Séminaire Dubreil.
Algèbre et théorie
des nombres

Georges Poitou

Points rationnels sur les courbes

Séminaire Dubreil. Algèbre et théorie des nombres, tome 14, nº 2 (1960-1961), exp. nº 21, p. 1-12

<http://www.numdam.org/item?id=SD_1960-1961__14_2_A4_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1960-1961, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
14e année, 1960/61, n° 21

24 avril 1961

POINTS RATIONNELS SUR LES COURBES

par Georges POITOU

L'étude des points rationnels sur un corps k d'une variété abélienne A définie sur k met en évidence le groupe de Châtelet $H^1(k, A)$, dont les éléments s'interprètent comme les classes d'espaces homogènes principaux pour A, définis sur k, l'élément 0 du groupe correspondant aux espaces qui ont un point rationnel sur k.

Supposons que k soit un corps de nombres algébriques, et considérons le sous-groupe H de $H^1(k, A)$ formé des classes d'espaces qui ont un point rationnel sur chaque complété de k. Un point essentiel est la non-trivialité de H ; l'exemple d'un espace de classe non nulle dans H est fourni par la courbe $3x^3 + 4y^3 + 5z^3 = 0$ d'après SELMER.

Le problème abordé, mais non résolu ici, est de calculer le groupe A_k/mA_k, où A_k est le groupe des points de A rationnels sur k, et m un entier. Ce groupe se plonge dans le groupe $S = H^1(k, A_m)$, et même dans le sous-groupe $M^{(1)}$ de S, formé des éléments qui se projettent dans H par la projection naturelle de S dans $H^1(k, A)$. Ce groupe $M^{(1)}$ est fini, et peut être calculé. Si l'on désigne par $M^{(r)}$ la partie de S qui se projette dans $m^{r-1} H$, on définit une suite décroissante de groupes finis contenant A_k/mA_k, et l'on peut espérer calculer ces groupes au moyen de certaines formes bilinéaires antisymétriques.

Ces groupes coïncident à partir d'un certain rang avec leur intersection, dont on pourrait affirmer l'égalité avec A_k/mA_k si l'on savait, par exemple, que les ordres des éléments de H sont bornés, a fortiori si H est un groupe fini comme le bruit en court.

Ce texte suit de près les idées de CASSELS ([1], [2]) en empruntant quelques notions et des résultats fondamentaux à TATE et à LANG ([6], [7]).

1. Suite exacte fondamentale.

Soient k un corps de caractéristique 0, $\bar{k}$ sa clôture algébrique. Soient A une variété abélienne définie sur k, A_k le groupe des points de A rationnels sur k, m un entier au moins égal à 2, A_m le noyau de la multiplication par m sur A.

Le groupe de Châtelet $H^1(k , A)$ est le premier groupe de cohomologie, pour le complexe des cochaînes de type fini du groupe de Galois de $\overline{k}/k$ opérant sur A. En notant encore avec l'indice m le noyau de la multiplication par m dans ce groupe, on a d'après [6], p. 665, la suite exacte

$$(1) \qquad 0 \to A_k/mA_k \xrightarrow{h} H^1(k , A_m) \xrightarrow{g} H^1(k , A)_m \longrightarrow 0 \qquad .$$

Comparons la multiplication par m, par n, et par nm. La suite exacte

$$0 \to A_m \to A_{nm} \xrightarrow{m} A_n \to 0$$

implique d'après [6], proposition 3, p. 664, une suite exacte de cohomologie, qui est compatible avec (1) en ce sens que le diagramme suivant a ses lignes et ses colonnes exactes, et est commutatif, comme on le vérifie sans peine :

$$(2) \qquad \begin{tikzcd}
 & A_k/mA_k \arrow[r] \arrow[d] & A_k/nmA_k \arrow[r] \arrow[d] & A_k/nA_k \arrow[d] & \\
 {} \arrow[r] & H^1(k , A_m) \arrow[r, "\varkappa"] \arrow[d] & H^1(k , A_{nm}) \arrow[r, "m"] \arrow[d] & H^1(k , A_n) \arrow[r] \arrow[d] & {} \\
 & H^1(k , A)_m \arrow[r] & H^1(k , A)_{nm} \arrow[r, "m"] & H^1(k , A)_n &
\end{tikzcd}$$

