Diszkrét matematika III.

Polinomok

2009. május 15-16.

A modulo m maradékosztályok gyűrűje.

Legyen m tetszőleges egész szám, és tekintsük a $\equiv \pmod{m}$ modulo m kongruenciarelációt $\mathbb{Z}$-n:

$$a \equiv b \pmod{m} \iff m \mid a - b.$$

Tétel.

A $\equiv \pmod{m}$ modulo m kongruencareláció ekvivaleciareláció, sőt kongruenciareláció $\mathbb{Z}$-n, azaz teljesülnek a következők:

A modulo m maradékosztályok gyűrűje.

Legyen m tetszőleges egész szám, és tekintsük a $\equiv \pmod{m}$ modulo m kongruenciarelációt $\mathbb{Z}$-n:

$$a \equiv b \pmod{m} \iff m \mid a - b.$$

Tétel.

A $\equiv \pmod{m}$ modulo m kongruencareláció ekvivaleciareláció, sőt kongruenciareláció $\mathbb{Z}$-n, azaz teljesülnek a következők:

(a) $\equiv \pmod{m}$ reflexív, szimmetrikus és tranzitív;

A modulo m maradékosztályok gyűrűje.

Legyen m tetszőleges egész szám, és tekintsük a $\equiv \pmod{m}$ modulo m kongruenciarelációt $\mathbb{Z}$-n:

$$a \equiv b \pmod{m} \iff m \mid a - b.$$

Tétel.

A $\equiv \pmod{m}$ modulo m kongruencareláció ekvivaleciareláció, sőt kongruenciareláció $\mathbb{Z}$-n, azaz teljesülnek a következők:

(a) $\equiv \pmod{m}$ reflexív, szimmetrikus és tranzitív;

(b) ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

A modulo m maradékosztályok gyűrűje.

Legyen $m = 0$, akkor $\equiv \pmod{m}$ az egyenlőségreláció.
Ha $m = 1$, akkor $\equiv \pmod{m}$ a teljes reláció. Továbbá tetszőleges m természetes számra a $\equiv \pmod{m}$ reláció megegyezik a $\equiv \pmod{-m}$ relációval. A továbbiakban feltesszük, hogy $m \in \mathbb{N}$. A $\equiv \pmod{m}$ ekvivalenciareláció szerinti ekvivalenciaosztályok a következők:

$$\overline{0}, \ldots, \overline{m-1},$$

ahol $\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\} = \{bq + a \mid q \in \mathbb{Z}\}$, azaz $\mathbb{Z}/\equiv \pmod{m} = \{\overline{0}, \ldots, \overline{m-1}\}$. Műveleteket definiálunk a $\mathbb{Z}_m := \mathbb{Z}/\equiv \pmod{m}$ halmazon:

$$\overline{a} + \overline{b} = \overline{a+b},$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

A modulo m maradékosztályok gyűrűje.

Tétel.

A $(\mathbb{Z}_m; +, \cdot)$ algebra kommutatív, egységelemes gyűrű.

A $(\mathbb{Z}_m; +, \cdot)$ gyűrű neve: **modulo m maradékosztálygyűrű**.

A modulo m maradékosztályok gyűrűje.

Tétel.

A $(\mathbb{Z}_m; +, \cdot)$ algebra kommutatív, egységelemes gyűrű.

A $(\mathbb{Z}_m; +, \cdot)$ gyűrű neve: **modulo m maradékosztálygyűrű**.

Tétel.

A $\mathbb{Z}_m$ gyűrű pontosan akkor test, ha m prímszám.

Tétel.

Legyen K tetszőleges test, $f, g \in K[x]$, $g \neq 0$. Ekkor vannak olyan $q, r \in K[x]$ polinomok, amelyekre $f = gq + r$ teljesül és $r^* < g^*$.

Legyenek f és g K feletti polinomok, $f = f_n x^n + \cdots + f_0 \in K$, $g = g_m x^m + \cdots + g_0$ $(f_n, g_m \neq 0)$.
1. eset: $n < m$. Ekkor $f = g \cdot 0 + f$ és $f^* = n < m = g^*$.
2. eset: $m \leqslant n$. Ekkor az f és $f_n g_m^{-1} x^{n-m} g$ polinomok főegyüthatója megegyezik, így $f - f_n g_m^{-1} x^{n-m} g$ fokszáma kisebb, mint n. Legyen $f_1 = f - f_n g_m^{-1} x^{n-m} g$, és ismételjük meg a fent lépést. Folytassuk addig az eljárást, amíg g-nél alacsonyabb fokú polinomot kapunk.

