Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Yves Balasko

Travaux de Coates et Wiles sur la conjecture de Birch et Swinnerton-Dyer

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 1 (1976-1977), exp. n° 5, p. 1-12

<http://www.numdam.org/item?id=SDPP_1976-1977__18_1_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 5, 12 p.

8 novembre 1976

TRAVAUX DE COATES ET WILES SUR LA CONJECTURE DE BIRCH ET SWINNERTON-DYER

par Yves BALASKO

1. Introduction.

Soit E une courbe elliptique définie sur un corps de nombre F. Il résulte du théorème de Mordell-Weil que le groupe $E(F)$ des points de E à coordonnées dans F est de type fini ; soit g_F le rang de $E(F)$ modulo torsion. BIRCH et SWINNERTON-DYER ont alors conjoncturé que si la fonction $\zeta(E/F , s)$ est prolongeable analytiquement à tout le plan complexe (ceci est une conjecture différente), alors $\zeta(E/F , s)$ a un zéro en $s = 1$ d'ordre g_F. Le cas $g_F \geqslant 1$ fournit une forme plus faible de la conjecture : $\zeta(E/F , s)$ a un zéro en $s = 1$ si la courbe elliptique E admet un point d'ordre infini.

2. Le théorème de Coates et Wiles.

Soit K un corps quadratique imaginaire de nombre de classe 1. COATES et WILES ont démontré le théorème suivant.

THÉORÈME. - *Soit E une courbe elliptique définie sur $\underline{Q}$ (resp. K) à multiplication complexe par l'anneau des entiers $\mathcal{O}$ de K. Si E admet un point d'ordre infini, alors $\zeta(E/\underline{Q} , s)$ (resp. $\zeta(E/K , s)$) s'annule en $s = 1$.*

Ce résultat s'applique aux courbes $y^2 = 4x^3 - Dx$ qui admettent la multiplication complexe par l'anneau $\underline{Z}[i]$ des entiers de Gauss, courbes qui servirent à BIRCH et SWINNERTON-DYER pour établir leur conjecture.

Notons ψ le caractère de Hecke ou "Grössencharacter" de la courbe elliptique E : c'est un homomorphisme défini sur le groupe I_f des idéaux de K premiers avec le conducteur f de la courbe elliptique E, à valeur dans K.

On note $L(\psi , s)$ la fonction L associée à ψ [6]. DEURING [3] a démontré :

1° Si E est définie sur $\underline{Q}$, alors $\zeta(E/\underline{Q} , s)$ est égal au produit d'un nombre fini de facteurs eulériens et de $L(\psi , s)$, qui est en outre égal à $L(\overline{\psi} , s)$;

2° Si E est définie sur K, alors $\zeta(E/K , s) = L(\psi , s)\, L(\overline{\psi} , s)$.

Par conséquent, pour démontrer la forme faible de la conjecture de Birch et Swinnerton-Dyer, il suffit de démontrer que $L(\overline{\psi} , s)$ s'annule en $s = 1$ si E admet un point d'ordre infini.

3. Notations et définitions.

On choisit un modèle de la courbe elliptique E sous la forme

$$y^2 = 4x^3 - g_2 x - g_3 ,$$

où g_2 et g_3 appartiennent à $\mathcal{O}$, ce qui est possible puisque le nombre de classe de K étant égal à 1, l'invariant j_E est invariant par conjugaison complexe : il est réel ; comme c'est un entier algébrique, c'est donc un entier ; la suite est évidente.

On note L le réseau des périodes de la courbe elliptique E définie sur $\underset{\sim}{C}$, i. e. $E \simeq \underset{\sim}{C}/L$. L'anneau des endomorphismes de E s'identifie à $\mathcal{O} = \{\lambda \in \underset{\sim}{C} \ ; \ \lambda L \subset L\}$, donc L est un $\mathcal{O}$-module de rang 1 sans torsion : comme $\mathcal{O}$ est principal puisque K est de nombre de classe 1, on a donc $L = \mathcal{O}.\Omega$, où $\Omega \in \underset{\sim}{C}$.

On note S l'ensemble formé de 2, 3 et des nombres premiers q tels que E n'a pas bonne réduction en au moins un idéal premier de K au-dessus de q.

Soit p un nombre premier qui se décompose dans K, i. e. $p = \mathfrak{p}.\overline{\mathfrak{p}}$, et qui n'appartient pas à S. On note π le générateur de l'idéal principal $\mathfrak{p}$ tel que la réduction modulo $\mathfrak{p}$ de l'endomorphisme défini par π coïncide avec l'endomorphisme de Frobenius de la courbe elliptique E modulo $\mathfrak{p}$.

Pour tout $n \geqslant 0$, on définit $E_{\pi^{n+1}}$ = noyau de l'endomorphisme π^{n+1} de E ; soit $F_n = K(E_{\pi^{n+1}})$, et soit $G_n = \mathrm{Gal}(F_n/K)$. L'étude de ces corps, ainsi que des questions liées, est facilitée par l'introduction de groupes formels. On sait que le noyau de la réduction modulo $\mathfrak{p}$ de la courbe E définit un groupe formel $\hat{E}$ (voir par exemple [7]) défini sur l'anneau $\mathcal{O}_{\mathfrak{p}}$.

