Forelesning 4. mars 2024

Motivasjon: $\mathbb{Z}$: To operasjoner $+, \cdot$

Distributiv:

$M_n(\mathbb{R})$: To operasjoner $+, \cdot$

Defn. 18.1

$(R, +, \cdot)$ Ring

R_1 $\langle R, + \rangle$ abelsk gruppe

R_2 Multiplikasjon er assosiativ

R_3 Distributiv lov $a(b+c) = ab + ac$

$(a+b)c = ac + bc$.

Flere eksempler:

1) $F = \{f : \mathbb{R} \to \mathbb{R}\}$

2) $(\mathbb{Z}_n, +, \cdot)$

3) $R_1 \times R_2 \times \dots \times R_n$.

Thm 18.8

$a, b \in R$ ring

1) $0a = a0 = 0$
2) $a(-b) = (-a)b = -(ab)$
3) $(-a)(-b) = ab$

Bevis

1) $0 + 0a = 0a = (0+0)a = 0a + 0a \Rightarrow 0 = 0a$.

2) $a(-b) + ab = a(-b+b) = a0 = 0 \Rightarrow a(-b) = -(ab)$

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

$(-(-a)) + (-a) = 0$ og $a + (-a) = 0 \Rightarrow (-(-a)) = a$

$= ab$.

Defn 18.9

$\varphi : R \to R'$ Ringhomomorfi

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

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

Ex. 1). $F = \{f : \mathbb{R} \to \mathbb{R}\} \xrightarrow{\varphi_a} \mathbb{R}$ $a \in \mathbb{R}$

$\varphi_a(f) = f(a)$

2) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$

$a = q_1 n + r_1$ $\varphi(a) = r_1$

$b = q_2 n + r_2$ $\varphi(b) = r_2$

$\Rightarrow ab = q_1 q_2 n^2 + (q_1 r_2 + q_2 r_1) n + r_1 r_2 \Rightarrow \varphi(ab) = r_1 r_2$

Defn 18.12 $\varphi : R \to R'$ Ringshomomorfi φ bijektiv $\overset{\text{def}}{\iff}$ isomorfi

Defn. 18.14

$a, b \in R$ $ab = ba$: kommutativ ring.

$1 \in R$: Ring med enhet (enhetselement)

Ex. $\mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ $\gcd(r,s) = 1$

$1 \longmapsto (1,1)$

$n \longmapsto (a_1, a_2)$ $n = b_1 r + a_1 = b_2 s + a_2$

Injektiv: $n \longmapsto (0,0)$ betyr $n = b_1 r = b_2 s$ dvs $n = b \cdot rs$

sidan $\gcd(r,s) = 1$

Surjektiv: (a_1, a_2) Finn b_1, b_2 s.a $b_1 r + a_1 = b_2 s + a_2$

$\Rightarrow n = b_1 r + a_1 \longmapsto (a_1, a_2)$

Defn.

R ring $\quad R^* \subset R$ $\quad R^* = R \setminus \{0\}$ $\quad a \in R^*$ s.a. $a^{-1} \in R^*$ kalles MULTIPLIKATIV ENHET.

Defn 18.16

R ring kommutativ $\quad \forall x \in R^*, \exists\, y (= x^{-1}) \in R^*$ slik at $xy = 1$

$\Rightarrow$ R er en kropp

(Hvis ikke kommutativ: Divisjonsring eller skjevkropp)

Ex. $\mathbb{Z}_n$ er en kropp for n primtall

$x \in \mathbb{Z}_n$ hvis $\gcd(x,n) = 1$, sa°

$\exists\, s,t \in \mathbb{Z}$ slik at $xs + nt = 1$

dvs $xs \equiv 1 \pmod n$

$\Rightarrow s = x^{-1}$ i $\mathbb{Z}_n$

n: ikke primtall, f.eks $n = 15$

$\Rightarrow$ $5 \cdot m \neq 1 \mod 15$ siden $5m = \begin{cases} 0 \\ 5 \\ 10 \end{cases} \in \mathbb{Z}_{15}$

