Centrális egyszerű algebrák osztályozása

Zábrádi Gergely

2019. május 2.

Ez a jegyzet a 2019 tavaszi Algebra4 kruzushoz íródott, lényegében a [2] könyv alapján, de néhány bizonyítás eltér az ottanitól (pl. Wedderburn tételéé, de a 3.16. Lemmáé is). A jegyzet folyamatosan frissül, és tartalmaz olyan anyagokat is, melyekre esetleg nem jut idő előadáson – ezeket természetesen nem kell tudni a vizsgára. Ha valaki talál hibát (akár elírást, akár lényegit), azt kérem jelezze nekem.

1. Wedderburn tétele végesdimenziós egyszerű algebrákról

Legyen A egy végesdimenziós algebra a K test fölött, azaz A egy olyan egységelemes gyűrű, mely részgyűrűként tartalmazza K-t, ráadásul K elemei minden A-belivel felcserélhetők, azaz $K \leq Z(A)$ (és $\dim_K A < \infty$). Az elsődleges célunk Wedderburn alábbi klasszifikációs tételének bizonyítása:

1.1. Tétel (Wedderburn)**.** *Ha A egyszerű K fölötti végesdimenziós algebra, akkor izomorf egy alkalmas ferdetest feletti $n \times n$-es teljes mátrixgyűrűvel valamilyen $n \geq 1$ egészre.*

Az első természetesen fermerülő kérdés, honnan kapjuk a ferdetestet, ami felett majd A teljes mátrixgyűrű lesz. Tekintsünk egy M egyszerű bal-modulust A fölött. Ilyen létezik, hiszen ha $L \lhd_b A$ egy maximális balideál, akkor $M := A/L$ egyszerű. (Krull tétele szerint minden egységelemes gyűrűnek van maximális balideálja. Végesdimenziós algebrák esetén nincs szükség a Zorn-lemmára ennek igazolásához: a maximális dimenziós balideálok szükségképpen maximálisak a tartalmazásra nézve is.) Sőt, minden egyszerű modulus ilyen alakú: ha $0 \neq m \in M$ tetszőleges, akkor M egyszerűsége szerint $Am = M$. Tehát az

$$\begin{array}{rcl} \varphi\colon A & \to & M \\ 1 & \mapsto & m \end{array}$$

modulushomorfizmus szürjektív, speciálisan a homomorfizmus-tétel miatt $M \cong A/\mathrm{Ker}(\varphi)$, ahol $\mathrm{Ker}(\varphi)$ egy maximális balideál (II. izomorfizmus tétel). Vegyük észre, hogy M is természetes módon K-vektortér: valóban, $K \leq A$ miatt K-modulus is. Továbbá $\dim_K M < \infty$, hiszen előáll A faktormodulusaként.

1.2. Lemma (Schur)**.** *Ha M egy egyszerű modulus az R gyűrű fölött, akkor* $\mathrm{End}_R(M)$ *egy ferdetest az endomorfizmusok összeadására és a kompozícióra, mint szorzásra nézve.*

Bizonyítás. Az, hogy $\mathrm{End}_R(M)$ gyűrű világos a definícióból: az egyetlen ellenőrzendő a bal oldali disztributivitás: ha $\alpha, \beta, \gamma \in \mathrm{End}_R(M)$ endomorfizmusok, akkor $\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma$, hiszen α additív. Az identitás $\mathrm{id}\colon M \to M$ nyilván egységelem. Továbbá, ha $\alpha\colon M \to M$ egy nemnulla endomorfizmus, akkor $\mathrm{Ker}(\alpha) \lneq M$ egy részmodulus, tehát $\mathrm{Ker}(\alpha) = 0$, hiszen M egyszerű, azaz nincs nemtriviális részmodulusa. Hasonlóan $0 \neq \mathrm{Im}(\varphi) \leq M$ is részmodulus, ezért $\mathrm{Im}(\varphi) = M$, azaz φ bijektív. Speciálisan φ-nek van inverze. Azt kell még ellenőrizni, hogy φ^{-1} is egy endomorfizmus, de ez egy könnyű számolás, amit az olvasóra bízunk. □

Legyen $D := \mathrm{End}_A(M)$, mely a Schur-lemma szerint egy ferdetest. Ekkor M bal-modulus D fölött is, hiszen M elemeit szorozhatjuk D elemeivel: ha $\varphi \in D$ és $m \in M$, akkor a szorzat $\varphi(m)$ lesz. Másrészt K résztest D-ben is, hiszen ha $c \in K$ tetszőleges, akkor a c-vel való szorzás A-endomorfizmusa lesz M-nek, mert $c \in Z(A)$, azaz a c-vel való szorzás A-lineáris: $c \cdot (rm) = rc \cdot m$. Vegyük észre, hogy az „endomorfizmusgyűrűképzés" egyfajta dualitásfogalom: az, hogy $\varphi(rm) = r\varphi(m)$ minden $r \in A$-ra és $\varphi \in D$-re tekinthető úgy is, hogy az r-rel való szorzás D-lineáris. Ilymódon kapunk egy gyűrűhomomorfizmust A-ból $\mathrm{End}_D(M)$-be. Mivel M végesdimenziós K fölött (és $K \leq D$), ezért M végesdimenziós D fölött is. Legyen tehát $e_1, \ldots, e_n \in M$ egy bázisa M-nek, mint D feletti vektortérnek. Ha $r \in A$, akkor r-nek megfeleltethetünk egy $n \times n$-es D-beli együtthatós mátrixot az alábbi módon:

$$\begin{aligned} r &\mapsto (\varphi_{ij})_{i,j} \in D^{n\times n} \text{ , ha} \\ re_j &= \sum_{i=1}^{n} \varphi_{ij} e_i \end{aligned}$$

alkalmas $\varphi_{ij} \in D$ elemekkel ($1 \leq i, j \leq n$). A fenti $A \to D^{n\times n}$ hozzárendelés nyilván összegtartó, viszont a szorzással az alábbi furcsa módon viselkedik: ha $s \in A$-hoz a $(\psi_{ki})_{k,i}$ mátrixot rendeljük, akkor

$$sre_j = s\left(\sum_{i=1}^{n} \varphi_{ij} e_i\right) = \sum_{i=1}^{n} \varphi_{ij} s e_i = \sum_{i=1}^{n} \varphi_{ij} \sum_{k=1}^{n} \psi_{ki} e_k = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \varphi_{ij} \circ \psi_{ki}\right) e_k \ .$$

Itt $\sum_{i=1}^{n} \varphi_{ij} \circ \psi_{ki}$ szinte a szorzatmátrix képlete – az egyetlen probléma, hogy $\varphi_{ij} \circ \psi_{ki}$ rossz sorrendben van. Ezért szükség van az alábbi definícióra:

1.3. Definíció. Legyen R egy tetszőleges gyűrű. Ekkor az R oppozit gyűrűjén az R^{op} gyűrűt értjük, melynek additív csoportja R, de a szorzás „fordítva" van definiálva, azaz $r, s \in R$ esetén az oppozit gyűrűbeli szorzat $r \cdot_{op} s := s \cdot r$.

1.4. Megjegyzés. Ha R kommutatív, akkor nyilván $R \cong R^{op}$. Viszont a megfordítás nem igaz: például ha $R = M_n(K)$ egy K test feletti $n \times n$-es teljes mátrixgyűrű, akkor $R \cong R^{op}$: az izomorfizmust a transzponálás ($A \mapsto A^T$) adja. Ha $R = KG$ csoportalgebra, akkor is $R \cong R^{op}$: itt pedig az izomorfizmust a G elemein való invertálás adja.

A fentiek szerint kapunk tehát egy $A \to M_n(D^{op})$ gyűrűhomomorfizmust, ahol $M_n(D^{op})$ az D^{op} oppozit gyűrű feletti teljes $n \times n$-es mátrixgyűrű. Az alábbi egy lineáris algebrai emlékeztető feladat.

1.5. Gyakorlat. (*a*) *Igazoljuk, hogy* $E_{ij}E_{kl} = \begin{cases} 0 & \text{ha } j \neq k \\ E_{il} & \text{ha } j = k \end{cases}$, *ahol* $E_{uv} \in M_n(D^{op})$ *azt a mátrixot jelöli, melynek* u*-adik sorának* v*-edik eleme* 1*, az összes többi pedig* 0 *(*$1 \leq i, j, k, l, u, v \leq n$*.*

(*b*) *Igazoljuk, hogy ha* $0 \neq I \lhd M_n(D^{op})$ *egy tetszőleges nemnulla kétoldali ideál, akkor van olyan* $1 \leq i, j \leq n$*, melyre* $E_{ij} \in I$*.*

(*c*) *Igazoljuk, hogy* $M_n(D^{op})$ *egyszerű gyűrű, azaz nincs nemtriviális kétoldali ideálja.*

Ugyan elsőrendű célunk a test fölötti végesdimenziós egyszerű algebrák osztályozása, a Schur-lemmához hasonlóan a következőt is általánosabb formában igazoljuk.

1.6. Tétel (Jacobson sűrűségi tétele)**.** *Legyen* R *egy tetszőleges gyűrű, és* M *egy egyszerű* R*-modulus,* $D := \mathrm{End}_R(M)$*. Ekkor* R *képe* sűrű $\mathrm{End}_D(M)$*-ben: ha* $x_1, \ldots, x_k$ *lineárisan függetlenek* D *fölött,* $y_1, \ldots, y_k \in M$ *pedig tetszőlegesek, akkor van olyan* $r \in R$*, melyre* $rx_j = y_j$ *minden* $j = 1, \ldots, k$*-ra.*

Bizonyítás. Az állítást k szerinti indukcióval bizonyítjuk. Ha $k=1$, akkor x_1 függetlensége annyit tesz, hogy $x_1 \neq 0$. Ekkor $0 \neq Rx_1 \leq M$ egy részmodulus, ami egyenlő M-mel, hiszen M egyszerű. Speciálisan $y_1 \in Rx_1$, azaz van olyan $r \in R$, melyre $y_1 = rx_1$. Tegyük fel, hogy az állítást $k-1$-re már beláttuk. Speciálisan van egy olyan $r' \in R$ elem, melyre $y_j = r'x_j$ minden $j = 1, \ldots, k-1$-re. Ekkor r-et $r = r' + s$ alakban keressük, ahol $sx_j = 0$ $(j = 1, \ldots, k-1)$ és $sx_k = y_k - r'x_k$. A feltétel $j = 1, \ldots, k-1$-re azt jelenti, hogy $s \in R$ benne van az $\{x_1, \ldots, x_{k-1}\}$ halmaz $L_{k-1} := \mathrm{Ann}_R(x_1, \ldots, x_{k-1})$ annullátorában, mely egy balideál R-ben.

1.7. Lemma. *Ha az $x_1, \ldots, x_k \in M$ elemek lineárisan függetlenek D fölött, akkor $L_{k-1}x_k \neq 0$.*

Bizonyítás. Tegyük fel az állítással ellentétben, hogy $L_{k-1}x_k = 0$. Az indukciós feltevés szerint az $(x_1, \ldots, x_{k-1}) \in M^{k-1}$ vektor generálja M^{k-1}-t, mint R-modulust: tetszőleges $(z_1, \ldots, z_{k-1}) \in M^{k-1}$ vektorra van olyan $t \in R$, hogy $t(x_1, \ldots, x_{k-1}) = (z_1, \ldots, z_{k-1})$, azaz $R(x_1, \ldots, x_{k-1}) = M^{k-1}$. Így a

$$\begin{aligned} \Phi\colon M^{k-1} &\to M \\ t(x_1, \ldots, x_{k-1}) &\mapsto tx_k \end{aligned}$$

egy jóldefiniált R-modulus homomorfizmus: Azért jóldefiniált, mert egyrészt a bal oldal minden eleme előáll $t(x_1, \ldots, x_{k-1})$ alakban. Másrészt ha $t(x_1, \ldots, x_{k-1}) = t'(x_1, \ldots, x_{k-1})$ valamely $t, t' \in R$ elemekre, akkor $t - t' \in L_{k-1}$ és az indirekt feltevésünk szerint így $(t-t')x_k = 0$, azaz $tx_k = t'x_k$. Az pedig, hogy ez összeget és R-beli elemszerest tart, világos a definícióból. Tehát

$$\Phi \in \mathrm{Hom}_R(M^{k-1}, M) = \bigoplus_{j=1}^{k-1} \mathrm{Hom}_R(M, M) = \bigoplus_{j=1}^{k-1} D\ .$$

Ennél az azonosításnál Φ egy $(\varphi_1, \ldots, \varphi_{k-1}) \in \bigoplus_{j=1}^{k-1} D$ elemnek felel meg, ami azt jelenti, hogy

$$tx_k = \Phi(t(x_1, \ldots, x_{k-1})) = \varphi_1(tx_1) + \cdots + \varphi_{k-1}(tx_{k-1})$$

minden $t \in R$-re teljesül. Speciálisan $t = 1$-re is, azaz $x_k = \sum_{j=1}^{k-1} \varphi_j(x_j)$. Ez azt jelenti, hogy x_k-t előállítottuk $x_1, \ldots, x_{k-1}$ elemek D-lineáris kombinációjaként, ami ellentmond annak a feltevések, hogy lineárisan függetlenek. □

Mivel $L_{k-1}x_k$ egy nemnulla részmodulus M-ben, ezért $L_{k-1}x_k = M$. Speciálisan van olyan $s \in L_{k-1}$, melyre $sx_k = y_k - r'x_k$, így $r := r' + s$ megfelel. □

1.8. Megjegyzés. A sűrűség egy topológiai fogalom, mégpedig egy X topologikus tér egy $H \subset X$ részhalmaza *sűrű*, ha tetszőleges $U \subset X$ nyílt halmazzal vett metszete nemüres. Ez nem véletlen: létezik $\mathrm{End}_D(M)$-en egy olyan topológia, melyben a fenti tétel állítása épp az, hogy R képe sűrű. Ezt a topológiát a következőképp adhatjuk meg. Tegyük M-re a diszkrét topológiát. Ekkor minden $M \to M$ függvény folytonos lesz, tehát $\mathrm{Hom}_R(M, M)$ egy részhalmaza $C(M, M)$-nek (azaz az összes $M \to M$ – folytonos – függvény terének). Lássuk el $C(M, M)$-et az ún. *kompakt-nyílt* topológiával, melynek előbázisát a $V(K, U) := \{f \in C(M, M) \mid f(K) \subseteq U\}$ halmazok alkotják, ahol $K \subset M$ kompakt, $U \subset M$ nyílt. Persze mivel M diszkrét $K \subseteq M$ pontosan akkor kompakt, ha véges, továbbá tetszőleges $U \subseteq M$ nyílt. Tehát ez nem más, mint ha vennénk $|M|$ példányát M-nek, és azok direkt szorzatára rátennénk a szorzattopológiát. Lássuk el ebben a topológiában $\mathrm{End}_D(M) \subset C(M, M)$-et az altértopológiával. Ebben a topológiában egy adott $f \in \mathrm{End}_D(M)$ endomorfizmus környezetbázisát alkotják a $V(x_1, \ldots, x_k, f) = \{g \in \mathrm{End}_D(M) \mid g(x_i) = f(x_i),\ i = 1, \ldots, k\}$ alakú halmazok, ahol $x_1, \ldots, x_k \in M$ és $k \geq 1$, ezért a sűrűségi tétel állítása épp az, hogy R képe sűrű $\mathrm{End}_D(M)$-ben.

