

Mveletek és struktúrák

Ebben a fejezetben megismerkedünk a mvelet, majd az algebrai struktúra fogalmával, miután ismétlésként áttekintettük a függvény fogalmát. Ezután az alapvető egy- és kétmveletes struktúrákkal foglalkozunk. Részletesen tárgyaljuk az izomorfia fogalmát. A kérdések, példák, feladatok szerves részét képezik a fejezetnek, javasoljuk ezek alapos feldolgozását.

▼ A függvény fogalma

12.1.1. Definíció

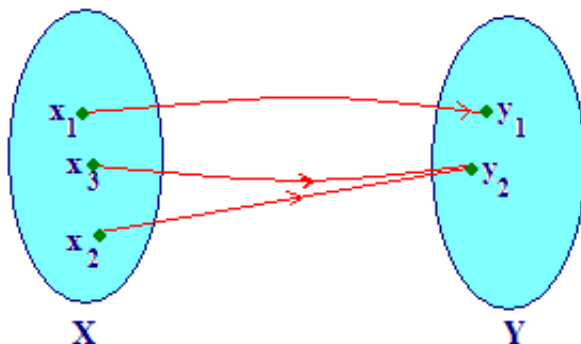
Az f relációt az X -et Y -ba leképez függvénynek mondjuk, ha

$$f \subset X \times Y$$

és X minden x eleméhez található olyan $y \in Y$, hogy $(x, y) \in f$ és,

ha $(x, y_1) \in f$ és $(x, y_2) \in f$, akkor $y_1 = y_2$.

Ez utóbbi azt jelenti, hogy a leképezés egyértelmű. Különböző változóértékekhez (az X halmaz elemei) hozzárendelhetjük ugyanazt a függvényértéket (Y -beli értéket), de az X minden eleméhez pontosan egy értéket rendelünk. (1. ábra)



1. ábra

▼ A mvelet fogalma

12.2.1. Definíció

Egy f függvényt, amely az $A \times A$ halmazt az A halmazba képezi le, az A halmazon értelmezett (bináris, belső) mveletnek nevezünk.

Ezt a leképezést így jelöljük:

$$f: A \times A \rightarrow A$$

A mveleteket a megszokot prefix jelöléstl eltéren infix módon jelöljük.

prefix jelölés: $fx y$ vagy $f(x, y)$

infix jelölés: $x f y$

A definícióban zárójelben szerepl "bináris" jelz arra utal, hogy a mveletnek két operandusa van. Ha n-áris relációból indulunk ki, akkor az n-változós mvelet fogalmához jutunk:

Az

$$f: A^n \rightarrow A$$

leképezés az A halmazon értelmezett n-változós mvelet. (Másképpen n-áris mvelet)
Speciálisan az egyváltozós (unáris) mveletek az

$$f: A \rightarrow A$$

leképezések, a nullváltozós mveletek pedig a konstansok. Egyváltozós mvelet pl. a halmazalgebrában a komplementerképzés, az ítéletalgebrában a negáció.

A "bels" jelz azt jelenti, hogy a mvelet definíciójában csak egyetlen halmaz szerepel, az amelyiken a mveletet értelmeztük. Ezzel szemben az A halmazon értelmezett küls mvelet például egy

$$f: B \times A \rightarrow A$$

függvény. Ilyen például a vektorok skalárral való szorzása.

Algebrai struktúra

Ha egy halmazon mveleteket definiálunk, akkor algebrai struktúrát kapunk.

12.3.1. Definíció

Egy mveletes S struktúrán egy $S = (A, \#)$ párt értünk, ahol A egy halmaz, # pedig az A-n értelmezett mvelet.

12.3.2. Példák

1) $(\mathbb{N}, \cdot)$

Mindenekeltt megállapítjuk, hogy a természetes számok halmaza zárt a szorzás mveletére nézve, azaz

két természetes szám összege természetes szám. Eszerint az $\mathbb{N}$ a szorzás mveletével algebrai struktúrát alkot-

A szorzás mvelete

- asszociatív, azaz $\forall a, b, c \in \mathbb{N}$ esetén $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- és
- kommutatív, azaz $\forall a, b \in \mathbb{N}$ esetén $a \cdot b = b \cdot a$

Az $\mathbb{N}$ -ben van ún. neutrális elem (egységelem), az 1 úgy, hogy $\forall a \in \mathbb{N}$ esetén $1 \cdot a = a$.
Az $a \cdot x = b$ egyenlet bizonyos $a, b \in \mathbb{N}$ elemekre megoldható, de általában nem.

2) $(\mathbb{N} +, +)$

Az elz példához hasonlóan a pozitív természetes számok halmaza az összeadás mveletére nézve is zárt. Tehát

a pozitív természetes számok halmaza a szokásos összeadással algebrai struktúra. Az $+$ asszociatív és kommutatív.

A struktúra neutrális elemet (zéruselemet) nem tartalmaz. Az $a + x = b$ egyenlet általában nem oldható meg az $\mathbb{N} +$ halmazban, csak néha (akkor, ha $a < b$).

Az tekintett példák egymveletes asszociatív struktúrák.

12.3.3. Feladat

Mutassuk meg, hogy $(\mathbb{N}, \nabla)$ algebrai struktúra, ahol $a \nabla b = a + 5 \cdot b$. Asszociatív-e ez a struktúra?

Megoldás

Az $a \nabla b$ mvelet bármely természetes számpárhoz természetes számot rendel, tehát $(\mathbb{N}, \nabla)$ algebrai struktúra. A mvelet azonban nem asszociatív, u.i.

$$(a \nabla b) \nabla c = (a + 5 \cdot b) \nabla c = a + 5 \cdot b + 5 \cdot c, \\ a \nabla (b \nabla c) = a \nabla (b + 5 \cdot c) = a + 5 \cdot (b + 5 \cdot c) = a + 5 \cdot b + 25 \cdot c,$$

tehát, ha $c \neq 0$, akkor

$$(a \nabla b) \nabla c \neq a \nabla (b \nabla c)$$

12.3.4. Feladat

Vizsgáljuk meg, hogy algebrai struktúra-e a következő:

$$(\{2 \cdot x + 1 \mid x \in \mathbb{Z}\}, +)$$

Megoldás

A páratlan számok halmaza az összeadás mveletével nem alkot algebrai struktúrát, mert nem zárt a mveletre nézve, azaz két páratlan szám összege páros.

Félcsoport

12.4.1. Definíció

Egy egymveletes $F = (A, \circ)$ struktúrát, amelyben az értelmezett mvelet asszociatív, félcsoportnak nevezünk.

Megjegyzés.

Nem minden mvelet asszociatív, például a hatványozás sem az. Ugyanis

$$(2^3)^2 = 64 \neq 2^{(3^2)} = 512.$$

Nem asszociatív a vektorok vektoriális szorzása sem.

A félcsoporthoz mveletének kommutativitását nem követeljük meg. Ha a művelet mégis kommutatív, akkor kommutatív félcsoporthoz beszélünk.

Kitüntetett elemek a félcsoporthoz

12.4.2. Definíció

Ha az $F = (A, \circ)$ félcsoporthoz van olyan e eleme, amelyre
$$e \circ a = a \quad (a \circ e = a),$$
tetszőleges $a \in A$ esetén, akkor e -t az F baloldali (jobboldali) neutrális elemének nevezzük.

12.4.3. Definíció

Ha az $F = (A, \circ)$ félcsoporthoz van olyan e eleme, amelyre
$$e \circ a = a \circ e = a,$$
tetszőleges $a \in A$ esetén, akkor e -t az F neutrális elemének nevezzük.

12.4.4. Tétel

Ha egy $F = (A, \circ)$ félcsoporthoz e baloldali neutrális elem, és f jobboldali neutrális elem, akkor $e = f$. Ennélfogva F neutrális eleme egyértelműen van meghatározva

Bizonyítás

Tekintsük az $e \cdot f$ ($\in F$) szorzatot. Mivel e baloldali neutrális elem, ezért $e \cdot f = f$, s mivel f jobboldali neutrális elem, ezért $e \cdot f = e$. Innen $e = f$. Ha e_1, e_2 az F -nek két neutrális eleme, akkor e_1 -et baloldali, e_2 -t jobboldali neutrális elemként fogva fel, az elbbiek szerint $e_1 = e_2$.

Megjegyzések

1. Ha F -ben nincs jobboldali neutrális elem, akkor F -ben még lehet végtelen sok különböző baloldali neutrális elem.
2. Ha az F -beli műveletet szorzásnak írjuk, akkor a neutrális elemet többnyire **egységelemnek** nevezzük.

12.4.5. Definíció

Ha F -nek van e neutrális eleme, és valamely $a \in F$ -hez létezik olyan $a^* \in F$, hogy

$$a^* \cdot a = e,$$

akkor a^* -ot az a elem baloldali inverzének nevezzük.

A jobboldali inverz és az inverz elem definíciója hasonlóan történik. Az a elemet invertálható elemnek mondjuk, ha van inverze. Ha a -nak van inverze, akkor ez is invertálható, és inverze a , azaz $(a^*)^* = a$.

12.4.6. Tétel

Ha az F neutrális elemes félcsoporthban az a elemnek van a^* baloldali inverze, és van

a^{**} jobboldali inverze, akkor $a^* = a^{***}$. Ezért az inverz elem, ha létezik, egyértelműen van meghatározva.

Bizonyítás

A feltételek alapján:

$$a^* = a^* \cdot e = a^* \cdot (a \cdot a^{**}) = (a^* \cdot a) \cdot a^{**} = e \cdot a^{**} = a^{**}.$$

12.4.7. Tétel

Ha az a és a b elemeknek van inverzük, a^* ill. b^* , akkor $a \cdot b$ -nek is van inverze, és ez $b^* \cdot a^*$.

Bizonyítás

Mivel

$$(b^* \cdot a^*) \cdot (a \cdot b) = b^* \cdot (a^* \cdot a) \cdot b = b^* \cdot e \cdot b = b^* \cdot b = e,$$

ezért $b^* \cdot a^*$ az $a \cdot b$ baloldali inverze. Hasonlóan belátható, hogy $b^* \cdot a^*$ az $a \cdot b$ -nek jobboldali inverze is.

Példák

12.4.8. Példa

Tekintsük a $(2^H, \cap)$ struktúrát, azaz a H nemüres halmaz összes részhalmazát a metszetképzés mveletére nézve.

Ez a struktúra neutrális elemes félcsoporth. Neutrális eleme maga a H halmaz. A neutrális elemén kívül más elemnek nincs inverze.