Ex. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ er kropper

Begrep: Underring, Underkropp. $K \leq L$

$\mathbb{Z}_{15} = \{0, 1, \ldots 14\}$ $\quad 3 \cdot 5 = 0$

Defn. 19.2

R ring $\quad a, b \neq 0$, $ab = 0$ i R

kalles NULL-DIVISORER

Nulldivisorer i $\mathbb{Z}_n$: Alle $x \in \mathbb{Z}_n$ s.a $\gcd(x,n) \neq 1$.

fordi $x \cdot \frac{n}{\gcd(x,n)} \equiv 0 \pmod n$

Ex. Løs ligningen $x^2 - 5x + 6 = 0$ i $\mathbb{Z}_{12}$

$x^2 - 5x + 6 = (x-3)(x-2) = 0$

$\Rightarrow$ $x = 2$, $x = 3$ løsninger

Men i $\mathbb{Z}_{12}$: $2 \cdot 6 = 3 \cdot 4 = 0$

$3 \cdot 8 = 6 \cdot 4 = 9 \cdot 4 = 8 \cdot 6 = 8 \cdot 6 = 0$

Kan vi ha

$x-2$	2	6	3	4	3	8	6	4	9	4	6	8	6	10	6	8	9
$x-3$	6	2	4	3	8	3	4	6	4	9	6	6	8	6	10	9	8
$x=$	4	8	5	6	5	10	8	6	11	6	8	10	8	0	8	10	11
	9	5	7	6	11	6	7	9	7	12	9	9	11	9	1	0	11

Løsninger $x = 2, 3, 6, 11$

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ $f(x) = x(x-1)(x-2)(x-3)(x-4)$

$= x^5 - 10x^4 + 35x^3 - 50x^2 + 24x$

En ring består av

- 0
- null-divisorer
- ikke-null-divisorer { Invertible elementer / Elementer uten invers

$\mathbb{Z}$: ingen null-divisorer, invertible elementer ± 1

$\mathbb{Q}$: kropp

$\mathbb{Z}_{12}$: - 0
- 2,3,4,6,8,9,10
- 1,5,7,11 $\quad 1^{-1}=1 \quad 5^{-1}=5 \quad 7^{-1}=7 \quad 11^{-1}=11$

$\mathbb{Z}_p$: - 0
p prim - invertible elementer } kropp

Defn 19.6.

R ring
- kommutativ
- (med enhet)
- uten null-divisorer

$\Rightarrow$ R INTEGRITETSOMRÅDE

Ex

Integritetsområder	Ikke integritetsområder
$\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$	$\mathbb{Z}_n$ n: ikke prim
$\mathbb{R}$, $\mathbb{C}$	$M_n(\mathbb{R})$

Thm 19.9 Enhver kropp er et integritetsområde

Bevis

La $a, b \in K$ slik at $ab = 0$, og slik at $a \neq 0$

Da $\exists\, a^{-1} \in K$ slikt at $aa^{-1} = 1$. Det gir

$$a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b = 0$$

Motsigelse

$\Rightarrow$ $ab \neq 0$ og K har ingen null-divisorer

Thm 19.11 Ethvert endelig integritetsområde er en kropp

Bevis La $x \in K, x \neq 0$ og $K = \{0, 1, x_2, \ldots, x_m\}$

$\Rightarrow xK = \{0, x, xx_2, \ldots, xx_m\}$

Hvis $xK = K$ $\exists\, x_i \in K$ slik at $xx_i = 1$

Hvis $xK \neq K$ så betyr det at $\exists\, i$ slik at

$$xx_i = 0 \quad \text{eller} \quad xx_i = xx_j$$

dvs $xx_i = 0$ eller $x(x_i - x_j) = 0$

Siden K er integritetsområde og $x \neq 0$

så må $x_i = 0$ eller $x_i - x_j = 0$

Motsigelse

$\Rightarrow \exists\, i$; $xx_i = 1$ og $x_i = x^{-1}$.

$\Rightarrow$ $\mathbb{Z}_p$ er en kropp, vi skriver $\mathbb{F}_p$