KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2008-03-04

1. Eisensteins irreducibilitetskriterium

Sats 1.1 (Eisensteins kriterium). *Om ett moniskt polynom $f(x)$ med koefficienter i ett integritetsområde har alla övriga koefficienter i ett primideal P så är $f(x)$ irreducibelt om inte konstanttermen ligger i P^2.*

Bevis. Antag att det finns en faktorisering $f(x) = g(x)h(x)$ och reducera denna ekvation modulo P. Vi får då att $\overline{f(x)} = \overline{x^n} = \overline{g(x)} \cdot \overline{h(x)}$ i $(R/P)[x]$ som är ett integritetsområde, men det betyder att konstanttermerna i både $\overline{g(x)}$ och $\overline{h(x)}$ är noll, vilket visar att konstanttermen i $f(x)$ måste ligga i P^2. □

2. Polynomringar över kroppar

Sats 2.1. *Om vi kan faktorisera ett moniskt polynom $f(x) = f_1(x)^{m_1} f_2(x)^{m_2} \cdots f_k(x)^{m_k}$ där $f_1(x), f_2(x), \ldots, f_k(x)$ är relativt prima så är*

$$k[x]/(f(x)) \cong k[x]/(f_1(x)^{m_1}) \times k[x]/(f_2(x)^{m_2}) \times \cdots \times k[x]/(f_k(x)^{m_k}).$$

Bevis. Detta är en direkt följd av den kinesiska restsatsen, eftersom idealen $(f_i(x)^{m_i})$ och $(f_i(x)^{m_i})$ är komaximala för $i \neq j$. □

Sats 2.2 (Faktorsatsen). *Om $a_1, a_2, \ldots, a_m$ är distinkta rötter till polynomet $f(x)$ i $k[x]$ är $f(x)$ delbart med $(x - a_1)(x - a_2) \cdots (x - a_m)$.*

Bevis. Vi får att $x - a_i$ är en faktor i $f(x)$ eftersom $f(x)$ ligger i kärnan till avbildningen $k[x] \longrightarrow k[x]/(x - a_i)$. Eftersom rötterna är distinkta är faktorerna relativt prima och då måste produkten dela $f(x)$ i och med att $k[x]$ har unik faktorisering. □

Sats 2.3. *Varje ändlig delgrupp till den multiplikativa gruppen i en kropp är cyklisk.*

Bevis. Antalet element som uppfyller $x^n = 1$ är enligt faktorsatsen högst n för varje heltal n. En cyklisk grupp har precis n element som uppfyller $x^n = 1$ för varje n som delar gruppens ordning. Om gruppen inte är cyklisk kommer det att finnas för många element av någon ordning, eftersom det totala antalet element fortfarande skall vara lika stort. □

3. Polynomringar i flera variabler och Gröbnerbaser

Definition 3.1. En kommutativ ring med etta är *noethersk* om varje ideal är ändligt genererade.

Sats 3.1 (Hilberts bassats)**.** *Om R är noethersk så är $R[x]$ noethersk.*

Vi hoppar över beviset av denna sats, men konstaterar att det följer att polynomringar över en kropp är noetherska.

Sats 3.2. *Om k är en kropp är $k[x_1, x_2, \ldots, x_n]$ noethersk.*

Bevis. Vi vet redan att k är noehtersk eftersom den bara har idealen (0) och (1). Genom induktion över n får vi därmed att $k[x_1, x_2, \ldots, x_n] = k[x_1, x_2, \ldots, x_{n-1}][x_n]$ är noethersk eftersom $k[x_1, x_2, \ldots, x_{n-1}]$ är det. $\square$

För att kunna göra beräkningar i polynomringar behöver vi kunna göra prioriteringar och därför inför man monomordningar. Ett monom är ett polynom med bara en term, men oftast menar vi egentligen monom med koefficient 1, dvs $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$.

Definition 3.2 (Monomordning)**.** En välordning av monomen är en *monomordning* om den respekterar multiplikationen av monom, dvs

$$m' \leq m'' \Longrightarrow mm' \leq mm''.$$

Givet en monomordning kan vi se på ledande termer i polynom.

Definition 3.3. För ett polynom $f(x)$ i $k[x_1, x_2, \ldots, x_n]$ är den ledande termen $LT(f)$ det monom som har störst ordning bland monomen i $f(x)$. För ett ideal I är det *initialidealet*, $\mathrm{in} I$, det ideal som genereras av de ledande termerna för alla polynom i I.

Exempel 3.1.