Cours 1 Quelques fonctions L d'origine galoisienne

But: Expliquer deux constructions de fonctions L "d'origine arithmétique" : fonctions L d'Artin et fonctions L de courbes elliptiques / c.d.m. (cas particuliers de fonctions L / ξ à la Hasse-Weil). Dans les deux cas elles sont associées à des représentations de Groupes de Galois (ce sera évident pour celles d'Artin). On rappellera quelques conjectures classiques portant sur ces fonctions L (prob. analytique, valeurs spéciales). Dans tous les cas où ces conj. ont été résolues, c'est en montrant qu'elles sont de nature "automorphe" : motivation importante des conj. de Langlands.

I) Rappels sur les Frobeniens

(1.) $K/\mathbb{Q}$ corps de nombres galoisien sur $\mathbb{Q}$

$p \in \mathbb{Z}$ premier, $\mathcal{P}_p = \{ \mathfrak{P} \subset \mathcal{O}_K$ id. premiers (i.e contenant p) $\mid (p) \}$

(on a $(p)\mathcal{O}_K = \prod_{\mathfrak{P} \in \mathcal{P}_p} \mathfrak{P}^{e_{\mathfrak{P}}}$)

$G := \mathrm{Gal}(K/\mathbb{Q})$ agit sur $\mathcal{P}_p$: $(\sigma, \mathfrak{P}) \longmapsto \sigma(\mathfrak{P})$

on sait que cette action est transitive ($\Leftrightarrow e_{\mathfrak{P}} = e_p$ ind. de $\mathfrak{P}$)

$G \supset G_{\mathfrak{P}}$ = stabilisateur de $\mathfrak{P}$ dans G = gp. déc. en $\mathfrak{P}$

il agit sur $k_{\mathfrak{P}} := \mathcal{O}_K/\mathfrak{P}$ corps fini $\simeq \mathbb{F}_q$ $q = p^{f_{\mathfrak{P}}}$ (cor. ?)

$\mathrm{red}_{\mathfrak{P}} : G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ un hom. $I_{\mathfrak{P}} = \ker_{\mathfrak{P}}$ groupe d'inertie en $\mathfrak{P}$.

(i.e $I_{\mathfrak{P}} = \{ \sigma \in G_{\mathfrak{P}},\ \sigma x \equiv x \ (\mathfrak{P}) \ \forall x \in \mathcal{O}_K \}$.)

Fait 1. $\mathrm{red}_{\mathfrak{P}}$ est surjectif, i.e. $\exists\, \mathrm{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}}$, unique mod $I_{\mathfrak{P}}$, t.q. $\mathrm{red}_{\mathfrak{P}}(\mathrm{Frob}_{\mathfrak{P}}) =$ le frob. de $k_{\mathfrak{P}}/\mathbb{F}_p = x \mapsto x^p$.

autrement dit $\mathrm{Frob}_{\mathfrak{P}}\, x \equiv x^p \ (\mathfrak{P}) \quad \forall x \in \mathcal{O}_K$.

une façon de le voir : (point de vue local sur $G_{\mathfrak{P}}$).

on regarde $K_{\mathfrak{P}}$ = complété de K pour $|x| = q^{-v_{\mathfrak{P}}(x)}$ valuation $\mathfrak{P}$-adique.

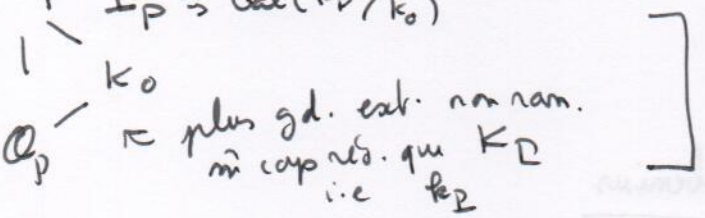
$$= \left(\varprojlim_n \left(\mathcal{O}_K / \mathfrak{P}^n \right) \right) \left[\tfrac{1}{p} \right]$$

c'est une ext. gal. finie de $\mathbb{Q}_p$, $K \longrightarrow K_{\mathfrak{P}}$ inj. d'im. dense.

d'où $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$, induit $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbb{Q}_p) \xrightarrow{\sim} G_{\mathfrak{P}}$

$\sigma \longmapsto \sigma|_K$.

on a



Fait 2 (évident) Soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, on a $\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\sigma(\mathfrak{P})}$, $\sigma I_{\mathfrak{P}} \sigma^{-1} = I_{\sigma(\mathfrak{P})}$ et $\sigma\, \mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1} \equiv \mathrm{Frob}_{\sigma(\mathfrak{P})} \mod I_{\mathfrak{P}}$

Cor : i) $\forall \mathfrak{p}$, les $G_{\mathfrak{P}}$ avec $\mathfrak{P} | \mathfrak{p}$ classe de conj. can. de ss-ens gpes de $\mathrm{Gal}(K/\mathbb{Q})$.

ii) si p non ram dans K, i.e. $p \nmid \mathrm{disc}\, \mathcal{O}_K \Leftrightarrow e = 1$, $\Rightarrow I_{\mathfrak{P}} = 1$, alors $\mathrm{Frob}_{\mathfrak{p}} = \{ \mathrm{Frob}_{\mathfrak{P}},\ \mathfrak{P} \in \mathcal{S}_{\mathfrak{p}} \}$ classe de conj. dans $\mathrm{Gal}(K/\mathbb{Q})$

Rk : $\mathfrak{p} \longmapsto \mathrm{Frob}_{\mathfrak{p}} \subset G$ contient beaucoup de l'arithm. de K.