12.4.9. Példa

Félcsoporthot alkotnak a valós elem

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

alakú mátrixok a mátrix-szorzással, mint mvelettel.

```
> restart;
> with(linalg):
> A:=matrix(2,2);B:=matrix(2,2);C:=matrix(2,2);
Tekintsük két tetszőleges, 2×2-es mátrix szorzatát!
> evalm(A&*B);
```

A szorzat is 2×2-es mátrix. Megmutatjuk, hogy a művelet asszociatív, azaz $\forall A, C, B$ 2×2-es mátrix-hármasra

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

```
> simplify(evalm((A&*B)&*C));
> simplify(evalm(A&*(B&*C)));
> equal(%,%);#Megvizsgálja, hogy a két mátrix egyenl-e
```

Látható, hogy a két mátrix elemről-elemre megegyezik, s ezt állapítja meg az equal eljárás is.

Egységelem az $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ mátrix, s a mátrix akkor invertálható, ha $D = a \cdot d - b \cdot c \neq 0$.

12.4.10.. Példa

A valós elem,

$$\begin{bmatrix} a & b \\ a & b \end{bmatrix}$$

alakú mátrixok olyan multiplikatív (a művelet a szorzás) félcsoportot alkotnak, ahol az összes $a + b = 1$ feltételnek eleget tevő mátrix baloldali neutrális elem. Belátható, hogy jobboldali neutrális elem nincsen.

12.4.11. Példa

Félcsoportot alkotnak az egész számok a szorzás műveletére nézve. A félcsoportban van egységelem, az 1, de az 1 és a -1 kivételével nincs a halmazban inverzük az elemeknek.

A művelet invertálhatósága

Az [algebrai struktúra](#) fogalmát bevezető fejezet példáiban bizonyos [egyenletek megoldhatóságát](#) vizsgáltuk. Ebből kiindulva definiáljuk a művelet invertálhatóságának fogalmát.

12.4.12. Definíció

Az $F = (A, \circ)$ félcsoportbeli $\circ$ műveletet invertálhatónak nevezzük, ha tetszőleges $a, b \in A$ elemekhez egyetlenegy x_0 és y_0 létezik úgy, hogy

$$a \cdot x_0 = b \text{ és } y_0 \cdot a = b$$

A definíció két fontos elemet tartalmaz:

1. Az $a \cdot x = b$ és az $y \cdot a = b$ egyenleteknek létezik az A halmazban megoldása;
2. A megoldás egyértelmű.

A következ fontos tétel a mvelet invertálhatóságának és az elemek invertálhatóságának fogalmát kapcsolja össze.

12.4.13. Tétel

Egy asszociatív $(A, \circ)$ struktúrában a $\circ$ mveletet akkor és csak akkor , invertálható, ha

1. $(A, \circ)$ -ben van egységelem és
2. A minden elemének van inverze.

Csoport

A kombinatorikáról szóló fejezetben bevezettük a permutáció fogalmát:

H halmaznak egy önmagára való egy-egyértelm leképezését H permutációjának nevezzük.

A permutációkat így is jelölhetjük:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Itt három elem permutációiról van szó. Az els esetben az els helyre a 2, a második helyre a 3, a harmadik helyre az 1 kerül.

A második esetben a 3 1 2 permutációt kaptuk.

Tekintsük most a következ $G = (H, \circ)$ struktúrát, ahol $H = \{ \text{az } 1, 2, 3 \text{ elemek összes permutációjának halmaza} \}$, $\circ$ mvelet a permutációk egymás utáni végrehajtása.

Például:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Az els permutáció az 1-hez a 3-at rendeli, a második a 3-hoz önmagát, a két permutáció szorzata - ennek megfelelen- az 1-hez a 3-at. Az els permutáció a 2-höz az 1-et rendeli, a második az 1-hez a 2-t, így a szorzat a 2-höz a 2-t. Végül az els permutáció a 3-hoz a 2-t, a második a 2-höz az 1-et, s így a szorzat a 3-hoz az 1-et rendeli.

Tudjuk, hogy 3 elemnek összesen 6 permutációja van. Jelöljük ezeket a következőképpen:

$$e = P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

A $G = (H, \circ)$ struktúra vizsgálata

```
[> restart:  
[> with(linalg):
```

A következőkben eljárást adunk meg két permutáció szorzatának kiszámítására. Az eljárás mátrix alakban kezeli a permutációkat. Adjuk meg három elem fent definiált összes permutációját ilyen alakban:

```
> P||1:=matrix(2,3,[1,2,3,1,2,3]):P||2:=matrix(2,3,[1,2,3,2,3,1]):P||3:=matrix(2,3,[1,2,3,3,1,2]):P||4:=matrix(2,3,[1,2,3,1,3,2]):P||5:=matrix(2,3,[1,2,3,3,2,1]):P||6:=matrix(2,3,[1,2,3,2,1,3]):
```

Így a permutációk a következő alakot öltik:

```
> seq(P||i=evalm(P||i),i=1..6);
```

Eljárás a permutációk szorzatának kiszámítására,

Az alábbi **permszor** eljárás kiszámítja a permutációk szorzatát. Paraméterei a szorzótényezők, mátrixként definiálva.

```
> permszor:=proc()
  local szor,k,j,i,sor,p1,p2:
  p1:=evalm(args[1]);
  p2:=evalm(args[2]):
  k:=linalg[coldim](p1):
  sor:=seq(j,j=1..k):
  szor:=matrix(2,k,0):
  if linalg[coldim](p1)<>linalg[coldim](p2)
    then RETURN(`A permutációk nem azonos elemszámúak`)
  fi:
  for i to k do
    szor[1,i]:=i:
    szor[2,i]:=p2[2,p1[2,i]]
  od:
  evalm(szor)
end:
```

Képezzük néhány permutáció szorzatát

```
> `P2 P5`=permszor(P2,P5);
```

Ez éppen a P6 permutáció, tehát

$$P2 \cdot P5 = P6$$

Végezzük el a műveletet fordított sorrendben:

```
> `P5 P2`=permszor(P5,P2);
```

Ez éppen a P4 permutáció, tehát

$$P5 \cdot P2 = P4$$

Ez azt jelenti, hogy a művelet nem kommutatív, hisz találtunk olyan elempárt, amelyek szorzata függ a sorrendtől.

Készítsük el az ún. műveleti táblát. Vagyis végezzük el minden lehetséges párral mindkét sorrendben a műveletet:

```
> matrix(6,6,[seq(seq(permszor(P||i,P||j),i=1..6),j=1..6)]);
```

A műveleti tábla "rövidebben", a permutációk jelölésével:

$\circ$	$P1$	$P2$	$P3$	$P4$	$P5$	$P6$
$P1$	$P1$	$P2$	$P3$	$P4$	$P5$	$P6$
$P2$	$P2$	$P3$	$P1$	$P5$	$P6$	$P4$
$P3$	$P3$	$P1$	$P2$	$P6$	$P4$	$P5$
$P4$	$P4$	$P6$	$P5$	$P1$	$P3$	$P2$
$P5$	$P5$	$P4$	$P6$	$P2$	$P1$	$P3$
$P6$	$P6$	$P5$	$P4$	$P3$	$P2$	$P1$

A táblázatot megfigyelve több mindent észrevehetünk:

- Minden elem minden sorban és minden oszlopban pontosan egyszer fordul el;
- A $P1$ identikus permutáció sora és oszlopa a másik tényezékből áll. Ez azt jeleli, hogy $P1$ -el szorozva minden elem változatlan marad, vagyis a $P1$ permutáció a neutrális elem;
- $P2 \cdot P3 = P3 \cdot P2 = P1$, $P4 \cdot P4 = P5 \cdot P5 = P6 \cdot P6 = P1$, tehát a $P2$ elem inverze a $P3$, míg a $P1$, $P4$, $P5$, $P6$ elemek saját maguk inverzei.
- Kiderült, hogy van egységelem (neutrális elem), és minden elemnek van inverze. Ezért, az előző szakasz tétele szerint, a művelet invertálható.

Vizsgáljuk meg, hogy asszociatív-e a művelet! Először egy esetet nézzünk meg:

```
> permszor(P1, permszor(P3, P4)) = permszor(permszor(P1, P3), P4);
```

A linalg csomag equal eljárásával megvizsgálhatjuk, hogy a két eredmény, a két mátrix egyenl-e.

```
> equal(lhs(%), rhs(%));
```

Azt kaptuk, hogy $P1 \cdot (P3 \cdot P4) = (P1 \cdot P3) \cdot P4$, tehát esetünkben teljesült a csoportosíthatóság, az asszociativitás. Most vizsgáljuk meg az összes esetet.

Az asszociatív változónak true (igaz) logikai értéket adunk, majd három egymásba ágyazott ciklussal valamennyi elemhármasra megnézzük, hogy teljesül-e az asszociativitás.

```
> asszociativ:=true;
```

```
> for i to 6 do
```

```
  for j to 6 do
```

```
    for k to 6 do
```

```
      if not(equal(permszor(P[i], permszor(P[j], P[k])), permszor(
permszor(P[i], P[j]), P[k]))) then
```

```
        asszociativ:=false
```

```
      fi od od od;
```

```
> asszociativ;
```

Az asszociativ változó értéke igaz maradt, tehát a művelet asszociatív. Természetesen az asszociativitás teljesülése általánosan is bizonyítható, anélkül tehát, hogy végig vizsgálnánk a szóbanforgó eseteket.

A csoport definíciója

12.5.1. Definíció

A $G = (H, \circ)$ asszociatív struktúrát **csoportnak** nevezzük, ha a $\circ$ mvelet invertálható.

Tudjuk, hogy az asszociatív struktúra mveletének invertálhatósága egyenérték azzal, hogy a struktúrában van egységelem (neutrális elem) és a struktúra minden elemének van inverze. Ennek alapján a definíciót a következő, az elbbivel természetesen egyenérték, módon is megfogalmazhatjuk:

12.5.2. Definíció

A G halmaz csoport, ha

1. G tetszleges a, b elempárjához hozzá van rendelve G -nek egyértelműen meghatározott c eleme:

$$a \circ b = c;$$

2. A $\circ$ mvelet asszociatív, azaz $\forall a, b, c \in G$ esetén $a \circ (b \circ c) = (a \circ b) \circ c$;

3. Létezik olyan $e \in G$, amelyre $e \circ a = a \circ e = a$, azaz létezik egységelem;

4. $\forall a \in G$ -hez létezik olyan $a_0 \in G$, hogy

$$a_0 \circ a = a \circ a_0 = e,$$

azaz G minden elemének van inverze G -ben.

