_n^n \in [a_n, b_n]$.
Nu is $(a_n)_{n=1}^{\infty}$ een begrensde niet-dalende rij getallen, en $(b_n)_{n=1}^{\infty}$ een begrensde niet-stijgende rij getallen. Dus bestaan

$$\alpha = \sup_n a_n \quad \text{en} \quad \beta = \inf_n b_n,$$

met $a \leq \alpha \leq \beta \leq b$, en $\alpha, \beta \in [a_n, b_n]$ voor elk natuurlijk getal n.
Bovendien is $|\beta - \alpha| \leq b_n - a_n = 2^{-n}(b-a)$ voor elk natuurlijk getal n, dus $\alpha = \beta$.
Zij $\epsilon > 0$. Dan is er een n_ϵ zodat

$$\alpha - \epsilon < a_{n_\epsilon} \leq \alpha = \beta \leq b_{n_\epsilon} < \beta + \epsilon.$$

Maar dan geldt voor elke $n \geq n_\epsilon$ dat

$$\alpha - \epsilon < a_{n_\epsilon} \leq a_n \leq x_n^n \leq b_n \leq b_{n_\epsilon} < \beta + \epsilon.$$

Dus

$$x_n^n \in (\alpha - \epsilon, \alpha + \epsilon), \quad \text{m.a.w.} \quad |x_n^n - \alpha| < \epsilon.$$

Omdat $\epsilon > 0$ willekeurig was, betekent dit dat de (deel)rij $(x_n^n)_{n=1}^\infty$ convergent is met limiet $\alpha \in [a, b]$. $\square$

Gevolg.(Bolzano-Weierstrass) Iedere begrensde rij in $\mathbf{R}$ heeft een convergente deelrij.

Stelling 6.20. Laat $A \subseteq \mathbf{R}$. Dan geldt

$$A \ \text{ is rijkompakt} \iff A \text{ is gesloten en begrensd.}$$

Bewijs. $\Longrightarrow$: Stelling 6.14.
$\Longleftarrow$: Stel A is begrensd en gesloten. Dan is er een $M \in \mathbf{R}$ met $A \in [-M, M]$. Volgens Stelling 6.19 is $[-M, M]$ rijkompakt. Volgens Stelling 6.13 is dan ook A rijkompakt. $\square$

De volgende stelling toont aan dat $\mathbf{R}$ ook volledig is als metrische ruimte.

Stelling 6.21. Iedere Cauchyrij in $\mathbf{R}$ is convergent.

Bewijs. Opgave.

Stelling 6.22. (absoluut convergente reeksen zijn convergent)
Als $(a_k)_{k=1}^\infty$ een rij is in $\mathbf{R}$, en

$$\sum_{k=1}^\infty |a_k| \ = \ \lim_{n\to\infty} \sum_{k=1}^n |a_k|$$

bestaat, dan bestaat ook

$$\sum_{k=1}^{\infty} a_k = \lim_{n\to\infty} \sum_{k=1}^{n} a_k.$$

Bewijs. Omdat $\sum_{k=1}^{\infty} |a_k|$ bestaat, geldt

$$\forall \epsilon > 0 \ \exists n_\epsilon : m > n \geq n_\epsilon \Longrightarrow |\sum_{k=1}^{m} |a_k| - \sum_{k=1}^{n} |a_k|| < \epsilon.$$

Merk op dat

$$\sum_{k=1}^{m} |a_k| - \sum_{k=1}^{n} |a_k| = \sum_{k=n+1}^{m} |a_k| \geq |\sum_{k=n+1}^{m} a_k| = |\sum_{k=1}^{m} a_k - \sum_{k=1}^{n} a_k|.$$

Dus bestaat $\sum_{k=1}^{\infty} a_k$. $\square$

6.6 Kompaktheid en rijkompaktheid. (AO)

Definitie. Laat $A \subseteq X$.
(i) Een door een verzameling I geïndexeerde collectie (open) deelverzamelingen $\{\mathcal{O}_i : i \in I\}$ van X heet een *(open) overdekking* van A als

$$A \subseteq \cup_{i\in I} \ \mathcal{O}_i.$$

(ii) Als iedere open overdekking $\{\mathcal{O}_i : i \in I\}$ van A een eindige deeloverdekking van A bevat d.w.z.

$$\exists i_1, i_2, ..., i_m \in I : \quad A \subseteq \cup_{j=1,2,...,m} \ \mathcal{O}_{i_j},$$

dan heet A *kompakt*.

Stelling 6.23. Laat $A \subseteq X$. Dan

$$A \ \text{ is kompakt } \iff \ A \ \text{ is rijkompakt.}$$

Bewijs. $\Longrightarrow$: Stel A is kompakt en laat $(a_n)_{n=1}^{\infty}$ een rij zijn in A. We moeten bewijzen dat A een convergente deelrij met limiet in A heeft. Stel niet, dan is er voor elke $p \in A$ een $\epsilon_p > 0$ en een n_p zodanig dat $a_n \notin B_{\epsilon_p}(p)$ voor alle $n > n_p$. Neem nu als open overdekking van A de zojuist gevonden open bollen, dus

$$\{B_{\epsilon_p}(p) : p \in A\}.$$

Omdat A kompakt is heeft deze overdekking een eindige deeloverdekking, dus zijn er $p_1, p_2, ..., p_m$ in A zodat

$$A \subseteq B_{\epsilon_{p1}}(p_1) \cup B_{\epsilon_{p_2}}(p_2) \cup ... \cup B_{\epsilon_{p_m}}(p_m),$$

waardoor A op zijn hoogst $n_{p_1} + n_{p_2} + ... + n_{p_m}$ punten van de rij kan bevatten, m.a.w. de rij bevat slechts eindig veel verschillende punten van A, en tenminste één punt moet dus oneindig vaak voorkomen. Dus kunnen we een deelrij maken waarin dit punt alleen maar voorkomt, en dit is dan de gezochte deelrij.
$\Longleftarrow$: Dit heeft wat meer voeten in de aarde. Daartoe eerst het volgende.

Definitie. Laat A een deelverzameling zijn van een metrische ruimte X. Dan heet A *aftelbaar kompakt* als voor elke aftelbare rij open verzamelingen $(\mathcal{O}_n)_{n=1}^{\infty}$ met

$$A \subseteq \cup_{n=1}^{\infty} \mathcal{O}_n,$$

er een index k is zo dat

$$A \subseteq \cup_{n=1}^{k} \mathcal{O}_n.$$

Stelling 6.24. Als $A \subseteq X$ rijkompakt is, dan is A aftelbaar kompakt.

Bewijs. Neem aan dat A rijkompakt is maar niet aftelbaar kompakt. Dan is er een rij open verzamelingen $(\mathcal{O}_n)_{n=1}^{\infty}$ van A die A geheel bedekt, en die geen eindige deeloverdekking heeft. Dat betekent dat er voor elk natuurlijk getal k een punt p_k in A is met

$$p_k \notin \cup_{n=1}^{k} \mathcal{O}_n.$$

Omdat A rijkompakt is, heeft de rij $(p_k)_{k=1}^{\infty}$ een convergente deelrij met limiet p in A. Dus moet er een m zijn waarvoor $p \in \mathcal{O}_m$. Omdat $\mathcal{O}_m$ open is, zijn er dus oneindig veel punten van de rij $(p_k)_{k=1}^{\infty}$ die in $\mathcal{O}_m$ liggen. Voor $k > m$ is dit in tegenspraak met de keuze van p_k. $\square$

Definitie. Laat A een deelverzameling zijn van een metrische ruimte X. Dan heet A *totaal begrensd* als er voor elke $\epsilon > 0$ een eindige deelverzameling $\{p_1, p_2, ..., p_n\}$ van A bestaat met

$$A \subseteq B_{\epsilon}(p_1) \cup B_{\epsilon}(p_2) \cup ... \cup B_{\epsilon}(p_n).$$

Stelling 6.25. Als $A \subseteq X$ rijkompakt is, dan is A totaal begrensd.