Wedderburn tételének bizonyítása. Legyen A egy K feletti végesdimenziós algebra és $D := \mathrm{End}_A(M)$ valamely M egyszerű A-modulusra, továbbá $n := \dim_D M$. Ekkor Jacobson sűrűségi tétele szerint az $A \to M_n(D^{op})$ gyűrűhomomorfizmus szürjektív. Ha A-ról még azt is feltesszük, hogy egyszerű gyűrű, akkor az $A \to M_n(D^{op})$ gyűrűhomomorfizmus nemcsak szürjektív, hanem injektív is, hiszen magja egy ideál A-ban, mely nem tartalmazza az egységelemet. Ezzel Wedderburn 1.1. Tételét bizonyítottuk. □

1.9. Gyakorlat. *Legyen D egy ferdetest. Mutassuk meg, hogy az n-dimenziós oszlopvektorok D^n vektortere egyszerű modulus az $M_n(D)$ mátrixgyűrű fölött a szokásos mátrix-vektor szorzással.*

A fenti gyakorlat segítségével $M_n(D)$-t, mint saját maga fölötti balmosulust is előállíthatjuk egyszerű modulusok direkt összegeként: valóban, ha M_j-vel jelöljük azon mátrixok halmazát, melyeknek csak a j-edik oszlopban van nemnulla eleme ($j = 1, \dots, n$), akkor M_j egy balideál $M_n(D)$-ben, és izomorf D^n-nel, mint $M_n(D)$ fölötti modulus. Ugyanakkor $M_n(D) = \bigoplus_{j=1}^{n} M_j$.

1.10. Következmény. *Az $M_n(D)$ ferdetest fölötti teljes mátrixgyűrű fölött izomorfia erejéig egyetlen egyszerű (bal-)modulus van.*

Bizonyítás. Ha M egy egyszerű modulus, akkor előáll $M_n(D)$ faktormodulusaként, azaz van egy

$$\pi\colon M_n(D) = \bigoplus_{j=1}^{n} M_j \to M$$

szürjektív modulushomomorfizmus. Ekkor van olyan $j \in \{1, \dots, n\}$, melyre π megszorítása M_j-re nem azonosan 0 (hiszen egyébként π azonosan 0 lenne). Viszont ekkor π izomorfizmust indukál M_j és M között, hiszen mindkettő egyszerű. □

1.11. Következmény. *Wedderburn tételében n és D (izomorfia erejéig) egyértelműen meghatározott az A egyszerű algebra által. Más szavakkal: ha $M_n(D) \cong M_m(D')$ valamely $n, m \geq 1$ egész számokra és D, D' ferdetestekre, akkor $n = m$ és $D \cong D'$.*

Bizonyítás. Az 1.10. Következmény szerint legyen M az (izomorfia erejéig egyértelmű) egyszerű modulus $A := M_n(D) \cong M_m(D')$ fölött. Ekkor Wedderburn tételének konstrukciója szerint $D^{op} \cong \mathrm{End}_A(M) \cong D'^{op}$ és $n = \dim_{D^{op}} M = m$. □

A továbbiakban a cél az lesz, hogy konkrét K test esetében klasszifikáljuk a K felett végesdimenziós D ferdetesteket is. Természetesen K véges testbővítései megfelelnek – ezeket ismerjük Galois-elméletből. Ezeket kiküszöbölendő tesszük az alábbi feltételt:

1.12. Definíció. Egy adott K test feletti *centrális egyszerű algebrának* egy olyan K felett végesdimenziós A algebrát nevezünk, melynek centruma $Z(A) = K$.

A fenti definíció kizárja a testbővítéseket, viszont megengedi a K feletti $M_n(K)$ teljes mátrixgyűrűt.

1.13. Gyakorlat. *Mutassuk meg, hogy ha A egy centrális egyszerű algebra K fölött és $n \geq 1$ egész, akkor $M_n(A)$ is centrális egyszerű algebra.*

1.14. Példa. (a) Legyen $K = \mathbb{R}$. Frobenius tétele szerint olyan ferdetest, mely $\mathbb{R}$ felett végesdimenziós és a centruma $\mathbb{R}$ csak kettő létezik: $\mathbb{R}$ és $\mathbb{H}$ (kvaterniók), hiszen $\mathbb{C}$ centruma nem $\mathbb{R}$. Tehát az $\mathbb{R}$ fölötti centrális egyszerű algebrák a következők: $M_n(\mathbb{R})$, illetve $M_n(\mathbb{H})$, ahol $n \geq 1$.

(b) Ha K algebrailag zárt (azaz $K = \overline{K}$, pl. $K = \mathbb{C}$), akkor K fölött minden centrális egyszerű algebra $M_n(K)$-val izomorf alkalmas $n \geq 1$ egésszel. Valóban, ha D egy végesdimenziós ferdetest K fölött és $\alpha \in D$, akkor α minimálpolinomja irreducibilis (hiszen D nullosztómentes), speciálisan elsőfokú K fölött, azaz $\alpha \in K$.

2. Hasítás véges bővítéssel

Ha A és B két K-algebra, akkor az $A \otimes_K B$ tenzorszorzaton a szorzást a következőképp értelmezzük: két elemi tenzor szorzata $(a_1 \otimes b_1)(a_2 \otimes b_2) := (a_1 a_2) \otimes (b_1 b_2)$ ($a_1, a_2 \in A$, $b_1, b_2 \in B$), és elemi tenzorok lineáris kombinációjára ezt a disztributivitási szabály segítségével terjesztjük ki. Egyszerű számolás mutatja, hogy így egy K-algebra struktúrát kapunk $A \otimes_K B$-n.

2.1. Lemma. *Ha $n, m \geq 1$ egészek, akkor $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$.*

Bizonyítás. Ha $X \colon K^n \to K^n$ (ill. $Y \colon K^m \to K^m$) egy $n \times n$-es ($m \times m$-es) mátrix, akkor tenzorszorzatuk egy $X \otimes Y \colon K^n \otimes_K K^m \to K^n \otimes_K K^m$ leképezés. Itt $K^n \otimes_K K^m$ egy nm-dimenziós vektortér K fölött, így kapunk egy $M_n(K) \otimes_K M_m(K) \to M_{nm}(K)$ leképezést, ami gyűrűhomomorfizmus és injektív, ezért dimenzió okokból szürjektív is. □

2.2. Gyakorlat. *Igazoljuk, hogy ha A egy K-algebra és $n \geq 1$, akkor $M_n(K) \otimes_K A \cong M_n(A)$. Ha A egy centrális egyszerű algebra, akkor $M_n(A)$ is az.*

2.3. Állítás. *Ha A egy centrális egyszerű algebra K fölött és $K \leq L$ egy véges bővítés, akkor $A \otimes_K L$ egy centrális egyszerű algebra L fölött. Sőt, ha A egy olyan K-algebra, melyre $A \otimes_K L$ centrális egyszerű algebra egy adott $K \leq L$ véges bővítés felett, akkor A is centrális egyszerű algebra K fölött.*

Bizonyítás. Tegyük fel először, hogy $A \otimes_K L$ centrális egyszerű algebra L fölött. Ha I egy ideál A-ban, akkor $I \otimes_K L$ is ideál lesz $A \otimes_K L$-ben. Mivel utóbbi egyszerű, $I = 0$ vagy $I = A$, tehát A is egyszerű. Másrészt ha A centruma $Z(A)$ szigorúan bővebb, mint K, akkor $\dim_L(Z(A) \otimes_K L) = \dim_K Z(A) > 1$. Node $Z(A) \otimes_K L$ benne van $A \otimes_K L$ centrumában, ami ellentmond a feltevésnek. Tehát A is centrális.

Megfordítva tegyük fel, hogy A centrális egyszerű algebra K fölött. Wedderburn tétele szerint $A \cong M_n(D)$ valamely K ferdetestre. Feltehetjük tehát (lsd. 2.2. Gyakorlat), hogy $A = D$ (azaz $n = 1$), hiszen

$$A \otimes_K L \cong M_n(D) \otimes_K L \cong (M_n(K) \otimes_K D) \otimes_K L \cong M_n(K) \otimes_K (D \otimes_K L) \cong M_n(D \otimes_K L) \ .$$

Vegyük L-nek egy $u_1, \ldots, u_k$ bázisát K fölött. Ekkor $D \otimes_K L$ egy α eleme egyértelműen írható $\alpha = \sum_{j=1}^k d_i \otimes u_i$ alakba, ahol $d_i \in D$ ($i = 1, \ldots, k$). Ha α benne van $D \otimes_K L$ centrumában, akkor a $d \otimes 1$ alakú elemekkel is felcserélhető ($d \in D$), azaz $\sum_{j=1}^k (dd_i) \otimes u_i = (d \otimes 1)\alpha = \alpha(d \otimes 1) = \sum_{j=1}^k (d_i d) \otimes u_i$. A felírás egyértelműsége miatt $dd_i = d_i d$ minden $i = 1, \ldots, k$-ra és $d \in D$-re, azaz $d_i \in Z(D) = K$, így $\alpha \in K \otimes_K L = L$, azaz $D \otimes_K L$ centrális.

Végezetül tegyük föl, hogy $0 \neq J \lhd D \otimes_K L$ egy kétoldali ideál. Legyen $z_1, \ldots, z_r$ egy bázisa J-nek D fölött. Másrészt mivel $\{1 \otimes u_1, \ldots, 1 \otimes u_k\}$ egy bázisa $D \otimes_K L$-nek D fölött, ezért $z_1, \ldots, z_r$ kiegészíthető $\{1 \otimes u_1, \ldots, 1 \otimes u_k\}$ egy részhalmazával $D \otimes_K L$ egy bázisává (kicserélési tétel lineáris algebrából!). A számozás esetleges megváltoztatásával feltehetjük tehát, hogy $z_1, \ldots, z_r, 1 \otimes u_{r+1}, \ldots, 1 \otimes u_k$ egy D-bázis $D \otimes_K L$-ben, azaz

$$D \otimes_K L = J \oplus \Big(\bigoplus_{j=r+1}^{k} D \otimes u_i \Big) \ .$$

Speciálisan ezt az $1 \otimes u_i$ elemekre ($i = 1, \ldots, r$) alkalmazva

$$1 \otimes u_i = y_i + \sum_{j=r+1}^{k} \alpha_{ij} \otimes u_j \tag{1}$$

alkalmas $y_i \in J$ és $\alpha_{ij} \in D$ elemekkel ($j = r+1, \dots, k$). Továbbá ez a felírás egyértelmű, ráadásul az $y_1, \dots, y_r$ elemek is J egy D fölötti bázisát alkotják, hiszen ezek lineárisan függetlenek és számuk $r = \dim_D J$. Viszont a (1) egyenletet $d \otimes 1$-gyel ($0 \neq d \in D$) megkonjugálva

$$1 \otimes u_i = (d^{-1} \otimes 1)(1 \otimes u_i)(d \otimes 1) = (d^{-1} \otimes 1) y_i (d \otimes 1) + \sum_{j=r+1}^{k} (d^{-1} \alpha_{ij} d) \otimes u_j$$

adódik. Viszont mivel J kétoldali ideál, $(d^{-1} \otimes 1) y_i (d \otimes 1) \in J$. A felírás egyértelműsége miatt tehát $(d^{-1} \otimes 1) y_i (d \otimes 1) = y_i$ és $d^{-1} \alpha_{ij} d = \alpha_{ij}$ minden $i = 1, \dots, r$, $j = r+1, \dots, k$, és $d \in D$ esetén. Speciálisan $\alpha_{ij} \in Z(D) = K$. Az (1) egyenletet y_i-re rendezve azt kapjuk, hogy $y_i = 1 \otimes u_i - \sum_{j=r+1}^{k} \alpha_{ij} \otimes u_j \in K \otimes_K L = L$ minden $i = 1, \dots, r$-re. Speciálisan J-nek van $J \cap L$-beli elemekből álló generátorrendszere. Viszont $J \cap L$ egy ideál L-ben, ezért $J \cap L = L$, hiszen L test. Azt kaptuk, hogy $L \subseteq J$, és így $D \otimes_K L = J$ (hiszen J ideál), azaz $D \otimes_K L$ egyszerű. □

2.4. Megjegyzés. A fenti állítás nemcsak véges, hanem tetszőleges $K \leq L$ algebrai bővítésre is igaz.

Bizonyítás. Az általánosabb állítás következik a fentiből, hiszen minden algebrai bővítés véges bővítések felszálló uniója: Valóban, ahhoz az irányhoz, hogy ha $A \otimes_K L$ centrális egyszerű L fölött, akkor A is az K fölött, nem használtuk, hogy L/K véges bővítés. Hasonlóképp annak igazolásához sem (vehetünk végtelen bázist is), hogy $Z(A \otimes_K L) = L$. Legyen tehát D egy centrális egyszerű ferdetest K fölött, $0 \neq J \lhd D \otimes_K L$ pedig egy nemtriviális ideál. Mivel $D \otimes_K L$ végesdimenziós L fölött, ezért J is, tehát vehetjük egy $x_1, \dots, x_k \in J$ véges bázisát. Viszont mivel $D \otimes_K L = \bigcup_{K \leq_{\text{véges}} L_1 \leq L} D \otimes_K L_1$, ezért van olyan L_1/K véges bővítés, hogy $x_1, \dots, x_k \in D \otimes_K L_1$. Viszont ekkor ezen elemek által kifeszített L_1-vektortér egy nemtriviális (tudjuk a dimenzióját L_1 fölött!) ideál lesz $D \otimes_K L_1$-ben, ami ellentmond a fenti tételnek. □

2.5. Tétel. *Legyen A egy végesdimenziós algebra a K test fölött. A pontosan akkor centrális egyszerű algebra K fölött, ha van olyan $K \leq L$ véges bővítés és $n \geq 1$ egész, melyre $A \otimes_K L \cong M_n(L)$.*

Bizonyítás. Ha van ilyen L bővítés, akkor A centrális egyszerű a 2.3. Állítás szerint. Megfordítva legyen A egy centrális egyszerű algebra K fölött. Ekkor a 2.4. Megjegyzés szerint $A \otimes_K \overline{K}$ egy centrális egyszerű algebra az algebrailag zárt $\overline{K}$ fölött, tehát $A \otimes_K \overline{K} \cong M_n(\overline{K})$ alkalmas $n \geq 1$ egésszel. Legyen $e_{ij} \in M_n(\overline{K})$ az a mátrix, melynek i-edik sorának j-edik eleme 1, az összes többi pedig 0 ($1 \leq i, j \leq n$). Mivel

$$A \otimes_K \overline{K} = \bigcup_{K \leq L \leq \overline{K} \text{ véges bővítés}} A \otimes_K L \ ,$$

van egy olyan $K \leq L$ véges bővítés, hogy $A \otimes_K L$-ben már az összes e_{ij} elemi mátrix benne van. Sőt, mivel ezen elemek L fölött lineárisan függetlenek és számuk $\dim_L(A \otimes_K L) = n^2$, ezért az e_{ij} elemek $A \otimes_K L$ egy L fölötti bázisát alkotják. Továbbá

$$e_{ij} e_{kl} = \begin{cases} 0 & \text{ha } j \neq k \\ e_{il} & \text{ha } j = k \end{cases}$$

nyilván teljesül $M_n(\overline{K})$-ban (és így $A \otimes_K L$-ben is), ezért ez a bázis megad egy izomorfizmust $A \otimes_K L$ és $M_n(L)$ között. □

2.6. Definíció. Ha A egy centrális egyszerű algebra és $K \leq L$ egy olyan véges bővítés, melyre $A \otimes_K L \cong M_n(L)$, akkor L-et az A egy *felbontási testének* (splitting field) nevezzük. Továbbá azt mondjuk, hogy a $K \leq L$ bővítés *felhasítja* (splits) A-t. Ha $A \cong M_n(K)$, akkor azt mondjuk, hogy A *hasad* (K fölött).

