KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2008-02-27

1. KINESISKA RESTSATSEN

Sats 1.1 (Kinesiska restsatsen)**.** *Om R är en kommutativ ring med etta och $I_1, I_2, \ldots, I_n$ är en uppsättning ideal som uppfyller*

$$I_i + I_j = R, \qquad 1 \leq i, j \leq n$$

så är den naturliga homomorfin

$$\Phi : R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

surjektiv med kärna $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$ och därmed

$$R/I_1 I_2 \cdots I_n \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

Bevis. Vi börjar med att konstatera att kärnan till homomorfin ges av $I = I_1 \cap I_2 \cap \cdots \cap I_n$. För att visa att homomorfin är surjektiv använder vi att $I_i + I_j = R$ och att vi därför kan hitta element $x_{ij} \in I_i$ som uppfyller

$$x_{ij} + x_{ji} = 1, \qquad 1 \leq i, j \leq n.$$

Vi kan nu bilda elementen

$$y_i = \prod_{j \neq i} x_{ji} = \prod_{j \neq i} (1 - x_{ij}) \in 1 + I_i, \qquad i = 1, 2, \ldots, n.$$

På grund av konstruktionen ligger $y_i \in I_j$ för alla $j \neq i$ och därför har vi att

$$\Phi(a_1 y_1 + a_2 y_2 + \cdots + a_n y_n) = (a_1 + I_1, a_2 + I_2, \ldots, a_n + I_n)$$

och Φ är surjektiv.

Det återstår att visa att $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$. Vi kan använda induktion över n och basfallet $n = 1$ är trivialt. Vi kan därför anta att $J = I_2 \cap I_3 \cap \cdots \cap I_n = I_2 I_3 \cdots I_n$. Vidare har vi att

$$I_1 + J = R$$

eftersom $1 = (x_{12} + x_{21})(x_{13} + x_{31}) \cdots (x_{1n} + x_{n1}) \in I_1 + J$. Vi kan nu ta ett element a i $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cap J$ och får att

$$a = ax + ay$$

där $x \in I_1$ och $y \in J = I_2 I_3 \cdots I_n$, vilket visar att $a \in I_1 J = I_1 I_2 \cdots I_n$. □

Exempel 1.1. Om $f(x) = g(x)h(x)$ i polynomringen $\mathrm{R}[x]$ och $g(x)$ och $h(x)$ är relativt prima får vi att

$$\mathbb{R}[x]/f(x) \cong \mathbb{R}[x]/(g(x)) \times \mathbb{R}[x]/(h(x)).$$

För gruppringen $\mathbb{R}Z_2$ har vi till exempel att

$$\mathbb{R}Z_2 \cong \mathbb{R}[x]/(x^2-1) \cong \mathbb{R}[x]/(x-1) \times \mathbb{R}[x]/(x+1) \cong \mathbb{R} \times \mathbb{R}.$$

2. Euklidiska områden

Definition 2.1. Ett *Euklidiskt område* är ett integritetsområde R där det finns en norm $N : R \longrightarrow \mathbb{N}$ så att det för alla a, b i R med $b \neq 0$ finns en kvot k och en rest r med

$$a = bk + r$$

där $N(r) < N(b)$ eller $r = 0$.

Anledningen till att det kallas för ett Euklidiskt område är att vi då kan använda Euklides algoritm för att finna den största gemensamma delaren mellan två element i ringen.

Definition 2.2. Euklides algoritm tar två element a, b i ringen och definierar en följd $r_0, r_1, r_2 \ldots$, rekursivt genom $r_0 = a$, $r_1 = b$ och

$$r_k = k_{k+2}r_{k+1} + r_{k+2}$$

där k_{k+2} och r_{k+2} är kvot och rest vid division av r_k med r_{k+1}.

Eftersom normen är strikt avtagande måste resten till slut bli noll och den sista nollskillda resten är den största gemensamma delaren mellan a och b. Dessutom kan vi gå baklänges i algoritmen och utttrycka denna sista nollskilda rest som

$$r_n = \lambda a + \mu b$$

där λ och μ är element i ringen.

Sats 2.1. *Varje ideal i ett Euklidiskt område är principalt.*

Bevis. Vi kan välja d i I som det element som har minst norm och enligt divisionsalgoritmen måste varje annat element a i I vara delbart med d, eftersom vi annars resten vid division med d skulle vara ett element i I med lägre norm än d. □

Definition 2.3. Den *största gemensamma delaren* d mellan två element, a och b, i en kommutativ ring är ett element som delar a och b och alla gemensamma delare mellan a och b. Vi skriver $d = \mathrm{sgd}(a, b)$.

3. Principalidealområden

Sats 3.1. *I ett principalidealområde R kan vi finna den största gemensamma delaren mellan två element a och b som generatorn till (a, b). Denna är unikt bestämd upp till multiplikation med inverterbara element i R.*

Bevis. Om $(a, b) = (d)$ har vi att d delar a och b, och om något annat element d delar både a och b har vi att $(d) = (a, b) \subseteq (d')$ och därmed delar d' också d. Två olika generatorer till (d) skiljer bara med multiplikation med en enhet eftersom $(d) = (d')$ innebär att $d = kd'$ och $\ell d = d'$, vilket ger $0 = (1 - \ell k)d'$ och k är inverterbart. □

Sats 3.2. *I ett principalidealområde är varje nollskilt primideal ett maximalideal.*

Bevis. Tag ett nollskilt primideal $P = (a)$ och ett maximalideal $\mathfrak{m} = (b)$ som innehåller P. Vi har då att $(a) \subseteq (b)$, dvs att $a = kb$, för något k i R. Eftersom kb tillhör P som är ett primideal, måste $k \in P$ eller $b \in P$. Om $k \in P$ har vi att $k = a\ell$ för något ℓ i R, vilket ger

$$a = a\ell b \iff a(1 - \ell b) = 0$$

vilket ger att b är inverterbart vilket motsäger att $\mathfrak{m} = (b)$ var ett maximalideal. Alltså måste b ligga i P och $P = \mathfrak{m}$ är ett maximalideal. □

Vi får som en följd av detta att $R[x]$ är ett principalidealområde om och endast om R är en kropp, eftersom (x) alltid är ett primideal, men bara ett maximalideal om R är en kropp.