Algebra jegyzet államvizsga témákból

Babeş-Bolyai Tudományegyetem
Matematika és Informatika Kar
Magyar Matematika és Informatika Intézet

Andrei Marcus *Algebra* jegyzetéből és
Cosmin Pelea és Ioan Purdea *Algebra* példatárából összeállította Szántó Csaba

2013 Február

1 Csoportok, gyűrűk és testek

1.1 A csoport fogalma. Példák

Értelmezés 1.1 Legyen G egy halmaz és $\phi : G \times G \to G$ egy függvény.
a) Az (G, ϕ) elempárt *grupoidnak* nevezzük. Ha $x, y \in G$, akkor $\phi(x, y)$ helyett gyakran az

$$x + y,\ x \cdot y,\ x \circ y,\ x \cap y,\ x \cup y,\ x * y$$

stb. jelöléseket használjuk.
A „+" (illetve „·") jelölést *additív* (illetve *multiplikatív*) jelölésnek nevezzük.
b) $(G, *)$ *félcsoport*, ha „$*$" *asszociatív* művelet, azaz minden $x, y, z \in G$ esetén

$$(x * y) * z = x * (y * z).$$

c) $(G, *)$ *monoid*, ha „$*$" asszociatív művelet, és G-ben létezik *semleges elem*:

$$(\exists) e \in G\ (\forall) x \in G\ x * e = e * x = x.$$

Additív (illetve multiplikatív) jelölés esetén e-t 0-val (illetve 1-gyel) szoktuk jelölni.
d) $(G, *)$ *csoport*, ha $(G, *)$ monoid és minden eleme *szimmetrizálható (invertálható)*:

$$(\forall) x \in G\ (\exists) x' \in G\ x * x' = x' * x = e.$$

Additív (illetve multiplikatív) jelölés esetén x'-et $-x$-el (illetve x^{-1}-gyel) jelöljük.
e) Azt mondjuk, hogy az $(G, *)$ csoport *kommutatív* vagy *Abel-csoport*, ha minden $x, y \in G$ esetén, $x * y = y * x$.
f) Az $|G|$ kardinális számot az $(G, *)$ csoport *rend*jének nevezzük.

Lemma 1.2 *Legyen $(M, \cdot)$ egy monoid.*
a) *Ha $e, e' \in M$ semleges elemek, akkor $e = e'$.*
b) *Ha $x \in M$ és $x', x'' \in M$ x-nek inverzei, akkor $x' = x''$.*
c) *Legyen $U(M) = \{x \in M \mid x \text{ invertálható}\}$ az M egységeinek a halmaza. Akkor $(U(M), \cdot)$ csoport.*

Bizonyítás. a) $e = ee' = e'$.
b) $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$.
c) Az M semleges eleme invertálható, mert $ee = e$. Ha $x \in U(M)$, akkor $x' \in U(M)$ és $(x')' = x$, mert $x'x = xx' = e$. Ha $x, y \in U(M)$, akkor

$$(xy)(y'x') = (y'x')(xy) = e,$$

tehát $xy \in U(M)$ és $(xy)' = y'x'$. Az asszociativitás öröklődik. ■

Példa 1.3 a) $(\mathbb{N}^*, +)$ félcsoport, $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ monoidok, nem csoportok.
b) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ Abel-csoportok.
c) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ kommutatív monoidok, $(U(\mathbb{Z}) = \{1, -1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ Abel-csoportok.

Példa 1.4 Legyen M egy halmaz és $\mathcal{F}(M) = \{f \mid f : M \to M\}$. Akkor $(\mathcal{F}(M), \circ)$ monoid. Az

$$S_M := U(\mathcal{F}(M)) = \{f \in \mathcal{F}(M) \mid f \text{ bijektív}\}$$

csoportot az M halmaz *szimmetrikus-csoport*jának nevezzük.

Feladat 1 Legyen $M = \mathbb{R} \setminus \{0, 1\}$, $G = \{f_i \mid i = 1, \dots, 6\}$, ahol $f_i : M \to M$,

$$f_1(t) = t,\quad f_2(t) = \frac{1}{1-t},\quad f_3(t) = \frac{t-1}{t},\quad f_4(t) = \frac{1}{t},$$

$$f_5(t) = 1 - t,\quad f_6(t) = \frac{t}{t-1},\quad (\forall) t \in M.$$

Igazoljuk, hogy $(G, \circ)$ nemkommutatív csoport (készítsünk művelettáblát).

Feladat 2 (Csoportok direkt szorzata) Legyen G_1 és G_2 két csoport, és legyen

$$G := G_1 \times G_2 = \{g = (g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}.$$

Értelmezés szerint, legyen

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Akkor G csoport.

Megjegyzés 1.5 (Számítási szabályok) a) Legyen $(G,\cdot)$ egy csoport és $a,b \in G$. Az $ax = b$ egyenlet egyetlen megoldása $x = a^{-1}b$, és az $ya = b$ egyenlet egyetlen megoldása $y = ba^{-1}$; következik, hogy a

$$t_a : G \to G, \quad t_a(x) = ax$$

és

$$t'_a : G \to G, \quad t'_a(x) = xa$$

bijektív függvények (ezeket *bal oldali* illetve *jobb oldali transzlációnak* nevezzük). Ha $x,y \in G$, akkor $ax = ay \Rightarrow x = y$ és $xa = ya \Rightarrow x = y$.

b) (*Hatványozás*) Legyen $(G,\cdot)$ egy csoport, $x \in G$ és $n \in \mathbb{N}^*$. A „$\cdot$” asszociatívitását felhasználva, értelmezzük az x^n-et:

$$x^1 = x, \quad x^{n+1} = x^n \cdot x = x \cdot x^n.$$

Továbbá, legyen $x^0 = e$ és $(x^{-1})^n = (x^n)^{-1}$.

Feladat 3 Igazoljuk, hogy $x^{n+m} = x^n x^m$ és $(x^n)^m = x^{mn}$ minden $x \in G$ és $m,n \in \mathbb{Z}$ esetén.

Ha a $(G,+)$ additív jelölést alkalmazzuk, akkor legyen $1\cdot x = x$, $(n+1)x = nx+x = x+nx$, $0\cdot x = 0$, $(-n)x = -(nx) = n(-x)$. Ebben az esetben, $(m+n)x = mx+nx$ és $m(nx) = (mn)x$ minden $m,n \in \mathbb{Z}$ esetén.

Feladat 4 Legyen $(G,\cdot)$ egy félcsoport. Igazoljuk, hogy G csoport akkor és csak akkor, ha:
a) $(\exists)e \in G$ úgy, hogy $(\forall)x \in G$ $xe = x$.
b) $(\forall)x \in G$ $(\exists)x' \in G$ úgy, hogy $xx' = e$.

Feladat 5 Legyen $(G,\cdot)$ egy nemüres félcsoport, és $t_a, t'_a : G \to G$, $t_a(x) = ax$, $t'_a(x) = xa$, ahol $a \in G$. Bizonyítsuk be, hogy:
a) G csoport $\Leftrightarrow t_a, t'_a$ szürjektívek, $(\forall)a \in G$.
b) Ha G véges, akkor G akkor és csak akkor csoport, ha $(\forall)a,x,y \in G$ $ax = ay \Rightarrow x = y$ és $xa = ya \Rightarrow x = y$.

Feladat 6 Legyen $(G,\cdot)$ egy csoport és $x,y \in G$. Igazoljuk, hogy:
a) $x^2 = y^6 = e$, $xy = y^4x \Rightarrow y^3 = e$, $xy = yx$.
b) $x^5 = y^4 = e$, $xy = yx^3 \Rightarrow x^2y = yx$, $xy^3 = y^3x^2$.
c) $x^3 = y^4 = e$, $yx = xy^3 \Rightarrow xy = yx$.

Feladat 7 Legyen $(G,\cdot)$ egy csoport és $x,y \in G$. Igazoljuk, hogy :
a) Ha $xy = yx$, akkor $x^m y^n = y^n x^m$ és $(xy)^n = x^n y^n$ $(\forall)m,n \in \mathbb{Z}$.
b) Ha $n \in \mathbb{Z}$ és $(xy)^k = x^k y^k$, ahol $k = n-1, n, n+1$, akkor $xy = yx$.

1.2 Csoportmorfizmusok

Értelmezés 1.6 Legyen $(G,*)$ és $(G',\circ)$ két csoport és $f : G \to G'$ egy függvény,
a) Azt mondjuk, hogy f *csoportmorfizmus*, ha minden $x,y \in G$ esetén

$$f(x * y) = f(x) \circ f(y).$$

Az f-et *endomorfizmusnak* nevezzük, ha $(G,*) = (G',\circ)$.
b) Azt mondjuk, hogy f *izomorfizmus*, ha létezik egy $f' : G' \to G$ morfizmus úgy, hogy $f' \circ f = 1_G$ és $f \circ f' = 1_{G'}$. Az f izomorfizmust *automorfizmusnak* nevezzük, ha $(G,*) = (G,\circ)$.
Jelölések: $\mathrm{End}(G)$ – az endomorfizmusok halmaza, $\mathrm{Aut}(G)$ – az automorfizmusok halmaza.

Lemma 1.7 *Legyen $f : G \to G'$ és $f' : G' \to G''$ két morfizmus.*
a) $f(e) = e'$;
b) $f(x^{-1}) = f(x)^{-1}$ *minden $x \in G$ esetén.*
c) $1_G : G \to G$ *és* $f' \circ f : G \to G''$ *morfizmusok.*
d) f *akkor és csak akkor izomorfizmus, ha bijektív.*

Bizonyítás. a) $e'f(e) = f(e) = f(ee) = f(e)f(e)$, tehát $f(e) = e'$.
b) Ha $x \in G$, akkor $xx^{-1} = x^{-1}x = e$, tehát $f(x)f(x^{-1}) = f(x^{-1})f(x) = e'$, és következik, hogy $f(x)^{-1} = f(x^{-1})$.
c) Minden $x,y \in G$ esetén $1_G(x,y) = xy = 1_G(x)1_G(y)$ és

$$(f' \circ f)(xy) = f'(f(xy)) = f'(f(x)f(y)) = f'(f(x))f'(f(y)) = (f' \circ f)(x)(f' \circ f)(y).$$

d) Ha f izomorfizmus, akkor bijektív, mert van inverze. Fordítva, feltételezzük, hogy f bijektív, és igazoljuk, hogy f^{-1} izomorfizmus. Legyen $u,v \in G'$, $x = f^{-1}(u)$ és $y = f^{-1}(v)$. Ekkor

$$f^{-1}(uv) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v). \quad \blacksquare$$

Feladat 8 Ha $a \in \mathbb{R}_+^* \setminus \{1\}$, és $f : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$, $f(x) = a^x$, akkor f izomorfizmus, és $f^{-1}(x) = \log_a(x)$.

Feladat 9 A $p_i : G_1 \times G_2 \to G_i$, $p_i(x_1, x_2) = x_i$ *kanonikus projekciók* szürjektív morfizmusok, $i = 1, 2$.

Feladat 10 Ha $(G, \cdot)$ egy csoport, akkor $(\mathrm{End}(G), \circ)$ monoid, és $U(\mathrm{End}(G)) = \mathrm{Aut}(G)$ (tehát $(\mathrm{Aut}(G), \circ)$ csoport).

Feladat 11 (Lorenz-csoport) Legyen $a > 0$, $G = (-a, a)$ és $x * y = \frac{x+y}{1+xy/a^2}$. Igazoljuk, hogy:
a) $(G, *)$ Abel-csoport;
b) létezik egy $f : (\mathbb{R}_+^*, \cdot) \to (G, *)$, $f(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ alakú izomorfizmus.

Feladat 12 Legyen M egy halmaz és $(G, \cdot)$ egy csoport. A $G^M = \{f \mid f : M \to G\}$ halmazon értelmezzük a következő műveletet: $(fg)(x) = f(x)g(x)$, $(\forall)x \in M$, $f, g \in G^M$. Igazoljuk, hogy $(G^M, \cdot)$ csoport, és létezik egy $\phi : G \to G^M$ injektív morfizmus.

Feladat 13 Legyen $(G, \cdot)$ egy csoport és $f, g : G \to G$, $f(x) = x^{-1}$, $g(x) = x^2$. A következő állítások ekvivalensek:
(i) G Abel-csoport.
(ii) $f \in \mathrm{Aut}(G)$.
(iii) $g \in \mathrm{End}(G)$.

Feladat 14 Legyen $(G, \cdot)$ egy csoport, és $i_g : G \to G$, $i_g(x) = gxg^{-1}$, ahol $g \in G$. Igazoljuk, hogy $i_g \in \mathrm{Aut}(G)$. (i_g-t *belső automorfizmus*nak nevezzük. Jelölés: $\mathrm{Int}(G) = \{i_g \mid g \in G\}$).

Feladat 15 Legyen M és N két halmaz és $f : M \to N$ egy bijektív függvény. Igazoljuk, hogy $(S_M, \circ) \simeq (S_N, \circ)$.

1.3 Részcsoportok

Értelmezés 1.8 Legyen $(G, \cdot)$ egy csoport és H egy részhalmaza G-nek. Azt mondjuk, hogy H *részcsoport*ja G-nek (jelölés: $H \leq (G, \cdot)$), ha H zárt a műveletre nézve (azaz minden $x, y \in H$ esetén $xy \in H$-nak) és $(H, \cdot)$ csoportot alkot a „$\cdot$” által indukált művelettel.

Tétel 1.9 (részcsoport jellemzése) *Legyen $(G, \cdot)$ egy csoport és H részhalmaza G-nek. A következő állítások ekvivalensek:*
1) *H részcsoportja G-nek.*
2) *$H \neq \emptyset$ és $xy, x^{-1} \in H$ minden $x, y \in H$ esetén.*
3) *$H \neq \emptyset$ és $xy^{-1} \in H$ minden $x, y \in H$ esetén.*

Bizonyítás. (1)$\Longrightarrow$(2) Mivel $(H, \cdot)$ csoport következik, hogy van egy e' semleges eleme. Ha e a G semleges eleme, akkor $e'e' = e' = e'e$, vagyis $e = e' \in H$.

Minden $x \in H$ esetén létezik $x' \in H$ úgy, hogy $xx' = x'x = e$, és létezik $x^{-1} \in G$ úgy, hogy $xx^{-1} = x^{-1}x = e$. Az inverz elem egyértelműségéből következik, hogy $x' = x^{-1} \in H$.

(2)$\Longrightarrow$(3) Ha $x, y \in H$, akkor $x, y^{-1} \in H$ és $xy^{-1} \in H$.

(3)$\Longrightarrow$(1) Feltevés szerint $H \neq \emptyset$; ha $x \in H$, akkor $e = xx^{-1} \in H$ és $ex^{-1} = x^{-1} \in H$ Ha $x, y \in H$, akkor $x, y^{-1} \in H$ és $x(y^{-1})^{-1} \in H$, vagyis $xy \in H$.

Ezzel igazoltuk, hogy H zárt a műveletre nézve, H-ban létezik semleges elem, és H minden elemének van inverze. Mivel az indukált művelet asszociativitása öröklődik, a fentiekből következik, hogy $(H, \cdot)$ csoport és a G részcsoportja. ■

Példa 1.10 1) $\mathbb{Z}$ részcsoportja $(\mathbb{Q}, +)$-nak, $\mathbb{Q}$ részcsoportja $(\mathbb{R}, +)$-nak és $\mathbb{R}$ részcsoportja $(\mathbb{C}, +)$-nak.
2) $(\mathbb{Q}^*, \cdot)$ részcsoportja $(\mathbb{R}^*, \cdot)$-nak és $(\mathbb{R}^*, \cdot)$ részcsoportja $(\mathbb{C}^*, \cdot)$-nak.
3) $n\mathbb{Z}$ részcsoportja $(\mathbb{Z}, +)$-nak, ahol $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ és $n \in \mathbb{Z}$ rögzített.
4) $\{e\}$ és a G részcsoportjai $(G, \cdot)$-nak, ezeket a G csoport *triviális részcsoportjainak* nevezzük. Ha $H \leq G$ és $H \neq \{e\}$, $H \neq G$, akkor H-t *valódi részcsoportnak* nevezzük.
5) $(U_n, \cdot)$ részcsoportja $(\mathbb{C}^*, \cdot)$-nak, ahol $n \in \mathbb{N}^*$-nak és

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid 0 \leq k \leq n-1,\ k \in \mathbb{Z}\}$$

az n-*ed rendű egységgyökök* halmaza.
6) Legyen $(G, \cdot)$ egy csoport, és

$$Z(G) = \{g \in G \mid gx = xg \ \ \forall x \in G\}$$

a G *centruma*. Akkor $Z(G)$ részcsoportja G-nek.

Vegyük észre, hogy G akkor és csak akkor kommutatív csoport, ha $Z(G) = G$.

Lemma 1.11 *Legyen* $f : G \longrightarrow G'$ *egy csoportmorfizmus.*
1) *Ha* H *részcsoportja* G*-nek, akkor* $f(H)$ *részcsoportja* G'*-nek.*
2) *Ha* H' *részcsoportja* G'*-nek, akkor* $f^{-1}(H)$ *részcsoportja* G*-nek.*

Bizonyítás. 1) Mivel $H \neq \emptyset$ következik, hogy $f(H) \neq \emptyset$.

Ha $x', y' \in f(H)$, akkor létezik $x, y \in H$ úgy, hogy $x' = f(x)$ és $y' = f(y)$, tehát $x'y' = f(x)f(y)$. Mivel f morfizmus $f(x)f(y) = f(xy)$, ahol $xy \in H$-nak (mert H részcsoport), tehát $x'y' = f(xy) \in f(H)$.

Továbbá, $(x')^{-1} = f(x)^{-1} = f(x^{-1})$ (mert f morfizmus), de $x^{-1} \in H$ (mert H csoport), tehát $f(x^{-1}) \in f(H)$. A részcsoportok jellemzési tételéből következik, hogy $f(H)$ részcsoportja G'-nek.

2) Mivel H' részcsoportja G'-nek és f morfizmus, fennáll az, hogy $f(e) = e'$, (ahol e a G semleges eleme és e' a G' semleges eleme); következik, hogy $e \in f^{-1}(e')$, vagyis $f^{-1}(H') \neq \emptyset$.

Ha $x, y \in f^{-1}(H')$, vagyis $f(x), f(y) \in H'$, akkor $f(x)f^{-1}(y) = f(x)f(y^{-1}) = f(xy^{-1}) \in H'$, vagyis $xy^{-1} \in f^{-1}(H')$. ■

Értelmezés 1.12 Legyen $f : G \longrightarrow G'$ egy morfizmus.
1) Az $\operatorname{Im} f = f(G) = \{f(x) \mid x \in G\}$ halmazt az f *kép*ének nevezzük.
2) A $\operatorname{Ker} f = \{x \in G \mid f(x) = e'\} = f^{-1}(e')$ halmazt az f *mag*jának nevezzük.

Megjegyzés 1.13 1) A fenti lemmából következik, hogy $\operatorname{Ker} f \leq G$ és $\operatorname{Im} f \leq G'$.

2) Ha H részcsoportja G-nek és $i : H \longrightarrow G$, $i(h) = h$, akkor i injektív morfizmus.

Fordítva, ha $f : G \longrightarrow G'$ injektív morfizmus, akkor $f(G) = \operatorname{Im} f$ részcsoportja G'-nek és $H \simeq f(H)$. Egy injektív morfizmust *beágyazás*nak is nevezünk.

Tétel 1.14 (Injektív morfizmusok jellemzése) *Az* $f : G \longrightarrow G'$ *morfizmus akkor és csak akkor injektív, ha* $\operatorname{Ker} f = \{e\}$.

Bizonyítás. Feltételezzük, hogy f injektív és legyen $x \in \operatorname{Ker} f$, vagyis $f(x) = e' = f(e)$; következik, hogy $x = e$, tehát $\operatorname{Ker} f = \{e\}$.

Fordítva, feltételezzük, hogy $\operatorname{Ker} f = \{e\}$. Legyen $x_1, x_2 \in G$ úgy, hogy $f(x_1) = f(x_2)$. Ekkor $f(x_1)f^{-1}(x_2) = e'$, és mivel f morfizmus $f(x_1x_2^{-1}) = e'$, vagyis $x_1x_2^{-1} \in \operatorname{Ker} f = \{e\}$; következik, hogy $x_1x_2^{-1} = e$ tehát $x_1 = ex_2 = x_2$. ■

Tétel 1.15 (Cayley) *Minden csoport beágyazható egy szimmetrikus csoportba.*

Bizonyítás. Legyen $(G, \cdot)$ egy csoport, $a \in G$ és $t_a : G \longrightarrow G$, $t_a(x) = ax$ (t_a a bal oldali transzláció). Mivel t_a bijektív függvény, következik, hogy $t_a \in S_G := \{f : G \to G \mid f \text{ bijektív}\}$.

Legyen $\varphi : G \longrightarrow S_G$ úgy, hogy $\varphi(a) = t_a$ és igazoljuk, hogy φ injektív morfizmus. Valóban, $\varphi(ab) = t_{ab}$ és $\varphi(a) \circ \varphi(b) = t_a \circ t_b$, és minden $x \in G$ esetén

$$t_{ab}(x) = (ab)x = a(bx) = t_a(bx) = t_a(t_b(x)) = (t_a \circ t_b)(x). \tag{1}$$

Továbbá, legyen $a, b \in G$ úgy, hogy $\varphi(a) = \varphi(b)$, vagyis $t_a = t_b$. Ez azt jelenti, hogy $t_a(x) = t_b(x)$ minden $x \in G$ esetén, tehát $ax = bx$ és $a = b$, vagyis φ injektív. ■

Feladat 16 Legyen $(G, \cdot)$ egy csoport és $H_1, H_2, H_3 \leq G$. Igazoljuk, hogy:
a) $H_1 \cup H_2$ akkor és csak akkor részcsoport, ha $H_1 \leq H_2$ vagy $H_2 \leq H_1$.
b) $H_1 \cup H_2 = G$ akkor és csak akkor, ha $H_1 = G$ vagy $H_2 = G$.
c) $H_3 \subseteq H_1 \cup H_2$ akkor és csak akkor, ha $H_3 \leq H_1$ vagy $H_3 \leq H_2$.

Feladat 17 Legyen $(A, +)$ egy Abel-csoport, $mA = \{ma \mid a \in A\}$ és $A_m = \{a \in A \mid ma = 0\}$, ahol $m \in \mathbb{Z}$. Bizonyítsuk be, hogy:
a) $mA,\ A_m \leq (A, +)$.
b) Ha $f : (A, +) \to (B, +)$ egy morfizmus, akkor $f(mA) \subseteq mB$ és $f(A_m) \subseteq B_m$.
c) Legyen $G = (S_3, \circ)$. Igazoljuk, hogy G^3 és G_2 nem részcsoportok.

Feladat 18 Legyen $(G, \cdot)$ egy csoport és $H \subseteq G$ egy véges nemüres részhalmaz. Igazoljuk, hogy $H \leq G$ akkor és csak akkor, ha H zárt részhalmaza G-nek.

Feladat 19 Legyen $(G, \cdot)$ egy csoport és $Z(G) = \{x \in G \mid xg = gx\ (\forall) g \in G\}$ a G *centruma*.
a) Bizonyítsuk be, hogy $Z(G) \leq G$.
b) Ha $f : G \to G'$ egy izomorfizmus, akkor $f(Z(G)) = Z(G')$.

1.4 Az S_n szimmetrikus csoport

Legyen $S_n = S_{\{1,\dots,n\}} = \{f : \{1,\dots,n\} \to \{1,\dots,n\} \mid f \text{ bijektív}\}$. Az $(S_n, \circ)$ csoportot n-*ed fokú szimmetrikus csoport*nak nevezzük. Egy $\sigma \in S_n$ elemet n-ed fokú *permutáció*nak nevezzük, és gyakran egy táblázat segítségével adjuk meg:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

(e-t az *identikus permutáció*nak nevezzük.) Ha $\sigma, \tau \in S_n$, akkor

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix},$$

és

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Matematikai indukcióval könnyen igazolható, hogy $|S_n| = n!$.

Értelmezés 1.16 Legyen $\sigma \in S_n$.

a) Az (i, j) elempárt *inverzió*nak nevezzük, ha $1 \le i < j \le n$ és $\sigma(i) > \sigma(j)$; $\mathrm{inv}(\sigma)$-val jelöljük a σ inverzióinak a számát.

b) $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)} \in \{1, -1\}$ a σ *szignatúrája*; σ *páros* permutáció, ha $\mathrm{sgn}(\sigma) = 1$, és σ *páratlan* permutáció, ha $\mathrm{sgn}(\sigma) = -1$.

A páros permutációk halmazát A_n-nel jelöljük.

Feladat 20 a) Minden $\sigma \in S_n$ esetén, $0 \le \mathrm{inv}(\sigma) \le \frac{n(n-1)}{2}$.

b) $\mathrm{inv}(\sigma) = 0 \Leftrightarrow \sigma = e$; $\mathrm{inv}(\sigma) = \frac{n(n-1)}{2} \Leftrightarrow \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$.;

c) Ha $n \ge 2$ és $1 \le j < k \le n$, legyen $\tau_{jk} \in S_n$,

$$\tau_{jk}(i) = \begin{cases} k, & i = j \\ j, & i = k \\ i, & i \ne j, k \end{cases}.$$

Akkor $\mathrm{inv}(\tau_{jk}) = 2(k-j) - 1$ és $\mathrm{sgn}(\tau_{jk}) = -1$. ($\tau_{jk}$-t *transzpozíció*nak nevezzük).

Feladat 21 Legyen $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ és $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. Határozzuk meg az $\mathrm{inv}(\sigma)$-t, $\mathrm{sgn}(\sigma)$-t, σ^{-1}-t, $\sigma\tau$-t, $\tau\sigma$-t és σ^{1457}-t!

Feladat 22 Írjuk fel az összes 3-ad és 4-ed fokú transzpozíciókat.

Feladat 23 Számítsuk ki $\mathrm{inv}(\sigma)$-t ha:

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n & n+1 & n+2 & \dots & 2n \\ 1 & 3 & 5 & 7 & \dots & 2n-1 & 2 & 4 & \dots & 2n \end{pmatrix}$

b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & n+3 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & 5 & \dots & 2n-1 \end{pmatrix}$

Tétel 1.17 a) *Minden $\sigma \in S_n$ esetén,*

$$\mathrm{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

b) $\mathrm{sgn} : (S_n, \circ) \to (\{1, -1\}, \cdot)$ *szürjektív morfizmus.*

c) $(A_n, \circ)$ *csoport és* $|A_n| = \frac{n!}{2}$. (A_n-*et alternáló csoportnak nevezzük*).

Bizonyítás. a) Mivel σ bijektív függvény, minden $i, j \in \{1,\dots,n\}$ esetén léteznek az egyértelműen meghatározott $k, l \in \{1,\dots,n\}$ elemek, $k \ne l$, úgy, hogy $\sigma(k) = i$ és $\sigma(l) = j$; továbbá, $k > l$ pontosan akkor ha (i, j) σ-nak egy inverziója. Következik, hogy a $\prod_{1 \le i < j \le n} \frac{\sigma(j)-\sigma(i)}{j-i}$ szorzatban, az egyszerűsítések után, a (-1)-gyel egyenlő tényezők száma $\mathrm{inv}(\sigma)$.

b) Mivel $\mathrm{sgn}(e) = 1$, és ha τ_{ij} egy transzpozíció, akkor $\mathrm{sgn}(\tau) = -1$, következik, hogy sgn szürjektív.

Legyen $\sigma, \tau \in S_n$. Mivel τ bijektív, minden $i, j \in \{1, \dots, n\}$ esetén léteznek az egyértelműen meghatározott $k, l \in \{1, \dots, n\}$ elemek, $k \neq l$, úgy, hogy $\tau(k) = i$ és $\tau(l) = j$. Ekkor

$$\begin{aligned}\operatorname{sgn}(\sigma\tau) &= \prod_{1 \le i < j \le n} \frac{(\sigma\tau)(j) - (\sigma\tau)(i)}{j - i} = \prod_{1 \le i < j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{1 \le i < j \le n} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).\end{aligned}$$

c) Vegyük észre, hogy $A_n = \operatorname{Ker}(\operatorname{sgn})$, tehát A_n részcsoport.

Legyen $\tau \in S_n$ egy transzpozíció. Mivel S_n csoport és sgn csoportmorfizmus, $\phi : A_n \to S_n \setminus A_n$, $\phi(\sigma) = \sigma\tau$ jólértelmezett bijektív függvény; következik, hogy $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$. ■

1.5 Lagrange tétele

Értelmezés 1.18 Legyen $(G, \cdot)$ egy csoport és H részcsoportja G-nek. Értelmezzünk G-n két relációt:
$x \rho_H y \iff x^{-1}y \in H$ a H szerinti *bal oldali kongruencia*, és
$x \rho'_H y \iff xy^{-1} \in H$ a H szerinti *jobb oldali kongruencia* reláció.

Lemma 1.19 1) ρ_H *és* ρ'_H *ekvivalenciarelációk* G*-n.*
2) *Ha* $G/\rho_H = \{\rho_H\langle x\rangle \mid x \in G\}$ *és* $G/\rho'_H = \{\rho'_H\langle x\rangle \mid x \in G\}$*, akkor*

$$\rho_H\langle x\rangle = xH = \{xh \mid h \in H\}$$

x-nek H szerinti bal oldali mellékosztálya *és*

$$\rho'_H\langle x\rangle = Hx = \{hx \mid h \in H\}$$

x-nek H szerinti jobb oldali mellékosztálya.

Bizonyítás. 1) Igazoljuk, hogy ρ_H reflexív, tranzitív és szimmetrikus. Reflexivitás: $x\rho_H x$ minden $x \in G$ esetén, mert $x^{-1}x = e \in H$. Tranzitivitás: ha $x\rho_H y$ és $y\rho_H z$, akkor értelmezés szerint $x^{-1}y \in H$ és $y^{-1}z \in H$, tehát $(x^{-1}y)(y^{-1}z) \in H$, vagyis $x^{-1}z \in H$ és $x\rho_H z$. Szimmetria: ha $x\rho_H y$, akkor $x^{-1}y \in H$, tehát $(x^{-1}y)^{-1} = y^{-1}x \in H$, azaz $y\rho_H x$.

