MÉMOIRES DE LA S. M. F.

JEAN-PIERRE SERRE

Annexe : deux lettres de Serre

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 95-102
<http://www.numdam.org/item?id=MSMF_1980_2_2__95_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 95-102

ANNEXE

DEUX LETTRES DE SERRE

Comme l'indique K. Ribet, le théorème 1.1. de son article généralise des résultats de J.-P. Serre. Ceux-ci répondaient à des questions rencontrées par D. Masser dans ses travaux sur l'indépendance linéaire de périodes et de pseudo-périodes de fonctions elliptiques (voir le chapitre 6 de "Transcendence Theory : Advances and Applications", A. Baker and D. Masser eds., Academic Press 1977). On trouvera ci-dessous l'essentiel de deux lettres de Serre à Masser sur ces questions.

La première lettre (Novembre 75) concerne le problème suivant. On désigne par $E^1,\ldots,E^n$ des courbes elliptiques définies sur un corps de nombres $K \subset \bar{Q}$, admettant des multiplications complexes par des corps quadratiques imaginaires $F^1,\ldots,F^n \subset \bar{Q}$. On suppose que les corps F^i sont deux à deux distincts, de sorte que les courbes elliptiques E^i sont deux à deux non isogènes sur $\bar{Q}$. Soit K^{cycl} l'extension de K engendrée par toutes les racines de l'unité de $\bar{Q}$. Pour $i = 1,\ldots,n$, on note E^i_∞ le groupe des points de torsion de $E^i(\bar{Q})$ et $K(E^i_\infty)$ l'extension de K engendrée par les coordonnées des points de E^i_∞ ; les corps $K(E^i_\infty)$ contiennent K^{cycl}. D'après un résultat connu (cf. e.g. Serre, Invent. Math. 15, 259-331, Théorème 7) les extensions $K(E^i_\infty)/K^{cycl}$ sont presque disjointes deux à deux : pour tout couple (i,j) d'indices distincts, $K(E^i_\infty) \cap K(E^j_\infty)$ est une extension finie de K^{cycl}. Dans quelle mesure est-il encore vrai que les $K(E^i_\infty)/K^{cycl}$ sont presque disjointes "dans leur ensemble", i.e. que $K(E^i_\infty)$ est presque disjointe sur K^{cycl} du composé des $K(E^j_\infty)$, pour $j \neq i$?

[...] Distinguons deux cas :

a) Cas "agréable" . Les F^i sont non seulement distincts, mais même linéairement disjoints (i.e. aucun d'eux n'est contenu dans le composé des autres - cela exclut, par exemple, le cas de courbes elliptiques à mult. complexe par $Q(\sqrt{-a})$, $Q(\sqrt{-b})$, $Q(\sqrt{-c})$ et $Q(\sqrt{-abc})$.

Alors les extensions $K(E^i_\infty)/K^{cycl}$ $(i = 1,\dots,n)$ sont presque disjointes.

b) Cas général . On ne fait aucune hypothèse sur les F^i. La situation est un peu moins bonne. Pour la préciser, supposons K assez grand pour contenir les F^i (de sorte qu'on a des extensions abéliennes) ; posons $G^i_N = \mathrm{Gal}(K^{cycl}(E^i_N)/K^{cycl})$, où E^i_N est le groupe des points de division par N dans E^i, et soit G_N le groupe de Galois sur K^{cycl} de l'extension composée des $K^{cycl}(E^i_N)$ pour $i = 1,\dots,N$, de sorte que G_N s'identifie à un sous-groupe du produit $G^1_N \times\dots\times G^n_N = H_N$. La presque disjonction équivaudrait à l'affirmation que l'indice de G_N dans H_N est borné ; en fait, ce n'est pas exact, on peut simplement affirmer ceci : il existe des constantes A et B telles que $(H_N:G_N)$ soit un diviseur de $A.B^{r(N)}$, où $r(N)$ est le nombre de facteurs premiers (distincts) de N; de plus, on peut prendre pour B une puissance de 2 (i.e. il y a presque disjonction, à des 2-groupes près).

Notez que $r(N) = 1$ si $N = \ell^m$, ℓ premier, $m \geq 1$ arbitraire : l'indice de G_{ℓ^m} dans H_{ℓ^m} est donc borné par une constante indépendante de ℓ et de m ; n'est-ce pas suffisant pour les applications ? Cela me parait très probable.

Esquisse de la démonstration

Quitte à agrandir K, on peut supposer qu'il contient les F^i et que les E^i ont bonne réduction. Si ℓ est un nombre premier, je note $U_\ell(K)$ le produit des groupes des unités $U(K_v)$, pour $v|\ell$, où K_v est le complété de K en v (c'est le sous-groupe compact maximal du groupe des éléments inversibles de l'algèbre $Q_\ell \otimes K = K_\ell$); j'écris U_ℓ si $K = Q$.

