Eötvös Loránd Tudományegyetem
Természettudományi Kar

B.Sc. Tézis

Mátrixok normálformái

Készítette:
Sávoly János Gábor

Témavezető:
dr. Ágoston István

2010

Köszönetnyilvánítás

Hálával tartozom témavezetőmnek, dr. Ágoston Istvánnak a hasznos tanácsaiért és türelméért.

Köszönet illeti családomat a sok szeretetért, illetve felsőfokú tanulmányaim anyagi finanszrozásért.

Köszönöm barátaim, évfolymtársaim támogatását. Közülük kiemelném Árendás Pétert, aki mellettem állt a legnehezebb pillanatokban is.

Tartalomjegyzék

1. Bevezetés

Természetes dolog, hogy az ember igyekszik a bonyolult struktúrák közül a lehető legegyszerűbbet kiválasztani. A kanonikus alak keresésnek ez az alapelve. A kiinduló szituáció általában az, hogy adott objektumok egy S halmaza és azon ekvivalenciareláció. Az ekvivalenciaosztályokból választunk reprezentánsokat, melyekre azt mondjuk, hogy kanonikus alakban vannak. S tetszőleges eleme ekvivalens valamely kanonikus alakkal. Ahhoz, hogy tetszteljük két elem ekvivalenciáját elegendő a kanonikus alakjaik megegyezését belátni. A dolgozatomban ezek a bizonyos objetumok mátrixok lesznek. A kanonikus alak, illetve normálforma kifejezéseket szinonímaként fogom használni.

"Hogyan dönthetjük el, hogy egy lineáris diofantoszi egyenletrendszernek létezik megoldása? Ha létezik megoldás, hogyan adhatjuk meg (az összeset)?" Ezt a problémát H. J. S. Smith oldotta meg teljes általánosságban 1861-ben.

Akkoriban sok fontos, az Abel-csoportokkal kapcsolatos eredmény született. Az Abel-csoportok elmélete alkalmazása egyre elterjedtebb lett számelméleti tanulmányokban és az elliptikus függvényeket, Abel-integrálokat érintő munkákban.

G. Frobenius és L. Stickelberger 1879-ben felfedezte a kapcsolatot a végesen generált Abel-csoportok és Smith tétele között. Ugyanebben az évben Frobenius megmutatta, hogy Smith elmélete (kiterjesztve polinomgyűrűk fölötti mátrixokra) használható test fölötti négyzetes mátrixok klasszifikációjára hasonlóság erejéig.

A szakdolgozat felépítése:
A 2. fejezetben, a szükséges gyűrű és mátrixelméleti fogalmakat gyűjtöttem össze. A tételeket, ahol lehetett bizonyítással együtt közöltem.
A 3. fejezetben megismerkedünk a Smith-, Frobenius- és a Jordan-normálformával. Létezésük és egyértelműségük bizonyítása mellett több lényeges észrevételt teszünk.
A 4. fejezetben a kanonikus alakok néhány alkalmazását mutatom be.
Az 5. fejezetben röviden írok arról, hogy milyen egyéb megközelítési módok lehetségesek, illetve hogyan általánosíthatók az elhangzottak.

A szakdolgozat megírása során nagyrészt a [3] könyvre támaszkodtam.

2. Előkészületek

2.1. Gyűrűk

Ebben a fejezetben R kommutatív integritási tartomány. R invertálható elemeinek a halmazát R^*-gal jelöljük. Ha létezik $c \in R$, melyre $ac = b$, akkor azt mondjuk, hogy a osztja b-t. A nullosztómentességből következik, hogy az a/b hányados egyértelmű. Ha a osztja b-t és b osztja a-t, akkor azt mondjuk, hogy a és b asszociáltak.
Az R-beli d elemet az a és b közös osztójának nevezzük, ha osztja a-t és b-t. Ha d az a és b közös osztója, továbbá a és b összes közös osztója egyben d-nek is osztója, akkor d-t az a és b számok legnagyobb közös osztójának nevezzük. A legnagyobb közös osztó asszociáltság erejéig egyértelműen meg van határozva. Az a és b elemeket relatív prímeknek nevezzük, ha az összes közös osztójuk invertálható. Ebben az esetben $lnko(a, b) = 1$.

2.1.1. Definíció. *Egy R gyűrű valamely I részhalmazát ideálnak nevezzük, ha az R-beli összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $r{\cdot}a \in I$.*

Az egy elemmel generálható ideálokat főideáloknak nevezzük.

2.1.2. Definíció. *Az R kommutatív gyűrűt főideálgyűrűnek nevezzük, ha minden ideálja főideál.*

2.1.3. Állítás. *Főideálgyűrűben bármely két számnak létezik legnagyobb közös osztója. A legnagyobb közös osztóra teljesül az úgynevezett Bézout-azonosság: tetszőleges a és $b \in R$ esetén létezik olyan u, $v \in R$, hogy*

$$lnko(a, b) = ua + vb,$$

ahol u és v relatív prímek.

Bizonyítás:
Legyen R főideálgyűrű. Ha a és $b \in R$, akkor az $I := (a, b)$ ideál $ax + by$ alakú elemek halmaza, ahol x, $y \in R$. Az I főideál, így egy elemmel generálható: $I = (d)$. Belátjuk, hogy $d = lnko(a, b)$. Mivel a, $b \in I$, d osztja a-t és b-t, továbbá $d = ua+vb$, mert $d \in I$. Ha c osztja a-t és b-t, akkor c osztja az $ua + vb$-t is, így osztja d-t, ami így a és b legnagyobb közös osztója. Ha m osztja u-t és v-t, akkor $md|ua + vb$; így $d = smd$. Ha $d \neq 0$, akkor $sm = 1$, ami azt jelenti, hogy $m \in R^*$. Így u és v relatív prímek. Ha $d = 0$, akkor $a = b = 0$, és vehetjük az $u = v = 1$-et, melyek relatív

prímek. ■

Ez az állítás általánosítható 2-nél több elemre is. Léteznek olyan $u_1, \ldots, u_n$ elemek, hogy

$$lnko(a_1, \ldots, a_s) = a_1u_1 + \cdots + a_su_s.$$

2.1.4. Definíció. *Az R gyűrűt Noether-gyűrűnek nevezzük, ha az ideáljainak nem létezik végtelen hosszú szigorúan növekvő lánca, azaz, ha $I_0 \subset I_1 \subset \cdots \subset I_m \subset \cdots$, akkor létezik olyan l, hogy $I_l = I_{l+1} = \cdots$.*

2.1.5. Állítás. *A főideálgyűrűk Noether-gyűrűk.*

Bizonyítás:
Tegyük fel indirekt módon, hogy létezik R-beli ideáloknak egy végtelen hosszú növekvő, tartalmazásra nézve $(I_j)_{j\geq 0}$ sorozata.
Legyen $U = \bigcup I_n$. U ideál, legyen b a generátora. b benne van valamelyik I_k ideálban. Így $I_j = I_k$, ha $j \geq k$, azonban ez ellentmond a szigorú tartalmazásnak. ■

2.1.6. Definíció. *Az R integritási tartományt euklideszi gyűrűnek nevezzük, ha R nem nulla elemein értelmezve van egy nemnegatív egészértékű ϕ függvény (az úgynevezett euklideszi norma) a következő tulajdonsággal. Minden a, $b \in R$, $b \neq 0$ esetén létezik olyan q, $r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $\phi(r) < \phi(b)$ (euklideszi osztás, maradékos osztás).*

2.1.7. Tétel. *Minden euklideszi gyűrű főideálgyűrű.*

Bizonyítás:
Legyen I az R euklideszi gyűrű egy ideálja. Ha $I = (0)$, akkor nincs mit mutatni. Ellenkező esetben válasszunk $I\backslash 0$-ból egy minimális normájú a elemet. Ha $b \in I$, akkor r, a b elem a-val történő euklideszi osztásakor keletkező maradék I-nek egy olyan eleme, melyre $\phi(r) < \phi(a)$. $\phi(a)$ minimalitása miatt $r = 0$, azaz $a|b$. Ezek alapján $I = (a)$. ■

2.1.8. Tétel. *A k test fölötti $k[X]$ polinomgyűrű euklideszi gyűrű.*

2.1.9. Következmény. *A k test fölötti $k[X]$ polinomgyűrű főideálgyűrű.*

2.2. Mátrixok

Legyen R kommutatív egységelemes integritási tartomány, melynek 0 a nulleleme és 1 az egységeleme. Ebben a fejezetben ilyen gyűrűk fölötti mátrixokat fogok vizsgálni. Az $\mathbf{M}_n(R)$ gyűrű $n \geq 2$ esetén nem kommutatív. Ezt támasztja alá a következő példa:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Gyakran hasznosnak bizonyul, ha azt a determinánst vizsgáljuk, amelyet egy adott M mátrix bizonyos p különböző sorának és p különböző oszlopának metszéspontjaiban elhelyezkedő elemei alkotnak. Az ilyen determinánsokat az M mátrix p-edrendű aldeterminánsának (minorjának) nevezzük. Az $\mathrm{M} \in \mathbf{M}_{n\times m}(R)$ és $1 \leq \mathrm{p} \leq$ n, m esetén a következő jelölést használjuk:

$$\mathrm{A}\begin{pmatrix} i_1 & \cdots & i_p \\ k_1 & \cdots & k_p \end{pmatrix} = \begin{vmatrix} a_{i_1k_1} & a_{i_1k_2} & \dots & a_{i_1k_p} \\ \vdots & \vdots & \dots & \vdots \\ a_{i_pk_1} & a_{i_pk_2} & \dots & a_{i_pk_p} \end{vmatrix},$$

ahol $i_1 < \cdots < i_p$, $k_1 < \dots k_p$. Ha $\mathrm{i}_1 = \mathrm{k}_1$,...,$\mathrm{i}_p = \mathrm{k}_p$, akkor principális aldeterminánsról (minorról) beszélünk.

