



KTH Teknikvetenskap

**SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2008-03-03**

1. POLYNOMRINGAR

Vi har redan tidigare definierat polynomringen $R[x]$ för en godtycklig ring R . I själva verket kan vi göra det på många olika sätt och ett annat sätt att göra det är att se det som en delring i gruppringen $R\mathbb{Z}$. När vi går vidare och ska se på polynomringar i flera variabler finns ännu fler möjligheter.

Definition 1.1. Polynomringen i n variabler x_1, x_2, \dots, x_n över R kan definieras som

$$R[x_1, x_2, \dots, x_n] = S[x_n]$$

där $S = R[x_1, x_2, \dots, x_{n-1}]$ är polynomringen i $n - 1$ variabler över R .

Definition 1.2. Polynomringen i n variabler x_1, x_2, \dots, x_n över R kan också definieras som delringen av gruppringen $R\mathbb{Z}^n$ som genereras av R och de n fria generatorerna till \mathbb{Z}^n .

Vi kan också gå vägen över icke-kommutativa polynom och definiera den icke-kommutativa polynomringen som en delring av gruppringen över R för den fria gruppen på n symboler. Vi får då en icke-kommutativ polynomring $R\langle x_1, x_2, \dots, x_n \rangle$ och kan se den kommutativa polynomringen $R[x_1, x_2, \dots, x_n]$ på två olika sätt:

- (1) $R[x_1, x_2, \dots, x_n]$ är de symmetriska polynomen i $R\langle x_1, x_2, \dots, x_n \rangle$, dvs de polynom som fixeras under verkan av den symmetriska gruppen S_d på polynom av grad d .
- (2) $R[x_1, x_2, \dots, x_n]$ är kvoten av $R\langle x_1, x_2, \dots, x_n \rangle$ med idealet som genereras av $\{x_i x_j - x_j x_i \mid i \leq j\}$.

I varje fall kan vi se att varje polynom i $R[x_1, x_2, \dots, x_n]$ kan skrivas som en ändlig summa av monom, $ax_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$.

För att se att polynomringen $R[x_1, x_2, \dots, x_n]$ har unik faktorisering är det praktiskt att använda sig av den induktiva definitionen och visa följande sats:

Sats 1.1. $R[x]$ är ett område med unik faktorisering om och endast om R är det.

För att kunna bevisa det använder vi Gauss lemma.

Sats 1.2 (Gauss lemma). Om R är ett område med unik faktorisering och k är dess fraktionsskropp så är ett polynom $f(x)$ reducibelt i $R[x]$ om och endast om det är reducibelt i $k[x]$.

Bevis. Om polynomet är reducibelt i $R[x]$ är det uppenbart reducibelt i k eftersom R är en delring i k . Om vi har en faktorisering $f(x) = g(x)h(x)$ i $k[x]$ kan vi multiplicera detta med produkten av alla nämnare för att få en ekvation

$$af(x) = bG(x)H(x)$$

där $G(x)$ och $H(x)$ är polynom i $R[x]$ som är multipler $g(x)$ och $h(x)$ med element i R och där a och b är element i R .

Om a har en irreducibel faktor p kan vi se på ekvationen i kvotringen $R/(p)[x]$ där den säger att

$$0 = \bar{b} \cdot \bar{G}(x) \cdot \bar{H}(x).$$

Eftersom $R/(p)$ är ett integritetsområde är $R/(p)[x]$ också det och vi får att någon av faktorerna måste vara noll, dvs p delar antingen b , $G(x)$ eller $H(x)$. Vi kan därför dela hela ekvationen $af(x) = bG(x)H(x)$ med irreducibla faktorer till a tills vi har $f(x) = b'G'(x)H'(x)$ och $f(x)$ är reducibelt i $R[x]$. \square

Bevis av Sats 1.1. Om $R[x]$ är ett område med unik faktorisering har vi unik faktorisering av alla konstanta polynom, vilket betyder att R har unik faktorisering.

Antag därför att R är ett område med unik faktorisering och med fraktionskropp k . Vi kan skriva varje polynom $f(x)$ i $R[x]$ som ett element a i R gånger ett polynom $g(x)$ i $R[x]$ där det inte finns någon gemensam faktor mellan alla koefficienter. Eftersom R har unik faktorisering kan vi skriva a som en produkt av irreducibla element i R . Det återstår att visa att $g(x)$ kan skrivas som en produkt av irreducibla polynom.

Eftersom $g(x)$ också ligger i $k[x]$ som är ett område med unik faktorisering då k är en kropp, kan vi faktorisera $g(x)$ som en produkt av irreducibla polynom i $k[x]$. Enligt Gauss lemma får vi nu att varje sådan faktorisering leder till en faktorisering av $g(x)$ i $R[x]$. Det kan inte finnas någon gemensam delare mellan alla koefficienter i någon av faktorerna, eftersom detta skulle leda till en gemensam faktor mellan koefficienterna i $g(x)$. Alltså är faktorerna också irreducibla i $R[x]$.

Att bevisa att faktoriseringen är unik följer precis samma idé som beviset att faktoriseringen i ett principalidealområde är unik. \square