Nastavak: lokalno-globalni princip

Def. 9. Neka je H/F kvaternionska algebra. Kažemo da se H cijepa nad mjestom v (place) polja F ako i samo ako se $H_v := H \otimes_F F_v$ cijepa nad F_v. Ako je H_v divizijska algebra (valuacijska), onda kažemo da se H ramificira nad v. (račva)

Sa $\mathrm{Ram}(H)$ označavamo skup svih mjesta nad kojima se H ramificira (to je, kao što ćemo vidjeti) konačan skup.

Prva primjena globalnog lokalnog principa je sljedeći teorem.

Teorem 11: Neka su H i H' kvaternionske algebre nad F.

Vrijedi $H \simeq H'$ ako i samo ako $\mathrm{Ram}(H) = \mathrm{Ram}(H')$.

Napomena: Znamo da je prsten endom. s.s.e.k. maksimalni red u kv. algebri $B_{\infty,p}$ koji se ramificira u ∞ i p. Sada vidimo da je ta algebra jedinstvena do na izomorfizam.
$/\mathbb{Q}$ jedno

Cilj ostatka ovog odjeljka je razumjeti ovaj teorem bez ulaženja u prevelike detalje.

Na prethodnim predavanjima smo vidjeli da se cijepanje $\left(\frac{a,b}{F}\right)$ može okarakterizirati preko toga je li a norma nekog elementa iz $F(\sqrt{b})$.

(globalna)

Zato nam je važan sljedeći teorem iz alg. teorije brojeva.

Teorem 12: (Hasseov teorem o normi) Neka je K/F ciklično proširenje polja alg. brojeva. Tada je $a \in F$ globalna norma akko i samo akko je a lokalna norma za svaki $v \in \Omega_F$.

$a \in \mathrm{Im}\left(N_{K_w/F_v}\right)$, $w \mid v$

Nas će zanimati samo slučaj kada je K/F kvadratno proširenje.

Neka je $K = F(\sqrt{\delta})$ gdje je $\delta \in F - F^2$. Tada je $N(x + \sqrt{\delta}\, y) = x^2 - \delta y^2$, $x, y \in F$.

$a \in F$ je globalna norma ako postoji $x + \sqrt{\delta}\, y \in K$ t.d. $N(x + \sqrt{\delta}\, y) = a$, pa

prethodni teorem zapravo kaže da jednadžba $x^2 - \delta y^2 = a$ ima

rješenja u $F + F$ ako i samo ako ima rješenja u F_v za svaki $v \in \Omega_F$.

Uočimo da jednadžba sigurno ima rješenja ako je δ kvadrat u F

(jer jednadžba $x^2 - y^2 = (x-y)(x+y) = a$ uvijek ima rješenje)

Zato je dobro znati i za sljedeći teorem.

Teorem 13. Neka je $\sigma \in F$ gdje je F polje broja. Tada je σ kvadrat u F akko i samo akko je σ kvadrat u F_v za gotovo sve $v \in \Omega_F$.

Prisjetimo se terminologije vezane u kvadratne prostore...

Ako je v mjesto od F, za kvadratni prostor (V, Q), sa V_v označavamo kvadratni prostor $F_v \otimes_F V$ s kvadratnom formom

$Q_v(a \otimes x) = a^2 Q(v)$ $\forall a \in F_v$ (proširenje skalara, prirodna definicija)

Teorem 14 (Hasse-Minkowski) Neka je F polje alg. brojeva.

(a) Neka je V nedegeneriran kvadratni prostor nad poljem brojeva F.

Tada je V izotropan ako i samo ako je V_v izotropan

za sva mjesta v.

(b) Neka su V i W nedegenerirani kvadratni prostori nad F.

Tada su V i W izomorfni ako i samo ako su V_v i W_v

izomorfni za sva mjesta v od F.

