

Toepassingen van Algebra oplossingen oefeningen

Pieter-Jan Coenen

December 2016

Inhoudsopgave

| | | |
|----------|-----------------------|-----------|
| 1 | Oefenzitting 1 | 2 |
| 1.1 | Oefening 1 | 2 |
| 1.2 | Oefening 2 | 3 |
| 1.3 | Oefening 3 | 6 |
| 1.4 | Oefening 4 | 7 |
| 1.5 | Oefening 5 | 9 |
| | | |
| 2 | Oefenzitting 2 | 11 |
| 2.1 | Oefening 1 | 11 |
| 2.2 | Oefening 2 | 12 |
| 2.3 | Oefening 3 | 15 |
| 2.4 | Oefening 4 | 15 |
| 2.5 | Oefening 5 | 17 |
| 2.6 | Oefening 6 | 18 |

1 Oefenzitting 1

1.1 Oefening 1

Op \mathbb{R} definiëren we de samenstellingswet $a\tau b = a + b + a^2b^2$

- (a) Deze wet heeft een neutraal element. Welk?
- (b) Ze is niet associatief. Ga na!
- (c) Ze is commutatief. Waarom?

Oplossingsmethode

Ga al deze eigenschappen na voor de gegeven samenstellingswet. De eigenschappen kunnen worden gevonden in de cursus deel I blz 79.

Oplossing

- (a) Een snelle intuïtieve methode om dit op te lossen is door te testen of het neutraal element voor de optelling (0) of het neutraal element voor de vermenigvuldiging (1) een neutraal element is voor deze samenstellingswet.

We proberen eerst of het toepassen van de samenstellingswet op 0 en $x \in \mathbb{R}$ terug resulteert in x .

$$0\tau x = 0 + x + 0^2x^2 = x$$

$$x\tau 0 = x + 0 + x^20^2 = x$$

0 is dus het neutraal element.

Tweede manier om dit op te lossen is door de uitdrukking $e\tau x$ uit te werken en op zoek gaan naar een waarde van e zodat het $e\tau x = x$

$$\begin{aligned} e\tau x &= x \\ \Leftrightarrow e + x + e^2x^2 &= x \\ \Leftrightarrow e + e^2x^2 &= 0 \\ \Leftrightarrow e(1 + ex^2) &= 0 \\ \Leftrightarrow \begin{cases} e = 0 \\ e = \frac{-1}{x^2} \end{cases} \end{aligned}$$

Ook met deze methode is dus duidelijk dat 0 het neutraal element is.

- (b) Een samenstellingswet \top is associatief $\Leftrightarrow \forall x, y \in A : x \top (y \top z) = (x \top y) \top z$. (I blz 80).

We kunnen dus met een tegenvoorbeeld aantonen dat deze samenstellingswet niet associatief is.

Bijvoorbeeld:

$$1\tau(2\tau 3) = 1\tau(2 + 3 + 4 * 9) = 1\tau 41 = 1 + 41 + 1^2 41^2 = 1723$$

$$(1\tau 2)\tau 3 = (1 + 2 + 1 * 4)\tau 3 = 7\tau 3 = 7 + 3 + 7^2 3^2 = 451$$

- (c) \top is commutatief als $\Leftrightarrow \forall x, y \in A : x \top y = y \top x$ (I blz. 80).

Deze samenstellingswet maakt enkel gebruik van de operatoren "+" en "*". Aangezien dat deze beide commutatief zijn zal ook de samenstellingswet commutatief zijn.

$$\forall x, y \in \mathbb{R} : x\tau y = x + y + x^2 y^2 = y + x + y^2 x^2 = y\tau x$$

1.2 Oefening 2

Bewijs dat in $\mathbb{R}^2 \times \mathbb{R}^2$ volgende relaties equivalentierelaties zijn:

$$G = \{((a, b), (c, d)) | a^2 + b^2 = c^2 + d^2\}$$

$$H = \{((a, b), (c, d)) | b - a = d - c\}$$

$$J = \{((a, b), (c, d)) | a + b = c + d\}$$

Welke zijn de partities die hierdoor gedefinieerd worden? Welke partitie definieert $H \cap J$?

