Diszkrét matematika I. legfontosabb tételek/definíciók (II. javított verzió)

2014/2015. I. félév

1. Előszó

A jegyzet a Diszkrét matematika I. (DE IK PTI, tárgykód: INDK101-K5, Dr. Burai Pál) tantárgy 2014/2015. I. féléves előadásainak jegyzete alapján készült, melyeket **Szabó Marianna** készített, amiért nagy köszönet illeti.

2. Teljes indukció

2.1. Peano-axiómák

I. A nulla természetes szám.

$$0 \in \mathbb{N}$$

II. Minden természetes számnak egyértelműen létezik egy rákövetkezője, és ha két természetes szám rákövetkezője megegyezik, akkor a két természetes szám megegyezik.

$$\forall n \in \mathbb{N}\ \exists n' \in \mathbb{N}$$
$$\forall n, m \in \mathbb{N}\ n' = m' \to n = m$$

A nulla egyetlen természetes számnak sem rákövetkezője.

$$\forall n \in \mathbb{N}\ n' \neq 0$$

III. Ha $\mathbb{N}$ egy nullát is tartalmazó részhalmaza minden elemének a rákövetkezőjét is tartalmazza, akkor ez a halmaz megegyezik $\mathbb{N}$-nel.

$$M \subset \mathbb{N} \text{ és } 0 \in M \text{ és } \forall n \in M \text{ esetén } n' \in M \to M = \mathbb{N}$$

Legyen P egy tulajdonság, tegyük fel, hogy

- a nulla rendelkezik ezzel a tulajdonsággal,
- tetszőleges természetes szám esetén, mely rendelkezik ezzel a tulajdonsággal, a rákövetkezője is rendelkezik vele.

Ekkor minden természetes szám rendelkezik ezzel a tulajdonsággal.

2.2. Teljes indukciós bizonyítás

Olyan állítás bizonyítására használjuk, mely n természetes számtól függ. A bizonyítás lépései:

1. Bizonyítsuk $n = 1$-re, vagy $n = 0$-ra.
2. Feltételezzük, hogy az állítás igaz n-re (*indukciós feltevés*).
3. Ennek felhasználásával bebizonyítjuk, hogy az állítás igaz $n+1$-re $\to$ Ezzel az állítást minden n természetes számra belátjuk.

3. Kombinatorika

3.1. Faktoriális

Tetszőleges $n \in \mathbb{N}$ esetén az $n!$ számot a következő módon definiáljuk:

$$0! = 1 \; n! = n(n-1)!$$

3.2. Permutáció

Egy n elemű halmaz (a halmaz elemei **különbözőek**) önmagára való *bijektív* leképezéseit ismétlés nélküli permutációnak nevezzük. Más szavakkal, az n elem egy lehetséges sorbarendezését adja meg egy ilyen bijekció, melyet az n elem egy ismétlés nélküli permutációjának nevezünk.

Tegyük fel, hogy adott $k_1...k_m \in \mathbb{N}$ úgy, hogy $k_1 + ... + k_m = n$ és most a halmaz m különböző elemet tartalmaz oly módon, hogy az i. elemből k_i szerepel benne. Ezen halmaz *önmagára* vett egy bijektív leképezését $(k_1, ..., k_m)$ osztályú ismétléses permutációnak nevezzük. (*Itt két keletkező függvény között nem mindig tudunk különbséget tenni.*)

3.3. Binomiális együtthatók és tulajdonságaik

Legyen $n, k \in \mathbb{N}$ $k \leq n$, ekkor az $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ módon definiált számokat binomiális együtthatóknak nevezzük.

Tetszőleges $n, k \in \mathbb{N}$ $k \leq n$ esetén

$$\binom{n}{0} = \frac{n!}{n!0!} = 1 = \binom{n}{n}$$

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

A fenti állítások bizonyítását tudni kell, de mivel nem bonyolult, itt elhagyjuk.

3.4. Kombináció

Legyen $n, k \in \mathbb{N}$ $k \leq n$. Az $\{1...k\}$ halmaz $\{1...n\}$ halmazba való *szigorúan monoton* leképezéseit k-ad osztályú kombinációknak, a *monotonokat* pedig k-ad osztályú ismétléses kombinációknak nevezzük.

3.5. Variáció

Egy k elemű halmaz egy n elemű halmazba való leképezését az n elem k-ad osztályú ismétléses variációjának nevezzük. Ha a leképezés *injektív*, akkor az n elem k-ad osztályú ismétlés nélküli variációjáról beszélhetünk (ekkor $k \leq n$).