Toutes les extensions considérées sont abéliennes ; on peut donc considérer que ce sont les groupes d'idèles des corps considérés qui opèrent. En particulier, si $u \in U_\ell(K)$, on sait que l'action de u sur E^i_∞ est triviale sur les ℓ'-composantes de E^i_∞ pour $\ell' \neq \ell$, et qu'elle est donnée par la multiplication par $N_i(u^{-1})$ sur la ℓ-composante, où N_i est la norme de K à F^i (on a $N_i(u^{-1}) \in U_\ell(F^i)$); ce résultat est classique (voir par exemple mon article à Inventiones, fin du § 4).

Il résulte de ceci que le groupe $G^i = \varprojlim G^i_N$ s'identifie à un sous-groupe d'indice fini du groupe $U'(F^i) = \prod_\ell U'_\ell(F^i)$, où je note $U'_\ell(F^i)$ le sous-groupe de

$U_\ell(F^i)$ formé des éléments dont la norme dans U_ℓ est égale à 1.

On est donc ramené à considérer le problème suivant :

Soit ℓ un nombre premier. Notons $U'_\ell(F)$ le sous-groupe de $U_\ell(K)$ formé des éléments de norme 1 dans U_ℓ. Considérons l'application

$$f_\ell : U'_\ell(K) \to U'_\ell(F^1) \times \ldots \times U'_\ell(F^n)$$

donnée par $u \mapsto (N_1(u), \ldots, N_n(u))$.
Est-il vrai que $\mathrm{Im}(f_\ell)$ est <u>ouverte</u> pour tout ℓ, et que, pour presque tout ℓ, l'indice de $\mathrm{Im}(f_\ell)$ est <u>borné</u> par une constante B que l'on peut prendre égale à 1 dans le cas a) ?

C'est là un problème de nature élémentaire, mais un peu ennuyeux à traiter en détail en dehors des cas $n = 1,2$ qui sont faciles. Si l'on veut se fatiguer le moins possible, on peut utiliser un peu de géométrie algébrique, de la manière suivante :

Soit T un tore sur Q, de groupe des caractères X; j'entends par là un Q-groupe algébrique, qui est $\bar{Q}$-isomorphe à un produit de groupes multiplicatifs G_m ; on a $X = \mathrm{Hom}_{\bar{Q}}(T, G_m)$, c'est un Z-module libre sur lequel agit $\mathrm{Gal}(\bar{Q}/Q)$, et sa connaissance équivaut à celle de T. Si ℓ est un nombre premier, je note $T(Q_\ell)$ le groupe des Q_ℓ-points de T, et $T^c(Q_\ell)$ le sous-groupe compact maximal de $T(Q_\ell)$.
(Exemple : si K est un corps de nombres comme ci-dessus, et si je prends pour X le groupe libre de base l'ensemble des plongements de K dans $\bar{Q}$, je trouve pour T un tore T_K qui a la vertu que $T_K(Q_\ell) = (K \otimes Q_\ell)^*$, et $T_K^c(Q_\ell) = U_\ell(K)$.)

Soit maintenant $f : T_1 \to T_2$ un homomorphisme de tores, correspondant à un homomorphisme $\hat{f} : X_2 \to X_1$ des groupes de caractères correspondants. On suppose f surjectif (au sens géom.alg.), i.e. $\hat{f}$ injectif ; on identifie ainsi X_2 à un sous-groupe de X_1. Notons N le noyau de f, N^o la composante neutre de N, et B l'ordre du groupe fini N/N^o; l'entier B a une interprétation simple en termes de X_1 et X_2 :

si l'on désigne par $\tilde{X}_2$ le sous-groupe de X_1 formé des éléments $x \in X_1$ tels qu'il existe $m \geq 1$ avec $mx \in X_2$, B n'est autre que l'ordre de $\tilde{X}_2/X_2$, i.e. l'ordre du sous-groupe de torsion de X_1/X_2.

