Definicija Selmerove grupe:

e.g. $\phi = [m]$, $E' = E$

Neka je $\phi : E \to E'$ izogenija nad K kao i ranije.

Imamo sljedeći komutativni dijagram

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\phi(E(K)) \arrow[r, "\delta"] \arrow[d] & H^1(G_K, E[\phi]) \arrow[r] \arrow[d] & WC(E/K)[\phi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_{v \in M_K} E'(K_v)/\phi(E(K_v)) \arrow[r, "(\delta_v)_v"] & \prod_v H^1(G_v, E[\phi]) \arrow[r] & \prod WC(E/K_v)[\phi] \arrow[r] & 0
\end{tikzcd}$$

gdje smo identificirali $H^1(G_K, E)[\phi] \simeq WC(E/K)[\phi]$

ϕ-Selmerova grupa od E/K je podgrupa od $H^1(G_K, E[\phi])$ definirana s

$$S^{(\phi)}(E/K) = \ker\left\{ H^1(G_K, E[\phi]) \longrightarrow \prod_{v \in M_K} WC(E/K_v) \right\}$$

ili ekvivalentno, $S^{(\phi)}(E/K)$ se sastoji od klasa u $H^1(G_K, E[\phi])$ čija restrikcija na G_v se nalazi u slici lokalnog Kummerovog preslikavanja, za svaki $v \in M_K$.

Definicija Tate-Shavarevich grupe

$$Ш(E/K) = \ker\left\{ WC(E/K) \to \prod_{v \in M_K} WC(E/K_v) \right\}$$

(do na ekvivalenciji)

podgrupa homogenih prostora od E/K koji su lokalno svugdje njišni, a koji nemaju (osim trivijalne klase) K-racionalnu točku.

Teorem: Postoji egzaktni niz

a) $$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to$$

$$\to Ш(E/K)[\phi] \to 0$$

b) $S^{(\phi)}(E/K)$ je konačna

ova tvrdnja implicira slabi MW teorem ako uzmemo $\phi = [2]$

Komentari:

1. Tate-Shaf. slutnja kaže da je $\text{Ш}(E/K)$ konačna (red te grupe se javlja u iskazu BSD slutnje).

   Kolyvagin je to dokazao za $E/\mathbb{Q}$ analitičkog ranga ≤ 1.

   uz neke uvjete; npr vrijedi za K = totally real

   $\# \text{Ш}(E/K) < +\infty \overset{}{\Longrightarrow}$ the Parity conjecture

2. $$0 \to \underbrace{E(K)/\phi(E'(K))}_{\text{teško}} \to \underbrace{S^{(\phi)}(E/K)}_{\text{lako}} \to \underbrace{\text{Ш}(E/K)[\phi]}_{\text{teško}} \to 0$$

Ako je $\text{Ш}(E/K)[m] = \{0\}$ onda je

$$\operatorname{rank}_{\mathbb{F}_m} E(K)/mE(K) = \operatorname{rank}_{\mathbb{F}_m} S^{(m)}(E/K)$$ što nam

daje postupak za računanje $\operatorname{rank} E(K)$.

Ako je $\text{Ш}(E/K)$ konačna onda takav m uvijek postoji. Na ovu tvrdnju možemo gledati kao na "generalizaciji" lokalno - globalnog principa za krivulji genusa 0 koji kaže da krivulja ima K-racionalnu točku ako i samo ako ima K_v-rac. točku za svaki v.

Na kraju, sve što znamo reći o K-racionalnim točkama slijedi iz mod p rješenja nekih jednadžbi (može ih biti puno).

Osim onog što se zna o BSD slutnji (Heegnerove točke i modularna parametrizacija)

Dokaz teorema: (a) slijedi direktno iz definicije

(b)

Za dokaz će nam trebati sljedeća definicija

Def (unramified class)

K je lokalno polje (e.g. K_v)

Neka je M konačan G_K-modul. Tada je

unramified cohomology

klase koje "iščezavaju" na inercijskoj podgrupi

$$H^1_{nr}(G_K, M) := \ker\left(H^1(G_K, M) \xrightarrow{\text{res}} H^1(G_{K^{un}}, M)\right)$$

gdje je K^{un}/K maksimalno nerazmificirajuće proširenje od K (maximal unramified extension).

vrijedi: $Gal(K^{un}/K) \simeq \hat{\mathbb{Z}}$ dekomp. podgrupa.

Prema infl./restriction nizu

inercijska podgrupa

$$H^1_{nr}(G_K, M) = H^1(G_{K^{un}/K}, M^I)$$

$I = G_{K^{un}}$

nastavak dokaza:

Neka je $\xi \in S^{(\phi)}(E/K)$ i $v \in M_K$ konačno mjesto (place) koji ne dijeli $m = \deg(\phi)$.