Une conséquence des propriétés de ce diagramme sera utilisée plus loin : Soit β un élément de $H^1(k , A_{nm})$ tel que $m\beta$ appartienne à l'image de A_k/nA_k ; l'image $g\beta$ de β dans $H^1(k , A)_{nm}$ donne 0 dans $H^1(k , A)_n$, donc définit un élément bien déterminé de $H^1(k , A)_m$ qui sera noté $\Sigma^m \beta$. On vérifie aussitôt :

PROPOSITION 1. - Σ^m est un homomorphisme dans $H^1(k , A)_m$ de la partie de $H^1(k , A_{nm})$ dont l'image par m est contenue dans $h(A_k/nA_k)$; Σ^m est nul sur $h(A_k/nmA_k)$.

2. Accouplements.

Soit B la variété duale de A, et $[b , a] = e_m(a , b)$ la forme bilinéaire de Weil sur $B_m \times A_m$, à valeurs dans les racines de l'unité (donc dans $\overline{k}$). D'après LANG [5], p. 173, on a

$$[b\ ,\ a] = {}^tD(m\mathfrak{b}\ ,\ \mathfrak{a})\ D(m\mathfrak{a}\ ,\ \mathfrak{b})^{-1} \tag{3}$$

avec les notations suivantes : D est un diviseur de Poincaré convenable sur $A \times B$; $\mathfrak{a}$, $\mathfrak{b}$ sont des 0-cycles de degré 0 sur A , B respectivement, tels que $S(\mathfrak{a}) = a$, $S(\mathfrak{b}) = b$, S désignant la somme (dans le groupe de la variété) des points du cycle ; $D(\ ,\ )$ est le symbole défini par LANG [5], p. 169.

Soit alors $\alpha \in H^1(k\ ,\ A_m)$, $\beta \in H^1(k\ ,\ B_m)$; représentons-les par des cocycles (a_σ) , (b_σ) provenant d'une extension galoisienne finie K/k contenant les racines de l'unité d'ordre m ; on sait ([4]) que $c_{\sigma,\tau} = [b_\sigma\ ,\ a_\tau^\sigma]$ définit un 2-cocycle $(c_{\sigma,\tau})$ du groupe de Galois G de K/k opérant sur K^* , dont la classe dans $H^2(G\ ,\ K^*)$ est indépendante des représentants choisis pour α et β ; cette classe induit dans le groupe de Brauer $Br(k)$ un élément qui sera désigné par $\beta \cup \alpha$.

Introduisons des cycles $\mathfrak{a}_\sigma$, $\mathfrak{b}_\sigma$ tels que $S(\mathfrak{a}_\sigma) = a_\sigma$, $S(\mathfrak{b}_\sigma) = b_\sigma$, et portons dans (3) ; les cocyles définis par $D(m\mathfrak{a}_\tau^\sigma\ ,\ \mathfrak{b}_\sigma)^{-1}$ et $D(m\mathfrak{a}_\sigma\ ,\ \mathfrak{b}_\tau^\sigma)$ sont cohomologues d'après l'anticommutativité du cup-produit ; considérons que l'accouplement de Lang $D(\mathfrak{y}\ ,\ \mathfrak{z})$ entre 0-cycles de degré 0 tels que $S(\mathfrak{y}) = 0$ implique aussi pour les classes de cohomologie galoisienne un cup-produit qui sera noté $\mathfrak{D}(\ ,\ )$; alors on a

$$\beta \cup \alpha = \mathfrak{D}(m\mathfrak{a}\ ,\ \mathfrak{b})\ {}^t\mathfrak{D}(m\mathfrak{b}\ ,\ \mathfrak{a}) \tag{4}$$

$\mathfrak{a}$ et $\mathfrak{b}$ étant des cochaînes représentant α et β au moyen de la somme S dans les 0-cycles de degré 0 sur A et B respectivement.

