Inlever opdracht 4

Luc Veldhuis

17 april 2017

1. Gegeven is dat

$$G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ met } a = \pm 1 \text{ en } b \in \mathbb{Z}\}$$

een ondergroep is van $GL_2(\mathbb{Q})$, de matrixgroep van inverteerbare 2×2 matrices met rationele coëfficiënten.
Vind elementen x en y in G zo dat $G = \langle x, y \rangle$. *Aanwijzing: laat eerst zien dat* $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ met $b \in \mathbb{Z}\}$ *een cyklische groep is.*
Een groep H is cyklish als geldt dat het gegenereerd kan worden door slechts 1 element. Er is een element $x \in H$, zodat $H = \{x^n | n \in \mathbb{Z}\}$.
Claim: $W = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ met $b \in \mathbb{Z}\}$ is een cyklische groep.
We moeten eerst laten zien dat W een ondergroep is van G onder multiplicatie.
De verzameling W is ondergroep als geldt dat:

- $W \neq \emptyset$
  Klopt, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in W$
- $\forall x \in W$ geldt dat $x^{-1} \in W$
  Klopt, kies een willekeurige $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in W$, dan bestaat er ook een $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in W$, omdat $b, -b \in \mathbb{Z}$, zodat $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b-b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$, dus $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1}$
- $\forall x, y \in W$ geldt dat $xy \in W$
  Klopt, kies $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in W$, met $b, c \in \mathbb{Z}$.
  Dan is $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+c \\ 0 & 1 \end{pmatrix} \in W$, omdat $b + c \in \mathbb{Z}$

W voldoet hieraan, dus is het een ondergroep van G.
Claim: W is ook cyklisch.
We zijn nu opzoek naar een element in $x \in W$ zodat $W = \{x^n | n \in \mathbb{Z}\}$
Kies nu $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in W$
Gebruik nu inductie om te laten zien dat $x^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Basis stap: $x^0 = e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Dus het klopt voor $n = 0$

Inductie hypothese: $x^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Bewijs: $x^{n+1} = x^n x =^{IH} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$

Dus nu hebben we laten zien dat $\{x^n | n \in \mathbb{N} \cup \{0\}\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{N} \cup \{0\}\}$

Nu moeten we dit ook nog laten zien voor het geval als $n < 0$.

Gebruik weer inductie om te laten zien dat $x^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$:

Basisstap: $x^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ want $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$. Dus het klopt voor $n = -1$

Inductie hypothese: $x^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$

Bewijs: $x^{-n-1} = x^{-n} x^{-1} =^{IH} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n-1 \\ 0 & 1 \end{pmatrix}$

Dus nu hebben we laten zien dat voor alle $n \in \mathbb{Z}$ geldt dat $\{x^n | n \in \mathbb{Z}\} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{Z}\} = W$

Dus W is cyklisch.

Nu moeten we nog elementen $x, y \in G$ vinden zodat $G = \langle x, y \rangle$

Kies als $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en als $y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

We hebben al bewezen dat $\langle x \rangle$ een cyklische ondergroep van G is.

Per definitie geldt ook dat $\langle x \rangle \subseteq \langle x, y \rangle \subseteq G$.

De elementen die wel in G zitten, maar niet in $\langle x \rangle$, zijn de elementen van de vorm: $\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ met $b \in \mathbb{Z}$.

We hebben $y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Dus als we een element in de vorm $\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ willen hebben, kunnen we deze construeren door $yx^{-b} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ met $x^{-b} \in \langle x \rangle \subseteq \langle x, y \rangle$ en $y \in \langle x, y \rangle$, dus per definitie van een groep $yx^{-b} \in \langle x, y \rangle$

Dus alle elementen van de vorm $\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{Z}, a = \pm 1\} \subseteq \langle x, y \rangle \subseteq G$

Maar $G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{Z}, a = \pm 1\}$

Dus $G = \langle x, y \rangle$ voor $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en $y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

2. Zij $n \geq 3$ en $G = D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$, de diëder groep met $2n$ elementen.
We schrijven $R = \langle r \rangle$ voor de ondergorpen die bestaat uit alle rotaties.