Azt, hogy ρ'_H ekvivalencia reláció hasonlóan igazoljuk.

2) Igazoljuk, hogy $\rho_H\langle x\rangle = xH$. Értelmezés szerint

$$\rho_H\langle x\rangle = \{y \in G \mid x\rho_H y\} = \{y \in G \mid x^{-1}y \in H\}.$$

Legyen $y \in \rho_H\langle x\rangle$; ekkor $h = x^{-1}y \in H$, tehát $y = xh \in xH$.

Fordítva, ha $y = xh \in xH$, akkor $x^{-1}y = h \in H$; következik, hogy $x\rho_H y$, azaz $y \in \rho_H\langle x\rangle$.

Az $\rho'_H\langle x\rangle = Hx$ egyenlőség igazolása hasonló módon történik. ■

Tétel 1.20 (Lagrange-tétel) *Legyen* G *egy csoport és* $H \le G$ *egy részcsoport.*
1) *Fennáll, hogy* $|xH| = |Hx| = |H|$ *minden* $x \in G$ *esetén, vagyis minden osztályban ugyanannyi elem van.*
2) *Ha* $G/H = \{xH \mid x \in G\}$ *és* $H\backslash G = \{Hx \mid x \in G\}$*, akkor* $|G/H| = |H\backslash G|$.
(Jelölés: $[G : H] = |G/H| = |H\backslash G|$; ezt a kardinális számot a H részcsoport G-beli *indexének* nevezzük.)
3) $|G| = |H| \cdot [G : H]$*. Partikulárisan, ha* G *véges, akkor minden részcsoport rendje osztja a csoport rendjét.*
4) *Ha* H, K *részcsoportjai* G*-nek és* $K \subseteq H$*, akkor*

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

Bizonyítás. 1) Legyen $f : H \to xH$, $f(h) = xh$. Értelmezés szerint f szürjektív függvény, de injektív is (mert csoportban lehet egyszerűsíteni), tehát f bijektív függvény, ezért $|H| = |xH|$.

Hasonlóan $f' : H \longrightarrow Hx$, $f'(h) = hx$ bijektív függvény, tehát $|H| = |Hx|$.

2) Legyen $\varphi : G/H \longrightarrow H\backslash G$, $\varphi(xH) = Hx^{-1}$. Igazoljuk, hogy φ jól értelmezett: legyen $x' \in xH$, vagyis $x' = xh$ (ez azt is jelenti, hogy $xH = x'H$). Akkor

$$\varphi(x'H) = H(x')^{-1} = H(xh)^{-1} = H(h^{-1}x^{-1}) = Hx^{-1}.$$

Legyen $\psi : H\backslash G \longrightarrow G/H$, $\psi(Hx) = x^{-1}H$. Az előbbihez hasonlóan igazoljuk, hogy ψ jól értelmezett függvény.

Mivel

$$(\psi \circ \varphi)(xH) = \psi(\varphi(xH)) = \psi(Hx^{-1}) = (x^{-1})^{-1}H = xH$$

és

$$(\varphi \circ \psi)(Hx) = \varphi(\psi(Hx)) = \varphi(x^{-1}H) = H(x^{-1})^{-1} = Hx$$

következik, hogy $\psi = \varphi^{-1}$ és φ bijektív függvény, tehát $|G/H| = |H/G|$.

3) Létezik egy I halmaz és léteznek az $x_i \in G$ elemek, $i \in I$, úgy, hogy $G/H = \{x_iH \mid i \in I\}$ és $|I| = [G : H] = |G/H|$. Azt mondjuk, hogy $\{x_i \mid i \in I\} \subseteq G$ a G/H faktorhalmaznak egy *teljes reprezentáns rendszere* (vagyis $G = \bigcup_{i\in I} x_iH$ és, ha $i \neq j$, akkor $x_iH \cap x_jH = \emptyset$).

A fentiek alapján $|G| = \sum_{i\in I} |x_iH| = \sum_{i\in I} |H| = |I| \cdot |H| = [G : H] \cdot |H|$.

d) (Ez a pont tulajdonképpen a c)-pont általánositása.) Legyen $\{x_i \mid i \in I\}$ G/H-nak egy teljes reprezentáns rendszere, tehát $|I| = [G : H]$, és legyen $\{y_i \mid j \in J\}$ a H/K-nak egy teljes reprezentáns rendszere, tehát $|J| = [H : K]$.

Elég igazolni, hogy $\{x_iy_j \mid (i, j) \in I \times J\}$ G/K-nak egy teljes reprezentáns rendszere (mert akkor $|G/K| = [G : K] = |I \times J| = |I| \cdot |J| = [G : H][H : K]$).

Ahhoz, hogy $\{x_iy_j \mid (i, j) \in I \times J\}$ G/K-nak egy teljes reprezentáns rendszere legyen, az egyesítésnek fednie kell G-t és két különböző osztálynak diszjunktnak kell lennie. Valóban,

$$\bigcup_{(i,j)\in I\times J} x_iy_jK = \bigcup_{i\in I}\bigcup_{j\in J} x_iy_jK = \bigcup_{i\in I}\bigcup_{j\in J} t_{x_i}(y_jK) = \bigcup_{i\in I} t_{x_i}(\bigcup_{j\in J} y_jK) =$$

$$= \bigcup_{i\in I} t_{x_i}(H) = \bigcup_{i\in I} x_iH = G;$$

továbbá, igazoljuk, hogy ha $(i_1, j_1) \neq (i_2, j_2)$, akkor $x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K = \emptyset$. Feltételezzük, hogy $i_1 \neq i_2$, akkor $x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K \subseteq x_{i_1}H \cap x_{i_2}H = \emptyset$. Ha $i_1 = i_2 = i$, akkor $j_1 \neq j_2$, és

$$x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K = t_{x_i}(y_{j_1}K) \cap t_{x_i}(y_{j_2}K) = t_{x_i}(y_{j_1}K \cap y_{j_2}K) = t_{x_i}(\emptyset) = \emptyset$$

(felhasználtuk azt, hogy a t_x transzláció injektív). ■

1.6 Megoldott feladatok

1) Legyen M egy halmaz, $\mathcal{P}(M)$ az M részhalmazainak halmaza és jelölje $\triangle$ a halmazok szimmetrikus különbségét, vagyis minden $X, Y \subseteq M$-re $X\triangle Y = (X \setminus Y) \cup (Y \setminus X)$. Bizonyítsuk be, hogy $(\mathcal{P}(M), \triangle)$ csoport.

Megoldás: Legyen $C(X) = C_MX = M \setminus X$ ax $X \subseteq M$ részhalmaz komplemetuma. Felírható a következő egyenlőség:

$$X\triangle Y = [X \cap C(Y)] \cup [Y \cap C(X)]. \tag{1}$$

A $\triangle$ művelet asszociativitásának ellenőrzéséhez szükségünk lesz a következő azonosságra is:

$$C(X\triangle Y) = (X \cap Y) \cup [C(X) \cap C(Y)] \tag{2}$$

amit az (1) egyenlőségből vezethetünk le a de Morgan-azonosságok segítségével, használva azt, hogy a hamazok metszete disztributív az egyesítésre nézve:

$$\begin{aligned} C(X\triangle Y) &= C(X \cap C(Y)) \cap C(Y \cap C(X)) = [C(X) \cup Y] \cup [C(Y) \cup X] \\ &= \{[C(X) \cup Y] \cap C(Y)\} \cup \{[C(X) \cup Y] \cap X\} \\ &= [C(X) \cap C(Y)] \cup [Y \cap C(Y)] \cup [C(X) \cup X] \cup [Y \cap X] \\ &= [C(X) \cap C(Y)] \cup \emptyset \cup \emptyset \cup (X \cap Y) = (X \cap Y) \cup [C(X) \cap C(Y)]. \end{aligned}$$

Az (1) és (2) azonosságokat használva kapjuk, hogy

$$\begin{aligned} (X\triangle Y)\triangle Z &= [(X + Y) \cap C(Z)] \cup [C(X + Y) \cap Z] \\ &= \{[(X \cap C(Y)) \cup (Y \cap C(X))] \cap C(Z)\} \cup \{[(X \cap Y) \cup (C(X) \cap C(Y))] \cap Z\} \\ &= [X \cap C(Y) \cap C(Z)] \cup [Y \cap C(X) \cap C(Z)] \cup [X \cap Y \cap Z] \cup [C(X) \cap C(Y) \cap Z] \\ &= (X \cap Y \cap Z) \cup [X \cap C(Y) \cap C(Z)] \cup [C(X) \cap Y \cap C(Z)] \cup [C(X) \cap C(Y) \cap Z]. \end{aligned}$$

Ugyanerre az eredményre jutunk, ha $X\triangle(Y\triangle Z)$-t számoljuk ki. Tehát $\triangle$ asszociatív művelet.
A $\triangle$ művelet meghatározásából következik, hogy $\triangle$ kommutatív, semleges eleme az üres halmaz és $X\triangle X = \emptyset$, vagyis X inverze X. Tehát $(\mathcal{P}(M), \triangle)$ Abel-csoport.

2) Legyen $G = (-1, 1)$, $x, y \in G$ és

$$(*) \qquad x * y = \frac{x+y}{1+xy}\,.$$

Bizonyítsuk be, hogy:
i) az $(*)$ egyenlet egy $*$ műveletet határoz meg a G halmazon, amivel $(G, *)$ Abel-csoport;
ii) az $(\mathbb{R}_+^*, \cdot)$ pozitív valós számok multiplikatív csoportja és $(G, *)$ között létezik egy $f : \mathbb{R}_+^* \to G$, $f(x) = \dfrac{\alpha x - 1}{x+1}$ alakú izomorfizmus.

Megoldás: i) Ha $x, y \in G$, akkor $x * y \in G$, mert

$$x * y = -1 + \frac{(x+1)(y+1)}{1+xy} \quad \text{és} \quad x * y = 1 - \frac{(x-1)(y-1)}{1+xy}\,.$$

Tehát $*$ egy művelet a G halmazon. Az (1) egyenlőségből következik, hogy $*$ kommutatív. Az asszociativitást a következő módon igazolhatjuk:

$$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{xy+xz+yz+1}\,,$$
$$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{xy+xz+yz+1}\,.$$

Tegyük fel továbbá, hogy e semleges elem. Akkor $x * e = x$ bármely $x \in G$-re, vagyis $\dfrac{x+e}{1+xe} = x$, $\forall x \in G$. Következik, hogy $e = 0$, tehát ha létezik semleges elem, akkor az a 0. Mivel $x * 0 = x$ minden $x \in G$-re, azt jelenti, hogy valóban 0 a semleges elem. Ha x' az $x \in G$ elem inverze, akkor $x * x' = 0$, ahonnan látható, hogy $x' = -x \in G$. Tehát, ha létezik x inverze, akkor ez a $-x$. Könnyen ellenőrizhető, hogy $-x$ az x inverze bármely $x \in G$-re. Bizonyítottuk tehát, hogy $(G, *)$ Abel-csoport.
ii) Mivel f morfizmus, az 1 semleges elem képe a semleges elem lesz, vagyis tudjuk, hogy $f(1) = 0$, amiből rögtön következik, hogy $\alpha = 1$. Tehát

$$(2) \qquad f(x) = \frac{x-1}{x+1}\,.$$

Mivel

$$\frac{x-1}{x+1} > -1 \Leftrightarrow \frac{2x}{x+1} > 0\,,$$
$$\frac{x-1}{x+1} < +1 \Leftrightarrow \frac{-2}{x+1} < 0\,,$$

látható, hogy $f(x) \in G$ bármely $x \in \mathbb{R}_+^*$ esetében, ahonnan látható, hogy (2) egy $f : \mathbb{R}_+^* \to G$ függvény. Az f függvény bijektív, mert az $f(x) = y$ egyenlet egyetlen megoldása $x = \dfrac{1+y}{1-y} \in \mathbb{R}_+^*$. Számolással könnyen igazolható, hogy f morfizmus, vagyis

$$f(x_1 x_2) = \frac{x_1 x_2 - 1}{x_1 x_2 + 1} = f(x_1) * f(x_2)\,.$$

Tehát f izomorfizmus.

3) Legyen $(G, \cdot)$ egy véges csoport és $\emptyset \neq H \subseteq G$. Bizonyítsuk be, hogy H akkor és csak akkor részcsoportja G-nek, ha H zárt részhalmaz $(G, \cdot)$-ben.

Megoldás: Ha $H \leq G$, akkor nyilvánvaló, hogy H zárt részhalmaza $(G, \cdot)$-nek.
Legyen $h \in H$ tetszőleges. Ha H zárt részhalmaz $(G, \cdot)$-ben, akkor a H-ra leszűkített h-val való transzlációk képei H-ban maradnak. Bevezethetjük tehát a következő függvényeket:

$$t_h, t_h' : H \to H,\ t_h(x) = hx,\ t_h'(x) = xh.$$

Ha $x_1, x_2 \in H$ és $t_h(x_1) = t_h(x_2)$, vagyis $hx_1 = hx_2$, akkor egyszerűsíthetünk G-ben h-val az $x_1 = x_2$ egyenlőséghez jutva. Következik, hogy t_h injektív, és mivel H véges, t_h bijektív is. Analóg módon következik, hogy t_h' is bijektív.

A t_h függvény szürjektivitásából következik, hogy létezik, $e \in H$ úgy, hogy $h = t_h(e) = he$. Akkor igaz G-ben, hogy $1h = eh$, ahonnan h-val egyszerűsítve kapjuk, hogy $1 = e \in H$. Vagyis mivel t_h szürjekív, létezik $h' \in H$ úgy, hogy

$$1 = t_h(h') = hh' \Rightarrow hh^{-1} = 1 = hh' \Rightarrow h^{-1} = h' \in H.$$

Mivel $h \in H$ tetszőleges elem volt, következik, hogy $H \leq G$.

4) Igazoljuk, hogy egyetlen morfizmus létezik a $(\mathbb{Q}, +)$ és a $(\mathbb{Z}, +)$ csoport között.

Megoldás: Legyen $f : \mathbb{Q} \to \mathbb{Z}$ egy morfizmus, $x \in \mathbb{Q}$ tetszőleges és $f(x) = a \in \mathbb{Z}$. Bármely $n \in \mathbb{N}^*$ esetén felírható, hogy

$$a = f(x) = f\left(n \cdot \frac{x}{n}\right) = f\Big(\underbrace{\frac{x}{n} + \cdots + \frac{x}{n}}_{n \text{ tag}}\Big) = \underbrace{f\left(\frac{x}{n}\right) + \cdots + f\left(\frac{x}{n}\right)}_{n \text{ tag}} = n \cdot f\left(\frac{x}{n}\right),$$

és mivel $f\left(\frac{x}{n}\right) \in \mathbb{Z}$, következik, hogy $a = 0$ (mivel az összes $n \in \mathbb{N}^*$ többszöröse), tehát $f(x) = 0$ bármely $x \in \mathbb{Q}$-ra.

5) Határozzuk meg a $(\mathbb{Z}, +)$ csoport összes automorfizmusát.

Megoldás: Legyen $f : \mathbb{Z} \to \mathbb{Z}$ egy endomorfizmus $(\mathbb{Z}, +)$-ban. Ha $x \in \mathbb{N}^*$, akkor

$$f(x) = f(\underbrace{1 + 1 + \cdots + 1}_{x \text{ tag}}) = xf(1)$$

és $f(-x) = -f(x)$. Nyilvánvaló, hogy $f(0) = 0 = f(1) \cdot 0$, következésképpen

$$f(x) = f(1) \cdot x, \ \forall x \in \mathbb{Z}.$$

Ha f automorfizmus, mivel f szürjektív, létezik $a \in \mathbb{Z}$ úgy, hogy $1 = f(1) \cdot a$. Következik, hogy $f(1)$ osztója 1-nek, vagyis $f(1) \in \{-1, 1\}$. Ha $f(1) = 1$, akkor $f = 1_{\mathbb{Z}}$, ami nyilván automorfizmusa $(\mathbb{Z}, +)$-nak, ha pedig $f(1) = -1$, akkor f a következő függvény:

$$-1_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}, \ (-1_{\mathbb{Z}})(x) = -x,$$

amiről szintén könnyen igazolható, hogy $(\mathbb{Z}, +)$ automorfizmusa.
Tehát $(\mathbb{Z}, +)$ automorfizmusai $1_{\mathbb{Z}}$ és $-1_{\mathbb{Z}}$.

1.7 A gyűrű fogalma. Példák

Értelmezés 1.21 a) Az $(R, +, \cdot)$ algebrai struktúrát *gyűrű*nek nevezzük, ha:

1. $(R, +)$ Abel-csoport (az R *additív csoportja*);
2. A szorzás *disztributív* az összeadásra nézve, azaz minden $a, b, c \in R$ esetén,

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca.$$

b) R *egységelemes gyűrű*, ha létezik $1 \in R$ úgy, hogy $1 \cdot a = a \cdot 1 = a$ $(\forall) a \in R$ esetén.
c) R *asszociatív* (*kommutatív*) gyűrű, ha $(R, \cdot)$ asszociatív (kommutatív) gruppoid.
d) R *test*, ha R asszociatív egységelemes gyűrű, $1 \neq 0$, és R minden nemnulla eleme invertálható.
e) R *Lie-gyűrű*, ha minden $a, b, c \in R$ esetén

1. $a^2 = 0$;
2. $(ab)c + (bc)a + (ca)b = 0$ (*Jacobi-azonosság*).

Az alábbiakban a ,,gyűrű" mindig ,,asszociatív gyűrűt" fog jelenteni.

Feladat 24 (Számítási szabályok) a) Ha $(R, +, \cdot)$ gyűrű és $a \in R$, akkor igazoljuk, hogy

$$t_a, t'_a : (R, +) \to (R, +), \quad t_a(r) = ar, \quad t'_a(r) = ra$$

csoportmorfizmusok. Következtessük, hogy minden $a, b, c \in R$ esetén
(1) $a \cdot 0 = 0 \cdot a = 0$;
(2) $a(-b) = (-a)b = -ab$; $(-a)(-b) = ab$;
(3) $(-a)^n = a$ ha n páros, és $(-a)^n = -a$ ha n páratlan.
(4) $a(b - c) = ab - ac$, $(b - c)a = ba - ca$.
b) Ha R-ben $1 = 0$ akkor $R = \{0\}$, azaz R *null-gyűrű*.
Az alábbiakban, ha létezik $1 \in R$, akkor feltételezzuk, hogy $1 \neq 0$.
c) Az R egységelemes gyűrű test $\Leftrightarrow (R^*, \cdot)$ csoport, ahol $R^* = R \setminus \{0\}$. Általában, $(R^*, \cdot)$ monoid, és $(U(R), \cdot)$ csoport.
d) Ha R Lie-gyűrű, akkor R *antikommutatív*, azaz $ab = -ba$ minden $a, b \in R$ esetén.

Feladat 25 Ha R kommutatív gyűrű, akkor érvényesek a következő azonosságok:
a) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$;
b) $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ (*Newton binomiális képlete*).

Feladat 26 Legyen R egy (asszociatív) gyűrű, $[a,b] = ab - ba$, $(\forall) a, b \in R$. Igazoljuk, hogy $(R, +, [-,-])$ Lie-gyűrű.

Értelmezés 1.22 Legyen R egy gyűrű és $a, b \in R$.
a) Ha $a, b \neq 0$ és $ab = 0$ akkor azt mondjuk, hogy a *bal oldali zérusosztó* és b *jobb oldali zérusosztó*.
b) R *zérusosztómentes gyűrű*, ha minden $r, s \in R$ esetén $rs = 0 \Rightarrow r = 0$ vagy $s = 0$. Egy kommutatív, zérusosztómentes, egységelemes gyűrűt *integritástartomány*nak nevezünk.
c) a *idempotens*, ha $a^2 = a$. Jelölés: $\mathrm{Idemp}(R) = \{a \in R \mid a \text{ idempotens}\}$.
d) a *nilpotens*, ha létezik $n \in \mathbb{N}^*$ úgy, hogy $a^n = 0$.
Jelölés: $r(R) = \{a \in R \mid a \text{ nilpotens}\}$.

Feladat 27 a) 0, 1 idempotens elemek; ha $e \neq 0, 1$ idempotens, akkor zérusosztó, $e(1-e) = (1-e)e = 0$, és $1 - e$ is idempotens.
b) Ha $a \in R$ invertálható, akkor a nem zérusosztó.
c) (*Egyszerűsítés*) Ha $a \in R$ nem zérusosztó, és $ab = ac$ vagy $ba = ca$, akkor $b = c$.
d) Ha R test, akkor R zérusosztómentes gyűrű; fordítva nem igaz.

Tétel 1.23 *Minden véges integritástartomány test.*

Bizonyítás. Legyen $a \in R^*$ és $t_a : R \to R$, $t_a(x) = ax$. Azonnal következik, hogy t_a injektív. Mivel R véges, következik, hogy t_a szürjektív, tehát létezik $x \in R$ úgy, hogy $ax = 1$. ■

Feladat 28 Legyen R egy egységelemes gyűrű és $a, b \in R$.
a) Ha R kommutatív, a nilpotens és b invertálható, akkor $a + b$ invertálható.
b) Ha $1 - ab$ invertálható, akkor $1 - ba$ invertálható.
c) Ha $a, b, ab - 1$ invertálható elemek, akkor $a - b^{-1}$, $(a - b^{-1})^{-1} - a^{-1}$ invertálhatók, és $((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$.

Feladat 29 Legyen R egy gyűrű és $Z(R) = \{r \in R \mid rx = xr,\ \forall x \in R\}$ az R *centruma*. Igazoljuk, hogy
a) R kommutatív $\Leftrightarrow Z(R) = R$.
a) Ha R-ben nem léteznek nemnulla nilpotens elemek, akkor minden idempotens elem centrális (azaz eleme $Z(R)$-nek).
b) Ha $(\forall) x \in R$ $x^2 - x \in Z(R)$, akkor R kommutatív.

Feladat 30 Legyen R egy véges gyűrű.
a) Ha R egységelemes, akkor minden nemnulla elem vagy bal oldali zérusosztó vagy invertálható.
b) Feltételezzük, hogy $(\exists) a \in R$, a nem bal oldali zérusosztó, és $(\exists) b \in R$, b nem jobb oldali zérusosztó. Akkor R egységelemes gyűrű.

Feladat 31 Legyen R egy egységelemes gyűrű és $a \in R$. Ha a-nak több bal oldali inverze van, akkor végtelen sok van.

1.8 Gyűrűmorfizmusok

Értelmezés 1.24 Legyen R és R' két gyűrű.
a) Az $f : R \to R'$ függvényt *gyűrűmorfizmus*nak nevezzük, ha minden $a, b \in R$ esetén
(1) $f(a+b) = f(a) + f(b)$; (2) $f(ab) = f(a)f(b)$.
Az f-morfizmust *endomorfizmusnak* nevezzük, ha $(R, +, \cdot) = (R', +, \cdot)$.
b) Ha R és R' egységelemes gyűrűk, és $f(1) = 1$, akkor azt mondjuk, hogy f *unitér* morfizmus.
c) f *izomorfizmus*, ha létezik egy $f' : R' \to R$ morfizmus úgy, hogy $f' \circ f = 1_R$ és $f \circ f' = 1_{R'}$.
Jelölések:
- $\mathrm{Hom}(R, R')$ – a morfizmusok halmaza;
- $\mathrm{End}(R)$ – az endomorfizmusok halmaza;
- $\mathrm{Aut}(R)$ – az automorfizmusok halmaza.

Feladat 32 a) $\theta : R \to R'$, $\theta(a) = 0$, és $1_R : R \to R, 1_R(a) = a$ gyűrűmorfizmusok.
b) Ha $f : R \to R'$ morfizmus, akkor $f(0) = 0$ és $f(-a) = -f(a)$ minden $a \in R$ esetén; ha f unitér és $a \in U(R)$, akkor $f(a^{-1}) = f(a)^{-1}$.
c) Ha R, R' egységelemes gyűrűk és $f : R \to R'$ szürjektív morfizmus, akkor f unitér.

Feladat 33 a) $f : R \to R'$ izomorfizmus $\Leftrightarrow$ f bijektív morfizmus.

b) Morfizmusok összetétele morfizmus.

c) $(\mathrm{End}(R), \circ)$ monoid, és $(\mathrm{Aut}(R), \circ)$ csoport.

Feladat 34 Ha K és K' testek és $f : K \to K'$ egy morfizmus, akkor vagy $f = 0$ (*null-morfizmus*), vagy f unitér és injektív.

Feladat 35 (modulo n maradékosztályok gyűrűje) Legyen $n > 1$, $\mathbb{Z}_n = \{\hat{a} \mid a \in \mathbb{Z}\}$, és értelmezzük a következő műveleteket:

$$\hat{a} + \hat{b} = \widehat{a+b}, \qquad \hat{a}\hat{b} = \widehat{ab},$$

minden $a, b \in \mathbb{Z}$ esetén. Igazoljuk, hogy:

a) A fenti definiciók nem függnek a reprezentánsoktól.

b) $(\mathbb{Z}_n, +, \cdot)$ kommutatív egységelemes gyűrű.

c) Ha $a \equiv b \pmod{n}$, akkor $(a, n) = (b, n)$.

d) Ha $(a, n) = 1$, akkor $\hat{a}$ invertálható $\mathbb{Z}_n$-ben.

e) Ha $(a, n) = d > 1$, akkor $\hat{a}$ zérusosztó.

f) Ha p prímszám, akkor $\mathbb{Z}_p$ test.

g) Ha n nem prímszám, akkor $\mathbb{Z}_n$ nem integritástartomány.

h) Számítsuk ki a 7 inverzét modulo 16 és a 11 inverzét modulo 27.

Feladat 36 (komplex számok teste) Az $\mathbb{R} \times \mathbb{R} = \{z = (x, y) \mid x, y \in \mathbb{R}\}$ halmazon értelmezzük a következő műveleteket:

$$(x, y) + (x', y') = (x + x', y + y'), \qquad (x, y)(x', y') = (xx' - yy', xy' + yx').$$

Igazoljuk, hogy:

a) $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ kommutatív test és $\phi : \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \quad x \mapsto (x, 0)$ injektív testmorfizmus.

b) Azonosítjuk x-et $(x, 0)$-val, és legyen $i = (0, 1)$. Ekkor $i^2 = -1$ és $(x, y) = x + yi$. Ez a felírás egyértelmű, vagyis ha $(x, y) = x' + y'i$, akkor $x = x'$ és $y = y'$.

Jelölés: $\mathbb{C} = \{z = x + yi \mid x, y \in \mathbb{R},\ i^2 = -1\}$ a *komplex számok teste*, i az *immaginárius egység*; ha $z = x + yi$, akkor $\Re z = x$ a z *valós része* és $\Im z = yi$ a z *immaginárius része*.

c) Ha $z = x + yi$, legyen $\bar{z} = x - yi$ a z *konjugáltja* és $|z| = \sqrt{z\bar{z}}$ a z *modulusza*. Ekkor, $z \in \mathbb{R} \Leftrightarrow \bar{z} = z, \quad z = 0 \Leftrightarrow |z| = 0$, és

$$\overline{z + z'} = \bar{z} + \bar{z}', \quad \overline{zz'} = \bar{z}\bar{z}', \quad \bar{\bar{z}} = z;$$

$$|zz'| = |z| \cdot |z'|, \qquad |z + z'| \le |z| + |z'|.$$

d) Oldjuk meg a $z^2 = a + bi$ egyenletet. Alkalmazás: $a = 3, \quad b = 4$.

e) Ha $z = x + yi \in \mathbb{C}$ és $r = |z|$, akkor trigonometriából tudjuk, hogy létezik egyetlen $t \in [0, 2\pi)$ úgy, hogy $\cos t = \frac{x}{r}$ és $\sin t = \frac{y}{r}$, tehát $z = r(\cos t + i \sin t) = \exp(it)$. Ez a z *trigonometrikus alakja*. Ekkor:

- $zz' = rr'(\cos(t + t') + i \sin(t + t'))$;
- $\frac{1}{z} = \frac{1}{r}(\cos(-t) + i \sin(-t))$;
- $z^n = r^n(\cos(nt) + i \sin(nt))$.

f) Ha $z = r(\cos t + i \sin t)$ és $n \ge 1$, akkor a $Z^n = z$ egyenletnek pontosan n megoldása van $\mathbb{C}$-ben:

$$Z_k = \sqrt[n]{r}(\cos \frac{t + 2k\pi}{n} + i \sin \frac{t + 2k\pi}{n}), \quad k = 0, \dots, n - 1.$$

g) Legyen $U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\omega_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k = 0, \dots, n - 1\}$ az n-*edik egységgyökök* halmaza. Ekkor:

- $(U_n, \cdot)$ a $(\mathbb{Z}_n, +)$ csoporttal izomorf csoport;
- $Z_k = Z_0\omega_k$, minden $k = 0, \dots, n - 1$ esetén.

Feladat 37 (gyűrűk direkt szorzata) Legyenek $R_1, \dots, R_n$ gyűrűk, és $R = R_1 \times \cdots \times R_n$. Ha $r = (r_1, \dots, r_n)$ és $r' = (r'_1, \dots, r'_n)$, akkor értelmezés szerint,

$$r + r' = (r_1 + r'_1, \dots, r_n + r'_n), \qquad rr' = (r_1 r'_1, \dots, r_n r'_n).$$

Igazoljuk, hogy:

a) $(R, +, \cdot)$ gyűrű.

b) R egységelemes gyűrű $\Leftrightarrow$ R_i egységelemes gyűrűk, $i = 1, \dots, n$; ebben az esetben

$$U(R) = U(R_1) \times \cdots \times U(R_n).$$

c) $\mathrm{Idemp}(R) = \mathrm{Idemp}(R_1) \times \cdots \times \mathrm{Idemp}(R_n)$.

d) $r(R) = r(R_1) \times \cdots \times r(R_n)$.