2.2.1. Definíció. *Adott $M \in \boldsymbol{M}_n(R)$-hez tartozó kofaktorok mátrixán azt az $\hat{M}$ mátrixot értjük, melynek elemei az $\hat{m}_{ij} = (-1)^{i+j} \cdot M \begin{pmatrix} 1 & \cdots i-1 & i+1 \cdots & n \\ 1 & \cdots j-1 & j+1 \cdots & n \end{pmatrix}$ kifejezés által vannak megadva.*

2.2.2. Definíció. *adj $M := \hat{M}^T$, az M adjungáltja.*

2.2.3. Állítás. *Ha $M \in \boldsymbol{M}_n(R)$, akkor $M(adj\ M) = (adj\ M)M = det\ M \cdot I_n$.*

2.2.4. Állítás. *(Cauchy - Binet formula) Legyen $B \in \boldsymbol{M}_{n\times m}(R)$, $C \in \boldsymbol{M}_{m\times l}(R)$ és $p \leq n, l$ adva.*
Ekkor a

$$\begin{pmatrix} B & C \end{pmatrix} \begin{pmatrix} i_1 & \cdots & i_p \\ k_1 & \cdots & k_p \end{pmatrix}$$

aldetermináns megegyezik a

$$\sum_{1 \leq j_1 \leq j_2 \leq \cdots \leq m} B \begin{pmatrix} i_1 & \cdots & i_p \\ j_1 & \cdots & j_p \end{pmatrix} C \cdot \begin{pmatrix} j_1 & \cdots & j_p \\ k_1 & \cdots & k_p \end{pmatrix}$$

összeggel.

2.2.5. Következmény. *Legyen b és $c \in R$. Ha b osztja B összes p-edrendű aldeterminánsát, valamint c osztja C minden p-edrendű aldeterminánsát, akkor bc osztja BC összes p-edrendű aldeterminánsát.*

$l = m = n$ esetén a determinánsok szorzástételét kapjuk:

2.2.6. Tétel. *Ha $B, C \in \boldsymbol{M}_n(R)$, akkor $det\ (BC) = det\ B \cdot det\ C$.*

Más szóval, a determináns $\mathbf{M}_n(R)$-ből R-be képező multiplikatív homomorfizmus.

Következzen a Cauchy-Binet formula bizonyítása:
Bizonyítás:
Mivel a BC i-edik sorának (illetve a j-edik oszlopának) kiszámítása B-nek csak az i-edik sorát (illetve C j-edik oszlopát) veszi igénybe feltehetjük, hogy $p = n = l$. A $det\ BC$ aldeterminánst kell kiértékelnünk. Ha $m < n$, akkor nincs mit bizonyítani. Egyrészt BC rangja legfeljebb m, ezáltal $det\ BC$ értéke 0, másrészt a formula bal oldalán levő összeg üres.
Marad az $m \geq n$ eset. Írjuk fel a BC mátrix determinánsát oszlopainak függvényében (használjuk a determináns multilinearitását):

$$\begin{aligned} det\ BC &= det\ (\sum_{j_1=1}^{n} c_{j_1 1} B_{j_1}, (BC)_2, \ldots, (BC)_n) \\ &= \sum_{j_1=1}^{n} c_{j_1 1} det\ (B_{j_1}, \sum_{j_1=1}^{n} c_{j_2 2} B_{j_2}, (BC)_3, \ldots, (BC)_n) \\ &= \cdots = \sum_{1 \leq j_1, \ldots, j_n \leq n} c_{j_1 1} \cdots c_{j_n n} det\ (B_{j_1}, \ldots, B_{j_n}). \end{aligned}$$

Az összegben szereplő determináns értéke nulla, ha $j \mapsto j_f$ nem injektív, ekkor BC-nek két oszlopa azonos. Ellenben, ha j injektív, akkor ez a determináns B valamely aldeterminánsa előjel erejéig. Ez az előjel a $j_1, \ldots, j_p$-t növekvő sorrendbe rendező permutációhoz tartozik. Csoportosítva az összegzésben levő, ugyanahhoz az aldeterminánshoz tartozó tagokat, találjuk azt, hogy

$$\sum_{1 \leq k_1 < \cdots < k_n \leq m} \sum_{\sigma \in \mathbf{S}_n} I(\sigma) c_{k_1 \sigma(1)} \cdots c_{j_n \sigma(n)} B \begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix},$$

ami a megfelelő formula. ■

Mivel $\mathbf{M}_n(R)$ nem integritási tartomány, az invertálhatóság fogalmához szükség lesz a következő állításra.

2.2.7. Állítás. *Adott $M \in \boldsymbol{M}_n(R)$ esetén a következő állítások ekvivalensek:*

1. *Létezik $N \in \boldsymbol{M}_n(R)$, hogy $MN = I_n$.*
2. *Létezik $N' \in \boldsymbol{M}_n(R)$, hogy $N'M = I_n$.*
3. *det M invertálható.*

Ha M teljesíti ezen feltételek valamelyikét, akkor az N, N' mátrixok egyértelműen meg vannak határozva, és $N = N'$.

2.2.8. Definíció. *Ha teljesülnek a 2.2.6 Állítás feltételei, akkor M-et invertálhatónak nevezzük. Mondhatjuk azt is, hogy M nem szinguláris vagy reguláris. Az $N = N'$ mátrixot M inverzének nevezzük és M^{-1}-gyel jelöljük. Ha M nem invertálható, akkor szingulárisnak nevezzük.*

Bizonyítás:
Először megmutatom, hogy (1) ekvivalens (3)-mal. Ha $MN = I_n$, akkor $det\ M \cdot det\ N = 1$; így $det\ M \in R^*$. Fordítva, ha $det\ M$ invertálható, akkor a $(det\ M)^{-1}\hat{M}^T$ az M mátrix inverze.
Hasonlóan látható be a (2) és (3) ekvivalenciája. A három állítás tehát ekvivalens.
Ha $MN = N'M = I_n$, akkor $N = (N'M)N = N'(MN) = N'$. Ezzel beláttuk az egyértelműséget. ■

$\mathbf{M}_n(R)$ invertálható mátrixainak halmaza a 2.2.5. Tétel miatt csoportot alkot a szorzásra nézve. Ezt a multiplikatív csoportot általános lineáris csoportnak nevezzük, és $\mathbf{GL}_n(R)$-rel jelöljük.

2.2.9. Állítás. *Ha M és $N \in \boldsymbol{GL}_n(R)$, akkor:*

1. $(MN)^{-1} = N^{-1}M^{-1}$,
2. $(M^k)^{-1} = (M^{-1})^k$,
3. $(M^T)^{-1} = (M^{-1})^T$.

Az 1 determinánsú mátrixok halmaza $\mathbf{GL}_n(R)$ normális részcsoportja, mivel az $M \mapsto det\ M$ homomorfizmus magja. Speciális lineáris csoportnak nevezzük, és $\mathbf{SL}_n(R)$-rel jelöljük.

2.2.10. Definíció. *Az alábbi mátrixokat n-edrendű elemi mátrixoknak nevezzük:*

1. *Permutációmátrixok: ha* $\sigma \in S_n$*, akkor a* P_σ *elemei:* $p_{ij} = \delta^j_{\sigma(i)}$*, ahol* δ *a Kronecker-szimbólum.*

2. *Az* $I_n + aJ_{ik}$ *alakú mátrixok,* $a \in R$ *és* $1 \leq i \neq k \leq n$ *, hogy*

$$(J_{ik})_{lm} = \delta^l_i \delta^m_k.$$

3. *Diagonálmátrixok, melyek főátlóbeli elemei invertálhatók.*

2.2.11. Állítás. *Az előbb felsorolt mátrixok mindegyike invertálható, és a szóban forgó inverz szintén elemi.*

Bizonyítás:
P_σ inverze $P_{\sigma^{-1}}$.
Az I_n+aJ_{ik} inverze I_n-aJ_{ik}, hiszen $(I_n+aJ_{ik})(I_n-aJ_{ik}) = I_n-aJ_{ik}+aJ_{ik}+0_n = I_n$.
$diag(a_1, \ldots, a_r)$ inverze $diag(a_1^{-1}, \ldots, a_r^{-1})$. ■

Az 1. típusú mátrixszal történő balszorzás a mátrix sorait, jobbszorzás az oszlopait permutálja.
A 2. típusú mátrixszal történő balszorzás hozzáadja a mátrix i. sorához a j. a-szorosát, a jobbszorzás az oszlopokkal teszi ugyanezt.
A 3. típusú mátrixszal történő jobb- és balszorzás a mátrix sorait invertálható elemekkel szorozza.

