

IVO DE PAUW EN BIEKE MASSELIS

*WISKUNDE
VOOR IT*

Derde herziene druk: juni 2014

Tweede herziene druk: juni 2012

Eerste druk: maart 2010

Foto's: Hoofdstuk 1, David Ritter; Hoofdstuk 2, Wouter Tansens; Hoofdstuk 3, Daryl Beggs, Juan Pablo Arancibia Medina; Hoofdstuk 4, Sofie Eeckeman; Hoofdstuk 5, Filip Joos; Hoofdstuk 6, Wouter Tansens, Sofie Eeckeman; Hoofdstuk 7, Wouter Tansens; Hoofdstuk 8, Wouter Tansens; Hoofdstuk 9, Sofie Eeckeman; Hoofdstuk 10, Wouter Verweider; Hoofdstuk 11, Wouter Tansens; Hoofdstuk 12, Wouter Tansens, Sofie Eeckeman; Hoofdstuk 13, Brecht Wyseur; Hoofdstuk 14, Wouter Tansens; Hoofdstuk 15, Wouter Tansens, Sofie Eeckeman; Hoofdstuk 16, Wouter Tansens, Sofie Eeckeman; p.27, 71, 73, Bieke Masselis; p.82, 353, Wouter Verweider; p.341, Anneleen Tansens.

D/2014/45/465 – ISBN 978 94 014 2100 3 – NUR 918

Vormgeving cover en binnenwerk: Jurgen Leemans

Omslagontwerp: Jan Middendorp, in samenwerking met Ellen Deketele

© Ivo De Pauw, Bieke Masselis & Uitgeverij Lannoo nv, Tielt, 2010.

Uitgeverij LannooCampus maakt deel uit van Lannoo Uitgeverij,
de boeken- en multimedialdivisie van Uitgeverij Lannoo nv.

Alle rechten voorbehouden.

Niets van deze uitgave mag verveelvoudigd worden en/of
openbaar gemaakt, door middel van druk, fotokopie,
microfilm, of op welke andere wijze dan ook, zonder
voorafgaande schriftelijke toestemming van de uitgever.

Uitgeverij LannooCampus

Erasmie Ruelensvest 179 bus 101

3001 Leuven

België

www.lannoocampus.be

Dit boek is opgedragen aan Joke Ceuppens (1977-2006)

“Ze kijkt naar mij, ze ziet me niet: het sneeuwt soms in haar hoofd. Ze zegt me dat ze vlinders ruiken kan, kan ik dat ook?”

Lieven Tavernier (Niet voorbij, oktober 2004)

Inhoud

<i>Dankwoord</i>	15
Hoofdstuk 1 · Instapwiskunde	<u>17</u>
1.1 <i>Letterrekenen</i>	18
Reële getallen	18
Reële veeltermen	23
1.2 <i>Vergelijkingen met één onbekende</i>	25
Lineaire vergelijkingen	25
Kwadratische vergelijkingen	26
1.3 <i>Reflectie</i>	32
Hoofdstuk 2 · Logaritmen	<u>35</u>
2.1 <i>Begripsvorming</i>	36
Definitie	36
Eigenschap	37
Bestaansvoorwaarden	37
Soorten logaritmen	38
2.2 <i>Rekenregels</i>	40
Hoofdbewerkingen	40
Veranderen van grondtal	42
Een notatiekwestie	43
2.3 <i>Logaritmische vergelijkingen</i>	43
Via de definitie	43
Eenzelfde grondtal	43
Gemengde grondtallen	44
2.4 <i>Reflectie</i>	46
Hoofdstuk 3 · Functies	<u>49</u>
3.1 <i>Begrippen uit de reële analyse</i>	50
3.2 <i>Veeltermfuncties</i>	51
Lineaire functies	51
Kwadratische functies	53
Krommen	54
Hogere graadsfuncties	54
3.3 <i>Snijpunten tussen functies</i>	56

