Ringen en Lichamen

Luc Veldhuis

17 September 2017

Groepsringen

Definitie

Zij $G = \{g_1, g_2, \ldots, g_n\}$ een eindige groep, R een ring.
Dan is $RG = \{a_1g_1 + a_2g_2 + \cdots + a_ng_n | a_i \in R\}$ een **groepsring**.
Ring met optelling van coëfficiënten en vermenigvuldiging via distributiviteit en $a_ig_i \cdot a_jg_j = a_ia_jg_ig_j$ met $a_ia_j \in R$ en $g_ig_j \in G$.

Voorbeeld

$G = \{e, g\}$, $R = \mathbb{R}$.
$RG = \{ae + bg | a, b \in R\}$ en
$(a_1e + b_1g) + (a_2e + b_2g) = (a_1 + a_2)e + (b_1 + b_2)g$
$(a_1e + b_1g) \cdot (a_2e + b_2g) = (a_1a_2 + b_1b_2)e + (a_1b_2 + b_1a_2)g$

Groepsringen

Voorbeeld

$\pi = \frac{1}{2}e + \frac{1}{2}g$ is **idempotent:** $\pi^2 = \pi$. (Projectie van Lineaire algebra).
$\pi' = \frac{1}{2}e - \frac{1}{2}g$ is ook idempotent.

Idee van groepsringen

Als $\phi : G \to GL_m(\mathbb{R})$ groepshomomorfisme is.
Maak $\widetilde{\phi} : \mathbb{R}G \to M_m(\mathbb{R})$ ring homomorfisme.
Deze matrices kunnen we wel optellen.
$a_1g_1 + \cdots + a_ng_n \mapsto a_i\phi(g_1) + \cdots + a_n\phi(g_n)$
Analyseer ϕ door $\mathbb{R}G$ te bekijken en $\widetilde{\phi}$ te toe te passen.

Voorbeeld

Als $G = \{e, g\}$ dan is $\mathbb{R}G \cong \mathbb{R} \cdot \pi \times \mathbb{R} \cdot \pi'$ als ringen.

Definitie

Zij R, S ringen.

- $\phi : R \to S$ heet ringhomomorfisme als voor alle $a, b \in R$ geldt dat:
  - $\phi(a+b) = \phi(a) + \phi(b)$
  - $\phi(ab) = \phi(a)\phi(b)$
- $Ker(\phi) = \{a \in R | \phi(a) = 0\}$
- Een bijectief ringhomomorfisme heet een ringisomorfisme

Opgave

- De samenstelling van homomorfismen is een homomorfismen. Idem voor isomorfismen.
- De inverse van een ringisomorfisme is ook een ringisomorfisme.

Opmerking

- $\phi : (R, +) \to (S, +)$ is een groepen homomorfisme, dus $\phi(-a) = -\phi(a)$ en $\phi(0_R) = 0_s$. Ook: $Ker(\phi)$ als voor het optelhomomorfisme, $(R, +) \to (S, +)$, dus ϕ injectief $\Leftrightarrow$ $Ker(\phi) = \{0_R\}$
- $\phi(1_R) \neq 1_S$ is mogelijk.
  Voorbeeld: $R = \{\overline{0}, \overline{3}\}$, $S = \mathbb{Z}/6\mathbb{Z}$.
  ϕ is een ringhomomorfisme met $\overline{0} \mapsto \overline{0}$ en $1_S = \overline{1}$ maar $1_R = \overline{3}$.
  Als $\phi(1_R) = 1_S$ heeft ϕ unitair.

Definitie

$I \subseteq R$ heet een ideaal van R als:

- $I \neq \emptyset$
- Als $x, y \in I$, dan is $x - y \in I$
- Als $x \in I$ en $r \in R$, dan zijn rx en xr ook in I.

Als $rx \in I$ voor alle $x \in I, r \in I$, dan definieert dit een **linksideaal** van R.
Idem met $xr \in I$ voor alle $x \in I$, $r \in R$ heet dit **rechtsideaal**.

Opmerking

De eerste 2 eisen zijn equivalent met I een optelingsgroep van R.
Een ideaal is een deelring van R.

Voorbeeld

$R = \mathbb{Z}$. De optelondergroepen van $\mathbb{Z}$ zijn $\{0\}$ en $n\mathbb{Z}$ met $n \geq 1$.
Dit zijn allemaal idealen (ga na).

Stelling

Als $\phi : R \to S$ een ringhomomorfisme is, dan:

- $Im(\phi)$ is een deelring van S
- $Ker(\phi)$ is een ideaal van R

Bewijs

- Opgave
- We weten (omdat ϕ een optelhomomorfisme is) dat de kern van ϕ een ondergroep is van R voor de optelling.
  Voor de laatste eigenschap: neem $x \in Ker(\phi)$ en $r \in R$. Dan is $rx \in Ker(\phi) : \phi(rx) = \phi(r)\phi(x) = \phi(r)0_S = 0_S$. Net zo $xr \in Ker(\phi)$.

