Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a été consacré à la cohomologie galoisienne des extensions transcendantes pures. Il a comporté deux parties.

I. COHOMOLOGIE DE $k(T)$

Il s'agit de résultats essentiellement connus, dus à Faddeev, Scharlau, Arason, Elman,... On peut les résumer comme suit :

§1. Une suite exacte

Soient G un groupe profini, N un sous-groupe distingué fermé de G, Γ le quotient G/N, et C un G-module discret sur lequel N opère trivialement (i.e. un Γ-module). Faisons l'hypothèse :

(1.1) $H^i(N,C) = 0$ *pour tout* $i > 1$.

La suite spectrale $H^\cdot(\Gamma, H^\cdot(N,C)) \Rightarrow H^\cdot(G,C)$ dégénère alors en une suite exacte :

(1.2) $\ldots \to H^i(\Gamma,C) \to H^i(G,C) \xrightarrow{r} H^{i-1}(\Gamma,\mathrm{Hom}(N,C)) \to H^{i+1}(\Gamma,C) \to \ldots$

L'homomorphisme $r : H^i(G,C) \to H^{i-1}(\Gamma,\mathrm{Hom}(N,C))$ figurant dans (1.2) est défini de la manière suivante :

Si α est un élement de $H^i(G,C)$, on peut représenter α par un cocycle $a(g_1,\ldots,g_i)$ qui est normalisé (i.e. égal à 0 lorsqu'un des g_j est égal à 1), et qui ne dépend que de g_1 et des images $\gamma_2,\ldots,\gamma_i$ de $g_2,\ldots,g_i$ dans Γ. Pour $\gamma_2,\ldots,\gamma_i$ fixés, l'application de N dans C définie par

$n \mapsto a(n,g_2,\ldots,g_i) \qquad (n \in N),$

est un élément $b(\gamma_2,\ldots,\gamma_i)$ de Hom(N,C) et la $(i-1)$-cochaîne ainsi définie sur Γ est un $(i-1)$-cocycle à valeurs dans Hom(N,C) ; sa classe de cohomologie est $r(\alpha)$.

Faisons l'hypothèse supplémentaire :

(1.3) *L'extension* $1 \to \mathrm{N} \to \mathrm{G} \to \Gamma \to 1$ *est scindée.*

L'homomorphisme $\mathrm{H}^i(\Gamma,\mathrm{C}) \to \mathrm{H}^i(\mathrm{G},\mathrm{C})$ est alors injectif, et (1.2) se réduit à la suite exacte :

(1.4) $0 \to \mathrm{H}^i(\Gamma,\mathrm{C}) \to \mathrm{H}^i(\mathrm{G},\mathrm{C}) \xrightarrow{r} \mathrm{H}^{i-1}(\Gamma,\mathrm{Hom}(\mathrm{N},\mathrm{C})) \to 0.$

§2. Le cas local

Si K est un corps, on note K_s une clôture séparable de K, et l'on pose $\mathrm{G}_\mathrm{K} = \mathrm{Gal}(\mathrm{K}_s/\mathrm{K})$. Si C est un G_K-module (discret), on écrit $\mathrm{H}^i(\mathrm{K},\mathrm{C})$ à la place de $\mathrm{H}^i(\mathrm{G}_\mathrm{K},\mathrm{C})$.

Supposons que K soit muni d'une *valuation discrète* v, de corps résiduel $k(v)$; notons K_v le complété de K pour v. Choisissons un prolongement de v à K_s ; soient D et I les groupes de décomposition et d'inertie correspondants ; on a $\mathrm{D} \simeq \mathrm{G}_{\mathrm{K}_v}$ et $\mathrm{D}/\mathrm{I} \simeq \mathrm{G}_{k(v)}$.

Soit n un entier > 0, premier à la caractéristique de $k(v)$, et soit C un G_K-module tel que $n\mathrm{C} = 0$. Faisons l'hypothèse suivante :

(2.1) C *est non ramifié en* v (i.e. I opère trivialement sur C).