Legyenek $f = 2x^5 + x^4 - 3x^2 + 7x - 12 \in \mathbb{Q}[x]$, $g = 7x^3 - x + 3 \in \mathbb{Q}[x]$. Ekkor

$$f - \frac{2}{7}x^2 g = x^4 + \frac{2}{7}x^3 - \frac{27}{7}x^2 + 7x - 12 =: f_1,$$
$$f_1 - \frac{1}{7}xg = \frac{2}{7}x^3 - \frac{26}{7}x^2 + \frac{46}{7}x - 12 =: f_2,$$
$$f_2 - \frac{2}{49}g = -\frac{26}{7}x^2 + \frac{324}{49}x - \frac{594}{49} =: f_3.$$

Mivel $f_3^* < g^*$, ezért vége az eljárásnak, és azt kapjuk, hogy

$$f = g \underbrace{\left(\frac{2}{7}x^2 + \frac{1}{7}x + \frac{2}{49}\right)}_{q:=} + \underbrace{\left(-\frac{26}{7}x^2 + \frac{324}{49}x - \frac{594}{49}\right)}_{r:=}.$$

Tegyük fel, hogy $f = gq_i + r_i$ $(i = 1, 2)$, ahol $r_1^*, r_2^* < g^*$. Ekkor

$$\begin{aligned} gq_1 + r_1 = gq_2 + r_2 &\iff g(q_1 - q_2) = r_2 - r_1 \\ &\iff g \mid r_2 - r_1 \\ &\iff r_1 = r_2 \text{ és } q_1 = q_2. \end{aligned}$$

Azaz a maradékos osztás során a hányados (q) és maradék (r) egyértelmű.

Polinomok.
Gyöktényezős alak.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ gyöke f-nek, ha $f(\alpha) = 0$. Az α elem k-szoros gyöke f-nek, ha $f = (x - \alpha)^k g$, ahol $g \in K[x]$ és α nem gyöke g-nek.

Polinomok.
Gyöktényezős alak.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ gyöke f-nek, ha $f(\alpha) = 0$. Az α elem k-szoros gyöke f-nek, ha $f = (x - \alpha)^k g$, ahol $g \in K[x]$ és α nem gyöke g-nek.

Bézout-tétel.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ pontosan akkor gyöke az f polinomnak, ha $x - \alpha \mid f$ teljesül $K[x]$-ben.

Polinomok.
Gyöktényezős alak.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ gyöke f-nek, ha $f(\alpha) = 0$. Az α elem k-szoros gyöke f-nek, ha $f = (x - \alpha)^k g$, ahol $g \in K[x]$ és α nem gyöke g-nek.

Bézout-tétel.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ pontosan akkor gyöke az f polinomnak, ha $x - \alpha \mid f$ teljesül $K[x]$-ben.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ gyöke f-nek, ha $f(\alpha) = 0$. Az α elem k-szoros gyöke f-nek, ha $f = (x - \alpha)^k g$, ahol $g \in K[x]$ és α nem gyöke g-nek.

Bézout-tétel.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ pontosan akkor gyöke az f polinomnak, ha $x - \alpha \mid f$ teljesül $K[x]$-ben.

Legyen $f \in K[x]$ n-edfokú polinom, amelynek gyökei az L testben $\alpha_1, \ldots, \alpha_n$. Ekkor f gyöktényezős alakja:

$$f = (x - \alpha_1) \cdots (x - \alpha_n).$$

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ gyöke f-nek, ha $f(\alpha) = 0$. Az α elem k-szoros gyöke f-nek, ha $f = (x - \alpha)^k g$, ahol $g \in K[x]$ és α nem gyöke g-nek.

Bézout-tétel.

Legyen f tetszőleges K feletti polinom. Ekkor $\alpha \in K$ pontosan akkor gyöke az f polinomnak, ha $x - \alpha \mid f$ teljesül $K[x]$-ben.

Legyen $f \in K[x]$ n-edfokú polinom, amelynek gyökei az L testben $\alpha_1, \ldots, \alpha_n$. Ekkor f gyöktényezős alakja:

$$f = (x - \alpha_1) \cdots (x - \alpha_n).$$

Ha f kanonikus alakja $f = a_n x^n + \cdots + a_1 x + a_0$, akkor a két alak összehasonlításából megkapjuk a Viète-formulákat.

