Számelmélet, kémia és (multi)halmazok

Haladvány Kiadvány 230201

Szalkai István
Pannon Egyetem, Matematika Tanszék, Veszprém
SZALKAI.ISTVAN@MIK.UNI-PANNON.HU

Haladvány Kiadvány , http://math.bme.hu/~hujter/230201.pdf

0. Bevezetés

Elsősorban nem új eredményeket, hanem inkább új szemléletmódot kívánunk ismertetni, amellyel a diákok jobban megismerhetik az egész számok elméletét, kevesebb hibát vétenek következtetéseikben, mint például a (13) összefüggést is gyakran eltévesztik.

Ennek ellenére az Olvasó érdekességet, újdonságot, például a (37) összefüggést:

$$\boxed{lkkt(a,b,c)=\frac{a\cdot b\cdot c\cdot lnko\,(a,b,c)}{lnko\,(a,b)\cdot lnko\,(a,c)\cdot lnko\,(b,c)}\ ,}$$

vagy az egész 5. fejezetet, és talán még hasznosat is talál jelen cikkünkben.

A témához kapcsolódóan ajánlom még [10] cikkemet:

$$lnko\,(lkkt[a,b], lkkt[b,c], lkkt[c,a]) = lkkt\,[lnko(a,b), lnko(b,c), lnko(c,a)]$$

halmazműveletekkel azonos

$$(a\cup b)\cap(b\cup c)\cap(c\cup a) = (a\cap b)\cup(b\cap c)\cup(c\cap a)\ \ ,$$

valamint [9] könyvemet és a KöMaL [4] feladatát.

Ismertnek tételezzük fel a halmazelméleti $(\cup,\cap,\text{-},\emptyset)$, számelméleti (prímek, oszthatóság, *lnko* és *lkkt*) és kémiai (atom, mulekula) alapfogalmakat, a *Boole algebrák* ismerete azonban nem szükséges.

Mi csak pozitív számokkal foglalkozunk, bár a negatív számok és a 0 érdekes meglepetéseket tartogatnak[1)], 1 *egység* és hangsúlyozottan *nem prímszám*. *lnko* és *lkkt* elemi tulajdonságait például [3] és [5] is felsorolja (325.o. (8)-(12)). $\mathbb{N}$ jelöli a természetes számok, $\mathbb{P}$ a prímszámok halmazát. Ebben a cikkben a 0 sajnos (természetesen) *nem* természetes szám, $0 \notin \mathbb{N}$, vele mindig külön kell foglalkoznunk!

Meglepő módon *lnko* és *lkkt* -t nem csak törtek közös nevezőre hozásakor és lineáris Diophantikus egyenletek megoldásakor használjuk: Knuth [5] könyvében rengeteg más (nem csak számítástechnikai) alkalmazást ismertet részletesen[2)].

1. Alapok

Mint tudjuk, a *prímszámok* tovább már nem oszthatók és belőlük (szorzással) minden természetes szám (egyértelműen) felírható. Tehát ők *a számok atomjai*, vagyis építőkövei! Hiszen a görög "**atom**" szó elején az "*a*-" előtag a tagadás jele, a "$\tau o \mu \acute{\eta}$" ("tomosz") szó pedig "vágni", "darabolni", vagyis tényleg "atom" (ó-görögösen: atomosz) = "oszthatatlan" [3)].

Tehát, a molekulákkal megegyző módon, minden természetes számot tekinthetünk az őt alkotó prímszámok (multi) halmazának[4)]. Például: $76 = 2 \cdot 2 \cdot 19$ helyett írhatnánk, hogy $76 = \{2, 2, 19\}$, mint ahogy VIZ = {H,H,O} mert hiszen VIZ = H_2O = H✠H✠O ahol ✠ a megfelelő kémiai kötés. A prímszámokat a szorzás köti össze.

Így kiindulópontunk a következő táblázat (szótár):

H	He	Li	Be	B	C	N	O	F	Ne	Na	Mg	Al	Si	P	S	Cl	Ar	...
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	...

1. Táblázat: *Kémiai prímek és számelméleti atomok*

(Érdekes matematikai-kémiai kutatás lehetne a prímszámok periodikus és kémiai (matematikai) tulajdonságainak vizsgálata[5)]).

[1)] Pl. $v \mid 0$, $0 \mid 0$, $lnko(0, v) = v$ ha $v \neq 0$ és $lkkt(0, w) = 0$ ha $w \geq 0$, de $lnko(0, 0)$ értelmezhetetlen, stb.

[2)] Például: véletlen számok generálása (3.2.1.2.), statisztikai elméleti próbák (3.3.3.), moduláris aritmetika (4.3.2.), milyen gyorsan tudunk szorozni (4.3.3.), stb. .

[3)] ld.pl. https://hu.wikipedia.org/wiki/Atom , https://hu.wikipedia.org/wiki/Démokritosz https://en.wikipedia.org/wiki/Atom , https://de.wikipedia.org/wiki/Atom

[4)] A *multihalmazokkal* a következő alfejezetben kicsit részletesebben foglalkozunk.

[5)] Pl. végtelen sok van, eloszlásuk $\pi(x) \sim \frac{x}{\ln(x)}$, különbözű / azonos tulajdonságú prímek, periodikusság (?), stb. **Megjegyezzük**, hogy a kémiai atomok (elméletileg lehetséges) halmaza is végtelen!

Szóval, *prímszámok* $\Longleftrightarrow$ *atomok = egyatomos molekulák* , és *összetett számok* $\Longleftrightarrow$ (összetett) *molekulák*. De mi felel meg az 1 természetes számnak? Természetesen egy olyan molekula, amelyben egyetlen atom sincs, vagyis az üres molekula (azaz üres halmaz).

A továbbiakban haszos lesz a következő jelölés:

0. Jelölés: Tetszőleges a természetes szám vagy kémiai atom/molekula esetén jelölje $\mathfrak{p}\,(a)$ az a -t alkotó prímszámok illetve atomok (multi)halmazát. $\square$

Például: $\mathfrak{p}\,(76) = \{2, 2, 19\}$, $\mathfrak{p}\,(7) = \{7\}$, $\mathfrak{p}(\text{VIZ}) = \{\text{H,H,O}\}$, $\mathfrak{p}\,(1) = \{\,\} = \emptyset$, stb.

A későbbiekben néha egyszerűen csak a -t írunk $\mathfrak{p}\,(a)$ helyett.

Multihalmazok

Ha valaki nem kíváncsi a multihalmazok mibenlétének részletes boncolgatására, vagy túl nehéz számára a precíz matematikai definíció, akkor nyugodtan ugorjon az "Alaptulajdonságok" *alfejezethez* !

Mint láttuk, a (legtöbb) természetes számnak / molekulának ugyanazon prímosztója többször / több példányban is szerepelhet, ezért $\mathfrak{p}\,(a)$ nem közönséges halmaz. Mik is ezek a "*multihalmazok*"? Olyan "halmazok", amelyekben több elem is lehet azonos. Pontosabban**:** ezek az elemek (atomok, prímszámok, biliárdgolyók) fizikailag különbözőek, csak mi nem akarjuk megkülönböztetni őket (pedig az egyik H atom egészen más irányban mozog, mint a másik ...). Azonban a világban rengeteg H atom van, az általunk vizsgált vízmolekulán kívül is, sőt vízmolekulából is rengeteg, fizikailag különböző van, amiket mind mi (lustaságból?) azonosnak tekintünk. Igen ám, de a 76 "nevű" természetes számból nem létezik több, míg $\mathfrak{p}\,(76)$ -ban több 2 atom szerepel.

Van még egy különbség a fizikai világ (atomok, molekulák) és a természetes számok, prímszámok között. Amikor leírjuk, hogy $a \in A$ és $a \in B$, akkor a világ ("univerzum") *egyetlen*, ugyanazon a elemére gondolunk, vagy az A -beli és B -beli a atom különböző is lehet? Az anyagi világ atomjainál a lehet különböző A -ban és B -ben, míg a természetes számoknál ugye nem. Ez nagyon lényeges kérdés!

Ugyanis "*hagyományos*" *halmazok esetében*

$$a \in A \;\&\; a \in B \iff a \in A \cap B\ , \tag{1}$$

és ugyanez igaz a természetes számoknál is (lásd még (8), (9), (19)), míg az anyagi világban A és B diszjunkt (elkülönült) is lehet (1) esetén, hiszen "a" két, fizikailag különböző valami is lehet, mindkettőjüket a -vel jelöljük (pl. két H atom).

