Ringen en Lichamen - Opdracht 1

Luc Veldhuis - 2538227

September 2017

Q1) Zij $\omega = e^{2\pi i/3}$ in $\mathbb{C}$ en $R = \{a + b\omega \text{ met } a, b \text{ in } \mathbb{Z}\}$.

(a) Laat zien dat R een deelring van $\mathbb{C}$ is en dat $\mathbb{Z}[\sqrt{-3}] \subsetneq R$.
Een deelring van $\mathbb{C}$ is een deelgroep van $\mathbb{C}$ die gesloten is onder multiplicatie.
Het voldoet om te controleren of R gesloten is onder subtractie en multiplicatie en niet leeg is.
Opmerking: We zien direct dat $R \subseteq \mathbb{C}$, omdat $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$, en alle elementen in R van deze vorm moeten zijn.
Omdat $\mathbb{C}$ een commutatieve ring is (zie boek) mogen we eigenschappen zoals commutatieve additie, associativiteit en distributiviteit gebruiken.

- Bewijs niet leeg:
  $1 \in R$, voor $a = 1$, $b = 0$. Dus R is niet leeg.
- Bewijs gesloten onder subtractie:
  Neem 2 willekeurige elementen $\alpha, \beta \in R$ met $\alpha = a+b\omega$ en $\beta = c+d\omega$ voor $a, b, c, d \in \mathbb{Z}$.
  Dan geldt $\alpha - \beta = a + b\omega - (c + d\omega) = a - c + b\omega - d\omega = (a - c) + (b - d)\omega$.
  Omdat we hebben dat $a - c \in Z$ en $b - d \in \mathbb{Z}$, hebben we weer een vergelijking van de vorm $x + y\omega$ met $x = a - c$, $y = b - d$ voor $x, y \in \mathbb{Z}$, dus $(\alpha - \beta) \in R$ voor elke willekeurige α, β. Dus R is gesloten onder subtractie.
- Bewijs gesloten onder multiplicatie:
  Neem 2 willekeurige elementen $\alpha, \beta \in R$ met $\alpha = a+b\omega$ en $\beta = c+d\omega$ voor $a, b, c, d \in \mathbb{Z}$.
  We weten ook dat $\omega = e^{2\pi i/3}$, dus $\omega^2 = (e^{2\pi i/3})^2 = e^{4\pi i/3} = \cos(4\pi/3) + i\sin(4\pi/3) = \cos(-2\pi/3) + i\sin(-2\pi/3) = -\frac{1}{2} - i\sin(2\pi/3) = -(\frac{1}{2} + i\sin(2\pi/3)) = -(1 - \frac{1}{2} + i\sin(2\pi i/3)) = -(1 + e^{2\pi i/3}) = -1 - e^{2\pi i/3} = -1 - \omega$.
  Dan geldt $\alpha\beta = (a + b\omega)(c + d\omega) = ac + ad\omega + b\omega c + b\omega d\omega = ac + (ad + bc)\omega + bd\omega^2$.
  $ac+(ad+bc)\omega+bd\omega^2 = ac+(ad+bc)\omega+bd(-1-\omega) = ac+(ad+bc)\omega+-bd-bd\omega) = (ac - bd) + (ad + bc - bd)\omega$.
  Omdat we weten dat $a, b, c, d \in \mathbb{Z}$, weten we dat $ac, bd, ad, bc \in \mathbb{Z}$ en dus ook $(ac - bd), (ad + bc - bd) \in \mathbb{Z}$. Dus $(ac - bd) + (ad + bc - bd)\omega \in R$, dus R is gesloten onder multiplicatie.

