INLEIDING GROEPEN EN RINGEN 2021–2022

TENTAMEN 27 JUNI 2022

UITWERKING

Vraag 1.

10pt (a) Bereken de inverse van het element $\overline{119}$ in de groep $(\mathbf{Z}/2022)^*$ voor vermenigvuldiging, en schrijf het resultaat als $\overline{m}$ met $0 \leq m \leq 2021$.

We can use the Euclidean algorithm starting from the numbers 119 and 2022:

$$2022 = 119 \cdot 16 + 118$$
$$119 = 118 \cdot 1 + 1$$

Substituting equation $118 = 2022 - 119 \cdot 16$ into the second one above gives

$$1 = 119 - 118 = 119 - (2022 - 119 \cdot 16) = 2022 \cdot (-1) + 119 \cdot 17.$$

It follows that $119 \cdot 17 = 1$ in $\mathbf{Z}/2022$, that is, $\overline{119}^{-1} = \overline{17}$.

10pt (b) Bereken de orde van het element $(123)(12)(34)$ in A_4.

Its cycle decomposition is just the 3-cycle (134), which has order 3.

10pt (c) Stel dat M een willekeurige inverteerbare matrix is in $\mathrm{GL}_2(\mathbf{R})$ (de groep van inverteerbare 2×2 matrices over de reële getallen voor vermenigvuldiging), en stel dat $N := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Bereken de orde van MNM^{-1} in $\mathrm{GL}_2(\mathbf{R})$.

Note that for any $n \in \mathbf{Z}_{>0}$ we have

$$(MNM^{-1})^n = \underbrace{(MNM^{-1})(MNM^{-1}) \cdot \ldots \cdot (MNM^{-1})(MNM^{-1})}_{n}$$
$$= MN(\underbrace{M^{-1}M}_{=I})N \cdot \ldots \cdot N(\underbrace{M^{-1}M}_{=I})NM^{-1} = M\underbrace{N \cdot \ldots N}_{n}M^{-1} = MN^nM^{-1},$$

so $(MNM^{-1})^n = I \iff MN^nM^{-1} = I \iff N^n = I$. Thus, the order of MNM^{-1} equals the order of N. We compute

$$N^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad N^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad N^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Therefore, we see that for any invertible $M \in \mathrm{GL}_2(\mathbf{R})$, the order of MNM^{-1} equals 4.

10pt (d) Geef een lijst met alle elementen van de ring $\mathbf{Z}/3[x]$ (de ring van polynomen met coëfficiënten uit de ring $\mathbf{Z}/3$ van gehele getallen modulo 3) die voortbrenger zijn van het hoofdideaal (x).

If f, an element of $\mathbf{Z}/3[X]$, is a generator of the ideal (x), then $(f) = (x)$. For such f, there are some non-zero polynomials $h, g \in \mathbf{Z}/3[X]$ so that

$$f = x \cdot g \text{ and } x = f \cdot h.$$

From $f = x \cdot g$, we see $\deg(f) \geq 1$ and from $x = f \cdot h$, we see that $\deg(f) \leq 1$. Hence, we conclude that if f is a generator of (x), then $\deg(f) = 1$. The list of possible generators f is thus

$$\{x, \overline{2}x\},$$

and it is easy to verify that they are indeed the generators of (x). Alternatively, just use that generators of principal ideals differ by units, and $(\mathbf{Z}/3[X])^* = (\mathbf{Z}/3)^* = \{\overline{1}, \overline{2}\}$.

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

10pt (a) $\mathbf{R}[x]/(x^2+2)$ is geen lichaam.

onwaar: Een quotiëntring is een lichaam desda het ideaal maximaal is. In een Hoofdideaaldomein (HID) is een ideaal maximaal desda een voortbrenger irreducibel is. Omdat $\mathbf{R}$ een lichaam is, is $\mathbf{R}[x]$ een HID. Het ideaal (x^2+2) is irreducibel omdat x^2+2 geen nulpunten heeft in $\mathbf{R}$ (want van graad 2). Conclusie: $\mathbf{R}[x]/(x^2+2)$ is wel een lichaam.

10pt (b) Als $\varphi\colon G \to H$ een surjectief groepshomomorfisme is zodat G van orde 2022 is en de orde van H tussen 500 en 1000 ligt (d.w.z., $|G| = 2022$ en $500 < |H| < 1000$), dan moet H van orde 674 zijn (d.w.z. $|H| = 674$).

waar: De eerste homomorfismestelling zegt dat $|G| = |\varphi(G)| \cdot |\ker(\varphi)|$. Omdat φ surjectief is geldt $|G| = |H| \cdot |\ker(\varphi)|$. Omdat $|G| = 2022 = 2 \cdot 3 \cdot 337$ en $500 < |H| < 1000$ geldt inderdaad $|H| = 2 \cdot 337 = 674$.

10pt (c) Stel dat G een groep is, en er bestaat een surjectief groepshomomorfisme $\varphi\colon G \to \mathbf{Z}/2022$. Dan bestaat er een normale ondergroep in G van index 3.

waar: De groep $\overline{G} = \mathbf{Z}/2022$ bevat als ondergroep $\overline{K} = \mathbf{Z}/674$. Dit is automatisch een normale ondergroep in de abelse groep $\mathbf{Z}/2022$ en hij is van index $[\overline{G} : \overline{K}] = 3$. Vanwege de eerste homomorfismestelling is er dus een corresponderend surjectief groepshomomorfisme $\overline{G} \to \overline{G}/\overline{K} \cong \mathbf{Z}/3$. Als we φ hiermee samenstellen, dan is er dus een surjectief groepshomomorfisme $G \to \mathbf{Z}/3$. De kern K hiervan is een normale ondergroep in G en $G/K \cong \mathbf{Z}/3$ wegens de eerste homomorfismestelling. Dus de uitspraak is waar met de gezochte ondergroep K van index 3.