Voorbeeld

- $\phi : \mathbb{Z} \to Z/n\mathbb{Z}$ $(n \geq 1)$
  $a \mapsto \overline{a}$
  is surjectief ringhomomofrisme (bijvoorbeeld
  $\overline{a+b} = \phi(a+b) = \phi(a) + \phi(b) = \overline{a} + \overline{b}$ met $Ker(\phi) = n\mathbb{Z}$
- R commutatief met 1, $r \in R$
  $s_r : R[x] \to R$ met $f(x) \mapsto f(r)$ is een surjectief ring homomorfisme..
  $Ker(s_r) = R[x] \cdot (x - r)$ (later).
- k een lichaam, $n \geq 1$.
  $R = M_n(k)$, $I = \{$matrices met waardes in 1e kolom$\}$ is een linksideaal van R maar geen rechts ideaal als $n \geq 2$.
  $J = \{$matrices met waardes in de 1e rij$\}$ is een rechtsideaal van R maar geen linkideaal als $n \geq 2$.

Opgave

De idealen van R zijn $\{0_R\}$ en R.

Herhaling normaaldeler (groepen)

$N \triangleleft G \Leftrightarrow N \leqslant G$ en $gng^{-1} \in N$ voor alle $n \in N$, $g \in G$.
$G/N = \{gN | g \in G\}$

Definitie

Als $I \subseteq R$ een ideaal van R is, dan is I een optelgroep van R en een normaaldeler van $(R, +)$ want die groep is abels, dus $R/I = \{a + I | a \in R\}$ is een groep met $(a + I) + (b + I) = (a + b) + I$ of $\overline{a} + \overline{b} = \overline{a + b}$ als $\overline{c} = c + I$. Definieer nu $\overline{a} \cdot \overline{b} = \overline{ab}$. Dit is welgedefinieerd: andere keuzes uit $\overline{a}$ zijn $a' = a + i$ en $b' = b + j$, $i, j \in I$. Dan is $a'b' - ab = (a + i)(b + j) - ab = aj + ib + ij \in I$ dus $\overline{a'b'} = \overline{ab}$. Dan is R/I met deze $+$ en $\cdot$ een ring:

- We weten al dat R/I een abelse optelgroep is.
- Associativiteit van $\cdot$: doe zelf
- Distributiviteit: $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{(a + b)}\overline{c} = \overline{(a + b)c} = \overline{ac + bc} = \overline{ac} + \overline{bc} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$, want R een ring.

R/I heet de quotienten ring 'R modulo I'

Stelling

De afbeelding $\pi : R \to R/I$ met $a \mapsto \overline{a} = a + I$ is een surjectief ringhomomorfisme met $Ker(I)$.

Bewijs

We weten dat π een surjectief homomorfisme van optelgroepen is met $Ker(I)$. Alleen nog te controlleren: $\pi(a \cdot b) = \pi(a) \cdot \pi(b)$ voor alle $a, b \in R$. Maar $\pi(\overline{ab}) = \overline{ab} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b)$.

Voorbeeld

Als $R = \mathbb{Z}$ en $I = n\mathbb{Z}$ met $n = 0, 1, 2, \ldots$.
Dan is $\mathbb{Z}/n\mathbb{Z}$ de 'oude' $\mathbb{Z}/n\mathbb{Z}$ als $n \geq 2$.
Als $n = 1$: $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ met $\overline{0} + \overline{0} = \overline{0} = \overline{0} + \overline{0}$.
Als $n = 0$: $\mathbb{Z}/\{0\} = \{\{a\} | a \in \mathbb{Z}\} \cong \mathbb{Z}$.

Voorbeeld

$y^4 = x^4 + 3$ heeft geen oplossingen.
$(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
Stel maar dat hij wel bestaat, dus $a^4 = b^4 + 3$ in $\mathbb{Z}$.
Dan geldt in $\mathbb{Z}/5\mathbb{Z}$: $\overline{a^4} = \overline{b^4 + 3}$ dus $\overline{a}^4 = \overline{b}^4 + 3$ in $\mathbb{Z}/5\mathbb{Z}$.
Maar als $\mathbb{Z}/p\mathbb{Z}$ met p priem, dan geldt $\overline{c}^{p-1} = \begin{cases} \overline{0} & \overline{c} = \overline{0} \\ \overline{1} & \overline{c} \in (\mathbb{Z}/p\mathbb{Z})^* \end{cases}$.
Dan zijn er 4 mogelijke uitkomsten:
$\overline{0} = \overline{0} + \overline{3}$
$\overline{0} = \overline{1} + \overline{3}$
$\overline{1} = \overline{0} + \overline{3}$
$\overline{1} = \overline{1} + \overline{3}$
Dit kan niet, dus $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ bestaat niet.

Volgende keer

1e en 2e isomorfie stelling voor ringen. 1e: Als $\phi : R \to S$ een ringhomomorfisme is, dan $R/Ker(\phi) \cong Im(\phi)$ met $a + Ker(\phi) \mapsto \phi(a)$.