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

$$\begin{array}{ccccccccc}
0 \to & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_K, E[\phi]) & \to & Ш(E/K)[\phi] & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \prod_{v\in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{(\delta_v)_v} & \prod_v H^1(G_v, E[\phi]) & \to & \prod_{v\in M_K} Ш(E/K_v)[\phi] & \\
 & & & & & & \to 0
\end{array}$$

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

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

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

ili ekvivalentno, $S^{(\phi)}(E/K)$ se sastoji od klasa iz $H^1(G_K, E[\phi])$ čija restrikcija na G_v se anulira u svim lokalnom Kummerovom preslikavanju, za svaki $v \in M_K$.

Definicija Tate-Shavarevich grupe

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

(do na ekvivalenciji)

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

Teorem: Postoji egzaktni niz

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

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 Ш(E/K) konačna (red te grupe se javlja u iskazu BSD slutnji).

Kolgyagin je to dokazao za E/Q analitičnog ranga ≤ 1.

za neke ciklične; npr. kvadratne za K = totally real

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

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

↑ teško — ↑ lako — ↑ teško

Ako je $Ш(E/K)[m] = \{0\}$ onda je

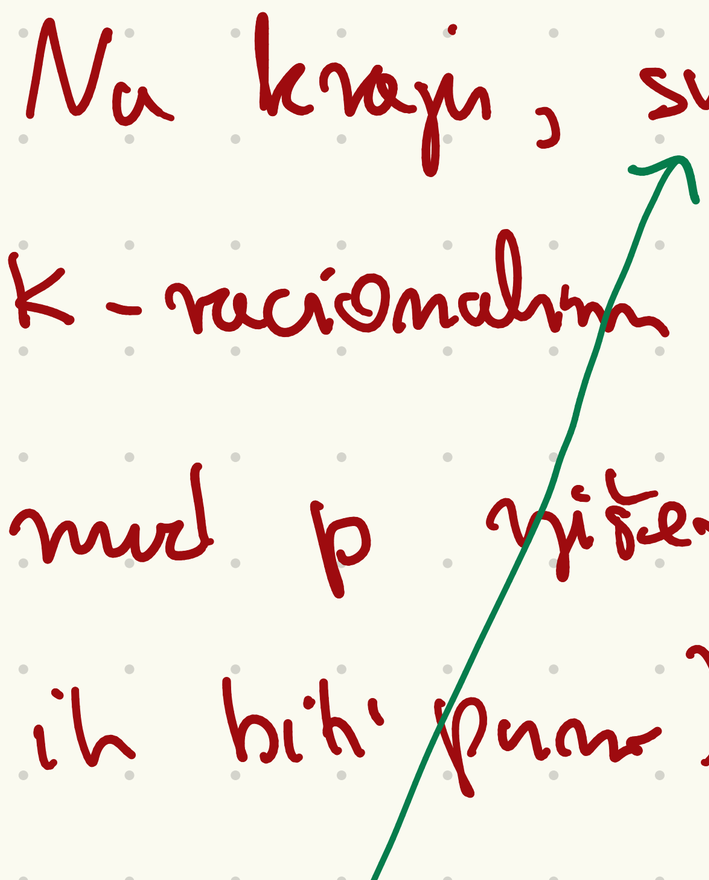
$\operatorname{rank}_{\mathbb{F}_m} E(K)/mE(K) = \operatorname{rank}_{\mathbb{F}_m} S^{(m)}(E/K)$ što nam

daje postupak za računanje rank $E(K)$.

Ako je $Ш(E/K)$ konačna onda takav m

uvijek postoji. Na ovu tvrdnju možemo

sledeći korak na "generalizaciji" lokalno - globalnog principa za konveksni genus 0 koji kaže da konveksni skup k-racionalnih točki ako i samo ako ima k-vec. točki za svaki v-



Na kraju, sve što znamo reći o k-racionalnim točkama skupa iz mod p veličine nekih jednadžbi (može ih biti puno).

