Primjer: Neka je E/K ek., $K(\sqrt{d})$ kvadratno proširenje od K i

$\chi : G_K \to \{\pm 1\}$, $\chi(\sigma) = \sqrt{d}^{\,\sigma} / \sqrt{d}$

kvadratni karakter pridružen $K(\sqrt{d})/K$.

Definiramo 1-kocikl (homomorfizam)

$\xi : G_K \to \mathrm{Isom}(\bar{E})$

$\xi_\sigma = [\chi(\sigma)]$

E/K

$y^2 = f(x)$

Neka je C/K pridruženi twist od E/K.

Izračunat ćemo model za C/K.

Funkcijsko polje $K(C)$ je fiksno polje od $\bar{K}(E)$

pri djelovanju $f^{\cdot\sigma} = f^\sigma \circ \xi_\sigma$.

Kako je $x(P) = x(-P) \Rightarrow x' \in K(C)$ ($x' = x$)

$y(P) = -y(P) \Rightarrow y/\sqrt{d} \in K(C)$ ($y' = y/\sqrt{d}$)

model od C/K

Relacija između ovih fja je:

$$dy'^2 = f(x')$$

Primjer: Neka je E/K e.k., $K(\sqrt{d})/K$ kvadratno proširenje ($\mathrm{char}\, K \neq 2$). Neka je $T \in E(K)$ netrivijalna točka reda 2.

Tada je homomorfizam $\xi : G_K \to E$

$$\sigma \mapsto \begin{cases} 0 & \text{ako } \sqrt{d}^{\sigma} = \sqrt{d} \\ T & \text{ako } \sqrt{d}^{\sigma} = -\sqrt{d} \end{cases}$$

1-kocikla

Konstruirat ćemo homogeni prostor (twist) pridruženi elementu $\{\xi\} \in H^1(G_K, E)$

odnosno elementu $\{\xi\} \in H^1(G_K, \mathrm{Isom}(E))$

Odabirom Weierstrassovog modela za E/K dobijemo:

$$E: y^2 = x^3 + ax^2 + bx, \quad T = (0,0).$$

Tada translacija za T, τ_T, ima oblik

$$\tau_T(P) = (x,y) + (0,0) = \left(\frac{b}{x}, -\frac{by}{x^2} \right)$$

Neka je $\sigma \in G_K$ netrivijalan automorfizam
od $K(\sqrt{d})/K$. Promotrimo djelovanje na $\tilde{K}(E)$

$$f^{\cdot\tau} = f^{\tau} \circ \xi_\tau \quad \text{za } \forall \tau \in G_K, \forall f \in \tilde{K}(E).$$

Kako je $\sqrt{d}^{\cdot\sigma} = -\sqrt{d}$, $x^{\cdot\sigma} = x \circ \tau_T = \frac{b}{x}$

i $y^{\cdot\sigma} = y \circ \tau_T = -\frac{by}{x^2}$ možemo pogoditi

da su funkcije $\frac{\sqrt{d}\,x}{y}$ i $\sqrt{d}\left(x - \frac{b}{x}\right)$

fiksirane sa σ, odnosno G_K-invarijantne.

Nastavno relacije koje te fje. zadovoljavaju.

Označimo $z = \frac{\sqrt{d}\,x}{y}$ i $w = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2$.

Tada je

$$C: dw^2 = d^2 - 2acdz^2 + (a^2 - 4b)z^4$$

Kako se ovo pogodi?, z i w su elementi
koji tvore Riemann-Rochovih prostora?

Kako vidimo da je ovo homogeni prostor?

Sjetimo se teorema $WC(E/K) \xrightarrow{\sim} H^1(G_K, E)$.

Kako se dokaže surjektivnost? Klasi $\xi \in H^1$

znamo pridružiti krivulju C (twist od E)

još je $E < Jac(E)$. Kako na tom twistu

općenito definiramo diferenciju?

nad $\bar{K}$

Jednostavno, neka je $\phi : C \to E$ izomorfizam

t.d. je $\phi^\sigma \circ \phi^{-1} = T_{-\xi_\sigma}$ ← translacija za $-\xi_\sigma$

definiramo je nad K ako ϕ koji

Definiramo diferenciju: $\mu : C \times E \to C$

$$\mu(P, P) = \phi^{-1}(\phi(P) + P)$$

Kako se pravilno sve što se treba pravilno...

