

Examen Algebraïsche Structuren – 20 juni 2024

Het examen was zoals de afgelopen paar jaren gesplitst in een deel theorie (gesloten boek) en een oefeningendeel (open boek). De richtlijn voor tijdsduur voor de theorievragen werd op 45 minuten gesteld; in totaal bedroeg de examentijd drie uur.

Theorie

- Geef en bewijs de stelling van Sylvester voor reële bilineaire ruimtes.
- Geef en bewijs de stelling van Bézout-Bachet. Wees duidelijk in je uitleg en notatie.

Oefeningen

Vraag 1 (10 punten)

- (2 ptn.) Zij $x \in \mathbb{Z}$, met $5x^3 + 1 \equiv 0 \pmod{2}$. Toon aan: $\text{ggd}(x, 2) = 1$.
- (8 ptn.) Bepaal alle oplossingen $x \in \mathbb{Z}$ van het stelsel

$$\begin{cases} 5x^3 + 1 & \equiv 0 \pmod{6} \\ 26x^{25} + x^8 + 1 & \equiv 0 \pmod{112}. \end{cases}$$

Hint: $112 = 16 \cdot 7$.

Vraag 2 (10 punten)

Zij $G, *$ een niet-Abelse groep van orde $2p$, waarbij p een priemgetal verschillend van twee is.

- (1 pt.) Bestaan er voorbeelden van zulke groepen die cyclisch zijn?
- (3 ptn.) Zij $K, \diamond$ een groep waarvoor geldt dat $\forall k \in K : k^2 = e_K$. Toon aan dat K Abels is.
- (3 ptn.) Toon aan dat G een deelgroep H heeft die orde p heeft.
- (3 ptn.) Toon aan dat voor elk element $g \in G$ geldt dat $g^2 \in H$ (met H de deelgroep van in de deelvraag hierboven).

Vraag 3 (10 punten)

Zij $B : V \times V \rightarrow K$ een bilineaire vorm over een eindigdimensionale vectorruimte V over het veld K . Veronderstel dat de rang van B gelijk is aan de dimensie van V .

- (3 ptn.) Toon aan dat $L_B : V \rightarrow V^* : v \mapsto B(-, v)$ een isomorfisme van vectorruimten is. Deze oefening vloeit voort uit oefening 11 van hoofdstuk 5; je hoeft dus niet meer aan te tonen dat de afbeelding lineair is.
- (3 ptn.) Zij $W \subseteq V$ een deelruimte van V . We definiëren het B -complement van W als volgt:

$$W^B := \{v \in V \mid \forall w \in W : B(w, v) = 0\}.$$

Toon aan dat W^B een deelruimte van V is, en dat $L_B(W^B) = \{f \in V^* \mid \forall w \in W : f(w) = 0\}$.

- (4 ptn.) Zij $W \subseteq V$ opnieuw een deelruimte van V . Toon aan dat

$$\dim_K(W) + \dim_K(W^B) = \dim_K(V).$$

Hint: neem eerst een basis voor W , en breid deze daarna uit tot een basis van V .

Oplossingen van oefeningen

Vraag 1

- a. Via $5x^3 + 1 \equiv 0 \pmod{2}$ bekom je $5x^3 \equiv 1 \pmod{2}$, dus $5x^{3 \bmod \varphi(2)} \equiv 1 \pmod{2}$, dus $5x \equiv 1 \pmod{2}$, dus $x \equiv 1 \pmod{2}$.
- b. We zetten een aantal stappen om de gegeven vergelijkingen wat te vereenvoudigen. Allereerst volgt uit $\phi(6) = 2$ dat $5x^3 + 1 \equiv 0 \pmod{6}$ te reduceren valt tot $-x + 1 \equiv 0 \pmod{6}$, ofwel $x \equiv 1 \pmod{6}$. We schrijven x als $6k + 1$, met $k \in \mathbb{Z}$.
We gebruiken de nuttige hint om de andere vergelijking op te splitsen in priemfactoren; immers is

$$26x^{25} + x^8 + 1 \equiv 0 \Leftrightarrow \begin{cases} 26x^{25} + x^8 + 1 \equiv 0 \pmod{16} \\ 26x^{25} + x^8 + 1 \equiv 0 \pmod{7} \end{cases}$$

In de vergelijking modulo 7 valt heel wat te schrappen: $\phi(7) = 6$, dus dat wordt $5x + x^2 + 1 \equiv 0 \pmod{7}$. We vullen $x = 6k + 1$ in: $30k + 5 + 36k^2 + 12k + 1 \equiv k^2 \pmod{7} \equiv 0 \pmod{7}$, dus k valt te schrijven als $7l$, met $l \in \mathbb{Z}$. Daaruit krijgen we dat $x = 42l + 1$.