Pour la loi formelle de $\hat{E}$, il est facile de vérifier que $[\pi]t \equiv \pi t$ mod degré 2, et $[\pi]t \equiv t^p \mod p\mathcal{O}_{\mathfrak{p}}$. Il résulte alors de la théorie de Lubin-Tate qu'il existe un groupe formel unique $\mathcal{E}$, isomorphe à $\hat{E}$, tel que l'endomorphisme $[\pi]$ de $\mathcal{E}$ est donné par la formule $[\pi](w) = \pi w + w^p$. Notons $\mathcal{E}_{\pi^{n+1}}$ le noyau de l'endomorphisme $[\pi^{n+1}]$ de $\mathcal{E}$; il est clair que $\Phi_n = K_{\mathfrak{p}}(E_{\pi^{n+1}}) = K_{\mathfrak{p}}(\mathcal{E}_{\pi^{n+1}})$; d'après la théorie de Lubin-Tate, Φ_n est une extension totalement ramifiée de $K_{\mathfrak{p}}$ de degré $p^n (p - 1)$. Un générateur u_n de $\mathcal{E}_{\pi^{n+1}}$ est une uniformisante locale de Φ_n et $N_{\Phi_n/K_{\mathfrak{p}}}(u_n) = \pi$.

Il résulte de tout ceci que F_n est aussi une extension totalement ramifiée de K : on note $\mathfrak{p}_n$ l'unique idéal premier de F_n au-dessus de $\mathfrak{p}$, on a aussi $\Phi_n = (F_n)_{\mathfrak{p}_n}$.

Soit Δ le groupe des racines $(p - 1)$-ièmes de l'unité dans $\mathcal{O}_{\mathfrak{p}}$. On vérifie (c'est facile, mais un peu calculatoire, voir [2], lemme 6) que $[\zeta].w = \zeta w$ pour tout $\zeta \in \Delta$ et $w \in \mathcal{E}$.

Enfin, soit $G_0 = \mathrm{Gal}(F_0/K)$. Soit u_0 un générateur de E_π, soit $\sigma \in G_0$,

alors $u_0^\sigma \in E_\pi$. On pose $u_0^\sigma = \chi(\sigma)\, u_0$: on définit ainsi un homomorphisme χ de G_0 dans Z^x , qui ne dépend pas du choix de u_0 . On dit que χ est le caractère canonique.

Soit A un $\underset{\sim}{Z}_p[G_0]$-module ; on définit, pour tout entier k , le sous-module $A^{(k)}$ comme le sous-ensemble sur lequel G_0 agit comme χ^k : on a la décomposition en somme directe

$$A = \oplus_{k=1}^{p-1} A^{(k)} .$$

On notera que le caractère χ donne aussi l'action de G_0 sur $\mathcal{E}_\pi$ par la formule $u^\sigma = [\chi(\sigma)](u) = \chi(\sigma).(u)$.

4. Fonctions L et unités elliptiques.

Un ingrédient essentiel de la démonstration du théorème de Coates et Wiles est fourni par les unités elliptiques de Gilles Robert. Je rappelle leur définition.

Soit $\mathfrak{L}$ un réseau du plan complexe, on pose

$$\sigma(z\ ,\ \mathfrak{L}) = z \prod_{\omega\in\mathfrak{L},\,\omega\neq 0} \left(1 - \frac{z}{\omega}\right) \exp\left((z/\omega) + \frac{1}{2}\,(z/\omega)^2\right) ,$$

$$\theta(z\ ,\ \mathfrak{L}) = \Delta(\mathfrak{L})\, \exp(-\,6 s_2(\mathfrak{L}) z^2)\, \sigma(z\ ,\ \mathfrak{L})^{12} ,$$

où $\Delta(\mathfrak{L})$ = fonction discriminant de $\mathfrak{L}$,

$$s_2(\mathfrak{L}) = \lim_{s\to 0,\, s>0} \sum_{\omega\in\mathfrak{L},\,\omega\neq 0} \omega^{-2}\, |\omega|^{-2s} .$$

Soit L le réseau de notre courbe elliptique : on a $L = \Omega\mathcal{O}$; soit $\wp(z)$ la fonction de Weierstrass associée à E . Soit $\mathfrak{A}$ un idéal entier de K :

$$\Theta(z\ ,\ \mathfrak{A}) = \frac{\theta(z\ ,\ L)^{N\mathfrak{A}}}{\theta(z\ ,\ \mathfrak{A}^{-1} L)} ,$$

où $N\mathfrak{A}$ = norme absolue de $\mathfrak{A}$, et $\mathfrak{A}^{-1}$ = réseau $\Omega\mathfrak{A}^{-1}$.

On note $\mathfrak{S}$ l'ensemble des triplets $(A\ ,\ \pi\ ,\ J)$ où J est un ensemble fini, $A = \{\mathfrak{A}_j\ ;\ j \in J\}$ et $\pi = \{n_j\ ;\ j \in J\}$, où les $\mathfrak{A}_j$ sont des idéaux entiers de K premiers avec p et les éléments de S , et les n_j des entiers rationnels tels que la relation $\sum_{j\in J} n_j\, (N\mathfrak{A}_j - 1) = 0$ soit vérifiée. On définit pour un tel triplet $(A\ ,\ \pi\ ,\ J)$ la fonction

$$\Theta(z\ ,\ A\ ,\ \pi\ ,\ J) = \prod_{j\in J} \Theta(z\ ,\ \mathfrak{A}_j)^{n_j} .$$

Soit maintenant $\mathfrak{f} = (f)$ un idéal de K . On note $I_\mathfrak{f}$ le groupe des idéaux premiers avec $(\mathfrak{f})$. Soit $R_\mathfrak{f} = \{(\lambda)\ ;\ \lambda \equiv 1 \mod^x \mathfrak{f}\}$ [1]. On définit le corps de classe du rayon modulo $\mathfrak{f}$ comme l'extension $K_\mathfrak{f}$ de K telle que, par la loi de réciprocité d'Artin, on ait l'isomorphisme

$$I_\mathfrak{f}/R_\mathfrak{f} \xrightarrow{\sim} \mathrm{Gal}(K_\mathfrak{f}/K) .$$

([1]) i. e. si $\lambda = \alpha/\beta$, avec α et β dans $\mathcal{O}$ et premiers à $\mathfrak{f}$, alors $\alpha \equiv \beta \mod \mathfrak{f}$.

