Samenvatting Math For IT

# Boole Algebra

## Rekenen in Boole Algebra

### Axioma’s

∀ x, y ∈ B x + y ∈ B Intern  
 x \* y ∈ B

∀ x, y ∈ B x + y = y + x Commutatief  
 x \* y = y \* x

∀ x, y, z ∈ B x \* (y + z) = x \* y + x \* z Distributief  
 x + y \* z = (x + y) \* (x + z)

0 ∈ B, ∀ x ∈ B x + 0 = x Neutraal element  
1 ∈ B, ∀ x ∈ B x \* 1 = x

∀ x ∈ B : ∃ ∈ B x + = 1 Complementering  
 x \* = 0

### Stellingen

∀ x, ∈ B = x Involutief

∀ x, ∈ B x + x = x Idempotentie  
 x \* x = x

∀ x, ∈ B x + 1 = 1 Absorberend element  
 x \* 0 = 0

∀ x, y ∈ B x + x \* y = x Absorptiewet  
 x \* (x + y) = x

∀ x, y ∈ B Wetten van De Morgan

### Bewijzen van stellingen

*Stelling : het complement is uniek*Bewijs : stel dat a en b complement zijn van x  
 x + a = 1 x + b = 1  
 x \* a = 0 x \* b = 0  
  
 a = a \* 1 b = b \* 1  
 = a . (x + b) = b \* (x + a)  
 = a \* x + a \* b = b \* x + b \* a  
 = x \* a + a \* b = x \* b + b \* a  
 = 0 + a \* b = 0 + b \* a  
 = a \* b = a \* b

1 neutraal el voor \*  
def complement  
\* distri tov +  
commutatief  
def complement  
0 neutraal el voor +

1 neutraal el voor \*  
def complement  
\* distri tov +  
commutatief  
def complement  
0 neutraal el voor +

def complement

Conclusie : a = a \* b en b = a \* b ⇒ a = b

*Stelling : het complement is involutief (complement van complement is oorspronkelijk)*Bewijs :

def commutativiteit

def complement

def complement

is het complement van   
 is het complement van

is het complement van want het complement is uniek

*Stelling : idempotentie*Bewijs : Omwille van dualiteit volstaat het aan te tonen dat

1 neutraal el voor \*  
def complement  
def distributiviteit  
def complement  
0 neutraal el voor +

*Stelling : absorberende elementen*Bewijs : Omwille van dualiteit volstaat het aan te tonen dat

1 neutraal el voor \*  
def complement  
+ distr tov \*  
1 neutraal el voor \*  
def complement

*Stelling : absorptiewetten*Bewijs : Omwille van dualiteit volstaat het aan te tonen dat

1 neutraal el voor \*  
\* distr tov +  
1 absorberend el voor +  
1 neutraal el voor \*

*Stelling : wetten van De Morgan*Bewijs : Omwille van dualiteit volstaat het aan te tonen dat   
  
We tonen aan dat en  
 .

We hebben dan bewezen dat want het complement is uniek.

### Volgorde van bewerkingen

\* distri tov +  
def complement & commutatief  
def complement  
0 absorberend el voor \*  
0 neutraal el voor +

+ distri tov x  
def complement  
1 neutraal el voor \*  
def commutativiteit  
def complement  
1 absorberend el voor +

1. Haakjes uitwerken
2. Gemeenschappelijke factoren
3. Distributiviteit van + t.o.v. \*
4. Dualiteitsprincipe

## De Disjunctieve Normaalvorm (DNV)

### Definitie

Een Boole-functie is geschreven in de disjunctieve (doorsnede) normaalvorm, als ze de som is van minimale termen.

## Veitch – Karnaugh diagram (VK)

### Samenvatting

* Elk rechthoekje van de VK stelt een minimale term voor.
* Een product van 2 veranderlijke wordt voorgesteld door 2 aangrenzende vakjes.
* Aangrenzend wil ook zeggen alsof de rechterkant op de linkerkant aansluit. Idem voor de boven- en onderkant.

### Werkwijze

1. Breng de Boole functie in de vorm van som van producten.
2. Stel een VK-diagram op.
3. Lees de VK vereenvoudigd af. Let hierbij op zoveel mogelijk aangrenzende vakjes samen te nemen.
4. ! Omcirkel de vakjes die je samen neemt !

## Propositielogica

### Definities

Een propositie is een uitspraak over iets die waar of onwaar kan zijn.

Een samengestelde uitspraak is een tautologie of een wat als ze waar is voor alle waarheidswaarden van de enkelvoudige uitspraken.

Een samengestelde uitspraak is een contradictie als ze vals is voor alle waarheidswaarden van de enkelvoudige uitspraken.