A G csoportot **végesnek** vagy **végtelemnek** mondjuk, aszerint, hogy elemeinek száma véges, vagy végtelen. A csoport elemeinek számossága a G **csoport rendje**. Ennek jele: $|G|$.

Az elzetes vizsgálat és a definíció alapján mondhatjuk, hogy

12.5.3. Tétel

n elem halmaz önmagára való leképezései, azaz az adott n számú elem összes permutációi, csoportot alkotnak. Ezt a csoportot **n -edfokú szimmetrikus csoportnak** nevezzük. Jelölése: S_n , rendje $n!$

A szimmetrikus csoport mvelete nem kommutatív, tehát általában $a \circ b \neq b \circ a$. Azokat a csoportokat, amelyeknél az értelmezett mvelet kommutatív, kommutatív csoportoknak, vagy **Abel-csoportoknak** nevezzük.

Példák csoportra

A következőkben megadott halmazok a megadott mveletekre nézve csoportot alkotnak.

1. Az egész számok az összeadásra nézve. $(\mathbb{Z}, +)$.
2. Az összes racionális (vagy valós, vagy komplex) számok az összeadásra nézve.
3. A nem zérus (másképpen szólva a 0-tól különböző) racionális (vagy valós) számok a szorzás mveletével.

4. Legyen H a modulo m szerint vett teljes maradékrendszer ($H = \{0, 1, \dots, m-1\}$), a mvelet pedig a maradékosztályokon értelmezett összeadás.

A művelet zártága egyértelmű, hiszen két maradékosztályt összeadva ismét egy maradékosztályt kapunk, ha az összeadás a maradékosztályokon értelmezett összeadás. Az asszociativitás szintén triviálisan teljesül. Az egységelem a 0 maradékosztály, hiszen ha egy tetszőleges számhoz m -mel osztható számot adunk, akkor a szám maradéka nem változik modulo m . Az x maradékosztály inverze pedig az $m - x$ maradékosztály, hiszen ha $a \equiv x \pmod{m}$ és $b \equiv m - x \pmod{m}$, akkor $a + b \equiv x + m - x = 0 \pmod{m}$. Vagyis a csoporttulajdonság mindegyik feltétele teljesül.

5. A tér vektorai a vektorösszeadás műveletére nézve.

6. Az $n \times n$ -es mátrixok az összeadás műveletére nézve.

Részcsoporth

A G csoport részhalmazait **komplexusoknak** is szokták nevezni.

Tekintsük a 3-adfokú szimmetrikus csoport következő komplexusát:

```
> A:=[seq(evalm(P||i),i=1..3)];
```

Megmutatjuk, hogy A a permutációk egymás utáni elvégzésére, mint műveletre nézve maga is csoportot alkot.

Elsőször megmutatjuk, hogy A a $\circ$ műveletre nézve zárt, tehát A bármely két elemével elvégezve a műveletet, ismét A -beli elemhez jutunk.

Képezzük a műveleti táblát!

```
> M:=matrix(4,3,[A1,A2,A3,seq(seq(permszor(A[i],A[j])),i=1..3),j=1..3)]);
```

```
> Oszlop:=matrix(4,1,['o',A1,A2,A3]);
```

```
> M1:=linalg[concat](Oszlop,M);
```

```
> map(t->evalm(t),M1);
```

Azonnal látható, hogy a művelet zárt. A műveleti tábla az elemek nevével:

```
> matrix(4,4,['o',A1,A2,A3,A1,A1,A2,A3,A2,A2,A3,A1,A3,A3,A1,A2]);
```

Mivel $A \subset H$, és $G = (H, \circ)$ csoport, tehát a művelet asszociatív, így ez nyilván teljesül az A -beli elemekre is. A -ban van egységelem, ez $A1$. Minden elemnek van inverze. Az $A2$ inverze $A3$, s nyilván $A3$ inverze $A2$, s az egységelem inverze önmaga.

Ezzel megmutattuk, hogy a $(A, \circ)$ struktúra maga is csoport.

12.6.1. Definíció

A G csoport A komplexusát a G részcsoporthjának mondjuk, ha A elemei a G -beli műveletre nézve maguk is csoportot alkotnak.

Mondhatjuk tehát, hogy a harmadfokú szimmetrikus csoport

$$A := \left[\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right]$$

komplexusa (részhalmaza) a szimmetrikus csoport részcsoporthját alkotja.

12.6.2. Definíció

Az n -edfokú szimmetrikus csoport részcsoportjait n -edfokú permutációcsoportoknak hívjuk.

Ennek alapján a $G_1 = (A, \circ)$ harmadfokú permutációcsoport.

Mivel a csoport asszociatív struktúra, másképpen szólva az értelmezett művelet asszociatív, beszélhetünk a **csoport elemeinek hatványáról**. Így

$$a^n = a \cdot a \cdot \dots \cdot a$$

minden $n \in \mathbb{N}$ eseten természetesen eleme a csoportnak. A csoport minden elemével együtt az elem inverze is eleme a csoportnak, s ezt a^{-1} -nel jelöljük, mivel

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

$$(a^2)^{-1} = a^{-1} \cdot a^{-1} = (a^{-1})^2$$

s általánosan

$$(a^{-1})^n = (a^n)^{-1} = a^{-n}.$$

Vizsgáljuk a G_1 egységelemtől különböző elemeinek hatványait. Az A_2^2 :

```
> 'A[2]^2'=permszor(A[2],A[2]);
```

Az $A_2^2 = A_3$. Képezzük most az A_2^3 -öt:

```
> 'A[2]^3'=permszor(permszor(A[2],A[2]),A[2]);
```

Ez éppen $A_1 = e$, vagyis az egységelem (neutrális elem). Észrevehetjük, hogy az A_2 elem hatványai a G_1 csoport valamennyi elemét előállítják. Adott elem 0-adik hatványa minden, az egységelemet tartalmazó struktúrában az egységelem, tehát $A^0 = e$.

Mondhatjuk tehát, hogy az e, A_2, A_2^2 alapséma ciklikusan ismétlődik, hiszen pl. $A_2^3 = e, A_2^4 = A_2$,

Ugyanezt elmondhatjuk az A_3 elem hatványairól is.

12.6.3. Definíció

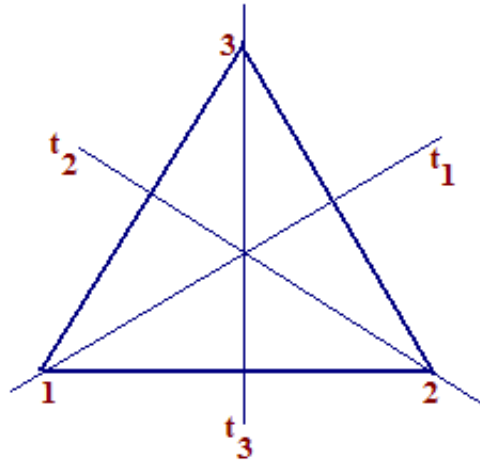
Ha egy csoport minden eleme kifejezhető (másképpen szólva **generálható**) egyetlen elem hatványaival, akkor a csoportot **ciklikus csoportnak** mondjuk. A szóbanforgó elemet a csoport **generátorelemének**, rövidebben **generátorának** mondjuk. Ha n az a legkisebb pozitív kitevő, amelyre $a^n = e$, akkor az a által generált csoport n -edrendű.

A $G_1 = (A, \circ)$ harmadfokú permutációcsoport egyetlen elemével, A_2 -vel, vagy A_3 -mal generálható, tehát harmadrendű ciklikus csoport.

Izomorf csoportok

12.7.1. Példa.

Adott a síkon egy szabályos háromszög. Hány olyan egybevágósági transzformációja van a síknak, amely a háromszöget önmagába viszi át? Adjuk meg ezeket a transzformációkat! Bizonyítsuk be, hogy ezek a transzformációk csoportot alkotnak. (A művelet a transzformációk egymás utáni végrehajtása.)



2. ábra

Könnyen látható, hogy az identikus (azonos) transzformáció, a háromszög középpontja körüli $\frac{2 \cdot \pi}{3}$ és $\frac{4 \cdot \pi}{3}$ szög elforgatások, továbbá a szimmetriatengelyekre vonatkozó tükrözések az adott

háromszöget önmagába viszik át. A keresett transzformációknak a háromszög csúcsait csúcsba kell átvinniük. Jelöljük a háromszög csúcsait az 1, 2 és 3 számokkal. (2. ábra)

Ha megadjuk, hogy az 1 és 2 pont mibe megy át, akkor a harmadik csúcs helye egyértelműen meghatározott. Az 1 és 2 pontokkal határolt szakaszt mindegyik háromszögoldalra kétféleképpen helyezhetjük rá, ezért $3 \cdot 2 = 6$ olyan egybevágósági transzformáció van, amely a háromszöget önmagába viszi át. A felsorolt 6 transzformációnál több nincs.

A csoportaxiómák teljesülése nyilvánvaló. Mint láttuk a transzformációkat egyértelműen meghatározza, ha megadjuk a csúcsok képét.

Észrevehetjük, hogy a bevezetett jelöléssel minden egyes transzformáció az 1, 2, 3 elemek egy permutációja. Ezek szerint természetes módon használhatjuk a permutációknál bevezetett jelölést:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Az e az identikus transzformációt, f_1 és f_2 a forgatásokat, t_1 , t_2 és t_3 a tengelyes tükrözéseket jelenti.

Azonnal látszik, hogy ezek rendre épp a 3-odfokú szimmetrikus csoport elemei, azaz a

$$P_1, P_2, P_3, P_4, P_5, P_6$$

permutációk. Feleltessük meg minden egyes transzformációnak éppen azt a permutációt, amely a háromszög csúcsait a megfelelő helyzetbe hozza. Ilyen módon olyan egy-egyértelmű megfeleltetést hoztunk létre a most tárgyalt transzformációkból álló csoport (transzformációcsoport) és a 3-odfokú szimmetrikus csoport elemei között, amely leépezés mvelettartó, tehát bármely két elem szorzatának képe megegyezik a képelemek összegével. (Itt a mveletek megjelölésére jelentés-kiterjesztéssel használjuk a "szorzat" ill. az "összeg" megjelölést. Jelöljük ugyanis a transzformációk egymásutáni elvégzésének mveletét # -kal, a permutációk szorzatát $\circ$ -rel.

Ekkor például

$$f_1 \# t_2 = t_3$$

azaz az $f_1 \frac{2 \cdot \pi}{3}$ szög forgatás és a t_2 tengelyre való tükrözés egymásutáni elvégzése egyenérték a t_3 tengelyre való tükrözéssel.