Skica dokaza:

a) BSOMP postoji $v_1 \in V$ t.d. $Q(v_1) = 1$. Proširimo v_1 do $\{v_1, \dots, v_m\}$.

ortogonalnu bazu za V (to možemo napraviti iako to nismo dokazali)

Dokaz ide indukcijom po n. Ako je $n=2$, tada postoji $\delta \in F^*$

takav da je $Q(v)$ oblika $x^2 - \delta y^2$ $(x, y \in F)$ za sve $v \in V$.

$\delta = Q(v_2)$ $\qquad$ $v = x \cdot v_1 + y \cdot v_2$

pretpostavimo: Ako je $\{v_1, \dots, v_m\}$ ortog. baza s $Q(v_i) = a_i$ onda

za $v = \sum x_i v_i$ vrijedi $Q(v) = \sum a_i x_i^2$ (dokažite to!)

Sada je jasno da je V izotropan ako i samo ako je $-\delta$ kvadrat u F.

Prema prethodnom teoremu slijedi da je V izotropan ako i samo ako je $-\delta$ kvadrat u F_v za svaki v, odnosno ako je V_v izotropan za svaki v.

Ako je $n=3$, onda kvadratna forma ima oblik $x^2 + \delta y^2 + \gamma z^2$.

Možemo pretpostaviti da $-\delta$ nije kvadrat u F (zašto?). Tada je V izotropan ako i samo ako je $-\gamma$ norma nekog elementa iz $F(\sqrt{-\delta})$.

Iz Hasseovog teorema o normi slijedi tvrdnja u ovom slučaju.

Za korak indukcije možete pogledati str. 187 u O'Meara: Introduction to quadr. forms

(h) dio preskačemo

Def. 10. Neka je v mjesto od F. Za $a, b \in F_v^*$ definiramo Hilbertov simbol

$$(a,b)_v = \begin{cases} 1 & \text{ako } ax^2+by^2=1 \text{ ima rješenje u } F_v \\ -1 & \text{inače.} \end{cases}$$

Znamo da je $(a,b)_v = 1$ ako i samo ako se algebra $\left(\frac{a,b}{F_v}\right)$ cijepa.

Za gotovo sve v a i b su iz $\mathcal{O}_v^*$ (tj. nisu "djeljivi" s v), pa je $(a,b)_v = 1$

↗

Za gotovo sve v.

zašto? znamo za zadnji predavanje da slika norme neracionalnog proširenja sadrži sve (invertibilne) elemente iz prstena cijelih (to nismo dokazivali). Pa za $a, b \in \mathcal{O}_v^*$ vrijedi da je b norma nekog elementa iz $F_v(\sqrt{a})/F_v$.

→

ovo je racionalan broj jer je $a \in \mathcal{O}_v^*$? ne baš! d.z.

Općenitu imamo ovaj teorem.

npr. $\mathbb{Q}_p$ za $p \neq 1$.

Teorem 15. Neka je F padski polje čije je polje "ostataka" repome karakteristike.

Neka je $H = \left(\frac{a,b}{F}\right)$ za $a, b \in \mathcal{O}_F$.

a) Ako $a, b \in \mathcal{O}_F^*$, onda se H cijepa.

b) Ako $a \in \mathcal{O}_F^*$ i $b \in p\mathcal{O}_F - p^2\mathcal{O}_F$ onda se H cijepa

ako i samo ako je a kvadrat.

c) Ako $a, b \in p\mathcal{O}_F - p^2\mathcal{O}_F$, onda se H cijepa ako i samo ako

$-a^{-1}b$ kvadrat.

Teorem 16 (Hilbertov zakon recipročnosti) Neka su $a, b \in F^*$.

Tada $\prod_v (a,b)_v = 1$, gdje produkt ide po svim mjestima od F.

Napomena: a) Ako je F u kompleksnom mjestu, onda se F_v ničim ne razlikuje.

b) $\#\mathrm{Ram}(H)$ je paran.

Teorem 17. Neka je H/F kv. alg. Tada se H cijepa nad F akko i samo ako se H_v cijepa nad F_v za svako mjesto v.

