INLEIDING GROEPEN EN RINGEN 2020–2021

TENTAMEN 28 JUNI 2021,

UITWERKING

Vraag 1.

8pt (a) Bereken de inverse van het element $\overline{13}$ in de groep $(\mathbf{Z}/2021)^*$ voor vermenigvuldiging, en schrijf het resultaat als $\overline{m}$ met $0 \leq m \leq 2020$.

We voeren het uitgebreide euclidische algoritme uit:

$$2021 = 155 \cdot 13 + 6$$
$$13 = 2 \cdot 6 + 1$$

Dus de ggd van 13 en 2021 is 1; daarom bestaat de inverse, en door terugsubstitueren vinden we

$$1 = 13 - 2 \cdot 6 = 13 - 2 \cdot (2021 - 155 \cdot 13) = 311 \cdot 13 - 2 \cdot 2021 = 1.$$

Door dit modulo 2021 te bekijken vinden we dat $\overline{311} \cdot \overline{13} = \overline{1}$ in $(\mathbf{Z}/2021)^*$, dus het antwoord is $m = 311$.

8pt (b) Stel $D_{18} = \langle r, s \mid r^9 = s^2 = e, rsr = s \rangle$ is de diëdergroep van orde 18. Schrijf het element

$$r^{28} s r^{2021} \in D_{14}$$

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

We substitueren de gegeven relaties iteratief en beginnen met $r^9 = e$ te gebruiken:

$$r^{28} s r^{2021} = r^{3 \cdot 9 + 1} s r^{224 \cdot 9 + 5} = (r^9)^3 r s (r^9)^{224} r^5 = r s r^5 = r s r r^4 = s r^4,$$

waarbij in de laatste gelijkheid de relatie $rsr = s$ is gebruikt.

8pt (c) Beschouw de elementen $\sigma_1 = (152)(34)$ en $\sigma_2 = (163)(45)$ in S_6. Bereken een element $\tau \in S_6$, geschreven als product van disjuncte cykels, zodat $\sigma_2 = \tau \sigma_1 \tau^{-1}$.

Merk op dat $\sigma_1(6) = 6$ en $\sigma_2(2) = 2$. Wegens de regel dat conjugatie "hernoemen" is van de entries m.b.v. de conjugerende permutatie, d.w.z. $\tau(152)(34)(6)\tau^{-1} = (\tau(1)\tau(5)\tau(2))(\tau(3)\tau(4))(\tau(6))$, vinden we dat $\tau = (56234)$ voldoet. Inderdaad rekenen we na dat $\tau\sigma_1\tau^{-1} = (56234)(152)(34)(65432) = (163)(45)$.

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

8pt (a) In de permutatiegroep S_{2021} is een product van alle transposities (waarbij iedere transpositie precies één keer voorkomt) altijd een even permutatie.

Een transpositie krijgen we door twee verschillende elementen te kiezen uit $\{1, \ldots, 2021\}$ (nl. de twee elementen die door de transpositie worden verwisseld), waarbij de volgorde niet uitmaakt. Dat kan op $n := 2021 \cdot 2020/2 = 2021 \cdot 1010$ manieren, een even aantal. Zetten we die transposities in willekeurige volgorde $t_1, \ldots, t_n$, dan is $\mathrm{sign}(t_1 \cdots t_n) = (-1)^n = 1$, omdat $\mathrm{sign}(t_i) = -1$ voor alle i. De bewering is dus waar.

8pt (b) Als H een ondergroep is van G, dan is H een normale ondergroep in G dan en slechts dan als $H \times A_{2021}$ een normale ondergroep is in $G \times S_{2021}$.

De bewering is waar. Er geldt $H \times A_{2021} \lhd G \times S_{2021}$ desda voor alle $g \in G, h \in H, \sigma \in S_{2021}, \tau \in A_{2021}$ geldt dat

$$(g, \sigma)(h, \tau)(g, \sigma)^{-1} \in H \times A_{2021}.$$

Door uitwerken is dit equivalent met

$$(ghg^{-1}, \sigma\tau\sigma^{-1}) \in H \times A_{2021}.$$

Dit is op zijn beurt door uitschrijven in componenten equivalent met $ghg^{-1} \in H$ en $\sigma\tau\sigma^{-1} \in A_{2021}$. De twee conditie geldt altijd, want dit zegt dat $A_{2021} \lhd S_{2021}$, en dat klopt (bijv. omdat de index 2 is); de eerste conditie is equivalent met $H \lhd G$, dus is het gestelde hiermee ook equivalent.

