Forelesning 13. mars 2024

Defn. 26.1

$\varphi : R \to R'$ ringer

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

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

homomorfi av ringer

$\Rightarrow$ Bevarer struktur:

$\varphi(0) = 0$

$\varphi(-a) = -\varphi(a)$

$\varphi(1) = 1$

Gitt $\varphi : R \to R'$; $\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$

Egenskaper: - Abelsk gruppe

- $r \in R, x \in \ker \varphi \Rightarrow \varphi(rx) = \varphi(r)\varphi(x) = 0$ så $rx \in \ker \varphi$
- $\varphi(1) = 1 \neq 0$, så $1 \notin \ker \varphi$.

Defn 26.10

$I \subset R$ slik at $RI = IR = R$

additiv undergruppe

kalles et IDEAL

Spesielt er $\ker \varphi$ et ideal.

Siden $I \subset R$ er en normal undergruppe har vi

R/I

gruppe

Også ring! $(a+I)(b+I) = ab+I$ vel definert

$(1+I)(a+I) = a+I$

assosiativitet

distributivitet

$$I \hookrightarrow R \longrightarrow R/I$$

kvotienttring
eller
faktorring

Ekv.

Idealer i $\mathbb{Z}$: $(n) = n\mathbb{Z}$

i $\mathbb{Q}$ (kropp): (0) og $\mathbb{Q}$

i $F[x]$: $(f(x)) = \{ g(x) \cdot f(x) \mid g(x) \in F[x] \}$

i $F[x,y]$: $(f_1(x,y), f_2(x,y), \dots, f_n(x,y))$

$$= \sum_{i=1}^{n} p_i(x,y) f_i(x,y) \quad p_i(x,y) \in F[x]$$

$$(x) \hookrightarrow F[x] \longrightarrow F[x]/(x) \simeq F$$

$$(x^2+1) \hookrightarrow \mathbb{R}[x] \longrightarrow \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$$

$$(p) \hookrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/(p) \simeq \mathbb{Z}_p$$

$\mathbb{Z}$: int. domene; $\mathbb{Z}/(p)$: felt

Thm 27.5

$I \subset R$ ideal mng

Hvis $1 \in I$, så er $I = R$

Bevis. Vi har $I \subset R$, la $r \in R$

Da er $r = 1 \cdot r \in IR = I$, så $I = R$ □

Cor 27.6

F kropp

Eneste idealer er (0) og F.

Bevis La $x \neq 0$, $x \in I$. Da $\exists\, y \in F$ slik at $xy = 1$. $\Rightarrow 1 = xy \in I$, $F = I \underset{27.5}{\Rightarrow} I = F$. □

Defn 27.7.

$I \subset R$ ideal Hvis $I \subsetneq J \subset R$ betyr $J = R$ så er I et MAKSIMALT ideal

Ex. $(p) \subset \mathbb{Z}$ maks
primm

$(f(x)) \subset F[x]$ maks
irreduks

Thm 27.9

$I \subset R$ maks ideal $\iff$ R/I kropp

Bevis $\Leftarrow$ Anta $I \subsetneq J \subseteq R \Rightarrow J/I \subset R/I$
$\#$
$\Rightarrow J/I = R/I$ dvs $J = R$.

$\Rightarrow$ $a \notin I$
$a+I \in R/I$, fnta at $a+I$ ikke har noen invers $\Rightarrow 1+I \notin R/I(a+I)$
Men $R/I(a+I) \subsetneq R/I$ er et ideal

Betrakt $\varphi : R \longrightarrow R/I$

$\Rightarrow \varphi^{-1}(R/I(a+I)) \subset R$
ekte ideal som inneholder I
og $a \in \varphi^{-1}(R/I(a+I))$ side

$\varphi(a) = a+I = (1+I)(a+I) \in R/I(a+I)$

$$\begin{array}{ccccc} I & \subset & J & \subset & R \\ \downarrow & & \downarrow & & \downarrow \\ \{0\} = I/I & \subset & J/I & \subset & R/I \end{array}$$

1-1-korrespondanse mellan idealer i R som innehåller I och idealer i R/I

Ex

$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ kropp hvis $n=p$ primtall

Defn 27.13

$I \subset R$ — I ideal, R ring

I primideal $\overset{\text{def}}{\iff}$ $\forall a,b \in R$ sådan att $ab \in I$ har vi $a \in I$ eller $b \in I$

Alternativt $a,b \notin I \Rightarrow ab \notin I$

R integral domän $\iff$ $\{0\}$ primideal.

Thm 27.15

$I \subsetneq R$ — I ideal, R ring

R/I integritetsområde $\iff$ I primideal

Bevis

I prim, $a+I, b+I \in R/I$, $a,b \notin I$

Anta $(a+I)(b+I) = I$ dvs $ab \in I$

Motsägelse, R/I int. omr

R/I integritetsområde, $a,b \in R$, $a,b \notin I$

$\Rightarrow a+I, b+I \in R/I$, $a+I, b+I \neq I$

$\Rightarrow ab+I \neq I$ dvs $ab \notin I$

□

Thm 27.16

Maximala idealer är prim

Bevis

$I \subset R \Rightarrow R/I \Rightarrow R/I \Rightarrow I$

I max — R/I kropp — R/I integritetsområde — I primideal

Alternativt bevis.

$I \subset R$ maks, $a \notin I$ betyr $I \subsetneq I + Ra \subset R$, så $I + Ra = R$

dvs $\exists\, x \in I, r \in R$ slik at $x + ra = 1$

La $b \notin I$, da har vi

$$b(x + ra) = b$$

$$\Downarrow$$

$$bx + rab = b$$

Anta $ab \in I$. Det gir $bx + rab \in I$, altså $b \in I$ Motsigelse

$\Rightarrow ab \notin I$ og I er prim.

Eks.

Prim/maks idealer i

$\mathbb{Z}_n$, $\mathbb{Z}$, $\mathbb{Z}[x]$, $F[x]$, $F[x,y]$, $\mathbb{Q}$

F kropp

$\mathbb{R}[x]$ $\quad$ $\mathbb{C}[x]$

Defn 27.21

$R \ni a$ ring $\quad I = aR = (a)$ Hovedideal (Principal ideal) generert av a.

Thm 27.24

$\{0\} \neq I \subset F[x] \Rightarrow I = (a)$

ideal, kropp

Bevis La $f \in I$ være av lavest grad. For $g(x) \in I$ kan vi skrive $g(x) = q(x) f(x) + r(x)$ hvor $\deg(r) < \deg(f)$. Det betyr at $r(x) = 0$ eller $r(x) \notin I$. Hvis $r(x) = 0$ har vi $g(x) \in (f(x))$ og hvis $r(x) \neq 0$ har vi $r(x) = g(x) - q(x) f(x) \in I$ som er en motsigelse $\square$

Defn 45.7 Et integritetsområde der alle idealene er hovedidealer kalles et hovedidealområde (Principal ideal domain : PID).

Ex $\xi_p^p = 1, \ \xi_p \neq 1$

$\mathbb{Z}[\xi_p]$

def ⇙ PID

p regulært primtall

$x^p + y^p = z^p$ kan (enkelt) bevises ikke å ha løsninger

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ~~37~~
41, 43, 47, 53, ~~59~~, 61, ~~67~~ 71, 73, 79, 83
89, 97. (< 100)