2.2.12. Tétel. *Ha* M *n-edrendű invertálható négyzetes mátrix, melynek elemei egy* R *euklideszi gyűrűből valók , akkor* M *előáll* R*-beli elemeket tartalmazó elemi mátrixok szorzataként.*

Bizonyítás:
Az $n = 2$ esetre bizonyítjuk a tételt. Az általános eset bizonyítását, a speciális esetből és a 3.1.1. Tétel bizonyításából származtatjuk, mivel az abban a bizonytásban szereplő mátrixok blokkdiagonálisak 1×1 és 2×2-es diagonális blokkokkal. Legyen

$$\mathrm{M} = \begin{pmatrix} a & a_1 \\ c & d \end{pmatrix}$$

$\mathbf{SL}_2(R)$-beli mátrix. Ebben az esetben $ad - a_1c \in R^*$. Ha $\phi(a) < \phi(a_1)$, akkor szorozzuk meg jobbról M-et a következő mátrixszal:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ezt elvégezve teljesül a $\phi(a) \leq \phi(a_1)$ egyenlőtlenség. Legyen $a = a_1q + a_2$, az a a_1-el történő euklideszi osztása. Ekkor

$$M \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} =: M' = \begin{pmatrix} a_2 & a_1 \\ \cdot & d \end{pmatrix}.$$

Ezután

$$M' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =: M_1 = \begin{pmatrix} a_1 & a_2 \\ \cdot & \cdot \end{pmatrix},$$

ahol $\phi(a_2) < \phi(a_1)$. Konstruálunk egy következő alakú mátrixokból álló M_k sorozatot

$$\begin{pmatrix} a_{k-1} & a_k \\ \cdot & \cdot \end{pmatrix}$$

úgy, hogy $a_{k-1} \neq 0$, mindegyik egy előző mátrix elemi mátrixszal vett szorzata. Továbbá $\phi(a_2) < \phi(a_1)$. A 2.1.5 Állítás miatt ez egy véges sorozat és létezik egy olyan lépés, melyre $a_k = 0$. M_k invertálható háromszögmátrix, ezért a diagonálelemei invertálhatók. Ekkor M_kD^{-1} a következő alakú:

$$\begin{pmatrix} 1 & 0 \\ \cdot & 1 \end{pmatrix},$$

ami egy elemi mátrix. ■

Megjegyzés: Az állítás nem érvényes főideálgyűrűkre.

2.2.13. Definíció. *Az A és $B \in \boldsymbol{M}_{m\times} n(R)$ mátrixokat ekvivalensnek nevezünk, ha létezik $P \in \boldsymbol{GL}_m(R)$ és $Q \in \boldsymbol{GL}_n(R)$, hogy $B = PAQ$.*

2.2.14. Állítás. *Az előbbi definicióban szereplő ekvivalencia ekvivalenciareláció.*

2.2.15. Definíció. *Legyen k test. Az A és $B \in \boldsymbol{M}_n(k)$ mátrixokat hasonlónak nevezzük, ha létezik $P \in \boldsymbol{GL}_n(k)$, hogy $A = P^{-1}BP$.*

2.2.16. Állítás. *A hasonlóság ekvivalenciareláció.*

3. Mátrixok normálformái

3.1. Smith-normálforma

A most következő normálforma létezését Henry John Stephen Smith bizonyította $\mathbb{Z}$ fölötti mátrixokra, amelyet lineáris diofantoszi egyenletrendszerek megoldása során használt fel. Ebben a fejezetben megmutatom, hogy főideálgyűrű fölötti mátrixok esetén létezik a Smith-normálforma, és az lényegében egyértemű. Legyen a továbbiakban R főideálgyűrű.

3.1.1. Tétel. *Tekintsük az $M \in \boldsymbol{M}_{nk}(R)$ mátrixot. Ekkor létezik olyan $M = PDQ$ felbontás, ahol $P \in \boldsymbol{GL}_n(R)$ és $Q \in \boldsymbol{GL}_k(R)$ mátrixok, hogy a következők teljesülnek:*

- *D blokkdiagonális:*

$$\begin{pmatrix} d_1 & 0 & \dots & \dots & 0 \\ 0 & d_2 & \dots & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & d_n \end{pmatrix}.$$

- *$d_{i-1}|d_i$, ahol $i = 2, \dots, n$.*

Egy másik hasonló tulajdonságokkal rendelkező $M = P'D'Q'$ felbontás esetén d_i, a d_i' asszociáltja lesz.

A tételben szereplő D mátrix az M mátrix Smith-normálalakja. A tétel azt mutatja, hogy főideálgyűrű fölött minden mátrix ekvivalens egy diagonálmátrixszal. Látni fogjuk, hogy az ekvivalens alak elemi mátrixokkal történő bal-, illetve jobbszorzás segítségével elérhető. Mielőtt azonban elkezdeném a bizonyítást, következzen egy definíció:

3.1.2. Definíció. *A d_1, d_2, ..., d_r elemeket (r = min(n,k)) az M mátrix invariáns faktorainak nevezzük.*

Bizonyítás:

Az egyértelműség bizonyítása:

$k \leq r$ esetén jelölje $D_k(N)$ az N mátrix k-adrendű aldeterminánsainak a legnagyobb közös osztóját. A 2.2.5. Következmény alapján $D_k(M) = D_k(D) = D_k(D')$. Valóban a $D_k(PD) = D_k(P)D_k(D)$. A $D_k(P)$-k választható 1-nek, hiszen P invertálható, így $D_k(P) \in R^*$, ezért $D_k(P)$ asszociáltja 1-nek. Ezután $D_k(M) = D_k(PDQ) = D_k(PD)D_k(Q) = D_k(D)D_k(Q) = D_k(DQ) = D_k(D)$ (Q invertálhatósága miatt). $D_k(D) = D_k(D')$ triviálisan teljesül. Nyilvánvaló, hogy $D_k(D) = d_1 \cdots d_k$ (hiszen a k-adrendű aldeterminánsok 0-k vagy k különböző tag szorzatai), így

$$d_1 \cdots d_k = u_k d'_1 \cdots d'_k$$

valamely $u_k \in R^*$ esetén. Ebből következik, hogy d_1 és d'_1 asszociáltak. Innentől teljes indukciót alkalmazunk.R integritási tartomány, ezért $d'_k = u_k^{-1} u_{k-1} d_k$. Más szóval d_k és d'_k aszociáltak.

A létezés bizonyítása:

Az előzőek alapján látható, hogy a d_j-k a $d_1 \cdots d_j = D_j(M)$ egyenlőség alapján vannak meghatározva. d_1 az M mátrix elemeinek legnagyobb közös osztója. Ezért az első lépés az, hogy találjunk egy olyan M' mátrixot, amelyik ekvivalens M-el, amelynek m'_{11} eleme megegyezik ezzel a legnagyobb közös osztóval.

Hogy ezt elérjük, mátrixok egy ekvivalens $M^{(p)}$ sorozatát fogjuk megkonstruálni, ahol $M^{(0)} = M$ és $m_{11}^{(p)}$ osztja $m_{11}^{(p-1)}$-t. Legyen $N := M^{(p-1)}$, ekkor négy különböző eset lehetséges :

1. n_{11} osztja $n_{11}, \ldots, n_{1,j-1}$-t, azonban nem osztja n_{1j}-et. Legyen ekkor $d := lnko(n_{11},\, n_{1j})$, amit felírhatunk a $d = un_{11} + vn_{1j}$ alakban. Definiáljuk $w := -n_{1j}/d$-t és $z := n_{11}/d$-t. Legyen $Q \in \mathbf{GL}_m(R)$ mátrix a következő:

   - $q_{11} = u$, $q_{i1} = v$, $q_{1i} = w$, $q_{ii} = z$,
   - $q_{kl} = \delta_k^l$, egyébként.

$$M^{(p-1)} = \begin{pmatrix} n_{11} & \ldots & n_{1j} & * & * & * \\ * & \ldots & * & * & * & * \\ * & \ldots & * & * & * & * \\ * & \ldots & * & * & * & * \\ * & \ldots & * & * & * & * \end{pmatrix} \begin{pmatrix} u & -n_{1j}/d & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ v & -n_{1j}/d & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} = Q$$

   A Q mátrix determinánsa 1, ugyanis $det\ Q = un_{11}/d - v(-n_{1j})/d = un_{11} + vn_{1j})/d = 1$. $m_{11}^{(p)} = un_{11} + vn_{1j} = d$ lesz. Ebből következik, hogy a Q mátrix

invertálható.
$m_{1j}^{(p)} = n_{11}(-n_{1j}) + (-n_{1j})n_{11} = 0.$
Ekkor az $M^{(p)} := M^{(p-1)}Q$ megfelelő, hiszen $m_{11}^{(p)} = d|n_{11} = m_{11}^{(p-1)}$.

