2. Vektorterek, lineáris leképezések és mátrixaik

2.1 Vektorterek

2.1.1 Definíció: egy K test fölötti $(V,+,\cdot)$ vektortér egy olyan struktúra, melyben $(V,+)$ kommutatív csoport és az ún. skalárral szorzás, $\cdot: K\times V\to V$, disztributív a K-beli összeadásra balról, a V-belire jobbról, továbbá a skalárral való szorzás és a K-beli szorzás felcserélhető műveletek, végül a K egységével szorzás identitás V-n:

(V1) $+: V\times V\to V$

(V2) $\forall u,v,w\in V$: $u+(v+w)=(u+v)+w$

(V3) $\forall u,v\in V$: $u+v=v+u$

(V4) $\exists 0\in V$: $\forall v\in V$: $v+0=0+v=v$

(V5) $\forall v\in V$: $\exists(-v)\in V$: $v+(-v)=(-v)+v=0$

(V6) $\cdot: K\times V\to V$

(V7) $\forall \alpha,\beta\in K, v\in V$: $(\alpha\beta)\cdot v=\alpha\cdot(\beta\cdot v)$

(V8) $\forall \alpha,\beta\in K, v\in V$: $(\alpha+\beta)\cdot v=\alpha\cdot v+\beta\cdot v$

(V9) $\forall \alpha\in K, u,v\in V$: $\alpha\cdot(u+v)=\alpha\cdot u+\alpha\cdot v$

(V10) $\forall v\in V$: $1\cdot v=v$

Ebből már következik, hogy $\forall \alpha\in K, v\in V$: $\alpha\cdot 0_V=0_V, 0_K\cdot v=0_V$ és másféle szorzat nem 0.

2.1.2 Definíció: a K feletti V vektortér $v_1,v_2,\ldots,v_n$ elemeinek $\alpha_1,\alpha_2,\ldots,\alpha_n\in K$ együtthatókkal vett lineáris kombinációja $\sum_{k=1}^n \alpha_k\cdot v_k$.

2.1.3 Definíció: a K feletti V vektortér H – véges vagy végtelen – részhalmaza lineárisan összefüggő, ha található véges sok eleme, melyek valamely K feletti nem triviális lineáris kombinációja (nem minden együttható 0) 0. Ha nem lineárisan összefüggő, akkor lineárisan független.

2.1.4 Definíció: a K feletti V vektortér v eleme függ a H részhalmaztól, ha van H-ban véges sok elem, melyek K feletti lineáris kombinációjaként v felírható. Ha ez nem áll fenn, akkor független tőle.

2.1.5 Állítás: egy részhalmaz lineárisan összefüggő $\Leftrightarrow$ van olyan eleme, amely függ a többitől.

2.1.6 Állítás: egy részhalmaz lineárisan összefüggő $\Leftrightarrow$ van olyan eleme, amely függ a többitől.

Bizonyítás: $\Rightarrow$: írjuk fel a 0-t nem triviális lineáris kombinációként. Vegyünk egy nem 0 együtthatójú v elemet, osszunk le az együtthatójával és minden mást vigyünk át a másik oldalra. Előállítottuk v-t lineáris kombinációként.

$\Leftarrow$: írjuk fel ezen v elemét lineáris kombinációként és vigyük át a másik oldalra. v együtthatója -1 lesz, azaz a 0 nem triviális felírását kapjuk.

2.1.7 Állítás: egy lineárisan független H halmazhoz egy v elemet hozzávéve megszűnik független lenni $\Leftrightarrow$ v függ H-tól.

Bizonyítás: $\Rightarrow$: vegyük a 0 nem triviális felírását a kapott halmazban. Ha ebben v együtthatója 0, akkor H lineárisan összefüggő volt. Ha nem 0, akkor az előző állítás alapján lineárisan függ H-tól. $\Leftarrow$: mint fent.

2.1.8 Definíció: egy V vektortér U részhalmaza altér, ha vektortér ugyanazon K test felett az örökölt műveletekkel. Jelölése $U\le V$.

Ez nyilván pontosan akkor teljesül, ha U zárt a V feletti műveletekre és nem üres. (A műveleti szabályok érvényesek minden részhalmazban.) A 0 minden altérnek eleme.

2.1.9 Állítás: ha $\{U_\alpha \mid \alpha\in\mathbf{I}\}$ a V vektortér alterei, akkor $U=\bigcap_{\alpha\in\mathbf{I}} U_\alpha$ is.

Bizonyítás: U nem üres, mert $0\in U$. A műveletek nem vezetnek ki belőle, mert akkor valamelyik kiinduló altérből kivezetnének. Tehát a metszet is altér lesz.

2.1.10 Definíció: a V vektortér **H** részhalmaza által feszített altér az a legszűkebb altér, amely tartalmazza **H**-t. (Legszűkebb: minden **H**-t tartalmazó altér tartalmazza.) Jelölése $\langle\mathbf{H}\rangle$. Ez létezik, hiszen $\bigcap_{\mathbf{H}\subseteq U\le V} U$ altér, tartalmazza **H**-t és nyilván a lehető legszűkebb, tehát éppen $\langle\mathbf{H}\rangle$. Nyilván $\mathbf{H}\subseteq\mathbf{H}' \Rightarrow \langle\mathbf{H}\rangle\subseteq\langle\mathbf{H}'\rangle$.

2.1.11 Állítás: $\langle \mathbf{H} \rangle = \{\sum_{k=1}^{n} \alpha_k v_k \in V \,|\, n \in \mathbb{N}, \alpha_k \in K, v_k \in \mathbf{H}\}$. Ez nem üres (az üres összeg definíció szerint 0), zárt a műveletekre, tehát valóban altér. Továbbá mindegyik eleme megkapható **H** elemeiből a műveletekkel, tehát minden **H**-t tartalmazó altérben benne kell legyen.

2.1.12 Definíció: a V vektortér U alterének **X** részhalmaza generátorrendszere, ha $\langle \mathbf{X} \rangle = U$. A V vektortér végesen generált, ha van véges elemszámú generátorrendszere.

2.2 Vektortér bázisa, dimenziója. Mátrix rangja

2.2.1 Definíció: egy V vektortér egy **B** részhalmaza bázis, ha lineárisan független generátorrendszer.

2.2.2 Állítás: **B** bázis V-ben $\Leftrightarrow$ V minden v eleme egyértelműen áll elő **B** elemeinek lineáris kombinációjaként (értsd: pontosan egy olyan $v = \sum_{k=1}^{m} \alpha_k \cdot b_k$ előállítás található, ahol a b_k vektorok **B** páronként különböző elemei és $\alpha_k \in K \setminus \{0\}$).

Bizonyítás: $\Rightarrow$: minden előáll, mert generálórendszer. Ha valamely $v \in V$ kétféleképpen áll elő, akkor a két felírás különbsége a 0 előállítása, tehát minden együtthatója 0 a lineáris függetlenség miatt. Eszerint a két előállítás azonos.

$\Leftarrow$: ha mindent előállít, akkor generátorrendszer. Ha lineárisan összefüggő lenne, akkor a 0-t a triviális előállításon kívül másképp is előállítaná, ami ellentmond az egyértelműségnek.

2.2.3 Állítás: legyen V vektortér, $\mathbf{B} \subseteq V$. Ekkor az alábbi feltételek ekvivalensek:

(1) **B** bázis,
(2) **B** maximális független rendszer,
(3) **B** minimális generátorrendszer.

Bizonyítás: ha **B** bázis, akkor maximális független, mert független és mindent előállít; minimális generátorrendszer, mert generátorrendszer, de bármely b elemét elhagyva $\mathbf{B} \setminus \{b\}$ már nem generálja b-t, hiszen **B** független. Ha **B** maximális független rendszer, akkor V egyik eleme sem vehető hozzá, azaz V minden eleme függ **B**-től, tehát **B** generátorrendszer. Ha **B** minimális generátorrendszer, akkor egyik eleme sem hagyható el, tehát egyik sem függ a többitől, azaz **B** független.

Megjegyzés: a kiválasztási axiómával ekvivalens, hogy minden vektortérben van maximális független rendszer, azaz minden vektortérnek van bázisa.

2.2.4 Tétel: ha egy V vektortérben **F** k elemű lineárisan független rendszer és **X** l elemű generátorrendszer, akkor $k \leq l$.

Bizonyítás: válasszuk meg **F**-et úgy, hogy a feltételek mellett $\mathbf{M} = \mathbf{F} \cap \mathbf{X}$ maximális elemszámú legyen. Legyenek a metszet elemei rendre $x_1, x_2, \ldots, x_m$, **F** fennmaradó elemei $v_{m+1} \ldots v_k$, **X** fennmaradó elemei $x_{m+1} \ldots x_l$. Ha $m = k$, akkor kész vagyunk.

$\nmid$ $m < k$. Ekkor nem lehet $m = l$ sem, mert v_{m+1} függ **X**-től de nem függ $\mathbf{X} \cap \mathbf{F}$-től. Hagyjuk el **F**-ből v_{m+1}-et és vegyük helyette x_j-t $(1 \leq j \leq l)$. **F** választása miatt ekkor lineárisan összefüggővé válik, azaz **2.1.7** szerint x_j függ $\mathbf{F} \setminus \{v_{m+1}\}$-től. Írjuk fel v_{m+1}-et **X** elemeinek lineáris kombinációjaként, majd ebben a felírásban minden x_j-t $\mathbf{F} \setminus \{v_{m+1}\}$ elemeivel. Azt kapjuk, hogy v_{m+1} felírható $\mathbf{F} \setminus \{v_{m+1}\}$ elemeinek lineáris kombinációjaként, ami ellentmond **F** választásának.

2.2.5 Következmény: ha V végesen generált vektortér, akkor van (véges) bázisa.

Bizonyítás: ha V-nek van n elemű generátorrendszere, akkor minden független rendszere legfeljebb n elemű, tehát van köztük maximális elemszámú. Ez persze maximális.

Következmény: ha V-nek van $n \in \mathbb{N}$ elemű bázisa, akkor minden bázisa n elemű. Ugyanis minden független rendszer legfeljebb és minden generátorrendszer legalább n elemű, azaz minden bázis n elemű.

2.2.6 Definíció: egy K feletti V vektortér dimenziója – $\mathbf{dim}_K(V)$ – bázisának elemszáma. Beláttuk, hogy ha V végesen generált, akkor van véges elemszámú bázisa és minden bázisának azonos az elemszáma, tehát ekkor a definíció nem függ a bázis választásától.

2.2.7 Állítás: **(1)** V vektortér tetszőleges lineárisan független rendszere kiegészíthető bázissá és **(2)** tetszőleges generátorrendszere tartalmaz bázist.

Csak véges dimenziós vektorterekre látjuk be. Legyen tehát $\mathbf{dim}(V)=n\in\mathbb{N}$.