We vervolgen onze bittere tocht doorheen het Woud Der Vereenvoudigingen met de volgende vergelijking: $26x^{25} + x^8 + 1 \equiv 0 \pmod{16}$. Aangezien $\phi(16) = 8$ schaven we weg tot $10x + x^8 + 1 \equiv 0 \pmod{16}$. We vullen nu $x = 42l + 1$ in:

$$420l + 10 + (42l + 1)^8 + 1 \equiv 0 \pmod{16}$$

$$\begin{aligned} 4l + (10l + 1)^8 + 11 &\equiv 4l + (100l^2 + 20l + 1)^4 + 11 \\ &\equiv 4l + (4l^2 + 4l + 1)^4 \\ &\equiv 4l + (\cancel{16l^4} + \cancel{16l^3} + 4l^2 + \cancel{16l^3} + \cancel{16l^2} + 4l + 4l^2 + 4l + 1)^2 + 11 \\ &\equiv 4l + (8l^2 + 8l + 1)^2 + 11 \\ &\equiv 4l + (\cancel{64l^4} + \cancel{64l^3} + 8l^2 + \cancel{64l^3} + \cancel{64l^2} + 8l + 8l^2 + 8l + 1) + 11 \\ &\equiv 4l + 12 \equiv 0 \pmod{16} \end{aligned}$$

Na al dit gezever vinden we dat $l = 4m + 1$, met $m \in \mathbb{Z}$. Dit kunnen we tenslotte invullen in $x = 1 + 42l$ om te bekomen dat $x = 43 + 168m$. Dit is de uiteindelijke uitkomst.

Vraag 2

- a. Neen; elke cyclische groep is immers Abels, aangezien elke cyclische groep isomorf is aan ofwel $\mathbb{Z}$ ofwel $\mathbb{Z}_n$.
- b. Een directe edoch ietwat lompe methode om dit aan te tonen is als volgt: Aangezien $\forall k \in K : k^2 = e$, hebben we $k = k^{-1}$ voor elk element. Kies nu $a, b \in K$ willekeurig. Noem $a * b = g$. Dan geldt $a = gb^{-1}$ en $e = gb^{-1}a^{-1}$, dus $g^{-1} = b^{-1}a^{-1}$. Elk element is zijn eigen invers, dus inverteren we elk element om $g = b * a$ te bekomen.
Dus $a * b = g = b * a$ voor alle $a, b \in G$.
- c. Een manier om dit te doen: Kies een element uit G zodat $g^2 \neq e$. Als dit niet mogelijk zou zijn (m. a. w. als elk element $g \in G$ de eigenschap zou hebben dat $g^2 = e$), zou G zoals in deelvraag b aangetoond werd Abels zijn; dit is echter niet het geval, dus bestaat er altijd zo'n element g .
Beschouw nu $H := \langle g \rangle$. Duidelijk is dat $H \subset G$. We willen aantonen dat de orde van H gelijk is aan p .

Deelgroepen van G moeten wegens de stelling van Lagrange een orde hebben die een deler is van $\#G$, dus van $2p$. Aangezien p priem en strikt groter dan twee is, zijn dus enkel deelgroepen van orde 1, 2, p of $2p$ mogelijk.

- $\#H \neq 1$, want dan zou $H = \{e\}$ en dat is per constructie niet het geval (immers is $e^2 = e$).

- $\#H \neq 2$, want dan zou $H = \{e, g\}$ en dan zou $g^2 = e$, wat dus opnieuw per constructie niet kan gebeuren.
- $\#H \neq 2p$, want dan zou H de volledige groep G zijn, maar ook voortgebracht door g en dus cyclisch zijn; zoals in deelvraag a aangetoond is kan dat niet.

De enige mogelijkheid die ons rest is dus dat de orde van H gelijk is aan p , waarmee de stelling aangetoond is.

- d. Kies een $g \in G$ willekeurig.

Als $g \in H$, volgt $g^2 \in H$ direct uit het feit dat H een deelgroep is.

Als $g \notin H$, is er – wegens de stelling van Lagrange, die ons leert dat $[G : H] = 2$ – exact één linkernevenklasse die niet H zelf is; deze is precies gH . Als nu $g^2 \in gH$ vinden we een $h \in H$ zodat $g^2 = gh$, ofwel zodat $g = h$. Dit is een contradictie, want per constructie geldt $g \notin H$. Dus moet gelden dat $g^2 \in H$.