Notons $\mathfrak{f}_n$ le conducteur de $F_n = K(E_{\pi^{n+1}})$ sur K. Soit $\mathcal{R}_n$ le corps de classe de K du rayon $\mathfrak{f}_n$. Alors ROBERT [4] a montré que si ρ_n est un point de $\mathfrak{f}_n$-division primitif de L, alors $\Theta(\rho_n, A, \pi, J)$ est une unité de $\mathcal{R}_n$, et l'ensemble de ces valeurs forme un sous-groupe C_n du groupe des unités de $\mathcal{R}_n$: c'est le groupe des unités elliptiques de $\mathcal{R}_n$. Il est stable par l'action de $\mathrm{Gal}(\mathcal{R}_n/K)$, et ne dépend pas du choix de ρ_n.

COATES et WILES définissent les unités elliptiques C_n de F_n comme le groupe $N_{\mathcal{R}_n/F_n}(C_n)$. On démontre que chaque élément de C_n est $\equiv 1 \bmod \mathfrak{p}_n$.

Notons U_n les unités de Φ_n qui sont $\equiv 1 \bmod \mathfrak{p}_n$ et U_n' le sous-groupe de U_n des éléments de norme 1 sur $K_\mathfrak{p}$. Soit E_n les unités de F_n qui sont $\equiv 1 \bmod \mathfrak{p}_n$. On a donc $C_n \subset E_n$. Soit $\overline{C}_0$ l'adhérence de C_0 pour la topologie $\mathfrak{p}_0$-adique. On prend la décomposition de $U_0'/\overline{C}_0$ en tant que $\mathbb{Z}_p[G_0]$-module.

On dit que p est un bon nombre premier si :

1° p n'appartient pas à S ;

2° p se décompose dans K (et on note $p = \mathfrak{p}.\overline{\mathfrak{p}}$) ;

3° Φ_0 ne contient pas de racine p-ième de l'unité non triviale (on dit que p n'est pas "anormal").

Avec cette définition, on a le résultat suivant :

THÉORÈME A. - *Soit p un bon nombre premier. Alors pour chaque entier k tel que $1 \leqslant k \leqslant p-1$, on a $\Omega^{-k} L(\overline{\psi}^k, k) \in K$. En outre $\Omega^{-k} L(\overline{\psi}^k, k) \equiv 0 \bmod \mathfrak{p}$ si, et seulement si, $(U_0'/\overline{C}_0)^{(k)} \neq 0$.*

Nous n'allons pas démontrer ce résultat ici. Cependant, on peut expliquer le lien un peu mystérieux entre les unités elliptiques et la fonction L au moyen du prochain lemme.

Introduisons auparavant quelques notations supplémentaires. $\mathfrak{f} = (f)$ dénote le conducteur de E. On pose $\rho = \Omega/f$. Soit E_f le groupe des points de f-division. On montre ([2], lemmes 3 et 4) qu'on a le diagramme

$$\begin{array}{ccccc} & & \mathcal{R}_0 = HF_0 & & \\ & \nearrow & & \nwarrow & \\ H = K(E_f) & & & & F_0 = K(E_\pi) \\ & \nwarrow & & \nearrow & \\ & & K = H \cap F_0 & & \end{array}$$

où $H = K(E_f)$ est en fait le corps de classe de K du rayon modulo $\mathfrak{f}$. Si $\mathfrak{b}$ est un idéal entier de K premier avec $\mathfrak{f}_0$, on note $\sigma_\mathfrak{b}$ le symbole d'Artin de $\mathfrak{b}$ pour l'extension $\mathcal{R}_0/K$. Soit B un ensemble d'idéaux entiers de K premiers à $\mathfrak{f}_0$ et tels que

$$\{\sigma_\mathfrak{b} \; ; \; \mathfrak{b} \in B\} = \mathrm{Gal}(\mathcal{R}_0/F_0) .$$

Soit $\mathfrak{A}$ un idéal entier de K premier avec les éléments de S et p : on défi-

nit

$$\Lambda(z\ ,\ \mathfrak{A}) = \prod_{b\in B} \Theta(z + \psi(b)\ \rho\ ,\ \mathfrak{A})\ .$$

LEMME. - La fonction $\Lambda(z\ ,\ \mathfrak{A})$ est une fonction rationnelle de $\wp(z)$ et $\wp'(z)$ à coefficients dans K . De plus,

$$z\frac{d}{dz}\log \Lambda(z\ ,\ \mathfrak{A}) = \sum_{k=1}^{\infty} c_k(\mathfrak{A})\ z^k$$

vérifie

$$c_k(\mathfrak{A}) = 12(-1)^{k-1}\ \rho^{-k}\ (N\mathfrak{A} - \psi^k(\mathfrak{A}))\ L_f(\bar{\psi}^k\ ,\ k)\ , \qquad k = 1\ ,\ 2\ ,\ \ldots$$

Précisons encore plusieurs faits importants concernant les unités elliptiques.

Soient $G_\infty = \mathrm{Gal}(F_\infty/K) = \mathrm{Gal}(\Phi_\infty/K_\mathfrak{p})$ et $\Gamma = \mathrm{Gal}(F_\infty/F_0) = \mathrm{Gal}(\Phi_\infty/\Phi_0)$. On a $G_\infty = \Gamma \times G_0$, où $G_0 = \mathrm{Gal}(F_0/K) = \mathrm{Gal}(\Phi_0/K_\mathfrak{p})$.

