DISZKRÉT MATEMATIKA II (MBNXK112)

WALDHAUSER TAMÁS

elméleti összefoglaló

1. Számelmélet

1.1. Oszthatóság, prímszámok

1.1. Definíció. Tetszőleges a, b egész számok esetén azt mondjuk, hogy a osztója b-nek (b többszöröse a-nak), ha van olyan c egész szám, amelyre $b = ac$. Jelölés: $a \mid b$. Formálisan:

$$a \mid b \iff \exists c \in \mathbb{Z} \colon b = ac.$$

1.2. Tétel. Tetszőleges a, b, c egész számok esetén teljesülnek az alábbiak:

(1) $a \mid a$;

(2) $(a \mid b$ és $b \mid c) \implies a \mid c$;

(3) $(a \mid b$ és $b \mid a) \iff b = \pm a$;

(4) $(a \mid b$ és $a \mid c) \implies a \mid b \pm c$;

(5) $a \mid b \iff ac \mid bc$, feltéve, hogy $c \neq 0$;

(6) $1 \mid a$ és $a \mid 0$;

(7) $a \mid b \implies |a| \leq |b|$, ha $b \neq 0$.

1.3. Következmény. Az oszthatóság részbenrendezési reláció a nemnegatív egész számok halmazán, vagyis $(\mathbb{N}_0, |)$ részbenrendezett halmaz, amelynek legkisebb eleme 1, legnagyobb eleme 0.

1.4. Definíció. A p természetes szám felbonthatatlan (irreducibilis), ha $p > 1$ és csak úgy bontható két természetes szám szorzatára, hogy az egyik tényező 1:

$$\forall a, b \in \mathbb{N} \colon p = ab \implies a = 1 \text{ vagy } b = 1.$$

1.5. Definíció. A p természetes szám prím(tulajdonságú), ha $p > 1$ és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének:

$$\forall a, b \in \mathbb{N} \colon p \mid ab \implies p \mid a \text{ vagy } p \mid b.$$

1.6. Tétel. A természetes számok körében a felbonthatatlanság és a prímtulajdonság egymással ekvivalens.

1.7. Tétel (a számelmélet alaptétele)**.** Minden (1-nél nagyobb) természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

1.8. Tétel (Euklidész)**.** Végtelen sok prímszám van.

1.9. Tétel (prímszámtétel, Hadamard, 1896 és de la Vallée Poussin, 1896)**.** Az n-edik prímszám nagyságrendileg $n \cdot \log n$, azaz $\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$, ahol p_n az n-edik prímszám. (Megjegyzés: a prímszámtételt nem ilyen formában, hanem az x valós számnál nem nagyobb prímeket megszámoló $\pi(x)$ prímszámláló függvény segítségével szokás kimondani.)

1.10. Sejtés (Ikerprímsejtés)**.** Végtelen sokszor előfordul, hogy két szomszédos prím távolsága 2.

1.11. Tétel (Zhang, 2013)**.** Végtelen sokszor előfordul, hogy két szomszédos prím távolsága legfeljebb 70 000 000.

1.12. Tétel (Polymath8, 2014)**.** Végtelen sokszor előfordul, hogy két szomszédos prím távolsága legfeljebb 246.

1.2. Legnagyobb közös osztó

1.13. Definíció. Azt mondjuk, hogy a d egész szám legnagyobb közös osztója az a és b egész számoknak (jelölés: $d = \mathrm{lnko}(a, b)$ vagy egyszerűen csak $d = (a, b)$), ha

(KO) $d \mid a, b$, és

(LN) $\forall k \in \mathbb{Z} \colon k \mid a, b \implies k \mid d$.

1.14. Definíció. Azt mondjuk, hogy a t egész szám legkisebb közös többszöröse az a és b egész számoknak (jelölés: $t = \operatorname{lkkt}(a, b)$ vagy egyszerűen csak $t = [a, b]$), ha

(KT) $a, b \mid t$, és

(LK) $\forall k \in \mathbb{Z}\colon a, b \mid k \implies t \mid k$.

1.15. Definíció. Ha $\operatorname{lnko}(a, b) = 1$, akkor azt mondjuk, hogy a és b relatív prímek.

1.16. Tétel. Bármely két egész számnak létezik legnagyobb közös osztója és legkisebb közös többszöröse; ezek előjeltől eltekintve egyértelműen meghatározottak, és teljesül a következő összefüggés:

$$\operatorname{lnko}(a, b) \cdot \operatorname{lkkt}(a, b) = ab.$$

1.17. Lemma. Tetszőleges $a, b \in \mathbb{Z}$ esetén a és b közös osztói ugyanazok, mint $a - b$ és b közös osztói. Következésképp

$$\operatorname{lnko}(a, b) = \operatorname{lnko}(a - b, b).$$

1.18. Tétel (a maradékos osztás tétele)**.** Tetszőleges $a, b \in \mathbb{Z}\,(b \neq 0)$ esetén léteznek olyan q és r egész számok, amelyekre $a = q \cdot b + r$ és $0 \leq r < |b|$. Itt q és r egyértelműen meghatározottak; q az osztás hányadosa és r a maradék.

1.19. Tétel. Bármely két nullától különböző egész szám legnagyobb közös osztója kiszámítható az ismételt maradékos osztásokra épülő euklideszi algoritmussal, és a legnagyobb közös osztó előáll a két szám „lineáris kombinációjaként”:

$$\forall a, b \in \mathbb{Z}\ \exists u, v \in \mathbb{Z}\colon\ au + bv = \operatorname{lnko}(a, b).$$

1.20. Következmény. Ha $\operatorname{lnko}(a, b) \neq 0$, akkor $\frac{a}{\operatorname{lnko}(a,b)}$ és $\frac{b}{\operatorname{lnko}(a,b)}$ relatív prímek.

1.21. Következmény (Euklidész lemmája)**.** Ha $\operatorname{lnko}(a, b) \neq 0$, akkor

$$a \mid bc \iff \frac{a}{\operatorname{lnko}(a, b)} \mid c.$$

Speciálisan, ha a és b relatív prímek, akkor $a \mid bc \iff a \mid c$.

1.22. Tétel. Legyen az a és b természetes számok prímhatványtényezős felbontása

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \ \text{ és } \ b = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}.$$

(Azokat a prímeket, amelyek csak egyik szám felbontásában szerepelnek, a másik számban nulla kitevővel tüntetjük fel.) Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \forall i\colon \alpha_i \leq \beta_i$;

(2) $\operatorname{lnko}(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)}$;

(3) $\operatorname{lkkt}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)}$.

1.3. Kétismeretlenes lineáris diofantoszi egyenlet

1.23. Definíció. Kétismeretlenes lineáris diofantoszi egyenleten $ax + by = c$ alakú egyenletet értünk, ahol a, b, c adott egész számok $(a, b \neq 0)$, és az x, y ismeretleneket is az egész számok körében keressük.

1.24. Tétel. Tekintsük az $ax + by = c$ diofantoszi egyenletet, ahol a, b, c egész számok és $a, b \neq 0$.

- Az egyenletnek akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, b) \mid c$.
- Ha (x_0, y_0) egy partikuláris megoldás, akkor az általános megoldás:

$$x_t = x_0 + \frac{b}{\operatorname{lnko}(a, b)}t, \quad y_t = y_0 - \frac{a}{\operatorname{lnko}(a, b)}t \quad (t \in \mathbb{Z}).$$

1.4. Kongruenciareláció

1.25. Definíció. Tetszőleges a, b, m egész számok esetén azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$. Az m számot a kongruencia modulusának nevezzük. Jelölés: $a \equiv b \pmod{m}$.

1.26. Megjegyzés. Világos, hogy $m \mid a - b \iff -m \mid a - b$, ezért a modulo m kongruencia és a modulo $-m$ kongruencia ugyanaz. Tehát mindig feltehetjük, hogy a modulus nem negatív. Sőt, azt is feltehetjük, hogy $m \geq 2$, mert a modulo 0 és a modulo 1 kongruencia meglehetősen érdektelen (miért?).

1.27. Tétel. Ha $m \geq 2$, akkor két egész szám akkor és csak akkor kongruens modulo m, ha ugyanazt a maradékot adják m-mel osztva.

1.28. Tétel. Tetszőleges $a, a_1, a_2, b, b_1, b_2, c, m, m_1, m_2$ egész számok esetén teljesülnek a következők:

(1) $a \equiv a \pmod{m}$;

(2) $(a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$;

(3) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$;

(4) $\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m},\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;

(5) ha $\operatorname{lnko}(m, c) \neq 0$, akkor $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{\operatorname{lnko}(m,c)}}$;

(6) ha c és m relatív prímek, akkor $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{m}$;

(7) $\left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \iff a \equiv b \pmod{\operatorname{lkkt}(m_1, m_2)}$.

1.29. Következmény. A modulo m kongruencia ekvivalenciareláció az egész számok halmazán (és kompatibilis az első három alapművelettel). A megfelelő ekvivalenciaosztályokat modulo m maradékosztályoknak nevezzük.

1.5. Lineáris kongruencia

1.30. Definíció. Lineáris kongruencián $ax \equiv b \pmod{m}$ alakú „egyenletet” értünk, ahol a, b, m $(a \neq 0, m \geq 2)$ adott egész számok, és az x ismeretlent is az egész számok körében keressük.

