

Groepen en Ringen

8078254

26 mei 2025

RINGEN

4

Definitie. Een ring R is een verzameling met twee binaire operaties:

- $+: R \times R \rightarrow R$
 $(r, s) \mapsto r + s$
- $\times: R \times R \rightarrow R$
 $(r, s) \mapsto r \times s = rs$

zodat

1. $(R, +)$ is een (abelse¹) groep
2. Vermenigvuldiging $\times$ is associatief
3. Optelling en vermenigvuldiging zijn distributief

Opmerking. R heeft altijd een eenheid 0 voor optelling uit aanname (1). Als we zeggen dat “ R heeft een eenheid” dan is dat voor vermenigvuldiging:

$$1 \in R \text{ zodat } 1 \times r = r \times 1 = r \quad \forall r \in R$$

Opmerking. $(R, +)$ is abels door (3). Als we zeggen “ R is commutatief” bedoelen we dat voor vermenigvuldiging; $r \times s = s \times r \quad \forall r, s \in R$

Opmerking. R heeft additieve inverses $(-r)$ voor alle $r \in R$ door (1).

Als er ook multiplicatieve inverses ($r^{-1} = \frac{1}{r}$) voor alle $r \in R \setminus \{0\}$ dan heet R een delingsring. Als R ook commutatief is, dan heet R een *lichaam* (EN: “field”).

Voorbeelden

1

We hadden triviale groep $G = \{0\}$ en we hebben ook de triviale ring $R = \{0\}$. Dit is de enige ring waarbij $0 = 1$

2

Elke abelse groep $(G, +)$ kun je zien als ring met “triviale vermenigvuldiging” $a \times b = 0 \quad \forall a, b \in G$

3

$\mathbb{Z}$ is een ring:

- $(2\mathbb{Z})$ is een ring, maar heeft geen eenheid
- $\mathbb{Z}$ is geen delingsring/lichaam ($\mathbb{Q}$ wel!)

¹volgt uit 3. Beschouw $(1 + 1) \times (r + s)$

²eenheid van optelling

$\mathbb{Z}/n\mathbb{Z}$ heeft ook een vermenigvuldiging:

$$\bar{a} \times \bar{b} = \overline{ab}; \text{ hiermee wordt } \mathbb{Z}/n\mathbb{Z} \text{ een ring}$$

- $\mathbb{Z}/n\mathbb{Z}$ heeft een eenheid: $\bar{1}$
- $\mathbb{Z}/n\mathbb{Z}$ is commutatief (omdat $\mathbb{Z}$ dat is)
- Of $\mathbb{Z}/n\mathbb{Z}$ een lichaam is, hangt af van n :
we dagen dat $n = 6 \implies \bar{2} \times \bar{3} = \bar{6} = \bar{0}$, dus $\bar{2}, \bar{3}$ hebben geen multiplicatieve inverse.
maar $n = 5$ bijvoorbeeld wel (sterker nog, alle n priem)

Definitie.

- Een niet-nul element $r \in R$ is een nuldeeler als er ander niet-nul element $s \in R$ bestaat zodat $rs = 0$
- Een element $r \in R$ in een ring met eenheid is zelf een eenheid als er een $s \neq 0 \in R$ bestaat zodat $rs = 1$ (maw. Een element met een multiplicatieve inverse heet een eenheid)
De verzameling van eenheden in R heet $R^\times$

Lemma. $0 \times r = r \times 0 = 0 \quad \forall r \in R$

Bewijs. $0 \times r = (0 + 0) \times r = 0 \times r + 0 \times r$
dus $0 \times r = (0 \times r + 0 \times r) - (0 \times r) = 0$ □

Lemma. $(-r)s = s(-r) = -(rs) \quad \forall r, s \in R$ en $(-r)(-s) = rs$

Bewijs. $rs + (-r)s = (r + (-r))s = 0 \times s = 0$ dus $(-r)s = -(rs)$.

Evenzo voor $rs + r(-s) = 0$

En dus $(-r)(-s) - rs = (-r)(-s) + (-r)s = (-r)(-s + s) - (-r) \times 0 = 0$ □

Lemma. Als $1 \in R$ dan is die uniek en geldt $(-r) = (-1)r \quad \forall r \in R$

Bewijs. Stel dat er nog een eenheid bestaat: $1' \in R$.
Dan $1' = 1 \times 1' = 1$.

Deel 2 mag je lekker zelf doen. □

Lemma. $R^\times$ is een groep onder vermenigvuldiging.

Bewijs.

- Geslotenheid: als $r, s \in R^\times$ dan $\exists t, u \in R$ zodat $rt = 1$ en $su = 1$
Dus $(rs)(ut) = r(su)t = rt = 1$, dus $rs \in R^\times$
- Eenheid: $1 \in R^\times$

- Inverses: als $r \in R^\times$ dan $\exists t \in R$ zodat $rt = 1$ dus is $t = r^{-1} \in R^\times$

□

Voorbeelden

1

$$\mathbb{Z}^\times = \{1, -1\}$$

2

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$$

3

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : \text{ggd}(a, n) = 1\}$$

Opmerking. Als R een lichaam, dan $R^\times = R \setminus \{0\}$.

Definitie. Een (integraal)domein is een ring zonder nuldelers. Dus: iedere lichaam is een domein. Andersom hoeft niet te gelden! (bijv. $\mathbb{Z}$)

Stelling. in een domein geldt dat als $rs = rt$ (en $r \neq 0$) dan $s = t$.

Bewijs. $rs = rt \implies rs - rt = 0 \implies r(s - t) = 0$

En we werken in een domein, dus $s - t = 0 \implies s = t$ □

Definitie. Een deelring ($\neq$ delingsring!) (EN: subring) van een ring R is $S \leq R$. Het is een ondergroep en S is gesloten onder vermenigvuldiging.

Bijvoorbeeld, $\mathbb{Z} \leq \mathbb{Q}$, $2\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \not\leq \mathbb{Z}$

Voorbeeld. Een ring van functies.

Zij X een verzameling en T een ring. Zij $R = \{f : X \rightarrow T\}$

met optelling $f + g$ gedefiniëerd door $(f + g)(x) = f(x) + g(x)$ en vermenigvuldiging net zo, dus $(fg)(x) = f(x)g(x)$

1. $(R, +)$ is een abelse groep omdat $(T, +)$ dat is.
2. Vermenigvuldiging is associatief omdat de vermenigvuldiging in T dat is
3. Distributiviteit in R volgt ook uit die in T
 - R is commutatief $\iff T$ is commutatief
 - R heeft eenheid $f(x) = 1 \ \forall x \in X \iff T$ heeft eenheid 1

Quotes

“We mogen aftrekken, want we zijn in een groep”