

UNIVERSITATEA DIN BUCUREȘTI
Facultatea de Matematică și Informatică

Disertație masterală

Étale stuff

Autor:
Andrei Sipoș

Profesor coordonator:
Lect. dr. Victor Vuletescu

București, 2014

Cuprins

Introducere

Acest text își propune să:

- enunțe cadrul de desfășurare al coomologiei étale
- prezinte versiuni étale ale unor rezultate fundamentale în topologie, precum dualitatea Poincaré sau formulele de tip Lefschetz
- aplice aceste rezultate la studiul funcțiilor zeta asociate varietăților peste corpuri finite

Capitolul 1

Situl étale

Capitolul 2

De la étale la ℓ -adic

Din proprietățile de bază ale grupurilor de coomologie étală, avem că pentru orice grup abelian G are loc relația:

$$H^1(X, G) \simeq \text{Hom}_{\text{TopGr}}(\pi_1(X, x), G)$$

unde Hom -set-ul din dreapta este considerat în categoria grupurilor topologice (iar G este considerat cu topologia discretă). Dacă vom considera, de pildă, G ca fiind un grup infinit, fără torsiune, spre exemplu \mathbb{Z} (cum se obișnuiește în topologia algebrică), atunci grupul de coomologie va fi trivial. Iată de ce: dacă iau un element al acelui Hom -set, $f : \pi_1(X, x) \rightarrow \mathbb{Z}$ (i.e. un morfism de grupuri continuu), atunci $f^{-1}(0)$ este deschis în $\pi_1(X, x)$. Cum grupul de omotopie este compact, $f^{-1}(0)$ este de indice finit. Prin urmare, f atinge un număr finit de valori, însă singurul subgrup finit al lui \mathbb{Z} este cel trivial. Deci f este morfismul nul, iar $H^1(X, \mathbb{Z}) = 0$, comportament pe care nu ni-l dorim.

În argumentul de mai sus a intervenit în mod crucial faptul că grupul este considerat cu topologia discretă. Dacă am considera un grup topologic cu o structură canonică de grup profinit nediscret, cum ar fi \mathbb{Z}_ℓ , atunci analogul membrului drept, $\text{Hom}_{\text{TopGr}}(\pi_1(X, x), \mathbb{Z}_\ell)$, nu va mai fi în mod trivial nul. Însă:

$$\begin{aligned} \text{Hom}_{\text{TopGr}}(\pi_1(X, x), \mathbb{Z}_\ell) &\simeq \text{Hom}_{\text{TopGr}}(\pi_1(X, x), \varprojlim_n \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}) \\ &\simeq \varprojlim_n \text{Hom}_{\text{TopGr}}(\pi_1(X, x), \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}) \\ &\simeq \varprojlim_n H^1(X, \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}) \end{aligned}$$

Soluția este deci de a defini:

$$H^r(X, \mathbb{Z}_\ell) := \varprojlim_n H^r(X, \frac{\mathbb{Z}}{\ell^n \mathbb{Z}})$$

pentru orice r natural, relație în care se va înțelege că ceea ce este scris în membrul stâng este o notație „pur formală” pentru ceea ce vom numi **coomologie ℓ -adică**.

Ea se poate defini pe ceea ce se numește un fascicul de \mathbb{Z}_ℓ -module, adică o familie:

$$\mathcal{M} = (\{\mathcal{M}_n\}_n, \{f_{n+1} : \mathcal{M}_{n+1} \rightarrow \mathcal{M}_n\}_n)$$

astfel încât pentru orice n , \mathcal{M}_n este fascicul constructibil de $\frac{\mathbb{Z}}{\ell^n \mathbb{Z}}$ -module, $\text{Ker}(f_{n+1}) = \ell^{n+1} \mathcal{M}_{n+1}$, $\text{Im}(f_{n+1}) = \mathcal{M}_n$.

Un asemenea obiect se numește **plat** dacă pentru orice n și s naturale, șirul:

$$0 \rightarrow \frac{\mathcal{M}_{n+s}}{\ell^s \mathcal{M}_{n+s}} \xrightarrow{\cdot \ell^n} \mathcal{M}_{n+s} \rightarrow \frac{\mathcal{M}_{n+s}}{\ell^n \mathcal{M}_{n+s}} \rightarrow 0$$

este exact (unde fasciculul din stânga este izomorf cu \mathcal{M}_s , iar cel din dreapta cu \mathcal{M}_n).

Acum putem defini:

$$H^r(X, \mathcal{M}) := \varprojlim_n H^r(X, \mathcal{M}_n)$$

$$H_c^r(X, \mathcal{M}) := \varprojlim_n H_c^r(X, \mathcal{M}_n)$$

Aceste grupuri satisfac următoarea proprietate:

Teorema 2.1. (Teorema de finitudine) Fie X o varietate definită peste un corp separabil închis k . $\mathcal{M} = \{\mathcal{M}_n\}_n$ un fascicul plat de \mathbb{Z}_ℓ -module. Presupunem că X este completă sau $\ell \neq \text{char}(k)$. Atunci:

- (i) modulele $H^r(X, \mathcal{M})$ sunt finit generate;
- (ii) pentru orice n există un șir exact lung:

$$\cdots \rightarrow H^r(X, \mathcal{M}) \xrightarrow{\cdot \ell^n} H^r(X, \mathcal{M}) \rightarrow H^r(X, \mathcal{M}_n) \rightarrow H^{r+1}(X, \mathcal{M}) \rightarrow \cdots$$

Demonstrație. Avem pentru orice n și s șirul exact:

$$0 \rightarrow \mathcal{M}_s \xrightarrow{\cdot \ell^n} \mathcal{M}_{n+s} \rightarrow \mathcal{M}_n \rightarrow 0$$

compatibil cu familia $\{f_i\}$, care induce șirul exact lung:

$$\cdots H^r(X, \mathcal{M}_s) \xrightarrow{\cdot \ell^n} H^r(X, \mathcal{M}_{n+s}) \rightarrow H^r(X, \mathcal{M}_n) \rightarrow H^{r+1}(X, \mathcal{M}_s) \rightarrow \cdots$$

(adică al doilea punct al teoremei). Din compatibilitate, putem trece la limită după s și obținem șirul lung:

$$\cdots H^r(X, \mathcal{M}) \xrightarrow{\cdot \ell^n} H^r(X, \mathcal{M}) \rightarrow H^r(X, \mathcal{M}_n) \rightarrow H^{r+1}(X, \mathcal{M})$$

ce induce șirurile exacte scurte de forma:

$$0 \rightarrow \frac{H^r(X, \mathcal{M})}{\ell^n H^r(X, \mathcal{M})} \rightarrow H^r(X, \mathcal{M}_n) \rightarrow H^{r+1}(X, \mathcal{M})_{\ell^n} \rightarrow 0$$