Osim onog što se zna o BSD slutnji (Integerman teže i' molekularna parametrizacija)

Dokaz teorema: (a) slijedi direktno iz definicije

(b)

Za dokaz će nam trebati slijedeća definicija

Def (unramified class)

Neka je K je lokalno polje (e.g. K_v)

M konačan G_K-modul. Tada je

$$\hat{H}^r_{nr}(G_K, M) := \text{unramified cohomology}$$

klase koje "iščezavaju" na inercijskoj podgrupi

$$\ker\left(H^r(G_K, M) \xrightarrow{\text{res}} H^r(G_{K^{un}}, M) \right)$$

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

(maximal unramified extension) $\rightarrow$ dekomp. podgrupa

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

Prema inf./restrikcija niza

inercijska podgrupa

$$\hat{H}^r_{nr}(G_K, M) = H^r(G_{K^{un}/K}, M^I)$$

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

nastavak dokaza:

Neka je $\xi \in S^{(\phi)}(E/K)$ i $v \in M_K$ konačno

mjesto (place) koje 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 trivijalna

u $WC(\tilde{E}/K_v) \simeq H^1(G_{K_v}, E)$ pa postoji

$P \in E(\bar{K}_v)$ t.d. $\zeta_\sigma = \{P^\sigma - P\}\ \forall \sigma \in G_{K_v}$.

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

Promotrimo "redukciju modulo v", $E \to \tilde{E}_v$

ovdje $P^\sigma - P$ za $\forall \sigma \in I_v$

$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = \tilde{P}^\sigma - P^\sigma = O$ jer

po definiciji inercija djeluje trivijalno na $\tilde{E}_v$

$\Rightarrow P^\sigma - P \in E[\phi]$ se nalazi u jezgri

redukcija modulo v ali to ne može biti

jer znamo da ju redukcija mod v

injektivna na torziji: $E[m]^{E[\phi]} \to E/\mathfrak{p}[m]$.

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

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

gdje općenito za M konačan G_K-modul

definiramo

$$H^1(G_K, M; S) := \{ \} \in H^1(G_K, M) : \} \text{ je}$$

unramified izvan S \}

Dokaz konačnosti Selm. grupe slijedi iz

slijedeće propozicije

konačan modul

↓

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

Zbog inflation-restriction niza možemo

reducirati propoziciju na slučaj kad

G_K djeluje trivijalno na M (poli

def. od M je konačan proširenje zbog toga

što je djelovanje neprekidno). Tada je

što ovo označava?

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

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 ji prirodno preslikavanje

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

izomorfizam. zašto?

$f \mapsto (\sigma \mapsto \sigma_L \mapsto f(\sigma_L))$

1°) $H^1(G_K, M; S) = Hom(G_K, M; S)$ jer

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

2°) L/K je abelovo proširenje eksponenta m ← inercijalna podgrupa $I(\bar{K}_v/K_v)$

ako $G_{L/K}$ ima eksponent m.

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

za $\varphi \in Hom(G_K, M; S)$ proizvoljan, $I_v \subset \ker\varphi \ \forall v \notin S$

$\Rightarrow \langle I_v \rangle_{v \notin S} \subset \ker\varphi \Rightarrow \varphi$ se

faktorizira kroz polje $\tilde{L}$ za koje vrijedi ← podgrupa generirana podgrupama $G_{v,v\notin S}$

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

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

b) $\tilde{L}$ je unramified za $v \notin S$ jer

je $\tilde{L}$ sadržana u $\overline{K}^{I_v}$ jer je

$$\tilde{L} = \left(\overline{K}^{I_v}\right)^{\langle I_w \rangle_{\substack{w \notin S \\ w \neq v}}}$$

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

$$0 \to \ker\varphi \to G_K \xrightarrow{\varphi} M \to 0$$

$$\Rightarrow G_K/\ker\varphi \simeq \mathrm{Im}\, M$$ pa je poseban

$G_K/\ker\varphi$ abelova grupa eksponenta m

Dalje, $\ker\varphi$ je manje "veća" od $\langle I_v \rangle_{v \notin S}$,

sadrži najmanju grupu $G < G_K$

koja sadrži $\langle I_v \rangle_{v \notin S}$ te za koju je G_K/G

abelova grupa (G je generirana sa svim I_v, $v \notin S$

kao i s njihovim komutatorima). Po definiciji

$\overline{K}^G \simeq L \simeq$ maksimalno abelovo proširenje eksponenta m od K

unramificirano izvan S. Dakle, φ se faktorizira

preko $G_{L/K}$. tj. dokazali surjektivnost

Kraj dokaza:

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

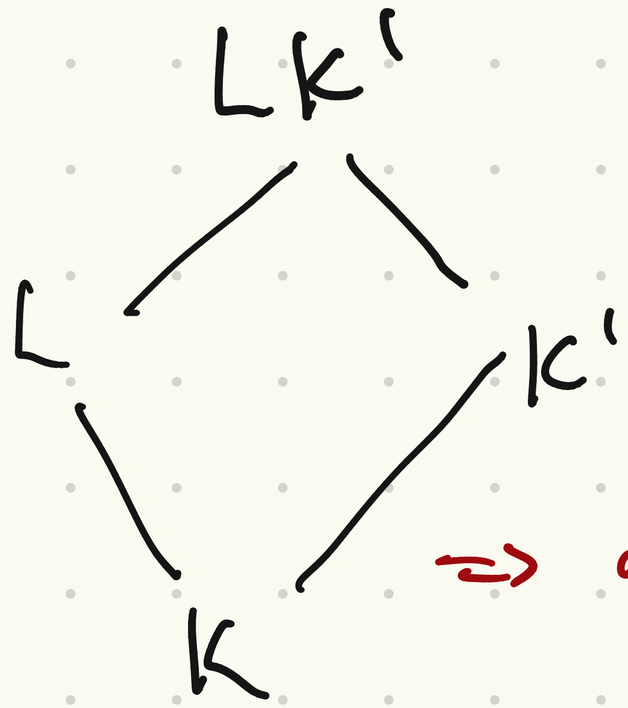
Propozicija. Neka je K polje alg. brojeva, $S \subset M_K$
t.d. $M_K^\infty \subseteq S$ i $m \geq 2$ prirodan broj.
Neka je L/K maksimalno abelovo proširenje
od K eksponenta m koje je unramified
izvan S. Tada je L/K konačno proširenje.

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?



svako ulaganje $\varphi \in \mathrm{Hom}(LK', \bar{K})$ je jednoznačno određeno restrikcijom

$\varphi_{|L}$ i $\varphi_{|K}$

$\Rightarrow$ ako su $\varphi_{|L}$ i $\varphi_{|K}$ autom. onda je to i φ

$\Rightarrow \mathrm{Gal}(LK'/K') \xrightarrow{\sim} \mathrm{Gal}(L/K)$

$\varphi \longmapsto \varphi_{|L}$

2°) Možemo povećati S (jer tako povećavamo L)

kako bi prsten S - cijelih od K

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

postao domena glavnih ideala.

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

$I = \langle a, b \rangle \rightsquigarrow \lambda = \frac{a}{b}$ pa ako u S dodamo faktore od b λ će biti jedinica u R_S

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 $\Delta \leq K^*/(K^*)^m$ takva da je $L = K\left(\Delta^{\frac{1}{m}}\right)$ gdje je

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

Precizniji za Δ možemo ureći: $\Delta \simeq \mathrm{Gal}(L/K)$

$$\Delta = \left(K^* \cap (L^*)^m\right) / (K^*)^m .$$

Dokaz: (protopostavimo samo $\mu_m \subset K$)

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

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

Općenito $\begin{matrix} L \\ | \\ K \end{matrix}$ je neramificirano nad v ako

je L_v/K_v neramificirano.

za neki $v \in M_L$

(znači $v \in M_K$)

Konkretno, zanima nas kada je

$K_v(\sqrt[m]{a})/K_v$ neramificirano.

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 ramificiranje u faktorizaciji

ideala (π) u $\mathcal{O}_{K_v}(\sqrt[m]{a})$.

Natrag na dokaz, neka je

↑ ovo se može argumentirati i preko diskrim.

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

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

$\Rightarrow$ potrebno je još dokazati da je $\leq$ kup

T_S konačan

Promotrimo prirodno preslikavanje

$$R_S^* \longrightarrow T_S .$$

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 $v \nmid S$). 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.

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

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

Nadalje, jezgra preslikavanja sadrži R_S^{+m}

pa cimamo sanjikaju

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

Po Dirichletovom teoremu za S-jedinice

R_S^+ je konačno generirana grupa.

$\Rightarrow T_S$ je konačan

∎