KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS ANTECKNINGAR 2009-02-24

1. Egenskaper hos ideal

För en mängd A i en ring R kan vi bilda det minsta ideal (A) som innehåller A och vi kan bilda

$$RAR = \{r_1a_1s_1 + \cdots + r_ma_ms_m | r_i, s_i \in R, a_i \in A\}$$

som är ett ideal som innehåller A. Precis som för delgrupper får vi att $(A) = RAR$. Vi kan göra liknande för vänster- och högerideal.

Ett ideal som kan skrivas $(a_1, a_2, \ldots, a_m)$ kallas *ändligt genererat* och om det räcker med en enda generator är det ett *principalideal*.

Definition 1.1 (maximalideal). Ett ideal $\mathfrak{m} \in R$ är ett *maximalideal* om det inte är innehållet i något annat äkta ideal.

Med hjälp av Zorns lemma kan man visa att varje ideal är innehållet i ett maximalideal om det finns en etta i ringen. Då är ett ideal äkta om och endast om det inte innehåller ettan.

Zorns lemma säger att en partiellt ordnad mängd där varje totalordnad delmängd (*kedja*) har en övre gräns har ett maximalt element. Vi använder Zorns lemma på mängden av äkta ideal som innehåller det givna idealet och visar att varje kedja av ideal i denna mängd har en övre gräns som ges av unionen av idealen.

Definition 1.2 (primideal). Ett äkta ideal P i en kommutativ ring R är ett *primideal* om

$$ab \in P \iff a \in P \text{ eller } b \in P.$$

Sats 1.1. *I en kommutativ ring R är I ett primideal om och endast om R/P är ett integritets-område.*

Bevis. Vi ser att $(a+I)(b+I) = I$ är detsamma som att $ab \in I$, och därmed är $(a+I)(b+I) = 0$ i R/I detsamma som att $ab \in I$. □

Sats 1.2. *I en kommutativ ring R med etta är I ett maximalideal om och endast om R/I är en kropp.*

Bevis. Om $a \in R$ inte är inverterbar modulo I så kan vi bilda $(a) + I$ som är ett äkta ideal som innehåller I. Om I är maximalt måste varje $a \notin I$ vara inverterbart modulo I eftersom $(a) + I$ inte kan vara äkta. □

2. Fraktionsringar

Om R är en kommutativ ring och D är en icke-tom delmängd av icke-nolldelarna i R som inte innehåller 0 och är sluten under multiplikation kan vi bilda en fraktionsring $D^{-1}R$ som har följande egenskaper:

$i)$ $D^{-1}R$ är en kommutativ ring med etta.
$ii)$ Det finns en injektiv homomorfi $R \longrightarrow D^{-1}R$ och varje element i D avbildas på ett inverterbart element i $D^{-1}R$.
$iii)$ $D^{-1}R$ är minimal i den meningen att det för varje annan ring S med ovanstående två egenskaper finns en injektiv homomorfi $D^{-1}R \longrightarrow S$ genom vilken $R \longrightarrow S$ faktoriserar.

Vi kan konstruera $D^{-1}R$ som mängden av ekvivalensklasser av $R \times D$ under ekvivalensrelationen

$$(a, c) \sim (b, d) \iff ad = bc.$$

Vi skriver $[a, c]$ för ekvivalensklassen som innehåller (a, c) och definierar addition och multiplikation genom

$$[a, c] + [b, d] = [ad + bc, cd] \quad \text{och} \quad [a, c] \cdot [b, d] = [ab, cd].$$

Vi behöver konstatera att dessa operationer är väldefinerade, dvs att

$$(a, c) \sim (a', c'), \quad (b, d) \sim (b', d') \Longrightarrow (ad + bc, cd) \sim (a'd' + b'c, c'd'), (ab, cd) \sim (a'b', c'd')$$

Detta kan vi se genom att

$$(a'd' + b'c')cd - (ad + bc)c'd' = (a'c - ac')dd' + (b'd - bd')cc' = 0$$

och

$$abc'd' - a'b'cd = (ac' - a'c)bd' + (bd' - b'd)a'c = 0.$$

Vidare behöver vi se att operationerna uppfyller ringaxiomen, att multiplikationen är kommutativ och att det finns en etta. Allt detta följer från egenskaperna hos operationerna på R.

Den injektiva homomorfin $R \longrightarrow D^{-1}R$ ges av $a \mapsto [ab, b]$ för något b i D och ettan ges av klassen $[b, b]$ för något $b \in D$.

Om vi nu har en annan ring S med de två översta egenskaperna kan vi få en injektiv homomorfi

$$D^{-1}R \longrightarrow D^{-1}S \cong S$$

genom att skicka $[a, d]$ till $\phi(a)\phi(d)^{-1}$, där $\phi : R \longrightarrow S$ är den injektiva homomorfin som ges av $i)$. Detta är en väldefinierad homomorfi vars kärna ges av klasser $[a, d]$ som uppfyller $\phi(a)\phi(d)^{-1} = 1$ i S, men detta innebär att $\phi(a) = \phi(d)$ och eftersom ϕ är injektiv måste $a = d$. Alltså är $[a, d] = [d, d] = 1$ i $D^{-1}R$, och homomorfin $D^{-1}R \longrightarrow S$ är injektiv.

3. Kinesiska restsatsen

Från heltalsaritmetiken känner vi till kinesiska restsatsen som att $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, men det visar sig att detta är ett specialfall av något mycket mer generellt.

Sats 3.1 (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 $a \in I_1 J = I_1 I_2 \cdots I_n$. $\square$

Exempel 3.1. 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

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

Rekommenderade uppgifter

7.4 Egenskaper hos ideal. 4, 5, 7, 9, 15, 16, 23, 40

7.5 Fraktionsringar. 2, 3, 4

7.6 Kinesiska restsatsen. 1, 2, 3, 5, 7