Bizonyítás: **(1)** ha $\mathbf{F}$ független rendszer és nem generálja V-t, akkor tetszőleges $v\in V\setminus\langle\mathbf{F}\rangle$ hozzávehető és így egy nagyobb független rendszert kapunk. Folytassuk ezt mindaddig, amíg $\mathbf{F}$ nem generálja V-t. Az algoritmus megáll, mert nincs n-nél nagyobb elemszámú független rendszer.

(2) legyen $\mathbf{X}$ generátorrendszer. Legyen $\mathbf{X}_0=\emptyset\subseteq\mathbf{X}$, ez független. Ezután legyen $\mathbf{X}_k\subseteq\mathbf{X}$ független rendszer. Ha $\mathbf{X}_k$ generálja V-t, örvendezzünk. Ha nem, akkor $\langle\mathbf{X}_k\rangle<V=\langle\mathbf{X}\rangle$ miatt található $x_{k+1}\in\mathbf{X}\setminus\langle\mathbf{X}_k\rangle$ elem. Legyen $\mathbf{X}_{k+1}=\mathbf{X}_k\cup\{x_{k+1}\}$. $\mathbf{X}_k$ független rendszer, x_{k+1} nem függ $\mathbf{X}_k$-tól, azaz $\mathbf{X}_{k+1}$ is független. Folytassuk ezt addig, amíg $\langle\mathbf{X}_k\rangle=V$ lesz (persze ekkor $k=n$). $\mathbf{X}_k\subseteq\mathbf{X}$ független generátorrendszer lesz.

2.2.8 Definíció: az $\mathbf{M}\in K^{n\times k}$ mátrix rangja
- a legnagyobb olyan r egész, melyre van $r\times r$-es nem 0 aldeterminánsa (determinánsrang),
- lineárisan független sorai maximális száma (sorrang), ill.
- lineárisan független oszlopai maximális száma (oszloprang).

Jelölése $r(\mathbf{M})$.

2.2.9 Tétel: ezen definíciók ekvivalensek.

Bizonyítás: elég belátni, hogy a determinánsrang és az oszloprang egyenlő, hiszen ekkor transzponálással $r_{\text{sor}}=r_{\text{det}}$.

$r_{\text{det}}\le r_{\text{oszlop}}$, mert egy $r\times r$-es nem 0 aldetermináns oszlopai nem lehetnek lineárisan összefüggőek **(D7)** és **2.1.5** szerint.

Azt kell még belátnunk, hogy $r_{\text{det}}(\mathbf{M})\ge r_{\text{oszlop}}(\mathbf{M})$. Vegyünk egy $r\times r$-es nem 0 aldeterminánst, $\mathbf{B}$-t. Feltehetjük, hogy ez az első r sor és oszlop által megadott aldetermináns. Rögzítsünk egy $1\le j<n$ egész számot. Vegyük hozzá $\mathbf{B}$-hez $r+1$-edik oszlopnak $\mathbf{M}$ j-edik oszlopát, $r+1$-edik sornak pedig egy tetszőleges t-edik sorát. A kapott $\mathbf{A}$ mátrix determinánsa 0 lesz, mert vagy van két azonos sora, vagy van két azonos oszlopa, vagy egy $(r+1)\times(r+1)$-es aldetermináns, ami 0. Fejtsük ki $\mathbf{A}$-t t-edik sora szerint. Azt kapjuk, hogy

$$0=\left(\sum_{h=1}^{r}a_{th}\cdot A_{th}\right)+a_{tj}\cdot A_{tj}=a_{tj}\cdot\mathbf{det}(\mathbf{B})+\left(\sum_{h=1}^{r}a_{th}\cdot A_{th}\right)$$
$$a_{tj}=\sum_{h=1}^{r}a_{th}\cdot\frac{A_{th}}{\mathbf{det}(\mathbf{B})}$$

ahol A_{th} $(1\le h<r)$ az az előjeles aldetermináns, amit akkor kapunk, ha $\mathbf{A}$-ból elhagyjuk $\mathbf{M}$ t-edik sorát és h-adik oszlopát. Ez $\mathbf{A}$-ban mindig az $r+1$-edik sor, tehát A_{th} nem függ t-től. Így amit felírtunk, az a_{tj} felírása $a_{t1},\dots,a_{tr}$ lineáris kombinációjaként t-től független együtthatókkal, azaz a j-edik sor felírása az első r oszlop lineáris kombinációjaként. Eszerint ez az r oszlop generálja az összes oszlopot, tehát nincs r-nél több lineárisan független oszlop. Épp ezt akartuk bizonyítani.

2.3 Lineáris egyenletrendszerek összes megoldása

2.3.1 Állítás: ha az $x\mathbf{A}=0$ n egyenletből álló, n ismeretlenes homogén egyenletrendszerben $\mathbf{det}(\mathbf{A})=0$, akkor van nem triviális megoldása.

Bizonyítás: $\mathbf{A}$ determinánsrangja legfeljebb $n-1$, azaz oszlopai a fenti tétel szerint összefüggnek, így van nem triviális lineáris kombinációjuk, ami 0. Az együtthatók egy nem triviális megoldást adnak.

Vegyünk most egy lineáris egyenletrendszert, melynek $\mathbf{A}$ mátrixa $n\times k$-as és a rangja r. Legyen $\mathbf{A}'$ az az $n\times(k+1)$-es mátrix, melyet úgy kapunk, hogy $\mathbf{A}$-hoz $k+1$-edik oszlopként hozzávesszük $(b_1,\dots,b_n)$-t. Ennek az oszloprangja nyilván vagy r, vagy $r+1$.

2.3.2 Tétel: pontosan akkor van megoldás, ha $r(\mathbf{A})=r(\mathbf{A}')$.

Bizonyítás: ha van megoldás, akkor a hozzávett oszlop lineárisan függ az előzőktől, azaz a két rang valóban megegyezik. Ha pedig a két rang azonos, akkor az új oszlop benne van a többi sor által feszített vektortérben, így azok lineáris kombinációja, tehát van megoldás.

Persze szeretnénk megadni az összes megoldást.

Legyen mondjuk az első r sor és oszlop alkotta mátrix determinánsa 0-tól különböző. Rendezzük az első r egyenletet $\sum_{j=1}^{r} a_{ij}\cdot x_j = b_i - \sum_{j=r+1}^{k} a_{ij}\cdot x_j$ alakra. Válasszuk meg $x_{r+1},\dots,x_k$-t tetszőlegesen. Az első r egyenletnek minden esetben pontosan egy megoldását kapjuk $x_1,\dots,x_r$-re a Cramer-szabály szerint. Viszont pontosan azok az $x_1,\dots,x_k$ számok elégítik ki az összes egyenletet, melyek az első r-t kielégítik, mert az első r sor generálja $\mathbf{A}'$ sorait, tehát ha az első r egyenlet teljesül, akkor mind teljesül. Így megadtuk az összes megoldást.

Megjegyzés: $x_{r+1},\dots,x_k$-t szabad paramétereknek nevezzük.

2.4 Alterek összege, direkt összeg, direkt szorzat

2.4.1 Definíció: $U,W \le V$ alterek összege $U+W=\{u+w \mid u\in U, w\in W\}$. Könnyen beláthatóan ez $\langle U,W\rangle$.

2.4.2 Definíció: V direkt összege az U,W altereknek, ha $V=U+W$ és $U\cap W=\{0\}$. Jelölése $V=U\oplus W$.

2.4.3 Állítás: $V=U\oplus W \Leftrightarrow V$ minden eleme egyértelműen áll elő egy U-beli és egy W-beli elem összegeként.

Bizonyítás: $\Rightarrow$: ha V minden eleme előáll ilyen összegként, akkor $V\subseteq\langle U,W\rangle$. Mivel $V\supseteq\langle U,W\rangle$, ezek azonosak. Ha az előállítás egyértelmű, akkor nem létezhet $0\ne v\in U\cap W$ elem, mert az $0+v$ és $v+0$ alakban is előállna.

$\Leftarrow$: Ha $V=U\oplus W$, akkor nyilván minden előáll ilyen összegként. Ha valamit kétféleképp felírtunk: $u+w=u'+w'$, akkor $u-u'=w-w'\in U\cap W=\{0\} \Rightarrow$ a két felírás azonos. Tehát minden elem felírása egyértelmű.

2.4.4 Állítás: ha $V=U\oplus W$, akkor $\mathbf{dim}(V)=\mathbf{dim}(U)+\mathbf{dim}(W)$.

Bizonyítás: legyen **E** bázis U-ban, **F** bázis W-ben. Ekkor $\forall v\in V$ előáll $v=u+w$ alakban, ahol u véges sok **E**-beli, w véges sok **F**-beli elem lineáris kombinációja. Tehát $\langle \mathbf{E}\cup\mathbf{F}\rangle=V$. Tekintsünk a 0 felírását $\mathbf{E}\cup\mathbf{F}$-beli elemek lineáris kombinációjaként. Válasszuk szét az **E**-ből kapott tagokat, ezek összege legyen u, az **F**-ből származóak összege w. Ekkor $u+w=0, u\in U, w\in W$. Az előző állításból $u=0, w=0$. Mivel **E** és **F** egyaránt függetlenek, u és w egyaránt csupa 0 együtthatókkal állt elő, így v is. Eszerint $\mathbf{E}\cup\mathbf{F}$ független, tehát bázis V-ben $\Rightarrow$ $\mathbf{dim}(V)=|\mathbf{E}\cup\mathbf{F}|=|\mathbf{E}|+|\mathbf{F}|=\mathbf{dim}(U)+\mathbf{dim}(W)$.

2.4.5 Definíció: az U,V K feletti vektorterek direkt szorzata az (u,v) rendezett párok halmaza, ahol $u\in U, v\in V$. A műveleteket koordinátánként végezzük. Ez egy $\mathbf{dim}(U)+\mathbf{dim}(V)$ dimenziós vektortér K felett. Jelölése $U\times V$.

Megjegyzés: legyen $U'=\{(u,0)\in U\times V\}$, $V'=\{(0,v)\in U\times V\}$. Ekkor $U'\simeq U$; $V'\simeq V$; $U',V'\le U\times V$ és $U'\oplus V'\simeq U\times V$.

2.5 Lineáris leképezések

2.5.1 Definíció: az $\mathcal{A}: V\to W$ leképezés lineáris leképezés avagy homomorfizmus, ha V,W ugyanazon K test feletti vektorterek és $\mathcal{A}$ művelettartó, azaz $\forall a,b\in V, \alpha\in K$: $(a+b)\mathcal{A}=a\mathcal{A}+b\mathcal{A}$, $(\alpha\cdot a)\mathcal{A}=\alpha\cdot(a\mathcal{A})$. Ezen leképezések halmazát $Hom_K(V,W)$-vel jelöljük.