$\mathfrak{p} \nmid \mathrm{disc}\, K$

ex. ordre de $\mathrm{Frob}_{\mathfrak{P}} = f$ l'unique inconnue dans la déc. de (p)

• analogue archimédien : classe de conj. des conjugaisons complexes

$\mathrm{Frob}_{\mathcal{L}} = \{ c_\sigma,\ \sigma : K \to \mathbb{C} \}$ où $c_\sigma(x) = \sigma^{-1}(\sigma(x))$.

ξ

Exemple 1 $K = \mathbb{Q}(e^{2i\pi/N})$. $N \geq 1$ entier

hom. can. ε : $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ "can. cycl."

$\sigma \longmapsto$ l'unique k t.q. $\sigma(\xi) = \xi^k$

(ex : morph. de gplés. $\mathfrak{p} \nmid N \Rightarrow \mathfrak{p}$ non ram dans K.
inj. si σ

on a $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ (singleton : cas abélien).

$$\boxed{\varepsilon(\mathrm{Frob}_{\mathfrak{p}}) = p}$$

Ca bien connu (Gauss). ε surjectif ! i.e $[K : \mathbb{Q}] = \varphi(N)$.

Exemple 2 Soit $Q \in \mathbb{Z}[X]$ unitaire irréd. — soit $p \in \mathbb{Z}$
nb premier, $Q \bmod p \equiv \prod Q_i^{e_i}$, $Q_i \in \mathbb{Z}/p\mathbb{Z}[X]$ unit irréd.

pb non résolu de comprendre $p \longrightarrow$ type de décomp. de $Q \bmod p$
ex. $\deg Q_i$?

ex : pour quels p $Q \bmod p$ scindé mod p ? ($p \nmid \mathrm{disc}\, Q$ nécessaire).
$\prod_{i=1}^{r} e_i = \deg Q$

- $Q = X^2 - m$ .... solution donnée par la loi de réciprocité quad.

$p \nmid 4m$, m carré mod p $\Leftrightarrow$ $p \in H_m \subset (\mathbb{Z}/4m\mathbb{Z})^*$ "explicite"
où H_m ss groupe d'indice 2

Lien avec les Frobenius : K = un corps de déc. de Q.

si $R = \{$racines de Q dans $\mathbb{C}\}$, $K = \mathbb{Q}(R)$

$Q(X) = \prod_{x \in R} (X - x)$ scindé dans $\mathcal{O}_K[X]$.

$\mathrm{Gal}(K/\mathbb{Q})$ agit sur R : $g : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathfrak{S}(R)$

si $p \nmid \mathrm{disc}\, Q$ (donc de K) $\Rightarrow$ $g(\mathrm{Frob}_{\mathfrak{P}})$ est une permutation de R dont les cycles sont de longueur $\deg Q_i$!
$\mathfrak{P} \mid (p)$.

$\Rightarrow$ pt. cos pot. de répartition des $\mathrm{Frob}_{\mathfrak{p}}$ dans $\mathrm{Gal}(K/\mathbb{Q})$.

II Fonctions L d'Artin (Référence : dernier chapitre de Neukirch)

$K/\mathbb{Q}$ c.d.n Galoisien $\quad G = \mathrm{Gal}(K/\mathbb{Q})$ gpe fini.

soit $\rho : G \to GL(V)$ hom. V $\mathbb{C}$-ev de dim fini.

on va définir $L(s,\rho)$ une série de Dirichlet associée.

$$\| \\ \prod_p L_p(s,\rho).$$

cas le plus simple : p non ramifié dans K, $\mathrm{Frob}_p \subset \mathrm{Gal}(K/\mathbb{Q})$ classe de conj. constitué d'éléments 2 à 2 conjugués.

$\rho(\mathrm{Frob}_p) \subset GL(V)$

$\Rightarrow Q_p(X) := \det(1 - X\rho(\mathrm{Frob}_p))$ polynôme bien défini

$= 1 - \mathrm{tr}\,\rho(\mathrm{Frob}_p)X + \dots + (-1)^{\dim V} X^{\dim V} \det\rho(\mathrm{Frob}_p)$

On pose $\boxed{L_p(s,\rho) = \dfrac{1}{Q_p(p^{-s})}}$

- cas général $p \in \mathbb{Z}$, soit $\mathfrak{P} \mid (p)$. on regarde

$$V \supset V^{I_{\mathfrak{P}}} = \{v \in V,\ \rho(g)v = v \ \ \forall g \in I_{\mathfrak{P}}\}.$$

sous-esp. sur lequel agit $G_{\mathfrak{P}}/I_{\mathfrak{P}} = \langle \mathrm{Frob}_{\mathfrak{P}} \rangle$.

on pose $Q_p(X) := \det\left(1 - X\rho(\mathrm{Frob}_{\mathfrak{P}})\big|_{V^{I_{\mathfrak{P}}}}\right)$

ne dépend pas du choix de $\mathfrak{P}$ à cause du Fait 2.

($\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ $\quad \sigma(V^{I_{\mathfrak{P}}}) = V^{\sigma I_{\mathfrak{P}} \sigma^{-1}} = V^{I_{\sigma(\mathfrak{P})}}$ ...)

