Kvaternionska algebra

Literatura: John Voight: Quaternion algebras

M-F Vigneras: The Arithmetic of Quaternion algebra

Wai Kiu Chan: Arithmetic of Quaternion algebras

Motivacija: Deuringova korespodencija

Prsten endomorfizama End(E) (nad $\bar{K}$) je izomorfan maksimalnom

redu u kvaternionskoj algebri $B_{p,\infty}$ ramificiranoj u ∞ i u p ($p = \mathrm{char}\, K$).

Želimo razumjeti ove tablice (Deuringova korespodencija) ← ekvivalencija kategorija

supersing. j-inv. $j(E) \in \mathbb{F}_{p^2}$
(do na djelovanj Galoisove grupe)
$\longleftrightarrow$ maksimalni red $\mathcal{O} \subset B_{p,\infty}$ (do na izom.)
$\mathcal{O} \simeq \mathrm{End}(E)$

(E_1, φ) gdje je $\varphi : E \to E_1$ izogenija
$\longleftrightarrow$ I_φ integralni lijevi $\mathcal{O}$-ideal i desni $\mathcal{O}_1$-ideal

$\deg(\varphi)$
$\longleftrightarrow$ $n(I_\varphi)$

$\hat{\varphi}$
$\longleftrightarrow$ $\overline{I_\varphi}$

prvo čemo definirati sve ove pojmove

$\varphi : E \to E_1$, $\tau : E \to E_1$
$\longleftrightarrow$ ekvivalentni ideali $I_\varphi \sim I_\tau$

$\tau \circ \rho : E \to E_1 \to E_2$
$\longleftrightarrow$ $I_{\tau\circ\rho} = I_\rho \cdot I_\tau$

Definicija

pretpostavljam da je $\mathrm{char}\, F \neq 2$.

Def. 1. Kvaternionska algebra B nad poljem F je 4-dim algebra nad F s bazom $\{1, i, j, k\}$ t.d.

← standardna baza, ne mora biti jedinstvena

$$i^2 = a,\ j^2 = b,\ ij = k = -ji \quad \text{za neke } a, b \in F^*.$$

$(\Rightarrow k^2 = -ab)$ Pišemo $B = \left(\frac{a,b}{F}\right)$.

Uočimo, npr. $\left(\frac{a,b}{F}\right) = \left(\frac{ax^2, by^2}{F}\right) = \left(\frac{a, -ab}{F}\right)$.

Primjer 1: Neka su $i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $k = ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -ji$

matrice u $M_2(F)$. Tada je $i^2 = j^2 = 1$ i $\{1, i, j, k\}$ je baza za $M_2(F)$

$\Rightarrow M_2(F) = \left(\frac{1,1}{F}\right) = \left(\frac{1,-1}{F}\right)$.

Primjer 2: (Hamiltonovi kvaternioni) ← "proširenji" kompleksnih brojeva

Neka je $\mathbb{H}$ kvaternionska algebra nad $\mathbb{R}$ s bazom $\{1, i, j, k\}$ t.d.

$i^2 = j^2 = -1$ i $ij = k = -ji$, tj. $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$

Teorem 1: Neka su $a, b \in F^\times$. Tada $\left(\frac{a,b}{F}\right)$ postoji.

dokaz: d.z. (generalizacija Primjera 1)

Teorem 2: Kvaternionska algebra $\mathbb{H}$ nad F je centralna i prosta

elementi koji komutiraju sa svime → centar algebre je F ; nema pravih dvostranih ideala

Dokaz: Neka je $x = \alpha + \beta i + \gamma j + \delta k$ iz centra od $\mathbb{H}$ gdje su $\alpha, \beta, \gamma, \delta \in F$.

Tada $0 = jx - xj = 2k(\beta + \delta j)$. Slijedi $\beta = \delta = 0$.

Slično $\gamma = 0$, pa $x = \alpha \in F$.

Neka je $\mathcal{O}$ dvostrani ideal u $\mathbb{H}$. Dovoljno je pokazati da on sadrži element iz F.

Uzmimo neki $y = a + bi + cj + dk$ i pretp. da je neki od b, c, d različit od nule.

Množenjem y s i, j ili k možemo pretp. da je $a \neq 0$. Budući da je

$jx - xj = 2k(bi + cj) \in \mathcal{O}$ onda množenjem s $(2k)^{-1}$ (jer je $\operatorname{char} F \neq 2$) slijedi $bi + cj \in \mathcal{O}$.

Analogno, $a+bi$ i $a+dk$ su iz Q. Slijedi da je

$$0 \neq -2a = y - (a+bi) - (a+cj) - (a+dk) \in Q$$ što je trebalo pokazati.

