LUNDS UNIVERSITET

Matematikcentrum
Matematik NF

Polynompotenser

Kjell Elfström

Med ett konstant polynom skall vi mena ett polynom, som antingen är nollpolynomet, eller vars gradtal är noll. Vi låter genomgående A vara ett integritetsområde med entydig primfaktorisering. Då är också $A[x]$ ett integritetsområde med entydig primfaktorisering, och om Q är fraktionskroppen till A, så är $Q[x]$ en euklidisk ring. Om f och g är relativt prima polynom i $A[x]$, följer det av detta att det finns h och k i $A[x]$ och $c \neq 0$ i A, sådana att $hf + kg = c$. Vi antar vidare att det till varje icke-konstant polynom $f \in A[x]$ finns ett element $a \in A$, sådant att elementet $f(a)$ är skilt från noll och inte inverterbart.

Ringen $A = \mathbf{Z}$ av hela tal uppfyller dessa förutsättningar. Fraktionskroppen Q är då kroppen $\mathbf{Q}$ av rationella tal.

Definition 1 Låt $f \in A[x]$ och $p \in A$. Vi säger att p delar f och skriver $p \,||\, f$, om det finns ett $a \in A$, sådant att $p \mid f(a)$.

Lemma 1 Låt f vara ett icke-konstant polynom i $A[x]$. Då finns det oändligt många icke-associerade primelement $p \in A$, sådana att $p \,||\, f$.

Bevis Enligt förutsättningarna antar f ett värde, som varken är noll eller inverterbart. Det följer att det finns minst ett primelement p, sådant att $p \,||\, f$. Antag att de icke-associerade primelementen $p_1, p_2, \ldots, p_m$ delar f. Låt a och b vara element i A, sådana att $f(a) = b \neq 0$. Då är polynomet

$$g(x) = \frac{1}{b} f(a + bp_1 \cdots p_m x) \in A[x]$$

icke-konstant. Det gäller vidare att $g(c) \equiv 1 \pmod{p_1 \cdots p_m}$ för varje $c \in A$. Det måste därför finnas ett primelement p, ej associerat med $p_1, p_2, \ldots, p_m$, sådant att $p \,||\, g$. Eftersom då också $p \,||\, f$, visar detta påståendet. ■

Lemma 2 Låt f och g vara relativt prima polynom i $A[x]$, och antag att f inte är konstant. Då finns det ett primelement $p \in A$ och ett element $a \in A$, sådana att $p \mid f(a)$ och $p \nmid g(a)$.

Bevis Eftersom f och g är relativt prima, finns det polynom h och k i $A[x]$ och ett element $c \neq 0$ i A, sådana att $hf + kg = c$. Det finns enligt lemma 1 oändligt många icke-associerade primelement $p \in A$, sådana att $p \,||\, f$. Eftersom bara ändligt många av dessa delar c, finns det ett primelement p, sådant att $p \,||\, f$ och $p \nmid c$. Det finns därför ett element $a \in A$, sådant att $p \mid f(a)$. Eftersom $p \nmid c$, så kan inte p dela $g(a)$. ■

Lemma 3 Låt f och g vara relativt prima polynom i $A[x]$, och antag att f är irreducibelt och inte konstant. Då finns det ett primelement $p \in A$ och ett element $a \in A$, sådana att $p \mid f(a)$, $p^2 \nmid f(a)$ och $p \nmid g(a)$.

Bevis Eftersom f är irreducibelt och inte konstant, så är f och f' relativt prima. Det följer att f och $h = f'g$ är relativt prima. Det finns därför enligt lemma 2 ett primelement $p \in A$ och ett element $c \in A$, sådana att $p \mid f(c)$ och $p \nmid h(c)$. Det gäller då också att $p \mid f(c+p)$ och $p \nmid h(c+p)$. Eftersom $p^2 \mid f(c+p) - f(c) - pf'(c)$, kan det inte vara så, att p^2 delar både $f(c)$ och $f(c+p)$. Om $p^2 \mid f(c+p)$, kan vi välja $a = c$ och annars $a = c + p$. ■

Sats 1 Låt $f \in A[x]$ och $n \in \mathbf{Z}_+$, och antag att det till varje $a \in A$ finns ett $b \in A$, sådant att $f(a) = b^n$. Då finns det ett polynom $g \in A[x]$, sådant att $f = g^n$.

Bevis Om $n = 1$, eller f är konstant, så är påståendet trivialt. Vi kan därför antaga att $n \geq 2$ och att f inte är konstant. Eftersom man har entydig faktorisering i $A[x]$, så är

$$f = \varepsilon f_1^{n_1} \cdots f_m^{n_m},$$

där ε är ett inverterbart element i A, $m \geq 1$, $n_i > 0$, $i = 1, \ldots, m$, och $f_1, \ldots, f_m$ är icke-associerade irreducibla polynom i $A[x]$. Välj nu heltal q_i och r_i, $i = 1, \ldots, m$, sådana att $n_i = nq_i + r_i$ och $0 \leq r_i < n$. Vi kan då skriva

$$f = \varepsilon g^n f_1^{r_1} \cdots f_m^{r_m},$$

där $g = f_1^{q_1} \cdots f_m^{q_m}$.

Antag att $r_i > 0$ för något i. Om polynomet $f_1^{r_1} \cdots f_m^{r_m}$ är konstant, kan vi, eftersom f inte är konstant, välja ett element $a \in A$, sådant att $f(a) \neq 0$. Vi får att antalet förekomster av primelementet $p = f_i$ i faktoriseringen av $f(a)$ inte är delbart med n, vilket motsäger förutsättningarna.

Om polynomet $f_1^{r_1} \cdots f_m^{r_m}$ inte är konstant, kan vi efter eventuell omnumrering antaga att $r_1 > 0$ och att f_1 inte är konstant. Sätt $h = f_2^{r_2} \cdots f_m^{r_m}$, där produkten skall tolkas som 1, om $m = 1$. Enligt lemma 3 finns det ett primelement $p \in A$ och ett element $a \in A$, sådana att $p \mid f_1(a)$, $p^2 \nmid f_1(a)$ och $p \nmid h(a)$. Att detta strider mot förutsättningarna inser man på samma sätt som i det förra stycket.

Därför är $f = \varepsilon g^n$. Eftersom f inte är konstant, kan vi välja ett $a \in A$, sådant att $f(a) \neq 0$. Det finns enligt förutsättningarna ett $b \in A$, sådant att $f(a) = b^n = \varepsilon(g(a))^n$, och det följer att $\varepsilon = (b/g(a))^n$. Detta visar att $f = (bg/g(a))^n$. ■

Korollarium 1 Låt $f \in Q[x]$ och $n \in \mathbf{Z}_+$, och antag att det till varje $a \in Q$ finns ett $b \in Q$, sådant att $f(a) = b^n$. Då finns det ett polynom $g \in Q[x]$, sådant att $f = g^n$.

Bevis Om $f = 0$, är påståendet trivialt. Låt i annat fall c vara en minsta gemensamma multipel till koefficienternas nämnare. Då gäller det att $h = c^n f \in A[x]$. Om $a \in A$, så finns det ett $b \in Q$, sådant att $h(a) = b^n$, och eftersom $h(a) \in A$, så gäller det att $b \in A$. Enligt sats 1 finns det därför ett polynom $k \in A[x]$, sådant att $h = k^n$, och det följer att $f = g^n$, där $g = k/c \in Q[x]$. ■