INLEIDING GROEPEN EN RINGEN 2019–2020

TENTAMEN: UITWERKING

Vraag 1.

8pt (a) Representeer de restklasse $\overline{7}^{-1}$ in $(\mathbf{Z}/2020)^*$ door een element in $\{0, \ldots, 2019\}$.

Oplossing. We berekenen met het Euclidische algoritme de grootste gemene deler d van 7 en 2020, als volgt:

$$\begin{aligned} 2020 &= 288 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

Dus is $d = 1$ en door terugrekenen vinden we

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (2020 - 288 \cdot 7) - 7 \\ &= 2 \cdot 2020 - (1 + 2 \cdot 288) \cdot 7. \end{aligned}$$

Modulo 2020 is dus $\overline{1} = -\overline{577} \cdot \overline{7}$, dus omdat $2020 - 577 = 1443$ is $\overline{7}^{-1} = \overline{1443}$.

8pt (b) Stel $D_{14} = \langle r, s \mid r^7 = s^2 = e, rsr = s \rangle$ is de diëdergroep van orde 14. Schrijf het element

$$r^{23} s^6 r^{2020} \in D_{14}$$

met hoogstens 3 symbolen (iedere letter, teken en cijfer telt als één symbool).

Oplossing. Omdat $s^6 = (s^2)^3 = e$ is dus $r^{23} s^6 r^{2020} = r^{2043} = r^{7 \cdot 291 + 6} = (r^7)^{291} r^6 = r^6$.

8pt (c) Bereken de orde van de matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathrm{GL}_2(\mathbf{R})$.

Oplossing. Als m de matrix is en I de identiteitsmatrix, dan is $m^2 = -I \neq I$; vervolgens $m^3 = m \cdot m^2 = m \neq I$, en $m^4 = (-I)^2 = I$, dus is de orde $|m| = 4$.

8pt (d) Definieer de hoofdidealen $I := (x)$, $J := (x + 1)$ en $K := (x^{2020} + x)$ in de polynomenring $\mathbf{R}[x]$. Schrijf het ideaal $I(I + (J \cap K))$ als hoofdideaal.

Oplossing. We merken op dat $J \cap K = (\mathrm{kgv}(x + 1, x^{2020} + x))$ en dat $x + 1$ een deler is van $x^{2020} + x$, want -1 is een nulpunt van dat laatste polynoom. Bijgevolg is het kleinste gemeenschappelijke veelvoud gelijk aan $x^{2020} + x$ en dus $J \cap K = K$. Vervolgens is $I + K = (\mathrm{ggd}(x, x^{2020} + x))$. Omdat x een deler is van $x^{2020} + x$, is dus $I + K = (x) = I$. Uiteindelijk is $I(I + (J \cap K)) = I^2 = (x)^2 = (x^2)$.

Vraag 2. Zijn onderstaande beweringen waar of onwaar? Bewijs of weerleg.

8pt (a) In de permutatiegroep S_5 is het product van 2020 4-cykels een even permutatie.

Oplossing. Waar. Ten eerste zijn 4-cykels oneven, dus hebben teken -1. Ten tweede is het teken van het product van twee permutaties het product van de tekens van die permutaties. Bijgevolg heeft het gevraagde product als teken $(-1)^{2020} = 1$, en dus is het even.

8pt (b) Als een groep G werkt op een ruimte X, dan vormt de collectie stabilisatoren $\{G_x \colon x \in X\}$ een partitie van G.

Oplossing. Onwaar. Alle stabilizatoren bevatten het neutrale element e van de groep, dus vormen ze een partitie desda ze allemaal gelijk zijn. Maar als $G = S_X \cong S_3$ werkt op $X = \{1, 2, 3\}$ door permutaties, dan is $(23) \in G_1 = S_{\{2,3\}} \leq G$ maar $(23) \notin G_2 = S_{\{1,3\}} \leq G$. (Vele andere voorbeelden zijn mogelijk.)

8pt (c) De ring $\mathbf{Z}/4$ (voor de ringstructuur die komt van modulorekenen) is een lichaam.

Oplossing. Onwaar. Anders zou ieder niet-nul element een inverse moeten hebben voor vermenigvuldiging. Maar als $\overline{2}$ inverse $\overline{n}$ zou hebben, dan is $\overline{2n} = \overline{1}$. Vermenigvuldigen aan beide kanten met $\overline{2}$ geeft dan $\overline{4n} = \overline{0} = \overline{2}$, wat niet klopt. (Andere redenatie: $\overline{2} \neq \overline{0}$ is een nuldeler, want $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$, maar in een lichaam zijn er geen nuldelers.)