On peut alors appliquer à la suite exacte $1 \to \mathrm{I} \to \mathrm{D} \to \mathrm{G}_{k(v)} \to 1$ les résultats du §1 (les hypothèses (1.1) et (1.3) se vérifient sans difficulté). Le $\mathrm{G}_{k(v)}$-module Hom(I,C) s'identifie à $\mathrm{C}(-1) = \mathrm{Hom}(\mu_n,\mathrm{C})$, où μ_n désigne le groupe des racines n-èmes de l'unité (dans $k(v)_s$ ou dans K_s, cela revient au même). Vu (1.4), cela donne la suite exacte :

(2.2) $0 \to \mathrm{H}^i(k(v),\mathrm{C}) \to \mathrm{H}^i(\mathrm{K}_v,\mathrm{C}) \xrightarrow{r} \mathrm{H}^{i-1}(k(v),\mathrm{C}(-1)) \to 0.$

Soit $\alpha \in \mathrm{H}^i(\mathrm{K},\mathrm{C})$ et soit α_v son image (par restriction) dans $\mathrm{H}^i(\mathrm{K}_v,\mathrm{C})$. L'élément $r(\alpha_v)$ de $\mathrm{H}^{i-1}(k(v),\mathrm{C}(-1))$ est appelé le *résidu de* α *en* v, et noté $r_v(\alpha)$. S'il est non nul, on dit que α *a un pôle en* v. S'il est nul, on dit que α est *régulier* (ou « holomorphe ») *en* v ; dans ce cas, α_v s'identifie à un élément de $\mathrm{H}^i(k(v),\mathrm{C})$, qui est appelé la *valeur de* α *en* v, et noté $\alpha(v)$.

§3. Courbes algébriques et corps de fonctions d'une variable

Soit X une courbe projective lisse connexe sur un corps k, et soit $\mathrm{K} = k(\mathrm{X})$ le corps de fonctions correspondant. Soit $\underline{\mathrm{X}}$ l'ensemble des points fermés du schéma X. Un élément x de $\underline{X}$ peut être identifié à une *valuation discrète* de K, triviale sur k ; on note $k(x)$ le corps résiduel correspondant ; c'est une extension finie de k.

Comme ci-dessus, soit n un entier > 0, premier à la caractéristique de k, et soit C un G_k-module tel que $nC = 0$. Le choix d'un plongement de k_s dans K_s définit un homomorphisme $G_K \to G_k$, ce qui permet de considérer C comme un G_K-module. Pour tout $x \in \underline{X}$, l'hypothèse (2.1) est satisfaite. Si $\alpha \in H^i(K,C)$, on peut donc parler du *résidu* $r_x(\alpha)$ *de* α *en* x ; on a $r_x(\alpha) \in H^{i-1}(k(x),C(-1))$. On démontre :

(3.1) *On a* $r_x(\alpha) = 0$ *pour tout* $x \in \underline{X}$ *sauf un nombre fini* (autrement dit l'ensemble des pôles de α est fini).

De façon plus précise, soit L/K une extension galoisienne finie de K assez grande pour que α provienne d'un élément de $H^i(\mathrm{Gal}(L/K),C_L)$, où $C_L = H^0(G_L,C)$. On a $r_x(\alpha) = 0$ pour tout x en lequel l'indice de ramification de L/K est premier à n.

(3.2) *On a la « formule des résidus »* :

$$\sum_{x \in \underline{X}} \mathrm{Cor}_k^{k(x)}\, r_x(\alpha) = 0 \qquad \textit{dans } H^{i-1}(k,C(-1)),$$

où $\mathrm{Cor}_k^{k(x)} : H^{i-1}(k(x),C(-1)) \to H^{i-1}(k,C(-1))$ *désigne l'homomorphisme de corestriction relativement à l'extension* $k(x)/k$.

[Précisons ce que l'on entend par Cor_E^F si F/E est une extension finie : c'est le produit de la corestriction galoisienne usuelle (correspondant à l'inclusion $G_F \to G_E$) par le degré inséparable $[F:E]_i$. Le composé $\mathrm{Cor}_E^F \circ \mathrm{Res}_F^E$ est égal à la multiplication par $[F:E]$.]