Bewijs. Stel A is niet totaal begrensd. Dan is er een $\epsilon > 0$ waarvoor geen eindige verzameling als in de definitie kan worden gevonden. Kies nu $p_1 \in A$. Inductief kiezen we nu voor $n = 1, 2, ...$ een punt $p_{n+1} \in A$ met de eigenschap dat

$$p_{n+1} \notin B_\epsilon(p_1) \cup ... \cup B_\epsilon(p_n).$$

Maar dan is $d(p_i, p_j) \geq \epsilon$ voor alle $i \neq j$. Dus de rij $(p_n)_{n=1}^{\infty}$ kan geen convergente deelrij hebben, in tegenspraak met de rijkompaktheid van A. $\square$

Definitie. Een metrische ruimte X heet *separabel* als er een rij in X is zo dat elk punt van X een limietpunt is van deze rij.

Stelling 6.26. Als $A \subseteq X$ totaal begrensd is, dan is A separabel.

Bewijs. Voor elke k bestaat er een eindige deelverzameling A_k van A zo dat elk punt van A dichter dan $\frac{1}{k}$ bij een punt van A_k ligt. Maak nu een rij door eerst de elementen van A_1 te kiezen, dan de elementen van A_2, A_3, enzovoort. Dan is elk punt van A een limietpunt van de aldus verkregen rij. $\square$

Stelling 6.27. Als $A \subseteq X$ separabel is, dan heeft elke open overdekking van A een aftelbare deeloverdekking.

Bewijs. Laat $(p_n)_{n=1}^{\infty}$ een rij zijn in A met de eigenschap dat elk punt van A limietpunt is van deze rij, en laat $\{\mathcal{O}_i : i \in I\}$ een open overdekking zijn van A. Dan is elk punt p in A bevat in een $\mathcal{O}_i$. Kies nu een natuurlijk getal m zo groot dat $B_{\frac{2}{m}}(p) \subseteq \mathcal{O}_i$, en daarna een n zo dat $d(p_n, p) < \frac{1}{m}$. Dan is

$$p \in B_{\frac{1}{m}}(p_n) \subseteq \mathcal{O}_i.$$

Laat J de verzameling zijn van de paren natuurlijke getallen (m, n) die we zo tegenkomen als p de verzameling A doorloopt. Dan is J aftelbaar en

$$A \subseteq \sup_{(m,n) \in J} B_{\frac{1}{m}}(p_n).$$

Maar voor elke $(m, n) \in J$ is er tenminste één $\mathcal{O}_i$ die $B_{\frac{1}{m}}(p_n)$ bevat. Kies er voor elke $(m, n) \in J$ precies één. Dit geeft een aftelbare deelcollectie die A overdekt. $\square$

Uit bovenstaande stellingen volgt dat als $A \subseteq X$ rijkompakt is, A kompakt is.

6.7 De Banach contractiestelling. (AO)

Stelling 6.28. S. Banach (1892-1945). Laat X een volledige metrische ruimte zijn, en $T : X \to X$ een contractie, d.w.z. een afbeelding met de eigenschap dat

$$\exists \theta \in [0,1) : \; d(T(x), T(y)) \leq \theta d(x,y) \quad \forall x, y \in X.$$

Dan is er precies één vast punt van T, d.w.z. een punt $\tilde{x}$ in X met de eigenschap dat $T(\tilde{x}) = \tilde{x}$. Bovendien geldt voor elke $x \in X$ dat de rij gedefinieerd door

$$x_1 = T(x), \; x_{n+1} = T(x_n) \quad (n = 1, 2, ...),$$

convergent is met limiet $\tilde{x}$.

Bewijs. Merk eerst op dat er hoogstens één vast punt kan zijn. Immers als $\tilde{x}$ en $\tilde{y}$ vaste punten zijn, dan geldt

$$d(\tilde{x}, \tilde{y}) = d(T(\tilde{x}), T(\tilde{y})) \leq \theta d(\tilde{x}, \tilde{y}) \Longrightarrow d(\tilde{x}, \tilde{y}) = 0 \Longrightarrow \tilde{x} = \tilde{y}.$$

Laat nu $x \in X$ willekeurig en laat de rij $(x_n)_{n=1}^{\infty}$ de in de stelling gedefinieerde rij zijn. We gaan bewijzen dat dit een Cauchyrij is. Neem hiertoe twee natuurlijke getallen m, n met $m < n$. Dan volgt, door herhaald toepassen van de driehoeksongelijkheid,

$$d(x_m, x_n) \leq d(x_m, x_{m+1}) + d(x_{m+1}, x_{m+2}) + ... + d(x_{n-1}, x_n).$$

We gebruiken de notatie

$$T^0(x) = x, T^1(x) = T(x), T^2(x) = T(T(x)), T^3(x) = T(T(T(x))), \text{etc.}$$

Omdat

$$d(x_k, x_{k+1}) = d(T^k(x), T^{k+1}(x)) \leq \theta^k d(x, T(x)),$$

volgt nu dat

$$d(x_m, x_n) \leq (\theta^m + \theta^{m+1} + ... + \theta^{n-1}) d(x, T(x)) \leq \frac{\theta^m}{1-\theta} d(x, T(x)) \to 0 \text{ als } m \to \infty.$$

Dus $(x_n)_{n=1}^{\infty}$ is een Cauchyrij. Omdat X volledig is, heeft deze rij een limiet $\tilde{x}$, dus $T^n(x) \to \tilde{x}$. Maar dan geldt ook dat $T^{n+1}(x) \to \tilde{x}$, terwijl

$$d(T^{n+1}(x), T(\tilde{x})) = d(T(T^n(x)), T(\tilde{x})) \leq \theta d(T^n(x), \tilde{x}) \leq d(T^n(x), \tilde{x}) \to 0.$$

Dit impliceert dat $T^{n+1}(x) \to T(\tilde{x})$. Omdat de limiet van een convergente rij uniek bepaald is, kunnen we dus concluderen dat $\tilde{x} = T(\tilde{x})$. $\square$

Literatuur bij Hoofdstukken 6 en 7.

[1] T.M. Apostol. *Mathematical Analysis, a modern approach to advanced calculus*, Addison-Wesley, 1957.

[2] W. Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, 1964.

[3] R.S. Strichartz, *The Way of Analysis*, Jones and Bartlett, 1995, Ch. 1.

Opgaven bij Hoofdstuk 6. De reële getallen.

Tenzij anders vermeld beschouwen we in $\mathbf{R}$ en $\mathbf{Z}$ de metriek $d(x, y) = |x - y|$.

6.1. Bewijs dat voor elementen a, b, c, d uit een geordend lichaam K geldt:
a) als $a < c$ en $b < d$, dan $a + b < c + d$
b) als $a < b$ en $c > 0$, dan $ac < bc$
c) als $a < b$ en $c < 0$, dan $ac > bc$
d) als $a \neq 0$, dan $a^2 > 0$ e) $1 > 0$.

6.2. Laat zien dat de getallen $a + b\sqrt{2}$ met $a, b \in \mathbf{Q}$ met de gewone optelling en vermenigvuldiging een geordend lichaam vormen.

6.3. Laat $X = \mathbf{R}, A = \{x \mid 2x^2 < 4 \text{ of } x \geq 9\}$
a) Wat zijn de inwendige punten van A?
b) Wat zijn de ophopingspunten van A?
c) Is A open? d) Is A gesloten?

6.4. Laat $A \subseteq X$. Ga na dat elk punt van X hetzij inwendig punt, hetzij randpunt, hetzij uitwendig punt van A is.