Trecem la limită după n și obținem:

$$0 \rightarrow \varprojlim_n \frac{H^r(X, \mathcal{M})}{\ell^n H^r(X, \mathcal{M})} \rightarrow H^r(X, \mathcal{M}) \rightarrow \varprojlim_n H^{r+1}(X, \mathcal{M})_{\ell^n} \rightarrow 0$$

Însă

$$\begin{aligned} \varprojlim_n H^{r+1}(X, \mathcal{M})_{\ell^n} &= \varprojlim_n (H^{r+1}(X, \mathcal{M})_{\ell^n} \xleftarrow{\ell} H^{r+1}(X, \mathcal{M})_{\ell^{n+1}}) \\ &= \{(x_n)_n \mid \forall n, \ell^n x_n = 0, \ell x_{n+1} = x_n\} \\ &= 0 \end{aligned}$$

(fiindcă nu există elemente nenule infinit divizibile, $H^{r+1}(X, \mathcal{M})$ fiind limită proiectivă de grupuri finite de ℓ^n -torsione). Deci $H^r(X, \mathcal{M}) \simeq \varprojlim_n \frac{H^r(X, \mathcal{M})}{\ell^n H^r(X, \mathcal{M})}$, ce este finit generat. \square

Vom nota în continuare, la fel de formal,

$$H^r(X, \mathbb{Q}_\ell) = H^r(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

Un rezultat ce se moștenește în mod trivial la această coomologie ℓ -adică este dimensiunea coomologică.

Teorema 2.2. (*Formula Künneth*) *Are loc izomorfismul de inele graduate:*

$$H^*(X \times Y, \mathbb{Q}_\ell) \simeq H^*(X, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} H^*(Y, \mathbb{Q}_\ell)$$

Capitolul 3

Numărarea punctelor

Problema pe care urmează să o formulăm a pornit de la cea a studiului modului cum variază numărul de puncte de pe o curbă eliptică, în momentul în care extindem corpul de bază. Ne este cunoscută din studiul acelor curbe inegalitatea Hasse-Weil, care spune că pentru orice curbă eliptică X definită peste un corp finit \mathbb{F}_q , dacă notăm $N_m(X) = \#X(\mathbb{F}_{q^m})$, are loc relația:

$$|N_m(X) - (q^m + 1)| \leq 2\sqrt{q^m}$$

Mai precis, există două numere algebrice α_1, α_2 de modul \sqrt{q} astfel încât pentru orice m :

$$N_m(X) = 1 - \alpha_1^m - \alpha_2^m + q^m$$

André Weil a propus următoarea generalizare:

Teorema 3.1. (Conjecturile Weil) Fie X o varietate proiectivă netedă definită peste \mathbb{F}_q de dimensiune d . Atunci:

1. există $2d$ numere naturale b_0, \dots, b_{2d} și o familie de numere complexe $\{\alpha_{j,u}\}_{\substack{j \in \overline{0, 2d} \\ u \in \overline{1, b_j}}}$ astfel încât pentru orice m am:

$$N_m(X) = \sum_{j=0}^{2d} (-1)^j \left(\sum_{u=1}^{b_j} \alpha_{j,u}^m \right)$$

Mai mult, $b_0 = b_{2d} = 1$, $\alpha_{0,1} = 1$, $\alpha_{2d,1} = q^d$. Numărul $\sum_j (-1)^j b_j$ va fi notat cu χ .

2. pentru orice j , b_j este egal cu b_{2d-j} , iar $(\frac{q^d}{\alpha_{2d-j,1}}, \dots, \frac{q^d}{\alpha_{2d-j,b_j}})$ e o permutare a enumerării $(\alpha_{j,1}, \dots, \alpha_{j,b_j})$.
3. pentru orice j, u , avem că $\alpha_{j,u}$ e număr algebric de modul $q^{\frac{j}{2}}$.

Se observă că dacă X este curbă eliptică se reconstituie relația de mai devreme, cu $b_1 = 2 = \dim H^1(\mathbb{C}/\Lambda, \mathbb{Q})$ (pentru Λ o latice în planul complex).

Un mod mai pragmatic de a exprima conjecturile Weil este reprezentat de instrumentul funcțiilor generatoare.

Ne bazăm pe identitatea formală:

$$\log\left(\frac{1}{1-x}\right) = \sum_{m=1}^{\infty} \frac{x^m}{m}$$

scrisă eventual

$$\frac{1}{1-x} = \exp\left(\sum_{m=1}^{\infty} \frac{x^m}{m}\right)$$

ce se poate verifica via expansiune în serie Taylor în jurul lui zero.

Definind $Z_X(t) = \exp\left(\sum_{m=1}^{\infty} N_m(X) \frac{t^m}{m}\right)$, obținem din punctul 1 al conjecturilor:

$$\begin{aligned} Z_X(t) &= \exp\left(\sum_{m=1}^{\infty} \sum_{j=0}^{2d} (-1)^j \sum_{u=1}^{b_j} \alpha_{j,u}^m \frac{t^m}{m}\right) \\ &= \prod_{j=0}^{2d} \left(\prod_{u=1}^{b_j} \exp\left(\sum_{m=1}^{\infty} \frac{(\alpha_{j,u} t)^m}{m}\right)\right)^{(-1)^j} \\ &= \prod_{j=0}^{2d} \left(\frac{1}{\prod_{u=1}^{b_j} (1 - \alpha_{j,u} t)}\right)^{(-1)^j} \\ &= \prod_{j=0}^{2d} P_j(t)^{(-1)^{j+1}} \end{aligned}$$

unde am notat $P_j(t) = \prod_{u=1}^{b_j} (1 - \alpha_{j,u} t)$ (și am $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$).

Vom deriva acum din punctul 2 o relație pe care o va satisface $Z_X(t)$. Aplicăm relația de permutare între enumerări și obținem:

$$\begin{aligned} P_{2d-j}(t) &= \prod_u (1 - \alpha_{2d-j,u} t) = \prod_u \left(1 - \frac{q^d}{\alpha_{j,u}} t\right) \\ &= \left(\prod_u \alpha_{j,u}\right)^{-1} \prod_u (\alpha_{j,u} - q^d t) \\ &= \left(\prod_u \alpha_{j,u}\right)^{-1} (-1)^{b_j} (q^d t)^{b_j} \prod_u \left(1 - \frac{\alpha_{j,u}}{q^d t}\right) \\ &= \left(\prod_u \alpha_{j,u}\right)^{-1} (-1)^{b_j} (q^d t)^{b_j} P_j\left(\frac{1}{q^d t}\right) \end{aligned}$$

Folosim acum atât simetria b_j -urilor cât și permutarea enumerărilor:

$$\begin{aligned} P_j(t)P_{2d-j}(t) &= (q^d t)^{2b_j} (q^d)^{-b_j} P_j\left(\frac{1}{q^d t}\right) P_{2d-j}\left(\frac{1}{q^d t}\right) \\ &= (q^d)^{\frac{b_j + b_{2d-j}}{2}} t^{b_j + b_{2d-j}} P_j\left(\frac{1}{q^d t}\right) P_{2d-j}\left(\frac{1}{q^d t}\right) \end{aligned}$$