### Samenvatting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Symbool | Betekenis | Benaming | Boole | Prioriteit |
| ^ | En | Conjunctie | p \* q | 2 |
| v | Of | Disjunctie | p + q | 3 |
|  | Niet | Negatie |  | 1 |
| ⊕ | Exclusieve of |  | p ⊕ q = \* q + p \* | 3 |
|  | Implicatie | Als … dan … | p q = + q | 4 |
|  | Equivalentie | Als en slechts als | P q = \* + p \* q | 4 |

## Schakelalgebra

### Samenvatting

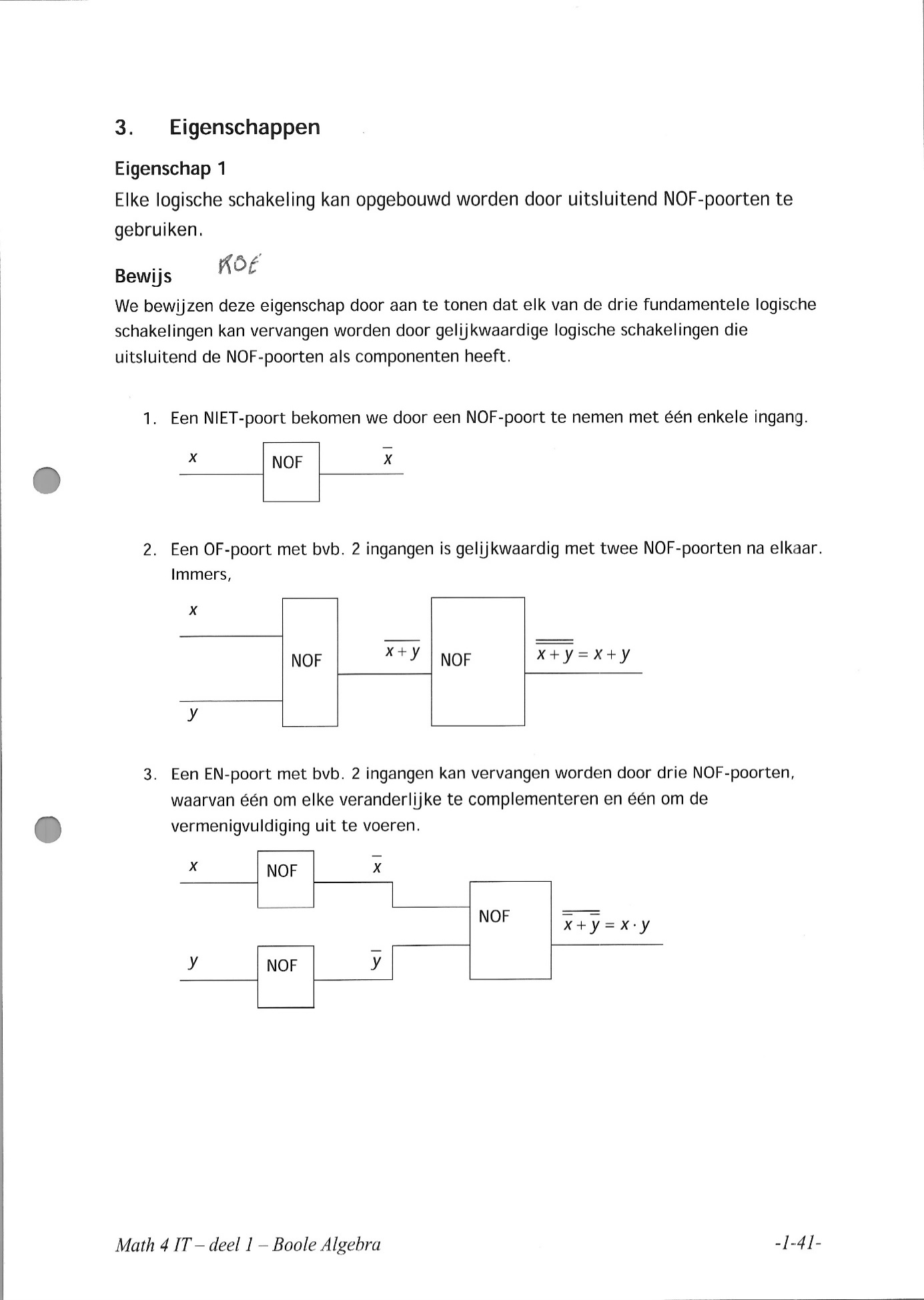
|  |  |  |  |
| --- | --- | --- | --- |
| Poort | Aantal ingangen | Voorstelling | Herkenbaar door |
| EN | 2 of meer ingangen |  | & |
| OF | 2 of meer ingangen |  | ≥1 |
| NIET | 1 ingang |  | 1  0 achteraan |
| XOF – XOR | 2 of meer ingangen |  | =1 |
| NEN | 1 ingang  2 of meer ingangen |  | 1  0 achteraan  &  0 achteraan |
| NOF – NOR | 1 ingang  2 of meer ingangen |  | 1  0 achteraan  ≥1  0 achteraan |