Application

Soit $f \in K^*$, et soit $D = \sum_{x \in \underline{X}} n_x x$ le diviseur de f. Supposons D disjoint de l'ensemble des pôles de α. Cela permet de définir un élément $\alpha(D)$ de $H^i(k,C)$ par la formule

$$\alpha(D) = \sum_{x \in |D|} n_x \mathrm{Cor}_k^{k(x)}\, \alpha(x).$$

On déduit de (3.2) la formule suivante :

$$(3.3) \quad \alpha(D) = \sum_{x \text{ pôle de } \alpha} \mathrm{Cor}_k^{k(x)}\, (f(x)).r_x(\alpha),$$

où :

$(f(x))$ est l'élément de $H^1(k(x),\mu_n)$ défini par l'élément $f(x)$ de $k(x)$, *via* la théorie de Kummer ;

$r_x(\alpha) \in H^{i-1}(k(x),C(-1))$ est le résidu de α en x ;

$(f(x)).r_x(\alpha)$ est le cup-produit de $(f(x))$ et de $r_x(\alpha)$ dans $H^i(k(x),C)$, relativement à l'application bilinéaire $\mu_n \times C(-1) \to C$.

Lorsque α n'a pas de pôles, (3.3) se réduit à :

$\alpha(D) = 0,$

analogue cohomologique du *théorème d'Abel.* Cela permet d'associer à α un homomorphisme du groupe des points rationnels de la jacobienne de X dans le groupe $H^i(k,C)$; pour $i = 1$, on retrouve une situation étudiée dans le cours de 1956-1957 (cf. *Groupes algébriques et corps de classes,* Hermann, Paris, 1959).

§4. Le cas où $K = k(T)$

C'est celui où X est la droite projective $\mathbf{P}_1$. Du fait que X possède un point rationnel, l'homomorphisme canonique $H^i(k,C) \to H^i(K,C)$ est injectif. Un élément de $H^i(K,C)$ est dit *constant* s'il appartient à $H^i(k,C)$. On démontre :

(4.1) *Pour que* $\alpha \in H^i(K,C)$ *soit constant, il faut et il suffit que* $r_x(\alpha) = 0$ *pour tout* $x \in \underline{X}$ (i.e. que α n'ait pas de pôles).

(4.2) *Pour tout* $x \in \underline{X}$, *soit* $\rho_x \in H^{i-1}(k(x),C(-1))$. *Supposons que* $\rho_x = 0$ *pour tout* x *sauf un nombre fini, et que* :

$$\sum_{x \in \underline{X}} \mathrm{Cor}_k^{k(x)} \rho_x = 0 \qquad \textit{dans } H^{i-1}(k,C(-1)).$$

Il existe alors $\alpha \in H^i(K,C)$ *tel que* $r_x(\alpha) = \rho_x$ *pour tout* $x \in \underline{X}$.

On peut résumer (3.1), (3.2), (4.1), (4.2) par la suite exacte :

$$(4.3) \quad 0 \to H^i(k,C) \to H^i(K,C) \to \bigoplus_{x \in \underline{X}} H^{i-1}(k(x),C(-1)) \to H^{i-1}(k,C(-1)) \to 0.$$

Remarque — Soit $\alpha \in H^i(K,C)$, et soit P l'ensemble de ses pôles. Les énoncés ci-dessus montrent que α est déterminé sans ambiguïté par ses résidus, et par sa valeur en un point rationnel de X non contenu dans P. En particulier, la *valeur* de α peut se calculer à partir de ces données. Voici une formule permettant de faire un tel calcul si $\infty \notin P$:

$$(4.4) \quad \alpha(x) = \alpha(\infty) + \sum_{y \in P} \mathrm{Cor}_k^{k(y)} (x - y).r_y(\alpha),$$

où :

$\alpha(x)$ est la valeur de α en un point rationnel $x \in X(k)$, $x \notin P$, $x \neq \infty$;

$\alpha(\infty)$ est la valeur de α au point ∞ ;

$(x - y)$ est l'élément de $H^1(k(y),\mu_n)$ défini par $x - y$;

$(x - y).r_y(\alpha)$ est le cup-produit de $(x - y)$ par le résidu $r_y(\alpha)$, calculé dans $H^i(k(y),C)$;

$\mathrm{Cor}_k^{k(y)}$ est la corestriction : $H^i(k(y),C) \to H^i(k,C)$.

Cela se déduit de (3.3), appliqué à la fonction $f(T) = x - T$, dont le diviseur D est $(x) - (\infty)$.