Omdat R aan alle eisen voldoet, is R een deelring van $\mathbb{C}$.
Bewijs $\mathbb{Z}[\sqrt{-3}] \subsetneq R$:
We moeten laten zien dat $Z[\sqrt{-3}]$ een deelring is, maar niet gelijk is aan R.
We laten eerst zien dat $Z[\sqrt{-3}]$ een deelverzameling is van R. We weten dat $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\} = \{a + bi\sqrt{3} | a, b \in \mathbb{Z}\}$.
Ook weten we dat $e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$.
Dus we kunnen R schrijven als $R = \{a - b\frac{1}{2} + b\frac{1}{2}i\sqrt{3} | a, b \in \mathbb{Z}\}$.
Neem nu een willekeurig element $x \in \mathbb{Z}[\sqrt{-3}]$ met $x = a + bi\sqrt{3}$ voor $a, b \in \mathbb{Z}$.
Neem nu het element $y = c + d\omega = c - \frac{1}{2}d + di\frac{1}{2}\sqrt{3}$ met $d = 2b$ en $c = a - b$.

Dan geldt $y = a + b - \frac{1}{2}2b + 2b\frac{1}{2}i\sqrt{3} = a + bi\sqrt{3} = x$. Omdat $d = 2b \in \mathbb{Z}$ en $c = a + b \in \mathbb{Z}$ geldt dat $y \in R$ zit, en dus ook $y = x \in R$, voor alle $x \in \mathbb{Z}[\sqrt{-3}]$. Dus $\mathbb{Z}[\sqrt{-3}] \subset R$.
Nu moeten we laten zien dat $\mathbb{Z}[\sqrt{-3}]$ niet leeg is en gesloten is onder subtractie en multiplicatie.

- Bewijs niet leeg:
  $1 \in \mathbb{Z}[\sqrt{-3}]$ voor $a = 1$, $b = 0$. Dus niet leeg.
- Bewijs gesloten onder subtractie:
  $(a + bi\sqrt{3}), (c + di\sqrt{3}) \in \mathbb{Z}[\sqrt{-3}]$ met $a, b, c, d \in \mathbb{Z}$.
  Dan geldt $(a + bi\sqrt{3}) - (c + di\sqrt{3}) = (a - c) + (b - d)i\sqrt{3}$. En $a - c \in \mathbb{Z}$, $b - d \in \mathbb{Z}$, dus $(a - c) + (b - d)i\sqrt{3} \in \mathbb{Z}[\sqrt{-3}]$.
  Dus gesloten onder subtractie.
- Bewijs gesloten onder multiplicatie:
  $(a + bi\sqrt{3}), (c + di\sqrt{3}) \in \mathbb{Z}[\sqrt{-3}]$ met $a, b, c, d \in \mathbb{Z}$.
  Dan geldt $(a+bi\sqrt{3})(c+di\sqrt{3}) = ac+adi\sqrt{3}+bci\sqrt{3}-3bd = (ac-3bd)+(ad+bc)i\sqrt{3}$.
  En $ac, 3bd, ac, bc \in \mathbb{Z}$ dus ook $ac - 3bd, ad + bc \in \mathbb{Z}$, dus $(ac - 3bd) + (ad + bc)i\sqrt{3} \in \mathbb{Z}[\sqrt{-3}]$.
  Dus gesloten onder multiplicatie.

Nu moeten we nog laten zien dat $\mathbb{Z}[\sqrt{-3}]$ ongelijk is aan R.
Het element $\omega \in R$, zit niet in $\mathbb{Z}[\sqrt{-3}]$, omdat $\omega = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$ en dit heeft de vorm $a + bi\sqrt{3}$, met $a, b \notin \mathbb{Z}$, dus $\omega \notin \mathbb{Z}[\sqrt{-3}]$.
Dus $\mathbb{Z}[\sqrt{-3}] \subsetneq R$.