A felbontási test nem egyértelmű: általában nincs olyan „legszűkebb” test, ami felhasítja az adott A centrális egyszerű algebrát:

2.7. Példa. Tekintsük a K fölötti $K(a,b)$ kvaternióalgebrát ($\mathrm{char}(K) \neq 2$), ahol $a, b \in K$ 0-tól különböző testelemek. Ez egy 4-dimenziós centrális egyszerű K-algebra, melynek bázisa $1, i, j, k$, amikre $i^2 = a$, $j^2 = b$, és $ij = -ji = k$ teljesül. Ekkor $K(a,b)$ hasad a $K(\sqrt{a})$, a $K(\sqrt{b})$, és a $K(\sqrt{-ab})$ testek mindegyike fölött. Amennyiben $K(a,b)$ nem hasad még K fölött (azaz egy ferdetest), akkor ezen másodfokú bővítések mindegyike részteste $K(a,b)$-nek: rendre a $K(i)$, $K(j)$, ill. $K(k)$ résztestek ezen kvadratikus bővítésekkel izomorfak, hiszen $i^2 = a$, $j^2 = b$, és $k^2 = -ab$.

2.8. Gyakorlat. *Legyen A egy centrális egyszerű algebra a K test fölött, ami felhasad a (véges) $K \leq L$ bővítés fölött, továbbá $L \leq F$ egy véges bővítés. Mutassuk meg, hogy A hasad F fölött is.*

2.9. Következmény. *Ha A egy centrális egyszerű algebra K fölött, akkor dimenziója egy egész szám négyzete.*

Bizonyítás. $\dim_K A = \dim_L (A \otimes_K L) = \dim_L M_n(L) = n^2$. □

2.10. Definíció. Az $n := \sqrt{\dim_K A}$ egész számot az A centrális egyszerű algebra *fokának* nevezzük.

2.11. Következmény. *Legyenek A és B centrális egyszerű algebrák K fölött. Ekkor $A \otimes_K B$ is egy centrális egyszerű algebra K fölött.*

Bizonyítás. A 2.5. Tétel miatt elegendő azt ellenőriznünk, hogy van olyan $K \leq L$ véges bővítés, melyre $(A \otimes_K B) \otimes_K L$ egy L fölötti teljes mátrixgyűrűvel izomorf. Node A és B is felhasad egy alkalmas véges bővítés fölött, ezért ha L mindkettőnek tartalmazza egy felbontási testét, akkor egyszerre hasítja A-t is és B-t is, azaz $A \otimes_K L \cong M_n(L)$ és $B \otimes_K L \cong M_m(L)$ alkalmas $n, m \geq 1$ egészekkel. Tekintsük az

$$\begin{aligned} (A \otimes_K B) \otimes_K L &\to (A \otimes_K L) \otimes_L (B \otimes_K L) \\ (a \otimes b) \otimes \lambda &\mapsto (a \otimes \lambda) \otimes (b \otimes 1) = (a \otimes 1) \otimes (b \otimes \lambda) \end{aligned}$$

leképezést (a jobb oldali egyenlőség azért áll fenn, mert itt L fölött tenzorszorzunk, ezért $\lambda \in L$ átvihető a túloldalra). Könnyű számolás mutatja, hogy ez szorzattartó és L-lineáris (utóbbi definíció szerint teljesül, mert a fenti elemi tenzorokon megadott leképezést L-lineárisan terjesztjük ki), és szürjektív. Mivel a két oldal dimenziója megegyezik (n^2m^2), ezért ez egy izomorfizmus a két L-algebra között. Viszont a jobb oldal izomorf $M_n(L) \otimes M_m(L) \cong M_{nm}(L)$-lel is (2.1. Lemma), tehát $A \otimes_K B$ egy centrális egyszerű K-algebra. □

Vegyük észre, hogy ha A egy centrális egyszerű K-algebra, akkor A^{op} is az: ugyanaz a testbővítés fogja felhasítani.

2.12. Állítás. *Legyen A egy n-edfokú centrális egyszerű K-algebra. Ekkor $A \otimes_K A^{op} \cong M_{n^2}(K)$, azaz $A \otimes A^{op}$ hasad.*

Bizonyítás. Tekintsük a

$$\begin{aligned} \Phi\colon A \otimes_K A^{op} &\to \mathrm{End}_K(A) \\ a \otimes b &\mapsto (x \mapsto axb) \end{aligned} \tag{2}$$

K-lineáris leképezést. Vegyük észre, hogy ez szorzattartó is (a jobb oldalon a kompozíció a szorzás), hiszen ha $a_1, a_2, b_1, b_2 \in A$, akkor $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1a_2) \otimes (b_2b_1)$, melynek képe x-et $(a_1a_2)x(b_2b_1) = a_1(a_2xb_2)b_1$-be küldi, ez pedig épp az $a_1 \otimes b_1$ és $a_2 \otimes b_2$ képének kompozíciója. Tehát Φ egy K-algebra homomorfizmus két azonosdimenziós (n^4) algebra között. Φ nyilván nem azonosan 0 (hiszen az $1 \otimes 1$ egységelemet az identitásba viszi), ezért izomorfizmus, mert $A \otimes_K A^{op}$ egyszerű a 2.11. Következmény szerint. Viszont $\dim_K A = n^2$, ezért $\mathrm{End}_K(A) \cong M_{n^2}(K)$, hiszen $\mathrm{End}_K(A)$ elemei nem mások, mint az $A \to A$ K-lineáris leképezések. □

Következő célunk a 2.7. Példa általánosítása magasabbfokú centrális egyszerű algebrákra, azaz olyan $K \leq L$ bővítést szeretnénk találni, ami résztest A-ban és A-t felhasítja. Akövetkező állítás szerint ha találunk elég nagy résztestet A-ban, az már valóban fel fogja hasítani.

2.13. Állítás. *Legyen A egy n-edfokú centrális egyszerű K-algebra és tegyük föl, hogy $L \leq A$ egy résztest, mely K-nak n-edfokú bővítése. Ekkor A hasad L fölött.*

Bizonyítás. Legyen A^{op} az oppozit algebra. Ha L egy ilyen bővítés, akkor mivel L kommutatív, ezért L ebben is részgyűrű. Tehát $A \otimes_K L \subset A \otimes_K A^{op} \cong \mathrm{End}_K(A)$ (2.12. Állítás). Vegyük észre, hogy A vektortér L fölött is (kétféleképpen is: a bal-, ill. a jobbszorzással), és $\dim_L A = n$, hiszen $\dim_K L = n$ és $\dim_K A = n^2$. Ha A-ra a jobbszorzáson keresztül tekintünk, mint L-vektortérre, akkor $A \otimes_K L$ elemeinek Φ-szerinti képe a (2) leképezésnél L-lineárisak: Valóban, ha $\lambda, \mu \in L$ és $a, x \in A$, akkor $\Phi(a \otimes \lambda)(x\mu) = ax\mu\lambda = ax\lambda\mu = \Phi(a \otimes \lambda)(x)\mu$, azaz $\Phi(a \otimes \lambda)$ egy L-lineáris leképezés. Tehát $\Phi(A \otimes_K L) \subseteq \mathrm{End}_L(A) \subset \mathrm{End}_K(A)$. Viszont $\dim_L \mathrm{End}_L(A) = n^2$, tehát Φ egy izomorfizmust indukál $A \otimes_K L$ és $\mathrm{End}_L(A) \cong M_n(L)$ között, azaz A hasad L fölött. □

Az A-beli résztestek keresésének esetében Wedderburn tétele miatt elegendő az $A = D$ (ferdetest) esettel foglalkoznunk. Továbbá Wedderburn másik, véges ferdetestek nemlétezéséről szóló tétele miatt azt is feltehetjük, hogy K végtelen.

2.14. Tétel. *Legyen D egy centrális n-edfokú ferdetest a K* végtelen *test fölött. Ekkor D-nek létezik olyan $L \leq D$ részteste, mely K-nak n-edfokú szeparábilis bővítése. Ekkor $D \otimes_K L \cong M_n(L)$.*

Bizonyítás. Egy olyan $\alpha \in D$ elemet szeretnénk találni, melynek K fölötti $m_\alpha(x)$ minimálpolinomja n-edfokú, és nincs többszörös gyöke. Ekkor $m_\alpha(x)$ irreducibilis, hiszen D nullosztómentes, tehát $L := K(\alpha) \leq D$ megfelel. Valójában azt fogjuk belátni, hogy bizonyos értelemben D szinte minden eleme megfelel: Zariski-nyílt halmazt alkotnak azon $\alpha \in D$ elemek, melyek minimálpolinomja n-edfokú. Ehhez szükségünk lesz az alábbi, önmagában is érdekes lemmára.

2.15. Lemma. *Legyen $\beta \in D$ tetszőleges, és jelöljük $m_\beta(x) \in K[x]$-szel a minimálpolinomját D-ben. A $\beta \otimes 1 \in A \otimes_K \overline{K} \cong M_n(\overline{K})$ mátrix minimálpolinomja szintén $m_\beta(x)$. Speciálisan $m_\beta(x)$ legfeljebb n-edfokú.*

Bizonyítás. Az világos, hogy $m_\beta(\beta \otimes 1) = m_\beta(\beta) \otimes 1 = 0 \otimes 1 = 0$. A nehézséget annak igazolása okozza, hogy $\beta \otimes 1$ nem gyöke egy alacsonyabb fokú $\overline{K}$-beli együtthatós polinomnak. Ennek igazolásához tekintsük a β-val való

$$\begin{aligned} s_\beta \colon D &\to D \\ \gamma &\mapsto \beta\gamma \end{aligned}$$

balszorzást, mint K-lineáris leképezést (az n^2-dimenziós D vektortéren). Ha $f(x) \in K[x]$ egy tetszőleges polinom, akkor $f(s_\beta)$ épp az $f(\beta)$-val való szorzás. Speciálisan az s_β lineáris leképezés minimálpolinomja szintén $m_\beta(x)$. Lineáris algebrából tudjuk, hogy a lineáris leképezés minimálpolinomja megegyezik a – tetszőleges bázisban felírt – mátrixának a minimálpolinomjával, mely jelen esetben egy $n^2 \times n^2$-es K-beli együtthatós M mátrix. Node M minimálpolinomja ugyanaz akkor is, ha M-et egy $\overline{K}$-beli együtthatós mátrixnak tekintjük. Utóbbi pedig megegyezik a $\beta \otimes 1$-gyel való szorzás, mint $s_{\beta\otimes 1} \colon A \otimes_K \overline{K} \to A \otimes_K \overline{K}$ lineáris leképezés mátrixával. Viszont a fenti érveléshez hasonlóan $\beta \otimes 1 \in M_n(\overline{K})$ minimálpolinomja megegyezik $s_{\beta\otimes 1}$ minimálpolinomjával, ami pedig $m_\beta(x) \in K[x]$. A Cayley-Hamilton tétel szerint $n \times n$-es mátrixok minimálpolinomja viszont legfeljebb n-edfokú. □

Vegyük D-nek egy $e_1, \dots, e_{n^2}$ bázisát K fölött és keressük α-t $\alpha = \sum_{j=1}^{n^2} y_j e_j$ alakban, ahol $y_j \in K$. Ekkor $\alpha \otimes 1 = \sum_{j=1}^{n^2} y_j (e_j \otimes 1)$ elemnek az $M_\alpha = \sum_{j=1}^{n^2} y_j M_j \in M_n(\overline{K})$ mátrix felel, ahol $M_1, \dots, M_{n^2} \in M_n(\overline{K})$ adott mátrixok úgy, hogy $e_j \otimes 1$-nek az $A \otimes_K \overline{K} \cong M_n(\overline{K})$ azonosításnál M_j felel meg ($j = 1, \dots, n^2$). Ha az $y_1, \dots, y_{n^2}$ számokat sikerül úgy választani, hogy M_α karakterisztikus polinomjának ne legyen többszörös gyöke, akkor szükségképpen ez a minimálpolinom is, hiszen annak is gyöke az összes sajátérték. Ez esetben $m_\alpha(x)$ n-edfokú és nincs többszörös gyöke. Tekintsük tehát az

$$F(x, z_1, \dots, z_{n^2}) := \det\left(xI - \sum_{j=1}^{n^2} z_j M_j\right) \in \overline{K}[x, z_1, \dots, z_{n^2}]$$

n^2+1-változós polinomot. Ennek x-szerinti diszkriminánsa egy $R(F, \frac{\partial F}{\partial x}) =: H(z_1, \dots, z_{n^2}) \in \overline{K}[z_1, \dots, z_{n^2}]$ polinom, ami ha egy adott $z_j \mapsto y_j \in K$ ($j = 1, \dots, n^2$) behelyettesítésre $H(y_1, \dots, y_{n^2}) \neq 0$, akkor az $F(x, y_1, \dots, y_{n^2}) = \det(xI - M_\alpha)$ karakterisztikus polinomnak nincs többszörös gyöke, tehát α megfelel. Viszont H nem lehet az azonosan 0 polinom, hiszen $\overline{K}$ végtelen test, ezért *van olyan* $M_n(\overline{K})$-beli mátrix, aminek n különböző sajátértéke van, azaz a z_j-knek létezik $u_j \in \overline{K}$-beli behelyettesítése, melyekre $H(u_1, \dots, u_{n^2}) \neq 0$. Végezetül K végtelen test, ezért van olyan K-beli behelyettesítés is, ami nem 0: ennek változószám szerinti indukcióval való igazolását az olvasóra bízzuk. □

2.16. Következmény. *Ha A egy centrális egyszerű algebra egy K test fölött, akkor K-nak létezik olyan $K \leq L$ véges* Galois-*bővítése, mely fölött A hasad.*

Bizonyítás. Minden véges szeparábilis bővítés benne van egy Galois-bővítésben. □

2.17. Megjegyzés. (a) Legyen $K \leq L$ egy Galois bővítés $G := \mathrm{Gal}(L/K)$ Galois-csoporttal és A egy K fölötti nemhasadó centrális egyszerű algebra, mely L fölött már hasad. Ekkor az $A \otimes_K L \cong M_n(L)$ izomorfizmus *nem* Galois-ekvivariáns! G hat ugyanis mindkét oldalon: az $n \times n$-es L-beli együtthatós mátrixokon együtthatónként, a bal oldalon pedig a második tényezőn keresztül: ha $g \in G$ és $a \otimes \lambda \in L$ egy elemi tenzor, akkor $g(a \otimes \lambda) := a \otimes g(\lambda)$. Ugyanis ha az azonosítás G-ekvivariáns lenne, akkor a G-hatás fixpontjai között is kapnánk egy izomorfizmust. Node a bal oldalon a G-hatás fixpontjai $A \otimes_K K \cong A$ elemei, a jobb oldalon pedig $M_n(K)$, ezek pedig nem izomorfak, hiszen A nem hasad. Erre az észrevételre még szükségünk lesz a későbbiekben.