1.31. Tétel. Tekintsük az $ax \equiv b \pmod{m}$ lineáris kongruenciát.

- A kongruenciának akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, m) \mid b$.
- Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\frac{m}{\operatorname{lnko}(a,m)}$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\frac{m}{\operatorname{lnko}(a, m)}}.$$

1.6. Lineáris kongruenciarendszer

1.32. Definíció. Adott a_i, b_i, n_i $(i = 1, 2, \ldots, k)$ egész számok esetén az alábbi alakú „egyenletrendszereket” lineáris kongruenciarendszereknek nevezzük (az x ismeretlent természetesen az egész számok körében keressük):

$$\left.\begin{array}{rcll} a_1x & \equiv & b_1 & \pmod{n_1} \\ & \vdots & & \\ a_kx & \equiv & b_k & \pmod{n_k} \end{array}\right\}$$

1.33. Megjegyzés. Ha a kongruenciarendszerbeli kongruenciák közül valamelyiknek nincs megoldása, akkor természetesen az egész rendszernek sincs. Ha mindegyik kongruenciának van megoldása, akkor külön-külön megoldva őket, ilyen alakú kongruenciarendszert kapunk (figyelem, az itt szereplő m_i modulusok nem feltétlenül ugyanazok, mint a fenti n_i modulusok!):

$$\left.\begin{array}{rcll} x & \equiv & c_1 & \pmod{m_1} \\ & \vdots & & \\ x & \equiv & c_k & \pmod{m_k} \end{array}\right\} \qquad (*)$$

1.34. Tétel. Tekintsük $(*)$ kongruenciarendszert.

- A kongruenciarendszernek akkor és csak akkor van megoldása, ha minden i, j esetén $\operatorname{lnko}(m_i, m_j) \mid c_i - c_j$.
- Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\operatorname{lkkt}(m_1, \ldots, m_k)$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\operatorname{lkkt}(m_1, \ldots, m_k)}.$$

1.35. Tétel (kínai maradéktétel)**.** Ha a $(*)$ kongruenciarendszerben a modulusok páronként relatív prímek (azaz $i \neq j$ esetén $\operatorname{lnko}(m_i, m_j) = 1$), akkor mindig van megoldás, és a megoldás megkapható a következő módon. Tekintsük azt a kongruenciarendszert, amelyet úgy kapunk $(*)$-ból, hogy az i-edik sorban a jobb oldalra 1-et írunk, a többi sorban pedig 0-t:

$$\left.\begin{array}{rcll} x & \equiv & 0 & \pmod{m_1} \\ & \vdots & & \\ x & \equiv & 1 & \pmod{m_i} \\ & \vdots & & \\ x & \equiv & 0 & \pmod{m_k} \end{array}\right\}$$

Legyen e_i egy tetszőleges megoldása ennek a kongruenciarendszernek $(k = 1, \ldots, k)$. Ekkor az eredeti $(*)$ kongruenciarendszer általános megoldása:

$$x \equiv c_1e_1 + \cdots + c_ke_k \pmod{m_1 \cdots m_k}.$$

1.7. Maradékosztályok

1.36. Definíció. A modulo m kongruencia ekvivalenciareláció az egész számok halmazán. A megfelelő ekvivalencia-osztályokat modulo m maradékosztályoknak nevezzük. Egy a egész szám modulo m maradékosztálya tehát a következő halmaz:

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{a + km : k \in \mathbb{Z}\} = \{\dots, a-2m, a-m, a, a+m, a+2m, \dots\}.$$

A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$.

1.37. Megjegyzés. Az $\overline{a}$ jelölés nem utal a modulusra, de a szövegkörnyezetből mindig világosnak kell lennie, hogy mi a modulus. A definícióból világos, hogy tetszőleges a, b egész számok esetén $\overline{a} = \overline{b} \iff a \equiv b \pmod{m}$.

1.38. Definíció. Ha egy ekvivalenciareláció minden osztályából választunk egy elemet, akkor egy *teljes reprezentánsrendszert kapunk.* A modulo m kongruencia esetén a teljes reprezentánsrendszereket teljes maradékrendszereknek nevezzük. Tehát az $a_1, \dots, a_m$ egész számok akkor alkotnak teljes maradékrendszert modulo m, ha $\{\overline{a_1}, \dots, \overline{a_m}\} = \mathbb{Z}_m$.

1.39. Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást, a kivonást és a szorzást a következőképpen:

$$\overline{a} \oplus \overline{b} := \overline{a+b}, \quad \overline{a} \ominus \overline{b} := \overline{a-b}, \quad \overline{a} \odot \overline{b} := \overline{a \cdot b}.$$

A továbbiakban az egyszerűség kedvéért lehagyjuk a „karikákat” a műveleti jelekről, de fontos, hogy mindig tudjuk, hogy egész számokkal vagy maradékosztályokkal számolunk.

1.40. Tétel. A fenti műveletek jóldefiniáltak, vagyis maradékosztályok összege (különbsége, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik számokat választjuk reprezentánsnak. A $(\mathbb{Z}_m; +, \cdot)$ struktúra egységelemes kommutatív gyűrű, amelyet modulo m maradékosztály-gyűrűnek nevezünk.

1.8. Redukált maradékosztályok, egész kitevős hatványozás

1.41. Definíció. Azt mondjuk, hogy $\overline{a} \in \mathbb{Z}_m$ redukált maradékosztály, ha $\operatorname{lnko}(a, m) = 1$. A modulo m redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli: $\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m : \operatorname{lnko}(a, m) = 1\}$.

1.42. Definíció. Azt mondjuk, hogy az $\overline{a}, \overline{b} \in \mathbb{Z}_m$ maradékosztályok egymás multiplikatív inverzei, ha $\overline{a} \cdot \overline{b} = \overline{1}$. Jelölés: $\overline{b} = \overline{a}^{-1}$ (és persze ekkor $\overline{a} = \overline{b}^{-1}$ is igaz). Hasonlóan, az a, b egész számok egymás multiplikatív inverzei modulo m, ha $a \cdot b \equiv 1 \pmod{m}$. Jelölés: $b \equiv a^{-1} \pmod{m}$. Vigyázat: itt a^{-1} **nem** a reciprokát jelenti (az többnyire nem is egész szám)!

1.43. Tétel. Egy $\overline{a} \in \mathbb{Z}_m$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha $\operatorname{lnko}(a, m) = 1$, azaz $\overline{a} \in \mathbb{Z}_m^*$.

1.44. Definíció. Maradékosztály nemnegatív egész kitevős hatványát természetes módon lehet értelmezni: $\overline{a} \in \mathbb{Z}_m$ és $n \in \mathbb{N}$ esetén legyen $\overline{a}^n = \underbrace{\overline{a} \cdot \ldots \cdot \overline{a}}_{n}$ és $\overline{a}^0 = \overline{1}$. A negatív egész kitevős hatványozást viszont csak redukált maradékosztályok esetén értelmezzük: $\overline{a} \in \mathbb{Z}_m^*$ és $n \in \mathbb{N}$ esetén legyen $a^{-n} = (a^{-1})^n$. (Megjegyzés: $(a^{-1})^n = (a^n)^{-1}$, és a hatványozás többi szokásos azonossága is érvényes redukált maradékosztályokra.)

1.45. Definíció. Egy $\overline{a}$ redukált maradékosztály (multiplikatív) rendjén azt a legkisebb pozitív egész kitevőt értjük, amelyre $\overline{a}$-t emelve $\overline{1}$-t kapunk. (Ha $\operatorname{lnko}(a, m) = 1$ akkor (és csak akkor!) valóban létezik ilyen kitevő.) Az $\overline{a} \in \mathbb{Z}_m^*$ maradékosztály rendjét $o(\overline{a})$ jelöli (olvasd: *ordó*). Formálisan:

$$o(\overline{a}) := \min\{n \in \mathbb{N} : \overline{a}^n = \overline{1}\}.$$

1.46. Tétel. Ha $\overline{a} \in \mathbb{Z}_m^*$ és $o(\overline{a}) = n$, akkor minden $k, \ell \in \mathbb{Z}$ esetén

$$\overline{a}^k = \overline{a}^\ell \iff k \equiv \ell \pmod{n}.$$

Az $\ell = 0$ speciális esetben azt kapjuk, hogy

$$\overline{a}^k = \overline{1} \iff n \mid k.$$

1.9. Az Euler-féle φ függvény és az Euler–Fermat-tétel

1.47. Definíció. Tetszőleges n természetes szám esetén $\varphi(n)$ jelöli azt, hogy 1-től n-ig hány olyan szám van, ami relatív prím n-hez:

$$\varphi(n) = |\{a : 1 \le a \le n \text{ és } \operatorname{lnko}(a, n) = 1\}|.$$

Az így kapott $\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto \varphi(n)$ függvényt Euler-féle φ függvénynek nevezzük.

1.48. Megjegyzés. Nyilván $\varphi(1) = 1$, és $m \ge 2$ esetén $\varphi(m) = |\mathbb{Z}_m^*|$.

1.49. Tétel. Ha p prímszám, akkor $\varphi(p) = p - 1$; általánosabban, prímhatványokra úgy kapjuk meg φ értékét, hogy a prímhatványból levonjuk ugyanannak a prímnek az eggyel kisebb kitevős hatványát: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. Tetszőleges $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ prímhatványtényezős alakban megadott természetes szám esetén pedig φ értéke nem más, mint az egyes prímhatványok φ-értékeinek szorzata:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

1.50. Tétel. A komplex számok körében a primitív n-edik egységgyökök száma $\varphi(n)$.

1.51. Tétel (Euler–Fermat-tétel)**.** Ha az a egész szám relatív prím az m modulushoz, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

1.52. Következmény (kis Fermat-tétel)**.** Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod{p}$. Más (ekvivalens) megfogalmazásban: Ha p prímszám, akkor minden a egész számra $a^p \equiv a \pmod{p}$.

1.53. Következmény. Ha az a egész szám relatív prím az m modulushoz, akkor tetszőleges $k, \ell \in \mathbb{Z}$ kitevők esetén

$$k \equiv \ell \pmod{\varphi(m)} \implies a^k \equiv a^\ell \pmod{m}.$$

1.54. Megjegyzés. A fenti állítás megfordítása nem igaz. Ha ekvivalenciát szeretnénk, akkor a kitevőket nem modulo $\varphi(m)$, hanem modulo $o(\overline{a})$ kell tekinteni (lásd a 1.46. Tételt).

1.55. Következmény. Tetszőleges $\overline{a} \in \mathbb{Z}_m^*$ redukált maradékosztályra $o(\overline{a}) \mid \varphi(m)$.

2. Kombinatorika

2.1. Alapelvek

2.1. Tétel. Tetszőleges A, B véges halmazokra teljesülnek az alábbiak.

(1) Ha létezik $A \to B$ bijekció, akkor (és csak akkor) $|A| = |B|$.

(2) Ha A és B diszjunkt, akkor $|A \cup B| = |A| + |B|$.

