

AZ ABSZTRAKT ALGEBRA KIALAKULÁSA ÉS FEJLŐDÉSÉNEK NÉHÁNY MÉRFÖLDKÖVE.

Klukovits Lajos

TTIK Bolyai Intézet

2013. április 24.

A gyökek.

- Bombelli formális kalkulusa az $a \pm b\sqrt{-1}$ alakú kifejezésekre.
- A „helyettesítések csoportja.”
- Az általános n -edfokú egyenlet vizsgálatokor vagy az együtthatókat, vagy az $x_1, \dots, x_n$ gyököket független változóknak tekintették.
- Lagrange, Ruffini, Abel, Cayley: a lehető legalacsonyabb fokú „segédegyenletet” keresték, amely a gyökök egy $f(x_1, \dots, x_n)$ racionális függvénye. **Kérdésük:**
 - ▶ Hány különböző értéket vesz föl e polinom a gyökök permutálásakor.
 - ▶ Ha ezek a különböző értékek $f_1, \dots, f_s$, akkor a keresett egyenlet

$$(t - f_1)(t - f_2) \dots (t - f_s) = 0.$$

- ▶ A feladat az s meghatározása volt.

A gyökek.

A csoport fogalmának első jele.

Az eredmény (mai terminológiával): Ha H azon S_n -beli permutációk halmaza (részcsoportja!), amelyek az f polinomot fixen hagyják (önmagába viszik), akkor S_n H szerinti mellékosztályai f -et a különböző

$$f_1, \dots, f_s$$

polinomokba viszik (azaz az f s számú különböző értéket vesz föl), és így

$$s = (S_n : H).$$

Példák.

- 1 Ha $n = 4$, akkor az $f = x_1x_2 + x_3x_4$ választással $s = 3$.
- 2 $n = 5$ -re $s = 6$, ami „rossz” eredmény.

A gyökek.

Lineáris törtfüggvények

Felix Klein egy 1875-ös dolgozatában a

$$z' = \frac{az + b}{cz + d}$$

alakú lineáris transzformációkat vizsgálta a komplex síkon. Ezek, és szorzataik az egységkört körbe viszik át.

Ami már majdnem absztrakt algebra.

- Euler kalkulusa maradékosztályokra (lényegében megadta a $\mathbb{Z}_n$ gyűrűket és a $\mathbb{Z}_p$ testeket, pontosabban műveleteiket).
- Gauss kvadratikus formái: e formák bizonyos transzformációi.
- Galois véges teste.
- Hamilton kvaterniói.

Az első, már majdnem „Igazán Absztrakt” struktúra.

Hamilton kvaterniói 1.

Definíció. Legyen F test, továbbá $\mathcal{V}$ vektortér F fölött. Defináljunk e vektortéren egy (asszociatív) szorzást is, amelyre teljesül a

$$(\lambda a)b = \lambda(ab) = a(\lambda b) \quad (1)$$

azonosság minden $a, b \in \mathcal{V}$ és $\lambda \in F$ esetén. Azt mondjuk, hogy $\mathcal{V}$ (asszociatív) algebra az F test fölött, ha

- (1) $\mathcal{V}$ gyűrű,
- (2) $\mathcal{V}$ vektortér az F test fölött,
- (3) teljesül az (1) azonosság.
- (4) $\mathcal{V}$ zérusosztómentes algebra, ha $\mathcal{V}$ zérusosztómentes gyűrű.

Megjegyzés.

A kvaterniók (négydimenziós, asszociatív, zérusosztómentes) algebra a valós számtest fölött.

Az első, már majdnem „igazán absztrakt” struktúra.

Hamilton kvaterniói 2.

Definíció. Legyen

$$\mathbf{Q} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

továbbá i, j, k olyan szimbólumok, amelyekre

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \quad jk = i, \quad ki = j, \\ ji &= -k, \quad kj = -i, \quad ik = -j. \end{aligned}$$

A számolás ezen kifejezésekkel a „szokásos algebrai”, a három szimbólum fölcserélhető szorzásnál a valós számokkal.

Megjegyzés.

$\mathbf{Q}$ ferdetest az előbbi műveletekkel, de $\mathbb{R}$ fölötti négydimenziós zérusosztómentes algebra is.

A számfogalom bővítésének lezárása.

Frobenius tétele. 1882.

A valós számtest fölötti végesdimenziós, zérusosztómentes (asszociatív) algebrák a következők egyikével izomorfak.

- ❶ A valós számtest,
- ❷ a komplex számtest,
- ❸ a kvaterniók ferdeteste.

Megjegyzés.