6.5 a) Zij $X = \mathbf{R}$ en $A = \mathbf{Z}$.
(i) Wat zijn de inwendige punten van A?
(ii) Wat zijn de randpunten van A?

(iii) Wat zijn de ophopingspunten van A?
(iv) Is A open? (v) Is A gesloten?
(vi) Wat zijn de geïsoleerde punten van A?
b) Dezelfde vragen voor $X = \mathbf{R}$ en $A = \mathbf{Q}$.

6.6 a) Laat zien dat in $\mathbf{Z}$ elke verzameling open èn gesloten is.
b) Zoek een metriek in $\mathbf{R}$ waarvoor elke verzameling reële getallen open èn gesloten is.
c) Is het waar dat elk inwendig punt een ophopingspunt is?

6.7. a) Bewijs Stelling 6.3. b) Bewijs Stelling 6.5.

6.8. Laat $A \subseteq X$.
a) Bewijs: A is gesloten dan en slechts dan als A al zijn randpunten bevat.
b) Bewijs: A is open dan en slechts dan als A geen van zijn randpunten bevat.

6.9 a) Construeer een rij rationale getallen die in $\mathbf{R}$ convergeert, maar niet in $\mathbf{Q}$.
b) Bewijs dat in $\mathbf{R}$ elke monotoon stijgende, naar boven begrensde rij convergeert naar het supremum van de rij.
c) Bewijs dat in $\mathbf{R}$ elke monotoon dalende, naar beneden begrensde rij convergeert naar het infimum van de rij.

6.10 Ga na of de volgende verzamelingen rijkompakt zijn in $\mathbf{R}$:
a) $\{ x \mid 0 \leq x \leq 1 \text{ of } 2 \leq x \leq 3\}$,
b) $\{ x \mid 0 \leq x < 1\}$, c) $\mathbf{Z}$.

6.11 a) Bewijs Stelling 6.9. b) Bewijs Stelling 6.14.

6.12. Ga na of the volgende rijen $(x_n)_{n=1}^{\infty}$ Cauchyrijen zijn:
a) $x_n = \frac{(-1)^n}{n}$, b) $x_n = \begin{cases} \frac{1}{n} & \text{als } n \text{ is oneven} \\ 1 - \frac{1}{n} & \text{als } n \text{ is even} \end{cases}$.

6.13 a) Toon aan: als X rijkompakt is, is X volledig.
b) Bewijs Stelling 6.21.

6.14. Laat zien: a) Elke begrensde rij in $\mathbf{R}$ heeft een limietpunt.
b) Een begrensde rij in $\mathbf{R}$ heeft maar één limietpunt als en alleen als de rij convergent is.

7 HOOFDSTUK: CONTINUE REËLE FUNCTIES

7.1 Continuïteit.

In dit hoofdstuk werken we enkele gevolgen uit van de resultaten van het vorige hoofdstuk. Dit levert een stel basisstellingen op voor de theorie van de reële functies. In plaats van over functies $f : X \to Y$ spreekt men, als het beeld Y een algemene metrische ruimte is, vaak over afbeeldingen.

Definitie. Laat X en Y metrische ruimten zijn, $A \subseteq X$ en $f : A \to Y$ een afbeelding.
(i) f heet *continu* in $a \in A$, als

$$\forall \epsilon > 0\ \exists \delta > 0\ \forall x \in A :\ d(x, a) < \delta \Longrightarrow d(f(x), f(a)) < \epsilon.$$

(ii) f heet *continu op* A als f continu is in elke $a \in A$.

Stelling 7.1. Laat X en Y metrische ruimten zijn, $A \subseteq X, f : A \to Y$ een afbeelding, en $a \in A$. Dan is f continu in a dan en slechts dan als voor elke rij $(a_n)_{n=1}^{\infty}$ in A met $a_n \to a$ in X geldt dat $f(a_n) \to f(a)$ in Y.

Bewijs. Neem aan dat f continu is in a en laat $(a_n)_{n=1}^{\infty}$ een rij zijn in A met $a_n \to a$. Kies $\epsilon > 0$ willekeurig, en laat $\delta > 0$ de bijbehorende δ uit de definitie van continuïteit van f in a zijn. Gebruik deze δ nu als ϵ in de definitie van convergentie. Dan volgt voor $n \geq n_\delta$ dat $d(a_n, a) < \delta$. Dus $n \geq n_\delta \Longrightarrow d(f(a_n), f(a)) < \epsilon$. Hieruit volgt dat de rij $(f(a_n))_{n=1}^{\infty}$ convergeert naar $f(a)$.
Anderzijds, als f niet continu is in a, dan

$$\exists \epsilon > 0\ \forall \delta > 0\ \exists a_\delta \in A :\ d(a_\delta, a) < \delta \text{ en } d(f(a_\delta), f(a)) \geq \epsilon.$$

Kies $\delta = \frac{1}{n}$, en noem de bijbehorende a_δ nu a_n. Dan is $(a_n)_{n=1}^{\infty}$ een rij in A met $a_n \to a$, terwijl de rij $(f(a_n))_{n=1}^{\infty}$ niet convergeert naar $f(a)$. □

Stelling 7.2. Laat X en Y metrische ruimten zijn, en $f : X \to Y$ een afbeelding. Dan is f continu op X dan en slechts dan als het inverse beeld onder f van iedere open deelverzameling van Y weer een open deelverzameling van X is.

Bewijs. Neem aan dat f continu is, en zij B een open verzameling in Y. We moeten bewijzen dat het inverse beeld onder f van B open is. We laten zien

dat elk punt van $A = f^{-1}(B)$ een inwendig punt is. Laat hiertoe $a \in A$ en $b = f(a) \in B$. Omdat B open is, is b een inwendig punt van B. Dus bestaat er een $\epsilon > 0$ met $B_\epsilon(b) \subseteq B$. Kies de bij ϵ horende δ uit de definitie van continuïteit. Dan is $f(B_\delta(a)) \subseteq B_\epsilon(b)$ waardoor $B_\delta(a) \subseteq A = f^{-1}(B)$. Dit geldt voor elke $a \in A$. Dus is A open.
Omgekeerd is te bewijzen dat f continu is in elk punt van X, als het inverse beeld van elke open verzameling open is. Laat hiertoe $a \in X$ en $b = f(a)$. Zij $\epsilon > 0$ willekeurig. Dan is $B_\epsilon(b)$ open in Y. Dus is $A = f^{-1}(B_\epsilon(b))$ open in X. Omdat $a \in A$, is er een $\delta > 0$ zo dat $B_\delta(a) \subseteq A$. Met deze δ is dan aan de uitspraak in de definitie van continuïteit voldaan. □

Stelling 7.3. Laat $A \subseteq X$. Zij $f : A \to \mathbf{R}$ een continue functie. Als A rijkompakt is, dan heeft f een maximum in A.

Bewijs. Laat M het supremum van $f(A)$ zijn. We definiëren een rij $(x_n)_{n=1}^\infty$ in A als volgt: als $M < \infty$ kiezen we $x_n \in A$ zo dat $f(x_n) > M - \frac{1}{n}$, en als $M = \infty$ dan $x_n \in A$ zo dat $f(x_n) > n$. Omdat A rijkompakt is, heeft deze rij een convergente deelrij $(x_{n_k})_{k=1}^\infty$ met limiet $a \in A$. Vanwege de continuïteit van f in a is de rij $(f(x_{n_k}))_{k=1}^\infty$ convergent met limiet $f(a)$. Omdat een convergente rij begrensd is, sluit dit de mogelijkheid $M = \infty$ uit, zodat

$$M - \frac{1}{n} < f(x_n) \leq M \quad \text{voor elke } n.$$

De rij $(f(x_n)_{n=1}^\infty$ convergeert dus naar M. Maar we weten dat een deelrij naar $f(a)$ convergeert. Dus $f(a) = M$. □

Stelling 7.4. Laat X en Y metrische ruimten zijn, $A \subseteq X$, en $f : A \to Y$ een continue afbeelding. Als A rijkompakt is in X, dan is het beeld $f(A)$ van A onder f rijkompakt in Y.