Prop : i) $L(s,\rho)$ conv. abs. pour $\mathrm{Re}\, s > 1$

ii) $L(s,\rho)$ ne dépend que de la classe d'éq. de ρ. (comme rep.)

iii) $L(s,\rho_1 \oplus \rho_2) = L(s,\rho_1)\,L(s,\rho_2)$.

iv) $L(s,\rho) = \sum a_n n^{-s}$, $p \nmid \mathrm{disc}\, K$, $a_p = \mathrm{trace}(\rho(\mathrm{Frob}_p))$

preuve : i) tout élément de G est d'ordre fini, donc les vp des $\rho(g)$ sont de racine de l'unité $\Rightarrow$ racine de $Q_p(X)$ donc Φ sont de module 1 i.e ${}^{\chi}Q_1(p^{-s})$ est produit de termes de la forme $\frac{1}{1-\alpha_p p^{-s}}$. $\Rightarrow |L(s,\rho)| \leq \zeta(\mathrm{Re}(s))^{[K:\mathbb{Q}]}$.

ii) iii) iv) évidents ■

Exemple 1 ρ = rep. triviale de dim 1, on a $L(s,\rho) = \zeta(s)$ Riemann. car $Q_p(X) = 1 - X \ \forall p$.

Exemple 2 K = corps de déc. de $\mathbb{Q}(R)$ où R = trait. de $\mathbb{Q}$ dans $\mathbb{Q}$. $\uparrow \mathbb{Z}[X]$.

$(\rho, V) = \mathbb{C}[R]$ (rep. de permutation).

alors $L(s,\rho) = \zeta_K(s)$ ζ de Dedekind.

(laissé en exercice, au moins si $p \nmid \mathrm{disc}\,\mathbb{Q}$ c'est une conséquence immédiate de l'exemple 2 précédent).

Exemple 3 $K = \mathbb{Q}(e^{2i\pi/N})$, $\varepsilon : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$

et $\dim V = 1$. Ops $V = \Phi$, $\rho = \chi \circ \varepsilon$: $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow GL_1(\mathbb{C}) = \mathbb{C}^\times$

où χ car. de Dirichlet.

Alors $L(s,\rho) = L(s,\chi')$ où χ' est le car. de Dirichlet primitif ↖ fonction L de Dirichlet ass. à χ. i.e χ se factorise en

$$(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$$
$$\chi$$

avec $M \mid N$ minimal.

Laissé en exercice pour $p \mid N$, si $p \nmid N$ c'est une conséquence immédiate de l'Exemple 1 précédent.

En général on doit utiliser le

Lemme : $L / K / \mathbb{Q}$ (Galois / Galois), $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$ rep.

$\tilde{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\text{can}} \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$

rep. composée ("inflation de ρ"), alors $L(s, \tilde{\rho}) = L(s, \rho)$.

preuve compatibilité de formation des gpes de déc. / Frob.

$p \in \mathbb{Z}$, $P \subset \mathcal{O}_K$, $\mathfrak{Q} \subset \mathcal{O}_L$ avec $\mathfrak{Q} \mid P \mid p$, on a $L_{\mathfrak{Q}} / K_P / \mathbb{Q}_p$

on a $\mathrm{Gal}(L_{\mathfrak{Q}} / \mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(K_P / \mathbb{Q}_p)$. via

$G_{\mathfrak{Q}} \twoheadrightarrow G_P$ $\quad \sigma \mapsto \sigma \mid K$

puis $I_{\mathfrak{Q}} \twoheadrightarrow I_P$

$\mathrm{Frob}_{\mathfrak{Q}} \mid P \equiv \mathrm{Frob}_P \bmod I_P$ ■

Conjecture (Artin). ρ arbitraire

i) $L(s, \rho)$ se prolonge méro. à $\mathbb{C}$ tout entier, avec $s = 1$ pour unique pole éventuel, et $\mathrm{ord}_{s=1} L(s, \rho) = \langle 1, \rho \rangle$ ("le seul pole possible est $s=1$ et vient de ζ éventuellement")

ii) soit $n_\pm$ = dim du sous-esp de V où "Frob_∞" vaut $\pm \mathrm{id}$

$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2)$ avec $\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$.

fonction Γ d'Euler.

alors si on pose $\xi(s, \rho) = \Gamma_{\mathbb{R}}(s)^{n_+} \Gamma_{\mathbb{R}}(s+1)^{n_-} L(s, \rho)$

on a $$\boxed{\xi(s, \rho) = \varepsilon \cdot N^{s-1/2} \xi(1-s, \rho^\vee)}$$

$\varepsilon \in \mathbb{C}^\times$ (root number). entier explicite (cond. d'Artin)

Théorème La conj. d'Artin est vraie si $\mathrm{Im}\,\rho$ abélien

Preuve : On a $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$.

ρ se factorise par ρ' où $M = K^{\ker \rho} \subset K$

Lemme $\Rightarrow$ $L(s,\rho) = L(s,\rho')$ $\quad \mathrm{Gal}(M/\mathbb{Q})$ et $\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Im}\,\rho$

$\Rightarrow$ o.p.s. $\mathrm{Gal}(K/\mathbb{Q})$ abélien.

- Kronecker-Weber : $K \subset \mathbb{Q}(e^{2i\pi/N})$ $\quad N \geq 1$.

  Lemme encore $\Rightarrow$ o.p.s. $K = \mathbb{Q}(e^{2i\pi/N})$

- $\mathrm{Im}\,\rho$ ab $\Rightarrow$ ρ somme directe de caractères

  Exemple 3 $\Rightarrow$ $L(s,\rho)$ produit de f. L de Dirichlet.

