Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae, 25. (1998) pp. 71–76

Egy euklidészi gyűrű

KIRÁLY BERTALAN,* OROSZ GYULÁNÉ

Abstract. We showe in this paper that the polynomial ring over a field of the infinite cyclic group is an Euclidean one.

Legyen $R\langle g\rangle$ a $\langle g\rangle$ végtelen ciklikus csoport T test fölötti csoportgyűrűje. A $T\langle g\rangle$ minden eleme felírható

$$x = \sum_{i\in Z} \alpha_i g^i, \qquad \alpha_i \in T \tag{1}$$

alakban, ahol csak véges sok $\alpha_i \neq 0$. Könnyű belátni, hogy a $T[g]$ és $T[g^{-1}]$ polinomgyűrűk (ha úgy tekintünk a g-re, ill. a g^{-1}-re mint határozatlanokra) a $T\langle g\rangle$ részgyűrűi.

Ismeretes, hogy a test fölötti egyhatározatlanú polinomok gyűrűje euklidészi gyűrű. Az euklidészi gyűrűk fontos szerepet játszanak a matematikában, többek között az algebrában és a számelméletben is. Ez annak tulajdonítható, hogy egész sor olyan tulajdonsággal rendelkeznek, amelyek megkönnyítik alkalmazásukat (pl. az euklidészi gyűrűk főideálgyűrűk, érvényes bennük az egyértelmű prímfaktorizáció tétele, legnagyobb közös osztó létezése stb.). Az is ismeretes, hogy a test fölötti kéthatározatlanú polinomok gyűrűje nem euklidészi gyűrű. A $T\langle g\rangle$ csoportgyűrűt nem tekinthetjük sem egyhatározatlanú, sem pedig kéthatározatlanú polinomgyűrűnek. Bebizonyítjuk, hogy ennek ellenére a $T\langle g\rangle$ euklidészi gyűrű.

Tétel. *A végtelen ciklikus csoport test fölötti csoportgyűrűje euklidészi gyűrű.*

A tétel bizonyításához szükségünk lesz néhány jól ismert fogalomra és állításra.

Ismeretes, hogy a gyűrű egységeinek halmaza a szorzásra nézve csoportot alkot amelyet $U(R)$-rel fogunk jelölni és az R gyűrű egységcsoportjának fogunk nevezni.

A továbbiakban R integritástartományt fog jelölni, azaz kommutatív, egységelemes, nullosztómentes gyűrűt.

* A kutatást az OTKA T16432 sz. pályázata támogatta.

Az a elemet a b $(a, b \in R)$ *asszociáltjának* nevezzük, ha $a = \varepsilon b$ valamely $\varepsilon \in U(R)$ elem esetén. Ezt $a \sim b$-vel jelöljük. Könnyű belátni, hogy a $\sim$ ekvivalenciareláció az R-en. Ezért a továbbiakban úgy is mondhatjuk, hogy az a és b elemek asszociáltak.

Definíció. A $T\langle g\rangle$ csoportgyűrű

$$x' = 1 + \sum_{0<i\in Z} \alpha_i g^i, \qquad \alpha_i \in T$$

alakú elemeit normált elemeknek nevezzük.

Világos, hogy ha x' normált elem, akkor $x' \in T[g] \subset T\langle g\rangle$.

1. Lemma. *A $T\langle g\rangle$ csoportgyűrűben igazak a következő állítások:*

1. Minden $x \neq 0$ $T\langle g\rangle$-beli elemhez létezik olyan egyértelműen meghatározott x' normált elem, hogy $x \sim x'$ és egy megfelelő α $(\alpha \in T)$ és egy meghatározott k egész számmal teljesül az

$$x = \alpha g^k x' \tag{2}$$

egyenlőség. Az x' elemet az x normáltjának fogjuk nevezni.

2. Ha x' és y' normált elemek, akkor az $x'y'$ is normált elem.

3. Tetszőleges nem nulla x, y $T\langle g\rangle$-beli elemek esetén igaz az

$$(xy)' = x'y',$$

egyenlőség.

Bizonyítás. 1. Legyen $x \in T\langle g\rangle$. Akkor az (1) szerint x előállítható

$$x = \sum_{i\in Z} \alpha_i g^i, \qquad \alpha_i \in T$$

alakban, ahol csak véges sok $\alpha_i \neq 0$. Legyen

$$k = \min_{\alpha_i \neq 0}\{i\}$$

és

$$x' = \alpha_k^{-1} g^{-k} x = \alpha_k^{-1} g^{-k} \sum_{i\in Z} \alpha_i g^i = 1 + \sum_{\substack{i\in Z\\ i\neq k}} \alpha_k^{-1} g^{-k} \alpha_i g^{i-k}.$$

Mivel $i - k \geq 0$, az x' elem felírásában a g-nek csak nemnegatív hatványai szerepelnek. Így

$$x' = 1 + \sum_{0<j\in Z} \delta_i g^i$$

alakú, vagyis x' normált elem. Az

$$x' = \alpha_k^{-1} g^{-k} x$$

egyenlőségekből nyerjük, hogy

$$x = \alpha_k g^k x'.$$

Tehát x előállítható (2) alakban és $x \sim x'$.