Comparons avec l'accouplement de Tate [7]. Soit v un point de $B_k = H^0(k\ ,\ B)$, représenté par le cycle $\mathfrak{v}$; δ désignant le cobord, la forme de Tate peut être définie par

$$T(\alpha\ ,\ v) = \mathfrak{D}(\delta\mathfrak{a}\ ,\ \mathfrak{v}) \tag{5}$$

D'après (1), hv peut être représenté par le cocycle (b_σ) avec $b_\sigma = w^\sigma - w$, et $mw = v$; si l'on représente le point w par le cycle $\mathfrak{w}$, on peut considérer que hv est représenté par $\delta\mathfrak{w}$ de sorte que l'on a

$$hv \cup \alpha = \mathfrak{D}(m\mathfrak{a}\ ,\ \delta\mathfrak{w})\ {}^t\mathfrak{D}(m\delta\mathfrak{w}\ ,\ \mathfrak{a}) \quad .$$

En modifiant ceci du cobord de $\mathfrak{Q}(m\alpha , \mathfrak{m})$ puis du cobord de ${}^t\mathfrak{Q}((m\mathfrak{m} - \mathfrak{v}) , \alpha)$ on égale $hv \cup \alpha$ à

$$\mathfrak{Q}(m\delta\alpha , \mathfrak{m})\ {}^t\mathfrak{Q}(m\delta\mathfrak{m} , \alpha)$$

puis à

$$\mathfrak{Q}(m\delta\alpha , \mathfrak{m})\ {}^t\mathfrak{Q}((\mathfrak{v} - m\mathfrak{m}) , \delta\alpha)$$

et, en remarquant que

$$\mathfrak{Q}(m\delta\alpha , \mathfrak{m}) = \mathfrak{Q}(\delta\alpha , \mathfrak{m})^m = \mathfrak{Q}(\delta\alpha , m\mathfrak{m})$$

et d'après la réciprocité de LANG [5], théorème 9, p. 169, il vient

$$hv \cup \alpha = \mathfrak{Q}(\delta\alpha , \mathfrak{v} - m\mathfrak{m})\ \mathfrak{Q}(\delta\alpha , m\mathfrak{m}) = \mathfrak{Q}(\delta\alpha , \mathfrak{v}) = T(g\alpha , v)$$

puisque le cocycle qui représente α représente aussi $g\alpha$.

PROPOSITION 2. - L'accouplement (4) est compatible avec celui de Tate, en ce sens que $hv \cup \alpha = T(g\alpha , v)$.

Examinons les relations avec le tableau (2). Donnons des éléments $\alpha \in H^1(k , A_m)$ et $\beta \in H^1(k , B_{mn})$; représentons β par le cocycle (b_σ) , donc $n\beta$ par le cocycle (nb_σ) , et α ainsi que $\varkappa\alpha$ par le cocycle (a_σ) . Les cup-produits $n\beta \cup \alpha$ et $\beta \cup \varkappa\alpha$ sont représentés par les cocycles de valeurs respectives

$$e_m(a_\tau^\sigma , nb_\sigma) , \quad e_{mn}(a_\tau^\sigma , b_\sigma)$$

mais ces deux expressions sont égales d'après LANG [5], proposition 5, p. 190 ; d'où la règle

$$n\beta \cup \alpha = \beta \cup \varkappa\alpha \qquad . \tag{6}$$

3. Dualité locale.

Soit k un corps p-adique. Son groupe de Brauer s'identifie au groupe des rationnels modulo 1 par une application canonique $i : Br(k) \longrightarrow Q/Z$; ceci permet de déduire des accouplements précédents des propriétés de dualité au sens de PONTRJAGIN. En effet, TATE [7] a établi que la forme T met en dualité les groupes A_k/mA_k et $H^1(k , A)_m$. Désignons par M l'image de A_k/mA_k dans $H^1(k , A_m) = S$, $\hat{M}$ et $\hat{S}$ étant relatifs à la variété duale. La proposition 2 implique alors :

PROPOSITION 3. - La forme (4) sur $\hat{S} \times S$ est nulle sur $\hat{M} \times M$; si $\alpha \in S$ et $\beta \cup \alpha = 0$ pour tout $\beta \in \hat{M}$, alors $\alpha \in M$.