(3) $|A \times B| = |A| \cdot |B|$.

2.2. Megjegyzés. A fentiek végtelen halmazokra is igazak, és ott ezek valójában nem tételek, hanem definíciók: (1) a számosság definíciója, (2) és (3) pedig számosságok összegének és szorzatának definíciója. (Véges halmazok esetén is tekinthetjük ezeket definícióknak – ez a számfogalom felépítésétől függ.)

2.3. Megjegyzés. Összeszámlálási feladatoknál a következőképpen használhatjuk a 2.1. Tételt.

(1) Ha a megszámolandó dolgok A halmaza helyett találunk egy B halmazt és egy $A \to B$ bijekciót, akkor elég B elemeit megszámolni. (Ez persze csak akkor célravezető, ha olyan B halmazt találunk, aminek az elemeit könnyebb megszámolni.)

(2) Két egymást kizáró esetet különböztetünk meg, és külön-külön megszámoljuk a lehetőségeket az egyes esetekben, majd az eredményeket összeadjuk. Tehát a kombinatorikai képletekben az összeadás a *kizáró vagy* logikai kapcsolatnak felel meg.

(3) A szorzás az *és* logikai műveltnek felel meg: itt mindkét eset (egymás után vagy egyszerre) bekövetkezik, de fontos, hogy ezek egymástól függetlenek legyenek, ne befolyásolják egymást.

2.2. A hat alapeset

2.4. Definíció. Az n-elemű A halmaz (ismétlés nélküli) permutációján elemeinek egy sorbarendezését értjük. Egy permutáció tehát megadható egy $(a_1, \ldots, a_n)$ sorozattal, ahol minden elem pontosan egyszer fordul elő, azaz $\{a_1, \ldots, a_n\} = A$. Az $A = \{1, \ldots, n\}$ esetben ezt a permutációt megadhatjuk egy $A \to A,\ i \mapsto a_i$ bijekcióval is. (A permutációkról, mint véges halmazokat önmagukra képező bijektív leképezésekről a Diszkrét matematika III tantárgyban lesz bővebben szó.)

2.5. Tétel. Az n-elemű halmaz (ismétlés nélküli) permutációinak száma $n!$.

Egy halmazban minden elem csak egyszer szerepelhet; ha elemek olyan összességéről van szó, amelyben egy elem többször is felléphet, akkor nem halmazról, hanem rendszerről beszélünk (szokás multihalmaznak is nevezni). Például $1, 1, 2, 3, 3, 3, 4$ egy hételemű rendszer, de az $\{1, 1, 2, 3, 3, 3, 4\}$ halmaz csak négyelemű.

2.6. Definíció. Egy ismétlődéseket tartalmazó rendszer elemeinek sorbarendezését ismétléses permutációnak nevezzük.

2.7. Tétel. Ha egy n-elemű rendszerben r-féle különböző elem van, és ezek rendre $k_1, \ldots, k_r$ példányban fordulnak elő (ekkor persze $n = k_1 + \cdots + k_r$), akkor a rendszer (ismétléses) permutációinak száma

$$\frac{n!}{k_1! \cdots k_r!}.$$

2.8. Definíció. Ha egy n-elemű halmazból kiválasztunk k elemet úgy, hogy a sorrendet nem vesszük figyelembe és minden elemet legfeljebb egyszer választhatunk, akkor n elem k-adosztályú ismétlés nélküli kombinációjáról beszélünk. Egy k-adosztályú ismétlés nélküli kombináció tehát nem más, mint egy k-elemű részhalmaz.

2.9. Tétel. Egy n elemű halmaz k-adosztályú ismétlés nélküli kombinációinak száma (vagyis az n-elemű halmaz k-elemű részhalmazainak száma)

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}.$$

2.10. Definíció. A fenti tételben szereplő $\binom{n}{k}$ kifejezést (ahol $0 \le k \le n$) binomiális együtthatónak nevezzük.

2.11. Definíció. Ha egy n-elemű halmazból kiválasztunk k elemet úgy, hogy a sorrendet nem vesszük figyelembe és egy elemet többször is választhatunk, akkor n elem k-adosztályú ismétléses kombinációjáról beszélünk. Egy k-adosztályú ismétléses kombináció tehát nem más, mint a halmaz elemeiből alkotott k-elemű rendszer.

2.12. Tétel. Egy n elemű halmaz k-adosztályú ismétléses kombinációinak száma

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

2.13. Definíció. Ha egy n-elemű halmazból kiválasztunk k elemet úgy, hogy a sorrendet figyelembe vesszük és egy elemet többször is választhatunk, akkor n elem k-adosztályú ismétléses variációjáról beszélünk. Egy k-adosztályú ismétléses variáció tehát nem más, mint a halmaz elemeiből alkotott $(a_1, \dots, a_k)$ elem k-as, vagyis az $A \times \dots \times A = A^k$ Descartes-szorzat egy eleme. Ezt az elem k-ast leírhatjuk egy $\{1, \dots, k\} \to A, i \mapsto a_i$ leképezéssel is.

2.14. Tétel. Egy n elemű halmaz k-adosztályú ismétléses variációinak száma n^k.

2.15. Definíció. Ha egy n-elemű halmazból kiválasztunk k elemet úgy, hogy a sorrendet figyelembe vesszük és egy elemet legfeljebb egyszer választhatunk, akkor n elem k-adosztályú ismétlés nélküli variációjáról beszélünk. Egy k-adosztályú ismétlés nélküli variáció tehát nem más, mint a halmaz elemeiből alkotott $(a_1, \dots, a_k) \in A^k$ elem k-as, amelynek tagjai páronként különbözők. Ezt az elem k-ast leírhatjuk egy $\{1, \dots, k\} \to A, i \mapsto a_i$ *injektív* leképezéssel is.

2.16. Tétel. Egy n elemű halmaz k-adosztályú ismétlés nélküli variációinak száma $n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \binom{n}{k} \cdot k!$.

2.3. Szita-formula

2.17. Tétel (szita-formula)**.** Ha U egy véges halmaz és $R_1, \dots, R_n \subseteq U$, akkor

$$\left|\overline{R_1 \cup \dots \cup R_n}\right| = \sum_{\substack{s=0,\dots,n \\ 1 \le i_1 < \dots < i_s \le n}} (-1)^s \cdot |R_{i_1} \cap \dots \cap R_{i_s}|.$$

2.18. Megjegyzés. Szokás szita-formulának nevezni az alábbi képletet is:

$$|R_1 \cup \dots \cup R_n| = \sum_{\substack{s=1,\dots,n \\ 1 \le i_1 < \dots < i_s \le n}} (-1)^{s-1} \cdot |R_{i_1} \cap \dots \cap R_{i_s}|.$$

2.19. Példa. Az $n = 2$ és $n = 3$ esetben így fest a szita-formula:

- $\left|\overline{R_1 \cup R_2}\right| = |U| - |R_1| - |R_2| + |R_1 \cap R_2|$;
- $\left|\overline{R_1 \cup R_2 \cup R_3}\right| = |U| - |R_1| - |R_2| - |R_3| + |R_1 \cap R_2| + |R_1 \cap R_3| + |R_2 \cap R_3| - |R_1 \cap R_2 \cap R_3|$.

2.20. Tétel. Ha A egy k-elemű halmaz és B egy n-elemű halmaz, akkor

- az $A \to B$ szürjektív leképezések száma
$$\sum_{s=0}^{n} (-1)^s \cdot \binom{n}{s} \cdot (n-s)^k;$$
- az $A \to B$ injektív leképezések száma $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$;
- az összes $A \to B$ leképezések száma pedig n^k.

2.21. Megjegyzés. Ha $n > k$, akkor nem létezik $A \to B$ szürjektív leképezés, $n < k$ esetén pedig injektív leképezés nem létezik. A fenti formulák ekkor is érvényesek, és 0-t adnak eredményül.

2.4. Binomiális és polinomiális tétel, Pascal-háromszög

2.22. Definíció. A binomiális együtthatókat szokás az alábbi módon háromszög alakban elrendezni; ezt nevezzük Pascal-háromszögnek.

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\iddots & & & & \vdots & & & & \ddots
\end{array}$$

2.23. Tétel (binomiális tétel)**.** Tetszőleges a, b komplex számok és n természetes szám esetén

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k b^{n-k}.$$

2.24. Következmény. Tetszőleges n természetes szám esetén az n-elemű halmaznak 2^n részhalmaza van, azaz

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

2.25. Tétel (a Pascal-háromszög néhány tulajdonsága)**.**

(1) Az n-edik sor összege: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

(2) Az n-edik sor alternáló összege: $\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} = 0$.

(3) Szimmetria: $\binom{n}{k} = \binom{n}{n-k}$.

(4) Rekurzió: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

2.26. Tétel (polinomiális tétel)**.** Tetszőleges $a_1, \ldots, a_d$ komplex számok és n természetes szám esetén

$$(a_1 + \cdots + a_d)^n = \sum_{k_1+\cdots+k_d=n} \binom{n}{k_1, \ldots, k_d} \cdot a_1^{k_1} \cdots a_d^{k_d}.$$

Itt az $\binom{n}{k_1, \ldots, k_d}$ együtthatókat polinomiális együtthatóknak nevezzük:

$$\binom{n}{k_1, \ldots, k_d} = \frac{n!}{k_1! \cdots k_d!}.$$

2.27. Megjegyzés. A $d = 3$ esetben kapjuk a trinomiális tételt: tetszőleges a, b, c komplex számok és n természetes szám esetén

$$(a+b+c)^n = \sum_{k+\ell+m=n} \binom{n}{k, \ell, m} \cdot a^k b^\ell c^m = \sum_{k+\ell+m=n} \frac{n!}{k!\,\ell!\,m!} \cdot a^k b^\ell c^m.$$

3. Gráfelmélet

3.1. Alapfogalmak

3.1. Definíció. Legyenek V és E tetszőleges halmazok és legyen $\iota\colon E \to V \cup \binom{V}{2}$ egy leképezés, ahol $\binom{V}{2}$ a V halmaz kételemű részhalmazainak halmazát jelöli. Ekkor a $G = (V, E, \iota)$ hármast gráfnak nevezzük; a $V = V(G)$ halmaz elemei a gráf csúcsai, az $E = E(G)$ halmaz elemei a gráf élei. Ha az $e \in E$ élre $e\iota = \{u, v\} \in \binom{V}{2}$, akkor u és v az e él végpontjai (másképp fogalmazva, az e él összeköti az u és v csúcsokat, vagy az e él illeszkedik az u és v csúcsokra). Ha $e\iota = v \in V$, akkor az e él a v csúcsot saját magával köti össze; az ilyen élt hurokélnek nevezzük.

