Csoportok, testbővítések.

Klukovits Lajos

TTIK Bolyai Intézet

2020. november 27.

Műveletartó leképezések.

Definition

Legyenek $(G, \cdot)$ csoport, $(H, \circ)$ grupoid, $\varphi\colon G \to H$ leképezés. Ha bármely $a, b \in G$-re $(a \cdot b)\varphi = (a\varphi) \circ (b\varphi)$, akkor azt mondjuk, hogy a φ leképezés megőrzi a G csoport műveletét. A műveletőrző leképezéseket homomorfizmusoknak nevezzük, a bijektív homomorfizmusokat pedig izomorfizmusoknak.

Theorem

Legyen S egységelemes félcsoport, H grupoid, $\varphi\colon S \to H$ szürjektív homomorfizmus. A következő állítások igazak.

1. *H művelete asszociatív, azaz H félcsoport.*
2. *Ha S művelete kommutatív, akkor H művelete is kommutatív.*
3. *Ha $1 \in S$ egységeleme S-nek, akkor 1φ egységelem H-ban.*
4. *Ha $a \in S$ invertálható, akkor $a\varphi$ is invertálható, és $(a\varphi)^{-1} = (a^{-1})\varphi$.*

Műveletartó leképezések.

Bizonyítás.

(1) Legyenek $a, b, c \in H$ tetszőlegesek. A φ szürjektív, így léteznek olyan $a', b', c' \in S$ elemek, hogy $a'\varphi = a$, $b'\varphi = b$, $c'\varphi = c$. Ekkor

$$\begin{aligned} a(bc) &= (a'\varphi)\left((b'\varphi)(c'\varphi)\right) = \left(a'(b'c')\right)\varphi \\ &= \left((a'b')c'\right) = \left((a\varphi b\varphi)\right)c\varphi \\ &= (ab)c \end{aligned}$$

(2) Analóg módon igazolható, mint (1).

(3) $a \in H$ tetszőleges, $a = a'\varphi$ valamely $a' \in S$-re. $a(1\varphi) = (a'\varphi)(1\varphi) = (a'1)\varphi = a'\varphi = a$. A másik oldal hasonlóan megy.

(4) Legyen $a \in S$ invertálható elem, inverzét jelölje a^{-1}. $(a\varphi)(a^{-1}\varphi) = (aa^{-1})\varphi = 1\varphi$. Mivel az inverz egyértelmű, amennyiben a művelet asszociatív, a bizonyítás kész.

Permutációcsoportok

Definíció.

Legyen A tetszőleges nemüres halmaz. A $\sigma\colon A \to A$ bijektív leképezéseket A **fölötti permutációknak** nevezzük. Az összes A fölötti permutációk halmazát S_A-val jelöljük.

Állítás.

Tetszőleges nemüres A halmaz esetén S_A csoport a leképezésszorzással.

Definíció.

Az előbbi S_A csoportot **A fölötti teljes permutációcsoportnak** nevezzük, míg részcsoportjait **A fölötti permutációcsoportoknak**.

Cayley tétele.

Minden csoport izomorf egy — az elemei halmaza fölötti — permutációcsoporttal.

Cayley tételének bizonyítása,

Bizonyítás.

Legyen G egy tetszőleges csoport és $g \in G$.

A $\sigma_g \colon G \to G$, $a\sigma_g = ag$ minden $a \in G$-re leképezések a G halmaz permutációi.

A $P = \{\sigma_g \colon g \in G\} \subseteq S_G$ halmaz csoport a leképezésszorzással, ugyanis bármely $g, h \in G$-re $\sigma_g\sigma_h = \sigma_{gh}$.

Egyszerű számolással kapható, hogy a $\psi \colon G \to P$, $g \mapsto \sigma_g$ leképezés adja a kívánt izomorfizmust.

□

Megjegyzés,

Cayley e tételt eredetileg véges csoportokra találta, de a végességnek itt nincs szerepe.

Elemrend, ciklikus csoportok.

Definíció (egész kitevős hatványozás csoportban).

Legyen $a \in G$ és $n \in \mathbb{N}$. Az a elem n-edig hatványa az $a^n = a \cdot \ldots \cdot a$ n tényezős szorzat. Továbbá legyen $a^{-n} = a^{-1} \cdot \ldots \cdot a^{-1}$, amely szintén egy n tényezős szorzat. Végül, $a^0 = 1$.

