Matematikus szak, második évfolyam, második félév

Részletes vizsgatematika (2005. tavasza)

A vizsganapok és a konzultációk időpontja az ETR-ben olvasható, a szobámban lesznek (déli épület, 3.202/A). Emailben lehet további konzultációkat kérni, vagy kérdéseket föltenni (`ewkiss@cs.elte.hu`). A vizsgák negyed kilenckor kezdődnek, akkorra négy ember jöjjön, azután fél tíztől 25 percenként egyvalaki. Leckekönyv nélkül vizsgázni nem lehet.

Szigorlatra csak az mehet, aki a kollokviumon legalább kettest kapott. Gyakorlatilag mindenki három tételt húz: egy bizonyítást a tematika végén található listából, és két összefoglaló (azaz szigorlati) tételt. A kollokviumhoz a bizonyítást kell tudni, és az összefoglaló tételek erre a félévre eső részét (a bizonyításokkal együtt; a könnyebb bizonyítások vizsga közben kitalálhatók, többek között ez is méri a megfelelő matematikai/algebrai érettséget, ahogy az eddigi kollokviumokon is). A szigorlati részben a bizonyításokat nem kell tudni, de gondolkodtató kérdések (példák, ellenpéldák adása állításokra) itt is szerepelhetnek. Ismerni kell a bizonyítási módszereket, és azt is, hogy milyen tételhez milyen apparátust használunk. A szigorlati jegyet az szabja meg, hogy ki mennyire látja (az egyes állításokon túlmenően) a tananyag *összefüggéseit.* Ezért ezekre a kérdésekre a felkészülési idő alatt bő vázlatot érdemes írni. Szigorlati tematika külön nincs, mert ennek a tematikának a végén egy rövid összefoglaló olvasható a számelmélet részről, az algebrai rész anyaga pedig az eddigi négy félév egyesített tematikája. Az ajánlott irodalom a Freud- és a Hermann-Kiss jegyzeten kívül Fried Ervin: *Algebra II* (zöld egyetemi tankönyv), valamint a homepage-emről letölthető „haladó csoportelmélet" jegyzet 16–32. oldalai. GY: az állítást a gyakorlaton vettük.

Csoportok. Csoport automorfizmusa, belső automorfizmusa. Ciklikus csoport automorfizmus-csoportja. Karakterisztikus részcsoport, kapcsolatok a normálosztókkal (GY). Csoport hatása normálosztón konjugálással, szemidirekt szorzat. Egy csoport hatása a részcsoportjainak halmazán konjugálással. Részcsoport normalizátora, ennek indexe a részcsoport konjugáltjainak a száma. A H normalizátora a legnagyobb részcsoport, amelyben H normálosztó. A Sylow-tételek bizonyítása. A pq rendű csoportok szerkezete, számuk (NB).

Két elem kommutátora. A H és K normálosztók kommutátorrészcsoportja mint a megfelelő kommutátorok által generált részcsoport, ez normálosztó, és része H és K metszetének. Kommutátorrészcsoport, ez a legkisebb olyan normálosztó, amely szerinti faktor Abel. A feloldhatóság jellemzése a kommutátorlánc segítségével. A kommutátorlánc főlánc, sőt elemei karakterisztikus részcsoportok. A feloldható csoportok osztálya zárt a részcsoport, a homomorf kép, a véges direkt szorzat képzésére, és a bővítésre. Véges feloldható csoport minimális normálosztói, minden maximális részcsoportja prímindexű (GY).

Permutációcsoport mint univerzális algebra, ekvivalencia, hatás magja (GY). Minden tranzitív permutációcsoport ekvivalens egy részcsoport szerinti mellékosztályokon való hatással. Többszörös (szigorú) tranzitivitás, regularitás. Abel-féle tranzitív csoport reguláris (GY). Egy tranzitív csoport akkor és csak akkor k-szorosan tranzitív, ha a stabilizátorok $k-1$-szeresen tranzitívak, egy n elemű halmazon ható k-tranzitív csoport rendje osztható $n(n-1)...(n-k+1)$-gyel (GY). Egy csoport automorfizmuscsoportja mikor hat többszörösen tranzitívan az egységtől különböző elemeken (GY). Az affin csoport, ennek tranzitivitása. A projektív egyenes törtlineáris leképezéseinek példája szigorúan 3-tranzitív csoportra. A Frobenius-csoport fogalma, jellemzése (GY), példák, Frobenius tétele (NB). A Mathieu-csoportok fokai és tranzitivitása.