Généralisation à plusieurs variables

Soit $K = k(T_1,...,T_m)$ le corps des fonctions de l'espace projectif $\mathbf{P}_m$ de dimension m. Tout diviseur irréductible W de $\mathbf{P}_m$ définit une valuation discrète v_W de K. L'énoncé suivant se déduit de (4.1) par récurrence sur m :

(4.5) *Pour que* $\alpha \in H^i(K,C)$ *soit constant* (i.e. appartienne à $H^i(k,C)$), *il faut et il suffit que* α *n'ait de pôle en aucun* v_W (et l'on peut même se borner aux W distincts de l'hyperplan à l'infini, i.e. se placer sur *l'espace affine* de dimension m, et non sur l'espace projectif).

II. Application : spécialisation du groupe de Brauer

§5. Notations

Ce sont celles du §4, avec $i = 2$ et $C = \mu_n$, d'où $C(-1) = \mathbf{Z}/n\mathbf{Z}$. On a $H^2(K,C) = \mathrm{Br}_n K$, noyau de la multiplication par n dans le groupe de Brauer de K. La suite exacte (4.3) s'écrit alors :

$$0 \to \mathrm{Br}_n k \to \mathrm{Br}_n K \to \bigoplus_{x \in \underline{X}} H^1(k(x),\mathbf{Z}/n\mathbf{Z}) \to H^1(k,\mathbf{Z}/n\mathbf{Z}) \to 0.$$

Elle est due à D.K. Faddeev (*Trud. Math. Inst. Steklov* 38 (1951), 321-344).

Soit $\alpha \in \mathrm{Br}_n K$, et soit $P(\alpha) \subset \underline{X}$ l'ensemble de ses pôles. Si $x \in X(k)$ est un point rationnel de $X = \mathbf{P}_1$, et si $x \notin P(\alpha)$, la valeur de α en x est un élément $\alpha(x)$ de $\mathrm{Br}_n k$. On s'intéresse à la variation de $\alpha(x)$ avec x, et en particulier à l'ensemble $V(\alpha)$ des x tels que $\alpha(x) = 0$ (« *lieu des zéros de* α »). On aimerait comprendre la structure de $V(\alpha)$. (Par exemple, si k est infini, est-il vrai que $V(\alpha)$ est soit vide, soit de cardinal égal à celui de k ?).

Le cas où $n = 2$ et où α est un symbole (f,g), avec $f,g \in K^*$, est particulièrement intéressant, à cause de son interprétation en termes du *fibré en coniques* de base X défini par l'équation homogène

$$U^2 - f(T)V^2 - g(T)W^2 = 0.$$

L'étude de $V(\alpha)$ peut être abordée de plusieurs points de vue. Le cours en a envisagé trois :

annulation de α par changement de base rationnel (cf. §6) ;

conditions de Manin et approximation faible (cf. §7) ;

bornes du crible (cf. §8).

§6. Annulation par changement de base

On suppose, pour simplifier, que k est de caractéristique 0.

Soit $\alpha \in \mathrm{Br}_n\mathrm{K}$, avec $\mathrm{K} = k(\mathrm{T})$ comme ci-dessus. Soit $f(\mathrm{T}')$ une fonction rationnelle en une variable T' ; supposons f non constante. Si l'on pose $\mathrm{T} = f(\mathrm{T}')$, on obtient un plongement de K dans $\mathrm{K}' = k(\mathrm{T}')$. D'où, par changement de base, un élément $f^*\alpha$ de $\mathrm{Br}_n\mathrm{K}'$. On dit que α est *tué par* K'/K (ou par f) si $f^*\alpha = 0$ dans $\mathrm{Br}_n\mathrm{K}'$. S'il en est ainsi, on a $\alpha(t) = 0$ pour tout $t \in \mathrm{X}(k)$ qui n'est pas un pôle de α, et qui est de la forme $f(t')$, avec $t' \in \mathbf{P}_1(k)$. En particulier, $\mathrm{V}(\alpha)$ est *non vide* (et même de cardinal égal à celui de k). On peut se demander s'il y a une réciproque. D'où la question suivante :

(6.1) *Supposons* $\mathrm{V}(\alpha)$ *non vide. Existe-t-il une fonction rationnelle non constante f qui tue α ?*

Voici une variante « à point-base » de (6.1) :

(6.2) *Soit* $t_{\mathrm{o}} \in \mathrm{V}(\alpha)$. *Existe-t-il f comme dans* (6.1), *telle que t_{o} soit de la forme $f(t'_{\mathrm{o}})$, avec $t'_{\mathrm{o}} \in \mathbf{P}_1(k)$?*

On sait (Janchevskii, *Dokl. Akad. Nauk URSS,* 29, 1985, 1061-1064) que (6.2) a une réponse positive lorsque k est hensélien (ou lorsque $k = \mathbf{R}$).