Tétel.

Legyen G csoport, $a, b \in G$ és $m, n \in \mathbb{Z}$. Ekkor érvényesek az alábbi egyenlőségek.

1. $a^m \cdot a^n = a^{m+n}$,
2. $(a^m)^n = a^{mn}$,
3. ha $ab = ba$, akkor $(ab)^m = a^m \cdot b^m$.

Elemrend, ciklikus csoportok.

Definíció.

Az $a \in G$ **elem rendje** az a legkisebb $n \in \mathbb{N}$, amelyre $a^n = 1$. Ha ilyen kitevő nem létezik, azaz az a elem egyetlen természetes szám kitevős hatványa sem 1, akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét $\mathrm{o}(a)$ jelöli. A G **csoport rendjén** pedig elemei számát értjük.

Állítás.

Ha $a \in G$ véges rendű elem, mondjuk $\mathrm{o}(a) = n$, akkor bármely $r, s \in \mathbb{Z}$-re

1. $a^r = 1 \quad \Leftrightarrow \quad n | r$,
2. $a^r = a^s \quad \Leftrightarrow \quad r \equiv s \pmod{n}$,
3. $\mathrm{o}(a^r) = \frac{n}{\text{l.n.k.o.}(r,n)}$.

Elemrend, ciklikus csoportok.

Megjegyzés.

A $\mathbb{C}^*$ csoport (a nemzéró komplex számok multiplikatív csoportja) véges rendű elemei épp az egységgyökök. Ha valamely $\varepsilon \in \mathbb{C}^*$-ra $\mathrm{o}(\varepsilon) = n$, akkor ε primitív n-edik egységgyök.

Definíció.

Azt mondjuk, hogy G **ciklikus csoport**, ha $G = [a]$ valamely $a \in G$-re, ahol $[a]$ az $\in G$ összes egész kitevős hatványainak halmaza.

Tétel.

Legyen G egy tetszőleges csoport és $a \in G$. Ha $\mathrm{o}(a) = n$, akkor $([a], \cdot) \cong (\mathbb{Z}_n, +)$, míg ha a rendje végtelen, akkor $([a], \cdot) \cong (\mathbb{Z}, +)$.

Elemrend, ciklikus csoportok.

Következmény.

Egy csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \ldots$ additív csoportok valamelyikével.

Tétel.

Ciklikus csoport minden részcsoportja és homomorf képe ciklikus csoport.

Ciklikus csoportok.

Legyen $G = [a]$ ciklikus csoport.

Bizonyítás.

Legyen $H \subseteq G$ tetszőleges részcsoport Ha $|H| = 1$, nincs mit bizonyítni. Legyen $k \in \mathbb{N}$ a legkisebb olyan kitevő, amelyre $a^k \in H$.

Állítjuk, hogy $H = [a^k]$. Ugyanis, ha $a^m \in H$ tetszőleges, akkor maradékos osztást végezve: $m = kq + r$, ahol $0 \leq r < k$.

$a^r = a^m \cdot \left((a^k)^q\right)^{-1}$.

A jobb oldalon álló elem H-beli, így szükségképp $r = 0$.

A második állítást igazolja, hogy ha $\varphi\colon G \to H$ szürjektív homomrfizmus, akkor $H = [a\varphi]$.

□

Részcsoport, generálás.

Állítás.

Legyen G csoport és $H \subseteq G$. H **részcsoportja** G**-nek,** ha

1. $1 \in H$,
2. $\forall a, b \in H \quad \Rightarrow \quad ab \in H$;
3. $\forall a \in H \quad \Rightarrow \quad a^{-1} \in H$.

Tétel.

Részcsoportok metszete részcsoport: azaz ha $(H_i)_{i \in I}$ a G csoport részcsoportjai tetszőleges rendszere (azaz $H_i \leq G\colon \forall i \in I$), akkor $\bigcap_{i \in I} H_i \leq G$.

Definíció

Legyen G csoport, és $B \subseteq G$. A B halmaz által **generált részcsoport** a legszűkebb olyan részcsoport, amely tartalmazza B részhalmazt. Jelölése: $[B]$.

Részcsoport, generálás.

Definíció.

Ha $[B] = G$ a G csoport valamely B részhalmazára, akkor azt mondjuk, hogy B a G csoport (egy) **generátorrendszere**.

Állítás.