Însă $(\prod_s \alpha_{d,u})^2 = (q^d)^{b_d}$, deci $\prod_s \alpha_{d,u} = \pm (q^d)^{\frac{b_d}{2}}$, și pot scoate relația (pentru indicele d):

$$P_d(t) = \pm (-1)^{b_d} (q^d t)^{b_d} (q^d)^{\frac{b_d}{2}} P_d\left(\frac{1}{q^d t}\right)$$

Și obțin astfel formula pentru funcția Z_X :

$$\begin{aligned} Z_X(t) &= \prod_{j=0}^{2d} P_j(t)^{(-1)^{j+1}} \\ &= \pm \prod_{j=0}^{2d} P_j\left(\frac{1}{q^d t}\right)^{(-1)^{j+1}} (q^d)^{-\frac{\sum_j (-1)^{j+1} b_j}{2}} t^{-\sum_j (-1)^{j+1} b_j} \\ &= \pm q^{\frac{d_X}{2}} t^X Z_X\left(\frac{1}{q^d t}\right) \end{aligned}$$

numită **ecuația funcțională** a lui Z_X .

O altă reformulare ne este dată de următoarea substituție:

$$\zeta_X(s) = Z_X(q^{-s})$$

Notând pentru un punct închis $x \in X$ cu $\kappa(x)$ corpul rezidual al său, cu $\deg(x)$ gradul extinderii $\kappa(x) : \mathbb{F}_q$ și cu

$$N_m(x) = \begin{cases} \deg(x) & \text{dacă } \deg(x) \mid m \\ 0 & \text{altfel} \end{cases}$$

avem din cele cunoscute de la teoria schemelor:

$$N_m(X) = \sum_x N_m(x)$$

Obținem rescrierile:

$$\begin{aligned}
 Z_X(t) &= \exp\left(\sum_{m \geq 1} N_m(X) \frac{t^m}{m}\right) = \exp\left(\sum_{m \geq 1} \sum_x N_m(x) \frac{t^m}{m}\right) \\
 &= \exp\left(\sum_x \sum_{\substack{m \geq 1 \\ \deg(x) | m}} N_m(x) \frac{t^m}{m}\right) \\
 &= \exp\left(\sum_x \sum_{n \geq 1} \deg(x) \frac{t^{n \cdot \deg(x)}}{n \cdot \deg(x)}\right) \\
 &= \exp\left(\sum_x \sum_{n \geq 1} \frac{(t^{\deg(x)})^n}{n}\right) = \exp\left(\sum_x \log \frac{1}{1 - t^{\deg(x)}}\right) \\
 &= \exp \log \prod_x \frac{1}{1 - t^{\deg(x)}} = \prod_x \frac{1}{1 - t^{\deg(x)}}
 \end{aligned}$$

și deci

$$\zeta_X(s) = \prod_x \frac{1}{1 - (q^{\deg(x)})^{-s}} = \prod_x \frac{1}{1 - (\#k(x))^{-s}}$$

Ultima formulă are sens pentru o schemă oarecare, nu neapărat peste un corp finit. De pildă, înlocuind X cu $\text{Spec } \mathbb{Z}$, apare:

$$\zeta_{\text{Spec } \mathbb{Z}}(s) = \prod_{p \in \text{Max } \mathbb{Z}} \frac{1}{1 - (\#(\mathbb{Z}/p))^{-s}} = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}$$

binecunoscuta funcție zeta a lui Riemann (punctele închise din $\text{Spec } \mathbb{Z}$ sunt precis idealele maximale ale lui \mathbb{Z}), ceea ce ne justifică notația.

Atenție, însă: funcția Z_X nu are sens decât pentru scheme definite peste un corp finit!

Este clar că $s \in \mathbb{C}$ este zerou, respectiv pol, pentru ζ_X dacă și numai dacă q^{-s} va avea aceeași calitate pentru Z_X (și orice $t \in \mathbb{C}^*$ se poate scrie ca q^{-s} , e drept, într-o infinitate de moduri). Iau un astfel de s . Din exprimarea rațională a lui Z_X rezultă că $q^{-s} = \frac{1}{\alpha_{j,u}}$ pentru anumite j și u , iar ultima afirmație din coniecturi implică $|q^{-s}| = q^{-\frac{j}{2}}$. Scriu $s = a + bi$, cu $a, b \in \mathbb{R}$, și am $q^{-s} = e^{-s \ln q} = e^{-a \ln q - bi \ln q}$. Deci $q^{-\frac{j}{2}} = |e^{-a \ln q - bi \ln q}| = q^{-a}$ și $\frac{j}{2} = a = \text{Re } s$.

Invers, acum, dacă fac presupunerea că orice s zerou sau pol al lui ζ_X are proprietatea că $\text{Re } s = \frac{j}{2}$ (cu $j \in \overline{0, 2d}$), pot face următorul raționament. Iau $t \in \mathbb{C}^*$ zerou sau pol pentru Z_X și fie s cu $t = q^{-s}$. Atunci s este zerou/pol pentru ζ_X și $\text{Re } s = \frac{j}{2}$. Ca înainte, avem $|t| = |q^{-s}| = q^{-\text{Re } s} = q^{-\frac{j}{2}}$. Deci zerourile și polii lui Z_X au modulul $q^{-\frac{j}{2}}$.

Rezultă că acea condiție 3 este echivalentă cu faptul că funcția zeta a varietății are zerourile și polii pe liniile $\text{Re } s = \frac{j}{2}$, ceea ce justifică numele dat condiției de **ipoteză Riemann**.

Mai mult decât atât, această separare după modul a zerourilor și polilor lui Z_X ne permit să extragem P_j -urile din Z_X și să obținem în mod reciproc din ecuația funcțională condiția 2 din coniecturile Weil.

Toate aceste manipulări de formule ne învață să apreciem modul cum coomologia étală conduce în mod natural măcar la expresia rațională și la ecuația funcțională a funcției Z_X .

Să vedem cum. Mai întâi, vom obține o altă descriere a lui $X(\mathbb{F}_{q^m})$ cu ajutorul aplicației Frobenius.

Orice \mathbb{F}_q -algebră A admite endomorfismul Frobenius $a \mapsto a^q$, ce se dualizează la o aplicație $\text{Spec } A \rightarrow \text{Spec } A$. Această familie de aplicații se prelungește unic la o întreagă transformare naturală $\{F_X : X \rightarrow X\}_{X \in \mathbb{F}_q\text{-Sch}}$. Din naturalitate, rezultă că acționează pe varietăți afine sau proiective în modul firesc, prin ridicarea la puterea q a coordonatelor. În particular F_X are gradul $q^{\dim X}$, după cum se verifică ușor pe spațiile afine.

