Oefeningenexamen Algebra I — 8 januari 2024

Veel succes!

Op dit examen onderstellen we steeds dat ringen commutatief met eenheid zijn.

Opgave 1. Zij G een eindige groep. We zeggen dat een echte, niet-triviale, deelgroep $1 < H < G$ eigenschap $(\star)$ heeft indien $H \cap H^g = 1$ voor alle elementen $g \in G \setminus H$.

(i) Zij $1 < A < G$ een echte deelgroep die voldoet aan $(\star)$. Zij $X = G \setminus \bigcup_{g\in G} A^g$. Toon aan dat $|X| = |G|/|A| - 1$.

(ii) Stel $1 < B < G$ nog een echte deelgroep die voldoet aan $(\star)$. Toon aan dat er een element $g \in G$ bestaat zodat $A \cap B^g \neq 1$.

(iii) Zij $A \leq N \leq G$ een willekeurige deelgroep die A bevat, met A zoals in (i). Gegeven $g \in G$, toon aan dat als $A^g \cap N > 1$, dat $g \in N$. Concludeer dat als $N \trianglelefteq G$, dan $N = G$.
Hint: toon aan dat $A^g \cap N$ voldoet aan eigenschap $(\star)$ als deelgroep van N.

Oplossing:

(i) Noem $n = [G : A]$. Zij $g, h \in G$ zo dat $A^g = A^h$. Dit kan enkel als $A = A^{gh^{-1}}$, of dus door $(\star)$ als $gh^{-1} \in A$. Ofwel, $A^g = A^h$ als en slechts als g en h in dezelfde rechtse nevenklasse van A bevat zijn. Dus geldt $\bigcup_{g\in G} A^g = A^{g_1} \cup \cdots \cup A^{g_n}$, waarbij $\{g_1, \ldots, g_n\}$ een verzameling representanten is van de rechtse nevenklassen van A. Nu hebben deze deelgroepen twee aan twee een triviale doorsnede, want $\left|A^g \cap A^h\right| = \left|A \cap A^{hg^{-1}}\right| = 1$ voor elke $g, h \in G$ zo dat $gh^{-1} \notin A$. Daardoor bevat $\bigcup_{g\in G} A^g$ juist $n \cdot (|A| - 1)$ niet-triviale elementen, en dus is $|X| = |G|/|A| - 1$.

(ii) Neem aan dat $A \cap B^g = 1$ voor alle $g \in G$. Dan geldt zoals in (i) dat $A^g \cap B^h = 1$ voor alle $g, h \in G$. Met andere woorden geldt $\left(\bigcup_{g\in G} A^g\right) \cap \left(\bigcup_{g\in G} B^g\right) = 1$. Dit geeft ons dat de unie van deze twee verzamelingen minstens $k = 2|G| - |G|/|A| - |G|/|B| + 1$ elementen bevat. Maar als $|A|, |B| \geq 2$ hebben we dat $k > |G|$, een strijdigheid.

(iii) Je kan A en $H = A^g \cap N$ gebruiken als deelgroepen met eigenschap $(\star)$ van N . Het is meteen duidelijk dat $A \leq N$ eigenschap $(\star)$ heeft als deelgroep van N. De deelgroep $H \leq N$ heeft eigenschap $(\star)$ omdat voor elke $n \in N \setminus A$ geldt dat $(A^g \cap N)^n \cap (A^g \cap N) \leq A^g \cap A^{gn} = A \cap A^{gng^{-1}}$. De laatste doorsnede is triviaal, want $gng^{-1} \notin A$ omdat $n \notin A^g$. Dan volgt uit het vorige puntje dat er een $h \in N$ bestaat met $A \cap (A^g \cap N)^h > 1$. Dit is enkel mogelijk als $g = h^{-1}$, en dus is $g \in N$. De conclusie volgt dan ook, want als N een normaaldeler is, geldt voor elke $g \in G$ dat $A^g \leq N^g = N$, en dus $g \in N$.

Opgave 2. Zij G een deelgroep van $\mathbf{S}_5$ die transitief werkt op $\{1, \ldots, 5\}$. In deze oefening mag je gebruikmaken van het feit dat de enige echte niet-triviale normaaldeler van $\mathbf{S}_5$ juist $\mathbf{A}_5$ is.