Legyen G csoport. A $B \subseteq G$ részhalmaz által generált részcsoport azokból az elemekből áll, amelyek megkaphatók B elemeiből a szorzás és az inverzképzés véges számú alkalmazásával:

$$[B] = \{b_1^{\varepsilon_1} \cdot \ldots \cdot b_k^{\varepsilon_k} \colon k \in \mathbb{N}_0,\ b_1, \ldots, b_k \in B,\ \varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}\}$$

Tétel.

Legyen G csoport és $H \leq G$ Tetszőleges $a, b \in G$-re a $a \sim b \ \Leftrightarrow \ a^{-1}b \in H$ reláció ekvivalenciareláció G-n. Egy $a \in G$ elem ekvivalencia-osztálya $aH = \{ah\colon h \in H\}$.

Részcsoport, generálás.

Következmény.

Egy $H \leq G$ részcsoport szerinti összes különböző bal oldali aH mellékosztályai G-nek egy osztályozását alkotják.

Bizonyítás.

Legyen $g \in aH \cap bH$. Ekkor $g = ah_1 = bh_2$, $h_1, h_2 \in H$.

Ebből $a = b(h_2 h_1^{-1})$, azaz $a \in bH$.

Ez maga után vonja, $aH \subseteq bH$.

Mivel a fordított irányú tartalmazás ugyanígy kapható, $aH = bH$. □

Részcsoport, generálás.

Definíció.

A véges G csoport H részcsoportja szerinti bal oldali mellékosztályai számát H (bal oldali) **indexének** nevezzük. jelölése: $|G : H|$

(Lagrange-tétele)

Tetszőleges G véges csoport és $H \leq G$ részcsoportra $|G| = |H| \cdot |G : H|$. Másképpen mondva, véges csoport részcsoportjának rendje osztója a csoport rendjének.

Bizonyítás.

Legyen $H, a_1H, \ldots, a_{k-1}H$ az összes különböző H szerinti baloldali mellékosztály.

Mivel a $\varphi_i : H \to a_iH$, $\varphi_i : h \mapsto a_ih$ leképezések bijektívek, $|H| = |a_iH|$ minden $1 \leq i < k$.

Mivel $G = H \cup a_1H \cup \ldots \cup a_{k-1}H$, a bizonyítás kész. □

Normálosztó, faktorcsoport.

Definíció.

Legyen G csoport. Azt mondjuk, hogy a $N \subseteq G$ részcsoport **normálosztó,** másképpen mondva **normális részcsoport**, ha tetszőleges $a \in G$-re $aN = Na$, azaz bármely $g \in N$-hez van olyan $h \in N$, hogy $ag = ha$. Jelölése: $G \triangleright N$.

Definíció.

Legyen G csoport és $G \triangleright N$. A $G/N = \{aN : a \in G\}$ halmazt G N **szerinti faktorhalmazának** nevezzük.

Definíció.

Legyen G csoport és $A, B \subseteq G$. A $\mathcal{P}(G)$ halmazon definiált $AB = \{ab : a \in A,\ b \in B\}$ műveletet **komplexusszorzásnak** nevezzük.

Normálosztó, faktorcsoport.

Állítás.

Legyen G csoport és $G \triangleright N$. A G/N faktorhalmaz csoport a komplexusszorzással. Az előbbi G/N csoportot G N **szerinti faktorcsoportjának** nevezzük.

Tétel (csoportelméleti homorfiatétel).

Ha G, H csoportok és $\varphi : G \to H$ szürjektív homomorfizmus, akkor van G-nek olyan N normálosztója, hogy $H \cong G/N$.

Testbővítések.

Definíció.

Azt mondjuk, hogy az L test a K test **bővítése**, ha $K \subseteq L$. Ez esetben használni fogjuk a $L\colon K$ jelölést.

Állítás.

Ha $(K_i)_{i\in I}$ az L test résztestei, akkor $\bigcap_{i\in I} K_i$ test.

Definíció.

Legyen $L\colon K$ testbővítés, és $\alpha \in L$. Az L test $K \cup \{\alpha\}$-t tartalmazó legszűkebb résztestét (e halmaz által generált résztestét) a K test α-val való **egyszerű bővítésének** nevezzük, és $K(\alpha)$-val jelöljük.
Világos, hogy

$$K(\alpha) = \bigcap \{L' \subseteq L\colon K \subseteq L',\ \alpha \in L',\ L' \text{ test}\}.$$

Testbővítések.

