Algebra és számelmélet gyakorlat
(matematika BSc)
2024/2025 I. félév

2024. December 02.

1. Absztrakt algebra

1.1. Definíció. *Ha egy nem üres halmazon értelmezett egy asszociatív művelet, akkor félcsoportról beszélünk.*

1.2. Definíció (Csoport). *Egy G nem üres halmaz csoport, ha értelmezett rajta egy $*$ művelet a következő tulajdonságokkal:*

(1) A $*$ művelet asszociatív;

(2) A $*$-ra nézve az 1 egységelem. (neutrális elem)

(3) G minden elemének van inverze.

Kommutatív(Abel-csoport) csoport: ha $*$ kommutatív.

Példák:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}[x], \mathbb{R}^{n\times m}$ kommutatív csoport az összeadása.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$-ből a 0-t kihagyva kommutatív csoport a szorzásra.
- Az S_n permutációi nemkommutatív csoport a kompozícióra $n > 2$ esetén.
- $\mathbb{Z}_5$ elemei kommutatív csoport a mod 5 összeadásra

1.3. Definíció (Gyűrű). *Az R gyűrű, ha értelmezett az összeadás és a szorzás művelete úgy, hogy*

(1) Az összeadás asszociatív.

(2) Az összeadás kommutatív.

(3) Van az összeadásra nézve egy 0 nullelem.

(4) Minden elemnek van ellentettje.

(5) A szorzás asszociatív.

(6) Tetszőleges $x, y, z \in R$ esetén igaz a disztributivitás: $(x+y)z = xz+yz$ és $z(x+y) = zx+zy$.

Kommutatív gyűrű: a szorzás kommutatív.
Egységelemes gyűrű: a szorzásra nézve van egységelem (jele 1).
Test: egységelemes, kommutatív gyűrű, amelyben minden nem nulla elemnek van (a szorzásra) inverze.

1.4. Definíció. *Ha egy gyűrű nem nulla elemei csoportot alkotnak a szorzásra, akkor a gyűrűt ferdetestnek hívjuk. A testek a kommutatív ferdetestek.*

1.1. Tétel. *Minden ferdetest nullosztómentes*

1.1. Állítás. *A $\mathbb{Z}_m$ gyűrű akkor és csak akkor nullosztómentes, ha m prímszám és ebben az esetben test is.*

Példák:

- A polinomok, azaz $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ gyűrű.
- A négyzetes mátrixok, azaz $\mathbb{Q}^{n\times n}, \mathbb{R}^{n\times n}, \mathbb{C}^{n\times n}$ gyűrű.
- Folytonos (differenciálható) $\mathbb{R} \to \mathbb{R}$ függvények: gyűrű
- Az $a+bi$ alakú számok $(a, b \in \mathbb{Z})$: gyűrű
- Az $a+bi$ alakú számok $(a, b \in \mathbb{Q})$: test
- Az $a+b\sqrt{2}$ alakú számok $(a, b \in \mathbb{Z})$: gyűrű
- Az $a+b\sqrt{2}$ alakú számok $(a, b \in \mathbb{Q})$: test

1.5. Definíció (Euklideszi gyűrű). *Az R szokásos gyűrűt euklideszi gyűrűnek nevezzük, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény (az úgynevezett euklideszi norma) a következő tulajdonsággal. Minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $\varphi(r) < \varphi(b)$.*

Az egészek gyűrűje euklideszi, φ az abszolút érték. Test fölötti polinomgyűrű euklideszi, φ a fokszám. Az euklideszi gyűrűben érvényes a számelmélet alaptétele.

2. Polinomok

2.1. Tétel (Polinomok azonossági tétele). *Ha egy R nullosztómentes gyűrű fölött adott két, legfeljebb n-edfokú polinom, amelyek több, mint n (R-beli) helyen megegyeznek, akkor a két polinom egyenlő.*

2.2. Tétel (K 2.5.8). *Ha az R kommutatív, egységelemes gyűrű fölötti f polimomra*

$$f(x) = (x - b_1)(x - b_2)\cdots(x - b_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \cdots + (-1)^n \sigma_n$$

akkor a Viéte-formulák, azaz a gyökök és együtthatók közötti összefüggések a következők:

$$\begin{aligned}
\sigma_1 &= b_1 + b_2 + \cdots + b_n \qquad \textit{tagok száma: } \binom{n}{1} = n \\
\sigma_2 &= b_1 b_2 + \cdots + b_1 b_n + b_2 b_3 + \cdots + b_{n-1} b_n \qquad \textit{tagok száma: } \binom{n}{2} \\
\sigma_k &= b_1 b_2 \ldots b_k + \ldots \qquad \textit{tagok száma: } \binom{n}{k} \\
\sigma_k &= b_1 b_2 \ldots b_n \qquad \textit{tagok száma: } \binom{n}{n} = 1
\end{aligned}$$

A σ_k úgy keletkezik, hogy a $b_1, \ldots, b_n$ közül az összes lehetséges módon kiválasztunk k darabot, a kiválasztott b_i-ket összeszorozzuk, majd a kapott szorzatokat összeadjuk. Szokás a σ_0-ról is beszélni és a fenti f főegyütthatójaként konstans 1-nek tekinteni.

2.3. Tétel (K 2.5.8). *Legyen*

$$f(x) = a_0 + a_1 x + \ldots a_n x^n = a_n(x - b_1)\cdots(x - b_n)$$

Ekkor $0 \leq k \leq n$ *esetén* $a_k = a_n(-1)^{n-k}\sigma_{n-k}(b_1, b_2, \ldots b_n)$ *így*

$$\sigma_k(b_1, b_2, \ldots b_n) = (-1)^k a_{n-k}/a_n$$

Ez a gyökök és együtthatók összefüggése (Viéte-formulák).

Müllner Károly
Email: mullni@hotmail.com
https://mullni.elte.hu