Rezultă deci $X(\mathbb{F}_{q^m}) = \text{Fix}(F_X^m)$.

Lema 3.2. $\Gamma_{F^m} \cdot \Delta_X = \sum_{P \in \text{Fix}(F_X^m)} P$ (în sensul că toate apar cu multiplicitate 1).

Demonstrație. E suficient să arătăm pentru $m = 1$ (F^m este Frobeniusul lui \mathbb{F}_{q^m}). Notez $F = F_X$.

Fie $P \in \text{Fix}(F)$. Înlocuiesc X cu o vecinătate afină a lui P , să zicem $U = \text{Spec } A$, cu $A = \mathbb{F}_q[t_1, \dots, t_n] = \frac{\mathbb{F}_q[T_1, \dots, T_n]}{a}$.

Atunci pentru orice i am $t_i \circ F = t_i^q$ și $(dt_i)_P \circ (dF)_P = (dt_i^q)_P = qt_i^{q-1}(dt_i)_P = 0$.

Ca urmare diferențiala lui F în P este zero, ca urmare graficul lui Frobenius nu este tangent la diagonală în (P, P) , iar numărul de intersecție (multiplicitatea) este 1. \square

Aplicând formula de punct fix a lui Lefschetz, rezultă (pentru $(\ell, q) = 1$):

$$N_m(X) = \sum_r (-1)^r \text{Tr}(F_{|H^r(X, \mathbb{Q}_\ell)}^m)$$

Putem folosi formula pentru a prelucra funcția Z a lui X :

$$\begin{aligned} Z_X(t) &= \exp\left(\sum_{m=1}^{\infty} N_m(X) \frac{t^m}{m}\right) \\ &= \exp\left(\sum_{m=1}^{\infty} \left(\sum_{r=0}^{2d} (-1)^r \text{Tr}(F_{|H^r(X, \mathbb{Q}_\ell)}^m)\right) \frac{t^m}{m}\right) \\ &= \prod_{r=0}^{2d} \exp\left(\sum_{m=1}^{\infty} \text{Tr}(F_{|H^r(X, \mathbb{Q}_\ell)}^m) \frac{t^m}{m}\right) (-1)^r \end{aligned}$$

Scriem acum fiecare $F_{|H^r(X, \mathbb{Q}_\ell)}$ ca matrice pătratică superior triunghiulară (eventual peste o extindere a lui \mathbb{F}_q) cu numărul de linii egal cu $b_r = \dim H^r(X, \mathbb{Q}_\ell)$. Se observă atunci că dacă elementele de pe diagonală (valorile proprii) sunt $\alpha_{r,1}, \dots, \alpha_{r,b_r}$, atunci $\text{Tr}(F_{|H^r(X, \mathbb{Q}_\ell)}^m)$ va fi egal cu $\sum_{i=1}^{b_r} \alpha_{r,i}^m$ și deci pot aplica exact același raționament ca mai devreme pentru a exprima rațional pe Z_X .

Vom avea $Z_X \in \mathbb{Q}_\ell(t) \cap \mathbb{Q}[[t]] \subseteq \mathbb{Q}(t)$, însă aceasta nu ne garantează că fiecare P_j este în $\mathbb{Q}[t]$ (altfel spus, că este „independent de ℓ ”) - aceasta se poate face doar presupunând ipoteza lui Riemann, care ne permite, după cum am spus și mai devreme, să separăm P_j -urile după modulul rădăcinilor.

Altă consecință a raționamentului precedent a fost că am identificat $\alpha_{j,u}$ -urile ca fiind valorile proprii ale operatorilor induși de Frobenius pe spațiile de coomologie.

Aceasta ne arată în particular că $b_0 = b_{2d} = 1$.

Trecem acum la demonstrarea simetriei între valorile proprii pe spațiile de ordin r și $2d - r$, relație care după cum am observat ne implică o ecuație funcțională.

Avem biliniara nedegenerată dată de dualitatea Poincaré:

$$\langle, \rangle = \eta_X \circ \smile : H^{2d-r}(X, \mathbb{Q}_\ell) \times H^r(X, \mathbb{Q}_\ell) \rightarrow H^{2d}(X, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell(-d)$$

ce din start ne indică $b_r = b_{2d-r}$.

Știm că $F_r^* = F_{|H^r(X, \mathbb{Q}_\ell)}$ are adjunct relativ la \langle, \rangle :

$$\langle F_{*2d-r}(x), x' \rangle = \langle x, F_r^*(x') \rangle, \forall x \in H^{2d-r}(X, \mathbb{Q}_\ell), x' \in H^r(X, \mathbb{Q}_\ell)$$

Din considerente de algebră liniară rezultă că valorile proprii ale lui F_r^* coincid cu ale lui F_{*2d-r} . Însă $F_{*r} \circ F_r^* = q^d (= \deg F)$.

De aici rezultă că dacă $(\alpha_1, \dots, \alpha_v)$ sunt valorile proprii ale lui F_r^* , $(\frac{q^d}{\alpha_1}, \dots, \frac{q^d}{\alpha_v})$ sunt cele ale lui F_{*r} , deci (din cele anterioare) și ale lui F_{*2d-r}^* , i.e. exact ce ni se cerea. Iar faptul că $\alpha_{0,1} = 1$ și $\alpha_{2d,1} = q^d$ rezultă din modul cum acționează operatorii Frobenius pe H^0 , respectiv pe H^{2d} .

În acest moment, tot ce ne rămâne este să demonstrăm ipoteza lui Riemann.

Capitolul 4

«La conjecture de Weil»

Mai precis, ce avem de demonstrat este:

Teorema 4.1. (Deligne, 1974) Fie X o varietate proiectivă d -dimensională absolut nesingulară și absolut ireductibilă definită peste \mathbb{F}_q ; α o valoare proprie a lui F_q^* ; τ o scufundare a lui \mathbb{Q}_ℓ în \mathbb{C} .

Atunci $\tau(\alpha)$ (mai departe simbolul τ va fi subînțeles) este algebric și de modul $q^{\frac{r}{2}}$.

În primul rând, se observă că este suficient să demonstrăm pentru varietatea obținută după o schimbare de bază spre o extindere finită a corpului de definiție - să zicem, de grad m . Asta deoarece operatorul Frobenius pe varietatea nouă va fi puterea m a celui de pe varietatea veche. Dacă α este valoare proprie pentru Frobenius-ul vechi, α^m este pentru cel nou. Din ipoteza noastră, α^m are modulul $(q^m)^{\frac{r}{2}}$. Ca urmare, α va avea modulul $q^{\frac{r}{2}}$. Aceasta ne va permite să facem un număr finit de extinderi finite de-a lungul demonstrației, fără a pierde din generalitatea enunțului.