### Eigenschappen en hun bijhorende bewijzen

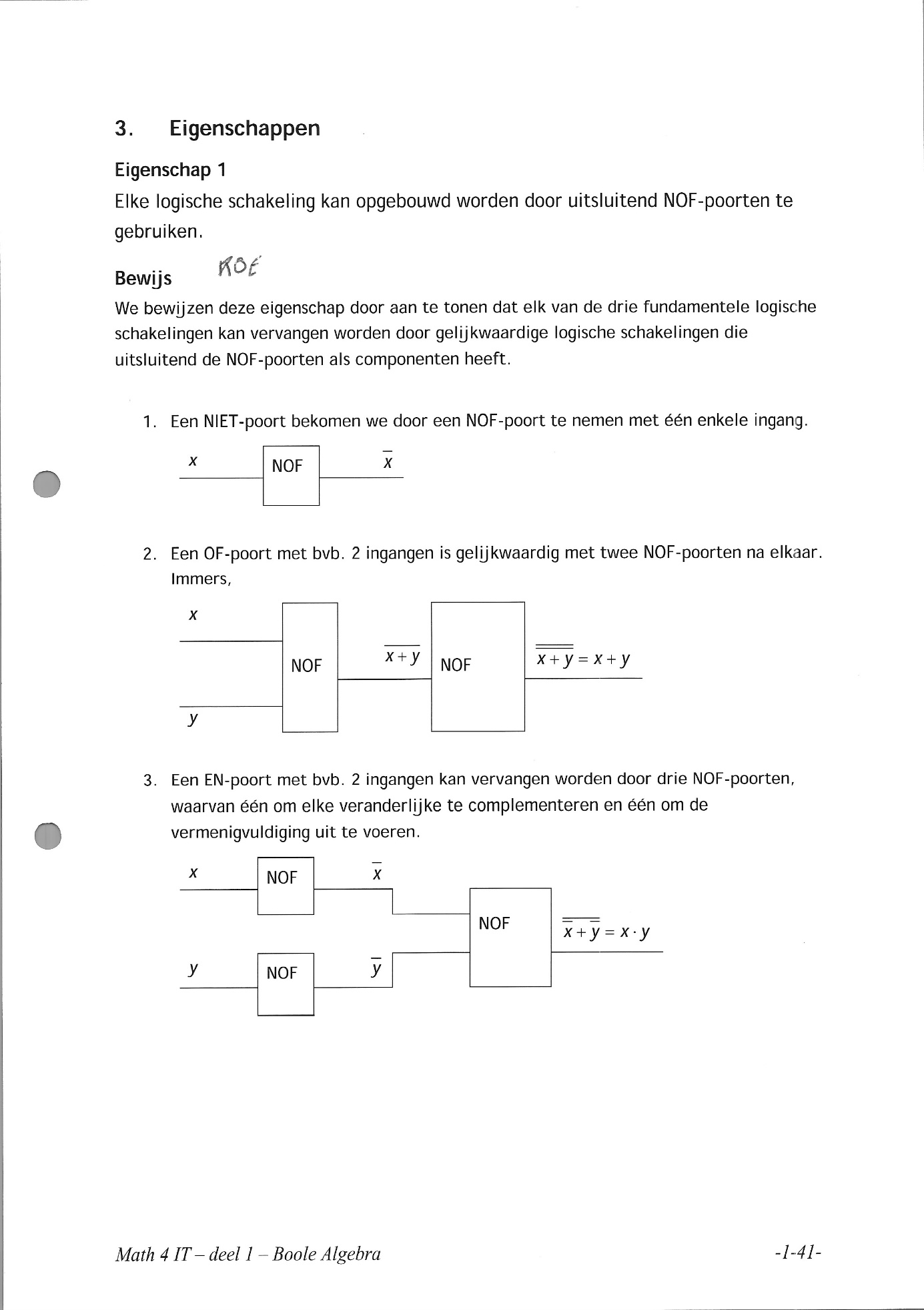
#### Elke logische schakeling kan opgebouwd worden door uitsluitend NOF-poorten te gebruiken

Dit bewijzen we doordat elke fundamentele logische schakeling kan vervangen worden door een evenwaardige schakeling met enkel NOF-poorten.

