Odaberimo sad jedan par (b_1,b_2) za koji je $H_{b_1,b_2}(\mathbb{Q}) \neq \emptyset$. $\varphi : H_{b_1 b_2} \xrightarrow{4:1} E$

Što možemo reći o $\varphi(H_{b_1 b_2}(\mathbb{Q}))$?

Budući da je preslikavanje $E(\mathbb{Q}) \to \left(\mathbb{Q}^* / \mathbb{Q}^{*2}\right)^2$

$$P \mapsto (x(P) - e_1, x(P) - e_2)$$

homomorfizam s jezgrom $2E(\mathbb{Q})$ slijedi da se svaka dva elementa iz $\varphi(H(\mathbb{Q}))$ razlikuju za element iz $2E(\mathbb{Q})$.

Ova činjenica bi moglo objasniti djelovanje E na $H_{b_1 b_2}$ za koji vrijedi

$$\begin{tikzcd}
H_{b_1 b_2} \arrow[r, "+P"] \arrow[d, "\varphi"] \arrow[dr, phantom, "="] & H_{b_1 b_2} \arrow[d, "\varphi"] \\
E \arrow[r, "+2P"] & E
\end{tikzcd}$$

?

Definicija (homogeni prostor)

principal homogeneous space

Neka je E/K el. krivulja. Glavni homogeni prostor za E/K je glatka krivulja C/K zajedno s jednostavno tranzitivnim djelovanjem alg. grupe E na C nad K. Drugim riječima to je par (C, μ) gdje je C/K glatka krivulja i

$$\mu : C \times E \to C \quad \text{morfizam}$$

definiran nad K sa sljedeća tri svojstva

(i) $\mu(p, O) = p \quad \forall p \in C$

(ii) $\mu(\mu(p, P), Q) = \mu(p, P+Q) \quad \forall p, P, Q$

(iii) Za sve $p, q \in C$ postoji jedinstveni $P \in E$ t.d. $\mu(p, P) = q$.

Umjesto $\mu(p, P)$ pišemo $p + P$. Npr.

vrijedi
(ii) $\Leftrightarrow$
$$(p+P) + Q = p + (P+Q)$$

djelovanje E na C

zbrajanje na E

Pokazat ćemo da je H_{b_1,b_2} (glavni) homogeni prostor za $E/\mathbb{Q}$.

Opservacija: • Za $(b_1,b_2)=(1,1)$ $H_{1,1}\simeq E$ i $\varphi: H_{1,1}\to E$ je množenje s $[2]$.

• Također, $H_{1,1}\simeq H_{b_1,b_2}$ nad $\mathbb{Q}(\sqrt{b_1},\sqrt{b_2}) = K$

• H_{b_1,b_2} je krivulja genusa 1 i ako $H_{b_1,b_2}(\mathbb{Q})\neq\emptyset$ onda je $H_{b_1,b_2}\simeq E$.

$$
\begin{tikzcd}
H_{b_1,b_2} \arrow[r, dashed, "\sim", "K"'] \arrow[d, "\varphi"] & H_{1,1} \arrow[d, "\varphi"] \arrow[r, phantom, "\simeq"] & E \arrow[dl, "{[2]}"] \\
E \arrow[r, phantom, "="] & E &
\end{tikzcd}
$$

ovo je 2-natkrivanje

zašto?

ako H_{b_1,b_2} ima racionalnu točku onda

$$
\begin{tikzcd}
H_{b_1,b_2} \arrow[d, "\varphi"] \arrow[r, phantom, "\simeq"] & \tilde{E} \arrow[dl, dashed, "\tilde{\varphi}"] \\
E &
\end{tikzcd}
$$

$\tilde{\varphi}$ je morfizam stupnja 4

→ faktorizira se kroz izogeniju stupnja 4 ...

