Ringen en Lichamen - Opdracht 2

Luc Veldhuis - 2538227

Oktober 2017

1. Zij $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \text{ met } a, b \text{ in } \mathbb{Z}\}$, een deelring van $\mathbb{C}$.
   (a) Toon aan dat $\varphi : R \to \mathbb{Z}/3\mathbb{Z}$ met $\varphi(a + b\sqrt{-5}) = \overline{a + 2b}$ een surjectief ringhomomorfisme is.
   We weten dat $\mathbb{C}$ en $\mathbb{Z}/3\mathbb{Z}$ commutatieve ringen zijn. Deze eigenschappen gebruiken we hier.
   We gaan eerst laten zien dat φ een ring homomorfisme is.
   We moeten controleren:

   - $\varphi(a + b) = \varphi(a) + \varphi(b)$ voor alle $a, b \in R$.
     Kies willekeurig een $a, b \in R$ met $a = c + d\sqrt{-5} = c + id\sqrt{5}$ en $b = e + if\sqrt{5}$ voor $c, d, e, f \in \mathbb{Z}$.
     Dan geldt $\varphi(a+b) = \varphi(c+id\sqrt{5}+e+if\sqrt{5}) = \varphi((c+d)+i(d+f)\sqrt{5}) = \overline{c + d + 2(d + f)}$
     Maar ook $\varphi(a)+\varphi(b) = \varphi(c+id\sqrt{5})+\varphi(e+if\sqrt{5}) = \overline{c + 2d}+\overline{e + 2f} = \overline{c + d + 2(d + f)}$.
     Dus $\varphi(a + b) = \varphi(a) + \varphi(b)$ voor alle $a, b \in R$.
   - $\varphi(ab) = \varphi(a)\varphi(b)$ voor alle $a, b \in R$.
     Kies willekeurig een $a, b \in R$ met $a = c + d\sqrt{-5} = c + id\sqrt{5}$ en $b = e + if\sqrt{5}$ voor $c, d, e, f \in \mathbb{Z}$.
     Dan geldt $\varphi(ab) = \varphi((c + id\sqrt{5})(e + if\sqrt{5})) = \varphi(ce + icf\sqrt{5} + ide\sqrt{5} - df\sqrt{5}) = \varphi(ce - 5df + i(cf + de)\sqrt{5}) = \overline{ce - 5df + 2(cf + de)} = \overline{ce + 2cf + 2de} + \overline{-5df}$
     Maar ook $\varphi(a)\varphi(b) = \varphi(c+id\sqrt{5})\varphi(e+if\sqrt{5}) = \overline{c + 2de + 2f} = \overline{ce + 2cf + 2de + 4df} = \overline{ce + 2cf + 2de} + \overline{4df}$.
     We moeten nu dus laten zien dat $\overline{-5x} = \overline{4x}$ in $\mathbb{Z}/3\mathbb{Z}$ voor $x \in \mathbb{Z}$.
     We zien dat $\overline{4x} = \overline{4} \cdot \overline{x}$ en $\overline{-5x} = \overline{-5} \cdot \overline{x}$ maar $\overline{4} = \overline{1}$ en $\overline{-5} = \overline{1}$.
     Dus nu volgt dat $\varphi(a)\varphi(b) = \overline{ce + 2cf + 2de + 1df} = \overline{ce + 2cf + 2de + df}$ en dat $\varphi(ab) = \overline{ce + 2cf + 2de + 1df} = \overline{ce + 2cf + 2de + df}$.
     Dus $\varphi(ab) = \varphi(a)\varphi(b)$ voor alle $a, b \in R$.

   We hebben nu laten zien dat φ een ringhomomorfisme is. Nu moeten we nog laten zien dat deze surjectief is.
   We doen dit aan de hand van 3 voorbeelden:

   - $0 \in R$, $\varphi(0) = \overline{0}$.
   - $1 \in R$, $\varphi(1) = \overline{1}$.
   - $2 \in R$, $\varphi(2) = \overline{2}$.

   En $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. Dus dit ringhomomorfisme is surjectief, want hij beeld minimaal 1 keer af op elk element in $\mathbb{Z}/3\mathbb{Z}$.

