Maradékosztály-gyűrű fölötti polinomgyűrű ideáljairól

VERES ZSUZSANNA

Abstract. (On a ideals of a polinomial ring over a residue class ring) In this paper we describe the system of generators of ideals of the ring $\mathbf{Z}_{p^n}[x]$, where $\mathbf{Z}_{p^n}$ is the residue class modulo p^n, p is a prime and n is a natural number.

Jelöljük $\mathbf{Z}_{p^n}[x]$-szel a $\mathbf{Z}_{p^n}$ — p^n szerinti ($p \in \mathbf{Z}$ prím, $n \in \mathbf{N}$) maradékosztály-gyűrű — fölötti polinomgyűrűt. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja. A továbbiakban $g(x) \neq 0$ egy rögzített minimális fokszámú polinom azon I-beli polinomok közül, melyek főegyütthatója osztható p-vel, és $h(x) \neq 0$ egy rögzített minimális fokszámú polinom azon I-beli polinomok közül, melyek főegyütthatója nem osztható p-vel. Jelölje $\deg f(x)$ az $f(x)$ polinom fokát.

1. Lemma. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja és $g(x)$, $h(x)$ a fent említett polinomok. Ekkor a $g(x)$ polinom minden együtthatója osztható p-vel, és foka nem nagyobb $h(x)$ polinom fokánál, azaz a $g(x)$ fokszáma minimális az I-beli polinomok között.

Bizonyítás. Legyen $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Ekkor p osztja az a_n-t, azaz az a_n együttható $a_n = p \cdot a'_n$ alakban írható fel, ahol a'_n nem osztható p-vel. Mivel $g(x)$ az I ideál eleme, ezért $pg(x)$ is az I ideál eleme és

$$pg(x) = p^2 a'_n x^n + pa_{n-1}x^{n-1} + \cdots + pa_1 x + pa_0.$$

A $pg(x)$ polinom minden együtthatója osztható p-vel, és mivel a $\mathbf{Z}_{p^2}$ gyűrűben $p^2 = 0$, foka kisebb a $g(x)$ fokánál. Ez csak abban az esetben lehetséges, ha $pg(x) = 0$. Tehát $pa_i = 0\,(i = 1, 2, \ldots, n)$, azaz a $g(x)$ polinom minden együtthatója osztható p-vel, és így, $g(x) = pg_1(x)$ ($g_1(x) \in \mathbf{Z}_{p^2}[x]$) alakban írható fel.

Ha $h(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$, akkor a feltétel szerint b_k nem osztható p-vel, és ezért a $\mathbf{Z}_{p^2}$ együtthatógyűrű egységcsoportjának eleme. Így $pb_k \neq 0$, és a $ph(x) = pb_k x^k + pb_{k-1}x^{k-1} + \cdots + pb_1 x + pb_0$ polinom foka megegyezik a $h(x)$ polinom fokával. A $ph(x)$ polinom főegyütthatója osztható p-vel, ezért foka nem lehet kisebb a $g(x)$ polinom fokánál. Mivel $\deg h(x) = \deg ph(x)$, így a $h(x)$ polinom foka sem kisebb a $g(x)$ polinom

fokánál.

2. Lemma. Ha $t(x) \in \mathbf{Z}_{p^2}[x]$ egy olyan polinom, melynek főegyütthatója nem osztható p-vel, akkor tetszőleges $f(x)$ polinom ($f(x) \in \mathbf{Z}_{p^2}[x]$) felírható a következő alakban:

$$f(x) = t(x)s(x) + r(x),$$

ahol $s(x), r(x) \in \mathbf{Z}_{p^2}[x]$ és $\deg r(x) < \deg t(x)$

Bizonyítás. Legyen

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$t(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0.$$

Ha $k > n$ akkor $f(x) = t(x)0 + f(x)$ és ebben az esetben a lemma be van bizonyítva. Tekintsük a $k \leq n$ esetet. Mivel p nem osztja a b_k együtthatót, ezért $a_n b_k^{-1} \neq 0$, ahol b_k^{-1} a b_k inverze. Így az

$$r_1(x) = f(x) - a_n b_k^{-1} x^{n-k} t(x)$$

polinom foka kisebb $f(x)$ fokánál. Tehát $f(x) = t(x)s_1(x) + r_1(x)$ alakú, ahol $s_1(x) = a_n b_k^{-1} x^{n-k}$. Ha $\deg r_1(x) < \deg t(x)$, akkor a lemma bizonyítást nyert. Ha $\deg r_1(x) \geq \deg t(x)$, akkor megismételve az előző eljárást az $r_1(x)$ polinomra, a következő egyenlőséget kapjuk

$$r_1(x) = t(x)s_2(x) + r_2(x),$$

ahol $\deg r_2(x) < \deg r_1(x)$. Ezt az eljárást addig folytatjuk, míg eljutunk egy olyan $r_i(x)$ polinomig, melynek foka már kisebb a $t(x)$ polinom fokánál. Így

$$f(x) = t(x)s_1(x) + t(x)s_2(x) + \cdots + t(x)s_i(x) + r_i(x),$$

és ezért

$$f(x) = t(x)s(x) + r(x),$$

ahol $s(x) = s_1(x) + s_2(x) + \cdots + s_i(x)$, $r(x) = r_i(x)$ és $\deg r(x) < \deg t(x)$.