(b) We definiëren de afbeelding $N : R \to Z_{\geq 0}$ door $N(\alpha) = \alpha\overline{\alpha}$, waarbij $\overline{\alpha}$ de complex geconjugeerde van α is. Laat zien dat voor alle α en β in R geldt dat $N(\alpha\beta) = N(\alpha)N(\beta)$, maar dat in het algemeen niet geldt dat $N(\alpha + \beta) = N(\alpha) + N(\beta)$.
Neem 2 willekeurige elementen $\alpha, \beta \in R$ met $\alpha = a + b\omega$ en $\beta = c + d\omega$ voor $a, b, c, d \in \mathbb{Z}$.
Omdat $\mathbb{C}$ commutatief is, is ook R commutatief, want R is een deelring.
Te laten zien: $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$.
$\overline{\alpha}\overline{\beta} = \overline{(a + b\omega)}\ \overline{(c + d\omega)} = (a + b\overline{\omega})(c + d\overline{\omega}) = ac + ad\overline{\omega} + bc\overline{\omega} + bd\overline{\omega}^2$, want $a, b, c, d \in \mathbb{Z}$ en bevatten geen imaginair deel, dus voor deze delen gelden $\overline{x} = x$.
Ook hebben we dat $\overline{\alpha\beta} = \overline{(a + b\omega)(c + d\omega)} = \overline{ac + ad\omega + bc\omega + bd\omega^2} = ac + ad\overline{\omega} + bc\overline{\omega} + bd\overline{\omega}^2$.
Dus $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$.
Dan geldt $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$ uit de commutativiteit van $\mathbb{C}$.
Dus $N(\alpha + \beta) = (\alpha + \beta)\overline{(\alpha + \beta)} = \alpha\overline{\alpha} + \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta}$.
Maar $N(\alpha) + N(\beta) = \alpha\overline{\alpha} + \beta\overline{\beta}$ Dus als $\alpha\overline{\beta} + \beta\overline{\alpha} \neq 0$, geldt dat $N(\alpha + \beta) \neq N(\alpha) + N(\beta)$.
Voorbeeld:
Kies $\alpha, \beta = 1$.
Dan geldt $N(1 + 1) = N(2) = 2 \cdot 2 = 4$, maar $N(1) + N(1) = 1 \cdot 1 + 1 \cdot 1 = 2$.

(c) Gebruik N om de verzameling R^* van eenheden van R te bepalen. *Aanwijzing: druk $N(a + b\omega)$ uit in a en b uit.*
We weten dat een element $x \in R$ een eenheid is al $N(x) = \pm 1$, maar het bereik van N is $\mathbb{Z}_{\geq 0}$, dus kijken we alleen naar $N(x) = 1$.
Kies een willekeurig element $x \in R$ met $x = a + b\omega$ voor $a, b \in \mathbb{Z}$.
We weten ook dat $\omega = -\frac{1}{2}+\frac{1}{2}i\sqrt{3}$ en $\overline{\omega} = -\frac{1}{2}-\frac{1}{2}i\sqrt{3}$. Dus $\omega\overline{\omega} = (-\frac{1}{2}+\frac{1}{2}i\sqrt{3})(-\frac{1}{2}-\frac{1}{2}i\sqrt{3}) = \frac{1}{4} + \frac{3}{4} = 1$.
Dit geeft $N(x) = x\overline{x} = (a + b\omega)(a + b\overline{\omega}) = aa + ab\overline{\omega} + ba\omega + bb\omega\overline{\omega} = a^2 + b^2 + ab(\overline{\omega} + \omega) = a^2 + b^2 - ab$.

Dus als $N(x) = 1$ moet gelden: $a^2 + b^2 - ab = 1$ voor $a, b \in \mathbb{Z}$.
Dit geeft $R^* = \{(a + b\omega) \in R | a^2 + b^2 - ab = 1; a, b \in \mathbb{Z}\}$

Q2) Zij k een lichaam en $n \geq 1$. Bepaal het centrum van de matrixring $M_n(k)$. *Aanwijzing: gebruik Exercise 6 uit Sectie 7.2 om te bepalen welke elementen commuteren met alle* E_{ij}.
Een lichaam is een commutatieve delingsring. Een delingsring is een ring met een $1 \neq 0$ en voor elk element a moet er een b bestaan, zodat $ab = ba = 1$.
Een matrixring $M_n(k)$ is een verzameling van $n \times n$ matrices met op alle posities elementen uit k.
Het centrum van een groep is gegeven door de verzameling van alle elementen x waarvoor geldt $xy = yx$ voor alle y. Ik neem hier aan dat dit voor een ring ook de bedoeling is op de multiplicatie operatie? Kan dit niet vinden in de eerste 2 paragrafen van het boek of de aantekeningen.