Feladat 38 (függvények gyűrűje) Legyen M egy nemüres halmaz és R egy gyűrű. Az

$$R^M = \{\alpha \mid \alpha : M \to R\}$$

halmazon értelmezzük a következő műveleteket:

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x); \quad (\alpha\beta)(x) = \alpha(x)\beta(x)$$

$(\forall)x \in M$.

a) R^M gyűrű; R^M kommutatív (egységelemes gyűrű) $\Leftrightarrow$ R kommutatív (egységelemes gyűrű).

b) $\alpha \in R^M$ invertálható (idempotens, nilpotens) $\Leftrightarrow$ $(\forall)x \in M$, $\alpha(x)$ invertálható (idempotens, nilpotens (ha M véges)).

c) Ha $|R| \geq 2$ és $|M| \geq 2$, akkor R^M-ben léteznek zérusosztók.

d) Létezik egy $\phi : R \to R^M$ injektív morfizmus.

e) Ha $f : M' \to M$ egy függvény és $g : R \to R'$ egy gyűrű morfizmus, akkor

$$g^f : R^M \to R'^{M'}, \quad (g^f)(\alpha) = g \circ \alpha \circ f$$

is morfizmus.

Feladat 39 Legyen R egy gyűrű és értelmezzük $\mathbb{Z} \times R$-en a következő műveleteket:

$$(m, r) + (n, s) = (m + n, r + s), \quad (m, r)(n, s) = (mn, ms + nr + rs).$$

Igazoljuk, hogy $\mathbb{Z} \times R$ egységelemes gyűrű, és létezik $\phi : R \to \mathbb{Z} \times R$ injektív morfizmus (tehát *minden gyűrű beágyazható egy egységelemes gyűrűbe*).

Feladat 40 (másodfokú algebrai számok) Legyen $d \in \mathbb{Z}$ négyzetmentes,

$$\mathbb{Z}[\sqrt{d}] = \{z = a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

és legyen

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}, \ N(z) = |z\bar{z}|,$$

a *norma* függvény, ahol $\bar{z} = a - b\sqrt{d}$ a z *konjugáltja*. Igazoljuk, hogy:

a) $\sqrt{d} \notin \mathbb{Q}$; $a + b\sqrt{d} = x + y\sqrt{d} \Leftrightarrow a = x$ és $b = y$.

b) $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ integritástartomány.

c) $N(zw) = N(z)N(w)$; z invertálható $\Leftrightarrow N(z) = 1$.

d) $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$; $U(\mathbb{Z}[i\sqrt{d}]) = \{\pm 1\}$ ha $d \geq 2$; $U(\mathbb{Z}[\sqrt{2}])$ végtelen csoport.

e) Ha $e \in \mathbb{Z}$ négyzetmentes, $d \neq e$, akkor $\mathbb{Z}[\sqrt{d}] \cap \mathbb{Z}[\sqrt{e}] = \mathbb{Z}$.

Feladat 41 (kvadratikus testek) Legyen $d \in \mathbb{Z}$ négyzetmentes szám, és legyen

$$\mathbb{Q}(\sqrt{d}) = \{z = a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Igazoljuk, hogy $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ kommutatív test.

Feladat 42 Igazoljuk, hogy a következő struktúrák *véges testek*:

a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$, ahol $(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac + bd, ad + bc + bd)$.

b) $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, \cdot)$, ahol $(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac - bd, ad + bc)$.

Feladat 43 (mátrixgyűrű) Legyen R egy gyűrű és $m, n \in \mathbb{N}^*$. Egy $A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to R$ függvényt $m \times n$-típusú R-feletti *mátrix*nak nevezünk, és az

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & & \ldots & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} = [a_{ij}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(R)$$

jelöléseket használjuk. Ha $A, A' \in M_{m,n}(R)$ és $B \in M_{n,p}(R)$, akkor értelmezés szerint

$$A + A' = [a_{ij} + a'_{ij}] \in M_{m,n}(R), \qquad AB = [\sum_{k=1}^{n} a_{ik}b_{kj}] \in M_{m,p}(R).$$

Legyen $A = (a_{ij}) \in M_{k,m}(R)$, $B = (b_{ij}), B' = (b'_{ij}) \in M_{m,n}(R)$, $C = (c_{ij}) \in M_{n,p}(R)$. Igazoljuk, hogy:

a) $(AB)C = A(BC)$, $A(B+B') = AB + AB'$ és $(B+B')C = BC + B'C$.

b) $(M_n(R), +, \cdot)$ gyűrű, ahol $M_n(R) := M_{n,n}(R)$.

c) $M_n(R)$ egységelemes gyűrű $\Leftrightarrow$ R egységelemes gyűrű. Ebben az esetben, $AI_n = I_m A = A$ $(\forall) A \in M_{m,n}(R)$, ahol $I_n = (\delta_{ij})_{1 \le i,j \le n} \in M_n(R)$, és $\delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j \end{cases}$ a *Kronecker-szimbólum.*

d) $M_n(R)$ kommutatív $\Leftrightarrow$ $R \cdot R = 0$.

e) Ha R egységelemes gyűrű, $n \ge 2$ és $\phi, \psi : R \to M_n(R)$, $\phi(r) = rI_n$, $\psi(r) = E_{11}$, akkor ϕ és ψ injektív morfizmusok, ϕ unitér, ψ nem unitér.

f) Ha R kommutatív gyűrű, akkor $\phi : M_n(R) \to M_n(R)$, $\phi(A) = A^t = (a_{ji})$ antiautomorfizmus, $\phi^2 = 1_{M_n(R)}$, és ha A invertálható, akkor $(A^{-1})^t = (A^t)^{-1}$.

g) $M_n(M_m(R)) \simeq M_{mn}(R)$.

Feladat 44 Ha $f : R \to S$ egy morfizmus, legyen

$$M_n(f) : M_n(R) \to M_n(S),\ M_n(f)((a_{ij})) = (f(a_{ij})).$$

Bizonyítsuk be, hogy:

a) $M_n(f)$ morfizmus.

b) $M_n(1_R) = 1_{M_n(R)}$ és $M_n(g \circ f) = M_n(g) \circ M_n(f)$.

Feladat 45 Legyen $K = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ és $A_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$, $k \in \mathbb{Z}$. Igazoljuk, hogy:

a) $(K, +, \cdot)$ test és $K \simeq \mathbb{C}$.

b) $(A_k, +, \cdot)$ kommutatív egységelemes gyűrű.

c) A_k integritástartomány $\Leftrightarrow$ k nem teljes négyzet.

d) $A_k \simeq B_k$, ahol $B_k = (\mathbb{Z} \times \mathbb{Z}, +, \cdot)$,

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)(c, d) = (ac + kbd, ad + bc).$$

e) Ha $d \in \mathbb{Z}$ négyzetmentes szám, akkor $\mathbb{Z}[\sqrt{d}] \simeq A_d \simeq B_d$.

Feladat 46 (kvaterniók teste) Legyen $\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$. Bizonyítsuk be, hogy:

a) $(\mathbb{H}, +, \cdot)$ nemkommutatív test és létezik egy $\psi : \mathbb{C} \to \mathbb{H}$ injektív testmorfizmus. *Jelölés*:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

tehát

$$\mathbb{H} = \{x = a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

b) $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$.

c) $\mathbb{H} \simeq \mathbb{H}_1$, ahol $\mathbb{H}_1 = \left\{ \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$.

d) $\mathbb{H}_0$ test, ahol $\mathbb{H}_0 := \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\}$ (*racionális kvaterniók*).

e) Ha $\mathbb{I} := \{\frac{a}{2}1 + \frac{b}{2}i + \frac{c}{2}j + \frac{d}{2}k \mid a, b, c, d \in \mathbb{Z}$ mind páros vagy mind páratlan$\}$, akkor $\mathbb{I}$ gyűrű és nem test.

f) $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ csoport (készítsünk művelettáblát). Q_8-cat a nyolcelemű *kvaterniócsoport*nak nevezzük.

Feladat 47 Ha $x = a1 + bi + cj + dk$, legyen $\bar{x} = a1 - bi - cj - dk$, $N(x) = x\bar{x}$ és $\mathrm{Tr}(x) = x + \bar{x}$. Igazoljuk, hogy :

a) $\phi : \mathbb{H} \to \mathbb{H}$, $x \mapsto \bar{x}$ másodrendű antiautomorfizmusa $\mathbb{H}$-nak, és $\phi \circ \phi = 1_{\mathbb{H}}$. (Azt mondjuk, hogy ϕ *involució*).

b) $N(xy) = N(x)N(y)$, és ha $x \neq 0$ akkor $x^{-1} = \bar{x}/N(x)$.

Feladat 48 (Abel-csoport endomorfizmusgyűrűje) Legyen $(A, +)$ egy Abel-csoport, és legyen

$$f + g : A \to A, \quad (f + g)(x) = f(x) + g(x)$$

minden $f, g \in \mathrm{End}(A, +)$ esetén.

a) Igazoljuk, hogy $(\mathrm{End}(A, +), +, \circ)$ egységelemes gyűrű.

b) Ha $(R,+,\cdot)$ egy egységelemes gyűrű, akkor $\phi : R \to \mathrm{End}(R,+),\ \phi(a) = t_a$ injektív unitér gyűrűmorfizmus, ahol $t_a : R \to R,\ t_a(r) = ar$.

c) Határozzuk meg az $\mathrm{End}(\mathbb{Z},+)$ és $\mathrm{End}(\mathbb{Q},+)$ gyűrűket.

d) Határozzuk meg a $(\mathbb{Z},+)$ automorfizmusait. Igazoljuk, hogy $(\mathrm{Aut}(\mathbb{Z},+),\circ) \simeq (U_2,\cdot)$.

e) Határozzuk meg a $(\mathbb{Q},+)$ automorfizmusait. Igazoljuk, hogy $(\mathrm{Aut}(\mathbb{Q},+),\circ) \simeq (\mathbb{Q}^*,\cdot)$.

Feladat 49 a) Határozzuk meg a $(\mathbb{Z},+,\cdot)$ endomorfizmusait.

b) Határozzuk meg a $\mathrm{Hom}(\mathbb{Z},\mathbb{Q})$ halmazt.

c) Legyen R egy gyűrű. Igazoljuk, hogy $\phi : \mathrm{Hom}(\mathbb{Z},R) \to \mathrm{Idemp}(R),\ \phi(f) = f(1)$ bijektív függvény.

d) Határozzuk meg a $\mathrm{Hom}(\mathbb{Q}(\sqrt{d}),\mathbb{Q}(\sqrt{e}))$ halmazt és az $(\mathrm{Aut}(\mathbb{Q}(\sqrt{d})),\circ)$ csoportot, ahol $d \neq e$ négyzetmentes egész számok.

Feladat 50 Határozzuk meg az $(\mathrm{Aut}(\mathbb{R}),\circ)$ csoportot.

Feladat 51 Ha $n \in \mathbb{N},\ n \geq 2$ és $(\mathbb{Z}_n,+,*)$ egységelemes gyűrű, akkor $(\mathbb{Z}_n,+,*) \simeq (\mathbb{Z}_n,+,\cdot)$.

Feladat 52 Határozzuk meg az összes 4-elemű nemizomorf egységelemes gyűrűt.

Feladat 53 a) Ha $(R,+,\cdot) \simeq (S,+,\cdot)$, akkor $(U(R),\cdot) \simeq (U(S),\cdot)$.

b) Igazoljuk, hogy $(\mathbb{R}\times\mathbb{R},+,\cdot) \not\simeq (\mathbb{C},+,\cdot)$.

Feladat 54 a) Ha K egy kommutatív test, akkor $(K,+) \not\simeq (K^*,\cdot)$.

b) Határozzuk meg az $f : (\mathbb{Q},+) \to (\mathbb{Q}^*,\cdot)$ homomorfizmusokat.

Feladat 55 (injektív morfizmusok jellemzése) Legyen $f : R \to S$ egy gyűrűhomomorfizmus. A következő állítások ekvivalensek:

(i) f injektív.

(ii) $\mathrm{Ker}\, f = \{0\}$.

(iii) f *monomorfizmus*, (azaz minden $\alpha,\beta : R' \to R$ gyűrűmorfizmus esetén, $f\circ\alpha = f\circ\beta \Rightarrow \alpha = \beta$).

Feladat 56 Legyen $f : R \to S$ egy gyűrűmorfizmus. Azt mondjuk, hogy f *epimorfizmus*, ha minden $\alpha,\beta : S \to S'$ gyűrűmorfizmusok esetén $\alpha\circ f = \beta\circ f \Rightarrow \alpha = \beta$. Igazoljuk, hogy:

a) Ha f szürjektív, akkor f epimorfizmus.

b) $\mathbb{Z} \to \mathbb{Q},\ n \mapsto n$ epimorfizmus és nem szürjektív.

c) $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}],\ n \mapsto n$ nem epimorfizmus.

Feladat 57 Legyenek R és S egységelemes gyűrűk és $f : R \to S$ egy szürjektív (tehát unitér) morfizmus. Igazoljuk, hogy:

a) ha $r \in R$ invertálható (centrális, idempotens, nilpotens), akkor $f(r)$ invertálható (centrális, idempotens, nilpotens);

b) a fordított állítás nem igaz.

1.9 Részgyűrűk, résztestek

Értelmezés 1.25 a) Legyen $(R,+,\cdot)$ egy gyűrű és $S \subseteq R$. Azt mondjuk, hogy S *részgyűrűje* R-nek (*jelölés*: $S \leq R$), ha S zárt részhalmaza R-nek az „+”-ra és „·”-ra nézve és, ha az $(S,+,\cdot)$ szintén gyűrű.

Ha R egységelemes és $1 \in S$, az S részgyűrűje R-nek, akkor S *unitér részgyűrű*.

b) Legyen $(K,+,\cdot)$ test , $L \subseteq K$. Azt mondjuk, hogy L *részteste* K-nak (*jelölés*: $L \leq K$), ha az L zárt a két műveletre nézve és az $(L,+,\cdot)$ szintén test.

Tétel 1.26 (részgyűrűk és résztestek jellemzése) a) *Adott az* $(R,+,\cdot)$ *gyűrű és legyen* $S \subseteq R$. S *akkor és csak akkor részgyűrűje az* R*-nek, ha*

1. $S \neq \emptyset$;
2. *minden* $a,b \in S$ *esetén* $a-b, ab \in S$.

b) *Adott a* $(K,+,\cdot)$ *test és* $L \subseteq K$. L *akkor és csak akkor részteste* K*-nak, ha*

1. $|L| \geq 2$;
2. *minden* $a,b \in L,\ b \neq 0$ *esetén,* $a-b, ab^{-1} \in L$.

Bizonyítás. a),,$\Longrightarrow$" Feltételezzük, hogy S részgyűrűje R-nek. Ebből következik, hogy S gyűrű az indukált műveletekkel. Alkalmazva a részcsoportok jellemzési tételét következik, hogy $S \neq \emptyset$, minden $a, b \in S$ esetén $a - b \in S$. A ,,$\cdot$" indukált művelet értelmezéséből következik, hogy $a \cdot b \in S$.

,,$\Longleftarrow$" Mivel $S \neq \emptyset$ és minden $a, b \in S$ esetén $a - b \in S$, a részcsoportok jellemzési tételéből következik, hogy S részcsoportja $(R, +)$-nak, tehát S zárt az összeadásra nézve és $(S, +)$ csoport. Mivel S zárt a szorzásra nézve is, és a műveletek tulajdonságai öröklődnek, következik, hogy $(S, +, \cdot)$ gyűrű.

b) ,,$\Longrightarrow$" Feltételezzük, hogy L részteste K-nak. Akkor L test, tehát L-nek van legalább két eleme. Az $(L, +)$ részcsoportja $(K, +)$-ból, következik, hogy minden $a, b \in L$ esetén $a - b \in L$. Abból, hogy $(L^*, \cdot)$ csoport, következik, hogy minden $a, b \in L$ esetén $ab^{-1} \in L$.

,,$\Longleftarrow$" Mivel $|L| \geq 2$ és minden $a, b \in L$ esetén $a - b \in L$, következik, hogy L részcsoportja $(K, +)$-nak. Minden $a, b \in L^*$ esetén $ab^{-1} \in L$, de egy testben nincsenek zérusosztók és nem nulla elem inverze nemnulla, következik, hogy $ab^{-1} \in L^*$. Tehát L^* részcsoportja $(K^*, \cdot)$. Mivel L zárt a két műveletre nézve is, és a műveletek tulajdonságai öröklődnek, következik, hogy $(L, +, \cdot)$ test. ■

Példa 1.27 $\mathbb{Z}$ részgyűrűje $(\mathbb{Q}, +, \cdot)$-nak, $\mathbb{Q}$ részteste $(\mathbb{R}, +, \cdot)$-nak és $\mathbb{R}$ részteste $(\mathbb{C}, +, \cdot)$-nak.

2) Ha R gyűrű, akkor $\{0\}$ és R részgyűrűi R-nek. Ezeket *triviális* részgyűrűknek nevezzük. Ha S az R-nek olyan részgyűrűje, hogy $S \neq \{0\}$ és $S \neq R$, akkor S-et *valódi részgyűrűnek* nevezzük.

3) Ha R egy gyűrű (test), akkor

$$Z(R) = \{r \in R \mid rx = xr,\ \forall x \in R\}$$

részgyűrűje (részteste) R-nek. A $Z(R)$-et az R *centrum*ának nevezzük.

Feladat 58 a) $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \leq M_2(\mathbb{C})$; R-ben nem létezik jobb oldali egységelem, és végtelen sok bal oldali egységelem létezik.

b) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$ unitér részgyűrűje $M_2(\mathbb{C})$-nek.

c) $T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \leq M_2(\mathbb{C})$, nem unitér, de T egységelemes gyűrű.

Feladat 59 (trianguláris mátrixok) Legyen R egy gyűrű és

$$T_n(R) = \{A = (a_{ij}) \in M_n(R) \mid a_{ij} = 0 \text{ ha } i > j\}$$

a *felső trianguláris mátrixok* halmaza. Bizonyítsuk be, hogy:

a) $T_n(R) \leq M_n(R)$.

b) $f : T_n(R) \to R^n,\ f((a_{ij})) = (a_{11}, \ldots, a_{nn})$ szürjektív homomorfizmus.

c) Ha $A \in \operatorname{Ker} f$, akkor $A^n = 0_n$.

Feladat 60 Ha R egységelemes gyűrű, akkor $Z(M_n(R)) = Z(T_n(R)) = \{aI_n \mid a \in Z(R)\}$.

Feladat 61 Legyen p egy prímszám és

$$\mathbb{Q}(\sqrt[3]{p}) = \{z = a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}.$$

Bizonyítsuk be, hogy:

a) $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0 \Leftrightarrow a = b = c = 0$.

b) $\mathbb{Q}(\sqrt[3]{p})$ részteste $\mathbb{R}$-nek.

c) $\{a + b\sqrt[3]{p} \mid a, b \in Q\}$ nem részteste $\mathbb{R}$-nek.

Feladat 62 Legyen $S \subseteq \mathbb{Z}[\sqrt{d}]$. Igazoljuk, hogy S unitér részgyűrűje $\mathbb{Z}[\sqrt{d}]$-nek $\Leftrightarrow (\exists) n \in \mathbb{N}$ úgy, hogy $S = \mathbb{Z} + n\sqrt{d}\mathbb{Z}$.

Feladat 63 Legyen $C([0, 1]) = \{\alpha : [0, 1] \to \mathbb{R} \mid \alpha \text{ folytonos}\}$. Igazoljuk, hogy:

a) $C([0, 1]) \leq (\mathbb{R}^{[0,1]}, +, \cdot)$.

b) α invertálható $\Leftrightarrow \alpha > 0$ vagy $\alpha < 0$.

c) α idempotens $\Leftrightarrow \alpha = 0$ vagy $\alpha = 1$.

d) α nilpotens $\Leftrightarrow \alpha = 0$.

e) α zérusosztó $\Leftrightarrow (\exists) \varnothing \neq I \subseteq [0, 1]$ nyílt intervallum úgy, hogy $\alpha(t) = 0$ $(\forall) t \in I$.

Feladat 64 Legyen R egy gyűrű, $X \subseteq R$ és

$$C_R(X) = \{r \in R \mid rx = xr \ (\forall)x \in X\}$$

az X *centralizátora* (tehát $C_R(R) = Z(R)$, az R *centruma*). Igazoljuk, hogy:
a) $C_R(X) \leq R$; ha R test, akkor $C_R(X)$ résztest.
b) $X \subseteq Y \Rightarrow C_R(X) \supseteq C_R(Y)$.
c) $X \subseteq C_R(C_R(X))$.
d) $C_R(C_R(C_R(X))) = C_R(X)$.
e) Határozzuk meg $Z(\mathbb{H})$-t és $C_{\mathbb{H}}(i)$-t.

1.10 Megoldott feladatok

1) Legyen M egy halmaz és $\mathcal{P}(M)$ az M részhalmazainak halmaza. Bevezetjük a $\mathcal{P}(M)$ halmazon a $+$ és $\cdot$ műveleteket:

$$X + Y = (X \setminus Y) \cup (Y \setminus X) \quad \text{és} \quad X \cdot Y = X \cap Y.$$

Igazoljuk, hogy:
i) $(\mathcal{P}(M), +, \cdot)$ kommutatív, egységelemes, asszociatív gyűrű;
ii) ha $|M| \geq 2$, akkor bármely $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ zérusosztó;
iii) $(\mathcal{P}(M), +, \cdot)$ akkor és csak akkor test, ha $|M| = 1$.

Megoldás: i) Látjuk, hogy $X + Y$ az X és Y részhalmazok szimmetrikus különbsége. Az előző részben az 1) feladatban bizonyítottuk, hogy $(\mathcal{P}(M), +)$ Abel-csoport. A metszet tulajdonságaiból és a „$\cdot$” műveletből következik, hogy „$\cdot$” asszociatív, kommutatív és M a semleges elem. Tehát $(\mathcal{P}(M), \cdot)$ kommutatív monoid.

A következőkben levezetjük a „$\cdot$” disztributivitását a „$+$”-ra nézve. Valóban,

$$\begin{aligned}
X \cdot Y + X \cdot Z &= (X \cap Y) + (X \cap Z) \\
&= [(X \cap Y) \cap C(X \cap Z)] \cup [(X \cap Z) \cap C(X \cap Y)] \\
&= [X \cap Y \cap (C(X) \cup C(Z))] \cup [X \cap Z \cap (C(X) \cup C(Y))] \\
&= [X \cap Y \cap C(X)] \cup [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(X)] \cup [X \cap Z \cap C(Y)] \\
&= \emptyset \cup [X \cap Y \cap C(Z)] \cup \emptyset \cup [X \cap Z \cap C(Y)] \\
&= [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(Y)] = X \cap [(Y \cap C(Z)) \cup (Z \cap C(Y))] \\
&= X \cdot (Y + Z),
\end{aligned}$$

tehát a szorzás disztributív az összeadásra nézve. Tehát $(\mathcal{P}(M), +, \cdot)$ kommutatív, egységelemes, asszociatív gyűrű, ahol a zérus $\emptyset$, az egység pedig M.
ii) Ebben a gyűrűben igaz, hogy $X \subseteq M$, $X^2 = X$, vagyis $X(X - 1) = 0$, vagy ekvivalens módon, $X(X + M) = \emptyset$, ami azt jelenti, hogy bármely $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ zérusosztó.
iii) Az előző pontból következik, hogy a $(\mathcal{P}(M), +, \cdot)$ gyűrű akkor és csak akkor zérusosztómentes, ha $P(M) = \{\emptyset, M\}$, vagyis $|M| \leq 1$. Ha $|M| = 0$, akkor $M = \emptyset$ és $(\mathcal{P}(M), +, \cdot)$ triviális, ha pedig $|M| = 1$, akkor $(\mathcal{P}(M), +, \cdot)$ izomorf $(\mathbb{Z}_2, +, \cdot)$-vel, ahonnan következik, hogy $(\mathcal{P}(M), +, \cdot)$ test.

2) Legyen $(R, +, \cdot)$ asszociatív gyűrű és $a, b \in R$. Igazoljuk, hogy:
a) $(a + b)^2 = a^2 + 2ab + b^2 \Leftrightarrow ab = ba \Leftrightarrow a^2 - b^2 = (a - b)(a + b)$;
b) ha $ab = ba$ akkor minden $n \in \mathbb{N}^*$-re igazak a következő azonosságok:

$$\begin{aligned}
(a + b)^n &= C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n; \\
a^n - b^n &= (a - b)\left(a^{n-1} + a^{n-2} b + \cdots + a b^{n-2} + b^{n-1}\right); \\
a^{2n+1} + b^{2n+1} &= (a + b)\left(a^{2n} - a^{2n-1} b + \cdots - a b^{2n-1} + b^{2n}\right).
\end{aligned}$$

Megoldás: a) Ha $(a + b)^2 = a^2 + 2ab + b^2$, akkor $a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2$, és mivel $(R, +)$-ban bármely elemmel egyszerűsíteni lehet, következik, hogy $ab = ba$. Az $a^2 - b^2 = (a - b)(a + b)$ egyenletből következik, hogy $a^2 - b^2 = a^2 + ab - ba - b^2$, ahonnan kapjuk, hogy $0 = ab - ba$, vagyis $ab = ba$. Ha $ab = ba$, akkor a két egyenlet helyessége rögtön igazolható.
b) Figyelembe vesszük azt a tényt, hogy $a^i b^j = b^j a^i$, $\forall i, j \in \mathbb{N}^*$ és indukciót alkalmazunk n szerint. Az $n = 1$ nyilvánvalóan igaz, és ha feltételezzük, hogy igaz n-re, akkor

$$\begin{aligned}
(a + b)^{n+1} = (a + b)^n (a + b) &= (C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n) a \\
&\quad + (C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n) b \\
&= C_n^0 a^{n+1} + (C_n^1 + C_n^0) a^n b + \cdots + (C_n^{n-1} + C_n^n) a b^n + C_n^n b^{n+1}.
\end{aligned}$$

Mivel $C_n^0 = C_n^n = 1$ és $C_n^k + C_n^{k-1} = C_{n+1}^k$ bármely $n \in \mathbb{N}^*$-re és $1 \leq k \leq n$, kapjuk, hogy

$$(a+b)^{n+1} = C_{n+1}^0 a^{n+1} + C_{n+1}^1 a^n b + \cdots + C_{n+1}^n ab^n + C_{n+1}^{n+1} b^{n+1},$$

vagyis az egyenlet $n+1$-re is igaz. A másik két egyenletet úgy vezethetük le, hogy kifejtjük az előbbi egyenlet jobb oldalát.

3) Legyen $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ és $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Bizonyítsuk be, hogy:
i) $\mathbb{Z}[\sqrt{2}]$ egységelemes részgyűrűje $(\mathbb{R}, +, \cdot)$-nak;
ii) $\mathbb{Q}(\sqrt{2})$ részteste $(\mathbb{R}, +, \cdot)$-nak;
iii) $S_1 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ nem részgyűrűje $(\mathbb{R}, +, \cdot)$-nak;
iv) $S_2 = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ nem részgyűrűje $(\mathbb{R}, +, \cdot)$-nak.
Megoldás: i) Nyilván $\mathbb{Z}[\sqrt{2}] \neq \emptyset$. Bármely $u = a + b\sqrt{2},\ u' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ $(a, a', b, b' \in \mathbb{Z})$ elemekre felírható, hogy:

$$u - u' = (a - a') + (b - b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}],\ uu' = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

és $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Tehát $\mathbb{Z}[\sqrt{2}]$ részgyűrű és $1 \in \mathbb{Z}[\sqrt{2}]$.
ii) Nyilván $|\mathbb{Q}(\sqrt{2})| \geq 2$. Az előbbivel analóg módon bizonyítjuk, hogy bármely $u, u' \in \mathbb{Q}(\sqrt{2})$-ra igaz, hogy $u - u', uu' \in \mathbb{Q}(\sqrt{2})$. Legyen $u = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $u \neq 0$. Ez azt jelenti, hogy $a, b \in \mathbb{Q}$ és $a^2 - 2b^2 \neq 0$, következkezésképpen

$$u^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Tehát $\mathbb{Q}(\sqrt{2})$ résztest.
iii) Legyen $u = \sqrt[3]{2}$, így $u \in S_1$. Kimutatjuk, hogy $u^2 \notin S_1$. Ha $u^2 \in S_1$ igaz lenne, következne, hogy $u^2 = a + bu$ ahol $a, b \in \mathbb{Z}$, ahonnan $u^3 = au + bu^2$, vagyis

$$2 = au + b(a + bu) = ab + (a + b^2)u,$$

de mivel u irracionális, $ab = 2$ és $a + b^2 = 0$. Ennek az egyenletrendszernek nincs megoldása $\mathbb{Z}$-ben. Tehát S_1 nem zárt a szorzásra nézve és emiatt S_1 nem lehet $(\mathbb{R}, +, \cdot)$ részgyűrűje.
iv) Az előbbihez hasonló módon kimutatható, hogy $u = \sqrt[3]{2} \in S_2$, de $u^2 \notin S_2$.

4) Határozzuk meg a $\mathbb{Q}(\sqrt{2})$ test automorfizmusait.
Megoldás: Feltételezzük, hogy $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ automorfizmus. Mivel a testek közti nemnulla morfizmusok unitérek, $f(1) = 1$.