A multihalmazok definiálásához kiindulópontuk a "hagyományos" halmazok következő (naiv, precízkedő) definíciója lehet:

1. Definíció: Rögzített egy $U = \{u_1, u_2, ...\}$ *univerzum*[6] ("alaphalmaz"), melynek u_i elemei mind különbözőek. Ekkor egy tetszőleges A **halmaz** a következő: $A \subset U$, vagyis

(i) minden $a \in A$ esetén $a \in U$, és

(ii) minden $u \in U$ esetén egyértelműen vagy $u \in A$ vagy $u \notin A$. □

Tehát:

2. Definíció: Rögzített egy $U = \{u_1, u_2, ...\}$ *univerzum* ("alaphalmaz"), más jelöléssel $U = \{u_i \mid i \in I\}$, melynek u_i elemei mind különbözőek. Ekkor egy tetszőleges A **multihalmaz** egy $A_m = (A, m)$ alakú *rendezett pár*, ahol $A \subset U$ az 1. Definíció szerint, és $m : A \to \mathbb{N}$ tetszőleges függvény, melyet **multiplicitás**nak ("többszörösségnek") nevezünk. □

Az Olvasó már kitalálta, hogy $m\,(a)$ mondja meg pontosan, hogy az $a \in A$ elem *hányszor* szerepel az a molekulában / természetes számban. Ne feledjük, hogy m -nek az egész A halmazon kell értelmezve lennie, $Dom\,(m) = A$ és $0 < m\,(a)$ ha $a \in A$. Az $A = \emptyset$ eset sem nehéz, $Dom\,(m) = \emptyset$ megengedett.

Feltevésünk szerint azonban $0 \notin \mathbb{N}$, vagyis $m\,(a) > 0$ mindig.

A mi esetünkben (számelmélet) $U = \mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, ...\}$ a prímszámok halmaza, és a $76 = \{2, 2, 19\}$ számnak az $A_{76} = \{2, 19\}$ halmaz felel meg az $m\,(2) = 2$ és $m\,(19) = 1$ multiplicitásokkal.

Általában pedig az $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$ természetes számnak az $A_n = \{p_1, p_2, ..., p_t\}$ halmaz felel meg[7] az $m\,(p_i) = \alpha_i$, $i = 1, 2, ..., t$ multiplicitásokkal.

Feltételeink szerint $m\,(a) \neq 0$ ha $a \in A$. Módosíthatnánk a definíciót úgy is, hogy megengednénk az $m\,(a) = 0$ esetet is, amikor $a \notin A$, de ez nem egyszerűsítené további munkánkat.

A továbbiakban A_m vagy (A, m) helyett néha egyszerűen csak A -t írunk, nem okoz félreértést.

Emlékeztetjük az Olvasót: gráfelméletben a *többszörös* ("multiple") *éleket* tartalmazó gráfokat is a 2. Definícióhoz hasonlóan definiáljuk (pl. [6]). Sajnálatos módon, ha egy többszörös élt több különböző élnek kellene tekintenünk (mint például két helység között több út), akkor a definíciót még tovább kellene bonyolítanunk. Szerencsére a számelméletben csak arról van szó, hogy egyazon prímszámra többször van szükségünk.

---

[6] vagy még "precízebben": $U = \{u_i \ : \ i \in I\}$

[7] pontosabban az $n = \prod_{i \in I} p_i^{\alpha_i}$ és $A = \{p_i \mid i \in I\}$ jelöléseket kellene használnunk, hiszen minden számban más és más prímszámok szerepelnek, míg a $\mathbb{P}$ alaphalmazban $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ...

Érdemes észrevennünk, hogy A akkor és csak akkor hagyományos halmaz ha $m(a) = 1$ minden $a \in A$ esetén, és persze a hagyományos halmazokat is hívhatjuk (nagyképűen) multihalmazoknak.

Fontos tény, hogy $a \in \mathbb{N}$ természetes számokra $\mathfrak{p}(a)$ pontosan akkor hagyományos halmaz, ha a *négyzetmentes* szám ($1 < x$ esetén $x^2 \nmid a$, vagyis a prímfelbontásában mindegyik prímszám kitevője 1).

A multihalmazokat néha "gót" (Fraktur) betűtípussal[8)] jelöljük, mint például $\mathfrak{p}(76) = \{2, 2, 19\}$. Sajnos magyar nyelvű wikipédia nincs a multihalmazokról, csak angol: https://en.wikipedia.org/wiki/Multiset .

Műveletek

A továbbiakban $A_m = (A, m)$ és $B_n = (B, n)$ multihalmazok a 2. Definíció értelmében. Az új, multihalmaz műveletekre a $\mathring{\cup}$, $\mathring{\cap}$, $\mathring{\subset}$ jeleket használjuk, attól függetlenül, hogy azok néha megegyeznek a hagyományos halmazműveletekkel.

Kezdjük az egyszerűbb, egyértelmű műveletekkel.

3. Definíció: Üres multihalmaz: $A_m = \mathring{\emptyset}$ pontosan $A_m = (\emptyset, m)$, ahol m az üres függvény, vagyis lényegében a hagyományos üres halmaz: $\mathring{\emptyset} = \emptyset$.

Részhalmaz (tartalmazás) : $A_m \mathring{\subset} B_n$ nyilvánvalóan pontosan akkor, ha $A \subset B$ és minden $a \in A$ esetén $m(a) \leq n(a)$.

Metszet (közös rész): $C_k = (C, k) = A_m \mathring{\cap} B_n$ ahol $C = A \cap B$ és minden $c \in C$ esetén $k(c) = \min\{m(c), n(c)\}$.

A_m és B_n **diszjunktak** (idegenek), ha $A_m \mathring{\cap} B_n = \mathring{\emptyset}$. $\square$

Az únió (egyesítés) már nehezebb feladat: A_m és B_n "összeöntésekor" az elemeket mind (fizikailag) különbözőnek tekintjük és egyesítjük őket ($\biguplus$), vagy csak a *szükséges* darabszámot (m és n alapján) emeljük meg a közös szintre ($\mathring{\cup}$). Mindkettő műveletre szükségünk lesz.

4. Definíció: Unió (egyesítés):

$C_k = (C, k) = A_m \mathring{\cup} B_n$ ahol $C = A \cup B$ és minden $c \in C$ esetén

$k(c) = \max\{m(c), n(c)\}$.

$D_\ell = (D, \ell) = A_m \biguplus B_n$ ahol $D = A \cup B$ és minden $d \in D$ esetén

$\ell(d) = m(c) + n(c)$. $\square$

5. Definíció: Kivonás (összhangban legyen a hagyományos halmaz- és számelméleti műveletekkel, lásd a 11. Állítást is):

[8)] $\mathfrak{a}\ \mathfrak{b}\ \mathfrak{c}\ \mathfrak{d}\ \mathfrak{e}\ \mathfrak{f}\ \mathfrak{g}\ \mathfrak{h}\ \mathfrak{i}\ \mathfrak{j}\ \mathfrak{k}\ \mathfrak{l}\ \mathfrak{m}\ \mathfrak{n}\ \mathfrak{o}\ \mathfrak{p}\ \mathfrak{q}\ \mathfrak{r}\ \mathfrak{s}\ \mathfrak{t}\ \mathfrak{u}\ \mathfrak{v}\ \mathfrak{w}\ \mathfrak{x}\ \mathfrak{y}\ \mathfrak{z}\ \ \mathfrak{A}\ \mathfrak{B}\ \mathfrak{C}\ \mathfrak{D}\ \mathfrak{E}\ \mathfrak{F}\ \mathfrak{G}\ \mathfrak{H}\ \mathfrak{I}\ \mathfrak{J}\ \mathfrak{K}\ \mathfrak{L}\ \mathfrak{M}\ \mathfrak{N}\ \mathfrak{O}\ \mathfrak{P}\ \mathfrak{Q}\ \mathfrak{R}\ \mathfrak{S}\ \mathfrak{T}\ \mathfrak{U}\ \mathfrak{V}\ \mathfrak{W}\ \mathfrak{X}\ \mathfrak{Y}\ \mathfrak{Z}$

$C_k = (C,k) = A_m \mathring{\setminus} B_n \quad$ ahol $\quad C = \{a \in A : m(c) > n(c)\}$
és minden $c \in C$ esetén $k(c) = m(c) - n(c)$. $\quad \square$

Többek között nyilván $C \subset A$ és $C_k \mathring{\subset} A_m$.

Megjegyezzük még, hogy a fenti műveletekben és $\mathring{\subset}$ -ben $m(a) = 0$ *nem* lehetséges, de $A_m = \mathring{\emptyset}$ előfordulhat. Hagyományos halmazokra $\mathring{\cup}$, $\mathring{\cap}$, $\mathring{\subset}$ megegyezik a hagyományos $\cup$, $\cap$, $\subset$ műveletekkel és relációval, de $\bigcup$ csak diszjunkt hagyományos halmazok esetén létezik.

Az **alaphalmaz** és a **komplementer** művelet megválasztásának kérdése nehéz, részletesen a 4. "*Boole - algebra axiómák*" fejezetben foglalkozunk vele.

Ezek után már könnyen megfogalmazhatjuk a fenti műveletek (kémia) és a számelmélet alapvető kapcsolatait.