Što se zna općenito o centralnim prostim algebrama? Dva teorema o strukturi.

Teorem 3: (Wedderburn) Neka je A konačnodimenzionalna prosta algebra nad F. Tada je A izomorfna s $M_n(D)$ gdje je $D \simeq End_A(N)$ divizijska algebra nad F, a N minimalni desni ideal od A. Prirodan broj n i D (do na izom.) su jednoznačno određeni s A.

↑ svaki element ima mult. inverz.

Teorem 4 (Skolem-Noether) Neka je A konačno dimenz. centralna prosta algebra nad F i neka je B k. dim. prosta algebra nad F.

Ako su φ, ψ homomorfizmi algebri s B u A, onda postoji invertibilan element $c \in A$ t.d. $\varphi(b) = c^{-1}\psi(b)c$ za sve $b \in B$.

Posebno, svi ne-nul endomorfizmi od A su unutarnji ($x \mapsto c^{-1}xc \ \forall x \in A$)
automorfizmi

Teorem 5: Neka je H kvaternionska algebra nad F.

a) ili je H divizijska algebra ili $H \simeq M_2(F)$

b) Neka je $E \subset H$ kvadratno proširenje od F i $\tau \in Gal(E/F)$. Tada postoji
pažnja
$j \in H^\times$ t.d. $j^2 \in F^\times$, $H = E + Ej$ i $jx = \tau(x)j \ \forall x \in E$.

Dokaz: b) Postoji $i \in H$ t.d. $E = F(i)$ i $i^2 \in F^*$.

Prema Skolem-Noether teoremu $-i = \tau(i) = j i j^{-1}$ za neki invertibilni $j \in H$. Budući da $j \notin E$ (jer ne komutira s $i \in E$) $\{1, i, j\}$ su linearno nezavisni nad F. Ako je ij u ljusci od $\{i, j, 1\}$ tj. $ij = \alpha + \beta i + \gamma j$ za $\alpha, \beta, \gamma \in F$, onda $(i - \gamma) j = \alpha + \beta i$
$\in F^*$ $\in E$

implicira $j \in E$ što ne može biti. Dakle $\{1, j, i, ij\}$ je baza za H.

Još $-ij = ji$ slijedi $j^2 i j^{-2} = j(-ij) j^{-2} = -j i j^{-1} = -(-i) = i$

$\Rightarrow j^2$ je u centru $\Rightarrow j^2 = b \in F$. Očito je $H = E + Ej$.

Def. 2. Neka je $\{1, i, j, k\}$ standardna baza za $\mathbb{H}$. Elemente potprostora $\mathbb{H}_0$ razapetog s $\{i, j, k\}$ zovemo čistim kvaternionima od $\mathbb{H}$.

Pokazat ćemo da $\mathbb{H}_0$ ne ovisi o izboru standardne baze.

Propozicija 1 Ne-nul element $x \in \mathbb{H}$ je čisti kvaternion ako i samo ako $x \notin F$ i $x^2 \in F$.

Dokaz: Neka je $\{1, i, j, k\}$ standardna baza za $\mathbb{H} = \left(\frac{a, b}{F}\right)$. Neka je $x \in \mathbb{H}$, $x \neq 0$. Tada je $x = a_0 + a_1 i + a_2 j + a_3 k$ gdje je $a_i \in F$.

Tada je $x^2 = (a_0^2 + a a_1^2 + b a_2^2 - ab a_3^2) + 2a_0(a_1 i + a_2 j + a_3 k)$.

Ako je $x \in \langle i, j, k \rangle$, onda je $a_0 = 0$ pa je $x^2 \in F$, tj. $x \notin F$.

Obratno, pretpostavimo da $x \notin F$ i $x^2 \in F$. Tada je jedan od a_1, a_2 i $a_3 \neq 0$

pa je nužno $a_0 = 0$, odnosno x je čisti kvaternion. ∎

Dakle, svaki $x \in H$ ima jedinstvenu dekompoziciju $x = a + \alpha$ gdje je

$a \in F$ i $\alpha \in H_0$.

Def 3. Konjugat od x, u oznaci $\bar{x}$, se definira kao $\bar{x} = a - \alpha$.

Vrijedi: (i) $\overline{x+y} = \bar{x} + \bar{y}$ (ii) $\overline{xy} = \bar{y}\,\bar{x}$ (iii) $\bar{\bar{x}} = x$

(iv) $\overline{rx} = r\bar{x}$ za sve $r \in F$ (v) $\bar{x} = x$ ako i samo ako $x \in F$

Posebno, konjugiranje i involucija na $\mathbb{H}$. U $M_2(F)$

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \text{ odnosno za } M \in M_2(F),\ \bar{M} = \text{adjunkta od } M^t.$$

Def 4. Za $x \in \mathbb{H}$ (redukcirana) norma i (redukcirani) trag od x su elementi $nr(x) = x\bar{x}$ i $tr(x) = x + \bar{x}$.

