1. Mit mondhatunk irányítatlan gráfban a fokszámok összegéről?

Állítás

A $G = (\varphi, E, V)$ gráfra
$$\sum_{v \in V} d(v) = 2|E|.$$

Bizonyítás

Élszám szerinti teljes indukció: $|E| = 0$ esetén mindkét oldal 0. Tfh. $|E| = n$ esetén igaz az állítás. Ha adott egy gráf, amelynek $n + 1$ éle van, akkor annak egy élét elhagyva egy n élű gráfot kapunk. Erre teljesül az állítás az indukciós feltevés miatt. Az elhagyott élt újra hozzávéve a gráfhoz az egyenlőség mindkét oldala 2-vel nő.

2. Mikor létezik feszítőfája egy gráfnak?

Állítás

Minden összefüggő véges gráfnak létezik feszítőfája.

Bizonyítás

Amíg van kör a gráfban, hagyjuk el annak egy élét. A kapott gráf összefüggő marad. Véges sok lépésben fát kapunk.

3. Hogyan szól Euler tétele síkbarajzolható gráfokról?

Tétel (Euler-formula)

Egy $G = (\varphi, E, V)$ összefüggő síkgráf tetszőleges síkbeli reprezentációját tekintve, melyre t jelöli a tartományok számát, teljesül a következő összefüggés.
$$|E| + 2 = |V| + t$$

Bizonyítás (vázlat)

Ha a gráfban van kör, annak egy élét törölve az általa elválasztott két tartomány egyesül, így a tartományok és élek száma is (vagyis az egyenlet mindkét oldala) 1-gyel csökken. Az eljárás ismétlésével fát kapunk, aminek 1 tartománya van, így teljesül rá az összefüggés (Miért?).

4. Bizonyítsd be, hogy K_5 nem síkgráf!

Állítás

K_5 nem síkgráf.

Bizonyítás

Indirekt tfh. K_5 síkgráf. $|E| = 10$ és $|V| = 5$, így az élszámra vonatkozó becslés alapján $10 \leq 3 \cdot 5 - 6 = 9$, ami ellentmondás.

5., 6. Mit mondhatunk polinomok összegének/szorzatának fokáról?

Állítás

Legyen $f, g \in R[x]$, $deg(f) = n$, és $deg(g) = k$. Ekkor:

- $deg(f + g) \leq \max(n, k)$;
- $deg(f \cdot g) \leq n + k$.

Bizonyítás

Legyen $h = f + g$. Ekkor $j > \max(n, k)$ esetén $h_j = 0 + 0 = 0$.
Legyen $h = f \cdot g$. Ekkor $j > n + k$ esetén

$$h_j = \sum_{i=0}^{j} f_i g_{j-i} = \sum_{i=0}^{n} f_i g_{j-i} + \sum_{i=n+1}^{j} f_i g_{j-i} = 0.$$

7. Hogy szól a gyöktényező leválasztására vonatkozó tétel?

Következmény (gyöktényező leválasztása)

Ha $0 \neq f \in R[x]$, és $c \in R$ gyöke f-nek, akkor létezik olyan $q \in R[x]$, amire $f(x) = (x - c)q(x)$.

Bizonyítás

Osszuk el maradékosan f-et $(x - c)$-vel (Miért lehet?):

$$f(x) = q(x)(x - c) + r(x).$$

Mivel $deg(r(x)) < deg(x - c) = 1$, ezért r konstans polinom.
Helyettesítsünk be c-t, így azt kapjuk, hogy
$0 = f(c) = q(c)(c - c) + r(c) = r(c)$,
amiből $r = 0$.

8. Hány gyöke lehet egy polinomnak?

Következmény

Az $f \neq 0$ polinomnak legfeljebb $deg(f)$ gyöke van.