(Silverman X.3.)

Vratimo se natrag na prostore H_{b_1,b_2}.

To su twistori od E čiji kocikle poprima vrijednosti u $E \subset Isom(E)$ – homogeni prostori.

Ali za njih vrijedi nešto više. Slijedeći dijagram komutira

$$\begin{array}{ccc} H & \xrightarrow{\sim} & E \\ {\scriptstyle 4:1}\downarrow{\scriptstyle \varphi} & = & \downarrow{\scriptstyle \cdot 2} \\ E & = & E \end{array}$$

(2-covering)

Definirajmo kategoriju 2-natkrivanja:

Fiksirajmo E/k.

étale covering

Objekti: natkrivanja $C \downarrow E$ 4:1

unramified kao u topologiji

Morfizmi: (između dva objekta $C_1 \downarrow E$ i $C_2 \downarrow E$)

su morfizmi $C_1 \xrightarrow{\varphi} C_2$ t.d.

$$\begin{array}{ccc} C_1 & \xrightarrow{\varphi} & C_2 \\ & \searrow \quad = \quad \swarrow & \\ & E & \end{array}$$

Za X odaberemo $E \xrightarrow{\cdot 2} E$.

Tada su twistovi od X natkrivanja $C \xrightarrow{\varphi} E$

t.d. $C \xrightarrow{\sim} E$, $\varphi \cdot 2 = \cdot 2$ za neki $\bar{K}$-izom.

Dakle, $H_{b_1,b_2} \xrightarrow{\psi} E$ je twist od X.

"Znamo" da su twistovi do na K-izom. parametrizirani s $H^1(G_K, \mathrm{Isom}(X))$.

Što je $\mathrm{Isom}(X)$? Neka je $\Theta \in \mathrm{Isom}(X)$.

Tj.

$$\begin{array}{ccc} E & \xrightarrow{\Theta}_{\sim} & E \\ \downarrow \cdot 2 & = & \downarrow \cdot 2 \\ E & = & E \end{array}$$

Odnosno

$2 \cdot \Theta(P) = 2P \quad \forall P \in E$

Θ je translacija za točku reda 2

a onda, Θ je translacija $P \mapsto P + T$

ili: $P \mapsto -P + T$

$\mathrm{Isom}\, X = E[2]$

$\Rightarrow$ svakom $H_{b_1 b_2}$ su parametrizirani s

$H^1(G_K, E[2])$

↑ to očekujemo
↖ nismo dokazali

Interpretacija preko homogenih prostora

dolazi od $H^1(K, E[2]) \to H^1(K, E)$.

Elementi 2-Selmerove grupe bi onda

bile klase u $H^1(K, E[2])$ čiji pripadni

homogeni prostori su svugdje lokalno rješivi.

Napomena: Slično možemo definirati

i m-Selmerovu grupu - kroneč

od $E \xrightarrow{\cdot m} E$ ....

Abstract nonsense – pristup preko homološke algebre

Neka je $\phi : E \to E'$ izogenija. Npr. možemo uzeti nad K.

sve nad K

$\phi = [2]$ i $E' = E$.

Tada imamo egzaktni niz G_K-modula

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0.$$

ČINJENICA IZ GALOISOVE KOHOMOLOGIJE:

Neka je $0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0$ egzaktan niz

kratki egzaktni niz

G-modula. Tada postoji **dugi egzaktni niz**:

$$0 \to H^0(G, P) \to H^0(G, M) \to H^0(G, N) \xrightarrow{\delta}$$
$$\to H^1(G, P) \to H^1(G, M) \to H^1(G, N) \xrightarrow{\delta}$$
$$\to H^2(G, P) \to \dots$$

gdje se homomorfizam $\delta : H^0(G,N) \to H^1(G,P)$

ovako definiramo: ↑ connecting homomorphism

Neka je $n \in H^0(G,N) = N^G$. Odaberimo

$m \in M$ t.d. $\varphi(m) = n$ i definiramo

kociklus $\xi \in C^1(G,M)$ sa

$$\xi_\sigma = m^\sigma - m.$$

No $m^\sigma - m \in \ker(P)$ jer je

$$\varphi(m^\sigma - m) = \varphi(m)^\sigma - \varphi(m) = n^\sigma - n = 0.$$

Ako $\ker(P)$ identificiramo s P onda

ξ definira klasu u $H^1(G,P)$.