În al doilea rând, se vede că pot demonstra doar pentru spațiile cu rangul cel mult d . Aceasta deoarece de la rangul $d + 1$ încolo, valorile proprii au simetria implicată de dualitatea Poincaré pe care am văzut-o mai devreme.

În al treilea rând, vom arăta că este suficient să arătăm teorema doar pentru $r = d$. Iată de ce: din teorema lui Bertini, există $Z \subset X$ o secțiune hiperplană netedă (eventual extinzând corpul). Aplicând teorema Lefschetz slabă, aplicația canonică (ce este compatibilă cu Frobenius) $H^r(X, \mathbb{Q}_\ell) \rightarrow H^r(Z, \mathbb{Q}_\ell)$ este injectivă pentru $r \leq d - 1$ și pot aplica un raționament prin inducție (pasul de bază fiind varietățile zero-dimensionale, pentru care clar este adevărat, din modul cum acționează Frobenius pe H^0).

În al patrulea rând, putem să arătăm chiar și numai pentru varietățile de dimensiune pară, iar pentru acelea, doar că valorile proprii α corespundătoare spațiului de coomologie din mijloc satisfac inegalitatea

$$q^{\frac{d}{2} - \frac{1}{2}} \leq |\alpha| \leq q^{\frac{d}{2} + \frac{1}{2}}$$

Presupunând că am arătat așa ceva, vreau să demonstrez teorema pentru o varietate oarecare X și α valoare proprie a lui F_d^* . Fie k număr natural. Iau Y ca fiind produsul lui X cu el însuși

de $2k$ ori. Conform Künneth, $H^d(X, \mathbb{Q}_\ell)^{\otimes 2k}$ se scufundă în $H^{2kd}(Y, \mathbb{Q}_\ell)$, iar α^{2k} va fi valoare proprie a lui Frobenius aplicat pe spațiul de pe urmă. Ca urmare, va avea loc:

$$q^{\frac{2kd}{2} - \frac{1}{2}} \leq |\alpha|^{2k} \leq q^{\frac{2kd}{2} + \frac{1}{2}}$$

Scoțând radical de ordin $2k$, obținem:

$$q^{\frac{d}{2} - \frac{1}{4k}} \leq |\alpha| \leq q^{\frac{d}{2} + \frac{1}{4k}}$$

Cum relația are loc pentru k arbitrar, trecându-l la infinit, obținem $|\alpha| = q^{\frac{d}{2}}$.

De acum înainte, prin urmare, d va fi par.

În acest moment, după ce am încheiat reducerile geometrice de mai devreme, putem trece la miezul problemei și să introducem tehnica numită *pencil Lefschetz*.

Alegem o scufundare a lui X într-un \mathbb{P}^N și luăm L un subspațiu liniar proiectiv de codimensionalitate 2 ce intersectează transversal pe X . Mulțimea hiperplanelor din \mathbb{P}^N ce conțin pe L are ca spațiu de moduli pe \mathbb{P}^1 și deci poate fi organizată ca o familie $\{H_d\}_{d \in \mathbb{P}^1}$. Iau apoi mulțimea:

$$\tilde{X} = \{(x, d) \in X \times \mathbb{P}^1 \mid x \in H_d\}$$

ce are structură de varietate algebrică, anume este *eclatarea lui X în $L \cap X$* (este netedă, din faptul că L intersectează transversal pe X). Ea este înzestrată cu două aplicații canonice:

$$X \leftarrow \tilde{X} \xrightarrow{f} \mathbb{P}^1$$

iar din teoria eclatării, aplicația $H^d(X, \mathbb{Q}_\ell) \rightarrow H^d(\tilde{X}, \mathbb{Q}_\ell)$ este injectivă. Putem trece deci de la X la \tilde{X} fără probleme.

Ceea ce caracterizează \tilde{X} este că este înzestrat cu aplicația $f : \tilde{X} \rightarrow \mathbb{P}^1$. Ea se numește **pencil Lefschetz** dacă numai un număr finit de fibre $f^{-1}(d)$, pentru d din \mathbb{P}^1 (fibre pe care le vom nota cu \tilde{X}_d) sunt singulare, iar acelea care sunt au drept singularități numai câte un punct dublu ordinare. Presupun că fac o extindere a corpului astfel încât toate aceste singularități să fie definite de ecuații peste corpul nou.

Toată această construcție depinde de alegerea scufundării și a L -ului. Însă există un rezultat ce ne spune că există măcar o scufundare și un L corespunzător astfel încât f -ul rezultat să fie pencil Lefschetz (dacă lucrăm în caracteristică 0 există un L în fiecare scufundare).

Notăm cu U mulțimea d -urilor din \mathbb{P}^1 pentru care fibra e netedă, cu S complementara lui U și cu j aplicația de incluziune a lui U în \mathbb{P}^1 .

Ne vom folosi în continuare de șirul spectral Leray, ale cărui aplicații sunt compatibile cu operatorii Frobenius:

$$E_2^{p,q} = H^p(\mathbb{P}^1, R^q f_* \mathbb{Q}_\ell) \Rightarrow H^{p+q}(\tilde{X}, \mathbb{Q}_\ell)$$

Deci $H^d(\tilde{X}, \mathbb{Q}_\ell)$ admite o filtrare cu spațiile cât $\{E_\infty^{p,q}\}_{p+q=d}$, care la rândul lor sunt subcături ale $E_2^{p,q}$ -uri, ca urmare e suficient să arăt pentru spațiile din stânga. Dintr-o teoremă de anulare, acestea sunt nenule doar pentru p între 0 și 2.

Notez $d - 1$ cu n (număr impar). Astfel ne-am redus la a considera următoarele spații:

$$H^2(\mathbb{P}^1, R^{n-1}f_*\mathbb{Q}_\ell); H^0(\mathbb{P}^1, R^{n+1}f_*\mathbb{Q}_\ell); H^1(\mathbb{P}^1, R^n f_*\mathbb{Q}_\ell)$$

Ne va fi de folos următorul rezultat:

Teorema 4.2. (a ciclilor evanescenti) Fie u din U . Există E subspațiu vectorial al lui $H^n(\tilde{X}_u, \mathbb{Q}_\ell)$ (spațiul ciclilor evanescenti) astfel încât:

I. Când $E = 0$:

1. Fasciculul $R^i f_*\mathbb{Q}_\ell$ este constant pentru $i \neq n + 1$.
2. Există un șir exact scurt de fascicule pe \mathbb{P}^1 :

$$0 \rightarrow \bigoplus_{s \in S} (\mathbb{Q}_\ell(-\frac{n+1}{2}))_s \rightarrow R^{n+1}f_*\mathbb{Q}_\ell \rightarrow \underline{H^{n+1}(\tilde{X}_u, \mathbb{Q}_\ell)} \rightarrow 0$$