2. n_{11} osztja az n_{1j}-ket, illetve az $n_{11}, \ldots, n_{i-1,1}$-et, azonban nem osztja n_{i1}-t. Ez az eset szimmetrikus az előzőre nézve. Definiáljuk $w := -n_{1j}/d$-t és $z := n_{11}/d$-t. Legyen $P \in \mathbf{GL}_n(R)$ mátrix a következő:

   - $p_{11} = u$, $p_{i1} = w$, $p_{1i} = v$, $p_{ii} = z$,
   - $p_{kl} = \delta_k^l$, egyébként.

$$P = \begin{pmatrix} u & \cdots & v & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -n_{i1}/d & \cdots & n_{11}/d & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} n_{11} & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n_{i1} & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{pmatrix} = M^{(p-1)}$$

   A P mátrix determinánsa 1, mivel $det\ P = un_{11}/d - v(-n_{i1})/d =$
   $un_{11}\ +vn_{i1})/d = 1$. P így invertálható.
   $m_{11}^{(p)} = un_{11} + vn_{i1} = d$ lesz, $m_{i1}^{(p)} = n_{11}(-n_{i1})/d + (-n_{i1})n_{11}/d = 0$.
   Ekkor $M^{(p)} = \mathrm{P}M^{(p-1)}$. Ezzel teljesül $m_{11}^{(p)} = lnko(n_{11}, n_{i1})|m_{11}^{(p-1)}$.

3. n_{11} osztja az n_{1j}, illetve n_{i1}-eket, azonban nem osztja valamelyik n_{ij}-t $i, j \geq 2$ esetén. Ekkor $n_{i1} = an_{11}$. Legyen $P \in \mathbf{GL}_n(R)$ a következő mátrix:

   - $p_{11} = a + 1$, $p_{i1} = 1$, $p_{1i} = -1$, $p_{ii} = 0$
   - $p_{kl} = \delta_k^l$, egyébként.

$$P = \begin{pmatrix} a+1 & \ldots & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} n_{11} & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & n_{ij} & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{pmatrix} = M^{(p-1)}$$

A P mátrix determinánsa 1, mivel $det\ P = -(1 \cdot (-1)) = 1$. A P mátrix így invertálható.
Ha tekintjük az $N' = PN$ mátrixot, akkor $n'_{11} = n_{11}$ és $n'_{1j} = (a+1)n_{1j} - n_{ij}$.
Visszatértünk az első esethez, és létezik egy ekvivalens mátrix $M^{(p)}$, hogy $m_{11}^{(p)} = \gcd(n'_{11}, n'_{1j}) = n'_{1j} = \gcd(n_{11}, n_{ij})|n_{11} = m_{11}^{(p-1)}$.

4. n_{11} osztja az N mátrix összes elemét. Ebben az esetben, $M^{(p)} := M^{(p-1)}$.

Alapvető észrevétel, hogy az első három esetben $m_{11}^{(p)}$ nem asszociáltja $m_{11}^{(p-1)}$-nek, noha osztja.

Ennek következtében az $(m_{11}^{(p)})_{p\geq 0}$ sorozat tagjai páronként asszociáltak, ha p elég nagy. Ekkor a negyedik eset áll fenn: $m_{11}^{(q)}$ osztja az M mátrix minden elemét. Ekkor $m_{i1}^{(q)} = a_i m_{11}^{(q)}$ és $a_{1j}^{(q)} = b_j m_{11}^{(q)}$. Legyenek a $P \in \mathbf{GL}_n(R)$ és $Q \in \mathbf{GL}_m(R)$ mátrixok a következőképpen megadva:

- $p_{ii} = 1$, $p_{i1} = -a_i$, ha $i \geq 2$, $p_{ij} = 0$, különben.
- $q_{jj} = 1$, $p_{1j} = -b_j$, ha $j \geq 2$, $q_{ij} = 0$, különben.

Az $M' := PM^{(q)}Q$ mátrix ekvivalens $M^{(q)}$-val, így M-mel is. M' a következőképpen néz ki:

$$M' = \begin{pmatrix} m & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \mathbf{M''} & \\ 0 & & & \end{pmatrix},$$

ahol m osztja M'' összes elemét. Nyilvánvalóan igaz, hogy $m = D_1(M') = D_1(M)$.

Megmutattuk, hogy minden M mátrix a fentivel ekvivalens alakra hozható. Ezek után alkalmazzunk teljes indukciót M méretére (azaz az $r = min(n, m)$-re). Legyen $r = 1$, erre az előbb mutattuk meg, hogy létezik a Smith-normálforma. Amennyiben $r \geq 2$, és a feltevés igaz $r-1$-ed rendig, akkor alkalmazhatjuk az indukciós hipotézist a fenti redukcióban levő $\mathbf{M}'' \in M_{(n-1)\times(m-1)}(R)$-re: léteznek a $P'' \in \mathbf{GL}_{n-1}(R)$ és $Q'' \in \mathbf{GL}_{m-1}(R)$ mátrixok, úgy, hogy $P''M''Q''$ kvázidiagonális, az átlójában levő $d_2, \dots, d_r$ elemekre, pedig teljesül a $d_l|d_{l+1}l \geq 2$ feltétel. Az egyértelműségi lépésből következik, hogy $d_2 = D_1(M'')$. Mivel m osztja M'' elemeit, ezért $m|d_2$. Definiáljuk a $P' =$diag$(1, P'')$ és $Q' =$diag$(1, Q'')$ mátrixokat. Ezek invertálhatók. $P'M'Q'$ kvázidiagonális, a $d_1 = m$, $d_2, \dots,$ átlóelemekkel , melyek az R-beli osztásra nézve nem csökkenő sorozat alkotnak. Mivel M ekvivalens M'-vel, bebizonyítottuk a létezést. ∎

Megjegyzések

Ha egy mátrix invariáns faktorai között szerepel a 0, azaz valamelyik $d_j = 0$, akkor $d_{j+1} = \cdots = d_r$.

Ha $m = n$ és M invariáns faktorai $(1, ..., 1)$, akkor $D = I_n$ és $M = PQ$ invertálható. Fordítva, ha M inverálható, akkor az $M = MI_nI_n$ felírás mutatja, hogy $d_1 = \cdots = d_n = 1$.

Ha R test, akkor csak két ideál van, (0) és (1). Az invariáns faktorok listája $(1, ..., 1, 0, ..., 0)$ alakú. Előfordulhat, hogy nem szerepel a 0 vagy az 1 az invariáns faktorok között. Ezek alapján pontosan $min(n, m) + 1$ ekvivalenciaosztály van $\mathbf{M}_n(R)$-ben. Két mátrix akkor és csak akkor ekvivalens, ha megegyezik a rangjuk. A mátrix rangja adja meg az invariáns faktorok között szereplő egyesek számát. Az $M = PDQ$ felbontást ezesetben rang szerinti felbontásnak nevezzük.

Az elhangzott észrevételeket megfogalmazom egy tételben:

3.1.3. Tétel. *Legyen k test és $M \in M_{n\times m}(k)$ egy mátrix. Legyen q az M mátrix rangja, azaz a mátrix oszlopai által kifeszített k^n altér dimenziója. Ekkor léteznek olyan P, illetve Q mátrixok, hogy $M = PDQ$, $d_{ii} = 1$, ha $i \leq q$ és $d_{ij} = 0$ egyébként.*

A Smith-normálforma a főideálgyűrűk fölötti mátrixok esetén, az ekvivalenciára (2.2.13. Definció) nézve kanonikus alakot szolgáltat.

Ha V és W ugyanazon k test fölötti végesdimenziós vektorterek, és M egy V-ből W-be menő lineáris leképezés, akkor új bázispárra való áttérés esetén az M mátrixát a $P^{-1}MQ$ alakban kapjuk meg. Mivel k főideálgyűrű, M diagonális alakra hozható: $D = AMB$. $A = P^{-1}$ és $B = Q$ esetén ez azt jelenti, hogy a V, illetve a W vektorterek bázisait alkalmasan megválasztva elérhető, hogy az M lineáris leképezés mátrixa ezekben a bázisokban diagonális legyen.