Les groupes U'_n et $\overline{C}_n$ sont alors munis d'une façon naturelle d'une structure de G_∞-module. Soit γ un générateur topologique fixé une fois pour toutes de Γ . COATES et WILES montrent qu'il existe un G_∞-module compact Y_∞ et un isomorphisme de G_∞-modules tel que

$$Y_\infty^{(k)}/(\gamma^{p^n} - 1)Y_\infty^{(k)} \xrightarrow{\sim} (U'_n/\overline{C}_n)^{(k)} \quad \text{pour} \quad k \not\equiv 0 \mod (p-1)\ .$$

Comme Γ est un sous-groupe de G_∞ , on en déduit un isomorphisme de Γ-modules, et on peut considérer les k-composantes pour l'action de G_0 : $(U'_n/\overline{C}_n)^{(k)}$ est isomorphe à $Y_\infty^{(k)}/(\gamma^{p^n} - 1)Y_\infty^{(k)}$. Pour un Γ-module compact, on a $Y_\infty^{(k)} = 0$ si, et seulement si, $Y_\infty^{(k)} = (\gamma - 1)Y_\infty^{(k)}$, alors $(U'_0/\overline{C}_0)^{(k)} \neq 0$ si, et seulement si, $(U'_n/\overline{C}_n)^{(k)} \neq 0$ pour tout entier $n \geqslant 0$.

5. Lois de réciprocité explicites.

Il existe maintenant une démonstration du théorème de Coates et Wiles ne nécessitant pas l'utilisation des lois de réciprocité. Néanmoins, outre leur intérêt propre, il est probable qu'elles seront utiles pour des résultats ultérieurs sur la fonction ζ . On note par $*$ l'addition formelle de $\mathcal{E}$ et par $\sim$ la soustraction formelle. Il est d'abord clair que si $\mathfrak{M}$ est l'idéal maximal de l'anneau des entiers de $K_\mathfrak{p}$, alors $\mathcal{E}(\mathfrak{M})$ est un $\mathcal{O}_\mathfrak{p}$-module divisible.

Soit $n \geqslant 0$ fixé. Le symbole de norme résiduelle généralisé est un couplage

$$(\ ,\ )_n : \ \mathcal{E}(\mathfrak{p}_n) \times \Phi_n \longrightarrow \mathcal{E}_{\pi^{n+1}}\ ,$$

défini comme suit

1° Soit $\beta \in \Phi_n^\times$, soit σ_β l'image de β par l'application $\Phi_n^\times \longrightarrow \mathrm{Gal}(\Phi_{n,ab}/\Phi_n)$ (réciprocité d'Artin) ;

2° Soit $\alpha \in \mathfrak{p}_n$, on lui associe $\gamma \in \mathfrak{M}$ tel que $[\pi^{n+1}](\gamma) = \alpha$.

On pose $(\alpha\ ,\ \beta)_n = \sigma_\beta\ \gamma\ \sim \gamma$.

Il faut vérifier que cette définition est bien à valeur dans $\mathcal{E}_{\pi^{n+1}}$ et ne dépend

pas du choix de γ .

Soit γ' tel que $[\pi^{n+1}]\gamma' = \alpha$. Il existe $\gamma'' \in \mathcal{E}_{\pi^{n+1}}$ tel que $\gamma' = \gamma * \gamma''$, d'où

$$\sigma_\beta(\gamma') \sim \gamma' = \sigma_\beta(\gamma * \gamma'') \sim (\gamma * \gamma'') .$$

Or

$$\sigma_\beta(\gamma * \gamma'') = \sigma_\beta(\gamma) * \gamma''$$

car $\gamma'' \in \Phi_n$ est invariant par σ_β .

Donc, on a $\sigma_\beta(\gamma') \sim \gamma' = \sigma_\beta(\gamma) \sim \gamma$.

Calculons $[\pi^{n+1}](\sigma_\beta(\gamma) \sim \gamma)$: on a

$$[\pi^{n+1}](\sigma_\beta(\gamma) \sim \gamma) = [\pi^{n+1}](\sigma_\beta(\gamma)) \sim [\pi^{n+1}](\gamma)$$

or $[\pi^{n+1}](\gamma) = \alpha \Longrightarrow [\pi^{n+1}](\sigma_\beta(\gamma)) = \sigma_\beta(\alpha) = \alpha$, car $\alpha \in \mathfrak{p}_n$ invariant par σ_β , donc

$$[\pi^{n+1}](\sigma_\beta(\gamma) \sim \gamma) = \alpha \sim \alpha = 0 .$$

Le symbole $(\ , \ )_n$ vérifie les propriétés suivantes :

1° Le symbole $(\ , \ )_n$ est bilinéaire,

2° $(\alpha , \beta)_n = 0 \Longleftrightarrow \beta$ norme de $\Phi_n(\gamma)$ où $[\pi^{n+1}](\gamma) = \alpha$,

3° $(\alpha , \alpha)_n = 0$ pour tout $\alpha \in \mathfrak{p}_n$,

4° $(\ , \ )_n$ définit un couplage non dégénéré

$$\mathcal{E}(\mathfrak{p}_n)/[\pi^{n+1}]\mathcal{E}(\mathfrak{p}_n) \times \Phi_n^\times/\Phi_n^{\times p^{n+1}} \longrightarrow \mathcal{E}_{\pi^{n+1}}$$

si, et seulement si, Φ_0 ne contient aucune racine p-ième de l'unité non triviale.