Oplossingsmethode

Een relatie $R \subseteq A \times A$ is een equivalentierelatie (I blz.58) \Leftrightarrow

1. R is reflexief \Leftrightarrow elk element staat in relatie met zichzelf (I blz 59) :

$$\forall x \in A : (x, x) \in R \text{ of } \forall x \in A : xRx$$

Voorbeeld hiervan is de "equals-relatie" elk element is gelijk aan zichzelf $x = x$.

2. R is symmetrisch \Leftrightarrow de relatie in twee richtingen geldt (I blz 59) :

$$(x, y) \in R \Rightarrow (y, x) \in R \text{ of } xRy \Rightarrow yRx$$

De "equals-relatie" is bijvoorbeeld symmetrisch want als $x = y \Rightarrow y = x$. De kleiner dan relatie is bijvoorbeeld niet symmetrisch wat als $x < y \nRightarrow y < x$.

3. R is transitief \Leftrightarrow de relatie kan doorgegeven worden (erfelijk is). (I blz 60) :

$$(x, y) \in R \text{ en } (y, z) \in R \Rightarrow (x, z) \in R \text{ of } xRy \text{ en } yRz \Rightarrow xRz$$

De kleiner dan relatie is bijvoorbeeld transitief want als $x < y$ en $y < z \Rightarrow x < z$.

Oplossing voor G

1. G is reflexief want

$$\forall (x, y) \in \mathbb{R}^2 \Rightarrow x^2 + y^2 = x^2 + y^2$$

dus geldt dat

$$\forall (x, y) \in \mathbb{R}^2 : (x, y)G(x, y)$$

2. G is symmetrisch want

$$\forall (x, y), (z, q) \in \mathbb{R}^2 : x^2 + y^2 = z^2 + q^2 \Rightarrow z^2 + q^2 = x^2 + y^2$$

dus geldt dat

$$(x, y)G(z, q) \Rightarrow (z, q)G(x, y)$$

3. G is transitief want

$$\forall (x, y), (z, q), (v, w) \in \mathbb{R}^2 : (x^2 + y^2 = z^2 + q^2 \ \& \ z^2 + q^2 = v^2 + w^2) \Rightarrow x^2 + y^2 = v^2 + w^2$$

dus geldt dat

$$(x, y)G(z, q) \ \& \ (z, q)G(v, w) \Rightarrow (x, y)G(v, w)$$

Elke equivalentie relatie definieert een partitie (stelling 9.1 deel I blz 62). Aangezien dat aan alle voorwaarden is voldaan, is G een equivalentierelatie.

Oplossing voor H

1. H is reflexief want

$$\forall (x, y) \in \mathbb{R}^2 \Rightarrow y - x = y - x$$

dus geldt dat

$$\forall (x, y) \in \mathbb{R}^2 : (x, y)H(x, y)$$

2. H is symmetrisch want

$$\forall (x, y), (z, q) \in \mathbb{R}^2 : y - x = q - z \Rightarrow q - z = y - x$$

dus geldt dat

$$(x, y)H(z, q) \Rightarrow (z, q)H(x, y)$$

3. H is transitief want

$$\forall (x, y), (z, q), (v, w) \in \mathbb{R}^2 : (y-x = q-z \ \& \ q-z = w-v) \Rightarrow y-x = w-v$$

dus geldt dat

$$(x, y)H(z, q) \ \& \ (z, q)H(v, w) \Rightarrow (x, y)H(v, w)$$

Aangezien dat aan alle voorwaarden is voldaan, is H een equivalentierelatie.

