Lektion 6

Def: Låt R, S vara ringer.

En ring homomorfism fra R til S är en avbildning $\varphi: R \to S$ s.a.

- $\varphi(0_R) = 0_S$ (inte nödvendig)
- $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$
- $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$
- $\varphi(1_R) = 1_S$

Eks. $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$

$z \mapsto z \bmod m$

$$5 \cdot 3 \bmod 2 = 15 \bmod 2 = 1$$

$$\| $$

$$1 \cdot 1 \bmod 2 = 1 \bmod 2$$

Def: En homomorfism $\varphi: R \to S$ är en isomorfism om det finnes en homomorfism $\psi: S \to R$ s.a.

$\psi \circ \varphi = id_R$, $\varphi \circ \psi = id_S$ $\left(\Leftrightarrow \varphi \text{ hom \&} \atop \varphi \text{ bij.}\right.$

Slogan: Isomorfe ringer är "det samma", själv om mengdorna R, S är inte lika.

93 $f: R \to S$ hom., $g: S \to T$ hom.

Visa att $g \circ f$ är hom. Bevis: Låt $r, s \in R$

i) $(g \circ f)(r+s) = g(f(r+s))$ (Gå igjennom definitionen)

$= g(f(r) + f(s))$

$= g(f(r)) + g(f(s))$

$= (g \circ f)(r) + (g \circ f)(s)$

ii) $(g \circ f)(r \cdot s) = g(f(r \cdot s))$

$= g(f(r) \cdot f(s))$

$= g(f(r)) \cdot g(f(s)) = (g \circ f)(r) \cdot (g \circ f)(s)$

iii) $(g \circ f)(1_R) = g(f(1_R)) = g(1_S) = 1_T$.

94 Låt $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.

Visa att $\varphi: R \to \mathbb{C}$, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$ är en isomorfism.

$\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \leftarrow a+bi \text{ är uppenbart invers} \right]$

i) $\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) = \varphi \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} =$

$(a+c) + i(b+d) = a + bi + c + di = \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$.

ii) $\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) = \varphi \begin{pmatrix} \underline{ac - bd} & \underline{ad + bc} \\ \underline{-bc - ad} & \underline{-bd + ac} \end{pmatrix} = ac - bd + (ad + bc)i$

$\|$

$\varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \varphi\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = (a+bi)(c+di) = ac - bd + (ad + bc)i$

iii) $\varphi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 + 0 \cdot i = 1$ $\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1_R \right]$

φ är en hom. För att vara en iso måste φ vara inverterbar.

Inversen: $\psi: \mathbb{C} \to R$, $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

$\psi \circ \varphi = id_R$ och $\varphi \circ \psi = id_{\mathbb{C}}$ är "uppenbart".

95| Är $f: \mathbb{Z}_9 \to \mathbb{Z}_{12}$, $x \mapsto 4x$ väldefinierad? En hom?

• $\mathbb{Z}_9 = \{\bar 0, \bar 1, \bar 2, \dots, \bar 8\}$ Beror f på vilka repr. vi tar från en restklasse?

$4\cdot 1 \equiv_{12} 4\cdot 10 \equiv_{12} 4\cdot 19$ där $1 \equiv_9 10 \equiv_9 19$?

Anta att $\bar a = \bar b$ i $\mathbb{Z}_9 \Leftrightarrow a + k\cdot 9 = b$, $k\in\mathbb{Z}$.

$4(b) = 4(a+k\cdot 9) = 4a + k\cdot 9\cdot 4 = 4a + k\cdot 3\cdot 12$

$\Leftrightarrow \overline{4b} = \overline{4a}$ i $\mathbb{Z}_{12}$

• $f(\bar a + \bar b) = \overline{4\cdot(a+b)} = \overline{4a+4b} = \overline{4a} + \overline{4b} = f(\bar a) + f(\bar b)$

• mod 9
• mod 12

Men $4xy = 4x\,4y$? $\quad f(\bar 1\cdot \bar 1) = \overline{4\cdot 1} = \bar 4$

$\qquad\qquad\qquad\qquad f(\bar 1)\cdot f(\bar 1) = \bar 4\cdot\bar 4 = \overline{16}$

Ja... men ⇐

⇒ f är inte en hom. fordi $f(\bar 1) = \bar 4 \neq \bar 1$ i $\mathbb{Z}_{12}$

96| Visa att en hom. $f: R\to S$ sender inv. element til inv.

Låt $r\in R$ vara inv. $\Rightarrow \exists\, r^{-1}\in R: rr^{-1} = 1_R = r^{-1}r$

$1_S = f(1_R) = f(r\cdot r^{-1}) = f(r)\cdot f(r^{-1})$

$\Rightarrow f(r)^{-1} = f(r^{-1})$. (Och $f(r)\cdot f(r^{-1}) = f(rr^{-1}) = f(r^{-1}r) = f(r^{-1})f(r)$)

97| Låt $f: R\to S$ vara en monomorfism. Visa att
f tar nolldelare til nolldelare. ⇕ f inj.