3.4	<i>Logaritmische functies</i>	57
3.5	<i>Exponentiële functies</i>	58
3.6	<i>De absolute waarde-functie</i>	60
3.7	<i>Discrete functies</i>	60
	De functie ‘floor’	61
	De functie ‘ceiling’	61
3.8	<i>Reflectie</i>	62
Hoofdstuk 4 · Getalformaten		65
4.1	<i>Soorten getallen</i>	66
	Begrippen uit de rekenkunde	66
	Tiendelige getallen	69
	Tweedelige getallen	70
	Achtdelige getallen	74
	Zestiendelige getallen	76
4.2	<i>Converteren tussen getalformaten</i>	78
	Converteren naar decimaal formaat	78
	Modulorekenen	79
	Converteren van tiendelige naar vreemde getalbases	80
	Hoekformaten	82
	Converteren tussen getalbases die een macht van 2 zijn	83
4.3	<i>Reflectie</i>	85
Hoofdstuk 5 · Getallen in computers		87
5.1	<i>De moderne computer</i>	88
5.2	<i>Getalopslag van natuurlijke getallen</i>	90
	Opslagformaten	91
	Natuurlijke overflow	91
5.3	<i>Getalopslag van gehele getallen</i>	92
	Keuze voor het 2-komplement	93
	Converteren tussen decimale en 2-komplementweergave	95
	2-komplementformaten	96
	Gehele overflow	96
5.4	<i>Getalopslag van reële getallen</i>	98
	Reële opslagfouten	99
	De reële getalopslag als idee	104
	Visualisering van de reële getalopslag	106
	IEEE opslagstandaarden voor \mathbb{R}	113
	Foutvoortplanting	118
5.5	<i>Reflectie</i>	125

Hoofdstuk 6 · Booleaanse wiskunde	<u>127</u>
6.1 <i>Uitsprakenlogica</i>	128
Uitspraken	129
Verbindingen	129
Samengestelde uitspraken en redeneerwetten	131
Bewijsvoering	137
Structuur	138
Paradoxen	138
6.2 <i>Schakelalgebra</i>	140
Schakelaarcircuits	140
Combinatorische circuits	142
6.3 <i>Booleaanse algebra</i>	147
Structuur	147
Axioma's van Huntington	148
Booleaanse rekenregels	149
Booleaanse functies	151
6.4 <i>Karnaughkaarten</i>	156
Begrippen	157
Normaliseren van functies	159
Vereenvoudigen van functies	161
6.5 <i>IT-toepassingen</i>	167
Programmeren	167
RAID4/5	168
Subnetting	170
Nand-technologie	171
6.6 <i>Reflectie</i>	172
Hoofdstuk 7 · Inleiding tot de cryptografie	<u>175</u>
7.1 <i>Begrippen omtrent cryptografie</i>	176
7.2 <i>Het schema van de cryptografie</i>	176
7.3 <i>Soorten cryptografie</i>	177
Indeling naar invoer	177
Indeling naar symmetrie	178
Indeling naar algoritme	179
7.4 <i>Kraakpogingen</i>	179
De kracht van de sleutel	179
De kwaliteit van het algoritme	180
Kraaktechnieken	180
7.5 <i>Cryptografische rekenomgevingen</i>	181
Associatietabellen	181

Restsystemen	183
Oplossen van lineaire vergelijkingen	190
Structuren met één bewerking	192
Structuren met twee bewerkingen	198
7.6 <i>Reflectie</i>	199
Hoofdstuk 8 · Lineaire cijfers	<u>201</u>
8.1 <i>Rekenomgeving</i>	202
De ringstructuur met twee bewerkingen	202
Tweede vuistregel voor modulorekenen	205
8.2 <i>Lineaire cijfers</i>	205
De publieke rekenomgeving	205
De vercijfering	206
De ontcijfering	207
Het algoritme	208
De kraakpoging	209
8.3 <i>Soorten lineaire cijfers</i>	210
Het caesarcijfer	210
Het multiplicatiecijfer	210
Een bijzondere kraakpoging	211
8.4 <i>Reflectie</i>	213
Hoofdstuk 9 · Klutsfuncties	<u>215</u>
9.1 <i>Eenrichtingsfuncties</i>	216
9.2 <i>Klutsfuncties</i>	216
Toepassingen	218
Kwaliteiten van een klutsfunctie	218
9.3 <i>Parallellisatie</i>	219
Restvectoren	220
Chinees reststelling	220
Parallelliseren van hoofdbewerkingen	224
9.4 <i>Uitgebreide grootste gemene deler</i>	225
Het algoritme ‘uggd’	225
Invers element in een reststelsel	226
Bewijs van de chinese reststelling	227
Lineaire vergelijkingen in een reststelsel	228
9.5 <i>Reflectie</i>	234