Lorsqu'on ne fait pas d'hypothèse sur k, on n'a de résultats que pour $n = 2$. Pour les énoncer, introduisons la notation suivante :

(6.3) $d(\alpha) = \deg \mathrm{P}(\alpha) = \sum_{x \in \mathrm{P}(\alpha)} [k(x):k]$.

(L'entier $d(\alpha)$ est le *nombre de pôles* de α, multiplicités comprises.)

Théorème 6.4. (J.-F. Mestre, non publié) (i) *La question* (6.2) *a une réponse positive lorsque $n = 2$ et $d(\alpha) \leqslant 4$.*

(ii) *La question* (6.1) *a une réponse positive lorsque $n = 2$, $d(\alpha) = 5$, et que tout élément de* Br_2k *est un symbole* (i.e. toute forme quadratique sur k de rang 6 et de discriminant -1 représente 0).

Remarques

1) Dans (ii), la condition portant sur k est satisfaite lorsque k est un corps de nombres algébriques.

2) La démonstration du th. 6.4 donne des informations supplémentaires sur les corps $\mathrm{K}' = k(\mathrm{T}')$ qui tuent α : par exemple, on peut choisir K' tel que $[\mathrm{K}':\mathrm{K}] = 8$ dans le cas (i), et $[\mathrm{K}':\mathrm{K}] = 16$ dans le cas (ii).

Du th. 6.4, Mestre a déduit le résultat suivant :

Théorème 6.5. *Le groupe* $\mathbf{SL}_2(\mathbf{F}_7)$ *a la propriété* « Gal_T », *i.e. est groupe de Galois d'une extension galoisienne régulière de* $\mathbf{Q}(\mathrm{T})$.

En particulier, il existe une infinité d'extensions galoisiennes de $\mathbf{Q}$, deux à deux disjointes, dont le groupe de Galois est $\mathbf{SL}_2(\mathbf{F}_7)$.

Mestre a obtenu des résultats analogues pour les groupes $6.A_6$ et $6.A_7$.

§7. Conditions de Manin, approximation faible et hypothèse de Schinzel

On suppose maintenant que k est un *corps de nombres* algébriques, de degré fini sur $\mathbf{Q}$. Soit Σ l'ensemble de ses places (archimédiennes et ultramétriques) ; si $v \in \Sigma$, on note k_v le complété de k pour v. Soit $\mathbf{A}$ *l'anneau des adèles* de k, autrement dit le produit restreint des k_v $(v \in \Sigma)$.

Soit $X(\mathbf{A}) = \prod_v X(k_v)$ l'espace des points adéliques de $X = \mathbf{P}_1$. C'est un espace compact. A un élément α de $\mathrm{Br}_n\mathrm{K}$ on associe le sous-espace $V_{\mathbf{A}}(\alpha)$ défini de la façon suivante :

un point adélique $x = (x_v)$ appartient à $V_{\mathbf{A}}(\alpha)$ si, pour tout $v \in \Sigma$, on a $x_v \notin P(\alpha)$ et $\alpha(x_v) = 0$ dans $\mathrm{Br}_n k_v$.

(Autrement dit, $V_{\mathbf{A}}(\alpha)$ est l'ensemble des *solutions adéliques* de l'équation $\alpha(x) = 0$.)