Oplossing voor J

1. J is reflexief want

$$\forall (x, y) \in \mathbb{R}^2 \Rightarrow x + y = x + y$$

dus geldt dat

$$\forall (x, y) \in \mathbb{R}^2 : (x, y)J(x, y)$$

2. J is symmetrisch want

$$\forall (x, y), (z, q) \in \mathbb{R}^2 : x + y = z + q \Rightarrow q + z = x + y$$

dus geldt dat

$$(x, y)J(z, q) \Rightarrow (z, q)J(x, y)$$

3. J is transitief want

$$\forall (x, y), (z, q), (v, w) \in \mathbb{R}^2 : (x+y = z+q \ \& \ z+q = v+w) \Rightarrow x+y = v+w$$

dus geldt dat

$$(x, y)J(z, q) \ \& \ (z, q)J(v, w) \Rightarrow (x, y)J(v, w)$$

Aangezien dat aan alle voorwaarden is voldaan, is J een equivalentierelatie.

Oplossing bijvragen

Aangezien G , H en J alle drie equivalentierelaties zijn definiëren ze ook alle drie een partitie (zie stelling 9.1 deel I blz 62).

$H \cap J$ zijn dus alle koppels uit \mathbb{R}^2 die behoren tot zowel H als J .
Dit geeft de volgende formele beschrijving:

$$H \cap J = \{((a, b), (c, d)) | b - a = d - c \ \& \ a + b = c + d\}$$

We kunnen dit verder uitwerken door dit in een stelsel te gieten:

$$\begin{cases} b - a = d - c \\ a + b = c + d \end{cases}$$

Als we dit stelsel verder uitwerken krijgen we:

$$\begin{cases} b - a = d - c \\ a + b = c + d \end{cases} = \begin{cases} 2b = 2d \\ a + b = c + d \end{cases} = \begin{cases} b = d \\ a = c \end{cases}$$

Nu kunnen we $H \cap J$ schrijven als:

$$\begin{aligned} H \cap J &= \{((a, b), (c, d)) | a = c \text{ \& } b = d\} \\ &= \{(x, y) | x \in \mathbb{R}^2, y \in \mathbb{R}^2, x = y\} \\ &= \{(x, x) | x \in \mathbb{R}^2\} \end{aligned}$$

1.3 Oefening 3

Los het volgende stelsel op in (mod 7):

$$\begin{cases} 3x_1 - 2x_2 + 6x_3 = 4 \\ 4x_1 - x_2 + x_3 = 0 \\ 2x_1 - x_2 + 2x_3 = -1 \end{cases}$$

Oplossingsmethode

Zie volledig uitgewerkt voorbeeld in deel I blz. 85.

Je kan beter geen deling gebruiken, want in sommige omstandigheden zorgt dit voor fouten. In plaats van een getal x dus te delen door x om een 1 te bekomen moet je opzoek gaan naar een getal y zodat $x * y = 1$.

Bijvoorbeeld in modulo 5, om van 2 naar 1 te gaan doe je $2 * 3 = 6 \text{ mod } 5 = 1$.

Let op als je een gelijkaardige opgave krijgt met (mod k) waarbij k geen priemgetal is, meer info zie blz 86 voorbeeld 14.5.

Oplossing

We zetten dit stelsel eerst om naar een matrix

$$\left[\begin{array}{ccc|c} 3 & -2 & 6 & 4 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array} \right] \xrightarrow{R_1=R_1*5} \left[\begin{array}{ccc|c} 15 & -10 & 30 & 20 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array} \right]$$

$$\begin{array}{ccc}
\frac{R_1=R_1 \bmod 7}{\rightarrow} & \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array} \right] & \begin{array}{c} \frac{R_2=R_2-4*R_1}{\rightarrow} \\ \frac{R_3=R_3-2*R_1}{\rightarrow} \end{array} & \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & -15 & -7 & -24 \\ 0 & -7 & -2 & -13 \end{array} \right] \\
\\
\frac{R_2=R_2 \bmod 7}{\rightarrow} & \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & 6 & 0 & 4 \\ 0 & 0 & 5 & 1 \end{array} \right] & \begin{array}{c} \frac{R_2=R_2*6 \pmod{7}}{\rightarrow} \\ \frac{R_3=R_3*3 \pmod{7}}{\rightarrow} \end{array} & \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 3 \end{array} \right]
\end{array}$$

Dit resulteert in

$$\begin{cases} x_1 + 4x_2 + 2x_3 = 6 \\ x_2 = 3 \\ x_3 = 3 \end{cases} \rightarrow \begin{cases} x_1 + 18 \pmod{7} = x_1 + 4 = 6 \\ x_2 = 3 \\ x_3 = 3 \end{cases} \rightarrow \begin{cases} x_1 = 2 \\ x_2 = 3 \\ x_3 = 3 \end{cases}$$

1.4 Oefening 4

Bepaal de isometrieën van een gelijkzijdige driehoek. Stel voor deze isometrieën de bewerkingstabel op, onder de samenstellingswet \circ .