2. Legyen $x' = 1 + \sum_{0<i\in Z} \alpha_i g^i$ és $y' = 1 + \sum_{0<i\in Z} \beta_i g^i$. Az x', y' a $T[g]$ polinomgyűrű elemei és

$$x'y' = 1 + \sum_{0<i\in Z} \gamma_i g^i \in T[g],$$

azaz $x'y'$ normált elem.

3. A (2) szerint x és y felírható

$$x = \alpha g^k x' \qquad \text{és} \qquad y = \beta g^n y', \qquad (\alpha, \beta \in T,\ k, n \in Z)$$

alakban. Ezért

$$xy = \alpha\beta g^{k+n} x'y' = \alpha\beta g^{k+n}(1 + \sum_{0<i\in Z} \delta_i g^i) \in T[g]. \tag{3}$$

Innen következik, hogy $(xy)' = x'y'$.

A továbbiakban a (2)-re való hivatkozás nélkül is fogjuk alkalmazni a $T\langle g\rangle$-beli elemek (2) alakú előállítását.

2. Lemma. *A $T\langle g\rangle$ egységcsoportjának elemei γg^i $(\gamma \in R, i \in Z)$ alakúak.*

Bizonyítás. Legyen $x \in U(T\langle g\rangle)$. Az előző Lemma értelmében x és x^{-1} előállíthatók

$$x = \alpha g^k x' \qquad \text{és} \qquad x^{-1} = \beta g^n y' \qquad (\alpha, \beta \in T, \qquad k, n \in Z)$$

alakban. Ekkor figyelembe véve azt, hogy x' és y' normált elemek az

$$x'y' = 1 + \sum_{0<i\in Z} \delta_i g^i \in T[g]$$

egyenlőségből kapjuk, hogy

$$1 = xx^{-1} = \alpha\beta g^{k+n}x'y' = \alpha\beta g^{k+n}(1 + \sum_{0<i\in Z} \delta_i g^i). \tag{4}$$

Mivel x', y' és $x'y'$ a $T[g]$ elemei a (4) csak abban az esetben teljesül, ha $x' = y' = 1$. Tehát $x = \alpha g^k$ és $y = \beta g^n$.

3. Lemma. *A $T\langle g\rangle$ csoportgyűrűben az asszociált elemek normáltja megegyezik. Azaz, ha $x \sim y$, akkor $x' = y'$.*

Bizonyítás. Ha $x \sim y$, akkor található olyan ε ($\varepsilon \in U(T\langle g\rangle)$), hogy $x = \varepsilon y$ A 2. Lemma szerint $\varepsilon = \gamma g^m$ $(\gamma \in T, m \in Z)$. Evidens, hogy $\varepsilon' = 1$. Ekkor az 1. Lemma értelmében

$$x' = (\varepsilon y)' = \varepsilon' y' = y'.$$

4. Lemma. *A $T\langle g\rangle$ nullosztómentes gyűrű.*

Bizonyítás. Tegyük fel, hogy x és y nem nulla $T\langle g\rangle$-beli elemek és $xy = 0$. Ekkor felhasználva az x és y elemek $x = \alpha g^k x'$ és $y = \beta g^n y'$ $(\alpha\beta \in T,\ k, n \in Z)$ előállítását normáltjaik segítségével, az $xy = 0$-ból az

$$xy = \alpha\beta g^{k+n}x'y' = 0$$

következik. Mivel $\alpha\beta g^{k+n} \in U(T\langle g\rangle)$, innen az $x'y' = 0$ egyenlőséget kapjuk. Ez ellentmondás, mert $x' \neq 0$, $y' \neq 0$ és $x', y' \in T[g]$.

Jelöljük Z^+-szal a nemnegatív egész számok halmazát.

Definíció. Az R integritástartomány euklidészi gyűrűnek nevezzük, ha létezik olyan

$$\varphi\colon R \setminus \{0\} \to Z^+$$

leképezés, hogy minden $a, b \in R \setminus \{0\}$ elempárra igaz a $\varphi(ab) \geq \varphi(a)$ egyenlőtlenség. Továbbá, tetszőleges a és $b \neq 0$ R-beli elemekre teljesül a következő egyenlőség:

$$a = bq + r, \qquad \text{ahol vagy } r = 0, \ \text{ vagy } \varphi(r) < \varphi(b), \ (r, q \in R). \tag{5}$$

A φ leképezést euklidészi normának, az (5)-öt pedig euklidészi osztásnak nevezzük.