Låt $r\in R$ vara en nolld.: $\exists\, s\in R: r\cdot s = 0,\ s\neq 0$.

$0_S = f(0_R) = f(r\cdot s) = f(r)\cdot f(s)$

För att vara en nolldelare måste $f(r)\neq 0 \neq f(s)$!

Men f inj. $\Rightarrow |f^{-1}(\{x\})| \le 1$ för alla $x\in S$.

$\Rightarrow (f(s) = 0_S \Leftrightarrow s = 0_R)$.

98| Låt $f: R\to S$ vara en iso. Visa att
$r\in R$ irr. $\Leftrightarrow f(r)\in S$ irr.

Det rekker att visa „⇒".

$r = xy \in R \Rightarrow x$ inv. eller y inv.

Anta att $f(r) = s\cdot t \in S$.

$\Rightarrow r = f^{-1}(f(r)) = f^{-1}(s)\cdot f^{-1}(t)$

$\overset{r\text{ irr.}}{\Longrightarrow} f^{-1}(s)$ inv. eller $f^{-1}(t)$ inv.

$\overset{96|}{\Longrightarrow} f(f^{-1}(s)) = s$ inv. eller $f(f^{-1}(t)) = t$ inv.

101| Låt R och S vara isomorfe via $\varphi: R \to S$. Visa att

a) R komm. $\Leftrightarrow$ S komm.

"$\Rightarrow$" $r, s \in R$. $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$

$$\begin{aligned} \varphi(r\cdot s) &= \varphi(r)\cdot\varphi(s) \\ \| \quad & \\ \varphi(s\cdot r) &= \varphi(s)\cdot\varphi(r) \end{aligned}$$

Notis: Alla $x \in S$ kan skrivas som $\varphi(r)$ för en $r \in R$.

b) R int.om. $\Leftrightarrow$ S int.omr.

"$\Leftarrow$" $r, s \in R$, $\varphi(r) \cdot \varphi(s) = 0$.

$\Leftrightarrow$ $\varphi(r \cdot s) = 0$ $\Leftrightarrow$ $r \cdot s = 0$ $\Leftrightarrow$ $r = 0 \vee s = 0$

$\Leftrightarrow$ $\varphi(r) = 0 \vee \varphi(s) = 0$.

c) R kropp $\Leftrightarrow$ S kropp

Följer fra 96|. $\varphi(R^*) = S^*$ fordi φ bij.

d) R fakt. $\Leftrightarrow$ S fakt.

"$\Rightarrow$" $s \in S$, kan faktoriseras via

i) $\varphi^{-1}(s) \in R$.

ii) R fakt.: $\varphi^{-1}(s) = r_1 \cdots r_n \cdot c$ $\quad r_i$ irr., $c \in R^*$

iii) $s = \varphi(r_1) \cdots \varphi(r_n) \cdot \varphi(c)$ med $\varphi(r_i)$ irr., $\varphi(c) \in S^*$ (96| och 97|)

Om $s = t_1 \cdots t_m \cdot d$, t_i irr., $d \in S^*$

så är $\varphi^{-1}(s) = \varphi^{-1}(t_1) \cdots \varphi^{-1}(t_m)\, \varphi^{-1}(d) = r_1 \cdots r_n c$ med

$\varphi^{-1}(t_i)$ irr., $\varphi^{-1}(d) \in R^*$

$\xrightarrow{R \text{ fakt.}}$ $n = m$, $\varphi^{-1}(t_i) \sim r_j$ för unika (i,j).

$\Rightarrow$ $t_i \sim \varphi(r_j)$ för unika (i,j) $\Rightarrow$ faktoriseringen av s är entydig upp till associerade element.

102| Låt R vara komm. av karaktäristik p, p prim.

Visa att $a \mapsto a^p$ är en hom.

$(a+b)^p = a^p + b^p$ "Freshman's dream"

i) $(a+b)^p \overset{(*)}{=} \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$

(*) Binomialsatsen gäller i varje komm. ring.

$= 1 \cdot a^0 b^p + \underline{\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}} + 1 \cdot a^p \cdot b^0$

$= b^p + \underline{0} + a^p$

Heltal fordi $p \nmid i!$ för $0 < i < p$
$p \nmid (p-i)!$

• fordi $\binom{p}{i} = \frac{p!}{i!(p-i)!} = p \cdot \frac{(p-1)!}{\underline{i!(p-i)!}} = 0$ i char. p.

ii) $(a \cdot b)^p = a^p b^p$ stämmer i varje komm. ring.

iii) $1_R^p = 1_R$

106| Vilka är isomorfe?

a) $\mathbb{Z}_{45}$ och $\mathbb{Z}_5 \times \mathbb{Z}_9$? Använd KRS.

$\mathbb{Z}_{45} = \mathbb{Z}/45\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ fordi $45\mathbb{Z} = (5\mathbb{Z}) \cdot (9\mathbb{Z})$

c) $\mathbb{Z}_{24}$ och $\mathbb{Z}_7 \times \mathbb{Z}_3$ inte isom. fordi

char: $24 \neq 21$