(b) Az nem igaz általában, hogy a véges Galois-bővítés is választható úgy, hogy D tartalmazza. Erre Amitsur adott először ellenpéldát.

3. A Brauer-csoport

Az alábbiakban célunk a centrális egyszerű algebrák ekvivalencia-osztályain egy csoportstruktúra értelmezése. A csoportművelet a 2.11. Következmény fényében a K fölötti *tenzorszorzás* lesz. A tenzorszorzás egy asszociatív művelet: $(A \otimes_K B) \otimes_K C \cong A \otimes_K (B \otimes_K C)$, ha A, B, C K-algebrák. Sőt, az alaptesttel való tenzorszorzás nem változtatja meg az adott algebra izomorfiosztályát: $A \otimes_K K \cong A$, tehát K egy egységelem. Továbbá az

$$\begin{aligned} A \otimes_K B &\to B \otimes_K A \\ a \otimes b &\mapsto b \otimes a \end{aligned}$$

leképezés egy izomorfizmus tetszőleges A, B K-algebrák esetén. Viszont mivel a dimenzió összeszorzódik tenzorszorzásnál, ezért az inverz létezéséhez szükségünk van egy, az izomorfiánál durvább ekvivalencia-relációra a centrális egyszerű algebrák osztályán.

3.1. Definíció. Ha A és B centrális egyszerű algebrák a K test fölött, akkor azt mondjuk, hogy A és B *Brauer-ekvivalens* (jel.: $A \sim B$), ha van olyan D ferdetest K fölött és $n, m \geq 1$ egész számok, melyekre $A \cong M_n(D)$ és $B \cong M_m(D)$. Egy adott A centrális egyszerű algebra Brauer-osztályát $[A]$-val jelöljük.

Az 1.11. Következmény szerint minden Brauer-ekvivalencia osztályban izomorfia erejéig pontosan egy ferdetest van.

3.2. Lemma. *Legyen A és B centrális egyszerű algebra K fölött. Ekkor $A \sim B$ pontosan akkor, ha van olyan $k, k' \geq 1$ egész szám, melyre $A \otimes_K M_k(K) \cong B \otimes_K M_{k'}(K)$.*

Bizonyítás. Vegyük észre, hogy $A \otimes_K M_k(K) \cong M_k(A) \cong M_k(M_n(D)) \cong M_{kn}(D)$, tehát a lemmában szereplő feltétel ekvivalens azzal, hogy A és B ugyanazon ferdetest feletti teljes mátrixgyűrűk. □

3.3. Állítás. *Adott K test esetén a K feletti centrális egyszerű algebrák Brauer-ekvivalncia osztályai Abel-csoportot alkotnak $[A][B] := [A \otimes_K B]$ műveletre nézve. Az egységelem $[K]$, $[A]$ inverze pedig $[A^{op}]$. Azon centrális egyszerű algebrák osztályai, melyek egy adott $K \leq L$ (véges) bővítés fölött hasadnak, részcsoportot alkotnak.*

3.4. Definíció. Az így kapott csoportot K Brauer-csoportjának nevezzük és $\mathrm{Br}(K)$-val jelöljük. Az adott L bővítés fölött hasadó centrális egyszerű algebrák Brauer-osztályainak részcsoportját $\mathrm{Br}(L|K)$-val jelöljük, és a K test L-hez relatív Brauer-csoportjának hívjuk.

Bizonyítás. A művelet jóldefiniáltságához azt kell igazolni, hogy ha $A \sim A'$ és $B \sim B'$ centrális egyszerű algebrák, akkor $A \otimes_K B \sim A' \otimes_K B'$. Legyen tehát $A \cong M_n(D)$, $A' \cong M_{n'}(D)$, $B \cong M_m(E)$, $B' \cong M_{m'}(E)$ valamely D, E ferdetestekre. Ekkor Wedderburn tétele szerint

$$A \otimes_K B \cong M_{nm}(D \otimes_K E) \sim D \otimes_K E \sim M_{n'm'}(D \otimes_K E) \cong A' \otimes_K B' \ .$$

$[A]$ inverze valóban $[A^{op}]$ a 2.12. Állítás szerint. A 2.11 Következmény bizonyítása szerint ha A és B is hasad L fölött, akkor $A \otimes_K B$ is, tehát $\mathrm{Br}(L|K)$ részcsoport $\mathrm{Br}(K)$-ban. □

3.5. Megjegyzés. Egy A centrális egyszerű algebra Brauer-osztálya pontosan akkor triviális (azaz az egységelem $\mathrm{Br}(K)$-ban), ha A hasad K fölött.

3.6. Példa. (*a*) Az $\mathbb{R}$ fölötti nullosztómentes algebrákról szóló Frobenius-tétel szerint $\mathrm{Br}(\mathbb{R}) \cong Z_2$ a kételemű csoport.

(*b*) Ha $\mathbb{F}_q$ egy véges test ($q = p^f$ prímhatvány), akkor Wedderburn véges ferdetestek kommutativitásáról szóló tétele szerint $\mathrm{Br}(\mathbb{F}_q) = \{1\}$ triviális.

A következő célunk a Brauer-csoport mélyebb megértése a Galois-elméleten keresztül. Ehhez legelőször szükségünk lesz az alábbi – lényegében lineáris algebrai, de egyáltalán nem triviális – lemmára.

3.7. Lemma. *Az $M_n(K)$ mátrixgyűrű minden K-lineáris automorfizmusa belső, azaz ha $\varphi\colon M_n(K) \to M_n(K)$ egy K-lineáris automorfizmus, akkor van olyan $P \in \mathrm{GL}_n(K)$ invertálható mátrix, melyre $\varphi(M) = PMP^{-1}$ minden $M \in M_n(K)$-ra. Speciálisan $\mathrm{Aut}_K(M_n(K)) \cong \mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$.*

Bizonyítás. Vegyünk egy $X \in M_n(K)$ mátrixot, melynek sorvektorai $x_1, \ldots, x_n$. Ekkor az $M_n(K)X$ balideál pontosan azon mátrixokból áll, melyeknek minden sora $x_1, \ldots, x_n$ lineáris kombinációja. Speciálisan ha X rangja r, akkor $M_n(K)X$ egy nr-dimenziós vektortér K fölött. Ha most $\varphi \in \mathrm{Aut}_K(M_n(K))$ egy automorfizmus, akkor $\dim_K(M_n(K)X) = \dim_K \varphi(M_n(K)X) = \dim_K M_n(K)\varphi(X)$. Speciálisan φ megtartja a mátrixok rangját.

Tehát ha $E_{ij} \in M_n(K)$ az a mátrix, melynek minden eleme 0, az i-edik sor j-edik eleme, ami 1-es ($1 \leq i, j \leq n$), akkor $\varphi(E_{11})$ egy 1-rangú mátrix, melyre $\varphi(E_{11})^2 = \varphi(E_{11}^2) = \varphi(E_{11})$ (azaz idempotens).

Ezért van két olyan $C, C' \in K^n$ oszlopvektor, melyekre $\varphi(E_{11}) = CC'^T$ (diádszorzat) és $C'^T C = 1$ (skaláris szorzat). Legyen $C_j := \varphi(E_{j1})C$ és P az a mátrix, melynek j-edik oszlopa C_j $(j = 1, \dots, n)$. Ekkor $C_1 = CC'^T C = C \cdot 1 = C$.

Belátjuk, hogy a C_j vektorok lineárisan függetlenek: tegyük fel ugyanis, hogy $\sum_{j=1}^n \lambda_j C_j = 0$. Ekkor

$$0 \neq \varphi(\sum_{j=1}^n \lambda_j E_{j1}) = \sum_{j=1}^n \lambda_j \varphi(E_{j1}E_{11}) = \sum_{j=1}^n \lambda_j \varphi(E_{j1})\varphi(E_{11}) =$$
$$= \sum_{j=1}^n \lambda_j \varphi(E_{j1})CC'^T = \left(\sum_{j=1}^n \lambda_j C_j\right) C'^T = 0 \ ,$$

ellentmondás. Tehát a P mátrix invertálható.

Végezetül tetszőleges $1 \leq k, l \leq n$ esetén

$$\varphi(E_{kl})C_j = \varphi(E_{kl})\varphi(E_{j1})C = \varphi(E_{kl}E_{j1})C = \begin{cases} 0 & \text{ha } l \neq j \\ \varphi(E_{k1})C = C_k & \text{ha } l = j \ . \end{cases}$$

Ez azt jelenti, hogy a $\varphi(E_{kl})P$ egy olyan mátrix, melynek l-edik oszlopa C_k, az összes többi pedig 0. Ez pont a PE_{kl} mátrix, azaz $\varphi(E_{kl})P = PE_{kl}$ minden $k, l \in \{1, \dots, n\}$-re. Lineáris kombinációt véve $\varphi(X)P = PX$ minden $X \in M_n(K)$ mátrixra teljesül, azaz $\varphi(X) = PXP^{-1}$, hiszen P invertálható.

Tehát a

$$\begin{array}{rcl} \mathrm{GL}_n(K) & \to & \mathrm{Aut}_K(M_n(K)) \\ P & \mapsto & (X \mapsto PXP^{-1}) \end{array}$$

egy szürjektív csoporthomomorfizmus, melynek magja azon P mátrixokból áll, melyek minden $X \in M_n(K)$ mátrixszal felcserélhetők. Ezek pont a skalármátrixok, azaz $\mathrm{GL}_n(K)$ centruma. A második állítás a homomorfizmus-tételből következik. □

Vegyünk egy A centrális egyszerű algebrát K fölött. Ekkor a 2.16. Következmény szerint van egy olyan véges Galois $K \leq L$ bővítés, melyre létezik egy $f\colon M_n(L) \xrightarrow{\sim} A \otimes_K L$ izomorfizmus. A $G := \mathrm{Gal}(L/K)$ Galois csoport hat mindkét oldalon, de másképp. Hogy a két hatás eltérését megértsük, definiáljuk az

$$f_A\colon G \to \mathrm{Aut}_L(M_n(L)) \cong \mathrm{PGL}_n(L)$$

függvényt a következőképpen: Ha van egy $g \in G$ elemünk, akkor megnézhetjük, mennyiben tér el a g-hatás a két oldalon: az

$$f_A(g) := f^{-1} \circ (\mathrm{id} \otimes g) \circ f \circ g^{-1}\colon M_n(L) \xrightarrow{g^{-1}} M_n(L) \xrightarrow{f} A \otimes_K L \xrightarrow{\mathrm{id}\otimes g} A \otimes_K L \xrightarrow{f^{-1}} M_n(L)$$

izomorfizmus már L-lineáris lesz, azaz egy automorfizmusát adja $M_n(L)$-nek. Valóban, ha $X \in M_n(L)$ egy mátrix, $\lambda \in L$ pedig egy skalár, akkor

$$f_A(g)(X\lambda) = f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(X\lambda)))) =$$
$$= f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(X)g^{-1}(\lambda)))) = f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(X))g^{-1}(\lambda)))) =$$
$$= f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(X)))\lambda) = f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(X))))\lambda = f_A(g)(X)\lambda \ .$$

Általában f_A nem lesz csoporthomomorfizmus. Vizsgáljuk meg, hogy viselkedik f_A a G-beli szorzásra nézve! Legyen $g, h \in G$ és tegyük fel, hogy $f_A(g)$ (ill. $f_A(h)$) a P (ill. Q) mátrixszal való konjugálás.

$$f_A(gh)(X) = f^{-1}(\mathrm{id} \otimes g(\mathrm{id} \otimes h(f(h^{-1}g^{-1}(X))))) = f^{-1}(\mathrm{id} \otimes g(f(\underbrace{f^{-1}(\mathrm{id} \otimes h(f(h^{-1}}_{f_A(h)} g^{-1}(X)))))))) =$$

$$= f^{-1}(\mathrm{id} \otimes g(f(Q(g^{-1}(X))Q^{-1}))) = \underbrace{f^{-1}(\mathrm{id} \otimes g(f(g^{-1}}_{f_A(g)}(g(Q)Xg(Q)^{-1})))) = Pg(Q)Xg(Q)^{-1}P^{-1} \ .$$

Azt kaptuk, hogy

$$f_A(gh) = f_A(g)g(f_A(h)) \ .$$

Ennek fényében tesszük a következő definíciót.

3.8. Definíció. Tegyük fel, hogy a G csoport automorfizmusokkal hat a H csoporton, azaz adott egy $\alpha\colon G \to \mathrm{Aut}(H)$ csoporthomomorfizmus. Ekkor egy $\psi\colon G \to H$ függvényt *keresztezett homomorfizmusnak* nevezünk, ha $\psi(gh) = \psi(g)\alpha(g)(\psi(h))$ teljesül minden $g, h \in G$-re. Ha az α csoporthomomorfizmus magától értetődik, akkor elhagyjuk a jelölésből, azaz $g \in G$ hatását egy $h \in H$ elemen egyszerűen $g(h)$-val jelöljük.