Oplossingsmethode

Volledig uitgewerkt voorbeeld is te vinden in de cursus deel I op blz 94-95.

Als alle n zijden dezelfde lengte hebben, dan geldt dat het aantal isometrieën gelijk is aan $2n$.

Oplossing

Bij een gelijkzijdige driehoek hebben we dus $3 * 2 = 6$ isometrieën.

1. e : de identieke afbeelding

$$\begin{array}{c} 1 \\ \triangle \\ 2 \quad 3 \end{array} \rightarrow \begin{array}{c} 1 \\ \triangle \\ 2 \quad 3 \end{array}$$

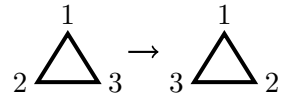
2. r_1 : rotatie om het middelpunt over 90° in wijzerzin

$$\begin{array}{c} 1 \\ \triangle \\ 2 \quad 3 \end{array} \rightarrow \begin{array}{c} 2 \\ \triangle \\ 3 \quad 1 \end{array}$$

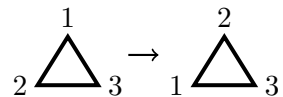
3. r_2 : rotatie om het middelpunt over 180° in wijzerzin

$$\begin{array}{c} 1 \\ \triangle \\ 2 \quad 3 \end{array} \rightarrow \begin{array}{c} 3 \\ \triangle \\ 1 \quad 2 \end{array}$$

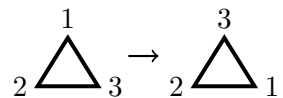
4. m_1 : spiegeling in de middellijn door bovenste hoekpunt



5. m_2 : spiegeling in de diagonaal door hoekpunt rechtsonder



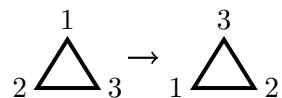
6. m_3 : spiegeling in de diagonaal door hoekpunt linksonder



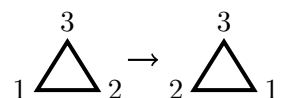
Dit geeft ons de volgende bewerkingstabel:

| \circ | e | r_1 | r_2 | m_1 | m_2 | m_3 |
|---------|-------|-------|-------|-------|-------|-------|
| e | e | r_1 | r_2 | m_1 | m_2 | m_3 |
| r_1 | r_1 | r_2 | e | m_3 | m_1 | m_2 |
| r_2 | r_2 | e | r_1 | m_2 | m_3 | m_1 |
| m_1 | m_1 | m_2 | m_3 | e | r_1 | r_2 |
| m_2 | m_2 | m_3 | m_1 | r_2 | e | r_1 |
| m_3 | m_3 | m_1 | m_2 | r_1 | r_2 | e |

m_3 wordt bijvoorbeeld bekomen door eerst r_2 toe te passen



op dit resultaat passen we nu m_1 toe



Het toepassen van " $m_1 \circ r_2$ " is dus hetzelfde als het toepassen van m_3 .

De verkregen tabel is duidelijk niet symmetrisch, dit betekend dat niet alle samenstellingen commutatief zijn en dus dat \circ niet commutatief is.

1.5 Oefening 5

Een latijns vierkant is een $n \times n$ tabel waarin slechts n verschillende elementen voorkomen.

In elke rij en elke kolom komt namelijk elk element juist eenmaal voor.