4. Számelmélet

4.1. Binomiális együtthatók tulajdonságai 2.

Legyen $n \in \mathbb{N}$, ekkor

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Bizonyítás:

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$$

4.2. Binomiális tétel

Legyenek $x, y \in \mathbb{R}$ és $n \in \mathbb{N}$, ekkor

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Kifejtve:

$$(x+y)^n = \binom{n}{0} x^0 y^n + \binom{n}{1} x^1 y^{n-1} + ... + \binom{n}{n} x^n y^0$$

Bizonyítás (teljes indukcióval):

$n = 1$ esetén:

$$(x+y)^1 = x + y$$

$$\sum_{k=0}^{1} \binom{1}{k} x^k y^{1-k} = \binom{1}{0} x^0 y^1 + \binom{1}{1} x^1 y^0 = y + x = x + y$$

Tegyük fel, hogy n-re igaz. Bizonyítsuk $n+1$-re:

$$(x+y)^{n+1} = (x+y)\cdot \underbrace{(x+y)^n}_{\text{indukciós feltétel}} =$$

$$(x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} =$$

$$\sum_{k=0}^{n}\left[\binom{n}{k}x^{k+1}y^{n-k} + \binom{n}{k}x^k y^{n-k+1}\right] =$$

$$\binom{n}{0}x^1y^n + \binom{n}{1}x^2y^{n-1} + ... + \binom{n}{n-1}x^n y^1 + \binom{n}{n}x^{n+1}y^0$$

$$+\binom{n}{0}x^0y^{n+1} + \binom{n}{1}x^1y^n + ... + \binom{n}{n-1}x^{n-1}y^2 + \binom{n}{n}x^n y^1 =$$

$$\binom{n+1}{0}y^{n+1} + \left[\binom{n}{0}+\binom{n}{1}\right]x^1y^n + \left[\binom{n}{1}+\binom{n}{2}\right]x^n y^{n-1} + ...$$

$$+\left[\binom{n}{n-2}+\binom{n}{n-1}\right]x^{n-1}y^n + \left[\binom{n}{n-1}+\binom{n}{n}\right]x^n y^1 + \binom{n+1}{n+1}x^{n+1} =$$

$$\sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}$$ *Ami pontosan az, amit bizonyítani akartunk.*

A bizonyításhoz felhasználtuk, hogy

$$\binom{n+1}{0} = \binom{n+1}{n+1} = 1$$

illetve az összevonásokhoz azt, hogy

$$\left[\binom{n}{0}+\binom{n}{1}\right] = \binom{n+1}{1}$$

és így tovább.

4.3. Polinomiális tétel

Legyenek $x_1 ... x_m \in \mathbb{R}$ és $n \in \mathbb{N}$, ekkor

$$(x_1 + ... + x_m)^n = \sum_{\substack{k_1 ... k_m \in \mathbb{N} \\ k_1 + ... + k_m = n}} \frac{n!}{k_1! \cdot \ldots \cdot k_m!} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m}$$

4.4. Oszthatóság

At mondjuk, hogy az *a egész szám* osztója a b egész számnak, vagy b többszöröse a-nak, ha létezik olyan q egész szám, hogy

$$a \cdot q = b \text{ jele: } a \mid b$$

Ha a nem osztója b-nek, azt így jelöljük: $a \nmid b$

Ha a *pozitív* és $a \nmid b$, akkor maradékos osztásról beszélünk. Ekkor van olyan $0 \leq m < a$ és q egész, hogy

$$a \cdot q + m = b$$

4.5. Prímszám

Egy $p > 1$ számot prímszámnak (röviden prímnek) nevezünk, ha az $1, -1, p, -p$ számokon kívül nincs más osztója.

A nem prím, 1-nél nagyobb egészeket összetett számoknak nevezzük.

4.6. A számelmélet alaptétele

Minden 1-nél nagyobb pozitív egész szám felírható prímszámok szorzataként és ez a felírás (a tényezők sorrendjétől eltekintve) egyértelmű.