Dokaz: Znamo da se H cijepa nad F akko i samo akko je H_0 izotropan.

Prema Hasse-Minkowski teoremu a) H_0 je izotropan akko i samo akko su $H_{0,v}$ izotropni za sva mjesta v što je opet ekvivalentno tome da se H_v cijepa za svaki v.

Dokaz Teorema 11: Znamo da su H i H' izomorfni akko i samo akko su kvadratni prostori H_0 i H'_0 izometrični. Po Hasse-Minkowski teoremu H_0 i H'_0 su izometrični akko i samo akko su $(H_0)_v$ i $(H'_0)_v$ izometrični za svako mjesto v. $\uparrow$ N_0, kako imamo samo konačno mnogo klasa neizom. kv. algebri nad lokalnim poljima, slijedi da su H i H' izomorfni nad svim mjestima akko i samo akko se cijepaju ili oboje ramificiraju.

ili izomorfni (sinonimi!)

Redovi u kvaterniomskim algebrama

pomaljajmo alg. teoriji brojeva

- F je polje alg. brojeva ili p-adsko polje.
- $\mathcal{O}_F$ prsten cijelih
- $\mathcal{I}_F$ = skup konačno-generiranih $\mathcal{O}_F$ - podmodula od F

$\mathcal{I}_F$ sadrži "obične" ideale od $\mathcal{O}_F$, zovemo ih - cijeli ideali

↑ elementi se zovu razlomljeni ideali (fractional ideals)

- neka su $\alpha, \beta \in \mathcal{I}_F$ takvi da
  - a) $\alpha\beta$ = $\mathcal{O}_F$-modul (konačno) generiran s produktima oblika ab za $a \in \alpha$, $b \in \beta$
  - b) $\alpha^{-1} = \{x \in F : x\alpha \subseteq \mathcal{O}_F\}$ inverz

↑ takvi razlomljeni ideali ←

- $\mathcal{I}_F$ je grupa u odnosu na množenje (neutralni element je $\mathcal{O}_F$)

- I_F je slobodna abelova grupa generirana prostim idealima

  tj. $\alpha = p_1^{a_1} \cdots p_t^{a_t}$ ⇝ jedinstvena faktorizacija

- P_F = skup glavnih ideala oblika $\alpha \mathcal{O}_F$, $\alpha \in F^*$; $P_F < I_1$
- P_F / I_F = grupa klasa ideala ← konačna grupa

  ← red grupe se zove broj klasa

Def. 11. Neka je V k.d.v.p. nad F. **$\mathcal{O}_F$-rešetka** u V je konačno generirani $\mathcal{O}_F$-modul sadržan u V. Kažemo da je $\mathcal{O}_F$-rešetka **potpuna** ako je $L \otimes_{\mathcal{O}_F} F = V$ (tj. $FL = V$).

Primjer 5. a) $F = \mathbb{Q}$, $V = \mathbb{Q}^2$, $\langle (1,0), (0,1) \rangle$ je $\mathbb{Z}$-rešetka u V

↑ $\mathbb{Z}$-modul generiran s $(1,0)$ i $(0,1)$

b) $\langle (1,0), (\pi,0) \rangle$ nije rešetka jer $(1,0)$ i $(\pi,0)$ jesu linearno nezavisni nad $\mathbb{Q}$ ne čine bazu za V.

Napomena: Nekad se u definiciji rešetke zahtijeva potpunost.

Od sada nadalje svuda v.p. je konačno dim nad F i svuda rešetka je $\mathcal{O}_F$-rešetka.

Budući da je $\mathcal{O}_F$ Dedekindova domena svaka rešetka $L \subset V$ se može zapisati kao $L = \mathcal{O}_F x_1 \oplus \dots \oplus \mathcal{O}_F x_{n-1} \oplus \underline{\mathfrak{a} x_n}$ za neke $x_i \in V$ i razlomljeni ideal $\mathfrak{a}$.

zašto?

Teorem 18: Neka je L potpuna rešetka i V i M^{cV} $\mathcal{O}_F$ - modul.