3.2. Frobenius-normálforma

Az előző fejezetben elért eredményeket alkalmazva egy újabb normálformát fogunk nyerni elemi mátrixokkal történő bal-, illetve jobbszorzás segítségével. Ebben a fejezetben a mátrixaink elemei egy k test fölötti $k[X]$ polinomgyűrű elemei lesznek. Ez euklideszi gyűrű, ezáltal főideálgyűrű is.

3.2.1. Állítás. *$\boldsymbol{M}_n(k[X])$ minden eleme felirható az X változó mátrixpolinomjaként azaz, ha az $A \in \boldsymbol{M}_n(k[X])$ legmagasabb fokú eleme l-edfokú, akkor*

$$A = A_0X^l + A_1X^{l-1} + \cdots A_{l-1}X + A_l.$$

A maradékos osztás végrehajtható mátrixpolinomok esetén, azonban vigyázni kell, a mátrixok szorzásának nem kommutatív volta és nullosztók jelenléte miatt.

3.2.2. Tétel. *Legyen adva a k test fölött két n-edrendű $\boldsymbol{M}_n(k[X])$-beli mátrix,*

$$A = A_0X^k + A_1X^{k-1} + \cdots A_{k-1}X + A_k,$$
$$B = B_0X^k + B_1X^{k-1} + \cdots B_{k-1}X + B_k,$$

és tegyük fel, hogy a B_0 mátrix nem szinguláris, azaz létezik a B_0^{-1} mátrix. Akkor található a k test fölött két olyan, szintén n-edrendű $\boldsymbol{M}_n(k[X])$-beli mátrix, Q_1 és R_1, hogy

$$A = BQ_1 + R_1,$$

ahol R_1 fokszáma kisebb, mint B-é, vagy pedig $R = 0$. Található másrészt a k test fölött két olyan $\boldsymbol{M}_n(k[X])$-beli mátrix, Q_2 és R_2, hogy

$$A = Q_2B + R_2,$$

ahol R fokszáma kisebb, mint B-é, vagy pedig $R_2 = 0$. Az ezen feltételeknek eleget tevő Q_1 és R_1, valamint Q_2 és R_2 mátrix egyértelműen meghatárzott.

Adott $B \in \mathbf{M}_n(k)$ mátrix esetén tekintsük az $XI_n - B \in \mathbf{M}_n(k[X])$ mátrixot, ahol X az A-beli határozatlan.

3.2.3. Definíció. *Ha $B \in \boldsymbol{M}_n(k)$, akkor az $M := XI_n - B$ invariáns faktorait B invariáns polinomjainak vagy B hasonlósági invariánsainak nevezzük.*

Az elnevezés jogosságát a következő állítás biztosítja:

3.2.4. Tétel. *Két $\boldsymbol{M}_n(k)$-beli mátrix akkor és csak akkor hasonló, ha az invariáns polinomjaik listája megegyezik (multiplicitással számolva).*

Ez a tétel speciális esete a következőnek:

3.2.5. Tétel. *Legyenek $A_0, A_1, B_0, B_1 \in \boldsymbol{M}_n(k)$ mátrixok, hogy $A_0, A_1 \in \boldsymbol{GL}_n(k)$. Az $XA_0 + B_0$ és $XA_1 + B_1$ mátrixok akkor és csak akkor ekvivalensek, ha léteznek olyan G, $H \in \boldsymbol{GL}_n(k)$ mátrixok, hogy*

$$GA_0 = A_1H,\ GB_0 = B_1H.$$

Ha $A_0 = A_1 = I_n$, akkor az utóbbi tétel szerint $XI_n - B_0$ és $XI_n - B_1$ akkor és csak akkor ekvivalensek, azaz ugyanazok az invariáns polinomok tartoznak mindkét mátrixhoz, ha létezik olyan $P \in \mathbf{GL}_n(k)$, amire $PB_0 = B_1P$ teljesül, ami az előbbi tétel kritériuma.

Bizonyítás:
A feltétel elégségessége triviális.
Megfordítva, ha XA_0+B_0 és XA_1+B_1 ekvivalensek, akkor léteznek olyan P és $Q \in \mathbf{GL}_n(A)$ mátrixok, melyekkel $P(XA_0+B_0) = (XA_1+B_1)Q$. Mivel A_1 invertálható, eloszthatjuk jobbról P-t $(XA_1 + B_1)$-el:

$$P = (XA_1 + B_1)P_1 + G,$$

ahol G egy mátrix, melynek az elemei konstans polinomok. Mivel $\mathbf{M}_n(k)$ nem kommutatív, az euklideszi osztást jobbról, illetve balról elvégezve különböző hányadosokat és maradékokat kaphatunk. Hasonlóan $Q = Q_1(XA_0 + B_0) + H$, ahol $H \in \mathbf{M}_n(k)$. Helyettesítsük be a $P(XA_0 + B_0) = (XA_1 + B_1)Q$ egyenletbe P-t és Q-t, majd alakítsuk át.

$$((XA_1 + B_1)P_1 + G)(XA_0 + B_0) = (XA_1 + B_1)(Q_1(XA_0 + B_0) + H)$$
$$(XA_1 + B_1)P_1(XA_0 + B_0) + G(XA_0 + B_0) = (XA_1 + B1)Q_1(XA_0 + B_0) + (XA_1 + B_1)H$$
$$(XA_1 + B_1)(P_1 - Q_1)(XA_0 + B_0) = (XA_1 + B_1)H - G(XA_0 + B_0)$$

Az egyenlet bal oldalának a foka (ez a fok a mátrix elemei fokának a szuprémuma) $2 + deg(P_1 - Q_1)$, míg a jobb oldalé legfeljebb 1. Mivel a két oldal megegyezik, el kell, hogy tűnjön, így

$$GA_0 = A_1H,\ GB_0 = B_1H.$$

Már csak azt kell megmutatnunk, hogy G és H invertálható. Ehhez definiáljuk az $R \in \mathbf{M}_n(k[X])$ mátrixot P inverzeként (ami a feltevés miatt létezik). Ekkor maradékosan osztva

$$R = (XA_0 + B_0)R_1 + K, \text{ ahol } K \in \mathbf{M}_n(k).$$

A fenti egyenletekből adódik:

$$\begin{aligned}
I_n &= PP^{-1}\\
I_n &= ((XA_1 + B_1)P_1 + G)((XA_0 + B_0)R_1 + K)\\
I_n &= (XA_1 + B_1)P_1(XA_0 + B_0)R_1 + (XA_1 + B_1)P_1K + G(XA_0 + B_0)R_1 + GK\\
I_n - GK &= ((XA_1 + B_1)P_1 + G)(XA_0 + B_0)R_1 + (XA_1 + B_1)P_1K\\
I_n - GK &= P(XA_0 + B_0)R_1 + (XA_1 + B_1)P_1K\\
I_n - GK &= (XA_1 + B_1)QR_1 + (XA_1 + B_1)P_1K\\
I_n - GK &= (XA_1 + B_1)(QR_1 + P_1K).
\end{aligned}$$

Mivel a bal oldal konstans és a jobb oldal foka $1 + deg(QR_1 + P_1K)$, teljesülnie kell az $I_n = GK$ egyenlőségnek, így G invertálható. Hasonlóan H is az. ■

3.2.6. Következmény. *Ha $B \in \boldsymbol{M}_n(k)$, akkor B és B^T hasonlók.*

Bizonyítás:
Valóban, hiszen $XI_n - B$ és $XI_n - B^T$ egymás transzponáltjai, így aldeterminánsaik, és ezáltal invariáns faktoraik megegyeznek. ■

3.2.7. Állítás. *Adott*

$$P(X) = X^n + a_1X^{n-1} + \cdots + a_n$$

polinom esetén létezik egy $B \in \boldsymbol{M}_n(k)$ mátrix, hogy az $XI_n - B$ mátrix invariáns faktorainak a listája $(1, ..., 1, P)$.

Bizonyítás:

3.2.8. Definíció. *A*

$$B_P := \begin{pmatrix} 0 & \dots & \dots & 0 & -a_n \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_1 \end{pmatrix}$$

mátrixot, a P polinom kísérőmátrixának nevezzük.