Alaptulajdonságok

6. Állítás: Tetszőleges $a, b \in \mathbb{N}$ természetes számokra

$$\mathfrak{p}(a) \mathring{\subset} \mathfrak{p}(b) \iff a \mid b \,, \tag{2}$$

$$\begin{aligned} \mathfrak{p}(a) \mathring{\cap} \mathfrak{p}(b) &= \mathfrak{p}(lnko(a,b)) \,, & (3)\\ \mathfrak{p}(a) \mathring{\cup} \mathfrak{p}(b) &= \mathfrak{p}(lkkt(a,b)) \,, & (4)\\ \mathfrak{p}(a) \bigcup \mathfrak{p}(b) &= \mathfrak{p}(a \cdot b) \,, & (5) \end{aligned}$$

továbbá $\mathfrak{p}(a)$ és $\mathfrak{p}(b)$ multi-**diszjunktak** (idegenek) akkor és csak akkor ha a és b **relatív** ("viszonylagos") **prímek** (azaz $lnko(a,b) = 1$, vagyis nincs közös prímosztójuk[9]), hiszen $\mathfrak{p}(1) = \emptyset$. Bár ez következik (3) -ból, érdemes jelentését átgondolnunk.

Ezen összefüggéseket érdemes a diákoknak szóban is megmagyaráznunk, például:

" $a \mid b$ pontosan akkor, ha a *összes* prímosztója megtalálható (multiplicitással) b prímosztói között, "

" $lnko(a,b)$ -ban a *közös* prímosztók szerepelnek a *közös* multiplicitásnak megfelelően, "

" $lkkt(a,b)$ -ban a és b prímosztói is mind belefférnek (külön-külön), "

" $a \cdot b$ -ben pedig a és b összes prímosztóját felhasználjuk, mintha (fizikailag) különbözőek lennének. "

[9] A relatív ("viszonylagos") jelző azt jelenti, hogy a nézőpontjából b prím és fordítva, b nézőpontjából a is prím: $(\forall p \in \mathbb{P})\ (p \mid a \implies p \nmid b)$ és $(\forall q \in \mathbb{P})\ (q \mid b \implies q \nmid a)$.

7. Következmény:

$$\mathfrak{p}\,(a\cdot b)=\mathfrak{p}\,(a)\bigcup\mathfrak{p}\,(b)=$$
$$(\mathfrak{p}\,(a)\,\mathring{\cup}\mathfrak{p}\,(b)\,)\bigcup(\mathfrak{p}\,(a)\,\mathring{\cap}\mathfrak{p}\,(b)\,)=\ \mathfrak{p}\,(lkkt\,(a,b))\bigcup\mathfrak{p}\,(lnko\,(a,b))$$

azaz

$$\boxed{a\cdot b=\ lkkt(a,b)\cdot\ lnko(a,b)} \tag{6}$$

ami megfelel (prímkitevőkre gondolva) az

$$\boxed{\alpha{+}\beta{=}\Big(\min\,(\alpha,\beta)\Big){+}\Big(\max\,(\alpha,\beta)\Big)} \tag{7}$$

összefüggésnek. □

8. Továbbá nyilván $\mathfrak{p}\,(a)=\emptyset\iff a=1$, és

$$a\mid b\iff\mathfrak{p}\,(a)\,\mathring{\subseteq}\mathfrak{p}\,(b)\ , \tag{8}$$

vagyis " a osztója b -nek $\iff$ részmolekulája".

Ez nagyon hasznos a következő összefüggésekben (amit a diákok mindig eltévesztenek).

9. Következmény

$$\boxed{x\mid a\ \acute{e}s\ x\mid b\iff x\mid lnko(a,b)} \tag{9}$$

hiszen hagyományos- és multihalmazoknál

$$X\mathring{\subset}A\ \acute{e}s\ X\mathring{\subset}B\iff X\mathring{\subset}A\mathring{\cap}B\ , \tag{10}$$

de természetesen

$$\boxed{x\mid a\ \acute{e}s\ x\mid b\not\Leftarrow x\mid lkkt(a,b)} \tag{11}$$

hiszen

$$X\mathring{\subset}A\ \acute{e}s\ X\mathring{\subset}B\not\Leftarrow X\mathring{\subset}A\mathring{\cup}B\ . \tag{12}$$

Az általános és közép iskolában gyakran eltévesztik az alábbi következtetést, pedig (8) alapján könnyen belátható:

10. Állítás:

$$\boxed{a_1\mid b\ \acute{e}s\ a_2\mid b\iff lkkt(a_1,a_2)\mid b} \tag{13}$$

hiszen

$$A_1\mathring{\subset}B\ \acute{e}s\ A_2\mathring{\subset}B\iff A_1\mathring{\cup}A_2\mathring{\subset}B\ , \tag{14}$$

és nem több, tehát, mint tudjuk, általában:

$$\boxed{a_1 \mid b \text{ és } a_2 \mid b \;\not\Rightarrow\; a_1 \cdot a_2 \mid b} \;, \tag{15}$$

hiszen hagyományos és multi halmazoknál is:

$$A_1 \subseteqq B \text{ és } A_2 \subseteqq B \text{ -ből} \quad \text{csak} \quad A_1 \cup A_2 \subseteqq B \quad \text{következik,}$$

($\subseteqq$ és $\cup$ helyett $\mathring{\subseteqq}$ és $\mathring{\cup}$ is írható), vagyis az $A_1 \cap A_2$ metszet nem szerepel kétszer B -ben, *de* $\bigcup$ már nem írható:

$$A_1 \mathring{\subseteqq} B \text{ és } A_2 \mathring{\subseteqq} B \quad \not\Rightarrow \quad A_1 \bigcup A_2 \mathring{\subseteqq} B \;.$$

□

Ha azonban a_1 és a_2 *relatív prímek*: $lnko(a_1, a_2) = 1$, vagyis $\mathfrak{p}(a_1) \mathring{\cap} \mathfrak{p}(a_2) = \mathring{\emptyset}$ (diszjunktak), akkor $\mathfrak{p}(a_1) \bigcup \mathfrak{p}(a_2) = \mathfrak{p}(a_1) \mathring{\cup} \mathfrak{p}(a_2)$, és így (13) alapján $a_1 \cdot a_2 \mid b$. **De csak ekkor !**

11. Állítás: Tetszőleges a, b számokra

$$\mathfrak{p}(b) \mathring{\setminus} \mathfrak{p}(a) = \mathfrak{p}\left(\frac{b}{lnko(a,b)}\right) \;, \tag{16}$$

ami megfelel a jólismert

$$B \setminus A = B \setminus (A \cap B) \tag{17}$$

összefüggésnek.

Speciálisan: $a \mid b$, azaz $\mathfrak{p}(a) \mathring{\subset} \mathfrak{p}(b)$ (vagyis $A \subseteqq B$) esetén $lnko(a, b) = a$, tehát

$$\mathfrak{p}(b) \mathring{\setminus} \mathfrak{p}(a) = \mathfrak{p}\left(\frac{b}{a}\right) \;, \tag{18}$$

hiszen b -ből kivesszük az a *részmolekulát* (például a kristályvizet). □

lnko* és *lkkt

Vizsgáljuk meg $\mathfrak{p}(a) \hat{\cap} \mathfrak{p}(b)$ -t közelebbről. Ez a két molekula (a és b) *közös* atomjainak a maximuma, a legnagyobb közös rész-molekulájuk, vagyis a *legnagyobb közös osztó*[10]:

$$\mathfrak{p}(lnko(a,b)) = \mathfrak{p}(a) \hat{\cap} \mathfrak{p}(b) \ . \tag{19}$$

Ha a közös prímszámok kitevőire, vagy a közös atomok számára gondolunk (ami 0 is lehet), $\min(\alpha, \beta)$ jut eszünkbe, hiszen az előforduló prímek kitevőinek legnagyobb közös, vagyis minimumáról van szó. Ezt a kapcsolatot a 4. fejezetben a Boole algebrák címszó alatt folytatjuk.

Mivel a $\hat{\cap}$, *lnko* és *min* kapcsolata mélyebb, mint csupán (19), és hasonlóan $\mathring{\cup}$, *lkkt* és *max* is közeli rokonok, érdemes bevezetnünk $\hat{\cap}$ és $\mathring{\cup}$ -hez hasonló jeleket.

12. Jelölés: Tetszőleges $a, b \in \mathbb{N}$ természetes számokra legyen[11]

$$a \sqcap b := lnko(a,b) \quad \text{és} \quad a \sqcup b := lkkt(a,b) \ . \tag{20}$$

Ha a szövegkörnyezetből kiderül, akkor a *min* és *max* műveletekre is használhatjuk a $\sqcap$ és $\sqcup$ jeleket:

$$a \sqcap b := \min(a,b) \quad \text{és} \quad a \sqcup b := \max(a,b) \ . \quad \square \tag{21}$$

Első hallásra furcsának tűnnek ezek a jelölések, de nagyon hasznosak. Például:

13. Állítás: A nem ismeretlen

$$lnko(a,b,c) = \boxed{lnko(lnko(a,b),c) = lnko(a, lnko(b,c))} \tag{22}$$

összefüggés második egyenlősége új jeleinkkel így írható:

$$\boxed{(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)} \ , \tag{23}$$

és hasonlóan:

$$lkkt(a,b,c) = \boxed{lkkt(lkkt(a,b),c) = lkkt(a, lkkt(b,c))} \tag{24}$$

és

$$\boxed{(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)} \ , \tag{25}$$

[10] amint ezt már (3) -ban is felírtuk

[11] [9] -ben $lnko(a,b)$ helyett $a \Delta b$, $lkkt(a,b)$ helyett az $a \nabla b$ jelölést használjuk.

amik az *asszociativitás* ("társíthatóság") összefüggései, és tényleg: (22) és (24) második egyenlősége valóban az asszociativitás összefüggés!