Tada je M potpuna rešetka ako i samo ako postoji $a^{\times 0} \in or$

t.d. $aL \subseteq M \subseteq a^{-1}L$.

Def. 12. Neka je H/F ku. algebra. $\mathcal{O}_F$ - **ideal** u H je potpuna $\mathcal{O}_F$ - rešetka u H. **Red** u H je $\mathcal{O}_F$ - ideal koji je i prsten.

Maksimalan red je red koji je maksimalan u odnosu na inkluziju.

Neka je I ideal u H (ako ne preciziramo, pretp. da je $\mathcal{O}_F$-ideal).

Sa

$$\mathcal{O}_\ell(I) = \{\alpha \in H : \alpha I \subset I\} \quad i \quad \mathcal{O}_r(I) = \{\alpha \in H : I\alpha \subseteq I\}$$

označavamo njima pripadan lijevi red i desni red.

Propozicija 3 Ako je I ideal u H, onda su $\mathcal{O}_\ell(I)$ i $\mathcal{O}_r(I)$ redovi u H.

Dokaz: Dokazujemo tvrdnju za $\mathcal{O}_\ell(I)$. Očito je $\mathcal{O}_\ell(I)$ $\mathcal{O}_F$-modul i prsten.

Dokažimo da je konačno-generiran (tj. rešetka) i $F\mathcal{O}_\ell(I) = H$ (potpuna rešetka).

Budući da je I potpuna rešetka, $1 = \sum a_i v_i$ gdje su $a_i \in F$ i $v_i \in I$ pa

postoji $s \in \mathcal{O}_F$ t.d. $s \cdot 1 \in I$. Tada $\mathcal{O}_\ell(I)(s \cdot 1) \subset I \Rightarrow \mathcal{O}_\ell(I) \subset s^{-1} I$

konačno generiran!

Za potpunost, neka je $y \in H$. Tada je yI rešetka u H pa postoji

$\overset{+}{a} \in G_F$ t.j. $ayI \subset I \Rightarrow ay \in G_e(I) \Rightarrow y \in a^{-1} G_e(I) \subset F G_e(I)$. ∎

zašto? jer je G konačno generiran i G_F Noeth. prsten

Neka je G red u H. Svaki element od G je cijeli nad G_F. d.z.

Općenito, neka je $\alpha \in H$ cijeli nad G_F. Budući da je

karakter. polinom nekim potprstenima

$\alpha^2 - \mathrm{tr}(\alpha)\alpha + \mathrm{nr}(\alpha) = 0$ slijedi da su $\mathrm{tr}(\alpha), \mathrm{nr}(\alpha) \in G_F$.

Propozicija 4. Neka je G potprsten od H. Tada je G red u H

akko i samo akko G sadrži G_F, $FG = H$ i G je cijeli nad G_F.

Sada primjenom Zornove leme dokazujemo (presjek ...)

Korolar 3 Svaki red u H je sadržan u nekom maksimalnom redu.

Dokaz Propozicije 4 $\Rightarrow$ očito iz prethodne dekomp.

budući da $G_F \subset G$ slijedi da je G G_F-modul

$\Leftarrow$ Neka je $\{x_1, x_2 x_3, x_4\}$ baza za H t.d. $x_i \in G$ $\forall i$.

↑ postoji jer $FG = H$

preostaji dokazati konačnu generiranost

H zajedno s simetričnom bilinearnom formom tr je nedegeneriran kvadratni prostor. $\Rightarrow$ $d = \det(tr(x_i x_j)) \neq 0$. Neka je L ideal razapet s x_i-ovima (dakle $L \subseteq G$). Dokazat ćemo $0 \subseteq d^{-1} L$ iz čega će slijediti konačna generiranost od G.