8pt (c) De ring $\mathbf{R}[x, y]/(x + 1)$ is een lichaam.

De bewering is fout. Als het wel waar was, dan zou $(x + 1)$ een maximaal ideaal zijn in $\mathbf{R}[x, y]$. Echter, $(x+1, y)$ is een ideal dat $(x+1)$ bevat (duidelijk), en niet gelijk is aan $\mathbf{R}[x, y]$. Mocht dat laatste namelijk gelden, dan zouden er polynomen $r(x, y)$ en $s(x, y)$ in $\mathbf{R}[x, y]$ bestaan met $r(x, y)(x+1)+s(x, y)y = 1$. Vullen we hier $x = -1, y = 0$ in, dan staat er $0 = 1$, een tegenspraak.

8pt (d) De ring $\mathbf{Z}[x]/(7)$ is een hoofdideaaldomein.

De bewering is waar. Er is een ringisomorfisme $\mathbf{Z}[x]/(7) \cong \mathbf{Z}/7[x]$ (bijv. zoals in het bewijs van het Lemma van Gauß: het ringhomomorfisme $\mathbf{Z}[x] \to \mathbf{Z}/7[x]$ gegeven door alle coëfficiënten van een polynoom modulo 7 te bekijken is surjectief, en de kern is (7), het hoofdideaal voortgebracht door 7 in $\mathbf{Z}[x]$). Nu is $\mathbf{Z}/7$ een lichaam (want 7 is priem, dus iedere niet-nul klasse modulo 7 heeft een multiplicatieve inverse wegens het euclidisch algoritme), en een polynoomring over een lichaam is een ED, i.h.b. een HID.

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

8pt (a) Oneindig veel verschillende elementen van orde 2 in $\mathrm{GL}_2(\mathbf{R})$.

De matrix $m = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ heeft duidelijk orde 2. Als $p = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ een willekeurige inverteerbare matrix is, dan heeft pmp^{-1} ook orde 2, want

$$(pmp^{-1})^2 = pmp^{-1}pmp^{-1} = pm^2p^{-1} = pp^{-1} = e.$$

Dit geeft oneindig veel verschillende elementen van orde 2 in $\mathrm{GL}_2(\mathbf{R})$, expliciet:

$$(ad - bc)^{-1} \left(\begin{smallmatrix} ad+bc & -2ab \\ 2cd & -ad-bc \end{smallmatrix}\right)$$

voor alle $a, b, c, d \in \mathbf{R}$ met $ad \neq bc$.

8pt (b) Een groepsactie van de diëdergroep D_{32768} van orde $32768 = 2^{15}$ met een baan die precies 2021 elementen heeft.

Wegens de baan-stabilizator stelling is het aantal element in de baan van een willekeurig element x gelijk aan de index van de stabilizator G_x in $G = D_{32768}$; i.h.b. is dat aantal elementen een deler van de orde van de groep, maar $2021 = 43 \cdot 47$ is geen deler van $32768 = 2^{15}$. Zoiets bestaat dus niet.

8pt (c) Een deelring van $\mathbf{Q}[x]$ die geen euclidisch domein is voor de norm $N(f) = \deg(f)$ als $f \neq 0$ en $N(0) = 0$.

Dit bestaat, bijv. $\mathbf{Z}[x]$. Dat is een HID (bijv. is $(2, x)$ geen hoofdideaal), en i.h.b. geen ED, voor geen enkele norm.

Vraag 4. Stel dat $R = \mathbf{Q}[x]/(x^2)$.

4pt (a) Bepaal de nuldelers in R.