Kako E deluje na H_{b_1,b_2} ?

$$\begin{cases} b_1 y_1^2 = x - e_1 \\ b_2 y_2^2 = x - e_2 \\ b_1 b_2 y_3^2 = x - e_3 \end{cases}$$

$$\begin{tikzcd} H \arrow[r, dashed, "+P"] \arrow[d, "\varphi"] & H \arrow[d, "\varphi"] \\ E \arrow[r, "+2P"] & E \end{tikzcd}$$

<u>Lema</u>: Fix P. Funkcija $f_i(Q)$

$Q \mapsto x(Q+2P) - e_i$

je oblike $f_i(Q) = b_1 \cdot g_i(Q)^2$

za neku racionalnu fn g_i

$$\begin{tikzcd} (x, y_1, y_2, y_3) \arrow[r, mapsto, "+P"] \arrow[d, mapsto] & (x(Q+2P), \pm y_1', \pm y_2', \pm y_3') \arrow[d, dashed] \\ (x = x(Q), y(Q)) \arrow[r, mapsto, "+2P"] & Q+2P \end{tikzcd}$$

$*y_1 y_2 y_3$
$\parallel$

$(x(Q+2P), \pm y_1', \pm y_2', \pm y_3')$
$\parallel$
$(x(Q+2P), g_1(Q), g_2(Q), g_3(Q))$

$X(Q+2P)$

racionalna fja u varijablama

$x = x(Q)$ i $y = b_1 b_2 y_1 y_2 y_3$

Ova propozicija govori općenito o vezi homogenih prostora i eliptičkih krivulja.

Propozicija: Neka je E/K eliptička krivulja i C/K homogeni prostor za E/K. Fiksirajmo $p_0 \in C$ i def. preslikavanje

$$\theta : E \to C, \quad \theta(P) = p_0 + P$$

dobiveno od djelovanja

(a) θ je izomorfizam nad $K(p_0)$. Posebno C/K je twist od E/K

(b) Za sve $p \in C$ i sve $P \in E$

zbrajanje na E

$$p + P = \theta\left(\theta^{-1}(p) + P\right)$$

djelovanje

usklađenost dva zbrajanja

c) $\forall p, q \in C$

$$q - p = \theta^{-1}(q) - \theta^{-1}(p)$$

Po definiciji to je $P \in E$ za koji je $p + P = q$. Postoji zbog tranzitivnosti djelovanja

d) $v : C \times C \to E$

$v(p, q) = p - q$ je morfizam definiran nad K

dokaz:

(a) Neka je $\sigma \in Gal(\overline{K}/K(P_0))$ (posebno $P_0^\sigma = P_0$)

Tada je $\theta(P)^\sigma = \mu(P_0, P)^\sigma = \mu^\sigma(P_0^\sigma, P^\sigma)$

$$= \mu(P_0, P^\sigma) = \theta(P^\sigma)$$

$\Rightarrow$ θ je definiran nad $K(P_0)$

θ je stupnja 1 zbog tranzitivnosti $\Rightarrow$ θ je izomorf.

(b) $\theta(\theta^{-1}(p) + P) = P_0 + \theta^{-1}(p) + P = p + P$

(c) $\theta^{-1}(q) - \theta^{-1}(p) = (P_0 + \theta^{-1}(q)) - (P_0 + \theta^{-1}(p))$

$$= q - p$$

(d) Oduzimanje na C je morfizam zbog (c)

jer je θ^{-1} morfizam kao i oduzimanje na E

Definiran je nad K jer

$(q-p)^\sigma = (\theta^{-1}(q) - \theta^{-1}(p))^\sigma$

oduzimanje na E je def. nad K $= \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma$

$= (P_0 + \theta^{-1}(q))^\sigma - (P_0 + \theta^{-1}(p))^\sigma$

$= q^\sigma - p^\sigma$ ☒

Kako možemo opisati sve homogene prostore za djelovanje od E/K? Kada su dva homogena prostora "jednaka"?