  On conclut par les prop de ces fonctions (Riemann, Dirichlet). ●

Remarque (loi de réciprocité). Si $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$ est injective, alors $\rho(g) = 1 \Leftrightarrow g = 1 \Leftrightarrow$ tt $\rho(s) = \dim V$

donc si $p \nmid \mathrm{disc}\, K$, p tel. déc. dans $K \Leftrightarrow$ tt $\rho(\mathrm{Frob}_p) = \dim V$

donc identifier $L(s,\rho) \Leftrightarrow$ loi de réciprocité généralisée à $\mathrm{Gal}(K/\mathbb{Q})$.

(cette remarque aurait sa place avant !)

Autres choses connues (et difficiles !)

Thm i) $L(s,\rho)$ méro sur $\mathbb{C}$ + ii) connue (Artin, Hecke, Brauer)

(mais on ne connaît pas le pôle dans $0 < \mathrm{Re}(s) < 1$

iii) Si ρ irréd. de dim ≥ 2, et $n_+ = 1$,

conjecture connue (Khare-Wintenberger, Wiles, Serre, ...) Langlands, ...

on montre $\Rightarrow$ $L(s,\rho)$ et la fonction L ass. à une forme modul. pour GL_2

si $n_+ \neq 1$, on conj. que $L(s,\rho)$ et la fonction L d'une "forme de Maass" pour GL_2 .... et plus rad !

III Fonction L d'une courbe elliptique sur un c.d.n

(référence : Tate "arithmetic of elliptic curve" inventiones math.)

soit k un corps. Une courbe ell. sur k sera ici une courbe projective plane cubique $E \subset \mathbb{P}^2_{/k}$ non singulière, munie d'un point point rationnel $O \in E(k)$ qui est d'inflexion.

Exemple fondamental (universel, quitte à changer de coord. linéaires /k, lorsque $6 \in k^\times$) $E :=$ courbe définie par $Y^2Z = X^3 + aXZ^2 + bZ^3$ avec $a, b \in k$, et $\Delta_E := 4a^3 + 27b^2 \in k^\times$, et $2 \in k^\times$ munie de $O := (0:1:0)$.

partie affine $E \cap (Z=1)$: $(x:y:1)$ $\quad y^2 = x^3 + ax + b$ (éq. de Weierstrass) familière.

le lieu singulier vérifierait $2y = 0$ et $P'(x) = 0$ où $P = x^3 + ax + b$ (i.e. $y = 0$ et $2 \in k^\times$ / $P(x)$) donc vide car $2\Delta_E \in k^\times$.

dessin $k = \mathbb{R}$ $\quad O$ ⟨ ou ⟨

partie à ∞ $E \cap (Z=0)$: $\quad 0 = X^3$ un seul point (triple) qui est $O = (0:1:0)$

point lisse / $\bar{k}$? on se place sur $Y=1$ on a $(x:1:z)$ avec $z = x^3 + axz + bz^3$ cqfd

Prop $\exists!$ loi de groupe sur $E(k)$ de neutre O t.q. $\forall P, Q, R \in E(k)$

$P + Q + R = 0 \iff \exists$ droite $D \subset \mathbb{P}^2_{/k}$ t.q $D \cap E(k) = \{P, Q, R\}$ (avec mult.)

Rmq: • $P = -Q \iff \exists$ dte passant par P, Q et O

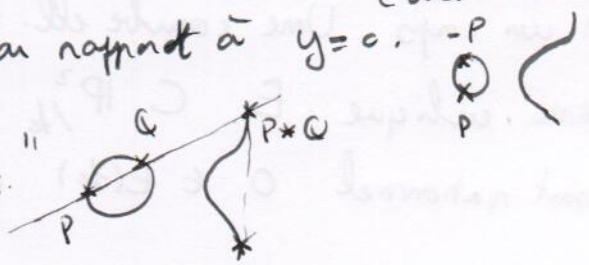
soit $\alpha X + \beta Y + \gamma Z = 0$ une dte générale $\alpha, \beta, \gamma \in k$.

elle passe par $O \iff \beta = 0$. 2 cas: . $\alpha = 0 \Rightarrow$ c'est ssi $Z = 0$

. $\alpha \neq 0 \Rightarrow$ ssi $x = \text{cste}$.

(dte verticale)

$\Rightarrow$ l'opposé de P est le sym. par rapport à $y=0$.



$\Rightarrow P + Q =$ l'opposé du "3e pt d'inter"

• $E(k)$ abélien. L'associativité est la partie la plus difficile.

Citons deux résultats fameux:

Thm (Mordell) k corps de nombres $\Rightarrow E(k)$ gr. ab. type fini

Thm (Hasse) k fini $\Rightarrow \#E(k) = q + 1 - a$

où $q = \#k$ et $|a| \leq 2\sqrt{q}$

Preuves: (cf. Silverman "Arithmetic of ell. curves", ou Tate, pour déf. pour réf.)

On suppose maintenant $k = K$ c.d.n. et E donnée sous forme de Weierstrass avec $a, b \in \mathcal{O}_K$.

Soit $\mathfrak{P}$ premier t.q. $P \nmid 2 \operatorname{disc} E$,

$\mathcal{O}_K$

$\Rightarrow E \bmod \mathfrak{P}$ c. ell sur $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$. $\#k_{\mathfrak{P}} = N\mathfrak{P}$

Hasse $\Rightarrow \#E(k_{\mathfrak{P}}) = \#k_{\mathfrak{P}} + 1 - a_{\mathfrak{P}}$. avec $|a_{\mathfrak{P}}| \leq 2\sqrt{\#k_{\mathfrak{P}}}$

Def: (Hasse, Weil) $$L(s, E) := \prod_{\mathfrak{P} \nmid 2 \operatorname{disc} E} \frac{1}{1 - a_{\mathfrak{P}} N\mathfrak{P}^{-s} + N\mathfrak{P}^{1-2s}}$$

(code "analytiquement" $a_{\mathfrak{P}}$ $\forall \mathfrak{P}$).