Ha $m, n \in \mathbb{N}^*$, akkor $f\left(\frac{m}{n}\right) = f\left(\underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{m \text{ tag}}\right) = mf\left(\frac{1}{n}\right)$. Következik, hogy

$$1 = f(1) = f\left(\frac{n}{n}\right) = nf\left(\frac{1}{n}\right),$$

tehát $f\left(\frac{1}{n}\right) = \frac{1}{n} f(1) = \frac{1}{n}$, $f\left(\frac{m}{n}\right) = \frac{m}{n} f(1) = \frac{m}{n}$ és $f\left(-\frac{m}{n}\right) = -f\left(\frac{m}{n}\right) = -\frac{m}{n}$. Vagyis $f(x) = x$ bármely $x \in \mathbb{Q}$-ra. Mivel $(\sqrt{2})^2 = 2$ következik, hogy $[f(\sqrt{2})]^2 = 2$, ahonnan $f(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$. Tehát $f \in \{f_1, f_2\}$, ahol $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$ és $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$. Az $f_1 = 1_{\mathbb{Q}(\sqrt{2})}$ egyenletből következik, hogy f_1 automorfizmus. Továbbá, mivel $f_2 \circ f_2 = 1_{\mathbb{Q}(\sqrt{2})}$ következik, hogy f_2 bijektív és $f_2^{-1} = f_2$. Könnyen igazolható, hogy f_2 morfizmus. Tehát f_2 is automorfizmus. A $\mathbb{Q}(\sqrt{2})$ test automorfizmusai tehát f_1 és f_2.

5) Bizonyítsuk be, hogy a $(\mathbb{R}, +, \cdot)$ test egyetlen nemnulla endomorfizmusa $1_{\mathbb{R}}$.
Megoldás: Legyen f egy endomorfizmusa $(\mathbb{R}, +, \cdot)$-nak. Mivel $(f(1))^2 = f(1)$ két esetünk van: $f(1) = 1$ vagy $f(1) = 0$. A második esetben f a nullmorfizmus. Ha f nem a nullmorfizmus, akkor f injektív. Hasonlóan az előző feldat megoldásához, kimutatjuk, hogy $f(x) = x$ bármely $x \in \mathbb{Q}$-ra, és ha $x \in \mathbb{R}$, $x > 0$, akkor $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 > 0$ (az, hogy $f(\sqrt{x}))^2$ szigorúan nagyobb mint 0, ahonnan következik, hogy f injektív). Kapjuk tehát, hogy bármely $x, y \in \mathbb{R}$-re, ahol $x < y$

$$f(y) - f(x) = f(y - x) > 0,$$

vagyis f szigorúan növekvő. Egy $a \in \mathbb{R} \setminus \mathbb{Q}$ értéket közelíthetünk alulról egy $(a'_n)_{n\in\mathbb{N}}$, felülről pedig egy $(a''_n)_{n\in\mathbb{N}}$ racionális sorozattal, így $a'_n \leq a \leq a''_n$ bármely $n \in \mathbb{N}$-re, következkezésképpen

$$a'_n = f(a'_n) \leq f(a) \leq f(a''_n) = a''_n$$

$\forall n \in \mathbb{N}$. Határértékben kapjuk, hogy $f(a) = a$. Tehát $f = 1_{\mathbb{R}}$.

2 Vektorterek

2.1 Alapfogalmak

Legyen K egy kommutatív test.

Értelmezés 2.1 a) Legyen $(V,+)$ egy Abel-csoport. Azt mondjuk, hogy $V = (V,+,K)$ K-*feletti vektortér* (vagy K-*lineáris tér*), ha értelmezett egy

$$\phi : K \times V \to V, \qquad \phi(a,x) = ax$$

függvény (külső művelet) úgy, hogy a következő négy axióma teljesül:
(M1) $a(x+y) = ax + ay$,
(M2) $(a+b)x = ax + bx$,
(M3) $(ab)x = a(bx)$,
(M4) $1x = x$,
minden $a, b \in K$ és $x, y \in V$ esetén.

Az K test elemeit *skalár*oknak nevezzük, és a ϕ külső műveletet *skalárokkal való szorzásnak*. $(V,+)$ a V vektortér *additív csoportja*, elemeit *vektoroknak* nevezzük, semleges elemét 0_V-t pedig *zérusvektornak*.

Megjegyzés 2.2 (Számítási szabályok) a) Legyen V egy K-lineáris tér, és tekintsük az $f_a : V \to V$, $f_a(x) = ax$ és $f'_x : K \to V$, $f'_x(a) = ax$ függvényeket. Az (M1)–(M4) axiomákból következik, hogy $f_a : (V,+) \to (V,+)$ és $f'_x : (K,+) \to (V,+)$ csoportmorfizmusok, tehát minden $a, b \in K$ és $x, y \in V$ esetén
(1) $a0_V = 0_K x = 0_V$.
(2) $(-a)x = a(-x) = -ax$, $(-a)(-x) = ax$.
(3) $a(x-y) = ax - ay$.
(4) $(a-b)x = ax - bx$.
b) Ha $ax = 0$, akkor $a = 0$ vagy $x = 0$.
Valóban, ha $a \neq 0$, akkor létezik $a^{-1} \in K$. Ekkor $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0 = 0$.

Feladat 65 K K-lineáris tér, ahol $\phi(a,x) = ax$ $\forall a, x \in K$. Általánosabban, $K^n = \{x = (x_1, \ldots, x_n) \mid x_i \in K\}$ K-lineáris tér, ahol

$$x + y = (x_1 + y_1, \ldots, x_n + y_n),$$
$$ax = (ax_1, \ldots, ax_n)$$

minden $x, y \in K^n$ és $a \in K$ esetén.

Feladat 66 (szabad vektorok) a) $\mathcal{V}_2 = \{\vec{v} = x\vec{i} + y\vec{j} \mid x, y \in \mathbb{R}\}$, (a síkbeli szabad vektorok halmaza) $\mathbb{R}$-feletti vektortér és azonosítható $\mathbb{R}^2$-tel. b) $\mathcal{V}_3 = (\mathcal{V}_3, +, \times, \mathbb{R}) = \{\vec{v} = x\vec{i} + y\vec{j} + z\vec{k} \mid x, y, z \in \mathbb{R}\}$, (a térbeli szabad vektorok halmaza) $\mathbb{R}$-feletti vektortér és azonosítható $\mathbb{R}^3$-nel.

Feladat 67 Legyen $V = \mathbb{R}_+^* = (0, +\infty)$, $K = \mathbb{R}$, $x \oplus y = xy$ és $a \odot x = x^a$, $\forall\, a \in K,\ x, y \in V$. Akkor V K-feletti vektortér.

Feladat 68 Legyen $V \neq \{0\}$ egy K-feletti vektortér. Igazoljuk, hogy $|K| \leq |V|$.

2.2 Részterek

Értelmezés 2.3 Legyen V egy K-lineáris tér és U egy nemüres részhalmaza. Azt mondjuk, hogy U *résztere* $V-$nek (jelölés: $U \leq_K V$ ha
(1) $\forall x, y \in U,\ x + y \in U$.
(2) $\forall a \in K,\ x \in U,\ ax \in U$.

Megjegyzés 2.4 a) Ha $U \leq_K V$, akkor U K-lineáris tér az indukált műveletekkel.
b) $\emptyset \neq U \leq_K V$ akkor és csak akkor, ha $\forall\, x, y \in U,\ a, b \in K\ \ ax + by \in U$.
c) $\{0\},\ V \leq_K V$. Ezek a *triviális* részterek. Ha $U \leq_K V$, $U \neq \{0\},\ V$, akkor U *valódi* résztér.

Feladat 69 Legyenek $U_1, \ldots, U_n$ részterek. Akkor

$$\bigcap_{i=1}^{n} U_i := U_1 \cap \cdots \cap U_n,$$
$$\sum_{i=1}^{n} U_i := U_1 + \cdots + U_n = \{x_1 + \cdots + x_n \mid x_i \in U_i\}$$

is résztér.

Feladat 70 Legyenek U_1, U_2 részterek. Akkor $U_1 \cup U_2 \leq_K V \Leftrightarrow U_1 \subseteq U_2$ vagy $U_2 \subseteq U_1$.

Feladat 71 A $\mathcal{V}_2$ valódi részterei azonosíthatók az origót tartalmazó egyenesekkel.
A $\mathcal{V}_3$ valódi részterei azonosíthatók az origót tartalmazó egyenesekkel vagy síkokkal.

2.3 Lineáris függvények

Értelmezés 2.5 Legyen U és V két K-lineáris tér és $f : U \to V$ egy függvény. Azt mondjuk, hogy f K-*lineáris*, ha

(1) $f(x + y) = f(x) + f(y)$,
(2) $f(ax) = af(x)$.

minden $x, y \in U$ és $a \in K$ esetén.

Az $f : U \to V$ linearis függvény *izomorfizmus* ha létezik $f' : V \to U$ úgy, hogy $f' \circ f = \mathbf{1}_U$ és $f \circ f' = \mathbf{1}_V$.

A következő jelöléseket gyakran fogjuk használni:

• $\mathrm{Hom}_K(U, V) = \{f : U \to V \mid f \ \ K\text{-lineáris}\}$. • $\mathrm{End}_K(V) = \mathrm{Hom}_K(V, V)$ (*endomorfizmusok* halmaza). • $\mathrm{Aut}_K(V) = \{f : V \to V \mid f \ \ K\text{-izomorfizmus}\}$ (*automorfizmusok* halmaza).

• $U \simeq V$ ha létezik $f : U \to V$ izomorfizmus.

Feladat 72 a) $f : U \to V$ K-lineáris $\Leftrightarrow f(ax + by) = af(x) + bf(y)$ minden $x, y \in U$ és $a, b \in K$ esetén.
b) Ebben az esteben $f(0) = 0$ és $f(-x) = -f(x) \ \ \forall x \in U$.

Feladat 73 Legyen $f : U \to V$ egy morfizmus. f izomorfizmus $\Leftrightarrow f$ bijektív.

Feladat 74 Legyenek $f, f' : U \to V$, $g : U' \to U$ és $h : V \to V'$ K-lineáris függvények.
a) $f \circ g : U' \to V$ K-lineáris.
b) $h \circ (f + f') \circ g = h \circ f \circ g + h \circ f' \circ g$.
c) $(\mathrm{Hom}_K(U, V), +, K)$ K-lineáris tér, ahol

$$(f + f')(x) = f(x) + f'(x)$$
$$(af)(x) = af(x) \quad \forall\, a \in K, x \in U.$$

Értelmezés 2.6 Legyen U és V két vektortér és $f : U \to V$ egy lineáris függvény. Ha $U' \leq_K U$ és $V' \leq_K V$, akkor értelmezzük a következő részhalmazokat:
a) $f(U') = \{f(x) \mid x \in U'\} \subseteq V$.
b) $\mathrm{Im}(f) = f(U) \subseteq V$ (az f *képe*.)
c) $f^{-1}(V') = \{x \in U \mid f(x) \in V'\}$.
d) $\mathrm{Ker}(f) = f^{-1}(\{0\}) = \{x \in U \mid f(x) = 0\}$ (az f *magja*.)

Feladat 75 a) $f(U') \leq_K V$ és $f^{-1}(V') \leq U$. Partikulárisan, $\mathrm{Im}(f) \leq_K V$ és $\mathrm{Ker} f \leq_K U$.
b) f injektív $\Leftrightarrow \mathrm{Ker} f = \{0\} \Leftrightarrow \ (f(x) = 0 \ \Rightarrow \ x = 0)$.

2.4 Megoldott feladatok

1) Lehet-e egy véges halmaznak vektortér struktúrája egy végtelen elemű test fölött?

Megoldás: Legyen V egy véges halmaz és K egy végtelen elemű test. Ha V-nek egyetlen eleme van, akkor egyetlen vektortér struktúra jöhet szóba K fölött, a triviális vektortér. Ha $|V| \geq 2$, feltételezzük, hogy létezik V-nek egy vektortér struktúrája K fölött. Tekintsük az $x \neq 0$ elemet. Ekkor a $t'_x : K \to V$, $t'_x(\alpha) = \alpha x$ függvény injektív, mert

$$\alpha_1, \alpha_2 \in K,\ t'_x(\alpha_1) = t'_x(\alpha_2) \Rightarrow \alpha_1 x = \alpha_2 x \Rightarrow (\alpha_1 - \alpha_2)x = 0 \overset{x \neq 0}{\Rightarrow} \alpha_1 - \alpha_2 = 0 \Rightarrow \alpha_1 = \alpha_2.$$

Következik, hogy $|K| \leq |V|$, ami ellentmond annak, hogy V véges halmaz.

2) Legyen V egy vektortér K fölött, $S \leq_K V$ és $x, y \in V$. Használjuk a következő jelölést: $\langle S, x\rangle = \langle S \cup \{x\}\rangle$. Bizonyítsuk be, hogy ha $x \in V \setminus S$ és $x \in \langle S, y\rangle$, akkor $y \in \langle S, x\rangle$.

Megoldás: Mivel $x \in \langle S, y\rangle$ következik, hogy léteznek $s_1, \ldots, s_n \in S$ és $\alpha_1, \ldots, \alpha_n, \alpha \in K$ úgy, hogy

$$x = \alpha_1 s_1 + \cdots + \alpha_n s_n + \alpha y.$$

Ha $\alpha = 0$ lenne, akkor $x = \alpha_1 s_1 + \cdots + \alpha_n s_n \in S$, ami ellentmond a feltevésnek, tehát $\alpha \neq 0$ és invertálható K-ban. Felírhatjuk, hogy

$$y = -\alpha^{-1}\alpha_1 s_1 - \cdots - \alpha^{-1}\alpha_n s_n + \alpha^{-1} x \in \langle S, x\rangle.$$

3) Ha V egy vektortér K fölött, $V_1, V_2 \leq_K V$ és $V = V_1 \oplus V_2$, akkor azt mondjuk, a V_i $(i = 1, 2)$ részterek direkt összeadandók V-ben. Igazoljuk, hogy egy résztérnek azon tulajdonsága, hogy direkt összeadandó, tranzitív tulajdonság (a résztereire nézve).

Megoldás: Legyen V egy vektortér K fölött és V_1, V_2, V_3, V_4 részterei V-nek úgy, hogy $V = V_1 \oplus V_2$ és $V_1 = V_3 \oplus V_4$. Következik, hogy $V = V_1 + V_2 = V_3 + V_4 + V_2$. Sőt, ha $v_3 \in V_3 \cap (V_4 + V_2)$, akkor léteznek $v_4 \in V_4$, $v_2 \in V_2$ vektorok úgy, hogy $v_3 = v_4 + v_2$. Tehát $v_2 = v_3 - v_4 \in V_3 + V_4 = V_1$, következésképpen $v_2 \in V_1 \cap V_2 = \{0\}$. Kapjuk, hogy $v_2 = 0$ és $v_3 = v_4 \in V_3 \cap V_4 = \{0\}$. Így tehát $V_3 \cap (V_4 + V_2) = \{0\}$ és $V = V_3 \oplus (V_4 + V_2)$, ami azt jelenti, hogy V_3 direkt összeadandó V-ben.

4) Létezik-e olyan $f : \mathbb{R}^3 \to \mathbb{R}^2$ $\mathbb{R}$-lineáris függvény, ami teljesíti a következő azonosságot:

$$f(1, 0, 3) = (1, 1) \text{ és } f(-2, 0, -6) = (2, 1)?$$

Megoldás: Nem, mert $f(-2, 0, -6) \neq (-2)f(1, 0, 3)$, mivel $f(-2, 0, -6) = (2, 1)$ és $(-2)f(1, 0, 3) = (-2)(1, 1) = (-2, -2)$.

2.5 Véges generátorrendszer. Lineáris függőség és függetlenség. Bázis

Értelmezés 2.7 a) Legyen V egy K-lineáris tér, $x_1, \ldots, x_n \in V$ és $a_1, \ldots, a_n \in K$. Azt mondjuk, hogy $x = a_1x_1 + \cdots + a_nx_n \in V$ az $x_1, \ldots, x_n$ elemeknek egy *lineáris kombinációja.* Jelölés:

$$\langle x_1, \ldots, x_n \rangle = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in K\}.$$

b) $\{x_1, \ldots, x_n\}$ *generátorrendszere* V-nek, ha

$$\langle x_1, \ldots, x_n \rangle = V.$$

Azt mondjuk, hogy V *végesen generált* ha van egy (véges) $\{x_1, \ldots, x_n\}$ generátorrendszere.

c) $x_1, \ldots, x_n \in V$ *lineárisan független* elemek ha minden $a_1 \ldots, a_n \in K$ esetén

$$a_1x_1 + \cdots + a_nx_n = 0 \;\Rightarrow\; a_1 = \cdots = a_n = 0.$$

d) Ellenkező esetben azt mondjuk, hogy az $\{x_1, \ldots, x_n\}$ rendszer *lineárisan összefüggő*, azaz, léteznek a nem mind nulla $a_1 \ldots, a_n \in K$ skalárok úgy, hogy

$$a_1x_1 + \cdots + a_nx_n = 0.$$

e) Egy lineárisan független generátorrendszert *bázis*nak nevezünk.

Lemma 2.8 *Legyenek* $x, x_1, \ldots, x_n \in V$.

a) $\langle x_1, \ldots, x_n \rangle \leq_K V$.

b) $x \in \langle x_1, \ldots, x_n \rangle \Leftrightarrow \langle x, x_1, \ldots, x_n \rangle = \langle x_1, \ldots, x_n \rangle$

c) $\{x_1, \ldots, x_n\}$ *akkor és csak akkor bázisa* V*-nek, ha minden* $x \in V$ *egyértelműen felírható az* $x_1, \ldots, x_n$ *elemek lineáris kombinációjaként.*

Bizonyítás. a) Legyen $x, y \in \langle x_1, \ldots, x_n \rangle$, $x = a_1x_1 + \cdots + a_nx_n$, $y = b_1x_1 + \cdots + b_nx_n$, és legyen $a \in K$. Ekkor

$$x + y = (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \in \langle x_1, \ldots, x_n \rangle,$$
$$ax = a_1x_1 + \cdots + a_nx_n \in \langle x_1, \ldots, x_n \rangle.$$

b) Vegyük észre, hogy $\langle x_1, \ldots, x_n \rangle \subseteq \langle x, x_1, \ldots, x_n \rangle$. Fordítva, ha $x = a_1x_1 + \cdots + a_nx_n$ és $y = bx + b_1x_1 + \cdots + b_nx_n \in \langle x, x_1, \ldots, x_n \rangle$, akkor $y = (a_1b + b_1)x_1 + \cdots + (a_nb + b_n)x_n \in \langle x_1, \ldots, x_n \rangle$.

c) „⇒” Ha $\{x_1, \ldots, x_n\}$ bázis, akkor minden $x \in V$ lineáris kombinációja $x_1, \ldots, x_n$-nek. Feltételezzük, hogy

$$x = a_1x_1 + \cdots + a_nx_n = a_1'x_1 + \cdots + a_n'x_n.$$

Akkor $(a_1 - a_1')x_1 + \cdots + (a_n - a_n')x_n = 0$, és mivel $\{x_1, \ldots, x_n\}$ lineárisan független, következik, hogy $a_i = a_i',\ i = 1, \ldots, n$.

„⇐” Elég igazolni, hogy $\{x_1, \ldots, x_n\}$ lineárisan független rendszer. Valóban, ha

$$a_1x_1 + \cdots + a_nx_n = 0 = 0x_1 + \cdots + 0x_n,$$

akkor $a_i = 0,\ i = 1, \ldots, n$. ■

Feladat 76 $\mathbb{C}$ $\mathbb{R}$-feletti vektortér és $\{1, i\}$ bázisa.

Feladat 77 $\{\vec{i}, \vec{j}\}$ bázisa a $\mathcal{V}_2$ $\mathbb{R}$-feletti vektortérnek, és $\{\vec{i}, \vec{j}, \vec{k}\}$ bázisa a $\mathcal{V}_3$ $\mathbb{R}$-feletti vektortérnek.

Feladat 78 $\{1, X, \dots, X^n\}$ bázisa $K_n[X]$-nek. $K[X]$ nem végesen generált K-modulus.

Feladat 79 K^n-ben tekintsük a következő elemeket:

$$\begin{aligned} e_1 &= (1, 0, 0, \dots, 0) \\ e_2 &= (0, 1, 0, \dots, 0) \\ e_3 &= (0, 0, 1, \dots, 0) \\ &\dots \\ e_n &= (0, 0, 0, \dots, 1) \end{aligned}$$

Akkor $e = \{e_1, \dots, e_n\}$ bázisa K^n-nek. e-t *kanonikus bázisnak* nevezzük.

Feladat 80 Az üres halmaz lineárisan független és bázisa $\{0\}$-nak.

Tétel 2.9 *Legyen V egy K-feletti vektortér.*

a) $x_1 \in V$ *lineárisan független* $\Leftrightarrow x_1 \neq 0$.

b) *Az $x_1, \dots, x_n \in V$ vektorok akkor és csak akkor összefüggők, ha létezik $i \in \{1, \dots, n\}$ úgy, hogy x_i felírható a többi vektor egy lineáris kombinációjaként.*

c) *Ha V végesen generált, akkor minden generátorrendszeréből kiválasztható egy bázis.*

Bizonyítás. a) Mivel $1 \cdot 0_V = 0_V$ és $1 \neq 0$, következik, hogy $\{0_V\}$ lineárisan összefüggő rendszer.

Ha $x_1 \neq 0$ és $a_1 x_1 = 0$, akkor (1.2.b)-ből következik, hogy $a_1 = 0$.

b) Ha $a_1 x_1 + \dots + a_n x_n = 0$ és $a_i \neq 0$, akkor

$$x_i = a_i^{-1} a_1 x_1 + \dots + a_i^{-1} a_{i-1} x_{i-1} + a_i^{-1} a_{i+1} x_{i+1} + \dots + a_i^{-1} a_n x_n.$$

Fordítva, ha $x_i = b_1 x_1 + \dots + b_{i-1} x_{i-1} + b_{i+1} x_{i+1} + \dots + b_n x_n$, akkor

$$b_1 x_1 + \dots + b_{i-1} x_{i-1} + (-1) x_i + b_{i+1} x_{i+1} + \dots + b_n x_n = 0,$$

és $-1 \neq 0$.

c) Feltételezhetjük, hogy $V \neq \{0\}$, és hogy az $X = \{x_1, \dots, x_n\}$ generátorrendszerben minden vektor nemnulla. n szerinti indukciót alkalmazunk.

Ha $n = 1$, akkor $X = \{x_1\}$ generátorrendszer, és a)-szerint lineárisan független, mert $x_1 \neq 0$.

Feltételezzük, hogy $n \geq 1$ és hogy az állítás igaz $n-1$-re, és legyen $X = \{x_1, \dots, x_n\}$ generátorrendszer. Két eset van:

(i) Ha létezik $i \in \{1, \dots, n\}$ úgy, hogy x_i lineáris kombinációja a többi vektornak, akkor b) szerint, $X' = X \setminus \{x_i\}$ generátorrendszer. Mivel X'-nek $n - 1$ eleme van, X'-ből kiválasztható egy bázis, tehát X-ből is kiválasztható.

(ii) Ellenkező esetben b)-ből következik, hogy X lineárisan független, tehát X bázis. ∎

Feladat 81 Igazoljuk, hogy a következő rendszerek lineárisan függetlenek $\mathbb{R}^{\mathbb{R}}$-ben:

a) $\sin \lambda_1 t, , \dots, \sin \lambda_n t$, ahol $\lambda_1, \dots, \lambda_n \in \mathbb{R}_+^*$ különböző számok.

b) $1, \sin t, \dots, \sin nt, \cos t, \dots, \cos nt$, ahol $n \in \mathbb{N}^*$.

Feladat 82 Legyen $(S, \cdot)$ egy monoid, $\sigma_i : (S, \cdot) \to (K^*, \cdot)$ különböző homomorfizmusok, $i = 1, \dots, n$. Igazoljuk, hogy $\sigma_1, \dots, \sigma_n$ lineárisan függetlenek K^S-ben.

2.6 Vektorterek univerzális tulajdonsága

Tétel 2.10 *Legyenek U és V K-lineáris terek, $X = \{x_1, \dots, x_n\}$ bázisa U-nak, és $f : X \to V$ egy függvény. Ekkor létezik egyetlen $\bar{f} : U \to V$ lineáris függvény úgy, hogy az $\bar{f}$ leszükítése X-re megeggyezik f-el.*

Bizonyítás. Tételezzük fel, hogy $\bar{f}$ létezik. Ha $x \in U$, akkor léteznek az egyértelműen meghatárrozott $a_1, \dots a_n \in K$ skalárok úgy, hogy $x = a_1 x_1 + \dots + a_n x_n$ Ekkor

$$\bar{f}(x) = \bar{f}(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} a_i \bar{f}(x_i) = \sum_{i=1}^{n} a_i f(x_i),$$

tehát $\bar{f}$ egyértelműen van meghatározva.

Legyen most $\bar{f}: U \to V$, $\bar{f}(x) = \sum_{i=1}^{n} a_i f(x_i)$ ahol $x = a_1x_1 + \cdots + a_nx_n \in V$. Igazoljuk, hogy $\bar{f}$ lineáris és $\bar{f}_{|X} = f$. Valóban, ha $x' = a'_1x_1 + \cdots + a'_nx_n \in V$ és $a \in K$, akkor

$$\bar{f}(x + x') = \bar{f}(\sum_{i=1}^{n}(a_i + a'_i)x_i) = \sum_{i=1}^{n}(a_i + a'_i)f(x_i) =$$
$$= \sum_{i=1}^{n} a_i f(x_i) + \sum_{i=1}^{n} a'_i f(x_i) = \bar{f}(x) + \bar{f}(x'),$$
$$\bar{f}(ax) = \bar{f}(a\sum_{i=1}^{n} a_i x_i) = \bar{f}(\sum_{i=1}^{n} aa_i x_i) =$$
$$= \sum_{i=1}^{n} aa_i f(x_i) = a(\sum_{i=1}^{n} a_i f(x_i)) = a\bar{f}(x).$$

Ha $x_i \in X$, akkor $x_i = 1 \cdot x_i$, tehát $\bar{f}(x_i) = 1 \cdot f(x_i) = f(x_i)$. ■

Lemma 2.11 *Legyen $f: V \to V'$ egy K-lineáris függvény és $X = \{x_1, \ldots, x_n\} \subseteq V$.*
a) *Ha X lineárisan független és f injektív, akkor $f(X) = \{f(x_1), \ldots, f(x_n)\}$ is lineárisan független.*
b) *Ha $\langle X\rangle = V$ és f szürjektív, akkor $\langle f(X)\rangle = V'$*
c) *Ha X bázis és $f(X)$ független, akkor f injektív.*
d) *Ha $\langle f(X)\rangle = V'$, akkor f szürjektív.*
e) *f akkor és csak akkor izomorfizmus, ha minden bázist egy bázisba visz át.*

Bizonyítás. a) Legyen $a_1, \ldots, a_n \in K$ úgy, hogy $\sum_{i=1}^{n} a_i f(x_i) = 0$; következik, hogy $f(\sum_{i=1}^{n} a_i x_i) = 0$, tehát $\sum_{i=1}^{n} a_i x_i = 0$, mivel f injektív, és $a_1 = \cdots = a_n = 0$ mivel X lineárisan független.

b) Ha $x' \in V'$, akkor létezik $x \in V$ úgy, hogy $f(x) = x'$. Mivel $\langle X\rangle = V$, létezik $a_1, \ldots, a_n \in K$ úgy, hogy $x = \sum_{i=1}^{n} a_i x_i$, es ekkor

$$x' = f(x) = f(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} a_i f(x_i) \in \langle f(X)\rangle,$$

tehát $\langle f(X)\rangle = V'$.

c) Legyen $x \in V$ és tételezzük fel, hogy $f(x) = 0$. Mivel X bázis, léteznek az $a_1, \ldots, a_n \in K$ skalárok úgy, hogy $x = \sum_{i=1}^{n} a_i x_i$. Mivel $0 = f(x) = \sum_{i=1}^{n} a_i f(x_i)$ és $f(X)$ független, következik, hogy $a_1 = \cdots = a_n = 0$, tehát $x = 0$, és f injektív.

d) Legyen $x' \in V'$. Mivel $\langle f(X)\rangle = V'$, következik, hogy léteznek az $a_1, \ldots, a_n \in K$ skalárok úgy, hogy $x' = \sum_{i=1}^{n} a_i f(x_i)$, tehát $x' = f(\sum_{i=1}^{n} a_i x_i)$ és f szürjektív.

e) az a), b), c) és d) pontokbol következik. ■

Következmény 2.12 *Ha V-nek van egy n-elemű X bázisa, akkor $V \simeq K^n$.*

Bizonyítás. Legyen $e = \{e_1, \ldots, e_n\}$ a K^n kanonikus bázisa, és legyen $f: X \to K^n$, $f(x_i) = e_i$, $i = 1, \ldots, n$. Ekkor $\bar{f}$ izomorfizmus. ■

2.7 Steinitz-tétel. Vektortér dimenziója

Tétel 2.13 *Legyen V egy K-feletti vektortér, $r, n \in \mathbb{N}^*$, $\{x_1, \ldots, x_r\}$ egy lineárisan független rendszer és legyen $\{y_1, \ldots, y_n\}$ egy generátorrendszer. Ekkor $r \leq n$, és az $y_1, \ldots, y_n$ vektorok közül r vektor kicserélhető az $x_1, \ldots, x_r$ vektorokkal úgy, hogy*

$$\langle x_1, \ldots, x_r, y_{r+1}, \ldots, y_n\rangle = V.$$

Bizonyítás. r szerinti indukciót alkalmazunk. Ha $r = 1$, akkor $r \leq n$. Legyen $a_1, \ldots, a_n \in K$ úgy, hogy $x_1 = a_1y_1 + \cdots + a_ny_n$. Mivel $x_1 \neq 0$, létezik i úgy, hogy $a_i \neq 0$; feltételezhetjük, hogy $a_1 \neq 0$. Ekkor

$$y_1 = a_1^{-1}x_1 - a_1^{-1}a_2y_2 - \cdots - a_1^{-1}a_ny_n$$

és $V = \langle y_1, y_2 \ldots, y_n\rangle = \langle x_1, y_2 \ldots, y_n\rangle$.