3. Lemma. A $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja legfeljebb két polinommal generálódik.

Bizonyítás. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű ideálja és $f(x)$ az I ideál tetszőleges eleme. Elégséges megmutatni, hogy az $f(x)$ polinom felírható

$$f(x) = h(x)s(x) + g(x)q(x)$$

alakban, ahol $h(x)$ és $g(x)$ az 1. Lemmában említett polinomok, $s(x)$ és $q(x)$ pedig a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű megfelelő polinomjai. Két eset lehetséges:

$$\deg f(x) \geq \deg h(x);$$
$$\deg f(x) < \deg h(x).$$

Megjegyezzük, hogy az 1. Lemma miatt igaz a következő egyenlőtlenség:

$$\deg f(x) \geq \deg g(x).$$

Tekintsük az első esetet. A 2. Lemma értelmében

$$f(x) = h(x)s(x) + r(x), \tag{1}$$

ahol

$$\deg r(x) < \deg h(x). \tag{2}$$

Könnyen belátható, hogy $r(x) \in I$, és ezért a (2) egyenlőtlenségből és a $h(x)$ polinom tulajdonságából következik, hogy az $r(x)$ főegyütthatója osztható p-vel.

Ha $\deg r(x) < \deg g(x)$, akkor az 1. Lemma következtében $r(x) = 0$, és így $f(x) = h(x)s(x) + g(x)0$ és ebben az esetben a Lemma állítása igazolást nyert. Tekintsük most azt az esetet, amikor $\deg r(x) \geq \deg g(x)$. Írjuk fel $r(x)$-et két polinom összegeként

$$r(x) = \varphi_1(x) + \varphi_2(x)$$

úgy, hogy az $\varphi_1(x)$ az $r(x)$ polinom azon tagjaiból áll, melyek együtthatói nem oszthatók p-vel, a $\varphi_2(x)$ pedig az $r(x)$ azon tagjait tartalmazza, melyek együtthatói oszthatók p-vel, azaz

$$\varphi_2(x) = p\varphi_2'(x)$$

alakú, ahol $\varphi_2'(x)$ egyik együtthatója sem osztható p-vel. Mivel az $r(x)$ polinom főegyütthatója osztható p-vel,

$$\deg r(x) = \deg \varphi_2(x) > \deg \varphi_1(x). \tag{3}$$

Figyelembe véve a (2) egyenlőtlenséget a

$$\deg \varphi_1(x) < \deg h(x) \tag{4}$$

egyenlőtlenséghez jutunk.

Az 1. Lemma szerint $g(x) = pg_1(x)$ alakba írható, ahol $g_1(x)$ egyik együtthatója sem osztható p-vel. A 2. Lemma szerint

$$\varphi_2'(x) = g_1(x)q(x) + r_1(x),$$

ahol

$$\deg r_1(x) < \deg g_1(x) = \deg g(x). \tag{5}$$

Ekkor

$$\begin{aligned} r(x) &= \varphi_1(x) + p(g_1(x)q(x) + r_1(x)) = \\ &= \varphi_1(x) + g(x)q(x) + pr_1(x). \end{aligned}$$

Könnyű belátni, hogy a $\varphi_1(x) + pr_1(x)$ polinom az I ideál eleme. Mivel $\deg pr_1(x) = \deg r_1(x)$ az (5) egyenlőtlenségből és az 1. Lemmából a

$$\deg(\varphi_1(x) + pr_1(x)) = \deg \varphi_1(x)$$

egyenlőséghez jutunk. Ez azt jelenti, hogy a $\varphi_1(x) + pr_1(x)$ polinom főegyütthatója nem osztható p-vel. Figyelembe véve a (4) egyenlőtlenséget és azt, hogy az I ideálban azon polinomok fokszáma, melyek főegyütthatója nem osztható p-vel, nem lehet kisebb a $h(x)$ polinom fokszámánál, az utolsó egyenlőségből a $\varphi_1(x) + pr_1(x) = 0$ következik. Így $r(x) = g(x)q(x)$ és az (1) egyenlőség szerínt

$$f(x) = h(x)s(x) + g(x)q(x).$$

Tekintsük most a második esetet, azaz amikor

$$\deg f(x) < \deg h(x).$$

Felírjuk az $f(x)$ polinomot két polinom összegeként

$$f(x) = f_1(x) + f_2(x),$$

ahol az $f_1(x)$ polinom az $f(x)$ azon tagjaiból áll, melyek együtthatói nem oszthatók p-vel, az $f_2(x)$ pedig $f(x)$ polinom azon tagjait tartalmazza, melyek együtthatói oszthatók p-vel. Mivel az $f(x)$ polinom fokszáma kisebb a $h(x)$ fokszámánál, ezért $f(x)$ főegyütthatójának osztható p-vel. Ezért

$$\deg f(x) = \deg f_2(x) = \deg pf_2'(x) > \deg f_1(x),$$

ahol $f_2(x) = pf_2'(x)$ és az $f_2'(x)$ polinom egyik együtthatója sem osztható p-vel. A 2. Lemma miatt

$$f_2'(x) = g'(x)q(x) + r_1(x)$$

alakú, ahol $\deg r_1(x) < \deg g'(x) = \deg g(x)$. Ebből nyerjük, hogy

$$\begin{aligned} f(x) &= f_1(x) + p(g'(x)q(x) + r_1(x)) = \\ &= f_1(x) + g(x)q(x) + pr_1(x) \end{aligned}$$