Hoofdstuk 10 · RSA	<u>237</u>
10.1 <i>Rekenomgeving</i>	238
10.2 <i>Getaltheorie</i>	238
De totiëntfunctie	238
De stelling van Euler	240
Het gemengd modularekenen	240
10.3 <i>Rivest Shamir Adleman</i>	241
De publieke rekenomgeving	241
De versleuteling	241
De ontsleuteling	242
Het algoritme	242
Voorbeeld	243
De kraakpoging	245
10.4 <i>Handtekenen met RSA</i>	246
De handtekening	246
De authenticatie	246
Het algoritme	247
Een gelaagde toepassing	247
10.5 <i>Paralliseren van RSA</i>	249
10.6 <i>Reflectie</i>	253
Hoofdstuk 11 · DSA	<u>255</u>
11.1 <i>Rekenomgeving</i>	256
De veldstructuur met twee bewerkingen	256
Generatoren	258
11.2 <i>Discrete functies</i>	260
Discrete logaritmen	260
Discrete logaritmische functie	260
Discrete exponentiële functie	261
11.3 <i>Diffie-Hellman-sleuteluitwisseling</i>	262
De publieke rekenomgeving	262
De uitwisseling	262
Het algoritme	263
De kraakpoging	264
11.4 <i>Digital Signature Algorithm</i>	266
De publieke rekenomgeving	266
De handtekening	267
De authenticatie	268
Het algoritme	269
De kraakpoging	270
11.5 <i>Reflectie</i>	272

Hoofdstuk 12 · Elliptische krommenversleuteling	<u>275</u>
12.1 <i>Rekenomgeving</i>	276
12.2 <i>Reële elliptische krommen</i>	276
De reële elliptische krommengroep	277
Analytische aspecten	280
12.3 <i>Discrete elliptische krommen</i>	281
Kwadratische residu's	281
Priemkrommen $\mathbb{E}_p(b, c)$	282
De priemkrommengroep	285
Generatorpunten	285
12.4 <i>Priemkrommenencryptografie</i>	289
De publieke rekenomgeving	289
De versleuteling	290
De ontsleuteling	292
Het priemkrommenalgoritme	293
De kraakpoging	294
12.5 <i>Priemkrommenleuteluitwisseling</i>	294
De uitwisseling	295
Het uitwisselingsalgoritme	295
De kraakpoging	296
12.6 <i>Priemkrommenhandtekening</i>	297
De handtekening	297
De authenticatie	298
12.7 <i>Reflectie</i>	299
Hoofdstuk 13 · AES	<u>301</u>
13.1 <i>Rekenomgeving</i>	302
Het binair priemveld \mathbb{Z}_2	302
De binaire quotiëntenringen	303
De binaire galoisvelden	309
13.2 <i>Advanced Encryption Standard</i>	311
De publieke rekenomgeving	311
Het AES-versleutelingsalgoritme	313
De versleuteling als functie	319
Het ontsleutelingsalgoritme	321
De ontsleuteling als omgekeerde functie	326
Herbruikbaarheid van het algoritme	326
Implementeren van het algoritme	328
13.3 <i>De kraakpoging</i>	328
De brute kracht aanval	328
De AES-eenrichtingsfunctie	329
13.4 <i>Reflectie</i>	333

Hoofdstuk 14 · Inleiding tot codes	<u>335</u>
14.1 <i>Begrippen omtrent codes</i>	336
14.2 <i>Het schema van de codeertheorie</i>	337
14.3 <i>Soorten codes</i>	338
Indeling naar doelstelling	338
Indeling naar afstand	339
Indeling naar algoritme	339
14.4 <i>Rekenomgevingen van codes</i>	340
14.5 <i>Constructie van codes</i>	341
De ‘codering’ zonder extra bits	341
Coderingen met één extra bit	342
Een codering met twee overtallige bits	342
Een 3-bit overtallige codering	342
Een 4-bit overtallige codering	343
14.6 <i>Parameters van codes</i>	343
14.7 <i>Foutafhandeling bij algemene codes</i>	346
De ‘codering’ zonder extra bits	346
Coderingen met één extra bit	346
Een codering met twee overtallige bits	347
Een 3-bit overtallige codering	347
Een 4-bit overtallige codering	348
De muisknoppen-codering $C(5, 4, 3)$	348
Een spoorwegsein-codering	349
Dichtste buur-corrigering	351
14.8 <i>Reflectie</i>	353
Hoofdstuk 15 · Lineaire codes	<u>355</u>
15.1 <i>Rekenomgeving</i>	356
Vectorruimten	356
Interne allocatie	358
15.2 <i>Constructie van lineaire codes</i>	358
Het nulcodewoord	359
Hamming gewicht	360
Basiscodewoorden	360
Notatie	361
15.3 <i>Matrixweergave van lineaire codes</i>	362
Generatormatrix G	362
Pariteitstester H	364
15.4 <i>Foutafhandeling bij lineaire codes</i>	366
Syndromen	366

