Algèbre et géométrie

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

Le cours a continué ceux de 1962/1963, 1990/1991 et 1991/1992, consacrés à la *cohomologie galoisienne*. Il a comporté trois parties :

1. Cohomologie négligeable

1.1. *Notations.* Si k est un corps commutatif, on note k_s une clôture séparable de k, et Γ_k le groupe de Galois de k_s sur k. Si M est un Γ_k-module (discret), on note indifféremment $H^q(\Gamma_k, M)$ et $H^q(k, M)$ ses groupes de cohomologie.

1.2. *Définition de la cohomologie négligeable.* Soient G un groupe fini et M un G-module. Un élément x de $H^q(G,M)$ est dit *négligeable* si, pour tout corps k et tout homomorphisme continu $\varphi : \Gamma_k \to G$, on a $\varphi^*(x) = 0$ dans $H^q(k,M)$, cf. *Résumé de cours* 1990/1991, §7.

Cette définition fait intervenir, en apparence, tous les corps k, et tous les homomorphismes φ. En fait, on peut construire, pour chaque groupe fini G, une extension galoisienne « verselle » L_G/K_G, de groupe de Galois G, telle que $x \in H^q(G,M)$ soit négligeable si et seulement si $\varphi^*(x) = 0$ pour l'homomorphisme $\varphi : \Gamma_{K_G} \to G$ associé à L_G. (Si l'on choisit un plongement de G dans un groupe symétrique S_N, on peut prendre pour L_G le corps de fonctions rationnelles $\mathbf{Q}(T_1, \ldots, T_N)$, sur lequel G opère de façon évidente.)

On déduit de là :

1.3. *Il existe un entier* $q(G)$ *tel que, si* $q > q(G)$, *les deux propriétés suivantes d'un élément* x *de* $H^q(G,M)$ *soient équivalentes* :

(i) *x est négligeable* ;

(ii) *la restriction de x aux sous-groupes d'ordre* 2 *de* G *est nulle.*

(Noter que l'implication (i) $\Rightarrow$ (ii) est vraie sans supposer $q > q(\mathrm{G})$.)

En particulier, *tout élément d'ordre impair de* $\mathrm{H}^q(\mathrm{G},\mathrm{M})$ *est négligeable si* $q > q(\mathrm{G})$.

1.4. L'énoncé ci-dessus donne une caractérisation simple des classes de cohomologie négligeables lorsque la dimension q est grande. Dans la direction opposée, on a :

(a) *Si* $q \leqslant 1$, *ou si* $q = 2$ *et* G *opère trivialement sur* M, *aucun élément non nul de* $\mathrm{H}^q(\mathrm{G},\mathrm{M})$ *n'est négligeable.*

D'autre part (cf. B.B. Lure, *Trudy Math. Inst. Steklov* 183, 1990) :

b) *Si l'ordre de* G *est* > 2, *il existe un* G-*module fini* M *tel que* $\mathrm{H}^2(\mathrm{G},\mathrm{M})$ *contienne un élément négligeable* $\neq 0$.

1.5. *Détermination des classes de cohomologie négligeables lorsque* G *est cyclique d'ordre premier.*

Supposons G cyclique d'ordre premier p, et soit s un générateur de G. Le cas $p = 2$ est peu intéressant : il n'y a pas de classe de cohomologie négligeable, à part 0, comme on le voit en prenant $k = \mathbf{R}$.

Supposons donc $p > 2$. Soit $\hat{\mathrm{G}}$ le pro-p-groupe défini par deux générateurs u,v liés par la relation $uvu^{-1} = v^{1+p}$, et soit $\varphi : \hat{\mathrm{G}} \rightarrow \mathrm{G}$ l'unique homomorphisme continu tel que $\varphi(u) = 1$ et $\varphi(v) = s$. On démontre :

(a) *Pour que* $x \in \mathrm{H}^q(\mathrm{G},\mathrm{M})$ *soit négligeable, il faut et il suffit que* $\varphi^*(x) = 0$ *dans* $\mathrm{H}^q(\hat{\mathrm{G}},\mathrm{M})$.