Természetesen bármely B_P-hez hasonló mátrix megfelelne, mert ha $B = Q^{-1}B_PQ$, akkor $XI_n - B$ hasonló, ennélfogva ekvivalens $XI_n - B_P$-vel. Hogy megmutassuk B_P invariáns faktorai valóban az $(1, \dots, 1, P)$ polinomok, vegyük észre, hogy $XI_n - B_P$-nek létezik olyan $n-1$-edrendű részmátrixa, melynek nem nulla konstans a determinánsa:

$$det \begin{pmatrix} -1 & X & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & X \\ 0 & \dots & \dots & 0 & -1 \end{pmatrix} = (-1)^{n-1}$$

Így $D_{n-1}(XI_n - B_P) = 1$, így a $d_1, \dots, d_{n-1}$ invariáns faktorok mindegyike 1. Ebből következik, hogy $d_n = D_n(XI_n - B_P) = det\ (XI_n - B_P)$, ami B_P karakterisztikus polinomja, nevezetesen P.
P egyben minimálpolinomja is B_P-nek. Valóban, ha a Q lefeljebb $n-1$-edfokú polinom, pl.:

$$Q(X) = b_0X^{n-1} + \dots + b_{n-1},$$

akkor

$$Q(A)e_1 = b_0e_n + \dots + b_{n-1}e_1 \text{ (itt az } e_i\text{-vel az i.standard bázisvektort jelöli).}$$

Így $Q(A) = 0$ esetén $Q(A)e_1 = 0$ és az e_i-k függetlensége következtében $Q = 0$. A minimálpolinom ennélfogva legalább n-edfokú. Így meg kell, hogy egyezzen a karakterisztikus polinommal. ∎

Legyen $M \in M_n(k)$ négyzetes mátrix, melynek hasonlósági invariánsai a $P_1, \dots, P_n \in k[X]$ polinomok.

3.2.9. Állítás. $\sum_{i=1}^{n} deg\ P_i = n.$

Bizonyítás:

Tegyük fel indirekt módon, hogy $\sum_{i=1}^{n} deg\ P_i > n$. Ekkor az $XI_n - M$ főátlójában szereplő hasonlósági invariánsok szorzat polinomjának a foka nagyobb, mint n. Azonban $deg\ (det\ XI_n - M) =$ n, hiszen a kifejtésben szereplő legnagyobb fokszámú tag n-edfokú. A hasonlósági invariánsok szorzata $det\ XI_n - M$ egy nem nulla konstanssal való szorzata. Ezzel ellentmondásra jutottok, tehát $\sum_{i=1}^{n} deg\ P_i \leq n$, mivel deg (det $XI_n - M$) = n, ezért az állítás igaz. ■

Jelölje $M^{(j)} \in \mathbf{M}_{n_j}(k)$ a P_j polinom kísérőmátrixát. Tekintsük, azt az M' mátrixot, amely blokkdiagonális, és melynek blokkjai az $M^{(j)}$-k. Az első néhány P_j polinom általában konstans (látni fogjuk, ha P_1 nem konstans, akkor $M = \alpha I_n$), a megfelelő blokkok üresek, a megfelelő sorok szintúgy. Hogy precízek legyünk m, a diagonális blokkok száma megegyezik a nem konstans hasonlósági invariánsok számával. Mivel az $XI_{n_j} - M^{(j)}$ ekvivalens az $N^{(j)} = diag(1, ..., 1, P_j)$-vel, ezért

$$XI_{n_j} - M^{(j)} = P^{(j)} N^{(j)} Q^{(j)},$$

ahol $P^{(j)}, Q^{(j)} \in \mathbf{GL}_{n_j}(k[X])$. Legyenek P, $Q \in \mathbf{GL}_n(k[X])$ mátrixok a következők:

$$P = diag(P^{(1)}, \ldots, P^{(n)}),\ Q = diag(Q^{(1)}, \ldots, Q^{(n)}).$$

Így nyerjük:

$$XI_n - M' = PNQ, N = diag(N^{(1)}, \ldots, N^{(n)})$$

Itt N diagonálmátrix, amelynek főátlójában elhelyezkedő elemei M hasonlósági invariánsai, rend erejéig. Valóban, az összes nem konstans P_j feltűnik a hozzátartozó $N^{(j)}$ blokkban. A többi diagonálelem 1, amiből $n - m$ darab van; ezek a várt $P_1, \ldots, P_{n-m}$ polinomok. Permutációmátrixszal való konjugálás után kapjuk, hogy $XI_n - M'$ ekvivalens $XI_n - M$-mel. A 3.2.2. Tétel miatt, M és M' hasonlók.

3.2.10. Tétel. *Legyen k test, $M \in \mathbf{M}_n(k)$ egy négyzetes mátrix $P_1, \ldots, P_n$ hasonlósági invariánsokkal. Ekkor M hasonló egy M' blokkdiagonális mátrixhoz, amelynek a j-edik diagonális blokkja P_j kísérőmátrixa.*
Az M' mátrixot, az M első kanonikus alakjának vagy M Frobenius kanonikus alakjának nevezzük.

3.2.11. Tétel. *Legyen k egy test, $M \in \mathbf{M}_n(k)$ egy négyzetes mátrix $P_1, \ldots, P_n$ hasonlósági invariánsokkal. Ekkor P_n az M minimálpolinomja. A minimálpolinom független az alaptesttől.*

Bizonyítás:
Tekintsük az M mátrix M' Frobenius kanonikus alakját. Mivel M' és M hasonlók,

megegyezik a minimálpolinomjuk. Így feltehetjük, hogy M, az M =diag$(M_1, \ldots, M_n)$ kanonikus alakban van, ahol M_j a P_j kísérőmátrixa. Mivel $P_j(M_j) = 0$ (Cayley-Hamilton tétel) és $P_j|P_n$, ezért $P_n(M_j) = 0$, így $P_n(M) = 0_n$ Ebből következik, hogy a Q_M minimálpolinom osztja P_n-t. Fordítva $Q(M) = 0_n$-ból következik, hogy $Q(M_n) = 0$. Mivel P_n az M_n minimálpolinomja, P_n osztja Q-t. Tehát $P_n = Q_M$. Legvégül, mivel a hasonlósági invariánsok nem függenek a kérdéses test megválasztásától, P_n szintén független tőle. ■

A Frobenius-normálforma $M_n(k)$-beli mátrixok kanonikus alakja a hasonlóságra nézve. Segítségével eldönthetjük, hogy hasonló-e két A, B $M_n(k)$-beli mátrix az alaptest bővítése nélkül.

3.3. Jordan-normálforma

Bontsuk fel M hasonlósági invariánsait irreducibilis polinomok szorzatára. Ez a felbontás függ a választott testtől. $p_1, \ldots, p_t$-vel jelölve a P_n különböző irreducibilis faktorait,

$$P_j = \prod_{k=1}^{t} p_k^{\alpha(j,k)}, 1 \leq j \leq n,$$

ahol az $\alpha(j,k)$ egy j-re nézve nem csökkenő sorozat, mivel P_j osztja P_{j+1}-et.

3.3.1. Definíció. *Az $M \in \boldsymbol{M}_n(k)$ mátrix elemi osztói azok a $p_k^{\alpha(j,k)}$ polinomok, melyekre az $\alpha(j,k)$ kitevő nem nulla. Egy p_k^m elemi osztó multiplicitása az $\alpha(j,k) = m$ egyenlet megoldásainak a száma. Az elemi osztók listája ezen polinomok sorozata, multiplicitással tekintve.*

Vegyük azt az esetet, amikor N egy P polinom kísérőmátrixa. N hasonlósági invariánsai $(1, \ldots, P)$. Legyenek az elemi osztói $Q_1, Q_2, \ldots, Q_t$. Ekkor $P = Q_1 \cdots Q_t$ ahol a Q_i-k páronként relatív prímek. Minden Q_l mátrixhoz rendeljük hozzá az N_l kísérő mátrixát, és tekintsük az $N' :=$diag$(N_1, N_2, \ldots, N_t)$ mátrixot. Mivel az összes $N_l - XI_l$ ekvivalens egy

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & Q_l \end{pmatrix}$$

$\mathbf{M}_n(l)(k[X])$-beli diagonálmátrixszal, az egész $N' - XI_n$ mátrix ekvivalens a következővel:

$$Q := \begin{pmatrix} 1 & & & & \\ & \ddots & & & 0 \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & Q_t \end{pmatrix}.$$

Számoljuk ki N' hasonlósági invariánsait, azaz Q invariáns faktorait. Elég meghatározni D_{n-1}-et, az $n-1$-edrendű aldeterminánsok legnagyobb közös osztóját. Figyelembe véve a Q alapvető aldeterminánsait, látjuk hogy D_{n-1}-nek osztania kell az összes

$\prod_{l \neq k} Q_l, 1 \leq k \leq n$ alakú szorzatot.

Mivel a Q_l-ek páronként relatív prímek, $D_{n-1} = 1$. Ez azt jelenti, hogy az N' hasonlósági invariánsai $(1, \dots, 1, \cdot)$ alakúak, ahol az utolsó polinomnak meg kell egyeznie az N' karakterisztikus polinomjával. Ez a polinom az N_l-ek karakterisztikus polinomjainak a szorzata. Ezek megegyeznek a Q_l-kel, így az N' karakterisztikus polinomja P. Végül, N és N'-nek ugyanazok a hasonlóságai invariánsaik, így hasonlóak.

