9. Hálók

9.1 Alapfogalmak

9.1.1 Definíció: a $(H,\leq)$ struktúra részbenrendezett halmaz, ha $\leq$ a H halmazon értelmezett reláció, amely

(1) reflexív, azaz $\forall a\in H\colon a\leq a$,

(2) antiszimmetrikus; ez reflexív relációra azt jelenti, hogy $a\leq b, b\leq a \Rightarrow a=b$,

(3) tranzitív, azaz $a\leq b, b\leq c \Rightarrow a\leq c$.

Alternatív definíció: $(H,<)$ részbenrendezett halmaz, ha

(1*) antireflexív, azaz $\nexists a\in H\colon a<a$,

(2*) antiszimmetrikus; ez antireflexív relációra azt jelenti, hogy $\nexists a,b\in H\colon a<b, b<a$,

(3*) tranzitív, azaz $a\neq b, b<c \Rightarrow a<c$.

Ekkor a relációt részbenrendezésnek nevezzük.

Ha $\leq$ egy, az első feltételhármasnak megfelelő részbenrendezés, akkor $a<b \Leftrightarrow (a\leq b$ és $a\neq b)$ a második feltételhármast teljesíti. Ha pedig $<$ második típusú részbenrendezés, akkor $a\leq b \Leftrightarrow (a<b$ vagy $a=b)$ első típusú részbenrendezés. Tehát nem okoz komoly zavart, ha ugyanazt az elnevezést alkalmazzuk mindkét esetre. (Általában a csillag nélküli feltételeket fogjuk használni.)

9.1.2 Definíció: $(L,\leq)$ (teljesen) rendezett halmaz vagy más néven lánc, ha részbenrendezett halmaz és bármely két elem összehasonlítható, azaz $\forall a,b\colon (a\leq b$ vagy $b\leq a)$. Ekkor $\leq$-t rendezésnek hívjuk.

9.1.3 Definíció: a $(H,\leq)$ és $(H',\preceq)$ részbenrendezett halmazok izomorfak, ha található olyan $\varphi\colon H\to H'$ bijekció, amelyre φ és φ^{-1} is rendezéstartó, azaz $\forall a,b\in H\colon \left(a\leq b \Rightarrow \varphi(a)\preceq\varphi(b)\right)$ és $\forall a',b'\in H\colon \left(a'\preceq b' \Rightarrow \varphi^{-1}(a)\leq\varphi^{-1}(b)\right)$. (A feltétel átírható $a\leq b \Leftrightarrow \varphi(a)\preceq\varphi(b)$ alakba.) Jelölése $(H,\leq)\simeq(H',\preceq)$.

Megjegyzés: nem felesleges kikötni, hogy φ^{-1} is legyen műveletttartó, ugyanis csak így lehet elkerülni, hogy nem összehasonlítható elemek φ alkalmazása után összehasonlíthatóvá váljanak. Ha kikötjük, hogy $a\nleq b \Rightarrow \varphi(a)\npreceq\varphi(b)$, abból már következik, hogy φ^{-1} is rendezéstartó.

A következő négy definícióban jelöljön $(H,\leq)$ részbenrendezett halmazt.

9.1.4 Definíció: $a,b\in H$-ra b fedi a-t, ha $a<b$ és $\nexists c\in H\colon a<c<b$ (azaz b minimális az a-nál nagyobb elemek között). Jelölése $a\prec b$ vagy $b\succ a$.

9.1.5 Definíció: legyen $A\subseteq H$. A $b\in H$ elem felső korlátja A-nak, ha $\forall a\in A\colon a\leq b$. $c\in H$ alsó korlátja, ha $\forall a\in A\colon c\leq a$. Amennyiben A-hoz található ilyen $b\in H$ ill. ilyen $c\in H$, úgy A-t felülről ill. alulról korlátosnak nevezzük. A korlátos, ha mindkét irányból korlátos.

9.1.6 Definíció: legyen $A\subseteq H$. $m\in H$ legkisebb felső korlátja avagy szuprémuma A-nak, ha felső korlátja, továbbá A minden x felső korlátjára $m\leq x$. $m'\in H$ legnagyobb alsó korlátja avagy infimuma A-nak, ha alsó korlátja, továbbá A minden x' alsó korlátjára $x'\leq m'$. Jelölése $m=sup(A)$ ill. $m'=inf(A)$.

Az antiszimmetria miatt $sup(A)$ és $inf(A)$ egyértelmű, valahányszor létezik.

Jelölés: $sup(a,b)$-vel és $inf(a,b)$-vel $sup(\{a,b\})$-t és $inf(\{a,b\})$-t jelöljük, amennyiben ezek léteznek.

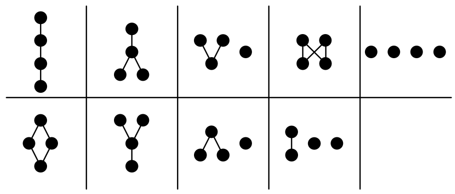
9.1.7 Definíció: $(H,\leq)$ háló, ha $\forall a,b\in H\colon \left(\exists sup(a,b)\text{ és }\exists inf(a,b)\right)$. Ekkor $sup(a,b)$-t $a\wedge b$-vel, $inf(a,b)$-t $a\vee b$-vel jelöljük ($a\wedge b$-t szokás metszetnek, $a\vee b$-t uniónak hívni).

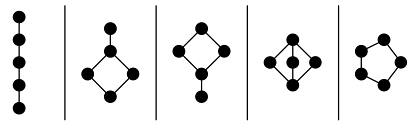
Példák:

- minden lánc háló, mert $a\leq b$ esetén $a\wedge b=a$ és $a\vee b=b$ léteznek.
- $(\mathcal{P}(H),\subseteq)$ háló, mert $A,B\subseteq H$ esetén $A\wedge B=A\cap B$, $A\vee B=A\cup B$ teljesül.

9.2 Részbenrendezett halmazok ábrázolása

Egy $(H,\leq)$ véges részbenrendezett halmaz ábráját az alábbi módon készítjük el:
Kijelölünk a síkon egy „felfele” irányt (jellemzően a lap aljától a lap teteje felé). H minden egyes elemének injektív módon megfeleltetjük a sík pontjait úgy, hogy ha valamely a,b-re $a<b$, akkor b feljebb kerüljön a-nál. Kössük össze azon elemek képeit, melyek egyike fedi a másikat. (Ha szaggatott vonallal kötünk össze két elemet, az azt jelenti, hogy összahasonlíthatóak, de nem feltétlenül fedi egyik a másikat. Ez akkor hasznos, ha nem akarunk minden elemet berajzolni.)





Az ábra elkészítése messze nem egyértelmű, viszont az ábra (izomorfia erejéig) egyértelműen meghatározza a hozzátartozó hálót. Ugyanis $a<b$ pontosan akkor teljesül, ha a-ból el lehet jutni élek mentén b-be úgy, hogy minden érintett élen felfele megyünk (ez könnyen ellenőrizhető).

Példa: a felső ábrán az összes páronként nemizomorf négyelemű részbenrendezett halmaz látható. Az első oszlop két eleme háló, a többi elem nem. Az alsó ábra az ötelemű hálókat mutatja; az első három disztributív, a negyedik moduláris, de nem disztributív, míg az utolsó nem moduláris. (Ezeket a tulajdonságokat később definiálni fogjuk.)

9.3 Hálóaxiómák

9.3.1 Állítás: ha $(L,\leq)$ háló, akkor a $\wedge,\vee$ műveletekre az alábbiak teljesülnek:

(L1) $a\wedge a=a\vee a=a$ $\forall a\in L$-re, azaz $\wedge,\vee$ idempotens,
(L2) $a\wedge b=b\wedge a$, $a\vee b=b\vee a$ $\forall a,b\in L$-re, azaz $\wedge,\vee$ kommutatív,
(L3) $(a\wedge b)\wedge c=a\wedge(b\wedge c)$, $(a\vee b)\vee c=a\vee(b\vee c)$ $\forall a,b,c\in L$-re, azaz $\wedge,\vee$ asszociatív,
(L4) $(a\wedge b)\vee a=a$, $(a\vee b)\wedge a$ $\forall a,b\in L$-re (abszorpciós tulajdonság).

Ezek mind triviálisan leellenőrizhetőek.

Megjegyzés: ha az $(L,\wedge,\vee)$ algebrai struktúrában a $\wedge,\vee$ műveletekre teljesül a **(L2)**, **(L3)** és **(L4)**, akkor **(L1)** is.

9.3.2 Definíció: ha $(H,\leq)$ háló, $n\in\mathbb{Z}^+$ és $a_1,\ldots,a_n\in H$, akkor legyen $\bigvee_{i=1}^{n} a_i=a_1\vee a_2\vee a_3\vee\ldots\vee a_{n-1}\vee a_n$ és $\bigwedge_{i=1}^{n} a_i=a_1\wedge a_2\wedge a_3\wedge\ldots\wedge a_{n-1}\wedge a_n$. (A definíció értelmes, mert $\wedge,\vee$ egyaránt asszociatív, így hát zárójelek nélkül is van értelme az $a_1\vee a_2\vee\ldots\vee a_n$ és $a_1\wedge a_2\wedge\ldots\wedge a_n$ kifejezéseknek. Mivel kommutatívak is, a sorrend sem számit.)