3.2. Definíció. Ha a G gráfban nincsenek se hurokélek se többszörös élek (azaz két pontot legfeljebb egy él köt össze), akkor minden élt megadhatunk a két végpontjával, és ekkor nincs szükség az ι leképezésre. Az ilyen egyszerű gráfot tehát egyszerűen(!) egy $G = (V, E)$ párral lehet megadni, ahol $E \subseteq \binom{V}{2}$.

3.3. Definíció. Azt mondjuk, hogy a G és H egyszerű gráfok izomorfak, ha létezik olyan $f\colon V(G) \to V(H)$ bijekció, amelyre $\{u, v\} \in E(G) \iff \{f(u), f(v)\} \in E(H)$ teljesül tetszőleges $u, v \in V(G)$ csúcsok esetén. (Az f leképezést izomorfizmusnak nevezzük.)

3.4. Definíció. Irányított gráfon egy $G = (V, \rho)$ párt értünk, ahol V tetszőleges halmaz, és $\rho \subseteq V \times V$ egy reláció a V halmazon. Itt V a csúcsok halmaza, ρ pedig az irányított élek halmaza. Ha $e = (u, v) \in \rho$, akkor az u csúcs az e él kezdőpontja, v pedig az e él végpontja (másképp fogalmazva, az e él u-ból v-be vezet; ezt u-ból v-be mutató nyíllal szoktuk ábrázolni). Az $e = (v, v)$ esetben itt is hurokélről beszélünk. (Lehet definiálni többszörös éleket is megengedő irányított gráfokat is, de ettől eltekintünk.)

A továbbiakban gráfon mindig véges irányítatlan gráfot értünk.

3.5. Definíció. A G gráf v csúcsának fokszámán a v-re illeszkedő élek számát értjük (az esetleges hurokéleket kétszer számolva, hiszen az „kétszer illeszkedik” a csúcsra). Jelölés $d(v)$. Ha $d(v) = 0$, akkor v-t izolált csúcsnak nevezzük.

3.6. Tétel. Bármely gráfban a csúcsok fokszámainak összege páros szám, mégpedig az élek számának kétszerese:

$$\sum_{v \in V(G)} d(v) = 2 \cdot |E(G)|.$$

3.7. Definíció. A G gráfban a v csúcsból a w csúcsba vezető sétának nevezzük csúcsoknak és éleknek egy olyan $v = v_0, e_1, v_1, e_2, \ldots, v_{\ell-1}, e_\ell, v_\ell = w$ sorozatát, ahol az e_i él két végpontja v_{i-1} és v_i minden $i \in \{1, \ldots, \ell\}$ esetén. Ha $v_0 = v_\ell$, azaz a séta kezdőpontja és végpontja egybeesik, akkor zárt sétáról beszélünk. (Ha G egyszerű gráf, akkor az éleket nem kell feltüntetni, tehát a sétát megadhatjuk a $v_0, v_1, \ldots, v_\ell$ csúcssorozattal, ahol $\{v_{i-1}, v_i\} \in E(G)$ minden $i \in \{1, \ldots, \ell\}$ esetén.)

3.8. Definíció. Ha egy sétában csupa különböző csúcsok szerepelnek (és így persze élek sem ismétlődhetnek), akkor útnak nevezzük. (Következésképp egy zárt séta sosem lehet út.)

3.9. Definíció. Körnek nevezzük az olyan zárt sétát, amelyben nem ismétlődnek sem csúcsok sem élek (a kezdőpont és a végpont egybeesésétől eltekintve).

3.10. Definíció. Azt mondjuk, hogy a H gráf részgráfja G-nek, ha $V(H) \subseteq V(G)$ és $E(H) \subseteq E(G)$. A részgráfok tehát olyan gráfok, amelyek az eredeti gráfból csúcsok és élek elhagyásával keletkeznek (minden csúcs elhagyásakor természetesen a rá illeszkedő éleket is el kell hagynunk). Ha a H részgráf tartalmazza az összes olyan G-beli élt, amely $V(H)$-beli csúcsokat köt össze, akkor azt mondjuk, hogy H a $V(H)$ csúcshalmaz által feszített részgráfja G-nek. A feszített részgráfok tehát olyan gráfok, amelyek az eredeti gráfból csúcsok elhagyásával keletkeznek.

3.11. Definíció. Egy gráf összefüggő, ha bármely két csúcsa között vezet séta. (Ezzel ekvivalens, hogy bármely két csúcs között van út.)

3.12. Tétel. Definiáljuk a G gráf csúcshalmazán a $\sim$ elérhetőségi relációt a következőképpen: $v \sim w$ akkor és csak akkor, ha létezik G-ben v-ből w-be vezető séta. Ekkor $\sim$ ekvivalenciareláció a $V(G)$ halmazon. Minden $\sim$ szerinti ekvivalenciaosztály kifeszít egy részgráfot; ezeket nevezzük a G gráf összefüggő komponenseinek. Az összefüggő komponensek tehát páronként diszjunkt maximális összefüggő feszített részgráfok.

3.2. Euler-vonal, Hamilton-út

3.13. Definíció. Az olyan sétát, amely egy gráf minden élén pontosan egyszer halad át, Euler-vonalnak nevezzük. Ha ez a séta zárt, akkor zárt Euler-vonalról, ellenkező esetben nyílt Euler-vonalról beszélünk.

3.14. Tétel (Euler, 1736 és Hierholzer, 1871)**.** Egy izolált csúcsokat nem tartalmazó gráfban akkor és csak akkor van Euler-vonal, ha a gráf összefüggő, és legfeljebb két páratlan fokú csúcsa van. Tehát tetszőleges G *összefüggő* gráf esetén az alábbi három eset lehetséges:

- Minden csúcs foka páros. Ekkor van zárt Euler-vonal (és nyílt Euler-vonal nincs).
- Pontosan két páratlan fokú csúcs van. Ekkor van nyílt Euler-vonal (és zárt Euler-vonal nincs). Minden nyílt Euler-vonal szükségképpen a két páratlan fokú csúcsot köti össze.
- Több, mint két páratlan fokú csúcs van. Ekkor nincs Euler-vonal (se zárt, se nyílt).

3.15. Definíció. Az olyan utat, ami egy gráf minden csúcsán áthalad (és, út lévén, minden csúcson *csak egyszer* halad át), Hamilton-útnak nevezzük. Az olyan kört, ami egy gráf minden csúcsán áthalad (és, kör lévén, minden csúcson *csak egyszer* halad át, a kezdőpont és a végpont egybeesésétől eltekintve), Hamilton-körnek nevezzük.

3.16. Tétel. Ha egy gráfban van Hamilton-kör, akkor egy csúcsot elhagyva, a gráf összefüggő marad (általánosabban: k csúcsot elhagyva, legfeljebb k összefüggő komponensre „esik szét" a gráf). Ha egy gráfban van Hamilton-út, akkor egy csúcsot elhagyva, a gráf legfeljebb két összefüggő komponensre esik szét (általánosabban: k csúcsot elhagyva legfeljebb $k+1$ összefüggő komponensre esik szét).

3.17. Tétel (Dirac, 1952)**.** Ha egy egyszerű gráfnak $n \geq 3$ csúcsa van, és minden csúcs foka legalább $n/2$, akkor a gráfban van Hamilton-kör.

3.3. Síkgráfok, színezések

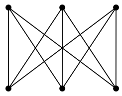
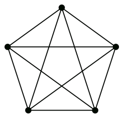
3.18. Definíció. Az olyan gráfot, amelyet le lehet rajzolni úgy, hogy a csúcsok síkbeli pontoknak felelnek meg, az élek pedig olyan görbéknek, amelyek nem metszik egymást (csak a végpontjaikban találkozhatnak), síkbarajzolható gráfnak vagy röviden síkgráfnak nevezzük.

3.19. Tétel (Wagner, 1936 és Fáry István, 1948)**.** Minden egyszerű síkgráf lerajzolható úgy, hogy az élek egyenes szakaszok legyenek.

3.20. Definíció. Ha egy egyszerű gráfban bármely két csúcs össze van kötve éllel, akkor teljes gráfnak nevezzük. Az n-csúcsú teljes gráfot K_n jelöli (a határozott névelőt az indokolja, hogy bármely két n-csúcsú teljes gráf izomorf egymással).

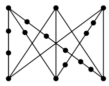
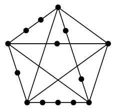
3.21. Definíció. Az olyan egyszerű gráfot, amelynek csúcshalmazát két nemüres diszjunkt részre lehet osztani úgy, hogy az egyes részeken belül nem fut él, de a két rész között minden él be van húzva, teljes páros gráfnak nevezzük. Formálisan: $V(G) = A \cup B$, ahol $A, B \neq \emptyset$, $A \cap B = \emptyset$ és $E(G) = \big\{\{a, b\} : a \in A,\, b \in B\big\}$. Ha $|A| = m$ és $|B| = n$, akkor ezt a gráfot $K_{m,n}$ jelöli (az m és n paraméterek izomorfia erejéig egyértelműen meghatározzák a gráfot).

3.22. Példa. A $K_{3,3}$ gráfot szokás „három ház-három kút"-gráfnak nevezni. Az ábra ezt a gráfot, valamint az ötpontú teljes gráfot (K_5) mutatja.

3.23. Definíció. A G gráf felosztásán olyan G' gráfot értünk, amely G-ből úgy keletkezik, hogy bizonyos élekre új csúcsokat illesztünk, ezzel több élre felosztva őket. Precízebben: G' úgy keletkezik G-ből, hogy éleit olyan utakkal helyettesítjük, amelyek a végpontjaiktól eltekintve diszjunktak.