Vegyük észre: a $\cap$, $\cup$, $\hat{\cap}$, $\hat{\cup}$, $\sqcap$ és $\sqcup$ műveleti jeleket a változók *közé* írtuk ("infix" jelölés), amint a matematikában szokásos, míg az *lnko, lkkt, min, max* jeleket a változók *elé* ("prefix" jelölés), mint függvények esetében szokásos. Pedig nem a jelölés a lényeg!

Mivel mindegyik *kétváltozós művelet*, ezért javasolt az infix jelölés[12)].

Például írjuk át a KöMaL **B. 4493.** feladatát

$$lnko\left(lkkt[a,b], lkkt[b,c], lkkt[c,a]\right) = lkkt\left[lnko(a,b), lnko(b,c), lnko(c,a)\right] \qquad (26)$$

halmazműveletekre:

$$(a \cup b) \cap (b \cup c) \cap (c \cup a) = (a \cap b) \cup (b \cap c) \cup (c \cap a) \ , \qquad (27)$$

vagy pontosabban:

$$\left(a \hat{\cup} b\right) \hat{\cap} \left(b \hat{\cup} c\right) \hat{\cap} \left(c \hat{\cup} a\right) = \left(a \hat{\cap} b\right) \hat{\cup} \left(b \hat{\cap} c\right) \hat{\cup} \left(c \hat{\cap} a\right) \ . \qquad (28)$$

Talán így egyszerűbb a feladat megoldása! (Lásd a [10] cikket.)

Az $\cup$, $\hat{\cup}$, $\sqcup$ (*lkkt, max*), stb. műveletek közös alaptulajdonságaival (axiómák) és azok következményeivel a 4. "*Boole - algebra axiómái*" fejezetben foglalkozunk részletesen.

Diákoknak érdemes $lnko(a,b)$, $lkkt(a,b)$ és $a \cdot b$ jelentéseire (és a különbségekre) hétköznapi magyarázatot is adni: két molekula esetén megkeresni a legnagyobb megegyező rész molekulájukat, illetve *legkisebb* nagy molekula, *amiben* mindkettő megtalálható részmolekulaként, és végül: korlátozás nélkül csak összeragasztjuk a két molekulát. (Értsd: számelméleti atomok és kémiai prímszámok.) Szerintünk ez a számelméleti feladatoknál is segíthet.

14. Például:

$a \cdot b$ = összeolvasztás korlátozás nélkül, pl. kristályvíz $CuSO_4 + 5H_2O = CuSO_4 \sqcup 5H_2O =$ "$CuSO_9H_5$" , vagy a kémiai reakció: $2C \sqcup O_2 = 2CO_2 =$ "C_2O_4 ",

$lnko$: $CuSO_4 \sqcap 5H_2O = O_4$,

[12)] A prefix jelölés például a számítógépek programozásakor használt jelölés: általában egy kétváltozós (vagy egy- vagy többváltozós) függvényt / műveletet a FUNCTION NEV (változók) utasítással kell kezdenünk, és később a NEV (változók) utasítással használunk.

Számítástechnikában hasznos jelölés még a "postfix" jelölés, pl. $a + b$ helyett $(a, b) +$.

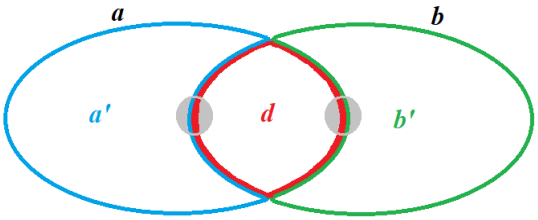
lkkt : $\mathrm{CuSO_4} \sqcup 5\mathrm{H_2O} = \mathrm{CuSO_5H_{10}}$ (((lehet, hogy kémiailag semmi értelme))).

Jegyezzük meg, hogy *lnko* és *lkkt* **megfelelnek** a min és max műveleteknek, hiszen $lnko(a,b)$ kiszámításakor a prímszámok a és b -beli hatványkitevőinek a minimumait, míg $lkkt(a,b)$ kiszámításakor a maximumait vesszük.

A cikk hátralevő részében felváltva fogjuk használni az $lnko(a,b)$, $a \sqcap b$, $a \cap b$ és $\min(a,b)$ jeleket, ahogyan épp kedvünk tartja (és hasonlóan $lkkt(a,b)$ -t is többféleképpen jelölgetjük). Az elmondottak nagy része min, max -ra is teljesül, jelezzük, ahol nem.

2. Két szám vizsgálata

Először vizsgáljuk meg még alaposabban két tetszőleges szám és *lnko* -juk kapcsolatát:



1. Ábra: $lnko(a,b)$

Nyilván $d = lnko(a,b)$, $a' = \dfrac{a}{d}$ és $b' = \dfrac{b}{d}$, vagyis $a = a' \cdot d$ és $b = b' \cdot d$, vagy halmaz- jelölésekkel: $\mathfrak{p}(a) = \mathfrak{p}(a') \mathring{\cup} \mathfrak{p}(d)$ és $\mathfrak{p}(b) = \mathfrak{p}(b') \mathring{\cup} \mathfrak{p}(d)$. Molekuláknál d a közös atomokat sorolja fel a a metszetben, utána a maradék molekulák a' és b'.

Mint tudjuk: $a' \cap b' = \emptyset$ és $a' \mathring{\cap} b' = \mathring{\emptyset}$ és $lnko(a',b') = 1$.

Azonban:

15. Vigyázat: A metszetben a (szándékosan) homályos szürke foltok arra figyelmeztetnek, hogy tetszőleges $a,b \in \mathbb{N}$ számokra *nem feltétlenül* teljesül a $\mathfrak{p}(a') \cap \mathfrak{p}(d) = \emptyset$ vagy a $\mathfrak{p}(b') \cap \mathfrak{p}(d) = \emptyset$, más jelekkel az $lnko(a',d) = 1$ vagy $lnko(b',d)$) összefüggés, hiszen a' -nek d -vel, és b' -nek d -vel lehetnek (valódi) közös osztói**!**

Például $a = 12 = 2^2 \cdot 3$ és $b = 18 = 2 \cdot 3^2$ esetében $d = lnko(a,b) = 6$, $a' = a/d = 2$ és $b' = b/d = 3$.

Vagyis: a *hagyományos halmazábrán* $a' \cap d = b' \cap d = \emptyset$ mindig igaz[13)], de számelméletben (és multihalmazoknál) $\mathfrak{p}(a') \cap \mathfrak{p}(d) = \emptyset$ vagy $\mathfrak{p}(b') \cap \mathfrak{p}(d) = \emptyset$ már *nem* feltétlenül teljesül!

Természetesen a' és b' biztosan relatív prímek (mivel d a legnagyobb):

$$\mathfrak{p}(a') \cap \mathfrak{p}(b') = \emptyset \quad \text{azaz} \quad lnko(a', b') = 1 \tag{29}$$

vagyis $a' \sqcap b' = 1$, **de** $lnko(a', d) \neq 1$ és $lnko(b', d) \neq 1$ elképzelhető (lásd a fenti példát).

Azonban a jólismert, és nagyon hasznos (6) összefüggés látszik az 1. ábrán. Új jelöléseinkkel:

$$\boxed{a \sqcup b = \frac{a \cdot b}{a \sqcap b}} \ , \tag{30}$$

ami pontosan megfelel a *logikai szitaformulának* (tartalmazás és kizárás elve):

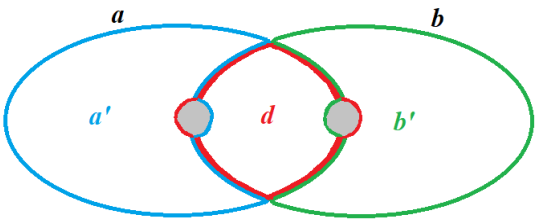
$$\boxed{|a \cup b| = |a| + |b| - |a \cap b|} \ , \tag{31}$$

"*mintha a* (30) *egyenlet logaritmusát vettük volna* ."

A fenti összefüggések általánosítása lesz a (37) összefüggés.

Ha a szürke foltjait vizsgáljuk, akkor a $d'_a := lnko(a', d)$ és $d'_b := lnko(b', d)$ jelöléssel d'_a és d'_b *biztosan* relatív prímek, hiszen osztói a' és b' -nek (amik biztosan relatív prímek). Az $a = 12$ és $b = 18$ példában $d'_a = lnko(a', d) = 2$ és $d'_b := lnko(b', d) = 3$.