Megjegyzés: ha $(H,\leq)$ háló, akkor minden véges A részhalmazának van szuprémuma és infimuma, mégpedig $\bigvee_{a\in A} a$ és $\bigwedge_{a\in A} a$.

Egy végtelen részhalmaznak nem mindig van szuprémuma és infimuma, pl. a $(\mathbb{Q},\leq)$ láncban a $-\pi$ és π közé eső rac. számok A halmaza korlátos, de $\mathbb{Q}$-ban $\nexists sup(A),\nexists inf(A)$. Ezért nem érdektelen az alábbi definíció:

9.3.3 Definíció: $(H,\leq)$ teljes háló, ha tetszőleges A részhalmazára $\exists sup(A)$ és $\exists inf(A)$. Nyilván minden véges háló teljes.

Definíció: ha H-nak van legnagyobb eleme (azaz felső korlátja), akkor azt 1-el jelöljük. Ha van legkisebb, azt 0-val. Ha mindkettő létezik, akkor H korlátos háló. Nyilván minden teljes háló korlátos. (A jelölés onnan származik, hogy ha $\mathbb{N}$ felett az $a\leq b \Leftrightarrow b|a$ relációval definiált hálót tekintjük, abban 0 a legkisebb, 1 a legnagyobb elem.)

Elnevezés: két állítást, feltételt, bizonyítást stb. egymás duálisának nevezzük, ha a $\wedge\leftrightarrow\vee$, $\geq\leftrightarrow\leq$, $>\leftrightarrow<$, $inf\leftrightarrow sup$, $min\leftrightarrow max$ (stb.) cserék elvégzésével (és esetleg átbetűzéssel) egymásba alakíthatóak. Minthogy ez a megfeleltetés az **(L1)**…**(L5)** axiómákat nem változtatja, ha egy állítás levezethető az axiómákból, akkor a duálisa is és viszont. (Vigyázat, az esetleges feltételek helyett is a duálisukat kell venni, tehát pl. $a\vee b=c$ nem ekvivalens $a\wedge b=c$-vel.)

9.3.4 Állítás: ha az $(L,\wedge,\vee)$ struktúra teljesíti **9.3.2** feltételeit, akkor háló (értsd: alkalmas $\leq$ relációval $(L,\leq)$ háló és ebben a hálóban $inf(a,b)=a\wedge b$ és $sup(a,b)=a\vee b$).

Bizonyítás: legyen $a\leq b \Leftrightarrow a\vee b=b$.

Vegyük észre, hogy $a\vee b=b \Leftrightarrow a\wedge b=a$. (A két irány egymás duálisa, tehát elég az egyik irányt igazolni: $a\wedge b=a \Rightarrow a\vee b=(a\wedge b)\vee b \underset{\mathbf{(L4)}}{=} b$.

Belátjuk, hogy a fent definiált reláció részbenrendezés. Reflexív, mert $a\vee a\underset{\mathbf{(L1)}}{=}a$, azaz $a\leq a$. Antiszimmetrikus, mert $a\leq b, b\leq a$ esetén $a=a\vee b\underset{\mathbf{(L2)}}{=}b\vee a=b$. Tranzitív, mert $a\leq b, b\leq c$, azaz $a\vee b=b, b\vee c=c$ esetén $a\vee c=a\vee(b\vee c)\underset{\mathbf{(L3)}}{=}(a\vee b)\vee c=b\vee c=c$.

Az van még hátra, hogy $a\vee b=sup(a,b)$. $a\wedge(a\vee b)\underset{\mathbf{(L2)}}{=}(a\vee b)\wedge a\underset{\mathbf{(L4)}}{=}a$, tehát $a\leq a\vee b$. Hasonlóan $b\leq a\vee b$, tehát felső korlát. Ha $a,b\leq x$, akkor $a\vee x=b\vee x=x$. Ekkor $a\vee(b\vee x)=x \underset{\mathbf{(L3)}}{\Rightarrow} (a\vee b)\vee x=x \Rightarrow (a\vee b)\leq x$, így $a\vee b$ valóban legkisebb felső korlát. $a\vee b=sup(a,b)$ ennek duálisa, szintén igaz. Ezzel az állítást beláttuk.

9.3.5 Definíció: L háló duálisa az az L^* háló, amelynek alaphalmaza L alaphalmazával azonos, a $\wedge$ és az $\vee$ műveletek pedig felcserélődnek. Könnyen látható, hogy a műveletek által indukált részbenrendezés is megfordul. A duális háló ábráját L ábrájából a felfele és lefele irányok felcserélésével kapjuk. L duálisának duálisa önmaga. Az is nyilvánvaló, hogy egy állítás pontosan akkor igaz L-ben, ha duálisa igaz L duálisában.

9.3.6 Definíció: L' részhálója $(L,\wedge,\vee,)-$nek, ha $L'\subseteq L$ nem üres részhalmaz és zárt a $\wedge,\vee$ műveletekre. Jelölése $L'\leq L$.

Példa: az ábrán – – látható L hálóban a teli pontok L' halmaza az L-ből örökölt relációra nézve mint részbenrendezett halmaz hálót alkotnak, de L' nem részhálója L-nek, mert a két nem-összehasonlítható elemre az $\vee$ művelet L'-ben mást ad, mint L-ben.

9.3.7 Definíció: az L,L' hálók izomorfak, ha mint részbenrendezett halmazok izomorfak, azaz található olyan $\varphi\colon L\to L'$ bijekció, hogy φ és φ^{-1} is rendezéstartó.

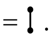
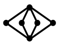
Állítás: $\varphi\colon(L,\wedge,\vee)\to(L',\wedge,\vee)$ pontosan akkor hálóizomorfizmus, ha művelettartó bijekció.

Bizonyítás: φ pontosan akkor művelettartó, ha φ^{-1} művelettartó. Tudjuk, hogy $(L,\wedge,\vee,)$ egyértelműen megadja $(L,\leq)$-t és viszont, tehát ha φ,φ^{-1} művelettartó, akkor rendezéstartó. Egyszerű és érdektelen számolással adódik, hogy ha φ hálóizomorfizmus, akkor valóban művelettartó.

9.4 Részcsoportháló, normálosztóháló, ideálháló

9.4.1 Definíció: G csoport $L(G)$ részcsoporthálójának elemei G részcsoportjai, $H_1\leq H_2$ (rr. reláció) $\Leftrightarrow$ $H_1\leq H_2$ (részcsoport). Ekkor $H_1\wedge H_2=H_1\cap H_2$ és $H_1\vee H_2=\langle H_1,H_2\rangle$. A háló korlátos, $0=\{1\}$ és $1=G$.

Példák:

- $G\simeq Z_p$ valamely p prímre $\Leftrightarrow$ $L(G)=$ .
- $G\simeq Z_{p^k}$ valamely p prímre és $k\in\mathbb{Z}^+$-ra $\Leftrightarrow$ $L(G)$ a $k+1$ elemű lánc. Ebből $\Rightarrow$ triviális; lássuk be a másik irányt. G ciklikus, mert ha nem lenne egyelemű generátorrendszere, akkor véve az $\langle a\rangle$ alakú részcsoportok közül egy maximálisat és egy $b\in G\setminus\langle a\rangle$ elemet sem $\langle a\rangle\leq\langle b\rangle$, sem $\langle a\rangle\geq\langle b\rangle$ nem teljesülhetne. Tehát $G\simeq Z_n$ valamely $n\in\mathbb{N}$-re. n-nek nem lehet egynél több prímosztója, mert akkor a Z_p,Z_q részcsoportok nem lennének összehasonlíthatóak. Ezért $n=p^k$.
- $L(S_3)=L(Z_3\times Z_3)=$ . A középső sorban $L(S_3)$-ban az $\langle(123)\rangle\simeq Z_3$ és az $\langle(12)\rangle,\langle(13)\rangle,\langle(14)\rangle\simeq Z_2$ részcsoportok vannak, $L(Z_3\times Z_3=\langle a\rangle\times\langle b\rangle)$ esetén az $\langle a\rangle,\langle b\rangle,\langle ab\rangle,\langle a^2b\rangle\simeq Z_3$ részcsoportok.

Állítás: $G=Q \Leftrightarrow L(G)=$ .

Bizonyítás: $L(Q)$ ábrája valóban ez, a részcsoportok rendre (ez most és a jövőben is azt jelzi, hogy a háló elemeit az ábrán fentről lefelé, balról jobbra soroljuk fel) $Q,\langle i\rangle,\langle j\rangle,\langle k\rangle,\langle -1\rangle,\langle 1\rangle$. Azt kell még belátnunk, hogy $L(G)=L(Q) \Rightarrow G=Q$.