3.9. Példa. A konstans 1 függvény, ami G minden eleméhez H egységelemét rendeli tetszőleges csoporthatás esetén keresztezett homomorfizmus. Ezt nevezzük a *triviális keresztezett homomorfizmusnak.*

3.10. Gyakorlat. *Igazoljuk, hogy ha G triviálisan hat H-n, akkor a $G \to H$ keresztezett homomorfizmusok nem mások, mint a $G \to H$ csoporthomomorfizmusok.*

A mi példánkban a $G = \mathrm{Gal}(L/K)$ Galois-csoport hat a $H = \mathrm{PGL}_n(L)$ csoporton automorfizmusokkal: valóban, ha $g \in G$ és $P \in \mathrm{GL}_n(L)$, akkor g (mint az L test automorfizmusa) hat a P mátrix összes elemén. Továbbá $g(P)$ osztálya a $\mathrm{PGL}_n(L)$ faktorcsoportban csak P osztályától függ, hiszen skalármátrix Galois-konjugáltja is skalármátrix.

A következőkben azt vizsgáljuk meg, mennyire egyértelműen határozza meg az A centrális egyszerű algebra (és az L test, mely fölött A hasad) az $f_A\colon \mathrm{Gal}(L/K) \to \mathrm{PGL}_n(L)$ keresztezett homomorfizmust. A fenti konstrukcióban egyetlen ponton van szabad választásunk: az f izomorfizmus $A \otimes_K L$ és $M_n(L)$ között nincs egyértelműen meghatározva. Vegyük észre ugyanakkor, hogy ha f' egy másik izomorfizmus, akkor $f^{-1} \circ f'$ egy automorfizmusa $M_n(L)$-nek. A 3.7. Állítás szerint tehát $f^{-1} \circ f'$ egy alkalmas $P \in \mathrm{GL}_n(L)$ mátrixszal való konjugálás. Ha ehhez az azonosításhoz az f'_A kersztezett homomorfizmus tartozik, akkor tehát $g \in \mathrm{Gal}(L/K)$ és $X \in M_n(L)$ esetén

$$f'_A(g)(X) = P^{-1}f^{-1}(\mathrm{id} \otimes g(f(Pg^{-1}(X)P^{-1})))P =$$
$$= P^{-1}f^{-1}(\mathrm{id} \otimes g(f(g^{-1}(g(P)Xg(P)^{-1}))))P = P^{-1}f_A(g)(g(P)Xg(P)^{-1})P$$

Tehát $f'_A(g) = \overline{P}^{-1} f_A(g) g(\overline{P})$, ahol $\overline{P}$ jelöli P osztályát $\mathrm{PGL}_n(L)$-ben.

3.11. Definíció. Tegyük fel, hogy a G csoport automorfizmusokkal hat a H csoporton. A $\varphi, \psi\colon G \to H$ keresztezett homomorfizmusokat ekvivalensnek mondjuk (jel.: $\varphi \sim \psi$), ha van olyan $h \in H$ elem, melyre $\varphi(g) = h^{-1}\psi(g)g(h)$ minden $g \in G$-re teljesül. A keresztezett homomorfizmusok ekvivalenciaosztályait a G *csoport H együtthatós első kohomológiahalmazának* nevezzük és $H^1(G, H)$-val jelöljük. Ez egy pontozott halmaz: a triviális keresztezett homomorfizmus osztálya a kitüntetett elem.

3.12. Megjegyzés. A fenti $\sim$ reláció valóban ekvivalenciareláció: (i) $\varphi \sim \varphi$, hiszen $h = 1$ megfelel; (ii) $\varphi \sim \psi$ esetén $\psi \sim \varphi$: a fordított irányú ekvivalenciát $h^{-1} \in H$ mutatja, hiszen $\varphi(g) = h^{-1}\psi(g)g(h)$ esetén $\psi(g) = h\varphi(g)g(h)^{-1} = (h^{-1})^{-1}\varphi(g)g(h^{-1})$; (iii) $\chi \sim \varphi$ és $\varphi \sim \psi$ esetén pedig van olyan $h_1, h_2 \in H$, melyre $\chi(g) = h_1^{-1}\varphi(g)g(h_1) = h_1^{-1}h_2^{-1}\psi(g)g(h_2)g(h_1) = (h_2h_1)^{-1}\psi(g)g(h_2h_1)$, azaz $\chi \sim \psi$.

3.13. Gyakorlat. *Tegyük fel, hogy H* kommutatív *(és a műveletet additívan írjuk). Ekkor a $G \to H$ keresztezett homomorfizmusok egy $Z(G, H)$ csoportot alkotnak a pontonkénti szorzásra nézve. Ebben az esetben $H^1(G, H) = Z(G, H)/B(G, H)$ is Abel-csoport, ahol $B(G, H) = \{f \in Z(G, H) \mid \exists h \in H\colon f(g) = g(h) - h \ \forall g \in G\}$ a* principális keresztezett homomorfizmusok *részcsoportja.*

Tehát ha H kommutatív, akkor első *kohomológiacsoportról* beszélhetünk. A legtöbb alkalmazásban valóban ez a helyzet, ezért a kommutatív csoportkohomológiának kiterjedt elmélete van, melyet a

csoportelméleten kívül az algebrai topológiában, algebrai geometriában, és az algebrai számelméletben is használnak. Kommutatív együtthatók esetén léteznek magasabb $H^i(G,H)$ kohomológiacsoportok is ($i \geq 0$ egész): ezek a nulladik $H^0(G,H) := H^G = \{h \in H \mid g(h) = h \forall g \in G\}$ kohomológiacsoport (mint H függvényének) *derivált funktorai.* Ezek kétségkívül legfontosabb tulajdonsága az ún. *hosszú egzakt sorozat* létezése: Legyenek A, B, C Abel-csoportok, melyeken a G (nem feltétlen kommutatív) csoport hat automorfizmusokkal, és tegyük fel, hogy létezik egy

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

rövid egzakt sorozat, melynek leképezései *G-ekvivariánsak*, azaz ha $a \in A$, $b \in B$, $g \in G$ tetszőleges, akkor $\alpha(g(a)) = g(\alpha(a))$, illetve $\beta(g(b)) = g(\beta(b))$. Másszóval az α és a β megőrzi a G-hatást. Ekkor létezik egy

$$\begin{aligned} 0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to \cdots \qquad (3) \\ \cdots \to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \to H^{i+1}(G,A) \to H^{i+1}(G,B) \to H^{i+1}(G,C) \to \cdots \end{aligned}$$

(hosszú) egzakt sorozat, melyben a leképezéseket α és β indukálja.

3.14. Feladat. *Igazoljuk a* (3) *sorozat egzaktságát a tanult részig ($H^1(G,C)$-ig).*

3.15. Tétel. *Legyen $K \leq L$ egy véges Galois-bővítés $G := \mathrm{Gal}(L/K)$ Galois-csoporttal. A fenti $[A] \mapsto [f_A] \in H^1(G, \mathrm{PGL}_n(L))$ hozzárendelés egy bijekciót indukál az n-edfokú L fölött hasadó centrális egyszerű K-algebrák izomorfiaosztályainak $CSA_L(n)$ halmaza és $H^1(G, \mathrm{PGL}_n(L))$ között. Ennél a bijekciónál $[M_n(K)]$-nak a triviális keresztezett homomorfizmus osztálya felel meg.*

Bizonyítás. Jóldefiniáltság: Azt láttuk a fentiekben, hogy az

$$\begin{array}{rcl} CSA_L(n) & \to & \mathrm{PGL}_n(L) \\ [A] & \mapsto & [f_A] \end{array}$$

hozzárendelés jóldefiniált, hiszen ha $A \cong A'$ izomorf n-edfokú centrális egyszerű K-algebrák (melyek L fölött hasadnak), akkor az f_A és $f_{A'}$ keresztezett homomorfizmusok ekvivalensek, tehát ugyanaz az osztályuk $H^1(G, \mathrm{PGL}_n(L))$-ben. Így ahhoz, hogy belássuk, hogy ez egy bijekció, meg kell adnunk az inverzét.

Csavart hatás megadása: Vegyünk tehát egy $f\colon G \to \mathrm{PGL}_n(L)$ keresztezett homomorfizmust. Definiáljuk G-nek egy f-fel csavart – K-lineáris – hatását az $M_n(L)$ gyűrűn (azaz egy $\beta\colon G \to \mathrm{Aut}_K(M_n(L))$ csoporthomomorfizmust) a következőképpen:

$$\beta(g)(X) := f(g)(g(X)) \ ,$$

ahol $g \in G$ és $X \in M_n(L)$. Az világos, hogy rögzített $g \in G$-re a $\beta(g)$ egy K-lineáris automorfizmusa $M_n(L)$-nek, hiszen két K-lineáris automorfizmus kompozíciója: az eredeti Galois-hatásé és az $f(g) \in \mathrm{PGL}_n(L) \cong \mathrm{Aut}_L(M_n(L)) \subseteq \mathrm{Aut}_K(M_n(L))$ automorfizmusé. Azt kell még megvizsgálnunk, hogy β hogy viselkedik a G-beli szorzásra nézve:

$$\begin{aligned} \beta(g_1g_2)(X) := f(g_1g_2)(g_1g_2(X)) = f(g_1)g_1(f(g_2))(g_1g_2(X)) = \\ = f(g_1)g_1(f(g_2)(g_2(X))) = \beta(g_1)(\beta(g_2)(X)) \ , \end{aligned}$$

azaz $\beta(g_1g_2) = \beta(g_1) \circ \beta(g_2)$ tetszőleges $g_1, g_2 \in G$ esetén. Tehát β valóban egy $G \to \mathrm{Aut}_K(M_n(L))$ csoporthomomorfizmus.

Az f-hez tartozó centrális egyszerű algebra konstrukciója: Definiáljuk az A_f K-algebrát, mint az f-fel csavart Galois-hatás fixpontjainak a

$$A_f := M_n(L)^{\beta(G)} := \{X \in M_n(L) \mid \beta(g)(X) = X \text{ minden } g \in G\text{-re}\}$$

halmazát. A_f egy részgyűrű $M_n(L)$-ben, hiszen $X_1, X_2 \in A_f$ esetén nyilván $X_1 \pm X_2$ és X_1X_2 is A_f-ben van, hiszen $\beta(g)$ megtartja a gyűrűműveleteket minden $g \in G$-re. Sőt, ha $\lambda \in L \subset M_n(L)$ egy skalármátrix, akkor $\beta(g)(\lambda) = g(\lambda)$, hiszen az $f(g)$ L-lineáris automorfizmus triviálisan hat a skalármátrixokon (skalármátrix felcserélhető tetszőleges $\mathrm{GL}_n(L)$-beli mátrixszal). Speciálisan $\lambda \in K$ esetén $\beta(g)(\lambda) = \lambda$, azaz A_f egy K-lineáris altér $M_n(L)$-ben, hiszen $\beta(g)$ egy K-lineáris leképezés. Tehát A_f valóban egy végesdimenziós K-algebra. A következő lemma önmagában is érdekes, rengeteg alkalmazása van:

3.16. Lemma. *Legyen $K \leq L$ egy véges Galois-bővítés G Galois-csoporttal és V egy végesdimenziós vektortér L fölött, melyen G* szemilineárisan *hat, azaz $g(\lambda v) = g(\lambda)g(v)$, ha $\lambda \in L$ és $v \in V$. Ekkor a*

$$\begin{aligned} \alpha\colon L \otimes_K V^G &\to V \\ \lambda \otimes v &\mapsto \lambda v \end{aligned}$$

leképezés egy bijektív lineáris leképezés, ahol V^G a G-hatás fixpontjainak a halmazát jelöli.

Bizonyítás. Injektivitás: Mivel V végesdimenziós L fölött, és $|L : K| < \infty$, $\dim_K V^G \leq \dim_K V = |L : K| \dim_L V < \infty$. Vegyünk tehát egy $u_1, \ldots, u_k$ bázist V^G-ben. Ekkor $1 \otimes u_1, \ldots, 1 \otimes u_k$ egy bázis $L \otimes_K V^G$-ben. Azt kell tehát belátnunk, hogy $u_1, \ldots, u_k$ lineárisan független a bővebb L test fölött is: ugyanis ha $\sum_{i=1}^k \lambda_i \otimes u_i$ benne van α magjában, akkor $\sum_{i=1}^k \lambda_i u_i = \alpha(\sum_{i=1}^k \lambda_i \otimes u_i) = 0$. Tegyük fel tehát, hogy $\sum_{i=1}^k \lambda_i u_i = 0$ valamely $\lambda_1, \ldots, \lambda_k \in L$ együtthatókkal és ez a lineáris kombináció a lehető legkevesebb nemnulla együtthatót tartalmaz (azon lineáris kombinációk között, melyek értéke 0). Feltehetjük, hogy $\lambda_1 \neq 0$, sőt, λ_1-gyel leosztva azt is, hogy $\lambda_1 = 1$. Belátjuk, hogy ekkor $\lambda_i \in K$ minden $i = 1, \ldots, k$-ra, ami ellentmond annak a feltevésnek, hogy $u_1, \ldots, u_k$ lineárisan független K fölött. Tegyük fel ugyanis, hogy $\lambda_j \notin K$ valamely $j \in \{1, \ldots, k\}$-ra. Ekkor a Galois-elmélet főtétele szerint van olyan $g \in G$ elem a Galois-csoportban, melyre $g(\lambda_j) \neq \lambda_j$. Viszont

$$0 = g(0) - 0 = g(\sum_{i=1}^k \lambda_i u_i) - \sum_{i=1}^k \lambda_i u_i = \sum_{i=1}^k (g(\lambda_i)g(u_i) - \lambda_i u_i) = \sum_{i=1}^k (g(\lambda_i) - \lambda_i)u_i \ .$$

A jobb oldal nem egy triviális lineáris kombináció, hiszen $g(\lambda_j) - \lambda_j \neq 0$, viszont $g(\lambda_1) - \lambda_1 = g(1) - 1 = 0$ miatt szigorúan kevesebb nemnulla tag van benne, mint az eredeti lineáris kombinációban. Ez ellentmondás.