Ha $\mathcal{A}\in Hom_K(V,W)$, akkor nyilván $(0_V)\mathcal{A}=0_W$ és $(-v)\mathcal{A}=-(v\mathcal{A})$.

2.5.2 Definíció: egy $\mathcal{A}: V\to W$ lineáris leképezés képtere $Im\,\mathcal{A}=\{x\in W \mid \exists v\in V: v\mathcal{A}=x\}=V\mathcal{A}$, magtere $Ker\,\mathcal{A}=\{v\in V \mid v\mathcal{A}=0\}$.

2.5.3 Állítás: a fenti jelölésekkel $Im\,\mathcal{A}\le V, Ker\,\mathcal{A}\le W$.

Bizonyítás: $0\mathcal{A}=0$ miatt $0\in Im\,\mathcal{A}, 0\in Ker\,\mathcal{A}$. A képtér elemeinek lineáris kombinációja előáll az ősképek megfelelő lineáris kombinációjának képeként, tehát szintén $Im\,\mathcal{A}$ eleme. Ha $v\in V$ a magtér néhány elemének lineáris kombinációjanak, akkor $v\mathcal{A}$ a megfelelő képek lineáris kombinációja. Ezen képek mindegyike 0, így $v\mathcal{A}=0$, $v\in Ker\,\mathcal{A}$.

Következmény: ha $\mathcal{A}$ lineáris leképezés, akkor $\langle\mathbf{X}\rangle\mathcal{A}=\langle\mathbf{X}\mathcal{A}\rangle$, azaz generátorrendszer képe generátorrendszer a képtérben.

2.5.4 Tétel: legyenek V és W vektorterek K felett, **B** bázis V-ben, $\varphi: \mathbf{B}\to W$ tetszőleges. Ekkor φ egyértelműen terjeszthető ki $\mathcal{A}_\varphi: V\to W$ homomorfizmussá.

Bizonyítás: legyen $v \in V$ tetszőleges. Ez egyértelműen áll elő $v = \sum_{b \in \mathbf{B}^*} \alpha_b \cdot b$ alakban, ahol $\mathbf{B}^*$ a $\mathbf{B}$ bázis véges részhalmaza, az α_b-k pedig K nem 0 elemei. Ha $\mathcal{A}_\varphi$ lineáris leképezés, akkor $v\mathcal{A}_\varphi = (\sum_{b \in \mathbf{B}^*} \alpha_b \cdot b)\mathcal{A}_\varphi = \sum_{b \in \mathbf{B}^*} \alpha_b \cdot (b\mathcal{A}_\varphi) = \sum_{b \in \mathbf{B}^*} \alpha_b \cdot (b\varphi)$ fenn kell álljon, ez biztosítja az egyértelműséget. Ha pedig $\mathcal{A}_\varphi$-t ezzel az egyenlettel adjuk meg, akkor könnyen ellenőrizhetően a definíció értelmes és $\mathcal{A}_\varphi$ lineáris leképezés lesz.

A lineáris leképezések felett értelemszerűen definiálhatóak a műveletek: $\mathcal{A}+\mathcal{B}: v \mapsto v\mathcal{A}+v\mathcal{B}$ és $\alpha \cdot \mathcal{A}: v \mapsto \alpha \cdot (v\mathcal{A})$. Nullelem az azonosan 0 lineáris leképezés. Így $Hom_K(V,W)$ is vektortér lesz K felett.

2.5.5 Állítás: ha V,W vektorterek K felett és $\mathbf{dim}_K(V)<\infty$, akkor $\mathbf{dim}_K(Hom_K(V,W)) = \mathbf{dim}_K(V) \cdot \mathbf{dim}_K(W)$.

Bizonyítás: legyenek $\mathbf{B} = \{v_\alpha \mid \alpha \in \mathbf{I}\}$ és $\{w_\beta \mid \beta \in \mathbf{J}\}$ V-beli ill. W-beli bázisok. Legyen a $\varphi_{\alpha\beta}: \mathbf{B} \to W$ leképezés a v_α helyen w_β, máshol 0. Legyen $\mathcal{A}_{\alpha\beta}: V \to W$ $\varphi_{\alpha\beta}$ lineáris kiterjesztése és $\mathbf{B}^* = \{\mathcal{A}_{\alpha\beta} \mid (\alpha,\beta) \in \mathbf{I} \times \mathbf{J}\}$. Ez nyilván független rendszer $Hom_K(V,W)$-ben (akkor is, ha $|\mathbf{B}|$ nem véges) és $|\mathbf{B}|<\infty$ esetén generálja is. Így hát bázis, amiből $|\mathbf{B}^*| = |\mathbf{I}| \cdot |\mathbf{J}|$ miatt következik az állítás második fele. ($\mathcal{A}$ egyértelmű előállítása $\mathcal{A} = \sum_{\alpha \in \mathbf{I}, \beta \in \mathbf{J}(\alpha)} c_{\alpha\beta} \cdot \mathcal{A}_{\alpha\beta}$, ahol vektor a $c_{\alpha\beta} \in K$ elemek $(v_\alpha \mathcal{A})$ együtthatói a W bázisa szerinti felírásban, $\mathbf{J}(\alpha)$ pedig az a véges részhalmaza $\mathbf{J}$-nek, amelyre $c_{\alpha\beta} \neq 0$.)

Megjegyzés: ha κ végtelen számosság és V egy $\mathbb{F}_2$ feletti κ dimenziós vektortér, akkor $\mathbf{dim}_{\mathbb{F}_2}(Hom(V,\mathbb{F}_2)) = |Hom(V,\mathbb{F}_2)| = 2^\kappa \neq \kappa$ (ld. **2.10.5**), tehát a fenti állítás megfelelője ez esetben nem teljesül.

2.5.6 Állítás: $\mathcal{A} \in Hom_K(U,V), \mathcal{B} \in Hom_K(V,W) \Rightarrow \mathcal{AB} \in Hom_K(U,W)$, ahol $\mathcal{AB}$ az $u \mapsto (u\mathcal{A})\mathcal{B}$ leképezést jelöli; nyilvánvaló.

2.5.7 Definíció: $\mathcal{A}: V \to W$ izomorfizmus, ha kölcsönösen egyértelmű homomorfizmus. Jelölése $\mathcal{A}: V \xrightarrow{\sim} W$. Ha a V,W vektorterekre található $V \xrightarrow{\sim} W$ izomorfizmus, akkor V és W izomorfak, jelölése $V \simeq W$.

Ez ekvivalencia-reláció, mert izomorfizmus inverze, izomorfizmusok kompozíciója és a $V \to V$ identikus leképezés izomorfizmusok, tehát $\simeq$ szimmetrikus, tranzitív és reflexív.

2.5.8 Definíció: az $\mathcal{A}: V \to W$ homomorfizmus epimorfizmus, ha $Im\,\mathcal{A} = W$, azaz ha szürjektív. Monomorfizmus, ha injektív. Nyilván pontosan akkor izomorfizmus, ha mindkettő.

2.5.9 Állítás: az alábbi feltételek
- **(1)** $\mathcal{A}: V \to W$ monomorfizmus,
- **(2)** $Ker\,\mathcal{A} = \{0\}$,
- **(3)** minden V-beli független rendszer képe független W-ben,
- **(4)** valamely $\mathbf{B} \subseteq V$ bázisra megszorítva $\mathcal{A}$ injektív és $\mathbf{B}$ képe független W-ben.

Bizonyítás: **(1)** $\Leftrightarrow$ **(2)**: ha $\mathcal{A}$ injektív, akkor legfeljebb egy elemre teljesül $v\mathcal{A}=0$, így csak $v=0$ lehet $Ker\,\mathcal{A}$-ban. Ha pedig $Ker\,\mathcal{A} = \{0\}$, akkor $u\mathcal{A} = v\mathcal{A} \Rightarrow (u-v)\mathcal{A} = 0 \Rightarrow u-v=0 \Rightarrow u=v$ tehát $\mathcal{A}$ valóban injektív.

(2) $\Rightarrow$ **(3)**: legyen $\mathbf{F}$ független V-ben és $Ker\,\mathcal{A} = \{0\}$. Állítsuk elő 0_W-t $\mathbf{F}$-beli elemek képeinek $0_W = \sum \alpha_k (v_k \mathcal{A})$ lineáris kombinációjaként. Ekkor $0_W = (\sum \alpha_k v_k)\mathcal{A}$, így $(\sum \alpha_k v_k) \in Ker\,\mathcal{A} = \{0_V\}$. Mivel $\mathbf{F}$ független, minden együttható 0, tehát 0_W csak triviálisan áll elő $\mathbf{F}\mathcal{A}$-beli elemek lineáris kombinációjaként, azaz $\mathbf{F}\mathcal{A}$ független.

(3) $\Rightarrow$ **(4)**: $\mathbf{B}$ képe független W-ben, hiszen $\mathbf{B}$ független V-ben. Különböző $u,v \in \mathbf{B}$ elemekre $\{u-v\} \subseteq V$ független, azaz $\{u-v\}\mathcal{A} = \{u\mathcal{A} - v\mathcal{A}\}$ is, így $u\mathcal{A} - v\mathcal{A} \neq 0$, $u\mathcal{A} \neq v\mathcal{A}$. Tehát különböző báziselemek képe különböző, $\mathcal{A}|_{\mathbf{B}}$ injektív.

(4) $\Rightarrow$ **(1)**: legyen $u,v \in V$-re $u\mathcal{A} = v\mathcal{A}$. Írjuk fel $(u-v)$-t a $\mathbf{B}$ bázisban: $u-v = \sum_{i=1}^k \alpha_k b_k$. Alkalmazva $\mathcal{A}$-t: $\sum_{i=1}^k \alpha_k (b_k \mathcal{A}) = (u-v)\mathcal{A} = u\mathcal{A} - v\mathcal{A} = 0$. Feltételeink szerint a $b_k\mathcal{A}$ vektorok páronként különböző elemei a $\mathbf{B}\mathcal{A}$ független rendszernek, azaz függetlenek. Így $\sum_{i=1}^k \alpha_k (b_k \mathcal{A}) = 0$ csak $\forall k$: $\alpha_k = 0$ esetén állhat fenn, ekkor persze $u=v$.

2.5.10 Állítás: V és W vektorterek izomorfak $\Leftrightarrow$ dimenziójuk azonos.

Bizonyítás: legyen $\mathbf{B}$ bázis V-ben, $\mathbf{B}'$ bázis W-ben.

$\Rightarrow$: legyen az izomorfizmus $\mathcal{A}$. Lineárisan független rendszer képe lineárisan független, generátorrendszer képe a képtérben generátorrendszer, azaz $\mathbf{B}$ képe bázis W-ben és $\mathcal{A}$ bijekciót létesít a $\mathbf{B} \subseteq V$ és a $\mathbf{B}\mathcal{A} \subseteq W$ bázisok közt. Ekkor $\mathbf{dim}(V) = |\mathbf{B}| = |\mathbf{B}\mathcal{A}| = \mathbf{dim}(W)$.