Toute solution dans k de $\alpha(x) = 0$ est évidemment une solution adélique. On a donc une inclusion :

$V(\alpha) \subset V_{\mathbf{A}}(\alpha)$,

et l'on peut se demander quelle est *l'adhérence* de $V(\alpha)$ dans $V_{\mathbf{A}}(\alpha)$. Pour répondre (ou tenter de répondre) à cette question, il y a lieu d'introduire (à la suite de Colliot-Thélène et Sansuc) les « *conditions de Manin* » :

Disons qu'un élément β de $\mathrm{Br}_n\mathrm{K}$ est *subordonné* à α si, pour tout $x \in \underline{X}$, $r_x(\beta)$ est un multiple entier de $r_x(\alpha)$; on a en particulier $P(\beta) \subset P(\alpha)$. Soit $\mathrm{Sub}(\alpha)$ l'ensemble de ces éléments ; c'est un sous-groupe de $\mathrm{Br}_n\mathrm{K}$ contenant $\mathrm{Br}_n k$, et le quotient $\mathrm{Sub}(\alpha)/\mathrm{Br}_n k$ est fini. Si $\beta \in \mathrm{Sub}(\alpha)$, et si $x = (x_v)$ est un point de $V_{\mathbf{A}}(\alpha)$, on a $\beta(x_v) = 0$ pour presque tout v. Cela permet de définir un élément $m(\beta,x)$ de $\mathbf{Q}/\mathbf{Z}$ par la formule :

(7.1) $m(\beta,x) = \sum_v \mathrm{inv}_v\, \beta(x_v)$,

où inv_v désigne l'homomorphisme canonique de $\mathrm{Br}\, k_v$ dans $\mathbf{Q}/\mathbf{Z}$. La fonction $x \mapsto m(\beta,x)$ est localement constante sur $V_{\mathbf{A}}(\alpha)$ et s'annule sur $V(\alpha)$; de plus, elle ne dépend que de la classe de β mod $\mathrm{Br}_n k$. Notons $V_{\mathbf{A}}^{\mathrm{M}}(\alpha)$ le sous-espace de $V_{\mathbf{A}}(\alpha)$ défini par les « conditions de Manin » :

(7.2) $m(\beta,x) = 0$ *pour tout* $\beta \in \mathrm{Sub}(\alpha)$.

C'est un sous-espace *ouvert et fermé* de $V_{\mathbf{A}}(\alpha)$ qui contient $V(\alpha)$. Il paraît raisonnable de faire la *conjecture* suivante :

(7.3 ?) $V(\alpha)$ *est dense dans* $V_{\mathbf{A}}^{\mathrm{M}}(\alpha)$.

En particulier :

(7.4 ?) *Si* $V_{\mathbf{A}}^{M}(\alpha) \neq \emptyset$, *on a* $V(\alpha) \neq \emptyset$: les conditions de Manin sont « les seules » à s'opposer à l'existence d'une solution rationnelle de l'équation $\alpha(x) = 0$.

(7.5 ?) *Si* $\mathrm{Sub}(\alpha) = \mathrm{Br}_n k$ (i.e. s'il n'y a pas de conditions de Manin), $V(\alpha)$ *est dense dans* $V_{\mathbf{A}}(\alpha)$; il y a *approximation faible* ; le principe de Hasse est valable.

La plupart des résultats concernant (7.3 ?), (7.4 ?) et (7.5 ?) sont relatifs au cas $n = 2$. Dans le cas général, on a toutefois le théorème suivant, qui complète des résultats antérieurs de Colliot-Thélène et Sansuc (1982) et Swinnerton-Dyer (1991) :

Théorème 7.6. *L'hypothèse* (H) *de Schinzel entraîne* (7.3 ?).

[Rappelons l'énoncé de l'hypothèse (H) : soient $P_1(T),\ldots,P_m(T)$ des polynômes à coefficients dans $\mathbf{Z}$, irréductibles sur $\mathbf{Q}$, de termes dominants > 0, et tels que, pour tout nombre premier p, il existe $n_p \in \mathbf{Z}$ tel que $P_i(n_p) \not\equiv 0 \pmod{p}$ pour $i = 1,\ldots,m$. Alors il existe une infinité d'entiers $n > 0$ tels que $P_i(n)$ soit un nombre premier pour $i = 1,\ldots,m$.]

Remarque

Le th. 7.6 peut être étendu aux *systèmes d'équations* $\alpha_i(x) = 0$, où les α_i sont des éléments de $\mathrm{Br}_n K$ en nombre fini. On doit alors remplacer $\mathrm{Sub}(\alpha)$ par l'ensemble des $\beta \in \mathrm{Br}_n K$ tels que, pour tout $x \in \underline{X}$, $r_x(\beta)$ appartienne au sous-groupe de $H^1(k(x),\mathbf{Z}/n\mathbf{Z})$ engendré par les $r_x(\alpha_i)$.

