Mat-tanári szak, második évfolyam, második félév

Részletes vizsgatematika

Az anyag az, ami az előadáson (vagy a gyakorlaton) elhangzott. A csoportelmélet tárgyalásakor az általam írt jegyzet szerint haladtunk. A gyűrű- és testelméleti részhez kiegészítésül az F = Fuchs: *Algebra* egyetemi jegyzetet ajánlom. Az NB jelentése: a bizonyítást nem kell tudni.

Csoportelmélet. A részcsoport fogalma, jellemzései zártsággal és komplexusszorzás segítségével. Véges rendű elem esetén az inverzre való zártságot nem kell ellenőrizni. Partició, ekvivalencia-reláció, kapcsolatuk. A mellékosztály fogalma, mellékosztályokra való felbontás, Lagrange tétele. Az index fogalma, a balindex és a jobbindex ugyanaz. Egy elemmel generált részcsoport. Elem rendje osztója a csoport rendjének, kapcsolat az Euler-Fermat tétellel. Ciklikus csoport. Minden prímrendű csoport ciklikus. Ciklikus csoport részcsoportja is ciklikus. Ciklikus csoport részcsoportjai és adott rendű elemeinek a száma. Részcsoportok metszete részcsoport. A generálás általános fogalma, generált részcsoport, létezésének bizonyítása, elemeinek leírása a kommutatív esetben és általában.

Permutációcsoport, orbit, stabilizátor, összefüggés a csoport rendjével. Gráfok szimmetriacsoportja, a kocka szimmetriáinak a száma.

Csoporthomomorfizmus és izomorfizmus. Minden ciklikus csoport izomorf a $\mathbb{Z}^+$ illetve $\mathbb{Z}_n^+$ csoportok valamelyikével. Ha p prím, akkor p rendű csoport izomorfia erejéig csak egy van. Negyedrendű csoport kettő van. Hatodrendű szintén (NB). Cayley-táblázat, Cayley tétele: minden csoport izomorf egy permutációcsoporttal.

A homomorfizmus egység- és inverztartó. Homomorfizmus képe és magja. Előbbi tetszőleges részcsoport lehet. Utóbbi is részcsoport, ami szerinti bal- és jobboldali mellékosztályok megegyeznek. Ha N ilyen tulajdonságú részcsoport, akkor ő alkalmas homomorfizmus magja. Normálosztó, faktorcsoport, természetes homomorfizmus, homomorfizmus-tétel.

Kettő indexű részcsoport normálosztó. Konjugáltság, konjugált osztályok, normálosztó jellemzése. Centralizátor, a konjugált osztályok elemszáma. Centrum, ennek minden részcsoportja normálosztó. A p-csoport fogalma (p prím), centruma nemtriviális. Prímnégyzet rendű csoport kommutatív.

Egyszerű csoportok. A kommutatív egyszerű csoportok a prímrendű ciklikusak. A véges egyszerű p-csoportok p rendűek. Az A_n alternáló csoport egyszerű, ha $n \geq 5$ (NB). Normállánc, kompozíciólánc, feloldhatóság. A véges Abel-csoportok és p-csoportok feloldhatók. Burnside tétele: ha egy csoport rendjének csak két különböző prímosztója van, akkor a csoport feloldható (NB). Feit-Thompson tétel: minden páratlan rendű csoport feloldható (NB). Az S_n szimmetrikus csoport akkor és csak akkor feloldható, ha $n < 5$.

Vektorterek izomorfiájának jellemzése a dimenzióval. A direkt szorzat fogalma és belső jellemzése csoportok esetén. Elemrend direkt szorzatban, a direkt szorzat mikor ciklikus. Alkalmazás: primitív gyök nemlétezése. A véges Abel-csoportok alaptétele, egyértelműség (NB). Prímnégyzet, és prímköb (NB) rendű csoportok izomorfiatípusainak száma. Csoportok, melyek rendje két prím szorzata (NB). A véges egyszerű csoportok osztályozása, spóradikus csoportok (csak mese, NB).

 Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Testbővítések és alkalmazásaik *(lásd F, VI. Fejezet).* Résztest és testbővítés. Adott elemek által generált résztest fogalma, a $K(\alpha)$ jellemzése az $f(\alpha)/g(\alpha)$ törtek segítségével. Ha $K \leq L$ és $\alpha \in L$, akkor azok a K-beli együtthatós polinomok, amelyeknek az α gyöke, ideált alkotnak $K[x]$-ben, ennek normált generátoreleme az α elem K feletti minimálpolinomja, jele m_α. Algebrai és transzcendens elemek K felett. Ha α algebrai, akkor a minimálpolinomja a legalacsonyabb fokú normált polinom, amelynek α gyöke. A minimálpolinom irreducibilis, ennek oka, hogy L nullosztómentes. Megfordítva, ha az α elem gyöke egy normált, irreducibilis, K-beli együtthatós polinomnak, akkor ez az α elem K feletti minimálpolinomja. A $K(\alpha)$ testbővítés szerkezete algebrai α esetén, egyértelműség.

Ha K részteste L-nek, akkor L vektortér, sőt algebra K felett a megfelelő műveletekre. Ennek dimenziója a testbővítés foka. Ha az L test α eleme algebrai K felett, akkor a $K(\alpha)$ test K feletti foka éppen az α elem K feletti minimálpolinomjának a fokával egyenlő, ezt nevezzük az α elem K feletti fokának. Ez a fok tehát véges, ha viszont α transzcendens K felett, akkor a $K(\alpha)$ foka végtelen lesz K felett.

A testbővítések fokszámainak szorzástétele. Következmény: elem foka osztója a bővítés fokának. Ezért véges fokú bővítésben minden elem foka véges. Véges és algebrai bővítés fogalma, minden véges bővítés algebrai. A $K(\alpha, \beta)$ bővítés K feletti foka legfeljebb akkora, mint az α és a β elemek K feletti fokainak szorzata, ez becsli $\alpha + \beta$ és $\alpha\beta$ fokát is. Következmény: ha L bővítése K-nak, akkor az L-nek a K felett algebrai elemei résztestet alkotnak. Az algebrai és transzcendens szám fogalma, az algebrai számok teste. Az algebrai számok teste algebrailag zárt (NB). Az e transzcendens (Hermite, 1873, NB). A π szám transzcendens (Lindemann, 1882, NB). A Gelfond-Schneider tétel (NB).

A geometriai szerkeszthetőség alapjai. Ha a kiindulási alakzatok (pontok, egyenesek, körök) koordinátái egy K testből valók, akkor a szerkeszthető alakzatok koordinátái benne vannak K egy olyan bővítésében, ami elérhető K-ból négyzetgyökökkel való bővítések sorozatával. Következmény: minden szerkeszthető szám algebrai, és foka K felett kettő-hatvány. Klasszikus nem szerkeszthető problémák: kockakettőzés, körnégyszögesítés, szögharmadolás. Szabályos sokszög szerkeszthetősége, a primitív egységgyökök szerepe.

Ha a felvett koordinátarendszerben $(0, 0)$ és $(1, 0)$ adott vagy szerkeszthető, akkor a kiindulási adatok által generált testet a szerkeszthetőségi feladat alaptestének nevezzük. Valós és komplex *szám* szerkeszthetősége. Összeg, különbség, szorzat, hányados és négyzetgyök szerkeszthető. Komplex számokból álló testek esetében minden másodfokú bővítés egy alkalmas négyzetgyök adjungálásával kapható. Következmény: ha egy szám elérhető az alaptestből kiindulva másodfokú bővítések sorozatával, akkor szerkeszthető (de nem minden kettő-hatvány fokú bővítés szerkeszthető). A szerkeszthetőség szükséges és elégséges feltétele: egy α szám pontosan akkor szerkeszthető, ha a K alaptestet az α minimálpolinomjának *összes* gyökével *egyszerre* bővítve a kapott bővítés foka K felett kettő-hatvány (bizonyítás csak részben). Szabályos sokszög szerkeszthetősége (elégségesség).

A közbülső testek megtalálásának problémája. Egy bővítés szimmetriái (relatív automorfizmusai). A felbontási test és a normális bővítés fogalma, minden felbontási test normális bővítést ad (NB). Közbülső testek, mint szimmetriák közös fixponthalmazai. A Galois-csoport fogalma, a Galois-elmélet főtétele: normális bővítés esetén a Galois-csoport rendje épp a bővítés foka, és kölcsönösen egyértelmű a megfeleltetés a Galois-csoport részcsoportjai és a közbülső testek között (NB).