Szürjektivitás: Mivel $K \leq L$ egy véges Galois bővítés, $L = K(\gamma)$ alkalmas $\gamma \in L$ elemmel. Ekkor az $1, \gamma, \ldots, \gamma^{r-1}$ egy bázis L-ben K fölött, ha $r = |L : K| = |G|$. Továbbá mivel γ minimálpolinomja r-edfokú, és nincs többszörös gyöke, ezért a $g(\gamma) \in L$ Galois-konjugáltak mind különbözőek, ha g végigfut G-n. Válasszunk egy $v \in V$ elemet, azt szeretnénk belátni, hogy v benne van α képében. Vegyük észre, hogy

$$v_j := \sum_{g \in G} g(\gamma^{j-1}v) \in V^G$$

egy fixpont tetszőleges $j = 1, \ldots, r$ esetén. Viszont G elemeit sorbarendezve (azaz $G = \{g_1 = 1, g_2, \ldots, g_r\}$ választással) az $X := ((g_i(\gamma^{j-1}))_{1 \leq i,j \leq r} \in L^{r \times r}$ egy Vandermonde-típusú mátrix, speciálisan determinánsa nem nulla, azaz invertálható. Tehát van egy olyan $(\lambda_1, \ldots, \lambda_r)^T$ oszlopvektor, melyre $X(\lambda_1, \ldots, \lambda_r)^T = (1, 0, \ldots, 0)^T$, azaz

$$\sum_{j=1}^r g_i(\gamma^{j-1})\lambda_j = \begin{cases} 1 & \text{ha } i = 1 \\ 0 & \text{ha } i \neq 1 \ . \end{cases}$$

Speciálisan

$$\alpha(L\otimes_K V^G)\ni\alpha\left(\sum_{j=1}^r\lambda_j\otimes v_j\right)=\sum_{j=1}^r\lambda_j v_j=\sum_{j=1}^r\lambda_j\sum_{i=1}^r g_i(\gamma^{j-1})g_i(v)=$$
$$=\sum_{i=1}^r\left(\sum_{j=1}^r\lambda_j g_i(\gamma^{j-1})\right)g_i(v)=g_1(v)=v\ .$$

□

A Lemmát a $V:=M_n(L)$ vektortérre és a fent definiált csavart hatásra alkalmazva azt kapjuk, hogy az

$$\begin{array}{rcl}A_f\otimes_K L & \to & M_n(L)\\ X\otimes\lambda & \mapsto & X\lambda\end{array}$$

leképezés egy izomorfizmusa L-algebráknak. A 2.5. Tétel miatt tehát A_f egy centrális egyszerű K-algebra. Mivel f épp a két különböző Galois-hatás eltérését méri, ezért az A_f-hez rendelt keresztezett homomorfizmus épp f. Megfordítva, ha egy A centrális egyszerű algebrából indulunk ki, akkor az f_A keresztezett homomorfizmushoz legyártott A_{f_A} centrális egyszerű algebra izomorf A-val. □

Ahhoz, hogy a Brauer-csoportot azonosítsuk egy kohomológia-halmazzal, meg kell értenünk, hogyan viselkedik az n-edfokú A centrális egyszerű algebrához rendelt $f_A\colon G\to\mathrm{PGL}_n(L)$ keresztezett homomorfizmus Brauer-ekvivalenciára nézve. Ha $k\geq 1$ egy egész szám és $f_A(g)\in\mathrm{Aut}_L(M_n(L))$ a $P\in\mathrm{GL}_n(L)$-beli mátrixszal való konjugálás, akkor $f_{M_k(A)}(g)$ az $M_k(M_n(L))$-beli mátrix minden elemét konjugálja P-vel, ez pedig nem más, mint a $\mathrm{diag}(P,\dots,P)$ blokkdiagonális mátrxiszal való kojugálás.

3.17. Következmény. *Legyen L/K egy véges Galois-bővítés G Galois csoporttal. Ekkor* $\mathrm{Br}(L|K)\cong H^1(G,\mathrm{PGL}_\infty(L)):=\bigcup_n H^1(G,\mathrm{PGL}_n(L))$ *(mint Abel-csoportok), ahol a felszálló unió a*

$$\begin{array}{rcl}\mathrm{PGL}_n(L) & \hookrightarrow & \mathrm{PGL}_{nk}(L)\\ P & \mapsto & \begin{pmatrix}P & & 0\\ & \ddots & \\ 0 & & P\end{pmatrix}\end{array}$$

beágyazásakon keresztül vétetik. A jobb oldalon a csoportstruktúra mátrixok tenzorszorzatán keresztül van definiálva: ha $P\in\mathrm{PGL}_n(L)$, $Q\in\mathrm{PGL}_m(L)$, akkor $P\otimes Q\in\mathrm{PGL}_{nm}(L)$.

3.18. Következmény (Hilbert 90-es tétele)**.** *Legyen $K\leq L$ egy véges Galois-bővítés G Galois-csoporttal. Ekkor $H^1(G,\mathrm{GL}_n(L))=\{1\}$ triviális minden $n\geq 1$-re.*

Bizonyítás. Ez lényegében a 3.16. Lemma: vegyünk egy $f\colon G\to\mathrm{GL}_n(L)$ keresztezett homomorfizmust valamely $n\geq 1$-re és tekintsük G-nek az f-fel csavart β hatását a $V:=L^n$ vektortéren, azaz $\beta(g)(v):=f(g)\cdot g(v)$ (ahol $\cdot$ itt az $f(g)\in\mathrm{GL}_n(L)$ mátrix és a $v\in K^n$ oszlopvektor szokásos szorzatát jelöli). A 3.16. Lemma szerint V ezzel a hatással ellátva izomorf $L\otimes_K V^{\beta(G)}$-vel. Ha vesszük $V^{\beta(G)}$-nek egy K fölötti $v_1,\dots,v_n$ bázisát, akkor az izomorfizmus azt jelenti, hogy $v_1,\dots,v_n$ L-fölötti bázis V-ben és G csavart hatása a $v_1,\dots,v_n$ elemeken triviális, formulával: $f(g)\cdot g(v_i)=v_i$ $(i=1,\dots,n)$. Ha a $v_1,\dots,v_n\in L^n$ vektorokat összegyűjtjük egy $P\in\mathrm{GL}_n(L)$ mátrixba, akkor ezen azonosságokat egymás mellé rendezve az $f(g)\cdot g(P)=P$ azonosságot kapjuk minden $g\in G$-re, azaz $f(g)=(P^{-1})^{-1}\cdot g(P^{-1})$ ekvivalens a triviális keresztezett homomorfizmussal. □

Hogy a fenti következmény jelentőségét mutassuk, vázoljuk ennek segítségével a Kummer-elmélet bizonyítását:

3.19. Következmény. *Tegyük fel, hogy K-ban van primitív n-edik egységgyök és $K \leq L$ egy olyan Galois-bővítés, melynek G Galois-csoportja n-edrendű ciklikus. Ekkor $L = K(\sqrt[n]{a})$ alakú alkalmas $a \in K$ elemmel.*

Bizonyítás. Tekintsük ugyanis azt az $f\colon G \to L^\times = \mathrm{GL}_1(L)$ keresztezett homomorfizmust, mely G egy rögzített $\sigma \in G$ generátorelemét a $\zeta_n \in K \subset L$ primitív n-edik egységgyökbe küldi. Mivel G triviálisan hat ζ_n-en (hiszen az már a K alaptestben is benne van), ezért $f(\sigma^j) = \zeta_n^j$ jóldefiniált és egy igazi (nemcsak keresztezett) homomorfizmus lesz. Mivel $H^1(G, L^\times)$ triviális (3.18. Következmény $n = 1$-re), ezért f ekvivalens a triviális keresztezett homomorfizmussal, azaz van olyan $\alpha \in L^\times$, melyre $\zeta_n^j = f(\sigma^j) = \frac{\sigma^j(\alpha)}{\alpha}$ ($j = 0, \dots, n-1$ – a művelet $L^\times$-ben a szorzás, nem pedig az összeadás, ezért kell hányadost venni és nem különbséget). Így α minimálpolinomja

$$\prod_{j=0}^{n-1}(x - \sigma^j(\alpha)) = \prod_{j=0}^{n-1}(x - \zeta_n^j\alpha) = x^n - \alpha^n \in K[x]$$

n-edfokú, azaz $a := \alpha^n \in K$ választással $L = K(\alpha) = K(\sqrt[n]{a})$. □

Egy picit koncepciózusabban a következő történik: Most csak annyit tegyünk fel, hogy $K \leq L$ egy Galois-bővítés G Galois-csoporttal, és $\zeta_n \in L$ (azaz a *bővebb* testben már benne vannak az n-edik egységgyökök, de K-ban nem feltétlen és G nem feltétlen ciklikus). Tekintsük $L^\times$-en az n-edik hatványra emelést, mint csoporthomomorfizmust. Ennek magja nem más, mint az n-edik egységgyökök μ_n csoportja, képe pedig az n-edik hatványok $(L^\times)^n$ részcsoportja, azaz kapunk egy

$$1 \to \mu_n \to L^\times \xrightarrow{(\cdot)^n} (L^\times)^n \to 1$$

rövid egzakt sorozatot. Mivel a G-invariánsok éppen K elemei, a (3) sorozat ebben az esetben a következő formát ölti:

$$1 \to \mu_n \cap K^\times \to K^\times \xrightarrow{(\cdot)^n} K^\times \cap (L^\times)^n \to H^1(G, \mu_n) \to H^1(G, L^\times) = 1\ .$$

Speciálisan $K^\times \cap (L^\times)^n/(K^\times)^n \cong H^1(G, \mu_n)$. Sőt, ha $\mu_n \subset K$ is teljesül, akkor $H^1(G, \mu_n)$ elemei valójában $G \to \mu_n \cong (\mathbb{Z}/(n), +)$ csoporthomomorfizmusok. Vegyük észre, hogy a bal oldalon álló $K^\times \cap (L^\times)^n/(K^\times)^n$ csoport pont azt méri, hogy hány $K^\times$-beli elem válik $L^\times$-ben már n-edik hatvánnyá azok közül, amik nem eleve n-edik hatványok.

4. Alkalmazások és kitekintés

Joggal felmerül a kérdés, hogy miért jó, ha a centrális egyszerű algebrák ekvivalenciaosztályait egy nagyon absztrakt kohomológiacsoportként fogjuk fel, ha utóbbiakat még kevésbé értjük. Egyrészt ez azért nincs teljesen így, másrészt pedig lássunk pár alkalmazást kitekintésként (ebben a fejezetben mellőzzük a precíz bizonyításokat, az érdeklődő olvasónak az [2] könyvet ajánljuk).

4.1. Severi-Brauer varietások

A [3] jegyzetben (vagy akár [2]-ben) láttuk, hogy egy K feletti $K(a, b)$ kvaternióalgebrához hozzá tudunk rendelni egy háromváltozós kvadratikus alakot (jelesül a $-ax^2 - by^2 + abz^2$-et), melynek pontosan akkor van K fölött nemtriviális megoldása, ha $K(a, b)$ hasad K fölött. Ezt próbáljuk általánosítani

magasabb fokú centrális egyszerű algebrákra. Először is vegyük észre a következőt. Ha K egy algebrailag zárt test (pl. $K = \mathbb{C}$) és $\mathrm{char}(K) \neq 2$, akkor tekintsük $-ax^2-by^2+abz^2 = 0$ egyenletű V görbe (kúpszelet) pontjait a projektív síkon (homogén koordinátákban). Algebrailag zárt test fölött a-nak és b-nek is van négyzetgyöke, tehát feltehetjük, hogy $a = b = 1$, azaz az $x^2 + y^2 = z^2$ egyenletű görbét szeretnénk paraméterezni. Ez elsőéves számelmélet: $x = s^2 - t^2$, $y = 2st$, $z = s^2 + t^2$ a paraméterezés, tehát a

$$\begin{array}{rcl} \mathbb{P}^1(K) & \to & V \\ [s:t] & \mapsto & [s^2 - t^2 : 2st : s^2 + t^2] \end{array}$$

egy izomorfizmus.

A magasabbdimenziós alkalmazáshoz használjuk a fenti kohomologikus interpretációt. Az alapelv az, hogy $\mathrm{PGL}_n(L)$ nemcsak az $M_n(L)$ mátrixgyűrűnek az automorfizmuscsoportja, hanem az L fölötti $n-1$-dimenziós $\mathbb{P}^{n-1}(L)$ projektív térnek is. Valóban, $\mathbb{P}^{n-1}(L)$ pontjai nem mások, mint az 1-dimenziós alterek L^n-ben – ezeken hat $\mathrm{GL}_n(L)$, de a skalármátrixok triviálisan hatnak, így tehát $\mathrm{PGL}_n(L)$ hatását kapjuk $\mathbb{P}^{n-1}(L)$-en. Ez a hatás már hű, és tranzitív, továbbá bizonyítás nélkül elfogadjuk azt az algebrai geometriai tényt, hogy minden olyan homogén racionális törtfüggvény, mely bijekciót ad a $\mathbb{P}^{n-1}(L)$ projektív téren (homogén koordinátákat használva), törtlineáris, azaz a $\mathrm{PGL}_n(L)$ csoport egy elemének hatásával egyezik meg. Tehát ha L/K egy Galois bővítés G Galois-csoporttal, akkor a $H^1(G, \mathrm{PGL}_n(L))$ kohomológiatér nemcsak az $M_n(L)$ mátrixgyűrű K fölötti formáit (azaz a K fölött n-edfokú L felett hasadó centrális egyszerű algebrákat) osztályozza, hanem a $\mathbb{P}^{n-1}(L)$ projektív tér K fölötti formáit is – utóbbiakat nevezzük Severi–Brauer varietásnak. A centrális egyszerű algebrák kohomologikus klasszifikációjához hasonlóan belátható, hogy $H^1(G, \mathrm{PGL}_n(L))$ a K fölött definiált, L fölött hasadó $n-1$-dimenziós Severi–Brauer varietásokat is klasszifikálja! Másszóval kapunk egy bijekciót a K fölötti n-edfokú (adott L/K véges bővítés fölött hasadó) centrális egyszerű algebrák, illetve a K fölötti $n-1$-dimenziós (adott L/K véges bővítés fölött hasadó) Severi–Brauer varietások között. Igaz továbbá az alábbi rendkívül hasznos

4.1. Tétel (Châtelet)**.** *Legyen X egy $n-1$-dimenziós Severi–Brauer varietás egy K test fölött. X pontosan akkor izomorf $\mathbb{P}^{n-1}(K)$-val K fölött (azaz hasad), ha van K-racionális pontja.*

Ennek segítségével centrális egyszerű algebrákkal kapcsolatos kérdések vizsgálatára lehet használni algebrai geometriai eszközöket. Az ilyen típusú kapcsolatok különböző területek között szinte mindig rendkívül hasznosak. Pl. Chevalley és Warning alábbi jól ismert tételének segítségével is lehet bizonyítani Wedderburn véges ferdetestek nemlétezéséről szóló tételét.