Tvrdnja: ξ is unramified at v

Neka je $I_v < G_v$ inercijska podgrupa za v.
Po def. Selm. grupe ξ je trivijalno u $WC(E/K_v) \cong H^1(G_{K_v}, E)$ pa postoji
$P \in E(\overline{K}_v)$ t.d. $\xi_\sigma = \{P^\sigma - P\}$ $\forall \sigma \in G_{K_v}$.

Kako je $\phi(P^\sigma - P) = 0 \Rightarrow P^\sigma - P \in E[\phi]$.

Promotrimo "redukciju modulo v", $E \to \tilde{E}_v$
od $P^\sigma - P$ za $\forall \sigma \in I_v$

$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = \tilde{P}^\sigma - \tilde{P}^\sigma = 0$ jer
po definiciji inercija djeluje trivijalno na $\tilde{E}_v$

$\Rightarrow P^\sigma - P \in E[\phi]$ se nalazi u jezgri redukciji modulo v ali to ne može biti

jer znamo da je redukcija mod v

injektivna na torziji $E[m]^{?\,E[\phi]}$ ako $v \nmid m$.

$\Longrightarrow$ postoji $S \subset M_K$ konačan t.d.

$$S^{(\phi)}(E/K) \subset H^1(G_K, E[\phi]; S)$$

gdje općenito za M konačan G_K-modul

definiramo

$$H^1(G_K, M; S) := \left\{ \xi \in H^1(G_K, M) : \xi \text{ je unramified izvan } S \right\}$$

Dokaz konačnosti Selm. grupe slijedi iz slijedeće propozicije

konačan modul

Propozicija: $H^1(G_K, M; S)$ je konačna

Zbog inflation-restriction niza možemo reducirati propoziciju na slučaj kad G_K djeluje trivijalno na M (polje def. od M je konačno proširenje zbog toga što je djelovanje neprekidno). Tada je

što ovo označava?

$H^1(G_K, M; S) = \mathrm{Hom}(G_K, M; S)$.

Nadalje, neka je m eksponent od M tj. najmanji prirodan broj takav da vrijedi $mx = 0 \ \forall x \in M$ i neka je L/K maksimalno abelovo proširenje od K s eksponentom m koje je unramified za $v \notin S$.

što to znači? zašto?

Tada je prirodno preslikavanje

$$(*)\ \mathrm{Hom}(G_{L/K}, M; S) \longrightarrow \mathrm{Hom}(G_K, M; S)$$

$$f \longmapsto (\sigma \longmapsto \sigma|_L \longmapsto f(\sigma|_L))$$

izomorfizam. zašto?

1°) $H^1(G_K, M; S) = \mathrm{Hom}(G_K, M; S)$ jer

$\mathrm{Hom}(G_K, M; S) = \{\varphi \in \mathrm{Hom}(G_K, M) : \varphi|_{G_v} = id \ \forall v \notin S\}$

2°) L/K je abelovo proširenje eksponenta m ako $G_{L/K}$ ima eksponent m.

3°) zašto je $(*)$ izomorfizam? dokaz surjektivnosti:

za $\varphi \in \mathrm{Hom}(G_K, M; S)$ proizvoljan, $G_v < \ker\varphi \ \forall v \notin S$

$\Rightarrow \langle G_v \rangle_{v \notin S} < \ker\varphi \Rightarrow \varphi$ se

podgrupa generirana podgrupama $G_v, v \notin S$

faktorizira kroz polje $\tilde{L}$ za koji vrijedi

$$\mathrm{Gal}(\bar{K}/\tilde{L}) \simeq \langle G_v \rangle_{v \notin S}$$

a) $\tilde{L}$ postoji zbog osnovnog teorema Galoisove teorije

b) $\tilde{L}$ je unramified za $v \notin S$ jer je $\tilde{L}$ sadržana u $\bar{K}^{G_v}$ jer je

$$\tilde{L} = \left(\bar{K}^{G_v}\right)^{\langle G_w \rangle_{\substack{w \notin S \\ w \neq v}}}$$

c) no za svaki $\varphi : G_K \to M \in \mathrm{Hom}(G_K, M; S)$

$$0 \to \mathrm{Ker}\,\varphi \to G_K \xrightarrow{\varphi} M \to 0$$

$\Rightarrow$ $G_K / \mathrm{Ker}\,\varphi \simeq \mathrm{Im}\, M$ pa je posebno $G_K / \mathrm{Ker}\,\varphi$ abelova grupa eksponenta m.

Dakle, $\mathrm{Ker}\,\varphi$ je nužno "veća" od $\langle G_v \rangle_{v \notin S}$, sadrži najmanju grupu $G < G_K$ koja sadrži $\langle G_v \rangle_{v \notin S}$ te za koju je G_K / G abelova grupa (G je generirana sa svim $G_v, v \notin S$ kao i s njihovim komutatorima). Po definiciji $\bar{K}^G = L$ = maksimalno abelovo proširenje eksponenta m od K unramified izvan S. Dakle, φ se faktorizira kroz $G_{L/K}$. d.z. dokažite injektivnost

Kraj dokaza.