Hasse $1 - a_{\mathfrak{p}} X + N\mathfrak{p} X^2 = (1 - \alpha_{\mathfrak{p}} X)(1 - \beta_{\mathfrak{p}} X)$

$a_{\mathfrak{p}}^2 - 4N\mathfrak{p} < 0 \implies \beta_{\mathfrak{p}} = \overline{\alpha_{\mathfrak{p}}}$ et $|\alpha_{\mathfrak{p}}| = |\beta_{\mathfrak{p}}| = \sqrt{N\mathfrak{p}}$.

ex. $\Rightarrow$ $L(s, E)$ cv. abs pour $\mathrm{Re}\, s > 3/2$

Conjectures i) (Hasse-Weil) $L(s, E)$ a un prol. hol. à $\mathbb{C}$ + eq. f. $s \to 2-s$ (convenablement complétée)

ii) (Birch Swinnerton-Dyer) ord$_{s=1} L(s, E) = \dim_{\mathbb{Q}} E(k) \otimes \mathbb{Q}$.

Cas connus : (1) (Wiles - B.C.D.T.) i) connue si $k = \mathbb{Q}$.
ils montrent "E modulaire", ce que l'on peut interpréter comme $L(s, E)$ et la fonction L d'une forme modulaire.

(2) "presque rien" n'est connu sur ii) ($\widehat{m}$ si $k = \mathbb{Q}$)
(de général...).
cs ord = 1 ou 0

(3) Deuring, Hecke : ces "CM" de i) connues.

IV) Esquisse de preuve du prolongement analytique de $L(s, E)$ pour $E : y^2 = x^3 - x$ / $\mathbb{Q}$ (Hecke, Deuring)

$\Delta_E = -4$. $p \neq 2$.

Lemme 1 $\#E(\mathbb{F}_p) = \begin{cases} p+1 & \text{si } p \equiv 3 \ (4) \\ p+1-\pi-\overline{\pi} & \text{si } p \equiv 1 \ (4) \\ & \text{où } \pi \in \mathbb{Z}[i] \text{ t.q. } \pi\overline{\pi} = p \\ & \text{et } \pi \equiv 1 \ (1+i)^3 \ (= -2i(1+i)) \end{cases}$

(ex. Conj de Gauss "last entry", prouvé par Hasse en 1921)

Preuve • cas $p \equiv 3$ (4) exercice : $x \to -x$, $x^3 - x \to -(x^3 - x)$
et -1 non carré dans $\mathbb{Z}/p\mathbb{Z}$ donc. $\#E(\mathbb{F}_p) = \underset{\uparrow}{1} + \underset{\uparrow}{3} + \underset{\uparrow}{\frac{1}{2}(p-3)\times 2}$
$0 \quad x^3 - x = 0 \quad x^3 - x \neq 0$.

Cas $p \equiv 1 \ (4)$ (esquisse) on se ramène à compter les points de la courbe plane $C := \{(u,v),\ u^2 = v^4 + 4\}$.

En effet, le changement de variables $\begin{cases} y = vx \\ 2x = u + v^2 \end{cases}$ montre que pour tout corps k, $2 \in k^\times$ on a $E(k) - \{0, (0;0;1)\} \xrightarrow{\sim} C(k)$. (exercice !)

$\# C(\mathbb{F}_p)$ se calcule par la méthode des sommes de Jacobi et conduit au résultat (cf. Ireland & Rosen ch. 18 §4)

Lemme 2 i) On a $1 - a_p X + p X^2 = \begin{cases} 1 - (-p) X^2 & \text{si } p \equiv 3 \ (4) \\ (1 - \pi X)(1 - \bar{\pi} X) & \text{avec } \pi, \bar{\pi} \text{ comme} \\ & \text{dans le lemme 1} \end{cases}$ si $p \equiv 1 \ (4)$

ii) $L(s,E) = \prod_{\substack{\pi \in \mathbb{Z}[i] \\ \pi \text{ irréd} \equiv 1 \ (1+i)^3}} \frac{1}{1 - N\bar{\pi}^s \pi} = \sum_{\substack{\pi \in \mathbb{Z}[i] \\ \pi \equiv 1 \ (1+i)^3}} \frac{\pi}{(N\pi)^s}$

Preuve : i) c'est le lemme 1 !

ii) c'est conséquence du i) et de la classif. bien connue des irréductibles de $\mathbb{Z}[i]$.

Lemme 3 i) La fonction $\vartheta : \mathbb{R}_{>0} \to \mathbb{C}$, définie par

$$\vartheta(t) = \sum_{\substack{z \in \mathbb{Z}[i] \\ z \equiv 1 \ (1+i)^3}} z\, e^{-\pi t |z|^2}$$

converge abs. $\forall\, t$ et vérifie $\vartheta(t) \sim_{t \to +\infty} e^{-\pi t}$

ii) On a $\pi^{-s} \Gamma(s) L(s,E) = \int_0^\infty \vartheta(t)\, t^s \frac{dt}{t}$ pour $\mathrm{Re}(s) > 3/2$.

