

Groepen en Ringen

8078254

27 mei 2025

Stel X verzameling, T ring, $R = \{f : X \rightarrow T\}$ is een ring van functies.

Nuldeler: $r \neq 0$ zodat $\exists s \neq 0$

Als $f \neq 0$ maar wel $f(x) = 0$ voor een $x \in X$ dan: kies $g \in R$ zodat $g(x) = 0$ als $f(x) \neq 0$ en $g(x) \neq 0$ als $f(x) = 0$, dan $fg(x) = 0$

Eenheid: $f(x) \neq 0 \forall x \in X$

Voorbeeld (polynoomring).

Een polynoom is $f(x) = a_0 + a_1x + \dots + a_nx^n$ variabele $x, n \geq 0$ eindig.¹

a_i coëfficiënten, elementen van een ring R , commutatief en met eenheid.

Naamgeving: $n = \text{def}(f)$ is de graad van f . Deze functie is additief: $\text{def}(fg) = \text{def}(f) + \text{def}(g)$

Operaties op polynomen:

- optelling: $(a_0 + \dots + a_nx^n) + (b_0 + \dots + b_mx^m) = (a_0 + b_0) + (a_1 + b_1)x + \dots$
- vermenigvuldiging: $(a_0 + \dots + a_nx^n)(b_0 + \dots + b_mx^m) = \sum_{j=0}^{n+m} (\sum_{i=0}^j a_i b_{j-i}) x^j$

Definitie.

$R[x] = \{\text{polynomen in variabele } x \text{ met coëfficiënten in } R\}$

- commutatief (want R is dat ook)
- Eenheid $f = 1$

We hebben $R \leq R[x]$

$$r \mapsto f(x) = r \quad (\text{constant polynoom})$$

Matrixringen

we hebben al matrixringen gezien: GL_n, O_n, SO_n , groepen van $n \times n$ matrices

Voorbeeld. kies een ring R .

$$M_n(R) = \{n \times n \text{ matrices } A = (a_{ij})_{ij}, a_{ij} \in R\}$$

- Optelling: Voor $n = 2$ $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$
- Vermenigvuldiging: Matrixvermenigvuldiging
Merk op: niet commutatief voor $n \geq 2$
Eenheid is de identiteitsmatrix

Merk op: GL_n is geen ring, alleen een groep onder matrixvermenigvuldiging. $GL_n(R) = M_n(R)^*$

Definitie. Zij R, S twee ringen. Een ringhomomorfisme $\varphi : R \rightarrow S$ is zodat

$$\bullet \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\bullet \varphi(ab) = \varphi(a)\varphi(b)$$

Voorbeeld. Voor $R = \mathbb{Z} = S$, is $\varphi : n \mapsto 2n$ is wel een groepshomomorfisme ($\varphi(n+m) = 2(n+m) = 2n+2m = \varphi(n) + \varphi(m)$)

Maar géén ringhomomorfisme: $\varphi(nm) = 2nm \neq (2n)(2m) = \varphi(n)\varphi(m)$

Definitie. De kern van een ringhomomorfisme $\varphi : R \rightarrow S$ is $\{r \in R : \varphi(r) = 0\} = \text{Ker}(\varphi)$

$\text{Ker}(\varphi) \leq R$ deelring. (zie aantekeningen Valentijn voor bewijs.)

Het beeld is $\{\varphi(r) : r \in R\} = \text{im}(\varphi)$

$\text{im}(\varphi) \leq S$ deelring.

Als φ bijectief is, dus $\text{Ker}(\varphi) = \{0\}$ en $\text{im}(\varphi) = S$, dan is het een ringisomorfisme; dit geeft een equivalentie-relatie op ringen: $R \cong S$

$\text{Ker}(\varphi)$ heeft de eigenschap dat $a \in \text{Ker}(\varphi) \Rightarrow ra \in \text{Ker}(\varphi), ar \in \text{Ker}(\varphi), \forall r \in R$ want $\varphi(ra) = \varphi(r)\varphi(a) = 0, \forall r \in R$

Definitie. Een (links)ideaal I van een ring R is een $I \subset R$ zodat

- $I \leq R$ een deelring
- $rI = \{ri | i \in I\} \subset I, \forall r \in R$

Ook rechts-, en tweezijdig ideaal.