Laat $A, B \in M_n(k)$ met $A = (a_{i,j})_{1 \leq i,j \leq n}$ en $B = (b_{i,j})_{1 \leq i,j \leq n}$ met $a_{i,j}, b_{i,j} \in k$ voor alle $1 \leq i, j \leq n$.
We willen kijken welke A in het centrum zitten, oftewel een A zodat $AB = BA$ voor alle $B \in M_n(k)$.
Omdat k een veld is, commuteren de elementen uit k en zijn ze abels onder additie.

In exercitie 7.2.6 hebben we gezien dat $E_{m,l}A$ met $1 \leq m, l \leq n$ de matrix geeft met op de m-de rij, de l-de rij van A en de rest 0, en $AE_{m,l}$ de matrix geeft met op de l-de kolom de m-de kolom van A en de rest 0.
We bekijken nu eerst of er elementen $A \in M_n(k)$ bestaan zodat $AE_{m,l} = E_{m,l}A$.
Als A een nulmatrix is, geldt deze gelijkheid zeker.
Stel nu dat A geen nulmatrix is.
Dan zit A in het centrum als voor zowel $AE_{m,l}$ als $E_{m,l}A$ geldt dat alleen op de m, l-de plaats een element staat ongelijk aan 0, alle andere elementen moeten gelijk zijn aan 0, omdat bij $AE_{m,l}$ slechts 1 kolom ongelijk aan 0 kan zijn en in $E_{m,l}A$ slechts 1 rij ongelijk aan 0 kan zijn.
Als deze gelijk moeten zijn, is het duidelijk dat in de rij op slechts 1 positie een element ongelijk aan 0 kan staan, en hetzelfde geldt voor de kolom. Dit geldt alleen op de m, l-de positie. De overige elementen in de m-de rij en l-de kolom moeten dus gelijk zijn aan 0.
Dit element moeten ook nog eens gelijk zijn.
Dat is alleen mogelijk als het l-de element op de l-de rij van A gelijk is aan het m-de element op de m-de kolom, oftewel $a_{m,m} = a_{l,l}$.
Dus alle matrices met waardes zodat $a_{m,m} = a_{l,l}$ en de rest van de m-de rij en l-de kolom gelijk zijn aan 0, commuteren met $E_{m,l}$.
Omdat we willen dat A commuteert met alle matrices van deze vorm, beschouwen we nu $W = \{E_{i,j} | 1 \leq i, j \leq m\}$.
We hebben net gezien dat A commuteert met $E_{i,j}$ als $a_{ii} = a_{jj}$ en de i-de rij en j-de kolom op alle andere posities 0 zijn.
Dan commuteert A met alle $E_{i,j} \in W$ als geldt dat $a_{ii} = a_{jj}$ voor alle $1 \leq i, j \leq n$ en alleen als op alle andere posities een 0 staat. Dit geldt nu voor alle elementen $a \in k$.
Alle matrices van deze vorm zijn de scalaire matrices uit $M_n(k)$.
De nulmatrix is ook een scalaire matrix, dus deze zit ook in deze verzameling.
Dit zijn de enigste matrices die in het centrum zouden kunnen zitten.
We willen nu laten zien dat A commuteert met alle matrices $B \in M_n(k)$.
Neem $A, B \in M_n(k)$ met A een scalaire matrix met element $x \in k$ en B een willekeurige matrix.
Dat volgt:
$AB = (\sum_{k=1}^{n} a_{ik}b_{kj})_{1 \leq i,j \leq n} = (xb_{ij})_{1 \leq i,j \leq n} = (b_{ij}x)_{1 \leq i,j \leq n} = (\sum_{k=1}^{n} b_{ik}a_{kj})_{1 \leq i,j \leq n} = BA$, uit

de standaard rekenregels voor matrices en uit het feit dat k een veld is en elementen dus commuteren.
Dit geeft $Z(M_n(k)) = \{C = (c_{i,j})_{1\leq i,j\leq n} | \begin{cases} c_{i,j} = l & i = j \\ c_{i,j} = 0 & i \neq j \end{cases} \text{ met } l \in k\}$