Preuve i) exercice

ii) utilisons que pour $z \in \mathbb{C} - \{0\}$, on a pour $\mathrm{Re}(s) > 0$

$$\int_0^\infty e^{-\pi t |z|^2} t^s \frac{dt}{t} = \pi^{-s} |z|^{-2s} \Gamma(s)$$

$u = \pi t |z|^2$ ∎

Lemme 4 (Lemme clé) Soit $\lambda = (1+i)^3$. On a $|\lambda| = 8^{1/2}$ et la fonction $\underline{\vartheta}(t) := \vartheta(t/|\lambda|)$ vérifie

$$\underline{\vartheta}(t) = t^{-2} \underline{\vartheta}(1/t) \quad \forall t \in \mathbb{R}_{>0}$$

Lemme 4 $\Rightarrow$ Thm :

$$\pi^{-s} \Gamma(s) L(s, \xi) = \int_0^\infty \vartheta(t) t^s \frac{dt}{t} = |\lambda|^{-s} \int_0^\infty \underline{\vartheta}(t) t^s \frac{dt}{t}$$

$$= |\lambda|^{-s} \int_1^\infty \left(\underline{\vartheta}(t) t^s + \underbrace{\underline{\vartheta}\left(\tfrac{1}{t}\right) t^{-s}}_{\underline{\vartheta}(t) t^{2-s}} \right) \frac{dt}{t}$$

cette expression converge $\forall s \in \mathbb{C}$. (plus de sing. en 0) : holomorphe,

et $|\lambda|^s \pi^{-s} \Gamma(s) L(s, \xi)$ invariante par $s \to 2-s$ ∎.

Preuve Lemme 4 Soit $t > 0$ réel.

On a $\vartheta(t) = \sum_{z \in \mathbb{Z}[i]} f(z)$ où $f : \mathbb{C} \to \mathbb{C}$ est la f.

$$f(z) = (1+\lambda z) e^{-t\pi |1+\lambda z|^2}.$$

formule de Poisson : $\vartheta(t) = \sum_{z \in \mathbb{Z}[i]} \hat{f}(z)$

où $\hat{f}(w) := \int_{\mathbb{C}} f(z) e^{-2i\pi \mathrm{Re}\, z\bar{w}} \, dw.$

($\mathbb{C} \simeq \mathbb{R}^2$ $\mathrm{Re}\, z\bar{w} \leftrightarrow$ prod. scalaire usuel

$1, i \to (1,0), (0,1)$ $\mathbb{Z}[i]$ autodual.

Exercice $\hat{f}(w) = -\frac{i}{|\lambda|^2 t^2}\frac{w}{\bar{\lambda}} e^{-\pi\frac{|w|^2}{t|\lambda|^2}} e^{2i\pi \mathrm{Re}\,\bar{w}/\lambda}$

Il faut ensuite étudier $\sum_{z\in\mathbb{Z}[i]} \hat{f}(z)$ et reconnaître $\frac{1}{|\lambda|^2 t^2}\vartheta(1/t|\lambda|^2)$

On ne détaille pas tous les calculs, mais disons simplement qu'il est commode d'introduire la fonction

$$\gamma : \mathbb{Z}[i] \longrightarrow \mathbb{C}$$
$$w \longmapsto -\frac{i}{\bar{\lambda}} \sum_{k=0}^{3} i^k e^{\frac{2i\pi}{8}\mathrm{Re}(w i^k \lambda)}$$

on observe alors les faits (faciles!) suivants:

- $\gamma(wi) = i^{-1}\gamma(w) \quad \forall\, w \in \mathbb{Z}[i]$
- $\gamma(w+\lambda z) = \gamma(w) \quad \forall\, w, z \in \mathbb{Z}[i]$
- $\gamma(1) = 1$ (calcul)

Comme le groupe $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ agissant sur $\mathbb{Z}[i]/(1+i)^3$ (anneau à 8 éléments) a 1 seule orbite libre, i.e. celle des inversibles, on en déduit $\gamma(w) = 0$ si $w \equiv 0\ (1+i)$

On réécrit ensuite $\sum_{z\in\mathbb{Z}[i]} \hat{f}(z)$ sous la forme

$$\frac{1}{|\lambda|^2 t^2} \sum_{w \equiv 1\,(\lambda)} \gamma(w)\, w\, e^{-\frac{\pi|w|^2}{t|\lambda|^2}} = \frac{1}{|\lambda|^2 t^2}\vartheta\left(\frac{1}{t|\lambda|^2}\right) \quad \blacksquare$$

V) Module de Tate d'une courbe elliptique

but : "montrer" que si k c.d.m. et E/k c.ell alors $L(s, E)$ est d'origine galoisienne ("à la Artin")

réf : Tate, Silverman

suite E/k c.ell et L/k ext. corps

$\mathbb{P}^2 \supset$ alors $\mathrm{Aut}_k L$ agit sur $\mathbb{P}^2(L)$ en préservant $E(L)$

($\sigma(X:Y:Z) = (\sigma X : \sigma Y : \sigma Z)$: il agit par aut. de groupes

$\forall\, \sigma \in \mathrm{Aut}_k L$: $\sigma O = O$ et $\sigma(P+Q) = \sigma P + \sigma Q$ $\forall P, Q \in E(L)$

Thm on suppose E/k avec k alg clos, $N \geq 1$ entier inversible dans k.

groupe $E(k)[N] = \{ P \in E(k),\ \underbrace{P+P+\cdots+P}_{N \text{ fois}} = O \}$ est $\simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^2$

(cas : $N = 2, 3 \ldots$)

Preuve : cas particulier $k \hookrightarrow \mathbb{C}$.