G véges csoport, mert véges sok részcsoportja van. Csak egy minimális részcsoportja van, tehát G rendjének csak egy prímosztója van a Cauchy-tétel szerint. Tehát G p-csoport. Csak egy Z_p-vel izomorf részcsoportja van, tehát vagy ciklikus p-csoport, vagy általánosított kvaterniócsoport. Ciklikus p-csoport részcsoporthálója lánc, tehát $G\simeq Q_{2^k}$ és a részcsoportok megszámolásából $k=3$ adódik.

Megjegyzés: nincs olyan csoport, amelynek részcsoporthálója . Ha ugyanis ez lenne $L(G)$, akkor G-nek csak egy maximális részcsoportja lenne. Eszerint ciklikus p-csoport kellene legyen, de akkor $L(G)$ lánc lenne.

9.4.2 Definíció: G csoport $N(G)$ normálosztóhálójának elemei G normálosztói, a reláció a tartalmazás. Ekkor $N_1\wedge N_2=N_1\cap N_2$ és $N_1\vee N_2=\langle N_1,N_2\rangle=N_1N_2$. Korlátos háló, $0=\{1\}$ és $1=G$. Nyilván $N(G)\leq L(G)$.

9.4.3 Definíció: R gyűrűre és M (bal- vagy jobboldali) R-modulusra M részmodulushálója az, amit az ember gondolna. $M_1\wedge M_2=M_1\cap M_2$ és $M_1\vee M_2=M_1+M_2$. Korlátos.

9.4.4 Definíció: R gyűrű balideál-, jobbideál- és ideálhálója az, ami. Ebben $I_1\wedge I_2=I_1\cap I_2$ és $I_1\vee I_2=I_1+I_2$. Vegyük észre, hogy az első kettő azonos $_RR$ ill. R_R részmodulushálójával, a harmadik pedig ezek részhálója (a kettő metszete). Ez utóbbit $I(R)$-el fogom jelölni. Kommutatív gyűrűben ezek mind azonosak.

Példák:

- $N(Z_3\times Z_3)=L(Z_3\times Z_3)$, mert kommutatív csoport.
- $N(Q)=L(Q)$, mert minden részcsoportja normálosztó.
- $N(S_3)=$, mert egyetlen nem-triviális normálosztója A_3.

9.5 Moduláris és disztributív hálók

9.5.1 Definíció: az L háló moduláris, ha teljesül rá

(L5) $(a\vee b)\wedge c=a\vee(b\wedge c)$ $\forall a,b,c\in L; a\leq c$ esetén.

Ez az feltétel a $c\leftrightarrow a$ átbetűzéssel a duálisába megy át, tehát L moduláris $\Leftrightarrow$ duálisa moduláris.

9.5.2 Megjegyzés: ha ezt is azonosság formájában akarjuk felírni, megtehetjük $a'=a\wedge c$ helyettesítéssel, ahol $a\in L$ tetszőleges (minden $a'\leq c$ előáll ilyen alakban, hiszen $a'=a'\wedge c$ és minden $a\in L$-re $a\wedge c\leq c$):

(L5′) $((a\wedge c)\vee b)\wedge c=(a\wedge c)\vee(b\wedge c)$ $\forall a,b,c\in L$ esetén.

Lemma: $x,y\leq u,v$ esetén $x\vee y\leq u\wedge v$. Valóban, $x,y\leq u,v$-ből $sup(x,y)$ definíciója szerint $x\vee y\leq u,v$, amiből $inf(u,v)$ definíciója szerint $x\vee y\leq u\wedge v$.

9.5.3 Állítás: tetszőleges L hálóban teljesül $a\leq c$ esetén $(a\vee b)\wedge c\geq a\vee(b\wedge c)$. (Alkalmazzuk a lemmát az $x=a$, $y=b\wedge c$, $u=b\wedge c$, $v=c$ elemekre.) Eszerint a modularitáshoz elegendő, hogy **(L5)**-ben ill. **(L5′)**-ben '$\leq$' teljesüljön.

9.5.4 Definíció: az L háló disztributív, ha teljesül rá az alábbi két ekvivalens feltétel:

(L6) $a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)$ $\forall a,b,c\in L$-re,
(L6′) $a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$ $\forall a,b,c\in L$-re.

Mivel ezek egymás duálisai, L disztributív $\Leftrightarrow$ duálisa disztributív.

Persze először be kell látnunk, hogy **(L6)** $\Leftrightarrow$ **(L6′)**, amihez a dualitás miatt elég **(L6)** $\Rightarrow$ **(L6′)**:

$$(a\wedge b)\vee(a\wedge c)\underset{\textbf{(L6)}}{=}((a\wedge b)\vee a)\wedge((a\wedge b)\vee c)\underset{\textbf{(L4)}}{=}a\wedge((a\wedge b)\vee c)\underset{\textbf{(L6)}}{=}a\wedge((a\vee c)\wedge(b\vee c))=(a\wedge(a\vee c))\wedge(b\vee c)\underset{\textbf{(L4)}}{=}a\wedge(b\vee c).$$

9.5.5 Állítás: $a\vee(b\wedge c)\leq(a\vee b)\wedge(a\vee c)$ minden hálóban teljesül, tehát a disztributivitáshoz elég, hogy **(L6)**-ban '$\geq$' teljesüljön. (Alkalmazzuk a lemmát az $x=a$, $y=b\wedge c$, $u=b\wedge c$ $v=b\wedge c$ esetre.) Hasonlóan minden hálóban igaz $a\wedge(b\vee c)\geq(a\wedge b)\vee(a\wedge c)$, tehát **(L6′)**-ben '$\leq$' elég a disztributivitáshoz.

Megjegyzés: a jövőben az axióma mindkét változatára **(L6)** néven fogok hivatkozni.

Állítás: minden lánc disztributív (esetszétválasztással bizonyítható).

9.5.6 Állítás: ha L disztributív, akkor moduláris. Ha ugyanis **(L6)** és $a\leq c$, akkor $a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)=(a\vee b)\wedge c$.

9.5.7 Állítás: legyen $L_1\leq L$. Ekkor ha L moduláris, akkor L_1 is és ha L disztributív, akkor L_1 is.

Bizonyítás: az **(L5′)** illetve **(L6)** axiómák nyilvánvalóan öröklődnek minden $\wedge,\vee$-re zárt részhalmazra.

9.5.8 Állítás: $N(G)$ moduláris.

Bizonyítás: **9.5.3** szerint elég belátni, hogy ha $A,B,C\triangleleft G$ és $A\subseteq C$, akkor $AB\cap C\subseteq A(B\cap C)$. A bal oldal egy tipikus x eleme felírható egyrészt $x=ab$: $a\in A, b\in B$ alakban, másrészt eleme C-nek, tehát $ab\in C$. Ezt balról szorozva $a^{-1}\in A\subseteq C$-vel $b\in C$, azaz $b\in B\cap C$ és $ab\in A(B\cap C)$. Ezt akartuk belátni.

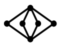
9.5.9 Állítás: részmodulusháló moduláris.

Bizonyítás: nyilván elég az állítást baloldali R-modulusokra belátni. Az kell, hogy ha $A \subseteq C$ és B egyaránt ${}_R M$ részmodulusai, akkor $(A+B) \cap C \subseteq A+(B \cap C)$. A bal oldal egy tipikus eleme $a+b=c$ alakba írható, ahol $a \in A, b \in B, c \in C$. Ekkor $b=c-a \in C$, azaz $b \in B \cap C$, kész vagyunk.

9.5.10 Következmény: ideálháló moduláris (továbbá minden bal- és jobbideálháló is).

9.5.11 Állítás: $N_5=$  nem moduláris; $L=$  moduláris, de nem disztributív.

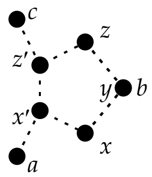
Bizonyítás: legyenek  elemei rendre $1, c, b, a, 0$. Ekkor $a \le c$, de $(a \vee b) \wedge c = 1 \wedge c = c \ne a = a \vee 0 = a \vee (b \wedge c)$.

Legyenek  elemei rendre $1, c, b, a, 0$. Ekkor $a \wedge (b \vee c) = a \wedge 1 = a \ne 0 = 0 \vee 0 = (a \wedge b) \vee (a \wedge c)$, tehát L nem disztributív. Másrészt L részhálója $N(Z_3 \times Z_3) = L(Z_3 \times Z_3) =$  -nak, ami **9.5.8** szerint moduláris. **9.5.7** alapján L is moduláris.

9.5.12 Tétel (Dedekind): L pontosan akkor moduláris, ha nincs N_5-tel izomorf részhálója.

Bizonyítás: $\Rightarrow$: ha $N_5 \le L$, akkor **9.5.7** és **9.5.11** szerint L nem moduláris.