Feltételezzük, hogy az állítás igaz $(r-1)$-re és legyen $\{x_1, \ldots, x_r\}$ egy lineárisan független rendszer. Akkor $\{x_1, \ldots, x_{r-1}\}$ is lineárisan független. Az indukció hipotézisából következik, hogy $r - 1 \leq n$ és

$$V = \langle y_1, y_2 \ldots, y_n\rangle = \langle x_1, \ldots x_{r-1}, y_r \ldots, y_n\rangle.$$

Ha $r - 1 = n$, akkor $V = \langle x_1, \ldots, x_{r-1}\rangle$ és x_r függ $x_1, \ldots, x_r$-től, ellentmondás, tehát $r - 1 < n$ és $r \leq n$. Mivel $x_r \in V = \langle x_1, \ldots x_{r-1}, y_r \ldots, y_n\rangle$, következik, hogy

$$x_r = b_1x_1 + \cdots + b_{r-1}x_{r-1} + b_ry_r + \cdots + b_ny_n.$$

Mivel $x_1, \dots, x_r$ függetlenek, létezik i, $r \le i \le n$ úgy, hogy $b_i \neq 0$; feltételezhetjük, hogy $b_r \neq 0$. Ekkor

$$y_r = -a_r^{-1}b_1x_1 - \cdots - a_r^{-1}b_{r-1}x_{r-1} + a_r^{-1}x_r - a_r^{-1}b_{r+1}y_{r+1} - \cdots - a_r^{-1}b_ny_n,$$

tehát $V = \langle y_1, y_2 \dots, y_n\rangle = \langle x_1, \dots x_r, y_{r+1} \dots, y_n\rangle$. ■

Következmény 2.14 a) *Ha* $B, B' \subseteq V$ *bázisok és* B *véges, akkor* B' *is véges és* $|B| = |B'|$.
b) V*-nek van egy* n*-elemű bázisa akkor és csakis akkor ha* $V \simeq K^n$.

Megjegyzés 2.15 Általában igaz, hogy ha $B, B' \subseteq V$ bázisok, akkor $|B| = |B'|$.

Értelmezés 2.16 Ha V-nek van egy n-elemű bázisa, akkor minden bázisának n eleme van. A bázis számosságát a V (K-feletti) *dimenziójának* nevezzük. Jelölés: $\dim_K V = n$.
Jegyezzük meg, hogy ha $\dim_K V = \dim_K V'$, akkor $V \simeq V'$.

Következmény 2.17 (alternatíva tételek) *Feltételezzük, hogy* $\dim_K V = n$.
a) *Ha* $B \subseteq V$ *és* $|B| = n$*, akkor a következő állítások ekvivalensek:*

1. B *bázis*
2. B *lineárisan független.*
3. B *generátorrendszer.*

b) *Ha* $f \in \mathrm{End}_K(V)$ *a következő állítások ekvivalensek:*

1. f *izomorfizmus*
2. f *injektív.*
3. f *szürjektív.*

Bizonyítás. a) Ha B független, akkor a Steinitz-tételből következik, hogy $|B| \le \dim_K V$ és létezik egy bázis amely tartalmazza B-t. Mivel $|B| = n = \dim_K V$, következik, hogy B bázis.
Ha $\langle B\rangle = V$, akkor létezik egy B' bázis úgy, hogy $B' \subseteq B$. Mivel $|B'| = n$, következik, hogy $B' = B$, tehát B bázis.
b) Legyen B egy bázis. Ha f injektív, $|f(B)| = n$ és 2.11.a) szerint $f(B)$ független; a)-ból következik, hogy $f(B)$ bázis, es 2.11.d)-ből következik, hogy f szürjektív.
Ha f szürjektív, akkor 2.11.b) szerint $\langle f(B)\rangle = V$, és a) szerint $f(B)$ bázisa V-nek, tehát lineárisan független. 2.11.c)-ből következik, hogy f injektív. ■

Feladat 83 a) Ha I véges halmaz, akkor $\dim_K K^I = |I|$.
b) $\dim_K M_{m,n}(K) = mn$.
c) $\dim_{\mathbb{R}} \mathcal{S}_n(\mathbb{R}) = \frac{n(n+1)}{2}$; $\dim_{\mathbb{R}} \mathcal{A}_n(\mathbb{R}) = \frac{n(n-1)}{2}$;

Feladat 84 Ha $\dim_K U = m$ és $\dim_K V = n$, akkor $\dim_K U \times V = m + n$.

Feladat 85 Legyen $f : U \to V$ egy K-homomorfizmus. Igazoljuk, hogy:
a) f akkor és csak akkor injektív, ha létezik $g \in \mathrm{Hom}_K(V, U)$ úgy, hogy $g \circ f = 1_U$.
b) f akkor és csak akkor szürjektív, ha létezik $g \in \mathrm{Hom}_K(V, U)$ úgy, hogy $f \circ g = 1_V$.

2.8 Dimenzióra vonatkozó képletek

Tétel 2.18 *Legyenek* V *és* V' K*-feletti vektorterek és* $f : V \to V'$ *egy lineáris függvény. Ekkor*

$$\dim_K V = \dim_K \mathrm{Ker}\, f + \dim_K \mathrm{Im}\, f.$$

Bizonyítás. Legyen $\{x_1, \dots, x_r\} \subset V$ bázisa $\mathrm{Ker}\, f$-nek, és legyen $\{x'_{r+1}, \dots, x'_n\} \subset V'$ bázisa $\mathrm{Im}\, f$-nek. Ekkor léteznek az $x_{r+1}, \dots, x_n \in V$ vektorok úgy, hogy $f(x_i) = x'_i$, $i = r+1, \dots, n$, és elég igazolni, hogy $\{x_1, \dots, x_r, x_{r+1}, \dots, x_n\}$ bázisa V-nek.

Feltételezzük, hogy $\sum_{i=1}^{n} a_i x_i = 0$. Ekkor

$$\begin{aligned} 0 = f(\sum_{i=1}^{n} a_i x_i) &= \sum_{i=1}^{n} a_i f(x_i) \\ &= \sum_{i=1}^{r} a_i f(x_i) + \sum_{i=r+1}^{n} a_i f(x_i) \\ &= \sum_{i=r+1}^{n} a_i x_i'; \end{aligned}$$

következik, hogy $a_{r+1} = \cdots = a_n = 0$, $\sum_{i=1}^{r} a_i x_i = 0$, és végül, $a_1 = \cdots = a_r = 0$, tehát $\{x_1, \ldots, x_r, x_{r+1}, \ldots, x_n\}$ lineárisan független rendszer.

Ha $x' = f(x) \in \operatorname{Im} f$, akkor léteznek az $a_{r+1}, \ldots, a_n \in K$ skalárok úgy, hogy

$$f(x) = x' = \sum_{i=r+1}^{n} a_i x_i' = \sum_{i=r+1}^{n} a_i f(x_i) = f(\sum_{i=r+1}^{n} a_i x_i);$$

következik, hogy $f(x - \sum_{i=r+1}^{n} a_i x_i) = 0$, és legyen $y = x - \sum_{i=r+1}^{n} a_i x_i$. Mivel $y \in \operatorname{Ker} f$, léteznek az $a_1, \ldots, a_r \in K$ skalárok úgy, hogy $y = \sum_{i=1}^{r} a_i x_i$, tehát

$$x = y + \sum_{i=r+1}^{n} a_i x_i = \sum_{i=1}^{n} a_i x_i \in \langle x_1, \ldots, x_n \rangle. \blacksquare$$

Tétel 2.19 *Legyen egy V K-feletti vektortér és $U, W \leq_K V$. Ekkor*

$$\dim_K(U + W) = \dim_K U + \dim_K W - \dim_K(U \cap W).$$

Bizonyítás. Tekintsük az $U \times W = \{(u, w) \mid u \in U,\ w \in W\}$ vektorteret. Könnyű igazolni hogy, ha $\{u_1, \ldots, u_n\}$ bázisa U-nak és $\{w_1, \ldots, w_m\}$ bázisa W-nek, akkor

$$\{(u_1, 0), \ldots, (u_n, 0), (0, w_1), \ldots, (0, w_m)\}$$

bázisa $U \times W$-nek, tehát $\dim_K(U \times W) = n + m$.

Legyen $f : U \times W \to U + W,\ f(u, w) = u + w$; ekkor f lineáris, szürjektív (azaz $\operatorname{Im} f = U + W$), és

$$\begin{aligned} \operatorname{Ker} f &= \{(u, w) \in U \times W \mid f(u, w) = 0\} \\ &= \{(u, w) \in U \times W \mid u + w = 0\} \\ &= \{(u, -u) \in U \times W \mid u \in U \cap W\}. \end{aligned}$$

Mivel $g : U \cap W \to \operatorname{Ker} f,\ g(u) = (u, -u)$ izomorfizmus, következik, hogy $\dim_K \operatorname{Ker} f = \dim_K(U \cap W)$, és végül,

$$\begin{aligned} \dim_K U + \dim_K W &= \dim_K(U \times W) \\ &= \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f \\ &= \dim_K(U \cap W) + \dim_K(U + W). \blacksquare \end{aligned}$$

Feladat 86 Legyen V egy K-feletti vektortér, $\dim_K V = n,\ S, T \leq_K V$. Igazoljuk, hogy:
a) Ha $\dim_K S = n - 1$ és $T \not\subseteq S$, akkor $S + T = V$ és $\dim_K(S \cap T) = \dim_K T - 1$.
b) Ha $\dim_K(S + T) = \dim_K(S \cap T) + 1$, akkor $S \subseteq T$ vagy $T \subseteq S$.

Feladat 87 Legyen $\dim_K V = n$ és $f, g \in \operatorname{End}_K(V)$. Igazoljuk, hogy, ha $f \circ g = \theta$ és $f + g \in \operatorname{Aut}_K(V)$, akkor $\dim_K \operatorname{Im} f + \dim_K \operatorname{Im} g = n$.

Feladat 88 (Sylvester) Legyenek $f : U \to V,\ g : V \to W$ K-homomorfizmusok, $\dim_K U = m,\ \dim_K V = n,\ \dim_K W = p$. Igazoljuk, hogy $\dim_K \operatorname{Ker}(g \circ f) \leq \dim_K \operatorname{Ker} f + \dim_K \operatorname{Ker} g$.

2.9 Megoldott feladatok

1) Legyen $n \in \mathbb{N}$ és $f_n : \mathbb{R} \to \mathbb{R}$, $f_n(x) = \sin^n x$. Igazoljuk, hogy az $L = \{f_n \mid n \in \mathbb{N}\}$ halmaz vektorai lineárisan függetlenek az $\mathbb{R}$ fölötti $\mathbb{R}^{\mathbb{R}}$ vektortérben.

Megoldás: Legyenek $n_1, \dots, n_k \in \mathbb{N}$ különböző természetes számok és $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ úgy, hogy $\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k} = \theta$ (ahol θ a konstans nulla függvény). Következik, hogy

$$\forall x \in \mathbb{R},\ \alpha_1 \sin^{n_1} x + \dots + \alpha_k \sin^{n_k} x = 0,$$

ahonnan a

$$p = \alpha_1 X^{n_1} + \dots + \alpha_k X^{n_k} \in \mathbb{R}[X]$$

polinomnak bármely $t(= \sin x) \in [-1, 1]$ érték gyöke, vagyis végtelen sok gyöke van. Ez azt jelenti, hogy $p = 0$, tehát $\alpha_1 = \dots = \alpha_k = 0$.

2) Legyen $p \in \mathbb{N}$ egy prím. Igazoljuk, hogy a szokásos összeadás és szorzás műveletek vektortér struktúrát adnak a $V = \{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$ halmaznak $\mathbb{Q}$ fölött. Adjunk egy bázist ebben a vektortérben és határozzuk meg a dimenzióját.

Megoldás: V a ${}_{\mathbb{Q}}\mathbb{R}$ vektortérnek egy $\{1, \sqrt[3]{p}, \sqrt[3]{p^2}\}$ által generált résztere. Kimutatjuk, hogy $1, \sqrt[3]{p}, \sqrt[3]{p^2}$ lineárisan függetlenek. Ha $a, b, c \in \mathbb{Q}$ és $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$ akkor beszorozhatunk $\sqrt[3]{p}$-vel és kapjuk, hogy $a\sqrt[3]{p} + b\sqrt[3]{p^2} + cp = 0$. Kiejtjük a $\sqrt[3]{p^2}$ tagot a két egyenlőségből és következik, hogy $(ab - c^2p) + (b^2 - ac)\sqrt[3]{p} = 0$, ahonnan a $\sqrt[3]{p} \notin \mathbb{Q}$ alapján felírható, hogy $ab - c^2p = 0 = b^2 - ac$. Ha feltételezzük, hogy $a \neq 0$, akkor $c = \dfrac{b^2}{a}$ és $ab - \dfrac{b^4}{a^2}\sqrt[3]{p} = 0$, vagyis $\sqrt[3]{p} = \dfrac{b^3}{a^3}$. Ebből az következik, hogy $\sqrt[3]{p} = \dfrac{b}{a} \in \mathbb{Q}$, ami ellentmond annak, hogy $\sqrt[3]{p} \notin \mathbb{Q}$. Tehát $a = 0$, amiből következik az is, hogy $b = c = 0$.

3) Legyen V egy 3 dimenziós vektortér K fölött és V_1, V_2 két kölönböző, 2 dimenziós résztér. Igazoljuk, hogy $V_1 \cap V_2$-nek a dimenziója 1. Mi a mértani értelmezése a $K = \mathbb{R}$, $V = \mathbb{R}^3$ esetnek?

Megoldás: $V_1 \neq V_2$ és $\dim V_1 = \dim V_2$ összefüggésekből következik, hogy $V_2 \nsubseteq V_1$. Tehát

$$V_1 \subsetneqq V_1 + V_2 \subseteq V,$$

ahonnan $\dim(V_1 + V_2) = 3$ és

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = 1.$$

$\mathbb{R}^3$-ban a mértani értelmezés az, hogy két, origón átmenő, különböző sík metszete egy origón átmenő egyenes.

4) Legyen V egy $n \in \mathbb{N}^*$ dimenziós vektortér K fölött és V_1, V_2 részterei V-nek. Igazoljuk, hogy ha $\dim V_1 = n-1$ és $V_2 \nsubseteq V_1$, akkor

$$\dim(V_1 \cap V_2) = \dim V_2 - 1 \text{şi} V_1 + V_2 = V.$$

Megoldás: Mivel $V_2 \nsubseteq V_1$, következik, hogy $V_1 \cap V_2 \subsetneqq V_2$, tehát $\dim(V_1 \cap V_2) < \dim V_2$, vagyis $\dim V_2 - \dim(V_1 \cap V_2) \geq 1$. Akkor

$$n = \dim V \geq \dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2) \geq n - 1 + 1 = n.$$

Így tehát $\dim(V_1 + V_2) = n = \dim V$ ahonnan $V = V_1 + V_2$. Ebből rögtön felírható, hogy

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = n - 1 + \dim V_2 - n = \dim V_2 - 1.$$

3 Lineáris függvények és mátrixok, lineáris egyenletrendszerek

3.1 Lineáris függvény mátrixa

Legyen $u = (u_1, \dots, u_n)$ U-nak egy bázisa és $v = (v_1, \dots, v_m)$ V-nek egy bázisa. (Figyelembe vesszük az elemek sorrendjét, azaz rendezett bázisokat tekintünk.)

Ha $x \in U$, akkor léteznek az egyértelműen meghatározott $x_1, \dots, x_n \in R$ skalárok, úgy, hogy $x = \sum_{i=1}^{n} x_i u_i$. Azt mondjuk, hogy $(x_1, \dots, x_n)$ az x vektor az u bázisra vonatkozó *koordinátavektora*, és legyen

$$M_u(x) = [x]_u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$$

az x vektor az u *bázisra vonatkozó mátrixa.*

Feladat 89 Igazoljuk, hogy:
a) $M_u : U \to M_{n,1}(K)$, $M_u(x) = [x]_u$ K-izomorfizmus;
b) $M_{n,1}(K) \simeq K^n$.

Legyen $f : U \to V$ egy lineáris függvény. A vektorterek univerzális tulajdonságából következik, hogy az $f(u_1), \dots, f(u_n) \in V$ elemek meghatározzák f-et. Legyen

$$f(u_j) = \sum_{i=1}^{m} a_{ij} v_i, \quad 1 \le j \le n.$$

Az $a_{ij} \in K$ skalárok egyértelműen meghatározottak, és legyen

$$M_{uv}(f) = [f]_{uv} = [a_{ij}]_{\substack{1 \le i \le m \\ 1 \le j \le n}} \in M_{m,n}(K)$$

az f függvény az (u, v) *bázispárra vonatkozó mátrixa.* Vegyük észre, hogy $[f(u_j)]_v$ egyenlő az $[f]_{uv}$ mátrix j-edik oszlopával.

Ha $A \in M_{m,n}(K)$, a következő jelöléseket fogjuk használni:
- o_j^A = az A mátrix j-edik oszlopa.
- s_i^A = az A mátrix i-edik sora.

Tétel 3.1 *Legyenek U,V és W vektorterek $u = (u_1, \dots, u_n)$, $v = (v_1, \dots, v_m)$ illetve $w = (w_1, \dots, w_p)$ bázisokkal. Továbbá, legyenek $f, f' \in \mathrm{Hom}_K(U, V)$ és $g \in \mathrm{Hom}_K(V, W)$.*
a) $[f(x)]_v = [f]_{uv}[x]_u$, *minden $x \in U$ esetén.*
b) $[f + f']_{uv} = [f]_{uv} + [f']_{uv}$
c) $[af]_{uv} = a[f]_{uv}$, *minden $a \in K$ esetén.*
d) $[g \circ f]_{uw} = [g]_{vw} \cdot [f]_{uv}$.

Bizonyítás. a) Legyen $y = f(x) = \sum_{i=1}^{m} y_i v_i$, tehát

$$[y]_v = [f(x)]_v = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Ekkor

$$\sum_{i=1}^{m} y_i v_i = y = f(x) = f(\sum_{j=1}^{n} x_j u_j) = \sum_{j=1}^{n} x_j f(u_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} a_{ij} x_j) v_i.$$

Mivel $\{v_1, \dots, v_m\}$ bázis, következik, hogy

$$y_i = \sum_{j=1}^{n} a_{ij} x_j, \quad 1 \le i \le m,$$

vagy mátrixokkal,

$$[f(x)]_v = [f]_{uv}[x]_u.$$

b) Ki kell számítani az $(f+f')(u_j)$ koordinátáit, ha $1 \le j \le n$:

$$(f+f')(u_j) = f(u_j) + f'(u_j) = \sum_{i=1}^{m} a_{ij}v_i + \sum_{i=1}^{m} a'_{ij}v_i = \sum_{i=1}^{m} (a_{ij} + a'_{ij})v_i,$$

tehát

$$[f+f']_{uv} = [a_{ij} + a'_{ij}] = [a_{ij}] + [a'_{ij}] = [f]_{uv} + [f']_{uv}.$$

c) Hasonló módon, minden $1 \le j \le n$ esetén,

$$(af)(u_j) = af(u_j) = a(\sum_{i=1}^{m} a_{ij}v_i) = \sum_{i=1}^{m} (aa_{ij})v_i,$$

tehát

$$[af]_{uv} = [aa_{ij}] = a[a_{ij}] = a[f]_{uv}.$$

d) Ha $1 \le j \le n$, legyen

$$(g \circ f)(u_j) = \sum_{k=1}^{p} c_{kj}w_k,$$

azaz

$$[g \circ f]_{u,w} = [c_{kj}]_{\substack{1 \le k \le p \\ 1 \le j \le n}} \in M_{p,n}(K).$$

Megismételve a fenti számításokat,

$$(g \circ f)(u_j) = g(f(u_j)) = g(\sum_{i=1}^{m} a_{ij}v_i) = \sum_{i=1}^{m} a_{ij}g(v_i) = \sum_{i=1}^{m} a_{ij} \sum_{k=1}^{p} b_{ki}w_k = \sum_{k=1}^{p} (\sum_{i=1}^{m} b_{ki}a_{ij})w_k.$$

Mivel $\{w_1, \dots, w_p\}$ W egy bázisa, következik, hogy

$$c_{kj} = \sum_{i=1}^{m} b_{ki}a_{ij}, \quad 1 \le k \le p, \ 1 \le j \le n,$$

és mátrixokkal,

$$[g \circ f]_{uw} = [c_{kj}] = [\sum_{i=1}^{m} b_{ki}a_{ij}] = [g]_{vw} \cdot [f]_{uv}. \qquad \blacksquare$$

Következmény 3.2 $M_{u,v} : \mathrm{Hom}_K(U, V) \to M_{m,n}(K)$ K-*lineáris izomorfizmus.*

Feladat 90 Ha $\dim_K U = m$ és $\dim_K V = n$, akkor $\dim_K \mathrm{Hom}_K(U, V) = mn$.

Feladat 91 Legyen $t \in \mathbb{R}$, $f_t, g_t : \mathbb{R}^2 \to \mathbb{R}^2$, $f_t(x) = (x_1 \cos t - x_2 \sin t, x_1 \sin t + x_2 \cos t)$, $g_t(x) = (x_2 \cos t + x_2 \sin t, x_1 \sin t - x_2 \cos t)$.

a) Igazoljuk, hogy f_t, $g_t \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$.

b) Határozzuk meg az $[f_t]_{e,e}$ és $[g_t]_{e,e}$ mátrixokat, ahol $e = (e_1, e_2)$ a kanonikus bázis.

c) Határozzuk meg az $f_t \circ f_{t'}$, $g_t \circ g_{t'}$, $f_t \circ g_{t'}$, $g_t \circ f_{t'}$ morfizmusok mátrixát.

Feladat 92 Legyen $V = \mathbb{R}_n[X] = \{f \in \mathbb{R}[X] \mid \mathrm{gr}(f) \le n\}$, $a \in \mathbb{R}$, $f \in \mathbb{R}[X]$, és legyen $B = (1, X - a, \dots, (X - a)^n/n!)$.

a) Igazoljuk, hogy B bázisa V-nek.

b) Határozzuk meg az f koordinátáit a B bázisban (*Taylor-képlet*).

c) Legyen $D : V \to V$, $D(f) = f'$. Határozzuk meg a D mátrixát a kanonikus bázisban.

3.2 Báziscsere

Legyen U egy vektortér $u = (u_1, \dots, u_n)$ bázissal. Ha $u' = (u'_1, \dots, u'_n)$ egy elemrendszer, $u'_j \in U$, akkor léteznek az egyértelműen meghatározott $t_{ij} \in K$ skalárok úgy, hogy

$$u'_j = \sum_{i=1}^{n} t_{ij}u_i, \quad 1 \le j \le n,$$

azaz,

$$[u_j']_u = \begin{pmatrix} t_{1j} \\ \vdots \\ t_{nj} \end{pmatrix} = o_j^T,$$

ahol

$$T = T_u^{u'} = [t_{ij}]_{1 \le i,j \le n} \in M_n(K).$$

Azt mondjuk, hogy $T = T_u^{u'}$ *az* u *bázisról az* u' *rendszerre való áttérési mátrix.*

Tétel 3.3 a) $u' = (u_1', \dots, u_n')$ *bázis* $\Leftrightarrow$ $T = T_u^{u'}$ *invertálható mátrix.* (Informálisan, u a ,,régi" bázis és u' az ,,új"bázis.)

b) *Ha* u' *bázis, akkor minden* $x \in U$ *esetén*

$$\boxed{[x]_{u'} = (T_u^{u'})^{-1}[x]_u}.$$

c) *Legyen* V *egy szabad modulus,* $v = (v_1, \dots, v_m)$ *és* $v' = (v_1', \dots, v_m')$ *két bázisa, és legyen*

$$S = T_v^{v'} = [s_{ij}]_{1 \le i,j \le m} \in M_m(R)$$

az áttérési mátrix, ahol

$$v_j' = \sum_{i=1}^{m} s_{ij} v_i, \quad 1 \le j \le m.$$

Ha $f : U \to V$ *egy lineáris függvény, akkor*

$$\boxed{[f]_{u',v'} = S^{-1}[f]_{u,v}T}.$$

Bizonyítás. a) A vektorterek univerzális tulajdonságából következik, hogy létezik egy egyértelműen meghatározott $h : U \to V$ lineáris függvény úgy, hogy $h(u_j) = u_j'$, $1 \le j \le n$, és vegyük észre, hogy $[h]_{u,u} = T$. A 2.11. Lemmából és 3.2.-ből következik, hogy $u' = (h(u_1), \dots, h(u_n))$ bázis $\Leftrightarrow$ h izomorfizmus $\Leftrightarrow$ $T = [h]_{u,u} \in M_n(K)$ invertálható mátrix.

b) Legyen $x = \sum_{i=1}^n x_i u_i = \sum_{j=1}^n x_j' u_j' \in U$. Ekkor

$$x = \sum_{j=1}^{n} x_j' u_j' = \sum_{j=1}^{n} x_j' \sum_{i=1}^{n} t_{ij} u_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} t_{ij} x_j') u_i = \sum_{i=1}^{n} x_i u_i.$$

Mivel $u = \{u_1, \dots, u_n\}$ bázis, következik, hogy

$$x_i = \sum_{j=1}^{n} t_{ij} x_j', \quad 1 \le i \le n,$$

azaz,

$$[x]_u = T[x]_{u'}.$$

c) Kétféleképpen kiszámítva az $[f(x)]_v$ mátrixot, kapjuk, hogy

$$[f(x)]_v = [f]_{u,v}[x]_u = [f]_{u,v}T[x]_{u'},$$

és

$$[f(x)]_v = S[f(x)]_{v'} = S[f]_{u',v'}[x]_{u'}.$$

Rendre behelyetesítve $[x]_{u'}$-et az $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \in M_{m,1}(R)$ mátrixokkal, következik, hogy $[f]_{u,v}T = S[f]_{u',v'}$, tehát

$$[f]_{u',v'} = S^{-1}[f]_{u,v}T. \qquad \blacksquare$$

3.3 A determináns értelmezése

3.3.1 A. Másod és harmad rendű determinánsok

Legyen K egy kommutatív test és tekintsük a következő egyenletrendszert:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a_{21}x_1 + a_{22}x_2 = b_2. \end{cases}$$

Legyen $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(R)$ az *egyenletrendszer mátrixa* és $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in M_{21}(R)$ a *szabad tagok oszlopmátrixa*.

Alkalmazva a kiküszöbölési módszert, kapjuk, hogy az egyenletrendszer ekvivalens a következő egyenletrendszerrel:

$$\begin{cases} (a_{11}a_{22} - a_{12}a_{21})x_1 = b_1a_{22} - a_{12}b_2 \\ (a_{11}a_{22} - a_{12}a_{21})x_2 = b_2a_{22} - a_{21}b_1. \end{cases}$$

Definíció szerint, legyen

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} \in R$$

as A mátrix *determinánsa*.

Vegyük észre, hogy ha $A_1 = \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}$ és $A_2 = \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}$, akkor

$$x_1 \det A = \det A_1, \quad x_2 \det A = \det A_2.$$

Tekintsük most a következő egyenletrendszert:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3, \end{cases}$$

és legyenek $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, $A_1 = \begin{pmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{pmatrix}$, $A_2 = \begin{pmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{pmatrix}$

és $A_3 = \begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{pmatrix} \in M_3(R)$. Hasonló módon kapjuk a következő ekvivalens egyenletrendszert:

$$x_1 \det A = \det A_1, \quad x_2 \det A = \det A_2. \quad x_3 \det A = \det A_3,$$

ahol definíció szerint,

$$\begin{aligned} \det A &= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} \end{aligned}$$

Feladat 93 Számítsuk ki a következő determinánsokat:

a) $\begin{vmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{vmatrix}$; b) $\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}$; c) $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}$.

3.3.2 B. n-ed rendű determináns

A fenti számításokat folytatni bonyolult lenne, de szugerálják a következő általánosítást:

Értelmezés 3.4 Ha $A = [a_{ij}] \in M_n(K)$, akkor az A mátrix *determinánsának* nevezzük a következő K-beli elemet:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Az összegnek $n!$ tagja van, és mindegyik szorzat tartalmaz az A mátrix minden sorából és minden oszlopából pontosan egy elemet.

Lemma 3.5 $\det A = \det A^t$.

Bizonyítás. Legyen $A^t = [a_{ij}^t] \in M_n(K)$ az A mátrix transzponáltja, ahol $a_{ij}^t = a_{ji}$, $1 \le i,j \le n$. Ekkor

$$\begin{aligned}\det A^t &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}^t a_{2\sigma(2)}^t \dots a_{n\sigma(n)}^t \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma^{-1}(1)} a_{2\sigma^{-1}(2)} \dots a_{n\sigma^{-1}(n)} \\ &= \sum_{\tau\in S_n} \operatorname{sgn}(\tau) a_{1\tau(1)} a_{2\tau(2)} \dots a_{n\tau(n)} \\ &= \det A.\end{aligned}$$

Az utolsó előtti egyelőségben felhasználtuk az K kommutatívitását és a következő tényeket:
- Az $S_n \to S_n$, $\sigma \mapsto \tau = \sigma^{-1}$ bijektív függvény;
- $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$. ■

3.4 A determináns induktív értelmezése

3.4.1 A. Multilineáris alakok

Legyenek U, V K-lineáris terek és legyen $U^n = U \times \dots \times U$.

Értelmezés 3.6 a) A $\phi : U^n \to V$ függvényt n-*lineárisnak* nevezzük, ha

$$\phi(x_1, \dots, ax_i + a'x_i', \dots, x_n) = a\phi(x_1, \dots, x_i, \dots, x_n) + a'\phi(x_1, \dots, x_i', \dots, x_n)$$

minden $a, a' \in K$ és $x_1, \dots, x_i, x_i', \dots, x_n \in U$ esetén (azaz, ϕ minden változójában lineáris).
Ha $V = K$, akkor ϕ-t *alaknak* nevezzük.
b) Azt mondjuk, hogy $\phi : U^n \to K$ *alternáló alak*, ha

$$x_i = x_{i+1} \;\Rightarrow\; \phi(x_1, \dots, x_i, x_{i+i}, \dots, x_n) = 0$$

minden $i \in \{1, \dots, n-1\}$ esetén.

