Norma és nyom, a normál bázis tétel

Az alábbi jegyzetből nem minden bizonyítás szerepelt előadáson. Természetesen ezeket a bizonyításokat nem kell tudni a vizsgára. Az anyag nagy része megtalálható Pelikán József internetes Algebra jegyzetében [1] is.

Legyen L/K egy véges testbővítés, és $\alpha \in L$. Ekkor az

$$\begin{array}{rccc} s_\alpha \colon & L & \to & L \\ & \beta & \mapsto & \alpha\beta \end{array}$$

egy K-lineáris leképezés.

1. Definíció. *Az α nyomát a $\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Tr}(s_\alpha)$, az α normáját pedig a $N_{L/K}(\alpha) := \det(s_\alpha)$ képlettel definiáljuk.*

Vegyük észre, hogy $N_{L/K} \colon L^\times \to K^\times$ egy csoporthomomorfizmus, $\mathrm{Tr}_{L/K} \colon L \to K$ pedig egy K-lineáris leképezés. Továbbá ha $\alpha \in K \subseteq L$, akkor $\mathrm{Tr}_{L/K}(\alpha) = n\alpha$ és $N_{L/K}(\alpha) = \alpha^n$, ahol $n = |L : K|$, hiszen ekkor s_α egy skalármátrix.

2. Lemma. *(i) Ha $L = K(\alpha)$ egyszerű bővítés, és $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, akkor $\mathrm{Tr}_{L/K}(\alpha) = -a_{n-1}$ és $N_{L/K}(\alpha) = (-1)^n a_0$.*

(ii) Ha $K \le L \le M$ véges bővítések, akkor $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$.

Bizonyítás. *(i)* Vegyük észre, hogy ebben az esetben $1, \alpha, \ldots, \alpha^{n-1}$ bázis, melyben s_α mátrixa $\begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$, melynek nyoma $-a_{n-1}$, determinánsa pedig $(-1)^n a_0$.

(ii) Legyen $\beta = (\beta_1, \ldots, \beta_n)$ az L/K bővítés, $\gamma = (\gamma_1, \ldots, \gamma_m)$ pedig az M/L bővítés bázisa és $\alpha \in M$. Speciálisan $\beta\gamma = (\beta_i\gamma_j)_{1 \le i \le n, 1 \le j \le m}$ az M/K bővítés egy bázisa. Jelöljük a_{ij}-vel az α-val való szorzás mátrixában az i-edik sor j-edik elemét a γ bázisban. Ekkor s_α mátrixa a $\beta\gamma$ bázisban a $\begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{pmatrix}$ blokkmátrix, ahol A_{ki} az a_{ki}-vel való szorzás mátrixa β bázisban. (Valóban, a_{ki} definíciója szerint $\alpha\gamma_i = \sum_{k=1}^m a_{ki}\gamma_k$, ezért $\alpha\gamma_i\beta_j = \sum_{k=1}^m (a_{ki}\beta_j)\gamma_k$, és $a_{ki}\beta_j$ pedig az A_{ki} mátrix j-edik oszlopának és a $(\beta_1, \ldots, \beta_n)$ vektornak a skaláris szorzata az A_{ki} definíciója miatt.) Tehát

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{k=1}^m \mathrm{Tr}(A_{kk}) = \sum_{k=1}^m \mathrm{Tr}_{L/K}(a_{kk}) = \mathrm{Tr}_{L/K}(\sum_{k=1}^m a_{kk}) = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}(\alpha) \ .$$

□

3. Megjegyzés. *A normára is igaz a $N_{L/K} \circ N_{M/L} = N_{M/K}$ összefüggés, de erre most nincs szükségünk, ezért nem bizonyítjuk.*

4. Állítás. *Ha L/K* nem *szeparábilis, akkor* $\mathrm{Tr}_{L/K}$ *azonosan* 0.