3.24. Példa. Az ábra $K_{3,3}$ és K_5 egy-egy felosztását mutatja.

3.25. Tétel (Kuratowski, 1930)**.** Egy gráf akkor és csak akkor síkgráf, ha nem tartalmazza részgráfként K_5 vagy $K_{3,3}$ valamely felosztását.

3.26. Tétel (Euler-formula)**.** Egy összefüggő síkbarajzolt G gráf tartományokra osztja a síkot; legyen t a tartományok száma (beleszámítva a „külső" végtelen tartományt is). Ekkor fennáll a $|V(G)| - |E(G)| + t = 2$ összefüggés.

3.27. Definíció. Egy G gráf jó színezésén olyan $f\colon V(G) \to C$ leképezést értünk, ahol C egy tetszőleges halmaz (ennek elemeit nevezzük színeknek), és éllel összekötött csúcsok mindig különböző színt kapnak: $u, v \in E(G) \implies uf \neq vf$ minden $u, v \in V(G)$ esetén. A legkisebb olyan k értéket, amelyre van G-nek olyan jó színezése, amelyben k szín szerepel, a gráf kromatikus számának nevezzük, és $\chi(G)$-vel jelöljük. (Tehát $\chi(G) = k$ azt jelenti, hogy k színnel G jól színezhető, de $k-1$ színnel már nem.)

3.28. Tétel (négyszíntétel, Appel és Haken, 1976)**.** Ha G síkgráf, akkor $\chi(G) \leq 4$.

3.29. Megjegyzés. A négyszíntételből következik, hogy minden térképet ki lehet színezni legfeljebb négy színt használva úgy, hogy a szomszédos országok különböző színűek legyenek. Ehhez arra a gráfra kell alkalmazni a négyszíntételt, amelynek csúcsai az országok, és két csúcsot akkor és csak akkor kötünk össze éllel, ha a megfelelő két ország szomszédos.

3.4. Fák és erdők

3.30. Definíció. A körmentes összefüggő gráfokat fáknak nevezzük. A körmentes gráfokat erdőknek nevezzük (hiszen összefüggő komponenseik fák).

3.31. Tétel. Tetszőleges n-csúcsú gráf esetén ekvivalensek az alábbiak:

(1) G fa;

(2) G összefüggő, de bármely élét törölve már nem marad összefüggő;

(3) G körmentes, de bárhogy adunk hozzá egy új élt, már nem marad körmentes;

(4) G összefüggő, és $|E(G)| = n - 1$;

(5) G körmentes, és $|E(G)| = n - 1$.

3.32. Következmény. Ha egy fának legalább két csúcsa van, akkor legalább két elsőfokú csúcsa van.

3.5. Páros gráfok, párosítások

3.33. Definíció. A G gráfot páros gráfnak nevezzük, ha csúcshalmazát két diszjunkt részre lehet osztani úgy, hogy az egyes részeken belül nincsenek élek (azaz minden él „keresztben" megy): $V(G) = A \cup B$, ahol $A \cap B = \emptyset$ és minden él $\{a, b\}$ alakú, alkalmas $a \in A$, $b \in B$ csúcsokkal.

3.34. Megjegyzés. Egy gráf akkor és csak akkor páros, ha részgráfja egy teljes páros gráfnak (lásd a 3.21). Definíciót). A párossággal ekvivalens az is, hogy a gráfot két színnel ki lehet színezni (azaz a kromatikus száma legfeljebb 2): az A-beli csúcsokat színezzük az egyik színnel, a B-beli csúcsokat a másik színnel. A páros gráfokat úgy szokás lerajzolni, hogy az A-beli pontokat egymás mellé alulra, a B-beli pontokat egymás mellé fölülre helyezzük, és így beszélhetünk „alsó" és „fölső" csúcsokról.

3.35. Tétel. Egy gráf akkor és csak akkor páros, ha nem tartalmaz páratlan hosszúságú kört.

3.36. Definíció. Élek egy M halmazát párosításnak nevezzük, ha semelyik két M-beli élnek nincs közös végpontja. Az M-beli éleket párosított éleknek nevezzük, ezek végpontjait pedig párosított csúcsoknak (a többi élet és csúcsot pedig párosítatlannak). Ha minden csúcs párosítva van, akkor teljes párosításról beszélünk. A G gráfban található legnagyobb elemszámú párosítás méretét $\nu(G)$ jelöli: $\nu(G) = \max\{|M| : M \subseteq E(G) \text{ párosítás}\}$.

3.37. Definíció. Csúcsok egy C halmazát lefogó ponthalmaznak nevezzük, ha minden G-beli élnek legalább az egyik végpontja C-ben van. A G gráfban található legkisebb elemszámú lefogó ponthalmaz méretét $\tau(G)$ jelöli: $\tau(G) = \min\{|C| : C \subseteq V(G) \text{ lefogó ponthalmaz}\}$.

3.38. Tétel. Minden G gráfra teljesül a $\nu(G) \leq \tau(G)$ egyenlőtlenség.

3.39. Definíció. Legyen G egy gráf és $M \subseteq E(G)$ egy párosítás. Egy G-beli utat alternáló útnak nevezünk (M-re nézve), ha benne felváltva következnek párosított és párosítatlan élek. Javító útnak nevezzük az olyan alternáló utat, amelynek mindkét végpontja párosítatlan.

3.40. Tétel (Berge-tétel)**.** Egy párosítás akkor és csak akkor maximális elemszámú, ha nincs hozzá javító út.

3.41. Megjegyzés. Párosítások és lefogó ponthalmazok nemcsak páros gráfokban definiálhatóak, hanem tetszőleges gráfokban, és az eddigiek (a $\nu(G) \leq \tau(G)$ egyenlőtlenség és a Berge-tétel) minden gráfban érvényesek. A következő tételek viszont már kimondottan páros gráfokra vonatkoznak.

3.42. Tétel (Kőnig-tétel)**.** Ha G páros gráf, akkor $\nu(G) = \tau(G)$.

3.43. Következmény. Legyen G páros gráf, és M egy párosítás G-ben. Az M párosítás akkor és csak akkor maximális elemszámú, ha létezik olyan C lefogó ponthalmaz, amelyre $|M| = |C|$. (Ekkor szükségképpen $\nu(G) = |M| = |C| = \tau(G)$.)

3.44. Megjegyzés. A Kőnig-tétel bizonyítása hatékony algoritmust ad maximális elemszámú párosítás keresésére páros gráfokban. Ez az úgynevezett magyar módszer; az elnevezés Harold Kuhn amerikai matematikustól származik (1955), aki egy általánosabb algoritmust adott, ami Kőnig Dénes és Egerváry Jenő eredményeire (1931) épül. A magyar módszer vázlata:

1. Kiindulunk egy tetszőleges M párosításból (lehet akár $M = \emptyset$ is).
2. Az összes alsó párosítatlan csúcsból minden lehetséges módon alternáló utakat „növesztünk”. Eközben megcímkézzük a csúcsokat: minden csúcshoz, amibe eljutunk, odaírjuk, hogy milyen hosszú alternáló úttal sikerült elérni.
3. Ha valamelyik alternáló út elér egy fölső párosítatlan csúcsot, akkor az javító út. Ekkor javítjuk a párosítást, és visszatérünk a 2. lépésre.
4. Ha nem lehet alternáló úttal elérni egyik fölső párosítatlan csúcsot sem, akkor M maximális elemszámú párosítás, és ezt igazolja a következő C lefogó ponthalmaz: $C = \{\text{alsó címkézetlen csúcsok}\} \cup \{\text{fölső címkézett csúcsok}\}$. (Erre a lefogó ponthalmazra $|C| = |M|$ teljesül.)

3.45. Definíció. Tetszőleges G gráf és $X \subseteq V(G)$ csúcshalmaz esetén X szomszédsága az X-beli csúcsokkal éllel összekötött csúcsok halmaza. Jelölés : $N(X) = \{y \in V(G) : \{x, y\} \in E(G) \text{ valamely } x \in X \text{ csúcsra}\}$.

3.46. Tétel (Kőnig–Hall-tétel)**.** Egy páros gráfban akkor és csak akkor van teljes párosítás, ha az alsó és fölső pontok száma ugyanannyi, és (fölső) csúcsok bármely X halmazára $|N(X)| \geq |X|$ teljesül.

4. Absztrakt algebra

4.1. Műveletek, algebrai struktúrák

4.1. Definíció. Tetszőleges A nemüres halmaz és $n \in \mathbb{N}_0$ esetén A-n értelmezett n-változós műveleten egy

$$f\colon A^n \to A,\ (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$$

leképezést értünk.

4.2. Megjegyzés. Mivel A^0 egyelemű halmaz (egészen pontosan $A^0 = \{\emptyset\}$), bármely $f\colon A^0 \to A$ leképezést egyértelműen meghatározza az A^0 halmaz egyetlen elemén felvett értéke. Tehát egy nullaváltozós művelet egyszerűen az alaphalmaz egy elemének kijelölését jelenti.

4.3. Definíció. Algebrai struktúrán vagy röviden algebrán egy műveletekkel „felszerelt” nemüres halmazt értünk. Formálisan: $\mathbb{A} = (A; F)$ algebrai struktúra, ha A egy nemüres halmaz, F pedig A-n értelmezett műveletek egy halmaza. Az A halmazt az $\mathbb{A}$ algebra alaphalmazának vagy tartóhalmazának nevezzük.

4.4. Megjegyzés. Ha a műveletek világosak a szövegkörnyezetből, akkor az algebrát és a tartóhalmazát nem mindig különböztetjük meg élesen egymástól.

4.5. Definíció. Ha f egy kétváltozós művelet az A halmazon, akkor $f(x, y)$ helyett általában azt írjuk, hogy $x * y$ (persze más szimbólumot is írhatunk x és y közé). Ilyenkor az $\mathbb{A} = (A; *)$ algebrát grupoidnak nevezzük.

