Algebraiska strukturer, 6 mars, 11 mars

HOMOMORFIER AV RINGAR

En avbildning $\Phi : R \to S$ mellan ringar kallas en **ringhomomotfi**, eller bara **homomorfi** om

- $\Phi(a+b) = \Phi(a) + \Phi(b)$ för alla $a, b \in R$.
- $\Phi(ab) = \Phi(a)\Phi(b)$ för alla $a, b \in R$.

Alltså är Φ speciellt en grupphomomorfi mellan de additiva grupperna i R och S ($\Phi(0_R) = 0_S$, $\Phi(-a) = -\Phi(a)$, $\Phi(na) = n\Phi(a)$, $\forall a \in R$).

En ringisomorfi = en bijektiv ringhomomorfi.

Exempel 1. Definiera $\Phi : \mathbb{Z} \to \mathbb{Z}_n$ genom $\Phi(k) = [k]_n$. Då är Φ en ringhomomorfi men ej isomorfi.

2. Definiera $\Phi : \mathbb{C} \to M_2(\mathbb{R})$ genom

$$\Phi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Φ är en injektiv ringhomomorfi:

$$\Phi((a+ib)+(c+id)) = \Phi((a+c)+i(b+d)) =$$
$$\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} =$$
$$\Phi(a+ib) + \Phi(c+id),$$

$$\Phi((a+ib)(c+id)) = \Phi((ac-bd)+i(ad+bc)) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$
$$\Phi(a+ib)\Phi(c+id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

BILD OCH KÄRNA

Om $\Phi : R \to S$ är en ringhomomorfi ges **bilden** till Φ av

$$\Phi(R) = Im\Phi = \{\Phi(a) \in S \mid a \in R\}$$

och **kärnan** till Φ av

$$\ker \Phi = \{a \in R \mid \Phi(a) = 0_S\}$$

IDEAL

En delring I till en ring R är ett **ideal** om $ab \in I$ och $ba \in I$ för alla $a \in R$ och alla $b \in I$. Det betyder att I är invariant under multiplikation med alla element i ringen.

Exempel 1. $n\mathbb{Z}$ är ett ideal i $\mathbb{Z}$.
2. $\mathbb{Z}$ är ej ideal i $\mathbb{Q}$, ty $\frac{1}{2} \in Q$, $1 \in \mathbb{Z}$, men $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

Sats 45.1. Låt $\Phi : R \to S$ vara en ringhomomorfi. Då gäller att

(i) $\Phi(R)$ är en delring i S.
(ii) $\ker \Phi$ är ett ideal i R.
(iii) Φ är injektiv omm $\ker \Phi = \{0_R\}$.

Bevis. Eftersom Φ är en grupphomomorfi mellan de additiva grupperna har vi att $\Phi(R)$ och $\ker \Phi$ är additiva delgrupper till $(S, +)$ respektive $(R, +)$. Det räcker nu att se på multiplikationen.

(i) Om $b = \Phi(a)$ och $b' = \Phi(a')$ i $\Phi(R)$ är

$$bb' = \Phi(a)\Phi(a') = \Phi(aa') \in \Phi(R)$$

dvs $\Phi(R)$ är sluten under multiplikation. Detta visar att $\Phi(R)$ är en delring i S.

(ii) Om $a \in R$ $b \in \ker \Phi \Leftrightarrow ab, ba \in \ker \Phi$, ty

$$\Phi(ab) = \Phi(a)\Phi(b) = \Phi(a)0_S = 0_S$$
$$\Phi(ba) = \Phi(b)\Phi(a) = 0_S\Phi(a) = 0_S$$

vilket visar att $\ker \Phi$ är sluten under multiplikation och därmed är en delring i R, och att $\ker \Phi$ är ett ideal.

(iii) samma som för grupper.

Varje element a i en ring R genererar ett ideal (a) (ett **huvudideal**, det minsta ideal som innehåller a) som består av alla element som kan skrivas $\sum_i b_i a c_i$ för b_i, c_i i R.

Om R är kommutativ , $a \in R$, så är

$$(a) = \{ra \mid r \in R\}.$$

Exampel. 1. Varje ideal i $\mathbb{Z}$ är ett huvudideal.