Bizonyítás. Legyen $\mathrm{char}(K) = p > 0$, és $\alpha \in L$ egy inszeparábilis elem. Ekkor α minimálpolinomja $m_\alpha(x) = g(x^p)$ alakba írható valamilyen $g(x) \in K[x]$ irreducibilis polinomra. Ekkor $K \leq K(\alpha^p) \lneq K(\alpha) \leq L$, ahol a $K(\alpha)/K(\alpha^p)$ egy p-edfokú (tisztán) inszeparábilis bővítés ($|K(\alpha) : K(\alpha^p)| = p$ a fokszámtételből következik, hiszen α^p minimálpolinomja $g(x)$, az inszeparabilitás pedig abból, hogy α p-edik hatványa benne van $K(\alpha^p)$-ben). A $2(ii)$-es Lemma szerint elég belátni, hogy $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)} = 0$. Node α^i $(i = 1, \ldots, p-1)$ minimálpolinomja ebben a bővítésben $x^p - \alpha^{pi}$, hiszen ez egy p-ed-fokú $K(\alpha^p)[x]$-beli polinom, aminek α^i gyöke, és $\alpha^i \notin K(\alpha^p)$, mivel egyébként α is benne lenne ebben a testben, ugyanis kifejezhető α^p és α^i egész kitevős hatványainak szorzataként. Tehát a $2(i)$-es Lemma szerint $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}(\alpha^i) = 0$ minden $1 \leq i \leq p-1$-re, sőt, $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}(1) = |K(\alpha) : K(\alpha^p)| \cdot 1 = p \cdot 1 = 0$. Vagyis a $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}$ lineáris leképezés eltűnik egy bázison, azaz azonosan 0. □

5. Lemma (Dedekind)**.** *Legyen L/K véges szeparábilis bővítés. Ekkor* $\mathrm{Hom}_K(L, \overline{K})$ *elemei lineárisan függetlenek $\overline{K}$ felett. (Azaz ha $\{\tau_1, \ldots, \tau_n\} = \mathrm{Hom}_K(L, \overline{K})$, $a_1, \ldots, a_n \in \overline{K}$, melyre $\sum_{i=1}^n a_i\tau_i \colon L \to \overline{K}$ az azonosan 0 K-lineáris leképezés, akkor $a_1 = \cdots = a_n = 0$.)*

Bizonyítás. Legyen $a_1, \ldots, a_n \in \overline{K}$. Tegyük fel, hogy $\sum_{i=1}^n a_i\tau_i(\alpha) = 0$ minden $\alpha \in L$-re. Az a_i-k közti nem 0 elemek száma szerinti indukcióval belátjuk, hogy $a_1 = \cdots = a_n = 0$. Ha csak 1 darab $\neq 0$ van az a_i-k között, akkor készen vagyunk, hiszen egyik τ_i sem azonosan 0. Tegyük fel most, hogy $a_1 \neq 0 \neq a_2$. Mivel $\tau_1 \neq \tau_2$, ezért van olyan $\beta \in L$, melyre $\tau_1(\beta) \neq \tau_2(\beta)$. Ekkor a $\sum_i a_i\tau_i(\alpha) = 0$ egyenletet $\tau_1(\beta)$-val megszorozva, es levonva a $\sum_i a_i\tau_i(\beta\alpha) = 0$ egyenletből a $\sum_{i=2}^n a_i(\tau_i(\beta) - \tau_1(\beta))\tau_i(\alpha) = 0$ egyenletet kapjuk, melyben az indukciós feltevés miatt minden tag 0. Speciálisan $a_2 = 0$, ami ellentmondás. □

6. Állítás. *Legyen L/K szeparábilis bővítés, és* $\mathrm{Hom}_K(L, \overline{K}) = \{\tau_1, \ldots, \tau_n\}$. *Ekkor* $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \tau_i(\alpha)$, *és* $N_{L/K}(\alpha) = \prod_{i=1}^n \tau_i(\alpha)$.

Bizonyítás. Legyen $\beta_1, \ldots, \beta_n$ bázis L/K-ban (vegyük észre, hogy ez ugyanaz az n, hiszen feltettük, hogy L/K szeparábilis). Ekkor $S := (\tau_i(\beta_j))_{i,j}$ egy invertálható $n \times n$-es mátrix, hiszen az oszlopai lineárisan függetlenek a Dedekind Lemma miatt. Legyen $A = (a_{kj})_{k,j} \in K^{n\times n}$ az α-val való s_α szorzás mátrixa a $\beta_1, \ldots, \beta_n$ bázisban, azaz $\alpha\beta_j = \sum_{k=1}^n \beta_k a_{k,j}$. Utóbbi egyenletre ráalkalmazva a τ_i K-homomorfizmust a