4.7. Prímszámtétel

Jelölje $\pi(n)$ az $1, ..., n$ között található prímek számát, ekkor

$$\lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{logn}} = 1$$

Vagyis tetszőleges $\epsilon > 0$ esetén létezik olyan $n_0 \in \mathbb{N}$, hogy ha $n \in \mathbb{N}$ olyan, hogy $n_0 \leq n$, akkor

$$\left| \frac{\pi(n)}{\frac{n}{logn}} - 1 \right| < \epsilon$$

4.8. Legnagyobb közös osztó

Legyenek $d, n, m \in \mathbb{N}$, ha $d \mid n$ és $d \mid m$, akkor d-t n és m közös osztójának nevezzük. Világos, hogy ez a halmaz felülről korlátos a természetes számok halmazában, tehát van legnagyobb eleme, melyet n és m legnagyobb közös osztójának nevezünk. Jele: lnko(n,m)

4.9. Legkisebb közös többszörös

Legyenek $d, n, m \in \mathbb{N}$, ha $n \mid d$ és $m \mid d$, akkor d-t n és m közös többszörösének nevezzük. Világos, hogy ez a halmaz alulról korlátos a természetes számok halmazában, tehát van legkisebb eleme, melyet n és m legkisebb közös többszörösének nevezünk. Jele: lkkt(n,m)

4.10. Relatív prímek

Ha lnko(n, m)= 1, akkor n relatív prím m-hez, vagy n, m relatív prímek.

4.11. Kongruencia

Legyenek $a, b, m \in \mathbb{Z}$. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$.

Jele: $a \equiv b \pmod{m}$

4.12. A kongruencia, mint reláció

Az egész számok halmazában a modulo m vett kongruencia ekvivalencia reláció (reflexív, szimmetrikus, tranzitív).

4.13. Euklideszi algoritmus

Legyen $a, b, \in \mathbb{Z}$. Ekkor létezik olyan $q_1, r_1, r_2 \in \mathbb{Z}$, $|r_1| < |b|$, $|r_2| < |r_1|$, hogy

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$

majd tovább folytatva az eljárást

$$r_{i-1} = r_i q_{i+1} + r_{i+1}$$

Ha az utolsó nem nulla maradékot r_n jelöli, akkor

$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

Az utolsó nem nulla maradék megadja a és b legnagyobb közös osztóját.

4.14. Lineáris diofantoszi egyenlet

Legyenek $a, b, c \in \mathbb{Z}$, ekkor az $ax + by = c$ egyenletet lineáris diofantoszi egyenletnek nevezzük.
Az $(x_0, y_0) \in \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ pár a lineáris diofantoszi egyenlet megoldása, ha $ax_0 + by_0 = c$.

4.15. Lineáris diofantoszi egyenlet megoldásai, azok létezése

A fenti lineáris diofantoszi egyenletnek pontosan akkor van megoldása, ha $\text{lnko}(a, b) \mid c$.
Ha az (x_0, y_0) az egyenlet megoldása, akkor bármely $z \in \mathbb{Z}$ esetén az

$$x_0 + z \cdot \frac{b}{\text{lnko}(a, b)} \quad y_0 - z \cdot \frac{a}{\text{lnko}(a, b)}$$

pár is megoldása az egyenletnek és az összes megoldás előáll ilyen alakban.

4.16. Lineáris kongruencia

Legyenek $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ Ekkor az $ax \equiv b \pmod{n}$ kongruenciát lineáris kongruenciának nevezzük.
Az u egész szám a lineáris kongruencia megoldása, ha $au \equiv b \pmod{n}$.

4.17. Lineáris kongruencia megoldásai, azok létezése

A fenti lineáris kongruenciának pontosan akkor van megoldása, ha $\text{lnko}(a, n) \mid b$.
Ha a fenti kongruenciának van megoldása, akkor a megoldás modulo $\frac{n}{\text{lnko}(a,n)}$ egyértelműen meghatározott és modulo n a megoldások száma $\text{lnko}(a, n)$.

4.18. Redukált maradékosztály, teljes és redukált maradékrendszer

A modulo n vett maradékosztályokat $\overline{0}, ..., \overline{n-1}$-sal jelöljük. Ha $0 < d < n$ relatív prím n-hez, akkor a $\overline{d}$ maradékosztályt redukált maradékosztálynak nevezzük.

Egész számok egy halmazát modulo n teljes maradékrendszernek nevezzük, ha a halmaz minden modulo n maradékosztályból pontosan egy elemet tartalmaz.

Egész számok egy halmazát modulo n redukált maradékrendszernek nevezzük, ha a halmaz minden modulo n redukált maradékosztályból pontosan egy elemet tartalmaz.

4.19. Euler-féle φ-függvény

Tetszőleges $n \in \mathbb{N}$ esetén $\varphi(n)$ jelöli a redukált maradékosztályok számát. Ezt a számelméleti függvényt Euler-féle φ-függvénynek nevezzük.

