## Inlever opdracht 2

## Luc Veldhuis

## 6 maart 2017

- 1. In een groep G zijn gegeven elementen x en y met  $xy = y^{-1}x$ 
  - (a) Laat met inductie naar n zien dat  $xy^n = y^{-n}x$  voor alle  $n \ge 0$ . We doen eerst de basis stap:

$$xy^0 = xe = x = ex = y^{-0}x$$

Als inductie hypothese nemen we aan dat voor alle  $n \ge 1$  geldt  $xy^{n-1} = y^{-(n-1)}x$ Bewijs nu dat  $xy^n = y^{-n}x$ 

Vermenigvuldig beide kanten van de inductie hypothese met  $y^{-1}$ :

$$xy^{n} = y^{-n}x$$
 (IH)  

$$y^{-1}xy^{n-1} = y^{-1}y^{-(n-1)}x$$
  

$$xyy^{n-1} = y^{-1}y^{-n+1}x$$
 (Gegeven  $y^{-1}x = xy$ )  

$$xy^{n} = y^{-1-n+1}x$$
  

$$xy^{n} = y^{-n}x$$

(b) Leid nu af dat  $xy^n = y^{-n}x$  voor alle n in  $\mathbb{Z}$ . (Aanwijzing: als n < 0 neem m = -n zodat  $xy^m = y^{-m}x$  volgens (a). Vermenigvuldig met machten van y om hieruit  $y^{-n}x = xy^n$  te krijgen.) We hebben net bewezen dat  $xy^n = y^{-n}x$  voor alle  $n \geq 0$ . We willen dit nu bewijzen voor alle n < 0. We nemen hiervoor m = -n als n < 0, zodat  $m \geq 0$ . Omdat  $m \geq 0$  weten we nu dat geldt  $xy^m = y^{-m}x$ . We weten ook dat we het resultaat van (a) kunnen omschrijven:

$$xy^{n} = y^{-n}x$$

$$y^{n}xy^{n} = y^{n}y^{-n}x$$

$$y^{n}xy^{n} = x$$

$$y^{n}xy^{n}y^{-n} = xy^{-n}$$

$$y^{n}x = xy^{-n}$$

Nu vermenigvuldigen we beide kanten met  $y^{2m}$ . Dit geeft:

$$xy^{m} = y^{-m}x$$

$$y^{2m}xy^{m} = y^{2m}y^{-m}x$$

$$xy^{-2m}y^{m} = y^{2m}y^{-m}x$$

$$xy^{-2m+m} = y^{2m-m}x$$

$$xy^{2n-n} = y^{-n}x$$

$$xy^{n} = y^{-n}x$$

Hier zien we dat dit ook geldt voor n < 0, dus geldt dit voor alle  $n \in \mathbb{Z}$ .

## 2. Gegeven is dat

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ met } a, b \in \mathbb{R} \text{ en } a \neq 0 \right\}$$

een groep is onder matrix vermenigvuldiging.

(a) Vind een uitdrukking voor  $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^n$  als  $n \ge 1$  en bewijs dat die klopt met inductie naar n.

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} a^n & b(\sum_{i=0}^{n-1} a^i) \\ 0 & 1 \end{pmatrix}$$

Bewijs met inductie:

Basisstap:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^1 & b(\sum_{i=0}^{1-1} a^i) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^1 & b1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

Inductie hypothese: Neem aan dat  $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} a^n & b(\sum\limits_{i=0}^{n-1}a^i) \\ 0 & 1 \end{pmatrix}$ 

Bewijs nu dat 
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{(n+1)} = \begin{pmatrix} a^{(n+1)} & b(\sum_{i=0}^{n} a^i) \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{(n+1)} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} =_{\text{(IH)}} \begin{pmatrix} a^n & b(\sum\limits_{i=0}^{n-1}a^i) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} a^n * a + b(\sum_{i=0}^{n-1} a^i) * 0 & a^n * b + b(\sum_{i=0}^{n-1} a^i) * 1 \\ 0 * a + 0 * b + 1 * 0 & 0 * b(\sum_{i=0}^{n-1} a^i) + 1 * 1 \end{pmatrix} = \begin{pmatrix} a^{(n+1)} & b(\sum_{i=0}^{n} a^i) \\ 0 & 1 \end{pmatrix}$$

(b) Bepaal alle elementen van eindige orde in G met hun orde. We weten dat voor een matrix het neutrale element  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  is. Dus we moeten onderzoeken welke elementen uit G bestaan zodat

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} a^n & b(\sum_{i=0}^{n-1} a^i) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We zien direct dat  $a^n=1$ , omdat we in een groep werken met matrix multiplicatie in  $\mathbb{R}$  en geen rest klassen, kan deze vergelijking alleen kloppen als a=1 en  $b(\sum\limits_{i=0}^{n-1}a^i)=0$ . Omdat als a=1 we altijd hebben dat  $(\sum\limits_{i=0}^{n-1}a^i)\neq 0$ , moet wel gelden dat b=0. Dus het enige element met eindige orde in G is het neutrale element  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  met orde 1. Alle andere elementen hebben een oneindige orde.