Ringen en Lichamen

Luc Veldhuis

25 September 2017

Isomorfie

Isomorfiestellingen

1. $\phi : R \to S$ een ringhomomorfisme dan is $\psi : R/Ker(\phi) \cong Im(\phi)$ met $\overline{a} \mapsto \phi(a)$.
2. Als $S \subseteq R$ een deelring is, I een ideaal van R, dan is $S + I = \{s + i | s \in S, i \in I\}$ een deelring van R die I bevat, I een ideaal van $S + I$, $S \cap I$ een ideaal van S en $S/(S \cap I) \cong (S + I)/I$.
3. In boek.
4. In boek.

Isomorfie

Bewijs 1e stelling

We weten alles uit de 1e isomorfiestelling voor groepen uit $\phi((R,+)) \to (S,+)$, behalve dat $\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a}) \cdot \psi(\overline{b})$.
Dit geeft $\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{ab}) = \phi(ab)$, en $\psi(\overline{a}) = \phi(a)$ en $\psi(\overline{b}) = \phi(b)$.
Maar we weten ook dat $\phi(ab) = \phi(a)\phi(b)$ omdat ϕ een ring homomorfisme is.

Bewijs 2e stelling

Ga na: $S + I$ is een deelring van R, die I bevat als ideaal.
Neem ringhomomorfisme: $\phi : S \to (S + I)/I$ met $s \mapsto \overline{s + 0}$, samenstelling van inclusie homomorfisme $S \to S + I$ en quotient homomorfisme $S + I \to (S + I)/I$.
Ga na: ϕ is surjectief, met $Ker(\phi) = S \cap I$.
Pas dan 1e isomorfie stelling toe op ϕ.

Isomorfie

Voorbeeld

$\phi : \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z}$ met $a + bi \mapsto \overline{a + b}$ is een surjectief ringhomormofisme want $\phi(0) = \overline{0}, \phi(1) = \overline{1}$. (ga na) Wat is $Ker(\phi)$?

Claim

$Ker(\phi) = \{\beta(1 - i) | \beta \in \mathbb{Z}[i]\} = I$

Isomorfie

Bewijs

'$\supseteq$': $\phi(\beta(1-i)) = \phi(\beta)\phi(1-i) = \phi(\beta)\overline{0} = \overline{0}$.
Korter: $\phi(1-i) \in Ker(\phi)$, al gezien: $Ker(\phi)$ is ideaal. Dan geldt $\beta(1-i) \in \mathbb{Z}[i]$ foor alle β in $\mathbb{Z}[i]$.
'$\subseteq$': Neem $\alpha = a + bi$ in $Ker(\phi)$.
Dan is $\overline{a+b} = \overline{0} \in \mathbb{Z}/2\mathbb{Z}$.
Dan is $a + b = 2k$ voor een $k \in \mathbb{Z} \Rightarrow$
$\alpha = a + bi = -b + 2k + bi = ((1+i)k - b)(1-i)$ en dit zit zeker in $\{\beta(1-i) | \beta \in \mathbb{Z}[i]\}$
Gebruik dat $2 = (1+i)(1-i)$.
De eerste isomorfie stelling geeft nu $\mathbb{Z}[i]/I \cong \mathbb{Z}/2\mathbb{Z}$.
$(a+bi) + I \mapsto \overline{a+b}$.

Isomorfie

Voorbeeld 2e isomorfie stelling

k een lichaam, $R = k[x, y] = k[x][y]$.
(Voorbeeld: $xy + y + 2 = (x + 1)y + 2$ in $k[x][y]$, $yx + (y + 2)$ in $k[y][x]$)
$S = k[x]$, $I = \{f \cdot y | f \in R\}$
Dan is $S + I = R$, $S \cap I = \{0\}$, uit 2e isomorfie stelling volgt:
$S/(S \cap I) \cong (S + I)/I$ dus $k[x]/\{0\} \cong R/I$.

Opgave

Bewijs $R/I \cong k[x]$ via de 1e isomorfie stelling.
Hint: $R \to k[x]$ is surjectief ringhommomorfisme met $f(x, y) \mapsto f(x, 0)$.

Isomorfie

Definitie

I, J idealen van een ring R.

- De som $I + J = \{i + j | i \in I, j \in J\}$ een ideaal van R. Het is het kleinste ideaal van R dat I en J bevat.
- Het product $I \cdot J = \{\sum_{l=1}^{m} i_l j_l | i_l \in I, j_l \in J, m \geq 0\}$ is een ideaal.
- $I^n = I \cdot I \cdot I \cdots I$ (n keer)

Dan $R \supseteq I + J \begin{matrix} \supseteq I \supseteq \\ \supseteq J \supseteq \end{matrix} I \cap J \supseteq I \cdot J$, allemaal een ideaal van R.

Opgave

Welke idealen zijn dit als $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 9\mathbb{Z}$?
De idealen van $\mathbb{Z}$ zijn $n\mathbb{Z}$ met $n \geq 0$.

§7.4 Eigenschappen van idealen

Definitie

R altijd een ring met $1 \neq 0$.
$A \subseteq R$ een deelverzameling.