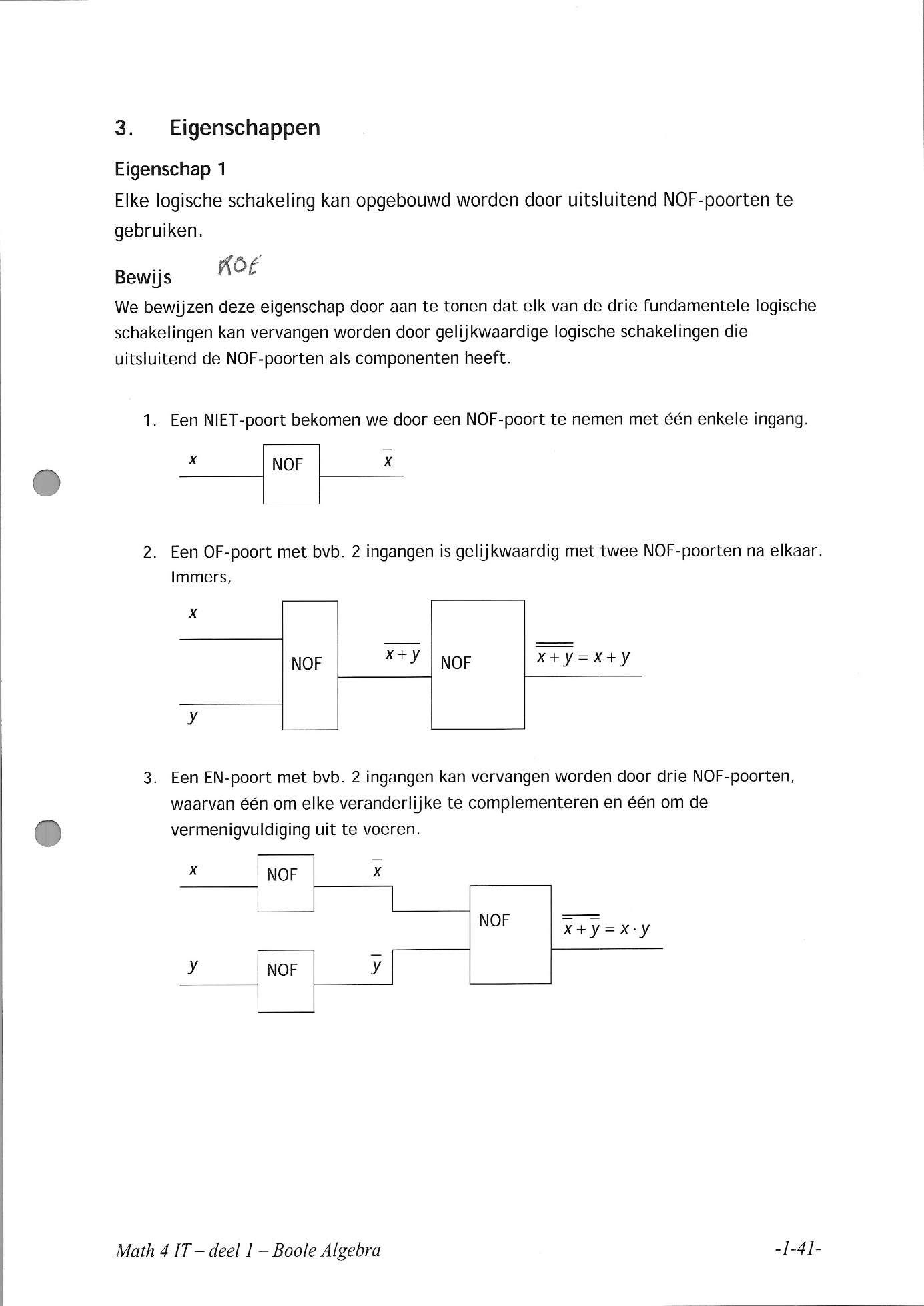
1. Een NIET-poort bekomen we door een NOF-poort te nemen met één enkele ingang.



1. Een OF-poort met bvb. 2 ingangen is gelijkwaardig met twee NOF-poorten na elkaar.



1. Een EN-poort met bvb. 2 ingangen kan vervangen worden door drie NOF-poorten, waarvan één om elke veranderlijke te complementeren en één om de vermenigvuldiging uit te voeren.



#### Elke logische schakeling kan opgebouwd worden door uitsluitend NEN-poorten te gebruiken

Dit bewijzen we doordat elke fundamentele logische schakeling kan vervangen worden door een evenwaardige schakeling met enkel NEN-poorten.

1. Een NIET-poort bekomen we door een NEN-poort te nemen met één enkele ingang.

Afbeelding met tekst

Beschrijving is gegenereerd met zeer hoge betrouwbaarheid

1. Een OF-poort met bvb. 2 ingangen kan vervangen worden door drie NEN-poorten, waarvan één om elke veranderlijke te complementeren en één om de optelling uit te voeren.