Bevis. Låt I vara ett ideal i $\mathbb{Z}$, $I \neq \{0\}$ och låt k vara det minsta positiva heltal som ligger i I. Då har vi att $km \in I$ för alla $m \in \mathbb{Z}$ och därmed $k\mathbb{Z} \subseteq I$. Antag att det finns $x \in I$ som inte tillhör $k\mathbb{Z}$. Enligt divisionsalgoritmen, $x = kq + r$, där $q, r \in \mathbb{Z}$ och $0 < r < k$. Eftersom $x \in I$, $kq \in I$, får vi att $x - kq = r \in I$ som strider mot minimalitetet av k. Därför $I = k\mathbb{Z} = (k)$.

2. Varje ideal i $K[x]$ är ett huvudideal (skall bevisas senare)

3. Om K är en kropp då saknar K icke-trivialla ideal I, dvs $I \neq \{0\}$, $I \neq K$.

Bevis. Om I är ett ideal, $I \neq \{0\}$, har I ett element $r \neq 0$. Då har vi att $r^{-1}r = 1 \in I$ (varje element $r \neq 0$ i en kropp har en invers) och $s \cdot 1 \in I$ för alla $s \in K$, som medför att $I = K$.

KVOTRINGAR

Låt I vara ett ideal i en ring R. Eftersom I är en delgrupp i den additiva gruppen i R kan vi definiera R/I som en abelsk grupp (med operation $+$: $(a+I)+(b+I)=(a+b)+I$).

Lemma. Om I är ett ideal i en ring R gäller att

$$a+I=c+I \text{ och } b+I=d+I \Rightarrow ab+I=cd+I.$$

Bevis. $a+I=c+I \Rightarrow (a-c)\in I$, och $b+I=d+I \Rightarrow (b-d)\in I$. Därmed gäller att

$$ab-cd=ab-ad+ad-cd=a(b-d)+(a-c)d$$

som ligger i I eftersom I är invariant under multiplikation med element i R.

Vi kan nu definiera en ringstruktur på R/I:

$(a+I)+(b+I)=(a+b)+I, \quad (a+I)\cdot(b+I)=ab+I,$ för alla $a,b\in R$.

Övning. Visa att R/I med de två operationerna är en ring. Denna ring kallas **kvoten av R med I**.

Exempel. $(n)=n\mathbb{Z}$ är ett ideal i ringen $\mathbb{Z}$ och kvoten $\mathbb{Z}/n\mathbb{Z}$ är $\mathbb{Z}_n$.

ISOMORFISATS

Om I är ett ideal i R finns en naturlig surjektiv homomorfi

$$\Phi : R \to R/I$$

genom $\Phi(a)=a+I$, för alla $a\in R$.

Sats. Om $\theta : R\to S$ är en ringhomomorfi då är

$$R/\ker\theta \approx \theta(R).$$

Bevis Definiera $\Phi : R/\ker\theta \to \theta(R)$ genom $\Phi(a+\ker\theta)=\theta(a)$. Eftersom vi vet att det är en isomorfi av abelska grupperna $(R/\ker\theta,+)$ och $(\theta(R),+)$ (se fundamentala homomorfisatsen för grupper) räcker det att visa att multiplikationen bevaras.

$$\Phi((a+\ker\theta)(b+\ker\theta))=\Phi(ab+\ker\theta)=$$
$$=\theta(ab)=\theta(a)\theta(b)=\Phi(a+\ker\theta)\Phi(b+\ker\theta).$$

KVOTRINGAR AV $K[x]$

Polynomet x^2+1 saknar nollställe i $\mathbb{R}$, men har ett nollställe i den större kroppen $\mathbb{C}$ ($\mathbb{R}\subset\mathbb{C}$). De komplexa talen fås från de reella talen precis genom att lägga till ett nollställe, som vi kallar i, till polynomet $x^2+1\in\mathbb{R}[x]$. Vi får se vidare att $\mathbb{C}\approx\mathbb{R}[x]/(x^2+1)$.