$\Leftarrow$: legyen $\varphi: \mathbf{B} \to \mathbf{B}'$ bijekció. φ egyértelműen kiterjed egy $\mathcal{A}_\varphi: V \to W$ homomorfizmussá. Ez szürjektív, mert $V\mathcal{A} = \langle \mathbf{B} \rangle \mathcal{A} = \langle \mathbf{B}\mathcal{A} \rangle = \langle \mathbf{B}\varphi \rangle = \langle \mathbf{B}' \rangle = W$ és injektív is, mert teljesíti **2.5.9.4**-et. Eszerint $\mathcal{A}$ izomorfizmus.

2.5.11 Következmény: van értelme „a” K feletti n dimenziós vektortérről beszélni. Ennek egy prototípusa $K^n=\{(\alpha_1,\alpha_2,\ldots,\alpha_n)\mid \alpha_i\in K\}$ a koordinátánkénti műveletekkel. Ebben az $e_i=(0,\ldots,0,1,0,\ldots,0)$ vektorok alkotta $\mathbf{E}$ bázist szoktuk természetes bázisnak hívni. Ezt a bázist azért szeretjük, mert $\mathcal{A}\in Hom(K^n,K^m)$ esetén $v\in K^n=K^{1\times n}$-re $v\mathcal{A}=v\cdot[\mathcal{A}]_{\mathbf{E},\mathbf{F}}$, ahol $\cdot$ a mátrixszorzást jelöli, $\mathbf{E}$ és $\mathbf{F}$ K^n ill. K^m természetes bázisa, $[\mathcal{A}]_{\mathbf{E},\mathbf{F}}$-et pedig mindjárt definiáljuk.

2.6 Lineáris leképezés mátrixa

2.6.1 Definíció: legyenek $\mathbf{E}=(e_i)_{i=1}^n$ illetve $\mathbf{F}=(f_i)_{i=1}^m$ bázisok a K test feletti V,W vektorterekben, $\mathcal{A}\in Hom_K(V,W)$. Írjuk fel $\mathbf{E}$ elemeinek képét $\mathbf{F}$ elemeivel: $e_i\mathcal{A}=\sum_{j=1}^m a_{ij}\cdot f_j$. Az a_{ij} számok által alkotott $n\times m$-es mátrixot hívjuk $\mathcal{A}$ mátrixának az $\mathbf{E},\mathbf{F}$ bázispárban. Jelölése $[\mathcal{A}]_{\mathbf{E},\mathbf{F}}$.

Ekkor a $v=(\sum_{i=1}^n x_i\cdot e_i)\in V$ vektor $\mathcal{A}$ szerinti képe

$$(\textstyle\sum_{i=1}^n x_i\cdot e_i)\mathcal{A}=\sum_{i=1}^n x_i\cdot(e_i\mathcal{A})=\sum_{i=1}^n x_i\cdot(\sum_{j=1}^m a_{ij}\cdot f_j)=\sum_{j=1}^m(\sum_{i=1}^n x_i a_{ij})\cdot f_j$$

Ha tehát v együtthatói az $\mathbf{E}$ szerinti felírásban $x=(x_i)_{i=1}^n$, akkor $v\mathcal{A}$ együtthatói az $\mathbf{F}$ szerinti felírásban $(\sum_{i=1}^n x_i a_{ij})_{j=1}^m=x\cdot[\mathcal{A}]_{\mathbf{E},\mathbf{F}}$.

Ha $\mathcal{A}:V\to V$ homomorfizmus, azaz lineáris transzformáció, akkor $\mathcal{A}$ mátrixát kettő helyett egy bázisban is felírhatjuk. Ekkor $[\mathcal{A}]_{\mathbf{B},\mathbf{B}}$-t $[\mathcal{A}]_{\mathbf{B}}$-vel jelöljük.

Megjegyzés: legyen $\mathcal{A}=\sum\alpha_k\mathcal{A}_k\in Hom_K(V,W)$. Ekkor nyilván bármely $\mathbf{E},\mathbf{F}$ bázispárra $[\mathcal{A}]_{\mathbf{E},\mathbf{F}}=\sum\alpha_k[\mathcal{A}_k]_{\mathbf{E},\mathbf{F}}$. Ebből látszik, hogy $Hom_K(V,W)$-nek bázisát alkotják azok a lineáris leképezések, melyek mátrixa $\mathbf{E},\mathbf{F}$-ben egy helyen 1, mindenütt másutt 0.

2.6.2 Állítás: legyen $\mathcal{A}\in Hom(U,V),\mathcal{B}\in Hom(V,W)$, $\mathbf{D},\mathbf{E},\mathbf{F}$ rendre U,V,W bázisai. Ekkor $[\mathcal{A}\mathcal{B}]_{\mathbf{D},\mathbf{F}}=[\mathcal{A}]_{\mathbf{D},\mathbf{E}}\cdot[\mathcal{B}]_{\mathbf{E},\mathbf{F}}$. (Egyszerű, érdektelen számolás.)

2.6.3 Állítás: legyen $\mathcal{A}\in Hom_K(V,W)$, $[\mathcal{A}]=\mathbf{A}\in K^{n\times k}$. Ekkor $r(\mathbf{A})=\mathbf{dim}_K(Im\,\mathcal{A})$.

Bizonyítás: $Im\,\mathcal{A}$-ban néhány V-beli báziselem képe pontosan akkor bázis, ha az ő képüket leíró sorok a mátrix sorai által feszített vektortérben bázist alkotnak (pontosan ekkor igaz, hogy függetlenek és generálják a bázis képét, ami generálja $Im\,\mathcal{A}$-t). Tehát $r_{\text{sor}}(\mathbf{A})=\mathbf{dim}_K(Im\,\mathcal{A})$.

2.6.4 Tétel: legyen $\mathcal{A}:V\to W$ lineáris leképezés, $\mathbf{E}$ és $\mathbf{E}^*$ V, $\mathbf{F}$ és $\mathbf{F}^*$ pedig W bázisai. Vigye a $\mathcal{P}:V\to V$ izomorfizmus $\mathbf{E}-$t $\mathbf{E}^*$-be, a $\mathcal{Q}:W\to W$ izomorfizmus $\mathbf{F}-$et $\mathbf{F}^*$-be. Ekkor $[\mathcal{A}]_{\mathbf{E}^*,\mathbf{F}^*}=[\mathcal{P}]_{\mathbf{E}}\cdot[\mathcal{A}]_{\mathbf{E},\mathbf{F}}\cdot[\mathcal{Q}]_{\mathbf{F}}^{-1}$.

Bizonyítás: alkalmazzuk **2.6.2**-t:

$$[\mathcal{A}]_{\mathbf{E}^*,\mathbf{F}^*}=[\mathcal{P}^{-1}\mathcal{P}\mathcal{A}\mathcal{Q}^{-1}\mathcal{Q}]_{\mathbf{E}^*,\mathbf{F}^*}=[\mathcal{P}^{-1}]_{\mathbf{E}^*,\mathbf{E}}\cdot[\mathcal{P}]_{\mathbf{E},\mathbf{E}}\cdot[\mathcal{A}]_{\mathbf{E},\mathbf{F}}\cdot[\mathcal{Q}^{-1}]_{\mathbf{F},\mathbf{F}}\cdot[\mathcal{Q}]_{\mathbf{F},\mathbf{F}^*}$$

$\mathcal{P}^{-1}$ az $\mathbf{E}^*$ elemeit rendre $\mathbf{E}$ elemeibe viszi, így $[\mathcal{P}^{-1}]_{\mathbf{E}^*,\mathbf{E}}=\mathbf{I}$. Ugyanígy $[\mathcal{Q}]_{\mathbf{F},\mathbf{F}^*}=\mathbf{I}$. A fenti szorzat két szélső tényezője tehát elhagyható. Ha még felhasználjuk, hogy $[\mathcal{Q}]_{\mathbf{F}}\cdot[\mathcal{Q}^{-1}]_{\mathbf{F}}=[\mathcal{Q}\mathcal{Q}^{-1}]_{\mathbf{F}}=\mathbf{I}$ miatt $[\mathcal{Q}^{-1}]_{\mathbf{F}}=[\mathcal{Q}]_{\mathbf{F}}^{-1}$, a bizonyítandó állítást kapjuk.

2.6.5 Következmény: legyen $\mathcal{A}:V\to V$ lineáris transzformáció, $\mathbf{E}=e_1,\ldots,e_n$ és $\mathbf{F}=f_1,\ldots,f_n$ V két bázisa. Legyen az a V feletti lineáris transzformáció, ami $\mathbf{E}$-t $\mathbf{F}$-be viszi, $\mathcal{P}$, továbbá $[\mathcal{P}]_{\mathbf{E}}=\mathbf{P}$ (azaz $f_i=\sum_{j=1}^n p_{ij}\cdot e_j$). Ekkor $[\mathcal{A}]_{\mathbf{F}}=[\mathcal{P}]_{\mathbf{E}}\cdot[\mathcal{A}]_{\mathbf{E}}\cdot[\mathcal{P}]_{\mathbf{E}}^{-1}=\mathbf{P}\cdot[\mathcal{A}]_{\mathbf{E}}\cdot\mathbf{P}^{-1}$.

2.6.6 Következmény: legyen az $\mathbf{A}\in M_n(K)$ mátrix rangja r. Ekkor alkalmas $\mathbf{P},\mathbf{Q}\in M_n(K)$ invertálható mátrixokra a $\mathbf{P}\cdot\mathbf{A}\cdot\mathbf{Q}$ mátrixban az átló első r eleme 1, minden más 0.