$\Leftarrow$: tegyük fel, hogy a L nem moduláris, azaz valamely $a \le c, b$ L-beli elemekre $a \vee (b \wedge c) < (a \vee b) \wedge c$. Legyen $y=b$, $z=a \vee b$, $x=b \wedge c$, $x'=a \vee x$, $z'=a \vee x$, $z'=z \wedge c$. Feltételeink szerint $x'<z'$.



Először azt látjuk be, hogy $N=\{x, x', y, z, z'\} \le L$, azaz hogy zárt a $\wedge, \vee$ műveletekre. $x \le x' < z' \le z$ lánc, így ez a négy elem zárt a műveletekre és $x \le y \le z$ miatt ez a három is. Azt kell már csak belátnunk, hogy $z' \vee y$, $x' \wedge y$, $x' \vee y$ és $z' \wedge y$ is N elemei.

$x' \vee y = (a \vee x) \vee b \underset{(L2)}{=} a \vee ((b \wedge c) \vee b) \underset{(L4)}{=} a \vee b = z$. Felhasználva $z' > x'$-t és $z \ge z', y$-t $z \ge z' \vee y \ge x' \vee y = z$, amiből $z' \vee y = z$. A duális számolás: $y \wedge z' = b \wedge (z \wedge c) = (b \wedge (b \vee a)) \wedge c = b \wedge c = x$ és $x \le y \wedge x' \le y \wedge z' = x$, amiből $y \wedge x' = x$. N tehát valóban részháló. Vegyük észre, hogy ezek szerint $x' \le z', y \in N$-re $(x' \vee y) \wedge z' = z \wedge z' = z' > x' = x' \wedge z = x' \vee (y \wedge z')$, tehát N nem moduláris. Eszerint $N \simeq N_5$, mert N_5 az egyetlen legfeljebb ötelemű nem-moduláris háló.

9.6 Komplementumos háló, Boole-algebra

9.6.1 Definíció: legyen L korlátos háló, $a \in L$. $a' \in L$ komplementere avagy komplementuma a-nak, ha $a \vee a' = 1$ és $a \wedge a' = 0$. Ekkor persze a is komplementuma a'-nek.

Példák:
- korlátos láncban csak 0-nak és 1-nek van komplementuma.
- -ben az üres körrel jelölt elemnek két komplementuma van.
- a  hálóban a két üres körrel jelölt elem egymás egyértelmű komplementuma.

9.6.2 Definíció: az L korlátos háló komplementumos, ha minden elemének van komplementuma.

9.6.3 Lemma: ha az L disztributív háló a elemének van komplementuma, akkor egyértelmű.

Bizonyítás: legyen a' és a'' egyaránt komplementuma a-nak. Ekkor

$$a' = a' \wedge 1 = a' \wedge (a \vee a'') \underset{(L6)}{=} (a' \wedge a) \vee (a' \wedge a'') = 0 \vee (a' \wedge a'') = a' \wedge a'' \;\Rightarrow\; a' \le a''.$$

Hasonlóan $a'' \le a'$, amiből $a' = a''$.

9.6.4 Definíció: az L háló Boole-algebra, ha korlátos, disztributív és minden elemének van komplementuma.

Megjegyzés: a Boole-algebra egy olyan struktúra, ahol adott két kétváltozós ($\wedge, \vee$), egy egyváltozós ($*: a \mapsto a'$ – komplementum hozzárendelése) és két nullaváltozós ($0, 1$) művelet.

Megjegyzés: tetszőleges $\mathbf{H}$ halmazra $\mathcal{P}(\mathbf{H})$-ból az alábbi műveletekkel tudunk Boole-algebrát csinálni: $\mathbf{A} \wedge \mathbf{B} := \mathbf{A} \cap \mathbf{B}$, $\mathbf{A} \vee \mathbf{B} := \mathbf{A} \cup \mathbf{B}$, $\mathbf{A}' := \mathbf{H} \setminus \mathbf{A}$, $0 = \emptyset$, $1 = \mathbf{H}$. Ez ráadásul teljes háló, hiszen egy $\mathbf{H}$ halmaz részhalmazai tetszőleges halmazának van metszete és uniója, ami megfelel infimumnak ill. szuprémumnak.

Ezen a módon azonban csak olyan számosságú Boole-algebrát tudunk konstruálni, amely valamely κ számosságra 2^κ alakú, tehát pl. $\aleph_0$ számosságút nem. Tekintsük ezért tetszőleges $\kappa \ge \aleph_0$-ra egy κ számosságú $\mathbf{K}$

halmaz véges és ko-véges (véges komplementerű) részhalmazait a fenti műveletekkel. Egy κ számosságú Boole-algebrát kapunk, amely $\mathcal{P}(\mathbf{K})$ részhálója.

9.6.5 Definíció: az R gyűrű Boole-gyűrű, ha $\forall a\in R$: $a^2=a$. Ekkor $2a=(2a)^2=4a^2=4a$ miatt $a+a=0$ minden $a\in R$ -re. Továbbá $ab=(a+b)^2-a^2-b^2-ba=(a+b)-a-b+ba=ba$, tehát minden Boole-gyűrű kommutatív.

9.6.6 Tétel: minden Boole-algebra egyben egységelemes Boole-gyűrű is és minden egységelemes Boole-gyűrű egyben Boole-algebra is (a bizonyításon látszani fog, hogy ez alatt tulajdonképpen mit értünk).

Lemma: tetszőleges B Boole-algebrában $(a\vee b)'=a'\wedge b'$ és $(a\wedge b)'=a'\vee b'$.

Bizonyítás: a dualitás miatt elég az elsőt belátni:

$$(a\vee b)\vee(a'\wedge b')\underset{\textbf{(L6)}}{=}\big((a\vee b)\vee a'\big)\wedge\big((a\vee b)\vee b'\big)=(b\vee a\vee a')\wedge(a\vee b\vee b')=1\wedge 1=1$$
$$\text{és } (a\vee b)\wedge(a'\wedge b')\underset{\textbf{(L6)}}{=}\big(a\wedge(a'\wedge b')\big)\vee\big(b\wedge(a'\wedge b')\big)=(a\wedge a'\wedge b)\vee(a'\wedge b\wedge b')=0\vee 0=0.$$

Tehát $(a\vee b)$ és $(a'\wedge b')$ valóban egymás komplementumai.

Bizonyítás: legyen $(B,\wedge,\vee,*)$ Boole-algebra. Definiáljuk a $+,\cdot:B\times B\to B$ műveleteket az alábbi módon: $(a+b):=(a\wedge b')\vee(a'\wedge b)$ és $ab:=a\wedge b$. Azt akarjuk belátni, hogy $(B,+,\cdot)$ Boole-gyűrű, amelyben 0 nullelem, 1 egységelem.

(1) $+$ kommutatív, mert $\wedge,\vee$ kommutativitása miatt az összeadás definíciója szimmetrikus.

(2) a lemma felhasználásával

$$(a+b)'=\big((a\wedge b')\vee(a'\wedge b)\big)'=(a\wedge b')'\wedge(a'\wedge b)'=(a'\vee b)\wedge(a\vee b'),\quad \text{ami } \textbf{(L6)} \text{ szerint}$$
$$(a'\wedge a)\vee(a'\wedge b')\vee(b\wedge a)\vee(b\wedge b')=(a'\wedge b')\vee(a\wedge b).\quad \text{Ebből pedig}$$
$$(a+b)+c=\big((a+b)\wedge c'\big)\vee\big((a+b)'\wedge c\big)=\Big(\big((a\wedge b')\vee(a'\wedge b)\big)\wedge c'\Big)\vee\Big(\big((a'\wedge b')\vee(a\wedge b)\big)\wedge c\Big)\underset{\textbf{(L6)}}{=}$$
$$(a'\wedge b\wedge c')\vee(a\wedge b'\wedge c')\vee(a'\wedge b'\wedge c)\vee(a\wedge b\wedge c).$$

Minthogy $\wedge,\vee$ asszociatív és kommutatív, ez szimmetrikus kifejezése a,b,c-nek, amiből $+$ asszociativitása következik.

(3) $(a+0)=(a\wedge 0')\vee(a'\wedge 0)=(a\wedge 1)\vee 0=a\vee 0=a$. Mellesleg $(a+a)=(a\wedge a')\vee(a'\wedge a)=0\vee 0=0$.

(4) a szorzás asszociatív, mert $\wedge$ asszociatív.

(5) 1 egységeleme a szorzásnak, mert $a\wedge 1=a$.

