Polynomien jakoalgoritmi

Tutkittaessa polynomien yli kunnan $(K,+,\cdot)$ jaollisuutta voidaan käyttää samanlaista jakoalgoritmia (jakokulmalaskua) kuin kokonaisluvuilla. Vertaa seuraavaa lausetta sivun Jakoalgoritmi lauseeseen.

Lause. Olkoon $(K[x],+,\cdot)$ polynomirengas yli kunnan $(K,+,\cdot)$. Jos $a(x), b(x) \in K[x]$ ja $b(x) \neq 0_K$, niin on olemassa sellaiset yksikäsitteiset polynomit $q(x)$ ja $r(x) \in K[x]$, että

$$a(x) = q(x)b(x) + r(x), \qquad \deg r(x) < \deg b(x).$$

Todistus. Olkoon $S = \{a(x) - k(x)b(x) \mid k(x) \in K[x]\}$. Valitaan joukosta S polynomi

$$r(x) = a(x) - q(x)b(x),$$

jonka aste on pienin mahdollinen. Jos $r(x) = 0_K$, niin $\deg r(x) = -\infty < \deg b(x)$ ja lauseen väite on voimassa.

Oletetaan, että $r(x)$ ei ole nollapolynomi ja $\deg r(x) = n$. Oletetaan lisäksi, että $\deg b(x) = m$. Pitää siis näyttää, että $n < m$. Olkoon polynomin $r(x)$ johtava kerroin r_n ja polynomin $b(x)$ johtava kerroin b_m. Tehdään vastaoletus, että $n \geq m$. Koska $b_m \in K \setminus \{0_K\}$, on olemassa käänteisalkio $b_m^{-1} \in K$. Tämän huomion ja vastaoletuksen nojalla voidaan muodostaa polynomi

$$s(x) = a(x) - \left(q(x) - \frac{r_n}{b_m} \cdot x^{n-m}\right) b(x) = r(x) - \frac{r_n}{b_m} \cdot x^{n-m} b(x).$$

Polynomi $s(x)$ kuuluu joukkoon S ja sen n:nnen asteen termin kerroin on

$$r_n - \frac{r_n}{b_m} \cdot b_m = 0_K.$$

Siis $s(x)$ on pienempää astetta kuin polynomi $r(x)$, mikä on ristiriita polynomin $r(x)$ valinnan kanssa. Täten $n < m$.

Vielä pitää osoittaa polynomien $q(x)$ ja $r(x)$ yksikäsitteisyys. Oletetaan, että on olemassa myös polynomit $q'(x)$ ja $r'(x)$, joilla $a(x) = q'(x)b(x) + r'(x)$ ja $\deg r'(x) < \deg b(x)$. Silloin

$$r(x) - r'(x) = (q'(x) - q(x))b(x), \qquad \deg(r(x) - r'(x)) < \deg b(x).$$

Toisaalta sivun Polynomin aste lauseen mukaan $\deg(r(x) - r'(x)) = \deg(q'(x) - q(x)) + \deg b(x)$. Täten välttämättä $q'(x) - q(x) = 0_K$ ja tästä seuraa, että $r(x) - r'(x) = 0_K b(x) = 0_K$. Siis $q(x) = q'(x)$ ja $r(x) = r'(x)$. $\square$

Linkit:

Polynomien jaollisuus

Jakoalgoritmi

Polynomin aste

Esimerkkejä polynomirenkaista