KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2008-02-29

1. Områden med unik faktorisering

Definition 1.1. 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 element som inte kan skrivas som en produkt av två andra element utan att något av dem är inverterbart.

Sats 1.1. *Om R är ett principalidealområde är 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 1.2. *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 $b_1, b_2, \ldots, b_n$. □

2. 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 2.1. *Ett primtal $p \neq 2$ kan skrivas som $a^2 + b^2$ för heltal a och b om och endast om*

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