

# DISZKRÉT MATEMATIKA II (MBNXK112)

WALDHAUSER TAMÁS

előadásvázlat  
(2021. április 29.)

## 1. SZÁMELMÉLET (DIOFANTOSZI EGYENLETEK ÉS KONGRUENCIÁK)

### 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:

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

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

- (1)  $a \mid a$ ;
- (2)  $(a \mid b \text{ és } b \mid c) \implies a \mid c$ ;
- (3)  $(a \mid b \text{ és } b \mid a) \iff b = \pm a$ ;
- (4)  $(a \mid b \text{ és } a \mid c) \implies a \mid b \pm c$ ;
- (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  $(\mathbb{N}_0, \mid)$  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:

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

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

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

**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  $\lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1$ , ahol  $p_n$  az  $n$ -edik prímszám. (Megjegyzés: a prímszámtételt nem ilyen formában, hanem az  $x$  valós számnál nem nagyobb prímekeket megszámláló  $\pi(x)$  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:  $d = \text{lko}(a, b)$  vagy egyszerűen csak  $d = (a, b)$ ), ha

$$(KO) \quad d \mid a, b, \text{ és}$$

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

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

(KT)  $a, b \mid t$ , és

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

**1.15. Definíció.** Ha  $\text{lko}(a, b) = 1$ , 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:

$$\text{lko}(a, b) \cdot \text{lkkt}(a, b) = ab.$$

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

$$\text{lko}(a, b) = \text{lko}(a - b, b).$$

**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”:

$$\forall a, b \in \mathbb{Z} \exists u, v \in \mathbb{Z}: au + bv = \text{lko}(a, b).$$

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

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

$$a \mid bc \iff \frac{a}{\text{lko}(a, b)} \mid c.$$

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 prímszorzattal felbontása

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

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

- (1)  $a \mid b \iff \forall i: \alpha_i \leq \beta_i$ ;
- (2)  $\text{lko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot p_k^{\min(\alpha_k, \beta_k)}$ ;
- (3)  $\text{lkkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot p_k^{\max(\alpha_k, \beta_k)}$ .

### 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  $\text{lko}(a, b) \mid c$ .
- Ha  $(x_0, y_0)$  egy **partikuláris megoldás**, akkor az **általános megoldás**:

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

### 1.4. Kongruenciareláció

**1.25. Definíció.** Tetszőleges  $a, b$  egész számok és  $m \geq 2$  természetes szám 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. Tétel.** Két egész szám akkor és csak akkor kongruens modulo  $m$ , ha ugyanazt a maradékot adják  $m$ -mel osztva.

**1.27. Tétel.** Tetszőleges  $a, a_1, a_2, b, b_1, b_2, c$  egész számok és  $m, m_1, m_2 \geq 2$  modulusok esetén teljesülnek a következők:

- (1)  $a \equiv a \pmod{m}$ ;
- (2)  $(a \equiv b \pmod{m} \text{ és } b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$ ;
- (3)  $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ ;
- (4)  $\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}, \quad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ ;
- (5) Ha  $c \neq 0$ , akkor  $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{\text{lko}(m, c)}}$ ;

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

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

**1.28. 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

**1.29. 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.

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

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

$$x \equiv x_0 \pmod{\frac{m}{\text{lko}(a, m)}}.$$

## 1.6. Lineáris kongruenciarendszer

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

$$\left. \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{array} \right\}$$

**1.32. 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!):

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

**1.33. Tétel.** Tekintsük a (\*) kongruenciarendszert.

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

$$x \equiv x_0 \pmod{\text{lkkt}(m_1, \dots, m_k)}.$$

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

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

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

$$x \equiv c_1 e_1 + \dots + c_k e_k \pmod{m_1 \cdots m_k}.$$

## 2. KOMBINATORIKA

### 2.1. Alapelvek

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

- (1) Ha létezik  $A \rightarrow B$  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 megszámlalendő dolgok  $A$  halmaza helyett találunk egy  $B$  halmazt és egy  $A \rightarrow B$  bijekciót, akkor elég  $B$  elemeit megszámlálni. (Ez persze csak akkor célravezető, ha olyan  $B$  halmazt találunk, aminek az elemeit könnyebb megszámlálni.)
- (2) Két egymást kizáró esetet különböztetünk meg, és külön-külön megszámloljuk 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 műveletnek 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  $(a_1, \dots, a_n)$  sorozattal, ahol minden elem pontosan egyszer fordul elő, azaz  $\{a_1, \dots, a_n\} = A$ . Az  $A = \{1, \dots, n\}$  esetben ezt a permutációt megadhatjuk egy  $A \rightarrow A$ ,  $i \mapsto a_i$  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 **rendszer**ről 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 **ismétlésees permutációnak** nevezük.

