

## BSc Matematika Alapszak, 2017.

Matematikai Intézet,  
Természettudományi Kar,  
Eötvös Loránd Tudományegyetem.

# Algebra3

- **Óraszám (ea+gy):** 2 + 2
- **Specializáció:** alk. mat.
- **Kredit (ea+gy):** 3 + 2
- **Számonkérés:** kollokvium + gyak. jegy
- **Tárgykód (ea, gy):** algebr3v0\_m17ea, algebr3v0\_m17ga
- **Ajánlott félév:** 3
- **Státusz:** kötelező
- **Specializáció:** elemző
- **Kredit (ea+gy):** 3 + 2
- **Számonkérés:** kollokvium + gyak. jegy
- **Tárgykód (ea, gy):** algebr3v0\_m17ea, algebr3v0\_m17ga
- **Ajánlott félév:** 3
- **Státusz:** köt. vál.

## Tantárgyfelelős

- Frenkel Péter, Algebra és Számelmélet Tanszék, Matematikai Intézet.

## Előfeltételek

### *A gyakorlat előfeltételei:*

- **Erős:** Algebra2E (algebr2\*0\_m17ea)
- **Erős:** Számelmélet1E (szamel1\*0\_m17ea)

### *Az előadás előfeltételei:*

- **Gyenge:** a gyakorlat

## Megjegyzések

- Ennél a tárgynál a gyakorlaton is legalább 50%-ban az elméleti anyag elmélyítése történik.
- **Pótlási lehetőség:** A félév végén, indokolt esetben, a gyakorlatvezető döntése alapján egy javító zárthelyi dolgozat írására van lehetőség.

### **A tematikát kidolgozta:**

- Frenkel Péter, Algebra és Számelmélet Tanszék, Matematikai Intézet.

## Szükséges előismeretek

Klasszikus és lineáris algebra, elemi számelmélet.

## A tantárgy célkitűzése

A tárgy célja az alkalmazásokhoz szükséges absztrakt algebrai alapfogalmak és szemléletmód bemutatása.

## Irodalom

- **Kiss Emil:** *Bevezetés az algebraiba.* TypoTeX Kiadó, 2007. [Információk, kiegészítések.](#)

# Tematika

- **Csoportok.** Szimmetriák és kompozícióik. Csoport fogalma. Neutrális elem és inverz egyértelmű. Kommutatív csoport fogalma. Additív és multiplikatív írásmód és terminológia. Példák: vektortér additív csoportja, gyűrűk additív és multiplikatív csoportja, általános lineáris csoport, a sík egybevágóságai. Csoportok megadása művelettáblával (Cayley-táblázat). Klein-csoport. Diédercsoport. Szimmetrikus csoport. Permutációk ciklusfölbontása.
- Részcsoport fogalma. Részcsoportok jellemzése műveletekre való zártsággal. Komplexusok, komplexusműveletek. Példák. Alternáló csoport, speciális lineáris csoport. Részcsoportok metszete részcsoport (uniójuk nem feltétlenül az). Generált részcsoport mint a legszűkebb, az adott halmazt tartalmazó részcsoport, vagyis az adott halmazt tartalmazó részcsoportok metszete. Generált részcsoport elemeinek fölrása általános és kommutatív esetben.
- Ciklikus csoportok, osztályozásuk. Csoportelem rendje; a rend a generált részcsoport elemszáma. Képlet hatvány rendjére. Ciklikus csoport részcsoportjai.
- Mellékosztályok. Partíciót alkotnak. A mellékosztályok jellemzése. A bal és a jobb oldali mellékosztályok száma ugyanaz. Részcsoport indexe. Lagrange-tétel: részcsoport, ill. elem rendje osztja a csoport rendjét (ha ez véges). Euler–Fermat-tétel. Prímrendű csoport ciklikus. Csoportnak pontosan akkor van pontosan két részcsoportja, ha prímrendű.
- Diédercsoportban a forgatások 2 indexű részcsoportot alkotnak; a másik mellékosztály elemei a tükrözések. Számolási szabályok.
- Csoporthomomorfizmusok. Példák, alaptulajdonságok. A konjugálás mint automorfizmus. Homomorfizmus magja és képe; a mag zárt a külső elemmel való konjugálásra. Normális részcsoport (normálosztó) mint konjugálásra zárt részcsoport.
- A normálosztók jellemzése: a jobb és a bal oldali mellékosztályok megegyeznek, a részcsoport konjugáltosztályok uniója. Kettő indexű részcsoport mindig normálosztó. Példák. Faktorcsoport. Homomorfizmustétel. Elem rendje a faktorcsoportban. Egyszerű csoportok. Klasszifikációs tétel és Feit–Thompson-tétel (bizonyítás nélkül).
- Kis elemszámú csoportok osztályozása, kvaterniócsoport. Módszerek csoportok izomorfájának vizsgálatára; pl. az elemrendek összehasonlításával. Példa olyan nem izomorf 27 elemű csoportokra, amelyekben minden elem köbe 1.
- Direkt szorzat. Elemrend a direkt szorzatban; ciklikusok direkt szorzata mikor ciklikus. Alkalmazás: szükséges feltétel primitív gyök létezésére modulo  $m$ . A direkt szorzat belső jellemzése; példák. A véges Abel-csoportok alaptétele; adott elemszámúak osztályozása.
- Konjugálás szimmetrikus csoportban. Véges szimmetrikus csoport két elemmel generálható. Permutációcsoportok. Fixpont; stabilizátor, eszerinti mellékosztályok jellemzése. Pálya (orbit); ennek elemszáma a stabilizátor indexe. Csoportthatás; Burnside-lemma: csoportthatás orbitjainak száma egyenlő a csoportelemek fixpontoszámának átlagával. Alkalmazás leszámítási feladatra.
- Tranzitivitás, Cayley tétele.
- **Egységelemes gyűrűk.** Részgyűrű, generált részgyűrű. Nullosztómentes gyűrű. Ferdetest nullosztómentes. Véges nullosztómentes gyűrű ferdetest. Wedderburn tétele (minden véges ferdetest kommutatív, bizonyítás nélkül).
- Nullosztómentes gyűrűben a nem nulla elemek additív rendje vagy végtelen, vagy mindegyiké ugyanaz a prímszám. Karakterisztika, prímtest.
- Homomorfizmus, mag és kép. Ideál, bal- és jobbideál. Balideálmentes gyűrűk.
- Faktorgyűrű, természetes homomorfizmus. Homomorfizmustétel. A komplex számtest mint faktorgyűrű.
- Generált ideál elemeinek felírása kommutatív gyűrűben.
- Főideáltartomány.  $Z$ ,  $K[x]$  az, de  $Z[x]$  nem. Kitüntetett közös osztó mint az elemek által generált ideál generátoreleme.
- $K[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis.  $K[x]/(f)$ -ben  $f$ -nek van gyöke.
- **Testbővítések.** Testbővítés fogalma. Közbülső test, adott elemek generálta közbülső test. Nullkarakterisztikájú test véges bővítése egyszerű (bizonyítás nélkül). Egyszerű testbővítés elemeinek leírása. Algebrai és transzcendens elem.
- Minimálpolinom mint az adott algebrai elemen eltűnő polinomok ideáljának generátoreleme. A