$k = \mathbb{C}$ théorie de Weierstrass : $E(\mathbb{C})$ est isom à $\mathbb{C}/\Lambda$, où $\Lambda \subset \mathbb{C}$ réseau bien choisi, entraînant groupe analytique / $\mathbb{C}$.

$$\Longrightarrow \quad E(\mathbb{C})[N] \simeq \tfrac{1}{N}\Lambda/\Lambda \simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^2$$

si $k \hookrightarrow \mathbb{C}$, $\circledast$ $E(k)[N] \subset E(\mathbb{C})[N]$ sous-groupe

si $(x:y:1) \in E(\mathbb{C})[N]$ alors $(\sigma(x):\sigma(y):1) \in E(\mathbb{C})[N]$

par la suite $\forall\, \sigma \in \mathrm{Aut}_k \mathbb{C} \Rightarrow \{ \sigma(x),\ \sigma \in \mathrm{Aut}_k \mathbb{C} \}$ fini (idem avec y)

$\Rightarrow x \in \overline{k} = k$, et $y \in k$ aussi.

donc $\circledast$ est une égalité ■ (le cas des corps finis sera aussi utile dans la suite. On peut en fait se ramener aussi au cas $k = \mathbb{C}$ dans ce cas [illegible] la fin du cours)

module de Tate de $E_{/k}$ (k quelconque). $\bar{k} :=$ clôture alg (sép) de

$n \geq 1$, ℓ premier, on regarde

$$0 \to E(\bar{k})[\ell] \longrightarrow E(\bar{k})[\ell^{n+1}] \xrightarrow{\times \ell} E(\bar{k})[\ell^n]$$

thm $\Rightarrow$ $\times \ell$ surjective. On pose $\boxed{T_\ell(E) := \varprojlim_n E(\bar{k})[\ell^n]}$

$T_\ell(E) \simeq \mathbb{Z}_\ell^2$ comme gpe abelien + action $\mathbb{Z}_\ell$-linéaire (sorite) de $\mathrm{Gal}(\bar{k}/k)$

$\rightsquigarrow$ $\boxed{\rho_{E,\ell} : \mathrm{Gal}(\bar{k}/k) \longrightarrow Gl_2(\mathbb{Z}_\ell)}$ (unique conj. près).

C'est une "représentation ℓ-adique", elle connaît beaucoup de choses sur $E_{/k}$, du moins si k de type fini / ss corps premier

Thm' (Hasse) k fini; $\det(X - \rho_{E,\ell}(\varphi)) = X^2 - aX + \#k$ (↓ du thm. Hasse)

$\varphi \in \mathrm{Gal}(\bar{k}/k)$
"Frob." : $x \to x^{\#k}$ (i.e $\det(1 - \rho_{E,\ell}(\varphi)) = \#E(k)$)

Pour finir $k = K$ est un corps de nombres.

Soit P idéal premier (↑ $\mathcal{O}_K$), on choisit $K_P \longrightarrow \overline{K_P}$, puis.

on prolonge arbitrairement $K \longrightarrow K_P \to \overline{K_P}$

en $\bar{K} \longrightarrow \overline{K_P}$. Cela fournit un morphisme

de groupes $\mathrm{Gal}(\overline{K_P}/K_P) \longrightarrow \mathrm{Gal}(\bar{K}/K)$

(changer de choix $\Leftrightarrow$ conjuguer par $\mathrm{Gal}(\bar{K}/K)$)

(exercice)

Thm 2 Soit E/K c. ell, ℓ premier, $\mathfrak{P} \subset \mathcal{O}_K$ idéal premier.

Alors i) $\rho_{E,\ell} \mid \mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}}) \simeq \rho_{E_{K_{\mathfrak{P}}},\ell}$

↑ E vue comme c. ell $/K_{\mathfrak{P}}$

ii) si E est ss forme de Weierstrass avec $a, b \in \mathcal{O}_K$, et si $\mathfrak{P} \nmid 2\ell \,\mathrm{disc}\, E$, alors

$\rho_{E_{K_{\mathfrak{P}}},\ell}$ est triviale sur le sous-groupe d'inertie de $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}})$ (i.e $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_0)$ où K_0 est l'ext. non ram. max. de $K_{\mathfrak{P}}$ dans $\bar{K}_{\mathfrak{P}}$) —

donc se factorise en une rep. de $\mathrm{Gal}(K_0/K_{\mathfrak{P}}) \simeq \mathrm{Gal}(\bar{k}_{\mathfrak{P}}/k_{\mathfrak{P}})$,

et en tant que telle, est isom. à $\rho_{\bar{E},\ell}$,

où $\bar{E} = E \bmod \mathfrak{P}$ (une c. ell $/k_{\mathfrak{P}}$). ∎

Enoncé a rallonge.... il répond au but affiché, d'après Hasse:

si $\mathfrak{P} \nmid 2\ell \,\mathrm{disc}\, E$, $X^2 - a_{\mathfrak{P}} X + N\mathfrak{P}$ est un pol. caractéristique de Frobenius, comme dans le cas d'Artin —

Preuves (esquisses : cf Tate, Silverman)

i) est conséquence immédiate de suite et du premier thm. (dans les cas démontrés) : on a $T_\ell(E) \xrightarrow{\sim} T_\ell(E_{K_{\mathfrak{P}}})$ (l'isom. étant induit par $\bar{K} \to \bar{K}_{\mathfrak{P}}$, et donc commutant à $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}})$).

ii) plus délicat. On se ramène à l'énoncé suivant :

On dira qu'un groupe abélien A est "uniquement N-divisible" si $A \to A$, $x \mapsto Nx$, est bijective.