**2.7. Tétel.** Ha egy  $n$ -elemű rendszerben  $r$ -féle különböző elem van, és ezek rendre  $k_1, \dots, k_r$  példányban fordulnak elő (akkor persze  $n = k_1 + \dots + k_r$ ), akkor a rendszer (ismétlésees) 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)

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

**2.10. Definíció.** A fenti tételben szereplő  $\binom{n}{k}$  kifejezést (ahol  $0 \leq k \leq n$ ) **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 **ismétlésees kombinációjáról** beszélünk. Egy  $k$ -adosztályú ismétlésees kombináció tehát nem más, mint a halmaz elemeiből alkotott  $k$ -elemű rendszer.

**2.12. Tétel.** Egy  $n$  elemű halmaz  $k$ -adosztályú ismétlésees 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 **ismétlésees variációjáról** beszélünk. Egy  $k$ -adosztályú ismétlésees 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  $\{1, \dots, k\} \rightarrow A$ ,  $i \mapsto a_i$  leképezéssel is.

**2.14. Tétel.** Egy  $n$  elemű halmaz  $k$ -adosztályú ismétlésees 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  $\{1, \dots, k\} \rightarrow A$ ,  $i \mapsto a_i$  *injektív* leképezéssel is.

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



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

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

**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. SZÁMELMÉLET (MARADÉKOSZTÁLYOK, HATVÁNYOZÁS MODULO $m$ )

Ebben a fejezetben  $m$  mindig egy 1-nél nagyobb természetes számot (modulust) jelöl.

#### 3.1. Maradékosztályok

**3.1. Definíció.** A modulo  $m$  kongruencia ekvivalenciareláció az egész számok halmazán. A megfelelő ekvivalenciaosztályokat **modulo  $m$  maradékosztályoknak** nevezzük. Egy  $a$  egész szám modulo  $m$  maradékosztálya tehát a következő halmaz:

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

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

**3.2. Megjegyzés.** Az  $\bar{a}$  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  $\bar{a} = \bar{b} \iff a \equiv b \pmod{m}$ .

**3.3. 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  $\{\bar{a}_1, \dots, \bar{a}_m\} = \mathbb{Z}_m$ .

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

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

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

**3.5. 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.

#### 3.2. Redukált maradékosztályok, egész kitevős hatványozás

**3.6. Definíció.** Azt mondjuk, hogy  $\bar{a} \in \mathbb{Z}_m$  **redukált maradékosztály**, ha  $\text{luko}(a, m) = 1$ . A modulo  $m$  redukált maradékosztályok halmazát  $\mathbb{Z}_m^*$  jelöli:  $\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : \text{luko}(a, m) = 1\}$ .

**3.7. Definíció.** Azt mondjuk, hogy az  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  maradékosztályok egymás **multiplikatív inverzei**, ha  $\bar{a} \cdot \bar{b} = \bar{1}$ . Jelölés:  $\bar{b} = \bar{a}^{-1}$  (és persze ekkor  $\bar{a} = \bar{b}^{-1}$  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)!

**3.8. Tétel.** Egy  $\bar{a} \in \mathbb{Z}_m$  maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha  $\text{luko}(a, m) = 1$ , azaz  $\bar{a} \in \mathbb{Z}_m^*$ .

**3.9. Definíció.** Maradékosztály nemnegatív egész kitevős hatványát természetes módon lehet értelmezni:  $\bar{a} \in \mathbb{Z}_m$  és  $n \in \mathbb{N}$  esetén legyen  $\bar{a}^n = \underbrace{\bar{a} \cdot \dots \cdot \bar{a}}_n$  és  $\bar{a}^0 = \bar{1}$ . A negatív egész kitevős hatványozást viszont csak redukált

maradékosztályok esetén értelmezzük:  $\bar{a} \in \mathbb{Z}_m^*$  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.)