- (a) Bewijs dat de bewerkingstabel voor een eindige groep steeds een Latijns vierkant is.
- (b) Is dit ook een voldoende voorwaarde om een groep te hebben? Bepaal of volgend Latijns vierkant de bewerkingstabel van een groep is:

| τ | a | b | c | d | e | f |
|--------|---|---|---|---|---|---|
| a | c | e | a | b | f | d |
| b | f | c | b | a | d | e |
| c | a | b | c | d | e | f |
| d | e | a | d | f | c | b |
| e | d | f | e | c | b | a |
| f | b | d | f | e | a | c |

Oplossingsmethode

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep als :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

Oplossing

- (a) Een groep is overal bepaald, dus de tabel is volledig ingevuld.

Nu bewijzen we dat elk element maar één keer voorkomt op elke rij. Dit doen we door te veronderstellen dat een element twee keer voorkomt op één rij en zo een contradictie te bekomen.

Bewijs. Een element komt twee keer voor op één rij als er een rij bestaat met rij element a en er twee verschillende kolommen bestaan met elementen x en y waarbij x en y verschillend zijn zodat $a\tau x = a\tau y$

Nu vinden we :

$$\begin{aligned}
a\tau x &= a\tau y \\
\Leftrightarrow a^{-1}\tau(a\tau x) &= a^{-1}\tau(a\tau y) \\
\Leftrightarrow (a^{-1}\tau a)\tau x &= (a^{-1}\tau a)\tau y \\
\Leftrightarrow e\tau x &= e\tau y \\
\Leftrightarrow x &= y
\end{aligned}$$

Aangezien dat x verschillend is van y kan dit dus niet en hebben we een contradictie. \square

Merk op dat we in het bovenstaande bewijs gebruik maken van het feit dat een groep associatief en symmetrisch is en neutraal element heeft.

Om te bewijzen dat er geen element twee keer voorkomt in een kolom is het bewijs analoog.

(b) We kijken of deze tabel voldoet aan alle eigenschappen van een groep:

- Deze bewerking is duidelijk overal bepaald, want de tabel is volledig ingevuld.
- Associativiteit is niet zo heel eenvoudig om na te kijken. Daarom proberen we dit systematisch rij per rij te doen.
We gaan altijd $x\tau(y\tau[a, b, c, d, e, f])$ berekenen en kijken of dit gelijk is aan $(x\tau y)\tau[a, b, c, d, e, f]$.
Op die manier vinden we het volgende tegenvoorbeeld:
 $a\tau(b\tau b) = a$ en $(a\tau b)\tau b = f$

- Om het neutraal element te zoeken in deze tabel zijn we dus opzoek naar een rij en kolom waar elk element op zichzelf wordt afgebeeld.
Het is duidelijk dat voor "c" elk element op zichzelf wordt afgebeeld. "c" is dus het neutraal element.
- Deze bewerking is duidelijk symmetriseerbaar want voor elk element kunnen we een symmetrisch element vinden.
"a", "b", "c" en "f" zijn zelf het symmetrisch element voor zichzelf. Want bijvoorbeeld $b\tau b = b\tau b = c$, dit klopt want "c" is het neutraal element.
Het symmetrisch element voor "d" is "e" en het symmetrisch element voor "e" is dus "d" want $d\tau e = e\tau d = c$.

Het Latijns vierkant kan dus geen bewerkingstabel zijn van een groep, want het is niet associatief.

2 Oefenzitting 2

2.1 Oefening 1

Bewijs dat $\mathbb{R}_0 \times \mathbb{R}$ voorzien van de samenstellingswet $((a, b), (c, d)) \mapsto (ac, bc + d)$ een groep is. Is hij abels?

Oplossingsmethode

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep als :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

Als $*$ commutatief is, dan is de groep abels.

Oplossing

- $*$ is overal bepaald in \mathbb{R}_0 , dus $ac \in \mathbb{R}_0$
 $*$ en $+$ zijn ook overal bepaald in \mathbb{R} , dus $bc + d \in \mathbb{R}$.

De bewerking is dus overal bepaald.