Def. Dva homogena prostora C/K i C'/K za E/K su ekvivalentna ako postoji izomorfizam $\theta : C \to C'$ definiran nad K koji je kompatibilan s djelovanjem od E na C i C'. Preciznije

$$\theta(p+P) = \theta(p)+P \quad \forall p \in C \ \forall P \in E$$

Trivijalna klasa je ona koja sadrži $C = E$ na kojem E djeluje s translacijama.

Skup klasa ekvivalencije se naziva Weil–Châteletova grupa za E/K i označava s $WC(E/K)$.

što je zbrajanje? kasnije...

Propozicija: Neka je C/K homogeni prostor za E/K. Tada je C/K u trivijalnoj klasi ako i samo ako $C(K) \neq \emptyset$.

Dokaz: Slijedi iz prethodne propozicije.

to je ono što nas zanima

Napokon Galoisova kohomologija.

Pokazat ćemo: postoji prirodna bijekcija između $WC(E/K) \longrightarrow H^1(G_{\bar{K}/K}, E)$

što je ovo?

Kohomologija grupa (group cohomology)

G grupa, X G-modul (abelova grupa na koju G djeluje)

G djeluje slijeva!

- $H^0(G,X) := X^G$ G-invarijante.
- $H^1(G,X) = \text{kociklusi} / \text{korubovi}$

cocycles

coboundaries

kociklus je preslikavanje $f: G \to X$ t.d. $f(g_1 g_2) = f(g_1) + g_1 f(g_2)$

korub je preslikavanje $f: G \to X$ za koje postoji $x \in X$ t.d. $\forall g \in G$

$$f(g) = gx - x$$

korub je kociklus jer:

$$f(g_1 g_2) = g_1 g_2 x - x$$
$$= g_1(g_2 x - x) + g_1 x - x$$
$$= g_1 f(g_2) + f(g_1)$$

ako G djeluje trivijalno na X onda su kociklusi homomorfizmi

Galoisova kohomologija

je kohomologija grupa za $G = G_{\bar{K}/K} = Gal(\bar{K}/K)$
gdje moramo uzeti u obzir topologiju.

topologija

$G_{\bar{K}/K} = \varprojlim_{\substack{L/K \\ \text{konačno}}} G_{L/K}$ je prokonačna grupa s topologijom u kojoj se baza za otvorene skupove oko id sastoji od normalnih podgrupa konačnog indeksa u $G_{\bar{K}/K}$.

Te podgrupe su jezgre preslikavanja
$G_{\bar{K}/K} \to G_{L/K}$ gdje L ide po konačnim Galoisovim proširenjima L/K.

Def. Diskretni $G_{\bar{K}/K}$-modul je abelova grupa na koju $G_{\bar{K}/K}$ djeluje neprekidno (u odnosu na prokonačnu topologiju na $G_{\bar{K}/K}$ i diskretnu topologiju na M), tj. takav da je stabilizator od

prirodan zahtjev, elementi $m \in M$

$\{\sigma \in G_{\bar{K}/K} : m^\sigma = m\}$ konačnog indeksa u $G_{\bar{K}/K}$.

su definirani nad konačnim podp.

Def. $H^0(G_{\bar K/K}, M) = M^{G_{\bar K/K}}$ kao i ranije

$$H^1(G_{\bar K/K}, M) = \frac{Z^1_{cont}(G_{\bar K/K}, M)}{B^1(G_{\bar K/K}, M)}$$

kao i ranije osim što zahtijevamo da kociklusi budu neprekidni.

korubovi su automatski neprekidni

preslikavanje

$f: G_{\bar K/K} \to M$ je neprekidn. ako $\forall m \in M$ skup $f^{-1}(m)$ je unija koseta podgrupa konačnog indeksa u $G_{\bar K/K}$.

u slučaju kad je M trivijalan modul f je homomorfizam i neprekidnost je ekviv. tome da se f faktorizira kroz konačno proširenje

$$G_{\bar K/K} \to G_{L/K} \to M, \text{ tj.}$$

$\ker f = G_{\bar K/L}$ za L konačno proširenje.