Schema van lineaire codes	374
15.5 <i>Hamming codes</i>	375
Het ontstaan	375
De constructie van hamming codes	375
De foutafhandeling bij hamming codes	376
15.6 <i>Reflectie</i>	377
Hoofdstuk 16 · Cyclische tests	<u>379</u>
16.1 <i>Rekenomgeving</i>	380
16.2 <i>Constructie van cyclische tests</i>	381
Cyclisch testen in \mathbb{Z}	381
Het CRC-algoritme met binaire veeltermen	382
16.3 <i>Cyclische tests versus klutsfuncties</i>	388
Geen integriteitsgarantie	388
Geen eenrichtingsfunctie	389
16.4 <i>Foutafhandeling bij cyclische tests</i>	389
Samenstelling van de CRC-veelterm	390
Illustraties en uitzonderingen	391
De troeven van cyclische tests	393
16.5 <i>Reflectie</i>	395
Hoofdstuk A · Notatie-afspraken	<u>397</u>
A.1 <i>Sleutels</i>	397
A.2 <i>Alfabetten</i>	398
Latijns alfabet	398
Grieks alfabet	398
A.3 <i>Wiskundige symboliek</i>	399
Verzamelingen	399
Wiskundige symbolen	400
Wiskundige sleutelwoorden	401
Getallen	401
Hoofdstuk B · (Windows)ANSI ASCII	<u>403</u>
Hoofdstuk C · Wegwijzers	<u>407</u>
C.1 <i>Didactische wegwijzer</i>	407
C.2 <i>Antwoorden wegwijzer</i>	407
<i>Bronvermelding</i>	408
<i>Index</i>	411

Dankwoord

Volgende mensen bleken van onmisbaar tot onschatbaar bij het maken van dit boek en worden door ons uitdrukkelijk bedankt: Prof. Dr. Leo Storme, Olga Coutrin, Wouter Tansens, Wouter Verweirder, Hilde De Maesschalck, Ellen Deketele, Conny Meuris, Hans Ameel, Tom Decavele, Johan De Gelas, Dr. Rolf Mertig, Dick Verkerck, ir. Gose Fischer, Dr. Tom Wickham-Jones, Prof. Dr. Fred Simons, Dr. Luc Gheysens, Johan Beke, ir. MBA Jan Devos, Marijn Verspecht, ir. Wouter Gevaert, Dr. Philippe Bocher, Tina Defloo, Bart Grimonprez, ir. Sarah Rommens, Wauter Leenknecht, Prof. Dr. Vincent Rijmen, Dr. Joan Daemen, Sofie Eeckeman, Peter Saerens, Mercè Aicart, Jurgen Leemans, Jan Middendorp, Hilde Vanmechelen, Leen Wouters, Jef De Langhe, Wannes Van Wichelen, Eric Van Remortel, Ann Deraedt, Rita Vanmeirhaeghe, Roel Vandommele, ir. Lode De Geyter, Bart Leenknecht, Pascal Voet, Jill Vandendriessche, Dieter Roobrouck, Nicolaas Bijvoet, dr. ir. Frederik Vercauteren, Jef Daels, Anne-Mieke Vandenbulcke, alle multimediale Howestcollega's en iedereen die we even waren vergeten!

Hoofdstuk I · Instapwiskunde



Dit hoofdstuk omvat de onmisbare lees- en rekenvaardigheden voor het verder bestuderen van technologische onderwerpen in hun rekenomgeving.

De opeenvolgende paragrafen van dit hoofdstuk stippen met dit oogmerk stapsgewijze aspecten van de ‘wiskundige taal’ aan die wordt gesproken op allerlei toepassingsniveaus.

1.1 Letterrekenen

REËLE GETALLEN

We noteren de verzameling van alle:

- ▷ natuurlijke getallen (unsigned integers) als \mathbb{N} ,
- ▷ gehele getallen (integers) als \mathbb{Z} ,
- ▷ rationale getallen of breuken als \mathbb{Q} ,
- ▷ reële getallen (floats of reals) als \mathbb{R} .

Deze getallenverzamelingen zijn als volgt genest: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

We vervolgen met wat terminologie, waar vaak verwarring over bestaat, zodat we dezelfde taal spreken. We wijzen erop dat het correct verwoorden ervan een weerspiegeling is van correct denken.