- Associatief want

$$((x, y), ((i, j), (u, v))) = ((x, y), (iu, ju + v)) = (xiu, yiu + ju + v)$$

en

$$(((x, y), (i, j)), (u, v)) = ((xi, yi + j), (u, v)) = (xiu, yiu + ju + v)$$

- Voor het neutraal element (e_1, e_2) moet gelden dat :

$$\begin{cases} ((x, y), (e_1, e_2)) = (x, y) \\ ((e_1, e_2), (x, y)) = (x, y) \end{cases}$$

Dus moet gelden dat

$$\begin{cases} ((x, y), (e_1, e_2)) = (xe_1, ye_1 + e_2) = (x, y) \\ ((e_1, e_2), (x, y)) = (e_1x, e_2x + y) = (x, y) \end{cases}$$

$$= \begin{cases} xe_1 = x \\ e_1x = x \\ ye_1 + e_2 = y \\ e_2x + y = y \end{cases}$$

Dus dan zal

$$\begin{cases} e_1 = 1 \\ e_2 = 0 \end{cases}$$

$(1, 0)$ is dus het neutraal element.

- Symmetriseerbaarheid:

$$\begin{aligned} ((x, y), (x^{-1}, y^{-1})) = (1, 0) &\Leftrightarrow \begin{cases} xx^{-1} = 1 \\ yx^{-1} + y^{-1} = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} x^{-1} = \frac{1}{x} \\ y^{-1} = -\frac{y}{x} \end{cases} \end{aligned}$$

Het symmetrisch element voor (x, y) is dus $(\frac{1}{x}, -\frac{y}{x})$

Aangezien dat aan alle eigenschappen van een groep zijn voldaan, is dit dus duidelijk een groep.

Een groep is abels als de bewerking commutatief is, we testen dit even uit:

$$((x, y), (v, w)) = (xv, yv + w)$$

$$((v, w), (x, y)) = (vx, wx + y)$$

Het is duidelijk dat de bovenstaande bewerkingen niet aan elkaar gelijk zijn en de groep dus niet commutatief (of abels) is.

2.2 Oefening 2

$\langle S_n, \circ \rangle$ is de groep van permutaties van een verzameling van n elementen. Stel de samenstellingstabel op voor $\langle S_3, \circ \rangle$. Zijn er deelgroepen? Normaal-dealers?

Oplossingsmethode

Voorbeelden voor het opstellen van een bewerkingstabel kan je vinden in deel I blz. 94-95.

In oefenzitting 1 is oefening 4 gelijkaardig.

De elementen van een deelgroep zijn een deelverzameling van de elementen van een groep en de deelgroep voldoet aan alle eigenschappen van een groep. Zie definitie 2.1 deel I blz 93 en stelling 2.1 deel I blz 94.

Een groep S , die een deelgroep is van G is een normaaldeler van $G \Leftrightarrow$

$$\forall g \in G : g^{-1}Sg = S$$

of

$$\forall x \in G : Sx = xS \quad \text{met } xS = \{x\tau s | s \in S\}$$

Zie definitie 4.2 en stelling 4.2 deel I blz 105. Voorbeeld zie voorbeeld 4.1 blz 107.

Oplossing

Voor een rij van 3 elementen zijn er $3! = 6$ permutaties mogelijk. We zoeken eerst deze permutaties.

1. e : de identieke afbeelding

$$[1, 2, 3] \rightarrow [1, 2, 3]$$

2. r_1 : we schuiven alle elementen één positie naar rechts

$$[1, 2, 3] \rightarrow [3, 1, 2]$$

3. r_2 : we schuiven alle elementen twee posities naar rechts

$$[1, 2, 3] \rightarrow [2, 3, 1]$$

4. m_1 : verwissel het laatste en eerste element

$$[1, 2, 3] \rightarrow [3, 2, 1]$$

5. m_2 : verwissel de eerste twee elementen

$$[1, 2, 3] \rightarrow [2, 1, 3]$$

6. m_3 :verwissel de laatste twee elementen

$$[1, 2, 3] \rightarrow [1, 3, 2]$$

Dit geeft ons de volgende samenstellingstabel:

| \circ | e | r_1 | r_2 | m_1 | m_2 | m_3 |
|---------|-------|-------|-------|-------|-------|-------|
| e | e | r_1 | r_2 | m_1 | m_2 | m_3 |
| r_1 | r_1 | r_2 | e | m_3 | m_1 | m_2 |
| r_2 | r_2 | e | r_1 | m_2 | m_3 | m_1 |
| m_1 | m_1 | m_2 | m_3 | e | r_1 | r_2 |
| m_2 | m_2 | m_3 | m_1 | r_2 | e | r_1 |
| m_3 | m_3 | m_1 | m_2 | r_1 | r_2 | e |

Aangezien dat een deelgroep zelf ook een groep is, moet deze dus altijd het neutraal element van de groep bevatten. Daarnaast moet de deelgroep ook overal bepaald zijn. Als de groep associatief is dan is de deelgroep dat normaal gezien ook.

We hebben sowieso de triviale deelgroep die enkel het neutraal element bevat en de triviale deelgroep die de volledige groep bevat.

We zien nu in de tabel dat er één niet-triviale deelgroep is, dit is de deelgroep die enkel de rotaties bevat $R = \{e, r_1, r_2\}$.

Tot slot vinden we ook nog de volgende deelgroepen: $M_1 = \{e, m_1\}$, $M_2 = \{e, m_2\}$, $M_3 = \{e, m_3\}$.

Merk op dat $\{e, r_1\}$ bijvoorbeeld geen deelgroep is want $r_1 \circ r_1 = r_2$ en r_2 behoort niet tot die deelgroep.

We moeten nu enkel nog de normaal delers zoeken. We kijken eerst na of de deelgroep van de rotaties R een normaaldeeler is. Dit doen we door te kijken of elke linker nevenklassen ook een rechter nevenklassen is (zie oplossingsmethode).

$$Re = R = eR$$

$$Rr_1 = \{e, r_1, r_2\} = r_1R$$

$$Rr_2 = \{e, r_1, r_2\} = r_2R$$

$$Rm_1 = \{m_1, m_2, m_3\} = m_1R$$

$$Rm_2 = \{m_1, m_2, m_3\} = m_2R$$

$$Rm_3 = \{m_1, m_2, m_3\} = m_3R$$

R is dus een normaaldeeler van G .

Ook de twee triviale deelgroepen zijn uiteraard nevenklassen.

M_1, M_2, M_3 zijn geen nevenklassen.

M_1 is bijvoorbeeld geen nevenklassen want:

$$M_1r_1 = \{r_1, m_2\} \neq \{r_1, m_3\} = r_1M_1$$

2.3 Oefening 3

Zoek de generatoren van de additieve cyclische groepen $\mathbb{Z}_{10}, \mathbb{Z}_{11}, \mathbb{Z}_{12}$

Oplossingsmethode

Voor een additieve groep, zoek je een element g zodat

$$\forall n \in \mathbb{N}_0 : \quad 0 * g = e, \quad 1 * g = g, \quad 2 * g = g + g, \quad \dots, \quad n * g = g + g + \dots + g$$

Waarbij g dus alle elementen van die groep kan genereren (en ook geen andere) dus $\forall n \in \mathbb{N}_0$ is $n * g$ een element van die groep.

Voor een additieve groep \mathbb{Z}_x zijn alle getallen y die geen delers gemeenschappelijk hebben met x generatoren voor \mathbb{Z}_x .

Zie definitie 2.5 deel I blz 97, definitie 1.3 en voorbeeld 1.5 blz 93.

Oplossing

\mathbb{Z}_{10} bevat de elementen $\{0, \dots, 9\}$ en de generatoren zijn dus $\{1, 3, 7, 9\}$

\mathbb{Z}_{11} bevat de elementen $\{0, \dots, 10\}$ en de generatoren zijn dus $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

\mathbb{Z}_{12} bevat de elementen $\{0, \dots, 11\}$ en de generatoren zijn dus $\{1, 5, 7, 11\}$

2.4 Oefening 4

Genereer de groep voortgebracht onder vermenigvuldiging door de matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ en } B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Bewijs dat die een niet-abelse groep is van orde 8.