E tétel lezárja a számfogalom bővítésének folyamatát, már a kvaterniók esetén is föl kell adni a szorzás kommutativitását.

Út a csoport absztrakt fogalmához 1.

Ernst SCHERING, 1869

- **Definíció.** Az $f = ax^2 + 2bxy + cy^2$ alakú kifejezéseket **kvadratikus formáknak** nevezik (Gauss), ahol $a, b, c \in \mathbb{R}$. E kvadratikus forma **diszkriminánsa** $\delta = b^2 - 4ac$.
- Gauss bevezette e kvadratikus formák **kompozícióját**, amely asszociatív és invertálható művelet (bizonyos feltételek mellett!).

Út a csoport absztrakt fogalmához 2.

Schering tétele.

Ha adott diszkriminánsú kvadratikus formák csoportjának $A, B, C, \dots$ generátorai rendre $a, b, c, \dots$ rendűek, akkor e csoport elemei egyértelműen reprezentálhatók, mint

$$A^\alpha B^\beta C^\gamma \dots$$

szorzatok, ahol α a modulo a , β a modulo b , ... maradékosztályokat futja végig.

Út a csoport absztrakt fogalmához 3.

Ernst SCHERING, 1869.

Megjegyzés. Vegyük észre, hogy ez lényegében a véges Abel-csoportok alaptétele, amelyet — ha nem is a ma megszokott általánosságban — L. Kronecker igazolt először 1853-as dolgozatában.

Arthur CAYLEY 1859-es dolgozata.

Legyen Θ olyan művelet-szimbólum, amelyre

$$\Theta(x, y, \dots) = (x', y', \dots).$$

Ha $x', y', \dots$ az $x, y, \dots$ szimbólumok egy permutációja, akkor Θ nem más, mint amit korábban „helyettesítésnek” neveztek. Ha pedig egyetlen x mennyiségre (szimbólumra) alkalmazzuk, akkor ő egy „közönséges függvényjel”:

$$\Theta x = x' = fx.$$

Az identikus operátort jelölje 1 , míg $\Theta\Psi$ az „összetett” operátort.

Út a csoport absztrakt fogalmához 4.

Arthur CAYLEY 1859-es dolgozata.

- Megjegyezte, hogy **a helyettesítések összetétele általában nem kommutatív.**
- Bevezette e dolgozatában a ma Cayley-táblának nevezett művelet megadást.

Cayley 1878-as dolgozata

Szimbólumok egy olyan $\alpha, \beta, \gamma, \dots$ összessége, amely tartalmazza e szimbólumok összes $\alpha\beta$ szorzatát minden lehetséges sorrendben, csoport. Egy csoport a benne szereplő szimbólumok kombinációinak szabályával együtt definiált.

Halmaz és művelet együttese!!!

Megjegyzés.

Cayley hallgatólagosan mindig feltételezte, hogy az általa tekintett kombinációk (szorzások) asszociatívok.

Út a csoport absztrakt fogalmához 5.

Cayley 1878-as dolgozata

- Fölvetette azt a kérdést, hogy adjuk meg az összes n elemű csoportot tetszőleges $n \in \mathbb{N}$ -re.
- Megfogalmazta azt az állítást, hogy „minden n elemű csoport reprezentálható, mint az n szimbólum helyettesítéseinek csoportja”, azaz azon állítást, amely ma Cayley reprezentációs tételeként (annak véges változataként) ismert:
- **Minden csoport izomorf egy permutációcsoporttal.**

Megjegyzés.

Cayley elmélete már majdnem általánosnak tekinthető: tartalmazza speciálisan a helyettesítéseket, és azt az általános kérdést, hogy adjuk meg az összes n elemű csoportot, ami ténylegesen azonos azzal a kérdéssel, hogy ugyanazon n -re adjuk meg az összes olyan csoportot, amely az n elem helyettesítéseiből áll.

Út a csoport absztrakt fogalmához 6.

Az „igazi” absztrakt definíció.

- Walter von DYCK és Heinrich WEBER nevéhez fűződik, akik egymástól függetlenül (de véletlenül ugyanazon folyóirat ugyanazon számában) közölték 1882-ben azt.
- Definíció.** A $(G, \cdot)$ pár (a G halmaz a rajta értelmezett $\cdot$ kétváltozós művelettel) csoport, ha
 - a művelet asszociatív,
 - van olyan $e \in G$, hogy minden $a \in G$ -re $a \cdot e = e \cdot a = a$,
 - minden $a \in G$ -hez van olyan $a' \in G$, hogy $a \cdot a' = a' \cdot a = e$.
- A kommutatív műveletű csoportokat Abel-csoportoknak nevezzük (N. H. Abel emlékére).