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

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

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

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

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

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

### 3.3. Az Euler-féle $\varphi$ függvény és az Euler–Fermat-tétel

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

$$\varphi(n) = |\{a : 1 \leq a \leq n \text{ és } \text{lko}(a, n) = 1\}|.$$

Az így kapott  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ ,  $n \mapsto \varphi(n)$  függvényt **Euler-féle  $\varphi$  függvénynek** nevezzük.

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

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

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

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

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

**3.17. 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  $a^p \equiv a \pmod{p}$ .

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

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

**3.19. Megjegyzés.** A fenti állítás megfordítása nem igaz. Ha ekvivalenciát szeretnénk, akkor a kitevőket nem modulo  $\varphi(m)$ , hanem modulo  $o(\bar{a})$  kell tekinteni (lásd a 3.11. Tételt).

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

## 4. GRÁFELMÉLET

### 4.1. Alapfogalmak

**4.1. Definíció.** Legyenek  $V$  és  $E$  tetszőleges halmazok és legyen  $\iota: E \rightarrow V \cup \binom{V}{2}$  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 **hurokélnak** nevezzük.

**4.2. 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  $\iota$  leképezésre. Az ilyen **egyszerű gráfot** tehát egyszerűen(!) egy  $G = (V, E)$  párral lehet megadni, ahol  $E \subseteq \binom{V}{2}$ .

**4.3. Definíció.** Azt mondjuk, hogy a  $G$  és  $H$  egyszerű gráfok **izomorfak**, ha létezik olyan  $f: V(G) \rightarrow V(H)$  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.)

**4.4. 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,  $\rho$  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 nyílal 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.

**4.5. 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.

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

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

**4.7. Definíció.** A  $G$  gráfban a  $v$  csúcsból a  $w$  csúcsba vezető **sétának** nevezzük csúcsoknak és éleknek egy olyan  $v = v_0, e_1, v_1, e_2, \dots, v_{\ell-1}, e_\ell, v_\ell = w$  sorozatát, ahol az  $e_i$  él két végpontja  $v_{i-1}$  és  $v_i$  minden  $i \in \{1, \dots, \ell\}$  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  $v_0, v_1, \dots, v_\ell$  csúcssorozattal, ahol  $\{v_{i-1}, v_i\} \in E(G)$  minden  $i \in \{1, \dots, \ell\}$  esetén.)

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

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

**4.10. 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.

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

**4.12. 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.

## 4.2. Euler-vonal, Hamilton-út

**4.13. 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.

**4.14. 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).
- Pontosán 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).

**4.15. 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.

**4.16. 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).

**4.17. 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.

## 4.3. Síkgráfok, színezések

**4.18. 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.

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

**4.20. 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).

**4.21. Definíció.** Az olyan egyszerű gráfot, amelynek csúcshalmazát két nemüres diszjunkt részre lehet osztani úgy, hogy az egyes részekben 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  $E(G) = \{\{a, b\} : a \in A, b \in B\}$ . 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).

**4.22. 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.



**4.23. 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.



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



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

**4.26. 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.

**4.27. Definíció.** Egy  $G$  gráf **jó színezésén** olyan  $f: V(G) \rightarrow C$  leképezést értünk, ahol  $C$  egy tetszőleges halmaz (ennek elemeit nevezzük színeknek), és éllel összekötött csúcsok mindig különböző szintet 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.)

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

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

#### 4.4. Fák és erdők

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

**4.31. 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  $|E(G)| = n - 1$ .

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

#### 4.5. Páros gráfok, párosítások

**4.33. Definíció.** A  $G$  gráfot **páros gráfnak** nevezzük, ha csúcshalmazát két diszjunkt részre lehet osztani úgy, hogy az egyes részekben 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.

**4.34. Megjegyzés.** Egy gráf akkor és csak akkor páros, ha részgráfja egy teljes páros gráfnak (lásd a 4.21). 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 fölültre helyezzük, és így beszélhetünk „alsó” és „felső” csúcsokról.

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

**4.36. Definíció.** Élek egy  $M$  halmazát **párosításnak** nevezzük, ha semelyik két  $M$ -beli élnek nincs közös végpontja. Az  $M$ -beli éleket párosított élekként 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:  $\nu(G) = \max \{|M| : M \subseteq E(G) \text{ párosítás}\}$ .