Bizonyítás: legyen $\mathbf{E}=(e_i)_{i=1}^n$ bázis K^n-ben. Tekintsük azt az $\mathcal{A}:K^n\to K^n$ lineáris transzformációt, amelyre $[\mathcal{A}]_{\mathbf{E}}=\mathbf{A}$. Legyen $\mathcal{P}$ olyan izomorfizmus K^n-ben, ami az $(e_i)_{i=r+1}^n$ elemeket $Ker\,\mathcal{A}$ egy bázisába viszi. Ekkor a $\mathcal{P}\mathcal{A}$ lineáris transzformáció képtere azonos $\mathcal{A}$ képterével, magtere pedig $\mathcal{A}$ magterének $\mathcal{P}$ szerinti ősképe, azaz $\langle e_i\,|\,r<i\leq n\rangle$. Az első r báziselem $\mathcal{P}\mathcal{A}$ szerinti képe lineárisan független, mert $\langle e_i\,|\,1\leq i\leq r\rangle$ független $\mathcal{P}\mathcal{A}$ magterétől. $\mathcal{P}\mathcal{A}$ képtere r dimenziós, r lineárisan független eleme már generálja. Azaz $\mathcal{P}\mathcal{A}$ izomorfizmus $\langle e_i\,|\,1\leq i\leq r\rangle$ és $Im\,\mathcal{A}$ között. Legyen $\mathcal{Q}$ olyan izomorfizmus K^n-ben, ami $Im\,\mathcal{A}$-n $\mathcal{P}\mathcal{A}$ inverze. Ekkor a $\mathcal{P}\mathcal{A}\mathcal{Q}$ lineáris transzformáció $\langle e_i\,|\,1\leq i\leq r\rangle$-re megszorítva identitás, $\langle e_i\,|\,r<i\leq n\rangle$-re megszorítva azonosan nulla (hiszen ezekre már $\mathcal{P}\mathcal{A}$ is azonosan 0). $\mathbf{P}=[\mathcal{P}]_{\mathbf{E}}$, $\mathbf{Q}=[\mathcal{Q}]_{\mathbf{E}}$ megfelel a feltételeknek.

2.6.7 Állítás: ha $\mathbf{P},\mathbf{Q}$ invertálható mátrixok, akkor $r(\mathbf{PAQ})=r(\mathbf{A})$.

Bizonyítás: válasszunk olyan $\mathcal{A}: V\to W, \mathcal{P}: V\to V, \mathcal{Q}: W\to W$ lineáris leképezéseket, melyekre $[\mathcal{A}]=\mathbf{A},[\mathcal{P}]=\mathbf{P},[\mathcal{Q}]=\mathbf{Q}$. Persze $\mathcal{P},\mathcal{Q}$ izomorfizmusok lesznek. Ekkor $Im(\mathcal{PAQ})=Im(\mathcal{AQ})=(V\mathcal{A})\mathcal{Q}\simeq V\mathcal{A}$, azaz $\mathbf{dim}(Im(\mathcal{PAQ}))=\mathbf{dim}(V\mathcal{A})$.

2.7 Faktortér, homomorfizmus-tétel

Legyen $U\le V$. Tekintsük a $v+U=\{v+u \mid u\in U\}$ halmazokat, ahol v befutja V-t. ($v+U$-t $[\![v]\!]$-vel fogom jelölni; szokták $\overline{v}$-vel is.) Ezek partícionálják (diszjunkt részhalmazok uniójára bontják) V-t, mert $[\![v_1]\!]$ és $[\![v_2]\!]$ vagy diszjunkt, ha $v_1-v_2\notin U$, vagy azonos, ha $v_1-v_2\in U$. A műveletek legyenek a következők: $[\![v_1]\!]+[\![v_2]\!]=[\![v_1+v_2]\!]$, $\alpha\cdot[\![v]\!]=[\![\alpha\cdot v]\!]$. Ha belátjuk, hogy ezek a műveletek jóldefiniáltak, akkor vektorteret kapunk, mert a műveleti szabályok átöröklődnek.

Tegyük fel, hogy $[\![v]\!]=[\![v']\!]$. Ekkor $v-v'\in U$, így $(v+w)-(v'+w)=v-v'\in U$, azaz $[\![v+w]\!]=[\![v'+w]\!]$, továbbá $\alpha\cdot v-\alpha\cdot v'=\alpha\cdot(v-v')\in U$, azaz $[\![\alpha\cdot v]\!]=[\![\alpha\cdot v']\!]$. Eszerint a műveletek valóban egyértelműek. Az (additív) egységelem $[\![0]\!]=U$.

2.7.1 Definíció: a fenti struktúra a V/U faktortér, a $\psi_U: v\mapsto[\![v]\!]$ leképezés a $V\to V/U$ természetes homomorfizmus.

2.7.2 Definíció: legyen $\mathcal{A}: V\to W$ lineáris leképezés, $U\le V$. Ekkor $\mathcal{A}$ megszorítása U-ra az az $\mathcal{A}|_U: U\to W$ leképezés, amelyre $\forall u\in U$: $u(\mathcal{A}|_U)=u\mathcal{A}$. Nyilván $\mathcal{A}$ is lineáris leképezés.

Megjegyzés: $Ker(\mathcal{A}|_U)=U\cap(Ker\,\mathcal{A})$.

2.7.3 Homomorfizmus-tétel: ha $\mathcal{A}\in Hom(V,V_1)$, akkor $Im\,\mathcal{A}\simeq V/Ker\,\mathcal{A}$.

Bizonyítás: legyen $\mathbf{F}$ bázis $Ker\,\mathcal{A}=W$-ben. Egészítsük ezt ki az $\mathbf{E}$ független rendszerrel V bázisává, Legyen $U=\langle\mathbf{E}\rangle$. Ekkor $V=U\oplus W$, amiből $Im\,\mathcal{A}=V\mathcal{A}=(U+W)\mathcal{A}=U\mathcal{A}+W\mathcal{A}=Im(\mathcal{A}|_U)+Im(\mathcal{A}|_W)=Im(\mathcal{A}|_U)+\{0\}=Im(\mathcal{A}|_U)$. Továbbá $Ker(\mathcal{A}|_U)=U\cap Ker\,\mathcal{A}=0$.

Eszerint $\mathcal{A}|_U$ monomorfizmus, így izomorfizmus U és $Im\,\mathcal{A}$ között, $U\simeq Im\,\mathcal{A}$. Alkalmazva ezt $\psi_W: V\to V/W$-ra $Ker(\psi_W)=W$ miatt választhatjuk $\mathbf{F}$-et, így $\mathbf{E}$-t és U-t ugyanannak, mint az előbb, ekkor $Im\,\mathcal{A}\simeq U\simeq Im(\psi_W)=V/U$.

2.7.4 Következmény: $\mathcal{A}: V\in Hom(V,V_1)$ esetén $\mathbf{dim}(V)=\mathbf{dim}(Im\,\mathcal{A})+\mathbf{dim}(Ker\,\mathcal{A})$. Speciálisan a ψ_U faktorleképezésre $\mathbf{dim}(V/U)+\mathbf{dim}(U)=\mathbf{dim}(V)$.

Bizonyítás: a fenti bizonyítás jelöléseivel $Im\,\mathcal{A}\simeq U$, így $\mathbf{dim}(Im\,\mathcal{A})=\mathbf{dim}(U)$. $V=U\oplus Ker\,\mathcal{A}$ miatt pedig $\mathbf{dim}(V)=\mathbf{dim}(U)\oplus\mathbf{dim}(Ker\,\mathcal{A})$, ld. **2.4.4**.

2.7.5 Állítás: $\mathbf{A}\in K^{n\times k},\mathbf{B}\in K^{k\times m}$ esetén $r(\mathbf{A})+r(\mathbf{B})-k\le r(\mathbf{AB})\le\mathbf{min}(r(\mathbf{A}),r(\mathbf{B}))$.

Bizonyítás: legyen $\mathcal{A}\in Hom(K^n,K^k),\mathcal{B}\in Hom(K^k,K^m)$ és a természetes bázisokban $[\mathcal{A}]=\mathbf{A},[\mathcal{B}]=\mathbf{B}$. Ekkor

$$r(\mathbf{AB})=\mathbf{dim}(Im\,\mathcal{AB})=\mathbf{dim}(Im(\mathcal{B}|_{Im\,\mathcal{A}}))=\mathbf{dim}(Im\,\mathcal{A})-\mathbf{dim}(Ker(\mathcal{B}|_{Im\,\mathcal{A}}))=r(\mathbf{A})-\mathbf{dim}(Im\,\mathcal{A}\cap Ker\,\mathcal{B})=r(\mathcal{A})-d$$

$(Im\,\mathcal{A}\cap Ker\,\mathcal{B})\le Ker\,\mathcal{B}$-ból $d\le\mathbf{dim}(Ker\,\mathcal{B})=k-r(\mathbf{B})$, azaz $r(\mathbf{A})-k+r(\mathbf{B})\le r(\mathbf{A})-d=r(\mathbf{AB})$. $Im\,\mathcal{AB}\le Im\,\mathcal{B}$ alapján $r(\mathbf{AB})\le r(\mathbf{B})$, $0\le d$-ből $r(\mathbf{AB})\le r(\mathbf{A})$.

2.7.6 Következmény: $\mathbf{A}\in M_n(K)$ esetén $\forall k\in\mathbb{N}$: $r(\mathbf{A}^k)\ge k\cdot r(\mathbf{A})-(k-1)\cdot n$.

Bizonyítás: $k=0,1$ esetén egyenlőség áll fenn. Ezután indukcióval

$$r(\mathbf{A}^{k+1})=r(\mathbf{A}^k\cdot\mathbf{A})\ge r(\mathbf{A}^k)+r(\mathbf{A})-n\ge k\cdot r(\mathbf{A})-(k-1)\cdot n+r(\mathbf{A})-n=(k+1)\cdot r(\mathbf{A})-k\cdot n.$$

2.8 Sajátérték, sajátvektor, karakterisztikus polinom

2.8.1 Definíció: az $\mathcal{A}: V\to V$ lineáris transzformációnak $v\in V\setminus\{0\}$ sajátvektora a $\lambda\in K$ sajátértékkel, ha $v\mathcal{A}=\lambda\cdot v$. A sajátértékek halmazát a transzformáció ill. a hozzátartozó mátrix spektrumának hívjuk, jelölése $\sigma(\mathcal{A})$ ill. $\sigma(\mathbf{A})$.

Legyen most $\mathbf{dim}_K(V)=n<\infty$. Ekkor $\mathbf{dim}_K(Hom_K(V,V))=n^2$, így az $\mathbf{I},\mathcal{A},\mathcal{A}^2,\dots,\mathcal{A}^{n^2}$ elemek lineárisan összefüggnek. Eszerint $\mathcal{A}$ gyöke egy legfeljebb n^2+1-edfokú polinomnak. Többek közt ezen az n^2+1-en szeretnénk javítani.

2.8.2 Definíció: az $\mathbf{A},\mathbf{B}\in M_n(K)$ mátrixok hasonlóak, ha alkalmas $\mathbf{P}\in M_n(K)$ invertálható mátrixra $\mathbf{B}=\mathbf{P}^{-1}\mathbf{AP}$. Jelölése $\mathbf{A}\sim\mathbf{B}$.

Megjegyzés: egyazon lineáris transzformáció különböző bázisban felírt mátrixai **2.6.5** szerint hasonlóak.

2.8.3 Definíció: az $\mathbf{A}\in M_n(K)$ mátrix karakterisztikus polinomja $\chi_{\mathbf{A}}(\lambda)=\mathbf{det}(\lambda\cdot\mathbf{I}-\mathbf{A})=\lambda^n+\alpha_{n-1}\lambda^{n-1}+\dots$ $\dots+\alpha_1\lambda+\alpha_0\in K[\lambda]$. Nyilván $\alpha_0=(-1)^n\cdot\mathbf{det}(\mathbf{A})$ és $\alpha_{n-1}=-\mathbf{tr}(\mathbf{A})$.