$$\tau_i(\alpha)\tau_i(\beta) = \sum_{k=1}^n \tau_i(\beta_k)\tau_i(a_{kj}) = \sum_{k=1}^n \tau_i(\beta_k)a_{kj}$$

egyenletet kapjuk, hiszen $a_{kj} \in K$. Ez pont azt jelenti, hogy

$$\begin{pmatrix} \tau_1(\alpha) & & \\ & \ddots & \\ & & \tau_n(\alpha) \end{pmatrix} S = SA \ ,$$

azaz $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(A) = \sum_{i=1}^n \tau_i(\alpha)$ és $N_{L/K}(\alpha) = \det(A) = \prod_{i=1}^n \tau_i(\alpha)$, hiszen S invertálható. □

7. Következmény. *Az L/K véges bővítés pontosan akkor szeparábilis, ha* $\mathrm{Tr}_{L/K}$ *nem azonosan* 0.

Bizonyítás. Ha L/K nem szeparábilis, akkor ez a 4-es Állítás, ha pedig L/K szeparábilis, akkor a 6-os Állításból következik, mivel $\mathrm{Tr}_{L/K} = \sum_{i=1}^{n} \tau_i$ nem azonosan 0 a Dedekind Lemma szerint, hiszen ez egy nemtriviális lineáris kombinációja a τ_i K-homomorfizmusoknak. □

8. Tétel (Hilbert 90)**.** *Tegyük fel, hogy L/K egy olyan Galois-bővítés, melyre* $\mathrm{Gal}(L/K) = \langle\sigma\rangle \cong Z_n$ *ciklikus (σ-val, mint generátorral) és $\alpha \in L$ egy 1-normájú elem. Ekkor van olyan $0 \neq \beta \in L$ elem, melyre $\alpha = \beta/\sigma(\beta)$.*

Megjegyzés: vegyük észre, hogy a megfordítás triviális, hiszen β és $\sigma(\beta)$ normája megegyezik.

Bizonyítás. A Dedekind Lemma miatt $\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}$ lineárisan függetlenek, ezért van olyan $\gamma \in L$, melyre

$$\beta := \mathrm{id}_L(\gamma) + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma) \neq 0 \ .$$

Könnyű számolás mutatja, hogy ekkor $\alpha\sigma(\beta) = \beta$. □

9. Következmény. *Ha $\mu_n \subseteq K$ és L/K olyan Galois-bővítés, melyre* $\mathrm{Gal}(L/K) \cong Z_n$*, akkor $L = K(\beta)$ alkalmas $\beta \in L$ elemmel, melynek minimálpolinomja $x^n - b$ alakú.*

Bizonyítás. Vegyük észre, hogy ha ε egy primitív n-edik egységgyök, akkor $\varepsilon \in K$ miatt $N_{L/K}(\varepsilon) = \varepsilon^n = 1$. Tehát Hilbert 90-es tétele szerint van olyan $0 \neq \beta \in L$, melyre $\beta/\sigma(\beta) = \varepsilon$. Ekkor $\sigma^i(\beta) = \beta\varepsilon^{-i}$, azaz β minimálpolinomja $m_\beta(x) = \prod_{i=0}^{n-1}(x - \beta\varepsilon^i) = x^n - \beta^n \in K[x]$ (hiszen $\sigma^i(\beta)$ mind különböző), azaz $b = \beta^n \in K$. □

10. Tétel (Normál bázis-)**.** *Legyen L/K egy véges Galois-bővítés és $G := \mathrm{Gal}(L/K)$. Ekkor van olyan $\beta \in L$, melyre a $\{\sigma(\beta) \mid \sigma \in G\}$ halmaz K-lineárisan független, tehát L egy K feletti bázisát alkotja. Egy ilyen bázist L/K* normál bázis*ának nevezünk.*

Bizonyítás. A bizonyítás két esetből áll.