4.2. Tétel (Chevalley–Warning, vö. 3.6.1. Tétel [1]-ben)**.** *Legyenek $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ polinomok, melyekre $\sum_{i=1}^r \deg(f_i) < n$ ($\mathbb{F}_q$ a $q = p^f$ elemű test). Ekkor p osztja az $f_1, \ldots, f_r$ polinomok $\mathbb{F}_q^n$-beli közös gyökeinek a számát. Speciálisan ha a $(0, \ldots, 0)$ gyök, akkor van nemtriviális gyök is.*

4.2. A Brauer-csoport torziócsoport

Egy másik fontos alkalmazása a Brauer-csoport kohomologikus interpretációjának, hogy a Brauer-csoport egy *torziócsoport*, azaz minden elem rendje véges. Sőt, ha D egy centrális egyszerű n-edfokú ferdetest (azaz $\dim_K D = n^2$), akkor D osztályának rendje a $\mathrm{Br}(K)$ Brauer-csoportban (azaz D *periódusa*) osztója n-nek (az n-et a D-vel ekvivalens centrális egyszerű algebrák *indexének* is nevezik). Más szóval $D^{\otimes n} := \underbrace{D \otimes_K \cdots \otimes_K D}_{n}$ hasad tetszőleges D n-edfokú centrális ferdetest esetén. Sőt a periódusnak ugyanazok a prímosztói, mint az indexnek (de általában nem egyenlők). Ennek bizonyítása használja a Brauer-csoport másik (kommutatív együtthatós) kohomologikus interpretációját is: az $1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 1$ rövid egzakt sorozathoz is tartozik egy „hosszú egzakt sorozat”,

mely ad egy $\delta\colon H^1(G,\mathrm{PGL}_n(L)) \to H^2(G,L^\times)$ határleképezést, mely ha n-nel tartunk a végtelenhez, akkor izomorfizmust indukál. Speciálisan $\mathrm{Br}(L|K) \cong H^2(G,L^\times)$. Viszont utóbbiról a csoportkohomológia eszközeivel könnyen következik, hogy torziócsoport.

4.3. Ciklikus algebrák és a Merkurjev-Szuszlin tétel

A centrális egyszerű algebrák elméletének (egyik) fő tétele egyfajta struktúratétel. Kimondásához szükségünk lesz az ún. *ciklikus algebrák* fogalmára, melyek speciális centrális egyszerű algebrák, bizonyos szempontból a kvaternióalgebrák magasabb dimenziós közvetlen általánosításai. Az egyszerűség kedvéért együk fel, hogy a K alaptest tartalmaz egy ω primitív n-edik egységgyököt valamilyen n-re. Ekkor az $a,b \in K^\times$ konstansokkal definiált n-edfokú $K(a,b)_\omega$ ciklikus algebrát az

$$\langle x,y \mid x^n = a,\ y^n = b,\ xy = \omega yx\rangle$$

prezentációval adhatjuk meg.

4.3. Feladat. *Igazoljuk, hogy a fenti generátorokkal és relációkkal megadott $K(a,b)_\omega$ algebra centrális egyszerű algebra K fölött.*

Valóban, a kvaternióalgebrák ennek speciális esetei $n=2$ és $\omega=-1$ választással. Amennyiben K nem tartalmaz primitív n-edik egységgyököt, akkor egy L/K bővítést kell választanunk (a helyett), melynek n-edrendű ciklikus a Galois-csoportja egy σ generátorral, a ciklikus algebránk pedig az $L[y,\sigma]$ algebra azokkal a relációkkal, hogy $y^n = b$, és y nem felcserélhető L elemeivel: jelesül az y-nal való konjugálás L-en épp a σ testautomorfizmus.

4.4. Tétel (Merkurjev–Szuszlin (1983))**.** *Tegyük fel, hogy K-ban van egy ω primitív n-edik egységgyök, és A egy centrális egyszerű K-algebra úgy, hogy A Brauer csoportbeli osztályának rendje (azaz A* periódusa*) osztja n-et. Ekkor A Brauer-ekvivalens néhány n-edfokú ciklikus algebra*

$$K(a_1,b_1)_\omega \otimes_K \cdots \otimes_K K(a_r,b_r)_\omega \tag{4}$$

tenzorszorzatával.

A fenti tétel következménye, hogy (legalábbis 0 karakterisztikában) minden centrális egyszerű algebra felhasad egy alkalmas *feloldható* Galois bővítés felett (azaz olyan Galois bővítés felett, melynek Galois csoportja feloldható). Valóban, minden centrális egyszerű algebra Brauer-osztálya véges rendű (hiszen $\mathrm{Br}(K)$ egy torziócsoport). Másrészt a körosztási bővítés Abel, ezért adott n-edfokú A centrális egyszerű algebra esetén a K alaptesthez adjungálhatjuk az ω primitív n-edik egységgyököt. $A \otimes_K K(\omega)$-ra már alkalmazhatjuk a Merkurjev–Szuszlin tételt, tehát elég belátni, hogy minden (4) alakú algebra hasad egy alkalmas feloldható bővítés fölött. Node a $K(\omega, \sqrt[n]{a_1},\dots,\sqrt[n]{a_r})$ bővítés fölött hasad a (4) alakú algebra, a $\mathrm{Gal}(K(\omega, \sqrt[n]{a_1},\dots,\sqrt[n]{a_r})/K)$ Galois csoport pedig feloldható. Erre a – viszonylag elemien megfogalmazható – következményre nem ismert elemi bizonyítás.

4.4. Reciprocitási tételek

A Brauer-csoport alapvető fontosságú az algebrai számelméletben is, azon belül az *osztálytestelméletben.* Az osztálytestelmélet fő célja általános reciprocitási tételek igazolása. Ezen kapcsolat megértéséhez vegyünk $\mathbb{Q}$ felett egy $\mathbb{Q}(a,b)$ kvaternióalgebrát. Ez a [3]-beli 12. Tétel szerint pontosan akkor hasad, ha a hozzátartozó

$$C(a,b) = \{[x:y:z] \in \mathbb{P}^2 \mid -ax^2 - by^2 + abz^2 = 0\}$$

projektív síkgörbének van racionális pontja, azaz $C(a,b)(\mathbb{Q}) \neq \emptyset$. Mivel $C(a,b)$ egy homogén másodfokú egyenlet, alkalmazhatjuk az alábbi tételt.

4.5. Tétel (Hasse (1923, $\mathbb{Q}$ véges bővítéseire is)–Minkowski (1900 körül, ebben a formában))**.** *Legyen $f(x_1, \cdots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ egy homogén másodfokú polinom. Ekkor f-nek pontosan akkor van nemtriviális megoldása $\mathbb{Q}$ fölött (azaz akkor van pontja a homogén koordinátákkal ellátott $\mathbb{P}^{n-1}(\mathbb{Q})$ projektív térben), ha van nemtriviális megoldása $\mathbb{R}$-ben és minden p prímszámra $\mathbb{Q}_p$-ben.*

4.6. Megjegyzés. A közös nevezővel beszorozva feltehetjük, hogy f egész együtthatós. Sőt, a homogenitás miatt pontosan akkor van racionális megoldás, ha van egész megoldás is, hiszen a megoldásokat is felszorozhatjuk a koordináták közös nevezőjével. Végezetül a $\mathbb{Q}_p$ feletti feltételt az alábbi, elmi módon is megfogalmazhatjuk: az kell, hogy f-nek legyen megoldása modulo p^n minden $n \geq 1$ egész számra. Ugyanis ha minden n-re van megoldásunk modulo p^n, akkor ezeket a König-lemma segítségével tudjuk összegyúrni egy p-adikus megoldássá.

Tehát $C(a,b)(\mathbb{Q}) \neq \emptyset$ pontosan akkor, ha $C(a,b)(\mathbb{R}) \neq \emptyset$ és minden p prímszámra $C(a,b)(\mathbb{Q}_p) \neq \emptyset$. Másszóval a $\mathbb{Q}(a,b)$ kvaternióalgebra pontosan akkor hasad $\mathbb{Q}$ fölött, ha hasad $\mathbb{Q}_p$ fölött minden p-re (beleértve a $p = \infty$-t is, melyre $\mathbb{Q}_\infty := \mathbb{R}$). Utóbbi nemcsak kvaternióalgebrákra igaz, hanem tetszőleges centrális egyszerű algebrára: tehát ez esetben teljesül a Hasse-féle *lokális–globális* elv. A Brauer-csoportok nyelvén ez annyit tesz, hogy a

$$\mathrm{Br}(\mathbb{Q}) \to \bigoplus_{p \leq \infty \text{ prím}} \mathrm{Br}(\mathbb{Q}_p)$$

természetes leképezés injektív. Ahhoz, hogy $\mathrm{Br}(\mathbb{Q})$ képét megértsük, meg kell határoznunk először a lokális testek Brauer csoportját. Megmutatható, hogy amennyiben p véges, akkor $\mathrm{Br}(\mathbb{Q}_p) \cong H^2(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}_p}^\times) \cong \mathbb{Q}/\mathbb{Z}$, illetve a $p = \infty$ esetben $\mathrm{Br}(\mathbb{R}) \cong H^2(G_{\mathbb{R}}, \mathbb{C}^\times) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ másodrendű ciklikus (utóbbi Frobenius tétele az $\mathbb{R}$ fölötti nullosztómentes végesdimenziós algebrákról). Ez az azonosítás *kanonikus* (nem függ semmilyen választástól): egy adott $\mathbb{Q}_p$ feletti centrális egyszerű algebrához tartozó $\mathbb{Q}/\mathbb{Z}$-beli elemet az algebra *Hasse-invariánsának* nevezzük. Továbbá vegyünk minden p prímre egy $a_p \in \mathbb{Q}/\mathbb{Z}$-beli (és $p = \infty$-re egy $a_\infty \in \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$-beli) elemet úgy, hogy véges sok kivétellel mindegyik 0 legyen. Pontosan akkor létezik olyan $\mathbb{Q}$ feletti centrális egyszerű algebra, melynek lokális Hasse-invariánsai az a_p számok, ha ezen számok összege 0. Másszóval a

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{p \leq \infty \text{ prím}} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0 \tag{5}$$

sorozat egzakt. Ez hasonló mélységű eredmény, mint maga az osztálytest elmélet: a $\mathbb{Q}$ véges bővítéseire vonatkozó általánosításaiból következnek a főbb reciprocitási tételek. Ennek illusztrálásaként megmutatjuk a Gauß-féle kvadratikus reciprocitási tételt. Mivel $\mathbb{Q}/\mathbb{Z}$-ben egyetlen másodrendű elem van (jelesül az $1/2$ mellékosztálya), a Brauer csoport 2-torziójában minden esetben egyetlen nemtriviális elem van lokálisan. Ezt a tényt beláthatjuk elemien is: $p = \infty$ esetén $\mathbb{H} = \mathbb{R}(-1,-1)$ az egyetlen nem hasadó kvaternióalgebra.

4.7. Feladat. *Legyen p páratlan prím és $u \in \{2, \ldots, p-1\}$ kvadratikus nemmaradék mod p. Igazoljuk a következőket. $\mathbb{Q}_p(u,p)$ egy ferdetest, és izomorfia erejéig nincs másik nemhasadó kvaternióalgebra $\mathbb{Q}_p$ fölött. Másrészt $p = 2$-re $\mathbb{Q}_2(-1,-1)$ egy ferdetest, és izomorfia erejéig nincs másik nemhasadó kvaternióalgebra $\mathbb{Q}_2$ fölött.*

Megoldásvázlat. Több lépésben bizonyítunk, mely közül az első az alábbi – önmagában is érdekes –

4.8. Lemma. *$|\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2| = 4$, és ennek (mint $\mathbb{F}_2$ fölötti vektortérnek) a bázisa p és u (mellékosztálya). $|\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2| = 8$, és ennek bázisa -1, -3, és 2.*

Bizonyítás. Vegyünk egy $\alpha \in \mathbb{Q}_p^\times$ elemet. Ezt egyértelműen tudjuk ep^k alakba írni, ahol $k = v_p(\alpha)$ (azaz $|\alpha|_p = p^{-k}$), és $v_p(e) = 0$, azaz $e \in \mathbb{Z}_p^\times$ (hiszen e és reciproka is p-adikus egész). Ha k páros, akkor p^k négyezetszám $\mathbb{Q}_p$-ben, ha pedig páratlan, akkor négyzetszám p-szerese. Sőt, ha α négyzetszám, akkor $v_p(\alpha) = k$ páros, hiszen v_p additív. Írjuk e-t $e = e_0 + e_1 p + \cdots + e_n p^n + \cdots$ alakban. Nyilván ha $e = \beta^2$ négyzetszám $\mathbb{Q}_p$-ben, akkor $0 = v_p(e) = 2v_p(\beta)$ miatt β is $\mathbb{Z}_p^\times$-ben van. Modulo p redukálva azt kapjuk, hogy e_0 is négyzetszám mod p. Viszont páratlan p esetén ez a feltétel elegséges is: ha $e_0 \neq 0$ kvadratikus maradék, akkor van olyan $\beta_0 \in \mathbb{Z}_p^\times$, melyre $\beta_0^2 \equiv e_0 \pmod p$, azaz $\frac{e}{\beta_0^2} = 1 + p(\cdots)$ alakú – elég ebből négyzetgyököt vonni. Ez egyrészt a „prímhatványalapú kongruencia visszavezetése prímalapúra" (avagy Hensel-lemma) fejezet elsőéves számelméletből, másrészt pedig a következőképpen is okoskodhatunk: tekintsük a

$$\sqrt{1+px} = \sum_{n=0}^{\infty} \binom{1/2}{n} (px)^n$$

binomiális sort. Ha $x \in \mathbb{Z}_p$, akkor ez p-adikusan konvergál, hiszen az $\binom{1/2}{n} = \frac{1/2(1/2-1)\cdots(1/2-n+1)}{n!}$ „binomiális" együttható p-adikus egész, hiszen $1/2 \in \mathbb{Z}_p$ (vagy ha úgy tetszik, ha az $\binom{1/2}{n}$ racionális szám modulo p^N érdekel minket, ahol $N \gg 0$, akkor az $1/2$-et lecserélhetjük a 2 multiplikatív inverzére mod p^N, és a számláló ugyanazt a maradékot adja, viszont a tört már egy közönséges binomiális együttható lesz, aminek értéke egész szám). Mivel két kvadratikus nemmaradék szorzata kvadratikus maradék modulo p, azt kapjuk, hogy $\alpha = u^{\varepsilon_1} p^{\varepsilon_2} \beta^2$ alakba írható egyértelmű módon, ahol $\varepsilon_i \in \{0,1\}$ $(i = 1,2)$, $\beta \in \mathbb{Q}_p^\times$, azaz az állítást igazoltuk.