Oplossingsmethode

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep asa :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

Het aantal elementen van een groep is de orde van de groep. De groep is niet-abels als de bewerking niet commutatief is.

De definitie van een multiplicatieve generator vind je in deel I blz. 97.

Oplossing

Zowel A als B zijn diagonaalmatrices, het vermenigvuldigen van twee diagonaal matrices resulteert opnieuw in een diagonaal matrix.

Het vermenigvuldigen van A en B zal dus steeds resulteren in een matrix van de vorm

$$\begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix} \text{ of } \begin{bmatrix} 0 & x_1 \\ x_2 & 0 \end{bmatrix}$$

Waarbij $x_1 = \pm 1$ en $x_2 = \pm 1$.

Hieruit kunnen we dus berekenen dat er in totaal 8 combinaties mogelijk zijn.

We genereren eerst alle elementen met de matrix A .

$$A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad A^1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Aangezien dat A^4 terug gelijk is aan de eenheidsmatrix en we deze al zijn tegen gekomen tijdens de generatie met A stoppen we bij A^3 .

Nu genereren we alle elementen met de matrix B .

$$B^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad B^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Nu genereren we ook nog de combinaties van A en B .

$$A^1 * B^1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^2 * B^1 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad A^2 * B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^3 * B^1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Nu hebben we dus 8 unieke elementen voor onze groep, namelijk:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Nu moeten we nog bewijzen dat deze elementen samen een groep vormen:

- Deze bewerking is duidelijk overal bepaald we hebben alle combinaties van diagonaal matrices met ± 1 als elementen. Deze met elkaar vermenigvuldigen levert terug een diagonaal matrix op van hetzelfde type.

- Het vermenigvuldigen van matrices is associatief
- Deze verzameling bevat het neutraal element voor vermenigvuldiging van matrices, nl. de eenheidsmatrix.
- Elk element kan ook worden gesymmetriseerd.

We kunnen dus spreken over een groep, aangezien deze 8 elementen bevat is de orde van de groep ook 8.

De vermenigvuldiging van matrices is niet commutatief, dus deze groep is niet abels.

2.5 Oefening 5

Beschouw een groep $G = (\mathbb{Z}_7/\{0\}, \cdot)$ van de gehele getallen modulo 7 zonder nul en met de vermenigvuldiging modulo 7. Bepaal de orde van al de elementen. Is de groep commutatief?

Oplossingsmethode

De orde van een element x is het kleinste natuurlijke getal r waarvoor $x^r = e$ met e het neutraal element. Zie def 2.5 deel I blz 97.

Oplossing

De verzameling G bevat de elementen $\{1, 2, 3, 4, 5, 6\}$, waarbij 1 het neutraal element is.

We gaan nu voor elk element apart zijn orde na.

1. De orde van 1 is 1 want $1^1 = 1$
2. De orde van 2 is 3 want $2^3 = 1$
3. De orde van 3 is 6 want $(3^2)^3 = 2^3 = 1$
4. De orde van 4 is 3 want $4^3 = 1$
5. De orde van 5 is 6 want $(5^2)^3 = 4^3 = 1$
6. De orde van 6 is 2 want $6^2 = 1$

De groep is commutatief want de vermenigvuldiging is commutatief.

2.6 Oefening 6

Bewijs dat elke deelgroep van een cyclische groep cyclisch is.

Oplossingsmethode

Definitie van een cyclische groep zie def. 2.5 deel I blz 97.

Oplossing

Opgelet, dit bewijs is niet correct/volledig.

Bewijs. Als G een cyclische groep is dan bestaat er een generator g zodat $G = \{g^0, g^1, g^2, \dots\}$

Als H een deelgroep is van G dan bevat H dus minstens één element $g^k \in G$. Aangezien dat H een groep is moet H ook $\forall i \in \mathbb{N} : (g^k)^i$ bevatten, want een groep is overal bepaald.

g^k is dus een generator voor H en H is dus een cyclische groep.

□