Comme $\hat{\mathrm{G}}$ est un groupe de dimension cohomologique stricte égale à 2, on déduit de là :

(b) *Si* $q > 2$, *tout élément de* $\mathrm{H}^q(\mathrm{G},\mathrm{M})$ *est négligeable.*

Pour $q = 2$, la situation est différente. Si l'on identifie $\mathrm{H}^2(\mathrm{G},\mathrm{M})$ à $\mathrm{Ker}_{\mathrm{M}}(1 - s)/\mathrm{Im}_{\mathrm{M}}(1 + s + \ldots + s^{p-1})$, on trouve :

(c) *Pour que* $x \in \mathrm{H}^2(\mathrm{G},\mathrm{M})$ *soit négligeable, il faut et il suffit que l'on puisse représenter* x *par un élément de* $\mathrm{Ker}_{\mathrm{M}}(1 - s)$ *de la forme* $y - sy$, *où* y *est un élément de* M *d'ordre une puissance de* p.

1.6. *Autres exemples.* On aimerait avoir des résultats aussi précis que ceux du n° 1.5 pour d'autres groupes finis, ne serait-ce que les groupes cycliques d'ordre p^m, $m > 1$. Cela ne paraît pas facile, à moins de faire des hypothèses restrictives sur le G-module M. Ainsi, lorsque $\mathrm{M} = \mathbf{Z}/2\mathbf{Z}$, on peut déterminer pour tout q la partie négligeable de $H^q(G,\mathbf{Z}/2\mathbf{Z})$ lorsque G est l'un des groupes suivants :

$C_2 \times \ldots \times C_2$, 2-groupe abélien élémentaire ;

C_{2^m}, groupe cyclique d'ordre 2^m ;

D_4, groupe diédral d'ordre 8 ;

Q_8, groupe quaternionien d'ordre 8.

Dans chacun de ces cas, on constate qu'un élément de $H^q(G,\mathbf{Z}/2\mathbf{Z})$, $q > 2$, est négligeable si et seulement si ses restrictions aux sous-groupes d'ordre 2 de G sont nulles. Par exemple, si $G = Q_8$, les éléments non nuls de $H^q(G,\mathbf{Z}/2\mathbf{Z})$, $q > 2$, sont négligeables si q n'est pas divisible par 4.

1.7. *Le cas du groupe symétrique* S_n

On démontre en utilisant les résultats du n° 2.2 ci-après :

(a) *Tout élément de* $H^q(S_n,\mathbf{Z}/N\mathbf{Z})$, $q > 0$, N *impair, est négligeable.*

(On suppose que l'action de S_n sur $\mathbf{Z}/N\mathbf{Z}$ est triviale.)

(b) *Pour qu'un élément de* $H^q(S_n,\mathbf{Z}/2\mathbf{Z})$ *soit négligeable, il faut et il suffit que ses restrictions aux sous-groupes d'ordre* 2 *de* S_n *soient nulles.*

2. Invariants des algèbres étales

2.1. *Invariants cohomologiques de* G*-torseurs*

Rappelons la définition (cf. *Sém. Bourbaki,* exposé 783, §6).

Les données sont :

— un groupe algébrique lisse G sur un corps k_o ;

— un entier $i \geqslant 0$ et un module galoisien C sur k_o, que l'on suppose fini d'ordre premier à la caractéristique de k_o.

A toute extension k de k_o sont attachés, d'une part l'ensemble pointé $H^1(k,G)$ des classes de G-torseurs sur k, et d'autre part le groupe de cohomologie $H^i(k,G)$

Un *invariant cohomologique* de type $H^i(.,C)$, pour les G-torseurs, est *un morphisme a du foncteur* $H^1(k,G)$ *dans le foncteur* $H^i(k,C)$, défini sur la catégorie des extensions k de k_o. Un tel invariant associe, à tout G-torseur X sur k, un élément $a(X)$ de $H^i(k,C)$; de plus, si k' est une extension de k, et si X' est le G-torseur sur k' déduit de X par extension des scalaires, l'invariant $a(X')$ est l'image de $a(X)$ par l'application $H^i(k,C) \to H^i(k',C)$.