8pt (d) Het ideaal $(x+1)$ is een maximaal ideaal in de ring $\mathbf{R}[x,y]$.

1e Oplossing. Onwaar. We hebben een isomorfisme $\mathbf{R}[x,y]/(x+1) \cong \mathbf{R}[y]$ (Bijvoorbeeld door de 1e isomorfismestelling van $(x+1)$ is de kern van het evaluatiehomomorfisme $\mathbf{R}[x,y] \to R[y] \colon f(x,y) \mapsto f(-1,y)$; of omdat wegens de 3e isomorfismestelling $\mathbf{R}[x,y]/(x+1) = \mathbf{R}[x]/(x+1)[y]$ en $\mathbf{R}[x]/(x+1) \cong \mathbf{R}$ doordat $(x+1)$ de kern van het evaluatiehomomorfisme is op $\mathbf{R}[x]$ in $x = -1$) Nu is $\mathbf{R}[y]$ geen lichaam (want omdat $\mathbf{R}$ een domein is is $\mathbf{R}[y]^\times = \mathbf{R}^\times \neq \mathbf{R}[y] - \{0\}$) en dus is $(x+1)$ niet maximaal wegens het criterium voor maximaal ideaal in termen van quotiënt.

2e Oplossing. Onwaar. Het is niet maximaal want het is bevat in het ideaal $I = (x+1, y)$ en $I \neq (x+1)$ en $I \neq (1)$. Mocht $I = (x+1)$ dan is $y \in (x+1)$ dus $y = (x+1)q(x,y)$ voor een $q(x,y) \in \mathbf{R}[x,y]$ maar dan is $\deg_x y = 0 = 1 + \deg_x q \geq 1$, contradictie. Mocht $I = (1)$ dan is $1 = a(x,y)(x+1) + b(x,y)y$ voor $a, b \in \mathbf{R}[x,y]$. Duidelijk is niet $a = b = 0$; als $a \neq 0$, dan is $\deg_x 1 = 0 = \deg_x a + 1 + \deg_x b \geq 1$ (waarbij de tweede term niet voorkomt als $b = 0$); contradictie; en als $b \neq 0$, dan is $\deg_y 1 = 0 = \deg_y a + \deg_y b + 1 > 1$ (waarbij de eerst term niet voorkomt als $a = 0$), contradictie.

Vraag 3. Geef een voorbeeld van, of laat zien dat zoiets niet kan bestaan:

8pt (a) Een groep van orde 6^{2020} met een ondergroep van orde 23.

Oplossing. Bestaat niet. Volgens de stelling van Lagrange is de orde van een ondergroep een deler van de orde van de groep, maar 23 is geen deler van 6^{2020}.

8pt (b) Een niet-injectief groepshomomorfisme $\varphi \colon G \to H$ waarbij de orde van G gelijk is aan $|G| = 505$ en het beeld van G niet commutatief is.

Oplossing. Bestaat niet. De kern N van φ is een een ondergroep van G. In het bijzonder is wegens de stelling van Lagrange de orde van N een deler van $505 = 5 \cdot 101$, dus $1, 5, 101$ of 505. Nu is de orde niet 1, want φ is niet injectief. Wegens de eerste isomorfismestelling is het beeld van φ isomorf met G/N, dus van orde $|G|/|N| \in \{1, 5, 101\}$. Een groep van orde 1 is triviaal, dus commutatief. Omdat 5 en 101 priemgetallen zijn, zijn groepen van die orde cyclisch. In het bijzonder zijn ze altijd commutatief.

8pt (c) Een niet-injectief ringhomomorfisme $\varphi \colon \mathbf{R} \to S$, met S een domein, en beeld $\varphi(\mathbf{R}) \neq \{0\}$.

Oplossing. Bestaat niet. Omdat $\mathbf{R}$ een lichaam is, heeft $\mathbf{R}$ slechts twee idealen, (0) en (1). De kern I van φ is een ideaal, en $I \neq (0)$ omdat φ niet injectief is. Dus $I = (1)$. Wegens de 1e isomorfismestelling voor ringen is $\varphi(\mathbf{R}) \cong \mathbf{R}/I = \{0\}$.

Vraag 4. Stel dat R een domein is met $0 \neq 1$, en I en J twee willekeurige idealen in R.