II. Când $E \neq 0$ (ceea ce se întâmplă mai frecvent):

1. Fasciculul $R^i f_*\mathbb{Q}_\ell$ este constant pentru $i \neq n$.
2. $R^n f_*\mathbb{Q}_\ell = j_* j^* R^n f_*\mathbb{Q}_\ell$.
3. E este subspațiu stabil la acțiunea lui $\pi_1(U, u)$ iar acțiunea pe spațiul cât este trivială.
4. Notând cu E^\perp subspațiul $H^n(\tilde{X}_u, \mathbb{Q}_\ell)^{\pi_1(U, u)}$, avem că acțiunea pe $\frac{E}{E \cap E^\perp}$ este absolut ireducibilă.
5. Notăm fasciculele constructibile pe U asociate lui E și E^\perp cu \mathcal{E} , respectiv \mathcal{E}^\perp (ambele sunt subfascicule ale lui $j^* R^n f_*\mathbb{Q}_\ell$, ce corespunde lui $H^n(\tilde{X}_u, \mathbb{Q}_\ell)$).
 - a) dacă $E \subseteq E^\perp$, există șirul exact de fascicule pe \mathbb{P}^1 :

$$0 \rightarrow j_* \mathcal{E}^\perp \rightarrow R^n f_*\mathbb{Q}_\ell \rightarrow j_* \left(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}^\perp} \right) \rightarrow \bigoplus_{s \in S} (\mathbb{Q}_\ell(-\frac{n+1}{2}))_s \rightarrow 0$$

- b) dacă $E \not\subseteq E^\perp$, există următoarele două șiruri exacte scurte de fascicule pe \mathbb{P}^1 :

$$0 \rightarrow j_* \mathcal{E} \rightarrow R^n f_*\mathbb{Q}_\ell \rightarrow j_* \left(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}} \right) \rightarrow 0$$

$$0 \rightarrow j_*(\mathcal{E} \cap \mathcal{E}^\perp) \rightarrow j_* \mathcal{E} \rightarrow j_* \left(\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp} \right) \rightarrow 0$$

6. Produsul cup pe coomologia lui \tilde{X}_u induce o biliniară symplectică

$$\psi : \frac{E}{E \cap E^\perp} \times \frac{E}{E \cap E^\perp} \rightarrow \mathbb{Q}_\ell(-n)$$

care este echivariantă relativ la acțiunea lui $\pi_1(U, u)$, iar aplicația canonică rezultantă:

$$\pi_1(U, u) \rightarrow \mathrm{Sp}\left(\frac{E}{E \cap E^\perp}, \psi\right)$$

are imaginea deschisă și densă.

Mai departe, pot presupune că există u_0 punct al lui U definit peste \mathbb{F}_q astfel încât \tilde{X}_{u_0} admite o secțiune hiperplană netedă Z_0 , la rândul ei definită peste \mathbb{F}_q (făcând eventual extinderi), de dimensiune, firește, $d-2$ (fiind tot pară, voi putea aplica un raționament prin inducție mai jos).

Demonstrăm mai întâi aserțiunea despre spațiile $H^2(\mathbb{P}^1, R^{n-1}f_*\mathbb{Q}_\ell)$ și $H^0(\mathbb{P}^1, R^{n+1}f_*\mathbb{Q}_\ell)$.

Dat fiind că fasciculul $R^{n-1}f_*\mathbb{Q}_\ell$ este constant în ambele cazuri, el are fibra $H^{n-1}(\tilde{X}_u, \mathbb{Q}_\ell)$, din teorema de schimbare proprie a bazei. Deci $H^2(\mathbb{P}^1, R^{n-1}f_*\mathbb{Q}_\ell) = H^2(\mathbb{P}^1, H^{n-1}(\tilde{X}_u, \mathbb{Q}_\ell)) = H^2(\mathbb{P}^1, \mathbb{Q}_\ell) \otimes H^{n-1}(\tilde{X}_u, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-1) \otimes H^{n-1}(\tilde{X}_u, \mathbb{Q}_\ell) = H^{n-1}(\tilde{X}_u, \mathbb{Q}_\ell)(-1)$. Pentru ultimul modul putem aplica ipoteza de inducție, deoarece se scufundă (din teorema Lefschetz slabă) în $H^{n-1}(Z, \mathbb{Q}_\ell)(-1)$, pentru care aplic ipoteza de inducție.

Pentru $H^0(\mathbb{P}^1, R^{n+1}f_*\mathbb{Q}_\ell)$, în cazul în care E e nenul, argumentul funcționează asemănător cu cel precedent, cu deosebirea că aplicăm surjectivitatea morfismului Gysin, care schimbă și rangul coomologiei de la $n+1$ la $n-1$ pentru Z pentru a putea funcționa inducția. Când E este nul, nu fac decât să trec de la șirul exact scurt din teoremă la șirul exact lung în coomologie și să aplic acolo inducția.

Ne-a rămas $H^1(\mathbb{P}^1, R^n f_*\mathbb{Q}_\ell)$. Când E este nul, $R^n f_*\mathbb{Q}_\ell$ este constant și cum $H^1(\mathbb{P}^1, \mathbb{Q}_\ell) = 0$, am și $H^1(\mathbb{P}^1, R^n f_*\mathbb{Q}_\ell) = 0$ și deci nu am nimic de demonstrat.

Când E este nenul, trec prin j_* incluziunea de fascicule de pe U într-una pe \mathbb{P}^1 :

$$0 \subseteq j_*(\mathcal{E} \cap \mathcal{E}^\perp) \subseteq j_*\mathcal{E} \subseteq R^n f_*\mathbb{Q}_\ell$$

(la ultimul am aplicat punctul 2 din cazul II al teoremei).

Subcazul simplu este $E \subseteq E^\perp$. Notând cu \mathcal{F} conucleul morfismului $j_*\mathcal{E}^\perp \rightarrow R^n f_*\mathbb{Q}_\ell$, ce este izomorf cu nucleul morfismului $j_*(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}^\perp}) \rightarrow \bigoplus_{s \in S} (\mathbb{Q}_\ell(-\frac{n+1}{2}))_s$, putem sparge șirul exact din teoremă în două șiruri exacte scurte:

$$\begin{aligned} 0 \rightarrow j_*\mathcal{E}^\perp \rightarrow R^n f_*\mathbb{Q}_\ell \rightarrow \mathcal{F} \rightarrow 0 \\ 0 \rightarrow \mathcal{F} \rightarrow j_*(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}^\perp}) \rightarrow \bigoplus_{s \in S} (\mathbb{Q}_\ell(-\frac{n+1}{2}))_s \rightarrow 0 \end{aligned}$$

Cum $j_*(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}^\perp})$ e constant, are H^1 nul (suntem pe \mathbb{P}^1), și rezultă că în al doilea șir exact lung corespunzător, morfismul conectant de la H^0 la H^1 e surjectiv, și rezultă ce trebuie pentru $H^1(\mathbb{P}^1, \mathcal{F})$. La fel, $j_*\mathcal{E}^\perp$ e constant și deci modulul nostru, $H^1(\mathbb{P}^1, R^n f_*\mathbb{Q}_\ell)$ se scufundă în $H^1(\mathbb{P}^1, \mathcal{F})$ (considerând primul șir exact lung corespunzător). De aici rezultă concluzia.