minimálpolinom irreducibilis; a minimálpolinom jellemzései. Algebrai elemmel való egyszerű bővítés elemeinek egyértelmű fölírása a generátorelem alacsonyfokú polinomjaként, műveletek az így felírt elemekkel, a bővítés mint faktorgyűrű. Algebrai elem foka, a testbővítés foka.

- Testbővítések fokának szorzástétele. Véges bővítés algebrai, elem foka osztja a bővítés fokát. Bővítés algebrai elemei közbülső testet alkotnak. Összeg és szorzat fokának becslése. Az algebrai számok teste algebrailag zárt.
- Minden testnek van algebrai lezártja (bizonyítás nélkül).
- Egyszerű algebrai testbővítés konstrukciója. Egyszerű algebrai bővítések izomorfak, ha azonos a generáló elemek minimálpolinomja. Felbontási test fogalma, létezése, egyértelműsége. Normális bővítés; példa bővítésre, amely nem normális. Véges bővítés pontosan akkor normális, ha egy polinom felbontási teste. Másodfokú bővítés normális.
- Véges test elemszáma prímhatvány; az additív és a multiplikatív csoport leírása. Minden prímhatványra egyértelműen létezik ilyen elemszámú test.  $x^q - x$  fölbontható. Véges test véges bővítése egyszerű és normális, a közbülső testek száma és foka.
- Véges test fölött létezik tetszőleges fokú irreducibilis polinom.
- **Alkalmazások.** Kódelmélet. Hibajelzés és javítás, Hamming-távolság. Perfekt kódok. Hamming-korlát, Singleton-korlát. Lineáris kódok, Hamming-kód és dekódolása, polinomkódok, elégséges feltétel a  $t$ -hibajavításra, Reed-Solomon-kód, BCH-kód.
- Kvaterniók. Konjugált, abszolút érték. A kvaterniók ferdetestet alkotnak. Kapcsolat a skaláris és vektoriális szorzással. Térbeli forgatások leírása kvaterniókonjugálással. Algebra fogalma. Frobenius tétele (bizonyítás nélkül); a feltételek egyike sem hagyható el.
- Unitér és ortogonális csoport, Galilei-téridő, Galilei-csoport, Minkowski-téridő, Poincaré- és Lorentz-csoport, kapcsolat a fizikával. Kártyakeverés, Zeeman-felhasadás (bizonyítás nélkül). Kristályok csoportjai.