Ha az 1. ábrán a szürke foltokat *multihalmazokra* és *egész számokra* nevesíteni (vagyis pontosan kiszámolni) akarjuk, akkor az ábrát javítanunk kell: az a, b, d halmazok kék-, zöld- és piros kontúrjait pontosítjuk:



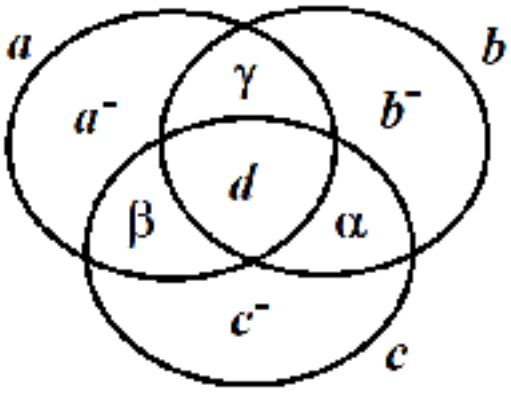
2. Ábra: *lnko(a,b) részletesen*

[13)] hagyományos halmazoknál $d = a \cap b$, $a' = a \setminus d$ és $b' = b \setminus d$,

Könnyen belátható, hogy a szürke foltok $lnko(a',d) = lnko\left(\frac{a}{d},d\right)$ és $lnko(b',d) = lnko\left(\frac{b}{d},d\right)$, amik nem feltétlenül 1 értékűek. Multihalmazoknál a szürke foltok "képlete" így $\left(a\mathring{\setminus}b\right)\mathring{\cap}\left(a\mathring{\cap}b\right)$ és $\left(b\mathring{\setminus}a\right)\mathring{\cap}\left(a\mathring{\cap}b\right)$.

A halmazábra (újabb és újabb ... szürke foltok) további vizsgálata házi feladat.

3. Három szám vizsgálata



3. Ábra: $lnko(a,b,c)$

16. Részletesebben: Először megkeressük az a, b, c molekulák (természetes számok) legnagyobb közös részét:

$$d := lnko(a,b,c) = a \sqcap b \sqcap c \ ,$$

majd a *maradék* molekulák $\left(\frac{a}{d}\ ,\frac{b}{d}\ ,\frac{c}{d}\right)$ közös részeit:

$$\alpha := lnko\left(\frac{b}{d},\frac{c}{d}\right) = \frac{b}{d}\sqcap\frac{c}{d}\ ,\ \beta := lnko\left(\frac{a}{d},\frac{c}{d}\right) = \frac{a}{d}\sqcap\frac{c}{d}\ ,\ \gamma := lnko\left(\frac{a}{d},\frac{b}{d}\right) = \frac{a}{d}\sqcap\frac{b}{d}\ .$$

Végül, a megmaradt molekula részeket a^-, b^-, c^- jelöli:

$$a^- := \frac{a}{d\beta\gamma} = a \setminus \left(d \cup \beta \cup \gamma\right) \ ,$$

$$b^- := \frac{b}{d\alpha\gamma} = b \setminus \left(d \cup \alpha \cup \gamma\right)$$

$$c^- := \frac{c}{d\alpha\beta} = c \setminus \left(d \cup \alpha \cup \beta\right) \ . \qquad \square$$

A fenti számolásokban felhasználtuk a következő összefüggést is:

ha $w \mid u, v$, akkor

$$lnko\left(\frac{u}{w}, \frac{v}{w}\right) = \frac{lnko\,(u,v)}{w}\ . \qquad \square \tag{32}$$

($lkkt(a,b,c)$ -re a (37) képletben adunk egy új formulát.)

17. Észrevétel: A fentiekből következik (az ábráról is leolvasható), hogy $a = a^{-}d\beta\gamma$, $b = b^{-}d\alpha\gamma$, $c = c^{-}d\alpha\beta$, továbbá $lnko(a,b) = d\gamma$, $lnko(a,c) = d\beta$, $lnko(b,c) = d\alpha$ és $d = lnko(a,b,c)$. $\square$

Fontos lesz a későbbiekben, hogy a fenti ábrában mely számok *biztosan* relatív prímek, és melyek nem feltétlenül.

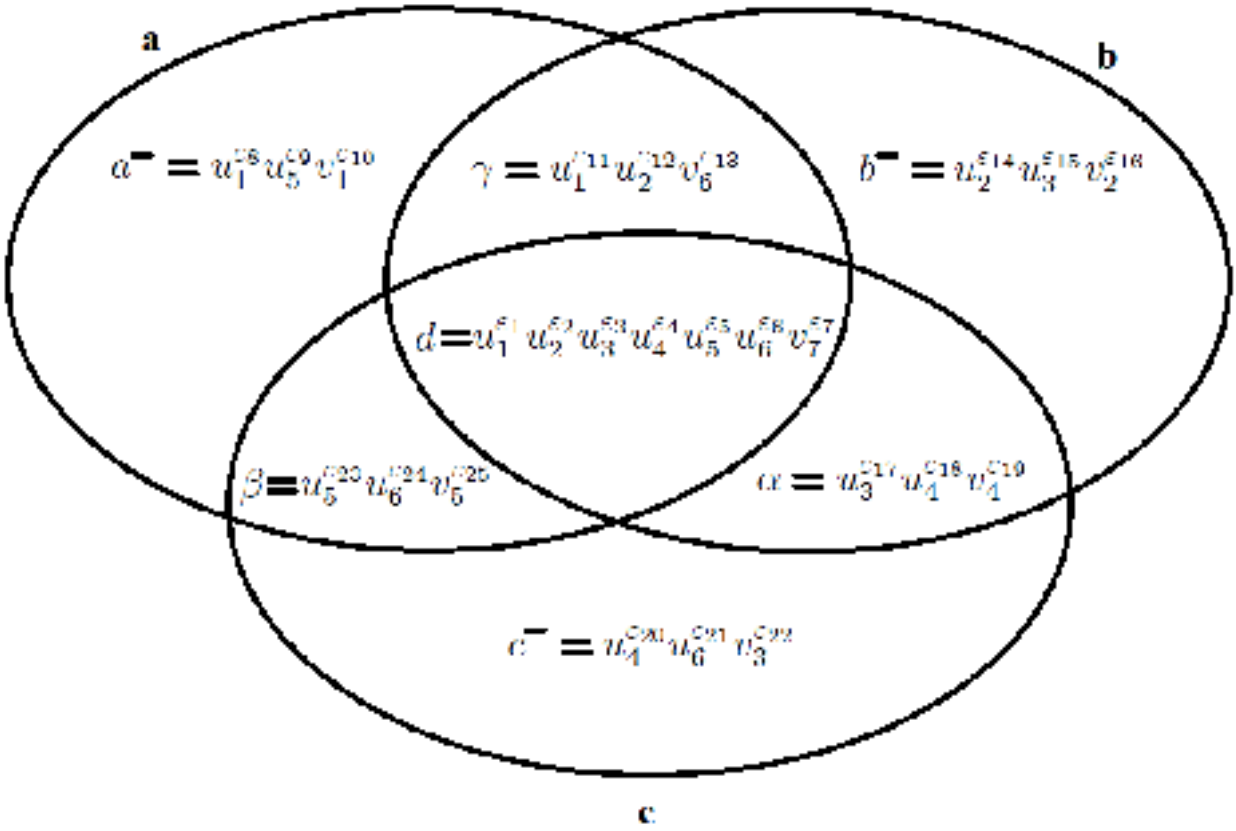
18. Észrevétel:

$\alpha\sqcap\gamma = \alpha\sqcap\beta = \beta\sqcap\gamma = \alpha\sqcap a^{-} = \beta\sqcap b^{-} = \gamma\sqcap c^{-} = a^{-}\sqcap b^{-} = a^{-}\sqcap c^{-} = b^{-}\sqcap c^{-} = 1$,

de a többi halmaz-pár már nem feltétlenül diszjunkt (relatív prím). $\square$

Egy lehetséges általános[14)] eset :

[14)] talán nem a legáltalánosabb



4. Ábra: *lnko*(a,b) részletesen

ahol

$a^- = u_1^{\varepsilon_8} u_5^{\varepsilon_9} v_1^{\varepsilon_{10}}, \quad b^- = u_2^{\varepsilon_{14}} u_3^{\varepsilon_{15}} v_2^{\varepsilon_{16}}, \quad c^- = u_4^{\varepsilon_{20}} u_6^{\varepsilon_{21}} v_3^{\varepsilon_{22}}, \quad d = u_1^{\varepsilon_1} u_2^{\varepsilon_2} u_3^{\varepsilon_3} u_4^{\varepsilon_4} u_5^{\varepsilon_5} u_6^{\varepsilon_6} v_7^{\varepsilon_7},$

$\alpha = u_3^{\varepsilon_{17}} u_4^{\varepsilon_{18}} v_4^{\varepsilon_{19}}, \quad \beta = u_5^{\varepsilon_{23}} u_6^{\varepsilon_{24}} v_5^{\varepsilon_{25}}, \quad \gamma = u_1^{\varepsilon_{11}} u_2^{\varepsilon_{12}} v_6^{\varepsilon_{13}}, \quad$ és $\quad u_1, ..., u_6, v_1, ..., v_7$

páronként relatív prímek (1 is lehet közöttük), ε_i tetszőleges természetes számok (0 is lehet közöttük).

