MBNK12: Algebrai struktúrák

(előadásvázlat, 2016. május 9.)

Maróti Miklós, Kátai-Urbán Kamilla

Jelölje $\mathbb{Z}$ az egész számok halmazát, $\mathbb{N}$ a pozitív egészek halmazát, $\mathbb{N}_0$ a nem negatív egészek halmazát, $\mathbb{Q}$ a racionális számok halmazát, $\mathbb{R}$ a valós számok halmazát, $\mathbb{R}_0^+$ a nem negatív valós számok halmazát, és $\mathbb{R}^{m\times n}$ az $m\times n$-es valós mátrixok halmazát, $\mathbb{Z}_m$ a modulo m maradékosztályok halmazát.

1. Félcsoport, csoport

1. Definíció. Az asszociatív grupoidokat félcsoportnak nevezzük. Az egységelmes félcsoportokat monoidnak nevezzük. Azokat a monoidokat, ahol minden elemnek van inverze csoportoknak hívjuk. A kommutatív csoportokat Abel-csoportoknak nevezzük.

2. Példa. Az $(\mathbb{N};+)$ félcsoport, de nem monoid.

3. Példa. A következők monoidok, de nem csoportok: $(\mathbb{N};\cdot)$, $(\mathbb{N}_0;+)$, $(\mathbb{R};\cdot)$, $(\mathbb{R}^{n\times n};\cdot)$, $(\mathbb{Z}_n;\cdot)$, $(\mathcal{P}(U);\cup)$.

4. Példa. A következők csoportok, de nem (feltétlen) Abel-csoportok: $(S_n;\cdot)$, melynek neve a teljes szimmetrikus csoport, és az $(\{\,M\in\mathbb{R}^{n\times n} : |M|\neq 0\,\};\cdot)$, melynek neve az általános lineáris csoport.

5. Példa. A következők Abel-csoportok: $(\mathbb{Z};+)$, $(\mathbb{Z}_n;+)$, $(\mathbb{R}\setminus\{0\};\cdot)$, $(\mathbb{R}^{n\times m};+)$, $(\mathcal{P}(U);\triangle)$, $(\{\mathbf{i},\mathbf{h}\};\leftrightarrow)$.

6. Tétel. Félcsoportban legfeljebb egy egységelem van.

7. Tétel. Az $(A;\cdot)$ monoidban minden elemnek legfeljebb egy inverze van. Ha az a,b elemnek van inverze: a^{-1},b^{-1}, akkor az a^{-1} és ab elemeknek is van inverze, mégpedig

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

8. Példa. Az $(\mathbb{R}^{n\times n};\cdot)$ monoidban pontosan a nem nulla determinánsú elemeknek van inverze, és éppen ezek az elemek alkotják az általános lineáris csoportot.

9. Megjegyzés. Tudjuk, hogy csoportban az egységelem és az elemek inverze egyértelműen meghatározott, de nem mindig egyértelmű, hogy ezeket hogyan is jelöljük. Ha ez meg szeretnénk adni, akkor a $(A;\cdot)$ helyett $(A;\cdot,{}^{-1},1)$-et írunk, ahol a második művelet az 1-változós inverzképzés, és 1 az egységelem (0-változós művelet). A csoportok multiplikatív írásmódja alatt a $(A;\cdot,{}^{-1},1)$ műveleti szimbólumokat értjük. Az additív írásmód alatt a $(A;+,-,0)$ műveleti szimbólumokat értjük, és általában csak akkor használjuk, ha a csoport kommutatív.