Legyen M egy tetszőleges $\mathbf{M}_n(k)$-beli mátrix. Alkalmazzuk az előző redukciót M_j Frobenius kanonikus alakbeli diagonális blokkjaira. Mindegyik M_j hasonló egy olyan blokkdiagonális mátrixhoz, melynek a diagonális blokkjai az M elemi osztóihoz tartozó kísérőmátrixok. Ezzel bebizonyítottuk a következő tételt:

3.3.2. Tétel. *Legyenek $Q_1, \dots, Q_s$ az $M \in \boldsymbol{M}_n(k)$ mátrix elemi osztói. Ekkor M hasonló egy M' blokkdiagonális mátrixhoz, melynek diagonális blokkjai a Q_l-ek kísérőmátrixai.*

Ezt az M' mátrixot M második kanonikus alakjának nevezzük.

Amikor a karakterisztikus polinom felbomlik k fölött, ami mindig teljesül, ha a k test algebrailag zárt, az elemi osztók $(X - a)^r$ alakúak, ahol $a \in k$ és $r \geq 1$. Ebben az esetben nagy mértékben egyszerűsíthetünk a második kanonikus alakon, ha az $(X - a)^r$ monomhoz tartozó kisérőmátrixot a

$$J(a; r) := \begin{pmatrix} a & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & a \end{pmatrix}$$

Jordan-blokkjával helyettesítjük. Valóban, a $J(a; r)$ mátrix karakterisztikus polinomja $(X - a)^r$, amíg az $XI_r - J(a; r)$-nek van egy $r - 1$-edrendű invertálható aldeterminánsa, nevezetesen:

$$\begin{pmatrix} -1 & 0 & \dots & 0 \\ X - a & \ddots & \ddots & \vdots \\ & \ddots & \ddots & 0 \\ & & X - a & -1 \end{pmatrix},$$

amit az első oszlop és az utolsó sor törlésével kapunk. Ez mutatja, hogy $D_{n-1}(XI_r - J) = 1$, így a $d_1, \dots d_{r-1}$ invariáns faktorok 1-el egyenlők. Így $d_r = D_r(XI_r - J) = det\ (XI_r - J) = (X - a)^r$. Az invariáns faktorai így $1, \dots, 1, (X - a)^r$. Így igaz a következő tétel.

3.3.3. Tétel. *Ha M egyik elemi osztója $(X-a)^r$ alakú, akkor az M második kanonikus alakjában kicserélhetjük a kísérőmátrixát a $J(a;r)$ Jordan-blokkra.*

3.3.4. Következmény. *Ha az M mátrix karakterisztikus polinomja lineáris faktorokra bomlik k fölött, akkor M hasonló egy blokkdiagonális mátrixhoz, melynek a j-edik diagonális blokkja egy $J(a_j;r_j)$ Jordan-blokk. Ez az alak a blokkok permutációja erejéig egyértelmű.*

3.3.5. Következmény. *Ha k algebrailag zárt, akkor minden M négyzetes mátrix hasonló egy blokkdiagonális mátrixhoz melynek j-edik diagonálblokkja a $J(a_j;r_j)$ Jordan-blokk. Ez az alak a blokkok permutációja erejéig egyértelmű.*

4. Alkalmazások

4.1. Lineáris diofantoszi mátrixegyenletek és a Smith-normálforma

Az egész együtthatós lineáris egyenletrendszereknek megoldása mind gyakorlati, mind pedig elméleti szempontból nagy jelentőséggel bír.
Az $AX = B$ mátrixegyenletetet szeretnénk megoldani, ahol A és B ismert, az X pedig ismeretlen ismeretlen egész elemű mátrix. Ebben a fejezetben egy szükséges és elégséges feltételt adunk az AX = B megoldásának létezésére, valamint explicit formulával adjuk meg a megoldás(oka)t.

Tekintsük az $A \in \mathbf{M}_{m\times n}(\mathbb{Z})$ mátrixot. Legyen ennek a Smith-normálformája a $D = diag(d_1, \ldots, d_r, 0, \ldots, 0)$ mátrix, melynek főátlóbeli elemeire $d_i|d_j$ i < j esetén. Léteznek olyan invertálható $P \in \mathbf{GL}_m(\mathbb{Z})$ és $Q \in \mathbf{GL}_n(\mathbb{Z})$ mátrixok, hogy $PAQ = D$.
Tegyük fel, hogy $r < m$ és $r < n$. Később megnézzük azokat az eseteket, amikor az egyik vagy mindkettő helyen egyenlőség szerepel.
Definiáljuk a

$$\overline{D} = diag(d_{11}, d_{22}, \ldots, d_{rr})$$

és az $U \in \mathbf{M}_{(m-r)\times p}(\mathbb{Z})$ mátrixot úgy, hogy

$$PB = \begin{pmatrix} \overline{PB} \\ U \end{pmatrix},$$

ahol $\overline{PB}$ a PB első r sorából álló mátrix. O-val jelölöm a csak 0-t tartalmazó mátrixokat. Ekkor igaz a következő tétel:

4.1.1. Tétel. *Az X egész elemű mátrix akkor és csak akkor elégíti ki az $AX = B$ egyenletet, ha*
a) $U = O$,
b) $\overline{D}^{-1}\overline{PB}$ egész elemű mátrix.
Ekkor az összes megoldás előáll az $X = Q \begin{pmatrix} \overline{D}^{-1}\overline{PB} \\ Z \end{pmatrix}$ alakban, valamely $Z \in \boldsymbol{M}_{(n-r)p}(\mathbb{Z})$ mátrixszal.

Bizonyítás:
Tegyük fel, hogy az X egész elemű mátrix kielégíti az $AX = B$ egyenletet. Ekkor a $PAQ = D$ miatt $P^{-1}DQ^{-1}X = B$, és $DQ^{-1}X = PB$. Legyen

$$\mathrm{Q}^{-1}X = Y = \begin{pmatrix} \overline{Y} \\ Z \end{pmatrix},$$

ahol $\overline{Y}$, az $n \times p$-es Y mátrix első r sorából áll. A Q^{-1} és X egész elemű mátrixok, szintúgy az $\overline{Y}$ és a $Z \in \mathbf{M}_{(n-r)p}(\mathbb{Z})$ mátrixok. Ekkor a $DY = PB$-t a következő alakban írhatjuk fel:

$$\begin{pmatrix} \overline{D} & O \\ O & O \end{pmatrix} \begin{pmatrix} \overline{Y} \\ Z \end{pmatrix} = \begin{pmatrix} \overline{PB} \\ U \end{pmatrix}.$$

Ekkor teljesül, hogy $U = O$ és $\overline{DY} = \overline{PB}$, ezért $\overline{Y} = \overline{D}^{-1}\overline{PB}$, aminek így egész elemű mátrixnak kell lennie. Ezek alapján:

$$X = QY = Q \begin{pmatrix} \overline{D}^{-1}\overline{PB} \\ Z \end{pmatrix}.$$

A másik irányhoz tegyük fel, hogy

$$X = \begin{pmatrix} \overline{D}^{-1}\overline{PB} \\ Z \end{pmatrix}$$

$\overline{D}^{-1}\overline{PB}$ és Z egész elemű mátrixokra. Tegyük fel, hogy $U = O$. Így

$$PB = \begin{pmatrix} \overline{PB} \\ O \end{pmatrix}.$$

X egész elemű mátrix a 4.1.1 Tétel feltétele miatt.

$$\begin{aligned} AX = P^{-1}DQ^{-1}Q \begin{pmatrix} \overline{D}^{-1}\overline{PB} \\ Z \end{pmatrix} \\ &= P^{-1} \begin{pmatrix} \overline{D} & O \\ O & O \end{pmatrix} \begin{pmatrix} \overline{D}^{-1}\overline{PB} \\ Z \end{pmatrix} \\ &= P^{-1} \begin{pmatrix} \overline{PB} \\ O \end{pmatrix} \\ &= P^{-1}PB = B. \end{aligned}$$

■ Az előzőnél több is igaz.

4.1.2. Állítás. *Az X akkor és csak akkor elégíti ki az $AX = B$ egyenletet, ha*
a) $U = O$,
b) $\overline{D}^{-1}\overline{PB}$ egész elemű mátrix.
Ekkor a megoldások az $X = Q \begin{pmatrix} \overline{PB} \\ Z \end{pmatrix}$ *valamely Z egész elemű mátrixra.*

Ha teljesülnek az állítás a) és b) feltételei, akkor az $AX = B$ összes megoldása előáll úgy, hogy a Z mátrix elemeit végigfuttatjuk az egészeken. Ebben az esetben a Q első r oszlopából egy $n \times r$-es Q_1 mátrixot és egy $n \times (n-r)$-es Q_2 mátrixot a Q utolsó $n-r$ oszlopából. Ekkor látható, hogy az X megoldás $Q_1\overline{PB} + Q_2 Z$ alakban írható fel, ahol az első tag az eredeti $AX = B$ egyenlet egy partikuláris megoldása. Mivel $PAQ_2 = O$ és P invertálható, Q_2 egész megoldása a homogén egyenletnek. Azaz $AQ_2 = O$, ahol O $m \times (n-r)$-es.