Om vi har något polynom som saknar nollställe i $K[x]$ kan vi uppfinna ett nollställe till polynomet genom att betrakta en ny

kropp L, som "innehåller" K och är av typen $K[x]/(p(x))$, där p är ett irreducibelt polynom i $K[x]$.

Sats 40.2 (47.2) Om K är en kropp, $p(x) = a_0 + a_1x + \ldots + a_nx^n$ är ett polynom av grad n i $K[x]$, och I är idealet $(p(x))$ i $K[x]$ så gäller att

(i) varje sidoklass kan skrivas entydigt som

$$I + (b_0 + b_1x + \ldots + b_{n-1}x^{n-1}),$$

där $b_0, b_1, \ldots, b_{n-1} \in K$.

(ii) $\{I + b : b \in K\}$ är en delkropp till $K[x]/I$ som är isomorf med K.

Bevis. (i) Låt $I + f(x) \in K[x]/I$. Enligt divisionsalgoritmen kan $f(x)$ skrivas som $f(x) = q(x)p(x) + r(x)$ med $q, r \in K[x]$, där $grad\ r(x) < grad\ p(x)$ eller $r(x) = 0$. Eftersom $f(x) - r(x) = q(x)p(x) \in I$ får vi att $f(x) \in I + r(x)$ och

$$I + f(x) = I + r(x).$$

Vidare,

$$I + (b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) = I + (c_0 + c_1x + \ldots + c_{n-1}x^{n-1})$$

medför att

$$(b_0 - c_0) + (b_1 - c_1)x + \ldots + (b_{n-1} - c_{n-1})x^{n-1} \in I$$

och

$$(b_0 - c_0) + (b_1 - c_1)x + \ldots + (b_{n-1} - c_{n-1})x^{n-1} = 0,$$

ty alla nollskilda polynom $s(x)$ i I har grad större eller lika med $grad\ p(x) = n$. Alltså kan vi konstatera att $c_0 = b_0, \ldots, c_{n-1} = b_{n-1}$ och varje sidoklass i $K[x]$ kan representeras av exakt ett polynom $b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$.

(ii) Betrakta funktionen $\Phi : \{I+b : b \in K\} \to K$, $\Phi(I+b) = b$, $b \in K$.

Anmärkning. Låt $p(x) \in K[x]$ och $I = (p(x))$. Då gäller att $I + f(x) = I + r(x)$, där $r(x)$ är resten vid division av $f(x)$ med $p(x)$.

Exempel. Ringen $\mathbb{R}[x]/(x^2 + 1)$ är isomorf med de komplexa talen $\mathbb{C}$.

Bevis. Varje sidoklass i $\mathbb{R}[x]/I$, där $I = (x^2 + 1)$, kan skrivas entydigt som $a+bx+I$, där $a, b \in \mathbb{R}$. Avbildningen $\Phi : \mathbb{R}[x]/I \to \mathbb{C}$ som ges av $\Phi(a + bx + I) = a + ib$ är väldefinierad eftersom alla sidoklasser i $\mathbb{R}[x]/I$ har en unik representant av grad högst 1. Vidare är den bijektiv och uppfyller

(i) om vi betecknar $a + bx + I = [a + bx]$, då är

$$\Phi([a + bx] + [c + dx]) = \Phi([(a + c) + (b + d)x]) = (a + c) + i(b + d) = (a + ib) + (c + id) = \Phi([a + bx]) + \Phi([c + dx])$$

(ii)

$$\Phi([a+bx]\cdot[c+dx]) =$$
$$\Phi(ac+(ad+bc)x+bdx^2+I) =$$
$$\Phi(ac-bd+(ad+bc)x+I) =$$
$$(\text{ty } bdx^2 = bd(x^2+1)-bd \in -bd+I) =$$
$$ac-bd+(ad+bc)i = (a+bi)\cdot(c+di) =$$
$$\Phi([a+bx])\Phi([c+dx]).$$

Alltså är $\mathbb{R}[x]/I$ isomorf med $\mathbb{C}$.