§8. Bornes du crible

On conserve les notations ci-dessus, et l'on suppose en outre (pour simplifier) que $k = \mathbf{Q}$. Si $x \in X(k) = \mathbf{P}_1(\mathbf{Q})$, on note $H(x)$ la *hauteur* de x : si $x = p/q$ où p et q sont des entiers premiers entre eux, on a $H(x) = \sup(|p|, |q|)$. Si $H \to \infty$, le nombre des x tels que $H(x) \leqslant H$ est $cH^2 + O(H.\log H)$, avec $c = 12/\pi^2$.

Soit $N_\alpha(H)$ le nombre des $x \in V(\alpha)$ tels que $H(x) \leqslant H$. On aimerait connaître la croissance de $N_\alpha(H)$ quand $H \to \infty$. Un argument de crible (cf. *C.R. Acad. Sci. Paris,* 311 (1990), 397-402) permet en tout cas d'en donner une *majoration.* Pour énoncer le résultat, convenons de noter $e_x(\alpha)$ l'ordre du résidu $r_x(\alpha)$ de α en x (pour $x \in \underline{X}$) ; on a $e_x(\alpha) = 1$ si x n'est pas un pôle de α. Posons

(8.1) $\delta(\alpha) = \sum_{x \in \underline{X}} (1 - 1/e_x(\alpha)).$

Théorème 8.2. *On a* $N_\alpha(H) << H^2/(\log H)^{\delta(\alpha)}$ *pour* $H \to \infty$.

Noter que, si α n'est pas constant, on a $\delta(\alpha) > 0$, et le théorème ci-dessus montre que « peu » de points rationnels appartiennent à $V(\alpha)$.

On peut se demander si la majoration ainsi obtenue est optimale, sous l'hypothèse $V(\alpha) \neq \emptyset$. Autrement dit :

(8.3) *Est-il vrai que* $N_\alpha(H) >> H^2/(\log H)^{\delta(\alpha)}$ *pour* H *assez grand, si* $V(\alpha) \neq \emptyset$?

Remarque

Il y a des énoncés analogues pour les corps de nombres, et pour les systèmes d'équations $\alpha_i(x) = 0$; on doit alors remplacer $e_x(\alpha)$ par l'ordre du groupe engendré par les $r_x(\alpha_i)$.

PUBLICATIONS

J.-P. SERRE, *Motifs*, Astérisque 198-199-200 (1991), 333-349.

— , *Lettre à M. Tsfasman*, Astérisque 198-199-200 (1991), 351-353.

— , *Topics in Galois Theory* (notes written by Henri Darmon), Jones and Bartlett Publ., Boston, 1992, 117 p.

— , *Lie Algebras and Lie Groups* (1964 Lectures given at Harvard University), 2e édition, Lect. Notes in Math. 1500, Springer-Verlag, 1992, 168 p.

MISSIONS

Exposés

— *Historical introduction to motives,* Seattle, juillet 1991.

— *The motivic Galois group,* Seattle, juillet 1991.

— *ℓ-adic representations associated to abelian varieties,* Seattle, août 1991.

— *Asymptotic properties of eigenvalues of graphs and Hecke operators,* Oxford, septembre 1991.

— *Le crible et les coniques*, Besançon, octobre 1991.

— *Problems in Galois cohomology*, Ascona, novembre 1991.

— *La forme trace en rang* 6 *ou* 7, Ascona, novembre 1991.

— *Revêtements de courbes algébriques*, séminaire Bourbaki, novembre 1991.

— *Une application de l'hypothèse* (H) *de Schinzel*, Bordeaux, février 1992.

— *Cohomologie galoisienne : éléments génériques, d'après Grothendieck* (2 exposés), séminaire de la chaire de Théorie des Groupes, Collège de France, mars 1992.

— *Nombres premiers, groupes de Galois, etc*, Genève, avril 1992.

— *Rademacher lectures* (3 exposés), Philadelphie, mai 1992.

— *Galois cohomology of* $k(t)$, Philadelphie, mai 1992 ; Sundance, mai 1992.

— *Negligible cohomology classes*, Sundance, mai 1992.