1. eset: $|K|$ végtelen. Mivel L/K Galois, speciálisan szeparábilis, ezért van olyan $\alpha \in L$, melyre $L = K(\alpha)$. Legyen $f(x) \in K[x]$ az α minimálpolinomja. Ez L fölött $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ gyöktényezők szorzatára bomlik ($\alpha = \alpha_1$), hiszen L/K normális bővítés. Legyen $g_i(x) := \frac{f(x)}{f'(\alpha_i)(x-\alpha_i)} \in L[x]$. Ekkor

$$\sum_{i=1}^{n} g_i(x) = 1 \ , \tag{1}$$

hiszen az $1 - \sum_{i=1}^{n} g_i(x)$ egy legfeljebb $n-1$-edfokú polinom, ami az $\alpha_1, \ldots, \alpha_n$ n különböző helyen eltűnik. Másrészt

$$g_i(x)g_j(x) \equiv \begin{cases} 0 \mod (f(x)) & \text{ha } i \neq j \\ g_i(x) \mod (f(x)) & \text{ha } i = j \end{cases} \ . \tag{2}$$

Valóban, $g_i(x)g_j(x)$-nek gyöke $\alpha_1, \ldots, \alpha_n$, ha $i \neq j$. Ha pedig $i = j$, akkor $g_i(x)^2 - g_i(x)$-nek gyöke minden α_k ($k = 1, \ldots, n$), hiszen $g_i(\alpha_i)^2 = g_i(\alpha_i) = 1$ és $k \neq i$-re $g_i(\alpha_k) = 0$.

Legyen most $\mathrm{Gal}(L/K) = \{\mathrm{id} = \sigma_1, \ldots, \sigma_n\}$ és $\alpha_i = \sigma_i(\alpha) \in L$. Képzzük az $A \in L[x]^{n\times n}$ mátrixot a következőképpen: legyen az i-edik sor j-edik eleme $\sigma_i(\sigma_j(g_1(x))) \in L[x]$. Ekkor az

(1) és (2) azonosságok épp azt mutatják, hogy $A^TA \equiv I \mod (f(x))$ (itt I az egységmátrix). Valóban, vegyük észre, hogy $\sigma_i(g_1(x)) = \frac{f(x)}{f'(\sigma_i(\alpha))(x-\sigma_i(\alpha))} = g_i(x)$, mivel $f(x)$ együtthatói K-ból valók, speciálisan minden σ_i fixálja őket. Tehát A^TA főátlójában $\sum_{i=1}^n g_i(x)^2$ áll, ami (1) és (2) kombinálásával 1-gyel kongruens modulo $(f(x))$. A főátlón kívüli elemek pedig $g_i(x)g_j(x)$ alakú tagok összegei, ahol $i \neq j$, tehát oszthatók $f(x)$-szel. Speciálisan $\det(A)^2 = \det(A^TA) \equiv 1 \pmod{(f(x))}$, azaz nem lehet azonosan 0, így $\det(A)$ sem azonosan 0. Mivel K végtelen, van olyan $\gamma \in K$, melyre $\det(A(\gamma)) = \det(\sigma_i\sigma_j(g_1(\gamma)))_{i,j} \neq 0$. Ekkor a $\beta = g_1(\gamma)$ választással tegyük fel, hogy $a_1\sigma_1(\beta) + \cdots + a_n\sigma_n(\beta) = 0$ valamilyen $a_1, \ldots, a_n \in K$ elemekkel. Erre a σ_i automorfizmust ráalkalmazva azt kapjuk, hogy $\sum_{j=1}^n a_j\sigma_i\sigma_j(\beta) = 0$, hiszen $\sigma_i(a_j) = a_j$ $(a_j \in K)$. Ez pedig azt jelenti, hogy $A(\gamma)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$, azaz $a_1 = \cdots = a_n = 0$, mert $A(\gamma)$ invertálható. Azt kaptuk, hogy $\sigma_1(\beta), \ldots, \sigma_n(\beta)$ lineárisan független K fölött, azaz egy bázisa L-nek, mint K feletti vektortérnek.

