

ELTE IK, Komputeralgebra Tanszék
Tantárgyi dokumentáció

TÁRGY NEVE: Diszkrét matematika 3 EA			
TÁRGY KÓDJA: IP-08eDM3E			
Összes kredit: 4			
Összes óraszám: 2			
Óra típusa	előadás	gyakorlat	konzultáció
Kredit	2		
Heti óraszám	2		2
Számonkérés módja	K		
Tematika: Testbővítés. Vektortér fogalma, bővítés foka. Fokszámtétel. Algebrai, transzcendens szám, elem, ill. bővítés. Test karakterisztikája. Prímtest, test prímteste, véges test lehetséges karakterisztikája, elemszáma. Bővítés elemének minimálpolinomja. Irreducibilis polinom által generált ideál szerinti faktorgyűrű test. Polinomhoz olyan bővítés készítése, melyben van gyöke. Felbontási test létezése. Prímhatvány elemű véges test konstrukciója. Véges test multiplikatív csoportja ciklikus. Gazdaságos kódolás. Betűnkénti kód, felbontható kód. Blokk- és prefix kód. Kódfa. McMillan-egyenlőtlenség és Kraft tétele. Átlagos szóhossz, optimális kód. Entrópia, Shannon tétele. Huffman-kód, LZW-algoritmus. Hibajaelző és -javító kód. Hamming-távolság és -súly. Minimális távolságú dekódolás. Hibajelző és hibajavító képesség és a kód távolságának kapcsolata. Hamming-korlát Lineáris kódok. Generátor- és ellenőrző mátrix. Singleton-korlát. Hamming-kód, BCH-kód, polinomkódok. Turing-gép definíciója, ábrázolása. Turing-gép változatok: többszalagos, nemdeterminisztikus Turing-gép. Ekvivalens számítási modell: RAM-gép. Church-tézis. Rekurzív és rekurzíve felsorolható nyelv. Algoritmikusan megoldhatatlan problémák. Kis- és nagy ordó. P és NP.			
Irodalom: Járai Antal: Bevezetés a matematikába (második kiadás, 2006)			
Ajánlott irodalom: Gonda János: Bevezető fejezetek a matematikába III. (egyetemi jegyzet)			