- (A) = het kleinste ideaal van R dat A bevat $= \bigcap_{A \subseteq I, I \text{ ideaal}} I$.
- $RA = \{\sum_{i=1}^{m} r_i a_i | r_i \in R, a_i \in A, n \geq 0\}$ het kleinste linksideaal van R dat A bevat want $1 \in R$.
- $AR =$ zelfde voor rechts.

$(A) = \{\sum_{i=1}^{n} r_i a_i s_i | a_i \in A, r_i, s_i \in R, n \geq 0\} = RAR$.
Als R **commutatief** is, dan is $RAR = RA = AR =$ kleinste ideaal van R dat A bevat.
Als R commutatief is en $A = \{a_1, a_2, a_3, \dots\}$ dan is
$(\{a_1, \dots, a_n\}) = \{\sum_{i=1}^{n} r_i a_i | r_i \in R\}$
$r_1 a + r_2 a = (r_1 + r_2)a$

§7.4 Eigenschappen van idealen

Voorbeeld

- $R = \mathbb{Z}[i]$
  $I = \{\beta(1-i) | \beta \in \mathbb{Z}[i]\} = (1-i)$ een ideaal, deelverzameling van $\mathbb{Z}[i]$.
- De idealen van Z zijn (n) met $n \geq 0$.

Voorbeeld

$R = \mathbb{Z}[i]$ dan geeft dit $(1-i) \cdot (1-i) = \begin{cases} -2i & \in \mathbb{Z}[i] \\ (2) & \subseteq \mathbb{Z}[i] \end{cases}$

Als R commutatief is (met $1 \neq 0$) en
$I = (a_1, \ldots, a_n) = \{r_1 a_1 + r_2 a_2 + \cdots + r_m a_m | a_i \in R\}$ is het ideaal voorgebracht door $a_1, \ldots, a_m$, deze elementen zijn de voortbrengers.
Een ideaal (a) heet een **hoofdideaal** (Engels: principal ideal) en a heet een voortbrenger.

§7.4 Eigenschappen van idealen

Voorbeeld

$R = \mathbb{Z}$, $(4, 6) = (2)$ is een hoofdideaal van $\mathbb{Z}$.
Dus in $\mathbb{Z}$ met $(4, 6) = (2)$, en er geldt '$(4, 6) \subseteq (2) \Leftrightarrow 4, 6 \in (2)$' en $2 \cdot 2 = 4$ en $2 \cdot 3 = 6$
We hebben ook dat '$(2) \subseteq (4, 6) \Leftrightarrow 2 \in (4, 6)$' want $2 = 4a + 6b$ met $a, b \in \mathbb{Z}$, klopt voor $a = -1$, $b = 1$.

Opgave

Als J een ideaal is van R, een commutatieve ring met $1 \neq 0$, en $a_1, \ldots, a_m \in R$, dan geldt:
$(a_1, \ldots, a_m) \subseteq J \Leftrightarrow a_1, \ldots, a_m \in J$

Voorbeeld

Met $R = \mathbb{Z}[x]$ is $(2, x)$ is geen hoofdideaal (zie boek).

§7.4 Eigenschappen van idealen

Stelling

R een ring met $1 \neq 0$, I een ideaal van R. Dan geldt:

- $I = R \Leftrightarrow I$ bevat een eenheid (element van R^*)
- Als R commutatief is dan geldt:
  R is een lichaam $\Leftrightarrow \{0\}$ en R zijn de enigste idealen van R.

Bewijs

1e stelling:
'$\Rightarrow$': $1 \in I = R$ en $1 \in \mathbb{R}^*$.
'$\Leftarrow$': Stel $u \in I$ en $u \in \mathbb{R}^*$. Dan bestaat $v \in \mathbb{R}^*$ met $uv = 1 = vu$, $1 \in I$, dus als $r \in R$ is $r \cdot 1 = r \in R$.
2e stelling:
Zie boek.

§7.4 Eigenschappen van idealen

Definitie

In een willekeurige ring S (misschien niet commutatief, zonder 1) heet een ideaal M van S een maximaal ideaal als:

- $M \neq S$
- Als N een ideaal is met $M \subseteq N \subseteq S$, dan geldt $N = S$ of $N = S$

Voorbeeld

$R = \mathbb{Z}$. Idealen: (n), $n \geq 0$.
$n = 0$ niet maximaal: $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.
$n = 1$ niet maximaal: $(1) = \mathbb{Z}$.

§7.4 Eigenschappen van idealen

Opgave

In Z geldt $(a) \subseteq (b) \Leftrightarrow a \in (b) \Leftrightarrow b|a$.
Dus voor $n \geq 2$ geldt als n niet priem is, dan is (n) niet maximaal.
$n = 6$, $(6) \subsetneq (2) \subsetneq \mathbb{Z}$.
Als n wel priem, dan is (n) een maximaal ideaal.
Conclusie: de maximale idealen van $\mathbb{Z}$ corresponderen met de priemgetallen: het zijn (p) met p priem.