Néhány klasszikus csoportelméleti tétel.

Lagrange tétele.

Véges csoport részcsoportjának rendje (elemeinek száma) osztója a csoport rendjének.

Megjegyzés.

A tétel megfordítása nem igaz, ezért érdekesek a „gyengítések”: milyen osztókhoz vannak annyi elemű részcsoportok?

M.L. Sylow (norvég) tételei, 1872.

- Legyen G n elemű csoport. Ha a p prímnek p^α a legnagyobb olyan hatványa amely osztója n -nek, akkor van G -nek p^α elemű részcsoportja.
- A(z előbbi) G csoportnak pontosan $pr + 1$ számú p^α rendű részcsoportja van.

Az első alkalmazások.

Galois-elméletben.

- Normális testbővítés, polinom Galois-csoportja.
- Föloldható csoport: van olyan normállánca (speciális részcsoportlánca), amelynek faktora Abel-csoportok.
- Tétel.** Ha egy algebrai egyenlet Galois-csoportjának rendje prímszám, akkor ezen egyenlet megoldható gyökvonásokkal.

Kristálytanban.

Szimmetriák.

Geometriában.

Transzformációcsoportok. Folytonos transzformációk csoportja.

Egy hosszú távú kérdés.

Egyszerű csoportok.

Definíció. A G csoport egyszerű, ha egyetlen nemtriviális H részcsoportjára sem teljesül, hogy $gH = Hg$ minden $g \in G$ -re.

Egy látszólag egyszerű kérdés.

Melyek a nemtriviális véges egyszerű csoportok?

Egy egyszerű eset.

Ha a nemtriviális G csoport művelete kommutatív, azaz Abel-csoport, akkor ő pontosan ekkor egyszerű, ha prímszámú (elemei száma valamely p prímszám).

A válasz.

Erre a XX. század végéig kellett várni.

Véges egyszerű csoportok.

Föloldható csoportok.

Definíció. A G csoport *föloldható*, ha van olyan

$$G = N_0 \triangleright N_1 \triangleright \dots \triangleright N_{k-1} \triangleright N_k = \{1\}$$

normállánca, amelyben az összes N_i/N_{i+1} faktorcsoporthoz kommutatív.

Észrevétel

A föloldható csoportok nyilván nem egyszerűk.

Burnside sejtése 1902.

A véges, nemkommutatív egyszerű csoportok rendje páros.

Véges egyszerű csoportok.

Az első eredmény.

- **Burnside két prím tétele.** Ha a G véges csoport rendjének legfölbbebb két prímosztója van, akkor G föloldható csoport.
- **Következmény.** A prímhatványrendű csoportok föloldhatóak.

A Burnside sejtés igazolása.

- **Feit - Thompson tétel.** A véges nemkommutatív egyszerű csoportok rendje páros.
- **Következmény.** Minden páratlan rendű csoport föloldható.

Thompson egy további eredménye, amely Fields-érmet hozott.

Kb. 600 oldalas cikksorozatban meghatározta azon egyszerű csoportokat, melyek minden valódi részcsoportja föloldható.

A véges egyszerű csoportok klasszifikációja.

Az 1980-as években lett teljes, részben számítógépek intenzív használatával.

A klasszifikáció 1.

- A véges nemkommutatív csoportoknak van 17 végtelen sorozata.
- Ilyenek az A_n alternálócsoporthoz, ha $n > 4$, és a $\text{PSL}(n, q)$ ún. projektív speciális lineáris csoportok, ha $q \neq 2, 3$.
- Az utóbbiak a q elemű test fölötti 1 determinánsú $n \times n$ típusú mátrixok csoportjainak centrum szerinti faktorcsoporthoz (q prímhatvány).

A véges egyszerű csoportok klasszifikációja.

A klasszifikáció 2.

- Van 26 ún. *sporadikus csoport*,
 - ezek legkisebbike az M_{11} Mathieu csoport (van e listán további 4 Mathieu csoport), az M_{11} rendje $2^4 \cdot 3^2 \cdot 5 \cdot 11$, míg a
 - legnagyobb, az ún. *Monster*, amelynek rendje
- $$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$
- E szám közelítőleg $8,08 \cdot 10^{53}$.

A véges egyszerű csoportok klasszifikációja.

Mekkora is e szám?