(6) a szorzás disztributív az összadásra, azaz $(a+b)c=ab+ac$.

$$(a+b)\cdot c=\big((a\wedge b')\vee(a'\wedge b)\big)\wedge c\underset{\textbf{(L6)}}{=}(a\wedge b'\wedge c)\vee(a'\wedge b\wedge c)\text{ és } ac+bc=\big((a\wedge c)'\wedge(b\wedge c)\big)\vee\big((a\wedge c)\wedge(b\wedge c)'\big)=$$
$$\big((a'\vee c')\wedge b\wedge c\big)\vee\big(a\wedge c\wedge(b'\vee c')\big)\underset{\textbf{(L6)}}{=}(a'\wedge b\wedge c)\vee(c'\wedge b\wedge c)\vee(a\wedge c\wedge b')\vee(a\wedge c\wedge c')=(a'\wedge b\wedge c)\vee 0\vee(a\wedge c\wedge b')\vee 0.$$

(7) $a^2\underset{\textbf{(L1)}}{=}a$, kész is vagyunk.

Legyen R Boole-gyűrű. Legyen $a\vee b:=a+b-ab$ és $a\wedge b:=ab$. Azt akarjuk belátni, hogy $(R,\wedge,\vee)$ Boole-gyűrű, amelynek alsó korlátja R nulleleme, felső korlátja R egységeleme.

(1) $a\wedge a=a^2=a$ és $a\vee a=a+a-a^2=a+a-a=a$, tehát **(L1)** teljesül.

(2) minden Boole-gyűrű kommutatív, így $\wedge,\vee$ definíciója szimmetrikus, tehát $\wedge,\vee$ kommutatív $\Rightarrow$ **(L2)**

(3) $\vee$ asszociatív, mert $(a\vee b)\vee c=(a+b-ab)+c-(a+b-ab)c=a+b+c-ab-bc-ca+abc$ szimmetrikus kifejezése a,b,c -nek. $\wedge$ asszociatív, mert a szorzás asszociatív. $\Rightarrow$ **(L3)**.

(4) $(a\wedge b)\vee a=ab+a-aba=a+ab-a^2b=a$ és $(a\vee b)\wedge a=(a+b-ab)a=a^2+ba-aba=a$ $\Rightarrow$ **(L4)**

(5) $(a\vee b)\wedge c=(a+b-ab)c=ac+bc-abbc=ac\vee bc=(a\wedge c)\vee(b\wedge c)$ $\Rightarrow$ **(L6)**

(6) $0\wedge a=0\cdot a=0$ és $1\wedge a=1\cdot a=a$, azaz $0\le a\le 1$ teljesül minden $a\in R$-re.

(7) $a\wedge(1-a)=a\cdot(1-a)=a-a^2=0$ és $a\vee(1-a)=a+1-a-a\cdot(1-a)=1$, tehát minden $a\in R$-nek van komplementuma, mégpedig $a'=1-a$. Ezzel az állítást beláttuk.

Megjegyzés: (aki akarja, kiszámolhatja ...) a fenti két megfeleltetés egymás inverze, tehát egy bijekciót találtunk a Boole-algebrák és az egységelemes Boole-gyűrűk között.

9.7 Ideál, prímideál stb. Stone-tétel

9.7.1 Definíció: az L háló $A\notin\{\emptyset,L\}$ részhalmaza ideál – jelölése $A\lhd L$ – , ha megfelel az alábbi követelményeknek:

(IL1) $\forall a,b\in A\colon a\vee b\in A$,

(IL2) $\forall a\in A,x\in L\colon a\wedge x\in A$.

Ez utóbbi feltétel ekivalens azzal, hogy

(IL2′) $a\in A,b\leq a\Rightarrow b\in A$,

hiszen $\forall x\in L\colon b_x=a\wedge x\leq a$ és minden $b\leq a$ előáll $a\wedge x$ alakban $x=b$ választással.

Megjegyzések:

- alulról korlátos hálóban $A\lhd L\Rightarrow 0\in A$ nyilván.
- $A\lhd L\Rightarrow A\leq L$, azaz minden ideál részháló.
- ideálok tetszőleges metszete ideál (ill. alulról nem korlátos hálóban lehet $\emptyset$ is).
- ideálok láncának uniója ideál (ill. felülről nem korlátos hálóban lehet az egész L is).

9.7.2 Definíció: legyen L háló, $a\in L$. Ekkor a által generált főideál $(a]=\{x\in L\,|\,x\leq a\}$. Ez valóban ideál és persze a legszűkebb az a-t tartalmazó ideálok közül.

9.7.3 Definíció: $P\leq L$ prímideál, ha egyrészt ideál, másrészt $a\wedge b\in P\Rightarrow(a\in P$ vagy $b\in P)$. Ezzel ekvivalens, hogy L minden véges H részhalmazára $inf(H)\in P\Rightarrow P\cap H\neq\emptyset$.

9.7.4 Definíció: legyen L háló, $F\subseteq L,F\notin\{\emptyset,L\}$. Ekkor F duális ideál avagy filter, ha $\forall a,b\in F\colon a\wedge b\in F$ és $\forall a\in F,x\in L\colon a\vee x\in F$. Ez utóbbi persze ekvivalens $a\in F,b\geq a\Rightarrow b\in F$-el. Minden duális ideál részháló. Duális ideálok metszete duális ideál, duális ideálok láncának uniója duális ideál (kivéve ha $\emptyset$ vagy az egész L, de korlátos hálóban ez nem fordulhat elő).

9.7.5 Definíció: $U\subseteq L$ duális prímideál avagy ultrafilter, ha duális ideál, továbbá $a\vee b\in U\Rightarrow(a\in U$ vagy $b\in U)$.

9.7.6 Állítás: $P\subseteq L$-re az alábbi három feltétel ekvivalens ($U=L\setminus P$):

(1) P prímideál,

(2) P ideál és U duális ideál,

(3) U duális prímideál.

Bizonyítás: a dualitás miatt elég belátni, hogy **(1)** $\Leftrightarrow$ **(2)**.

$\Rightarrow$: azt kell belátnunk, hogy $x,y\in U$-ra $x\wedge y\in U$ és $x\in U,a\in L$-re $a\vee x\in U$ −re $a\vee x\in U$. Ha $x,y\notin P$, akkor $x\wedge y\notin P$ (P prímideál), így az első feltétel teljseül. Ha $x\in U,a\in L$, akkor $(a\vee x)\wedge x=x\notin P$ miatt egyik tényező sem lehet P-ben (P ideál), így $a\vee x\in U$.

$\Leftarrow$: az kell, hogy ha $a,b\notin P$, akkor $a\wedge b\notin P$. Mivel U duális ideál, $a,b\in U$-ból valóban következik $a\wedge b\in U$.

9.7.7 Stone-tétel: legyen az L disztributív hálóban $b\nleq a$. Ekkor a és b prímideállal szétválasztható, azaz található olyan $P\lhd L$ prímideál, melyre $a\in P$ és $b\notin P$ ($b\leq a$ esetén ebben hiába is reménykednénk, hiszen $b\in(a]$ lenne).

Bizonyítás: vegyük az a-t tartalmazó, b-t nem tartalmazó I ideálok $\mathcal{X}$ halmazát. Ez nem üres, mert $b\notin(a]\lhd L$. $\mathcal{X}$-beli ideálok láncának uniója is $\mathcal{X}$-beli ideál, tehát a Zorn-lemma szerint $\mathcal{X}$-nek van maximális eleme. Jelölje ezt P. Lássuk be, hogy P prímideál.

$\lightning$ $\exists x,y\notin P\colon x\wedge y\in P$. Legyen $I=\{u\in L\,|\,\exists p\in P\colon u\leq x\vee p\}$. Ez ideál lesz, mert lefelé zárt ($u\in I,x\leq u\Rightarrow x\in I$ nyilván) és $u_1,u_2\in I$ esetén alkalmas $p_1,p_2\in P$-re $u_1\leq x\vee p_1$ és $u_2\leq x\vee p_2$, amiből $u_1\vee u_2\leq x\vee(p_1\vee p_2)$. Ekkor $u_1\vee u_2\in I$, hiszen $p_1\vee p_2\in P$.

$P \subset I$, mert $p \in P$-re $p \le x \vee p$ miatt $p \in I$ és $x \in I \setminus P$ miatt $I \ne P$. P maximalitása folytán ez csak $b \in I$ esetén lehetséges, tehát alkalmas $p' \in P$-re $b \le x \vee p'$. Ugyanígy adódik, hogy valamely $p'' \in P$ esetén $b \le y \vee p''$. Ekkor $p = p' \vee p''$ választással $p \in P$ és $b \le x \vee p$, $b \le y \vee p$. Ezek szerint $b \le (x \vee p) \wedge (y \vee p) \underset{\textbf{(L6)}}{=} (x \wedge y) \vee p \in P$, ↯.

Következmény: a fenti feltételek mellett b-t tartalmazó, a-t elkerülő duális prímideál is létezik, például a fenti P prímideál komplementere.

9.7.8 Definíció: az L háló halmazgyűrű, ha előáll valamely $\mathbf{H}$ halmazra $\mathcal{P}(\mathbf{H})$ részhálójaként (tehát nem üres, továbbá zárt a véges (de legalább egytényezős) metszetre és unióra). $\mathcal{P}(\mathbf{H})$ mindig disztributív, így minden halmazgyűrű is disztributív. (Ekkor L a szimmetrikus differencia, metszet műveletekre kommutatív gyűrűt alkot.)