Afbeelding met tekst

Beschrijving is gegenereerd met zeer hoge betrouwbaarheid

1. Een EN-poort met bvb. 2 ingangen is gelijkwaardig met twee NEN-poorten na elkaar.

Afbeelding met tekst

Beschrijving is gegenereerd met zeer hoge betrouwbaarheid

### Optelling van binaire getallen

#### Som van 2 binaire getallen met 1 bit waarde (halve opteller)

C = A . B  
S = A . + . B

#### Som van 3 binaire getallen met 1 bit waarde (hele opteller)

C = A . B + A . C + B . C  
S = A . . + . B . + . . C + A . B . C

#### Som van 2 binaire getallen met 4 bit waarde (4 bit adder)

2adder -> 3adder -> 3adder -> 3adder

### Binaire logische bewerkingen

#### AND – EN

Enkele bits op 0 te zetten en de rest ongewijzigd laten.

#### OR – OF

Enkele bits op 1 zetten en de rest ongewijzigd laten.

#### XOR – XOF

Enkele bits inverteren en de rest ongewijzigd laten.

#### NOT – NIET

Alle bits inverteren.

## Verzamelingenleer

### Definities

Een verzameling is een groep van elementen, die voldoen aan een bepaald criterium, dit noteren we door middel van U.

Een element p kan behoren tot een (deel)verzameling, dit noteren we door middel van p ∈ U.

Een verzameling A is een deelverzameling van verzameling U als elk element van A ook tot U behoort, dit noteren we door middel van A ⊂ U.

### Samenvatting

|  |  |  |  |
| --- | --- | --- | --- |
| Symbool | Betekenis | Benaming | Boole |
| ∩ | … en … | Doorsnede | A \* B |
| ∪ | … of … | Unie | A + B |
| AC | Niet | Complement | -A |
| A \ B | Alles tot A maar niet tot B | Verschil | A ∩ BC = A \* -B |
| A B | A of B maar niet A en B | Exclusieve of | A B = (A + B) \ (A \* B) |
| U | Heeft alle elementen | Niet-ledige verzameling | 1 |
| Ø | Heeft geen elementen | Ledige verzameling | 0 |
| D (U) | Verzameling van alle deelverzamelingen | |  |

# EuMathT

## Toolbox-commando’s

// commentaar op 1 lijn  
F5 meerdere regels commentaar  
F9 internal editor openen om functies te schrijven  
& uitrekenen in Maxima (preciezer)  
help # hulp bij # in Euler  
mxmhelp # hulp bij # in Maxima  
| iets aan iets toevoegen (strings aan elkaar of nieuw element in array)  
; output onderdrukken

## Berekeningen-commando’s

Fracprint print output in breuken  
printhex print output in wetenschappelijke notatie  
mod toont rest bij deling  
floor # toont grootste int onder #  
ceil # toont grootste int boven #  
intrandom # toont een random getal met bereik [1, #]  
plot2d toont een 2d-grafiek  
plot3d toont een 3d-grafiek

## Structuren

### If-else

if voorwaarde  
 then #  
 else #  
endif

### If-else-if

if voorwaarde  
 then #  
 elseif voorwaarde  
 then #  
 else #  
 endif  
endif

### For-loop

for i = # to # step #  
 //CODE  
end

### While-loop

repeat while voorwaarde  
 //CODE  
end

# Cryptografie

## Definitie

Een sleutel is de informatie die iemand nodig heeft om een boodschap te encrypteren of te decrypteren. Dit kan gaan om een getal, een paswoord of een sleutelzin.

## Symmetrische cryptosystemen

De zender en de ontvanger hebben dezelfde sleutel.

### Technieken

Transpositie: het wisselen van de letters van het bericht op een vooraf afgesproken manier.  
Substitutie: de letter vervangen door andere letters op een vooraf afgesproken manier.

### Caesarrotatie (Caesarsubstitutie methode)

Elke letter in het alfabet wordt cyclisch over k plaatsen verschoven. De sleutel is hier de k. Zender en ontvangen moeten duidelijk eerst de sleutel afspreken.

Encrypteren:

1. Letters naar getallen
2. Sleutel optellen
3. Modulo van aantal mogelijke tekens
4. Getallen naar letters

Decrypteren:

1. Letters naar getallen
2. Sleutel aftrekken
3. Modulo van aantal mogelijke tekens
4. Getallen naar letters

### Bitoperator XOR (XORsubstitutie methode)

Encrypteren:

1. Boodschap en sleutel naar getallen -> hexadecimaal -> binair
2. XOR-operator toepassen
3. Boodschap naar letters door -> hexadecimaal -> letters

Decrypteren:

1. Boodschap en sleutel naar getallen -> hexadecimaal -> binair
2. XOR-operator toepassen
3. Boodschap naar letters door -> hexadecimaal -> letters

### Kraken van substitutiemethoden

Elke letter wordt hetzelfde geëncrypteerd en er kan dus aan patroonherkenning gedaan worden. Een oplossing hiervoor is het gebruik van een blokcijfersysteem. Hierbij wordt de boodschap in blokjes verdeelt die de lengte van de sleutel hebben. Het is hier dus voordelig een korte sleutel te hebben.