Napomena: (i) $nr(x)$ i $tr(x)$ su elementi od F

(ii) $nr(xy) = nr(x)\,nr(y) \quad \forall x, y \in \mathbb{H}$

(iii) $tr(ax + by) = a\,tr(x) + b\,tr(y) \quad \forall x, y \in \mathbb{H};\ \forall a, b \in F$

(iv) u $M_2(F)$ norma elementa je jednaka determinanti.

Primjer 3: U dokazu Lagrangeovog teorema (svaki broj se može prikazati kao sumu četiri kvadrata) se javlja "čudan" identitet koji pokazuje da se produkt brojeva koji se mogu prikazati kao suma 4 kvadrata također može prikazati kao suma 4 kvadrata.

Kakve veze ima taj identitet s kvaternionskim algebrama?

Kada je $H_{/F}$ izomorfna s $M_2(F)$?

Def. 5 Za $x \in H^*$ kažemo da je izotropan ako je $nr(x) = 0$.

Teorem 6 Za $H = \left(\frac{a,b}{F}\right)$ sljedeće je ekvivalentno:

(a) $H \cong \left(\frac{1,1}{F}\right) \cong M_2(F)$

(b) H nije divizorska algebra

(c) H ima izotropan element

(d) H_0 ima izotropan element

(e) Jednadžba $ax^2 + by^2 = 1$ ima rješenje $(x, y) \in F \times F$.

(f) Ako je $E = F(\sqrt{b})$, onda je

$a \in N_{E/F}(E)$

↑ norma proširenja polja.

Dokaz: Teorem 5. a) implicira (a) $\Leftrightarrow$ (b).

Pretp. da H nije divizorska algebra. Tada postoji $x \in H^{\#}$ koji nije invertibilan.

pa je $nr(x) = 0$ (jer bi inače $\frac{\overline{x}}{nr(x)}$ bio inverz od x). Dakle (b) $\Rightarrow$ (c)

Za (c) $\Rightarrow$ (d) neka je $x \in H$ izotropan element. Neka je $\{1, i, j, k\}$ standardna

baza za H i neka je $x = a_0 + a_1 i + a_2 j + a_3 k$. Ako pretp. da je $a_0 \neq 0$

onda je još barem jedan od a_1, a_2 i a_3 različit od nule. BSO $a_1 \neq 0$.

Iz $nr(x) = 0$ dobivamo $a_0^2 - b a_2^2 = a(a_1^2 - b a_3^2)$

✓ od kuda ovo?

Neka je $y = b(a_0 a_3 + a_1 a_2) i + a(a_1^2 - b a_3^2) j + (a_0 a_1 + b a_2 a_3) k$.

Vrnjeh $nr(y) = 0$. Ako je $y \neq 0$ onda smo gotovi. Ako je $y = 0$, onda je

poseben $-a a_1^2 + ab a_3^2 = 0$ pa je $nr(a_1 i + a_3 k) = 0$.

Kako je $a_1 \neq 0$, $a_1 i + a_3 k$ je izotropni element u H_0.

Za (d) $\Rightarrow$ (e), neka je $a_1 i + a_2 j + a_3 k$ izotropni element u H_0.

Tada je $-a a_1^2 - b a_2^2 + ab a_3^2 = 0$. Ako je $a_3 \neq 0$ onda

$$a\left(\frac{a_2}{a a_3}\right)^2 + b\left(\frac{a_1}{b a_3}\right)^2 = 1.$$ Slično i ako je $a_3 = 0$ (d.z.).

Za (e) $\Rightarrow$ (f), pretp. da je $ax_0^2 + by_0^2 = 1$. Ako je $x_0 = 0$ onda

tvrdnja (f) trivijalno vrijedi. Ako je $x_0 \neq 0$ onda je

$$N_{E/F}\left(x_0^{-1} + x_0^{-1} y_0 \sqrt{b}\right) = a.$$

Za (f) $\Rightarrow$ (h) pretpostavimo da je a norma su $F(\sqrt{b}) \longrightarrow F$.

Ako je $b = c^2$ za neki $c \in F$, onda je $(c+j)(c-j) = b - b = 0$ pa

H nije divizorska algebra, pa možemo pretpostaviti da $\sqrt{b} \notin F$.

Tada je $a = x_1^2 - by_1^2$ za neke $x_1, y_1 \in F$, odnosno

$\operatorname{nr}(x_1 + i \cdot y_1 j) = 0$ pa i u ovom slučaju H nije divizorska algebra.