Bewijs. Opgave.

Definitie. Laat X en Y metrische ruimten zijn, $A \subseteq X$, en $f : A \to Y$ een afbeelding. Dan heet f *uniform continu in* A, als

$$\forall \epsilon > 0 \; \exists \delta > 0 \; \forall x, y \in A : \; d(x,y) < \delta \Longrightarrow d(f(x), f(y)) < \epsilon.$$

Stelling 7.5. Laat X en Y metrische ruimten zijn, $A \subseteq X$ en $f : A \to Y$ een continue afbeelding. Als A rijkompakt is in X, dan is f uniform continu in A.

Bewijs. Stel de bewering geldt niet. Dan

$$\exists \epsilon > 0 \ \forall \delta > 0 \ \exists x, y \in A: \quad d(x,y) < \delta \ \text{ en } \ d(f(x), f(y)) \geq \epsilon.$$

Kies $\delta = \frac{1}{n}$ en laat x_n en y_n de bijbehorende x en y zijn zoals in de regels hierboven. Omdat A rijkompakt is, heeft de rij $(x_n)_{n=1}^{\infty}$ een convergente deelrij $(x_{n_k})_{k=1}^{\infty}$, zeg met limiet $a \in A$. Dan is ook de rij $(y_{n_k})_{k=1}^{\infty}$ convergent met dezelfde limiet. (Waarom?) Maar nu geldt

$$\lim_{k\to\infty} f(x_{n_k}) = \lim_{k\to\infty} f(y_{n_k}) = f(a),$$

terwijl $d(f(x_{n_k}), f(y_{n_k})) \geq \epsilon$, tegenspraak. □

Stelling 7.6. Laat A een gesloten begrensde deelverzameling van $\mathbf{R}$ zijn. Als $f : A \to \mathbf{R}$ een continue functie is, dan neemt f een maximum op A aan.

Bewijs. Opgave.

7.2 De Tussenwaardenstelling.

In deze paragraaf leiden we eigenschappen van continue functies af die intuïtief duidelijk, maar daarom nog niet vanzelfsprekend zijn. Alles is voortaan in $\mathbf{R}$.

Stelling 7.7. Stel f is continu in c en $f(c) \neq 0$. Dan is er een $\delta > 0$ zó dat f op $(c - \delta, c + \delta)$ tekenvast is.

Bewijs. Stel $f(c) > 0$. Omdat f continu is in c, bestaat er bij elke $\epsilon > 0$ een $\delta > 0$ zó dat $f(c) - \epsilon < f(x) < f(c) + \epsilon$ als $c - \delta < x < c + \delta$. Neem nu $\epsilon = \frac{f(c)}{2}$. Dan volgt dat

$$0 < \frac{f(c)}{2} < f(x) \left(< \frac{3f(c)}{2} \right) \ \text{ als } \ c - \delta < x < c + \delta.$$

Als $f(c) < 0$, passen we het bovenstaande argument toe op $-f$. □

De volgende stelling van de katholieke priester Bolzano (1781-1848) zegt dat een continue functie tussen een negatieve en een positieve waarde de waarde 0 aanneemt.

Stellling 7.8. (Bolzano, 1817) Stel f is continu in elk punt van het interval $[a, b]$ terwijl $f(a)f(b) < 0$. Dan is er een $c \in (a, b)$ met $f(c) = 0$.

Bewijs. Stel $f(a) < 0, f(b) > 0$. Zij $S = \{x \in [a, b] : f(x) \leq 0\}$ en zij $c = \sup_{x \in S} x = \sup S$. Omdat $f(a) < 0$, is S niet leeg. Verder is S naar boven begrensd door b. Volgens het Volledigheidsaxioma is $c \in \mathbf{R}$, meer precies $c \in [a, b]$. Er geldt $f(c) < 0, f(c) > 0$ of $f(c) = 0$.
Als $f(c) < 0$, is er volgens Stelling 7.7 een $\delta > 0$ zó dat $f(x) < 0$ voor $c \leq x < c + \delta$ en is $[c, c + \delta) \subseteq S$, tegenspraak.
Als $f(c) > 0$, is er volgens Stelling 7.7 een $\delta > 0$ zó dat $f(x) > 0$ voor $c - \delta < x \leq c$ en is $\sup S \leq c - \delta$, tegenspraak.
Dus $f(c) = 0$. Het is duidelijk dat $c \neq a, b$. Dus $c \in (a, b)$.
Als $f(a) > 0, f(b) < 0$, passen we het argument toe op $-f$. □

Opmerking. Er kunnen meerdere nulpunten van f tussen a en b liggen.

Stelling 7.9. (Tussenwaardenstelling) Stel f is continu op $[a, b]$. Stel $x_1, x_2 \in [a, b]$ met $x_1 < x_2$ en $f(x_1) \neq f(x_2)$. Dan neemt f elke waarde tussen $f(x_1)$ en $f(x_2)$ ergens op het interval (x_1, x_2) aan.

Bewijs. Stel $f(x_1) < f(x_2)$ en k is een waarde met $f(x_1) < k < f(x_2)$. Definieer $g(x) = f(x) - k$. Dan is $g(x_1) < 0$, $g(x_2) > 0$ en g continu op $[x_1, x_2]$. Volgens Stelling 7.8 is er een $c \in (x_1, x_2)$ met $g(c) = 0$ en dus $f(c) = k$. □

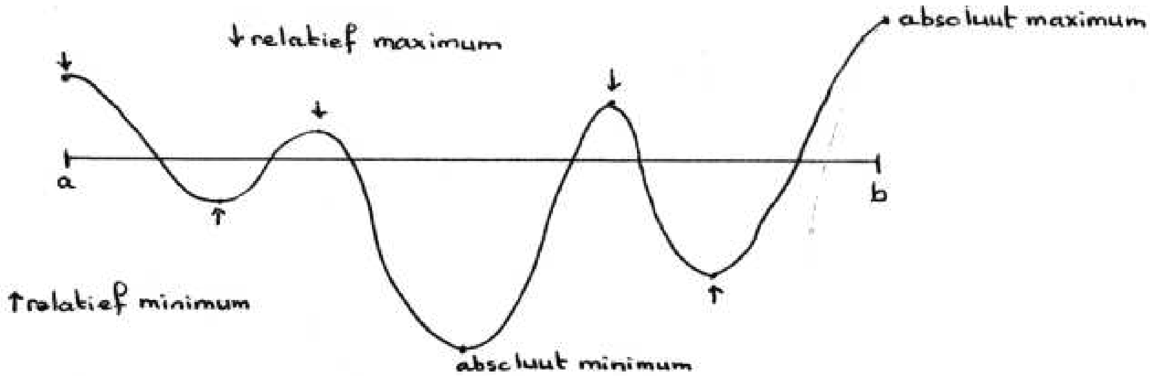
Gevolg. Stel $n \in \mathbf{N}$ en $a \in \mathbf{R}_{>0}$. Dan is er precies één positief getal b met $b^n = a$.

Bewijs. Kies een $d > 1$ zó dat $0 < a < d$. Beschouw de functie x^n op $[0, d]$. Er geldt $f(0) = 0 < a$ en $f(d) = d^n \geq d > a$. Omdat x^n continu is, moet er volgens Stelling 7.9 een punt b in $(0, d)$ zijn met $f(b) = b^n = a$. Omdat x^n een strict stijgende functie is, kan er maar één zo'n punt zijn. □

7.3 Middelwaardestellingen.

In deze paragraaf nemen we aan dat de basisregels van het differentiëren bekend zijn en leiden we enkele fundamentele stellingen af over maxima, minima en middelwaarden.

