Mat-alkmat szak, második évfolyam, első félév

Részletes vizsgatematika (2004 ősz)

A vizsganapok: alkalmazott matematikusoknak kedd (kollokvium+szigorlat), matematikusoknak csütörtök. A csütörtöki vizsgákhoz a konzultáció a keddi vizsganap délutánján 2-kor lesz (ha az aznapi vizsga elhúzódik, akkor kicsit később). A keddi vizsganapokhoz a konzultációk időpontja az ETR „megjegyzés" rovatában olvasható. A vizsgák és a konzultációk is a szobámban lesznek (déli épület, III. emelet 202/A). Emailben lehet további konzultációkat kérni, vagy kérdéseket föltenni (`ewkiss@cs.elte.hu`). A vizsgák negyed kilenckor kezdődnek a szobámban. Akkorra négy ember jöjjön, azután fél tíztől kedden 20 percenként, csütörtökön 15 percenként egyvalaki. Leckekönyv nélkül vizsgázni nem lehet.

Az anyag az, ami az előadáson (illetve részben a gyakorlaton) elhangzott. Irodalom: Freud Róbert: *Lineáris algebra* (a kódelmélethez), Kiss-Hermann: *Bevezetés az absztrakt algebrába* (`http://www.cs.elte.hu/~ewkiss/bboard/algebrabook/index.html`). NB: a bizonyítást nem kell tudni; GY: a bizonyítást a gyakorlaton vettük. A tematika végén a nehezebb bizonyítások listája szerepel, ezek önálló kérdések lehetnek a kollokviumon. A könnyebb bizonyításokat is tudni kell, ezek egy összefoglaló tétel részeként kerülhetnek elő, és helyben kitalálhatók.

Alkalmazott matematikusoknak a szigorlat és a kollokvium független, de szigorlatra csak az mehet, aki a kollokviumon átment. Gyakorlatilag mindenki három tételt húz: egy bizonyítást a listából, és két összefoglaló tételt. A kollokviumhoz a bizonyítást kell tudni, és az összefoglaló tételek erre a félévre eső részét (a bizonyításokkal együtt). A szigorlati részben a bizonyításokat nem kell tudni, de gondolkodtató kérdések (példák, ellenpéldák adása állításokra) itt is szerepelhetnek. 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, de ennek a tematikának a végén egy rövid összefoglaló olvasható a számelmélet részről. Az algebrai rész anyaga az eddigi három félév egyesített tematikája.

Gyűrűk. Véges nullosztómentes gyűrű test. Egyszerű gyűrűk, minden ferdetest feletti teljes mátrixgyűrű egyszerű (bizonyítás gyakorlaton). A jobb és baloldali annullátor fogalma gyűrűben. A balideálmentes gyűrűk szerkezete. Következmény: egységelemes kommutatív gyűrű maximális ideálja szerinti faktor test. Krull tétele: egységelemes gyűrű minden valódi ideálja benne van egy maximális ideálban. Minimálpolinom, algebrai és transzcendens elemek. A minimálpolinom jellemzése az irreducibilitás segítségével.

Prímtest, szerkezete. Rendezett integritási tartomány, pozitivitástartomány és jellemzése, az elrendezhetőség feltétele (NB). A kvaterniótest. Frobenius tétele a valós feletti véges dimenziós, nullosztómentes algebrákról (NB). A Wedderburn-Artin tétel (NB).

Galois-elmélet. A testbővítés fogalma, foka, adott elemekkel generált bővítés. Egyszerű testbővítés, ennek szerkezete a transzcendens és az algebrai esetben. A bővítés foka egyenlő a minimálpolinom fokával. Az egyszerű testbővítés, mint faktorgyűrű. Egyszerű testbővítés konstrukciója. Izomorfizmusok kiterjesztése.

Egymás utáni bővítések fokainak szorzástétele. Következmények: elem foka osztója a

További három oldal!

bővítés fokának, minden véges bővítés algebrai. Összeg és szorzat fokának becslése. Az algebrai elemek résztestet alkotnak, az algebrai számok teste, ez algebrailag zárt. Algebrailag zárt bővítés létezése általános test esetén (NB).