- A látható világegyetem nukleonjainak száma $3 \cdot 10^{77}$, jelenlegi térfogata 10^{85}cm^3 ,
- a Föld tömege $3,5 \cdot 10^{51}$ szerese egy proton tömegének, ami azt jelenti, hogy
- a Monsternek több eleme van, mint ahány atomból a Föld áll.
- Végül, az ősrobbanás óta „mindössze” $4,7 \cdot 10^{17}$ másodperc telt el.

Egy csoport konstrukció.

Szorzat.

Ha G, S csoportok, akkor a $G \times S$ halmaz a műveletet komponensenként végezve csoport, a két csoport **direkt szorzata**.

Megjegyzés.

Számos műveleti tulajdonság öröklődik direkt szorzatra. Speciálisan mindazok, amelyek elsőrendű univerzális ítélettel adhatók meg.

Az első struktúratétel: a véges Abel-csoportok alaptétele.

Minden véges Abel-csoport prímszámú rendű ciklikus csoportok direkt szorzatára bontható. A fölbontásban szereplő csoportok rendje egyértelműen meghatározott.

Általánosítás: végesen generált Abel-csoportok.

Minden végesen generált Abel-csoport egy végtelen ciklikus csoport és prímszámú rendű ciklikus csoportok direkt szorzatára bontható. A fölbontásban szereplő csoportok rendje egyértelműen meghatározott.

Megjegyzések.

- 1 Tetszőleges, pl. nemkommutatív csoportokra hasonló tétel nem érvényes.
- 2 Vegyük észre, hogy e tételek hasonlítanak a számelmélet alaptételére.

Egy további struktúra.

Definíció. Az $(R; +, \cdot)$ rendezett hármas (az R halmaz a rajta értelmezett két művelettel) **gyűrű**, ha

- $(R, +)$ Abel-csoport, $\cdot$ asszociatív,
- minden $a, b, c \in R$ -re
 $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

Egy csoportelméleti fogalom analogonja.

Definíció. Legyen R gyűrű. Az $L \subseteq R$ **balideál**, (**jobb**-, **kétoldali**-), ha

- $L \neq \emptyset$, és tetszőleges $a, b \in L$ -re $a - b \in L$,
- tetszőleges $r \in R$, $a \in L$ -re $ra \in L$ ($ar \in L$, ill. mindkettő benne van).

Gyűrűk.

Megjegyzés.

Az ideál a csoportelméleti normálosztó-fogalom megfelelője.

Szoratra bontás.

Definíció. Legyen R gyűrű, továbbá $L_1, \dots, L_k$ balideálok. R ezen balideálok direkt összegére bomlik,

$$R = L_1 \oplus \dots \oplus L_k,$$

ha R mint Abel-csoport e részcsoporthok (normálosztók) direkt összegére bomlik.

Gyűrűk.

Két fogalom.

- ❶ **Definíció.** Legyen R gyűrű. Azt mondjuk, hogy az $a \in R$ elem **nilpotens**, ha van olyan $n \in \mathbb{N}$, hogy $a^n = 0$. Az $L \triangleleft_b R$ **nilpotens balideál**, ha olyan $n \in \mathbb{N}$, hogy $L^n = \{0\}$.
- ❷ **Definíció.** Azt mondjuk, hogy az R gyűrű **féligegyszerű gyűrű**, ha
 - ❶ nincs végtelen leszálló balideál-lánca (balideáljaira teljesül a **minimumföltétel**),
 - ❷ nem tartalmaz $\{0\}$ -tól különböző nilpotens balideált.

Az első struktúratétel.

Tétel. (Emmy NOETHER) Minden féligegyszerű gyűrű véges sok olyan balideáljának direkt összegére bontható, amelyek idempotens elemmel ($a^2 = a$) generálhatók.

Gyűrűk.

Még két struktúratétel: a Wedderburn - Artin tételek.

- ❶ A féligegyszerű gyűrűk egységelemesek, továbbá véges sok olyan ideáljuk direkt összegére bonthatók, amelyek egyszerű gyűrűk, és balideáljaikra teljesül a minimumföltétel. Ezen fölbontás egyértelmű.
- ❷ Ha az R nem egyelemű egyszerű gyűrű balideáljaira teljesül a minimumföltétel, akkor R prímszámrendű zérógyűrű, vagy valamely F test fölötti $M(F_n)$ teljes mátrixgyűrűvel izomorf. Az állítás megfordítása nem igaz.

Megjegyzés.

Valamely R gyűrű **egyszerű**, ha nincs nemtriviális ideálja (azaz csak $\{0\}$, R ideálok R -ben).

Egyszerű gyűrűk.

A (véges) egyszerű gyűrűknek nincs olyan teljes leírása, mint a csoportoknak.

