Algèbre et géométrie

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

Le cours, comme celui de l'année précédente, a été consacré au « problème inverse de la théorie de Galois » : étant donné un groupe fini G, existe-t-il une extension galoisienne L de $\mathbf{Q}$ telle que le groupe de Galois $\mathrm{Gal}(L/\mathbf{Q})$ soit isomorphe à G ?

En fait, on s'est intéressé à la propriété plus précise suivante de G :
(Gal_T). — Il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois G.

Des exemples de groupes ayant cette propriété avaient déjà été donnés dans le cours de 1988-1989. La méthode suivie cette année a été basée sur la notion de « rigidité », due à Belyi, Fried, Matzat et Thompson (voir notamment B.H. Matzat, *Konstruktive Galoistheorie*, Lect. Notes in Math. n° 1284, Springer-Verlag, 1987, ainsi que l'exposé 689 du séminaire Bourbaki, 1987-1988).

Enoncé du théorème de rigidité

On considère un groupe fini G, dont on choisit des classes de conjugaison $C_1, \ldots, C_k$. On fait les deux hypothèses suivantes :

(1) (« rationalité »). Chacune des classes C_i est rationnelle sur $\mathbf{Q}$. Cela signifie que $x \in C_i$ entraîne $x^m \in C_i$ pour tout m premier à l'ordre de x.

(2) (« rigidité »). Il existe $x_1 \in C_1, \ldots, x_k \in C_k$ tels que $x_1 \ldots x_k = 1$ et que G soit engendré par les x_i. De plus, si $x'_1, \ldots, x'_k$ est une autre famille d'éléments jouissant des mêmes propriétés, il existe $g \in G$ tel que $x'_i = g x_i g^{-1}$ pour tout i.

Théorème - *Supposons que le centre de* G *soit trivial, et que les classes* $C_1, \ldots, C_k$ *satisfassent à* (1) *et* (2). *Soit* K *un corps de caractéristique zéro, et soient* $Q_1, \ldots, Q_k$ *des points* K*-rationnels, deux à deux distincts, de la droite*

projective $\mathbf{P}_1$. *Il existe alors une extension galoisienne régulière* L *du corps* K(T) *des fonctions rationnelles sur* $\mathbf{P}_1$ *jouissant des propriétés suivantes* :

(a) *Le groupe de Galois* Gal(L/K(T)) *est* G.

(b) *L'extension* L/K(T) *est non ramifiée en dehors des* Q_i.

(c) *Pour tout i, le groupe d'inertie en* Q_i (défini à conjugaison près) *est engendré par un élément appartenant à la classe* C_i.

De plus, une telle extension L *est unique, à isomorphisme unique près.*

Notons X la courbe algébrique, projective et lisse, dont le corps de fonctions est le corps L cherché. C'est un revêtement galoisien ramifié de $\mathbf{P}_1$. Lorsque le corps de base est le corps $\mathbf{C}$ des nombres complexes, l'existence et l'unicité de X résultent du théorème d'existence de Riemann (dont la démonstration a été rappelée dans le cours, en même temps que celle des théorèmes du type « GAGA »). On passe ensuite de $\mathbf{C}$ à K par un argument de « descente » reposant de façon essentielle sur *l'unicité* de la courbe cherchée.

Le théorème ci-dessus, appliqué avec $K = \mathbf{Q}$, donne :

Corollaire - *Tout groupe fini* G *à centre trivial possédant des classes ayant les propriétés* (1) *et* (2) *jouit de la propriété* Gal_T. *En particulier,* G *est groupe de Galois d'une infinité d'extensions de* $\mathbf{Q}$, *linéairement disjointes.*

Variantes du théorème de rigidité

Ces variantes visent à affaiblir les hypothèses (1) et (2), qui sont très difficiles à satisfaire. Un certain nombre d'entre elles ont été exposées dans le cours, avec applications aux groupes suivants :

— S_n, A_5 , $SL_2(\mathbf{F}_8)$, J_1, J_2 ;

— $PSL_2(\mathbf{F}_p)$ pour p premier tel que $\left(\frac{2}{p}\right) = -1$ ou $\left(\frac{3}{p}\right) = -1$;

— $3\cdot A_6$, $3\cdot A_7$, $3\cdot M_{22}$, 3·McL, 3·Suz, 3·O'N, $3\cdot F_{22}$, $3\cdot F'_{24}$, d'après W. Feit ;

— $PSL_2(\mathbf{F}_{p^2})$ pour p premier $\equiv \pm 2 \pmod 5$, d'après W. Feit.