Az f_1 forgatásnak a P_2 permutáció, a t_2 tükrözésnek a P_5 permutáció felel meg, s ezek szorzata

$$P_2 P_5 := \text{permszor}(P_2, P_5) = P_6;$$

s ez éppen a t_3 tükrözésnek megfelelő permutáció. Az mondjuk, hogy a két struktúra, a két csoport "azonos formájú", más szóval **izomorf**.

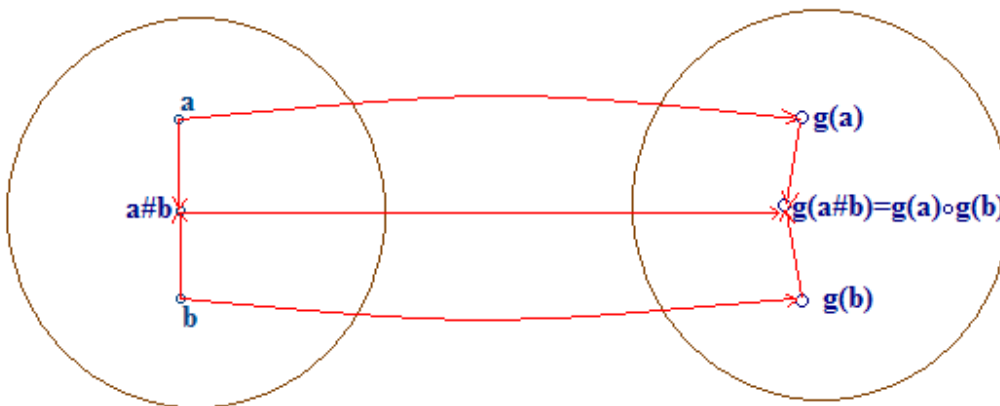
12.7.2. Definíció

Ha az $S = (A, \#)$ és az $S' = (A', \circ)$ struktúrákhoz létezik egy bijektív g leképezés úgy, hogy

$$\begin{aligned} g(a) = a' \text{ és } g(b) = b' \\ \text{esetén } (a, b \in A, a', b' \in A') \\ g(a \# b) = g(a) \circ g(b) = a' \circ b', \end{aligned}$$

akkor az S és az S' struktúrák **izomorfak**.

A $g(a \# b) = g(a) \circ g(b) = a' \circ b'$ egyenlőség azt jelenti, hogy a leképezés mvelettartó, azaz az elemek szorzatának képe megegyezik a képelemek összegével. A szorzat és összeg megjelölés itt természetesen tetszleges binér, bels mveletet jelenthet. (3. ábra)



3. ábra

Megjegyzés: a leképezést akkor mondjuk **bijektívnek**, ha *injektív* és *szurjektív* egyidejleg. Az injektivitás azt jelenti, hogy különböz elemek képe különböz (egy-egyértelmű a leképezés), a szurjektivitás pedig azt, hogy a leképezés értékkészlete megegyezik a képtartománnyal, tehát itt S' minden eleme képe valamely S -beli elemnek.

Mint láttuk a szabályos háromszöget önmagára leképez egybevágósági transzformációk csoportja

izomorf a 3-adfokú szimmetrikus csoporttal. Ez nem esetleges kapcsolat. Erről szól a következő tétel.

12.7.3. Tétel. (Cayley tétele)

Tetszőleges n -edrendű csoport izomorf egy n -edfokú permutációcsoporttal.

Bizonyítás

Legyen G n -edrendű, és legyenek elemei valamilyen sorrendben: $a_1, a_2, \dots, a_n$. Tekintjük az $a_1, a_2, \dots, a_n$ elemek permutációiból álló S_n n -edrendű szimmetrikus csoportot. G a_i elemének megfeleltetjük a

$$\pi_i = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \end{pmatrix} = \begin{pmatrix} x \\ x \cdot a_i \end{pmatrix}$$

permutációt. A π_i és a π_j szorzata

$$\pi_i \cdot \pi_j = \begin{pmatrix} x \\ x \cdot a_i \end{pmatrix} \cdot \begin{pmatrix} y \\ y \cdot a_j \end{pmatrix} = \begin{pmatrix} x \\ x \cdot a_i \end{pmatrix} \begin{pmatrix} x \cdot a_i \\ (x \cdot a_i) \cdot a_j \end{pmatrix} = \begin{pmatrix} x \\ (x \cdot a_i) \cdot a_j \end{pmatrix} = \begin{pmatrix} x \\ x \cdot (a_i \cdot a_j) \end{pmatrix},$$

vagyis az $a_i \cdot a_j$ szorzatelemnek megfelel permutáció. Az $a_i \rightarrow \pi_i$ leképezés tehát G -nek S_n -be való mvelettartó leképezése. Ha $a_i \neq a_j$, akkor $\pi_i \neq \pi_j$, mert π_i és π_j a G neutrális elemét az a_i -be, ill. az a_j -be viszi át. Így az $a_i \rightarrow \pi_i$ leképezés izomorfizmus G és S_n egy részcsoportja között.

12.7.4. Példa

Tekintsük a mod 6 maradékosztályok halmazát $H = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

- (1) Mutassuk meg, hogy a $\{H, +\}$ struktúra csoport.
- (2) Igazoljuk, hogy a csoport izomorf egy 6-edrendű permutációcsoporttal.

Megoldás

Ismétlésként tekintsük át a maradékosztály fogalmát. (1.8.7)

Kongruenciareláció, maradékosztályok

12.7.5. Definíció

Az a és b egész számokat az $m \neq 0$ rögzített egész számra nézve kongruensnek nevezzük, ha az a és b m -mel való osztásnál azonos maradékot adnak.

Az m számot modulusnak nevezzük. A kongruenciareláció jelölése

$$a \equiv b \pmod{m}$$

Könnyen látható, hogy a kongruenciareláció definícióját a következőképp is megadhatjuk.

12.7.6. Definíció

$$a \equiv b \pmod{m}, \text{ ha } m \mid (a - b)$$

12.7.7. Tétel

Legyen m pozitív egész és $m > 1$. Mutassuk meg, hogy az

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

ekvivalenciareláció az egészek halmazán.

Bizonyítás

Mivel $a - a = 0$, és a 0 bármely egész számmal osztható, a reláció **reflexív**.

Tegyük föl, hogy $a \equiv b \pmod{m}$. Ez azt jelenti, hogy van olyan k egész szám, amelyre

$a - b = k \cdot m$. Ebből következik, hogy $b - a = (-k) \cdot m$, tehát $b \equiv a \pmod{m}$, vagyis a reláció **szimmetrikus**.

Tegyük most föl, hogy $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}$ teljesül. De ekkor az m osztója az $a - b$ -nek és a $b - c$ -nek, azaz létezik olyan egész k és egész l szám, amelyekre $a - b = k \cdot m$ és $b - c = l \cdot m$ teljesül. Összeadva a két egyenletet adódik

$$a - c = (a - b) + (b - c) = k \cdot m + l \cdot m = (k + l) \cdot m,$$

tehát $a \equiv c \pmod{m}$. Ez azt jelenti, hogy a reláció **transzítív**. Ezzel beláttuk, hogy a kongruenciareláció rendelkezik az ekvivalenciareláció mindhárom tulajdonságával, tehát a kongruenciareláció ekvivalenciareláció.

Az egész számok adott m modulus esetén m különféle maradékot adhatnak. Ha pl. $m=5$, akkor a lehetséges maradékok: 0, 1, 2, 3, 4. Két egész szám pontosan akkor ad 5-tel osztva azonos maradékot, ha kongruensek egymással modulo 5. A kongruenciareláció figyelembe vételével tehát az egészeket ún. osztályokba sorolhatjuk.

Ezek az osztályok az ún. maradékosztályok modulo m . Minden egész beletartozik pontosan egy osztályba. Az osztályok szokásos jelölése $0, 1, 2, 3, 4, 5, \dots$

Állítsuk el a műveleti táblát. Az összeadást a maradékosztályok között úgy értelmezzük, hogy az összeadás elvégzése után az eredmény 6-tal való osztásának maradékát vesszük.

A műveleti tábla képzése

```
> Oszlop:=matrix(7,1,['+',seq('m'|i',i=0..5)]):
> M:=matrix(7,6,[seq('m'|i',i=0..5),seq(seq((i + j) mod 6,i=0..5),j=0..5)]):
> M1:=linalg[concat](Oszlop,M):
> tábla:=map(t->evalm(t),M1);
```

'+' m0 m1 m2 m3 m4 m5	m0	m1	m2	m3	m4	m5
m0	0	1	2	3	4	5
m1	1	2	3	4	5	0
m2	2	3	4	5	0	1
m3	3	4	5	0	1	2
m4	4	5	0	1	2	3
m5	5	0	1	2	3	4

A művelet zártága egyértelmű, hiszen két maradékosztályt összeadva ismét egy maradékosztályt kapunk, ha az összeadás a maradékosztályokon értelmezett összeadás. Az asszociativitás szintén triviálisan teljesül. Az egységelem a 0 maradékosztály, hiszen ha egy tetszőleges számhoz 6-tal osztható számot adunk, akkor a szám maradéka nem változik modulo 6. Az x maradékosztály inverze

pedig az $6 - x$ maradékosztály, hiszen ha $a \equiv x \pmod{6}$ és $b \equiv 6 - x \pmod{6}$, akkor $a+b \equiv x + 6 - x = 0 \pmod{6}$. Vagyis a csoporttulajdonság mindegyik feltétele teljesül.

Eljárás a Cayley-tétel realizálására

A `csop_izo` eljárás a mod n maradékosztályok additív csoportja esetén realizálja a Cayley-tételt, vagyis minden maradékosztályhoz hozzárendeli a tétel által elírt permutációt.

```
> csop_izo:=proc()
  local i,M,N,n,k,j,sor1,sor2;
  global A:
  n:=args[1]:
  if not(type(n,posint)) then RETURN(`n pozitív egész`) fi:
  k:=args[2]:
  if not(type(k,nonnegint)) then RETURN(`n pozitív egész`) fi:
  sor1:=seq(i,i=1..n):
  M:=matrix(1,n,[sor1]):
  sor2:=seq(j+k mod n,j=1..n):
  for i to n do if sor2[i]=0 then sor2[i]:=sor2[i]+n fi od:
  N:=matrix(1,n,sor2):
  A:=linalg[stackmatrix](M,N):
  evalm(A)
end:
```

Cayley tétele alapján a mod 6 maradékosztályok 6-odrend additív csoportja izomorf a 6-odfokú szimmetrikus csoport egy részcsoportjával, egy 6-odfokú permutációcsoporttal. A `csop_izo` eljárással megkeressük a megfelel permutációkat, s megmutatjuk, hogy ezek csoportot alkotnak.