10. Definíció. Legyen $(A;\cdot,{}^{-1},1)$ tetszőleges csoport. Az $a\in A$ elem n-edik hatványát ($n\in\mathbb{Z}$) a következőképpen definiáljuk:

$$a^n=\begin{cases}\underbrace{a\cdots a}_{n\text{ db}}, & \text{ha } n>0,\\ 1, & \text{ha } n=0,\\ \underbrace{a^{-1}\cdots a^{-1}}_{-n\text{ db}}, & \text{ha } n<0.\end{cases}$$

Ha az $(A;+,-,0)$ csoport additív írásmódban van megadva, akkor a hatványozást $n\cdot a$-val jelöljük, de ugyan úgy definiáljuk mint a multiplikatív írásmódnál:

$$n\cdot a=\begin{cases}\underbrace{a+\cdots+a}_{n\text{ db}}, & \text{ha } n>0,\\ 0, & \text{ha } n=0,\\ \underbrace{(-a)+\cdots+(-a)}_{-n\text{ db}}, & \text{ha } n<0.\end{cases}$$

11. Lemma. Legyen $(A;\cdot,^{-1},1)$ tetszőleges csoport, $a \in A$ és $n \in \mathbb{Z}$. Ekkor $a^n \cdot a = a \cdot a^n = a^{n+1}$ és $a^{-1} \cdot a^n = a^n \cdot a^{-1} = a^{n-1}$.

12. Tétel. Legyen $(A;\cdot)$ tetszőleges csoport. Bármely $m, n \in \mathbb{Z}$-re és $a, b \in A$-ra

(1) $a^m a^n = a^{m+n}$,
(2) $(a^m)^n = a^{mn}$,
(3) ha $ab = ba$, akkor $(ab)^n = a^n b^n$.

13. Példa. Az $(\mathbb{R} \setminus \{0\};.)$ csoportban az $a = 2$ elem harmadik hatványa 8, mert $2 \cdot 2 \cdot 2 = 8$. Az $(\mathbb{R};+)$ csoportban az $a = 2$ elem harmadik hatványa viszont 6, mert $2 + 2 + 2 = 6$.

14. Definíció. Legyen $(A;\cdot)$ csoport. Az $a \in A$ elem rendje az a legkisebb pozitív egész $n \in \mathbb{N}$, amelyre $a^n = 1$. Ha ilyen nincs, akkor a rendje végtelen. Az elem rendjét $o(a)$-val jelöljük.

15. Példa. A $(\mathbb{Z}_6;+)$ csoportban $o(\overline{4}) = 3$, mert $3 \cdot \overline{4} = \overline{0}$, azaz a harmadik hatvány az egységelem, de a kisebb hatványok nem az egységelemet adják. Az $(S_5;\cdot)$ csoportban $o((1\ 2\ 3)(4\ 5)) = 6$, mert a ciklusok függetlenek, azaz felcserélhetőek, így külön hatványozhatóak.

16. Tétel. Legyen $(A;\cdot)$ csoport, $a \in A$ véges rendű elem, és $n, m \in \mathbb{Z}$-re

(1) $a^n = 1$ akkor és csak akkor teljesül, ha $o(a) \mid n$,
(2) $a^n = a^m$ akkor és csak akkor teljesül, ha $n \equiv m \pmod{o(a)}$.

17. Tétel. Legyen $(A;\cdot)$ csoport, és $a, b \in A$ felcserélhető elemek, azaz $ab = ba$. Ekkor $o(ab) = o(a)o(b)$ akkor és csak akkor, ha $\text{lnko}(o(a), o(b)) = 1$.

2. Gyűrű, test

18. Definíció. Az $(A;+,\cdot)$ algebrát gyűrűnek nevezzük, ha $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport, és a $\cdot$ disztributív az $+$-ra. Az $(A;+)$ Abel-csoportot a gyűrű additív csoportjának, az $(A;\cdot)$ félcsoportot a gyűrű multiplikatív félcsoportjának nevezzük.

19. Példa. Gyűrűk: $(\mathbb{Z};+,\cdot)$, $(\mathbb{R};+,\cdot)$, $(\mathbb{R}^{2\times 2};+,\cdot)$, $(\{\mathbf{i},\mathbf{h}\};\leftrightarrow,\vee)$, $(\mathcal{P}(U);\triangle,\cap)$, $(\mathbb{Z}_5;+,\cdot)$.