### DES (Data Encryption Standard)

DES vercijfert in groepjes van 64 bits. De sleutel is ook 64 bits. Men kan 256 verschillende sleutels gebruiken. De tekst is moeilijk te ontcijferen. 3DES gebruikt men om driemaal een DES encryptie te doen (op basis van 3 sleutels). De opvolger AES (Advanced Encryption Standard) werkt met sleutels van 128, 192 of 256 bits.

## Asymmetrische cryptosystemen

Zender versleuteld bericht met openbare sleutel van ontvanger. Ontvanger kan ontcijferen met zijn privésleutel.

### Vercijferen

Stap 1: tekst naar ASCII  
Stap 2: e en m van ontvanger te weten komen  
Stap 3: mod(Me, m)  
Stap 4: ASCII naar tekst

### Ontcijferen

Stap 1: tekst naar ASCII  
Stap 2: d en m van ontvanger te weten komen  
Stap 3: mod(Md, m)  
Stap 4: ASCII naar tekst

### Definities en eigenschappen

Een getal groter dan 1 is een priemgetal als het alleen deelbaar is door zichzelf en door 1.  
  
Elk getal is op juist 1 manier te ontbinden in priemfactoren. Dat wil zeggen dat je elk getal op juist 1 manier kunt schrijven als het product van priemgetallen.

De grootste gemene deler van 2 getallen is het grootst getal dat een deler is van deze 2 getallen.

2 getallen zijn onderling ondeelbaar als de grootst gemene deler van deze 2 getallen 1 is.

### RSA methode

Stap 1: Ontvanger kiest 2 priemgetallen p en q  
Stap 2: Bereken m door m = p . q  
Stap 3: Bereken K door K = (p-1).(q-1)  
Stap 4: Kies een getal e waarbij   
 e < K  
 gcd(e, K) = 1  
Stap 5: Bereken d door {ggd, d, j}:= gcdext(e, K); ggd, d, j

### Elektronische handtekening

Stap 1: d en m van verzender te weten komen  
Stap 2: handtekenen door mod(Md, m)  
Stap 3: dehandtekenen door mod(Me, m)  
  
Wanneer er gehandtekend en geëncrypteerd moet worden, dan wordt er eerst gehandtekend en dan pas geëncrypteerd. De ontvanger moet eerst decypteren en dan pas dehandtekenen.

### Gebruikte functies

Strlen(tekst) geeft de lengte van een tekst  
substring(tekst, i, j) geeft een deel van de tekst beginnend op i tot en met j  
ascii(letter) geeft de ASCII-waarde van een letter  
char(x) geeft het karakter van een ASCII-waarde  
tekst1 | tekst2 plakt 2 string aan elkaar (1 string vormen)  
bitxor(x, y) XOR-operator op 2 gehele getallen x en y

Primes(n) geeft alle priemgetallen tot aan n  
isprime(n) geeft 1 als het een priemgetal is, 0 als het geen is  
mod(m, n) berekent m modulo n  
gcd(e, K) berekent de ggd van e en K  
gcdext(e, K) geeft meer info dan gcd zoals d en j  
factor(x) schrijft een getal x als een product van priemgetallen

&next\_prime(n) geeft het volgende priemgetal groter dan n  
&prev\_prime(n) geeft het vorige priemgetal kleiner dan n  
&mod(m, n) geeft m modulo n  
&gcd(e, K) berekent de ggd van e en K  
::factor(x) schrijft een getal x als een product van priemgetallen  
 Opgelet &factor(x) geeft als resultaat x!

# Lineaire Algebra

## Matrices

### Basisbegrippen en definities

Matrix:  
Een matrix is een geordend schema met m rijen en n kolommen, dit noemen we een m bij n matrix of m x n matrix.

Elementen:  
Elementen zijn getallen uit een matrix.

Gelijke matrices:  
Twee matrices worden gelijk genoemd als en slechts als alle overeenkomstige elementen gelijk zijn.

Kolommatrix:  
Een kolommatrix is een matrix met slechts 1 kolom.

Rijmatrix:  
Een rijmatrix is een matrix met slechts 1 rij.

Vierkante matrix:  
Een vierkante matrix is een matrix met evenveel rijen als kolommen.