Avertissement. - Soit désormais k un corps de nombres algébriques, et k_p son complété pour la valeur absolue relative à l'idéal premier (ordinaire ou à l'infini) p ; on notera j_p l'injection de k dans k_p, ainsi que les applications canoniques qui s'en déduisent.

4. Divisibilité locale et globale.

Faisons l'hypothèse $B_m \subset B_k$.

Soit γ un élément d'ordre n de B_m. Soit α un élément de $H^1(k , A)$, représenté par un cocycle (a_σ). S'il existe β dans $H^1(k , A)$ tel que $m\beta = \alpha$, il existe un cocycle (b_σ) tel que $mb_\sigma = a_\sigma$, et inversement. On dit alors que α est divisible par m sur k. Supposons qu'il en soit ainsi localement, c'est-à-dire que, pour tout p, $j_p(\alpha)$ soit divisible par m sur k_p.

Fixons dans A des b'_σ tels que $mb'_\sigma = a_\sigma$; $[\gamma , b'_{\sigma\tau} - b'_\sigma - b'^{\sigma}_\tau]$ définit un 2- cocycle à valeur dans le groupe E_n des racines n-ièmes de l'unité dans $\overline{k}$, donc aussi un élément de $Br(k)$ qui ne dépend que de γ et que nous noterons $b(\gamma)$.

LEMME. - Pour que α soit divisible par m sur k, il faut et il suffit que $b(\gamma) = 0$ pour tout $\gamma \in B_m$.

PREUVE. - D'après le théorème 90 de Hilbert, $H^2(E_n) \longrightarrow H^2(\overline{k})$ est une injection, donc $b(\gamma) = 0$ entraîne $[\gamma , b'_{\sigma\tau} - b'_\sigma - b'^{\sigma}_\tau] = d_{\sigma\tau}/d_\sigma d^\sigma_\tau$ avec des $d_\sigma \in E_n$. Soit V une base du groupe abélien fini B_m. Comme la forme de Weil est non-dégénérée, il existe un $c_\sigma \in A_m$ tel que $d_\sigma = [\gamma , c_\sigma]$ pour $\gamma \in V$, donc pour tout $\gamma \in B_m$. Posons $b_\sigma = b'_\sigma - c_\sigma$. L'hypothèse $\gamma \in B_k$ entraîne

$$[\gamma , b_{\sigma\tau} - b_\sigma - b^\sigma_\tau] = 0$$

pour tout $\gamma \in B_m$, donc (b_σ) est un cocycle et α est divisible par m sur k.

Ce lemme étant établi, remarquons que la nullité d'un élément de $Br(k)$ résulte de sa nullité locale, d'après un théorème de HASSE ([3], p. 72) ; donc :

PROPOSITION 4. - Sous l'hypothèse que les points de B_m sont rationnels sur k, la divisibilité par m d'un élément α de $H^1(k, A)$ dans ce groupe équivaut à la divisibilité par m, pour chaque p, de $j_p(\alpha)$ dans $H^1(k_p, A)$.

COROLLAIRE. - Si H est le sous-groupe de $H^1(k, A)$ formé des α tels que $j_p(\alpha) = 0$ pour tout p, H est contenu dans $mH^1(k, A)$ (sous l'hypothèse $B_m \subset B_k$).

5. Finitude.

PROPOSITION 5. - Si $\alpha \in H^1(k, A)_m$, on a $j_p(\alpha) = 0$ si p vérifie les conditions suivantes, qui ne comportent qu'un nombre fini d'exceptions.

1° p ne divise pas m.

2° La réduction de A modulo p est non-dégénérée.

3° K étant une extension finie de k où α se décompose, p n'est pas ramifié dans K.

PREUVE. - Théorème 1, corollaire 1, de [6], p. 676.

COROLLAIRE 1. - Si $\beta \in H^1(k, A_m)$, $j_p(\beta) \in h(A_{k_p}/mA_{k_p})$ avec un nombre fini d'exceptions.