4.20. Euler-tétel

Ha $\text{lnko}(a, n) = 1$, akkor

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

4.21. Fermat-tétel

Tetszőleges p prímszám és a számra, ha $p \nmid a$, akkor

$$a^{p-1} \equiv 1 \pmod{p}$$

5. Komplex számok

5.1. A komplex számok teste

Tetszőleges $(x, y), (u, v) \in \mathbb{R} \times \mathbb{R}$ esetén legyen

$$(x, y) + (u, v) := (x + u, y + v)$$
$$(x, y) \cdot (u, v) := (xu - yv, xv + yu)$$

Az így bevezetett műveletekkel $\mathbb{R} \times \mathbb{R}$ testet alkot, mely testet a komplex számok testének nevezzük. Jele: $\mathbb{C}$

5.2. Komplex számok algebrai alakja

Minden $z \in \mathbb{C}$ komplex szám előáll a következő alakban:

$$z = x + iy$$

ahol $x, y \in \mathbb{R}$ és x-et a szám valós, y-t a szám képzetes részének nevezzük.

5.3. Komplex számok konjugáltja

Legyen $z \in \mathbb{C}$, $z = x + iy$ komplex szám. Ekkor a $\bar{z} = x - iy$ számot z konjugáltjának nevezzük.
Tetszőleges $z, w \in \mathbb{C}$ esetén

$$\overline{z + w} = \bar{z} + \bar{w}$$
$$\overline{z \cdot w} = \bar{z} \cdot \bar{w}$$
$$z = \bar{z} \text{ pontosan akkor, ha } z \in \mathbb{R}$$
$$z + \bar{z}, z\bar{z} \in \mathbb{R}, \text{ sőt } z\bar{z} \geq 0$$

5.4. Komplex számok abszolút értéke

Legyen $z \in \mathbb{C}$, $z = x + iy$ komplex szám. Ekkor a $|z| = \sqrt{z\bar{z}}$ nemnegatív valós számot z komplex szám abszolút értékének, vagy hosszának nevezzük.

$$\sqrt{z\bar{z}} = (x + iy)(x - iy) = \sqrt{x^2 + y^2}$$

Tetszőleges $z, w \in \mathbb{C}$ esetén

$$|zw| = |z| \cdot |w|$$
$$|\bar{z}| = |z|$$
$$|z + w| \leq |z| + |w|$$

5.5. Komplex számok szöge

Legyen $z \in \mathbb{C}$, $|z| = 1$. Ekkor létezik olyan φ, hogy $z = cos\varphi + i \cdot sin\varphi$ és olyan $k \in \mathbb{Z}$, hogy $0 \leq \varphi + 2k\pi < 2\pi$. Tetszőleges, nem feltétlenül 1 normájú (abszolút értékű), $z \neq 0$ komplex szám esetén a $\frac{z}{|z|}$ 1 abszolút értékű komplex számhoz az előzőek szerint megkonstruálható $\varphi = \varphi + 2k\pi$ valós számot a z komplex szám szögének nevezzük.

Ekkor a z komplex szám trigonometrikus alakja

$$z = |z|(cos\varphi + i \cdot sin\varphi)$$

5.6. Euler-formula

Tetszőleges $\varphi \in \mathbb{R}$ esetén

$$e^{i\varphi} = cos\varphi + i \cdot sin\varphi$$

A $z \in \mathbb{C}$, $z \neq 0$ komplex szám az előbbiből következő

$$z = r \cdot e^{i\varphi}$$

előállítását a z komplex szám exponenciális alakjának nevezzük.

5.7. Moivre-tétel

Legyen $z \in \mathbb{C}$, $z \neq 0$, $z = r(cos\varphi + i \cdot sin\varphi)$ és $n \in \mathbb{Z}$, ekkor

$$z^n = r^n(cos(n\varphi) + i \cdot sin(n\varphi))$$

A $w \in \mathbb{C}$ a $z \in \mathbb{C}$ n. gyöke, ha

$$w^n = z$$

5.8. Komplex számok gyöke

Minden $z = r(cos\varphi + i \cdot sin\varphi) \neq 0$ komplex számnak n db különböző gyöke van és ezek a következő alakban állnak elő

$$\sqrt[n]{r}(cos\frac{\varphi + 2k\pi}{n} + i \cdot sin\frac{\varphi + 2k\pi}{n})$$

ahol $k = 0, ..., n - 1$.

Az 1 komplex szám n. gyökeit n. egységgyököknek hívjuk.