Hoofddiagonaal:  
Bij een vierkante matrix wordt de hoofddiagonaal gevormd door de elementen a11, a22, a33, …, ann.

Diagonaalmatrix:  
Een diagonaalmatrix is een vierkante matrix waarbij alle elementen buitende de hoofddiagonaal 0 zijn.

Eenheidsmatrix:  
Een eenheidsmatrix is een diagonaalmatrix met alle elementen op de hoofddiagonaal gelijk aan 1.

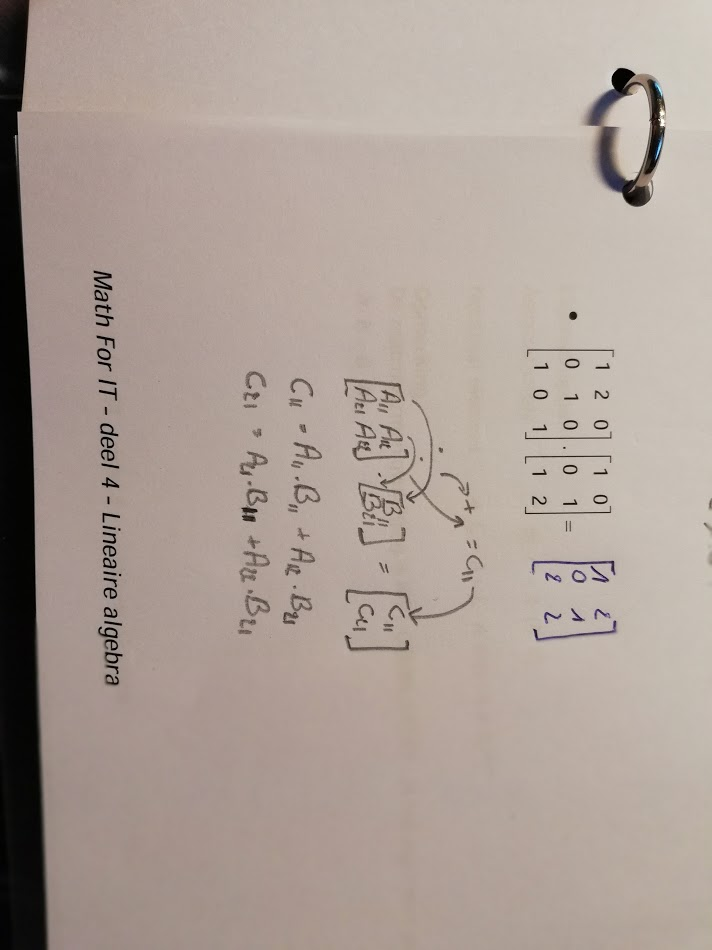
Nulmatrix:  
Een nulmatrix is een matrix waarvan alle elementen 0 zijn.

### Bewerkingen

Transponeren:  
De resulterende matrix wordt bekomen door de rijen en de kolommen met elkaar omwisselen (B -> BT).

Matrices optellen en aftrekken:  
De resulterende matrix wordt bekomen door de overeenkomstige elementen met elkaar op te tellen of af te trekken.

Scalaire vermenigvuldiging:  
De resulterende matrix wordt bekomen door het getal te vermenigvuldigen met elk element van de matrix.

Matrixvermenigvuldiging:  


Een matrixvermeningvuldiging is niet commutatief!

Machten van matrices:  
A² = A . A -> matrixvermenigvuldiging (Met EuMath -> matrixpower(A, 2))

### Eigenschappen

Commutativiteit A + B = B + A  
Associativiteit (A + B) + C = A + (B + C)  
Neutraal element A . I = A = I . A

### Matrixbewerking in Euler

|  |  |  |
| --- | --- | --- |
|  | Wiskunde | Euler |
| Dezelfde orde optellen | A + B | A + B |
| Dezelfde orde aftrekken | A – B | A – B |
| Elk element \* elk overeenkomstig element | Onbestaand | A \* B |
| Elk element / elk overeenkomstig element | Onbestaand | A / B |
| Matrixvermenigvuldiging | A . B | A . B |
| Elk element tot de macht | Onbestaand | A^n |
| Matrix tot de macht | An | Matrixpower(A, n) |
| Transponeren | AT | A’ |

## Toepassingen

### Overgangsmatrices

M stelt de overgangs- of migratiematrix voor. B stelt de beginmatrix of de beginsituatie voor.

De populatie na n periodes bereken: Mn . B (matrixpower gebruiken!)

Extra: Als de periode 2 jaar is en de populatie wordt om het jaar gevraagd, moet je de jaren 1, 3, 5, 7 … open laten of doorkruisen. Dit komt omdat deze niet berekenbaar zijn.