   (b) Bewijs dat $\ker(\varphi) = (3, 1 + \sqrt{-5})$ en dat $R/\ker(\varphi) \cong \mathbb{Z}/3\mathbb{Z}$ als ringen.
   We zien dat $\overline{0} \in \mathbb{Z}/3\mathbb{Z}$ het 'nulelement' is.
   We bewijzen eerst dat $\ker(\varphi) = (3, 1 + \sqrt{-5})$.
   Bewijs '$\supseteq$':

We zien direct dat $\varphi(3) = \overline{3} = \overline{0}$ en $\varphi(1+\sqrt{-5}) = \overline{1+2} = \overline{3} = \overline{0}$.
Ook weten we dat $\overline{0} + \overline{0} = \overline{0}$, en voor alle $\overline{k} \in \mathbb{Z}/3\mathbb{Z}$ geldt $\overline{k}\overline{0} = \overline{0}$.
Omdat $(3, 1+\sqrt{-5})$ een ideaal is wat wordt voortgebracht door 3 en $1+\sqrt{-5}$, en deze allebei afbeelden op $\overline{0}$, zien we nu dat voor elk element $e \in (3, 1+\sqrt{-5})$ geldt dat $\overline{e} = \overline{0}$.
Omdat $\ker(\varphi)$ gedefinieerd is als alle elementen uit R die afbeelden op $\overline{0}$, en alle elementen uit $(3, 1+\sqrt{-5})$ afbeelden op $\overline{0}$, geldt nu dat $\ker(\varphi) \supseteq (3, 1+\sqrt{-5})$.
Bewijs '$\subseteq$':
We weten dat voor elke element $r \in \ker(\varphi)$ met $r = a + b\sqrt{-5}$ geldt dat $\varphi(r) = \varphi(a + b\sqrt{-5}) = \overline{a+2b} = \overline{0} = \overline{3k}$ met $a, b, k \in \mathbb{Z}$.
Er moet dus gelden dat $a + 2b = 3k$ voor $a, b, k \in \mathbb{Z}$.
Dus alle elementen $r \in R$ met $r = a + b\sqrt{-5}$ die voldoen aan de vergelijking: $a = 3k - 2b$ voor alle $k, b \in \mathbb{Z}$ zitten in $\ker(\varphi)$.
Schrijf nu $r = 3k - 2b + b\sqrt{-5} = 3k - 3b + b + b\sqrt{-5} = 3(k-b) + b(1 + 1\sqrt{-5})$.
We zien dat $3(k-b) \in (3, 1+\sqrt{-5})$ en we zien dat $b(1+\sqrt{-5}) \in (3, 1+\sqrt{-5})$ voor alle $k, k-b \in \mathbb{Z}$ omdat deze k en $k-b$ ook in $\mathbb{Z}[\sqrt{-5}]$ zitten.
Omdat $(3, 1+\sqrt{-5})$ per definitie gesloten is onder optelling, geldt dat $3(k-b)+b(1+\sqrt{-5}) \in (3, 1+\sqrt{-5})$.
Dus elke $r \in \ker(\varphi)$ zit in $(3, 1+\sqrt{-5})$.
Dus $\ker(\varphi) \subseteq (3, 1+\sqrt{-5})$.
Nu moeten we nog bewijzen dat $R/\ker(\varphi) \cong \mathbb{Z}/3\mathbb{Z}$ als ringen.
Bewijs:
Omdat φ een surjectief ringhomomorfisme is met $\mathbb{Z}/3\mathbb{Z}$, geldt dat $\varphi(R) = \mathbb{Z}/3\mathbb{Z}$.
Dan volgt nu uit de eerste isomorfie stelling dat $R/\ker(\varphi) \cong \varphi(R)$, dus $R/\ker(\varphi) \cong \mathbb{Z}/3\mathbb{Z}$ als ringen.

2. Zij R een commutatieve ring met $1 \neq 0$, J een ideaal van R en $a_1, \ldots, a_n$ elementen van R. Toon aan dat equivalent zijn:

   (i) $(a_1, \ldots, a_n) \subseteq J$

   (ii) $a_1, \ldots, a_n$ zijn elementen van J.

   Bewijs $(i) \Rightarrow (ii)$:
   We nemen aan dat $(a_1, \ldots, a_n) \subseteq J$.
   Omdat $(a_1, \ldots, a_n) = \bigcap_{I \text{ een ideaal}, \{a_1, \ldots, a_n\} \subseteq I} I$ een ideaal is bij definitie, en er nu wel moet gelden dat $a_1, \ldots, a_n \in (a_1, \ldots, a_n)$ per definitie.
   Omdat $(a_1, \ldots, a_n) \subseteq J$, moet wel gelden dat $a_1, \ldots, a_n \in J$.
   Bewijs $(i) \Leftarrow (ii)$:
   Neem aan dat $a_1, \ldots, a_n$ elementen zijn van J.
   Dan volgt uit de definitie dat $(a_1, \ldots, a_n) = \bigcap_{I \text{ een ideaal}, \{a_1, \ldots, a_n\} \subseteq I} I$.
   Omdat $\{a_1, \ldots, a_n\} \subseteq J$, volgt direct dat $(a_1, \ldots, a_n) \subseteq J$.
   Dus de uitspraken zijn equivalent.
   [Dit is geponeerd op het hoorcollege, je moet het hier zorgvuldig bewijzen uit de definities.]