Bizonyítás

f foka szerinti TI:
$deg(f) = 0$-ra igaz az állítás (Miért?).
Ha $deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x - c)g(x)$ (Miért?), ahol $deg(g) + 1 = deg(f)$ (Miért?). Ha d gyöke f-nek, akkor $d - c = 0$, amiből $d = c$, vagy d gyöke g-nek (Miért?). Innen következik az állítás.

9. Mit mondhatunk két, $n + 1$ helyen megegyező, legfeljebb n-edfokú polinomról?

Következmény

Ha két, legfeljebb n-ed fokú polinomnak $n + 1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlőek.

Bizonyítás

A két polinom különbsége legfeljebb n-ed fokú, és $n + 1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlőek.

10. Mit mondhatunk végtelen R esetén a polinomfüggvényekről?

Következmény

Ha R végtelen, akkor két különböző $R[x]$-beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

11. Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban?

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $deg(f) = 1$, akkor f-nek van gyöke.

Bizonyítás

Ha $deg(f) = 1$, akkor felírható $f(x) = f_1 x + f_0$ alakban, ahol $f_1 \neq 0$.
Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1 c + f_0 = 0$.
Ekkor $f_1 c = -f_0$ (Miért?), és mivel létezik $f_1^{-1} \in F$, amire $f_1 \cdot f_1^{-1} = 1$ (Miért?), ezért $c = -f_0 \cdot f_1^{-1} \left(= -\frac{f_0}{f_1}\right)$ gyök lesz.

12. Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben felbonthatóság szempontjából?

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $deg(f) = 1$, akkor f felbonthatatlan.

Bizonyítás

Legyen $f = g \cdot h$. Ekkor $deg(g) + deg(h) = deg(f) = 1$ (Miért?) miatt $deg(g) = 0 \wedge deg(h) = 1$ vagy $deg(g) = 1 \wedge deg(h) = 0$. Előbbi esetben g, utóbbiban h egység a korábbi állítás értelmében.

13. Bizonyítsd be, hogy $\sqrt{2} \notin \mathbb{Q}$!

Állítás

$\sqrt{2} \notin \mathbb{Q}$.

Bizonyítás

Tekintsük az $x^2 - 2 \in \mathbb{Z}[x]$ polinomot.
Ennek a $\frac{p}{q}$ alakú gyökeire ($p, q \in \mathbb{Z}$, $(p, q) = 1$) teljesül, hogy $p|2$ és $q|1$, így a lehetséges racionális gyökei ± 1 és ± 2.

14., 15., 16. Bizonyítsd be, hogy a prefix, az egyenletes, és a vesszős kódok is felbonthatóak!

Állítás

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett betűkből összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjéhez tartozó kódszót, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűhöz rendelt kódszó sem lehet.

Állítás

Egyenletes kód prefix (így nyilván felbontható is).

Bizonyítás

Mivel a kódszavak hossza azonos, ezért csak úgy lehet egy kódszó prefixe egy másiknak, ha megegyeznek.

Állítás

Vesszős kód prefix (így nyilván felbontható is).

Bizonyítás

A vessző egyértelműen jelzi egy kódszó végét, hiszen ha folytatva kódszót kapnánk, abban a vessző tiltott módon szerepelne.

17. Fogalmazd meg a Singleton-korlátra vonatkozó állítást!

Tétel (Singleton-korlát)

Ha $K \subset A^n$, $|A| = q$ és $d(K) = d$, akkor $|K| \leq q^{n-d+1}$.

Bizonyítás

Ha minden kódszóból elhagyunk $d - 1$ betűt (ugyanazokból a pozíciókból), akkor az így kapott szavak még mindig különbözőek, és $n - d + 1$ hosszúak. Az ilyen hosszú szavak száma szerepel az egyenlőtlenség jobb oldalán.

18. Milyen összefüggés van lineáris kód súlya és távolsága között?

Állítás

Ha K lineáris kód, akkor $d(K) = w(K)$.

Bizonyítás

$d(u, v) = w(u - v)$, és mivel K linearitása miatt $u, v \in K$ esetén $u - v \in K$, ezért a minimumok is megegyeznek (Miért?).