Kettő-hatvány fokú normális bővítés Galois-csoportja 2-csoport, tehát feloldható. Ezért az ilyen bővítések megkaphatók másodfokú bővítések sorozatával, és így minden kettő-hatvány fokú normális bővítés elemei szerkeszthetők (csak vázlatos bizonyítás).

A gyökképlet fogalma, egyenletek megoldhatósága gyökjelekkel. A gyökjelekkel való megoldhatóság azzal ekvivalens, hogy a polinom felbontási testének Galois-csoportja feloldható (NB). Az általános n-edfokú egyenlet Galois-csoportja S_n, ezért pontosan a legfeljebb negyedfokú egyenletekre van gyökképlet (NB). Példa ötödfokú polinomra, melynek egyik gyöke sem gyökkifejezés (NB).

Gyűrűelmélet. Gyűrűhomomorfizmus, mag, ideál, faktorgyűrű, homomorfizmus-tétel, egyszerű gyűrű (FIII/6–7. §). Minden (ferde)test egyszerű gyűrű (F3.6). Test feletti teljes mátrixgyűrű egyszerű (F3.29, NB). Ha K test és $f \in K[x]$, akkor $K[x]/(f)$ akkor és csak akkor test, ha f irreducibilis K felett. Ha L bővítése K-nak, és az L egy α elemének a minimálpolinomja f, akkor $K[x]/(f)$ izomorf a $K(\alpha)$ testtel. Ennél az izomorfizmusnál az α elemnek az $x+(f)$, a K test egy c elemének a $c+(f)$ felel meg (F6.2). Ha most K és f tetszőleges, akkor a $K[x]/(f)$ testben a $c+(f)$ elemek egy K-val izomorf résztestet alkotnak, ennek elemeit K-val azonosíthatjuk. Ekkor a $\alpha = x + (f)$ elem minimálpolinomja pontosan f lesz. Ezáltal sikerült tetszőleges K testhez, és felette vett irreducibilis polinomhoz megkonstruálni a K egy olyan bővítését, amiben f-nek már van gyöke (F6.10). Speciális eset: a komplex számok konstrukciója. Ennek az eljárásnak az ismétlésével tetszőleges f polinomhoz elkészíthető egy olyan bővítés, amiben f már gyöktényezőkre bomlik, és így f-nek létezik felbontási teste (F6.14). Ez izomorfia erejéig egyértelmű (NB). Végtelen sok lépésben konstruálható olyan bővítés is, ami már algebrailag zárt (NB).

Nullosztómentes gyűrűben minden elem additív rendje ugyanaz, a karakterisztika fogalma, ez nulla, vagy prímszám (F3.16). Tetszőleges testben a legszűkebb résztest, azaz a prímtest vagy $\mathbb{Z}_p$-vel (p prím), vagy $\mathbb{Q}$-val izomorf aszerint, hogy a karakterisztika p vagy 0 (F3.17). Következmény: véges test elemszáma prímhatvány (F6.20). Megfordítva, minden prímhatványhoz izomorfia erejéig pontosan egy ilyen elemszámú test létezik (F6.21, F6.22, csak vázlatosan bizonyítva). Egy q elemű véges testben érvényes az $\alpha^q = \alpha$ azonosság, ami a kis-Fermat tétel általánosítása (és így a test az $x^q - x$ polinom felbontási teste lesz a saját prímteste fölött). Véges test multiplikatív csoportja ciklikus (bizonyítás annak mintájára, hogy létezik primitív gyök modulo tetszőleges prím, NB). Wedderburn tétele: minden véges ferdetest kommutatív (NB).

Hányadostest, konstrukciója (F3.15). Rendezett és elrendezett gyűrűk, $\mathbb{C}$ nem elrendezhető (F5.21). Frobenius tétele, mint a számfogalom lezárása (F4.10, NB). A $\mathbb{Z}_n$ mint $\mathbb{Z}$ faktora, a maradékosztály és a redukált maradékosztály fogalma.