### Populatiematrices of Lesliematrices

Graaf wordt voorgesteld door alle generaties naast elkaar te schrijven. Onder de graaf komen de overlevingskansen in %. Boven de graaf komen de vruchtbaarheidscijfers in decimaal.

### Verbindingsmatrices

In een verbindingsmatrix (V) staan eenen en nullen. Een 1 geeft aan dat er een rechtstreekse verbinding is. Een nul geeft aan dat er geen rechtstreekse verbinding is.

In een directe-wegenmatrix (W) staan het aantal rechtstreekse wegen. W² zegt ons hoeveel wegen er zijn met 1 tussenstop. W + W² zegt ons hoeveel wegen er zijn met hoogstens 1 tussenstop.

### Codematrices

Stap 1: Elk getal wordt met een letter geassocieerd.  
Stap 2: Stel VIERKANTE coderingsmatric (C) op van zelfgekozen orde  
Stap 3: Zet boodschap op naar matrix (Z) (adhv stap 1)  
Stap 4: matrixvermenigvuldiging van C . Z = O  
Stap 5: Decoderen met inverse matrix van C (D of C-1) -> D . O = Z

### 2D-computergrafieken

#### Definities

Een vector is een punt in het vlak |R² met coördinaten (x, y). We representeren deze vector als kolommatrix .  
e1 is een eenheidsvector of het punt met coördinaten (1, 0).  
e2 is een eenheidsvector of het punt met coördinaten (0, 1).  
Een transformatie T beeldt elk punt van |R² af op een punt van |R².

#### Verschuiving

Een verschuiving of translatie is een speciaal geval van een transformatie.

#### Lineaire transformatie

Een lineaire transformatie is een speciaal geval van een transformatie.

#### Rotatie rond de oorsprong

Een rotatie is een speciaal geval van een lineaire transformatie.

#### Samenstelling van 2 transformaties

S o T : S komt na T -> eerst T uitvoeren, daarna S

#### Affiene transformatie

Een affiene transformatie is een speciaal geval van een transformatie.

#### Rotatie rond een punt verschillend van de oorsprong

Stap 1: verplaats rotatiepunt naar de oorsprong door een verschuiving  
Stap 2: doe een rotatie rond de oorsprong  
Stap 3: verplaats de oorsprong terug naar het oorspronkelijk rotatiepunt door een verschuiving

#### Spiegeling t.o.v. een willekeurige rechte

Hoek nemen van een rechte -> atan(a) -- In Euler -> deg(atan(a))

Stap 1: verplaats rotatiepunt naar de oorsprong door een verschuiving  
Stap 2: hoek bepalen en rotatie doen over rond de oorsprong  
Stap 3: spiegeling t.o.v. de x-as (door lineaire transformatie)  
Stap 4: rotatie over een hoek rond de oorsprong  
Stap 5: verplaats de oorsprong terug naar het oorspronkelijk rotatiepunt door een verschuiving

### 3D-computergrafieken

#### Affiene transformatie

## Stelsels van lineaire vergelijkingen

Uitrekenen in stappen, alleen doen als men de canonieke vorm vraagt. Anders in Euler met  
&solve([vgl1, vgl2, vgl3],[x, y, z])

Bij het uitschrijven van een verzameling duiden de ronde haken erop dat de volgorde van de elementen in die verzameling bepaald en belangrijk is.

Als er m voorwaarden op n onbekenden zijn -> mag men (n – m) onbekenden vrij kiezen.  
neem bv z=r en u=s  
Dan heeft het stelsel oplossingen.

Als we een vals stelsel krijgen, heeft de verzameling geen oplossingen of is deze leeg.

### Evenwichtsverdeling

M . E = E waarbij E de evenwichtstoestand is.

Bepalen of evenwicht gegarandeerd is:  
Voorwaarde 1: Zijn de kolomsommen (verticaal) = 1?  
Voorwaarde 2: Zijn alle elementen groter of gelijk aan 0?   
Voorwaarde 3: Bestaat er een macht van M zodat alle elementen groter zijn dan 0?

(Indien voorwaarde 3 niet voldaan -> M³ bereken en terug nakijken, als er tussen Mn en Mn+1 op dezelfde plaats 0’en staan, is voorwaarde 3 niet voldaan)

## Inverse van een matrix

### Definitie

Een nxn matrix A is inverteerbaar als er een nxn matrix B bestaat zodat A . B = B . A = I  
We zeggen dan dat B de inverse is van A en noteren dit als A-1.

Men kan dit berekenen door:

1. Matrix A nemen en de eenheidsmatrix erachter toevoegen.  
   De matrix herleiden naar zijn canonieke vorm.  
   Indien dit lukt, is het 2de deel van de matrix de inverse matrix van A.
2. Matrixpower(A, -1) of inv(A)