4pt (a) Bewijs dat de afbeelding

$$\psi \colon R/I \times R/J \mapsto R/(I+J) \colon (r+I, s+J) \mapsto r - s + I + J$$

een welgedefinieerd surjectief groepshomomorfisme is (voor de optelling).

Oplossing. De afbeelding is welgedefinieerd: als $r + I = r' + I$ en $s + J = s' + J$ voor $r, r', s, s' \in R$ dan moeten we aantonen dat $r - s + I + J = r' - s' + I + J$. Dit geldt als $r - r' + s - s' \in I + J$, maar de aanname is dat $r - r' \in I$ en $s - s' \in J$, dus dit geldt bij definitie van de som van idealen.
De afbeelding is surjectief, want voor alle $r \in R$ geldt dat $r + I + J = \psi(r, 0)$ in het beeld van ψ ligt.
De afbeelding is een groepshomomorfisme want $\psi((r+I, s+J) + (r'+I, s'+J)) = \psi((r+r'+I, s+s'+J)) = r+r'-s-s'+I+J$ en $\psi(r+I, s+J) + \psi(r'+I, s'+J) = (r-s+I+J) + (r'-s'+I+J) = r+r'-s-s'+I+J$, wat hetzelfde is.

4pt (b) De afbeelding
$$\varphi\colon R \mapsto R/I \times R/J\colon r \mapsto (r+I, r+J)$$
is een ringhomomorfisme (dat hoef je niet te bewijzen). Toon aan dat $\varphi(R) = \ker(\psi)$.

Oplossing. Een element $\alpha \in \varphi(R)$ is van de vorm $\alpha = (r+I, r+J)$ voor een $r \in R$. Dan is dus $\psi(\alpha) = r - r + I + J = I + J$, het neutrale element van $R/(I+J)$. Bijgevolg is $\alpha \in \ker\psi$.
Omgekeerd, stel $\beta = (r+I, s+J) \in \ker(\psi)$. Dit betekent dat $r - s \in I + J$. De claim is dat er $z \in R$ bestaat met $\varphi(z) = \beta$, d.w.z. $(z+I, z+J) = (r+I, s+J)$, m.a.w. $z - r \in I$ en $z - s \in J$. Wegens de aanname $r - s \in I + J$ kunnen we schrijven $r - s = i + j$ met $i \in I$ en $j \in J$. Stel dan (†) $z := r - i$. Dan is ook (††) $z = s + j$. Uit de eerste vergelijking (†) volgt $z - r = -i \in I$ en uit de tweede vergelijking (††) volgt dat $z - s = j \in J$; dit is wat we moesten aantonen.

2pt (c) Hoe volgt uit (b) dat φ surjectief is voor twee comaximale idealen I en J?

Oplossing. De idealen I en J zijn bij definitie comaximaal als $I + J = R$. Dan is ψ de nulafbeelding en $\ker(\psi) = R/I \times R/J$. Wegens het vorige punt is dit ook $\varphi(R)$, dus φ is surjectief.

2pt (d) Hoe volgt uit (b) dat voor twee gehele getallen $a, b \in \mathbf{Z}$ altijd geldt dat
$$a \cdot b = \mathrm{ggd}(a,b) \cdot \mathrm{kgv}(a,b)?$$

Oplossing. We kiezen $R = \mathbf{Z}$ en stellen $I = (a)$ en $J = (b)$. We weten dat als idealen $I + J = (a,b) = (\mathrm{ggd}(a,b))$ en $I \cap J = (\mathrm{kgv}(a,b))$. Als commutatieve groepen voor optelling vinden we $\ker\varphi = I \cap J = (\mathrm{kgv}(a,b))$ dus wegens de eerste isomorfismestelling en (b) dat $\mathbf{Z}/(\mathrm{kgv}(a,b)) = \mathbf{Z}/\ker\varphi \cong \varphi(\mathbf{Z}) \cong \ker(\psi)$. Dit zijn eindige groepen en dus van dezelfde orde, dus $(*)$ $|\ker\psi| = \mathrm{kgv}(a,b)$. Verder is ψ een surjectief groepshomomorfisme, dus $(\mathbf{Z}/(a) \times \mathbf{Z}/(b))/\ker(\psi) \cong \mathbf{Z}/(\mathrm{ggd}(a,b))$. Door ordes te vergelijken is dus $(**)$ $ab/|\ker\psi| = \mathrm{ggd}(a,b)$. Het gestelde volgt door substitueren van $(*)$ in $(**)$.