Viète-formulák:

$$\alpha_1 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n},$$
$$\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n},$$
$$\vdots$$
$$\sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \alpha_{i_1}\cdots\alpha_{i_k} = (-1)^k\frac{a_{n-k}}{a_n},$$
$$\vdots$$
$$\alpha_1\cdots\alpha_n = (-1)^n\frac{a_0}{a_n}.$$

Definíció: Euklideszi algoritmus.

Legyenek f és g a K test feletti polinomok, $g \neq 0$. Definiáljuk az alábbi polinomokat:

$$
\begin{aligned}
f &= gq_1 + r_1, && (q_1, r_1 \in K[x],\ r_1^* < g^*),\\
g &= r_1 q_2 + r_2, && (q_2, r_2 \in K[x],\ r_2^* < r_1^*),\\
r_1 &= r_2 q_3 + r_3, && (q_3, r_3 \in K[x],\ r_3^* < r_2^*),\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, && (q_n, r_n \in K[x],\ r_n^* < r_{n-1}^*),\\
r_{n-1} &= r_n q_{n+1} + 0, && (q_{n+1} \in K[x]).
\end{aligned}
$$

Tétel.

Legyenek f és g a K test feletti polinomok. Ekkor az f és g polinomoknak létezik legnagyobb közös osztója, és

$$\text{ln.k.o.}(f,g) \sim \begin{cases} 0, & \text{ha } g = 0, \\ r_n, & \text{különben.} \end{cases}$$

Tétel.

Legyenek f és g a K test feletti polinomok. Ekkor az f és g polinomoknak létezik legnagyobb közös osztója, és

$$\text{ln.k.o.}(f,g) \sim \begin{cases} 0, & \text{ha } g = 0, \\ r_n, & \text{különben.} \end{cases}$$

Következmény.

Tetszőleges K test esetén $K[x]$ Euklideszi gyűrű.

Definíció: ideál.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű I részhalmaza **ideál**, ha I részgyűrű $K[x]$-ben és tetszőleges $f \in I$ és $g \in K[x]$ polinomokra $fg = gf \in I$. Jelölés: $I \lhd K[x]$.

Definíció: ideál.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű I részhalmaza **ideál**, ha I részgyűrű $K[x]$-ben és tetszőleges $f \in I$ és $g \in K[x]$ polinomokra $fg = gf \in I$. Jelölés: $I \triangleleft K[x]$.

Példa.

Az $K[x]$ polinomgyűrűben

Tetszőleges $f \in K[x]$-re az $(f) = \{fg \mid g \in K[x]\}$ ideál, amelyet az f **által generált főideálnak nevezünk.**

Definíció: ideál.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű I részhalmaza **ideál**, ha I részgyűrű $K[x]$-ben és tetszőleges $f \in I$ és $g \in K[x]$ polinomokra $fg = gf \in I$. Jelölés: $I \triangleleft K[x]$.

Példa.

Az $K[x]$ polinomgyűrűben

- $\{0\}$, $K[x]$ ideálok (ezek a triviális ideálok);

Tetszőleges $f \in K[x]$-re az $(f) = \{fg \mid g \in K[x]\}$ ideál, amelyet az f **által generált főideálnak nevezünk.**

Definíció: ideál.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű I részhalmaza **ideál**, ha I részgyűrű $K[x]$-ben és tetszőleges $f \in I$ és $g \in K[x]$ polinomokra $fg = gf \in I$. Jelölés: $I \triangleleft K[x]$.

Példa.

Az $K[x]$ polinomgyűrűben

- $\{0\}$, $K[x]$ ideálok (ezek a triviális ideálok);
- $\left\{(x^2+1)\cdot g \mid g \in K[x]\right\}$ ideál;

Tetszőleges $f \in K[x]$-re az $(f) = \{fg \mid g \in K[x]\}$ ideál, amelyet az f **által generált főideálnak nevezünk.**

Definíció: ideál.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű I részhalmaza **ideál**, ha I részgyűrű $K[x]$-ben és tetszőleges $f \in I$ és $g \in K[x]$ polinomokra $fg = gf \in I$. Jelölés: $I \triangleleft K[x]$.

Példa.