4.6. Definíció. Legyen $*$ egy kétváltozós művelet az A halmazon.

- A $*$ művelet kommutatív, ha minden $a, b \in A$ esetén $a * b = b * a$.
- A $*$ művelet asszociatív, ha minden $a, b, c \in A$ esetén $(a * b) * c = a * (b * c)$.
- A $z \in A$ elem zéruselem, ha minden $a \in A$ esetén $a * z = z * a = z$.
- Az $e \in A$ elem egységelem, ha minden $a \in A$ esetén $a * e = e * a = a$.
- Ha e egységelem, akkor a és b egymás inverzei, amennyiben $a * b = b * a = e$.
- A $*$ művelet kancellatív, ha minden $a, b, c \in A$ esetén $a * c = b * c \Longrightarrow a = b$ és $c * a = c * b \Longrightarrow a = b$.

4.7. Definíció. Legyen A nemüres halmaz.

- Ha $*$ kétváltozós művelet az A halmazon, akkor $(A; *)$ grupoid.
- Ha $(A; *)$ grupoid és $*$ asszociatív, akkor $(A; *)$ félcsoport.
- Ha $(A; *)$ félcsoport és van egységeleme, akkor $(A; *)$ monoid.
- Ha $(A; *)$ monoid és minden elemének van inverze, akkor $(A; *)$ csoport.
- Ha $(A; *)$ csoport és $*$ kommutatív, akkor $(A; *)$ Abel-csoport.

4.8. Definíció. Legyen A nemüres halmaz, és legyenek $+$ és $\cdot$ kétváltozós műveletek az A halmazon. Az $(A; +, \cdot)$ struktúrát gyűrűnek nevezzük, ha

(1) $(A; +)$ Abel-csoport, azaz
  - az összeadás asszociatív,
  - van additív egységelem (jelölése: 0),
  - minden elemnek van additív inverze (jelölése: $-a$),
  - az összeadás kommutatív;

(2) $(A; \cdot)$ félcsoport, azaz
  - a szorzás asszociatív;

(3) és a szorzás disztributív az összeadásra, azaz
  - $(a + b) \cdot c = a \cdot c + b \cdot c$ és $c \cdot (a + b) = c \cdot a + c \cdot b$ minden $a, b, c \in A$ esetén.

4.9. Definíció. Legyen A nemüres halmaz, és legyenek $+$ és $\cdot$ kétváltozós műveletek az A halmazon. Az $(A; +, \cdot)$ struktúrát testnek nevezzük, ha

(1) $(A; +, \cdot)$ gyűrű,

(2) $|A| \geq 2$,

(3) a szorzás kommutatív,

(4) van multiplikatív egységelem (jelölése: 1),

(5) minden nemnulla elemnek van multiplikatív inverze (jelölése: a^{-1}).

4.10. Tétel. A $\mathbb{Z}_m$ maradékosztály-gyűrű akkor és csak akkor test, ha m prímszám.

4.11. Definíció. Az $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \circ)$ grupoidok izomorfak (jelölés: $\mathbb{A} \cong \mathbb{B}$), ha létezik $\mathbb{A} \to \mathbb{B}$ izomorfizmus, azaz olyan $\varphi\colon\ A \to B$ bijekció, amelyre

$$\forall a_1, a_2 \in A\colon\ (a_1 * a_2)\varphi = a_1\varphi \circ a_2\varphi.$$

Az izomorfizmus hasonlóan definiálható tetszőleges algebrák (nem csak grupoidok) esetén (lásd az 4.68. Megjegyzést).

4.12. Tétel. Izomorfizmusok szorzata és inverze is izomorfizmus.

4.13. Következmény. Az izomorfia ekvivalenciareláció (grupoidok bármely halmazán).

4.14. Megjegyzés. Az izomorfizmus szemléletes jelentése az, hogy $\mathbb{A}$ és $\mathbb{B}$ szerkezete ugyanaz, csak „máshogy hívják” az elemeiket. Ezért izomorf algebrákat nem mindig érdemes (időnként nem is lehet!) megkülönböztetni (Steinitz-elv).

4.2. Részalgebra, generálás

4.15. Definíció. A $B \subseteq A$ részhalmaz zárt az $f\colon A^n \to A$ műveletre, ha $f(b_1, \ldots, b_n) \in B$ minden $b_1, \ldots, b_n \in B$ esetén. (Ha $n = 0$, akkor ez azt jelenti, hogy B tartalmazza az f által kijelölt elemet). Ha B zárt az $\mathbb{A} = (A; F)$ algebra minden műveletére (azaz minden $f \in F$-re), akkor egyszerűen csak zárt részhalmaznak nevezzük. Ha B nemüres zárt halmaz az $\mathbb{A} = (A; F)$ algebrában, akkor az F-beli műveletek megszorításaival egy $\mathbb{B}$ algebrát alkot, amelyet $\mathbb{A}$ részalgebrájának nevezünk. Jelölés: $\mathbb{B} \leq \mathbb{A}$.

4.16. Megjegyzés. Az üres halmaz zárt minden legalább egyváltozós műveletre, de a nullaváltozósokra nem.

4.17. Tétel. Zárt részhalmazok metszete is zárt: ha B_i $(i \in I)$ zárt részhalmazok egy családja az $\mathbb{A}$ algebrában (lehet végtelen sok halmaz is), akkor a $\bigcap_{i \in I} B_i$ halmaz is zárt.

4.18. Definíció. Az $\mathbb{A}$ algebrában a nemüres $B \subseteq A$ halmaz által generált részalgebra, más szóval B generátuma, a legszűkebb olyan részalgebrája $\mathbb{A}$-nak, amely tartalmazza B-t. Jelölés: $[B]$. Ha $[B] = A$, akkor azt mondjuk, hogy B generátorrendszere $\mathbb{A}$-nak.

4.19. Megjegyzés. Az 4.17. Tétel garantálja, hogy valóban létezik a B-t tartalmazó zárt halmazok között egy legszűkebb, nevezetesen a B-t tartalmazó összes zárt halmazok metszete.

4.20. Tétel. Tetszőleges $\mathbb{A} = (A; F)$ algebra és $B \subseteq A$ esetén $[B]$ azon elemek halmaza, amelyek megkaphatóak B elemeiből kiindulva az F-beli műveletek véges számú alkalmazásával.

4.3. A csoport fogalma, példák, alaptulajdonságok

4.21. Definíció. Csoportnak nevezünk egy $(A; *)$ grupoidot, ha
- $*$ asszociatív: $\forall a, b, c \in A\colon\ (a * b) * c = a * (b * c)$;
- létezik egységelem: $\exists e \in A\ \ \forall a \in A\colon\ a * e = e * a = a$;
- minden elemnek van inverze: $\forall a \in A\ \ \exists b \in A\colon\ a * b = b * a = e$.

4.22. Megjegyzés. Csoportoknál szokás *multiplikatív írásmódot* használni: $a * b$ helyett azt írjuk, hogy $a \cdot b$ (vagy egyszerűen csak azt, hogy ab), és a műveletet szorzásnak nevezzük. Ilyenkor az egységelemet 1 jelöli, az a elem inverzét pedig a^{-1}. Figyelem: ezek csak jelölések; nem jelentik azt, hogy a művelet valóban szorzás, és azt sem, hogy az egységelem az 1-es szám (a csoport elemei bármik lehetnek, nem csak számok). *Additív írásmód* esetén a műveletet $a + b$, az egységelemet 0, az a elem inverzét pedig $-a$ jelöli.

4.23. Példák. Néhány fontos példa csoportra:
- $(\mathbb{C}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{Z}; +)$, $(\{0\}; +)$, $(\{\text{páros számok}\}; +)$, $\ldots$;
- $(T^{n \times m}; +)$ tetszőleges T és $n, m \in \mathbb{N}$ esetén;
- $(\mathbb{Z}_n; +)$ tetszőleges $n \in \mathbb{N}$ esetén;
- $(\mathbb{C} \setminus \{0\}; \cdot)$, $(\mathbb{R} \setminus \{0\}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\{1\}; \cdot)$, $(\{1, -1\}; \cdot)$, $(\{1, -1, i, -i\}; \cdot)$;
- $(E_n; \cdot)$, ahol $E_n = \{z \in \mathbb{C} : z^n = 1\}$ (az n-edik komplex egységgyökök csoportja);
- $(\mathrm{GL}_n(T); \cdot)$, ahol $\mathrm{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}$ (a T test feletti n-dimenziós általános lineáris csoport);
- $(\mathbb{Z}_n^*; \cdot)$ tetszőleges $n \in \mathbb{N}$ esetén;
- $(S_n; \cdot)$, ahol $S_n = \big\{ f\colon \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijekciók } \big\}$ (az n-edfokú szimmetrikus csoport);
- (síkbeli vagy térbeli) alakzatok szimmetriacsoportjai.

4.24. Tétel.
(1) Bármely grupoidban legföljebb egy egységelem létezhet.
(2) Bármely monoidban egy elemnek legföljebb egy inverze lehet.

4.25. Definíció.
- Azt mondjuk, hogy az A halmazon értelmezett $\cdot$ kétváltozós művelet invertálható, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek *legalább* egy megoldása van.
- Azt mondjuk, hogy az A halmazon értelmezett $\cdot$ kétváltozós művelet kancellatív, ha bármely $a, b \in A$ elemek esetén az $ax = b$ és $ya = b$ egyenleteknek *legfeljebb* egy megoldása van.

4.26. Megjegyzés. A kancellativitás így is megfogalmazható: $\forall a, x_1, x_2, y_1, y_2 \in A$:

$$a \cdot x_1 = a \cdot x_2 \implies x_1 = x_2;$$
$$y_1 \cdot a = y_2 \cdot a \implies y_1 = y_2.$$

4.27. Megjegyzés. Az invertálhatóság azt jelenti, hogy a művelettáblázat minden sorában és minden oszlopában az A halmaz minden eleme *legalább* egyszer fellép. A kancellativitás pedig azt jelenti, hogy minden sorban és minden oszlopban minden elem *legfeljebb* egyszer lép fel.

4.28. Tétel. Csoport művelete mindig invertálható és kancellatív.

4.29. Tétel. Ha az A halmazon értelmezett $\cdot$ kétváltozós művelet asszociatív és invertálható, akkor $(A; \cdot)$ csoport.