Polynomet x^2+1 har ett nollställe i $\mathbb{R}[x]/I$ (på grund av isomorfi $a \mapsto a+I$, $a \in \mathbb{R}$ skall koeficienterna a i polynomet interpreteras som $a+I=[a]$): $\alpha=[x]$ uppfyller $\alpha^2+[1]=[0]$, ty $[x]^2+[1]=[x^2+1]=[0]$.

Sats 40.1 (47.1) Om K är en kropp och $p(x) \in K[x]$ så gäller att $K[x]/(p(x))$ är en kropp omm $p(x)$ är irreducibelt i $K[x]$.

Bevis. Antag att $p(x)$ är irreducibelt och låt $I=(p(x))$. Antag att $g(x)+I \neq I$ dvs $g(x) \notin I$ vilket är ekvivalent att $p(x)$ inte delar $g(x)$.

Då är $SGD(p(x),g(x))=1$ och därmed finns det polynom $h(x)$, $l(x) \in K[x]$ så att

$$1 = SGD(p(x),g(x)) = p(x)h(x)+g(x)l(x).$$

Vidare är $1-g(x)l(x)=p(x)h(x) \in I$ och $g(x)l(x)+I=1+I$. Detta innebär att

$$(l(x)+I)(g(x)+I)=1+I.$$

Elementet $g(x)+I$ är alltså inverterbart med inversen $l(x)+I$.

Antag att $p(x)$ inte är irreducibelt och $grad\ p(x)>0$, dvs $p(x)=a(x)b(x)$, där $a(x)$, $b(x) \in K[x]$ är av $grad \geq 1$. Då är

$$a(x)b(x)+I=I$$

och därmed

$$(a(x)+I)(b(x)+I)=I$$

som medför att $a(x)+I$ är en nolldelare i $K[x]/I$. Alltså är $K[x]/(p(x))$ inte en kropp.

Om $grad\ p(x)=0$ eller $p(x)=0$ är $K[x]/(p(x))$ inte någon kropp heller (Varför?)

Sats 40.3 (47.3) Om K är en kropp så gäller att varje ideal i $K[x]$ är ett huvudideal.

Bevis. Låt I vara ett ideal i $K[x]$. Om $I=\{0\}$ då är det huvudideal. Låt $I \neq \{0\}$ och låt $p(x)$ vara ett polynom av minsta grad i I. Då är $p(x)q(x) \in I$ för varje $q(x) \in K[x]$ och därmed $(p(x)) \subset I$. Låt $f(x) \in I$. Enligt divisionsalgoritmen kan $f(x)$ skrivas som $f(x)=q(x)p(x)+r(x)$ där $q(x)$, $r(x) \in K[x]$ och $grad\ r(x) < grad\ p(x)$ eller $r(x)=0$. Eftersom $f(x)$, $q(x)p(x) \in I$ får vi att $f(x)-q(x)p(x)=r(x) \in I$ och därför $r(x)=0$, dvs $f(x) \in (p(x))$. Alltså är $I=(p(x))$.

SPLITTRINGSKROPP

Varje polynom med koeficienter i en kropp kan uppdelas i förstagradsfaktorer i en lämlig utvidgning av denna kropp.

Sats. Låt K vara en kropp och $p(x)$ vara ett irreducibelt polynom. Då existerar en kropp $L \supseteq K$ sådan att p har ett nollställe i L.

Bevis. Låt $L = K[x]/(p(x))$ och $I = (p(x))$. Vi vet att L är en kropp och att den innehåller en delkropp som är isomorf med K så att vi kan identifiera varje element $I + b \in L$ med $b \in K$.

Låt $p(x) = a_0 + a_1x + \ldots + a_nx^n$ och låt α beteckna elementet $I + x \in L$. Då

$$p(\alpha) = a_0 + a_1(I + x) + \ldots + a_n(I + x)^n =$$
$$I + (a_0 + a_1x + \ldots + a_nx^n) = I + p(x) = I$$

vilket är noll i L.

Sats. Låt $p(x) \in K[x]$ och grad $p(x) \geq 1$. Då existerar en kropp $L \supseteq K$ sådan att p är en produkt av förstagradsfaktorer i $L[x]$.