6. Algebrai struktúrák

6.1. Művelet

Legyen G egy nemüres halmaz és $\circ : G \times G \to G$ egy függvény. Ekkor a $\circ$ leképezést G-n értelmezett kétváltozós műveletnek nevezzük.

6.2. Félcsoport

A $(G, \circ)$ párt félcsoportnak nevezzük, ha $\circ$ művelet G-n és $\circ$ *asszociatív*.

6.3. Csoport

A $(G, \circ)$ félcsoportot csoportnak nevezzük, ha G-nek van egységelem és minden elemnek létezik G-ben inverze.
Ha a művelet még kommutatív is, akkor Abel-csoportról beszélünk.

6.4. Gyűrű

A $(G, \circ, *)$ hármast gyűrűnek nevezzük, ha $(G, \circ)$ Abel-csoport, $(G, *)$ félcsoport és $*$ disztributív a $\circ$ műveletre nézve.

6.5. Zérusosztó mentesség

Az R gyűrűt zérusosztó mentesnek mondjuk, ha bármely két nullától különböző elemét összeszorozva nullától különböző elemet kapunk.

6.6. Integritási tartomány

A kommutatív, egységelemes, zérusosztó mentes gyűrűket integritási tartománynak nevezzük.

6.7. Egység, asszociált

Integritási tartományban az egységelem osztóit egységeknek nevezzük. Egy integritási tartomány a és b elemét asszociáltaknak nevezzük, jelölésben $a \sim b$, ha a osztója b-nek és b osztója a-nak.

6.8. Valódi osztó

Egy integritási tartományban az a elem valódi osztója b-nek, ha $a \mid b$ és $a \nsim b$

6.9. Irreducibilitás

Legyen D integritási tartomány, a $q \in D$ elemet irreducibilisnek nevezzük, ha nem nulla, nem egység és a saját asszociáltjain és az egységelemen kívül nincs más osztója.

6.10. Prímelem

Legyen D integritási tartomány, a $q \in D$ elem prímelem, ha nem nulla, nem egység és tetszőleges $a, b \in D$ esetén, ha $q \mid ab$, akkor vagy $q \mid a$ vagy $q \mid b$.

Minden prímelem irreducibilis elem, de nem minden irreducibilis elem prímelem.

6.11. Euklideszi-gyűrű

A D integritási tartományt Euklideszi-gyűrűnek nevezzük, ha adott egy $||\cdot|| : D \to \mathbb{N}$ leképezés, amely rendelkezik a következő tulajdonságokkal:

- $||0|| = 0$ és minden nullától különböző elem esetén $||a|| > 0$,
- ha $a \mid b$ és $b \neq 0$, akkor $||a|| \leq ||b||$,
- tetszőleges $a, b \in D$, $a \neq 0$ elemekhez létezik olyan $r, q \in D$, hogy $a = bq + r$ és $||r|| < ||b||$.

A fenti 3 tulajdonsággal rendelkező leképezést Euklideszi normának nevezzük.

7. Polinomok

7.1. Polinomgyűrű

Legyen R egy tetszőleges gyűrű és jelölje $R[x]$ az R fölötti egyhatározatlanú polinomokat, azaz az

$$a_0 + a_1 x + ... + a_n x^n$$

alakú formális kifejezések halmazát.

Legyen $p, q \in R[x]$

$$p(x) = \sum_{i=0}^{n} a_i x^i$$
$$q(x) = \sum_{j=0}^{m} b_j x^j$$

ekkor

$$p(x) + q(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$$
$$p(x) \cdot q(x) = \sum_{l=0}^{n+m} \left(\sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m \\ i+j=l}} (a_i + b_j) \right) x^l$$

7.2. Polinom foka, főegyütthatója

Legyen $p(x) = a_0 + a_1x + ... + a_nx^n$ $R[x]$ egy eleme úgy, hogy $a_n \neq 0$. Ekkor a $\deg(p) = n$ számot a polinom fokának, a_n-t p fokának nevezzük.

7.3. Polinom zérushelye

A $\xi \in R$ értéket a $p \in R[x]$ polinom zérushelyének nevezzük, ha $p(\xi) = 0$.

7.4. Horner-elrendezés

Legyen $p \in \mathbb{C}[x]$ polinom és $\xi \in \mathbb{C}$, ahol $a_n \dots a_0$ a polinom együtthatói. Ekkor a $p(\xi)$ értéket a következőképpen számolhatjuk ki:

	a_n	a_{n-1}	$\dots$	a_1	a_0
ξ	$b_{n-1} := a_n$	$b_{n-2} = \xi b_{n-1} + a_{n-1}$	$\dots$	$b_0 := \xi b_1 + a_1$	$p(\xi) = \xi b_0 + a_0$

7.5. Bézout-tétele

Legyen R integritási tartomány. Tetszőleges $p \in R[x]$ polinom és $\xi \in R$ esetén ξ pontosan akkor gyöke p-nek, ha $x - \xi$ osztója p-nek.