Nézzük meg elsőször, hogy melyik permutáció felel meg a 0 osztálynak

```
> csop_izo(6,0);
```

A várakozásnak megfelelően ez az identikus permutáció. Keressük meg az összes elemhez a megfelel permutációt!

```
> for i from 0 to 5 do
  csop_izo(6,i):
  q||i:=evalm(A)
od:
> seq(q||i:=evalm(q||i),i=0..5);
```

Mutassuk meg, hogy a kapott 6 permutáció csoportot alkot! Képezzük mindenekeltt a mveleti táblát

```
> Oszlop:=matrix(7,1,[`o`,seq('Q||i',i=0..5)]):
> M:=matrix(7,6,[seq('Q||i',i=0..5),seq(seq(permszor(q||i,q||j),
  i=0..5),j=0..5)]):
> M1:=linalg[concat](Oszlop,M):
> map(t->evalm(t),M1);
```

A táblából leolvasható, hogy a $\{q1, q2, q3, q4, q5, q6\}$ halmaz zárt a permutációk egymásutáni végrehajtására, mint mveletre nézve. A $q1$ elem inverze a $q5$, a $q2$ inverze a $q4$, a $q3$ inverze önmaga. Az asszociativitás természetesen teljesül.

A csoport ciklikus, a $q1=q$ hatványaként összes eleme eláll:

```
> q^1=evalm(q1);
> for i to 5 do q^(i+1)=permszor(rhs(%),q1) od;
```

Adalék a csoportok izomorfijához

12.8.1. Példa

Tekintsük a következő mátrixokat

$$M1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad M2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \quad M3 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}; \quad M4 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Mutassuk meg, hogy ezek a mátrixok a mátrixszorzás mveletére nézve csoportot alkotnak. (**Klein-féle négyes csoport**)

Megoldás

Mindenekelőtt idézzük fel a mátrixok szorzásáról tanultakat a 2×2 -es mátrixok szorzása kapcsán.

Adjuk meg a mátrixokat:

```
> A:=matrix(2,2);B:=matrix(2,2):
> evalm(A),evalm(B);
> A*B=evalm(A*B);
```

A szorzatmátrix els sorának els elemét úgy kapjuk, hogy az els tényez, tehát az A mátrix els sorának vesszük a második tényez, azaz a B mátrix, els oszlopával való kompozícióját, az $A_{1,1}B_{1,1} + A_{1,2}B_{2,1}$ kifejezést, tehát a megfelel elemek szorzatának összegét. Ugyanígy járunk el a többi esetben is.

Adjuk meg most a szóbanforgó mátrixokat:

```
> M|1:=matrix(2,2,[1,0,0,1]);M|2:=matrix(2,2,[1,0,0,-1]);M|3:=
matrix(2,2,[-1,0,0,1]);M|4:=matrix(2,2,[-1,0,0,-1]);
```

A mveleti tábla képzése

```
> h:=[seq(seq(evalm(M|i&*M|j)),i=1..4),j=1..4)];
> matrix(4,4,h):
> Oszlop:=matrix(5,1,['`',seq('M|i',i=1..4)]):
> A:=matrix(5,4,[seq('M|i',i=1..4),op(h)]):
> A1:=linalg[concat](Oszlop,A):
> tabla:=map(t->evalm(t),A1):
```

```
> map(t->evalm(t),tabla);
```

A mveleti tábláról leolvashatjuk, hogy valóban csoporthoz jutottunk, ez a Klein-féle négyes csoport.

A csoport egységeleme az $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ mátrix. Minden elem önmagával való szorzata, azaz második hatványa az egységelemet adja, másképpen szólva minden elem önmaga inverze.

12.8.2. Definíció

Ha G csoport, e a neutrális eleme és $a \in G$, akkor az a **elem rendjének** nevezzük azt a legkisebb pozitív egész k számot, melyre

$$a^k = e.$$

Az a elem rendjét $o(a)$ -val jelöljük.

A Klein-féle négyes csoport minden - az egységelemtől különböző - eleme másodrendű. A csoport rendje -elemeinek száma- 4. **Az elemek rendje osztója a csoport rendjének. Ez minden csoport minden elemére igaz.**

12.8.3. Példa

Ismeretes, hogy I a képzetes egység, amelyre $I^2 = -1$. Tekintsük a következő mátrixokat

$$M1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad M2 = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}; \quad M3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}; \quad M4 = \begin{bmatrix} -I & 0 \\ 0 & -I \end{bmatrix};$$

Legyen a művelet ismét a mátrix-szorzás!

```
> M1:=matrix(2,2,[1,0,0,1]);M2:=matrix(2,2,[I,0,0,I]);M3:=
matrix(2,2,[-1,0,0,-1]);M4:=matrix(2,2,[-I,0,0,-I]);
```

Képezzük ismét a műveleti táblát:

A műveleti tábla képzése

```
> h:=[seq(seq(evalm(M1+i*Mj),i=1..4),j=1..4)];
> matrix(4,4,h);
> Oszlop:=matrix(5,1,['*',seq('M'+i,i=1..4)]);
> A:=matrix(5,4,[seq('M'+i,i=1..4),op(h)]);
> A1:=linalg[concat](Oszlop,A);
> tabla:=map(t->evalm(t),A1);
```

```
> map(t->evalm(t),tabla);
```

Ismét csoporthoz jutottunk. Ez a csoport is 4-edrendű, s van egy érdekes tulajdonsága. Tekintsük ugyanis az $M2$ elem hatványait.

```
> seq(evalm(M2^i),i=1..4);
> seq(evalm(M3^i),i=1..4);
>
```

Az $M2$ hatványaként a csoport össze eleme eláll! Másképpen szólva a csoport egyetlen elemmel generálható. Mint már tudjuk, az ilyen csoportokat **ciklikus csoportnak** mondjuk. Az $M2$ elem rendje

4, azaz $o(M_2) = 4$. Ciklikus csoport rendje megegyezik a generáló elemének rendjével. Ez a csoport nem izomorf a Klein-féle négyes csoporttal. Ismeretes ugyanis a következő tétel:

12.8.4. Tétel

Minden négyelem csoport izomorf vagy a négyelem ciklikus csoporttal, vagy a Klein-csoporttal, attól függően, hogy van-e benne negyedrend elem, vagy nincs.

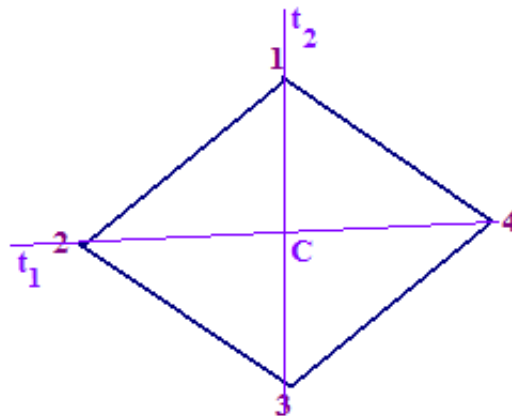
12.8.5. Példa

Adott a síkon egy rombusz. Tekintsük a sík azon egybevágósági transzformációit, amelyek a rombuszt önmagába viszik át.

- (1) Mutassuk meg, hogy ezek a transzformációk csoportot alkotnak. (A művelet a transzformációk egymás utáni végrehajtása.)
- (2) Igazoljuk, hogy ez a csoport izomorf a Klein-féle négyes csoporttal.

Megoldás

A keresett transzformációknak a rombusz csúcsait csúcsba kell átvinniük. Jelöljük a rombusz csúcsait az 1, 2, 3 és a 4 számokkal. (4. ábra)



4. ábra

Négy olyan transzformáció van, amely a rombuszt önmagába viszi át, ezek átlókra (t_1, t_2) való tükrözés, a középpontos tükrözés (C) , és az identitás (azonos leképezés). Ezek mindegyike leírható a csúcsok egy-egy permutációjával:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; \quad t_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}; \quad t_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}; \quad t_C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Az e, t_1, t_2, t_C rendre az identikus transzformációt, a tengelyes tükrözést és a középpontos tükrözést jelenti.

```

> e:=matrix(2,4,[1,2,3,4,1,2,3,4]);t|1:=matrix(2,4,[1,2,3,4,3,2,1,4]);t|2:=matrix(2,4,[1,2,3,4,1,4,3,2]);t|C:=matrix(2,4,[1,2,3,4,3,4,1,2]);
> L:=[e,t1,t2,tC];
> H:=seq(seq(permszor(L[i],L[j]),i=1..4),j=1..4):
> T:=matrix(4,4,[H]):
> Oszlop:=matrix(5,1,['*', 'e', 't1', 't2', 'tC']):
> Sor:=matrix(1,4,['e', 't1', 't2', 'tC']):
> M:=linalg[stackmatrix](Sor,T):
> M1:=linalg[concat](Oszlop,M):
> tábla:=map(t->evalm(t),M1);

```

A mveleti tábláról leolvasható, hogy csoportot kaptunk. Az e az egységelem, minden elem önmagának inverze, az egységelemet kivéve minden elem rendje 2. Ez a tétel alapján azt jelenti, hogy a csoport a Klein-féle négyes csoporttal izomorf. Ezt közvetlenül is beláthatjuk. Az $\{e, t1, t2, tC\}$ halmaz elemeinek feleltessük meg rendre az $\{M1, M2, M3, M4\}$ elemeit. Azonnal látható, hogy ekkor mvelettartó izomorf leképezést létesítettünk.

▼ Kétmveletes struktúrák

Az elzben olyan stuktúrákkal foglalkoztunk, amelyekben egy mvelet volt értelmezve. Most olyan struktúrák vizsgálatára térünk át, amelyekben két mvelet, az "összeadás" és a "szorzás" van definiálva.

▼ G y r

Az egész számok az összeadás mveletére nézve kommutatív csoportot alkotnak, a szorzás mveletére nézve pedig félcsoporthat. A szorzás mvelete disztributív az összeadásra nézve.

12.9.1. Definíció

Az $R = (A, +, \cdot)$ kétmveletes struktúrát **gyr** nek nevezzük, ha a következ tulajdonságokkal rendelkezik:

1. $(A, +)$ kommutatív csoport;
2. $(A, \cdot)$ félcsoporthat
3. A $\cdot$ mvelet disztributív a $+$ mveletre nézve, azaz $\forall a, b, c \in A$ esetén:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Ha a $\cdot$ mvelet kommutatív, akkor kommutatív gyrrl beszélünk.