Prop: (Tate, cf.) Soit F un corps complet pour une val. discrète, $\mathcal{O} \subset F$ l'anneau de val, $k = \mathcal{O}/\mathfrak{m}$ corps residuel, E/F une c. ell. On suppose que E a un modèle de Weierstrass avec $a, b \in \mathcal{O}$ et $2\,\mathrm{disc}\, E \in \mathcal{O}^\times$.

On note $\pi : \mathbb{P}^2(F) = \mathbb{P}^2(\mathcal{O}) \longrightarrow \mathbb{P}^2(k)$ l'application can. de réduction mod $\mathfrak{m}$. Alors

π induit un morphisme de groupes $E(F) = E(\mathcal{O}) \to \bar{E}(k)$, où $\bar{E}$ est la c. ell / k definie par réduction mod $\mathfrak{m}$ de E, et ce morphisme est : i) surjectif

ii) de noyau N-divisible $\forall N \in \mathcal{O}^\times$

Preuve i) Le fait que π induise un morph. de groupes $E(F) = E(\mathcal{O}) \to \bar{E}(k)$ est clair : toute droite de $\mathbb{P}^2_{/F}$ peut être choisie à coeff dans $\mathcal{O}$, l'un d'eux étant dans $\mathcal{O}^\times$.

ii) la surjectivité de π vient du fait que $\bar{E}$ est non singulière + lemme de Hensel (+ F complet !)

iii) plus subtile. On note $E_1 \subset E(\mathcal{O})$ le noyau de π.

$P = (x : y : 3) \in E_1 \Rightarrow$ OPS $y = 1$ puis $P = (x : 1 : 3)$, $x, 3 \in \mathfrak{m}$

on rappelle qu'alors $3 = x^3 + axz^2 + bz^3$

on montre que $E_1 \longrightarrow \mathfrak{m}$, $P \mapsto x$ bijection., et on fait la loi de groupe sur $\mathfrak{m}$

↳ induite par E : loi de groupe formel (cf Tate)

On vérifie notamment que la $\times N$ est de la forme

$$x \longmapsto Nx + f(x)x^2 \quad \text{avec } f(x) \in \mathcal{O}[[x]]$$

mais une telle série formelle est inversible (pour la composition !) si $N \in \mathcal{O}^\times$, cqfd. ∎

Cor ① sous les hypothèses de la prop., pour tout $N \geq 1$ avec $N \in \mathcal{O}^\times$, on a ⁋ : $E(F)[N] \xrightarrow{\sim} \bar{E}(k)[N]$.

preuve : exercice !

Autre Cor : on est maintenant en mesure de prouver le Thm. II.1 dans le cas où $k = \overline{\mathbb{F}_p}$. En effet, soit $N \geq 1$ premier à p, $E/\overline{\mathbb{F}_p}$ une c. ell., $\mathcal{O}_0 := W(\overline{\mathbb{F}_p})$ (vecteurs de Witt), $F_0 = \mathcal{O}_0[\frac{1}{p}]$.

$\mathcal{E} :=$ une courbe ell. arbitraire/F_0 ss forme de Weierstrass à coeff. dans $\mathcal{O}_0$ telle que $\bar{\mathcal{E}} = E$ (évidemment possible).

Soit F/F_0 finie telle que $\mathcal{E}(F)[N] \simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^2$

$\mathcal{E}(\bar{F})[N]$

(existe car $\bar{F}_0$ se plonge dans $\mathbb{C}$!)

$\mathcal{O} =$ anneau de val. de F a pour corps résiduel $\overline{\mathbb{F}_p}$

(F/F_0 totalement ramifiée nécessairement)

Prop (ou Cor ↑) $\Rightarrow$ $\mathcal{E}(F)[N] \xrightarrow{\sim} \bar{\mathcal{E}}(\overline{\mathbb{F}_p})[N]$ ∎

$E(\overline{\mathbb{F}_p})[N]$

si $\left(\mathbb{Z}/N\mathbb{Z}\right)^2$

Cor ② Soit F, $\mathcal{O}$ et E comme dans l'énoncé de la prop.

Soit $N \geq 1$ un entier $\in \mathcal{O}^\times$.

(On suppose F extension finie de $\mathbb{Q}_p$ si on veut)

Soit F^{un}/F une extension ma ramifiée de F

choisie assez grosse de sorte que l'on ait $E(k_{F^{un}})[N] = E(k_F)[N]$ (fini)

Alors
$$\begin{array}{ccc} E(F^{un})[N] & \xrightarrow{\pi}_{\sim} & E(k_F)[N] \\ \downarrow \text{inclusion} & \nearrow \text{un isomorphisme} & \\ E(\bar{F})[N] & & \end{array}$$

preuve π isom $\Rightarrow$ $E(F^{un})[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$

thm 1 $\Rightarrow$ inclusion égalité, cqfd. ∎

Cor: $\rho_{E,\ell}$ non ramifiée si $\ell \in \Theta^\times$, sous les mêmes hyp.

et $\rho_{E,\ell} \mid$ [redacted] $\cdot\, Gal(F^{un\,max}/F) \xrightarrow{\sim} \rho_{\bar{E},\ell}$:

Cela conclut la démonstration du thm 2.