7.6. Az algebra alaptétele

Minden legalább elsőfokú komplex polinomnak van komplex gyöke.

7.7. Gyöktényezős alak

Tetszőleges $p \in \mathbb{C}[x]$ nemkonstans polinom felírható

$$p(x) = a_n(x - \xi_1)...(x - \xi_n)$$
$$a_n, \xi_1...\xi_n \in \mathbb{C}\ a_n \neq 0$$

alakban, ahol a_n a polinom főegyütthatója, $\xi_1...\xi_n$ pedig a gyökei.
A felírás a tényezők sorrendjétől eltekintve egyértelmű.

7.8. Valós polinom gyöktényezős alakja

Tetszőleges valós p polinom felírható

$$p(x) = a_n(x - \xi_1)...(x - \xi_n)(x^2 - \alpha_1x + \beta_1)...(x^2 - \alpha_sx + \beta_s)$$
$$a_n, \xi_1...\xi_n, \alpha_1...\alpha_s, \beta_1...\beta_s \in \mathbb{R}$$

ahol a_n a polinom főegyütthatója, a $\xi_1...\xi_n$ a polinom gyökei, a másodfokú tagok diszkriminánsa pedig negatív.

7.9. Primitív polinom

Egy egész együtthatós polinomot primitívnek nevezünk, ha az együtthatóinak legnagyobb közös osztója 1.

7.10. Schönemann-Eisenstein tétel

Legyen $p \in \mathbb{Z}[x]$ legalább elsőfokú, primitív polinom. Ha létezik olyan t *prím*, hogy $t \mid a_{n-1} \ldots t \mid a_1$ és $t \nmid a_n$ és $t \nmid a_0^2$, akkor p irreducibilis $\mathbb{Z}$ fölött.
A tételben a_n és a_0 szerepe felcserélhető.

8. Rekurzió

8.1. Elsőrendű differenciaegyenlet

Legyen $f : \mathbb{N} \times \mathbb{R} \to \mathbb{R}$ adott függvény, ekkor a

$$x_m = f(n, x_{n-1})$$

egyenletet elsőrendű differenciaegyenletnek nevezzük. Ha még adott egy ξ_0 valós szám, úgy, hogy $x_0 := \xi_0$, akkor ezt a fenti differenciaegyenletre vonatkozó kezdeti feltételnek nevezzük.

8.2. Konstans együtthatós lineáris differenciaegyenlet

Legyen adott egy a valós szám és egy b_n valós sorozat, ekkor a

$$x_n = ax_{n-1} + b_{n-1}$$

egyenletet konstans együtthatós lineáris differenciaegyenletnek nevezzük.

Az egyenlet megoldása az $x_0 := \xi_0$ kezdeti feltétel esetén

$$x_n = a^n \xi_0 + \sum_{k=0}^{n-1} a^{n-1-k} b_k$$

Bizonyítás(teljes indukcióval):
$n = 1$-re

$$x_1 = ax_0 + b_0 = a\xi_0 + b_0$$

Tegyük fel, hogy n-re igaz. Bizonyítsuk be $(n+1)$-re:

$$x_{n+1} = a \cdot \underbrace{x_n}_{ind.feltevs} + b_n =$$

$$a(a^n\xi_0 + \sum_{k=0}^{n-1} a^{n-1-k}b_k) + b_n =$$

$$a^{n+1}\xi_0 + \sum_{k=0}^{n-1} a^{n-k}b_k + b_n =$$

$$a^{n+1}\xi_0 + \sum_{k=0}^{n} a^{n-1-k}b_k \text{ } \textit{Ami pontosan az, amit bizonyítani akartunk.}$$

8.3. Egyensúlyi állapot, stabilitás

Az $x_n = f(x_{n-1})$ autonóm egyenlet x^* megoldását egyensúlyi állapotnak (vagy stacionárius állapotnak) nevezzük, ha az f függvény fixpontja, azaz $f(x^*) = x^*$. Ekkor a differenciaegyenlet megoldása az $x_n = x^*$ konstans sorozat.