9.7.9 Definíció: B „halmaztest", ha alkalmas $\mathbf{H}$ halmazra $\mathcal{P}(\mathbf{H})$ rész-Boole-algebrája, azaz B nem üres, zárt a véges metszetre, a véges unióra és a komplementumképzésre. (Ekkor $\emptyset \in B$, hiszen egyrészt az üres unió definíció szerint $\emptyset$, másrészt $\exists \mathbf{A} \in B$, azaz $\emptyset = \mathbf{A} \wedge \mathbf{A}' \in B$; továbbá $\mathbf{H} = \emptyset' \in B$.) (Az elnevezés nem egészen szerencsés, ugyanis ez semmilyen, a Boole-algebra struktúrához kapcsolódó műveletre nem alkot testet.)

9.7.10 Tétel: minden L disztributív háló izomorf egy halmazgyűrűvel. Amennyiben még Boole-algebra is, úgy egy halmaztesttel.

Bizonyítás: legyen H az L-beli duális prímideálok halmaza és legyen $a \in L$-re $H(a) = \{U \in H \mid a \in U\}$.

A Stone-tétel következménye szerint $H(x) = H(y) \Rightarrow x = y$, tehát $H: L \to \mathcal{P}(H)$ injektív. Ha L korlátos, akkor $H(0) = \emptyset$, mert a 0 minden (prím)ideálnak eleme és $H(1) = H$, mert 1 minden duális (prím)ideálnak eleme. Azt kell még belátnunk, hogy H művelettartó. (Jelöljön U a bizonyítás közben végig tetszőleges duális prímideált.)

(1) ha $x \in U, y \in U$, akkor $x \wedge y \in U$, tehát $H(x \wedge y) \subseteq H(x) \cap H(y)$. Ha $x \wedge y \in U$, akkor $x \wedge y \le x, y$ miatt $x, y \in U$, amiből következik a másik irányú tartalmazás. Összevetve $H(x \wedge y) = H(x) \cap H(y)$.

(2) $U \in H(x \vee y) \Leftrightarrow x \vee y \in U \Leftrightarrow \{x, y\} \cap U \ne \emptyset \Leftrightarrow \left(U \in H(x) \text{ vagy } U \in H(y)\right) \Leftrightarrow U \in \left(H(x) \cup H(y)\right)$.

(3) ha L Boole-algebra, akkor azt is be kell látnunk, hogy $H(x') = H \setminus H(x)$. $x \vee x' = 1 \in U$ miatt x, x' közül legalább az egyik eleme U-nak. $x \wedge x' = 0 \notin U$ miatt legfeljebb az egyik, összevetve pontosan az egyik. Tehát $x \in U \Leftrightarrow x' \notin U$, amiből $U \in H(x) \Leftrightarrow U \notin H(x')$, a bizonyítandó állítás.

9.8 Moduláris és disztributív hálók II.; mediáns

9.8.1 Definíció: legyen az L hálóban $a \le b$. Ekkor az $[a, b]$ intervallum alatt a $\{x \in L \mid a \le x \le b\}$ korlátos részhálót értjük.

9.8.2 Definíció: az L háló relatív komplementumos, ha $[a, b]$ $\forall a, b \in L, a \le b$ esetén komplementumos. Az $[a, b]$-beli komplementumot relatív komplementumnak hívjuk.

Megjegyzés: ha L relatív komplementumos és korlátos, akkor nyilván komplementumos. Csak sajnos abból, hogy relatív komplementumos, nem következik, hogy korlátos. (Vegyük a véges sok hely kivételével 0-t felvevő $f: \mathbb{Z} \to \{0, 1\}$ függvények L halmazát. Legyen a reláció $f \le g \Leftrightarrow \forall k \in \mathbb{Z}: f(k) \le g(k)$. Ebben $f \le g$ esetén $[f, g] \simeq \{0, 1\}^{|\{k: f \ne g\}|}$ Boole-algebra, hiszen, de L-nek nincs felső korlátja.) A másik irányú implikáció sem teljesül, hiszen  komplementumos háló, de az üres pontok alkotta intervalluma nem komplementumos.

Most kissé más formában tudunk kimondani egy korábbi tételt:

9.8.3 Tétel: L moduláris $\Leftrightarrow$ nincs olyan $[d, e]$ intervalluma, amelyben valamelyik b elemnek két összhasonlítható komplementuma ($a < c$) van. Ugyanis ha van ilyen, akkor $\{e, c, b, a, d\}$ egy N_5-tel izomorf részháló, ha pedig L-nek van egy N_5-tel izomorf részhálója, akkor annak minimális és maximális elemét d-nek ill e-nek, a többit a szokott módon c, b, a-nak keresztelve $[d, e]$-ben c és a egyaránt komplementuma b-nek és $a < c$.

9.8.4 Állítás: $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \le (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$.

Bizonyítás: a jobb oldal bármely tagja felülről becsüli a bal oldal bármely tagját, mert a, b, c valamelyike elvágja őket. Eszerint a bal oldalon álló tagok bármelyike felülről becsüli a bal oldali tagok szuprémumát, így a jobb oldali tagok infimuma is.

9.8.5 Definíció: amennyiben $(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$, úgy ezt a,b,c mediánsának nevezzük és $med(a,b,c)$-vel jelöljük.

9.8.6 Tétel: **(1)** L moduláris $\Leftrightarrow$ $a\leq c$ esetén $\exists med(a,b,c)$, **(2)** L disztributív $\Leftrightarrow$ $\forall a,b,c$: $\exists med(a,b,c)$.

Bizonyítás: **(1)** azt kell belátnunk, hogy $a\leq c$ esetén $\exists med(a,b,c)$ ekvivalens $a\vee(b\wedge c)=(a\vee b)\wedge c$ -vel.

$a\wedge b\leq a$, $a\wedge c=a$ miatt $(a\wedge b)\vee(a\wedge c)=a$, amiből $(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)=\big((a\wedge b)\vee(a\wedge c)\big)\vee(b\wedge c)=a\vee(b\wedge c)$.
$c\leq b\vee c$, $c=a\vee c$ miatt $c=(a\vee c)\wedge(b\vee c)$, amiből $(a\vee b)\wedge(b\vee c)\wedge(c\vee a)=(a\vee b)\wedge\big((a\vee c)\wedge(b\vee c)\big)=(a\vee b)\wedge c$.

E két egyenlőség bal oldala pontosan akkor egyezik meg, ha a jobb oldaluk megegyezik, és épp ezt akartuk belátni.

(2) Minthogy mindkét feltételből következik a modularitás, **(L5)**-öt felhasználhatjuk. Kezdjük a $\Rightarrow$ iránnyal:

$$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)\underset{\textbf{(L6)}}{=}\big((a\wedge b)\vee(b\wedge c)\vee c\big)\wedge\big((a\wedge b)\vee(b\wedge c)\wedge a\big)=\ldots$$

Beírva $(a\wedge b)\vee a=a$-t és $(b\wedge c)\vee c=c$-t

$$\ldots=\big((a\wedge b)\vee c\big)\wedge\big(a\vee(b\wedge c)\big)\underset{\textbf{(L6)}}{=}(a\vee c)\wedge(b\vee c)\wedge(a\vee b)\wedge(b\vee c)=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)\,.$$

$\Leftarrow$: $a=a\wedge(a\vee b)\wedge(a\vee c)$, mert a két új tag $\geq a$. Eszerint

$$a\wedge(b\vee c)=a\wedge\big((a\vee b)\wedge(c\vee a)\wedge(b\vee c)\big)=a\wedge med(a,b,c)=$$
$$a\wedge\big((b\wedge c)\vee(a\wedge b)\vee(c\wedge a)\big)\underset{\textbf{(L5)}}{=}(a\wedge b\wedge c)\vee\big[(a\wedge b)\vee(a\wedge c)\big]$$

(**(L5)**-öt $c^{*}=(a\wedge b)\vee(c\wedge a)\geq a$, $b^{*}=b\wedge c$-re alkalmaztuk.) A szögletes zárójelben lévő tagok majorálják $(a\wedge b\wedge c)$-t, tehát az elhagyható és $a\wedge(b\vee c)=\ldots=(a\wedge b)\vee(a\wedge c)$. Persze beláthattuk volna az állítás duálisát is.

9.8.7 Tétel: az alábbi feltételek ekvivalensek:

(1) L disztributív,
(2) L-nek nincs -vel vagy -vel izomorf részhálója,
(3) L-ben nincs olyan $[d,e]$ intervallum, ahol valamely b elemnek egynél több komplementuma van.

Bizonyítás: ha L nem moduláris, akkor **9.8.3** szerint egyik feltétel sem teljesül. Szorítkozhatunk tehát arra az esetre, amikor L moduláris.