Trecem la subcazul ce prezintă probleme, $E \not\subseteq E^\perp$. Din cele două șiruri exacte lungi corespunzătoare șirurilor exacte scurte din teoremă, obțin că este suficient să arăt aserțiunea pentru modulul $H^1(\mathbb{P}^1, j_*(\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp}))$ (am folosit că $j_*(\mathcal{E} \cap \mathcal{E}^\perp)$ și $j_*(\frac{j^* R^n f_*\mathbb{Q}_\ell}{\mathcal{E}})$ sunt constante).

În primul rând, pot arăta doar $|\alpha| \leq q^{\frac{d+1}{2}}$ (utilizând dualitatea și forma symplectică).

În al doilea rând, dat fiind că $\text{supp coker}(j_!(\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp}) \rightarrow j_*(\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp})) = S$ (zero-dimensional și finit), am că $H^1(\mathbb{P}^1, \text{coker}) = 0$, și ca urmare morfismul indus pe H^1 este surjectiv. Am

redus la a studia problema pe $H^1(\mathbb{P}^1, j_!(\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp})) = H_c^1(U, \frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp})$. Vom refolosi notația \mathcal{F} pentru a denota fasciculul $\frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{E}^\perp}$ pe U , iar \mathcal{F}_0 va fi fasciculul corespunzător pe $U(\mathbb{F}_q)$. Notăm cu V $\pi_1(U_0, u)$ -reprezentarea corespunzătoare. Reamintim că avem biliniara symplectică $\pi_1(U, u)$ -echivariantă:

$$\psi : V \times V \rightarrow \mathbb{Q}_\ell(-n)$$

iar aplicația canonică rezultantă $\pi_1(U, u) \rightarrow \mathrm{Sp}(\frac{E}{E \cap E^\perp}, \psi)$ are imaginea deschisă și densă.

Definim, prin analogie cu funcția zeta, L-funcția fasciculului \mathcal{F}_0 ca:

$$L(U_0, \mathcal{F}_0, t) = \prod_{x \in U} \det(1 - t^{\deg(x)} F^{\deg(x)}, \mathcal{F}_x)^{-1}$$

care este egală dintr-o formulă de tip Lefschetz cu

$$\prod_{i=0}^2 \det(1 - t F_{|H_c^i(U, \mathcal{F})})^{(-1)^{i+1}}$$

Însă dat fiind că adică V este reprezentare absolut ireductibilă, H_c^2 , fiind egal cu dualul spațiului de coinvarianți, este nul. Din faptul că U este afină (dacă ar fi toată dreapta proiectivă, putem aplica tot raționamentul mai întâi scoțând 0, iar apoi scoțând ∞), H_c^0 este tot nul. Deci L-funcția conține doar termenul corespunzător lui H_c^1 , care se află în atenția noastră, și este în particular polinomială cu coeficienți raționali (de aici rezultă că valorile proprii sunt algebrice).

Întâi arătăm că este suficient să demonstrăm că pentru orice x și pentru orice α valoare proprie a operatorului Frobenius asociat fibrei \mathcal{F}_x am $|\alpha| = q^{\frac{n}{2} \deg(x)}$. Cum:

$$L(U_0, \mathcal{F}, t) = \prod_{x \in U_0} \det(1 - F^{\deg(x)} t^{\deg(x)}, \mathcal{F}_x)^{-1} = \prod_{x \in U_0} \prod_{i=1}^r (1 - t^{\deg(x)} \alpha_{x,i})^{-1}$$

a cărei absolut convergență (din faptul că $|\alpha_{x,i}| = q^{\frac{n}{2} \deg(x)}$) este echivalentă cu a seriei:

$$\sum_{x \in U_0} r q^{\deg(x) \frac{n}{2}} t^{\deg(x)} \leq \sum_{s \geq 1} r q^s q^s \frac{n}{2} t^s$$

ultima fiind convergentă pentru $|t| < q^{-\frac{n}{2}-1}$. Deci în acea zonă nu sunt poli, ca urmare $q^{-\frac{n}{2}-1} < \alpha^{-1}$, ceea ce trebuia demonstrat.

Mai departe vom vedea că putem să arătăm doar *condiția de raționalitate pe fibre*, i.e. că pentru orice x din U , $\det(1 - F^{\deg(x)} t_{|\mathcal{F}_x})$ este polinom cu coeficienți raționali (**lema principală a lui Deligne**).

Pentru aceasta, vom afirma și demonstra în primul rând că pentru orice k natural, $\det(1 - F^{\deg(x)} t_{|\mathcal{F}_x^{\otimes 2k}})^{-1}$ este serie formală cu coeficienți numere raționale pozitive. Notând $T = t^{\deg(x)}$, avem:

$$\begin{aligned} T \frac{d}{dT} \log \det(1 - F^{\deg(x)} t_{|\mathcal{F}_x^{\otimes 2k}})^{-1} &= \sum_{r \geq 1} \mathrm{Tr}(F_{|\mathcal{F}_x^{\otimes 2k}}^r)^{\deg(x)} T^r \\ &= \sum_{r \geq 1} \mathrm{Tr}(F_{|\mathcal{F}_x}^r)^{2k} T^r \in \mathbb{Q}_+[[t]] \end{aligned}$$

iar inversând operațiile aplicate la început se păstrează caracterul rațional pozitiv.

A doua afirmație pe care o facem este că dacă α este pol pentru $L(U_0, \mathcal{F}^{\otimes 2k}, t)$ și toți polii sunt situați pe raza de convergență, iar α_x este zerou pentru $\det(1 - F^{\deg(x)} t_{|\mathcal{F}_x^{\otimes 2k}})^{-1}$, primul are modulul mai mic ca al doilea.

Ca să demonstrăm aceasta, notăm $\det(1 - F^{\deg(x)} t_{|\mathcal{F}_x^{\otimes 2k}})^{-1}$ cu $f_x(t)$, și avem $L(U_0, \mathcal{F}^{\otimes 2k}, t) = \prod_x f_x(t)$. Prin urmare, din pozitivitate rezultă că raza de convergență a lui L e mai mică decât a oricărui f_x și deci $\alpha \leq \alpha_x$.

Putem trece acum la demonstrația lemei principale a lui Deligne.