Ekkor nyilván

$$a = a^- d\beta\gamma = u_1^{\varepsilon_1+\varepsilon_8+\varepsilon_{11}} u_2^{\varepsilon_2+\varepsilon_{12}} u_3^{\varepsilon_3} u_4^{\varepsilon_4} u_5^{\varepsilon_5+\varepsilon_9+\varepsilon_{23}} u_6^{\varepsilon_6+\varepsilon_{24}} v_1^{\varepsilon_{10}} v_5^{\varepsilon_{25}} v_6^{\varepsilon_{13}} v_7^{\varepsilon_7} \ ,$$

$$b = b^- d\alpha\gamma = u_1^{\varepsilon_1+\varepsilon_{11}} u_2^{\varepsilon_2+\varepsilon_{12}+\varepsilon_{14}} u_3^{\varepsilon_3+\varepsilon_{15}+\varepsilon_{17}} u_4^{\varepsilon_4+\varepsilon_{18}} u_5^{\varepsilon_5} u_6^{\varepsilon_6} v_2^{\varepsilon_{16}} v_4^{\varepsilon_{19}} v_6^{\varepsilon_{13}} v_7^{\varepsilon_7}$$

és

$$c = c^- d\alpha\beta = u_1^{\varepsilon} u_2^{\varepsilon_2} u_3^{\varepsilon_3+\varepsilon_{17}} u_4^{\varepsilon_4+\varepsilon_{18}+\varepsilon_{20}} u_5^{\varepsilon_5+\varepsilon_{23}} u_6^{\varepsilon_6+\varepsilon_{21}+\varepsilon_{24}} v_3^{\varepsilon_{22}} v_4^{\varepsilon_{19}} v_5^{\varepsilon_{25}} v_7^{\varepsilon_7} \ .$$

Még általánosabb lehetne: az x^{ε} hatványok helyett $x^{[\overrightarrow{\varepsilon}]}$ hatványokat írhatnánk, ahol $x^{[\overrightarrow{\varepsilon}]}$ a következőt jelöli: x prímtényezőinek *tetszőleges* hatványait vehetjük, vagyis precízen: $x = p_1^{\alpha_1}...p_t^{\alpha_t}$ és $\overrightarrow{\varepsilon} = (\varepsilon_1, ..., \varepsilon_t)$ esetén $\quad x^{[\overrightarrow{\varepsilon}]} := (p_1^{\alpha_1})^{\varepsilon_1} ... (p_t^{\alpha_t})^{\varepsilon_t}$.

19. Kérdés: ha a 4. ábra $\varepsilon_1, ..., \varepsilon_{25}$ kitevőit így módosítjuk, akkor az így kapott ábra már a legáltalánosabb esetet szemlélteti-e **?**

A (30) összefüggés három változós megfelelőjét, vagyis hogyan lehet kiszámolni $lkkt(a, b, c)$ -t a 6. "$Lkkt(a, b, c)$" fejezetben számoljuk ki.

4. Boole - algebra axiómák

Bár nem az elméletre akarjuk helyezni a hangsúlyt, hanem a feladatmegoldásokhoz kívánunk segítséget nyújtani, mégis hasznos lesz először általában a Boole algebrák axiómáival és azok következményeivel megismerkednünk. Képleteink és számolásaink utána könnyebbek lesznek.

20. Definíció: Egy **Boole algebra** egy *algebrai struktúra*, ami egy alaphalmaz és rajta értelmezett műveletek összessége, bizonyos azonosságok ("axiómák") teljesülése esetén, például az alábbi táblázat axiómái alapján. □

Többféle axiómarendszer van használatban, de hihetünk Urbán János [12] könyvének: ezek az axiómarendszerek *ekvivalensek*, vagyis bármelyikből levezethető bármelyik másik. Sőt, [12] több tucat egyéb összefüggést is levezet az általa használt axiómákból, és még azt is belátja, hogy bármely összefüggés (azonosság), amely igaz a Boole algebrákban, az le is vezethető az axiómákból.

Az alábbi táblázatok közül az első egy lehetséges axiómarendszer, a hagyományos halmazelméleti műveletekkel és jelölésekkel (I egy tetszőleges alaphalmaz, $A, B, C \subseteq I$ tetszőleges részhalmazai). A további vizsgálataink megkönnyítése érdekében ezen axiómákat átírtam $\sqcup$, $\sqcap$, *lkkt, lnko, max* és *min* műveletekre, melyek teljesülését alább tárgyaljuk. Közismert, hogy az axiómák a logikai $\vee$, $\wedge$, $\rceil$ (tagadás) műveletekre is teljesülnek, ezeket nem tüntettem fel a táblázatokban.

kommutatív	$A \cup B = B \cup A$	/1/	$a \sqcup b = b \sqcup a$
	$A \cap B = B \cap A$	/2/	$a \sqcap b = b \sqcap a$
asszociatív	$A \cup (B \cup C) = (A \cup B) \cup C$	/3/	$a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$
	$A \cap (B \cap C) = (A \cap B) \cap C$	/4/	$a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$
disztributív	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	/5/	$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	/6/	$a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$
elnyelési tul.	$A \cup (A \cap B) = A$	/7/	$a \sqcup (a \sqcap b) = a$
	$A \cap (A \cup B) = A$	/8/	$a \sqcap (a \sqcup b) = a$
$\emptyset$ és I tul.	$A \cup \overline{A} = I$	/9/	$a \sqcup \overline{a} = n$
	$A \cap \overline{A} = \emptyset$	/10/	$a \sqcap \overline{a} = 1$
	$A \cup \emptyset = A$	/11/	$a \sqcup 1 = a$
	$A \cap \emptyset = \emptyset$	/12/	$a \sqcap 1 = 1$
	$A \cup I = I$	/13/	$a \sqcup n = n$
	$A \cap I = A$	/14/	$a \sqcap n = a$

$lkkt(a,b) = lkkt(b,a)$	$\max(a,b) = \max(b,a)$
$lnko(a,b) = lnko(b,a)$	$\min(a,b) = \min(b,a)$
$lkkt(a, lkkt(b,c)) = lkkt(lkkt(a,b), c)$	$\max(a, \max(b,c)) = \max(\max(a,b), c)$
$lnko(a, lnko(b,c)) = lnko(lnko(a,b), c)$	$\min(a, \min(b,c)) = \min(\min(a,b), c)$
$lkkt(a, (lnko(b,c))) =$	$\max(a, (\min(b,c))) =$
$= lnko(lkkt(a,b), lkkt(a,c))$	$= \min(\max(a,b), \max(a,c))$
$lnko(a, (lkkt(b,c))) =$	$\min(a, (\max(b,c))) =$
$= lkkt(lnko(a,b), lnko(a,c))$	$= \max(\min(a,b), \min(a,c))$
$lkkt(a, lnko(a,b)) = a$	$\max(a, \min(a,b)) = a$
$lnko(a, lkkt(a,b)) = a$	$\min(a, \max(a,b)) = a$
$lkkt\left(a, \frac{n}{a}\right) = n$	$\max(a, \overline{a}) = n$ **NEM !!!**
$lnko\left(a, \frac{n}{a}\right) = 1$	$\min(a, \overline{a}) = I$ **NEM !!!**
$lkkt(a,1) = a$	$\max(a, I) = a$
$lnko(a,1) = 1$	$\min(a, I) = I$
$lkkt(a,n) = n$	$\max(a,n) = n$
$lnko(a,n) = a$	$\min(a,n) = a$

2. Táblázat: *Boole axiómák halmaz-, számelméleti és* min-max *nyelveken*

Csak helyhiány miatt nem ismételjük meg a táblázatot ötödször (és hatodszor, ...): a logikai $\vee$, $\wedge$, $\urcorner$, i , h műveletek[15)] is Boole algebrát alkotnak, és még sok Boole algebrát ismerünk.

[15)] $\vee$, $\wedge$, $\urcorner$, i , h helyett használatosak még a | , + ill. a **&** , · ill. ˜ill. 1 ill. 0 és egyéb jelek is.

Az /1/-/8/ axiómákkal nincs gond: bárki könnyen beláthatja, hogy teljesülnek *tetszőleges* a, b, c természetes számokra, molekulákra és multihalmazokra is (vagyis mind a négy táblázatban), sőt a negyedik táblázatban a, b, c tetszőleges valós számok is lehetnek.

Mi az *alaphalmaz* és mi a *komplementer* a kémiában és a számelméletben, és esetleg a multihalmazoknál és a min, max műveleteknél**?** Ezeket úgy kell megválasztanunk, hogy a /9/-/14/ axiómák teljesüljenek.