**4.37. 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:  $\tau(G) = \min \{|C| : C \subseteq V(G) \text{ lefogó ponthalmaz}\}$ .

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

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

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

**4.41. 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.

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

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

**4.44. Megjegyzés.** A Kőnig-tétel bizonyítása hatékony algoritmust ad maximális elemszámu 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 vázolata:

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

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

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

## 5. ABSZTRAKT ALGEBRA

### 5.1. Műveletek, algebrai struktúrák

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

$$f: A^n \rightarrow A, (a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$$

leképezést értünk.

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

**5.3. 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.

**5.4. Megjegyzés.** Ha a műveletek világosak a szöveggörnyezetből, akkor az algebrát és a tartóhalmazát nem mindig különböztetjük meg élesen egymástól.

**5.5. 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.

**5.6. 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  $a * c = b * c \implies a = b$  és  $c * a = c * b \implies a = b$ .

**5.7. 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**.

**5.8. 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.

**5.9. 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:  $a^{-1}$ ).

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

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

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

Az izomorfizmus hasonlóan definiálható tetszőleges algebrák (nem csak grupoidok) esetén (lásd az 5.29. Megjegyzést).

**5.12. Tétel.** Izomorfizmusok szorzata és inverze is izomorfizmus.

**5.13. Következmény.** Az izomorfia ekvivalenciareláció (grupoidok bármely halmazán).

**5.14. 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).

## 5.2. Részalgebra, generálás

**5.15. Definíció.** A  $B \subseteq A$  részhalmaz **zárt** az  $f: A^n \rightarrow A$  műveletre, ha  $f(b_1, \dots, b_n) \in B$  minden  $b_1, \dots, b_n \in B$  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  $\mathbb{A} = (A; F)$  algebraiban, akkor az  $F$ -beli műveletek megszorításaival egy  $\mathbb{B}$  algebrát alkot, amelyet **részalgebrájának** nevezünk. Jelölés:  $\mathbb{B} \leq \mathbb{A}$ .

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

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

**5.18. Definíció.** Az  $\mathbb{A}$  algebraiban 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.

**5.19. Megjegyzés.** Az 5.17. Tétel garantálja, hogy valóban létezik a  $B$ -t tartalmazó zárt halmazok között egy legszűkebb, nevezetesen a  $B$ -t tartalmazó összes zárt halmazok metszete.

**5.20. 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.

### 5.3. Kongruencia, faktoralgebra

**5.21. 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  $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in A$  elemek esetén

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

**5.22. 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  $C_1, C_2, \dots, C_n \in \mathcal{C}$  osztályok esetén létezik egy olyan (egyértelműen meghatározott)  $D \in \mathcal{C}$  osztály, amelyre

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

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

**5.24. 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.

**5.25. Definíció.** Legyen  $\sim$  kongruenciarelációja az  $\mathbb{A}$  algebrának. Minden  $f \in F$  ( $n$ -változós) művelet és tetszőleges  $C_1, C_2, \dots, C_n \in A/\sim$  osztályok esetén jelölje  $f(C_1, C_2, \dots, C_n)$  azt a  $D \in A/\sim$  osztályt, amelyre  $f(c_1, c_2, \dots, c_n) \in D$  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:  $\mathbb{A}/\sim$ .

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

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

$$f(\bar{c}_1, \bar{c}_2, \dots, \bar{c}_n) = \overline{f(c_1, c_2, \dots, c_n)}.$$

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

### 5.4. Homomorfizmus, homomorfiatétel

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

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

Ha létezik  $\varphi: \mathbb{A} \rightarrow \mathbb{B}$  szürjektív homomorfizmus, akkor azt mondjuk, hogy  $\mathbb{B}$  **homomorf képe**  $\mathbb{A}$ -nak. Speciális homomorfizmusok:

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

**5.29. 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  $\varphi: A \rightarrow B$  leképezés akkor gyűrűhomomorfizmus, ha minden  $a_1, a_2 \in A$  esetén

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

**5.30. Tétel.** Homomorfizmusok szorzata is homomorfizmus.

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

$$\nu: \mathbb{A} \rightarrow \mathbb{A}/\sim, \quad a \mapsto \bar{a}$$

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

**5.32. Definíció.** A  $\varphi: A \rightarrow B$  leképezés **magján** az alábbi  $\ker \varphi$  ekvivalenciarelációt értjük:

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

**5.33. Tétel (Homomorfiatétel).** Ha  $\varphi: \mathbb{A} \rightarrow \mathbb{B}$  homomorfizmus, akkor...

- (a)  $\mathbb{A}/\ker \varphi \cong \mathbb{B}$ , azaz  $\varphi$  értékkészlete részalgebrája  $\mathbb{B}$ -nek;
- (b)  $\ker \varphi$  kongruenciája  $\mathbb{A}$ -nak;
- (c)  $\mathbb{A}/\ker \varphi \cong \mathbb{A}/\ker \varphi$ , azaz a mag szerinti faktoralgebra izomorf a homomorf képpel.

**5.34. Következmény (Homomorfiatétel).** Ha  $\varphi: \mathbb{A} \rightarrow \mathbb{B}$  szürjektív homomorfizmus, akkor  $\mathbb{A}/\ker \varphi \cong \mathbb{B}$ .

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

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

### 5.5. Direkt szorzat

**5.36. 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:

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

**5.37. Megjegyzés.** Ha az algebraknak nem csak egy műveletük van, akkor minden műveletet komponensenként értelmezzük. 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

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

**5.38. Tétel.** Az alábbi leképezések (**projekciók**) szűrjektív homomorfizmusok:

$$\pi_1: \mathbb{A} \times \mathbb{B} \rightarrow \mathbb{A}, \quad (a, b) \mapsto a;$$

$$\pi_2: \mathbb{A} \times \mathbb{B} \rightarrow \mathbb{B}, \quad (a, b) \mapsto b.$$

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

## 6. CSOPORTOK

### 6.1. A csoport fogalma, példák, alaptulajdonságok

**6.1. Definíció.** **Csoportnak** nevezünk egy  $(A; *)$  grupoidot, ha

- \* asszociatív:  $\forall a, b, c \in A: (a * b) * c = a * (b * c)$ ;
- létezik egységelem:  $\exists e \in A \quad \forall a \in A: a * e = e * a = a$ ;
- minden elemnek van inverze:  $\forall a \in A \quad \exists b \in A: a * b = b * a = e$ .

**6.2. 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.

**6.3. Példák.** Néhány fontos példa csoportra:

- $(\mathbb{C}; +)$ ,  $(\mathbb{R}; +)$ ,  $(\mathbb{Q}; +)$ ,  $(\mathbb{Z}; +)$ ,  $(\{0\}; +)$ ,  $(\{\text{páros számok}\}; +)$ , ...;
- $(T^{n \times m}; +)$  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);
- $(\text{GL}_n(T); \cdot)$ , ahol  $\text{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}$  (a  $T$  test feletti  $n$ -dimenziós általános lineáris csoport);
- $(\mathbb{Z}_n^*; \cdot)$  tetszőleges  $n \in \mathbb{N}$  esetén;
- $(S_n; \cdot)$ , ahol  $S_n = \{f: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ bijekciók} \}$  (az  $n$ -edfokú szimmetrikus csoport);
- (síkbeli vagy térbeli) alakzatok szimmetriacsoportjai.

### 6.4. Tétel.

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

### 6.5. 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.

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

$$a \cdot x_1 = a \cdot x_2 \quad \implies \quad x_1 = x_2;$$

$$y_1 \cdot a = y_2 \cdot a \quad \implies \quad y_1 = y_2.$$

**6.7. Megjegyzés.** Az invertálhatóság azt jelenti, hogy a művelet táblázat 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.

**6.8. Tétel.** Csoport művelete mindig invertálható és kancellatív.

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

**6.10. 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.

**6.11. 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  $a_1 \cdot \dots \cdot a_n$  „szorzat” eredménye független a zárójelvezéstől.

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

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

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

## 6.2. Részcsoportok

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

**6.15. 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 ( $G \rightarrow G, a \mapsto a^{-1}$ ), az egységelemet pedig nullváltozós műveletnek. Ha ezeket is bevesszük az alpműveletek közé, akkor a  $(G; \cdot, ^{-1}, 1)$  algebrát kapjuk, és ennek a részalgebrái már épp a részcsoportok.