Zbog (*) dovoljno je pokazati da je proširenje L/K konačno.

Propozicija. Neka je K polje alg. brojeva, $S \subset M_K$ t.d. $M_K^\infty \subseteq S$ i $m \geq 2$ prirodan broj. Neka je L/K maksimalno abelovo proširenje od K eksponenta m koje je unramified izvan S. Tada je L/K konačno proširenje.

Dokaz:

1°) Možemo pretpostaviti da $\mu_m \subset K$ jer ako je propozicija točna za neko konačno proširenje K' od K gdje je S' skup mjesta od K' nad S, onda zbog toga što je $LK'/_{K'}$ abelovo eksponenta m, unramified izvan S'

zašto?

$\Rightarrow LK'/K'$ je konačno $\Rightarrow L/K$ konačno zašto?

$$\begin{tikzcd}
 & LK' \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & K' \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

2°) Možemo povećati S (još tako povećavamo L) kako bi prsten S-cijelih od K

$$R_S = \{ a \in K : v(a) \geq 0 \ \forall v \in M_K ,\, v \notin S \}$$

postao domena glavnih ideala.

zašto? Broj klasa od K je konačan, neka su $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ predstavnici. Dodajmo skupu S valuacije koje odgovaraju svim prostim idealima koji dijele neki od $\mathfrak{a}_i$-ova.

Povećajmo još S t.d. $v(m)=0$ $\forall v \notin S$.

Sada koristimo glavni teorem Kummerove teorije:

Teorem: Neka je K polje karakt. 0 i

Neka je L/K neko abelovo proširenje stupnja eksponenta m. Tada postoji podgrupa $\Delta \subseteq K^*/(K^*)^n$ takva da je $L = K(\Delta^{\frac{1}{m}})$ gdje je

$$\Delta^{\frac{1}{m}} := \left\{ \sqrt[m]{a} : a \in K^*, a \cdot (K^*)^n \in \Delta \right\}.$$

Preciznije za Δ možemo uzeti

$$\Delta = (K^* \cap (L^*)^n)/(K^*)^n.$$

$\Delta \cong Gal(L/K)$

Zaključujemo da je L najveće potpolje od $K(\sqrt[m]{a} : a \in K)$ koje je unramified izvan S.

Kako provjeriti ramifikaciju za neki $v \in M_K$?

Općenito $\begin{array}{c} L \\ | \\ K \end{array}$ je neramificiran nad v ako

je L_v/K_v neramificiran.

za neki $v \in M_L$
iznad $v \in M_K$

Konkretno, zanima nas kada je $K_v(\sqrt[m]{a})/K_v$ neramificirana.

Neka je $\pi \in \mathcal{O}_{K_v}$ generator i neka je $a = u \cdot \pi^n$ gdje je $u \in \mathcal{O}_{K_v}^*$.

Tada je maksimalni ideal u $\mathcal{O}_{K_v(\sqrt[m]{a})}$ generiran s $\pi^{n/m}$ pa ako $m \nmid n$ onda imamo ramifikaciju u faktorizaciji ideala (π) u $\mathcal{O}_{K_v(\sqrt[m]{a})}$.

Natrag na dokaz, neka je

$$T_S = \{a \in K^*/(K^*)^m : v(a) \equiv 0\ (m)\ \forall v \in M_K \text{ i } v \notin S\}.$$

Tada je $L = K(\sqrt[m]{a} : a \in T_S)$.

$\Rightarrow$ potrebno je još dokazati da je skup T_S konačan

Promotrimo prirodno preslikavanje

$$R_S^* \to T_S.$$

Dokažimo da je surjekcija. Pretp. da $a \in K^*$ reprezentira neki element od T_S.

Tada je ideal aR_S m-ta potencija nekog ideala u R_S jer je $v(aR_S) \equiv 0(m)$ za sve valuacije v od R_S (što su valuacije v od $\mathcal{O}_K$ za koje $v \notin S$). Budući da je R_S prsten jedinstvene faktorizacije postoji $b \in K^*$ t.d. $aR_S = b^m R_S$ pa postoji $u \in R_S^*$ t.d.

$$a = u \cdot b^m \Rightarrow a \equiv u \bmod T_S$$

$\Rightarrow R_S^* \to T_S$ je surjekcija

Nadalje, jezgra preslikavanja sadrži $R_S^{\times m}$

pa imamo surjekciju

$$R_S^{\times}/R_S^{\times m} \longrightarrow T_S \longrightarrow 0$$

Po Dirichletovom teoremu za S-jedinice

$R_S^{\times}$ je konačno generirana grupa.

$\Rightarrow T_S$ je konačan

$\boxtimes$