4.30. Megjegyzés. Az utolsó két tétel szerint egy $(A; \cdot)$ grupoid akkor és csak akkor csoport, ha a $\cdot$ művelet asszociatív és invertálható; ezt tekinthetjük a csoport egy alternatív definíciójának is. Véges alaphalmaz esetén itt kicserélhetjük az invertálhatóságot a kancellativitással, de végtelen alaphalmaz esetén nem.

4.31. Tétel (Az általános asszociativitás tétele)**.** Ha $(A;\cdot)$ félcsoport, akkor minden $n \in \mathbb{N}$ és $a_1, \dots, a_n \in A$ esetén az $a_1 \cdot \ldots \cdot a_n$ „szorzat” eredménye független a zárójelezéstől.

4.32. Definíció. Legyen G egy csoport és $a \in G$. Az a elem egész kitevős hatványait a következőképpen értelmezzük:

- $n > 0$ esetén legyen $a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$;
- $n = 0$ esetén legyen $a^n = 1$;
- $n < 0$ esetén legyen $a^n = (a^{-1})^{|n|}$.

4.33. Tétel. Tetszőleges G csoport, $a, b \in G$ elemek és $n, m \in \mathbb{Z}$ kitevők esetén teljesülnek az alábbi azonosságok:

(1) $a^n \cdot a^m = a^{n+m}$;

(2) $(a^n)^m = a^{nm}$;

(3) $(ab)^{-1} = b^{-1}a^{-1}$.

4.4. Részcsoportok

4.34. Definíció. Ha G csoport, és H olyan részgrupoid, ami maga is csoport, akkor azt mondjuk, hogy H részcsoportja G-nek, és ezt így jelöljük: $H \leq G$.

4.35. Megjegyzés. A $(G;\cdot)$ algebra részalgebrái nem mind részcsoportok, például a $G = (\mathbb{Z};+)$ csoportban a $H = \mathbb{N}$ részhalmaz zárt az összeadásra, de ez nem részcsoport (csak részfélcsoport). Tekintsük az inverzképzést egyváltozós műveletnek ($G \to G,\ a \mapsto a^{-1}$), az egységelemet pedig nullváltozós műveletnek. Ha ezeket is bevesszük az alapműveletek közé, akkor a $(G;\cdot,{}^{-1},1)$ algebrát kapjuk, és ennek a részalgebrái már épp a részcsoportok.

4.36. Tétel. Bármely G csoport és $H \subseteq G$ esetén H akkor és csak akkor részcsoportja G-nek, ha

(1) H zárt a szorzásra: $\forall h_1, h_2 \in H\colon\ h_1 \cdot h_2 \in H$;

(2) H tartalmazza G egységelemét: $1 \in H$;

(3) H zárt az inverzképzésre: $\forall h \in H\colon\ h^{-1} \in H$.

4.37. Tétel (Lagrange tétele)**.** Ha G véges csoport és H részcsoportja G-nek, akkor H elemszáma osztója G elemszámának: $|H| \mid |G|$.

4.38. Definíció. Legyen G egy csoport és $\emptyset \neq B \subseteq G$. A B részhalmaz által generált részcsoporton a G csoport *legszűkebb* olyan részcsoportját értjük, ami tartalmazza B-t. Jelölés: $[B]$. Ha $[B] = G$, akkor azt mondjuk, hogy B generátorrendszere G-nek.

4.39. Megjegyzés. Az 4.17. Tételt alkalmazva a $(G;\cdot,{}^{-1},1)$ algebrára, látható, hogy részcsoportok metszete is részcsoport (lásd a 4.35. Megjegyzést). Ez garantálja, hogy valóban létezik a B-t tartalmazó részcsoportok között egy legszűkebb, nevezetesen a B-t tartalmazó összes részcsoportok metszete.

4.40. Tétel. A B halmaz által generált részcsoport azon G-beli elemek halmaza, amelyek megkaphatók B elemeiből kiindulva a szorzás és az inverzképzés véges számú alkalmazásával.

4.5. Ciklikus csoportok, elem rendje

4.41. Definíció. A G csoportot ciklikus csoportnak nevezzük, ha egyetlen elemmel generálható, azaz $\exists a \in G\colon [a] = G$.

4.42. Tétel. Ciklikus csoport minden részcsoportja is ciklikus.

4.43. Tétel. Tetszőleges G csoport és $a \in G$ esetén $[a] = \{a^k : k \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$.

4.44. Tétel. Egy csoport akkor és csak akkor ciklikus, ha izomorf a következő csoportok valamelyikével:

$$\mathbb{Z}_1,\ \mathbb{Z}_2,\ \mathbb{Z}_3,\ \mathbb{Z}_4, \dots,\ \mathbb{Z}.$$

4.45. Definíció. Az $a \in G$ elem rendjén azt a legkisebb n pozitív egész számot értjük, amelyre $a^n = 1$. Ha nincs ilyen n, akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét $o(a)$ jelöli (olvasd: *ordó*):

$$o(a) = \min\left\{n \in \mathbb{N} : a^n = 1\right\} \qquad (\text{a } \min \emptyset = \infty \text{ megállapodással}).$$

4.46. Definíció. A G csoport rendjén elemeinek számát (számosságát) értjük.

4.47. Megjegyzés. Az a elem rendje nem más, mint az általa generált részcsoport rendje: $o(a) = |[a]|$.

4.48. Megjegyzés. Tetszőleges $z \in \mathbb{C}\backslash\{0\}$ komplex szám esetén $o(z) = n \iff [z] = E_n \cong \mathbb{Z}_n$. Az ilyen tulajdonságú számokat nevezzük primitív n-edik egységgyököknek. A primitív n-edik egységgyökök száma $\varphi(n)$. (A primitív gyökök létezéséből következik, hogy az n-edik egységgyökök csoportja ciklikus: $E_n \cong \mathbb{Z}_n$.)

4.49. Tétel. Legyen G egy véges csoport és $a \in G$ egy n-edrendű elem.

(1) $\forall k, \ell \in \mathbb{Z}\colon\ a^k = a^\ell \iff k \equiv \ell \pmod{n}$;

(2) $a^{-1} = a^{n-1}$;

(3) $\forall k \in \mathbb{Z}\colon\ a^k = 1 \iff n \mid k$;

(4) n osztója G elemszámának;

(5) $a^{|G|} = 1$.

4.50. Tétel. Minden prímrendű csoport ciklikus.

4.51. Tétel. A kis elemszámú csoportok (izomorfia erejéig) a következők:

(1) egyelemű: $\{1\}$;

(2) kételemű: $\mathbb{Z}_2$;

(3) háromelemű: $\mathbb{Z}_3$;

(4) négyelemű: $\mathbb{Z}_4$, V;

(5) ötelemű: $\mathbb{Z}_5$.

4.6. Mellékosztályok, Lagrange tétele

4.52. Definíció. A G csoport nemüres részhalmazait komplexusoknak nevezzük. Komplexusok szorzatát és inverzét elemenként értelmezzük:

$$AB = \{ab : a \in A, b \in B\}, \quad A^{-1} = \{a^{-1} : a \in A\} \qquad (\emptyset \neq A, B \subseteq G).$$

Egyelemű komplexusok esetén az alábbi egyszerűsített jelölést használjuk:

$$\{a\}B = aB, \quad B\{a\} = Ba \qquad (a \in G,\ \emptyset \neq B \subseteq G).$$

4.53. Tétel. Egy $H \subseteq G$ komplexus akkor és csak akkor részcsoport, ha

$$HH \subseteq H,\ 1 \in H,\ H^{-1} \subseteq H.$$

4.54. Megjegyzés. Ha $H \leq G$, akkor nemcsak $HH \subseteq H$, de $H \subseteq HH$ is teljesül, mert $H = \{1\}H \subseteq HH$, tehát $HH = H$. Hasonlóan $H^{-1} = H$ is teljesül.

4.55. Definíció. Tetszőleges $H \leq G$ és $a \in G$ esetén az a elem H részcsoport szerinti bal illetve jobb oldali mellékosztályának nevezzük az alábbi halmazokat:

$$aH = \{ah : h \in H\}, \qquad Ha = \{ha : h \in H\}.$$

4.56. Tétel. Legyen $H \leq G$, és definiáljunk a G halmazon egy $\sim$ relációt:

$$a \sim b \iff ab^{-1} \in H.$$

Ekkor $\sim$ ekvivalenciareláció, és egy $a \in G$ elem ekvivalenciaosztálya Ha.

4.57. Következmény. Tetszőleges $H \leq G$ esetén a H szerinti jobb oldali mellékosztályok a G halmaz egy osztályozását alkotják. Hasonló érvényes a bal oldali mellékosztályokra is.

4.58. Definíció. A G véges csoport H részcsoportja szerinti bal (vagy jobb) oldali mellékosztályok számát H indexének nevezzük. Jelölés: $[G : H]$.

4.59. Tétel (Lagrange tétele)**.** Tetszőleges G véges csoport és H részcsoport esetén

$$|G| = |H| \cdot [G : H].$$

Következésképp $|H|$ osztója $|G|$-nek.

4.7. Kongruencia, faktoralgebra

4.60. Definíció. Legyen $\mathbb{A} = (A; F)$ egy algebra, és legyen $\sim$ egy ekvivalenciareláció az A halmazon. Azt mondjuk, hogy $\sim$ kongruenciarelációja (vagy röviden kongruenciája) az $\mathbb{A}$ algebrának, ha minden $f \in F$ (n-változós) művelet és tetszőleges $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in A$ elemek esetén

$$(a_1 \sim b_1 \text{ és } a_2 \sim b_2 \text{ és } \ldots \text{ és } a_n \sim b_n) \implies f(a_1, a_2, \ldots, a_n) \sim f(b_1, b_2, \ldots, b_n).$$

4.61. Definíció. Legyen $\mathbb{A} = (A; F)$ egy algebra, és legyen $\mathcal{C}$ egy osztályozás az A halmazon. Azt mondjuk, hogy $\mathcal{C}$ kompatibilis osztályozása az $\mathbb{A}$ algebrának, ha minden $f \in F$ (n-változós) művelet és tetszőleges $C_1, C_2, \ldots, C_n \in \mathcal{C}$ osztályok esetén létezik egy olyan (egyértelműen meghatározott) $D \in \mathcal{C}$ osztály, amelyre

$$\{f(c_1, c_2, \ldots, c_n) : c_1 \in C_1,\ c_2 \in C_2,\ \ldots, c_n \in C_n\} \subseteq D. \qquad (\star)$$

4.62. Tétel. Tetszőleges $\mathbb{A}$ algebra és tetszőleges A-n értelmezett $\sim$ ekvivalanciareláció esetén $\sim$ akkor és csak akkor kongruenciája $\mathbb{A}$-nak, ha a hozzá tartozó $A/{\sim}$ osztályozás kompatibilis osztályozása $\mathbb{A}$-nak.