12.9.2. Példák

1. Az elz alapján az egész számok gyrt alkotnak az összeadásra és a szorzásra nézve. $(\mathbb{Z}, +)$.
2. Gyrt alkotnak a páros számok az összeadásra és a szorzásra nézve. A páratlan egészekre ez már nem teljesül, hisz két páratlan szám összege páros.

3. Gyűrűt alkotnak a valós (komplex) elemű $n \times n$ es mátrixok a mátrix-összeadással és a mátrix-szorzással.

4. Érdekes a következ

12.9.3. Példa

Tekintsük a [mod \$m\$ maradékosztályok](#) halmazát az összeadás és a szorzás mveletével. Az összeadást és a szorzást a maradékosztályok között úgy értelmezzük, hogy az összeadás ill a szorzás elvégzése után az eredmény m -mel való osztásának maradékát vesszük. Mutassuk meg, hogy a

$$(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}, +, \cdot)$$

struktúra minden $m \in \mathbb{Z} \setminus \{1\}$ esetén gyrt alkot. Vannak-e olyan m értékek, amelyekre a $(\{\overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}, \cdot)$ struktúra csoportot alkot?

Megoldás

Legyen először $m = 6$. Az osztályok közötti *összeadás* és *szorzás* mveletét az alábbi két eljárással végezzük. Az eljárások elkészítik a mveleti táblát. Paraméterük a modulus értéke.

Eljárások a maradékosztály-mveletek elvégzésére

```
> összeadás:=proc(n::posint)
  local oszlop,M,M1:
  oszlop:=matrix(n+1,1,['+ ',seq('i',i=0..n-1)]):
  M:=matrix(n+1,n,[seq('i',i=0..n-1),seq(seq((i+j) mod n,
i=0..n-1),j=0..n-1)]):
  M1:=linalg[concat](oszlop,M):
  print(map(t->evalm(t),M1));
end:

> szorzás:=proc(n::posint)
  local oszlop,M,M1:
  oszlop:=matrix(n+1,1,['* ',seq('i',i=0..n-1)]):
  M:=matrix(n+1,n,[seq('i',i=0..n-1),seq(seq((i*j) mod n,
i=0..n-1),j=0..n-1)]):
  M1:=linalg[concat](oszlop,M):
  print(map(t->evalm(t),M1));
end:
```

1. Összeadás

```
> összeadás(6);
```

Az összeadás a $(\mathbb{Z}, +)$ csoportból öröklően asszociatív és kommutatív. A táblázatból látható, hogy a 0 a neutrális elem, továbbá minden elemnek van ellentettje (inverze), ugyanis minden sorban és minden oszlopban elfordul a 0. Tehát a

$$(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}, +)$$

struktúra kommutatív csoport.

2. Szorzás

```
[> szorzás(6);
```

A szorzás asszociatív (és kommutatív), egységelem is létezik (1), de csak az 1 és az 5 invertálható, a többi sor (oszlop) nem tartalmazza az 1-et. Az 5 inverze önmaga (idempotens elem), $5 \cdot 5 = 1$. A $(\{0, 1, 2, 3, 4, 5\}, \cdot)$ struktúra nem alkot csoportot, csupán egységelemes kommutatív félcsoport. A disztributivitás az egészek körébe öröklően teljesül.

A $(\{0, 1, 2, 3, 4, 5\}, +, \cdot)$ struktúra tehát *kommutatív gyr*. Ezt a gyrt **maradékosztály-gyr** nek nevezzük.

Legyen most $m = 7$. A szorzás műveleténél most zárjuk ki a $\overline{0}$ osztályt. A szorzás eljárást módosítjuk

```
[> szorzás1:=proc(n::posint)
  local oszlop, M, M1:
  oszlop:=matrix(n, 1, [ `* ` , seq('i', i=1..n-1) ]):
  M:=matrix(n, n-1, [ seq('i', i=1..n-1), seq(seq((i * j) mod n, i=
1..n-1), j=1.. n-1) ]):
  M1:=linalg[concat](oszlop, M):
  print(map(t->evalm(t), M1));
end:
```

1. Összeadás

```
[> összeadás(7);
```

Az összeadás kapcsán ugyanazt mondhatjuk, mint az imént, a $(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, +)$ struktúra kommutatív csoport

Nézzük a szorzást!

```
[> _szorzás1(7);
```

A $\overline{0}$ osztály, tehát az összeadás neutrális elemének (zéruselemének) kizárásával kapott $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ halmaz kommutatív csoportot alkot az összeadás műveletére nézve. A szorzás kommutatív és asszociatív. Létezik egységelem és minden elemnek van inverze (minden sorban és minden oszlopban elfordul az 1) Teljesül a disztributivitás is. Tehát $m = 7$ esetén a $(\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, \cdot)$ struktúra is (kommutatív) csoport.

Vizsgáljuk meg most néhány m érték esetén a $(\{\overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}, \cdot)$ struktúrát!

Legyen először m prímszám!

```
[> seq(szorzás1(i), i=[3, 5, 7]):
```

A műveleti táblából látszik, hogy minden esetben csoportot kaptunk. Legyen most m összetett szám!

```
[> seq(szorzás1(i), i=[4, 6, 8]);
```

```
[>
```

Láthatóan egyik esetben sem kaptunk csoportot, hiszen minden esetben csak a modulushoz relatív prím elemeknek létezik az inverze.

12.9.4. Sejtés

A $(\{\overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}, \cdot)$ struktúra akkor és csak akkor csoport, ha m prímszám.

A sejtés bizonyítható.

A műveleti táblákat szemlélgetve egy érdekes jelenségre figyelhetünk föl. Vegyük például a mod 6 maradékosztály-gyrt. Itt a szorzás műveleti táblája a következő:

```
[> szorzás1(6);
```

Észrevehetjük, hogy a szorzás eredménye úgy is lehet 0 - pontosabban a $\overline{0}$ osztály, tehát az összeadás neutrális eleme, másképp zéruseleme, hogy egyik szorzótényez sem 0. Például:

$> (3 \cdot 2) \bmod 6;$

A szorzat eredménye 0, holott egyik tényez sem 0.

12.9.5. Definíció

Ha $a \neq 0$ és $b \neq 0$, de $a \cdot b = 0$, akkor az a -t baloldali, a b -t jobboldali **nullosztónak** nevezzük. Célszer magát a 0-t is nullosztónak tekinteni, így $a \in R$ baloldali nullosztó, ha létezik olyan $b \in R$, hogy $b \neq 0$ és $a \cdot b = 0$.

Az olyan gyrt, amelyben a 0-n kívül nincs nullosztó, nullosztómentes gyrnek nevezzük. A kommutatív, nullosztómentes gyrt **integritási tartománynak** nevezzük

A mod 6 maradékosztály-gyr tehát nem nullosztómentes, hiszen több nullosztója is van: a 2, a 3 és a 4.

Test

12.10.1. Definíció

A $T = (A, +, \cdot)$ kétmveletes struktúrát testnek nevezzük, ha

1. $(A, +)$ kommutatív csoport;
2. $(A \setminus \{0\}, \cdot)$ kommutatív csoport;
3. a szorzás disztributív az összeadásra nézve.

A 0 itt az + zéruselemét jelenti. Tehát az összeadás zéruselemét kizártuk a szorzásra vonatkozó halmazból. Ennek szükségessége a racionális (vagy a valós) számok példáján könnyen érthet. A 0 nem invertálható, mert nincs olyan elem, amelyet 0-val szorozva 1-et kapunk. Ezért nem értelmezhet a 0-val való osztás a racionális (valós) számok körében.

12.10.2. Példák

1. Az elz szakaszban azt kaptuk, hogy a $(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, +)$ struktúra kommutatív csoport, s a $\overline{0}$ osztály kizárásával kapott $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ halmaz is csoport a maradékosztály-szorzás mveletére nézve. Teljesül a disztributivitás is.

Tehát a modulo 7 maradékosztályok halmaza testet alkot az összeadás és a szorzás mveletére nézve, azaz a

$$(\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, +, \cdot)$$

struktúra test. Általában is igaz a következ

12.10.3. Tétel

A $\mathbb{Z}_m = (\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}, +, \cdot)$ ($m > 1$) maradékosztály-gyr akkor és csak akkor test, ha m prímszám.

2. Fontos számtestek a következ:

$(\mathbb{Q}, +, \cdot)$ a **racionális számok** teste az összeadás és a szorzás mveletére nézve;

$(\mathbb{R}, +, \cdot)$ a **valós számok** teste az összeadás és a szorzás mveletére nézve;

($\{\mathbb{C}, +, \cdot\}$) a **komplex számok** teste az összeadás és a szorzás műveletére nézve.

Ellenrz kérdések

1. Mit értünk a függvény fogalma alatt?
2. Igaz-e, hogy minden függvény reláció?
3. Mit értünk bináris művelet alatt? Fejtse ki, hogy mit jelent a bináris, ill. a belső jelző!
4. Mit nevezünk algebrai struktúrának?
5. Mit jelent az, hogy egy művelet asszociatív? Hozzon példát nem asszociatív műveletre!
6. Mit értünk félcsoporthoz?
7. Definálja a neutrális elem fogalmát!
8. Hány neutrális eleme lehet a félcsoporthoz?
9. Mit értünk az elem baloldali (jobboldali) inverze alatt?
10. Tegyük fel, hogy egy elemnek van baloldali- és jobboldali inverze is. Különözhetnek-e ezek egymástól?
11. Mit értünk az alatt, hogy a félcsoporthoz művelete invertálható?
12. Definálja a csoport fogalmát! Adjon példákat csoportra! Legyen ezek között véges- és végtelen elemszámú csoport is!
13. Mit értünk kompozitum alatt?
14. Definálja a részcsoporthoz fogalmát! A csoport mely elemét tartalmazza szükségképpen minden részcsoporthoz?
15. Adja meg a harmadfokú szimmetrikus csoport elemeit!
16. Mit értünk az alatt, hogy két egyműveletes struktúra izomorf?
17. Mit értünk ciklikus csoport alatt?
18. Adja meg azt a permutációcsoportot, amely izomorf a szabályos háromszöget önmagába átvivő (síkbeli) elforgatások csoportjával!
19. Definálja a gyűrű fogalmát! Adjon példákat gyűrűre! Legyen a példák között véges- és végtelen gyűrű is!
20. Mit értünk integritási tartomány alatt?
21. Definálja a test fogalmát! Adjon példákat testre! Legyen a példák között véges- és végtelen test is!