$(x,y) \mapsto tr(xy)$

Neka je $\alpha \in G$. Tada postoji $b_i \in F$ t.d.

$$\alpha = \sum_{i=1}^{4} b_i x_i .$$

Za svaki j, $\alpha x_j \in G$ pa (bilinearnost tragen)

$$tr(\alpha x_j) = \sum_{i=1}^{4} b_i \, tr(x_i x_j) \in G_F$$

jer je $\alpha x_j \in G$ cijeli nad G_F pa i $tr(\alpha x_j) \in G_F$

$\in G_F^4$

$\cdot$ tj. $\begin{bmatrix} tr(x_1x_1) & tr(x_1x_2) & \cdots & tr(x_1x_4) \\ \vdots & & & \\ & & & tr(x_4x_4) \end{bmatrix}^T \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} tr(\alpha x_1) \\ tr(\alpha x_2) \\ tr(\alpha x_3) \\ tr(\alpha x_4) \end{bmatrix}$

$\in G_F$

iz čega, rješavanjem sustava, dobivamo $b_i \in d^{-1} G_F$

odnosno budući da je α proizvoljan $G \subseteq d^{-1} L$ ▨

Inače, skup svih elemenata iz H koji su cijeli nad G_F nije nužno red.

Npr. ako $H = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ i standardna baza $\{1, i, j, k\}$, onda

$\alpha = i$ i $\beta = \frac{3i+4j}{5}$ su cijeli nad $\mathbb{Z}$, ali $\alpha\beta$ i $\alpha+\beta$

nisu cijeli nad $\mathbb{Z}$.

Ako je G red u H i $\alpha \in H^\times$, tada je $\alpha G \alpha^{-1}$ također red u H.

Konjugat maksimalnog reda je također maksimalan.

Lokalizacija:

H/F ku. algebra ; $\mathfrak{P} \subset \mathcal{O}_F$; $H_{\mathfrak{P}} := H \otimes_F F_{\mathfrak{P}}$

$L \subset H$ rešetka, $L_{\mathfrak{P}} := L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_{\mathfrak{P}}} \subset H_{\mathfrak{P}}$ rešetka u $H_{\mathfrak{P}}$

$\mathcal{O} \subset H$ red, $\mathcal{O}_{\mathfrak{P}} := \mathcal{O} \otimes_{\mathcal{O}_F} \mathcal{O}_{F_{\mathfrak{P}}}$ i $\mathcal{O}_{F_{\mathfrak{P}}}$ - red u $H_{\mathfrak{P}}$

Fiksirajmo $\mathcal{O}_F$ - ideal I u H. Neka je $\mathcal{J}$ skup svih $\mathcal{O}_F$ - ideala u H te neka je $\mathcal{I}$ skup svih nizova $(L_{\mathfrak{P}})_{\mathfrak{P}}$ takvih da je $L_{\mathfrak{P}}$ $\mathcal{O}_{F_{\mathfrak{P}}}$ - ideal u $H_{\mathfrak{P}}$ za sve $\mathfrak{P} \in \Omega_f$ i $L_{\mathfrak{P}} = I_{\mathfrak{P}}$ za gotovo sve $\mathfrak{P}$.

Propozicija 5 Preslikavanje $J \longmapsto (J_p)_p$ je bijekcija s $\mathcal{Y}$ na $\mathcal{I}$.

Korolar 4: Neka je G G_F-rel u H/F. Tada je G maksimalan ako i samo ako je G_p maksimalan G_{F_p}-rel u H_p za sve $p \in \Omega_f$.

Skica dokaza Propozicije 5: Uočimo prvo da je preslikavanje

dobro definirano jer postoji $a, b \in F^*$ t.d. $a\mathfrak{J} \subseteq I \subseteq b\mathfrak{J}$ (zašto?)

pa za sve osim konačno mnogo p-va $a, b \in \mathcal{O}_{F_\mathfrak{P}}^*$, tj. $\mathfrak{J}_\mathfrak{P} = I_\mathfrak{P}$.

Obratno, pretpostavimo da je dan niz $(I_\mathfrak{P})_\mathfrak{P}$ iz $\mathcal{I}$.

Za ostatak argumenta trebat će nam još jedna "vrsta" lokalizacije...