Példa 3.7 a) Minden $\phi \in \operatorname{Hom}_K(U, V)$ 1-lineáris függvény.
b) Legyen $M = M_{2,1}(K)$, $n = 2$, $x_1 = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}$ és $x_2 = \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}$. Ekkor

$$\phi : M \times M \to K, \quad \phi(x_1, x_2) = a_{11}a_{22} - a_{21}a_{12}$$

2-lineáris alternáló alak.

Lemma 3.8 *Legyen $\phi : U^n \to K$ egy n-lineáris alternáló alak.*
a) *Ha $i < j$, akkor $\phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\phi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$;*
b) *Ha $i \ne j$ és $x_i = x_j$, akkor $\phi(x_1, \dots, x_n) = 0$;*
c) *Ha $i \ne j$ és $a \in K$, akkor $\phi(x_1, \dots, x_i + ax_j, \dots, x_n) = \phi(x_1, \dots, x_i, \dots, x_n)$.*

Bizonyítás. a) Legyen $k = j - i$; k-szerinti indukciót alkalmazunk. Ha $k = 1$, akkor

$$\begin{aligned}\phi(\dots, x_i + x_{i+1}, x_i + x_{i+1}, \dots) &= \phi(\dots, x_i, x_i, \dots) + \phi(\dots, x_i, x_{i+1}, \dots) + \\ &+ \phi(\dots, x_{i+1}, x_i, \dots) + \phi(\dots, x_{i+1}, x_{i+1}, \dots) = \\ &= \phi(\dots, x_i, x_{i+1}, \dots) + \phi(\dots, x_{i+1}, x_i, \dots),\end{aligned}$$

tehát

$$\phi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = -\phi(x_1, \dots, x_{i+1}, x_i, \dots, x_n).$$

Legyen $k > 1$, és feltételezzük, hogy az állítás igaz $k-1$-re. Felcsréljük x_i-t x_{i+k}-val három lépésben: felcseréljük x_i-t x_{i+k-1}-gyel, utánna x_{i+k}-t x_i-vel, és végűl x_{i+k-1}-et x_{i+k}-val. Az indukció hipotézisából és a $k = 1$ esetből következik, hogy ϕ háromszor vált előjelet, tehát

$$\phi(x_1, \dots, x_i, \dots, x_{i+k}, \dots, x_n) = -\phi(x_1, \dots, x_{i+k}, \dots, x_i, \dots, x_n).$$

b) Feltételezhetjük, hogy $k = j - i > 1$; ekkor

$$\phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\phi(x_1, \dots, x_{j-1}, \dots, x_i, x_j, \dots, x_n) = -0 = 0.$$

c) Az $i < j$ esetet vizsgálva,

$$\phi(\dots, x_i + \alpha x_j, \dots, x_j, \dots) = \phi(\dots, x_i, \dots, x_j, \dots) + \alpha\phi(\dots, x_j, \dots, x_j, \dots) = \\ = \phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n). \qquad \blacksquare$$

Lemma 3.9 *Legyen $\phi : U^n \to K$ egy n-lineáris alternáló alak, $A = [a_{ij}] \in M_n(K)$, $x_1, \dots, x_n \in K$, és legyenek*

$$y_j = \sum_{i=1}^{n} a_{ij} x_i, \quad 1 \le j \le n,$$
$$z_i = \sum_{j=1}^{n} a_{ij} x_j, \quad 1 \le i \le n.$$

Ekkor

$$\phi(y_1, \dots, y_n) = \phi(z_1, \dots, z_n) = \det(A)\phi(x_1, \dots, x_n).$$

Bizonyítás. Mivel ϕ n-lineáris, következik, hogy

$$\phi(z_1, \dots, z_n) = \phi(\sum_{j=1}^{n} a_{1j} x_j, \dots, \sum_{j=1}^{n} a_{nj} x_j) = \\ = \sum_{1 \le i_1 \le \dots \le i_n \le n} a_{1 i_1} \dots a_{n i_n} \phi(x_{i_1}, \dots, x_{i_n}).$$

Legyen $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$, $\sigma(k) = i_k$; ha σ injektív, akkor σ bijektív, tehát $\sigma \in S_n$; ha σ nem injektív, akkor $\phi(x_{i_1}, \dots, x_{i_n}) = 0$, mert ϕ alternáló.

Következik, hogy

$$\phi(z_1, \dots, z_n) = \sum_{\sigma \in S_n} a_{1\sigma(1)} \dots a_{n\sigma(n)} \phi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \\ = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} \phi(x_{i_1}, \dots, x_{i_n}) = \\ = \det(A)\phi(x_1, \dots, x_n)$$

Vegyük észre, hogy

$$y_i = \sum_{j=1}^{n} a_{ji} x_j = \sum_{j=1}^{n} a^t_{ij} x_j,$$

tehát a második egyenlőség következik az elsőből, és abból, hogy $\det A = \det A^t$. $\blacksquare$

3.4.2 B. Determinánsok alaptétele

Ha $A = [a_{ij}] \in M_n(K)$, és $M := M_{n,1}(K)$ akkor legyen

- $o_j^A = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \in M$ az A j-edik oszlopa, $1 \le j \le n$;
- $s_i^A = \begin{pmatrix} a_{i1} \dots a_{1n} \end{pmatrix} \in M_{1,n}(K) \simeq M$ az A i-edik sora, $1 \le i \le n$.

Vegyük észre, hogy ha $I = I_n := [\delta_{ij}] \in M_n(K)$ az n-ed rendű egységmátrix, akkor az $(e_1 = o_1^I, \dots, e_n = o_n^I)$ vektorrendszer az M kanonikus bázisa.

Tétel 3.10 *Létezik az egyértelműen meghatározott $\delta_n : M^n \to K$ n-lineáris alternáló alak úgy, hogy*

$$\delta_n(e_1, \dots, e_n) = 1.$$

Minden $A \in M_n(K)$ esetén,

$$\det(A) = \delta_n(o_1^A, \dots, o_n^A).$$

Bizonyítás. Nem bizonyítjuk

Értelmezés 3.11 a) $\det : M_n(K) \to K, \quad A \mapsto \det(A)$ függvényt n-ed *rendű determinánsnak* nevezzük.

b) A $\Gamma_{ij} = (-1)^{i+j} \det(A_{ij}) \in K$ elem az a_{ij} elem *algebrai komplementuma.*

c) Azt mondjuk, hogy a

$$\det(A) = \sum_{j=1}^{n} a_{ij}\Gamma_{ij}$$

képlet az A determinánsának az i-edik *sora szerinti kifejtése*, $1 \le i \le n$.

Következmény 3.12 (Determinánsok alaptulajdonságai) a) *Az* A *determinánsa lineárisan függ az* A *oszlopaitól.*

b) *Ha* A*-nak van két egyenlő oszlopa, akkor* $\det(A) = 0$.

c) *Ha* A *két oszlopát felcseréljük, akkor a determinánsa* (-1)*-szeresére változik.*

d) *Az* A *determinánsa nem változik, ha egy oszlopának skalárszorosát egy másik oszlopához adjuk.*

e) *Mivel* $\det(A) = \det(A^t)$*, a fenti állítások sorokra is igazak.*

f) $\det(A)$ j*-edik oszlopa szerinti kifejtése:*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \quad 1 \le j \le n.$$

Feladat 94 Számítsuk ki a következő determinánsokat:

a) $\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix}$; b) $\begin{vmatrix} a+b & b+c & c+a \\ a^2+b^2 & b^2+c^2 & c^2+a^2 \\ a^3+c^3 & b^3+c^3 & c^3+a^3 \end{vmatrix}$; c) $\begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{vmatrix}$.

Feladat 95 a) Számítsuk ki az $A = (a_{ij}) \in M_n(K)$ determinánsát, ha $a_{ij} = 0,\ i > j$.

b) Számítsuk ki az $A = (a_{ij}) \in M_n(K)$ determinánsát, ha $a_{ij} = 0,\ i + j \le n$.

Feladat 96 Számítsuk ki a következő determinánsokat:

a) $A_n = \begin{vmatrix} a & x & x & \dots & x \\ x & a & x & \dots & x \\ x & x & a & \dots & x \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x & x & x & \dots & a \end{vmatrix}$ b) $D_n = \begin{vmatrix} a & b & 0 & 0 & \dots & 0 & 0 \\ c & a & b & 0 & \dots & 0 & 0 \\ 0 & c & a & b & \dots & 0 & 0 \\ 0 & 0 & c & a & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a & b \\ 0 & 0 & 0 & 0 & \dots & c & a \end{vmatrix}$

c) $B_n = \begin{vmatrix} x & y & y & y & \dots & y & y \\ z & x & y & y & \dots & y & y \\ z & z & x & y & \dots & y & y \\ z & z & z & x & \dots & y & y \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ z & z & z & z & \dots & x & y \\ z & z & z & z & \dots & z & x \end{vmatrix}$ d) $V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{vmatrix}$

e) $S_n = \begin{vmatrix} 0 & a_{12} & a_{13} & \dots & a_{1n} \\ -a_{12} & 0 & a_{23} & \dots & a_{2n} \\ -a_{13} & -a_{23} & 0 & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1n} & -a_{2n} & -a_{3n} & \dots & 0 \end{vmatrix}$ (S_n-nél n páratlan).

Feladat 97 Igazoljuk, hogy:

$$V_n^i(a_1, \dots, a_n) = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \dots & & & \dots & \\ a_1^{i-1} & a_2^{i-1} & a_3^{i-1} & \dots & a_n^{i-1} \\ a_1^{i+1} & a_2^{i+1} & a_3^{i+1} & \dots & a_n^{i+1} \\ \dots & & & \dots & \\ a_1^n & a_2^n & a_3^n & \dots & a_n^n \end{vmatrix} = s_{n-i}(a_1, \dots, a_n) V_n,$$

ahol

$$s_k = X_1 \dots X_k + \dots + X_{n-k+1} \dots X_n$$

a k-adik elemi szimmetrikus polinom és $V_n = V_n(a_1, \dots, a_n)$ a *Vandermonde-determináns.*

3.5 Determinánsok tulajdonságai. Invertálható mátrixok

Tétel 3.13 (Cramer-szabály) *Ha* $A \in M_n(K)$ *és* $b = \sum_{j=1}^n x_j o_j^A \in M_{n,1}(K)$*, akkor*

$$\delta_n(o_1^A, \dots, \underset{i}{b}, \dots, o_n^A) = x_i \det(A).$$

Bizonyítás. Mivel δ_n n-lineáris alternáló, következik, hogy

$$\delta_n(o_1^A, \dots, b, \dots, o_n^A) = \delta_n(o_1^A, \dots, \sum_{j=1}^n x_j o_j^A, \dots, o_n^A) = \sum_{j=1}^n x_j \delta_n(o_1^A, \dots, o_j^A, \dots, o_n^A) =$$
$$= x_i \delta_n(o_1^A, \dots, o_i^A, \dots, o_n^A) = x_i \det(A). \qquad \blacksquare$$

Tétel 3.14 (Determinánsok szorzástétele) *Ha* $A, B \in M_n(K)$*, akkor*

$$\det(AB) = \det(A)\det(B).$$

Bizonyítás. Legyen $(e_1, \dots, e_n)$ az $M = M_{n,1}(K)$ kanonikus bázisa. Az $x_j = \sum_{i=1}^n a_{ij} e_i$, $1 \le j \le n$ összefüggéseket a mátrix formában írva:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Ebben az esetben, a 3.9. Lemmából következik, hogy

$$\delta_n(x_1, \dots, x_n) = \det(A)\delta_n(e_1, \dots, e_n) = \det(A).$$

Vegyük észre, hogy

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} := (AB) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = A(B \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}) \quad \text{és legyen} \quad B \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} =: \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Ekkor

$$\begin{aligned} \det(AB) &= \det(AB)\delta_n(e_1, \dots, e_n) = \delta_n(z_1, \dots, z_n) = \\ &= \det(A)\delta_n(y_1, \dots, y_n) \\ &= \det(A)\det(B)\delta_n(e_1, \dots, e_n) \\ &= \det(A)\det(B). \qquad \blacksquare \end{aligned}$$

Tétel 3.15 (Adjungált mátrix) *Legyen* $A = [a_{ij}] \in M_n(K)$ *és legyen* $\tilde{A} = [\tilde{a}_{ij}] \in M_n(K)$*, ahol*

$$\tilde{a}_{ij} = \Gamma_{ji} = (-1)^{i+j} \det A_{ji}.$$

$\tilde{A}$*-t az* A *adjungáltjának nevezzük, és fennáll a következő egyenlőség:*

$$A\tilde{A} = \tilde{A}A = \det(A) \cdot I_n.$$

Bizonyítás. Mivel $A\tilde{A} = [\sum_{k=1}^n a_{ik}\tilde{a}_{kj}]_{1 \le i,j \le n}$ és $\tilde{A}A = [\sum_{k=1}^n \tilde{a}_{ik}a_{kj}]_{1 \le i,j \le n}$, igazolni kell, hogy

$$\sum_{k=1}^n a_{ik}\Gamma_{jk} = \delta_{ij}\det(A) \quad \text{és} \quad \sum_{k=1}^n a_{kj}\Gamma_{ki} = \delta_{ij}\det(A),$$

ahol δ_{ij} a Kronecker szimbólum.

Bizonyítsuk be az első egyenlőséget. Ha $i = j$, akkor valóban $\sum_{k=1}^n a_{ik}\Gamma_{ik} = \det(A)$ (i-edik sor szerinti kifejtés). Feltételezzük, hogy $i \ne j$ és legyen $A' = [a'_{ij}] \in M_n(K)$ úgy, hogy $s_l^{A'} = s_l^A$ ha $j \ne i$, és $s_i^{A'} = s_j^A$. Mivel A'-nek van két egyenlő sora, következik, hogy

$$0 = \det A' = \sum_{k=1}^n a'_{ik}\Gamma'_{ik} = \sum_{k=1}^n a_{jk}\Gamma_{ik}. \qquad \blacksquare$$

Feladat 98 Ha $A \in T_n(K)$ akkor $\tilde{A} = (\Gamma_{ji}) \in T_n(K)$.

Tétel 3.16 (Invertáható mátrixok) *Ha* $A = [a_{ij}] \in M_n(K)$*, akkor a következő állítások ekvivalensek:*
(i) A *invertáható mátrix.*
(ii) $\det(A) \in K$ *invertálható elem.*
(iii) $(o_1^A, \dots, o_n^A)$ *bázisa* M*-nek.*
(iv) $(s_1^A, \dots, s_n^A)$ *bázisa* $M_{1,n}(K)$*-nek.*

Bizonyítás. „(i)⇒(ii)" Ha létezik $B \in M_n(K)$ úgy, hogy $AB = BA = I_n$, akkor $\det(A)\det(B) = \det(I_n) = 1$, tehát $\det(A) \in U(K)$.

„(ii)⇒(i)" Ha $\det(A) \in U(K)$, akkor az előző tételből következik, hogy $A^{-1} = \det(A)^{-1}\tilde{A}$.

„(i)⇔(iii)" Létezik az egyértelműen meghatározott $f : M \to M$ lineáris függvény úgy, hogy $f(e_j) = o_j^A$, $1 \le j \le n$. Mivel $o_j^A = \sum_{i=1}^n a_{ij}e_i$, következik, hogy $[f]_{e,e} = A$. Ekkor 2.11. és 3.2.-ből következik, hogy A invertáható ⇔ f izomorfizmus ⇔ $(f(e_1), \dots, f(e_n))$ bázis ⇔ $(o_1^A, \dots, o_n^A)$ bázis. ■

Jegyezzük meg, hogy ha $\det(A) \in U(K)$, akkor

$$A^{-1} = \det(A)^{-1}\tilde{A} \quad \text{és} \quad \det(A^{-1}) = \det(A)^{-1}.$$

Az invertalható mátrixok halmazát $GL_n(K)$-el jelöljuk. Mivel $GL_n(K)$ az $(M_n(K), +, \cdot)$ gyűrű invertálható elemeinek a halmaza, következik, hogy $(GL_n(K), \cdot)$ csoport. Ezt a csoportot az *általános lineáris csoport*nak nevezzük. A fentiekből következik, hogy a

$$\det : GL_n(K) \to U(K), \qquad A \mapsto \det(A)$$

függvény csoportmorfizmus.

Feladat 99 Igazoljuk, hogy $SL_n(K) := \{A \in GL_n(K) \mid \det A = 1\}$ részcsoportja $(GL_n(K), \cdot)$-nak. ($SL_n(K)$-t a *speciális lineáris csoport*nak nevezzük.)

Feladat 100 Igazoljuk, hogy $GL_n(\mathbb{Q})$-nak van egy S_n-nel izomorf részcsoportja.

Feladat 101 (Ortogonális és unitér csoportok) Legyen $n \in \mathbb{N}^*$,

$$O(n) := \{A \in M_n(K) \mid A \cdot A^t = I_n\}$$

az *ortogonális* mátrixok halmaza és

$$U(n) := \{A \in M_n(\mathbb{C}) \mid A \cdot A^h = I_n\}$$

az *unitér* mátrixok halmaza, ahol: $A^h := \bar{A}^t$, $\bar{A} := [\bar{a}_{ij}]_{1 \le i,j \le n}$. Igazoljuk, hogy:
a) Ha $A \in O(n)$, akkor $A^tA = I_n$ és $\det A = \pm 1$.
b) Ha $A \in U(n)$, akkor $A^hA = I_n$ és $|\det A| = 1$.
c) $SO(n) \le O(n) \le GL_n(\mathbb{R})$, ahol $SO(n) := \{A \in O(n) \mid \det A = 1\}$ a *speciális ortogonális csoport.*
d) $SU(n) \le U(n) \le GL_n(\mathbb{C})$, ahol $SU(n) := \{A \in U(n) \mid \det A = 1\}$ a *speciális unitér csoport.*
e) $O(2) = \left\{ \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}, \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix} \mid t \in [0, 2\pi) \right\}$.

Feladat 102 (Blokkmátrix inverze) Legyen K egy kommutatív test, legyen

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \in M_n(K),$$

ahol $A_{11} \in M_p(K), A_{22} \in M_q(K)$, $p + q = n$, és feltételezzük, hogy A_{22} invertálható. Igazoljuk, hogy A invertálható akkor és csak akkor ha $A_{11} - A_{12}A_{22}^{-1}A_{21} \in M_p(K)$ invertálható. Ebben az esetben, fejezzük ki az A inverzét A_{22}^{-1} és $(A_{11} - A_{12}A_{22}^{-1}A_{21})^{-1}$ segítségével.

Alkalmazás. Számítsuk ki az $A = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 4 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in M_n(\mathbb{Q})$ mátrix inverzét.

Feladat 103 Számítsuk ki az $A \in M_n(K)$ inverzét, ahol

$$A = \begin{pmatrix} 1+a_1 & 1 & \dots & 1 \\ 1 & 1+a_2 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1+a_n \end{pmatrix}.$$

Feladat 104 (Gauss-szám) Feltételezzük, hogy $|K| = q$, és legyen

$$G_n^k(q) = |\{U \leq_K K^n \mid \dim_K U = k\}|.$$

Igazoljuk, hogy:

a) $|GL_n(K)| = (q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})$.
b) $G_n^0(q) = G_n^n(q) = 1$.
c) $G_n^k(q) = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$, $k = 1, \dots, n-1$.
d) $G_n^k(q) = G_n^{n-k}(q)$.
e) $G_n^k(q) = q^n G_{n-1}^k(q) + G_{n-1}^{k-1}(q)$, $k = 1, \dots, n-1$.
f) Hány rendezett bázisa és hány bázisa van a K^n vektortérnek?

Legyen $\det(A)$ egy n-ed rendű determináns, $1 \leq i_1 < \dots < i_r \leq n$, $1 \leq j_1 < \dots < j_r \leq n$ és $D_{i_1\dots i_r}^{j_1\dots j_r}$ az a minor (aldeterminány), amelyet a $\det(A)$ $i_1, \dots, i_r$ sorainak és $j_1, \dots, j_r$ oszlopainak a kiválasztásával kapunk. Jelöljük $\tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}$-el a $D_{i_1\dots i_r}^{j_1\dots j_r}$ *kiegészítő aldeterminánsát* (amelyet a megmaradt sorok és oszlopok természetes sorrendbeli kiválasztásával kapunk). Végül, $(-1)^{i_1+\dots+i_r+j_1+\dots+j_r}\tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}$ a $D_{i_1\dots i_r}^{j_1\dots j_r}$ *adjungált minora*.

Tétel 3.17 (Laplace-kifejtés)

$$\det(A) = \sum_{1 \leq j_1 < \dots < j_r \leq n} (-1)^{i_1+\dots+i_r+j_1+\dots+j_r} D_{i_1\dots i_r}^{j_1\dots j_r} \tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}.$$

($\det(A)$ kifejtése az $i_1, \dots, i_r$ sorok szerint; az összegnek C_n^r tagja van.)

Bizonyítás. Felhasználjuk a determináns definícióját:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Ha $\det(A)$-ből kiválasztunk r oszlopot, akkor a kiválasztott sorok és oszlopok egy r-ed rendű aldeterminánst határoznak meg. Ennek szorzata adjungáltjával $\det(A)$-nek $r!(n-r)!$ tagját szolgáltatja, mégpedig helyes előjellel. Mivel r oszlop C_n^r-féleképpen választható ki, az összes ilyen módon nyert determinánsszorzatok a $\det(A)$ determináns $C_n^r \cdot r!(n-r)! = n!$ tagját állítják elő. Ezek között $\det(A)$ mindegyik tagja szerepel (éspedig akkor csak egyszer). ■

Következmény 3.18 (Determinánsok szorzástétele) *Ha* $A, B \in M_n(K)$*, akkor*

$$\det(AB) = \det(A)\det(B).$$

Bizonyítás. Tekintsük a

$$C = \begin{pmatrix} A & 0_n \\ -I_n & B \end{pmatrix} \in M_{2n}(K)$$

blokkmátrixot. Laplace tétele szerint,

$$\det(C) = \det(A)\det(B)(-1)^{2\cdot\frac{n(n-1)}{2}} = \det(A)\det(B).$$

Minden $j = 1, \dots, n$ esetén adjunk hozzá az első oszlop b_{j1}-szeresét, a második oszlop b_{j2}-szeresét stb, az n-edik oszlop b_{jn}-szeresét az $n+j$-edik oszlophoz. Eljutottunk a

$$C' = \begin{pmatrix} A & AB \\ -I_n & 0_n \end{pmatrix}$$

mátrixhoz, és

$$\begin{aligned} \det(A)\det(B) = \det(C) &= \det(C') \\ &= (-1)^{n+\sum_{k=1}^{n} k + \sum_{k=n+1}^{2n} k} \det(AB) \\ &= \det(AB). \qquad \blacksquare \end{aligned}$$

Feladat 105 (Ciklikus determináns) Igazoljuk, hogy:

$$C_n = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{vmatrix} = f(\epsilon_0)\dots f(\epsilon_{n-1}),$$

ahol $f = a_1 + a_2X + \dots + a_nX^{n-1}$, és $\epsilon_i,\ i = 0, \dots, n-1$ az n-ed rendű egységgyökök.

Feladat 106 a) Alkalmazva a Laplace-képletet, számítsuk ki a következő determinánst:

$$D = \begin{vmatrix} a_1 & 0 & a_2 & 0 & a_3 \\ 0 & x_1 & 0 & x_2 & 0 \\ b_1 & 0 & b_2 & 0 & b_3 \\ 0 & y_1 & 0 & y_2 & 0 \\ c_1 & 0 & c_2 & 0 & c_3 \end{vmatrix}.$$

b) Számítsuk ki a következő determinánst:

$$D = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 & 0 & 0 \\ a_2 & b_2 & c_2 & d_2 & 0 & 0 \\ a_3 & b_3 & c_3 & d_3 & 0 & 0 \\ 0 & 0 & a_1 & b_1 & c_1 & d_1 \\ 0 & 0 & a_2 & b_2 & c_2 & d_2 \\ 0 & 0 & a_3 & b_3 & c_3 & d_3 \end{vmatrix}.$$

c) Számítsuk ki a $d_{2n} = \det(A)$ determinánst, ahol $A = [a_{ij}] \in M_{2n}(K)$,

$$a_{ij} = \begin{cases} x_i, & i = j \\ 0, & i \neq j,\ i + j = 2n + 1 \\ y_i, & i + j = 2n + 1 \end{cases}, \qquad x_i, y_i \in K.$$

d) Ha $A \in M_m(K),\ B \in M_{m,n}(K)$ és $C \in M_n(K)$, akkor $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)\det(C)$.

e) Ha $A, B, C \in M_n(K)$, akkor $\det \begin{pmatrix} 0 & A \\ B & C \end{pmatrix} = (-1)^n \det(A)\det(B)$.

Feladat 107 a) Legyen $A, B \in M_n(\mathbb{R})$ és $i = \sqrt{-1} \in \mathbb{C}$. Igazoljuk, hogy

$$\det \begin{pmatrix} A & -B \\ B & A \end{pmatrix} = |\det(A + iB)|^2,$$

és számítsuk ki a

$$D = \begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix}$$

determinánst, ahol $a, b, c, d \in \mathbb{R}$.

b) Számítsuk ki a

$$D = \begin{vmatrix} a & -b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{vmatrix}$$

determinánst, ahol $a, b, c, d \in \mathbb{R}$.

Feladat 108 (Binet–Cauchy) Legyen $A = (a_{ij}) \in M_{nm}(K),\ B = (b_{kl}) \in M_{mn}(K)$ és $C = AB$. Bizonyítsuk be, hogy:

$$\det C = \sum_{1 \le j_1 < \dots < j_n \le m} \begin{vmatrix} a_{1j_1} & a_{2j_1} & a_{3j_1} & \dots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & a_{3j_2} & \dots & a_{nj_2} \\ a_{1j_3} & a_{2j_3} & a_{3j_3} & \dots & a_{nj_3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1j_n} & a_{2j_n} & a_{3j_n} & \dots & a_{nj_n} \end{vmatrix} \cdot \begin{vmatrix} b_{j_1 1} & b_{j_1 2} & b_{j_1 3} & \dots & b_{j_1 n} \\ b_{j_2 1} & b_{j_2 2} & b_{j_2 3} & \dots & b_{j_2 n} \\ b_{j_3 1} & b_{j_3 2} & b_{j_3 3} & \dots & b_{j_3 n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{j_n 1} & b_{j_n 2} & b_{j_n 3} & \dots & b_{j_n n} \end{vmatrix}$$

(tehát $\det C = \det A \det B$ ha $m = n$ és $\det C = 0$ ha $n > m$).

Alkalmazás. Ha $A \in M_{mn}(K)$, $m \geq n$, akkor $\det(A^t \cdot A) = \sum_B B^2$, ahol B végig fut az A n-edrendű minorainak a halmazán.

Feladat 109 (Gram-determináns) Ha $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$, legyen

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

az x, y vektorok *kanonikus skaláris szorzata.* Legyen $v^1, \ldots, v^n \in \mathbb{R}^n$ egy vektorrendszer, $a_{ij} := \langle v^i, v^j \rangle$, $1 \leq i, j \leq n$, és legyen

$$G(v^1, \ldots, v^n) := \det(a_{ij}).$$

Igazoljuk, hogy $\{v^1, \ldots, v^n\}$ akkor és csak akkor független ha $G(v^1, \ldots, v^n) \neq 0$.

3.6 Mátrix rangja

Értelmezés 3.19 Legyenek U és V K-feletti vektorterek, $f : U \to V$ egy lineáris függvény, és $u_1, \ldots, u_m \in U$ vektorok.

a) Értelmezés szerint, a *vektorrendszer rangja* egyenlő a vektorok által generált résztér dimenziójával:

$$\operatorname{rang}(u_1, \ldots, u_m) = \dim_K \langle u_1, \ldots, u_m \rangle.$$

b) A *lineáris függvény rangja* egyenlő a képtér dimenziójával:

$$\operatorname{rang} f = \dim_K \operatorname{Im} f.$$

Megjegyzés 3.20 a) A 2.18. tételből következik, hogy $\operatorname{rang} f = \dim_K U - \dim_K \operatorname{Ker} f$.

b) Feltételezzük, hogy $(e_1, \ldots, e_n)$ U-nak egy bázisa, tehát $U = \{x = \sum_{i=1}^{n} x_i e_i \mid x_i \in K\}$. Ekkor

$$\begin{aligned} \operatorname{Im} f = f(U) &= \{f(x) \mid x \in U\} \\ &= \{\sum_{i=1}^{n} x_i f(e_i) \mid x_i \in K\} \\ &= \langle f(e_1), \ldots, f(e_n) \rangle \leq_K V, \end{aligned}$$

tehát, $\operatorname{rang} f = \operatorname{rang}(f(e_1), \ldots, f(e_n))$.

Értelmezés 3.21 Legyen $A = [a_{ij}] \in M_{m,n}(K)$, és legyen $0 \leq r \leq \min\{m, n\}$. Azt mondjuk, hogy az A *rangja* egyenlő r-el (jelölés: $\operatorname{rang} A = r$), ha A-nak van egy r-ed rendű nemnulla minora (aldeterminánsa), és minden r-nél nagyobb rendű minor egyenlő 0-val.

Tétel 3.22 (Kronecker-tétel) *Minden $A \in M_{m,n}(K)$ mátrix esetén,*

$$\operatorname{rang} A = \operatorname{rang}(o_1^A, \ldots, o_n^A) = \operatorname{rang}(s_1^A, \ldots, s_m^A).$$

Bizonyítás. Legyen $r = \operatorname{rang} A$. Ekkor A-nak van egy r-ed rendű nemnulla minora, és egyszerűség kedvéért, feltételezhetjük, hogy $\det(B) \neq 0$, ahol

$$B = \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}$$

Következik, hogy az $o_1^B, \ldots, o_r^B$ oszlopok lineárisan függetlenek, tehát az $o_1^A, \ldots, o_r^A$ oszlopok is lineárisan függetlenek; következik, hogy $r \leq \operatorname{rang}(o_1^A, \ldots, o_n^A)$.