Theorem

Legyen $L\colon K$ testbővítés és $\alpha \in L$. Ekkor

$$K(\alpha) = \{f(\alpha)/g(\alpha)\colon f, g \in K[x],\ g(\alpha) \neq 0\}.$$

Bizonyítás.

Rutin számolással kapható:
$T = \{f(\alpha)/g(\alpha)\colon f, g \in K[x],\ g(\alpha) \neq 0\}$ test, és $\alpha \in T$.

Ebből $K(\alpha)$ minimális volta alapján azonnal adódik, hogy $K(\alpha) \subseteq T$.

Megfordítva: legyen $f \in K[x]$ tetszőleges polinom.

Az $f(\alpha)$ elem α-ból és a K test elemeiből összeadással, kivonással és szorzással kapható, így $f(\alpha) \in K(\alpha)$.

Lévén $K(\alpha)$ test, bármely további g K fölötti polinomra, ha $g(\alpha) \neq 0$, akkor $f(\alpha)/g(\alpha) \in K(\alpha)$, azaz $K(\alpha) \supseteq T$.

□

Testbővítések.

Definíció.

Legyen $L\colon K$ egy testbővítés. Azt mondjuk, hogy az $\alpha \in L$ elem **algebrai K fölött**, ha van olyan $f \in K[x]$ nemkonstans polinom, hogy $f(\alpha) = 0$. Ellenkező esetnem α **transzcendens K fölött.**

Definíció.

Azt mondjuk, hogy $L\colon K$ **algebrai testbővítés**, ha L minden eleme algebrai K fölött. Ellenkező esetben $L\colon K$ **transzcendens testbővítés**.

Definíció.

Azt mondjuk, hogy $\alpha \in \mathbb{C}$ **algebrai szám**, ha algebrai elem a $\mathbb{Q}$ test fölött. A többi komplex számot **transzcendens számnak** nevezzük.

Transzcendens számok.

Euler.

(1) Euler sejtése: „bizonyos számok meghaladják az algebrai módszerek erejét". Ezek a transzcendens számok. Úgy vélte, hogy az e, π konstansok, továbbá az exponenciális és a trigonometrikus függvények legtöbb értéke transzcendens.
(2) Csak e irracionális voltát tudta igazolni.
(3) Tanítványa, Lambert ugyanezt mutatta meg a π-ről.
(4) Az első transzcendens számot Liouville konstruálta meg, és 1844-ben publikálta:

Liouville tétele.

Az

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001\ldots$$

szám transzcendens.

Transzcendens számok.

Példák.

(1) A π, az e és a $2^{\sqrt{2}}$ számok transzcendensek.
(2) Nem ismeretes, hogy $\pi + e$ milyen szám, de a $\pi + ie$ komplex szám transzcendens volta egyszerűen kapható.
(3) Egy K test minden elemei algebrai K fölött.
(4) Hilbert VII. problémája: Milyen szám az α^β, ahol α, β algebrai számok, $\alpha \neq 0, \pm 1$, β irracionális. Sejtése szerint mindig transzcendens, vagy legalább irracionális. Pl. $2^{\sqrt{2}}$ transzcendens (1932).

Theorem

(Gelfond-Schneider tétel 1934) *Ha α, β algebrai számok, $\alpha \neq 0, \pm 1$ és β irracionális, akkor α^β transzcendens szám.*

Algebrai bővítések.

Tétel.

Legyen $L\colon K$ testbővítés és $\alpha \in L$ algebrai K fölött. Pontosan egy olyan $f \in K[x]$ főpolinom létezik, amelyre $f(\alpha) = 0$ és ha valamely nemzéró $g \in K[x]$ polinomra $g(\alpha) = 0$, akkor $f | g$. Ezen f polinom irreducibilis K fölött.

Bizonyítás.

Legyen $J \subseteq K[x]$ azon legalább elsőfokú polinomok halmaza, amelyeknek α gyöke.

$J \neq \emptyset$, így van közöttük minimális fokszámú főpolinom. Jelöljön egy ilyet f.

Rutin számolással (maradékos osztás) kapható, hogy tetszőleges $g \in J$-re $f | g$, valamint az is hogy f irreducibilis:
$g = fq + r \Rightarrow g(\alpha) = r(\alpha) = 0 \Rightarrow r = 0$.

□

Algebrai bővítések.