Alaphalmaz, O és I **:**

21. Állítás: A /11/-/14/ axiómákról könnyen belátható, hogy teljesülnek, ha

- szokásos halmazoknál (első táblázat) $\emptyset$ = üres halmaz, I = tetszőleges (akár üres) halmaz = alaphalmaz, és $A, B, C \subseteq I$ tetszőleges halmazok,

- multihalmazoknál (első táblázat, $\mathring{\cup}$ és $\mathring{\cap}$ jelekkel) $\emptyset$ = üres (multi)halmaz, I = tetszőleges (akár üres) multihalmaz = alaphalmaz, és $A, B, C \mathring{\subseteq} I$ tetszőleges multihalmazok,

- számelméletben (második és harmadik táblázat) $\emptyset$ helyett $1 \in \mathbb{N}$ áll, hiszen $\mathfrak{p}(1) = \emptyset$, I helyett *tetszőleges* (akár 1) természetes szám, $n \in \mathbb{N}$ áll, és a, b, c tetszőleges *osztói* n -nek, hiszen ekkor $\mathfrak{p}(a), \mathfrak{p}(b), \mathfrak{p}(c) \mathring{\subseteq} \mathfrak{p}(n)$, vagyis az alaphalmaz = n osztóinak halmaza,

- *min-max* esetén (második és negyedik táblázat)

vagy először $H \subseteq \mathbb{R}$ tetszőleges olyan (nemüres) alaphalmaz, melynek létezik maximuma *és* minimuma (vagyis legkisebb- és legnagyobb eleme), és ekkor $I := \min H$, $n := \max H$ (n nem feltétlenül egész szám), továbbá $a, b, c \in H$ tetszőleges elemek, hiszen ekkor $I \leq a, b, c \leq n$,

vagy ha $H \subseteq \mathbb{R}$ -nek nincs maximuma vagy minimuma, akkor H -hoz hozzáveszünk egy, H minden eleménél nagyobb és egy, minden eleménél kisebb elemet,

vagy ha $H \subseteq \mathbb{R}$ nem korlátos halmaz, akkor tekintjük a $\overline{H} := H \cup \{-\infty, +\infty\}$ halmazt, $I := -\infty$, $n := +\infty$, és $a, b, c \in \overline{H}$ tetszőleges elemek. □

22. Jelölés: Tetszőleges $n \in \mathbb{N}$ természetes szám esetén jelölje D_n az n szám pozitív osztóinak[16)] halmazát:

$$D_n := \{\ x :\ x \mid n\}\ . \qquad \square \tag{33}$$

16) D = divisors = "osztók"

Komplementer, azaz /9/-/10/ axiómák **:**

23. Állítás:

- szokásos halmazoknál közismert $\overline{A}$ definíciója és tulajdonságai, /9/-/10/ teljesülnek,

- multihalmazoknál $\overline{a} := I \overset{\circ}{\setminus} a$,

- számelméletben kézenfekvőnek látszik az $\overline{a} := \dfrac{n}{a}$ definíció, ahol n a 21. Állításban szereplő szám, $a \mid n$. Alaposabb vizsgálat után rájöhetünk, hogy

$$\textit{csak négyzetmentes } n \text{ szám} \tag{34}$$

esetén teljesülnek az $lkkt\left(a, \frac{n}{a}\right) = n$ és $lnko\left(a, \frac{n}{a}\right) = 1$ összefüggések, a /9/-/10/ axiómák.

Ez nem véletlen, hiszen négyzetmentes n esetén a $\mathfrak{p}(n)$ multihalmaz minden elemének multiplicitása 1, vagyis $\mathfrak{p}(n)$ hagyományos halmaz, és ekkor minden $a \mid n$ esetén $\mathfrak{p}(a)$ is hagyományos halmaz, $\sqcup$, $\sqcap$ és $\overline{a}$ (azaz *lkkt, lnko* és $\frac{n}{a}$) megegyeznek a hagyományos $\cup$ és $\cap$ műveletekkel.

- *min-max* esetén meggondolható, hogy egyetlen esetben van lehetőségünk komplementerre: $H = \{0, 1\}$, $\overline{0} = 1$ és $\overline{1} = 0$, vagy kicsit általánosabban: $H = \{a, b\}$ ahol $a \leq b$, $\overline{a} = b$ és $\overline{b} = a$, stb.

Legalább 3-elemű alaphalmaznál komplementer egyetlen esetben *sem* definiálható úgy, hogy a /9/-/10/ axiómák teljesüljenek. □

Összefoglalva, a számelméleti esetek:

24. Tétel: a) tetszőleges $a, b, c \in \mathbb{N}$ számokra /9/ és /10/, /13/ és /14/ kivételével mind teljesül ($\emptyset$ helyett 1 írandó).

b) Ha n rögzített és $a \mid n$ akkor /13/ és /14/ is teljesül.

c) Ha n *négyzetmentes*, akkor $\overline{a} := \dfrac{n}{a}$ jelöléssel /1/-/14/ mind teljesül, vagyis a $\left(D_n, \sqcup, \sqcap, \frac{n}{x}, n, 1\right)$ struktúra *Boole-algebra*. (n négyzetmentessége csak a /9/ és /10/ azonosságokhoz kell.)

Bizonyítás: Házi Feladat. □

Jegyezzük meg, hogy a *min* és *max* műveletek is *majdnem* Boole algebra, de $\overline{a}$ nem értelmezhető[17)].

[17)] itt megszakad a kapcsolat $lnko(a, b)$ és *min*(*a* és *b* prímkitevői) között.

5. További azonosságok

Most nem részletezzük a Boole-algebrák *Dualitási* és *Teljességi* tulajdonságait, lásd [12]. A Boole-algebrák axiómáiból az összes, ismert azonosság már levezethető, most csak felsorolunk néhányat, a levezetés [12] 188-199 oldalain megtalálható.

25. Tétel: Az alábbi összefüggések következnek az /1/-/14/ axiómákból. Házi feladat az Olvasónak ezeket az összefüggéseket átírni *lnko-lkkt* és esetleg *min-max* -ra, logikai műveletekre is, ... (A, B, C helyett p, q -t írunk).

idempotencia: $A \cup A = A \cap A = A$, azaz $lnko(a,a) = lkkt(a,a) = a$,

$p \cap q = p \iff p \cup q = q$, azaz $lnko(a,b) = a \iff lkkt(a,b) = b$,

ha $\subset$ a következőt rövidíti: $p \cap q = p$, akkor ekvivalens: $p \cup q = q$,

azaz $a \mid b \iff lnko(a,b) = a \iff lkkt(a,b) = b$,

$p \subset p$, azaz $a \mid a$,

$(p \subset q)$ & $(q \subset p) \implies p = q$, azaz $a \mid b$ & $b \mid a \implies a = b$,

$(p \subset q)$ & $(q \subset r) \implies p \subset r$, azaz $a \mid b$ & $b \mid c \implies a \mid c$.

Az alábbiakban n *négyzetmentes* és $a, b \mid n$.

$p \cap \overline{p} = q \cap \overline{q}$, $p \cup \overline{p} = q \cup \overline{q}$ bármely p, q esetén,

azaz $lnko\left(a, \frac{n}{a}\right) = 1$ és $lkkt\left(a, \frac{n}{a}\right) = n$,

ha $(p \cap q = O)$ & $(p \cup q = I)$ akkor $q = \overline{p}$,

azaz ha $lnko(a,b) = 1$ & $lkkt(a,b) = n$ akkor $b = \frac{n}{a}$,

$\overline{\overline{p}} = p$, $\overline{I} = O$, $\overline{O} = I$,

azaz $\frac{n}{\frac{n}{a}} = a$, $\frac{n}{n} = 1$, $\frac{n}{1} = n$,

ha $O = I$ akkor $\forall p \;\; p = O$, azaz ha $n = 1$ akkor $\forall a : a \mid n \implies a = 1$.

DeMorgan szabályok:

$\overline{a \cup b} = \overline{a} \cap \overline{b}$ azaz $\frac{n}{lkkt\,(a,b)} = lnko\left(\frac{n}{a}, \frac{n}{b}\right)$,

$\overline{a \cap b} = \overline{a} \cup \overline{b}$ azaz $\frac{n}{lnko\,(a,b)} = lkkt\left(\frac{n}{a}, \frac{n}{b}\right)$. $\square$

6. *Lkkt(a,b,c)*

Most keressük meg a (30) összefüggés *három változós* megfelelőjét, vagyis hogyan lehet kiszámolni $lkkt(a,b,c)$ -t ?

Egyik lehetőség lépésről lépésre, vagyis az asszociativitást felhasználva:

$$lkkt\,(a,b,c) = \;\; lkkt(lkkt\,(a,b)\,,c) \quad , \tag{35}$$

vagy olvashatóbban: $\quad a \sqcup b \sqcup c = (a \sqcup b) \sqcup c$.