A $\mathbb{Q}_2$-re vonatkozó állítás esetében hasonlóan okoskodhatunk. Azt kell észrevenni, hogy $(\mathbb{Z}/8\mathbb{Z})^\times$ a Klein-csoporttal izomorf, és -1, ill. -3 mellékosztálya generálja. Továbbá a fenti érveléshez hasonlóan a kérdés arra redukálódik, hogy ha $e \equiv 1 \pmod 8$, akkor e-nek van négyzetgyöke $\mathbb{Z}_2$-ben. Ez is kijön elemien is, de elegánsabb a

$$\sqrt{1+8x} = \sum_{n=0}^{\infty} \binom{1/2}{n} (8x)^n$$

binomiális sor konvergenciáját megvizsgálni 2-adikusan:

$$\begin{aligned} v_2\left(\binom{1/2}{n}(8x)^n\right) &= nv_2(8x) + v_2(1/2(1/2-1)\cdots(1/2-n+1)) - v_2(n!) = \\ &= nv_2(x) + 3n - n - \lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor - \cdots - \lfloor \frac{n}{2^k} \rfloor - \cdots \geq n \to \infty \,. \end{aligned}$$

□

A fenti lemmát és a $K(a,b) \cong K(a,bc^2)$ izomorfizmust használva $(0 \neq a,b,c \in K)$ a $\mathbb{Q}_p(a,b)$ izomorfiaosztályát elég meghatároznunk az $a,b \in \{1,u,p,up\}$ esetekben, illetve $\mathbb{Q}_2$ fölött pedig $a,b \in \{1,-1,-3,3,2,-2,-6,6\}$ esetekben. Ezekhez pedig a $K(a,b) \cong K(a,-ab)$ izomorfiát használjuk elsősorban, illetve azt, hogy $K(a,1)$ hasad. Továbbá szükségünk lesz alábbi lemmákra is.

4.9. Lemma. *Legyenek $0 \neq a,b \in \mathbb{F}_p$ és $c \in \mathbb{F}_p$ tetszőlegesek (p prím). Ekkor az $ax^2 + by^2 = c$ egyenletnek van megoldása $\mathbb{F}_p$-ben.*

Bizonyítás. Tekintsük az $\{ax^2 \mid x = 0,1\ldots,p-1\} \subseteq \mathbb{F}_p$ és a $\{c - by^2 \mid y = 0,1\ldots,p-1\} \subseteq \mathbb{F}_p$ halmazokat. Mindkettő $\frac{p+1}{2}$ elemű, ezért nem lehetnek diszjunktak. □

4.10. Lemma. *Legyen p páratlan prím. Ekkor az x^2+y^2 és a $-x^2-y^2$ kvadratikus alakok ekvivalensek $\mathbb{Q}_p$ fölött.*

Bizonyítás. A 4.9. Lemma miatt az $x^2+y^2\equiv -1 \pmod p$ kongruenciának van megoldása. Ekkor a 4.8. Lemma bizonyításához hasonlóan az $x^2+y^2=-1$ egyenletnek van $\mathbb{Q}_p$-ben megoldása. Tehát a kétdimenziós $\mathbb{Q}_p^2$ vektortérben van olyan v vektor, melynek önmagával vett skalárszorzata -1. A Gram–Schmidt-féle ortogonalizációs eljárással kapunk egy w vektort, ami erre merőleges. Ráadásul mivel a kvadratikus alak determinánsa négyzetszám erejéig egyértelmű, w-t lenormálhatjuk úgy, hogy $[w,w]=-1$ legyen, hiszen a (v,w) bázisban a kvadratikus alak determinánsa $-[w,w]$, ami négyzetszám. Tehát a szokásos bázisban a kvadratikus alak x^2+y^2 alakú, a (v,w) bázisban pedig $-x^2-y^2$ alakú. □

4.11. Lemma. *Legyenek a és b páratlan számok. Az $ax^2+by^2=1$ egyenletnek pontosan akkor van megoldása $\mathbb{Q}_2$-ben, ha a és b közül legalább az egyik 1-et ad maradékul néggyel osztva. A $-3x^2+by^2=1$-nek nincs megoldása $\mathbb{Q}_2$-ben, ha $b=\pm 2,\pm 6$.*

Bizonyítás. A 4.8. Lemma miatt elég megvizsgálni, hogy az $ax^2+by^2\equiv 1 \pmod 8$ kongruenciának mikor van megoldása, ez pedig véges sok eset végignézése, amit az olvasóra bízunk. □

Tegyük fel először, hogy $p\equiv 1 \pmod 4$, azaz a -1 négyzetszám $\mathbb{Q}_p$-ben. Ekkor $\mathbb{Q}_p(u,p)\cong\mathbb{Q}_p(u,-up)\cong\mathbb{Q}_p(u,up)$ és $\mathbb{Q}_p(p,up)\cong\mathbb{Q}_p(p,-up^2)\cong\mathbb{Q}_p(p,u)\cong\mathbb{Q}_p(u,p)$. Továbbá $\mathbb{Q}_p(p,p)\cong\mathbb{Q}_p(p,-p^2)\cong\mathbb{Q}_p(p,1)\cong M_2(\mathbb{Q}_p)$. Hasonlóképp $\mathbb{Q}_p(u,u)$ és $\mathbb{Q}_p(up,up)$ is hasad. Tehát ebben az esetben csak azt kell még belátnunk, hogy $\mathbb{Q}_p(u,p)$ nem hasad, azaz a $-ux^2-py^2+upz^2$ kvadratikus alaknak nincs nemtriviális megoldása $\mathbb{Q}_p$-ben (vagy ezzel ekvivalensen $\mathbb{Z}_p$-ben). Ennek igazolásához tegyük fel, hogy $ux^2+py^2=upz^2$ valamely $x,y,z\in\mathbb{Z}_p$-re, melyek nem mind oszthatók p-vel. Ekkor nyilván $p\mid x$, azaz $x=px_1$ alakú, és p-vel leosztva $upx_1^2+y^2=uz^2$ adódik. Viszont ezt modulo p nézve ellentmondást kapunk, hiszen u kvadratikus nemmaradék, y és z pedig nem lehet egyszerre osztható p-vel. Ezzel a $p\equiv 1 \pmod 4$ esetet tisztáztuk.

Legyen most $p\equiv -1 \pmod 4$, azaz $-1=u$ is választható, hiszen -1 kvadratikus nemmaradék. A 4.10. Lemma szerint a px^2+py^2 és a $-px^2-py^2$ kvadratikus alakok is ekvivalensek. Speciálisan a [3]-beli 12. Tétel miatt $\mathbb{Q}_p(-1,p)\cong\mathbb{Q}_p(-1,-p)\cong\mathbb{Q}_p(-p,-p)\cong\mathbb{Q}_p(p,p)$, hiszen a hozzájuk tartozó kvadratikus alakok rendre $x^2-py^2-pz^2$, $x^2+py^2+pz^2$, $px^2+py^2+(pz)^2$, $-px^2-py^2+(pz)^2$, melyek ekvivalensek. Továbbá a $p\equiv 1 \pmod 4$ esethez hasonlóan ezeknek a kvadratikus alakoknak nincs nemtriviális megoldása. Végezetül $\mathbb{Q}_p(-1,-1)\cong\mathbb{Q}_p(1,1)$ hasad (ismét használva a 4.10. Lemmát), ugyancsak $\mathbb{Q}_p(p,-p)\cong\mathbb{Q}_p(p,p^2)$ is hasad, ezzel a $p\equiv -1 \pmod 4$ esetet is tisztáztuk.

$\mathbb{Q}_2$ fölött $\mathbb{Q}_2(3,-1)\cong\mathbb{Q}_2(3,3)$. Továbbá a 4.11. Lemma miatt a $-3x^2-3y^2$ kvadratikus alak előállítja az 1-et, így a Gram–Schmidt eljárást alkalmazva ekvivalens az x^2+y^2 kvadratikus alakkal. Tehát $\mathbb{Q}_2(3,3)\cong\mathbb{Q}_2(-1,-1)$ is teljesül, hiszen a hozzájuk tartozó kvadratikus alakok megegyeznek. Ráadásul a 4.11. Lemma (és a [3] 12. Tétel) miatt $\mathbb{Q}_2(-1,-1)$ nem hasad. Viszont ha a páratlan, akkor ugyanígy $\mathbb{Q}_2(a,-3)$ viszont hasad, hiszen $-3\equiv 1 \pmod 4$. Maradt tehát az az eset, amikor a és b közül legalább az egyik páros – tegyük fel először, hogy pontosan az egyik. Mivel a $2x^2-y^2=1$ egyenletnek az $x=y=1$ megoldása, ezért $\mathbb{Q}_2(2,-1)$ hasad. Hasonlóan $\mathbb{Q}_2(3,-2)\cong\mathbb{Q}_2(3,6)$ is hasad. Ugyanígy $-x^2-6y^2$ alakban előáll a $-7\equiv 1 \pmod 8$, ezért az 1 is, tehát $\mathbb{Q}_2(-1,-6)$ is hasad. Most jönnek azok, amik nem hasadnak: $\mathbb{Q}_2(3,2)\cong\mathbb{Q}_2(3,-6)$, sőt, az 5 előáll $2x^2+3y^2$ alakban, ezért a -3 is, hiszen kongruensek modulo 8. Ez pedig azt jelenti, hogy a $-2x^2-3y^2+6z^2$ kvadratikus alak ekvivalens a $3x^2+2y^2+6z^2$-tel, azaz $\mathbb{Q}_2(3,2)\cong\mathbb{Q}_2(-3,-2)\cong\mathbb{Q}_2(-3,-6)$ is teljesül. Hasonlóképp a $-3y^2+6z^2$ kvadratikus alak előállítja a 3-at, ezért ekvivalens a $3y^2-6z^2$ alakkal, így $\mathbb{Q}_2(2,3)\cong\mathbb{Q}_2(2,-3)$ is igaz. Itt viszont $\mathbb{Q}_2(-3,2)\cong\mathbb{Q}_2(-3,6)$, node a -1 nyilván előáll $-3x^2+2y^2$ alakban, ezért a $3x^2-2y^2-6z^2$ és az $x^2-6y^2-6z^2$ kvadratikus alakok ekvivalensek, azaz $\mathbb{Q}_2(-3,2)\cong\mathbb{Q}_2(-1,6)$. Továbbá $3y^2+3z^2$ alakban előáll a $3+3\cdot 4=15\equiv -1 \pmod 8$, ezért a -1 is előáll. Tehát $3y^2+3z^2$ ekvivalens a $-y^2-z^2$-tel, azaz $x^2-6y^2-6z^2$ ekvivalens $x^2+2y^2+2z^2$-tel, speciálisan $\mathbb{Q}_2(-1,6)\cong\mathbb{Q}_2(-1,-2)\cong\mathbb{Q}_2(-1,-1)$, hiszen az x^2+y^2 és a $2x^2+2y^2$ kvadratikus alakok ekvivalensek (a 2 előáll x^2+y^2 alakban), ezért az $x^2+y^2+z^2$ és $2x^2+2y^2+(2z)^2$ alakok is, azaz $\mathbb{Q}_2(-1,-1)\cong\mathbb{Q}_2(-1,-2)$. Végezetül a a és b is páros, akkor $\mathbb{Q}_2(a,b)\cong\mathbb{Q}_2(a,\frac{-ab}{4})$, azaz visszavezethető arra az esetre, amikor valamelyik páratlan. Az

átláthatóság kedvéért az alábbi táblázatban összefoglaljuk a $\mathbb{Q}_p$ és $\mathbb{Q}_2$ fölötti eredményeinket: az $(a,b)_{\mathbb{Q}_p}$ ún. Hilbert-szimbólum legyen 1, ha a $\mathbb{Q}_p(a,b)$ kvaternióalgebra hasad, a -1 pedig, ha nem hasad ($p \geq 2$ prím).

$p>2$ $(a,b)_{\mathbb{Q}_p}$	1	u	p	up
1	1	1	1	1
u	1	1	-1	-1
p	1	-1	$(-1)^{\frac{p-1}{2}}$	$(-1)^{\frac{p+1}{2}}$
up	1	-1	$(-1)^{\frac{p+1}{2}}$	$(-1)^{\frac{p-1}{2}}$

$(a,b)_{\mathbb{Q}_2}$	1	-3	-1	3	2	-6	-2	6
1	1	1	1	1	1	1	1	1
-3	1	1	1	1	-1	-1	-1	-1
-1	1	1	-1	-1	1	1	-1	-1
3	1	1	-1	-1	-1	-1	1	1
2	1	-1	1	-1	1	-1	1	-1
-6	1	-1	1	-1	-1	1	-1	1
-2	1	-1	-1	1	1	-1	-1	1
6	1	-1	-1	1	-1	1	1	-1

□

Tehát az (5) sorozat egzaktsága a 2-torzióra nézve azt jelenti, hogy minden $\mathbb{Q}$ feletti kvaternióalgebra páros sok $\ell \leq \infty$ prím esetén nem hasad lokálisan ℓ-nél (hiszen páros sok $1/2$ összege van $\mathbb{Z}$-ben, páratlan soké nem). Namármost, ha $p \neq q$ páratlan prímek, akkor a $\mathbb{Q}(p,q)$ kvaternióalgebra hasad $\mathbb{R}$ felett (hiszen p és q pozitívak), és minden $\ell \neq 2$ p-től és q-tól különböző prímre $\mathbb{Q}_\ell$ felett is. Ugyanis ha p vagy q négyzetszám mod ℓ, akkor $\mathbb{Q}_\ell(p,q)$ nyilván hasad, ha pedig egyik sem négyzetszám, akkor a 4.7. Feladat megoldásában láttuk, hogy $\mathbb{Q}_\ell(p,q) \cong \mathbb{Q}_\ell(u,u)$ ugyancsak hasad. Továbbá ismét használva a 4.7. Feladatot $\mathbb{Q}_p$ (ill. $\mathbb{Q}_q$) fölött pontosan akkor hasad $\mathbb{Q}(p,q)$, ha q (ill. p) kvadratikus maradék mod p (ill. mod q), azaz ha $\left(\frac{q}{p}\right) = 1$ (ill. ha $\left(\frac{p}{q}\right) = 1$). Végezetül $\mathbb{Q}_2$ fölött pedig pontosan akkor hasad, ha $p \equiv q \equiv -1 \pmod 4$ nem teljesül, azaz ha $(-1)^{\frac{(p-1)(q-1)}{4}} = 1$. Ezt összegezve a $\left(\frac{q}{p}\right)$, $\left(\frac{p}{q}\right)$, $(-1)^{\frac{(p-1)(q-1)}{4}}$ számok között páros sok -1-es van, így adódik a jól ismert

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}} = 1$$

kvadratikus reciprocitási tétel.

Hivatkozások

[1] Freud Róbert, Gyarmati Edit, *Számelmélet*, egyetemi tankönyv, Nemzeti Tankönyvkiadó, Budapest, 2000.

[2] Philippe Gille, Tamás Szamuely, *Central simple algebras and Galois cohomology*, 2nd ed., Cambridge studies in advanced mathematics **165**, Cambridge University Press, 2017.

[3] Zábrádi Gergely, *Kvaternióalgebrák és kvadratikus alakok*, internetes jegyzet.