A kihagyott esetek (bizonyítás nélkül):

$\mathbf{r = m = n}$

4.1.3. Tétel. *Az X egész elemű mátrix akkor és csak akkor elégíti ki az $AX = B$ egyenletet, ha $\overline{D}^{-1}PB$ egész elemű mátrix.*
Ekkor az összes megoldás előáll az $X = QPB$ alakban.

$\mathbf{r = m < n}$

4.1.4. Tétel. *Az X egész elemű mátrix akkor és csak akkor elégíti ki az $AX = B$ egyenletet, ha $\overline{D}^{-1}PB$ egész elemű mátrix.*
Ekkor az összes megoldás előáll az $X = Q\begin{pmatrix}\overline{D}^{-1}PB \\ Z\end{pmatrix}$ alakban, valamely $Z \in \boldsymbol{M}_{(n-r)p}(\mathbb{Z})$ mátrixra.

$\mathbf{r = n < m}$

4.1.5. Tétel. *Az X egész elemű mátrix akkor és csak akkor elégíti ki az $AX = B$ egyenletet, ha*
a) $U = O$ nullmátrix,
b) $\overline{D}^{-1}\overline{PB}$ egész elemű mátrix.
Ekkor az összes megoldás előáll az $X = Q\overline{D}^{-1}\overline{PB}$ alakban.

Hatékony algoritmust adni egészértékű mátrix Smith-normálformájának meghatározása nem triviális feladat. Az elemi transzformációk direkt alkalmazása nem vezet polinomiális algoritmushoz. Akit érdekel, hogyan lehet polinomiális algoritmust adni egész elemű mátrix Smith-normálformájának meghatározására, a [8] oldalon több cikket is találhat ezzel kapcsolatban.

4.2. A Frobenius-normálforma alkalmazásai

Az $A \in M_n(k)$ mátrix Frobenius-normálalakja

$$U^{-1}AU = F = \begin{pmatrix} C_{f_1} & & & 0 \\ & C_{f_1} & & \\ & & \ddots & \\ 0 & & & C_{f_l} \end{pmatrix} \in M_n(k).$$

Az összes C_{f_i} blokk az $f_i \in k[X]$ monom kísérőmátrixa, ahol $f_{i+1|f_i}$ $1 \leq i \leq l-1$. Az alakból A számos invariánsát leolvashatjuk: f_1 a minimálpolinom, a karakterisztikus polinom az $f_1 f_2 \cdots f_l$ szorzat, a determináns az $f_1 f_2 \cdots f_l$ szorzat konstans tagja, a mátrix rangja megegyezik $n-$ azon blokkok számával melynek kísérőpolinomja 0 konstans együtthatójú.

Mivel az előbbi invariánsokat meghatározhatjuk a Frobenius-normálalakból, nem mindegy, hogy mennyire gyors algoritmusok állnak a rendelkezésünkre ezen normálforma meghatározására. Storjohann (1998)-ban egy olyan algoritmust adott meg, amivel $2n^3 + O(n^2)$ lépéssel meghatározhatjuk a Frobenius-normálalakot. A transzformációmátrix kiszámítása $6n^3 + O(n^2(logn)^2)$ műveletet igényel. Segítségével megmutatható, hogy az A és B mátrixok hasonlók-e, az alaptest bővítése nélkül.

4.3. A Jordan-normálforma néhány alkalmazása

Tekintsük az A $= \begin{pmatrix} 1 & 1 \\ \epsilon & 1 \end{pmatrix}$ mátrixot. Ha $\epsilon = 0$, akkor a Jordan-normálforma egyszerűen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Amennyiben $\epsilon \neq 0$, akkor a Jordan-normálforma $\begin{pmatrix} 1+\sqrt{\epsilon} & 0 \\ 0 & 1-\sqrt{\epsilon} \end{pmatrix}$. Láthatjuk, hogy a paraméter legcsekélyebb változtatása is teljesen más Jordan-normálformát eredményez. Általában is igaz, ha egy A mátrixnak többszörös sajátértéke van, akkor érzékeny. Ez a rosszul kondícionáltság az oka annak, hogy nehéz robusztus numerikus algoritmust találni ennek a kanonikus alaknak a meghatározására.

A Jordan-normálforma inkább elméleti szempontból jelentős.

Lássunk egy példát az alkalmazására:

Legyen A $\in$ M$_n(\mathbb{C})$. Tekintsük az A, A^2,A^3, $\ldots$ sorozatot. Felmerülhet az kérdés, hogy ez a sorozat mikor tart 0_n-hoz.

4.3.1. Tétel. *$A^m \to 0_n$, akkor és csak akkor, ha a sajátértékeinek az abszolútértéke kisebb, mint 1.*

Bizonyítás:
Elég a J(a;r) Jordan-blokkot tekinteni. J(a;r) = aI$_r$ + N $\in$ M$_r(\mathbb{C})$
Mivel N^m = 0 m $\geq$ k esetén, így teljesül

$$\mathrm{J}^m = (\mathrm{aI}_r + \mathrm{N})_m = \sum_{i=0}^{m} \binom{m}{i} a^i N^{m-i} = \sum_{i=m-k+1}^{m} \binom{m}{i} a^i N^{m-i}$$

- Mivel J^m idagonálelemei a^m-ek, ha J$^m \to 0$, akkor a$^m \to 0$, azaz |a| < 1.
- Fordítva, ha |a| < 1, akkor $|\binom{m}{m-j}$a$^{m-j}|= |\frac{m(m-1)\cdots(m-j+1)a^m}{j!a^j}| \leq |\frac{m^j a^m}{j!a^j}| \to 0$, ha m $\to \infty$ a l'Hospital-szabály miatt.

■

5. Kitekintés

Vessünk egy pillantást az eddig elhangzottakra a moduluselmélet keretein belül. Legyen V végesdimenziós k fölötti vektortér és $\tau \in L(V)$. V-re tekinthetünk polinomgyűrű fölötti modulusként is, ha a skalár szorzást a

$$p(x)v = p(\tau)(v)$$

-vel definiáljuk. V_τ-t írunk, hogy jelezzük a τ-tól való függést. V_τ és V_σ egyazon $k[X]$ gyűrű fölötti modulusok, azonban a skalárszorzás különbözik $\tau \neq \sigma$ esetén. Belátható, hogy V_σ a $k[X]$ polinomgyűrű fölötti torziómodulus.

5.0.2. Tétel. *V_τ és V_σ modulusok akkor és csak akkor izomorfak, ha létezik a V vektortér egy ϕ automorfizmusa, hogy $\sigma = \phi\tau\phi^{-1}$.*

Lineáris transzformációk hasonlósága helyett vizsgálhatjuk az általuk „indukált" modulusok izomorfiáját.
A V_τ modulusra alkalmazva a főideálgyűrű feletti végesen generált modulusok alaptételét, megkaphatjuk a transzformációk mátrixainak Frobenius, illetve Jordan-normálformáját. Erről [2]-ben részletesen olvashatunk. A mátrixok kanonikus alak problémái legtöbbször mátrixok egy halmazán (ez gyakran vektortér) történő csoporthatás által meghatározott orbitjaiból történő elem kiválasztást takar. A mátrixok kanonikus alakjait vizsgálhatjuk speciális gyűrűk pl. kvaterniók fölött. Tekinthetjük mátrixpárok, lineáris leképezéspárok kanonikus alakjait.

6. Jelölések

0_n: n $\times$ n-es nullmátrix.

1_n: n $\times$ n-es egységmátrix.

O : nullmátrix.

$D_k(N)$: k. determinánsosztó.

$L(V)$: a V vektortér lineáris transzformációinak a halmaza.

7. Irodalomjegyzék

[1] Anthony W. Knapp: Basic Algebra, Cornerstones, Birkhauser, 2007.

[2] Steven Roman: Advanced Linear Algebra, 3rd edition, Graduate Texts in Math., Vol. 135, Springer-Verlag, 2008.

[3] Denis Serre: Matrices: Theory and Applications, Graduate Texts in Math., Vol.216, Springer-Verlag, 2002.

[4] Joseph J. Rotman: Advanced Modern Algebra, 2nd edition, Prentice Hall, 2003.

[5] Kiss Emil: Bevezetés az algebrába, Typotex, 2007.

[6] V.V. Praszolov: Lineáris Algebra, Typotex, 2005.

[7] A.G. Kuros: Felsőbb Algebra, Tankönyvkiadó, 1967.

[7] N. Jacobson: Lectures in Abstract Algebra, Vol. 2: Linear Algebra, Springer-Verlag, 1984.

[8] http://www.cs.uwaterloo.ca/ astorjoh/

[11] Raymond N. Greenwell and Stanley Kertzner: Solving Linear Diophantine Matrix Equations Using the Smith Normal Form (More or Less)

[10] http://en.wikipedia.org/wiki/