D'autres variantes, exploitant l'action du *groupe des tresses* sur les solutions de $x_1 \ldots x_k = 1$, ont été exposées dans le séminaire par G. Malle (le cours a tenté — avec un succès limité — d'en donner une interprétation géométrique).

Propriétés locales des extensions de $\mathbf{Q}$(T) *fournies par la méthode de rigidité*

Le cas réel n'est pas difficile, mais on sait peu de choses dans le cas p-adique. Ainsi, si G satisfait aux conditions du théorème ci-dessus, avec $k = 3$, et si $X \to \mathbf{P}_1$ désigne le revêtement correspondant, est-il vrai que ce revêtement « se réduit bien mod p » pourvu que p ne divise pas l'ordre des éléments de C_1, C_2, C_3 ? (C'est vrai lorsque p ne divise pas l'ordre de G.)

Un théorème de Harbater

Il ne s'agit plus ici de rigidité, mais de la propriété Gal_T pour un groupe fini donné G. Cette propriété est relative au corps **Q**. On peut se demander si elle est déjà vraie dans le cas local, c'est-à-dire lorsque l'on remplace **Q** par $\mathbf{Q}_p$ (ou par **R**, mais ce cas est facile). Il en est bien ainsi. De façon plus précise, on a :

Théorème (Harbater) - *Pour tout groupe fini* G *et tout corps local* K *de caractéristique* 0, *il existe une extension galoisienne régulière* L *de* K(T) *ayant les deux propriétés suivantes* :

(a) *Le groupe de Galois* Gal(L/K(T)) *est* G.

(b) *Il existe un point* $Q \in \mathbf{P}_1(K)$ *qui est complètement décomposé dans l'extension* L/K(T) (autrement dit, la courbe X correspondant à L possède un point rationnel sur K distinct des points de ramification).

La démonstration repose sur les théorèmes du type « GAGA formel » de Grothendieck (ou « GAGA *p*-adique rigide » de R. Kiehl et U. Köpf, cela revient au même, comme me l'a signalé M. Raynaud). On commence par vérifier que le théorème est vrai lorsque G est cyclique, ce qui peut se faire (sur tout corps de base) en utilisant des isogénies de tores. Lorsque G n'est pas cyclique on choisit des sous-groupes propres G_1 et G_2 de G engendrant G et l'on choisit dans la droite projective $\mathbf{P}_1$ deux disques fermés disjoints D_1 et D_2. Utilisant l'hypothèse de récurrence, on construit un revêtement rigide de D_i ($i = 1,2$), de groupe G, qui est trivial sur le bord de D_i et admet une « composante connexe » stable par G_i. Par recollement de ces revêtements (sur les D_i) et du revêtement trivial (sur le complémentaire de $D_1 \cup D_2$), on obtient un revêtement rigide (donc algébrique) de $\mathbf{P}_1$ ayant les propriétés voulues.

Les exemples de Mestre pour A_n *et* $\tilde{A}_n$

J.-F. Mestre a construit récemment (*J. of Algebra*, 1990) des extensions galoisiennes régulières de **Q**(T) à groupe de Galois le groupe alterné A_n jouissant de remarquables propriétés, parmi lesquelles :

(i) Les groupes d'inertie correspondant aux points de ramification sont d'ordre 3.

(ii) Il existe un « point-base » $Q \in \mathbf{P}_1(\mathbf{Q})$, i.e. un point rationnel qui est complètement décomposé dans l'extension considérée.