20. Tétel. Az $(A;+,\cdot)$ gyűrű esetén a 0 additív egységelem a szorzásra nézve zéruselem. Továbbá tetszőleges $a, b \in A$ elemekre $(-a)b = a(-b) = -(ab)$.

21. Definíció. Az $(A;+,\cdot)$ gyűrűt testnek nevezzük, ha az $(A\setminus\{0\};\cdot)$ Abel-csoportot alkot, amelyet a test multiplikatív csoportjának nevezzük.

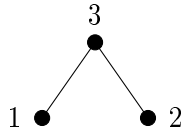
22. Tétel. A $(\mathbb{Z}_n;+,\cdot)$ gyűrű pontosan akkor test, ha n prím.

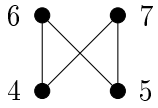
23. Példa. A 19. példában felsorolt gyűrűk közül testek: $(\mathbb{R};+,\cdot)$, $(\{\mathbf{i},\mathbf{h}\};\leftrightarrow,\vee)$, $(\mathbb{Z}_5;+,\cdot)$.

3. Háló

24. Definíció. Legyen $(A;\leq)$ részbenrendezett halmaz. Az $a, b \in A$ elemeknek $c \in A$ felső korlátja, ha $a \leq c$ és $b \leq c$. Az a, b elemeknek $d \in A$ legkisebb felső korlátja, ha d felső korlát, és a, b minden c felső korlátjára $d \leq c$. Duális módon definiálhatjuk a alsó korlátot és a legnagyobb alsó korlátot.

25. Példa. Az alábbi ábrán látható az első részbenrendezésben az 1, 2 elemeknek csak egy felső korlátjuk van, ami a legkisebb is egyben, de nincsen alsó korlátjuk. A második részbenrendezésben a 4, 5 elemeknek két felső korlátjuk van, de nincsen legkisebb felső korlátjuk.



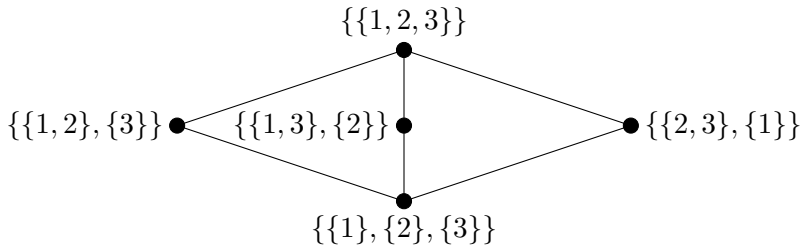


26. Tétel. Tetszőleges részbenrendezett halmaz bármely két elemének legfeljebb csak egy legkisebb felső korlátja (legnagyobb alsó korlátja) van.

27. Definíció. Az $(A;\leq)$ részbenrendezett halmaz hálószerűen rendezett, ha tetszőleges $a,b\in A$ elemeknek van legkisebb felső korlátjuk, melyet $a\vee b$-vel jelölünk és az a,b elemek egyesítésnek nevezzük, illetve legnagyobb alsó korlátjuk, melyet $a\wedge b$-vel jelölünk és az a,b elemek metszetnek nevezzük.

28. Példa. Az előző példában szereplő részbenrendezések nem hálószerűen rendezettek. Az $(\mathbb{N}_0;|)$ hálószerűen rendezett halmaz, amelyben az egyesítés a legkisebb közös többszörös és a metszet a legnagyobb közös osztó. Az $(\mathbb{R};\leq)$ hálószerűen rendezett halmaz, ahol az egyesítés a maximum és a metszet a minimum. A $(\mathcal{P}(U);\subseteq)$ hálószerűen rendezett halmaz, ahol a halmazelméleti egyesítés és metszet a legkiseb felső korlát és legnagyobb alsó korlát. A $(\{\mathbf{h},\mathbf{i}\};\rightarrow)$ hálószerűen rendezett halmaz, ahol a logikai „vagy” művelet a legkisebb felső korlát, és a logikai „és” művelet a legnagyobb alsó korlát.