4.63. Példa. Az egész számok gyűrűjén az $a \sim b \iff m \mid a - b$ képlettel definiált reláció mindig kongruencia, és a megfelelő osztályok a modulo m maradékosztályok.

4.64. Definíció. Legyen $\sim$ kongruenciarelációja az $\mathbb{A}$ algebrának. Minden $f \in F$ (n-változós) művelet és tetszőleges $C_1, C_2, \ldots, C_n \in A/\!\sim$ osztályok esetén jelölje $f(C_1, C_2, \ldots, C_n)$ azt a $D \in A/\!\sim$ osztályt, amelyre $f(c_1, c_2, \ldots, c_n) \in D$ minden $c_i \in C_i$ esetén. Az $A/\!\sim$ halmaz ezekkel a műveletekkel egy algebrát alkot, amelyet az $\mathbb{A}$ algebra $\sim$ szerinti faktoralgebrájának nevezzük. Jelölés: $\mathbb{A}/\!\sim$.

4.65. Megjegyzés. A ($\star$) képletben lehet valódi tartalmazás, tehát $f(C_1, C_2, \ldots, C_n)$ nem feltétlenül egyezik meg az összes $f(c_1, \ldots, c_n)$ $(c_1 \in C_1, \ldots, c_n \in C_n\}$ alakú elemek halmazával.

4.66. Megjegyzés. Ha a $c \in A$ elem $\sim$ kongruencia szerinti ekvivalenciaosztályát $\overline{c}$-sal jelöljük (a maradékosztályokhoz hasonlóan), akkor a faktoralgebra műveletei így definiálhatóak:

$$f(\overline{c_1}, \overline{c_2}, \ldots, \overline{c_n}) = \overline{f(c_1, c_2, \ldots, c_n)}.$$

Például egy kétváltozós $*$ művelet esetén $\overline{a} * \overline{b} = \overline{a * b}$. (A bal oldalon az $\mathbb{A}/\!\sim$ faktoralgebra művelete szerepel, a jobb oldalon pedig az eredeti $\mathbb{A}$ algebra művelete.)

4.8. Homomorfizmus, homomorfiatétel

4.67. Definíció. Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \circ)$ két grupoid. Azt mondjuk, hogy a $\varphi\colon A \to B$ leképezés homomorfizmus $\mathbb{A}$-ról $\mathbb{B}$-be, ha φ felcserélhető a műveletekkel, azaz

$$\forall a_1, a_2 \in A\colon \quad (a_1 * a_2)\varphi \;=\; a_1\varphi \circ a_2\varphi.$$

Ha létezik $\varphi\colon \mathbb{A} \to \mathbb{B}$ szürjektív homorfizmus, akkor azt mondjuk, hogy $\mathbb{B}$ homomorf képe $\mathbb{A}$-nak. Speciális homomorifzmusok:

- bijektív homomorfizmus = izomorfizmus,
- injektív homomorfizmus = beágyazás,
- $\mathbb{A} \to \mathbb{A}$ homomorfizmus = endomorfizmus,
- bijektív $\mathbb{A} \to \mathbb{A}$ homomorfizmus = automorfizmus.

4.68. Megjegyzés. Ha az algebráknak nem csak egy műveletük van, akkor minden műveletre külön-külön meg kell követelni a műveletekkel való felcserélhetőséget. Például, ha $\mathbb{A} = (A; +, \cdot)$ és $\mathbb{B} = (B; +, \cdot)$ gyűrűk, akkor egy $\varphi\colon A \to B$ leképezés akkor gyűrűhomomorfizmus, ha minden $a_1, a_2 \in A$ esetén

$$(a_1 + a_2)\varphi = a_1\varphi + a_2\varphi \quad \text{és} \quad (a_1 \cdot a_2)\varphi = a_1\varphi \cdot a_2\varphi.$$

4.69. Tétel. Homomorfizmusok szorzata is homomorfizmus.

4.70. Definíció. Legyen $\sim$ kongruenciája az $\mathbb{A}$ algebrának. Ekkor a

$$\nu\colon \mathbb{A} \to \mathbb{A}/\!\sim, \;\; a \mapsto \overline{a}$$

leképezés szürjektív homomorfizmus, amelyet a $\sim$ kongruenciához tartozó természetes homomorfizmusnak nevezünk.

4.71. Definíció. A $\varphi\colon A \to B$ leképezés magján az alábbi $\ker\varphi$ ekvivalenciarelációt értjük:

$$\ker\varphi = \big\{(a_1, a_2) : a_1\varphi = a_2\varphi\big\} \subseteq A \times A.$$

4.72. Tétel (Homomorfiatétel)**.** Ha $\varphi\colon \mathbb{A} \to \mathbb{B}$ homomorfizmus, akkor...

(a) $\mathbb{A}\varphi \leq \mathbb{B}$, azaz φ értékkészlete részalgebrája $\mathbb{B}$-nek;

(b) $\ker\varphi$ kongruenciája $\mathbb{A}$-nak;

(c) $\mathbb{A}/\ker\varphi \cong \mathbb{A}\varphi$, azaz a mag szerinti faktoralgebra izomorf a homomorf képpel.

4.73. Következmény (Homomorfiatétel)**.** Ha $\varphi\colon \mathbb{A} \to \mathbb{B}$ szürjektív homomorfizmus, akkor $\mathbb{A}/\ker\varphi \cong \mathbb{B}$.

4.74. Következmény. A homomorf képek és a faktoralgebrák „lényegében” ugyanazok:

- minden faktoralgebra homomorf kép;
- minden homomorf kép izomorf egy faktoralgebrával.

4.9. Direkt szorzat

4.75. Definíció. Az $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \circ)$ grupoidok direkt szorzata az $\mathbb{A} \times \mathbb{B} = (A \times B; \otimes)$ grupoid, amelynek műveletét az alábbi módon értelmezzük:

$$(a_1, b_1) \otimes (a_2, b_2) = (a_1 * a_2, b_1 \circ b_2) \qquad (a_1, a_2 \in A, b_1, b_2 \in B).$$

4.76. Megjegyzés. Ha az algebráknak nem csak egy műveletük van, akkor minden műveletet komponensenként értelmezünk. Például, ha $\mathbb{A} = (A; +, \cdot)$ és $\mathbb{B} = (B; +, \cdot)$ gyűrűk, akkor az $\mathbb{A} \times \mathbb{B} = (A \times B; +, \cdot)$ direkt szorzatban így fest az összeadás és a szorzás: minden $a_1, a_2 \in A$ és $b_1, b_2 \in B$ esetén

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{és} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

4.77. Tétel. Az alábbi leképezések (projekciók) szürjektív homomorfizmusok:

$$\pi_1\colon \mathbb{A}\times\mathbb{B}\to\mathbb{A},\quad (a,b)\mapsto a;$$
$$\pi_2\colon \mathbb{A}\times\mathbb{B}\to\mathbb{B},\quad (a,b)\mapsto b.$$

Következésképp $\mathbb{A}$ és $\mathbb{B}$ is izomorf $\mathbb{A}\times\mathbb{B}$ egy-egy faktoralgebrájával.

4.78. Tétel. Csoportok direkt szorzata mindig csoport.

4.79. Tétel. A $\mathbb{Z}_m\times\mathbb{Z}_n$ csoport akkor és csak akkor ciklikus, ha m és n relatív prímek. Ha ez a helyzet, akkor $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$ az alábbi izomorfizmus mellett:

$$\varphi\colon \mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n,\quad x \bmod mn\mapsto (x \bmod m, x \bmod n).$$

Ez nemcsak csoportizomorfizmus, hanem gyűrűizomorfizmus is.

4.80. Következmény. Ha m és n relatív prímek, akkor $\mathbb{Z}_{mn}^*\cong\mathbb{Z}_m^*\times\mathbb{Z}_n^*$.

4.81. Tétel (A véges Abel-csoportok alaptétele)**.** Minden véges Abel-csoport prímhatványrendű ciklikus csoportok direkt szorzatára bontható.

4.10. Normálosztók, faktorcsoportok

4.82. Definíció. Az $N\leq G$ részcsoportot normálosztónak nevezzük, ha az N szerinti bal és jobb oldali mellékosztályozás megegyezik: $\forall a\in G\colon\ aN=Na$. Jelölés: $N\lhd G$.

4.83. Megjegyzés. Abel-csoportban minden részcsoport normálosztó.

4.84. Tétel. Ha $N\lhd G$, akkor az N szerinti mellékosztályozás kompatibilis osztályozása a G csoportnak. A megfelelő kongruencia szerinti faktoralgebra csoport, amelyet a G csoport N normálosztó szerinti faktorcsoportjának nevezünk. Jelölés: G/N.

4.85. Tétel. Legyen $\sim$ kongruenciája a G csoportnak, és legyen $N=\{a\in G : a\sim 1\}$. Ekkor $N\lhd G$, és a $\sim$ kongruenciához tartozó kompatibilis osztályozás éppen az N szerinti mellékosztályozás.

4.86. Következmény. Csoportok esetén kölcsönösen egyértelmű megfeleltetés van a kongruenciák és a normálosztók között.

4.87. Tétel. Ha az $M,N\lhd G$ normálosztókra $MN=G$ és $M\cap N=\{1\}$ teljesül, akkor $G\cong M\times N$. Fordítva, G minden direkt felbontása egy ilyen normálosztó-párnak felel meg.