Ha az $x_n = ax_{n-1} + b$ lineáris differenciaegyenletet tekintjük, akkor ennek $a \neq 1$ esetén

$$x^* = \frac{b}{1-a}$$

a stacionárius pontja, azaz

$$x_n = a^n(\xi_0 - x^*) + x^* \text{ ha } \xi_0 \neq x^*$$

Ekkor az egyensúlyi állapottól való eltérés

$$x_n - x^* = a^n(\xi_0 - x^*)$$

Ha $|a| < 1$, akkor $x_n \to x^*$, ha $n \to \infty$ és x_n divergens, ha $|a| > 1$. Az első esetben stabil, a második esetben instabil egyensúlyi állapotról beszélünk.

8.4. Másodrendű homogén lineáris differenciaegyenlet

Legyenek a_n, b_n adott valós sorozatok, ekkor a következő egyenletet másodrendű homogén lineáris differenciaegyenletnek nevezzük.

$$x_{n+2} + a_n x_{n+1} + b_n x_n = 0$$

Az x_n^1, x_n^2 megoldásokat függetleneknek nevezzük, ha a nullsorozat csak triviálisan konstruálható ki belőlük, ellenkező esetben függők.
Az x_n^1, x_n^2 lineárisan független megoldáspárt alaprendszernek nevezzük.

Ha Az x_n^1, x_n^2 alaprendszer, akkor az egyenlet tetszőleges megoldása

$$x_n = c_1 x_n^1 + c_2 x_n^2$$

ahol c_1, c_2 tetszőleges konstansok.

8.5. Másodrendű inhomogén lineáris differenciaegyenlet

Legyenek a_n, b_n, k_n adott valós sorozatok, ekkor a következő egyenletet másodrendű inhomogén lineáris differenciaegyenletnek nevezzük.

$$x_{n+2} + a_n x_{n+1} + b_n x_n = k_n$$

Ha x_n^1, x_n^2 az inhomogén egyenlethez tartozó homogén egyenlet alaprendszere, akkor az inhomogén egyenlet tetszőleges megoldása

$$x_n = c_1 x_n^1 + c_2 x_n^2 + x_p$$

ahol c_1, c_2 tetszőleges konstansok és x_p az inhomogén egyenlet egy tetszőleges partikuláris megoldása.

9. Szita-formulák

9.1. Szita-formula

Legyen X nemüres halnaz, $A_1 ... A_n \subset X$, ekkor

$$|\overline{A_1 \cup ... \cup A_n}| = |X| + \sum_{=1}^{n} (-1)^r \cdot \sum_{1 \leq i_1 < ... < i_r \leq n} |A_1 \cap ... \cap A_n|$$

9.2. Speciális szita-formula

Legyen X egy véges halmaz, $A_1 ... A_n \subset X$. Ha minden $1 \leq r \leq n$ természetes szám esetén tetszőleges r db halmaz metszete azonos számosságú, akkor

$$|\overline{A_1 \cup ... \cup A_n}| = |X| + \sum_{=1}^{n} (-1)^r \binom{n}{r} |A_1 \cap ... \cap A_n|$$

10. Valószínűségszámítás

10.1. Algebra, σ-algebra

Legyen Ω egy nemüres halmaz. Azt mondjuk, hogy $\mathscr{A} \subset \mathscr{P}$ egy algebra Ω-n, ha

- $\Omega \subset \mathscr{A}$,
- $\mathscr{A}$ zárt a komplementerképzésre,
- $\mathscr{A}$ zárt a véges unióképzésre.

Ha a harmadik tulajdonságban a véges helyett a megszámlálható unióképzésre zárt $\mathscr{A}$, akkor azt mondjuk, hogy $\mathscr{A}$ σ-algebra Ω-n.

10.2. Eseménytér

Az előbbi Ω halmaz elemeit elemi eseményeknek, az $\mathscr{A}$ által tartalmazott részhalmazait eseményeknek nevezzük. Az üres halmaz a lehetetlen esemény, Ω a biztos esemény.
Azt mondjuk, hogy az A esemény maga után vonja a B eseményt, ha $A \subset B$. Két esemény összegén az egyesítésüket, szorzatukon pedig a metszetüket értjük.

10.3. Valószínűségi mérték

Legyen $\mathscr{A}$ az Ω halmaz egy részhalmazaiból álló σ-algebra, ekkor a

$$\mathcal{P} : \mathscr{A} \to \mathbb{R}$$

függvényt valószínűségi mértéknek nevezzük, $\mathscr{A}$-n, ha

- nemnegatív
- normált
- σ-additív

10.4. Kolmogorov-féle valószínűségi mező

Legyen $\mathscr{A}$ az Ω részhalmazainak egy σ-algebrája, $\mathcal{P}$ pedig egy valószínűségi mérték $\mathscr{A}$-n. Ekkor a $(\Omega, \mathscr{A}, \mathcal{P})$ hármast Kolmogorov-féle valószínűségi mezőnek nevezzük.