(a) le symbole est linéaire à gauche : soient γ et γ' tels que

$$[\pi^{n+1}](\gamma) = \alpha \quad \text{et} \quad [\pi^{n+1}](\gamma') = \alpha' .$$

On a $[\pi^{n+1}](\gamma * \gamma') = \alpha * \alpha'$, donc

$$(\alpha * \alpha' , \beta)_n = \sigma_\beta(\gamma * \gamma') \sim (\gamma * \gamma')$$
$$= \sigma_\beta(\gamma) * \sigma_\beta(\gamma') \sim (\gamma * \gamma') = (\alpha , \beta)_n * (\alpha' , \beta)_n .$$

(b) le symbole est linéaire à droite :

$$(\alpha , \beta\beta')_n = \sigma_{\beta\beta'}(\gamma) \sim \gamma = \sigma_\beta[\sigma_{\beta'}(\gamma)] \sim \gamma$$
$$= \sigma_\beta[\sigma_{\beta'}(\gamma)] \sim \sigma_\beta(\gamma) * \sigma_\beta(\gamma) \sim \gamma$$
$$= (\sigma_{\beta'}(\gamma) \sim \gamma) * (\sigma_\beta(\gamma) \sim \gamma)$$

car $\sigma_{\beta'}(\gamma) \sim \gamma \in \nu_{\pi^{n+1}}$ est invariant par σ_β , donc

$$(\alpha , \beta\beta')_n = (\alpha , \beta)_n * (\alpha , \beta')_n .$$

(c) $(\alpha , \beta)_n = 0 \Longleftrightarrow \beta$ norme de $\Phi_n(\gamma)$:

En effet, $(\alpha , \beta)_n = 0 \Longleftrightarrow \sigma_\beta(\gamma) \sim \gamma = 0 \Longleftrightarrow \sigma_\beta(\gamma) = \gamma$, donc γ est invariant par σ_β , donc σ_β laisse invariant $\Phi_n(\gamma)$, donc par la théorie du corps de clas-

se local, β est une norme de $\Phi_n(\gamma)^x$.

(d) $(\alpha , \alpha)_n = 0$ pour tout $\alpha \neq 0$, $\alpha \in \mathfrak{p}_n$:

Soit r le plus grand entier $\leqslant n$ tel que α est divisible par $[\pi^r]$, c'est-à-dire tel qu'il existe $\delta \in \mathfrak{p}_n$, $\delta \neq 0$ tel que $[\pi^r]\delta = \alpha$. Soit $\gamma \in \mathfrak{M}$ tel que $[\pi^{n-r+1}](\gamma) = \delta$; on pose $\rho = [\pi^{n-r}](\gamma)$.

D'abord ρ n'appartient pas à $\mathfrak{p}_n$; sinon, on aurait $[\pi^{r+1}](\rho) = [\pi^{n+1}](\gamma) = \alpha$, d'où une contradiction avec la définition de r .

Considérons maintenant le diagramme

$$\begin{array}{ccc} G(\Phi_n(\gamma)/\Phi_n) & \longrightarrow & \mathcal{E}_{\pi^{n-r+1}} \\ \downarrow & & \downarrow \\ G(\Phi_n(\rho)/\Phi_n) & \xrightarrow{\sim} & \mathcal{E}_{\pi} \end{array}$$

La première flèche verticale est définie par l'opération de restriction, la première flèche horizontale est $\sigma \longmapsto \sigma\gamma \sim \gamma$; la deuxième $\sigma \longmapsto \sigma\rho \sim \rho$. Il est immédiat que $[\pi^{r+1}](\rho) = \alpha$, et que $[\pi](\rho) = [\pi^{n-r+1}](\gamma) = \delta$, i. e. $\pi\rho + \rho^p = \delta$ où $\delta \in \mathfrak{p}_n$. Cette dernière équation étant irréductible, il est immédiat que le groupe de Galois $G(\Phi_n(\rho)/\Phi_n)$ est cyclique d'ordre p , et s'identifie par l'application horizontale à ν_π . En effet, dans le cas contraire, l'application ne serait pas surjective, donc nécessairement on aurait $\sigma\rho \sim \rho = 0$, d'où $\sigma\rho = \rho$, donc $\rho \in \Phi_n$, ce qui est impossible.

On en déduit que la composée $G(\Phi_n(\gamma)/\Phi_n) \longrightarrow \nu_\pi$ est surjective. Montrons que ceci implique que la première flèche horizontale est un isomorphisme. Supposons que la flèche ne soit pas surjective. Comme $\mathcal{E}_{\pi^{n-r+1}}$ est cyclique, l'image de $G(\Phi_n(\gamma)/\Phi_n)$ est un sous-groupe cyclique de $\mathcal{E}_{\pi^{n-r+1}}$, donc son ordre divise nécessairement p^{n-r} , donc il est contenu dans $\mathcal{E}_{\pi^{n-r}}$, et son image, après composition par $[\pi^{n-r}]$: $\mathcal{E}_{\pi^{n-r+1}} \longrightarrow \mathcal{E}_\pi$, est donc nulle. Ceci contredit la surjectivité de la composée des flèches de gauche, et $G(\Phi_n(\gamma)/\Phi_n) \longrightarrow \mathcal{E}_{\pi^{n-r+1}}$ est nécessairement surjective. Comme ces groupes ont le même nombre d'éléments, c'est un isomorphisme.

Il résulte de l'isomorphisme que $[\Phi_n(\gamma):\Phi_n] = p^{n-r+1}$.

Soient $\gamma_1 , \ldots , \gamma_{p^r}$ les éléments de $\mathcal{E}_{\pi^{n+1}}$ tels que $[\pi^{n-r+1}](\gamma_i)$ soient distincts dans $\mathcal{E}_{\pi^r}$. Alors $\gamma - \gamma_i$ vérifie l'équation $[\pi^{n-r+1}](X + \gamma_i) - \delta = 0$, car $[\pi^{n-r+1}](\gamma) = \delta$. C'est une équation de degré p^{n-r+1} à coefficients dans Φ_n : c'est l'équation minimale de $\gamma - \gamma_i$ sur Φ_n . Notons N la norme de $\Phi_n(\gamma)$ sur Φ_n . On déduit de l'équation précédente que $N(\gamma - \gamma_i) = \delta - [\pi^{n-r+1}](\gamma_i)$, donc

$$N\Big(\prod_{i=1}^{p^r} (\gamma - \gamma_i)\Big) = \prod_{u \in \mathcal{E}_\pi} (\delta - u) = [\pi^r](\delta) = \alpha ,$$

ce qui termine la démonstration.