We representeren een element t van $\mathbf{Q}[x]/(x^2)$ uniek als $t = a\overline{x} + b$ met $a, b \in \mathbf{Q}$. Dit is een nuldeler desda er bestaat $c, d \in \mathbf{Q}$ met $(c, d) \neq (0, 0)$ en $(a\overline{x}+b)(c\overline{x}+d) = 0$. Uitwerken geeft $(ad+bc)\overline{x}+bd = 0$, dus $ad + bc = 0$ en $bd = 0$. Als $d \neq 0$ volgt $b = 0$ en $a = 0$, dus $t = 0$; en als $d = 0$, volgt $c \neq 0$, dus $b = 0$. Inderdaad is dan $t = a\overline{x}$ een nuldeler voor $a \neq 0$, wegens $t\overline{x} = 0$. Conclusie: *de nuldelers zijn* $\{a\overline{x} \colon a \in \mathbf{Q}^*\}$.

8pt

(b) Bepaal de eenheden R^* in R, en bewijs dat er een groepsisomorfisme $R^* \cong \mathbf{Q}^* \times \mathbf{Q}$ bestaat (hier is $\mathbf{Q}$ de groep $\mathbf{Q}$ van rationale getallen onder optellen, en $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ de groep van inverteerbare rationale getallen onder vermenigvuldigen).

In R is $t = a\overline{x} + b$ een eenheid desda er bestaat $c, d \in \mathbf{Q}$ met $(a\overline{x} + b)(c\overline{x} + d) = 1$. Uitwerken geeft $(ad + bc)\overline{x} + bd = 1$, dus $ad + bc = 0$ en $bd = 1$. Dan is $b \neq 0$, en de keuze $d = 1/b, c = -a/b^2$ geeft een inverse. *We concluderen dat* $R^* = \{a\overline{x} + b \colon a \in \mathbf{Q}, b \in \mathbf{Q}^*\}$.
We herschrijven een element van R^* op unieke manier als $r(s\overline{x} + 1)$ met $r \in \mathbf{Q}^*$ en $s \in \mathbf{Q}$ ($r = b$ en $s = a/r$ in de vorige representatie). Bekijk de afbeelding

$$\varphi \colon R^* \to \mathbf{Q}^* \times \mathbf{Q} \text{ gegeven door } \varphi(r(s\overline{x} + 1)) = (r, s).$$

Dit is wegens de unieke manier van representeren een bijectie. Nu is voor twee elementen $\varphi(r(s\overline{x} + 1)r'(s'\overline{x} + 1)) = \varphi(rr'((s + s')\overline{x} + 1)) = (rr', s + s') = \varphi(r(s\overline{x} + 1))\varphi(r'(s'\overline{x} + 1))$, dus φ is een groepshomomorfisme, en dus een isomorfisme van groepen omdat de afbeelding ook bijectief is.

8pt

(c) Bepaal alle idealen van R, en geef aan welke hiervan priemidealen zijn en welke maximale idealen zijn.

We gebruiken de bijectie tussen idealen in $\mathbf{Q}[x]/(x^2)$ en idealen in $\mathbf{Q}[x]$ die (x^2) bevatten. Als I een ideaal is in $\mathbf{Q}[x]$ met $(x^2) \subseteq I \subseteq \mathbf{Q}[x]$, dan is I een hoofdideaal, stel, $I = (d)$ voor een $d \in \mathbf{Q}[x]$ (dit is zo omdat $\mathbf{Q}[x]$ een ED, en i.h.b. een HID is). Uit $(x^2) \subseteq (d)$ volgt dat het polynoom d een deler is van x, dus $d = 1$ (en $I = \mathbf{Q}[x]$) of $d = x$ of $d = x^2$ (en $I = (x^2)$).

De correspondentie met de idealen van R is gegeven door $(d) \to (\overline{d})$; er zijn in R dus *drie verschillende idealen, gegeven door de hoofdidealen* $(1), (\overline{x})$ *en* (0). Wegens de inclusies $(0) \subsetneq (\overline{x}) \subsetneq (1)$ is $(\overline{x})$ maximaal (en dus ook priem), en zijn de idealen (0) en (1) niet maximaal. Het ideaal (1) is bij definitie niet priem, en het ideaal (0) in R is ook niet priem, want R is geen domein (het heeft nuldelers, en voor twee nuldelers $t_1, t_2 \in R$ geldt $t_1 t_2 \in (0)$ zonder dat $t_1 \in (0)$ of $t_2 \in (0)$). In tabelvorm:

ideaal	priem?	maximaal?
(0)	nee	nee
$(\overline{x})$	ja	ja
(1)	nee	nee