Ceci étant, si ℓ est premier, f définit un homomorphisme

$$f_\ell : T_1^c(Q_\ell) \to T_2^c(Q_\ell) ,$$

et l'on a :

<u>Lemme</u>- i) <u>Pour tout ℓ, l'homomorphisme f_ℓ est ouvert</u>. <u>En particulier, son image est d'indice fini.</u>

ii) <u>Pour presque tout ℓ, l'indice de $\mathrm{Im}(f_\ell)$ est un diviseur de l'entier B défini plus haut.</u>

L'assertion i) est immédiate : l'application tangente à f à l'élement neutre est en effet surjective, et l'on applique la théorie des groupes de Lie - ou tout autre argument ! L'assertion ii) n'est guère plus difficile ; pour presque tout ℓ, on a bonne réduction et $T^c(Q_\ell)$ peut s'interpréter comme $T(Z_\ell)$, groupe des points entiers en ℓ. L'application f_ℓ est surjective pour les points congrus à 1 mod. ℓ (argument de Lie, de nouveau) ; le conoyau se voit sur la réduction mod. ℓ et l'on est ramené à un énoncé sur les corps finis, qui est facile. (On peut sûrement trouver les détails de ceci dans les articles d'Ono aux Annals en 1961, 63,65.) Un cas typique, qui fait bien comprendre ce qui se passe, est celui de l'isogénie $f : x \mapsto x^2$ entre G_m et G_m : l'indice $(U_\ell : U_\ell^2)$ est égal à 2 (c'est-à-dire à l'ordre du noyau de f) pour tout $\ell \neq 2$.

Vous voyez comment ce lemme s'applique ici : on prend pour T_1 le tore T'_K noyau de l'homomorphisme "norme" $T_K \to T_Q = G_m$, où T_K est le tore défini plus haut "groupe multiplicatif de K" ; on prend pour T_2 le produit des tores à une dimension T'_{F^i} ; on prend pour

$$f : T'_K \to \prod_{i=1}^{n} T'_{F^i}$$

l'application définie par les normes N_i.

La surjectivité de f est facile; d'où l'existence de B. Il faut un peu plus travailler pour prouver que B est une puissance de 2, et que B est même égal à 1 dans le cas "agréable" du début; cela se fait de la façon la plus commode en explicitant les groupes de caractères X_1 et X_2. [...]

[J'aurais sans doute dû dire pourquoi j'ai le droit de me borner à regarder l'action de $\prod_\ell U_\ell(K)$ sur les E^i_∞ : c'est que l'image de ce groupe dans $\mathrm{Gal}(K^{ab}/K)$ est un sous-groupe d'indice fini h (nombre de classes), et que toute la question est "à un groupe fini près".]

La deuxième lettre (Juin 76) concerne le corps $\mathcal{K}_\ell$ engendré par les coordonnées des points d'ordre ℓ premier d'un produit de courbes elliptiques à multiplications complexes. On suppose que les hypothèses du "cas agréable" de la première lettre sont vérifiées. D'après le résultat de cette lettre, le degré de $\mathcal{K}_\ell$ sur K est "aussi grand que possible" pour presque tous les nombres premiers ℓ . On trouvera ci-dessous une démonstration plus explicite de cette assertion. Les corps quadratiques F^i sont maintenant notés k_i .

[...] I start with quadratic imaginary fields $k_1,\dots,k_n$ contained in a number field K. I put $D = |\mathrm{disc}(K)|$. I assume the k_i's are independent, i.e. that they generate a field k whose degree is 2^n.

Take $\ell \nmid D$, so that ℓ is unramified in K and the k_i's. Denote by $k_i(\ell)$ the quotient of the ring of integers of k_i by the ideal generated by ℓ . We have :

$$k_i(\ell) = \begin{cases} F_\ell \times F_\ell & \text{if } \ell \text{ splits in } k_i \\ F_{\ell^2} & \text{if } \ell \text{ is inert in } k_i. \end{cases}$$

Define similarly $k(\ell)$ and $K(\ell)$; these are finite rings, products of fields corresponding to the prime ideals above ℓ. We have norm homomorphisms

$$N_{K/k_i} : K(\ell)^* \to k_i(\ell)^* \text{ and } \quad N_{k_i/Q} : k_i(\ell)^* \to F_\ell^* .$$

Putting together the N_{K/k_i} $(i = 1,\ldots,n)$, we get a homomorphism

$$N_K : K(\ell)^* \to k_1(\ell)^* \times \ldots \times k_n(\ell)^* .$$

<u>Lemma</u> : <u>The image of</u> N_K <u>is the set of</u> $(x_1,\ldots,x_n)$, $x_i \in k_i(\ell)^*$, <u>such that</u> $N_{k_1/Q}(x_1) = \ldots = N_{k_n/Q}(x_n)$ <u>in</u> F_ℓ .

Call V the set of (x_i) with the property $N_{k_1/Q}(x_1) = \ldots = N_{k_n/Q}(x_n)$. It is clear that $\mathrm{Im}(N_K) \subset V$. To prove the converse, we may assume that K is equal to $k = k_1\ldots k_n$; indeed it is well known that $N_{K/k} : K(\ell)^* \to k(\ell)^*$ is surjective. Use now induction on n, starting with n = 0, which is trivial.