   (a) Laat zien dat als M een ondergroep is van R en x is in $G \setminus R$, dan is de vereniging $M \cup xM$ een ondergroep van G.
   Hierbij is $xM = \{xm \text{ met } m \in M\}$
   Een set H is een ondergroep van de groep G dan en slechts dan als $H \neq \emptyset$ en als $\forall x, y \in H$

geldt dat $x^{-1} \in H$ en $xy \in H$.
Een groep F heet cyclisch dan en slechts dan als het gegenereerd kan worden door slechts 1 element. In andere woorden: er is een element $x \in F$ zodat $F = \{x^n | n \in \mathbb{Z}\}$
Er is gegeven dat M een ondergroep is van R. Dus M bestaat alleen uit rotaties.
Ook is gegeven dat x zit in $G \setminus R$, dus x heeft de volgende vorm: $x = sr^i$ met $0 \leq i \leq n-1$.
Dan heeft de verzameling xM de volgende vorm: $xM = \{sr^i r^j | r^j \in M\}$ voor een vaste $0 \leq i \leq n-1$.
Nu moeten we laten zien dat $M \cup xM$ een ondergroep is van G.
Omdat M een ondergroep is van R, en per definitie dus niet gelijk is aan de lege verzameling, is de vereniging van $M \cup xM$ ook ongelijk aan de lege verzameling.
Kies nu 2 elementen $y, z \in M \cup xM$.
Onderscheid nu 4 gevallen:

- $y = r^k$, $z = r^m$
  Omdat we weten dat alle elementen in de verzameling xM de vorm hebben volgens sr^p met $0 \leq p \leq n-1$, moeten deze elementen wel uit M komen. Dit is per definitie al een ondergroep. Dus er geldt nu zeker dat $y^{-1}z \in M \cup xM$.
- $y = r^k$, $z = sr^m$
  We moeten nu kijken of $y^{-1} \in M \cup xM$ en $yz \in M \cup xM$.
  Omdat y de vorm r^p heeft met $0 \leq p \leq n-1$, moet dit element wel uit M komen. Omdat M een ondergroep is, weten we dat $y^{-1} \in M$. Dus aan de eerste eis is voldaan.
  Nu moeten we nog aantonen dat $r^k sr^m \in M \cup xM$.
  We weten dat voor de elementen in xM geldt dat deze de vorm hebben van $sr^i r^j = sr^{i+j}$ voor een vaste $0 \leq i \leq n-1$ en met $r^j \in M$.
  Dit kunnen we gebruiken om yz op een andere manier op te schrijven.
  Ook gebruiken we het feit dat in diëder groepen de volgende vergelijking geldt: $sr^t = r^{-t}s$ en het feit dat $r^k \in M$ en $sr^m \in xM$.
  $r^k sr^m = sr^{-k}r^m = sr^{-k}r^{i+t} = sr^{-k+i+t} = sr^{i+(t-k)} = sr^i r^{t-k}$
  Hierbij is i vast gekozen toen x werd gekozen.
  Omdat $sr^m = sr^{i+t} \in xM$, weten we dat er een $r^t \in M$.
  Omdat M een ondergroep is, weten we dat voor elk element $r^k \in M$, ook de inverse, $(r^k)^{-1} = r^{-k} \in M$. Ook weten we dat voor elk tweetal elementen $r^t, r^{-k} \in M$ geldt dat $r^t r^{-k} = r^{t-k} \in M$
  Dus $sr^i r^{t-k} = xr^{t-k} \in xM$, omdat $r^{t-k} \in M$. Dus $yz \in M \cup xM$
- $y = sr^k$, $z = r^m$
  We moeten nu kijken of $y^{-1} \in M \cup xM$ en $yz \in M \cup xM$
  $y^{-1} = (sr^k)^{-1} = sr^k = y \in M \cup xM$, omdat $y \in M \cup xM$
  Nu moeten we nog laten zien dat $yz \in M \cup xM$
  $yz = sr^k r^m = sr^{i+t}r^m = sr^{i+t+m} = sr^i r^{t+m} = xr^{t+m}$.
  Omdat $sr^k = xr^t \in xM$, moet $r^t \in M$.
  Omdat we weten dat voor elk tweetal elementen $r^t, r^m \in M$ geldt dat $r^t r^m = r^{t+m} \in M$, dus geldt dat $xr^{t+m} \in xM$.
  Dus $yz \in M \cup xM$
- $y = sr^k$, $z = sr^m$
  We moeten nu kijken of $y^{-1} \in M \cup xM$ en $yz \in M \cup xM$
  $y^{-1} = (sr^k)^{-1} = sr^k = y \in M \cup xM$, omdat $y \in M \cup xM$
  Nu moeten we nog laten zien dat $yz \in M \cup xM$
  $yz = sr^k sr^m = sr^{i+t}sr^{i+j} = ssr^{-(i+t)}r^{i+j} = er^{-(i+t)}r^{i+j} = r^{-i-t+i+j} = r^{-t+j}$
  Omdat $sr^m = sr^{i+t} \in xM$, weten we dat er een $r^t \in M$.
  Omdat $sr^m = sr^{i+j} \in xM$, weten we dat er een $r^j \in M$.