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

10pt (a) Een polynoom $f \in \mathbf{R}[x]$ van graad 2 (d.w.z. $\deg(f) = 2$) zodat $\mathbf{R}[x]/(f)$ geen domein is.

bestaat wel: Bekijk bijvoorbeeld $f = x^2$. Dan geldt $x \notin (f)$ ($x = x^2 g(x)$ kan niet door graden te vergelijken), maar $x \cdot x \in (f)$, dus is $\overline{x}$ een nuldeler in $\mathbf{R}[x]/(f)$, want $\overline{x} \cdot \overline{x} = \overline{0}$ maar $\overline{x} \neq \overline{0}$. Zulke f bestaat dus.

10pt (b) Een enkelvoudige groep G (d.w.z. een groep met precies twee normale ondergroepen) van even orde $2n$ voor $n > 1$, die werkt op een verzameling X zodat de actie een baan heeft met precies 2 elementen.

bestaat niet: Stel dat $x \in X$ in een baan zit met twee elementen. Wegens de baan-stabilisator-stelling geldt $|G \cdot x| = [G : G_x]$, dus G_x is een ondergroep van G van index 2. Omdat ondergroepen van index 2 altijd normaal zijn, is G_x een normale ondergroep van G. Dan is dus $|G_x| = 2n/2 = n$, en dit is > 1 en $\neq 2n = |G|$, dus zijn $\{e\}, G_x$ en G drie verschillende normale ondergroepen van G.

Vraag 4. Stel dat $R = \{f\colon \mathbf{R} \to \mathbf{R}\}$ de verzameling is van alle functies van $\mathbf{R}$ naar $\mathbf{R}$. Dit is een commutatieve ring met $1 \neq 0$ voor 'puntsgewijs' optellen en vermenigvuldigen, d.w.z. als $f, g \in R$ dan is $f+g$ de functie met $(f+g)(x) := f(x) + g(x)$, en fg de functie met $(fg)(x) := f(x)g(x)$ voor alle $x \in \mathbf{R}$. Stel dat $A \subseteq \mathbf{R}$ een niet-lege verzameling van reële getallen is, en definieer

$$I_A := \{f \in R\colon f(a) = 0 \text{ voor alle } a \in A\} \subseteq R.$$

4pt (a) Bewijs dat I_A een ideaal is in de ring R.

R is een commutatieve ring met $1 \neq 0$. Merk op dat de functie die constant 0 is in I_A zit, dus I_A is niet leeg. Zij nu $f, g \in I_A$ en $h \in R$. Er geldt voor alle $a \in A$ dat

$$(f+g)(a) = f(a) + g(a) = 0 + 0 = 0 \quad \text{en} \quad (fh)(a) = f(a)h(a) = 0 \cdot h(a) = 0,$$

dus $f + g \in I_A$ en $fh \in I_A$. Dit bewijst dat I_A een ideaal is in R.

3pt (b) Voor welke A is I_A een priemideaal?

I_A is een priemideaal dan en slechts dan als $|A| = 1$.

Stel eerst dat $|A| = 1$, nu kunnen we dus schrijven $A = \{a\}$. Stel $f, g \in R$ met $fg \in I_A$. Omdat $fg \in I_A$ volgt er dat $f(a)g(a) = (fg)(a) = 0$, dit impliceert dat $f(a) = 0$ of $g(a) = 0$. In het eerste

geval volgt dat $f \in I_A$ en in het tweede geval volgt $g \in I_A$. We concluderen dus dat in dit geval I_A inderdaad een priemideaal is.

Stel nu dat $|A| > 1$. Zij $a \in A$, we weten nu dat $A \setminus \{a\}$ niet leeg is. Neem $f, g \in R$ met

$$f(x) = \begin{cases} 0 & \text{als } x = a, \\ 1 & \text{anders,} \end{cases}$$

$$g(x) = \begin{cases} 1 & \text{als } x = a, \\ 0 & \text{anders} \end{cases}$$

voor alle $x \in \mathbf{R}$. Merk op dat f en g beide niet in I_A zitten, maar dat het product voldoet aan $(fg)(x) = 0$ voor alle $x \in \mathbf{R}$, dus dit zit wel in I_A. We concluderen dat I_A niet priem is als $|A| \neq 1$.

3pt

(c) Bewijs dat R geen Noetherse ring is, d.w.z., bewijs dat er in R een oneindig lange stijgende keten van verschillende idealen bestaat $I_1 \subset I_2 \subset I_3 \ldots$.

Bekijk, voor elke $i \in \mathbf{Z}_{>0}$, de verzameling $A_i := \mathbf{R} \setminus \{1, \ldots, i\}$. Merk op dat voor alle $i \in \mathbf{Z}_{>0}$ geldt dat $A_{i+1} \subseteq A_i$, hieruit volgt, met de definitie van I_A, dat $I_{A_i} \subseteq I_{A_{i+1}}$. Bekijk voor elke i ook de functie $f_i \in R$ gedefinieerd door

$$f_i(x) = \begin{cases} 1 & \text{als } x = i + 1, \\ 0 & \text{anders} \end{cases}$$

voor alle $x \in \mathbf{R}$. Er geldt dat $f_i \in I_{A_{i+1}}$, maar $f_i \notin I_{A_i}$. We zien dus dat $I_{A_i} \neq I_{A_{i+1}}$, en dus vormen de idealen $I_{A_1} \subset I_{A_2} \subset \cdots$ een oneindige keten van verschillende idealen in R. De ring R is dus niet Noethers.