Verzamelingen

- ▷ **Deelverzamelingen** worden altijd tussen accolades genoteerd, bijvoorbeeld de **ledige verzameling** noteren we als $\{\}$.
- ▷ Een **singleton** definiëren we als een verzameling met juist één element. We geven $\{5\}$ als voorbeeld van een singleton. Dit is een deelverzameling van de verzameling van de natuurlijke getallen, $\{5\} \subset \mathbb{N}$.
- ▷ Een **paar** definiëren we als een verzameling met juist twee elementen. De verzameling van de Booleaanse waarheidswaarden vormt bijvoorbeeld een paar $\{\text{waar}, \text{onwaar}\}$, kortweg te noteren als \mathbb{B} . Geven we anderzijds $\{115, -4\}$ als voorbeeld, dan is dit paar een deelverzameling van de verzameling van de gehele getallen of in symbolen $\{115, -4\} \subset \mathbb{Z}$.
- ▷ Deelverzamelingen zoals \mathbb{Z}^- definiëren we als $\{\dots, -3, -2, -1, 0\}$ of de verzameling van enkel de negatieve gehele getallen. We noteren $-1234 \in \mathbb{Z}^-$ als we benadrukken dat het negatief getal -1234 een **element** is van \mathbb{Z}^- .

- ▷ Als we elementen uit een verzameling wegnemen, doen we dat met de **verschilbewerking** voor verzamelingen, die genoteerd wordt als ‘backslash’. Zo noteren we bij wijze van illustratie hiervan de verzameling van de natuurlijke getallen zonder nul als $\mathbb{N} \setminus \{0\}$, de verzameling van alle breuken uitgezonderd de gehele getallen als $\mathbb{Q} \setminus \mathbb{Z}$ en de verzameling van alle reële getallen uitgezonderd nul en één als $\mathbb{R} \setminus \{0, 1\}$.

Hoofdbewerkingen

operatie	voorbeeld	getal a heet	getal b heet	uitkomst c heet
optelling	$a + b = c$	term	term	som
aftrekking	$a - b = c$	term of aftrektal	term of aftrekker	verschil
vermenigvuldiging	$a \cdot b = c$	factor	factor	product
deling	$\frac{a}{b} = c, b \neq 0$	deeltal of teller	deler of noemer	quotiënt
machtsverheffing	$a^b = c$	grondtal	exponent	macht
worteltrekking	$\sqrt[b]{a} = c$	grondtal	wortel	wortel

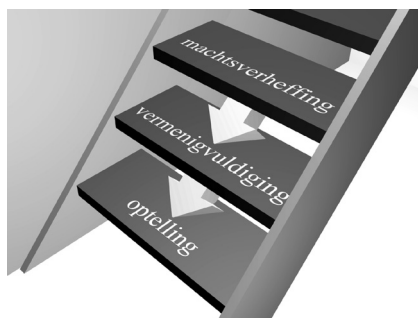
Het **tegengestelde** van een reëel getal r noteren we als $-r$ en definiëren we als $r + (-r) = 0$. Het **invers** of **omgekeerde** van een reëel getal r noteren we als $\frac{1}{r}$, ofwel r^{-1} en definiëren we als $r \cdot r^{-1} = 1$. Aftrekken definiëren we als het optellen met het tegengestelde: $a - b = a + (-b)$. Delen definiëren we als het vermenigvuldigen met het omgekeerde: $a : b = a \cdot b^{-1}$.

Wanneer bewerkingen elkaar ontmoeten, zijn we gehouden aan rekenregels. We herhalen hiertoe alle essentiële rekenregels in een notendop. Er geldt een vaste volgorde voor het uitvoeren van bewerkingen in \mathbb{R} , dat gememoriseerd kan worden met de volgende zin ‘Het Mannetje won Van De Oude Aap’.

- ▷ Eerst alles uitrekenen tussen de haakjes,
- ▷ daarna alle machten (een vierkantswortel is ook een macht),
- ▷ dan alle vermenigvuldigingen en delingen van links naar rechts,
- ▷ ten slotte de optellingen en aftrekkingen van links naar rechts.

Er geldt ook **distributiviteit** in \mathbb{R} . Distributiviteit definiëren we als de verdeel-eigenschap van een ‘hogere’ bewerking over een ‘lagere’ bewerking. Distributiviteit vereist dus twee *verschillende* bewerkingen.

Zo noteren we distributiviteit van *machtsverheffen* over *vermenigvuldigen* bijvoorbeeld als $(a \cdot b)^3 = a^3 \cdot b^3$. Eveneens noteren we de distributiviteit van *vermenigvuldigen* over *optellen* als $3 \cdot (a + b) = 3 \cdot a + 3 \cdot b$.