A felbontási test fogalma. Normális bővítés, polinom felbontási teste normális. A felbontási test egyértelmű. A tökéletes test fogalma, minden nulla karakterisztikájú test tökéletes. Tökéletes test véges bővítése egyszerű.

Relatív automorfizmus, a Galois-csoport fogalma. A Galois-elmélet főtétele. Konjugáltság, a konjugáltak a minimálpolinom gyökei. Konjugált résztestek és konjugált részcsoportok kapcsolata, normális közbülső test Galois-csoportja mint faktorcsoport (bizonyítás csak vázlatosan).

A véges testek elemszáma, létezése, egyértelműsége. Minden véges test tökéletes. Véges test multiplikatív csoportja ciklikus. Véges test véges bővítése mindig normális, a Galois-csoport ciklikus, a Galois-csoport generátoreleme, a közbülső testek száma és foka. Wedderburn tétele (minden véges ferdetest kommutatív).

Geometriai szerkeszthetőség. Az alapadatok által generált test. A szerkesztési lépések és a másodfokú bővítések kapcsolata. A szerkeszthető számok jellemzése: minimálpolinomjuk felbontási testének foka az alaptest felett 2-hatvány. Konkrét szerkesztési feladatok megoldhatatlansága: kockakettőzés, szögharmadolás, körnégyszögesítés. A körosztási test foka és Galois-csoportja. Szabályos sokszögek szerkeszthetőségének jellemzése.

Nulla karakterisztikájú test fölötti gyökkifejezés fogalma. Az $x^p - a$ polinom felbontási teste; ha az alaptest tartalmazza a p-edik egységgyököket, akkor ez a bővítés első vagy p-edfokú (p prím). Megfordítás: ha az alaptest tartalmazza a p-edik egységgyököket, akkor minden p fokú bővítés így kapható. A gyökökkel megoldható polinomok jellemzése a Galois-csoport feloldhatóságával. Minden egységgyök gyökkifejezés. Az x^5-4x+2 polinom Galois-csoportja S_5, és így nem oldható meg gyökjelekkel (NB). Az általános n-edfokú egyenlet Galois-csoportja S_n (NB). Következmény: a legalább ötödfokú egyenletre nincs általános megoldóképlet.

Modulusok. A modulus fogalma, unitér modulus, példák. Homomorfizmus, faktormodulus. Részmodulus, a generált részmodulus elemeinek képlete, ciklikus modulus. Direkt szorzat és belső jellemzése. A szabad modulusok leírása.

A rend fogalma általában, és főideálgyűrű fölött. Nulla rendű ciklikus modulus szabad. Nem nulla rendű ciklikus modulus, mint az alapgyűrű faktormodulusa. Főideálgyűrű fölött a nem nulla rendű ciklikus modulusok prímhatványrendű ciklikusok direkt összegei.

A bázis fogalma, a bázis szabad generátorrendszer. Gyenge függetlenség, gyenge bázis, kapcsolata ciklikus részmodulusok direkt összegére való felbonthatósággal. Ha a modulusban megadunk egy bázist, akkor egy részmodulus egy generátorrendszere egy mátrixszal adható meg. A mátrix elemi átalakításainak kapcsolata a bázis illetve a generátorrendszer megváltoztatásával. Euklideszi gyűrű felett minden mátrix elemi átalakításokkal normálalakra hozható. Következmény: euklideszi gyűrű feletti végesen generált modulus ciklikusok direkt összege, és minden részmodulusa is végesen generált. Kapcsolat a fellépő ciklikus modulusok generátorelemeinek rendjei, és a mátrix normálalakjának főátlójában szereplő elemek között. A főátló utolsó eleme a modulus exponense.

A felbontás egyértelműségének kérdése. Torzió-részmodulus, a szerinte vett faktor torziómentes. A nulla rendű elemek által generált ciklikus tényezők száma egyértelmű. Az

$M[p]$ részmodulus, ez vektortér az $R/(p)$ test felett, dimenziója a p-hatványrendű tényezők száma. Az $M[p]$ szerinti faktor felbontásában szereplő tényezők rendjei, az egyértelműség bizonyítása. (Ez a rész csak vázlatosan szerepelt.)

