

Maak alle zeven opgaven. Antwoorden zonder uitleg scoren slecht. Aantekeningen, boeken, rekenmachines en andere elektronische hulpmiddelen zijn **niet** toegestaan. Als je een onderdeel van een vraag niet kunt maken, mag je het antwoord wel gebruiken in de rest van de opgave. Het cijfer voor het tentamen wordt berekend met de formule $\text{cijfer} = 1 + \frac{\text{behaalde punten}}{10}$. Succes!

Opgave 1 (15 punten). Geef alle getallen $x \in \mathbb{Z}$ zodat

$$x \equiv 4 \pmod{5},$$

$$x \equiv 1 \pmod{7},$$

$$x \equiv 0 \pmod{2}.$$

Uitwerking 1. Met de standaard technieken, het Euclidische algoritme en het bewijs van de Chinese reststelling, vinden we dat $x = 64$ voldoet. De Chinese reststelling zegt ook dat de oplossing uniek is modulo $70 = 5 * 7 * 2$. Dus alle oplossingen van dit stelsel congruenties zijn

$$x = 64 + 70k \quad k \in \mathbb{Z}$$

Opgave 2 (15 punten). Zij G een groep. Definieer het *centrum* van G door middel van

$$Z(G) = \{a \in G \mid ag = ga \text{ voor alle } g \in G\}.$$

Dit zijn alle elementen van G die commuteren met alle andere elementen in de groep.

- Bewijs dat dit een ondergroep is van G .
- Bereken $Z(D_4)$, waarbij D_4 de dihedrale groep is van een vierkant.

Uitwerking 2.

- Het centrum is niet leeg want $e \in Z(G)$, omdat $eg = g = ge$ voor alle $g \in G$. Stel nu dat $x, y \in Z(G)$. Dan moeten we controleren dat $xy \in Z(G)$. Nu is dat makkelijk omdat,

$$xyg = xgy = gxy.$$

voor alle $g \in G$. Verder geldt

$$xg = gx,$$

bij aannamen. Vermenigvuldigen we links met x^{-1} en rechts met x^{-1} dan volgt

$$gx^{-1} = x^{-1}g,$$

dat dus $x^{-1} \in Z(G)$, waarmee we hebben aangetoond dat $Z(G)$ een ondergroep is.

- Omdat geldt

$$sr^i r = sr^{i+1} \neq r sr^i = sr^{i-1}$$

zien we dat $sr^i \notin Z(D_4)$ voor alle i . Verder geldt in D_4 dat

$$rs = sr^3 \neq sr,$$

en

$$r^3 s = sr \neq sr^3$$

dus $r, r^3 \notin Z(D_4)$. Het eenheidselement $r^0 \in Z(D_4)$ natuurlijk, en verder

$$r^2 r^i = r^{i+2} = r^i r^2$$

en

$$r^2 s r^i = s r^{-2} r^i = s r^2 r^i = s r^i r^2.$$

dus ook $r^2 \in Z(D_4)$. We gebruiken in de laatste stap dat $r^2 = r^{-2}$ in D_4 .

Opgave 3 (15 punten). Beschouw afbeeldingen $f : \mathbb{R} \rightarrow \mathbb{R}$ van de vorm

$$f(x) = ax + b \quad \text{met} \quad a \in \mathbb{R}^*, \quad b \in \mathbb{R}.$$

- a) Controleer dat de samenstelling van dit soort afbeeldingen weer van deze vorm is.
- b) Bewijs dat dit een groep wordt onder samenstelling.
- c) Geef voorbeelden van zulke functies zodat $f \circ g \neq g \circ f$.

Uitwerking 3.

- a) Zij $f, g : \mathbb{R} \rightarrow \mathbb{R}$ van de vorm

$$f(x) = ax + b,$$

$$g(x) = cx + d,$$

voor $a, c \in \mathbb{R}^*$ en $b, d \in \mathbb{R}$. Dan geldt dat

$$f \circ g(x) = f(cx + d) = acx + ad + b,$$

en het is duidelijk dat $ac \in \mathbb{R}^*$ en $ad + b \in \mathbb{R}$.

- b) Samenstelling van functies is associatief, en dus ook functies van deze vorm, d.w.z.

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Verder is de identiteit $\text{id}_{\mathbb{R}}$ de identiteit in deze groep omdat, voor alle $x \in \mathbb{R}$

$$f \circ \text{id}_{\mathbb{R}}(x) = f(\text{id}_{\mathbb{R}}(x)) = f(x) = \text{id}_{\mathbb{R}}(f(x)) = \text{id}_{\mathbb{R}} \circ f(x)$$

De inverse van $f = ax + b$ is natuurlijk $g = \frac{1}{a}x - \frac{b}{a}$, omdat voor alle $x \in \mathbb{R}$

$$f \circ g(x) = f\left(\frac{1}{a}x - \frac{b}{a}\right) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x = \text{id}_{\mathbb{R}}(x),$$

en

$$g \circ f(x) = g(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x = \text{id}_{\mathbb{R}}(x).$$

Het is dus een groep

- c) de functies $f(x) = 2x + 3$ en $g(x) = -1x + 2$ hebben

$$f \circ g(x) = -2x + 7$$

$$g \circ f(x) = -2x + -1.$$

De groep is dus niet abels.

