Torben Hansen
20091714

Rationelle moniske polynomier og et specialtilfælde

Jeg vil i det følgende bevise sætningen

Sætning Lad $f, g \in \mathbb{Q}[X]$ og antag f, g er moniske samt $fg \in \mathbb{Z}[X]$. Så gælder $f, g \in \mathbb{Z}[X]$

og give et alternativt bevis for et specialtilfælde af overstående sætning.

Vi lægger ud med specialtilfældet: Lad $r, s \in \mathbb{Q}$ og antag $r + s \in \mathbb{Z}$ samt $rs \in \mathbb{Z}$. Så vil $r, s \in Z$.

Bevis Antag WLOG $r, s \neq 0$, ellers fås resultatet af betingelsen $r + s \in \mathbb{Z}$. Da r og s er rationelle tal kan vi skrive $r = \frac{p}{q}$ og $s = \frac{v}{w}$ hvor $p, q, v, w \in \mathbb{Z} \setminus \{0\}$. vi kan yderligere antage WLOG $\gcd(p, q) = 1$ og $\gcd(v, w) = 1$. Til brug senere bemærker vi

$$\gcd(p^2, q^2) = 1, \quad \gcd(v^2, w^2) = 1 \tag{1}$$

Vi vil vise $p, w = \pm 1$. Fra vores første betingelse følger

$$\exists a \in \mathbb{Z} : \quad r + s = \frac{p}{q} + \frac{v}{w} = a$$

Dette giver $pw + qv = wqa$. Men heraf fås først $pw = q(wa - v)$ og derfor $q|pw$. Da $\gcd(q, p) = 1$ fås $q|w$. Tilsvarende kan vi ved at flytte leddet pw over på høresiden i stedet for qv, få $w|q$. Dermed må vi have $w = \pm q$.

Ved kvadrering fås

$$w^2 = (\pm q)^2 = q^2 = e$$

for et helt tal e. Dermed fås fra (1) $\gcd(p^2, e) = \gcd(q^2, e) = 1$. Fra antagelsen $rs \in \mathbb{Z}$ fås nu

$$\frac{p^2 v^2}{e^2} = \frac{p^2 v^2}{q^2 w^2} = (rs)^2 \in \mathbb{N}$$

Men vi har jo lige set at både p^2 og v^2 er indbyrdes primiske med e, dvs. de har ingen primtal tilfælles i deres primtalsfaktorisering. Eneste mulighed der er for at denne brøk kan give et naturligt tal er derfor $e^2 = 1$! Heraf følger $q^2 = 1$ samt $w^2 = 1$ og derfor $q, w = \pm 1$. Fra den måde vi skrev r og s følger $r = \pm p \in \mathbb{Z}$ og $s = \pm v \in \mathbb{Z}$. Som skulle vises.

□

Bemærk at vi udover antagelserne stortset kun benytter aritmetikkens fuldamentalsætning! Sætningen skrevet øverst er generaliseringen af ovenstående resultatet til polynomier.

Bevis for sætning Lad $fg = h$ og bemærk først at t må være monisk da f og g er det. Skriv $f = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i$ og $g = \sum_{i=0}^{m} \frac{c_i}{d_i} X^i$. Da både f og g er moniske kan vi antage $a_n, b_n, c_m, d_m = 1$. Lad $b = \prod_{i=0}^{n} b_i$ og $d = \prod_{i=0}^{m} d_i$. Vores mål vil være, at vise $b, d = \pm 1$, fordi det vil medfører $b_i, d_j = \pm 1$ for alle i, j ($i \neq n$ og $j \neq m$ som vi jo ved er 1). Konstruktionen beskrevet i 1.3.4 i videregående algebra noterne giver

$$\exists \frac{b}{e}, \ \frac{d}{s} \, med \, e, s \in \mathbb{Z} : \quad \frac{b}{e} f = f_o \in \mathbb{Z}[X], \ \frac{d}{s} g = g_o \in \mathbb{Z}[X] \tag{2}$$

er primitive. Det er værd at bemærke hvordan e og s er defineret:

$$e = \gcd(b_0, b_1, \ldots, b_n) = \gcd(b_0, b_1, \ldots, 1) = 1$$
$$s = \gcd(d_0, d_1, \ldots, d_m) = \gcd(d_0, d_1, \ldots, 1) = 1$$

da vi selvfølgelig ikke kan have en større divisor i 1, end 1 selv. Dermed fås fra (2) $bf = f_0$ og $dg = g_o$.

Lemma 1.3.3 i videregående algebra noterne fortæller: Produktet af to primitive polynomier over $\mathbb{Z}$ er igen primitiv. Anvender vi dette fås

$$f_o g_o = bfdg = bd(fg) = bdt$$

Hvor bdt er det primitive polynomie dannet udfra produktet af f_o og g_o. Lad $cont(h)$ betegne største fælles divisor af koefficienterne af et polynomie h over $\mathbb{Z}$. Da bdt er primitiv har vi dermed $cont(bdt) = 1$.

Skriv nu $t = \sum_{i=0}^{m+n} t_i X^i$ hvor $t_i \in \mathbb{Z}$. Men som vi bemærkede i starten er t monisk, hvilket giver $t_{m+n} = 1$. Vi har dermed

$$bdt = bd \sum_{i=0}^{m+n} t_i X^i = \sum_{i=0}^{m+n} bdt_i X^i$$

Men nu har vi

$$\begin{aligned} bd &= gcd(bdt_0, bdt_1, \ldots, bdt_{m+n-1}, bd) \\ &= gcd(bdt_0, bdt_1, \ldots, bdt_{m+n-1}, bd \cdot 1) \\ &= gcd(bdt_0, bdt_1, \ldots, bdt_{m+n-1}, bdt_{m+n}) \\ &= cont(bdt) \\ &= 1 \end{aligned}$$

Det kan kun betyde $b, d = \pm 1$, som vi netop ville vise.

□

Hvordan følger første resultat så af sætningen? Vælg $r, s \in \mathbb{Q}$ og betragt polynomierne $X+r$ og $X+s$ (klart moniske) i $\mathbb{Q}[X]$. Antag som i sætningen $X^2+(r+s)X+rs = (X+r)(X+s) \in \mathbb{Z}[X]$. Dvs. betingelsen $(X+r)(X+s) \in \mathbb{Z}[X]$ er ækvivalent med betingelsen $r+s \in \mathbb{Z}$ og $rs \in \mathbb{Z}$. Sætningen fortæller nu at $X+r, X+s \in \mathbb{Z}[X]$ som jo betyder $r, s \in \mathbb{Z}$.