COROLLAIRE 2. - Si $\beta \in H^1(k, A_{nm})$ et $mg(\beta) \in H$, de sorte que $\Sigma_p^m(\beta)$ est défini (au sens de la proposition 1, en remplaçant k par k_p), on a $\Sigma_p^m(\beta) = 0$ avec un nombre fini d'exceptions.

6. Dualité globale.

Donnons quelques définitions et notations relatives à la variété A ; les notions correspondantes relatives à la variété duale $B = \hat{A}$ seront affectées du signe $\hat{}$.

$S = H^1(k, A_m)$, $M = h(A_k/mA_k)$

$S_p = H^1(k_p, A_m)$, $M_p = h(A_{k_p}/mA_{k_p})$

J_S = produit direct restreint des groupes S_p relativement aux sous-groupes M_p, c'est-à-dire groupe des "vecteurs" (s_p) dont la p composante appartient à S_p, et presque toujours (c'est-à-dire avec un nombre fini d'exceptions) à M_p.

P_S = image naturelle de S dans J_S (cf. cor. 1 de la proposition 5)

E = ensemble fini convenable de diviseurs premiers

$J_S^E = \prod_{p\in E} S \times \prod_{p\notin E} M_p$, $P_S^E = P_S \cap J_S^E$.

Adoptons aussi les notations suivantes [3] :

U_p = groupe des unités p-adiques

P_k = image naturelle de k dans J_k

$P_k^E = P_k \cap J_k^E$

J_k = groupe des idèles de k

$J_k^E = \prod_{p\in E} k_p^* \times \prod_{p\notin E} U_p$

$J_k^{E,n} = \prod_{p\in E} k_p^{*n} \times \prod_{p\notin E} U_p$.

<u>Définition d'un accouplement global</u>. - Soit $s = (s_p)$ un vecteur de J_S, $\hat{s} = (\hat{s}_p)$ un vecteur de $J_{\hat{S}}$. Posons

$$C_0(\hat{s}, s) = \sum_p i_p(\hat{s}_p \cup s_p) \tag{7}$$

où $i_p : Br(k_p) \to Q/Z$ est l'application canonique notée ρ_p dans [3], p. 99.

Pour cette forme bilinéaire sur $J_{\hat{S}} \times J_S$, il y a orthogonalité entre $P_{\hat{S}}$ et P_S, puisque la somme des invariants d'un cocycle global est nulle ([3], p. 100).

Pour montrer que $P_{\hat{S}}$ est exactement l'orthogonal de P_S, suivons CASSELS [2], proposition 20.

LEMME (a). - Sous l'hypothèse $A_m \subset A_k$, S s'identifie au groupe des 2-classes de cohomologie symétriques du groupe $\hat{A}_m$ opérant trivialement sur k^*, par la correspondance suivante : $\alpha \in S$ est représenté par le cocycle (a_σ) : pour tout $x \in \hat{A}_m$, $[x, a_\sigma]$ est de la forme $\theta(x)^{\sigma-1}$ avec $\theta(x) \in \overline{k}^*$, et $\theta(x+y)/\theta(x)\,\theta(y)$ donne le 2-cocycle symétrique.

LEMME (b). - Pour presque tout p, si $\alpha \in S$, pour que $\alpha \in M_p$, il faut et il suffit que α soit associé à un 2-cocycle de la forme précédente, avec $v_p[\theta(x)^n] = 0$.

PREUVE de (a). - $[x, a_\sigma]$ définit d'après $A_m \subset A_k$ un cocycle à valeurs dans k^*, qui est un cobord d'après le théorème 90, etc. Pour tout groupe H, où $\hat{A}_m$ opère trivialement, notons $W(H) = H^2_{sym}(\hat{A}_m, H)$; on a donc $S = W(k^*)$, $S_p = W(k_p^*)$.

PREUVE de (b).