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

- (1)  $H$  zárt a szorzásra:  $\forall h_1, h_2 \in H: h_1 \cdot h_2 \in H$ ;
- (2)  $H$  tartalmazza  $G$  egységelemét:  $1 \in H$ ;
- (3)  $H$  zárt az inverzképzésre:  $\forall h \in H: h^{-1} \in H$ .

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

**6.18. 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.

**6.19. Megjegyzés.** Az 5.17. Tételt alkalmazva a  $(G; \cdot, ^{-1}, 1)$  algebrára, látható, hogy részcsoportok metszete is részcsoport (lásd a 6.15. Megjegyzést). Ez garantálja, hogy valóban létezik a  $B$ -t tartalmazó részcsoportok között egy legszűkebb, nevezetesen a  $B$ -t tartalmazó összes részcsoportok metszete.

**6.20. 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.

## 6.3. Ciklikus csoportok, elem rendje

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

**6.22. Tétel.** Ciklikus csoport minden részcsoportja is ciklikus.

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

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

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

**6.25. 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*):

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

**6.26. Definíció.** A  $G$  csoport **rendjén** elemeinek számát (számosságát) értjük.

**6.27. Megjegyzés.** Az  $a$  elem rendje nem más, mint az általa generált részcsoporthoz tartozó  $o(a) = |[a]|$ .

**6.28. Megjegyzés.** Tetszőleges  $z \in \mathbb{C} \setminus \{0\}$  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:  $E_n \cong \mathbb{Z}_n$ .)

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

- (1)  $\forall k, \ell \in \mathbb{Z}: a^k = a^\ell \iff k \equiv \ell \pmod{n}$ ;
- (2)  $a^{-1} = a^{n-1}$ ;
- (3)  $\forall k \in \mathbb{Z}: a^k = 1 \iff n \mid k$ ;
- (4)  $n$  osztója  $G$  elemszámának;
- (5)  $a^{|G|} = 1$ .

**6.30. Tétel.** Minden prírendű csoport ciklikus.

**6.31. 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:  $\mathbb{Z}_5$ .

#### 6.4. Mellékosztályok, Lagrange tétele

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

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

Egyelemű komplexusok esetén az alábbi egyszerűsített jelölést használjuk:

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

**6.33. Tétel.** Egy  $H \subseteq G$  komplexus akkor és csak akkor részcsoporthoz tartozó, ha

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

**6.34. 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.

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

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

**6.36. 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  $Ha$ .

**6.37. 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.

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

**6.39. Tétel (Lagrange tétele).** Tetszőleges  $G$  véges csoport és  $H$  részcsoporthoz tartozó esetén

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

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

## 6.5. Normálosztók, faktorcsoporthok

**6.40. Definíció.** Az  $N \leq G$  részcsoporthot **normálosztónak** nevezzük, ha az  $N$  szerinti bal és jobb oldali mellékosztályozás megegyezik:  $\forall a \in G: aN = Na$ . Jelölés:  $N \triangleleft G$ .

**6.41. Megjegyzés.** Abel-csoportban minden részcsoporth normálosztó.

**6.42. Tétel.** Ha  $N \triangleleft G$ , akkor az  $N$  szerinti mellékosztályozás kompatibilis osztályozása a  $G$  csoportnak. A megfelelő kongruencia szerinti faktoralgebra csoport, amelyet a  $G$  csoport  $N$  normálosztó szerinti **faktorcsoporthjának** nevezünk. Jelölés:  $G/N$ .

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

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

## 6.6. Direkt szorzat

**6.45. Definíció.** Az  $G$  és  $H$  csoportok **direkt szorzata** a  $G \times H$  csoport, amelynek műveletét az alábbi módon értelmezzük:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2) \quad (g_1, g_2 \in G, h_1, h_2 \in H).$$

**6.46. Tétel.** Csoportok direkt szorzata valóban csoport.

**6.47. 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:

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

Ez nemcsak csoportizomorfizmus, hanem gyűrűizomorfizmus is.

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

**6.49. Tétel** (A véges Abel-csoportok alaptétele). Minden véges Abel-csoport prímszorzattal felbontható ciklikus csoportok direkt szorzatára bontható.

**6.50. Tétel.** Ha az  $M, N \triangleleft G$  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.