2.2. *Invariants cohomologiques des algèbres étales de rang donné*

On peut appliquer ce qui précède au cas où G est le *groupe symétrique* S_n ($n \geqslant 1$), vu comme groupe algébrique de dimension 0. Dans ce cas, un G-torseur X sur k s'interprête comme :

— un homomorphisme continu $\varphi : \Gamma_k \to S_n$, à conjugaison près ;

— une k-algèbre étale E de rang n, à isomorphisme près.

Un invariant cohomologique de type $H^i(.,C)$ pour S_n, est une fonction

$$E \mapsto a\,(E) \in H^i(k,C)$$

qui, à toute algèbre étale E de rang n sur une extension k de k_o, associe un élément de $H^i(k,C)$, de façon compatible avec les extensions de scalaires. (Cette dernière propriété entraîne aussi une compatibilité avec les *spécialisations,* comme me l'a signalé M. Rost.)

Convenons de dire qu'une algèbre étale est *multiquadratique* si elle est produit d'algèbres de rang 1 ou 2. On démontre :

(i) *Supposons que* $a(E) = 0$ *pour toute algèbre multiquadratique. Alors* $a = 0$.

Disons que a est *normalisé* si $a(E) = 0$ lorsque E est *scindée* (i.e. isomorphe à $k \times \ldots \times k$).

(ii) *Si* a *est normalisé, on a* $2a = 0$.

Le cas le plus intéressant est celui où $C = \mathbf{Z}/2\mathbf{Z}$ (k_o étant de caractéristique $\neq 2$). Si E est une algèbre étale de rang n sur k, la *forme trace* q_E de E est une forme quadratique non dégénérée de rang n. Ses classes de Stiefel-Whitney $w_i(q_E) \in H^i(k,\mathbf{Z}/2\mathbf{Z})$ sont des *invariants cohomologiques* de type $H^i(.,\mathbf{Z}/2\mathbf{Z})$ de l'algèbre étale E. En fait, ce sont essentiellement les seuls. On déduit en effet de (i) le résultat suivant :

(iii) *Si* $C = \mathbf{Z}/2\mathbf{Z}$, *tout invariant cohomologique de type* $H^i(.,C)$ *s'écrit de façon unique sous la forme :*

$$a(E) = \sum_{j=0}^{m} \gamma_j \; w_j(q_E) \quad \textit{avec} \quad \gamma_j \in H^{i-j}(k_o,C) \textit{ et } m = [n/2].$$

Lorsqu'on applique ceci aux classes de Stiefel-Whitney *galoisiennes* $w_i^{\mathrm{gal}}(E)$, on retrouve une formule de B. Kahn (*Invent. Math.* 78, 1984) :

$$\text{(iv)} \quad w_i^{\mathrm{gal}}(E) = \begin{cases} w_i(q_E) & \textit{si } i \textit{ est impair} \\ w_i(q_E) + (2)\cdot w_{i-1}(q_E) & \textit{si } i \textit{ est pair} \end{cases}$$

De plus :

(v) *On a* $w_i^{\mathrm{gal}}(E) = 0$ *si* $i > m = [n/2]$.

2.3. *Invariants à valeurs dans le groupe de Grothendieck-Witt*

Supposons la caractéristique $\neq 2$. Dans la définition des invariants cohomologiques on peut remplacer le foncteur $k \mapsto \mathrm{H}^i(k,\mathrm{C})$ par le foncteur $k \mapsto \mathrm{GrW}(k)$, où $\mathrm{GrW}(k)$ est *l'anneau de Grothendieck-Witt* des classes de formes quadratiques sur k. (On pourrait utiliser aussi l'anneau de Witt usuel $\mathrm{W}(k)$, mais c'est moins commode, car les puissances extérieures λ^i sont définies sur $\mathrm{GrW}(k)$ mais pas sur $\mathrm{W}(k)$.) On obtient ainsi la notion d'*invariant de type* GrW des algèbres étales de rang n. Exemple : l'application

$$\mathrm{E} \mapsto \lambda^i(q_{\mathrm{E}}),$$

qui, à une k-algèbre étale E, associe la puissance extérieure i-ème de sa forme trace.