Dat fiind că U este afină, $H_c^0(U, \mathcal{F}^{\otimes 2k}) = 0$, iar

$$\begin{aligned} H_c^2(U, \mathcal{F}^{\otimes 2k}) &\simeq (H^0(U, (\mathcal{F}^\vee)^{\otimes 2k}))^\vee(-1) \\ &\simeq (((\mathcal{F}^\vee)^{\otimes 2k})_u)^{\pi_1(U, u)^\vee}(-1) \\ &\simeq ((\mathcal{F}^{\otimes 2k})_u)^{\pi_1(U, u)}(-1) \\ &\simeq ((\mathcal{F}^{\otimes 2k})_u)_{\text{Sp}(\mathcal{F}_u, \psi)}(-1) \\ &\simeq \mathbb{Q}_\ell(-kn - 1)^N \end{aligned}$$

pentru un anumit N , ultimul izomorfism rezultând din teoria reprezentării grupurilor simplectice.

Rezultă că numitorul L -funcției este $(1 - q^{kn+1}t)^N$, și deci toți polii sunt situați pe raza de convergență, q^{-kn-1} . A doua afirmație făcută mai sus ne spune că în acest caz:

$$q^{(-kn-1)\deg(x)} \leq |a^{2k}|^{-1}$$

Scoțând radical de ordin $2k$ și ducând pe k la infinit rezultă concluzia.

Rămâne să arătăm condiția de raționalitate pe fibre. Ne folosim de următorul rezultat:

Lema 4.3. Fie \mathcal{G}_0 un fascicul pe U_0 astfel încât \mathcal{G} e constant. Grupul Galois absolut al lui \mathbb{F}_q , $G_{\mathbb{F}_q}$, este cât al lui $\pi_1(U_0, u)$. Atunci aplicația canonică $\pi_1(U_0, u) \rightarrow GL(\mathcal{G}_u)$ factorizează prin $G_{\mathbb{F}_q}$ și deci există $\alpha_1, \dots, \alpha_k$ unități ℓ -adice astfel încât pentru orice x , $\det(1 - tF_x, \mathcal{G}_u) = \prod_{i=1}^k (1 - \alpha_i^{\deg(x)} t)$.

Demonstrație. Dat fiind că \mathcal{G} e constant, $\pi_1(U, u)$ acționează trivial, și de aici rezultă factorizarea prin $G_{\mathbb{F}_q}$. \square

Avem $\zeta_{\tilde{X}_x}(t) = \prod_i \det(1 - tF_{|H^i(\tilde{X}_x, \mathbb{Q}_\ell)}^{\deg(x)})^{(-1)^{i+1}} = \prod_i \det(1 - tF_{|(R^i f_* \mathbb{Q}_\ell)_x}^{\deg(x)})^{(-1)^{i+1}}$. Și cum toate fasciculele R^i sunt constante în afară de R^n , iar acesta din urmă se poate filtra în $\frac{R^n f_* \mathbb{Q}_\ell}{\mathcal{E} \cap \mathcal{E}^\perp}$ și $\mathcal{E} \cap \mathcal{E}^\perp$, unde primul și ultimul sunt constante. Deci putem scrie funcția ca:

$$\zeta_{\tilde{X}_x}(t) = \frac{(1 - \alpha_1^{\deg(x)} t) \dots (1 - \alpha_r^{\deg(x)} t)}{(1 - \beta_1^{\deg(x)} t) \dots (1 - \beta_s^{\deg(x)} t)} \det((1 - F_x t)|_V)$$

unde membrul stâng este clar rațional. Dacă arătăm că fracția din membrul drept este rațională, va reieși și raționalitatea ultimului termen, pe care dorim să o arătăm.

Este, însă, suficient să arătăm că pentru orice $\tau \in \text{Gal}(\overline{\mathbb{Q}_\ell})$ există $x \in U_0$ de grad k astfel încât:

1. nu există i, j cu $(\frac{\alpha_i}{\beta_j})^k = 1$
2. nu există i astfel încât $\frac{\alpha_i}{\tau(\alpha_i)}$ să fie rădăcină netrivială a unității (și la fel pentru β -uri)
3. α -urile și β -urile ridicate la puterea k (precum și imaginile lor prin τ^{-1}) nu sunt în $\text{Spec}(F_{x|V})$

Astfel, orice asemenea τ lasă fracția pe loc, ca urmare ea are coeficienții raționali.

Pentru a arăta însă presupunerea făcută, ne vom folosi de:

Propoziția 4.4. *Pentru orice λ unitate ℓ -adică, mulțimea $Z = \{\sigma \in \pi_1(U_0, u) \mid \lambda^{v(\sigma)} \in \text{Spec}(\sigma|_V)\}$ este închisă în $\pi_1(U_0, u)$ și de măsură Haar nulă.*

Demonstrație. Considerăm grupul de asemănări simplectice:

$$\text{GSp}(V, \psi) = \{\alpha \in \text{GL}(V) \mid \text{există } \mu \text{ astfel încât pentru orice } x, y \text{ avem } \psi(\alpha(x), \alpha(y)) = \mu\psi(x, y)\}$$

Din șirul exact de grupuri de mai devreme, orice acțiune a unui σ din $\pi_1(U_0, u)$ este o asemănare cu $\mu(\sigma) = q^{v(\sigma)}$.

Fie mulțimea:

$$H = \{(\alpha, n) \in \text{GSp}(V, \psi) \times \hat{\mathbb{Z}} \mid \mu(\alpha) = q^n\}$$

și aplicația naturală ρ_1 de la $\pi_1(U_0, u)$ la H .

Pentru simplificarea demonstrației, vom presupune că q este rest pătratic modulo ℓ .

Pot identifica H cu $H' = \text{Sp}(V) \times \hat{\mathbb{Z}}$ prin aplicația $(\alpha, n) \mapsto (q^{\frac{n}{2}}\alpha, n)$ și este suficient să arăt concluzia pentru mulțimea $Z' = \{(\alpha, n) \mid \lambda' \in \text{Spec}(\alpha)\}$ (unde am notat $\lambda' = q^{\frac{n}{2}}\lambda$).

Clar este o mulțime închisă, fiind dată de ecuații determinanțale.

Fixând n , notez P_n polinomul minimal al lui λ'^n peste \mathbb{Q}_ℓ . Mulțimea $Z'_n = \{\alpha \in \text{Sp}(V, \psi) \mid \lambda'^n \in \text{Spec}(\alpha)\}$ este algebrică, deci de măsură Haar nulă. În final, putem zice:

$$\mu(Z') = \int_{n \in \hat{\mathbb{Z}}} \mu(Z'_n) = 0$$

□

În sfârșit putem arăta existența punctului. Din teorema de densitate Cebotarev, rezultă că este suficient să arătăm că mulțimea acelor σ ce satisfac acele proprietăți 1-3 de mai sus (cu $k = v(\sigma)$, în cazul în care este întreg, și cu $F_{x|V}$ înlocuit de σ) conține un deschis de măsură Haar nenulă.

Însă propoziția anterioară arată că mulțimea elementelor ce satisfac (3) este deschisă de măsură Haar totală, iar mulțimea elementelor eliminate de condițiile (1) și (2) este clar neglijabilă.

S-a demonstrat deci ipoteza lui Riemann.