Algèbre et géométrie

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

Le cours a été consacré au problème suivant : peut-on construire des extensions galoisiennes de **Q** de groupe de Galois un groupe fini donné ?

1. *La construction de Scholz-Reichardt* (1936)

Cette construction s'applique aux p-groupes, $p \neq 2$.

Soit G un tel groupe. Choisissons un entier $n \geqslant 1$ tel que tout élément de G soit d'ordre $\leqslant p^n$.

SCHOLZ et REICHARDT prouvent l'existence d'extensions galoisiennes $L/\mathbf{Q}$, avec $\mathrm{Gal}(L/\mathbf{Q}) = G$, satisfaisant à la condition suivante :

(S_n) – Pour tout nombre premier $q \in \mathrm{ram}(L/\mathbf{Q})$, on a $q \equiv 1 \pmod{p^n}$, et le groupe d'inertie en q est égal au groupe de décomposition.

La démonstration procède par récurrence sur l'ordre de G. Si C est un sous-groupe central de G d'ordre p, l'hypothèse de récurrence montre qu'il existe une extension galoisienne $K/\mathbf{Q}$, avec $\mathrm{Gal}(K/\mathbf{Q}) = G/C$, qui satisfait à (S_n). On prouve alors (en utilisant par exemple des arguments cohomologiques) qu'il existe une extension L/K, cyclique de degré p, qui est galoisienne sur **Q** de groupe de Galois G et satisfait à (S_n). On peut même construire L de telle sorte que $\mathrm{ram}(L/\mathbf{Q}) = \mathrm{ram}(K/\mathbf{Q}) \cup \{q\}$, où q est un nombre premier aussi grand que l'on veut. D'où, si $|G| = p^m$, l'existence d'extensions galoisiennes de **Q** du groupe de Galois G, qui ne sont ramifiées qu'en m nombres premiers.

Le théorème de Scholz-Reichardt a été étendu par SHAFAREVICH (1954) à tous les groupes résolubles finis. La démonstration de Shafarevich n'a pas été exposée dans le cours. Elle contient d'ailleurs une erreur relative au nombre premier $p = 2$, erreur qu'il serait souhaitable de corriger (dans les notes de ses « Collected Mathematical Papers », Shafarevich esquisse une méthode possible).

2. *Le théorème d'irréductibilité de Hilbert et la propriété* $\mathrm{Gal_T}$

La plupart des méthodes de construction d'extensions galoisiennes à groupe de Galois donné utilisent le *théorème d'irréductibilité* de HILBERT (1892).

Grosso modo, ce théorème affirme ceci : si $L/\mathbf{Q}(T)$ est une extension galoisienne finie de groupe de Galois G, il existe une infinité de t appartenant à $\mathbf{Q}$ tels que l'extension « spécialisée » $L_t/\mathbf{Q}$ soit galoisienne de groupe G. Si de plus L est une extension *régulière* de $\mathbf{Q}(T)$ (i.e. ne contient aucune extension algébrique de $\mathbf{Q}$, à part $\mathbf{Q}$), on peut exiger que les L_t soient linéairement disjointes d'une extension donnée de $\mathbf{Q}$. (Le même énoncé vaut pour les extensions galoisiennes d'un corps de fonctions rationnelles $\mathbf{Q}(T_1, \ldots, T_n)$, $n \geqslant 1$.)

On peut prouver que les « mauvaises » valeurs de t ne sont pas très nombreuses. Cela se fait par un argument de « crible », qui avait été exposé dans le cours de 1980-1981.

Disons qu'un groupe fini G *possède la propriété* $\mathrm{Gal_T}$ s'il satisfait aux conditions équivalentes suivantes :

(i) Il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois G.

(ii) Il existe un entier $n \geqslant 1$ et une extension galoisienne régulière de $\mathbf{Q}(T_1, \ldots, T_n)$ de groupe de Galois G.

(Le fait que (ii) $\Longrightarrow$ (i) est une conséquence du théorème de Bertini.)

D'après le théorème de Hilbert ci-dessus, $\mathrm{Gal_T}$ entraîne que G est groupe de Galois d'une infinité d'extensions de $\mathbf{Q}$, deux à deux disjointes ; en particulier, pour tout corps de nombres K il existe une extension galoisienne L/K telle que $\mathrm{Gal}(L/K) = G$. Il est donc intéressant de donner des exemples de groupes G ayant la propriété $\mathrm{Gal_T}$:

— G abélien ;

— $G = S_n$ ou A_n, d'après HILBERT (1892) ;

— $G = \mathbf{PSL}_2(\mathbf{F}_p)$, où p est un nombre premier tel que $\left(\frac{2}{p}\right) = -1$, ou $\left(\frac{3}{p}\right) = -1$, ou $\left(\frac{7}{p}\right) = -1$, d'après K.-y. SHIH (1974).

D'autres exemples seront traités dans le cours de 1989-1990, par la méthode de « rigidité ».