Les résultats du n° 2.2. se transposent sans difficulté. Ainsi :

(i) *Si un invariant de type* GrW *s'annule sur les algèbres multiquadratiques, il est identiquement nul.*

(ii) *Tout invariant de type* GrW *est combinaison linéaire, à coefficients dans* $\mathrm{GrW}(k_o)$, *des* $\lambda^i(q_{\mathrm{E}})$, $0 \leqslant i \leqslant m = [n/2]$.

Ceci permet de prouver des identités portant sur les $\lambda^i(q_{\mathrm{E}})$ en les vérifiant lorsque E est multiquadratique. Or, dans ce cas, on peut écrire q_{E} sous la forme $\omega_n \oplus q'$, où q' est de rang m, et où ω_n est la forme de rang $n - m$ définie par :

$$\omega_n = \begin{cases} m\langle 2\rangle = \langle 2, \ldots, 2\rangle & \text{si } n = 2m \\ 1 + m\langle 2\rangle = \langle 1,2, \ldots, 2\rangle & \text{si } n = 2m + 1. \end{cases}$$

On obtient ainsi :

(iii) *Pour tout algèbre étale* E *de rang n, on a* :

$\lambda^n(q_{\mathrm{E}}) \cdot \lambda^i(q_{\mathrm{E}} - \omega_n) = \langle 2^m\rangle \cdot \lambda^{m-i}(q_{\mathrm{E}} - \omega_n)$ *pour tout* i.

Noter que $\lambda^n(q_{\mathrm{E}}) = \langle d_{\mathrm{E}}\rangle$, où d_{E} est le discriminant de E, de sorte que la formule ci-dessus peut s'écrire :

(iii′) $\lambda^i(q_{\mathrm{E}} - \omega_n) = \langle 2^m d_{\mathrm{E}}\rangle \cdot \lambda^{m-i}(q_{\mathrm{E}} - \omega_n)$ *pour tout* i.

En particulier :

(iv) *On a* $\lambda^i(q_{\mathrm{E}} - \omega_n) = 0$ *pour tout* $i > m$.

3. La forme trace en rang $\leqslant 7$

Soit k un corps de caractéristique $\neq 2$. Soit n un entier $\geqslant 1$. Une forme quadratique q sur k, de rang n, est appelée une *forme trace* s'il existe une k-algèbre étale E de rang n telle que q_{E} soit isomorphe à q.

Le cas où n est impair se ramène à celui où n est pair. En effet, il résulte d'une construction de Mestre (*J. Algebra* 131, 1990) que l'on a :

3.1. *Une forme quadratique de rang n impair est une forme trace si et seulement si elle est isomorphe à $<1> \oplus q'$, où q' est une forme trace de rang $n-1$.*

3.2. *Caractérisation des formes trace de rang $\leqslant 7$*

Vu 3.1., on peut se borner à $n = 2$, 4 ou 6. On trouve alors qu'*une forme quadratique q de rang n est une forme trace si et seulement si elle satisfait aux conditions suivantes* :

(pour $n = 2$) *q contient $<2>$* ;

(pour $n = 4$) *q contient $<1>$ et $w_3(q) = 0$* ;

(pour $n = 6$) *q contient $<1,2>$, et contient $<1,1,2>$ sur $k(\sqrt{2d})$, où d est le discriminant de q.*

3.3. *Action des automorphismes externes de S_6*

Le cas $n = 6$ présente un intérêt particulier : c'est le seul où le groupe $\mathrm{Out}(S_n) = \mathrm{Aut}(S_n)/\mathrm{Int}(S_n)$ soit non trivial. Si E est une algèbre étale de rang 6, correspondant à $\varphi : \Gamma_k \rightarrow S_6$, le composé φ' de φ et d'un automorphisme externe de S_6 définit une autre algèbre étale E′ de rang 6 (« résolvante sextique »). D'après le n° 2.3, la forme trace de E′ peut s'exprimer en termes des $\lambda^i(q_E)$. On trouve :

$$q_{E'} = \lambda^3(q_E) - <1,2> \cdot \lambda^2(q_E) + <1,1,2> \cdot q_E - <1,2> \quad \text{dans } \mathrm{GrW}(k).$$