Nous renvoyons au papier de COATES et WILES pour la démonstration du dernier

point qui ne présente pas de difficulté particulière. Le fait que Φ_0 ne doive pas contenir de racine p-ième de l'unité non triviale provient du fait que les groupes $\mathcal{E}(p_n)/[\pi^{n+1}]\mathcal{E}(p_n)$ et $\Phi_n^x/\Phi_n^{x^{p^{n+1}}}$ doivent avoir le même ordre si le couplage est non dégénéré (ce sont des groupes abéliens finis). Or, on montre (lemme 14 de [2]) que l'ordre de $\mathcal{E}(p_n)/[\pi^{n+1}]\mathcal{E}(p_n)$ est $(p^{p^{n+1}})^{(p-1)p^n+1}$.

Un calcul classique montre que l'ordre de $\Phi_n^x/\Phi_n^{x^{p^{n+1}}}$ est $(p^{p^{n+1}})^{(p-1)p^n+1}\, p^{r_n}$, où p^{r_n} est l'ordre du groupe des racines p-ièmes de l'unité dans Φ_n. Il est immédiat que $r_n = 0$ si, et seulement si, $r_0 = 0$.

Notons $\Phi_n' = \{$éléments de Φ_n^x de norme 1 sur $K_p\}$, $\lambda : \mathcal{E} \longrightarrow G_a$ l'application logarithme du groupe formel. Soit $\mathfrak{X}_n = \{\gamma \in \Phi_n ;\ Tr_n(\gamma\lambda(\alpha)) \in \underset{\sim}{Z}_p$, $\forall\ \alpha \in \mathcal{E}(p_n)\}$, où $Tr_n : \Phi_n \longrightarrow K_p$ est la trace.

Soit u_n un générateur de $\mathcal{E}_{\pi^{n+1}}$.

LEMME. - Il existe un homomorphisme

$$\psi_n : \Phi_n' \longrightarrow \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n$$

tel que $(\alpha, \beta)_n = [Tr_n(\lambda(\alpha)\ \psi_n(\beta))](u_n)$, $\forall\ \alpha \in \mathcal{E}(p_n)$ et $\forall\ \beta \in \Phi_n'$. En outre, ψ_n induit un isomorphisme

$$\Phi_n'/\Phi_n'^{p^{n+1}} \xrightarrow{\sim} \mathfrak{X}_n/p^{n+1}\mathfrak{X}_n .$$

Esquissons comment COATES et WILES démontrent le résultat suivant : On suppose, pour cette preuve, que Φ_0 ne contienne pas une racine p-ième non triviale de l'unité, mais l'énoncé est vrai en général.

THEOREME B. - Soit $\alpha \neq 0$, $\alpha \in \mathcal{E}(p)$. Soit α_n tel que $[\pi^{n+1}](\alpha_n) = \alpha$. Alors, pour n assez grand, $\Phi_\infty(\alpha_n)/\Phi_\infty$ est non triviale et ramifiée.

Seul le cas où α_n appartient à Φ_∞ présente quelques difficultés. Comme α_n est de degré au plus p^{n+1} sur Φ_n, on a $\alpha_n \in \Phi_{2n+1}$. Il suffit de démontrer que $\Phi_{2n+1}(\alpha_n)/\Phi_{2n+1}$ est non triviale et ramifiée pour n assez grand. Soit $\beta_n = [\pi^{n+1}(\alpha)]$. Puisque $[\pi^{2n+2}](\alpha_n) = \beta_n$, il suffit de démontrer, d'après la théorie du corps de classe local (SERRE [5], Corps locaux) qu'il existe une unité ε_{2n+1} de Φ_{2n+1}^x qui n'est pas une norme : il suffit que $(\beta_n, \varepsilon_{2n+1})_{2n+1} \neq 0$. En fait, COATES et WILES construisent au moyen des applications ψ_n des éléments ε_n qui vérifient les relations

$$Tr_n(\psi_n(\varepsilon_n)) = \text{Cte} \neq 0 \quad \text{pour tout } n ,$$

avec, en outre,

$$(\beta_n, \varepsilon_{2n+1})_{2n+1} = [\lambda(\alpha)\ Tr_{2n+1}(\psi_{2n+1}(\varepsilon_{2n+1}))](u_n)$$

donc

$$(\beta_n, \varepsilon_{2n+1})_{2n+1} = [\lambda(\alpha)\ Tr_0(\psi_0(\varepsilon_0))](u_n) .$$

Le terme entre crochets est constant, donc, pour n assez grand, π^{n+1} ne le divise pas, donc il ne peut pas tuer (u_n) pour n assez grand. Par conséquent,

$$(\beta_n , \varepsilon_{2n+1})_{2n+1} \neq 0 .$$

6. Démonstration du théorème.

Soit P un point d'ordre infini de $E(K)$. Soit p un bon nombre premier :

1° $p \notin S$;

2° p se décompose dans K ;

3° p n'est pas anormal.

Pour tout $n \geqslant 0$, on choisit $Q_n \in E(\overline{K})$ tel que $\pi^{n+1} Q_n = P$; on note $H_n = F_n(Q_n)$. Un argument basé sur la bonne réduction de E en dehors de S [2] montre que H_n/F_n est non ramifiée en dehors de $\mathfrak{p}_n$.