A Jordan-normálalakról szóló tétel bizonyítása modulusok segítségével. A karakterisztikus mátrix szerepe, normálalakjában az utolsó elem a minimálpolinom. Következmény: a Cayley-Hamilton tétel. A blokkok méreteinek leolvasása a normálalakról, determinánsosztók (Gy).

Kommutatív gyűrű feletti modulusok bihomomorfizmusa és tenzorszorzata, ennek univerzális tulajdonsága. Az alapgyűrűvel vett tenzorszorzat maga a modulus. Direkt összeg és tenzorszorzat (NB). Következmény: a tenzorszorzat szerkezete vektorterek esetében. Homomorfizmusok tenzorszorzata, mátrixok Kronecker-szorzata.

Algebrai struktúrák, hálók. A háló definíciója rendezés illetve műveletek segítségével, a dualitási elv. Teljes háló, itt elég az egyik művelet létezését feltenni. Fedés, hálók lerajzolása. Intervallum, leszálló, konvex részhalmaz, ideál, filter, komplementum.

Általános algebrai struktúrák, részstruktúra, részalgebraháló. Típus, homomorfizmus, direkt szorzat. Kongruencia, faktor, kongruenciaháló. Kongruenciák egyesítésének leírása, a kongruenciaháló a partícióháló teljes részhálója. Szubdirekt szorzat, triviális szubdirekt szorzat, szubdirekt irreducibilis algebrák, jellemzésük (NB), Birkhoff tétele a szubdirekt felbontásról (NB). A szabad algebra általános fogalma, Birkhoff tétele a szabad algebra létezéséről (NB).

A disztributív háló fogalma. Kongruenciák készítése, a szubdirekt irreducibilis disztributív hálók jellemzése (NB). Stone reprezentációs tétele. Többségi termmel rendelkező algebrák, speciálisan a hálók kongruenciahálója disztributív. A három elemmel generált szabad disztributív háló szerkezete (NB). A Boole algebra fogalma, azonosságai. Boole-gyűrűk. Szubdirekt irreducibilis Boole-algebrák, Stone reprezentáció (NB). A véges Boole-algebrák szerkezete, a végesen generált szabad Boole-algebrák elemszáma (NB).

A moduláris háló fogalma, példák. Dedekind és Birkhoff tételei a modularitás illetve a disztributivitás tiltott részhálókkal való jellemzéséről (NB). A három elemmel generált szabad moduláris háló rajza (NB). A négy elemmel generált szabad moduláris háló szóproblémája eldönthetetlen (Freese-Herrmann, NB). Az intervallumok izomorfizmus-tétele moduláris hálókban. Jordan-Dedekind tétel, a magasságfüggvény és a dimenzió-egyenlet (NB).

A kategória fogalma, kovariáns és kontravariáns funktorok. A Hom mint bifunktor. A direkt szorzat kategóriaelméleti jellemzése (NB).

A kódelmélet alapjai. Hibajelzés és javítás, Hamming-távolság, perfekt kódok, lineáris kódok, polinomkódok, elégséges feltétel a t-hibajavításra (NB).

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 komolyabb bizonyítások listája

1. Az egyszerű testbővítések szerkezete.
2. Egymás utáni bővítések fokainak szorzástétele, következmények.
3. Az algebrai számok teste algebrailag zárt.
4. Minden felbontási test normális.
5. Tökéletes test véges bővítése egyszerű.
6. A Galois-elmélet főtétele.
7. Egyszerű testbővítések konstrukciója.
8. Véges testek szerkezete, Galois-csoportja.
9. Wedderburn tétele.
10. Prímfokú normális bővítések és p-edik gyökök kapcsolata.
11. A balideálmentes gyűrűk szerkezete, következmények.
12. Krull tétele.
13. A főideálgyűrű fölötti modulusok alaptétele (az egyértelműség csak ötösért).
14. A Jordan normálalak létezése.
15. Háló kongruenciahálója disztributív.
16. A tenzorszorzat létezése.