Az $K[x]$ polinomgyűrűben

- $\{0\}$, $K[x]$ ideálok (ezek a triviális ideálok);
- $\left\{(x^2+1)\cdot g \mid g \in K[x]\right\}$ ideál;
- $\{f \in K[x] \mid f(0) = 0\}$ ideál.

Tetszőleges $f \in K[x]$-re az $(f) = \{fg \mid g \in K[x]\}$ ideál, amelyet az f **által generált főideálnak nevezünk.**

Tétel.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű valamennyi ideálja főideál.

Tétel.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű valamennyi ideálja főideál.

Tétel.

Legyen $f, g \in K[x]$. Ekkor

Tétel.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű valamennyi ideálja főideál.

Tétel.

Legyen $f, g \in K[x]$. Ekkor

- $f \mid g \iff (g) \subseteq (f)$;

Tétel.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű valamennyi ideálja főideál.

Tétel.

Legyen $f, g \in K[x]$. Ekkor

- $f \mid g \iff (g) \subseteq (f)$;
- $f \sim g \iff (f) = (g)$;

Tétel.

A K test feletti egyhatározatlanú $K[x]$ polinomgyűrű valamennyi ideálja főideál.

Tétel.

Legyen $f, g \in K[x]$. Ekkor

- $f \mid g \iff (g) \subseteq (f)$;
- $f \sim g \iff (f) = (g)$;
- az (f) főideál pontosan akkor maximális, ha f irreducibilis $K[x]$-ben.

Legyen $I \triangleleft K[x]$ és $g \in K[x]$. Ekkor a g polinom I szerinti mellékosztályának nevezzük a $g + I = \{g + f \mid f \in I\}$ halmazt. A $g + I$ és $h + I$ mellékosztályok pontosan akkor egyeznek meg, ha $g - h \in I$. Ha $I = (f)$, akkor $g - h \in I$ pontosan akkor teljesül, ha $f \mid g - h$. A $\{g + I \mid g \in K[x]\}$ halmazrendszer $K[x]$ egy osztályozását alkotja.

Definíció: polinom szerinti maradékosztálygyűrű.

Ha $I \triangleleft K[x]$, akkor $\{g + I \mid g \in K[x]\}$ halmaz szintén gyűrűt alkot a

$$(g + I) + (h + I) = (g + h) + I, \quad (g + I) \cdot (h + I) = (g \cdot h) + I$$

műveletekre vonatkozóan. A kapott gyűrűt **a $K[x]$ polinomgyűrű f polinomja szerinti maradékosztálygyűrűjének** nevezzük.

Tétel.

Legyen $I = (f)$ ideál a $K[x]$ polinomgyűrűben, ekkor $K[x]/I$ pontosan akkor test, ha I maximális ideál, azaz $f \in K[x]$ irreducibilis. Ha f irreducibilis $K[x]$-ben, akkor $K[x]/(f)$ minden eleme egyértelműen felírható $g + (f)$ alakban, ahol $g \in K[x]$ és $g^* < f^*$.

Ha $K = \mathbb{Z}_p$ és $f \in \mathbb{Z}_p[x]$ irreducibilis polinom, akkor a kapott $\mathbb{Z}_p[x]/(f)$ test véges lesz, melynek elemszáma p^n, ahol $n = f^*$.
Az $f = x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$ polinom irreducibilis, így $\mathbb{Z}_2[x]/(x^2 + x + \overline{1})$ test, melynek 4 eleme van: $\overline{0} + (f)$, $\overline{1} + (f)$, $x + (f)$ és $x + \overline{1} + (f)$. A test művelettáblázatai pedig a következők:

Polinomok.

Polinom szerinti maradékosztálygyűrűk.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Polinomok.

Polinom szerinti maradékosztálygyűrűk.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	$x+1$

Tétel.

Tétel.

(a) Ha K véges test, akkor K elemszáma prímhatvány.

Tétel.

(a) Ha K véges test, akkor K elemszáma prímhatvány.

(b) Ha K és L azonos elemszámú véges testek, akkor $K \cong L$.

Tétel.

(a) Ha K véges test, akkor K elemszáma prímhatvány.

(b) Ha K és L azonos elemszámú véges testek, akkor $K \cong L$.

(c) Tetszőleges p^n prímhatványra (p prímszám, $n \in \mathbb{N}$) van q-elemű test, és izomorf $\mathbb{Z}_p[x]/(f)$-fel, ahol $f \in \mathbb{Z}_p[x]$ egy n-edfokú irreducibilis polinom.