2. eset: $|K| = q = p^f$ véges. Ekkor $\mathrm{Gal}(L/K)$-t generálja a q-Frobenius Frob_q, melynek rendje $n = |L : K|$. A Dedekind Lemma miatt $\mathrm{id}, \mathrm{Frob}_q, \ldots, \mathrm{Frob}_q^{n-1}$ lineárisan független L felett, speciálisan Frob_q minimálpolinomja minimum n-edfokú. Viszont $\mathrm{Frob}_q^n = \mathrm{id}$, tehát $\mathrm{Frob}_q\colon L \to L$ K-lineáris leképezés minimálpolinomja $x^n - 1$. Tekintsük L-et a $K[x]$ polinomgyűrű feletti modulusnak, ahol az x-szel való szorzás a Frob_q lineáris leképezés. A főideálgyűrű feletti modulusok alaptételéből következik, hogy $L \cong \bigoplus_{i=1}^r K[x]/(f_i(x))$ prímhatványrendű ciklikusak direkt összegeként írható, ahol ráadásul az $f_i(x)$-ek legkisebb közös többszöröse $x^n - 1$ és $\sum_i \deg(f_i) = \dim_K L = n$. Tehát ha $x^n - 1 = \prod_j g_j(x)^{n_j}$ a K feletti irreducibilisekre való felbontás, akkor minden j-re van olyan i, melyre $g_j(x)^{n_j} \mid f_i(x)$. De ekkor $g_j(x)^{n_j} = f_i(x)$, mivel $\sum_j n_j \deg g_j = n = \sum_i \deg(f_i)$. Speciálisan $L \cong \bigoplus_j K[x]/(g_j(x)^{n_j} \cong K[x]/(x^n - 1)$. Ha $\beta \in L$ az $1 + (x^n - 1)$ képe ennél az izomorfizmusnál, akkor x^k képe éppen $\mathrm{Frob}_q^k(\beta)$, és $\beta, \mathrm{Frob}_q(\beta), \ldots, \mathrm{Frob}_q^{n-1}(\beta)$ bázis L-ben, hiszen $1, x, \ldots, x^{n-1}$ bázis $K[x]/(x^n - 1)$-ben. □

Legyen L/K egy véges Galois-bővítés, $G := \mathrm{Gal}(L/K)$. Ekkor L-en hat a G csoport K-lineárisan, azaz L, mint n-dimenziós K-vektortér, a G csoport egy reprezentációját alkotja. A fenti tétel azt mutatja, hogy ha L-re mint a KG csoportalgebra feletti modulusra tekintünk, akkor $L \cong KG$ (mint KG feletti balmodulusok). Az izomorfizmust az $KG \ni 1 \mapsto \beta \in L$ leképezés szolgáltatja. Tehát L természetes módon a G csoport reguláris reprezentációja (egy 1 rangú szabad KG-modulus). Ez az állítás fontos szerepet játszik a Galois-kohomológiában, speciálisan a Hilbert 90-es tétel általánosításaiban arra az esetre, amikor G nem feltétlenül ciklikus. A következő tételt is lehet a Galois-kohomológián (és a Normál Bázis Tételen) keresztül bizonyítani, de mivel előbbit nem tanuljuk, íme egy elemi bizonyítás:

11. Tétel (Artin-Schreier-elmélet)**.** *Legyen L/K egy p-edfokú Galois bővítése p-karakterisztikájú testeknek. Ekkor van olyan $\alpha \in L$, melynek minimálpolinomja $x^p - x - a$ alakú.*

Bizonyítás. Legyen $\mathrm{Gal}(L/K) = G$, ekkor G egy p-edrendű csoport, tehát ciklikus. Jelöljük σ-val az egyik generátorát. A Dedekind Lemma miatt $1, \sigma, \ldots, \sigma^{p-1}$ linárisan független, tehát $\sigma\colon L \to L$ minimálpolinomja csak $x^p - 1 = (x-1)^p$ lehet. Tehát $(\sigma - 1)(L)$ $p-1$-dimenziós (egyébként már a $p-1$-edik hatványa is 0 lenne), és tartalmazza $K = \mathrm{Ker}(\sigma - 1)$-et. Mivel $1 \in K$, ezért van olyan $\alpha \in L$, melyre $\sigma(\alpha) - \alpha = (\sigma - 1)(\alpha) = 1$. Ezt iterálva azt kapjuk, hogy $\sigma^i(\alpha) = \alpha + i$ mind különbözők $(i = 0, \ldots, p-1)$, tehát α minimálpolinomja

$\prod_{i=0}^{p-1}(x-\alpha-i) = (x-\alpha)^p - (x-\alpha) = x^p - x - a$ (ahol $a := \alpha^p - \alpha \in K$), hiszen $y^p - y = \prod_{i=0}^{p-1}(y-i)$ a gyöktényezős felbontás p-karakterisztikában. □

Hivatkozások

[1] Pelikán József, *Algebra*, `http://www.cs.elte.hu/~pelikan/11_Testek.pdf`