KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2009-02-26

Vi ska se på några egenskaper som är gemensamma mellan heltalen, $\mathbb{Z}$, och polynomringen i en variabel över en kropp, $k[x]$. Bland annat har vi i båda fallen unik faktorisering och Euklides algoritm för att hitta största gemensamma delare mellan element.[1]

1. Euklidiska områden

Definition 1.1 (Euklidiskt område). 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 1.2 (Euklides algoritm). *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 1.1. *Varje ideal i ett Euklidiskt område är principalt.*

[1] Föreläsningen behandlar avsnitt 8.1-8.3 i Abstract Algebra [1].

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 1.3 (Största gemensamma delare). Om a och b är två element i en kommutativ ring är den *största gemensamma delaren*, d, mellan a och b, ett element som delar både a och b och som dessutom delas av alla andra gemensamma delare mellan a och b. Vi skriver $d = \mathrm{sgd}(a, b)$.

2. Principalidealområden

Sats 2.1. *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 2.2. *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.

3. Områden med unik faktorisering

Definition 3.1 (Unik faktorisering, irreducibla element). Ett integritetsområde R har *unik faktorisering* om varje element kan skrivas som en produkt av irreducibla element på ett sätt som är unikt upp till permutation av faktorerna och multiplikation med inverterbara element.

Ett *irreducibelt* element är ett nollskilt element som inte kan skrivas som en produkt av två andra element utan att något av dem är inverterbart.

Sats 3.1. *Om R är ett principalidealområde är ett nollskilt element a irreducibelt om och endast om (a) är ett primideal.*

Bevis. Antag att a är irreducibelt. Då är (a) ett nollskilt ideal och därmed innehållet i ett maximalideal $\mathfrak{m} = (b)$. Alltså kan vi skriva $a = kb$ för något k, men eftersom a är irreducibelt och b inte är inverterbart så måste k vara inverterbart och $(a) = (b) = \mathfrak{m}$, som är ett primideal.

Om (a) är ett primideal och $a = bc$ måste vi ha $b \in (a)$ eller $c \in (a)$. Om $b = ka$ får vi $a = kac$, vilket är detsamma som $a(1 - kc) = 1$, och c är inverterbart. På samma sätt får vi att b är inverterbart om $c \in (a)$. □

Sats 3.2. *Ett principalidealområde har unik faktorisering.*

Bevis. Ett element är antingen irreducibelt, eller kan skrivas som en produkt av två faktorer. Vi kan då fortsätta och se om dessa faktorer är irreducibla eller inte. Om a inte kan skrivas som en produkt av irreducibla element får vi en oändlig sekvens av ideal

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq (a_3) \cdots$$

genom att vi väljer a_{k+1} som den faktor av a_k som inte går tt skriva som en produkt av irreducibla element. Genom att ta unionen av denna kedja av ideal får vi ett ideal (b) och vi måste då ha att $b \in (a_k)$ för något heltal k. Därmed måste $(b) \subseteq (a_k)$, men också $(a_k) \subseteq (b)$, vilket ger $(b) = (a_k) = (a_{k+1}) = \cdots$, vilket motsäger att $a_k = b_{k+1}a_{k+1}$, där b_{k+1} inte är inverterbar.

Alltså kan varje element i R skrivas som en produkt av irreducibla element och det återstår att visa att denna representation är unik upp till permutation av faktorerna och multiplikation med inverterbara element.

Om det finns element som inte har en sådan unik representation kan vi utgå från att

$$a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_n$$

där inget av $a_1, a_2, \ldots, a_m$ delar något av $b_1, b_2, \ldots, b_n$, eftersom vi kan dela båda sidor med eventuella gemensamma faktorer. Eftersom (a_1) är ett primideal måste någon av faktorerna ligga i (a_1), vilket ger en motsägelse eftersom vi antagit att inte a_1 delar något av $b_1, b_2, \ldots, b_n$. □

4. Gaussiska heltal

I ringen $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ finns en norm $N(a + ib) = a^2 + b^2$ som gör ringen till ett Euklidiskt område. Alltså har vi unik faktorisering och vi kan fråga oss vilka element som är irreducibla.

Till att börja med ser vi att $a+bi$ är irreducibelt om $N(a+bi) = a^2+b^2$ är ett primtal, eftersom normen är multiplikativ. Om vi har ett irreducibelt element $a+ib$ där $N(a+bi)$ inte är ett primtal kan vi se på de reella elementen i idealet som genereras av $a + bi$. Dessa bildar då ett primideal (p) och det betyder att $p \in (a + ib)$. Om vi nu skriver $p = (a + bi)(c + id)$ får vi att

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

och eftersom p är ett primtal måste nu $a^2 + b^2 = p$, eftersom vi annars har att $a + ib$ eller $c + di$ är en enhet.

Alltså ges de irreducibla elementen i $\mathbb{Z}[i]$ av de reella primtal som inte kan faktoriseras i $\mathbb{Z}[i]$ och de $a + bi$ som uppfyller $a^2 + b^2 = p$, för något reellt primtal p.

Sats 4.1. *Ett primtal $p \neq 2$ kan skrivas som $a^2 + b^2$ för heltal a och b om och endast om*

$$p \equiv 1 \pmod 4.$$

Bevis. Antag att p är ett udda primtal. Se först på när vi kan lösa ekvationen $x^2 + 1 = 0$ över $\mathbb{Z}_p$. Detta kan vi göra precis när det finns ett element av ordning fyra i $\mathbb{Z}_p^*$, dvs precis om $p - 1$ är delbart med fyra. Om $a^2 + b^2 = p$ får vi en lösning till $x^2 + 1 = 0$ i $\mathbb{Z}_p$ genom att dela restklassen till a med restklassen till b. Om vi har en lösning där p delar $x^2 + 1 = (x + i)(x - i)$ i $\mathbb{Z}[i]$ så kan inte p vara irreducibelt, eftersom det då skulle ha delat en av faktorerna. Alltså måste $p = (a + ib)(a - ib) = a^2 + b^2$. □

REKOMMENDERADE UPPGIFTER

8.1 Euklidiska områden. 1, 2, 4, 5, 7, 9

8.2 Principalidealområden. 2, 3

8.3 Områden med unik faktorisering. 5, 6

REFERENSER

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.