Mint az előző esetben, most is meggyőződhetünk róla, hogy $pr_1(x) + f_1(x) = 0$, ezért

$$f(x) = h(x)0 + g(x)q(x)$$

alakban írható fel. A Lemma be van bizonyítva.

1. Tétel. A $\mathbf{Z}_{p^n}[x]$ polinomgyűrű bármely ideálja legfeljebb n elemmel generálódik.

Bizonyítás. A bizonyítást n-szerinti teljes indukcióval végezzük. A $\mathbf{Z}_p[x]$, a $\mathbf{Z}_p$ test fölötti polinomgyűrű főideálgyűrű, $n = 2$ esetben pedig a 3. Lemma szerint a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű minden ideálja legfeljebb két elemmel generálódik.

Tegyük fel, hogy $\mathbf{Z}_{p^{n-1}}[x]$ minden ideálja legfeljebb $n-1$ elemmel generálódik. Tekintsük azt a

$$\varphi: \mathbf{Z}_{p^n}[x] \to \mathbf{Z}_{p^{n-1}}[x]$$

homomorfizmust, amelynek magja $\ker \varphi = p^{n-1}\mathbf{Z}_{p^n}[x]$. Ha I a $\mathbf{Z}_{p^n}[x]$ gyűrű ideálja, akkor a $\varphi(I) = \overline{I}$ ideál az indukciós feltevés alapján legfeljebb $n-1$,

$$\overline{g_0(x)}, \overline{g_1(x)}, \ldots, \overline{g_{n-2}(x)},$$

polinommal generálódik, és ezekre a polinomokra teljesül, hogy $\overline{g_i(x)}$ együtthatói oszthatók p^i-nel, de nem oszthatók p^{i+1}-nel $(i = 0, 1, \ldots, n-2)$ és fokszámuk minimális az ezzel a tulajdonsággal bíró $\overline{I}$ ideál polinomjai között. Ha $f(x) \in I$, akkor $\varphi(f(x)) = \overline{f(x)} \in \overline{I}$ és

$$\overline{f(x)} = \overline{g_0(x)}\,\overline{\psi_0(x)} + \overline{g_1(x)}\,\overline{\psi_1(x)} + \cdots + \overline{g_{n-2}(x)}\,\overline{\psi_{n-2}(x)}$$

alakban írható fel, ahol $\overline{\varphi_i(x)} \in \mathbf{Z}_{p^{n-1}}[x]\,(i = 0, 1, \ldots, n-2)$. Jelölje $g_i(x)$ és $\psi_i(x)\,(i = 0, 1, \ldots, n-2)$ megfelelően az $\overline{g_i(x)}$ és az $\overline{\psi_i(x)}$ polinomok valamelyik inverz képét. Ekkor

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \cdots + g_{n-2}(x)\psi_{n-2}(x) + t(x),$$

ahol $t(x)$ egy megfelelő polinom a φ homomorfizmus magjából. Így a $t(x)$ polinom minden együtthatója osztható p^{n-1}-nel, vagyis $t(x) = p^{n-1}t'(x)$ alakban írható fel. Tehát

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \cdots + g_{n-2}(x)\psi_{n-2}(x) + p^{n-1}t'(x).$$

Ez az egyenlőség azt jelenti, hogy a $\mathbf{Z}_{p^n}[x]$ polinomgyűrű tetszőleges ideálja legfeljebb n elemmel generálódik.

Ha a $t'(x)$ polinomnak nagyobb a foka mint az I ideál azon minimális fokszámú polinomjainak amelyek együtthatói p^{n-1}-nel oszthatók, akkor $t(x) = p^{n-1}t'(x)$ és a 2. Lemma szerint

$$t(x) = p^{n-1}t'(x) = p^{n-1}g'_{n-1}(x)\psi_{n-1}(x) = g_{n-1}(x)\psi_{n-1}(x),$$

ahol $g_{n-1}(x)$ polinom együtthatói oszthatók p^{n-1}-nel, és így,

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \cdots + g_{n-1}(x)\psi_{n-1}(x).$$

Tehát, a $\mathbf{Z}_{p^n}[x]$ gyűrű tetszőleges I ideáljának generátorrendszere olyan

$$g_0(x), g_1(x), \ldots, g_{n-1}(x)$$

polinomokból áll, hogy bármelyik $g_i(x)$-re igaz, hogy $g_i(x)$ együtthatói oszthatók p^i-nel, de nem oszthatók p^{i+1}-nel, és fokszámuk minimális az ezzel a tulajdonsággal bíró polinomok között.