Kiegészítjük B-t egy sorral és egy oszloppal, és legyen

$$D_{ij} = \begin{vmatrix} a_{11} & \ldots & a_{1r} & a_{ij} \\ \vdots & \ddots & \vdots & \vdots \\ a_{r1} & \ldots & a_{rr} & a_{rj} \\ a_{i1} & \ldots & a_{ir} & a_{ij} \end{vmatrix}, \quad 1 \leq i \leq m, \quad r < j \leq n.$$

Igazoljuk, hogy $D_{ij} = 0$ minden $1 \leq i \leq m$, $r < j \leq n$ esetén. Valóban, ha $1 \leq i \leq r$, akkor D_{ij}-nek van két egyenlő sora (az i-edik és az $r+1$-edik) tehát $D_{ij} = 0$; ha pedig $i > r$, akkor D_{ij} A-nak egy $r+1$-ed rendű minora, tehát feltevés szerint $D_{ij} = 0$.

Legyen $d = \det(B) \neq 0$, és legyenek $d_1, \ldots, d_r, d$ az $a_{i1}, \ldots, a_{ir}, a_{ij}$ elemek algebrai komplementumai; vegyük észre, hogy ezek az elemek nem függnek i-től. Kifejtjük D_{ij}-t az $r+1$-edik sora szerint; következik, hogy

$$0 = D_{ij} = a_{i1}d_1 + \ldots a_{ir}d_r + a_{ij}d.$$

Legyen $\alpha_k = -d^{-1}d_k,\ 1 \leq k \leq r$. Ekkor

$$a_{ij} = \alpha_1 a_{i1} + \alpha_2 a_{i2} + \cdots + \alpha_r a_{ir},\quad 1 \leq i \leq m,\ r < j \leq n.$$

Következik, hogy minden $r < j \leq n$ esetén,

$$o_j^A = \alpha_1 o_1^A + \cdots + \alpha_r o_r^A \in \langle o_1^A, \ldots o_r^A \rangle,$$

tehát $\operatorname{rang}(o_1^A, \ldots o_r^A) \leq r$. ■

Megjegyzés 3.23 A tétel bizonyításában csak azt használtuk fel, hogy A-nak van egy r-ed rendű nemnulla minora, és minden $r+1$-ed rendű *kiegészítő minor* egyenlő 0-val.

Példa 3.24 Tekintsük az

$$A = \begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 2 & -4 & 0 & 1 \end{pmatrix} \in M_{3,4}(\mathbb{R})$$

mátrixot. Ha $B_1 = [1]$, akkor $\det B_1 \neq 0$, és ha $B_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, akkor $\det B_2 \neq 0$, tehát $\operatorname{rang} A \geq 2$. Van két kiegészítő minor; mivel

$$\begin{vmatrix} 1 & -2 & 1 \\ 1 & -2 & -1 \\ 2 & -4 & 0 \end{vmatrix} = 0 \quad \text{és} \quad \begin{vmatrix} 1 & 1 & 3 \\ 1 & -1 & 1 \\ 2 & 0 & 1 \end{vmatrix} = 0,$$

következik, hogy $\operatorname{rang} A = 2$.

Feladat 110 Határozzuk meg az $A = (x_i y_j)_{1 \leq i \leq m, 1 \leq j \leq n} \in M_n(K)$ mátrix rangját.

Feladat 111 Igazoljuk, hogy $\operatorname{rang}(AB) \leq \min\{\operatorname{rang} A, \operatorname{rang} B\}$.

3.7 Lineáris egyenletrendszerek. A Kronecker–Capelli-tétel

Legyen K egy kommutatív test, $m, n \in \mathbb{N}^*$, és feltételezzük, hogy adottak az $a_{ij} \in K$, $b_i \in K$ elemek, $1 \leq i \leq m,\ 1 \leq j \leq n$.

Lineáris egyenletrenszernek nevezzük a következő feladatot: határozzuk meg az $x_1, \ldots, x_n \in K$ elemeket úgy, hogy

$$(S): \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = b_2 \\ \ldots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = b_m \end{cases}$$

Vezessük be a következő mátrixokat:

$$A = [a_{ij}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(K), \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K), \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K).$$

Ekkor könnyen észrevehető, hogy (S) egyenértékű a következő mátrixegyenletekkel:

$$(S) \iff Ax = b \iff \sum_{j=1}^{n} x_j o_j^A = b.$$

Értelmezés 3.25 a) Az a_{ij} elemeket *együtthatóknak*, a b_i elemeket *szabadtagoknak* és az x_j elemeket *ismeretleneknek* nevezzük.

b) Azt mondjuk, hogy A az *egyenletrendszer mátrixa*, és

$$\bar{A} = [A \vdots b] = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix} \in M_{m,n+1}(K)$$

az *egyenletrendszer bővített mátrixa.*

c) Ha $b = 0$, akkor (S) *homogén egyenletrendszer.*

d) (S) *kompatibilis* ha létezik $x \in M_{n,1}(K) \simeq K^n$ úgy, hogy $Ax = b$; ellenkező esetben, (S) *inkompatibilis.*

Tétel 3.26 (Kronecker–Capelli) *Az* (S) *egyenletrendszer kompatibilis akkor és csak akkor, ha*

$$\operatorname{rang} A = \operatorname{rang} \bar{A}.$$

Bizonyítás. Feltételezzük, hogy (S) kompatibilis. Ekkor léteznek az $x_1, \dots, x_n \in K$ elemek úgy, hogy $b = \sum_{j=1}^{n} x_j o_j^A$, azaz $b \in \langle o_1^A, \dots, o_n^A \rangle$. Következik, hogy $\langle o_1^A, \dots, o_n^A \rangle = \langle o_1^A, \dots, o_n^A, b \rangle$, tehát

$$\operatorname{rang} A = \dim_K \langle o_1^A, \dots, o_n^A \rangle = \dim_K \langle o_1^A, \dots, o_n^A, b \rangle = \operatorname{rang} \bar{A}.$$

Fordítva, feltételezzük, hogy $\operatorname{rang} A = \operatorname{rang} \bar{A}$, azaz

$$\dim_K \langle o_1^A, \dots, o_n^A \rangle = \dim_K \langle o_1^A, \dots, o_n^A, b \rangle.$$

Mivel $\langle o_1^A, \dots, o_n^A \rangle \leq_K \langle o_1^A, \dots, o_n^A, b \rangle$, az alternatíva tételből következik, hogy

$$\langle o_1^A, \dots, o_n^A \rangle = \langle o_1^A, \dots, o_n^A, b \rangle.$$

Akkor $b \in \langle o_1^A, \dots, o_n^A \rangle$, tehát léteznek az $x_1, \dots, x_n \in K$ elemek úgy, hogy $b = \sum_{j=1}^{n} x_j o_j^A$. ■

Következmény 3.27 (Rouché-tétel) *Feltételezzük, hogy* $\operatorname{rang} A = r$ *és legyen*

$$\det B = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0$$

az (S) *rendszer fődeterminánsa.* Az $\bar{A}$ bővített mátrix azon $(r+1)$-ed rendű minorjait amelyek bővítik B-t és tartalmaznak szabadtagokat *karakterisztikus minoroknak* nevezzük.

a) *A karakterisztikus minorok száma* $m - r$.

b) (S) *kompatibilis* $\iff$ *minden karakterisztikus minor egyenlő nullával.*

3.8 Lineáris egyenletrendszerek megoldása

Az előző paragrafus jelöléseit használjuk.

3.8.1 A. A megoldasok halmaza

Azonosítsuk az $M_{n,1}(K)$ és K^n vektortereket, valamint az $M_{m,1}(K)$ és K^m vektortereket, és jelöljük e-vel a kanonikus bázisokat. Legyen $f : K^n \to K^m$ az egyértelműen meghatározott lineáris függvény úgy, hogy $[f]_{e,e} = A$. A fenti azonosí tásokból következik, hogy $f(x) = Ax$ minden $x \in K^n$ esetén. Vegyük észre, hogy az

$$f^{-1}(b) = \{x \in K^n \mid f(x) = b\}$$

halmaz megegyezik az (S) megoldásainak a halmazával.

Tétel 3.28 a) *Ha* x^0 *az* (S) *egyenletrendszernek egy partikuláris megoldása, akkor*

$$f^{-1}(b) = x^0 + \operatorname{Ker} f.$$

b) $\dim_K \operatorname{Ker} f = n - \operatorname{rang} A$.

c) *(Cramer-szabály) Feltételezzük, hogy* $m = n$. *Az* (S) *rendszernek akkor és csak akkor van egyetlen megoldása, ha* $\det A \neq 0$.

Ebben az esetben

$$x_j = (\det A)^{-1} \cdot \det(o_1^A, \dots, \underset{j}{b}, \dots, o_n^A).$$

d) *Feltételezzük, hogy* (S) *kompatibilis,* $\operatorname{rang} A = r$, $\det B = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0$, *és legyen*

$$(S') : \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rn}x_n = b_r \end{cases}$$

a redukált egyenletrendszer. (Az utolsó $m-r$ egyenletet *mellékegyenletnek* nevezzük.)

Ekkor minden $x \in K^n$ *esetén,* x *megoldása* (S)*-nek* $\iff$ x *megoldása* (S')*-nek.*

Bizonyítás. a) Feltételezzük, hogy $f(x^0) = b$.

Ha $x \in f^{-1}(b)$, akkor $f(x) = b = f(x^0)$, tehát $f(x - x^0) = 0$, azaz $y := x - x^0 \in \operatorname{Ker} f$; következik, hogy $x = x^0 + y \in x^0 + \operatorname{Ker} f$.

Fordítva, ha $x = x^0 + y \in x^0 + \operatorname{Ker} f$, ahol $y \in \operatorname{Ker} f$, akkor $f(x) = f(x^0) + f(y) = f(x^0) = b$, tehát $x \in f^{-1}(b)$.

b) Tudjuk, hogy $\operatorname{Ker} f \leq_K K^n$, és $n = \dim_K K^n = \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f$. Továbbá,

$$\operatorname{Im} f = f(K^n) = \{f(x) \mid x \in K^n\} = \{Ax \mid x \in K^n\} =$$
$$= \{\sum_{j=1}^{n} x_j o_j^A \mid x_j \in K,\ j = 1, \dots, n\}\langle o_1^A, \dots, o_n^A\rangle.$$

Kronecker tétele szerint, $\operatorname{rang} A = \dim_K \langle o_1^A, \dots, o_n^A\rangle$, tehát $\dim_K \operatorname{Ker} f = n - \operatorname{rang} A$.

c) Feltételezzük, hogy $m = n$. Ekkor

$$\begin{aligned} |f^{-1}(b)| = 1 &\iff \operatorname{Ker} f = \{0\} \text{ és } f^{-1}(b) \neq \emptyset \\ &\iff f \text{ injektív és } f^{-1}(b) \neq \emptyset \\ &\iff f \text{ bijektív} \quad \text{(alternatíva tétel szerint)} \\ &\iff A = [f]_{e,e} \text{ invertálható} \\ &\iff \det A \neq 0. \end{aligned}$$

Ebben az esetben, mivel $b = Ax = \sum_{k=1}^{n} x_k o_k^A$, következik, hogy

$$\det(o_1^A, \dots, \underset{j}{b}, \dots, o_n^A) = \det(o_1^A, \dots, \sum_{k=1}^{n} x_k o_k^A, \dots, o_n^A) = \sum_{k=1}^{n} x_k \det(o_1^A, \dots, o_k^A, \dots, o_n^A)$$
$$= x_j \det(o_1^A, \dots, o_j^A, \dots, o_n^A) = x_j \det(A).$$

d) Ha $x^0 \in K^n$ megoldása (S)-nek, akkor nyilvánvaló, hogy x^0 megoldása (S')-nek is. Legyen

$$A' = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rn} \end{pmatrix}$$

az (S') egyenletrenszer mátrixa, $b' = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$, és legyen $f' : K^n \to K^r$, $f'(x) = A'x$.

Ha $f(x) = Ax = 0$, akkor $0 = A'x = f'(x)$, tehát $\operatorname{Ker} f \leq_K \operatorname{Ker} f'$. Mivel

$$\dim_K \operatorname{Ker} f' = n - \operatorname{rang} A' = n - r = n - \operatorname{rang} A = \dim_K \operatorname{Ker} f,$$

következik, hogy $\operatorname{Ker} f' = \operatorname{Ker} f$, és végül, $f^{-1}(b) = x^0 + \operatorname{Ker} f = x^0 + \operatorname{Ker} f' = f'^{-1}(b)$. ∎

Következmény 3.29 *Legyen* (S) *egy homogén egyenletrendszer. Ekkor*

a) (S) *kompatibilis.*

b) *Ha* $m = n$*, akkor* (S)*-nek van nemtriviális megoldása* $\Leftrightarrow \det A = 0$.

Feladat 112 Tárgyaljuk és oldjuk meg a következő egyenletrendszereket:

a) $\begin{cases} 2x_1 - x_2 + x_3 - x_4 &= 1 \\ x_1 + x_2 + \alpha x_3 + x_4 &= -1 \\ x_1 - x_2 + x_3 + \beta x_4 &= \gamma \end{cases}$

b) $\begin{cases} ax_1 + (a+1)x_2 + (a+2)x_3 &= a+3 \\ bx_1 + (b+1)x_2 + (b+2)x_3 &= b+3 \\ x_1 + cx_2 + c^2x_3 &= c^3 \end{cases}$

3.8.2 B. A mátrixegyenlet tárgyalása

A fenti egyenletrendszereket a Rouché és Cramer tételei alapján oldottuk meg. A következő módszer mátrixegyenletként kezeli (S)-et.

Ha (S) kompatibilis, akkor a 3.28. tétel d) pontjából következik, hogy feltételezhetjük, hogy $\operatorname{rang} A = m \leq n$, és legyen $\det B \neq 0$ az (S) *fődeterminánsa*, ahol

$$B = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \in M_{mm}(K).$$

Felírjuk A-t az $A = [B \vdots S]$ alakban, ahol

$$S = \begin{pmatrix} a_{1,m+1} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m,m+1} & \dots & a_{mm} \end{pmatrix} \in M_{m,n-m}(K),$$

és legyen $x = \begin{pmatrix} x_B \\ x_S \end{pmatrix}$, ahol $x_B = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ a *főismeretlenek* mátrixa, és $x_S = \begin{pmatrix} x_{m+1} \\ \vdots \\ x_n \end{pmatrix}$ a *mellékismeretlenek* mátrixa. Ekkor (S)-et felírhatjuk a következő alakban:

$$(S): \qquad Bx_B + Sx_S = b.$$

Tekinsük először az (S)-hez rendelt $Bx_B + Sx_S = 0$ *homogén* mátrixegyenletet. Ennek a megoldása

$$x_B = -B^{-1}Sx_S, \quad x_S \in K^{n-m}.$$

Legyen $x_S^{(1)} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $x_S^{(2)} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, x_S^{(n-m)} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ a K^{n-m} kanonikus bázisa, $x_B^{(j)} = -B^{-1}Sx_S^{(j)}$, ahol $1 \leq j \leq n-m$, és legyen

$$x^{(j)} = \begin{pmatrix} x_B^{(j)} \\ x_S^{(j)} \end{pmatrix} \in \operatorname{Ker} f, \quad 1 \leq j \leq n-m.$$

Mivel $\dim_K \operatorname{Ker} f = n-m$, következik, hogy $x^{(1)}, \dots, x^{(n-m)}$ bázisa $\operatorname{Ker} f$-nek, tehát

$$\operatorname{Ker} f = \langle x^{(1)}, \dots, x^{(n-m)} \rangle.$$

Továbbá, egy x^0 partikuláris megoldást a következő képpen kapunk: legyen $x_S^0 = 0 \in K^{n-m}$, és $x_B^0 := B^{-1}b - B^{-1}Sx_S^0 = B^{-1}b \in K^m$, tehát

$$x^0 = \begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix} \in K^n$$

megoldása (S)-nek.

Megkaptuk tehát az (S) megoldásainak a halmazát:

$$\begin{aligned} f^{-1}(b) &= x^0 + \operatorname{Ker} f = x^0 + \langle x^{(1)}, \dots, x^{(n-m)} \rangle = \\ &= \{x^0 + \lambda_1 x^{(1)} + \dots + \lambda_{n-m} x^{(n-m)} \mid \lambda_1, \dots, \lambda_{n-m} \in K\}. \end{aligned}$$

Azt mondjuk, hogy $\lambda_1, \dots, \lambda_{n-m} \in K$ *szabad paraméterek.*

Példa 3.30 Tekintsük az

$$(S): \quad \begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 & = 2 \end{cases}$$

egyenletrendszert. A fenti jelöléseket alkalmazva,

$$A = \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ -1 & -1 & -1 & -2 & -2 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 3 \\ -2 \\ 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 1 \\ -1 & -1 & -1 \\ 1 & 3 & 2 \end{pmatrix},$$

$$-B^{-1}S = \begin{pmatrix} 0 & -1 \\ -1 & -1 \\ -1 & 0 \end{pmatrix}, \quad B^{-1}b = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix},$$

tehát az (S) megoldásainak a halmaza

$$\{x^0 + \lambda_1 x^{(1)} + \lambda_2 x^{(2)} \mid \lambda_1, \lambda_2 \in K\},$$

ahol

$$x^0 = \begin{pmatrix} 3 \\ 1 \\ -2 \\ 0 \\ 0 \end{pmatrix}, \quad x^{(1)} = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad x^{(2)} = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Feladat 113 Oldjuk meg a következő egyenletrendszereket:

a) $\begin{cases} x_1 + 3x_2 - x_3 - 2x_4 & = 3 \\ 2x_1 - x_2 + 3x_3 - 4x_4 & = -1 \end{cases}$

b) $\begin{cases} x_1 - 2x_2 - 2x_3 - 2x_4 - x_5 & = 0 \\ x_1 - x_2 - x_3 - 3x_4 + x_5 & = 1 \\ x_1 + x_2 - 5x_3 - x_4 + 7x_5 & = 2 \end{cases}$

c) $\begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \end{cases}$

d) $\begin{cases} \hat{2}x_1 + x_2 - 2x_3 & = \hat{1} \\ x_1 + \hat{5}x_2 + \hat{2}x_3 & = \hat{2} \end{cases}, \quad (K = \mathbb{Z}_7)$

Gyakorlatban, ha m és n nagy számok, akkor a fenti módszerek nem hatékonyak. A következő paragrafusban egy sokkal gyorsabb eljárást mutatunk be.

3.9 Algoritmikus módszerek

3.9.1 A. Kicserélési lemma (Elemi báziscsere)

Legyen V egy K-feletti vektortér és $e = (e_1, \dots, e_n)$ egy rendezett bázisa,

Lemma 3.31 *Legyen* $v = a_1 e_1 + \cdots + a_n e_n \in V$ *és tekintsük az* $e' = (e_1, \dots, \underset{i}{v}, \dots, e_n)$ *vektorrendszert.*

a) e' *akkor és csak akkor bázisa* V*-nek, ha* $a_i \neq 0$.

b) *Feltételezzük, hogy* $a_i \neq 0$*, és legyen*

$$x = x_1 e_1 + \cdots + x_i e_i + \cdots + x_n e_n = x'_1 e_1 + \cdots + x'_i v + \cdots + x'_n e_n \in V.$$

Ekkor

$$x'_i = \frac{x_i}{a_i}, \quad x'_j = \frac{x_j a_i - x_i a_j}{a_i}, \ j \neq i.$$

Bizonyítás. a) Az alternatíva tétel szerint, e' akkor és csak akkor bázis, ha lineárisan független. Ha $b_1, \dots, b_n \in K$, akkor

$$\begin{aligned} b_1 e_1 + \cdots + b_i v + \cdots + b_n e_n = 0 &\iff b_1 e_1 + \cdots + b_i \sum_{j=1}^{n} a_j e_j + \cdots + b_n e_n = 0 \\ &\iff (b_1 + b_i a_1) e_1 + \cdots + b_i a_i v + \cdots + (b_n + b_i a_n) e_n = 0 \\ &\iff b_i a_i = 0, \quad b_j + b_i a_j = 0, \ j \neq i. \end{aligned}$$

Ha $a_i \neq 0$, akkor $b_i = 0$; következik, hogy $b_1 = \cdots = b_n = 0$, tehát e' bázis.
Ha $a_i = 0$, akkor legyen $b_i = 1$, és $b_j = -a_j$, $j \neq i$; következik, hogy e' nem független.

b) Ha $a_i \neq 0$, akkor

$$\begin{aligned} x &= x_1 e_1 + \cdots + x_i e_i + \cdots + x_j e_j + \cdots + x_n e_n = \\ &= x'_1 e_1 + \cdots + x'_i v + \cdots + x'_j e_j + \cdots + x'_n e_n = \\ &= (x'_1 + x'_i a_1) e_1 + \cdots + x'_i a_i e_i + \cdots + (x'_j + x'_i a_j) e_j + \cdots + (x'_n + x'_i a_n) e_n. \end{aligned}$$

Mivel e bázis, következik, hogy $x_i = x_i' a_i$ és $x_j = x_j' + x_i' a_j$ ha $j \neq i$, tehát

$$x_i' = \frac{x_i}{a_i}, \quad x_j' = x_j - \frac{x_i}{a_i} a_j, \ j \neq i. \qquad \blacksquare$$

Az $a_i \neq 0$ elemet *generáló elemnek* nevezzük. A fenti számításokat egy táblázatban rendszerezzük:

	v	x
e_1	a_1	x_1
$\vdots$	$\vdots$	$\vdots$
e_i	$\boxed{a_i}$	x_i
$\vdots$	$\vdots$	$\vdots$
e_j	a_j	x_j
$\vdots$	$\vdots$	$\vdots$
e_n	a_n	x_n

$\longrightarrow$

	v	x
e_1	0	$x_1' = \frac{x_1 a_i - x_i a_1}{a_i}$
$\vdots$	$\vdots$	$\vdots$
v	1	$x_i' = \frac{x_i}{a_i}$
$\vdots$	$\vdots$	$\vdots$
e_j	0	$x_j' = \frac{x_j a_i - x_i a_j}{a_i}$
$\vdots$	$\vdots$	$\vdots$
e_n	0	$x_n' = \frac{x_n a_i - x_i a_n}{a_i}$

Az alapműveletet könnyű megjegyezni: a generáló elem sorát osztjuk a generáló elemmel, a többi elemet az ún. *téglalap-szabállyal* számítjuk ki.

3.9.2 B. Alkalmazások

a) Báziscsere. Legyen $v = (v_1, \dots, v_n)$ egy vektorrendszer, ahol

$$v_j = \sum_{i=1}^{n} a_{ij} e_i, \quad 1 \leq j \leq n,$$

és legyen $T_e^v = [a_{ij}] \in M_n(K)$ az áttérési mátrix. Tudjuk, hogy v akkor és csak akkor bázis, ha T invertálható, és ha

$$x = x_1 e_1 + \dots + x_n e_n = x_1' v_1 + \dots + x_n' v_n,$$

akkor $[x]_v = T^{-1}[x]_e$. n-szer alkalmazva a kicserélési lemmát, meghatározhatjuk az $[x]_v$ mátrixot.

	v_1	$\dots$	v_n	x
e_1	a_{11}	$\dots$	a_{1n}	x_1
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
e_n	a_{n1}	$\dots$	a_{nn}	x_n

$\overset{n \text{ lépés}}{\longrightarrow}$

	v_1	$\dots$	v_n	x
v_1	1	$\dots$	0	x_1'
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
v_n	0	$\dots$	1	x_n'

Ha T nem invertálható, akkor az $e_1, \dots, e_n$ vektorokat nem lehet kicserélni a $v_1, \dots, v_n$ vektorokkal.

Például, legyen $V = \mathbb{R}^3$, $e = (e_1, e_2, e_3)$ a kanonikus bázisa, és legyen $v_1 = (1,4,2)$, $v_2 = (1,3,1)$, $v_3 = (1,2,1)$ és $x = (1,-2,-2)$.

	v_1	v_2	v_3	x
e_1	$\boxed{1}$	1	1	1
e_2	4	3	2	-2
e_3	2	1	1	-2
v_1	1	1	1	1
e_2	0	$\boxed{-1}$	-2	-6
e_3	0	-1	-1	-4
v_1	1	0	-1	-5
v_2	0	1	2	6
e_3	0	0	$\boxed{1}$	2
v_1	1	0	0	-3
v_2	0	1	0	2
v_3	0	0	1	2

Az utolsó táblázatból következik, hogy v bázis és $x = -3v_1 + 2v_2 + 2v_3$.

Feladat 114 Igazoljuk, hogy $v = (v_1, \dots, v_n)$ bázisa V-nek és határozzuk meg az x koordinátáit a v bázisban, ahol:

a) $V = \mathbb{Z}_5^3$, $v_1 = (\hat{2}, \hat{3}, \hat{1})$, $v_2 = (\hat{1}, \hat{2}, \hat{4})$, $v_3 = (\hat{0}, \hat{1}, \hat{1})$, $x = (\hat{4}, \hat{2}, \hat{1})$.
b) $V = \mathbb{R}^4$, $v_1 = (2,1,3,-2)$, $v_2 = (-1,1,-2,1)$, $v_3 = (4,5,3,-1)$, $v_4 = (1,5,-3,1)$, $x = (1,1,1,1)$.
c) $V = \mathbb{R}^3$, $v_1 = (1,2,1)$, $v_2 = (2,3,3)$, $v_3 = (3,7,1)$, $x = (1,1,1)$.

Feladat 115 Határozzuk meg az $U, V, U+V, U\cap V \leq_{\mathbb{R}} \mathbb{R}^3$ részterek egy-egy bázisát, ahol:
a) $U = \langle(1,0,4),(2,1,0),(1,1,-4)\rangle$, $V = \langle(-3,-2,4),(5,2,4),(-2,0,-8)\rangle$.
b) $U = \langle(1,1,0),(0,1,0),(0,1,1)\rangle$, $V = \langle(1,1,-1),(2,0,1)\rangle$.

b) Mátrix rangja. Ha $A \in M_{m,n}(K)$, akkor $\operatorname{rang} A = \dim_K \langle o_1^A, \dots o_n^A\rangle$, tehát alkalmazhatjuk a kicserélési lemmát. Például, legyen $A = \begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 2 & -4 & 0 & 4 \end{pmatrix}$.

	o_1^A	o_2^A	o_3^A	o_4^A
e_1	1	-2	1	3
e_2	1	-2	-1	1
e_3	2	-4	0	4
o_1^A	1	-2	1	3
e_2	0	0	-2	-2
e_3	0	0	-2	-2
o_1^A	1	-2	0	2
o_3^A	0	0	1	1
e_3	0	0	0	0

Az utolsó táblázatból következik, hogy $o_2^A = -2o_1^A$, $o_4^A = 2o_1^A + o_3^A$, és o_1^A, o_3^A lineárisan függetlenek, tehát $\operatorname{rang} A = 2$.

Feladat 116 Határozzuk meg a következő mátrixok rangját:
a) $\begin{pmatrix} 1 & -1 & 1 & 2 & 2 \\ 1 & -1 & -1 & 1 & 3 \\ 2 & 2 & 0 & 3 & 5 \end{pmatrix}$ b) $\begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 1 & -4 & 0 & 4 \end{pmatrix}$

c) Mátrix inverze és determinánsa. Az $A = [a_{ij}] \in M_n(K)$ mátrix akkor és csak akkor invertálható, ha $(o_1^A, \dots, o_n^A)$ bázis. Legyen $I = I_n$ az n-ed rendű egységmátrix, és tekintsük a következő táblázatokat:

	o_1^A	…	o_n^A	o_1^I	…	o_n^I
e_1	a_{11}	…	a_{1n}	1	…	0
⋮	⋮	⋱	⋮	⋮	⋱	⋮
e_n	a_{n1}	…	a_{nn}	0	…	1

$\xrightarrow{n \text{ lépés}}$

	v_1	…	v_n	o_1^I	…	o_n^I
o_1^A	1	…	0	b_{11}	…	b_{1n}
⋮	⋮	⋱	⋮	⋮	⋱	⋮
o_n^A	0	…	1	b_{n1}	…	b_{nn}

Legyen $B = [b_{ij}]$. Az utolsó táblázatból következik, hogy minden $1 \leq j \leq n$ esetén, $o_j^I = \sum_{k=1}^n o_k^A b_{kj}$, azaz

$$\delta_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad 1 \leq i,j \leq n,$$

tehát $I_n = AB$ és $B = A^{-1}$.

Legyen $a_{i_k j_k}^{(k)}$ a k-adik generáló elem. A determinánsok tulajdonságaiból következik, hogy

$$\det A = \prod_{k=1}^{n} (-1)^{i_k + j_k} a_{i_k j_k}^{(k)}.$$

Például, legyen $A = \begin{pmatrix} \hat{2} & \hat{4} & \hat{2} \\ \hat{1} & \hat{1} & \hat{1} \\ \hat{3} & \hat{2} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_5)$. Előállítjuk a következő táblázatokat:

	o_1^A	o_2^A	o_3^A	o_1^I	o_2^I	o_3^I
e_1	$\boxed{\hat{2}}$	$\hat{4}$	$\hat{2}$	$\hat{1}$	$\hat{0}$	$\hat{0}$
e_2	$\hat{1}$	$\hat{1}$	$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{0}$
e_3	$\hat{3}$	$\hat{2}$	$\hat{1}$	$\hat{0}$	$\hat{0}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{2}$	$\hat{1}$	$\hat{3}$	$\hat{0}$	$\hat{0}$
e_2	$\hat{0}$	$\boxed{\hat{4}}$	$\hat{0}$	$\hat{2}$	$\hat{1}$	$\hat{0}$
e_3	$\hat{0}$	$\hat{1}$	$\hat{3}$	$\hat{1}$	$\hat{0}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{0}$
o_2^A	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
e_3	$\hat{0}$	$\hat{0}$	$\boxed{\hat{3}}$	$\hat{3}$	$\hat{1}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$
o_2^A	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
o_3^A	$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$

Az utolsó táblázatból következik, hogy $A^{-1} = \begin{pmatrix} \hat{1} & \hat{0} & \hat{3} \\ \hat{3} & \hat{4} & \hat{0} \\ \hat{1} & \hat{2} & \hat{2} \end{pmatrix}$, és $\det A = \hat{2} \cdot \hat{4} \cdot \hat{3} = \hat{4}$.