Cette formule se simplifie si l'on écrit :

$$q_E = <1,2> \oplus Q \text{ et } q_{E'} = <1,2> \oplus Q',$$

où Q et Q′ sont des formes de rang 4, cf. n° 3.2 ; on obtient :

$$Q' = \lambda^3(Q) = <2d> \cdot Q, \text{ avec } d = \mathrm{discr}(E) = \mathrm{discr}(E').$$

Le cas particulier $d = 1$ avait été déjà obtenu dans le cours 1990/1991.

3.4. *Formes trace de rang 6 ou 7 avec $w_1 = w_2 = 0$*

Soit q une forme quadratique non dégénérée de rang 6 telle que $w_1(q) = w_2(q) = 0$.

On prouve en utilisant le critère du n° 3.2 :

(i) *Pour que q soit une forme trace, il faut et il suffit qu'il existe $c \in k^*$ tel que* :

(i_1) $q \simeq <1,1,c,c,c,c>$.

(i_2) *c est somme de* 4 *carrés dans* $k(\sqrt{2})$.

(i_3) $(2)(c) = 0$ *dans* $H^2(k,\mathbf{Z}/2\mathbf{Z})$, *i.e. c est représenté par la forme* $<1,-2>$.

D'après 3.1., il y a un énoncé analogue en rang 7 : dans (i_1) on remplace $<1,1,c,c,c,c>$ par $<1,1,1,c,c,c,c>$.

Disons qu'un corps k *a la propriété* (0) si tout $c \in k^*$ satisfaisant à (i_2) et (i_3) est somme de 4 carrés dans k (ce qui équivaut à $<c,c,c,c>$ isomorphe à $<1,1,1,1>$). D'après (i), cela revient à dire que toute forme trace q, de rang 6 ou 7 et telle que $w_1(q) = w_2(q) = 0$, est isomorphe à la forme unité $<1,\ldots,1>$. On démontre :

(ii) *Tout corps où* -1 *est somme de* 2 *carrés* (par exemple tout corps de caractéristique > 0) *a la propriété* (0).

(iii) *Toute extension transcendante pure d'un corps de nombres ou d'un corps local* (à corps résiduel fini) *a la propriété* (0).

(iv) *Il existe des corps n'ayant pas la propriété* (0), *par exemple le corps des fonctions sur* **Q** *de la quadrique projective d'équation homogène* :

$$7X_0^2 + X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0.$$

(Cela se voit en remarquant que $c = -1$ satisfait à (i_2) et (i_3), mais n'est pas somme de 4 carrés.)

L'exemple donné dans (iv) est de degré de transcendance 4 sur **Q**. J'ignore s'il existe des exemples analogues de degré de transcendance 1, 2, ou 3.

3.5. *Application au problème de Noether pour certains sous-groupes de* $2.A_7$

Soit $2.A_7$ l'unique extension non triviale du groupe alterné A_7 par un groupe à 2 éléments. Une algèbre étale E de rang 7 est telle que $w_1(q_E) = w_2(q_E) = 0$ si et seulement si E est définie par un homomorphisme $\Gamma_k \to S_7$ qui se factorise en $\Gamma_k \to 2.A_7 \to A_7 \to S_7$. En utilisant les résultats du n° 3.4, on démontre :

(i) *Soit* G *un sous-groupe d'indice impair de* $2.A_7$ (par exemple $2.A_7$, $2.A_6$, $\mathbf{SL}_2(\mathbf{F}_7)$ ou le groupe quaternionien Q_{16}). *Soit* L_G/K_G *une* G*-extension galoisienne verselle en caractéristique* 0. *Alors* K_G *n'est pas une extension transcendante pure de* **Q**.