Notons $E_1(K_\mathfrak{p})$ le noyau de la réduction modulo $\mathfrak{p}$ de $E(K_\mathfrak{p})$. Comme E a bonne réduction modulo ρ , $E_1(K_\mathfrak{p})$ est d'indice fini dans $E(K_\mathfrak{p})$: on peut alors choisir $\beta \in \mathcal{O}$ premier, avec π tel que $E(K_\mathfrak{p}) \subset E_1(K_\mathfrak{p})$. En outre, comme P est d'ordre infini, on a $\beta P \neq 0$ dans $E_1(K_\mathfrak{p})$. Comme $F_n(Q_n) = F_n(\beta Q_n)$, car $(\beta,\pi)=1$, on peut donc supposer que P est un élément non nul de $E_1(K_\mathfrak{p})$. On note δ l'image de P dans $\hat{E}(\mathfrak{p})$, et $\alpha \in \mathcal{E}(\mathfrak{p})$ est l'image de δ par l'isomorphisme entre $\hat{E}$ et $\mathcal{E}$. Soit $\alpha_n \in K_\mathfrak{p}$ tel que $[\pi^{n+1}]\alpha_n = \alpha$. Il est clair que $\Phi_n(\alpha_n) = \Phi_n(Q_n)$ (et aussi $\Phi_\infty(\alpha_n) = \Phi_\infty(Q_n)$).

Il résulte de la section précédente que $\mathrm{Gal}(\Phi_n(\alpha_n)/\Phi_n)$ est isomorphe à $\mathcal{E}_{\pi^{n+1}}$. En particulier H_n/F_n est une p-extension abélienne. En outre, on vérifie que $\mathrm{Gal}(\Phi_n(\alpha_n)/\Phi_n)^{(1)} = \mathrm{Gal}(\Phi_n(\alpha_n)/\Phi_n)$.

Soit N une extension abélienne de F_n galoisienne sur K . $\mathrm{Gal}(F_n/K) = G_n$ opère sur $X = \mathrm{Gal}(N/F_n)$: si $\sigma \in G_n$ et $x \in X$, on définit $x^\sigma = \rho\, x\, \rho^{-1}$, où $\rho \in \mathrm{Gal}(N/K)$ admet σ pour restriction à F_n . Comme $G_0 = \mathrm{Gal}(F_0/K)$ s'identifie à un sous-groupe de G_n , G_0 opère sur X , ce qui permet de prendre la décomposition de X en sous-espaces invariants pour l'action du caractère χ .

Par l'isomorphisme h : $\mathrm{Gal}(\Phi_n(\alpha_n)/\Phi_n) \xrightarrow{\sim} \mathcal{E}_{\pi^{n+1}}$, on a $h(x^\sigma) = \sigma' x \sigma'^{-1} \alpha_n \sim \alpha_n$, où $\sigma' \in \mathrm{Gal}(\Phi(\alpha_n)/\Phi_n)$ tel que σ' correspond à σ ,

$$h(x^\sigma) = \sigma' x \sigma'^{-1}\, \alpha_n \sim \sigma'\, \sigma'^{-1}\, \alpha_n ,$$

$\alpha'_n = \sigma'^{-1}\, \alpha_n$, donc

$$h(x^\sigma) = \sigma' x \alpha'_n \sim \sigma'\, \alpha'_n = \sigma' . (x\alpha'_n \sim \alpha'_n) ,$$

$$h(x^\sigma) = \sigma' . h(x) = \chi(\sigma) . h(x) = h(\chi(\sigma) . x) ,$$

donc $x^\sigma = \chi(\sigma) . x$.

Pour tout $n \geqslant 0$, on note :

M_n : p-extension abélienne maximale de F_n non ramifiée en dehors de $\mathfrak{p}_n$;
L_n : p-entension abélienne non ramifiée maximale de F_n .

On démontre (c'est un autre papier de COATES et WILES [1]) par la théorie du

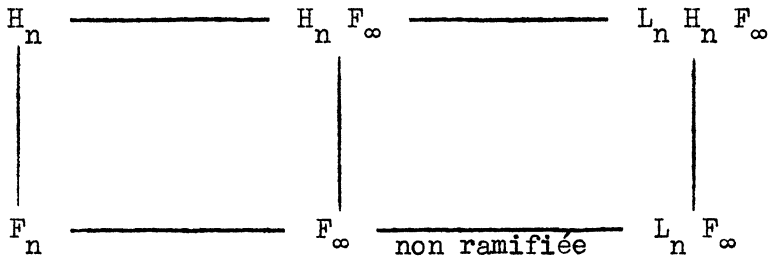
corps de classe global qu'on a un isomorphisme de G_n-module par l'application d'Artin

$$U'_n/\overline{E}_n \xrightarrow{\sim} \mathrm{Gal}(M_n/L_n F_\infty) .$$

Pour montrer que $\Omega^{-1} L(\overline{\psi}, 1) \equiv 0 \mod \mathfrak{p}$, il suffit de montrer que $(U'_0/\overline{C}_0)^{(1)}$ est $\neq 0$, ou encore qu'il existe $n \geqslant 0$ tel que $(U'_n/\overline{C}_n)^{(1)} \neq 0$.

Comme $C_n \subset E_n$, il suffit de trouver n tel que $(U'_n/\overline{E}_n)^{(1)} \neq 0$, donc, vu l'isomorphisme précédent, que $\mathrm{Gal}(M_n/L_n F_\infty)^{(1)} \neq 0$.

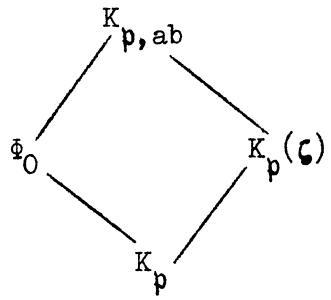
Comme $H_n \subset M_n$, il suffit de trouver n tel que $\mathrm{Gal}(H_n L_n F_\infty/L_n F_\infty)^{(1)} \neq 0$



L'extension $L_n F_\infty/F_\infty$ est non ramifiée car L_n/F_n est non ramifiée, donc $\mathrm{Gal}(L_n H_n F_\infty/L_n F_\infty)^{(1)}$ est non trivial si $H_n F_\infty/F_\infty$ est non triviale et ramifiée, ou encore si $\mathrm{Gal}(H_n/F_n)^{(1)} = \mathrm{Gal}(H_n/F_n) \neq 0$, donc si l'extension H_n/F_n est non triviale et ramifiée, ce qui a lieu pour n assez grand.