1° Si $\alpha \in M_p$ est représenté par (a_σ) avec $a_\sigma = b^\sigma - b$, $mb \in A_{k_p}$, l'extension $k_p(b)/k_p$ est non ramifiée d'après [6], proposition 9, p. 673, sous les conditions 1° et 2° de la proposition 5. Comme $\theta(x)^m \in k$ et $\theta(x) \in k_p(b)$ (car $\theta(x)^{\sigma-1} = 1$ chaque fois que $a_\sigma = 0$, c'est-à-dire $b^\sigma = b$), $v_p[\theta(x)^{m^p}]$ est un multiple de m qu'on peut annuler par un autre choix de $\theta(x)$.

2° Inversement, soit K le corps obtenu en adjoignant à k tous les $\theta(x)$; la condition $v_p[\theta(x)^m] = 0$ implique que p est non-ramifié dans K/k ; mais α est décomposé par K, donc $g\alpha$ aussi et d'après [6], corollaire 1 du théorème 1, p. 676, $g\alpha$ est d'ordre 1 sur k_p, donc $\alpha \in M_p$.

COROLLAIRE du lemme. - Si E contient les p qui divisent m et qui dégénèrent la réduction de A, $J_S^E = W(J_k^E)$ et $P_S^E = W(P_k^E)$, puisque $M_p = W(U_p)$ si $p \notin E$.

LEMME de CHEVALLEY ([3], p. 411). - Il existe un ensemble fini E' de diviseurs premiers, tel que, si $E \supset E'$, $J_k^{E,n} \cap P_k^E = (P_k^E)^n$.

COROLLAIRE. - La restriction de J_S^E au produit $\prod_E S_p$ est biunivoque sur P_S^E ; car si $j_p(s) \in M_p$ pour $p \notin E$ et $j_p(s) = 0$ pour $p \in E$, alors $\theta(x)^m \in U_p$ pour $p \notin E$ et $\theta(x)^m \in k^{*m}$ pour $p \in E$, donc $\theta(x)^m \in J_k^{E,m} \cap P_k^E$ donc $\theta(x)^m \in (P_k^E)^m$, ce qui entraîne $s = 0$ si les racines m-ièmes de l'unité sont dans k, ce qui est une conséquence des hypothèses $A_m \subset A_k$, $\hat{A}_m \subset \hat{A}_k$ que nous assumons désormais.

<u>Fin de la démonstration</u>. - Soit $s = (s_p)$ un élément de $J_{\hat{S}}$ orthogonal à P_S ; choisissons un ensemble fini E qui contienne les diviseurs à l'infini, les diviseurs de m, les diviseurs qui dégénèrent la réduction de A, les diviseurs de l'ensemble E' du lemme de Chevalley, et les p tels que $s_p \notin \hat{M}_p$.

C_0 induit une forme bilinéaire sur le produit de $\prod_E \hat{S}_p$ par $\prod_E S_p$; P_S^E se plonge dans le dual de $\prod_E \hat{S}_p$, tout en annulant $P_{\hat{S}}^E$; pour prouver que c'en est exactement l'annulateur, il suffit de compter, et de montrer que

$$(8) \qquad \mathrm{Card}(P_{\hat{S}}^E)\ \mathrm{Card}(P_S^E) = \mathrm{Card} \prod_E \hat{S}_p$$

c'est-à-dire

$$[\mathrm{Card}\ W(P_k^E)]^2 = \prod_E \mathrm{Card}\ W(k_p^*)$$

ou encore

$$[P_k^E : (P_k^E)^n]^2 = \prod_E [k_p : k_p^{*n}] \quad \text{pour} \quad n \not\equiv 0 \bmod p \qquad ;$$

ce qui résulte des calculs de Chevalley (loco citato).

PROPOSITION 6. - Par la forme C_0 sur $J_{\hat{S}} \times J_S$, $P_{\hat{S}}$ est l'orthogonal de P_S . Autrement dit, J_S/P_S s'identifie au dual de $\hat{S}$.

Ceci est obtenu sous les hypothèses $A_m \subset A_k$, $\hat{A}_m \subset \hat{A}_k$; pour s'en libérer, il suffirait de le faire pour l'égalité (8).