10.5. Diszkrét valószínűségi mező

Ha Ω megszámlálható halmaz és $(\Omega, \mathscr{A}, \mathcal{P})$ valószínűségi mező, akkor $(\Omega, \mathscr{A}, \mathcal{P})$-t diszkrét valószínűségi mezőnek nevezzük.

10.6. Diszkrét eloszlás

Megszámlálhatóan sok $[0,1]$-beli valós számot diszkrét eloszlásnak nevezünk, ha a belőlük alkotott sor konvergens és az összege 1, azaz

$$\mathcal{P}_i \geq 0,\ i = 1, 2... \qquad\qquad \sum_{i=1}^{\infty} \mathcal{P}_i = 1$$

10.7. A valószínűség geometriai kiszámítása

Legyen $\Omega \subset \mathbb{R}^k$ véges térfogatú halmaz, úgy, hogy $\text{vol}(\Omega) > 0$. Ekkor annak a valószínűsége, hogy egy pont az $A \subset \Omega$ halmazba esik

$$\frac{\text{vol}(A)}{\text{vol}(\Omega)}$$

Itt az A halmaz nem tetszőleges részhalmaza Ω-nak.

10.8. Feltételes valószínűség

Legyen A, B esemény, B pozitív valószínűségű. Ekkor az A esemény Bre vonatkozó feltételes valószínűségén a

$$\mathcal{P}(A|B) = \frac{\mathcal{P}(AB)}{\mathcal{P}(B)}$$

valós számot értjük.

10.9. Teljes eseményrendszer

Események egy megszámlálható halmazát teljes eseményrendszernek nevezzük, ha páronként diszjunktak és uniójuk a biztos esemény.

10.10. Teljes valószínűség tétele

Legyen B_i $i = 1, 2...$ pozitív valószínűségű eseményekből álló teljes eseményrendszer. Ekkor tetszőleges A esemény esetén

$$\mathcal{P}(A) = \sum_{i=1}^{\infty} \mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)$$

Bizonyítás:

$$\mathcal{P}(A|B_i) = \frac{\mathcal{P}(AB_i)}{\mathcal{P}(B_i)}$$

Ezt átrendezve:

$$\mathcal{P}(AB_i) = \mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)$$

Majd a valószínűségi mérték σ-additivitása miatt:

$$\mathcal{P}(A) = \mathcal{P}(\sum_{i=1}^{\infty} AB_i) = \sum_{i=1}^{\infty} \mathcal{P}(AB_i) = \sum_{i=1}^{\infty} \mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)$$

10.11. Bayes-formula

A feltételes valószínűségből levezetve:

$$\mathcal{P}(A), \mathcal{P}(B) \neq 0$$

$$\mathcal{P}(A|B) = \frac{(\mathcal{P}(AB))}{\mathcal{P}(B)}$$

$$\mathcal{P}(B|A) = \frac{\mathcal{P}(AB)}{\mathcal{P}(A)}$$

A két egyenletből következik, hogy

$$\mathcal{P}(A|B) \cdot \mathcal{P}(B) = \mathcal{P}(B|A) \cdot \mathcal{P}(A)$$

A Bayes-formula pedig ezt átrendezve

$$\mathcal{P}(B|A) = \frac{\mathcal{P}(A|B) \cdot \mathcal{P}(B)}{\mathcal{P}(A)}$$

10.12. Bayes-tétel

Legyen B_i, $i = 1, 2...$ pozitív valószínűségű eseményekből álló teljes eseményrendszer. Ekkor tetszőleges A pozitív valószínűségű esemény esetén:

$$\mathcal{P}(B_i|A) = \frac{\mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)}{\sum_{j=1}^{\infty} \mathcal{P}(A|B_j) \cdot \mathcal{P}(B_j)}$$

A tétel a Bayes-formula és a teljes valószínűség tétele alapján bebizonyítható:

$$\mathcal{P}(B_i|A) = \frac{\mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)}{\mathcal{P}(A)} = \frac{\mathcal{P}(A|B_i) \cdot \mathcal{P}(B_i)}{\sum_{j=1}^{\infty} \mathcal{P}(A|B_j) \cdot \mathcal{P}(B_j)}$$

Tartalomjegyzék