Permutációcsoport kongruenciája. Megfeleltetés tranzitív csoport esetén a kongruenciák és a stabilizátort tartalmazó részcsoportok között. Primitivitás, ennek jellemzése (a stabilizátorok maximális részcsoportok). A kongruenciaosztályok elemszáma egyenlő, prímfokú tranzitív csoport primitív. Minden 2-tranzitív csoport primitív. Primitív csoport nemtriviális normálosztója tranzitív. A_n egyszerű, ha $n \geq 5$. Az A_n automorfizmuscsoportja S_n ha $n \neq 2, 3, 6$ (NB), Schreier-sejtés.

A szabad csoport megadása, a Nielsen-Schreier tétel.

Modulusok. Egzakt, félig egzakt és rövid egzakt sorozat. Modulusok bővítésének fogalma, bővítések ekvivalenciája, a direkt szorzat, mint széteső bővítés. Abel csoportok bővítésének faktorrendszere. A széteső bővítéshez tartozó faktorrendszerek leírása, transzformációrendszer (NB). Ekvivalens bővítések jellemzése, az Ext csoport. Hosszú egzakt sorozat létezése Abel-csoportok esetén (Cartan-Eilenberg, NB). Következmény: $\mathrm{Ext}(\mathbb{Z}_n, A) \cong A/nA$.

A projektív és injektív modulus fogalma, kapcsolatuk a Hom egzaktságával és a megfelelő bővítések szétesésével. A projektívek pontosan a szabadok direkt összeadandói. Minden modulus beágyazható injektívbe (NB). Projektív és injektív modulusok főideálgyűrű fölött, az osztható Abel-csoportok struktúratétele (NB).

Kommutatív gyűrűk. A (kommutatív, egységelemes) Noether-gyűrű fogalma. Hilbert bázis tétele: Noether-gyűrű fölötti polinomgyűrű is Noether-féle. A prímideál és a primér ideál fogalma, ideál radikálja, primér ideál radikálja prímideál. Ideálok felbontása Noether-gyűrűben metszet-irreducibilisek metszetére; itt minden metszet-irreducibilis ideál primér. Következmény: Noether-Lasker tétele. Az egyértelműség kérdése (NB).

Egész elemek egységelemes integritási tartomány fölött. Az egészek jellemzése véges modulusbővítésekkel, az egészek részgyűrűt alkotnak. Minden algebrai elem egy egész és egy alapgyűrűbeli elem hányadosa. Minden alaptételes gyűrű egész-zárt. Ha egy test véges sok elemmel vett gyűrűbővítése is test, akkor a bővítő elemek mindegyike algebrai. Következmény: algebrailag zárt test fölötti polinomgyűrű maximális ideáljainak a leírása. Galois-kapcsolat többváltozós polinomok és gyökeik között, zárt halmazok a polinomgyűrűben, Hilbert nullahelytétele.

Nemkommutatív gyűrűk. A Schur-Lemma. Jacobson sűrűségi tétele. Egységelemes R gyűrű Jacobson-radikálja, mint az egyszerű R-modulusok annullátorainak metszete. A Jacobson-radikál az R maximális balideáljainak metszete, és azon x elemek halmaza, melyekre $1 - rx$ balinvertálható minden r gyűrűelemre. Következmény: a radikál minden nilpotens balideált tartalmaz. Az $1 - xr$ jobbinvertálható is, a radikál független attól, hogy balról vagy jobbról definiáljuk-e (NB).

Artin-gyűrű radikálja nilpotens, és így ez a gyűrű legnagyobb nilpotens (bal)ideálja. Wedderburn-Artin-tétel: Artin-gyűrű radikál szerinti faktora véges sok, ferdetest fölötti teljes mátrixgyűrű direkt szorzata. Modulusok algebrák fölött, a radikál és a Wedderburn-Artin tétel kiterjesztése (kommutatív test fölötti) algebrákra.

Részmodulusok függetlensége. Féligegyszerű modulus (egyszerű modulusok összege), ez néhány összeadandó direkt összege. Féligegyszerű modulus része és faktora is féligegyszerű, és minden részmodulus direkt összeadandó. Ha egy egyszerű gyűrűnek van minimális balideálja, akkor mint önmaga fölötti modulus féligegyszerű, és minden egyszerű modulus ezzel a balideállal izomorf. Következmény: teljes mátrixgyűrű fölött egyetlen egyszerű modulus van. A féligegyszerű Artin-gyűrűk jellemzései modulusokkal: minden modulus projektív (injektív), minden részmodulus direkt összeadandó, illetve minden modulus féligegyszerű (NB). Az irreducibilis modulusok száma. A Jacobson-radikál, mint részmodulus csak akkor direkt összeadandó, ha nulla. Véges dimenziós féligegyszerű algebrák algebrailag zárt test fölött, egyszerű modulusok, a centrum és dimenziója.