Példák, feladatok

1. Példa

$H = \mathbb{R} \setminus \{1\}$ halmazban definiáljuk a $\circ$ műveletet a következőképpen:

$$a \circ b = a + b - a \cdot b$$

Mutassuk meg, hogy a H halmaz a $\circ$ műveletre nézve kommutatív csoportot alkot!

Megoldás

1. A művelet zárttsága

Mindenekeltt megmutatjuk, hogy a **művelet zárt**, nem vezet ki az adott halmazból. Az $a + b - a \cdot b$ kifejezés láthatóan minden valós (a, b) számpárhoz valós számot rendel. Azt kell még megmutatnunk, hogy ha $a, b \in H = \mathbb{R} \setminus \{1\}$, akkor $a \circ b = a + b - a \cdot b$ is H -ban van. Nézzük, mely értékekre lenne az $a + b - a \cdot b$ kifejezés értéke 1:

$$a + b - a \cdot b = 1 \wedge \Leftrightarrow a + b - a \cdot b - 1 = 0 \Leftrightarrow a \cdot (1 - b) - (1 - b) = (a - 1) \cdot (1 - b) = 0 \Leftrightarrow a$$

$$= 1 \text{ vagy } b = 1$$

Ez azt jelenti, hogy a H egyetlen elemére sem lesz a művelet eredménye 1. Ez azt jelenti, hogy a művelet zárt.

2. Kommutativitás

A művelet kommutatív, mert

$$a \circ b = a + b - a \cdot b = b + a - b \cdot a = b \circ a$$

3. Asszociativitás

Azt kell megmutatnunk, hogy

$$a \circ (b \circ c) = (a \circ b) \circ c, \quad \forall a, b, c \in H$$

$$a \circ (b \circ c) = a \circ (b + c - b \cdot c) = a + b + c - b \cdot c - a \cdot (b + c - b \cdot c) = a + b + c - a \cdot b - b \cdot c - a \cdot c + a \cdot b \cdot c$$

A kapott kifejezés szimmetrikus, értéke nem változik, ha változóit ciklikusan felcseréljük, tehát

$$a \circ (b \circ c) = a + b + c - a \cdot b - b \cdot c - a \cdot c + a \cdot b \cdot c = c \circ (a \circ b) = (a \circ b) \circ c$$

Ezzel beláttuk, hogy a művelet asszociatív. Az utolsó lépésben felhasználtuk, hogy a művelet kommutatív.

4. Neutrális elem

Meg kell oldanunk az

$$a \circ e = a + e - a \cdot e = a$$

egyenletet a H halmazon.

$$a + e - a \cdot e = a \wedge a, e \in H \Leftrightarrow e - a \cdot e = 0 \wedge a, e \in H \Leftrightarrow e = 0$$

A neutrális elem $e = 0$.

5. Inverz elem

Meg kell mutatnunk, hogy H minden elemének van inverze H -ban. Ehhez meg kell oldanunk H -ban az

$$a \circ a^{-1} = a + a^{-1} - a \cdot a^{-1} = e = 0$$

egyenletet.

$$a + a^{-1} - a \cdot a^{-1} = a^{-1}(1 - a) + a = 0 \Leftrightarrow a^{-1} = \frac{a}{a - 1}$$

Mivel $a \neq 1$, $a^{-1} \neq 1$ teljesül, tehát minden H -beli a elemnek van inverze H -ban.

A megoldásban segítségünkre lehet a Maple is. Ehhez először létrehozuk a $\circ$ műveletet realizáló **muvelet** eljárást:

```
> muvelet:=proc(a,b)
    description "az eljárás kiszámítja az a+b-ab értékét";
    (a+b-a*b)
end;
```

```
> muvelet(a,b);
```

Az asszociativitást igazolandó képezzük először az $a \circ (b \circ c)$, majd a $(a \circ b) \circ c$ kifejezést!

```
> baloldal:=expand(muvelet(muvelet(a,b),c));#az expand elvégzi a
    beszorzásokat
```

```
> jobboldal:=expand(muvelet(a,muvelet(b,c)));
```

A két oldal láthatóan megegyezik.

```
> egyenlet:=muvelet(a,e)=a;
```

```
> e:=solve(egyenlet,e);
```

```
> egyenlet1:=muvelet(a,a_inv)=e;
```

```
> a_inv:=solve(egyenlet1,a_inv);
```

```
> muvelet(a,a_inv);#Képezzük az elem és inverzének "szorzatát"!
```

```
> simplify(%);#Hozzuk egyszerűbb alakra a kapott kifejezést!
```

Tehát az inverz elemet ezuttal is helyesen határoztuk meg.

1. Feladat

A valós számok $\mathbb{R}$ halmazában értelmezzük a következő mveletet:

$$a \circ b = \frac{a + b - a \cdot b + 1}{2}$$

a. Számítsuk ki a $3 \circ 1$, $(-1) \circ 2$, $0 \circ 4$ értékeket.

b. Mutassuk meg, hogy a $\circ$ mvelet kommutatív és asszociatív.

c. Mutassuk meg, hogy az $\mathbb{R} \setminus \{1\}$ halmaznak a $\circ$ mveletre nézve a -1 neutrális eleme.

d. Bizonyítsuk be, hogy az $\mathbb{R} \setminus \{1\}$ halmaz a $\circ$ mveletre nézve kommutatív csoportot alkot.

2. Példa

Bizonyítsuk be, hogy az $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$ függvények halmaza

csoportot alkot, ha mveletnek az összetett függvény képzését tekintjük.

Megoldás

Készítsük el a mvelet-táblázatot. Tegyük ezt meg papír-ceruza segítségével! Készítsünk Maple-eljárást is, amellyel ellenrizhetjük munkánkat!

```
> tabla:=proc(L::list)
```

```
    description "Az eljárás elkészíti az input L lista
```

```
    függvényeihez az összetett
```

```
    függvényképzés mveleti tábláját":
```

```
    local oszlop,oszlop1,M,M1,n,L1:
```

```
    n:=nops(L):
```

```
    L1:=map(t->unapply(t,x),L):
```

```
    oszlop:=matrix(n+2,1,['@ ',' ','seq('L1[i](x)',i=1..n)]):
```

```
    oszlop1:=matrix(n+2,1,['| ','-- ','seq('| ',i=1..n)]):
```

```
    M:=matrix(n+2,n,[seq('L[i]',i=1..n),seq('-- ',i=0..n-1),seq(seq(
    simplify((L1[i]@L1[j])(x)),i=1..n),j=1..n)]):
```

```
    M1:=linalg[concat](oszlop,oszlop1,M):
```

```
    print(map(t->evalm(t),M1));
```

```
end:
```

Adjuk meg a szóbanforgó függvényeket, mint kifejezéseket listában!

```
> L:=[x,1/x,-x,-1/x];
```

[Hívuk meg a tabla eljárást az L listára!

[> **tabla(L);**

- A táblázat minden sorában és minden oszlopában a struktúra minden eleme pontosan egyszer fordul el.
- Van olyan sor és oszlop, amelyben lev elemek sorrendje megegyezik a 0. sor és a 0. oszlop elemeivel. Ez a neutrális elem létezéséhez szükséges. A **neutrális elem az x függvény.**
- Az is látható, hogy **minden elemnek van inverze**, méghozzá minden elem önmaga inverze. Ez azt jelenti, hogy a neutrális elem kivételével a csoport minden eleme másodrend.
- Megmutatjuk, hogy **a mvelet asszociatív:**

A szükségesnél többet mutatunk meg, ti. azt, hogy bármely függvényhármassal esetén asszociatív a mvelet (feltéve természetesen, hogy képezhetők az összetett függvények) Megmutatjuk hogy

$$(h@(g@f)) = ((h@g)@f)$$

Képezzük elször a baloldalt, majd a jobboldalt.

[> **f:='f':g:='g':h:='h':**

[> **(h@(g@f))(x);**

[> **((h@g)@f)(x);**

A két kifejezés láthatóan azonos. Mindezek alapján kijelenthetjük, hogy a négy függvény csoportot alkot az összetett függvény képzésének mveletére nézve. A csoport izomorf a Klein-féle négyes csoporttal.

2. Feladat

Bizonyítsa be, hogy az $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{1}{1-x}$, $f_5(x) = \frac{x-1}{x}$,

$f_6(x) = \frac{x}{x-1}$ függvények halmaza csoportot alkot, ha mveletnek az összetett függvény képzését tekintjük.

Mutassuk meg, hogy a csoport minden elemének rendje osztója a csoport rendjének!

3. Példa

Tekintsük az $a + b\sqrt{3}$ alakú számok R halmazát, ahol a, b tetszleges egész számok.

(1) Bizonyítsuk be, hogy az R halmaz az összeadásra és a szorzásra nézve gyrt alkot.

(2) Mutassuk meg, hogy az $(R, +, \cdot)$ gyr izomorf az egész számokból képzett $\begin{bmatrix} a & b \\ 3 \cdot b & a \end{bmatrix}$ alakú

mátrixok $(M, +, \cdot)$ gyrjével, ahol az izomorfizmust az $a + b\sqrt{3} \rightarrow \begin{bmatrix} a & b \\ 3 \cdot b & a \end{bmatrix}$ leképezés valósítja

meg.

Megoldás

Mindenekeltt megmutatjuk, hogy az R halmaz az összeadás és a szorzás mveletére nézve zárt.

Az f függvény elállítja az R elemeit:

[> **f:=(x,y)->x+y*sqrt(3);**

[> **(f(a,b)+f(c,d));**

[> **expand(f(a,b)*f(c,d));**

Láthatóan a zártság mindkét mvelet esetén teljesül. Az összeadás és a szorzás mvelete a valós számok halmazából öröklően asszociatív. Az összeadás neutrális eleme a 0, a szorzásé az 1. Az $a + \sqrt{3} \cdot b$ elem additív (az összeadás mveletére vonatkozó) inverza a $-a - \sqrt{3} \cdot b$ elem. A disztibutivitás is teljesül, hiszen valós számokról van szó.