29.* Példa. Egy rögzített alaphalmazon az ekvivalenciarelációk halmaza a tartalmazásra nézve hálószerűen rendezett, ahol a metszet a halmazelméleti metszet, és az egyesítés a halmazelméleti unió tranzitív lezártja. Az $\{1,2,3\}$ alaphalmaz öt ekvivalenciarelációjának részbenrendezése a következő (az ekvivalenciarelációk helyett a megfelelő osztályozások vannak feltüntetve):



30. Tétel. Legyen $(A;\leq)$ hálószerűen rendezett halmaz. Ekkor

(1) a $\wedge$ és $\vee$ műveletek idempotensek, kommutatívak, és asszociatívak;
(2) $\wedge$ abszorptív az $\vee$-re és $\vee$ abszorptív a $\wedge$-re;
(3) $a\leq b$ akkor és csak akkor teljesül, ha $a\wedge b=a$.

31. Definíció. Az $(A;\wedge,\vee)$ algebrát hálónak nevezzük, ha a kétváltozós $\wedge$ és $\vee$ műveletek idempotensek, kommutatívak, és asszociatívak, illetve kölcsönösen abszorptívak egymásra.

32. Tétel. Ha adott az $(A;\wedge,\vee)$ háló, akkor az

$$a\leq b \iff a\wedge b=a$$

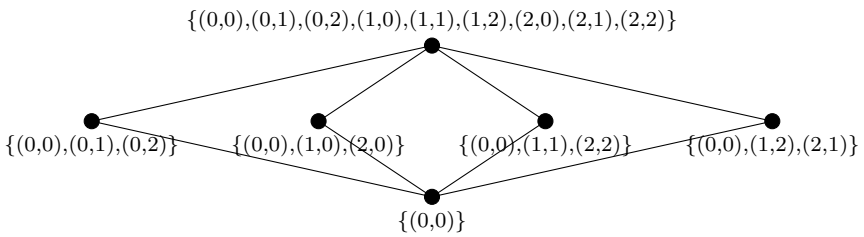
feltétel által definiált $\leq$ relációval $(A;\leq)$ hálószerűen rendezett halmaz, amelyben $a,b\in A$ legkisebb felső korlátja $a\vee b$ és legnagyobb alsó korlátja $a\wedge b$.

33.* Tétel. Adott alaphalmazon a hálószerűen rendezett halmazok és a hálók természetes módon (az előző két tétel szerint) megfeleltethetők egymásnak.

34. Példa. $(\mathbb{N}_0;\mathrm{lnko},\mathrm{lkkt})$, $(\mathbb{R};\min,\max)$, $(\mathbb{R};\max,\min)$, $(\mathcal{P}(U);\cap,\cup)$ és $(\{\mathbf{h},\mathbf{i}\};\wedge,\vee)$ hálók.

35. Példa. Az $\mathbb{R}^n$ alterei a tartalmazásra nézve hálószerűen rendezett halmazt alkotnak. Ha $U,V\leq\mathbb{R}^n$ két altér, akkor metszetük $U\cap V$ és egyesítésük $U+V=\{\,u+v:u\in U,v\in V\,\}$.

36.* Példa. A $\mathbb{Z}_3$ test feletti 2-dimenziós $\mathbb{Z}_3^2$ vektortér altereinek hálója a következő:



$\mathbb{Z}_2^3$ altereinek Hasse-diagrammja már lényegesen bonyolultabb (1 db 0-dimenziós, 7 db 1-dimenziós, 7 db 2-dimenziós és 1 db 3-dimenziós altere van):