2.8.4 Állítás: hasonló mátrixok karakterisztikus polinomja azonos.

$$\mathbf{det}(\lambda\mathbf{I}-\mathbf{PAP}^{-1})=\mathbf{det}(\mathbf{P}\lambda\mathbf{IP}^{-1}-\mathbf{PAP}^{-1})=\mathbf{det}(\mathbf{P}(\lambda\mathbf{I}-\mathbf{A})\mathbf{P}^{-1})=\mathbf{det}(\mathbf{P})\cdot\mathbf{det}(\lambda\mathbf{I}-\mathbf{A})\cdot\mathbf{det}(\mathbf{P}^{-1})=\mathbf{det}(\lambda\mathbf{I}-\mathbf{A})$$

2.8.5 Definíció: az $\mathcal{A}:V\to V$ lineáris transzformáció karakterisztikus polinomja $\chi_{\mathcal{A}}(\lambda)=\chi_{[\mathcal{A}]}(\lambda)\in K[\lambda]$. Előző állításunk szerint $\chi_{[\mathcal{A}]}(\lambda)$ nem függ attól, hogy $[\mathcal{A}]$-t melyik bázisban írjuk fel, tehát a definíció értelmes.

2.8.6 Definíció: λ-mátrix: olyan $n\times n$-es mátrix, amelynek elemei $K[\lambda]$-beli polinomok; azaz $M_n(K[\lambda])$ egy eleme.

2.8.7 Cayley-Hamilton tétel: minden $\mathbf{A}\in M_n(K)$ mátrix gyöke a saját karakterisztikus polinomjának, azaz $\chi_{\mathbf{A}}(\mathbf{A})=0$.

Bizonyítás: legyen $\mathbf{B}$ az az $n\times n$-es λ-mátrix, amelyben b_{ij} a $(\lambda\mathbf{I}-\mathbf{A})$ mátrix j-edik sorához és i-edik oszlopához tartozó előjeles aldetermináns. Minden b_{ij} egy legfeljebb $(n-1)$-edfokú $K[\lambda]$-beli polinom. Legyen $0\le k\le(n-1)$-re $\mathbf{B}^{(k)}$ az a mátrix, amelynek elemei $\mathbf{B}$ megfelelő helyen lévő elemeinek λ^k-hoz tartozó együtthatói. Ekkor $(\mathbf{B}^{(0)}+\lambda\mathbf{B}^{(1)}+\dots+\lambda^{n-1}\mathbf{B}^{(n-1)})(\lambda\mathbf{I}-\mathbf{A})=\mathbf{B}(\lambda\mathbf{I}-\mathbf{A})=\mathbf{det}(\lambda\mathbf{I}-\mathbf{A})\cdot\mathbf{I}=\chi_{\mathbf{A}}(\lambda)\cdot\mathbf{I}$. Azonos λ-polinomok együtthatói azonosak:

$$\begin{aligned}-\mathbf{B}^{(0)}\cdot\mathbf{A}&=\alpha_0\cdot\mathbf{I}\\-\mathbf{B}^{(1)}\cdot\mathbf{A}+\mathbf{B}^{(0)}&=\alpha_1\cdot\mathbf{I}\\&\vdots\\-\mathbf{B}^{(n-1)}\cdot\mathbf{A}+\mathbf{B}^{(n-2)}&=\alpha_{n-1}\cdot\mathbf{I}\\\mathbf{B}^{(n-1)}&=\mathbf{I}\end{aligned}$$

Szorozzuk meg jobbról az első egyenletet $\mathbf{A}^0=\mathbf{I}$-vel, a másodikat $\mathbf{A}$-val, a harmadikat $\mathbf{A}^2$-el stb., az utolsót $\mathbf{A}^n$-el és adjuk őket össze. Baloldalt minden kiesik, jobboldalt pedig $\chi_{\mathbf{A}}(\mathbf{A})$-t kapunk. Ezzel az állítást beláttuk.

2.8.8 Tétel: legyen $\mathcal{A}\in Hom(V,V)$. Ekkor $\lambda\in K$ pontosan akkor sajátérték, ha $\chi_{\mathcal{A}}(\lambda)=0$.

Bizonyítás: legyen $\mathbf{E}=e_1\dots e_n$ tetszőleges bázis, $v=\sum_{i=1}^n x_ie_i$, $x=(x_1,\dots,x_n)$. $v\mathcal{A}=\lambda\cdot v$ pontosan akkor teljesül, ha $x\cdot[\mathbf{A}]_{\mathbf{E}}=\lambda\cdot x$. Pontosan akkor található $v\neq0$, amelyre $v\mathcal{A}=\lambda\cdot v$, ha van nem triviális megoldása az $x\cdot(\lambda\mathbf{I}-\mathbf{A})=0$ egyenletrendszernek, ami a Cramer-szabály szerint ekvivalens $\mathbf{det}(\lambda\mathbf{I}-\mathbf{A})=0$-val.

2.8.9 Definíció: egy $\mathcal{A}\in Hom(V,V)$ λ sajátértékéhez tartozó sajátaltér $V_\lambda=\{v\in V\mid v\mathcal{A}=\lambda\cdot v\}$. Ez valóban altér lesz, mert benne van a 0 (bár a 0-t nem nevezzük sajátvektornak) és a műveletekre zárt, ugyanis ha $v_1\mathcal{A}=\lambda v_1, v_2\mathcal{A}=\lambda v_2$, akkor a lineáris transzformációk alaptulajdonságai miatt $(\alpha\cdot v_1+\beta\cdot v_2)\mathcal{A}=\lambda\cdot(\alpha\cdot v_1+\beta\cdot v_2)$, azaz egyazon λ-hoz tartozó sajátvektorok lineáris kombinációja is sajátvektor ugyanazzal a λ sajátértékkel.

2.8.10 Definíció: $\mathcal{A}\in Hom_K(V,V)$ λ sajátértékének algebrai multiplicitása (l) annyi, ahányszoros gyöke λ a karakterisztikus polinomnak, geometriai multiplicitása (k) pedig $\mathbf{dim}_K(V_\lambda)$.

2.8.11 Állítás: a λ_0 sajátérték geometriai multiplicitása nem nagyobb az algebrai multiplicitásnál.

Bizonyítás: vegyük V_λ egy $e_1\dots e_k$ bázisát, és egészítsük ki V bázisává $e_{k+1}\dots e_n$-el. Írjuk fel $\mathcal{A}$ mátrixát ebben a bázisban. Ezen $\mathbf{A}$ mátrix első k sorában a főátlón λ_0 lesz, máshol 0. Eszerint $(\lambda\mathbf{I}-\mathbf{A})$ kifejtésénél csak úgy kapunk nem 0 tagokat, ha az első k sorából $(\lambda-\lambda_0)$-t veszünk, tehát $\chi_{\mathbf{A}}(\lambda)=(\lambda-\lambda_0)^k\cdot(\dots)$.

Például az $\mathbf{A}=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\in M_2(K)$ mátrixra $\chi_{\mathbf{A}}(\lambda)=(\lambda-1)^2$, de $\lambda_0=1$ geometriai multiplicitása nem lehet 2, mert akkor $V_\lambda=V$ lenne, viszont az első bázisvektor képe nem önmaga, tehát nincs benne V_λ-ban. Az algebrai multiplicitás nyilván 2, azaz itt $k\neq l$. Ez egyben arra is példa, hogy ha két különböző transzformáció karakterisztikus polinomja azonos, attól még lehetnek különbözőek, hiszen a fenti $\mathbf{A}$ mátrix és $\mathbf{I}\in M_2(K)$ karakterisztikus polinomja azonos. Az viszont igaz, hogy ha két mátrix karakterisztikus polinomja megegyezik és minden gyöke egyszeres, akkor a két mátrix hasonló.

2.8.12 Definíció: $\mathbf{A}\in M_n(K)$ minimálpolinomja az a legalacsonyabb fokú egy főegyütthatójú $\varphi_{\mathbf{A}}(x)\in K[x]$ polinom, amelynek $\mathbf{A}$ gyöke. (Két ilyen nem létezhet, mert akkor azok különbségének skalárszorosa alacsonyabb fokú, egy főegyütthatójú polinom lenne, amelynek szintén gyöke lenne $\mathbf{A}$. Egy pedig van, mert van olyan polinom – $\chi_{\mathbf{A}}(x)$ – aminek $\mathbf{A}$ gyöke.)

2.8.13 Állítás: pontosan azoknak a polinomoknak gyöke $\mathbf{A}$, amelyeket $\varphi_{\mathbf{A}}(x)$ oszt., speciálisan $\varphi_{\mathbf{A}}(x)\,|\,\chi_{\mathbf{A}}(x)$.

Bizonyítás: ha p-nek gyöke $\mathbf{A}$, akkor osszuk el maradékosan $\varphi_{\mathbf{A}}(x)$-el: $p(x)=q(x)\cdot\varphi_{\mathbf{A}}(x)+r(x)$ Ekkor $r(\mathbf{A})=p(\mathbf{A})-q(\mathbf{A})\varphi_{\mathbf{A}}(\mathbf{A})=0$ és r foka alacsonyabb $\varphi_{\mathbf{A}}$ fokánál, vagy $r\equiv 0$. $\varphi_{\mathbf{A}}$ definíciója miatt csak ez utóbbi állhat fenn, azaz $\varphi_{\mathbf{A}}$ osztja p-t. Ha pedig $\varphi_{\mathbf{A}}$ osztja p-t, akkor nyilván gyöke $\mathbf{A}$. (Felhasználtuk, hogy az együtthatók a test elemei, amelyek mindennel felcserélhetőek, azaz a behelyettesítés felcserélhető a polinomok szorzásával.)

2.8.14 Állítás: hasonló mátrixok minimálpolinomjai azonosak.

Bizonyítás: tetszőleges $p(x)=\sum_{k=1}^{n}a_kx^k$ polinomra $p(\mathbf{PAP}^{-1})=\mathbf{P}\cdot p(\mathbf{A})\cdot\mathbf{P}^{-1}$, mert $a_k(\mathbf{PAP}^{-1})^k=\mathbf{P}(a_k\mathbf{A}^k)\mathbf{P}^{-1}$ miatt $p(x)=\sum_{k=1}^{n}a_k(\mathbf{PAP}^{-1})^k=\mathbf{P}\cdot\left(\sum_{k=1}^{n}a_k\mathbf{A}^k\right)\mathbf{P}^{-1}=\mathbf{P}\cdot p(\mathbf{A})\cdot\mathbf{P}^{-1}$. Ez alapján két hasonló mátrix pontosan ugyanazoknak a polinomoknak gyöke.