(En effet, soit $k = K_G$, et soit E la k-algèbre étale de rang 7 associée à

$$\Gamma_k \to \mathrm{Gal}(L_G/k) = G \to 2.A_7 \to A_7 \to S_7.$$

Si la forme trace de E était la forme unité $<1, \ldots 1>$, il en serait de même (vu le caractère versel de L_G/k) pour toute algèbre étale de rang 7 provenant d'un G-torseur. Or l'exemple du n° 3.4. (iv), convenablement précisé, montre que ce n'est pas toujours le cas. Il en résulte que k n'a pas la propriété (0). Vu le n° 3.4. (iii), ce n'est donc pas une extension transcendante pure de $\mathbf{Q}$.)

En particulier :

(ii) *Si l'on plonge* G *dans un groupe symétrique* S_N, *le corps des* G-*invariants de* $\mathbf{Q}(T_1, \ldots, T_N)$ *n'est pas une extension transcendante pure de* $\mathbf{Q}$.

En d'autres termes le *problème de Noether* a une solution négative pour G.

Publications

E. Bayer-Fluckiger et J.-P. Serre, *Torsions quadratiques et bases normales autoduales,* Amer. J. of Math. 116 (1994), 1-63.

T. Ekedahl et J.-P. Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable,* C.R. Acad. Sci. Paris 317 (1993), 509-513.

J.-P. Serre, *Gèbres,* L'Enseignement Math. 39 (1993), 33-85.

— , *Smith, Minkowski et l'Académie des Sciences* (avec des notes de N. Schappacher), Gazette des Mathématiciens 56 (1993), 3-9 ; traduction allemande : D.M.V. Mitteilungen 2 (1993), 4-7.

— , *Sur la semi-simplicité des produits tensoriels de représentations de groupes,* Invent. math. 116 (1994), 513-530.

— , *A letter as an appendix to the square-root parameterization paper of Abhyankar,* in *Algebraic Geometry and Its Applications* (C.L. Bajaj edit.), 85-88, Springer-Verlag, 1994.

— , *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques,* Proc. Symp. Pure Math. 55 (1994), vol. 1, 377-400.

Édition

U. Jannsen, S. Kleiman et J.-P. Serre (édit.), *Motives,* A.M.S. Symposia Pure Math. 55 (1994), 2 vol., 1423 p.

MISSIONS

Exposés

— *Tensor products of semisimple representations,* Spetses, juillet 1993 :

— *Negligible cohomology,* Spetses, juillet 1993 ;

— *Résultats préliminaires au théorème de Fermat-Wiles,* Bordeaux, septembre 1993 ;

— *Représentations linéaires sur les anneaux locaux, d'après Carayol,* Sém. Chevalley, octobre 1993 ; Orsay, mai 1994 ;

— *Distribution asymptotique des valeurs propres d'opérateurs de Hecke,* Besançon, octobre 1993 ;

— *Asymptotic repartition of eigenvalues of Hecke operators,* Hong Kong, décembre 1993 ;

— *Exemples* : $X_o(11)$ *et* $X_1(11)$, Inst. H. Poincaré, janvier 1994 ;

— *Les conjectures de Duke* (2 exposés), Inst. H. Poincaré, janvier 1994 ;

— *La stratégie de Wiles,* Inst. H. Poincaré, janvier 1994 ;

— *Cohomologie galoisienne : progrès et problèmes,* Sém. Bourbaki, mars 1994 ;

— *Sous-groupes finis de* $\mathbf{GL}_n(\mathbf{Q}),\ldots, E_8(\mathbf{Q})$, Sém. Chevalley, mars 1994 ;

— *Tensor products of group representations in characteristic p,* Berkeley, avril 1994 ;

— *Finite subgroups of exceptional Lie groups,* Berkeley, avril 1994 ;

— *Cohomological invariants of étale algebras,* Berkeley, mai 1994 ;

— *De* S_4 *dans* $\mathbf{SO}_3$ *à* $\mathbf{PGL}_2(\mathbf{F}_{31})$ *dans* E_8, Sém. Chevalley, juin 1994 ;

— *λ-opérations et formes quadratiques,* Luminy, juin 1994 ;

— *Galois representations and Chebotarev's density theorem,* Amsterdam, juin 1994.