Definities. Een functie $f : S \to \mathbf{R}$ heeft een *relatief maximum (minimum)* $f(c)$ in $c \in S$ als er een open omgeving I van c is zó dat $f(x) \leq f(c)$ $(f(x) \geq f(c))$ voor alle $x \in I \cap S$. De functie f heeft een *absoluut maximum (minimum)* $f(c)$ in $c \in S$ als $f(x) \leq f(c)$ $(f(x) \geq f(c))$ voor alle $x \in S$. Een *extremum* is een relatief maximum of relatief minimum.



Stelling 7.10. Stel I is een open verzameling in $\mathbf{R}$ en $f : I \to \mathbf{R}$ heeft een extremum in $c \in I$. Als f differentieerbaar is in c, dan is $f'(c) = 0$.

Bewijs. Defineer $Q(x) = \begin{cases} \frac{f(x)-f(c)}{x-c} & \text{als } x \neq c \\ f'(c) & \text{als } x = c \end{cases}$

Omdat $f'(c)$ bestaat, geldt $f'(c) = \lim_{x\to c} \frac{f(x)-f(c)}{x-c} = \lim_{x\to c} Q(x)$.
Dus $\lim_{x\to c} Q(x) = Q(c)$, d.w.z. Q is continu in c.
Er geldt $Q(c) > 0$ of $Q(c) < 0$ of $Q(c) = 0$. Stel $Q(c) > 0$. Volgens Stelling 7.7 is er een $\delta > 0$ zó dat $Q(x) > 0$ voor $|x - c| < \delta$. Hieruit volgt dat $f(x) > f(c)$ als $x > c$ en $f(x) < f(c)$ als $x < c$. Dit weerspreekt dat f een extremum heeft in c. Een soortgelijk argument leidt tot een tegenspraak als $x < c$. Dus $Q(c) = 0$, d.w.z. $f'(c) = 0$. $\square$

Als er een (inwendig) extremum is, moet de afgeleide nul zijn. Door de nulpunten van de afgeleide te bepalen vind je alle kandidaten.
Het omgekeerde is niet waar: $f(x) = x^3$ heeft een afgeleide $3x^2$ die nul is voor $x = 0$, maar x^3 heeft in $x = 0$ geen extremum! Je moet dus van de gevonden nulpunten nog nagaan of ze inderdaad extrema opleveren.

De volgende stelling is genoemd naar de Franse wiskundige Michel Rolle (1652-1719).

Stelling 7.11. (Stelling van Rolle) Stel f is continu op het interval $[a, b]$ en differentieerbaar op het open interval (a, b). Als $f(a) = f(b)$, dan is er een $c \in (a, b)$ met $f'(c) = 0$.

Bewijs. Uit het ongerijmde. Stel $f'(x) \neq 0$ voor $x \in (a, b)$. Omdat $[a, b]$ begrensd en gesloten is, is $[a, b]$ rijkompakt en neemt f volgens Stelling 7.3 een maximum M en een minimum m aan op het interval $[a, b]$. Volgens onze aanname en Stelling 7.10 kunnen de extrema alleen in a en b worden aangenomen. Omdat $f(a) = f(b)$, moet $m = M$ gelden, d.w.z. f is constant op $[a, b]$. Dan is $f'(x) = 0$ voor $x \in (a, b)$. Deze tegenspraak bewijst dat er een $x \in (a, b)$ is met $f'(x) = 0$. $\square$

De volgende stelling, de (eerste) middelwaardestelling, is een gevolg van de Stelling van Rolle. Ze zegt dat de afgeleide van f ergens tussen a en b gelijk is aan de gemiddelde toename $\frac{f(b)-f(a)}{b-a}$.

Stelling 7.12. (Middelwaardestelling) Als f continu is op $[a, b]$ en differentieerbaar op (a, b), dan is er een $c \in (a, b)$ met $f(b) - f(a) = f'(c)(b - a)$.

Bewijs. Definieer $h(x) = f(x)(b - a) - x(f(b) - f(a))$. Dan geldt $h(a) = h(b) = bf(a) - af(b)$. Verder is h continu op $[a, b]$ en differentieerbaar op (a, b). Passen we de stelling van Rolle toe op h, dan vinden we dat er een $c \in (a, b)$ is met $h'(c) = 0$. Omdat $h'(x) = (b-a)f'(x) - (f(b) - f(a))$, geldt $f(b) - f(a) = (b - a)f'(c)$. $\square$

De *tweede middelwaardestelling* betreft twee functies, f en g. Zij zegt dat er een punt c is met $\frac{f'(c)}{g'(c)} = \frac{f(b)-f(a)}{g(b)-g(a)}$.

Stelling 7.13. (Cauchy (1798-1857)) Stel f en g zijn continu op $[a, b]$ en differentieerbaar op (a, b). Dan is er een $c \in (a, b)$ met

$$f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a)).$$

Bewijs. Dit is een variant op het vorige bewijs. Zij

$$h(x) = f(x)(g(b) - g(a)) - g(x)(f(b) - f(a)).$$

Dan is $h(a) = h(b) = f(a)g(b) - g(a)f(b)$. Verder is h continu op $[a, b]$ en differentieerbaar (a, b). Volgens Rolle is er een $c \in (a, b)$ met $h'(c) = 0$.
Dus $f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a))$. $\square$

Opgaven bij Hoofdstuk 7. Continue reële functies.

1. a Bewijs Stelling 7.4.
   b) Bewijs Stelling 7.6.
   c) Laat zien dat in Stelling 7.6 noch het woord 'gesloten' noch het woord 'begrensde' mag worden weggelaten.

2. Beschouw de functie $f(x) = x^2$.
   a) Laat zien dat f continu is op $\mathbf{R}$.
   b) Toon aan dat f niet uniform continu is op $\mathbf{R}$.
   c) Laat zien dat f uniform continu is op $[-10, 10]$.

3. Beschouw de functie $f(x) = \sqrt{x}$ $(x \geq 0)$.
   a) Laat zien dat f continu is voor $x \geq 0$.
   b) Laat zien dat f uniform continu is op $\mathbf{R}^+$.

4. Is de volgende bewering waar?
   De functie $f : \mathbf{R} \to \mathbf{R}$ is continu dan en slechts dan als het beeld onder f van elke open deelverzameling open is.

5. Leg uit waarom $\tan\frac{\pi}{4} = 1, \tan\frac{3\pi}{4} = -1$ en er geen c is met $\frac{\pi}{4} < c < \frac{3\pi}{4}$ waarvoor $\tan c = 0$ (vgl. Stelling 7.8).

6. a) Stel f is continu op $[0, 1]$ en $0 \leq f(x) \leq 1$ voor $x \in [0, 1]$.
   Bewijs dat er een $c \in [0, 1]$ is met $f(c) = c$ (een zgn. *dekpunt*).
   Aanwijzing: beschouw $f(x) - x$.
   b) Stel $a < b$ en f is continu op $[a, b]$. Als $f(a) \leq a$ en $f(b) \geq b$, dan is er een punt $c \in [a, b]$ met $f(c) = c$. Bewijs dit.

7. Voor de functie $f(x) = |x|$ geldt $\frac{f(2)-f(-1)}{2-(-1)} = \frac{1}{3}$. Toch is er geen punt c met $f'(c) = \frac{1}{3}$. Waarom is de middelwaardestelling niet van toepassing?

8. a) Bewijs dat er voor elke b precies één $x \in \mathbf{R}$ is met $x^3 + 3x + b = 0$.
   b) Bewijs dat $x^2 = x \sin x + \cos x$ voor precies twee reële waarden van x.

9. Zij $f : \mathbf{R} \to \mathbf{R}$ differentieerbaar.
   a) Als f' begrensd is, is f uniform continu. Bewijs dit.
   b) Geef een voorbeeld van een uniform continue functie op $\mathbf{R}$ waarvan de afgeleide niet begrensd is.