7. Groupes intermédiaires.

Définissons $M^{(r)} = S \cap g^{-1}(m^{r-1} H)$. Ces groupes de S décroissent à partir de $M^{(1)}$ qui est fini ([6], p. 681-2), et contiennent tous $M = A_k/mA_k$.

On peut définir sur $\hat{M}^{(r)} \times M^{(r)}$ une forme bilinéaire C_r de la façon suivante :

Si $\alpha \in M^{(r)}$, d'après le corollaire de la proposition 4, $\alpha = m^r \lambda$ avec $\lambda \in H^1(k , A_{m^{r+1}})$, et $mg\lambda \in H$, donc $\Sigma_p^m(\lambda)$ est défini et égal à $g(\mu_p)$ pour un certain $\mu_p \in H^1(k_p , A_m)$; d'autre part, si $\hat{\alpha} \in \hat{M}^{(1)}$, $j_p(\alpha) = h\hat{a}_p$ avec $\hat{a}_p \in A_{k_p}$. D'après la proposition 2, on a

$$(9) \qquad \sum_p i_p\, T(\hat{a}_p , \Sigma_p^m \lambda) = \sum_p i_p(j_p \hat{\alpha} \cup \mu_p)$$

ces sommes étant finies d'après le corollaire 2 de la proposition 5 et la proposition 3. On peut noter l'expression (9) : $F(\hat{\alpha} , \lambda)$.

Je dis que, si $\hat{\alpha} \in \hat{M}^{(r)}$, $F(\hat{\alpha}, \lambda)$ ne dépend pas vraiment de λ , mais seulement de $m^r \lambda = \alpha$. Il suffit de prouver que $F(\hat{\alpha}, \lambda) = 0$ si $m^r \lambda = 0$. Dans ce cas λ provient (au sens du tableau (2)) d'un élément θ de $H^1(k, A_m^r)$, de telle sorte que $g\theta = g\lambda$. De plus, $\hat{\alpha} \in M^{(r)}$ implique $\hat{\alpha} = m^{r-1} \hat{\theta}$ avec $g\hat{\theta} \in H$; pour tout p , il existe $\hat{a}_p$ tel que $j_p(\hat{\theta}) = h(\hat{a}_p)$, donc aussi $j_p(\hat{\alpha}) = h(\hat{a}_p)$; si l'on choisit cet $\hat{a}_p$ pour écrire (9), on trouve

$$F(\hat{\alpha}, \lambda) = \sum_p i_p T(\hat{a}_p, j_p g\theta) = \sum_p i_p(j_p \hat{\theta} \cup j_p \theta) = \sum_p i_p j_p(\hat{\theta} \cup \theta)$$

ce qui est nul comme somme des invariants d'un cocycle global.

Ainsi (9) définit une forme bilinéaire $C_r(\hat{\alpha}, \alpha)$ sur $\hat{M}^{(r)} \times M^{(r)}$.

Supposons maintenant $\alpha \in M^{(r+1)}$; alors $\alpha = m^r \lambda$, avec $g\lambda \in H$, donc $j_p g\lambda = 0$, $\Sigma_p^m \lambda = 0$, donc $C_r(\hat{\alpha}, \alpha) = 0$.

Réciproquement, supposons que $\alpha \in M^{(r)}$ et que $C_r(\hat{\alpha}, \alpha) = 0$ pour tout $\hat{\alpha} \in \hat{M}^{(r)}$. Utilisons la règle (6) avec $n = m^{r-1}$. On trouve, avec les notations précédentes

$$C_r(\hat{\alpha}, \alpha) = \sum_p i_p(j_p \hat{\theta} \cup K\mu_p)$$

donc l'hypothèse et la proposition 6 entraînent l'existence de $\mu \in H^1(k, A_{m^r})$ tel que $g(\varkappa\mu_p) = j_p g(\mu)$; mais alors, quitte à remplacer λ par $\lambda - \mu$, on trouve $j_p g\lambda = 0$, donc $g\lambda \in H$ et $\alpha \in \hat{M}^{r+1}$.