Legyen $x = \sum\limits_{0<i\in Z} \alpha_i g^i \in T[g] \subset T\langle g\rangle$. Ekkor $x = \alpha_k g^k x'$. Evidens, hogy $k \geq 0$. Jelöljük x°-rel az x polinom fokát. Figyelembe véve, hogy $k \geq 0$ az előző egyenlőségből következik, hogy

$$x^\circ \geq (x')^\circ. \tag{6}$$

A Tétel bizonyítása. Legyen $x \in T\langle g\rangle \setminus \{0\}$ és legyen

$$x' = 1 + \sum_{0<i\in Z} \alpha_i g^i$$

az x normáltja. Nyilván $x' \in T[g]$. Legyen $\deg x = (x')^\circ$. A $\deg x$-et az *x elem módosított fokszámának* fogjuk nevezni. Könnyű belátni, hogy a $\deg v = \deg w$ egyenlőség pontosan akkor teljesül, ha $v \sim w$, és a $\deg x = 0$ egyenlőség akkor és csak akkor igaz, ha $x \in U(T\langle g\rangle)$.

Legyen $x, y \in T\langle g\rangle \setminus \{0\}$. Akkor $x = \varepsilon x'$ és $y = \delta y'$, ahol x', y' megfelelően az x, ill. az y normáltja és $\varepsilon, \delta \in U(T\langle g\rangle)$. Az 1. Lemma 3. pontja szerint $(xy)' = x'y'$, és mivel $x'y' \in T[g]$,

$$\deg(xy) = ((xy)')^\circ = (x'y')^\circ = (x')^\circ + (y')^\circ = \deg x + \deg y. \tag{7}$$

Legyen

$$\varphi\colon T\langle g\rangle \setminus \{0\} \to Z^+, \qquad \varphi(x) = \deg x. \tag{8}$$

Megmutatjuk, hogy φ a $T\langle g\rangle$ euklidészi normája. Ha $x, y \in T\langle g\rangle \setminus \{0\}$, akkor a (7)-ből kapjuk, hogy

$$\varphi(xy) = \deg(xy) = \deg x + \deg y \geq \deg x = \varphi(x).$$

és így a φ euklidészi norma a $T\langle g\rangle$-n.

Legyen $x, y \in T\langle g\rangle$ és $y \neq 0$. Írjuk fel az x-et és az y-t $x = \varepsilon x'$ és $y = \delta y'$ ($\varepsilon, \delta \in U(T\langle g\rangle)$ alakban. Ha $x = 0$, vagy $\varphi(x) < \varphi(y)$, akkor $x = y \cdot 0 + x$ és az (5) teljesül.

Legyen most $\varphi(x) \geq \varphi(y)$. Ekkor $\varphi(x) = \varphi(x') \geq \varphi(y) = \varphi(y')$. A $T[g]$ polinomgyűrűben érvényes az euklidészi osztás, és mivel x', y' $T[\langle g\rangle$-beli elemek, igaz a következő egyenlőség:

$$x' = y'q + r, \quad \text{ahol} \quad r = 0 \quad \text{vagy} \quad r^\circ < (y')^\circ \qquad (q, r \in T[g] \subset T\langle g\rangle).$$

Ekkor a (6)-ból következik, hogy $\deg r = (r')^\circ \leq (y')^\circ = \deg y$ és így $\varphi(r) \leq \varphi(y')$. Tehát

$$x' = y'q + r, \quad \text{ahol} \quad r = 0 \quad \text{vagy} \quad \varphi(r) < \varphi(y'). \tag{9}$$

Ha $x = \varepsilon x'$ és $y = \delta y'$ $(\varepsilon, \delta \in U(T\langle g\rangle))$, akkor a (9)-ből kapjuk, hogy $\delta\varepsilon x' = \delta x = \delta\varepsilon y' q + \delta\varepsilon r$ és így

$$x = y\overline{q} + \overline{r},$$

ahol $\overline{q} = \varepsilon\delta^{-1}q, \overline{r} = \varepsilon r$. Mivel $\overline{q} \sim q$ és $\overline{r} \sim r$, és az asszociált elemek módosított fokszáma megegyezik, a (9)-ből következik, hogy az előző egyenlőségben vagy $\overline{r} = 0$, vagy $\varphi(\overline{r}) < \varphi(y)$. Tehát a $T\langle g\rangle$ euklidészi gyűrű.

Irodalom

[1] B. L. Van der Warden, *Algebra I.*, Berlin · Heidelberg · New York.

Király Bertalan
Eszterházy Károly Tanárképző Főiskola
Matematika Tanszék
Leányka u. 4.
3301 Eger, Pf. 43.
E-mail: kiraly@ektf.hu

Dr. Orosz Gyuláné
Eszterházy Károly Tanárképző Főiskola
Matematika Tanszék
Leányka u. 4.
3301 Eger, Pf. 43.