CALEIDOSCOOP 2002
Huiswerk (1e deel van Hoofdstuk 1)

1 a) Bewijs met volledige inductie dat

$$1^2 + 3^2 + 5^2 + ... + (2n-1)^2 = \frac{1}{3}n(4n^2 - 1).$$

b) Bewijs met volledige inductie:
Als $a \mid b_1 b_2 \cdots b_n c$ en $(a, b_i) = 1$ voor $i = 1, ..., n$, dan $a \mid c$.

2. (Stelling van Nicomachus) Bewijs dat n^3 de som is van de n oneven getallen die het dichtste bij n^2 liggen.

3.) Zij gegeven: $a = 962, b = 629$.

a) Bereken ggd(a, b).

b) Bereken kgv(a, b).

Voor extra punten:

4. Bepaal voor elk natuurlijk getal k de paren gehele getallen (m, n) met $m > n > 0$ en m minimaal zó dat het euclidisch algoritme k stappen nodig heeft om de ggd te bereiken.

Huiswerk uiterlijk inleveren op donderdag 12 september om 13.45 uur.

CALEIDOSCOOP 2002
Huiswerk (2e deel van Hoofdstuk 1)

1.) Zij gegeven $a = 1353, b = 438$.

a) Bereken $\text{ggd}(a, b)$.

b) Bepaal zo mogelijk natuurlijke getallen x, y met $ax - by = 14$.

c) Bepaal zo mogelijk natuurlijke getallen x, y met $ax - by = 15$.

2a) Bewijs: als $n! + 1$ deelbaar door $n + 1$ is, dan is $n + 1$ een priemgetal.

b) Stel a en b zijn twee verschillende gehele getallen en n is een natuurlijk getal. Bewijs dat $a^n - b^n$ deelbaar is door $a - b$ en vind een uitdrukking voor het quotiënt.

3a) Zoek de titel en het ISBN-nummer van een wiskundeboek uit de bibliotheek dat informatie bevat over het ontbinden van grote getallen.

b) Noteer de gegevens van een tijdschriftartikel uit de bibliotheek waarvan in de titel het woord "surface" voorkomt.

c) Noteer de naam en het geboortejaar van een wiskundige waarvan de achternaam met dezelfde letter begint als jouw achternaam.

Voor extra punten:

4. Zoek een formule voor $\sum_{k=1}^{n} k^4$ en bewijs met volledige inductie dat de formule klopt.

Huiswerk uiterlijk inleveren op donderdag 19 september om 13.45 uur.

CALEIDOSCOOP 2002
Huiswerk (3e deel van Hoofdstuk 1)

1. Schrijf het decimale getal 7471 in het g-tallig stelsel waarbij

   a) $g = 2$, b) $g = 3$, c) $g = 15$ $(A = 10, B = 11, C = 12, D = 13, E = 14)$.

d) Schrijf het 13-tallige getal $(38A5)_{13}$ uit in het 10-tallig stelsel.

2. Voer de volgende berekeningen uit in het aangegeven getallenstelsel.

$$(ABC)_{14} \; + \; (C38)_{14}, \qquad (147)_8 \times (253)_8.$$

3. Bepaal de ontbinding in priemgetallen van de volgende getallen:
   a) 42, b) 87, c) 89, d) 143, e) 1250, f) 9991.

Voor extra punten:

4a) Laat zien dat als voor natuurlijke getallen $a > 1$ en $n > 1$ het getal $a^n - 1$ een priemgetal is, a gelijk is aan 2.

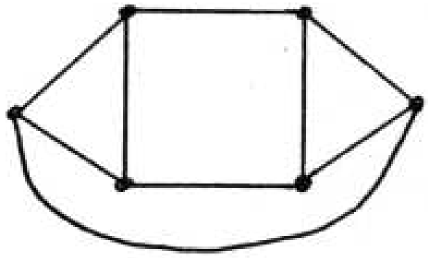
b) Laat zien dat als voor een natuurlijke getal $n > 1$ het getal $2^n - 1$ een priemgetal is, n zelf een priemgetal is.

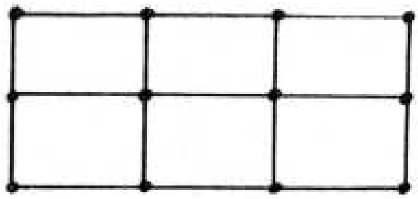
c) Toon aan dat er priemgetallen n bestaan waarvoor $2^n - 1$ geen priemgetal is.

Huiswerk uiterlijk inleveren op donderdag 26 september om 13.45 uur.

CALEIDOSCOOP 2002
Huiswerk over Hoofdstuk 2

1a) Bepaal het kleurgetal van de volgende grafen:





b) Ga van beide grafen na of ze vlak zijn.
c) Teken van de vlakke grafen uit a) platte versies.

2. Pas de invoegheuristiek toe op de volgende afstandstabel:

	A	B	C	D	E	F
A	–	24	31	21	28	19
B	24	–	12	18	34	17
C	31	12	–	25	22	27
D	21	18	25	–	27	23
E	28	34	22	27	–	29
F	19	17	27	23	29	–

3. Bewijs Stelling 2.2.

4. Bewijs dat een graaf met vijf knooppunten waarbij elk paar knooppunten door een tak verbonden is, niet vlak is.

5. Gebruik het internet om de volgende vragen te beantwoorden en vermeld telkens de geraadpleegde bronnen.
a) Wanneer werd L. Euler geboren en waar is hij overleden?
b) Hoe luidt het probleem van de driedeling van de hoek en door wie en wanneer is het opgelost?
c) Door wie en wanneer is bewezen dat het getal π irrationaal is?

Voor extra punten:

6. Vind de minimale oplossing van bovenstaand vraagstuk 2 en bewijs dat deze oplossing inderdaad de beste is.

Huiswerk inleveren uiterlijk op donderdag 10 oktober 2000 om 13.45 uur.

CALEIDOSCOOP 2002
Huiswerk over Hoofdstuk 3

1.a) Schrijf alle isometrieën van een regelmatige zeshoek uit.

b) Bereken van elke isometrie de orde.

c) Ga van elke isometrie na of deze even is.

2. In S_6 beschouwen we de permutaties $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 5 & 1 & 6 & 3 & 8 & 4 \end{bmatrix}$,
$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 1 & 2 & 8 & 5 & 4 & 7 \end{bmatrix}$, $\rho = \tau^{-1}\sigma$.

a) Schrijf σ, τ, ρ in disjuncte cykelnotatie.

b) Bereken de ordes van σ, τ, ρ.

c) Ga na welke van σ, τ, ρ even zijn.

d) Los de vergelijking $\sigma x = \tau$ in S_8 op.

e) Bereken het inversiegetal van σ.

3a) Bewijs dat elke permutatie in S_n een orde heeft die $n!$ deelt.

b) Bepaal een uitdrukking voor het kleinste gemene veelvoud van de ordes van de elementen uit S_n.

Voor extra punten:

4a) Bepaal de grootste orde van een element uit S_{12}.

b) Geef boven- en ondergrenzen voor de grootste orde van een element uit S_n voor grote n.

Huiswerk inleveren uiterlijk op donderdag 17 oktober 2000 om 13.45 uur.

