Ringen en Lichamen

Luc Veldhuis

4 September 2017

Inleiding ringen

Definitie

- Een **ring** R is een verzameling met 2 bewerkingen: Optelling $R \times R \to R$, $(a, b) \mapsto a + b$ en vermenigvuldiging $R \times R \to R$, $(a, b) \mapsto a \cdot b$ zodanig dat:
  - $(R, +)$ is een abelse groep
  - De vermenigvuldiging is associatief $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ voor alle $a, b, c \in R$.
  - $a \cdot (b + c) = a \cdot b + a \cdot c$ voor alle $a, b, c \in R$
    $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributiviteit)
- R heet **commutatief** als $a \cdot b = b \cdot a$ voor alle $a, b \in R$.
- R heeft een **identiteit** (eenheids element of 1) als er een element $1 = 1_R$ zodat $a \cdot 1_R = a = 1_R \cdot a$ voor alle $a \in R$.

Inleiding ringen

Opmerking

- $(R, +)$ is een abelse groep $\Leftrightarrow$
  - $R \neq \emptyset$
  - Er bestaat een $0 \in R$ zodat $a + 0 = a = 0 + a$ voor alle $a \in R$
  - $a + (b + c) = (a + b) + c$ voor alle $a, b, c \in R$
  - Voor elke $a \in R$ is er een $b \in R$ met $a + b = 0 = b + a$, b is uniek genoteerd als $-a$
  - $a + b = b + a$ voor alle $a, b \in R$

  We hebben ook dat $a - b = a + 1 - b$
- We weten: $0 = 0_R$ is uniek
  Als R een identiteit heeft, is die ook uniek:
  Stel $1, 1'$ voldoen allebei, dan geldt $1' = 1' \cdot 1 = 1$
- Vaak schrijven we ab voor $a \cdot b$

Voorbeeld

- Als R een abelse groep is met $+$ als bewerking, dan is R met $a \cdot b = 0$ voor alle $a, b \in R$ een ring.
- $R = \{0\}$ met $0 + 0 = 0$, $0 \cdot 0 = 0$ is een commutatieve ring met identiteit $1_R = 0$.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ zijn commutatieve ringen met 1
- Als $n \geq 2$, dan is $\mathbb{Z}/n\mathbb{Z}$ met $\overline{a} + \overline{b} = \overline{a + b}$ en $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ is een commutatieve ring met identiteit $\overline{1}$.
  Bijvoorbeeld:
  $\overline{a}(\overline{b}+\overline{c}) = \overline{a} \cdot (\overline{b + c}) = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$
- $R = \{\overline{0}, \overline{3}\} \subseteq \mathbb{Z}/6\mathbb{Z}$ is met de optelling en vermenigvuldiging van $\mathbb{Z}/6\mathbb{Z}$ een ring: $\overline{0} + \overline{0}, \overline{0} + \overline{3}, \overline{3} + \overline{0}, \overline{3} + \overline{3}$
  $\overline{0} \cdot \overline{0}, \overline{0} \cdot \overline{3}, \overline{3} \cdot \overline{0}, \overline{3} \cdot \overline{3}$ zijn in R

Voorbeeld (vervolg)

$(R, +) = \langle \overline{3} \rangle$ is een ondergroep van $(\mathbb{Z}/6\mathbb{Z}, +)$.
Associativiteit van de vermenigvuldiging en distributiviteit gelden in $\mathbb{Z}/6\mathbb{Z}$, dus ook in R.
R is commutatief want $\mathbb{Z}/6\mathbb{Z}$ is commutatief.
R heeft een identiteit, $1_R = \overline{3}$ want $\overline{a} \cdot \overline{3} = \overline{a} = \overline{3} \cdot \overline{a}$ voor alle $\overline{a} \in R$:
$\overline{0} \cdot \overline{3} = \overline{0} = \overline{3} \cdot \overline{0}$
$\overline{3} \cdot \overline{3} = \overline{3} = \overline{3} \cdot \overline{3}$
Dus: zowel R als $\mathbb{Z}/6\mathbb{Z}$ hebben identiteiten maar die zijn verschillend.

- Als X een niet lege verzameling is, A een ring dan is $\{f : X \to A\}$ een ring met 'puntsgewijze optelling en vermenigvuldiging':
  Voor $f, g \in R$ definieer $f + g$ via $(f + g)(x) = f(x) + g(x)$
  $f \cdot g$ via $(f \cdot g)(x) = f(x) \cdot g(x)$ voor alle $x \in X$.