PROPOSITION 7. - Sous l'hypothèse $A_{m^r} \subset A_k$, $\hat{A}_{m^r} \subset A_k$, la forme bilinéaire C_r étant définie par (9) sur $\hat{M}^{(r)} \times M^{(r)}$, le sous-groupe des $\alpha \in M^{(r)}$ tels que $C_r(\hat{\alpha}, \alpha) = 0$ pour tout $\hat{\alpha} \in \hat{M}^{(r)}$ coïncide avec $M^{(r+1)}$.

Pour se libérer des hypothèses de rationalité, il suffirait de le faire pour la proposition 6.

8. Cas des jacobiennes.

Si A est une jacobienne, elle s'identifie à $\hat{A}$ ([5], th. 3, p. 156) de sorte que si $\bar{a}$ est le point de $\hat{A}$ associé à un point a de A , on a l'identité

(10) $$[\bar{a}, a] = 1$$

d'après [5], proposition 7, p. 191. Il en résulte le lemme suivant :

LEMME. - Si α et β appartiennent à $H^1(k , A)$, $\overline{\alpha} \cup \beta = \overline{\beta} \cup \alpha$.

En effet, représentons α et β par des cocycles (a_σ) , (b_σ) ; le terme de gauche est représenté par $[\overline{a}_\sigma , b_\tau^\sigma]$, cohomologue à $[\overline{a}_\tau^\sigma , b_\sigma]^{-1}$ d'après l'antisymétrie du cup-produit ; mais ceci, d'après (10), égale $[\overline{b}_\sigma , a_\tau^\sigma]$ qui représente le terme de droite.

En utilisant la règle (6) avec $n = m^r$, on trouve

$$C_r(\hat{\alpha} , \alpha) = \sum_p i_p(j_p \hat{\lambda} \cup \varkappa\mu_p)$$

avec des notations du paragraphe 7 et $m^r \hat{\lambda} = \hat{\alpha}$. Comme $g(\varkappa\mu_p) = g(j_p \lambda)$, on a

$$\varkappa\mu_p = j_p \lambda - \lambda_p \quad \text{avec} \quad g(\lambda_p) = 0$$

de sorte que

$$C_r(\hat{\alpha} , \alpha) = \sum_p i_p[j_p \hat{\lambda} \cup (j_p \lambda - \lambda_p)] \quad .$$

Dans le cas où A est une jacobienne, calculons $C_r(\overline{\alpha} , \alpha)$ en remarquant que $\hat{\lambda}_p \cup \lambda = 0$ d'après la proposition 3 et que $(j_p \hat{\lambda} - \hat{\lambda}_p) \cup (j_p \lambda - \lambda_p) = 0$ d'après la règle (6) appliquée au multiplicateur m . Il en résulte que $2C_r(\hat{\alpha} , \alpha)$ est la somme des invariants du cocycle global $\overline{\lambda} \cup \lambda$, donc est nul ; par suite, les formes C_r sont antisymétriques, au moins si m est impair.

BIBLIOGRAPHIE

[1] CASSELS (J.W.S.). - Arithmetic on curves of genus 1, I : On a conjecture of Selmer, J. für reine und angew. Math., t. 202, 1959, p. 52-99.

[2] CASSELS (J.W.S.). - Arithmetic on curves of genus 1, II : A general result, J. für reine und angew. Math., t. 203, 1960, p. 174-208.

[3] CHEVALLEY (Claude). - La théorie du corps de classes, Annals of Math., séries 2, t. 41, 1940, p. 394-418 ; Class field theory. - Nagoya, Nagoya University, 1953/54, 104 p.

[4] EILENBERG (S.) and MACLANE (S.). - Cohomology theory in abstract groups, I., Annals of Math., t. 48, 1947, p. 51-78.

[5] LANG (Serge). - Abelian varieties. - New-York, Interscience Publishers, 1959. (Interscience Tracts in pure and appl. Mathematics, 7).

[6] LANG (S.) and TATE (J.). - Principal homogeneous spaces over abelian varieties, Amer. J. of Math., t. 80, 1958, p. 659-684.

[7] TATE (J.). - WC-groups over p-adic fields, Séminaire Bourbaki, t. 10, 1957/58, exposé 156, 13 p.