Opgave 4 (8 punten). Multiple choice! Geef aan van de onderstaande verzamelingen of ze ofwel eindig, aftelbaar oneindig, of overaftelbaar zijn. Je hoeft geen uitleg te geven.

- a) Zij $n \in \mathbb{N}$. De verzameling bijecties

$$B = \{f : [[n]] \rightarrow [[n]] \mid f \text{ is bijjectief}\}.$$

- b) De verzameling van eenheidswortels

$$E = \{x \in \mathbb{C} \mid \text{er is } n \in \mathbb{N} \text{ zodat } x^n = 1\}.$$

- c) De verzameling functies van $\mathbb{R}$ naar $\mathbb{R}$

$$F = \{f : \mathbb{R} \rightarrow \mathbb{R}\}.$$

d) De twee bij twee matrices met gehele coëfficiënten.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \quad \text{zodat} \quad ad - bc = 1 \right\}.$$

Uitwerking 4.

- a) $B = S_n$, en heeft eindige kardinaliteit $n!$.
 b) Voor elke $n \in \mathbb{N}$ zijn er n verschillende eenheidswortels $e^{2\pi i/n}$. De vereniging van al deze is de verzameling E . Aftelbare verenigingen van eindige verzamelingen zijn maximaal aftelbaar oneindig. Het is niet eindig omdat $e^{2\pi i/n} \neq e^{2\pi i/m}$ voor $m \neq n$.
 c) Alle constante functies $f_s(x) = s$ hebben dezelfde kardinaliteit als de verzameling $\mathbb{R}$, welke overaftelbaar is. De verzameling van alle functies bevat alle constante functies, dus is deze verzameling overaftelbaar.
 d) We kunnen een injectie maken $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathbb{Z}^4$, door middel van $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b, c, d)$. De verzameling $\mathbb{Z}^4$ is duidelijk aftelbaar. dus $\mathrm{SL}_2(\mathbb{Z})$ is maximaal aftelbaar oneindig. De matrices

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

zitten allen in $\mathrm{SL}_2(\mathbb{Z})$, en dat zijn er aftelbaar veel, dus $\mathrm{SL}_2(\mathbb{Z})$ is aftelbaar oneindig.

Opgave 5 (7 punten). Hoeveel elementen heeft $(\mathbb{Z}/20\mathbb{Z})^*$? Laat zien hoe je aan je antwoord komt.

Uitwerking 5. Alle 2- vouden en alle 5-vouden hebben $\mathrm{ggd}(x, 20) \neq 1$. De getallen

$$\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19},$$

zijn allen wel relatief priem met 20. Deze zitten dus in $(\mathbb{Z}/20\mathbb{Z})^*$. De orde van de groep is dus 8.

Opgave 6 (15 punten). Zij $G \subseteq \mathrm{GL}_2(\mathbb{R})$ de volgende ondergroep

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 \neq 0 \right\}.$$

Je hoeft niet te bewijzen dat dit een ondergroep is. Construeer een isomorfisme $\varphi : G \rightarrow \mathbb{C}^*$, en bewijs dat dit een isomorfisme is.

Uitwerking 6. We claimen dat de afbeelding $\varphi \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi$ voldoet. Het is duidelijk

dat als $a^2 + b^2 \neq 0$, dan $\varphi \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) \neq 0$. Het is ook een homomorfisme, namelijk

$$\varphi \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) = \varphi \left(\begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \right) = ac - bd + (ad + bc)i.$$

maar dat laatste is ook gelijk aan $(a + bi)(c + di)$. . Het is een ook bijectie omdat de afbeelding $\psi : \mathbb{C}^* \rightarrow G$ gedefinieerd door

$$\psi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

een inverse is, wat duidelijk is. φ is dus een isomorfisme.

Opgave 7 (15 punten). Zij

$$V = \{A \subseteq \mathbb{N} \mid 1 \in A \text{ en } 2 \notin A\}.$$

Dit zijn de deelverzamelingen van $\mathbb{N}$ die 1 bevatten, maar 2 niet.

- a) Construeer een injectieve functie $f : \mathcal{P}(\mathbb{N}) \rightarrow V$.
- b) Bewijs dat $\mathcal{P}(\mathbb{N}) \sim V$.

Uitwerking 7.

- a) De afbeelding $f(A) = \{x+2 \mid x \in A\} \cup \{1\}$ beeldt deelverzamelingen van $\mathbb{N}$ af op V . Het is ook injectief. Stel namelijk dat $f(A) = f(B)$. Neem $x \in A$. Dan geldt dat $x+2 \in f(A)$. Omdat $f(A) = f(B)$ is $x+2 \in f(B)$. Hieruit volgt dat $x \in B$, omdat $x+2 \neq 1$. Dus $A \subseteq B$. Compleet analoog $B \subseteq A$. Dus f is injectief.
- b) In a) hebben we bewezen dat $\mathcal{P}(\mathbb{N}) \preccurlyeq V$. Omdat $V \subseteq \mathcal{P}(\mathbb{N})$ geldt $V \preccurlyeq \mathcal{P}(\mathbb{N})$. Schroeder-Bernstein geeft nu dat $\mathcal{P}(\mathbb{N}) \sim V$. Ook is het natuurlijk mogelijk om direct te bewijzen dat de functie in a) surjectief is.