2.9 Invariáns altér. Reducibilis és direkt összeg mátrixok

2.9.1 Definíció: legyen a V vektortéren adott egy $\mathcal{A}$ lineáris transzformáció. V egy U altere $\mathcal{A}$-ra invariáns altér, ha $\forall x\in U$: $x\mathcal{A}\in U$. Nem triviális invariáns altér, ha invariáns altér és $\{0\}<U<V$.

2.9.2 Definíció: ha U $\mathcal{A}$-ra invariáns altér, akkor V/U-n legyen $\bar{\mathcal{A}}$ (esetleg $[\![\mathcal{A}]\!]$) az a leképezés, melyre $[\![v]\!]\bar{\mathcal{A}}=[\![v\mathcal{A}]\!]$. Ugyanúgy, ahogy a V/U feletti összeadás és skalárral szorzás, $\bar{\mathcal{A}}$ is jóldefiniált és könnyen láthatóan lineáris.

Megjegyzés: legyen $\mathcal{A}\colon V\to V$ lineáris transzformáció, U $\mathcal{A}$-ra invariáns altér. Ekkor $Im(\mathcal{A}|_U)\le U$, azaz $\mathcal{A}|_U$ tekinthető U feletti lineáris transzformációnak; általában annak is tekintjük.

2.9.3 Definíció: az $\mathbf{A}$ négyzetes mátrix az $\mathbf{A}_1,\dots,\mathbf{A}_k$ négyzetes mátrixok direkt összege, ha a főátlója mentén ezek a mátrixok vannak sorban ($\mathbf{A}_i$ főátlója ráesik $\mathbf{A}$ főátlójára) és mindenhol máshol csupa 0 van. Jelölése $\mathbf{A}=\mathbf{A}_1\oplus\mathbf{A}_2\oplus\ldots\oplus\mathbf{A}_k$.

Definíció: egy $\mathbf{A}$ négyzetes mátrix reducibilis, ha $\begin{pmatrix}\mathbf{A}_1 & 0\\ * & \mathbf{A}_2\end{pmatrix}$ vagy $\begin{pmatrix}\mathbf{A}_1 & *\\ 0 & \mathbf{A}_2\end{pmatrix}$ alakú, ahol $\mathbf{A}_1$ és $\mathbf{A}_2$ négyzetes mátrixok. (Hogy ezek közül melyik, az lényegtelen, ugyanis ha $\mathbf{A}$ $\begin{pmatrix}\mathbf{A}_2 & *\\ 0 & \mathbf{A}_1\end{pmatrix}$ alakú, akkor $\begin{pmatrix}\mathbf{A}_1 & 0\\ * & \mathbf{A}_2\end{pmatrix}$ alakúvá tehető olyan sor- és oszlopcserékkel, ahol a sorokat és az oszlopokat egyformán permutáljuk. Az így kapott mátrix hasonló lesz $\mathbf{A}$-hoz, mert ez egy lineáris leképezés mátrixánál a báziselemek permutálásának felel meg. Így megtehetjük, hogy reducibilis mátrix alatt mindig az első esetet értjük, ha a mátrixok csak hasonlóság erejéig érdekelnek minket.) Minden direkt összegre bomló mátrix reducibilis. $\mathbf{A}_1,\mathbf{A}_2$-t $\mathbf{A}$ faktorainak hívjuk.

2.9.4 Állítás: Reducibilis mátrixra $\chi_{\mathbf{A}}(\lambda)=\chi_{\mathbf{A}_1}(\lambda)\cdot\chi_{\mathbf{A}_2}(\lambda)$.

Bizonyítás: $\mathbf{det}(\mathbf{A})=\mathbf{det}(\mathbf{A}_1)\cdot\mathbf{det}(\mathbf{A}_2)$, mert csak akkor kaphatunk nem 0 kifejtési tagokat, ha $\mathbf{A}_1$ és $\mathbf{A}_2$ egy-egy kifejtési tagját párosítjuk össze. $(\lambda\mathbf{I}-\mathbf{A})$ is reducibilis, a faktorok $(\lambda\mathbf{I}-\mathbf{A}_1)$ és $(\lambda\mathbf{I}-\mathbf{A}_2)$, azaz $\mathbf{det}(\lambda\mathbf{I}-\mathbf{A})=\mathbf{det}(\lambda\mathbf{I}-\mathbf{A}_1)\cdot\mathbf{det}(\lambda\mathbf{I}-\mathbf{A}_2)$.

2.9.5 Megjegyzés: direkt összegre bomló mátrix minimálpolinomja a faktorok minimálpolinomjainak legkisebb közös többszöröse. Ugyanis egy ilyen mátrixot behelyettesítve egy polinomba ugyanazt kapjuk, mintha a faktorait helyettesítenénk be és aztán raknánk össze.

2.9.6 Állítás: legyen U nem triviális, $\mathcal{A}$-ra invariáns altér $V-$ben, $\mathbf{E}=\{e_1\dots e_k\}$ U egy bázisa. Egészítsük ki $\mathbf{E}$-t a $\mathbf{F}=\{e_{k+1}\dots e_n\}$ vektorokkal V bázisává, jelölje $\{[\![e_{k+1}]\!]\dots[\![e_n]\!]\}$-t $[\![\mathbf{F}]\!]$. Ekkor $\mathbf{A}=[\mathcal{A}]_{\mathbf{E}\cup\mathbf{F}}$ reducibilis az $[\mathcal{A}|_U]_{\mathbf{E}}$, $[\bar{\mathcal{A}}]_{[\![\mathbf{F}]\!]}$ faktorokkal. ($[\![\mathbf{F}]\!]$ bázis V/U-ban a homomorfizmus-tétel bizonyítása alapján, tehát $[\bar{\mathcal{A}}]_{[\![\mathbf{F}]\!]}$ értelmes.)

Bizonyítás: $\mathbf{A}$ első k sorában rendre $e_1\dots e_k$ képei vannak, így itt az első k oszlopban $[\mathcal{A}|_U]_{\mathbf{E}}$ szerepel, a többi oszlopban csupa 0.

$$\forall i\in\{1\ldots(n-k)\}:\ [\![e_{i+(n-k)}]\!]\overline{\mathcal{A}}=[\![e_{i+(n-k)}\mathcal{A}]\!]=\sum_{j=1}^{n}[\![a_{i+(n-k),j}\cdot e_j]\!]=\sum_{j=1}^{n}a_{i+(n-k),j}\cdot[\![e_j]\!]=\sum_{j=1}^{n-k}a_{i+(n-k),j+(n-k)}[\![e_{j+(n-k)}]\!]$$

Eszerint $\overline{\mathcal{A}}$ mátrixa az $\{[\![e_{k+1}]\!]\ldots[\![e_n]\!]\}$ bázisban az az $(n-k)\times(n-k)$-as mátrix, melyben az i-edik sor j-edik eleme $a_{i+(n-k),j+(n-k)}$. Ezzel az állítást beláttuk.

2.9.7 Állítás: legyen $\mathcal{A}$ mátrixa az $\mathbf{A}_1\in M_k(K)$ és az $\mathbf{A}_2\in M_{n-k}(K)$ mátrixok direkt összege az $\{e_1\ldots e_n\}$ bázisban. Ekkor a $V_1=\langle e_1\ldots e_k\rangle, V_2=\langle e_{k+1},\ldots,e_n\rangle$ alterek invariánsak $\mathcal{A}$-ra és V ezek direkt összege. Nyilvánvaló.

Az sajnos nem igaz, hogy minden reducibilis hasonló egy olyanhoz, ami direkt összegre bomlik. Viszont

2.9.8 Állítás: ha valamely $\mathbf{A}_1,\mathbf{A}_2,\mathbf{A}_3$ mátrixokra $\mathbf{A}=\left(\begin{smallmatrix}\mathbf{A}_1 & 0\\ * & \mathbf{A}_2\end{smallmatrix}\right)\sim\mathbf{A}_1\oplus\mathbf{A}_3$, akkor $\mathbf{A}\sim\mathbf{A}_1\oplus\mathbf{A}_2$.

2.10 Végtelen dimenziós vektorterek

Bebizonyítunk néhány alapvető állítást végtelen dimenziós vektorterekre is, melyeket véges dimenziósakra már ismerünk. Jelöljön az alábbiakban V egy K feletti vektorteret.

2.10.1 Tétel: **(1)** minden V-beli $\mathbf{F}$ független rendszer kiegészíthető bázissá és **(2)** minden V-beli $\mathbf{X}$ generátorrendszer tartalmaz bázist.

Bizonyítás: **(1)** vegyük észre, hogy $\mathbf{F}$-et tartalmazó független rendszerek $\mathcal{L}$ láncának uniója is $\mathbf{F}$-et tartalmazó független rendszer. $\mathbf{F}\subseteq\bigcup\mathcal{L}$ nyilvánvaló, ha pedig $\bigcup\mathcal{L}$ nem lenne független, akkor lenne egy $\mathbf{H}$ véges elemszámú, lienárisan összefüggő részhalmaza. Ez csak úgy lehet $\bigcup\mathcal{L}$ része, ha valamely $\mathbf{L}\in\mathcal{L}$-re $\mathbf{H}\subseteq\mathbf{L}$, ami ellentmond $\mathbf{L}$ függetlenségének.

Az $\mathbf{F}$-et fedő független rendszerekre tehát teljesülnek a Zorn-lemma feltételei, tehát van köztük (tartalmazásra nézve) maximális elem. Ez nyilván maximális független rendszer, azaz bázis.

(2) A fentihez hasonló módon belátható, hogy az $\mathbf{X}$-beli független rendszerek teljesülnek a Zorn-lemma feltételei, azaz van köztük (tartalmazásra nézve) maximális – legyen ez $\mathbf{M}$. Persze $\mathbf{X}\setminus\mathbf{M}$ egyik eleme sem lehet független $\mathbf{M}$-től, mert nem vehető hozzá úgy, hogy független maradjon. Ezért $\mathbf{M}$ generálja $\mathbf{X}$-et, így V-t is. Mivel független, $\mathbf{M}$ minimális generátorrendszer, azaz bázis.

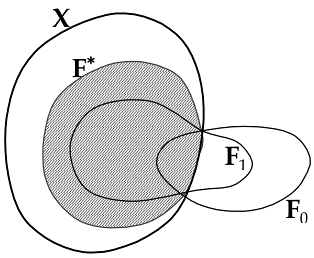
2.10.2 Következmény: minden vektortérnek van bázisa. Ugyanis a $\emptyset$ független rendszer kiegészíthető bázissá.

2.10.3 Tétel: legyen $\mathbf{X}$ generátorrendszer V-ben. Ekkor V-ben minden független rendszer legfeljebb $|\mathbf{X}|$ számosságú.