We weten dat voor elk tweetal elementen $r^t, r^j \in M$ moet gelden dat $r^{-t}r^j = r^{-t+j} \in M$.
Dus $yz = r^{-t+j} \in M \cup xM$

Omdat de groep $M \cup xM$ voldoet aan alle voorwaarden voor een ondergroep, is het een ondergroep van G.

(b) Neem nu $n = 12$ en $M = \langle r^3 \rangle$. Hoeveel verschillende ondergroepen krijg je uit de constructie in het vorige onderdeel?
De M is al gegeven, dus de de enige variatie van de ondergroep zit in de gekozen x.
$M = \langle r^3 \rangle = \{e, r^3, r^6, r^9\} = \{r^{3j} | 0 \leq j \leq 3\}$.
$|M| = 4$
$G \setminus R = \{s, sr, sr^2, \ldots, sr^{n-1}\}$
$|G \setminus R| = 12$
Dus er zijn 12 mogelijkheden voor x.
Maar $xM = \{sr^i r^{3j} | r^{3j} \in M\} = \{sr^{i+3j} | 0 \leq j \leq 3\}$ voor een vaste $0 \leq i \leq n-1$
Nu kunnen we gebruiken dat voor diëder groepen geldt dat $r^p = r^{p \bmod n}$.
Schrijf nu i in de vorm $i = 3w + v$, met v de rest van een deling door 3. Dus $v \in \{0, 1, 2\}$
Dit geeft $sr^{i+3j} = sr^{3w+v+3j} = sr^{3(w+j)+v} = sr^{(3(w+j)+v) \bmod 12}$.
Nu zien we dat voor elke $w \in \mathbb{Z}$ geldt dat dat $\{(3(w+j)+v) \bmod 12 | 0 \leq j \leq 3\} = \{v, 3+v, 6+v, 9+v\}$. Uitleg: De eerste term $3(w+j)$ neemt stappen van 3, omdat j elke keer maar 1 omhoog gaat. Omdat $j \in \{0, 1, 2, 3\}$ en $w \in \mathbb{Z}$, geldt dat $\{3(w+j) \bmod 12\} = \{0, 3, 6, 9\}$. Hier wordt elke keer v bij op geteld. Dus krijgen we $\{(3(w+j)+v) \bmod 12 | 0 \leq j \leq 3\} = \{v, 3+v, 6+v, 9+v\}$.
Dus dit betekent: $xM = \{sr^{3j+v} | 0 \leq j \leq 3\}$ met $x = sr^i$ en $i = 3w + v$. Omdat $v \in \{0, 1, 2\}$, zijn er slechts 3 keuzes mogelijk voor x die verschillende groepen xM construeren.
Dit betekend, dat $M \cup xM$ als 3 verschillende ondergroepen geconstrueerd kan worden, als $M = \langle r^3 \rangle$ en als $n = 12$.