$A \varphi(a + \sqrt{3} \cdot b) = \begin{bmatrix} a & b \\ 3 \cdot b & a \end{bmatrix}$ leképezés [bijektív](#). Megmutatjuk hogy mindkét mveletre nézve mvelettartó is.

$$\varphi((a + \sqrt{3} \cdot b) + (c + \sqrt{3} \cdot d)) = \varphi((a + c) + \sqrt{3} \cdot (b + d)) = \begin{bmatrix} a + c & b + d \\ 3 \cdot (b + d) & a + c \end{bmatrix} =$$

$$\begin{bmatrix} a & b \\ 3 \cdot b & a \end{bmatrix} + \begin{bmatrix} c & d \\ 3 \cdot d & c \end{bmatrix} =$$

$$= \varphi(a + \sqrt{3} \cdot b) + \varphi(c + \sqrt{3} \cdot d)$$

$$\varphi((a + \sqrt{3} \cdot b) \cdot (c + \sqrt{3} \cdot d)) = \varphi((a \cdot c + 3 \cdot b \cdot d) + \sqrt{3} \cdot (a \cdot d + b \cdot c)) =$$

$$\begin{bmatrix} a \cdot c + 3 \cdot b \cdot d & a \cdot d + b \cdot c \\ 3 \cdot (a \cdot d + b \cdot c) & a \cdot c + 3 \cdot b \cdot d \end{bmatrix} = \begin{bmatrix} a & b \\ 3 \cdot b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 3 \cdot d & c \end{bmatrix} = \varphi(a + \sqrt{3} \cdot b) \cdot \varphi(c + \sqrt{3} \cdot d)$$

3. Feladat

Tekintsük az $a + \sqrt{2} \cdot b$ alakú számok halmazát, ahol az a és b tetszleges egész számok. Ezeket a számokat H -egészeknek nevezzük. Bizonyítsuk be, hogy a H -egészek halmaza az összeadásra és a szorzásra nézve integritási tartományt (kommutatív, nullosztómentes gyrt) alkot.

4. Feladat

A valós számok $\mathbb{R}$ halmazában értelmezzük az

$$x \circ y = x \cdot y + 5 \cdot x + 5 \cdot y + 20$$

képlettel megadott mveletet.

(1) Oldjuk meg az $x \circ y = x \circ 25$ egyenletet!

(2) Határozzuk meg az $\mathbb{R}$ halmaznak az a részhalmazát, amely $a \circ$ mveletre nézve csoportot alkot!

5. Feladat

Bizonyítsa be, hogy az (a, b) alakú, valós számokból képezett számpárok H halmaza gyrt alkot az alábbiak szerint:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d),$$

ahol

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

6. Feladat

A racionális számokból képzett (a, b) rendezett számpárok H halmazában $a \circ$ és $a *$ mveleteket az alábbiak szerint értelmezzük:

$$(a, b) \circ (c, d) = (a + c, b + d),$$

$$(a, b) * (c, d) = (a \cdot c, a \cdot d + b \cdot c).$$

Bizonyítsa be, hogy a H halmaz a fenti mveletekre nézve gyrt alkot!

7. Feladat

Mutassuk meg, hogy a mod 2 maradékosztályok az összeadás és a szorzás mveletére nézve testet alkotnak

4. Példa

Tekintsük az alábbi mátrixok M halmazát:

$$A0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, A1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, A2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, A3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, A4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, A5 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

1. Mutassuk meg, hogy az $(M, \cdot)$ struktúra csoportot alkot. (A mvelet a mátrix-szorzás);
2. Bizonyíts be, hogy az $(M, \cdot)$ csoport izomorf a 3-adfokú szimmetrikus csoporttal.

Megoldás

Adjuk meg a mátrixokat

```
> A|0:=matrix(3,3,[1,0,0,0,1,0,0,0,1]):A|1:=matrix(3,3,[1,0,0,0,0,1,0,1,0]):A|2:=matrix(3,3,[0,1,0,1,0,0,0,0,1]):A|3:=matrix(3,3,[0,0,1,1,0,0,0,1,0]):A|4:=matrix(3,3,[0,1,0,0,0,1,1,0,0]):A|5:=matrix(3,3,[0,0,1,0,1,0,1,0,0]):  
> H:=seq(A|i=evalm(A|i),i=0..5);
```

A mátrixok harmadrendek, s mindegyik mátrix mindegyik sorában és mindegyik oszlopában pontosan egy 1-es van, a többi elem pedig 0. Az ilyen mátrixokat permutáló mátrixoknak nevezzük. Figyeljük meg ugyanis, mi történik, ha a harmadrend K mátrixot először jobbról, majd balról megszorozzuk a vele kompatibilis permutáló mátrixok valamelyikével

```
> K:=matrix(3,3);K=evalm(K);  
> map(t->evalm(K&rhs(t)),H);  
> map(t->evalm(rhs(t)&K),H);
```

Észrevehetjük, hogy

- az A_0 -al való szorzáskor nem történt változás;
- minden más szorzáskor az els esetben rendre helyet változtattak bizonyos oszlopok, ill sorok az alábbiak szerint:

$$(2 \leftrightarrow 3; \quad 1 \leftrightarrow 2; \quad 1 \rightarrow 3, 3 \rightarrow 2, 2 \rightarrow 1; \quad 1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1; \quad 1 \leftrightarrow 3)$$

(a sorcseréknél a végrehajtódás és a felsorolás sorrendje nem mindenütt azonos)

Észrevehetjük továbbá, hogy M bármely két elemét szorozva egymással ismét M -beli elemet kapunk, tehát az M halmaz zárt a mátrix-szorzásra mint mveletre nézve. Egy példa:

```
> `A2*A3`:=evalm(A2&A3)=A1;
```

A mveleti tábla:

```
> Oszlop:=matrix(7,1,['&*',seq(`A`|i,i=0..5)]):  
> M:=matrix(7,6,[seq('A'|i,i=0..5),seq(seq(evalm(A|i&A|j),i=0..5),j=0..5)]):
```

```

> M1:=linalg[concat](0szlop,M):
> map(t->evalm(t),M1);
> P||1:=matrix(2,3,[1,2,3,1,2,3]):P||2:=matrix(2,3,[1,2,3,2,3,1])
:P||3:=matrix(2,3,[1,2,3,3,1,2]):P||4:=matrix(2,3,[1,2,3,1,3,2])
:P||5:=matrix(2,3,[1,2,3,3,2,1]):P||6:=matrix(2,3,[1,2,3,2,1,3]):

```

A táblázatból látható, hogy minen elem minden sorban és minden oszlopban pontosan egyszer lép föl. Az els sorban és az els oszlopban az elemek sorrendje megegyezik a 0. sorral ill. 0. oszloppal. Az egységelem az A_0 . Minden elemnek van inverze. A mvelet, mint általában a mátrixok szorzása asszociatív. Ezzel igazoltuk, hogy az $(M, \cdot)$ struktúra csoportot alkot.

Most térjünk rá a második részfeladat megoldására. Tekintsük mindenekeltt a harmadfokú szimmetrikus csoport elemeit:

```

> seq(P||i=evalm(P||i),i=1..6);

```

Látható, hogy az elemek egyszer, vagy ciklikus cseréjét tekintve a következ megfeleltetések (leképezések) létesíthetk:

$$A_0 \rightarrow P_1, A_1 \rightarrow P_4, A_2 \rightarrow P_6, A_3 \rightarrow P_2, A_4 \rightarrow P_3, A_5 \rightarrow P_5$$

Ez a bijektív leképezés mmvelettartó, hiszen pl.:

Az A_1 és az A_3 mátrixok szorzata az A_5 mátrix:

```

> evalm(A1*A3)=A5;

```

Az A_1 mátrix megfelelje a leképezés során a P_4 permutáció, az A_3 -é pedig a P_2 permutáció, s ezek szorzata (A második tényeznek megfelel permutációt hajtjuk végre elször)

```

> permszor(P2,P4)=P5;

```

Ez éppen az A_5 képe.

Egy másik példa:

```

> evalm(A||1*A||4)=A2;

```

Az A_1 mátrix megfelelje a leképezés során a P_4 permutáció, az A_4 -é pedig a P_3 permutáció, s ezek szorzata

```

> permszor(P3,P4)=P6;

```

```

>

```

Ez éppen az A_2 képe. Hasonlóan látható a mvelettartás a többi pár esetében is.

Ezzel igazoltuk, hogy a két csoport izomorf.

8. Feladat

Tekintsük a 3-adfokú szimmetrikus csoportnak azt a (ciklikus) részcsoportját, amelyet az

$$A := \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$$

halmaz elemei alkotnak.

Mutassuk meg, hogy a 4. Példában szerepl mátrixok $(M, \cdot)$ csoportjának van olyan részcsoportja, amely izomorf a

3-adfokú szimmetrikus csoport idézett részcsoportjával.

5. Példa

Csoport-e az $(\mathbb{R} \setminus \{0\} \times \mathbb{R}, \circ)$ algebrai struktúra, ha a $\circ$ mveletet a következőképpen értelmezzük
 $(a, b) \circ (c, d) = (a \cdot c, b \cdot c + d)$

Megoldás

1. A mvelet zárt, hiszen $a \neq 0$ és $b \neq 0$ miatt $a \cdot c \neq 0$.

```

> `type/par` := [anything, anything];
> a:='a':b:='b':c:='c':d:='d':e:='e':f:='f':
> muvelet:=proc(a::par,b::par)
  description "az eljárás kiszámítja az a+b-ab értékét";
  [a[1]*b[1],a[2]*b[1]+b[2]]
end:

```

Megmutatjuk, hogy a mvelet asszociatív: Elször képezzük az $((a, b) \circ (c, d)) \circ (e, f)$, majd az $(a, b) \circ ((c, d) \circ (e, f))$ kifejezést:

```

> muvelet(muvelet([a,b],[c,d]),[e,f]);
> muvelet([a,b],muvelet([c,d],[e,f]));

```

A két oldal láthatóan megegyezik. Határozzuk most meg a neutrális elemet!

```

> egyenlet:=muvelet([a,b],[c,d])=[a,b];
> assume(a<>0);assume(c<>0);about(a);
> solve({a*c=a,b*c+d=b},{c,d});

```

Tehát a struktúra neutrális eleme:

```

> e:=[1,0];

```

Keressük meg az $[a,b]$ elem inverzét!

```

> muvelet([a,b],[i1,i2])=e;
> solve({a*i1=1,b*i1+i2=0},{i1,i2});
> ab_inv:=[1/a,-b/a];

```

Mivel $a \neq 0$, minden elemnek van inverze.

```

> muvelet([a,b],ab_inv);#Képezzük az elem és inverzének
"szorzatát"!

```

Ezzel igazoltuk, hogy a szóbanforgó algebrai struktúra csoport. Vizsgáljuk meg, kommutatív-e a csoport!

```

> muvelet([a,b],[c,d])=muvelet([c,d],[a,b]);

```

A mvelet nem kommutatív, mert $b \cdot c + d \neq a \cdot d + b$. Például $d = 0$, $a = 1$, $b = c = 2$ esetén a baloldal értéke 4, míg a jobboldalé 2.