Oprez – lijevo v.s. desno djelovanje

Neki, npr. Silverman, koriste drugačiju notaciju jer grupa djeluje zdesna. Npr. uvjet za kocikle izgleda ovako

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau$$

Natrag na

preko ove bijekcije definiramo grupovnu operaciju na $WC(E/K)$

Teorem: Postoji prirodna bijekcija

$$WC(E/K) \to H^1(G_{\bar{K}/K}, E)$$

definirana na sljedeći način.

Neka je C/K homogeni prostor za E/K i $p_0 \in C$ bilo koja točka. Tada

$$\{C/K\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\}$$

klasa ekv. od C/K

klasa kohomologije kocikla

Intuicija za ovaj teorem:

Neka je X neki algebarski objekt definiran nad K. Tvistovi od X su objekti Y definirani nad K koji su izomorfni s X nad $\bar{K}$.

"Teorem" Tvistovi od X (do na K-izom.) su parametrizirani s $H^1(G_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(X))$.

- nekomutativna kohomologija, M je grupa ne nužno komut.

1-kociklus je presl. $\xi : G \to M$ t.d.

$$\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau$$

ako $\mathrm{Aut}_{\bar{K}}(X)$ nije abelova grupa onda definicije od malo prije treba promijeniti

– H^1 više nije grupa, samo skup

dva kociklusa ξ i ζ su kohomologni (ekvivalentni) ako postoji $m \in M$ t.d.

$$m^\sigma \xi_\sigma = \zeta_\sigma m \quad \forall \sigma \in G.$$

$H^1 = \text{1-kociklusi} / \sim$

"Dokaz" $\Rightarrow$ Neka je Y twist od X.

Tada postoji izomorfizam $\phi : Y \to X$ definiran nad $\bar{K}$. Tada $\sigma \mapsto \xi_\sigma := \phi^\sigma \phi^{-1}$ definira 1-kociklus s vrijednostima u $\mathrm{Aut}_{\bar{K}}(X)$.

Ako ϕ komponiramo s automorfizmom od X dobijemo kociklus koji je kohomološki početnom ciklusu.

$\Leftarrow$ ćemo pokazati na konkretnom primjeru

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1} = (\phi^\sigma \phi^{-1})^\tau \phi^\sigma \phi^{-1}$$
$$= \xi_\sigma^\tau \xi_\tau \quad \forall \sigma, \tau$$

Zašto je $WC(E/K)$ povezan s $H^1(G_K, E)$?

Fiksirajmo E/K. Promotrimo kategoriju čiji su objekti homogeni prostori C/K s djelovanjem od E.

Morfizmi između objekata C_1/K i C_2/K su morfizmi $f: C_1 \longrightarrow C_2$ definirani nad K koji "čuvaju" djelovanje od E tj.

$$f \circ \tau_P = \tau'_P \circ f \quad \text{gdje je } \tau_P$$

translacija za $P \in E$ na C_1, a τ'_P translacija na C_2.

Fiksirajmo objekt $X = E$ na koji djeluje E prirodno (translacijama).

Tada je $WC(E/K)$ skup tvistova od X u ovoj kategoriji.

Što je $\mathrm{Aut}_{\bar{K}}(X)$?

$$\begin{tikzcd} E \arrow[loop above, "E"] \arrow[r, "\varphi"] & E \arrow[loop above, "E"] \end{tikzcd} \quad \text{t.d.}$$

- φ je izomorfizam
- $\varphi \circ \tau_P = \tau_P \circ \varphi \quad \forall P \in E$ ili ekv.

$$\varphi(P+Q) = \varphi(Q) + P \quad \forall P, Q \in E$$

ako $Q = O$ dobit ćemo

$$\varphi(P) = \varphi(O) + P$$

pa vidimo da je φ translacija za $\varphi(O)$ odnosno $\mathrm{Aut}_{\bar{K}}(X) \cong E$.

Prema "Teorem" imamo

$$WC(E/K) \simeq H^1(G_K, E)$$

što je tvrdnja Teorema.