

# Szóbeli tételek

## Diszkrét Matematika 2.

(az elhangzott anyag alapján folyamatosan bővül)

A szóbeli vizsga feltétele az írásbeli beugró sikeres teljesítése.

A beugrón 12 kérdésből kell legalább 5-re tudni a választ.

### 1. Gráfok alapfogalmai

Irányítatlan gráf, illeszkedés, párhuzamos élek, hurokélek, szomszédosság, fok, reguláris gráf, véges gráf, izomorfizmus, gráfok Descartes-szorzata, részgráf, feszített részgráf, komplementer, páros gráf, példák (hiperkocka, út, kör, teljes gráf, teljes páros gráf, pl. három ház-három kút). Séta, vonal, út, kör. Távolság, átmérő, összefüggőség. Fák definíciója. Fák jellemzése ekvivalens állításokkal, élszámmal. BIZONYÍTANDÓ TÉTEL: Sétából ugyanolyan végpontokkal rendelkező utat kaphatunk (7.1.20), összefüggőség és komponensek kapcsolatának részletei (7.1.24, a könyvben nem részletezett trivialisításokkal együtt, pl. miért ekvivalenciareláció az „összeköthető úttal” reláció stb.), fák ekvivalens jellemzése (7.1.29 és 7.1.31).

### 2. Fák, Euler-vonal, Hamilton-kör

Feszítőfa, körök száma, elvágó halmaz, vágás, vágások száma. Erdő, feszítőerdő. Euler-vonal, Hamilton-kör és -út. BIZONYÍTANDÓ TÉTEL: körök és vágások száma (7.1.38, 7.1.41.), Euler-vonal létezésének feltétele (7.1.45).

### 3. Címkezett gráfok, irányított gráfok

Címkezett és súlyozott gráfok. Minimális súlyú feszítőfa keresése Kruskal algoritmusával, az algoritmus helyessége. Irányított gráfok. Ki- és befok, összefüggés az élszámmal. Irányított séták, vonalak, utak, körök. Erős összefüggőség, erős komponensek. Irányított és gyökeres fák, szülő, gyerek, szint, mélység, levél fogalma. Síkbarajzolhatóság, jólszínezés, kromatikus szám. Csúcs- és élmátrix. BIZONYÍTANDÓ TÉTEL: Kruskal helyessége, erős komponensekre bontás részletei.

### 4. Ciklikus csoportok, polinomok alapja

Csoport, részcsoporthoz, generátum, ciklikus csoport és generátor fogalma. Ciklikus csoportok művelettartó (homomorf) képe is ciklikus. Izomorfizmus csoportok közt. Ciklikus csoportok jellemzése (vagy az egészekkel, vagy a modulo  $m$  maradékosztályok additív csoportjával izomorfak). Ciklikus csoport részcsoporthoz is ciklikus (8.1.1-8.1.40-ből az idevágó részek). Formális hatványsorok, összeadás, szorzás. Polinomok, összeadás, szorzás. Fok, főegyüttható, konstans tag, monom, lineáris polinom, konstans polinom fogalma. Fokok összeadódása szorzásnál, maximuma összeadásnál. Polinomfüggvények. Maradékos osztás (8.3.1-8.3.8). BIZONYÍTANDÓ TÉTEL: Fokok viselkedése polinomműveleteknél, maradékos osztás.

### 5. Gyűrűtípusok, polinomok

Karakterisztika (8.2.20), Gauss-gyűrű (8.2.67), Euklideszi gyűrű (8.2.69). Gyöktényező leválasztása, gyökök számának felső becslése egységelemes integritási tartományban. Horner-elrendezés (8.3.9-8.3.16). Polinom algebrai deriváltja, többszörös gyökök, kapcsolat a deriválttal (8.3.34), modulo egy polinom történő számolások. BIZONYÍTANDÓ TÉTEL: gyöktényező leválasztása, derivált és többszörös gyök kapcsolata.

## **6. Testbővítések, irreducibilitás interpoláció**

Testbővítés irreducibilis polinommal, véges testek elemszáma, konstrukciója. Irreducibilis polinomok ismert gyűrűk felett. Racionális gyökök keresése, Gauss-lemma, Schönemann-Eisenstein kritérium, Lagrange-interpoláció. Titokmegosztás interpolációval, parciális törtekre bontás, többhatározatlanú polinomok és kapcsolódó fogalmak: multifok, fok, multiindex. BIZONYÍTANDÓ TÉTEL: irreducibilis polinomok jellemzése komplex, valós felett, Lagrange-interpoláció, parciális törtekre bontás.

## **7. Kódolás alapjai, gazdaságos kódolás**

Kódolás: betűnkénti kódolás, felbonthatóság, egyenletes (blokk-), vesszős, prefix kódok. McMillan-egyenlőtlenség. Prefix, szuffix, infix fogalma, kódfa. Huffman-kód és tulajdonságai. Entrópia, Shannon-tétele. BIZONYÍTANDÓ TÉTEL: Prefix kód felbonthatósága, McMillan-egyenlőtlenségből következik, hogy optimális kód prefix kódnak választható.

## **8. Hibakorlátozó kódolás**

Hamming-távolság szavak közt. Kód távolsága. Csoportkód, szavak ill. kód súlya. Hibajelző és hibajavító képesség, kapcsolat a távolsággal. Singleton-korlát, MDS kód. Hamming-korlát. Polinomkódok és lineáris kódok. Generátormátrix, ellenőrző mátrix, szindróma. Távolság és ellenőrző mátrix kapcsolata. Konkrét kódok kódolásának ismertetése: pl. paritásbit (kétdimenziós is) CRC, Hamming, Reed-Solomon. BIZONYÍTANDÓ TÉTEL: Hamming-korlát, Singleton-korlát.

## **9. Algoritmusok**

Számítási modell fogalma. Szimulálás. Ordó. Turing-gép leírása, RAM gép leírása, szimulálásra vonatkozó tételek. Church-Turing tézis. RÉSZLETESEN ELMONDANDÓ: számítási eljárásra formális példa leírása (pl. az előadáson ismertetett vagy a könyvben látható példa az euklideszi algoritmussal).