Supposons $n \geqslant 4$. Le groupe A_n possède alors une unique extension centrale non triviale par un groupe d'ordre 2, notée $\tilde{A}_n$ (ou $2 \cdot A_n$). Si $L/\mathbf{Q}(T)$ est une extension galoisienne à groupe de Galois A_n, on peut se demander s'il existe une extension quadratique $\tilde{L}$ de L telle que $\tilde{L}$ soit galoisienne sur **Q**(T) à groupe de Galois $\tilde{A}_n$. Ce « problème de plongement » se heurte à une

obstruction qui est un élément x du groupe $H^2(\mathbf{Q}(T),\mathbf{Z}/2\mathbf{Z}) = Br_2\,\mathbf{Q}(T)$. Dans le cas des extensions de Mestre, *cet élément est* 0 (Mestre, *loc. cit.*). En effet, le fait que les groupes d'inertie soient d'ordres impairs entraîne que x est « constant », i.e. provient de $H^2(\mathbf{Q},\mathbf{Z}/2\mathbf{Z})$; comme cette constante prend la valeur 0 au point-base, elle est nulle. (La nullité de x peut aussi se prouver en utilisant l'invariant de Witt de la forme trace associée à l'extension de degré n définie par L ; c'est de cette façon que procède Mestre.)

On déduit de là l'existence de l'extension $\tilde{L}$. En particulier, $\tilde{A}_n$ *a la propriété* Gal_T *pour tout* $n \geqslant 4$, ce qui complète des résultats antérieurs de N. Vila. Lorsque n est *impair*, on peut aller plus loin, et construire une extension $\tilde{L}$ ayant les propriétés supplémentaires suivantes :

— elle est non ramifiée sur la sous-extension L correspondante ;

— elle a un point-base.

On utilise pour cela le résultat suivant :

Théorème - *Soit n un entier impair > 4. Soient $x_1, \ldots, x_{n-1}$ des 3-cycles engendrant A_n et tels que $x_1 \ldots x_{n-1} = 1$. Pour tout i, soit $\tilde{x}_i$ l'unique élément d'ordre 3 de $\tilde{A}_n$ se projetant sur x_i. On a alors $\tilde{x}_1 \ldots \tilde{x}_{n-1} = 1$ dans $\tilde{A}_n$.*

La démonstration peut se faire, soit par voie combinatoire, soit en utilisant les propriétés des « thêta-caractéristiques » des courbes algébriques. Elle n'a pas été donnée dans le cours, mais elle a fait l'objet d'un exposé de séminaire à l'E.N.S.

SÉMINAIRE

G. MALLE - *Braid orbit theorems* (2 exposés).

PUBLICATION

J.-P. SERRE, *Rapport au Comité Fields sur les travaux de A. Grothendieck* (*K-Theory* 3 (1989), p.199-204).

MISSIONS

Cours :

— *Topics in Number Theory and Group Theory*, Singapour, février 1990.

Exposés :

— $\tilde{A}_n$*-liftings*, Oberwolfach, octobre 1989 ;

— *Relèvements dans* $\tilde{A}_n$ *et thêta-caractéristiques*, E.N.S., octobre 1989 ; Bordeaux, janvier 1990 ;

— *Spécialisation d'éléments de* Br $\mathbf{Q}(T)$ (2 exposés), Univ. Paris VII, octobre 1989 ;

— *Un chapitre de théorie des groupes*, E.N.S., novembre 1989 ;

— *The « Hauptmoduln » for* $X_0(N)$, Singapour, février 1990 ;

— $\mathbf{C}$ *is algebraically closed*, Singapour, février 1990 ;

— *Bounds for number of solutions of equations over* $\mathbf{F}_q$, Singapour, mars 1990 ;

— *Spécialisations d'éléments du groupe de Brauer*, Luminy, mars 1990 ;

— *Cohomology and Galois groups* (3 exposés), Oxford, avril 1990 ;

— *Problème inverse de la théorie de Galois : succès et échecs*, Genève, avril 1990 ;

— *Points rationnels sur les variétés algébriques* (3 exposés), E.N.S. Lyon, avril 1990 ;

— *Bornes pour les nombres de points d'hypersurfaces sur les corps finis* (2 exposés), Besançon, mai 1990 ;

— *On coverings of algebraic curves in characteristic* $p > 0$, Purdue, juin 1990 ;

— *Sur les groupes fondamentaux des courbes algébriques en caractéristique* p, Orsay, juin 1990.