Vraag 3

- a. Aangezien we lineariteit niet meer aan hoeven te tonen, rest ons slechts te bewijzen dat L_B zowel injectief als surjectief is. Gelukkig is dit nogal een meevallertje, aangezien we gegeven krijgen dat $\text{rang}(B) = \dim_K(V)$. De dimensiestelling voor lineaire afbeeldingen doet het werk praktisch voor ons: $\dim_K(\ker L_B) = \dim_K(V) - \dim_K(\text{im } L_B) = \dim_K(V) - \text{rang}(B) = 0$. Aangezien de kern van L_B dus enkel uit de nulvector bestaat is de afbeelding injectief. Surjectiviteit aantonen gaat eveneens vlotjes: we willen aantonen dat $\forall \ell \in V^* : \exists v \in V : L_B(v) = \ell$, ofwel dat $\exists v \in V : \forall w \in V : L_B(v)(w) = B(w, v) = \ell(w)$. Aangezien de matrix M van B tegenover eender welke basis van volle rang is, heeft het homogene stelsel $Mw = v$ slechts de unieke oplossing. Hieruit volgt dat de afbeelding surjectief is.
- b. De directste manier is hier waarschijnlijk gewoon gebruik maken van het deelgroepecriterium. Kies daartoe twee vectoren $v, w \in V$ en twee scalaren $\lambda, \mu \in K$. We willen aantonen dat $v \in W^B \wedge w \in W^B \Rightarrow (\lambda v + \mu w) \in W^B$. Dit gaat zeer vlotjes omdat B bilineair is:

$$\begin{aligned} v \in W^B \wedge w \in W^B &\Leftrightarrow \forall x \in W : B(x, v) = 0 \wedge B(x, w) = 0 \\ &\Leftrightarrow \forall x \in W : B(x, \lambda v) = 0 \wedge B(x, \mu w) = 0 \\ &\Rightarrow \forall x \in W : B(x, \lambda v) + B(x, \mu w) = 0 \\ &\Leftrightarrow \forall x \in W : B(x, \lambda v + \mu w) = 0 \\ &\Leftrightarrow (\lambda v + \mu w) \in W^B. \end{aligned}$$

Aantonen dat het beeld van W^B onder L_B gelijk is aan $\{f \in V^* \mid \forall x \in W : f(x) = 0\}$ gaat nu bijna vanzelf, aangezien we precies de functionen wiens kern W omvat beschrijven.

- c. Zij $\mathcal{W} = \{w_1, w_2, \dots, w_n\}$ een basis van W , en $\mathcal{V} = \{w_1, \dots, w_n, v_1, \dots, v_m\}$ diezelfde basis uitgebreid tot een basis van heel V . Zij $\Phi : V \rightarrow V^{**} : v \mapsto \text{ev}_v$ het canonieke isomorfisme. Beschouw dan

$$f : V^* \rightarrow \Phi(W) : \ell \mapsto \sum_{w_i \in \mathcal{W}} \text{ev}_{w_i}(\ell) \text{ev}_{w_i}.$$

Dan $\ker f = \{\ell \in V^* \mid \forall w_i \in \mathcal{W} : \ell(w_i) = 0\}$. Omdat $\mathcal{W}$ een basis en dus in het bijzonder voortbrengend is, kunnen we dit herschrijven als $\{\ell \in V^* \mid \forall w \in W : \ell(w) = 0\}$; dit is precies $L_B(W^B)$.

We beschouwen nu W^* , de opspanning van coördinaatafbeeldingen van W . Er is geen canonieke manier om dit te doen. Dit is waarom we een basis van V moeten kiezen, opdat V^* een welbepaalde basis zou hebben (waardoor we W^* als deelruimte van V^* kunnen beschouwen).

We hebben dan dat

$$\begin{aligned}
\operatorname{im} f &\supset f(W^*) \\
&= \operatorname{vct} f(\{w_i^* \mid i = 1, \dots, n\}) \\
&= \operatorname{vct} \{\ell(v_{w_i}) \mid i = 1, \dots, n\} \\
&= \operatorname{vct} \Phi(w_i) \\
&= \Phi(\operatorname{vct} w_i) \\
&= \Phi(W)
\end{aligned}$$

De dimensiestelling leert ons dan dat $\dim V^* = \dim \Phi(W) + \dim L_B(W^B)$. Aangezien isomorfismen dimensie behouden, geldt $\dim V = \dim W + \dim W^B$.