CALEIDOSCOOP 2002
Huiswerk over Hoofdstuk 4

1. Bepaal de grootste gemene deler van

$$x^3 + 3x^2 + x - 2 \text{ en } x^4 - 3x^2 + 3x + 2.$$

2. Bepaal zo mogelijk polynomen P en Q in $\mathbf{Q}[x]$ zó dat

a) $(x^3 + 1)P(x) + (x^5 + 1)Q(x) = x + 2,$

b) $(x^3 + 1)P(x) + (x^2 + 1)Q(x) = x^2 - 1.$

3. Bepaal polynomen P en Q in $\mathbf{Z}[x]$ zó dat

$$\frac{3x+5}{(x^2-1)(x^2+x-1)} = \frac{P(x)}{x^2-1} + \frac{Q(x)}{x^2+x-1} \qquad (\mathrm{gr}(P), \mathrm{gr}(Q) < 2).$$

4. (voor extra punten.) Bepaaal een formule voor de u_n gedefinieerd door: $u_0 = 2, u_1 = 3, u_n = 2u_{n-1} + 3u_{n-2} \quad (n = 2, 3, \ldots).$

Huiswerk inleveren uiterlijk op donderdag 31 oktober om 13.45 uur.

CALEIDOSCOOP 2002
Maple huiswerk over Hoofdstuk 1-4

1. Noteer met $d(n)$ het aantal positieve delers van n. Bepaal een getal $n \in \{1, \ldots, 1000\}$ zó dat $d(n) \geq d(k)$ voor $k \in \{1, \ldots, 1000\}$.

2a) Bepaal de grootste gemene deler van

$$P(x) = x^8 + 10x^7 + 45x^6 + 120x^5 + 209x^4 + 246x^3 + 194x^2 + 96x + 24,$$

en

$$Q(x) = x^{10} + 10x^9 + 40x^8 + 80x^7 + 80x^6 + 32x^5.$$

b) Bepaal zo mogelijk polynomen P en Q in $\mathbf{Q}[x]$ zó dat

$$(x^3 - x - 1)P(x) + (x^2 - x - 1)Q(x) = x^5 + x^2 + 3.$$

3. Zij $F(x) = \frac{x-1}{x^2(x^2+1)(x^2+2)(x^2+3)(x^2+4)(x^2+5)}$. Schrijf $F(x)$ als

$$\frac{f_1(x)}{x^2} + \frac{f_2(x)}{x^2+1} + \frac{f_3(x)}{x^2+2} + \frac{f_4(x)}{x^2+3} + \frac{f_5(x)}{x^2+4} + \frac{f_6(x)}{x^2+5}.$$

Aanwijzing: gebruik de Maple procedure parfrac.

4a) Implementeer het algoritme gegeven in Sectie 1.3 in Maple.

b) Gebruik de procedure om de antwoorden te controleren van de vergelijkingen $ax + by = \gcd(a, b)$ in Opgave 5 van Hoofdstuk 1.

Voor extra punten:

5. Bereken het aantal elementen van de volgende verzameling:

$$\{(x, y, z) | x, y, z \in \mathbf{N}, x + y + z = 55, x \leq y \leq z, z - x > 30\}.$$

Maple worksheets als Text of Maple Text uiterlijk op donderdag 7 november om 13.45 uur per e-mail zenden naar tengely@math.leidenuniv.nl

CALEIDOSCOOP 2002
Huiswerk bij Hoofdstuk 5 (Logica enz.)

1.a) Werk de negaties van de volgende bewering uit:

$$\forall x\ \exists y \forall z : x > y \Longrightarrow y > z.$$

b) Welke van de volgende beweringen zijn waar, als $x, y, z \in \mathbf{R}$?

$$\forall x \exists y : x = y^3; \qquad \forall x \forall y \exists z : x = y^2 - z^2.$$

c) Volgt uit $(A \Longrightarrow B) \Longrightarrow A$ dat A waar is? Argumenteer uw antwoord.

2a) Ga na of de volgende relatie een equivalentierelaties is en geef in dat geval een equivalentieklasse aan. $(a, b \in \mathbf{R})$

$$a^2 - b^2 \in \mathbf{Z}.$$

3. Ga na of de volgende functies bijectief zijn en bepaal dan de inverse:
a) $y = e^{\sqrt{\log x}}$ $(x > 1, y > 1)$; b) $y = x - \frac{1}{x}$ $(x > 0, y > 0)$.

Huiswerk uiterlijk op **donderdag 14 november** om 13.45 uur inleveren.

CALEIDOSCOOP 2002
LaTeX huiswerk

1. Maak een LaTeX file van de tekst op bladzijde 57 van het dictaat vanaf de bovenste regel tot "In het vervolg ..." halverwege de bladzijde.

2a) Maak een LaTeX-file van de vermenigvuldigingstabel van de restklassen modulo 7.

3. Schrijf de volgende tekst in een LaTeX-file:
   Let
   $$A = \prod_{k=1}^{\infty} (1 + \frac{1}{k^2}). \qquad (1)$$
   Then A represents a real number, since $B = \sum_{n=1}^{\infty} \frac{1}{k^2}$ converges. In fact, $B = \frac{\pi^2}{6}$. There is no similar expression known for $B = \sum_{n=1}^{\infty} \frac{1}{k^3}$.

Latex files (dus *.tex files) uiterlijk op donderdag 21 november om 13.45 uur opzenden aan Szabolcs via tengely@math.leidenuniv.nl

CALEIDOSCOOP 2002
Huiswerk bij Hoofdstuk 6

1. Laat $X = \mathbf{R}, A = \{\ x \mid x \leq 0 \text{ of } 1 < x < 2\}$.
Geef beargumenteerde antwoorden op de volgende vragen:

a) Wat zijn de inwendige punten van A?

b) Wat zijn de randpunten van A?

c) Wat zijn de ophopingspunten van A?

d) Is A open? e) Is A gesloten? f) Is A begrensd?

g) Is A rijkompakt?

2. Bewijs Stelling 6.12.

3. Bewijs Stelling 6.16.

4. Welke van de volgende beweringen zijn waar in een willekeurige metrische ruimte? (Motiveer je antwoord.)

a) Een verzameling is open dan en slechts dan als zij geen van haar ophopingspunten bevat.

b) Een verzameling is open dan en slechts dan als zij geen van haar randpunten bevat.

Voor extra punten:

5a) Bewijs dat de verzameling Y van ophopingspunten van een verzameling X een gesloten verzameling vormt.

b) Bewijs dat de verzameling Z van ophopingspunten van Y bevat is in Y.

Huiswerk uiterlijk inleveren op donderdag **5 december** om 13.45 uur.

CALEIDOSCOOP 2002
HUISWERK BIJ HOOFDSTUK 7

1. Beschouw de functie $f(x) = \log x \quad (x > 0)$.

a) Laat zien dat f uniform continu is op $[1, \infty)$.

b) Laat zien dat f niet uniform continu is op $(0, 2)$.

2. Beschouw de functie $f(x) = e^{-1/x^2} \quad (x \in \mathbf{R})$.

a) Laat zien dat f continu is op $\mathbf{R}$.

b) Laat zien dat f uniform continu is op $\mathbf{R}$.

3a) Bewijs dat de vergelijking $\log x = \sin x$ tenminste één reële oplossing $x > 0$ heeft.

b) Bewijs: als voor de differentieerbare functie $f : [0, 1] \to \mathbf{R}$ geldt dat $f(0) = 1, f(1) = 3$, dan bestaat een punt $c \in (0, 1)$ met $f'(c) = 2$.

Huiswerk inleveren uiterlijk op donderdag 12 december om 13.00 uur
in mijn postvak in kamer 2.09 of per post:
R. Tijdeman, Mathematisch Instituut, Postbus 9512, 2300 RA Leiden.