Feladat 117 Határozzuk meg a következő mátrixok inverzét:

a) $\begin{pmatrix} \hat{2} & \hat{0} & \hat{1} \\ \hat{1} & \hat{2} & \hat{1} \\ \hat{2} & \hat{1} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_3)$ b) $\begin{pmatrix} \hat{2} & \hat{4} & \hat{2} \\ \hat{1} & \hat{1} & \hat{1} \\ \hat{0} & \hat{2} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_5)$.

Feladat 118 Legyen $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^4)$, $[f]_{e,e} = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 3 & 0 & -1 & 2 \\ 2 & 5 & 3 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}$, és legyen $e' = (e'_1, e'_2, e'_3, e'_4)$, ahol $e'_1 = e_1, e'_2 = e_1 + e_2$, $e'_3 = e_1 + e_2 + e_3$, $e'_4 = e_1 + e_2 + e_3 + e_4$. Határozzuk meg az f mátrixát az (e', e') bázispárban.

Feladat 119 Legyen $u = (u_1, u_2, u_3, u_4)$ és $v = (v_1, v_2, v_3, v_4)$, ahol $u_1 = (1, 2, -1, 0)$, $u_2 = (1, -1, 1, 1)$, $u_3 = (-1, 2, 1, 1)$, $u_4 = (-1, -1, 0, 1)$, $v_1 = (2, 1, 0, 1)$, $v_2 = (0, 1, 2, 2)$, $v_3 = (-2, 1, 1, 2)$, és $v_4 = (1, 3, 1, 2)$ $\mathbb{R}^4$-beli vektorok. Igazoljuk, hogy u, v bázisok, és határozzuk meg a T_u^v áttérési mátrixot.

d) Az egyenletrendszerek megoldása. Tekintsük az $Ax = b \iff Bx_B + Sx_S = b$ egyenletrendszert, ahol a 3.8.2. paragrafus jelölései használjuk. Ha $B \in M_m(K)$ invertálható, akkor az egyenletrendszer megoldasait megkapjuk m lépés után. A számítások azt is kimutatják, ha a rendszer összeférhetetlen, mert ebben az esetben $\operatorname{rang} A < \operatorname{rang} \bar{A}$.

	$o_1^A \ \dots \ o_m^A$	$o_{m+1}^A \ \dots \ o_n^A$	b
e_1			
$\vdots$	B	S	b
e_m			

$\downarrow$ m lépés

	$o_1^A \ \dots \ o_m^A$	$o_{m+1}^A \ \dots \ o_n^A$	b
o_1^A			
$\vdots$	I_m	$B^{-1}S$	$B^{-1}b$
o_m^A			

Például oldjuk meg az

$$(S): \quad \begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 & = 2 \end{cases}$$

egyenletrendszert.

	o_1^A	o_2^A	o_3^A	o_4^A	o_5^A	b
e_1	$\boxed{1}$	2	1	3	3	3
e_2	-1	-1	-1	-2	-2	-2
e_3	1	3	2	5	4	2
o_1^A	1	2	1	3	3	3
e_2	0	$\boxed{1}$	0	1	1	1
e_3	0	1	1	2	1	-1
o_1^A	1	0	1	1	1	1
o_2^A	0	1	0	1	1	1
e_3	0	0	$\boxed{1}$	1	0	-2
o_1^A	1	0	0	0	1	3
o_2^A	0	1	0	1	1	1
o_3^A	0	0	1	1	0	-2

Az utolsó táblázatból következik, hogy

$$-B^{-1}S = \begin{pmatrix} 0 & -1 \\ -1 & -1 \\ -1 & 0 \end{pmatrix}, \quad B^{-1}b = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix},$$

tehát az (S) megoldásainak a halmaza

$$\{x^0 + \lambda_1 x^{(1)} + \lambda_2 x^{(2)} \mid \lambda_1, \lambda_2 \in K\},$$

ahol

$$x^0 = \begin{pmatrix} 3 \\ 1 \\ -2 \\ 0 \\ 0 \end{pmatrix}, \quad x^{(1)} = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad x^{(2)} = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Feladat 120 Oldjuk meg a következő egyenletrendszereket:

a) $\begin{cases} x_1 + 3x_2 - x_3 - 2x_4 = 3 \\ 2x_1 - x_2 + 3x_3 - 4x_4 = -1 \\ 3x_1 - 5x_2 + 7x_3 - 6x_4 = 1 \end{cases}$

b) $\begin{cases} x_1 - 2x_2 - 2x_3 - 2x_4 - x_5 = 0 \\ x_1 - x_2 - x_3 - 3x_4 + x_5 = 1 \\ x_1 + x_2 - 5x_3 - x_4 + 7x_5 = 2 \end{cases}$

c) $\begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 = 2 \end{cases}$

d) $\begin{cases} \hat{2}x_1 + x_2 - 2x_3 = \hat{1} \\ \hat{2}x_1 + \hat{2}x_2 + \hat{2}x_3 = \hat{0}, \\ x_1 + \hat{4}x_2 + \hat{2}x_3 = \hat{2} \end{cases} \quad (K = \mathbb{Z}_5)$

Feladat 121 Legyen $f : \mathbb{R}^n \to \mathbb{R}^m$ egy lineáris leképezés. Határozzuk meg a $\operatorname{Ker} f$ és $\operatorname{Im} f$ vektorterek egy-egy bázisát, ha adott az f mátrixa a kanonikus bázisokban:

a) $[f]_{e,e} = \begin{pmatrix} 3 & -1 & -1 & 1 \\ 1 & 2 & -1 & -1 \end{pmatrix}$

b) $[f]_{e,e} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}$

c) $[f]_{e,e} = \begin{pmatrix} 1 & 0 & -3 & 2 \\ -2 & 3 & 0 & 1 \\ 3 & -3 & -1 & 1 \end{pmatrix}$

d) $[f]_{e,e} = \begin{pmatrix} 2 & 2 & 1 \\ -1 & -3 & 1 \\ 1 & 2 & -1 \end{pmatrix}$

3.10 Megoldott feladatok

1) Legyenek $\nu = ((1,2),(-2,1))$ és $\nu' = ((1,-1,0),(-1,0,1),(1,1,1))$. Mutassuk ki, hogy ν és ν' bázisok $\mathbb{R}^2$-ben, illetve $\mathbb{R}^3$-ban és írjuk fel az $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f(x,y) = (x+y, 2x-y, 3x+2y)$ lineáris függvény mátrixát a (ν, ν') bázisokban.

Megoldás: Mivel a ν vektoraiból képezett mátrix rangja 2, és a ν' vektoraiból képezett mátrix rangja 3, következik, hogy ν bázis $\mathbb{R}^2$-ben és ν' bázis $\mathbb{R}^3$-ban. Az $[f]_{\nu,\nu'} = (a_{ij}) \in M_{3,2}(\mathbb{R})$ mátrix oszlopait a következő egyenletek alapján írjuk fel:

$$(3,0,7) = f(1,2) = a_{11}(1,-1,0) + a_{21}(-1,0,1) + a_{31}(1,1,1),$$
$$(-1,-5,-4) = f(-2,1) = a_{12}(1,-1,0) + a_{22}(-1,0,1) + a_{32}(1,1,1).$$

Az előző két egyenlet a következő két egyenletrendszert eredményezi:

$$\begin{cases} a_{11} - a_{21} + a_{31} = 3 \\ -a_{11} \quad + a_{31} = 0 \\ a_{21} + a_{31} = 7 \end{cases} \quad \text{és} \quad \begin{cases} a_{12} - a_{22} + a_{32} = -1 \\ -a_{12} \quad + a_{32} = -5 \\ a_{22} + a_{32} = -4 \end{cases}$$

amiknek a megoldásai $\left(\frac{10}{3}, \frac{11}{3}, \frac{10}{3}\right)$ illetve $\left(\frac{5}{3}, -\frac{2}{3}, -\frac{10}{3}\right)$. Következésképpen

$$[f]_{\nu,\nu'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

Alternatív megoldás: Az $\mathbb{R}^3$ e' kanonikus bázisából ν'-be való áttérési mátrix $T = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, az f függvény mátrixa a ν, e' bázisokban pedig

$$[f]_{\nu,e'} = \begin{pmatrix} 3 & -1 \\ 0 & -5 \\ 7 & -4 \end{pmatrix},$$

(a mátrix oszlopai az $f(1,2)$ és $f(-2,1)$ koordinátái az e' bázisban), tehát

$$[f]_{\nu,\nu'} = T^{-1}[f]_{\nu,e'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

2) Legyen az $f : \mathbb{R}^3 \to \mathbb{R}^4$ lineáris függvény, ahol a kanonikus bázisvektorok képei:

$$f(e_1) = (1,2,3,4),\ f(e_2) = (4,3,2,1),\ f(e_3) = (-2,1,4,1).$$

Határozzuk meg:
i) $f(\nu)$-t bármely $\nu \in \mathbb{R}^3$-ra;
ii) az f mátrixát a kanonikus bázisokban;
iii) $\operatorname{Im} f$ és $\operatorname{Ker} f$ egy-egy bázisát.

Megoldás: i) $f(x_1,x_2,x_3) = x_1 f(e_1) + x_2 f(e_2) + x_3 f(e_3)$.
ii) f mátrixa a kanonikus bázisokban az a mátrixk aminek az oszlopai $f(e_1)$, $f(e_2)$ és $f(e_3)$, vagyis

$$\begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix}.$$

iii) $\operatorname{Im} f = f(\langle e_1, e_2, e_3\rangle) = \langle f(e_1), f(e_2), f(e_3)\rangle$, tehát

$$\dim(\operatorname{Im} f) = \operatorname{rang} \begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix} = 3,$$

következésképpen $f(e_1)$, $f(e_2)$ és $f(e_3)$ bázist alkotnak $\operatorname{Im} f$-ben. Akkor

$$\dim(\operatorname{Ker} f) = \dim \mathbb{R}^3 - \dim(\operatorname{Im} f) = 3 - 3 = 0,$$

tehát $\operatorname{Ker} f = \{(0,0,0)\}$ és $\emptyset$ a $\operatorname{Ker} f$ bázisa.

3) Legyenek V, V' vektorterek $\mathbb{R}$ fölött, $v = (v_1, v_2, v_3)$ bázis V-ben, $v' = (v_1', v_2', v_3')$ bázis V'-ben és $f : V \to V'$ lineáris függvény úgy, hogy

$$[f]_{v,v'} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}.$$

Határozzuk meg:
i) $\operatorname{Im} f$ és $\operatorname{Ker} f$ dimenzióját, adjunk mindegyikben egy-egy bázist;
ii) az $[f]_{v,e'}$ mátrixot abban az esetben, amikor $V' = \mathbb{R}^3$, $v_1' = (1,0,0)$, $v_2' = (0,1,1)$, $v_3' = (0,0,1)$ és e' az $\mathbb{R}^3$ kanonikus bázisa;
iii) $f(x)$ értéket $x = 2v_1 - v_2 + 3v_3$-re a ii) pontban megadott feltételek mellett.

Megoldás: i) Az $[f]_{v,v'}$ mátrix oszlopait az $f(v_1)$, $f(v_2)$, illetve $f(v_3)$ vektorok v' bázisbeli koordinátái alapján írjuk fel, vagyis

$$f(v_1) = v_2', \ f(v_2) = -v_1' + v_3' \quad \text{és} \quad f(v_3) = 5v_1' - 5v_3'.$$

Akkor $\dim(\operatorname{Im} f) = \operatorname{rang}[f]_{v,v'} = 2$. A $[f]_{v,v'}$ mátrix egy másodrendű nemnulla minorát kapjuk az első két oszlopból és az első két sorból, következésképpen, $f(v_1)$ és $f(v_2)$ bázist alkotnak $\operatorname{Im} f$-ben. Következik, hogy

$$\dim(\operatorname{Ker} f) = \dim V - \dim(\operatorname{Im} f) = 3 - 2 = 1,$$

és mivel az $[f]_{v,v'}$ mátrix második és harmadik oszlopa arányos, kapjuk, hogy

$$f(v_3) = -5f(v_2) \Leftrightarrow f(v_3 - 5v_2) = 0 \Leftrightarrow v_3 - 5v_2 \in \operatorname{Ker} f.$$

Tehát $v_3 - 5v_2$ bázis $\operatorname{Ker} f$-ben.
ii) Az e' kanonikus bázisból a v' bázisba való áttérési mátrix (T) oszlopai a v_1', v_2', v_3' vektorok és

$$[f]_{v,v'} = T^{-1}\,[f]_{v,e'} \ \Leftrightarrow \ [f]_{v,e'} = T\,[f]_{v,v'}.$$

iii) Mivel az $[f]_{v,e'}$ mátrix oszlopait az $f(v_1)$, $f(v_2)$ és $f(v_3)$ vektorok koordinátái adják az e' bázisban,

$$f(x) = f(2v_1 - v_2 + 3v_3) = 2f(v_1) - f(v_2) + 3f(v_3).$$

4) Legyen $f \in \operatorname{End}_{\mathbb{Q}}(\mathbb{Q}^4)$, aminek a következő mátrixa van a kanonikus bázisban:

$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 3 & 2 & 3 & 2 \\ -1 & -3 & 0 & 4 \\ 0 & 4 & -1 & -3 \end{pmatrix}.$$

Adjunk meg egy-egy bázist $\operatorname{Ker} f$-ben és $\operatorname{Im} f$-ben.

Megoldás: Legyen $e = (e_1, e_2, e_3, e_4)$ $_{\mathbb{Q}}\mathbb{Q}^4$ kanonikus bázisa. A megadott mátrix pont $[f]_e$, az oszlopai $f(e_1)$, $f(e_2)$, $f(e_3)$, illetve $f(e_4)$. $\operatorname{Im} f$ bázisának és dimenziójának kiszámításához kiszámoljuk $[f]_e$ rangját és figyelembe vesszük, hogy milyen oszlopokból tudtunk ,,kivágni" egy olyan nemnulla minort, aminek a rangja egyenlő $\operatorname{rang}[f]_e$-vel. Kapjuk, hogy $\dim(\operatorname{Im} f) = 3$, következésképpendim$(\operatorname{Ker} f) = 1$. $\operatorname{Ker} f$ bázisának meghatározásához ugyanúgy járunk el, mint az előző feladat i)-es pontjánál, figyelembe véve, hogy $7(c_1 - c_3) = c_2 - c_4$ (ahol c_i-vel jelöltük a mátrix i-edik oszlopát, ami pontosan $f(e_i)$). A bázis meghatározásához a következő módon is eljárhatunk:

$$(x_1, x_2, x_3, x_4) \in \operatorname{Ker} f \Leftrightarrow [f]_e \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x_1 + 2x_2 + x_3 + 2x_4 = 0 \\ 3x_1 + 2x_2 + 3x_3 + 2x_4 = 0 \\ -x_1 - 3x_2 \quad + 4x_4 = 0 \\ \quad +4x_2 - x_3 - 3x_4 = 0 \end{cases}.$$

A lineáris egyenletrendszernek a következő megoldáshalmaza van:

$$\{(7\alpha,-\alpha,-7\alpha,\alpha)\in\mathbb{Q}^4 \mid \alpha\in\mathbb{Q}\}=\{\alpha(7,-1,-7,1)\mid\alpha\in\mathbb{Q}\}=\langle(7,-1,-7,1)\rangle,$$

tehát a $(7,-1,-7,1)$ vektor lineárisan független generátora (vagyis bázisa) Ker f-nek.

5) Legyen $f:\mathbb{R}^2\to\mathbb{R}^2$, $f(x,y)=(3x+3y,2x+4y)$. Bizonyítsuk be, hogy $f\in\mathtt{End}_{\mathbb{R}}(\mathbb{R}^2)$. Mutassuk meg, hogy diagonalizálható az f függvény $[f]_E$ mátrixa (a kanonikus bázisban) és adjunk meg egy képletet $[f^n]$-re, ahol $f^n=f\circ f\circ\cdots\circ f$, $n\in\mathbb{N}^*$.

Megoldás:

Felírjuk f mátrixát: $[f]_E=\begin{pmatrix}3&3\\2&4\end{pmatrix}$ és meghatározzuk a sajátértékeit: $p_f(\lambda)=\det([f]_E-\lambda I_2)=\begin{vmatrix}3-\lambda&3\\2&4-\lambda\end{vmatrix}=$ $\lambda^2-7\lambda+6=0$, kapjuk, hogy $\lambda_1=1$, $\lambda_2=6$. Innen következik, hogy $m_{alg}(1)=1$ és $m_{alg}(6)=1$. Meghatározzuk a sajátértékekhez tartozó sajátrésztereket.

$$\begin{pmatrix}3-\lambda_1&3\\2&4-\lambda_1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\Longrightarrow\begin{cases}2x+3y&=0\\2x+3y&=0\end{cases}\Longrightarrow x=-\frac{3}{2}y.$$

A megoldáshalmaz $M_1=\{(-\frac{3}{2}y,y)|y\in\mathbb{R}\}=<(-3,2)>=V(1)\implies m_{geom}(1)=\dim_{\mathbb{R}}V(1)=1$.

$$\begin{pmatrix}3-\lambda_2&3\\2&4-\lambda_2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\Longrightarrow\begin{cases}-3x+3y&=0\\2x-2y&=0\end{cases}\Longrightarrow x=y.$$

A megoldáshalmaz $M_2=\{(y,y)|y\in\mathbb{R}\}=<(1,1)>=V(6)\implies m_{geom}(6)=\dim_{\mathbb{R}}V(6)=1$.

Látható, hogy $m_{geom}(1)=m_{alg}(1)$ és $m_{geom}(6)=m_{alg}(6)$, tehát a mátrix diagonalizálható. Legyen $B=((-3,2),(1,1))$. Tudjuk, hogy B bázisa $\mathbb{R}^2$-nek, mert különböző sajátértékekhez tartozó sajátvektorok lineárisan függetlenek és $\dim_{\mathbb{R}}\mathbb{R}^2=2$. Mivel $(-3,2)$ és $(1,1)$ sajátvektorok, akkor az f függvény mátrixa ebben a bázisban $[f]_B=\begin{pmatrix}\lambda_1&\\&\lambda_2\end{pmatrix}=\begin{pmatrix}1&0\\0&6\end{pmatrix}$. (Ügyeljünk a (saját) bázisvektorok sorrendjére! Ha a bázist $B=((1,1),(-3,2))$-nek írtuk volna fel, akkor $[f]_B=\begin{pmatrix}6&0\\0&1\end{pmatrix}$ lenne.) Vegyük észre, hogy $T_{EB}=\begin{pmatrix}-3&1\\2&1\end{pmatrix}$, tehát akkor $T_{BE}=T_{EB}^{-1}=\frac{1}{5}\begin{pmatrix}-1&1\\2&3\end{pmatrix}$. Az áttérési mátrixok segítségével felírható az $[f]_E=T_{EB}\cdot[f]_B\cdot T_{BE}$ egyenlet, tehát:

$$[f]_E=\begin{pmatrix}3&3\\2&4\end{pmatrix}=\begin{pmatrix}-3&1\\2&1\end{pmatrix}\begin{pmatrix}1&0\\0&6\end{pmatrix}\frac{1}{5}\begin{pmatrix}-1&1\\2&3\end{pmatrix}.$$

Tehát:

$$[f^n]_E=\begin{pmatrix}-3&1\\2&1\end{pmatrix}\begin{pmatrix}1^n&0\\0&6^n\end{pmatrix}\frac{1}{5}\begin{pmatrix}-1&1\\2&3\end{pmatrix}=\frac{1}{5}\begin{pmatrix}3+2\cdot6^n&-3+3\cdot6^n\\-2+2\cdot6^n&2+3\cdot6^n\end{pmatrix}.$$

6) Legyen $f:\mathbb{R}^3\to\mathbb{R}^3$ egy lineáris függvény, a következő mátrixszal: $[f]_E=\begin{pmatrix}0&-1&5\\1&0&0\\0&1&-5\end{pmatrix}$. Határozzuk meg a $\ker f$ és $\mathrm{Im}f$ vektorterek egy-egy bázisát.

Megoldás:

Megoldjuk az $[f]_E\cdot v=0$ egyenletet: $\begin{pmatrix}0&-1&5\\1&0&0\\0&1&-5\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\Longrightarrow\begin{cases}x&=0\\y&=5z\end{cases}\Longrightarrow M=\{(0,5z,z)|z\in\mathbb{R}\}=<(0,5,1)>$. Látható, hogy $\ker f$ egydimenziós résztér, bázisa lehet pl. a $B=((0,5,1))$. Továbbá $\dim_{\mathbb{R}}(\mathrm{Im}f)=\dim_{\mathbb{R}}\mathbb{R}^3-\dim_{\mathbb{R}}(\ker f)=3-1=2$, tehát elég találni két lineárisan független vektort Imf-ben és akkor azok bázist fognak alkotni. Ennek legegyszerűbb módja, hogy kellő számú lineárisan független vektort választunk ki az $[f]_E$ mátrix oszlopai közül. A mátrix oszlopai a bázisvektorok képei az f függvényen keresztül, tehát elemei Imf-nek. Ezért például $\mathrm{Im}f=<(0,1,0),(-1,0,1)>$, a bázis $B'=((0,1,0),(-1,0,1))$.

4 Egész számok aritmetikája

A következőkben néhány fontos fogalmat és tételt említünk. A bizonyításukra később kerül sor egy általánosabb kontextusban.

Tétel 4.1 (Maradékos osztás tétele) *Ha* $a, b \in \mathbb{Z}$ *és* $b \neq 0$*, akkor léteznek és egyértelműen meghatározottak* q *és* $r \overset{\text{jel}}{=} (a \mod b)$ *egész számok úgy, hogy*

$$a = bq + r, \qquad 0 \leq r < |b|.$$

Bizonyítás. Legyen $r := \min(\{a - kb \mid k \in \mathbb{Z}\} \cap \mathbb{N})$, és legyen $q := (a - r)/b$, téhát q és r léteznek.

Ha $a = bq + r = bq_1 + r_1$, ahol $0 \leq r, r_1 < |b|$, akkor $|b||q - q_1| = |r - r_1| < |b|$, tehát $q - q_1 = 0$, és innen $r = r_1$. ■

A következő eljárást **Euklideszi algoritmus**nak nevezzük.

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|;\\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2;\\
&\dots\\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2};\\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0.
\end{aligned}$$

Valóban, mivel az (r_k) sorozat szigorúan csökkenő, létezik n úgy, hogy $r_{n+1} = 0$. Azt mondjuk, hogy r_n az *utolsó nemnulla maradék.*

Értelmezés 4.2 Legyenek a és b egész számok.

a) a *osztója* b-nek (jelölés: $a|b$) ha létezik $x \in \mathbb{Z}$ úgy, hogy $b = ax$.

b) Egy $d \in \mathbb{N}$ szám az a és b *legnagyobb közös osztója*, (jelölés: $d = (a, b)$) ha

1. $d|a$ és $d|b$;
2. ha $d' \in \mathbb{Z}$, $d'|a$ és $d'|b$, akkor $d'|d$.

c) Egy $m \in \mathbb{N}$ szám az a és b *legkisebb közös többszöröse*, (jelölés: $m = [a, b]$) ha

1. $a|m$ és $b|m$;
2. ha $m' \in \mathbb{Z}$, $a|m'$ és $b|m'$, akkor $m|m'$.

d) a és b relatív prímek ha $(a, b) = 1$.

e) $p \in \mathbb{N}$ *prímszám*, ha $p \neq 1$, és ha $a \in \mathbb{Z}$, $a|p$, akkor $a = \pm 1$ vagy $a = \pm p$.

Feladat 122 a) 0 osztható minden számmal; minden szám osztható 1-gyel.

b) $a|b,\ a|c \Rightarrow a|b \pm c$.

c) $a|b \Rightarrow ax|bx$ minden $x \in \mathbb{Z}$ esetén. Fordítva, ha $ax|bx,\ x \neq 0$, akkor $a|b$.

Feladat 123 a) Legyen $a, b \in \mathbb{Z}$. Ha $a = b = 0$, akkor $(a, b) = 0$. Ellenkező esetben, legyen

$$d := \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$

és igazoljuk, hogy ekkor $d = (a, b)$.

(Tehát (a, b) létezik, és mitöbb, léteznek az $u, v \in \mathbb{Z}$ úgy, hogy $(a, b) = au + bv$.)

b) $(a, b) = 1 \Leftrightarrow (\exists) u, v \in \mathbb{Z}$ úgy, hogy $au + bv = 1$. (Ebben az esetben azt mondjuk, hogy a és b *relatív prímek.*)

Feladat 124 a) Ha $a = bq + r$, akkor $(a, b) = (b, r)$.

b) Az Euklideszi algoritmusban $\boxed{r_n = (a, b)}$.

c) Igazoljuk, hogy az Euklideszi algoritmus segítségével meg lehet határozni az u és v számokat úgy, hogy $(a, b) = au + bv$.

d) Az euklideszi algoritmust alkalmazva, számítsuk ki a következő számok legnagyobb közös osztóját, és fejezzük ki a két szám lineáris kombinációjaként:

(1) $a = 19,\ b = 26.$

(2) $a = 1082,\ b = 458$.
(3) $a = -187,\ b = 34$.
(4) $a = -841,\ b = -160$.
(5) $a = 2613,\ b = -2171$.
e) Ha $x \in \mathbb{N}$, akkor $(ax, bx) = (a, b)x$.
f) Ha $d = (a, b)$, $a = da'$ és $b = db'$, akkor $(a', b') = 1$.
g) Legyen $a, b, c \in \mathbb{Z}$ úgy, hogy $(a, b) = 1$. Igazoljuk, hogy :
(1) $(a, c) = 1 \Rightarrow (a, bc) = 1$; (2) $a|bc \Rightarrow a|c$; (3) $a|c$ és $b|c \Rightarrow ab|c$.
h) Ha $d = (a, b)$, $a = da'$ és $b = db'$, akkor

$$[a, b] = a'b'd = \frac{ab}{d}.$$

i) Legyen $p \in \mathbb{N}$, $p > 1$. Igazoljuk, hogy p prímszám $\Leftrightarrow$ minden $a, b \in \mathbb{Z}$ esetén, ha $p|ab$, akkor $p|a$ vagy $p|b$.

Értelmezés 4.3 Legyenek $x_1, \ldots, x_n$ egész számok, ahol $n \in \mathbb{N}^*$, és legyen $d, m \in \mathbb{N}$. Értelmezés szerint,

a) $d = (x_1, \ldots, x_n) \iff \begin{cases} d|x_1, \ldots, d|x_n, \\ \text{ha } d'|x_1, \ldots, d'|x_n, \text{ akkor } d'|d. \end{cases}$

b) $m = [x_1, \ldots, x_n] \iff \begin{cases} x_1|m, \ldots, x_n|m, \\ \text{ha } x_1|m', \ldots, x_n|m', \text{ akkor } m|m'. \end{cases}$

Feladat 125 Legyenek $x_1, \ldots, x_n$ egész számok. Igazoljuk, hogy:
a) $(x_1, \ldots, x_{n-1}, x_n) = ((x_1, \ldots, x_{n-1}), x_n)$; $[x_1, \ldots, x_{n-1}, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$.
b) $(x_1, \ldots, x_n) = \min\{x \in \mathbb{N}^* \mid \exists u_i \in \mathbb{Z}$ úgy, hogy $x = \sum_{i=1}^n u_i x_i\}$. Partikulárisan, $(x_1, \ldots, x_n) = d \Rightarrow \exists u_i \in \mathbb{Z}$ úgy, hogy $\sum_{i=1}^n u_i x_i = d$.
c) $(x_1, \ldots, x_n) = 1 \Leftrightarrow \exists u_i \in \mathbb{Z}$ úgy, hogy $\sum_{i=1}^n u_i x_i = 1$.
d) $(x_1 x, \ldots, x_n x) = (x_1, \ldots, x_n)x$ minden $x \in \mathbb{N}$ esetén.
e) Ha $(x, x_i) = 1$, $i = 1, \ldots, n$, akkor $(x, x_1 \ldots x_n) = 1$.
f) Ha $(x_i, x_j) = 1$ minden $i, j = 1, \ldots, n$, $i \neq j$ esetén, akkor $[x_1, \ldots, x_n] = x_1 \ldots x_n$. (Ebben az esetben azt mondjuk, hogy az x_i, $i = 1, \ldots, n$ számok *páronként relatív prímek.*)

Tétel 4.4 (Az aritmetika alaptétele) *Minden $a \neq 0, 1$ egész szám felírható egyértelműen a következő alakban:*

$$a = \pm p_1^{k_1} \ldots p_r^{k_r},$$

ahol p_i páronként különböző prímszámok és $k_i \in \mathbb{N}^*$, $1 \leq i \leq r$.

Következmény 4.5 *Ha $a = \pm p_1^{k_1} \ldots p_r^{k_r}$ és $b = \pm p_1^{l_1} \ldots p_r^{l_r}$, ahol $k_i, l_i \geq 0$, $1 \leq i \leq r$, akkor*

$$(a, b) = p_1^{\min\{k_1, l_1\}} \ldots p_r^{\min\{k_r, l_r\}} \quad \text{és} \quad [a, b] = p_1^{\max\{k_1, l_1\}} \ldots p_r^{\max\{k_r, l_r\}}.$$