Il suffit donc de montrer qu'il existe une infinité de bons nombres premiers pour en déduire que $L(\overline{\psi}, 1) = 0$.

Montrons d'abord que si $p \neq 2$ et si Φ_0 contient une racine p-ième de l'unité non triviale ζ, alors $\pi + \overline{\pi} = 1$. Nécessairement $K_p(\zeta) = \Phi_0$ puisque $[\Phi_0 : K_p] = p - 1$.



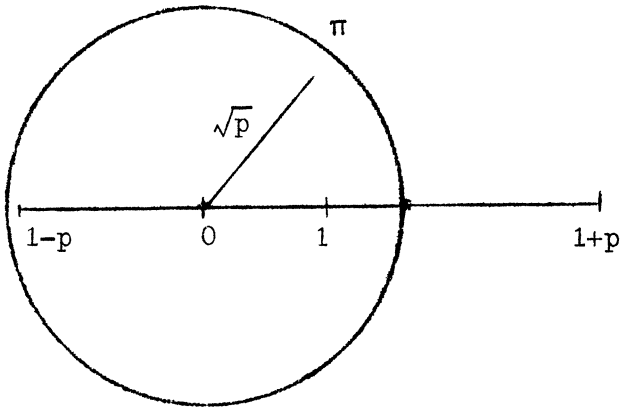
D'après la théorie du corps de classe local, Φ_0 et $K_p(\zeta)$ sont égaux si les groupes de normes de ces deux corps dans $K_p^\times$ sont égaux. Il est facile de voir que

$$N_{\Phi_0/K_p}(\Phi_0^\times) = \{\pi\} \times \{u \ ; \ u \equiv 1 \mod \mathfrak{p}\}$$

$$N_{K_p(\zeta)/K_p}(K_p(\zeta)^\times) = \{p\} \times \{u \ ; \ u \equiv 1 \mod \mathfrak{p}\} ,$$

donc ces groupes sont égaux si $p/\pi \equiv 1 \mod \mathfrak{p}$.

Comme $p = \pi.\overline{\pi}$, on a $\overline{\pi} \equiv 1 \mod \mathfrak{p}$, donc $\pi + \overline{\pi} \equiv 1 \mod \mathfrak{p}$ (puisque $\pi \in \mathfrak{p}$). Comme $\mathfrak{p} \cap \underset{\sim}{Z} = (p)$, on en déduit $\pi + \overline{\pi} \equiv 1 \mod p$.



Cette congruence implique l'égalité $\pi + \overline{\pi} = 1$ si le point $1 - p$ n'est pas dans le cercle de rayon $\sqrt{p}$, donc, dès que $(p - 1 > \sqrt{p}) \Longleftrightarrow (p^2 - 3p + 1 > 0)$, vérifiée pour tout nombre premier impair.

On en déduit que si 2 se ramifie ou se décompose dans K, il n'existe pas de nombre premier anormal.

En effet, dans les deux cas, on vérifie que $\pi + \overline{\pi}$ est pair.

Il n'y a donc pas de nombre premier anormal $\neq 2$ pour les corps K de discriminant -4, -7 et -8. Si K est un des 6 autres corps de nombre de classe 1, on a $\pi = (a + b\sqrt{-D})/2$, donc $p = \pi.\overline{\pi} = (a^2 + Db^2)/4$. Comme $\pi + \overline{\pi} = a = 1$, on en déduit $4p = 1 + Db^2$.

Soit q un nombre premier $\neq 2$ qui ne divise pas D. Il résulte de la relation $4p = 1 + Db^2$ qu'il existe au moins une classe résiduelle $\overline{n}$ modulo q telle que tous les nombres premiers dans cette classe ne sont pas anormaux : en effet, l'application $b \longmapsto 1 + Db^2$ n'est pas surjective, d'où la conclusion. Il existe au moins une classe $\overline{m}$ de $\underset{\sim}{Z}/D\underset{\sim}{Z}$ telle que tous les nombres premiers de cette classe se décomposent dans K. Comme $\underset{\sim}{Z}/qD\underset{\sim}{Z} = \underset{\sim}{Z}/D\underset{\sim}{Z} \times \underset{\sim}{Z}/q\underset{\sim}{Z}$, on regarde la classe $(\overline{m}, \overline{n})$ de $\underset{\sim}{Z}/qD\underset{\sim}{Z}$: elle contient une infinité de nombres premiers d'après le théorème de Dirichlet sur les progressions arithmétiques. Les nombres premiers de $(\overline{m}, \overline{n})$ n'appartenant pas à S, sont des bons nombres premiers.

BIBLIOGRAPHIE

[1] COATES (J.) and WILES (A.). - Hurwitz numbers and Iwasawa modules, "Proceedings of the International conference in algebraic number theory [1976. Kyoto]" (to appear).

[2] COATES (J.) and WILES (A.). - On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. (to appear).

[3] DEURING (M.). - Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, I-IV, Nachr. Akad. Wiss. Göttingen, Math.-Phys. KP., 1953, p. 85-94 ; 1955, p. 13-42 ; 1956, p. 89-101 ; 1957, p. 55-80.

[4] ROBERT (G.). - Unités elliptiques, Bull. Soc. math. France, Mémoire 36, 1973, 77 p.

[5] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[6] SHIMURA (G.). - Introduction to the arithmetic theory of automorphic functions. - Princeton, Princeton University Press, 1971 (Publications of the Mathematical Society of Japan, 11).

[7] TATE (J.). - The arithmetic of elliptic curves, Invent. Math., t. 23, 1974, p. 179-206.

(Texte reçu le 21 mars 1977)

Yves BALASKO
UER Sc. économiques
Université Paris-XII
58 avenue Didier
94210 LA VARENNE SAINT HILAIRE