Bizonyítás: válasszunk egy tetszőleges $\mathbf{F}_0$ független rendszert. Definiáljuk $\mathcal{P}(V)$ felett az alábbi relációt:

$$\mathbf{H}\preceq\mathbf{H}'\ \Leftrightarrow\ \begin{cases}(\mathbf{H}\cap\mathbf{X})\subseteq(\mathbf{H}'\cap\mathbf{X})\\ (\mathbf{H}'\setminus\mathbf{X})\subseteq(\mathbf{H}\setminus\mathbf{X})\\ |\mathbf{H}\setminus\mathbf{H}'|\le|\mathbf{H}'\setminus\mathbf{H}|\end{cases}$$

(Tehát egy $\mathbf{H}$ halmazból úgy kapunk egy „nagyobb" $\mathbf{H}'$-t, hogy $\mathbf{X}$-en kívüli részéből elhagyunk valamennyit és legalább annyit hozzáveszünk az $\mathbf{X}$-beli részéhez.) Könnyen ellenőrizhető, hogy $\preceq$ részbenrendezés, továbbá $\mathbf{H}\preceq\mathbf{H}'$ esetén $|\mathbf{H}|\le|\mathbf{H}'|, (\mathbf{H}'\setminus\mathbf{H})\subseteq\mathbf{X}$ és $\mathbf{H}\setminus\mathbf{H}'$ diszjunkt $\mathbf{X}$-től. Legyen $\Omega=\{\mathbf{F}\subseteq V\,|\,\mathbf{F}_0\preceq\mathbf{F}$ és $\mathbf{F}$ független$\}$. Tegyük fel, hogy Ω-nak van a $\preceq$ relációra nézve maximális eleme, $\mathbf{F}^*$. Azt állítjuk, hogy ekkor $\mathbf{F}^*\subseteq\mathbf{X}$.



$\lightning$ $\exists v\in\mathbf{F}^*\setminus\mathbf{X}$. Mivel $\mathbf{X}$ generátorrendszer, v függ $\mathbf{X}$-től. Legyen $x\in\mathbf{X}$ tetszőleges, $\mathbf{F}^\circ=\mathbf{F}^*\setminus\{v\}\cup\{x\}$. Mivel $\mathbf{F}^*\preceq\mathbf{F}^\circ$, $\mathbf{F}^*$ maximalitása miatt $\mathbf{F}^\circ\notin\Omega$. A tranzitivitásból $\mathbf{F}_0\preceq\mathbf{F}^\circ$, így $\mathbf{F}^\circ$ a másik feltételt kell megsértse, azaz lineárisan összefüggő. Ezért x függ $\mathbf{F}^*\setminus\{v\}$-től. Ez $\mathbf{X}$ minden elemére teljesül, tehát $\mathbf{F}^*\setminus\{v\}$ generálja $\mathbf{X}$-et. Másrészt $v\in V=\langle\mathbf{X}\rangle$, összefoglalva v függ $\mathbf{F}^*\setminus\{v\}$-től. Ez $\mathbf{F}^*$ függetlensége miatt $\lightning$.

Valóban, $\mathbf{F}^*\subseteq\mathbf{X}$. Ekkor $\mathbf{F}_0\preceq\mathbf{F}^*$ figyelembevételével $|\mathbf{F}_0|\le|\mathbf{F}^*|\le|\mathbf{X}|$, a bizonyítandó állítás igaz. Most már elég belátnunk, hogy Ω-nak van a $\preceq$ relációra nézve maximális eleme. Ehhez azt fogjuk igazolni, hogy Ω-ra teljesülnek a Zorn-lemma feltételei. $\mathbf{F}_0\in\Omega$ nyilvánvaló, tehát Ω nem üres.

Legyen $\mathcal{L}=\{\mathbf{F}_\alpha|\alpha\in\mathbf{I}\}\subseteq\Omega$ lánc a $\preceq$ relációra és lássuk be, hogy van Ω-beli korlátja. Mivel $\mathbf{F}_0$ a legkisebb Ω-beli elem, $\mathbf{F}_0\in\mathcal{L}$ feltehető. Vezessük be $\mathbf{I}$ felett a $\alpha\le\alpha' \Leftrightarrow \mathbf{F}_\alpha\preceq\mathbf{F}_{\alpha'}$ rendezést. Jelölje $\mathbf{F}_\alpha$ $\mathbf{X}$-beli részét $\mathbf{M}_\alpha$, $\mathbf{X}$-en kívüli részét $\mathbf{C}_\alpha$. Ekkor az, hogy $\mathcal{L}$ lánc, azt jelenti, hogy $\alpha\le\alpha'$ esetén $\mathbf{M}_\alpha\subseteq\mathbf{M}_{\alpha'},\mathbf{C}_{\alpha'}\subseteq\mathbf{C}_\alpha$ és $\boxdot$ $|\mathbf{C}_\alpha\setminus\mathbf{C}_{\alpha'}|\le|\mathbf{M}_{\alpha'}\setminus\mathbf{M}_\alpha|$. Az $\boxdot$ egyenlőtlenség $\alpha>\alpha'$ esetén is teljesül, hiszen ekkor mindkét oldal 0. Legyen $\mathbf{F}^*$ az a halmaz, melynek $\mathbf{X}$-beli része $\mathbf{F}^*\cap\mathbf{X}=\mathbf{M}^*=\bigcup_{\alpha\in\mathbf{I}}\mathbf{M}_\alpha$, $\mathbf{X}$-en kívüli része $\mathbf{F}^*\setminus\mathbf{X}=\mathbf{C}^*=\bigcap_{\alpha\in\mathbf{I}}\mathbf{C}_\alpha$. Azt akarjuk belátni, hogy $\mathbf{F}^*\in\Omega$ és $\mathbf{F}^*$ felső korlátja $\mathcal{L}$-nek.

$\mathbf{F}^*$ lineárisan független lesz, mert minden véges elemszámú $\mathbf{H}$ részhalmazához található olyan α, hogy $\mathbf{H}\subseteq\mathbf{F}_\alpha$ és $\mathbf{F}_\alpha$ független, tehát $\mathbf{H}$ is független. Már csak az van hátra, hogy bármely $\beta\in\mathbf{I}$ elemre $\mathbf{F}_\beta\preceq\mathbf{F}^*$ (ebből $\mathbf{F}_0\in\mathcal{L}$ miatt $\mathbf{F}^*\in\Omega$ már következik). A $\preceq$ reláció definíciójában szereplő első két feltétel nyilvánvalóan teljesül, tehát csak $|\mathbf{F}_\beta\setminus\mathbf{F}^*|\le|\mathbf{F}^*\setminus\mathbf{F}_\beta|$ szorul bizonyításra.

Vegyük észre, hogy $\mathbf{F}_\beta\setminus\mathbf{F}^*=\mathbf{C}_\beta\setminus\mathbf{C}^*=\mathbf{C}_\beta\setminus(\bigcap_{\alpha\in\mathbf{I}}\mathbf{C}_\alpha)=\bigcup_{\alpha\in\mathbf{I}}(\mathbf{C}_\beta\setminus\mathbf{C}_\alpha)$ és ugyanígy $\mathbf{F}^*\setminus\mathbf{F}_\beta=\bigcup_{\alpha\in\mathbf{I}}(\mathbf{M}_\alpha\setminus\mathbf{M}_\beta)$ $\boxdot$ szerint $|\mathbf{C}_\beta\setminus\mathbf{C}_\alpha|\le|\mathbf{M}_\alpha\setminus\mathbf{M}_\beta|\le\bigcup_{\alpha\in\mathbf{I}}|\mathbf{M}_\alpha\setminus\mathbf{M}_\beta|$, azaz $\forall\alpha\in\mathbf{I}$: $|\mathbf{C}_\beta\setminus\mathbf{C}_\alpha|\le|\mathbf{F}^*\setminus\mathbf{F}_\beta|$. Mivel a $\{\mathbf{C}_\beta\setminus\mathbf{C}_\alpha|\alpha\in\mathbf{I}\}$ halmazok láncotnak alkot a tartalmazásra, uniójuk számossága a számosságaik legkisebb felső korlátja, azaz $|\mathbf{F}_\beta\setminus\mathbf{F}^*|=|\bigcup_{\alpha\in\mathbf{I}}\mathbf{C}_\beta\setminus\mathbf{C}_\alpha|\le|\mathbf{F}^*\setminus\mathbf{F}_\beta|$. $(\Omega,\preceq)$ valóban teljesíti a Zorn-lemma feltételeit.

2.10.4 Tétel: egy vektortér dimenziója jóldefiniált.

Bizonyítás: beláttuk, hogy minden vektortérnek van bázisa. Továbbá ha $\mathbf{B}$ és $\mathbf{B}'$ is bázis, akkor – mivel $\mathbf{B}$ független és $\mathbf{B}'$ generátorrendszer – az előző tétel értelmében $|\mathbf{B}|\le|\mathbf{B}'|$ és persze ugyanígy $|\mathbf{B}'|\le|\mathbf{B}|$. Ezért bármely két bázis számossága megegyezik, mint azt bizonyítani akartuk.

2.10.5 Állítás: ha K tetszőleges test, κ pedig $|K|$-nál nem kisebb végtelen számosság, akkor K^κ – a K feletti κ dimenziós vektortér – elemszáma κ. Ha pedig $|K|$ végtelen és κ egy ennél nem nagyobb (nullától különböző) számosság, akkor $|K^\kappa|=|K|$.

Bizonyítás: legyen $\mathbf{B}$ bázis $V=K^\kappa$-ban. A $v\in V$ elemre $r(v)$ legyen a v vektor $\mathbf{B}$ szerinti egyértelmű előállításában a tagok száma (pl. $r(0)=0,\forall b\in\mathbf{B}: r(b)=1$). Ekkor $r: V\to\mathbb{N}$. $n\ge1$ esetén azon v elemek száma, ahol $r(v)=n$, nyilván $\binom{\kappa}{n}\cdot|K\setminus\{0\}|^n$ (kiválasztunk n báziselemet a rendelkezésre álló κ közül, majd mindhez egy-egy nullától különböző együtthatót – a keletkező lineáris kombinációk a megfelelő v-k). Az első esetben κ végtelen számosság és $2\le|K|\le\kappa$, tehát $\binom{\kappa}{n}\cdot|K\setminus\{0\}|^n$ éppen κ és $|V|=\sum_{n\in\mathbb{N}}|\{v\in V|r(v)=n\}|=1+\sum_{n=1}^{\infty}\kappa=|\aleph_0\cdot\kappa|=\kappa$. A második esetben $\binom{\kappa}{n}\cdot|K\setminus\{0\}|^n$ κ-nál nem nagyobb n-re $|K|$, egyébként 0 – ebből is az jön ki, amit ígértünk.