Inleiding ringen

Stelling

Zij R een ring

- $0 \cdot a = 0a \cdot 0$ voor alle $a \in R$
- $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ voor alle $a, b \in R$
- $(-a) \cdot (-b) = ab$ voor alle $a, b \in R$
- Als R een 1 heeft dan geldt $(-1) \cdot a = -a = a \cdot (-1)$ voor alle $a \in R$

Bewijs

- $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$ en uit $y + y = y$ in $(R, +)$ volgt $y = 0$. Neem $y = 0 \cdot a$.
  $a \cdot 0 = 0$ doe dit zelf.
- $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$
  Tel $-(ab)$ aan beide kanten op $(-a)b = -(ab)$ en $a(-b) = -(ab)$ net zo
- Volgt uit 2

Opmerking

As R een ring met $1 = 0$, dan geldt voor elke $x \in R$ dat $x = 1 \cdot x = 0 \cdot x = 0$, dan $R = \{0\}$ en die heeft $1_R = 0$.
Later zullen we vaak eisen dat $1_R \neq 0$ om dit uit te sluiten.

Inleiding ringen

Definitie

Een ring R met $1 \neq 0$ heet een **delingsring**. (Engels: *divisionring*) als voor elke $a \neq 0$ in R er een $b \in R$ bestaat met $ab = 1 = ba$. Je kunt 'delen door a' door vermenigvuldigen met b.
Opgave: voor $a \neq 0$ is die b uniek. Notatie: a^{-1}. Als R commutatief is, dan heet R een lichaam. (Engels: field)

Inleiding ringen

Voorbeeld

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ zijn lichamen
- $\mathbb{Z}$ is geen lichaam, er is geen $b \in \mathbb{Z}$ met $2b = 1$.
- $\mathbb{H} = \{a + bi + cj + dk\}$ met $a, b, c, d \in \mathbb{R}$ met optelling $(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b - 3)j + (a_4 + b_4)k$ en vermenigvuldiging via distributiviteit en rekenregels: reële coëfficiënten commuteren met alles en $i^2 = j^2 = k^2 = -1$. $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ is een deelring (niet commutatief)

Voorbeeld

$$\begin{aligned}(1+2i)(3j+4k) &= 1\cdot 3j + 1\cdot 4k + 2i\cdot 3j + 2i\cdot 4k \\ &= 3j + 4k + 6ij + 8ik \\ &= 3j + 4k + 6k + 8 - j \\ &= -5j + 10k\end{aligned}$$

Definieer als $\alpha = a + bi + cj + dk$
$\overline{\alpha} = a - bi - cj - dk$
Dan geldt $\alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 + b^2 + c^2 + d^2$ en $\overline{\alpha\beta} = \overline{\beta\alpha}$
Als $\alpha \neq 0$ dan is $\alpha^{-1} = (\alpha\overline{\alpha})^{-1} \cdot \overline{\alpha} \in \mathbb{R}^*$

Inleiding ringen

Voorbeeld

In $\mathbb{Z}/6\mathbb{Z}[x] = \{\text{polynomen in } x \text{ met coefficienten in } \mathbb{Z}/6\mathbb{Z}\}$ geldt $(\overline{2}x + \overline{1}) \cdot (\overline{3}x + \overline{1}) = \overline{2} \cdot \overline{3}x^2 + (\overline{2} \cdot \overline{1} + \overline{1} \cdot \overline{3})x + \overline{1} \cdot \overline{1} = \overline{5}x + \overline{1}$

Graad van product is 'te klein' doordat $\overline{2} \cdot \overline{3} = \overline{0}$.

Definitie

Zij R een ring.

- Een element $a \neq 0$ in R heet een **nuldeler** als er een $b \neq 0$ met $ab = 0$ of $ba = 0$
- Neem aan dat R $1 \neq 0$ heeft. Een element van $u \in R$ heet een **eenheid** van R als er een $v \in R$ is met $vu = 1 = vu$.

De verzameling van eenheden van R wordt genoteerd als $\mathbb{R}*$.

Inleiding ringen

Opgave

Gegeven $u \in R^*$ dan is de $v \in R$ met $uv = 1 = vu$ uniek en $v \in R^*$.
Notatie: schrijf u^{-1} voor v. Normale reken regels gelden voor exponenten (pas op als de ring niet commutatief is)

Voorbeeld

- $\mathbb{Z}^* = \{1, -1\}$
- Als R een delingsring is (bijvoorbeeld een lichaam) dan is $R^* = R \setminus \{0\}$.
- Als $n \geq 2$ dan is $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} | a \in \mathbb{Z}, ggd(a, n) = 1\}$