(i) Toon aan dat als $G \neq \mathbf{A}_5, \mathbf{S}_5$, dan geldt dat $[\mathbf{S}_5 : G] \geq 5$.
Hint: beschouw de actie op de rechtse nevenklassen.

(ii) Toon aan dat G een deelgroep $\langle\sigma\rangle$ van orde 5 heeft.

(iii) Toon aan dat als $G \neq \mathbf{A}_5, \mathbf{S}_5$, dat $G \leq N_{\mathbf{S}_5}(\langle\sigma\rangle) = H$.
Hint: Beschouw $\mathrm{Syl}_5(G)$.

(iv) Toon aan dat H een groep van orde 20 is.

(v) Toon aan dat G isomorf is aan één van de volgende groepen:
(a) $\mathbf{S}_5$, (b) $\mathbf{A}_5$, (c) De groep $A = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(\mathbb{F}_5) \,\middle|\, a \in \mathbb{F}_5^\times, b \in \mathbb{F}_5 \right\}$, (d) $\mathbf{D}_{10}$, (e) $\mathbf{C}_5$.

Oplossing:

(i) Beschouw de actie van $\mathbf{S}_5$ op rechtse nevenklassen $\{Gg \mid g \in \mathbf{S}_5\}$ door middel van rechtse vermenigvuldiging. De kern van deze actie (noem deze N) fixeert in het bijzonder de triviale nevenklasse G, en dus geldt $N \leq G$. Maar de enige normaaldelers van $\mathbf{S}_5$ zijn $\{e\}, \mathbf{A}_5$ en $\mathbf{S}_5$. Door de onderstelling in de opgave moet de kern dan triviaal zijn. De groep $\mathbf{S}_5$ werkt dus getrouw op $R_{\mathbf{S}_5}(G)$, dus moet in het bijzonder ook $5! \leq ([\mathbf{S}_5 : G])!$. Met andere woorden, $5 \leq [\mathbf{S}_5 : G]$.

(ii) De groep G werkt transitief op een verzameling van 5 elementen. Volgens de baanstabilisatorformule is 5 een deler van $|G|$. Uit de stelling van Cauchy volgt dat G een deelgroep van orde 5 heeft.

(iii) We moeten aantonen dat $\langle\sigma\rangle$ een normaaldeler is in G. We weten uit (i) dat $|G| \leq 24$ en uit (ii) dat $5 \mid |G|$. Dit impliceert $|G| = 5k$ met $1 \leq k \leq 4$. Dan moet $n_5(G) \mid k$ en $n_5(G) \cong 1 \pmod 5$. Uit het eerste volgt $n_5(G) \leq 5$ en uit het tweede dus $n_5(G) = 1$.

(iv) Oplossing 1:

Merk op dat σ noodzakelijk een 5-cykel is, en H voldoet aan de voorwaarden voor (i). De orde van H is dus hoogstens 20. Als we $\sigma = (1\,2\,3\,4\,5)$ stellen, vinden we eenvoudig een element van orde 4 dat in H bevat zit, bijvoorbeeld $\rho = (2\,3\,5\,4)$, want $\sigma^\rho = \sigma^2$. We hebben dat $4 \mid |H|$. Hieruit volgt het gewenste.

Oplossing 2:

Merk op dat σ noodzakelijk een 5-cykel is. De baanstabilisatorformule geeft $|C_{\mathbf{S}_5}(\sigma)| = |\mathbf{S}_5|/|\sigma^G| = 5!/4! = 5$. De normalisator heeft dan orde 20, omdat $\langle\sigma\rangle$ juist 4 elementen van orde 5 bevat, die allemaal toegevoegd zijn. De index van de centralisator in de normalisator is dus 4. Merk op dat deze redenering ook werd toegepast in Huistaak 2, Oefening 3.