(1) $\Rightarrow$ **(3)**: ↿ L disztributív, de van ilyen intervallum. Legyen a két komplementum a és c. Feltételeink szerint $a\vee c=e\wedge(a\vee c)=(a\vee b)\wedge(a\vee c)=a\vee(b\wedge c)=a\vee d=a$, azaz $a\geq c$, de **9.8.3** szerint a és c nem összehasonlítható össze, ↯.

(2) $\Rightarrow$ **(1)**: Az áttekinthetőség kedvéért a $\wedge$ műveletet a most következő számolásokban nem fogjuk kiírni és mint magasabb prioritású műveletet kezeljük (azaz pl. $xy\vee z$ a $(x\wedge y)\vee z$ kifejezést jelöli). Vegyünk egy L moduláris, de nem disztributív hálót. Ekkor alkalmas p,q,r elemekre $\nexists med(p,q,r)$. **9.8.4** szerint $u=pq\vee qr\vee rp$, $v=(p\vee q)(q\vee r)(r\vee q)$ választással $u<v$. Legyen $a=u\vee pv=(u\vee p)v$, $b=u\vee qv=(u\vee q)v$ és $c=u\vee rv=(u\vee r)v$. Tekintsük a $H=\{v,a,b,c,u\}\subseteq L$ halmazt. Ebben $u<a,b,c\leq v$.

$a=u\vee pv=pq\vee qr\vee rp\vee p(p\vee q)(q\vee r)(r\vee p)$. A soktényezős metszetben $p\vee q$ és $r\vee p$ felülről becsüli p−t, tehát felesleges; marad $a=pq\vee qr\vee rp\vee p(q\vee r)$. Itt $pq,pr\leq p(q\vee r)$, így pq és pr elhagyható és $a=qr\vee p(q\vee r)$. Hasonlóan $b=rp\vee q(r\vee p)$.

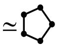
Tehát $a\vee b=qr\vee p(q\vee r)\vee rp\vee q(r\vee p)$, amiből $qr\leq q(r\vee p)$ és $rp\leq p(q\vee r)$ alapján $a\vee b=p(q\vee r)\vee q(r\vee p)$. $a^{*}=p(q\vee r)$, $b^{*}=q$, $c^{*}=r\vee p$ behelyettesítéssel (ekkor $a^{*}\leq p\leq c^{*}$) kihasználva a modularitást:

$$a\vee b=p(q\vee r)\vee q(r\vee p)=a^{*}\vee b^{*}c^{*}=(a^{*}\vee b^{*})c^{*}=\big(p(q\vee r)\vee q\big)(r\vee p)=\big[q\vee p(q\vee r)\big](r\vee p)\,.$$

A szögletes zárójelben ismét alkalmazhatjuk **(L5)**-öt, hiszen $q\leq q\vee r$:

$$a\vee b=\big(q\vee p(q\vee r)\big)(r\vee p)=\big((q\vee p)(q\vee r)\big)(r\vee p)=v\,.$$

Minthogy a,b,c megadása szimmetrikus, $a\vee b=b\vee c=c\vee a=v$. Ráadásul meghatározásuk egyben önmaga duálisa is, tehát $a\wedge b=b\wedge c=c\wedge a=u$. Mindezt összevetve $H=\{v,a,b,c,u\}$ zárt a műveletekre, tehát részháló. Már csak azt kell belátni, hogy minden eleme különböző.

Lemma: ha az L' legfeljebb ötelemű háló moduláris, de nem disztributív, akkor $L\simeq$ .

Bizonyítás: tekintsük a $\mathbf{H}=\{1,2,3,4\}$ halmaz következő részhalmazait: $\emptyset,\{1\},\{1,2\},\{1,3\},\{1,2,3\},\mathbf{H}$. Ez metszetre, unióra zárt részhalmaza $\mathcal{P}(\mathbf{H})$-nak, hálója tehát disztributív. Ezen háló ábrája , ami azért jó, mert N_5 és  kivételével minden legfeljebb ötelemű hálót részhálóként tartalmaz, így ezek mind disztributívak.

Ha H nem disztributív, akkor a lemma szerint legalább ötelemű, így személyesen . Ha disztributív lenne, akkor például $a=a\vee u=a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)=v\wedge v=v$, tehát $a=v$ is igaz lenne. Véve az állítás – szintén igaz – duálisát $u=a$, ami a $u<v$ kiindulófeltétellel összeegyeztethetetlen. H tehát mégsem disztributív így $\simeq H\leq L$.

(3) $\Rightarrow$ **(2)** ↯ van -vel izomorf részháló, de nincs tiltott intervallum. Legyen  felső pontja e, alsó pontja d, a többi a,b és c. Ekkor $[d,e]$-ben a,b és c közül bármely kettő relatív komplementuma egymásnak, ↯.

9.9 Transzponált-izomorfizmus és alkalmazásai; Jordan-Dedekind, Kuros-Ore tételek

9.9.1 Tétel (transzponált-izomorfizmus): legyen L moduláris, $a,b\in L$. Ekkor $[a\wedge b,a]\simeq[b,a\vee b]$.

Bizonyítás: legyen $\varphi:[a\wedge b,a]\to[b,a\vee b]$ az $x\mapsto x\vee b$ leképezés, $\psi:[b,a\vee b]\to[a\wedge b,a]$ pedig $y\mapsto y\vee a$. Ekkor $x\varphi\psi=(x\vee b)\wedge a\underset{(L5)}{=}x\vee(b\wedge a)=x$, hiszen $a\wedge b\leq x$. Továbbá $y\psi\varphi=(y\wedge a)\vee b\underset{(L5)}{=}y\wedge(b\vee a)=x$ hasonlóan. Eszerint ez a két leképezés egymás inverze. Még azt kell belátni, hogy φ és ψ rendezéstartó, tehát hogy $x\leq x'\Rightarrow x\vee b\leq x'\vee b$ és $y\leq y'\Rightarrow y\wedge a\leq y'\wedge a$, ami *inf*, *sup* definíciójából nyilvánvaló.

9.9.2 Jordan-Dedekind-tétel: legyen L moduláris, $a\leq b$ és $a\prec x_1\prec x_2\prec\ldots\prec x_n=b$. Ekkor minden $a<y_1<y_2<\ldots<y_k=b$ láncra $k\leq n$ és ha ez utóbbi lánc maximális, akkor $k=n$. (Ezekből következik, hogy pontosan akkor maximális, ha $n=k$.)

Vegyük észre, hogy elég az állítás első felét ($k\leq n$) belátni. Ugyanis ha az $a\prec x_1\prec x_2\prec\ldots\prec x_n=b$ és az $a\prec y_1\prec y_2\prec\ldots\prec y_k=b$ láncok egyaránt maximálisak, akkor a tétel első feléből $k\leq n$ és $n\leq k$ egyaránt következik, így $n=k$.

Bizonyítás: teljes indukció n-re. $n=1$-re az állítás következik '$\prec$' definíciójából, mely szerint $a\prec y_1=b$ esetén ez az egyetlen $a<y_1<\ldots<y_k=b$ lánc.

Legyen most $n\geq 2$ és tegyük fel, hogy az állítás minden n-nél kisebb pozitív egészre teljesül. Legyen $a\prec x_1\prec x_2\prec\ldots\prec x_n=b$ és $a<y_1<y_2<\ldots<y_k=b$. Két esetet különböztetünk meg:

1. eset: $x_1\leq y_1$. Ekkor alkalmazva az indukciós feltevést az $x_1\prec x_2\prec\ldots\prec x_n=b$ és az $x_1<y_2<\ldots<y_k=b$ láncokra kapjuk, hogy $k-1\leq n-1$, tehát $k\leq n$.

2. eset: $x_1\not\leq y_1$. Ekkor $a\leq x_1\wedge y_1<x_1$ és $a\prec x_1$ alapján $x_1\wedge y_1=a$. **9.9.1** szerint ekkor $[a,x_1]=[x_1\wedge y_1,x_1]\simeq[y_1,x_1\vee y_1]$, azaz $y_1\prec(x_1\vee y_1)$. Jelölje $x_1\vee y_1$-t y_2^*. Az indukciós feltevés szerint egy tetszőleges $x_1<y_2^*<x_3^*<\ldots<x_m^*=b$ láncra $m\leq n-1$, hiszen $x_1\prec x_2\prec\ldots\prec x_n=b$. Így egy $y_2^*<x_3^*<\ldots<x_m^*=b$ lánc hossza legfeljebb $n-2$. Minthogy ezek között nincs tetszőleges hosszú, van köztük maximális, $y_2^*\prec y_3^*\prec\ldots\prec y_m^*=b$. Ekkor $y_1\prec y_2^*$ miatt $y_1,y_2^*,\ldots,y_m^*=b$ egy m hosszú maximális lánc, $m\leq n-1$. Az indukciós feltevés szerint az $y_1<\ldots<y_k=b$ lánc hossza legfeljebb m, tehát $k-1\leq m\leq n-1$. Ezt akartuk belátni.