Als R commutatief, dan is ieder ideaal tweezijdig.

Notatie: $I \leq R$

Voorbeeld. iedere R heeft triviaal ideaal $0 \leq R$. Ook $R \leq R$. Anders “echt ideaal” (EN: “proper ideal”)

Voorbeeld. Idealen in $\mathbb{Z}$:

moeten additieve groepen zijn. Cyclisch!

$\langle n \rangle, \forall n \in \mathbb{Z}$ zijn allemaal ook idealen

Voorbeeld. De polynomen $xf(x)$ in $R[x]$ (met constante term 0) vormen ook een ideaal.

Voor ringen R, S ween we dat R/S weer een ring. De elementen van R/S zijn de nevenklassen $a + S, a \in R$

- Optelling: $(a + S) + (b + S) = (a + b) + S$
Dit is een additieve groep: $(R, +)$ is abels dus $S \leq R$ (ondergroep)

- Vermenigvuldiging: $(a + S)(b + S) = ab + S$ ($\star$)
Voor welgedefinieerd moet gelden: aks $a + S = a' + S$ en $b + S = b' + S$, dan $ab + S = a'b' + S$

We weten: $a + S = a' + S \iff a - a' \in S$, dus $a' + S = a + \alpha + S, \alpha \in S$. Evenzo voor $b' + S = b + \beta + S, \beta \in S$

¹Waar a_0 de constante term heet, en a_nx^n de kopterm

Dan $(a' + S)(b' + S) = (a + \alpha + S)(b + \beta + S) = ab + a\beta + \alpha b + \alpha\beta + S$

We willen dat dat uitkomt op $ab + S$, met andere woorden willen we dat $a\beta + \alpha b + \alpha\beta \in S$

$\alpha\beta$ zit in S vanwege de geslotenheid van de S . Dan moet nog gelden dat $a\beta \in S, \alpha b \in S, \forall a, b \in R$

Dus S moet een tweezijdig ideaal zijn.

Conclusie: $R/S = \{a + S : a \in R\}$ is een ring $\iff S \trianglelefteq R$ met optelling en verm. zoals hierboven.

Voorbeeld. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, dus $\mathbb{Z}/n\mathbb{Z}$ is een ring, zoals we al wisten.

Voor elk ringhomomorfisme $\varphi : R \rightarrow R$ is $\text{Ker}(\varphi) \trianglelefteq R$ een ideaal.

En andersom elk ideaal $I \trianglelefteq R$ is de kern van het ringhomomorfisme

$$\begin{aligned}\pi : R &\rightarrow R/I \\ r &\mapsto r + I\end{aligned}$$

isomorfismestellingen

1e

Voor een ringhomomorfisme $\varphi : R \rightarrow R'$ geldt $R/\text{ker}(\varphi) \simeq \text{im}(\varphi)$

2e

Zij R een ring, $A \leq R$ deelring, $B \trianglelefteq R$ ideaal, dan $A + B = \{a + b | a \in A, b \in B\} \leq R$ een deelring.

$A \cap B \trianglelefteq R$ een ideaal, en

$(A + B)/B \simeq A/(A \cap B)$

3e

Zij R een ring, $I, J \trianglelefteq R$ idealen, $I \subset J$, dan $J/I \trianglelefteq R/I$ en $(R/I)/(J/I) \simeq R/J$

“4e”

Zij $I \trianglelefteq R$ ideaal

Dan

$$\left\{ \begin{array}{l} \text{deelringen} \\ \text{zodat} \end{array} \begin{array}{l} S \leq R \\ I \subset S \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{l} \text{deelringen} \\ \text{van } R/J \end{array} \right\}$$