We hoeden ons ervoor tegen deze ‘trap van distributiviteit’ fouten te maken, daar in het algemeen geldt:

$$(a + b)^3 \neq a^3 + b^3,$$

$$\sqrt{a + b} \neq \sqrt{a} + \sqrt{b},$$

$$\sqrt{x^2 + y^2} \neq x + y.$$

Breuken

Een **breuk** is de schrijfwijze van een rationaal getal onder de vorm $\frac{t}{n}$ met $t, n \in \mathbb{N}$ en $n \neq 0$. In $\frac{t}{n}$ is t de **teller** en n de **noemer**. De omgekeerde breuk van $\frac{t}{n}$ met $t, n \neq 0$ definiëren we als $\frac{1}{\frac{t}{n}} = \frac{n}{t}$, ofwel $\left(\frac{t}{n}\right)^{-1}$. De tegengestelde breuk is dan gelijk aan $-\frac{t}{n} = \frac{-t}{n} = \frac{t}{-n}$. De rekenregels voor breuken kunnen we als volgt samenvatten:

$$\text{som} \quad \frac{t}{n} + \frac{a}{b} = \frac{t \cdot b + n \cdot a}{n \cdot b},$$

$$\text{verschil} \quad \frac{t}{n} - \frac{a}{b} = \frac{t \cdot b - n \cdot a}{n \cdot b},$$

$$\text{product} \quad \frac{t}{n} \cdot \frac{a}{b} = \frac{t \cdot a}{n \cdot b},$$

$$\text{deling} \quad \frac{\frac{t}{a}}{\frac{b}{c}} = \frac{t}{n} \cdot \frac{b}{a},$$

$$\text{machtsverheffing} \quad \left(\frac{t}{n}\right)^m = \frac{t^m}{n^m},$$

$$\text{singuliere breuken} \quad \frac{1}{0} = \pm\infty \text{ limietgeval},$$

$$\frac{0}{0} = ? \text{ onbepaald.}$$

Machten

Een **macht** is de schrijfwijze van een reëel getal onder de vorm g^m . In g^m is g het **grond-tal** en m de **exponent**. Een tegengestelde macht van g^m definiëren we als $-g^m$ en een omgekeerde macht wordt genoteerd als $\frac{1}{g^m} = g^{-m}$, met $g \neq 0$.

Afhankelijk van de waarde van de exponent hebben we een andere betekenis:

$$\begin{aligned} g^3 &= g \cdot g \cdot g & 3 \in \mathbb{N}, \\ g^{-3} &= \frac{1}{g^3} = \frac{1}{g \cdot g \cdot g} & -3 \in \mathbb{Z}, \\ g^{\frac{1}{3}} &= \sqrt[3]{g} = w \Leftrightarrow w^3 = g & \frac{1}{3} \in \mathbb{Q}, \\ g^0 &= 1 & g \neq 0. \end{aligned}$$

In de praktijk komen soms stappen voor, zoals:

$$\begin{aligned} \text{product} \quad & g^3 \cdot g^2 = g^{3+2} = g^5, \\ \text{deling} \quad & \frac{g^3}{g^2} = g^3 \cdot g^{-2} = g^{3-2} = g^1, \\ \text{macht} \quad & (g^3)^2 = g^{3 \cdot 2} = g^6. \end{aligned}$$

We wijzen erop dat het een goed idee is machtsworteltekens te herschrijven in de moderne notatie en uitdrukkingen zoals $\sqrt[7]{g^3}$ te herschrijven als een macht met grondtal g en exponent $\frac{3}{7}$, dus $g^{\frac{3}{7}}$. We merken bovendien op dat de vierkantswortel op zich altijd een positief getal is, $\sqrt{a} = a^{\frac{1}{2}} \in \mathbb{R}^+$.

Zowel de betekenis van de exponenten, als de rekenregels zijn vereist om succesvol met machten om te gaan. Verder is het handig de kwadraten in het gehele interval $1^2 = 1$, $2^2 = 4, \dots$, $15^2 = 225$, $16^2 = 256$ en derdemachten in het interval $1^3 = 1$, $2^3 = 8, \dots$, $7^3 = 343$, $8^3 = 512$ te (her)kennen.

Onthoud dat de enige manier om een macht op te heffen, de inverse machtsverheffing is. Hiertoe gebruiken we dus links én rechts (zoals we bij vergelijkingen, zie paragraaf 1.2, doen) de omgekeerde exponent.

Voorbeeld: bepaal x als we weten dat $\sqrt[7]{x^3} = 5$. We passen de rekenregel toe waarbij een macht van een macht herleid wordt tot één macht met product van exponenten.

$$(x)^{\frac{3}{7}} = 5 \iff \left((x)^{\frac{3}{7}} \right)^{\frac{7}{3}} = x = (5)^{\frac{7}{3}} \approx 42,7494.$$

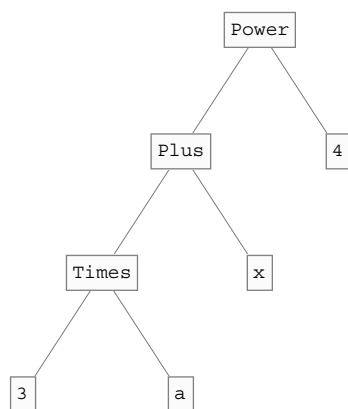
We stellen vast dat enkel met deze strategie het gezochte grondtal x bevrijd raakt van onder zijn exponent en kan worden afgelezen als uitdrukking of desgewenst numeriek benaderd.