(v) We onderstellen dat $G \neq \mathbf{A}_5, \mathbf{S}_5$. Dan is de orde van G gelijk aan $20, 10$ of 5. Merk op dat orde 15 niet meer kan, wegens de stelling van Lagrange. Indien G orde 5 is, dan geldt geval (e). Indien G orde 10 heeft, dan is $G \cong C_{10}$ of $G \cong D_{10}$. Maar in $\mathbf{S}_5$ bestaan we geen elementen van orde 10, dus dan moet $G \cong D_{10}$. Indien G orde 20 heeft, moet $G = H$. Er rest nog te bewijzen dat $H \cong A$. Je kan dit doen door de actie van A op $\mathbb{F}_5$ te beschouwen: matrixvermenigvuldiging met een kolomvector $\begin{pmatrix} x \\ 0 \end{pmatrix}$ geeft $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} ax+b \\ 0 \end{pmatrix}$. Dit is een getrouwe actie van A op 5 elementen, die in het bijzonder ook transitief is, en dus is $H = A$.

Opgave 3. Zij $R = \mathbb{Z}[x]$. We weten hoe de priemidealen eruitzien die ook een hoofdideaal zijn, want dit zijn juist de idealen voortgebracht door priemelementen. We willen de andere priemidealen ook begrijpen.

(i) Zij $p \in \mathbb{N}$ een priemgetal, en f een veelterm wiens beeld $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ modulo p irreduciebel is. Toon aan dat het ideaal $(p, f) \trianglelefteq \mathbb{Z}[x]$ een maximaal ideaal is dat geen hoofdideaal is.

(ii) Zij P een priemideaal dat geen hoofdideaal is. Toon aan dat $P \cap \mathbb{Z} \neq \{0\}$.
Hint: Werk vanuit het ongerijmde, en maak gebruik van het hoofdideaaldomein $\mathbb{Q}[x] \supseteq \mathbb{Z}[x]$.

(iii) Maak gebruik van het vorige puntje om aan te tonen dat elk priemideaal ofwel een hoofdideaal is, ofwel van de vorm (p, f) is met p en f zoals in (i).
Hint: Toon eerst aan dat $P \cap \mathbb{Z}$ *een priemideaal is van* $\mathbb{Z}$.

Oplossing:

(i) We beschouwen de quotientruimte $Z[x]/(p, f)$. Merk op dat dit isomorf is aan $\mathbb{Z}/p\mathbb{Z}[x]/(f)$. Uit Discrete Wiskunde I, Sectie 5.8.2 weten we dan dat dit een veld is, precies omdat f irreduciebel is over $\mathbb{Z}/p\mathbb{Z}$. Indien je niet wil verwijzen naar Discrete Wiskunde: f is irreduciebel in het hoofdideaaldomein $\mathbb{Z}/p\mathbb{Z}[x]$, en dus brengt het een maximaal ideaal voort. Dit is geen hoofdideaal. Inderdaad, mocht (p, f) een hoofdideaal zijn, dan zou het voortgebracht zijn door een geheel getal. Dit getal moet dan noodzakelijk p zijn, want enerzijds $p \in (p, f)$, en anderzijds als $k \in \mathbb{Z} \cap (p, f)$, dan geldt $p \mid k$. Maar $f \notin (p)$, een strijdigheid.

(ii) Stel $P \cap \mathbb{Z} = 0$ en beschouw het ideaal $Q \coloneqq P\mathbb{Q}[x]$ voortgebracht door P in $\mathbb{Q}[x]$. Merk op dat Q een hoofdideaal is. Het ideaal Q is niet gelijk aan heel $\mathbb{Q}[x]$, precies omdat $P \cap \mathbb{Z} = 0$. Elk element $r \in Q$ heeft dus $\deg(r) > 0$. We weten dus dat $Q = (f)$ voor een niet-constant polynoom $f \in \mathbb{Q}[x]$. Merk op dat we $f \in \mathbb{Z}[x]$ primitief kunnen kiezen, omdat de content van f een eenheid is in $\mathbb{Q}[x]$. We hoeven nu enkel nog te bewijzen dat $f \in P$. We kunnen $f = h \cdot q$ schrijven, met $h \in P$ en $q \in \mathbb{Q}[x]$. Maar $h \in (f) \trianglelefteq \mathbb{Q}[x]$, dus geldt $\deg(h) \geq \deg(f) > 0$. Dit is enkel mogelijk als $q \in \mathbb{Q}$ en $\deg(h) = \deg(f)$. Omdat we f primitief gekozen hebben, moet dan ook $q \in \mathbb{Z}$ door Lemma 2.8.2 (en de discussie die er op volgt). Omdat ook $h \in \mathbb{Z}[x]$ volgt dan ook dat $q = \pm 1$, door grootste gemene delers van de coëfficiënten in linkerlid en rechterlid te vergelijken. Dit bewijst $P = (f) \trianglelefteq \mathbb{Z}[x]$.