Megjegyzés: a tétel szerint a fenti feltételek mellett tetszőleges n-nél rövidebb lánc bővíthető, egy n hosszú pedig már nem. Tehát ha kiindulunk egy $k\leq n$ hosszú láncból, akkor folyamatos beszúrásokkal véges sok lépésben egy n hosszú maximális láncot kapunk $\Rightarrow$ minden $a<\ldots<b$ lánc kiegészíthető maximális lánccá.

9.9.3 Definíció: a Jordan-Dedekind-tétel szerint L alulról korlátos moduláris hálóban minden b elemének van magassága (egy $0\prec x_1\prec x_2\prec\ldots\prec x_n=a$ maximális lánc hossza; ez esetleg végtelen, de egyértelmű). Jogos tehát ezt minden $b\in L$-re definiálni és $h(b)$-vel jelölni. Nyilván $a\leq b\Rightarrow h(a)\leq h(b)$. (Persze a magasságot tetszőleges hálóban definiálhatjuk minden olyan elemre, amelyre egyértelmű.)

Például $L(A_4)=$ már csak azért sem moduláris, mert nem minden elemének egyértelmű a magassága.

Megjegyzés: G véges csoport pontosan akkor szuperfeloldható (van olyan invariáns lánca, amelynek minden faktora prímrendű ciklikus csoport), ha $L(G)$-ben minden maximális lánc hossza azonos (van egyértelmű magasság). Ez persze következik a modularitásból, de ebből nem következik a modularitás. Például a hálóban van egyértelmű magasság, de nem moduláris, mert a fekete pontok N_5 részhálót adnak.

9.9.4 Állítás: alulról korlátos moduláris hálóban a véges magasságú elemek ideált alkotnak. Ehhez elég azt belátni, hogy ha $a,b\in L$ véges magasságú elemek, akkor $h(a\vee b)$ is véges, hiszen $h(a\vee x)\le h(a)$ véges, ha $h(a)$ véges. Egy $a\wedge b\prec\ldots\prec a$ maximális lánc hossza nyilván $h(a)-h(a\wedge b)$. A transzponált-izomorfizmus miatt ez megegyezik egy tetszőleges $b\prec\ldots\prec b\vee a$ maximális lánc hosszával, amiből egy $0\prec\ldots\prec a\wedge b\prec\ldots\prec b\vee a$ maximális lánc hossza $h(a\vee b)=h(a)+h(b)-h(a\wedge b)$.

9.9.5 Definíció: az L korlátos háló a eleme atom, ha $0\prec a$ és duális atom, ha $a\prec 1$.

9.9.6 Definíció: $a\in L$ metszetirreducibilis, ha $\nexists x,y>a$: $a=x\wedge y$. Például minden duális atom ilyen.

Megjegyzés: véges hálóban pontosan azok az elemek metszetirreducibilisek, melyeket pontosan egy elem fed, továbbá a felső korlát.

9.9.7 Definíció: L kielégíti a maximumfeltételt, ha bármely nem üres részhalmazában van maximális elem. Például minden véges háló ilyen.

9.9.8 Állítás: ha L kielégíti a maximumfeltételt, akkor minden a eleme előáll véges sok metszetirreducibilis elem metszeteként.

Bizonyítás: $\lightning$ legyen a olyan, ami nem áll elő így, és erre a tulajdonságra nézve maximális. a nem lehet metszetirreducibilis, mert akkor $a=a$ épp egy metszetirreducibilisek véges metszetére való bontása lenne. Tehát $a=x\wedge y$, ahol $x,y>a$. a választása miatt x és y előállnak véges sok metszetirreducibilis elem metszeteként: $x=\wedge\chi_i$, $y=\wedge\gamma_j$, így $a=(\wedge\chi_i)\wedge(\wedge\gamma_j)$, $\lightning$.

9.9.9 Kuros-Ore tétel: legyen L moduláris háló, $x\in L$. Ha $x=u_1\wedge u_2\wedge\ldots\wedge u_n=v_1\wedge v_2\wedge\ldots\wedge v_m$ egyaránt x véges sok metszetirreducibilis elem metszeteként való felírásai úgy, hogy nincs bennük felesleges elem (bármelyiket elhagyva a metszet már nem x), akkor $n=m$, továbbá bármely u_i-hez található olyan v_k, hogy az első felírásban u_i kicserélhető v_k-ra.

Bizonyítás: először az állítás második felét bizonyítjuk.

Legyen $x_i=\wedge_{i\neq j}u_j$. Ekkor $x=u_i\wedge x_i$ és $x<x_i$ ($x=x_i$ esetén u_i felesleges lenne). Nekünk éppen egy olyan v_k kell, amelyre $v_k\wedge x_i=x$. Legyen minden $k\in\{1\ldots m\}$ –re $y_{ik}=v_k\wedge x_i$. Persze $x\le y_{ik}\le v_k$. Azt állítjuk, hogy $x=\wedge_{k=1}^{m}y_{ik}$. A jobb oldalon minden tényező felülről becsüli x-et, tehát $x\le \mathit{jobb\ oldal}$. Másrészt a jobb oldal felülről becsülhető $\wedge_{k=1}^{m}v_k=x$ -el, így $x\ge \mathit{jobb\ oldal}$ is teljesül.

A transzponált-izomorfizmus szerint $[x,x_i]=[u_i\wedge x_i,x_i]\simeq[u_i,u_i\vee x_i]$. u_i például $[u_i,u_i\vee x_i]$-ben is metszet-irreducibilis, tehát $[x,x_i]$-ben x metszetirreducibilis. Az $x=\wedge_{k=1}^{m}y_{ik}$ felírás tényezői $[x,x_i]$-ből valók, tehát ez triviális felírás, azaz valamely y_{ik} egyenlő x-el: $x=y_{ik}=v_k\wedge x_i$. Éppen ezt akartuk.

Térjünk most rá az állítás első felére. Induljunk ki az $x=\wedge_{i=1}^{n}u_i=\wedge_{k=1}^{m}v_k$ felírásokból. Cseréljük ki az első felírás egy u_i elemét valamely v_k-ra, a kapott felírásból hagyjuk el az esetleges felesleges tényezőket. Ismételjük ezt addig, amíg az összes u_i-t le nem cseréltük. Így x egy felírását kapjuk néhány – de legfeljebb n – v_k metszeteként. Mivel az $x=\wedge_{k=1}^{m}v_k$ felírásban nincs felesleges elem, csak ezt kaphattuk, amiből $m\le n$. Hasonlóan $n\le m$, kész vagyunk.

Megjegyzés: az már nem mindig igaz, hogy $\{u_i|1\le i\le n\}=\{v_j|1\le j\le m\}$, hiszen -ben 0 kivételével minden elem metszetirreducibilis, a 0-nak viszont rögtön három felírása is van, amiben egyik elem sem felesleges.

Megjegyzés: a fenti tétel bizonyításakor azt láttuk be, hogy ha x előállítható véges sok metszetirreducibilis elem metszeteként, akkor a metszetireducibilis elemek olyan halmazai, melyek kiegészíthetőek x egy „jó” felírásává (véges sok irreducibilis elem metszeteként való felírás úgy, hogy nincs köztük felesleges), matroidot alkotnak.

Lemma: ha y metszetirreducibilis és $y_1\wedge y_2\wedge\ldots\wedge y_t\le y$, akkor valamelyik $y_i\le y$, különben $y=y\vee\left(\bigwedge_{i=1}^{t}y_i\right)=\bigwedge_{i=1}^{t}(y\vee y_i)$ egy nem triviális metszetre bontása lenne y-nak.

9.9.10 Tétel: ha L disztributív és $x=\bigwedge_{i=1}^{n}u_i=\bigwedge_{j=1}^{m}v_j$ egyaránt olyan irreducibilis elemek metszetére való bontások, ahol nincs felesleges tényező, akkor $\{u_i|1\le i\le n\}=\{v_j|1\le j\le m\}$.

Bizonyítás: $u_i\ge\bigwedge_{j=1}^{m}v_j$, tehát a lemma szerint $u_i\ge v_k$ valamely k-ra. Hasonlóan $v_k\ge u_l$ alkalmas l esetén, összefoglalva $u_i\ge v_k\ge u_l$. Minthogy u_i nem felesleges tényező x felbontásában, ez csak $i=l$ esetén lehetséges. Az antiszimmetria szerint $u_i=v_k$, az állítást ezzel beláttuk.

Megjegyzés: egyik tétel sem működik visszafele. Az ábrán látható háló ugyanis nem moduláris (a körrel jelölt elemek egy N_5 részhálót adnak), pedig minden eleme egyértelműen bomlik úgy metszetirreducibilisek metszetére, hogy nincs felesleges tényező (a feketével jelölt elemek a metszetirreducibilisek).