If $(x_i) \in V$, induction shows that there is $y \in k(\ell)^*$ with $N_{k_2/Q}(y) = x_2$, $\ldots, N_{k_n/Q}(y) = x_n$. This allows us to reduce the problem to the case where $x_2 = \ldots = x_n = 1$, in which case we have $N_{k_1/Q}(x_1) = 1$. But, if we call $s_1,\ldots, s_n$ the obvious generators of $\mathrm{Gal}(k/Q)$ (so that s_i is trivial on k_j if and only if $j \neq i$), it is elementary that $N_{k_1/Q}(x_1) = 1$ implies the existence of $z_1 \in k_1(\ell)^*$ with $z_1^{1-s_1} = x_1$. Now, use the surjectivity of the norm map $N_{k/k_1} : k(\ell)^* \to k_1(\ell)^*$, and get $t \in k(\ell)^*$ with $N_{k/k_1}(t) = z_1$. Put $y = t^{1-s_1}$. I claim that y does the trick. Indeed :

$$N_{k/k_1}(y) = N_{k/k_1}(t)^{1-s_1} = z_1^{1-s_1} = x_1$$

$$N_{k/k_i}(y) = y^{(1+s_1)(1+s_2)\ldots(1+s_{i-1})(1+s_{i+1})\ldots(1+s_n)} = 1 \qquad (i \geqslant 2).$$

This proves the lemma.

(We could replace Q by any number field, and the k_i by any Galois extensions of that field -provided those extensions were linearly disjoint. But the above statement will be enough.)

Now I come to elliptic curves E_i $(1 \leq i \leq n)$, with complex multiplications by some orders O_i of k_i, and defined over the number field K. I will say that ℓ is large if :

a) $\ell \nmid D$ (as above),

b) ℓ does not divide any of the conductors of the orders O_i,

c) each E_i has good reduction at all the primes of K dividing ℓ. (Thus, we exclude a finite constructible set of bad primes ℓ.)

Call $E_i(\ell)$ the group of ℓ-division points of E_i ; by b), we have an action of $k_i(\ell)$ on $E_i(\ell)$, which makes it a free $k_i(\ell)$-module of rank 1. Hence the action of $Gal(\bar{K}/K)$ on $E_i(\ell)$ factors through a homomorphism

$$\rho_i : Gal(\bar{K}/K) \to k_i(\ell)^* .$$

The collection (ρ_i) defines a homomorphism :

$$\rho : Gal(\bar{K}/K) \to k_1(\ell)^* \times \ldots \times k_n(\ell)^* .$$

<u>Main Lemma</u> : <u>If</u> ℓ <u>is large</u>, <u>the image of</u> ρ <u>is equal to the set</u> V <u>of</u> (x_i) <u>with</u> $N_{k_1/\mathbb{Q}}(x_1) = \ldots = N_{k_n/\mathbb{Q}}(x_n)$, <u>as in the previous lemma</u>.

First, it is well known that $N_{k_i/\mathbb{Q}} \circ \rho_i : Gal(\bar{K}/K) \to \mathbb{F}_\ell^*$ gives the action of that Galois group on the ℓ-th roots of unity. Hence it is independent of the choice of i, and we have $Im(\rho) \subset V$. To prove the converse, one looks at the action of the <u>inertia group</u> at ℓ on the $E_i(\ell)$'s. More precisely, since the action is abelian, by class field theory we may interpret each ρ_i (and hence ρ) as a homomorphism from the idèle group of K ; inside this group, we have $K_\ell^* = \prod_{\underline{p}|\ell} K_{\underline{p}}^*$, and its unit group $U_\ell = \prod_{\underline{p}|\ell} U_{\underline{p}}$. We have a natural homomorphism $U_\ell \to K(\ell)^*$, given by reduction mod. ℓ . Now the theory of elliptic curves with complex multiplications tells us that, if $u \in U_\ell$, and if $\bar{u}$ is its image in $K(\ell)$, we have

$$\rho_i(u^{-1}) = N_{K/k_i}(\bar{u}) \quad \text{in } k_i(\ell)^* \text{ for all } i .$$

Hence, the main lemma follows from the elementary lemma above. [...]

[Two more remarks :

1 - One can prove that condition b) above is implied by conditions a) and c).

2 - If one does not assume that the fields k_i are independent, but merely that they are pairwise distinct, one can easily prove the following result (which is probably strong enough for applications to transcendency problems) : there exists constants A,B (depending only on the number n of elliptic curves), such that, for every ℓ large enough (depending on n and the curves), the order of the Galois group $\mathrm{Im}(\rho)$ is such that :

$$A\,\ell^{n+1} < |\mathrm{Im}(\rho)| < B\,\ell^{n+1} .$$

Moreover, A, B and "large enough" are effectively computable.]

J.-P. Serre
Collège de France
11, place Marcelin Berthelot
75005 Paris