

18. Ringer og kropper

Def: En ring $(R, +, \cdot)$ er en ikke-tom mengde R med to binæroperasjoner $+$ og \cdot , slik at følgende holder:

(R1) $(R, +)$ er en abelsk gruppe (operasjonen $+$ er kommutativ)

(R2) Operasjonen \cdot er assosiativ: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(R3) Distributive lover: $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$

Ringen R er kommutativ hvis $a \cdot b = b \cdot a \quad \forall a, b \in R$.

Eksempler: (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (kommutative ringer)

(2) $M_n(\mathbb{R}) =$ alle $n \times n$ -matriser over \mathbb{R} (ikke kommutativ for $n > 2$)

(3) $\mathbb{R}[x] = \{ p(x) \mid p \text{ polynom i } x \text{ med koeff i } \mathbb{R} \}$ (kommutativ ring)

Merk: (1) Det er vanlig å kalle $+$ for "addisjon" og \cdot for "mult". Det er også vanlig å droppe tegnet " \cdot "; skrive "ab" for "a · b".

(2) Se å si alle ringer vi ser på her et multiplikativt identitetselement $1 \in R$: $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$. Hvis ikke annet nevnes, vil vi anta det.

(3) $(R, +)$ gruppe $\Rightarrow \exists$ additivt id-elt 0 .

Eksempler: (1) Mult. id. elt i $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$: 1 (talet 1)

(2) Mult. id. elt i $M_n(\mathbb{R})$: $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = I_n$

(3) Mult. id. elt i $\mathbb{R}[x]$: konstantpolynomet $p(x) = 1$

(4) For $n \geq 2$ er $(\mathbb{Z}_n, +_n, \cdot_n)$ en ring ($\mathbb{Z}_n = \{0, 1, \dots, n-1\}$) hvor
 $+_n =$ addisjon mod n
 $\cdot_n =$ mult mod n

Eks: i \mathbb{Z}_8 har vi $2+4 = 8 \pmod{8} = 0$

$$3 \cdot (5+1) = 3 \cdot 6 = 18 \pmod{8} = 2$$

$(\mathbb{Z}_n, +_n, \cdot_n)$ er en kommutativ ring med 1 som mult. id-elt.

Def: La R være en ring

- (1) Et element $a \in R$ er en enhet hvis $\exists b \in R$ med $ab = 1 = ba$
- (2) Ringen R kalles en divisjonsring hvis ethvert ikke-null elt $0 \neq a \in R$ er en enhet. Dvs $\forall 0 \neq a \in R \exists b \in R$ med $ab = 1 = ba$.
- (3) En kropp er en kommutativ divisjonsring.

Eksempler: (1) De eneste enhetene i \mathbb{Z} er 1 og -1. Derfor er \mathbb{Z} ikke en div.-ring (eller kropp).

(2) \mathbb{Q}, \mathbb{R} og \mathbb{C} er kopper: $\forall a \neq 0$ finnes b med $ab = 1$

(3) Er $M_2(\mathbb{R})$ en div.-ring?

(4) Når er \mathbb{Z}_n en kropp? Hva er enheten i \mathbb{Z}_n ?

Merk: (1) R kropp $\Leftrightarrow \{(R, +) \text{ og } (R \setminus \{0\}, \cdot) \text{ abelskgr, og } a(b+c) = ab+ac \forall a, b, c\}$

(2) For en ring R , la

$$U(R) = \{a \in R \mid a \text{ er en enhet}\}$$

Da er $(U(R), \cdot)$ en gruppe.
(3) $a \in U(R) \Rightarrow \exists \text{ kun én } b \in R \text{ med } ab = ba = 1 : b = b(ab^{-1}) = (ba)b^{-1} = b'$

Teorem 18.8 La R være en ring, og la O betegne det additivt id-elt. (finnes jo alltid siden $(R, +)$ er en gruppe).

(1) $0a = a0 = 0 \quad \forall a \in R$

(2) $a(-b) = (-a)b = -(ab)$

(3) $(-a)(-b) = ab$

Def: La R og S være ringer. En ringhomomorf er en funksjon

$$\phi: R \rightarrow S \text{ med}$$

(1) $\phi(a+b) = \underbrace{\phi(a)}_{\text{add i } R} + \underbrace{\phi(b)}_{\text{add i } S} \quad \forall a, b \in R$

(2) $\phi(ab) = \underbrace{\phi(a)}_{\text{mult i } R} \underbrace{\phi(b)}_{\text{mult i } S} \quad \forall a, b \in R$

Den er en isomorf hvis den er bijektiv. Kjernen = $\text{Ker } \phi = \{a \in R \mid \phi(a) = 0\}$

Merk: En ringhom $\phi: R \rightarrow S$ er spesielt en grupphom $\phi: (R, +) \rightarrow (S, +)$.

Eksmplar: (1) Har sett før at $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ gitt ved
 $a \mapsto a \pmod{n}$
er en gruppehom, dvs $\phi(a+b) = \phi(a) + \phi(b) \quad \forall a, b \in \mathbb{Z}$. Vis
at også $\phi(ab) = \phi(a) \cdot \phi(b)$! Dette viser ϕ er ringhom.
 $\text{Ker } \phi = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{n}\} = n\mathbb{Z}$

(2) La $R = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \mid a_{ij} \in \mathbb{C} \right\}$. Dette er en ring! Definer

$$\phi: R \longrightarrow \mathbb{C}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \mapsto a_{22}$$

La $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}$ og $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{pmatrix}$ var i R .

$$\phi(A+B) = \phi \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ 0 & a_{22}+b_{22} & a_{23}+b_{23} \\ 0 & 0 & a_{33}+b_{33} \end{pmatrix} = a_{22}+b_{22} = \phi(A)+\phi(B)$$

$$\begin{aligned} \phi(AB) &= \phi \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12}+a_{12}b_{11} & a_{11}b_{13}+a_{12}b_{12}+a_{13}b_{11} \\ 0 & a_{11}b_{22} & a_{11}b_{23}+a_{12}b_{22}+a_{13}b_{21} \\ 0 & 0 & a_{11}b_{33} \end{pmatrix} \\ &= a_{22}b_{22} = \phi(A)\phi(B) \end{aligned}$$

$\implies \phi$ ringhom

$$\text{Ker } \phi = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \mid a_{ij} \in \mathbb{C} \right\}$$

(3) R_1, \dots, R_t ringer $\implies R_1 \times \dots \times R_n$ ringer. (Samme konstruksjon som før gjører).

$$\begin{aligned} \phi_i: R_i &\longrightarrow R_1 \times \dots \times R_n \\ a &\mapsto (0, \dots, a, \dots, 0) \end{aligned}$$

$$\begin{aligned} \pi_i: R_1 \times \dots \times R_n &\longrightarrow R_i \\ (a_1, \dots, a_n) &\mapsto a_i \end{aligned}$$