Definíció.

Az előbbi tételbeli f polinomot az α elem **minimálpolinomjának** nevezzük. Azt mondjuk, hogy $L\colon K$ **egyszerű algebrai bővítés**, ha van olyan $\alpha \in L$ elem, hogy $K(\alpha) = L$.

Állítás.

Legyen $L\colon K$ testbővítés, $\alpha \in L$ algebrai elem K fölött, minimálpolinomját jelölje m, $\deg m = n$. Tetszőleges $f \in K[x]$ polinomra $f(\alpha)$ fölírható, mint α legfőljebb $n-1$-edfokú polinomja.

Bizonyítás.

Ha r jelöli az f és m-en végzett euklideszi osztás maradékát, akkor az $f(\alpha) = r(\alpha)$ egyenlőségből adódik állításunk. □

Algebrai bővítések.

Theorem

Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek minimálpolinomja n-edfokú. Ekkor a $K(\alpha)$ test elemei fölírhatók

$$\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

alakban, ahol $a_0, \ldots, a_{n-1} \in K$. Ezen elemeket a β elem egyértelműen meghatározza.

Bizonyítás.

Csak az egzisztenciát igazoljuk. Legyenek $f, g \in F[x]$ polinomok, $g(\alpha) \neq 0$.

Az $f(\alpha)$ nyilván fölírható így.

Tekintsük a $g(\alpha)^{-1}$ elemet. Ha fölírható a kívánt módon, akkor van olyan $q \in K[x]$ polinom, hogy $1/g(\alpha) = q(\alpha)$, azaz $g(\alpha)q(\alpha) - 1 = 0$.

A bizonyítás folytatása.

Kaptuk α gyöke a $gq-1$ K fölötti polinomnak.

Az α elem minimálpolinomja m, ezért alkalmas $p \in K[x]$ polinomra: $gq-1=pm$, tehát $K[x]$-ben megoldható a $gq-mp=1$ egyenlet.

Ez akkor teljesül, ha $\ln.\,k.\,o.(g,m) \sim 1$.

$h \sim \ln.\,k.\,o.(g,m)$ főpolinom, akkor $h|m$.

m irreducibilis főpolinom, ezért $h=m$, vagy $h=1$. Az első eset lehetetlen, mert abból $m|g$, azaz $g(\alpha)=0$ következne, ami lehetetlen.

Kaptuk tehát hogy g, m relatív prímek, az egyenlet megoldható, ezért $g(\alpha)$ inverze is írható az α legföljebb $n-1$-edfokú polinomja.

Algebrai bővítések.

Következmény.

Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek minimálpolinomja n-edfokú. Ekkor a $K(\alpha)$ n dimenziós vektortér a K test fölött.

Theorem

Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek f minimálpolinomja n-edfokú. Ekkor

$$K(\alpha) \cong K[x]/(f).$$

Következmény.

$$\mathbb{C} \cong \mathbb{R}[x]/(x^2+1).$$

Algebrai bővítések.

Theorem

Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek f minimálpolinomja n-edfokú. Ekkor

$$K(\alpha) \cong K[x]/(f).$$

Bizonyítás.

$\beta \in K(\alpha)$ egy tetszőleges elem. Léteznek olyan egyértelműen meghatározott $a_0, \ldots, a_{n-1} \in K$ elemek, hogy $\beta = a_0 + a_1\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$.

Legyen $g(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in K[x]$. Egyszerűen igazolható a korábbiak alapján, hogy a

$$\varphi\colon K(\alpha) \to K[x]/(f), \quad \beta \mapsto \overline{g} = g + (f)$$

leképezés a kívánt izomorfizmus.

Véges testek.

Theorem

Minden véges test elemszáma prímhatvány, és tetszőleges p prímszám és $n \in \mathbb{N}$ esetén létezik p^n elemű test.

Részleges bizonyítás.

Legyen p prímszám és $n \in \mathbb{N}$.

Válasszunk egy f n-edfokú irreducibilis polinomot a $\mathbb{Z}_p[x]$ gyűrűben (ilyen biztosan van).

A $\mathbb{Z}_p[x]/(f)$ faktorgyűrű test, és elemszáma p^n.

Példa.

Az $x^4+x^3+x^2+x+1$ polinom irreducibilis a kételemű test fölötti polinomgyűrűben, így a $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$ faktorgyűrű test és 16 elemű.