Wiskundige uitdrukkingen

Vooral samengestelde wiskundige uitdrukkingen kunnen nogal intimiderend overkomen of ronduit leesdrempels veroorzaken. Om een uitdrukking vlot te doorzien, wijzen we alvast op het bestaan van geïndexeerde variabelen. Geïndexeerde variabelen definiëren we als onbekenden voorzien van een benedenindex om ze af te tellen, zoals:

$x_1, x_2, x_3, x_4, \dots, x_{99999}, x_{100000}, \dots$, en $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots$ enz. Industriële toepassingen die duizenden variabelen vereisen, zijn namelijk verre van uitzonderlijk, daar waar ons alfabet 26 letters telt.

Eindige uitdrukkingen definiëren we als een samenstelling van operatoren (bewerkingen) op objecten (getallen, variabelen of structuren). We doorgronden bijvoorbeeld een uitdrukking $(3a+x)^4$ (indien nodig) door het schetsen van zijn **boom-vorm**. In ons voorbeeld betreft het een macht (Power) met exponent 4 van grondtal een som (Plus), enzovoort.



We evalueren hier even onze uitdrukking $(3a+x)^4$. Stellen we $a = 1$, dan resulteert dit in een gedeeltelijk ‘inklappen’ tot de eenvoudiger expressie $(3+x)^4$. Stellen we vervolgens ook nog $x = 2$, dan verkrijgen we de corresponderende getalwaarde $(3+2)^4 = 5^4 = 625$ als resultaat.

Werken we deze 4^{de} macht uit tot de **som-vorm** $81a^4 + 108a^3x + 54a^2x^2 + 12ax^3 + x^4$, dan herschreven we de **product-vorm** $(3a+x)^4$ slechts naar een andere *gedaante*.

Deze expressie, die geen relatie is, proberen op te lossen is echter onzinnig. Enkel en alleen ongelijkheden, vergelijkingen of stelsels daarvan kunnen worden opgelost.

Relaties

We nemen hier ook de relationele uitdrukkingen heel beknopt onder de loep.

Een **ongelijkheid** definiëren we als een *veranderlijke* afweging waarin een linkerlid vergeleken wordt met een rechterlid door hetzij het ‘is-(strikt)-kleiner-dan’, hetzij het ‘is-(strikt)-groter-dan’ teken. Bij wijze van voorbeeld hiervan noteren we $(3a+x)^4 \leq (b+4)(x+3)$ in de onbekenden a, x, b . Ongelijkheden kunnen eventueel worden opgelost naar een onbekende a, x of b .

Een **vergelijking** definiëren we als een *veranderlijke* afweging waarin een linkerlid vergeleken wordt met een rechterlid door het gelijkheidsteken. De uitdrukking $(3a+x)^4 = (b+4)(x+3)$ is een vergelijking in de onbekenden a, x, b . Ook vergelijkingen kunnen eventueel worden opgelost naar een onbekende a, x of b .

Een **identiteit** (of gelijkheid) definiëren we als een uitspraak die constant *waar* is, bijvoorbeeld $7 = 7$. Een **contradictie** (of tegenstrijdigheid) definiëren we als een uitspraak die constant *onwaar* is, bijvoorbeeld $-10 > 5$.

REËLE VEELTERMEN

Op deze plaats gaan we even in op de rekenomgeving van de reële veeltermen in de variabele x ; een verzameling die we noteren als $\mathbb{R}_{[x]}$.

▷ Eentermen

Een **eenterm** in x definiëren we als een uitdrukking ax^n , met a een getal en $n \in \mathbb{N}$. Bij uitbreiding kan deze lettervorm ook bestaan uit een aantal variabelen x, y, z, \dots . Bijvoorbeeld $3(xy)^6$ en $3(x^2y^3z^6)$ zijn eentermen in respectievelijk xy en $x^2y^3z^6$.

De **graad** van een eenterm ax^n definiëren we als de natuurlijke exponent $n \in \mathbb{N}$ van de beoogde variabele x . Op deze manier onderscheiden we constante, lineaire, kwadratische, kubische of hogere graads eentermen. Constante eentermen zijn van graad 0, lineaire eentermen hebben graad 1, kwadratische graad 2 en kubische graad 3.