Reprezentációelmélet. A csoportreprezentáció fogalma, foka és karaktere. Ekvivalens reprezentációk. A csoportalgebra, kapcsolat a csoportalgebra fölötti modulusok és a reprezentációk között. Invariáns skaláris szorzat, Maschke tétele, $\mathbb{C}$ fölött a csoportalgebra féligegyszerű. A csoportalgebra centruma, osztályfüggvények. Az irreducibilis reprezentációk száma a csoport konjugált elemosztályainak a száma, a fokok négyzetösszege a csoport rendje. Abel-csoport reprezentációi, az elsőfokú reprezentációk száma a kommutátorrészcsoport indexe.

A karaktertábla, elemei algebrai egészek. A reguláris reprezentáció, karaktere, a reguláris reprezentációban minden irreducibilis reprezentáció annyiszor szerepel, amennyi a foka. A karakterek ortonormált bázist alkotnak az osztályfüggvények között. Következmény: ha a karakterek egyenlők, akkor a reprezentációk ekvivalensek.

Karakter magja és centruma. Irreducibilis karakter foka osztója a csoport rendjének. Burnside tétele: véges egyszerű csoportban minden prímhatványrendű konjugált elemosztály egyelemű. Következmény: ha egy csoport rendje legfeljebb két prímmel osztható, akkor a csoport feloldható.

Moduláris hálók. A Malcev-term fogalma, kongruencia-felcserélhető algebra kongruenciahálója moduláris. Az intervallumok izomorfizmus-tétele. Jordan-Dedekind tétel, a magasságfüggvény és a dimenzió-egyenlet. Metszet-irreducibilis elemek, Kuros-Ore tétel.

A szigorlati anyag számelméleti része. Az oszthatóság elemi tulajdonságai, a számelmélet alaptételének bizonyításához kapcsolódó fogalmak (általános gyűrűkben is, például legnagyobb közös osztó, a lineáris diofantoszi egyenlet megoldhatósága főideálgyűrűben).

Számelméleti függvények ($\omega(n)$, $\Omega(n)$, $d(n)$, $\sigma(n)$, $\varphi(n)$), additivitás, multiplikativitás, képletük. Tökéletes számok. Möbius-megfordítás.

Kongruenciák, maradékosztályok, maradékrendszerek, lineáris kongruenciarendszerek megoldhatósága. Magasabb fokú kongruenciák, redukció prímhatvány, illetve prím modulusra. A megoldások száma (kapcsolat a polinomok azonossági tételével), Wilson-tétel.

Elemrend számelméletben, az Euler-Fermat tétel, csoportelméleti vonatkozások. Az RSA titkosírás alapjai. Primitív gyök létezése (véges testekben is). Hatványmaradékok, binom kongruenciák. Kvadratikus maradékok, Euler-Lemma, Legendre-szimbólum, a kvadratikus reciprocitási tétel.

Nevezetes becslések: $\pi(x)$ és $\sum d(n)$ becslése.

A kollokviumon húzható bizonyítások

1. $\mathrm{Ext}(\mathbb{Z}_n, A) \cong A/nA$ (a Cartan-Eilenberg tételt nem kell belátni).
2. Hilbert bázis-tétele.
3. A Noether-Lasker tétel.
4. Az algebrai egészek alaptulajdonságai
5. Végesen generált gyűrűbővítés mikor test, a nullahelytétel.
6. Jacobson sűrűségi tétele.
7. A radikál jellemzései, Artin-gyűrű radikálja nilpotens.
8. Kuros-Ore tétele.
9. A Jordan-Hölder és a Jordan-Dedekind tétel.
10. A Sylow-tételek.
11. Primitív permutációcsoportok, A_n egyszerűsége.
12. Szabad csoport megadása.

---

13. Féligegyszerű modulusok, az irreducibilisek megadása féligegyszerű gyűrű fölött.
14. A csoportalgebra féligegyszerű, az irreducibilis reprezentációk száma.
15. Az első ortogonalitási reláció, az ekvivalens reprezentációk jellemzése karakterekkel.
16. Karakter magja és centruma, $\chi(g)|\mathcal{K}|/\chi(1)$ algebrai egész.
17. A Burnside-tétel.

A vonal alatti tételeket csak a kollokviumi ötösért kell tudni bizonyítani.