A számelmélet alaptétele főideálgyűrűkben (FIII/10–11. §). Két elem által generált ideál képlete kommutatív egységelemes gyűrűben. Ha $(a, b) = (c)$, akkor c az a és b elemek kitüntetett közös osztója, és felírható $ax + by$ alakban (ez az észrevétel helyettesíti az euklideszi algoritmust). Ezért főideálgyűrűben minden irreducibilis elem prím (bizonyítás mint egészekre). Minden főideálgyűrű alaptételes (NB). A $\mathbb{Z}[x]$ alaptételes, de nem főideálgyűrű, mert $(2, x)$ nem főideál.

Szigorlati mintakérdések

– Oldjuk meg az $5x + 17y = 3$ diofantikus egyenletet $\mathbb{Z}$-ben.
– Hogyan célszerű a primitív gyök fogalmát definiálni nem prím modulus esetén (miért így, miért nem máshogy)? Létezik-e primitív gyök modulo 16?
– Mely számelméleti tételek bizonyításában jött elő a teljes indukció valamilyen formája?
– Milyen megoldási módszereket tanultunk diofantikus egyenletekre?
– Írjuk fel a szumma-jelölés segítségével a szorzatpolinom általános alakját.
– Bontsuk fel az alaptétel szerint a $6x^4 + 36$ polinomot $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ felett.
– Hány bázisa van egy valós feletti 9 dimenziós vektortérnek?
– Ha egy racionális együtthatós lineáris egyenletrendszernek egyértelmű megoldása van $\mathbb{C}$-ben, hány megoldása lehet $\mathbb{Q}$-ban?
– Soroljunk példákat algebrára. Van-e 24 elemű példa $\mathbb{Q}$ illetve $\mathbb{R}$ felett?
– Ha egy síkbeli lineáris transzformációnak egyetlen sajátértéke a nulla, következik-e ebből, hogy a transzformáció nulla?
– A generálás fogalma hol jött elő az anyagban? (altér, részcsoport, ideál, test, stb.)
– Igaz-e, hogy $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{6}, \sqrt{2} + \sqrt{6})$?
– Az elemrend fogalmának milyen speciális esetei szerepeltek az anyagban?
– A $GL(2, \mathbb{C})$ csoportban normálosztót alkotnak-e a valós determinánsú mátrixok?
– Hány olyan ideálja van $\mathbb{R}[x]$-nek, ami $x^2 - 1$-et tartalmazza?
– Soroljuk fel azokat a tanult gyűrűket, melyekben érvényes a számelmélet alaptétele. Melyekben van végtelen sok egység?
– Lehet-e $\sqrt[7]{11} + \sqrt[11]{7}$ foka $\mathbb{Q}$ felett 18?
– Mi a hiba a következő állításban: egy komplex szám pontosan akkor algebrai $\mathbb{Q}$ felett, ha gyöke egy racionális együtthatós polinomnak?
– Szerkeszthető-e szabályos 100-szög? Elvégezhető-e a szög-ötödölés általában?

Kérdések a jobb jegyekre pályázóknak

– Van-e végtelen sok olyan prímszám, ami nem Mersenne- és nem Fermat-prím?
– Ha $a, b, c \in \mathbb{Z}$ és az $ax+by = c$ diofantikus egyenlet megoldható a Gauss-egészek között, megoldható-e $\mathbb{Z}$-ben is?
– Van-e akármilyen fokú irreducibilis polinom $\mathbb{Q}(\sqrt{2})$ felett?
– Van-e olyan valós mátrix, melynek minimálpolinomja x^n? Hányszor hányas lehet ez?
– Hány 8 dimenziós altere van egy 9 dimenziós valós feletti vektortérnek?
– Hogyan volna célszerű a generált normálosztó fogalmát értelmezni? Igaz-e hogy az egy elemmel generált normálosztók kommutatívak?
– Euklidész bizonyításából, hogy van végtelen sok prímszám, nagyságrendileg milyen (jó vagy rossz) becslés jön ki $\pi(x)$-re?
– A minimálpolinom fogalma hogyan terjeszthető ki algebrák elemeire? Létezik-e, illetve irreducibilis-e mindig ez a polinom? Mi lesz az $i + j$ kvaternió minimálpolinomja?
– Mennyire nőhet meg a generált részstruktúra mérete a generátorok számához képest a generálás tanult eseteiben?
– Megoldható-e a kockaötszörözés problémája, ha a körzőn és vonalzón kívül olyan eszközt is használhatunk, mellyel köbgyököt lehet szerkeszteni?