(iii) Uit het vorige puntje weten dat voor een priemideaal P dat geen hoofdideaal is geldt dat $P \cap \mathbb{Z} \neq 0$. Dit is duidelijk een echt priemideaal van $\mathbb{Z}$. We kunnen dus onderstellen dat $p\mathbb{Z} = P \cap \mathbb{Z}$ voor een zeker priemgetal p. Nu is P geen hoofdideaal, dus is $P \setminus (p) \neq \emptyset$. We kunnen dus $f \in P \setminus (p)$ kiezen met $\deg(f)$ minimaal in $P \setminus (p)$. We bewijzen nu dat f irreduciebel is modulo p. Inderdaad, stel dat f niet irreduciebel is modulo p, dan bestaan $g, h \in \mathbb{Z}/p\mathbb{Z}[x]$ met $\deg g, \deg h < \deg f$ zodat $f \equiv gh \pmod{p}$, ofwel $f + (p) = gh + (p)$. Dit impliceert $gh \in P \setminus (p)$, en dus (zonder verlies van algemeenheid) $g \in P \setminus (p)$, strijdig met de minimaliteit van $\deg(f)$. Nu geldt $(p, f) \subseteq P$, maar uit maximaliteit van (p, f) (zie (i)) volgt dat $(p, f_0) = P$.

Opgave 4. Zij R een ring, M een eindig voortgebracht R-moduul, voortgebracht door $\{v_1, \ldots, v_n\}$, en $J \trianglelefteq R$ een ideaal zodat $JM = M$.

(i) Toon aan dat er een $n \times n$ matrix $A \in M_n(R)$ bestaat met matrixcoefficiënten bevat in J zodat
$$(I_n - A) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0.$$

(ii) Toon aan dat $\det(I_n - A) = 1 + \alpha$ met $\alpha \in J$.

(iii) Toon aan dat $(-\alpha) \cdot v = v$ voor alle $v \in M$.

(iv) Zij nu M een getrouw R-moduul (dit wil zeggen dat als $r \in R$ zodat $rM = 0$, dat dan $r = 0$). Toon aan dat $J = R$.

Oplossing:

(i) Omdat $JM = M$ weten we dat $v_i = \sum_j a_{ij} v_j$, voor zekere $a_{ij} \in J$. Beschouwen we $A \coloneqq (a_{ij})_{i,j}$, dan zien we dat $A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, of dus $(I_n - A) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0$.

(ii) De tekenformule voor de determinant wordt gegeven door $\det(I_n - A) = \sum_{\sigma \in \mathbf{S}_n} \operatorname{sgn}(\sigma)(I_n - A)_{1,\sigma(1)}(I_n - A)_{2,\sigma(2)} \ldots (I_n - A)_{n,\sigma(n)}$. Om dit modulo J te berekenen, kunnen we elk product waar minstens 1 van de termen in J bevat is negeren. Dit betekent dat $\det(I_n - A) = (1 - a_{11}) \ldots (1 - a_{nn}) \pmod{J}$. Omdat $a_{ii} \in J$, geldt dus $\det(I_n - A) = 1 \pmod{J}$. Deze redenering lijkt sterk op die in Lemma 2.9.4(ii).

(iii) Dit volgt uit de stelling van Cayley Hamilton, uitgevoerd op $B = I_n - A$. Inderdaad, we weten dat $\chi_B(B) = 0$, en dus ook dat $\chi_B(B) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0$. Maar uit (i) volgt dat dit ook gelijk is aan $\begin{pmatrix} \det(B)v_1 \\ \vdots \\ \det(B)v_n \end{pmatrix}$. Dus $\det(B) = 1 + \alpha$ annihileert M, en het gestelde volgt.

(iv) $1 + \alpha$ annihileert M, dus $-1 = \alpha$. Hieruit volgt meteen dat $J = R$.