Nemen we als voorbeeld de reële eenterm $-\sqrt{12}x^6$, dan is de graad hiervan 6. Analoog is $3(xy)^6$ een eenterm in xy van graad 6, en is $3(x^2y^3z^6)^9$ een eenterm in $x^2y^3z^6$ van graad 9.

Gelijksoortige eentermen definiëren we als eentermen met identiek lettergedeelte. Zo zijn bijvoorbeeld de reële eentermen $\frac{5}{7}x^6$ en $-\sqrt{12}x^6$ gelijksoortig en ook $\frac{5}{7}x^3y^5z^2$ en $-\sqrt{12}x^3y^5z^2$ zijn gelijksoortig.

Alle (hoofd)bewerkingen op eentermen zijn uitvoerbaar als onmiddellijke toepassing van de rekenregels voor breuken en machten.

▷ Veeltermen

Een **veelterm** $V(x)$ definiëren we als een som van ongelijksoortige eentermen. De **graad** van een veelterm $V(x)$ definiëren we als de maximum exponent $m \in \mathbb{N}$ van de beoogde variabele x . Nemen we als voorbeeld de reële veelterm

$$V(x) = 17x^2 + \frac{1}{4}x^3 + 6x - 7x^2 - \sqrt{12}x^6 - 13x - 1,$$

dan is de graad van $V(x)$ gelijk aan de maximum exponent 6.

Herleiden of vereenvoudigen van veeltermen is mogelijk daar waar gelijksoortige eentermen ervan bijeen kunnen worden genomen. We vereenvoudigen even ons voorbeeld hiervoor tot de vorm $V(x) = 10x^2 + \frac{1}{4}x^3 - 7x - \sqrt{12}x^6 - 1$.

Eenzelfde veelterm kunnen we in op- of aflopende machten van x rangschikken. Rangschiikken we $V(x)$ naar oplopende machten van x , dan komt er $V(x) = -1 - 7x + 10x^2 + \frac{1}{4}x^3 - \sqrt{12}x^6$. Rangschiikken we $V(x)$ naar aflopende machten van x , dan noteren we $V(x) = -\sqrt{12}x^6 + \frac{1}{4}x^3 + 10x^2 - 7x - 1$.

Uiteraard kunnen we veeltermen ook als expressie evalueren tot een getalwaarde. Bepalen we bijvoorbeeld de getalwaarde van $V(x)$ in $x = -1$, dan komt er $V(-1) = -\sqrt{12}(-1)^6 + \frac{1}{4}(-1)^3 + 10(-1)^2 - 7(-1) - 1 = -\sqrt{12} - \frac{1}{4} + 16 = \frac{63}{4} - 2\sqrt{3} \in \mathbb{R}$.

▷ Hoofdbewerkingen

Som van twee gelijksoortige eentermen: we tellen de coëfficiënten op en behouden het lettergedeelte

$$5a^2 - 3a^2 = (5 - 3)a^2 = 2a^2.$$

Product van eentermen: we vermenigvuldigen de coëfficiënten en de lettergedeelten elk apart

$$-5ab \cdot \frac{7}{4}a^2b^3 = -5 \cdot \frac{7}{4} \cdot a^{1+2}b^{1+3} = \frac{-35}{4}a^3b^4.$$

Quotiënt van eentermen: we delen de coëfficiënten door elkaar en we delen de lettergedeelten

$$\frac{-8a^6b^4}{-4a^4} = \frac{-8}{-4} a^{6-4}b^{4-0} = 2a^2b^4.$$

Macht van een eenterm: we verheffen elke factor van de eenterm tot de macht

$$(-2a^2b^4)^3 = (-2)^3(a^2)^3(b^4)^3 = -8a^6b^{12}.$$

Optellen en aftrekken van veeltermen: we tellen de termen van de tweede veelterm op bij de eerste of we trekken de termen van de tweede af van de eerste veelterm

$$(x^2 - 4x + 8) - (2x^2 - 3x - 1) = x^2 - 4x + 8 - 2x^2 + 3x + 1 = -x^2 - x + 9.$$

Product van veeltermen: we vermenigvuldigen elke term van de ene veelterm met elke term van de andere veelterm en tellen de verkregen producten op

$$\begin{aligned} (2x^2 + 3y) \cdot (4x^2 - y) &= 2x^2(4x^2 - y) + 3y(4x^2 - y) \\ &= 2x^2 \cdot 4x^2 + 2x^2 \cdot (-y) + 3y \cdot 4x^2 \\ &\quad + 3y \cdot (-y) \\ &= 8x^4 - 2x^2y + 12x^2y - 3y^2 \\ &= 8x^4 + 10x^2y - 3y^2. \end{aligned}$$