A (30) összefüggés kétszeri alkalmazásával kapjuk:

$$lkkt(a,b,c) \;=\; a \sqcup (b \sqcup c) \;=\; (30)\ \text{alapján} \;=\; \frac{a \cdot (b \sqcup c)}{a \sqcap (b \sqcup c)} \;=\; /8/\ \text{alapján} \;=$$

$$\frac{a \cdot (b \sqcup c)}{(a \sqcap b) \sqcup (a \sqcap c)} = (30)\ \text{alapján} = \frac{a \cdot \frac{b \cdot c}{b \sqcap c}}{\frac{(a \sqcap b)\cdot(a \sqcap c)}{(a \sqcap b) \sqcap (a \sqcap c)}} = \frac{a \cdot \frac{b \cdot c}{b \sqcap c}}{\frac{(a \sqcap b)\cdot(a \sqcap c)}{a \sqcap b \sqcap c}} = \frac{a \cdot b \cdot c \cdot (a \sqcap b \sqcap c)}{(a \sqcap b) \cdot (a \sqcap c) \cdot (b \sqcap c)}$$

Kaptuk tehát:

26. Tétel:

$$a \sqcup b \sqcup c = \frac{a \cdot b \cdot c \cdot (a \sqcap b \sqcap c)}{(a \sqcap b) \cdot (a \sqcap c) \cdot (b \sqcap c)} \tag{36}$$

vagyis

$$\boxed{lkkt(a,b,c) = \frac{a \cdot b \cdot c \cdot lnko\,(a,b,c)}{lnko\,(a,b) \cdot lnko\,(a,c) \cdot lnko\,(b,c)}\ ,} \tag{37}$$

ahol, mint tudjuk

$$lnko\,(a,b,c) = lnko(lnko\,(a,b)\,,c) = lnko(a, lnko\,(b,c)\,) \tag{38}$$

A (36) egyenlet ismét pontosan megfelel a *logikai szitaformulának*:

$$|a \cup b \cup c| = |a| + |b| + |c| - |a \cap b| - |a \cap c| - |b \cap c| + |a \cap b \cap c| \quad , \tag{39}$$

mintha a (36) egyenlet *logaritmusát* vettük volna. (Vagy visszafelé: a fenti egyenletre az *exponenciális* függvényt alkalmazva kapjuk a (36) egyenletet.)

7. Az Euklideszi algoritmus és egyéb érdekességek

$lnko(a,b)$ -t a és b prímtényezős felbontásából, a prímek kitevőiből határozzuk meg. Azonban a modern számítógépes alkalmazásoknál (titkosírás, kódolás, stb.) többszáz jegyű számokkal ($\approx 10^{500}$) kell számolnunk, amik prímtényezős felbontása, még a legmodernebb szuperszámítógépekkel is *tucatnyi évmilliárdig* (!) tartana ! Lásd [8]. (Prímfelbontásokkal [9] és Knuth [5] is részletesen foglalkozik a 4.5.4. pontban.)

Ennyi idő alatt, ugye tudjuk, kihal az emberiség, a Nap felfúvódik Vörös Óriássá és a Föld ennek belsejében kerint (meleg helyzet), utána a Nap összehúzódik Fehér Törpévé (Föld=?), és talán a program még mindig fut ...

Szerencsére egy ókori (geometriai) algoritmust egész számokra alkalmazva nagyon gyorsan kiszámíthatjuk tetszőlegesen nagy egész számok *legnagyobb közös osztóját*, prímfelbontás nélkül. *Euklideszi algoritmus*nak hívják, mert Euklidesz *Elemek* [2] 7. könyvében írja le részletesen, bár egyes kutatások szerint (pl. [5] 325.old. vagy Waerden [13]) 200 évvel korábban is ismerték, például Eudoxosz i.e. 375 körül.

Csak annyit említünk meg, hogy *Gabriel Lamé*[18] 1844 -ben kelt tétele szerint az Euklideszi algoritmus legfeljebb 5-ször annyi lépést (maradékos osztást) kíván, mint a kisebbik szám *számjegyeinek száma*[19]. Vagyis, például 500 jegyű számoknál legfeljebb 5*500=2500 lépésig tart az Euklideszi algoritmus, ami pár század-másodperc. A Lehmer család (apa és fia) tovább gyorsította az Euklideszi algoritmust, elméletileg is és fogaskerekes-lánchajtásos "számológépükkel" is, lásd [5] 336-38.old. és [11].

Knuth [5] az Euklideszi algoritmus több alkalmazását is megemlíti: 3.2.1.2. pont = *véletlen számok generálása*, 3.3.3. pont = *statisztikai elméleti próbák*, 4.3.2. pont = *moduláris aritmetika* (számolás maradékokkal), 4.3.3. pont = *milyen gyorsan tudunk szorozni* .

(24) -hez hasolóan $lnko(u_1,...,u_n)$ -t iterációval szoktuk kiszámolni:

$$lnko\left(u_1,...,u_n\right) = lnko\left(lnko\left(u_1,...,u_{n-1}\right),u_n\right) = \ ... \ , \tag{40}$$

az asszociativitás alapján. Knuth [5] más, bonyolultabb algoritmust is ajánl erre, ami azonban gyorsabb.

Végül két érdekesség:

G.Lejeune Dirichlet 1849 tétele (Knuth [5] 332.old.): Ha $u,v \in \mathbb{N}$ véletlenszerűen választott egészek, akkor $6/\pi^2 \approx 0.60793$ annak a valószínűsége, hogy u és v relatív prímek. $\square$

[18] Gabriel Lamé (1795-1870) francia matematikus.

[19] A tétel bizonyításában ismét megjelennek a Fibonacci számok, lásd például Csete Lajos [1] cikkében.

Feladat (Knuth [5], 347. és 600. old.): Mutassuk meg, hogy tetszőleges $1 \leq a$ és u, v nem negatív egészekre

$$lnko\,(a^u - 1\ ,\ a^v - 1) = a^{lnko(u,v)} - 1 \tag{41}$$

és

$$a^u - 1 \equiv a^{u - u \bmod v} - 1 \pmod{a^v - 1}\ . \tag{42}$$

□

Hivatkozások

[1] **Csete Lajos:** *Az Euklideszi algoritmus legrosszabb esete és Gabriel Lamé*, Polygon, 1994, 83-88.

[2] **Euklidész:** *Elemek* (magyarul): Gondolat, 1977, http://mek.oszk.hu/06200/06232 (pdf), http://mek.oszk.hu/00800/00857 (html) , http://mek.iif.hu/06200/06232

[3] **Jaglom,I.M.:** *Boole struktúrák és modelljeik*, Műszaki Kiadó, 1983.

[4] *A* B.4493. *feladat és megoldása*, KöMaL, 2012/10 és 2013/8, 478-479., http://www.komal.hu/verseny/feladat.cgi?a=feladat&f=B4493&l=hu

[5] **Knuth, D.E.:** *A számítógép-programozás művészete*, 2. kötet, *Szeminumerikus algoritmusok*, Műszaki Kiadó, Budapest, 1987.

[6] **Szalkai István:** *Diszkrét matematika és algoritmuselmélet alapjai,* Pannon Egyetem Kiadó, Veszprém, 2000, 2006.

[7] **Szalkai István:** *Algebra és számelmélet feladatgyűjtemény*, Pannon Egyetem Kiadó, Veszprém, 2005, 2021.

[8] **Szalkai István:** *Nagy matematika,* Haladvány Kiadvány, 2013., http://math.bme.hu/~hujter/131120.pdf ,
vagy: *Újabb kombinatorikai feladatok* (*analízis, algebra,...*), 2008, https://math.uni-pannon.hu/~szalkai/KombUj+Felad2c.pdf

[9] **Szalkai István, Dósa György**: *Algoritmikus számelmélet*, Egyetemi jegyzet digitális mellékletekkel, Typotex Kiadó, 2011, https://dtk.tankonyvtar.hu/handle/123456789/7516

[10] **Szalkai István:** *Számelmélet, kémia, Boole-algebrák*, Haladvány Kiadvány, 2013., http://math.bme.hu/~hujter/131107.pdf , http://math.bme.hu/~hujter/halad.htm

[11] **Szalkai István:** *A Lehmer-szita* 2019, https://math.uni-pannon.hu/~szalkai/Lehmer-szita.pdf

[12] **Urbán János:** *Matematikai logika*, Példatár ("Bolyai könyvek" sorozat), Műszaki Könyvkiadó, Budapest, 1983.

[13] **van der Waerden, B.L.:** *Egy tudomány ébredése*, Gondolat, 1977.

[14] **Wikipédia:** *Boole-algebra*, [Részletes definíció], http://hu.wikipedia.org/wiki/Boole-algebra

[15] **Wikipedia**: *Symmetric difference*, https://en.wikipedia.org/wiki/Symmetric_difference

https://hu.wikipedia.org/wiki/Atom

https://hu.wikipedia.org/wiki/Démokritosz

https://en.wikipedia.org/wiki/Atom

https://de.wikipedia.org/wiki/Atom

https://en.wikipedia.org/wiki/Multiset