Egy egyszerű tétel.

- **Definíció.** Az $(F; +, \cdot)$ algebra **ferdetest**, ha
 - ❶ $(F; +, \cdot)$ egységelemes gyűrű,
 - ❷ F minden nemzéró elemének van (multiplikatív) inverze
- A kommutatív ferdetesteket **testnek** nevezzük.
- **Tétel.** Ha az R gyűrűnek csak a két triviális balideálja van, akkor vagy ferdetest, vagy prímszámrendű zérógyűrű, azaz bármely két elemének szorzata 0.
- **Következmény.** Egy kommutatív egységelemes gyűrű pontosan akkor egyszerű, ha test.

A számelmélet alaptétele.

Oszthatóság, maradékos osztás.

- **Definíció.** A kommutatív, zérusosztómentes egységelemes gyűrűket *integritástartományoknak* nevezzük.
- Az oszthatóság fogalma integritástartományokban ugyanúgy definiálható, mint az egész számok gyűrűjében. A tulajdonságok is lényegében ugyanazok.
- **Definíció.** Legyen I integritástartomány. Ha $q \in I$ olyan, hogy $q \neq 0$, $q \nmid 1$ és valahányszor $q = ab$, $a, b \in I$, mindannyiszor $a \mid 1$, vagy $b \mid 1$, akkor azt mondjuk, hogy q irreducibilis elem az I integritástartományban.
- Ha az I integritástartomány valamely nemzéró p elemére $p \nmid 1$ és valahányszor $p \mid ab$, $a, b \in I$, mindannyiszor $p \mid a$ vagy $p \mid b$, akkor p prímelem az I integritástartományban.
- E két fogalom az egész számok gyűrűjében egybeesik, de általában nem, pl. $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ -ben.

A számelmélet alaptétele.

- Emlékezzünk: a számelmélet alaptétele az állítja, hogy minden nemzéró a egész, ha $a \nmid 1$, sorrendtől és előjeltől eltekintve egyértelműen bomlik prímszámok (irreducibilis elemek) szorzatára.
- A bizonyításban a következőket használtuk:
 - ① Ha az a, b nemzéró egészekre $a \mid b$ és $a \neq b$, akkor $|a| < |b|$,
 - ② a prímszámok rendelkeztek az ún. prímtulajdonsággal, azaz a $\mathbb{Z}$ -beli irreducibilis elemek egyben prímelemek is.
- **Definíció.** Azt mondjuk, hogy az I integritástartomány *alaptételes gyűrű*, ha minden olyan a nemzéró eleme, amelyre $a \nmid 1$ sorrendtől és invertálható elem faktoroktól eltekintve egyértelműen bontható irreducibilis elemek szorzatára.

Alaptételes gyűrűk.

Euklideszi gyűrűk.

- **Definíció.** Az E integritástartomány *Euklideszi gyűrű* a ν euklideszi normával, ha $\nu: E \rightarrow \mathbb{N}_0$ olyan függvény, hogy
 - ① $\nu(a) = 0 \Leftrightarrow a = 0$,
 - ② tetszőleges $a, b \in E$ $b \neq 0$ elemekhez léteznek olyan $q, r \in E$ elemek, hogy
 - ① $a = bq + r$,
 - ② $\nu(r) < \nu(b)$.
- **1. Tétel.** Az euklideszi gyűrűk alaptételesek.

Példák euklideszi gyűrűkre.

$\mathbb{Z}$, tetszőleges T testre $T[x]$, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ az ún. Gauss-egészek gyűrűje.

Alaptételes gyűrűk.

Főideálgyűrűk.

Definíció. Egy integritástartomány *főideálgyűrű*, ha minden ideálja egy elemmel generálható.

2. Tétel. A főideálgyűrűk alaptételesek, és minden euklideszi gyűrű főideálgyűrű.

Példa főideálgyűrűre.

$\mathbb{Z}[\sqrt{19}]$ olyan főideálgyűrű, amely nem euklideszi.

Példa alaptételes, de nem főideálgyűrűkre.

$\mathbb{Z}[x]$, $\mathbb{C}[x, y]$.

Alaptételes gyűrűk.

Az alaptételes gyűrűk egy jellemzése.

- **3. Tétel.** *Egy I integritástartomány pontosan akkor alaptételes,*
 - *ha nem létezik főideáljainak végtelen fölszálló lánc,*
 - *továbbá az irreducibilis elemei prímek.*
- **Következmény.** *A $\mathbb{Z}[i\sqrt{5}]$ integritástartomány nem alaptételes.*