Primjenom prethodne činjenice dobivamo

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_K, E[\phi]) \to H^1(G_K, E) \to H^1(G_K, E') \to H^2(G_K, E[\phi]) \to \dots$$

Odnosno

$$0 \to \frac{E'(K)}{\phi(E(K))} \xrightarrow{\delta} H^1(G_K, E[\phi]) \to H^1(G_K, E)[\phi] \to 0$$

za $\phi = [2]$ i $E' = E$ imamo

$$0 \to \frac{E(K)}{2E(K)} \xrightarrow[\delta]{(a)} H^1(G_K, E[2]) \xrightarrow{(b)} H^1(G_K, E)[2] \to 0$$

geometrijski:

(a) svakoj točki do na $2E(K)$ odgovara točno jedna klasa iz $H^1(G_K, E[2])$ koja odgovara homogenom prostoru 2-torzije od $H^1(G_K, E)[2]$

(b) za točne te klase iz $H^1(G_K, E[2])$ homogeni prostor je trivijalan, odnosno ima K-rac točki.

Preslikavanje δ se zove Kummerovo preslikavanje i definirano je ovako: (bilo koji)

Neka je $P \in E(K)$ i $Q \in E(\bar{K})$ t.d. $2Q = P$. Definiramo

$$\sigma \mapsto Q^\sigma - Q \in H^1(G_K, E[2])$$

uočimo:

$2(Q^\sigma - Q) = P^\sigma - P = 0$

$\Rightarrow Q^\sigma - Q \in E[2]$.

Dakle, slika od δ opisuje one prostore koji imaju K-rac. točku!

Nas zanima **lokalna rješivost**.

Fiksirajmo valuaciju v od K i proširimo ju do $\bar{K}$ što definira uklapanje $\bar{K} \subset \widetilde{K_v}$ i dekompozicijsku grupu $G_v < G_K$.

↑ place

G_v djeluje na $\bar{K_v}$ pa onda i na $E(\bar{K_v})$ i na isti način dobivamo

← zašto?

$$0 \to \frac{E(K_v)}{2E(K_v)} \to H^1(G_v, E[2]) \to H^1(G_v, E)[2] \to 0$$

Koja je veza između $H^1(G_v, E[2]) \subset H^1(G_K, E[2])^?$

$G_v \subset G_K$ nije normalno ← trebat će nam kasnije

ČINJENICA IZ GALOISOVE KOHOMOLOGIJE:

Inflation - Restriction sequence

Propozicija: Neka je M G-modul i $H \triangleleft G$.

Također je slijedeći niz egzaktan ovo nas zanima ↙ ↑ normalna zatvorena

$$0 \to H^1(G/H, M^H) \xrightarrow{Inf} H^1(G, M) \xrightarrow{Res} H^1(H, M)$$

gdje je $Res : H^1(G, M) \to H^1(H, M)$ restrikcija s G na H

dok se $Inf : H^1(G/H, M^H) \to H^1(G, M)$ definira ↑ je prirodan G/H modul

ovako:

neka je $\xi : G/H \to M^H$ 1-kociklus.

Tada je $Inf\,\xi$ klasa od

$$G \hookrightarrow G/H \to M^H \hookrightarrow M$$

u $H^1(G, M)$.

↑ daje nam razumijevanje odnosa kohomologija za grupu i njenu normal. podgrupu

Koji je veza između homogenih prostora pridruženih klasama $\{\} \in H^1(G_K, E[2])$ i $Res_v\{\} \in H^1(G_v, E[2])$?

Ako $\{\} \rightsquigarrow C/K \in Wc(E/K)$

onda $Res_v\{\} \rightsquigarrow C/K_v \in Wc(E/K_v)$.

zašto? dokaz.

Zaključak: Homogeni prostor od $\{\} \in H^1(G_K, E[2])$ ima K_v-racionalnu točku ako i samo ako se $Res_v\{\}$ nalazi u slici Kummerovog preslikavanja

$$\delta_v : E(K_v)/2E(K_v) \hookrightarrow H^1(G_v, E[2])$$

Sada smo spremni definirati 2-Selmerovu grupu u jeziku Galoisove kohomologije.