Index

aantal 48
absoluut maximum 75
absoluut minimum 75
afbeelding 46
afstand 56
aftelbaar 48
aftelbaar kompakt 66
aftrekken 4
algoritme van Euclides
    voor getallen 5
    voor polynomen 37
alle 44
als 43
als en alleen als 43
Appel, K. 16
archimedisch 55
associatief 2
axioma 2, 42, 50, 54

Banach, S. 68
basis 8
beeld 46
beginpunt 20
begrensd 54
bestaat 44
bewijs 17, 49
    uit het ongerijmde 43
bijectief 25, 47
binaire getallen 8, 16
bipartiete graaf 22
Bolzano, B.P.J.N. 73
boom 21
bovengrens 55
breuksplitsing 39
bruggenprobleem 15

Cantor, G. 49, 51, 54, 62
carthesisch assenstelsel 45
carthesisch product 45
Catalan, E. 12
Cauchy, A.L. 76
cauchyrij 61
Cohen, P.J. 51
commutatief 2
complement 45, 57
compositie 47
constant 34, 47
continu 71
continuumhypothese 51
contractiestelling 68
convergent 55, 58
cykel 24

decimaal 8
Dedekind, R. 54
deelrij 60
deelverzameling 45
delen 4
deler
    van getal 5
    van polynoom 37
deling met rest
    van getallen 4
    van polynomen 35
Descartes, R. 45
disjunct 26, 45
disjuncte cykel-notatie 27
distributief 2
dodekaeder 31, 32
doorsnede 45
driehoeksongelijkheid 56

echte deelverzameling 45
eenduidige schrijfwijze 11, 27
eindig 48
eindpunt 20
elke 43
en 42
entier 8
equivalent 43
equivalentieklasse 46
equivalentierelatie 46
Euclides 5, 11
Euler, L. 11, 15, 19, 20, 21, 31
eulers 19,20
Euler's veelvlakformule 31
even permutatie 28
existentiële quantificator 44
extremum 75

Fermat, P. de 11
Fibonacci getallen 39
functie 46

gehele getallen 3
geïsoleerd punt 57
genererende functie 39
geordend lichaam 54
gerichte graaf 20
gesloten

van bewerking 3
van verzameling 57
getallenstelsel 9
Goldbach, C. 12
Gödel, K. 51
graad
van knooppunt 19
van polynoom 34
graaf 15
grafiek 46
grootste gemene deler
van getallen 5
van polynomen 37
grootste ondergrens 55
gulden snede 40

Haken, W. 16
handelsreizigersprobleem 17
heuristiek 17
hetzij 43
hexaeder 31, 32

icosaeder 31, 32
identieke afbeelding 47
identieke permutatie 26
impliceert 43
inductiestap 3
infimum 55
injectief 25, 47
insluitingsstelling 56
inverse
van getal 4
van permutatie 25
inverse functie 47
inversiegetal 28
inwendig punt 57
irreducibel 38
isometrie 24

kardinaliteit 48
keten 18,20
keuzeaxioma 50
kleinste bovengrens 55
kleinste gemene veelvoud 5
kleurgetal 17
knooppunt 15
kompakt 65
kopcoëfficiënt 34
kring 18, 20
kubus 31, 32

laatste stelling van Fermat 11
ladenprincipe 50
lege product 10
lege verzameling 44
lengte van een cykel 25
lichaam 54
limiet 58
limietpunt 60
lineaire combinatie 6, 37

maximum 55
Mersenne, M. 12
mersennepriemgetallen 12
metriek 56
metrische ruimte 56
middelwaardestelling 76
minimum 55
model 17
monisch 34

natuurlijke getallen 2
negatie 44
neutraal element 4
niet 42

of 42
oktaeder 31
omgekeerde 4
ondergrens 55
onderling ondeelbaar 5, 39
oneven permutatie 28
ongerijmd 43
open bol 57
open verzameling 57
optellen 2, 34
ophopingspunt 57
orde van permutatie 27
ordening 54
origineel 46
overaftelbaar 48
overdekking 65

paarwisseling 28
pariteit 28
Peano, G. 54
permutatie 26
platte graaf 21
platonisch lichaam 31, 32
polynoom 34
positieve getallen 54
priemgetal 10
priemgetaltweeling 12
product
van getallen 2

van polynomen 34
punt 56
pyramide 30

quantificator 44
quotiënt 4

randpunt 58
rationale functies 35
rationale getallen 4
reducibel 38
reële getallen 55
reflexief 46
regelmatige veelhoek 29
regelmatig veelvlak 31
relatie 46
relatief maximum 75
relatief minimum 75
relatief priem 5
representantensysteem 46
rest 4
restklasse 5, 37
Rolle, M. 75
rotatie 24
Russell, B. 51
rijkompakt 60
rijophopingspunt 60

samengesteld 10
samenhangend 18, 20
samenstelling 26, 47
samenstellingstabel 25
separabel 67
som
van getallen 2
van polynomen 34
spiegeling 25
staartdeling 36
stelling van
van Bolzano 74
van Bolzano-Weierstrass 64
van Cantor 62
van Euler, 19, 20
van Heine-Borel 63
van Rolle 75
supremum 55
surjectief 25, 46
symmetrisch 46

tak 15
Taylor, R. 12
tegengestelde 4
tetraeder 31, 32
tientallig 8
topologie 56
totaal begrensd 66
transitief 46
translatie 24
triviale deler 38
tussenwaardenstelling 74

uitwendig punt 58
uniform continu 72
universele quantificator 44

veelvlak 31
veelvoud 5, 37
vereniging 45
vermenigvuldigen 2, 35
verzameling 44
vierkleurenprobleem 16
viervlak 31
vlakke graaf 20
volledig
van geordend lichaam 55
van metrische ruimte 62
volledige inductie 3

waarheidstabel 48
Weierstrass, K. 54
Wiles, A. 12

Contents

1 HOOFDSTUK: GEHELE GETALLEN **2**

1.1 De natuurlijke getallen. 2

1.2 De gehele getallen. 3

1.3 Een algoritme voor een rekenapparaat (AO) 7

1.4 Representatie van getallen in het g-tallig stelsel. 8

1.5 Priemgetallen. 10

1.6 Meer over priemgetallen (AO) 11

Opgaven bij Hoofdstuk 1. Gehele getallen. 13

2 HOOFDSTUK: GRAFENTHEORIE **15**

2.1 Inleiding. 15

2.2 Eulerse kringen. 18

2.3 Gerichte grafen. 20

Opgaven bij Hoofdstuk 2. Grafentheorie. 22

3 HOOFDSTUK: PERMUTATIES **24**

3.1 Isometrieën. 24

3.2 Permutaties. 26

3.3 Het inversiegetal van een permutatie. 28

3.4 Regelmatige figuren. (AO) 29

3.5 Eulers veelvlakformule. (AO) 31

Opgaven bij Hoofdstuk 3. Permutaties. 33

4 HOOFDSTUK: POLYNOMEN **34**

4.1 Basiseigenschappen. 34

4.2 Breuksplitsing. 39

4.3 Fibonaccigetallen en genererende functies. (AO) 39

Opgaven bij Hoofdstuk 4. Polynomen. 41

5 HOOFDSTUK: LOGICA EN VERZAMELINGENLEER 42

5.1 Logica. 42

5.2 Verzamelingen. 44

5.3 Functies. 46

5.4 Aantal 48

5.5 Bewijzen. 49

5.6 Axioma's. (AO) 50

Opgaven bij Hoofdstuk 5. Logica en verzamelingenleer. 52

6 HOOFDSTUK: DE REËLE GETALLEN 54

6.1 Axioma's voor **R**. 54

6.2 Metrische ruimten. 56

6.3 Rijkompakte verzamelingen. 60

6.4 Volledigheid. 61

6.5 Het geval $X = \mathbf{R}$. 63

6.6 Kompaktheid en rijkompaktheid. (AO) 65

6.7 De Banach contractiestelling. (AO) 68

Opgaven bij Hoofdstuk 6. De reële getallen. 69

7 HOOFDSTUK: CONTINUE REËLE FUNCTIES 71

7.1 Continuïteit. 71

7.2 De Tussenwaardenstelling. 73

7.3 Middelwaardestellingen. 74

Opgaven bij Hoofdstuk 7. Continue reële functies. 77

Huiswerkopgaven **78**

Index **89**