3. *La méthode d'E. Noether* (1918)

On réalise le groupe donné G comme sous-groupe du groupe de permutations S_n, ce qui permet de le faire opérer sur le corps $L = \mathbf{Q}(X_1, \ldots, X_n)$. Si

$K = L^G$ désigne le corps des invariants de L on obtient ainsi une extension galoisienne régulière L/K de groupe de Galois G. Supposons que la condition suivante soit satisfaite :

(N) – Le corps K est une extension stablement rationnelle de $\mathbf{Q}$, i.e. $K(T_1, \ldots, T_m)$ est isomorphe à $\mathbf{Q}(T_1, \ldots, T_{n+m})$ pour m assez grand.

(On peut prouver que cette condition ne dépend pas du plongement choisi de G dans un groupe symétrique.)

On a alors Gal_T, ce qui montre que G est groupe de Galois d'une extension de $\mathbf{Q}$. C'est la méthode proposée par E. NOETHER.

Cette méthode est rarement applicable. La condition (N) est trop forte. Elle n'est pas satisfaite lorsque G est cyclique d'ordre 47 (SWAN, VOSKRESENSKII, 1969) ou d'ordre 8 (LENSTRA, 1974). En fait, même l'analogue de (N) sur $\mathbf{C}$ peut être en défaut : le corps $K_{\mathbf{C}}$ des invariants de G dans $\mathbf{C}(X_1, \ldots, X_n)$ n'est pas toujours stablement rationnel sur $\mathbf{C}$. De façon plus précise, SALTMAN (1984) a montré que, s'il existe un élément non nul de $H^2(G, \mathbf{Q}/\mathbf{Z})$ qui induit 0 sur tous les sous-groupes abéliens à deux générateurs de G, alors $K_{\mathbf{C}}$ n'est pas stablement rationnel sur $\mathbf{C}$ (on construit des exemples de tels groupes G en prenant des extensions centrales convenables de groupes abéliens élémentaires). La démonstration repose sur l'étude du « groupe de Brauer non ramifié » du corps $K_{\mathbf{C}}$. (Les résultats de Swan, Voskresenskii, Lenstra et Saltman ont été exposés dans le Séminaire par J.-L. COLLIOT-THÉLÈNE.)

4. *Une variante de la méthode d'E. Noether*

Cette variante, due à EKEDAHL et COLLIOT-THÉLÈNE (1987), vise à remplacer la condition (N) par une condition plus faible, susceptible d'être vérifiée pour tout groupe fini G.

Soit K une extension régulière de type fini de $\mathbf{Q}$, et soit V une $\mathbf{Q}$-variété intègre lisse de corps des fonctions K. Disons que K satisfait à la condition d'*approximation faible affaiblie* si :

(AFA) – Il existe un ensemble fini T de nombres premiers tel que, pour tout ensemble fini S de nombres premiers disjoint de T, l'image de $V(\mathbf{Q})$ dans le produit des $V(\mathbf{Q}_p)$, $p \in S$, est dense. (Cette propriété ne dépend pas du choix de V.)

La condition (AFA) est plus faible que « K est stablement rationnel ». Elle est cependant suffisante (Ekedahl et Colliot-Thélène) pour entraîner un théorème d'irréductibilité à la Hilbert :

Si L/K est une extension galoisienne de groupe de Galois G, et si K satisfait à (AFA), on peut en déduire par spécialisation des extensions galoisiennes de $\mathbf{Q}$ à groupe de Galois G. Si de plus L est $\mathbf{Q}$-régulière, on peut obtenir des extensions linéairement disjointes de toute extension finie de **Q** donnée.

Ainsi, la méthode d'E. Noether pourrait s'appliquer à tout groupe fini G, pourvu que l'on puisse montrer que les corps $K = L^G$ correspondants satisfont à (AFA), ce qui est vrai dans tous les cas connus. On peut même espérer (Colliot-Thélène) que (AFA) est vraie pour tout corps K qui est « unirationnel », i.e. sous-corps d'un corps $\mathbf{Q}(X_1, \ldots, X_n)$.

Séminaire

Jean-Louis Colliot-Thélène, *Exemples de variétés non rationnelles* (2 exposés).

Publications

J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves* (McGill University Lecture Notes, written with the collaboration of Willem Kuyk and John Labute), 2e édition révisée, Addison-Wesley, 1989.

— *Lectures on the Mordell-Weil Theorem* (translated and edited by Martin Brown from notes by Michel Waldschmidt), Vieweg, 1989.

Missions

Cours

— *Topics in Galois Theory*, Harvard, septembre-décembre 1988.

Exposés

— *Abelian varieties and their division points* (3 exposés), Schloss Ringberg, juillet 1988.

— *Galois groups and modular forms*, Stockholm, septembre 1988 ;

— *Homotopy groups : why and why not ?*, Harvard, octobre 1988 ;

— *Root systems*, Harvard, novembre 1988 ;

— *Galois groups over* **Q**, McGill University, novembre 1988 ; M.I.T., novembre 1988 ; State College, décembre 1988 ;

— *Modular forms* mod *p, and quaternions*, Columbia, novembre 1988 ;

— *La forme* $\mathrm{Tr}(x^2)$: *suite*, Bordeaux, mars 1989 ; Zurich, mai 1989 ;

— *Some examples of modular Galois representations* mod *p*, Texel, avril 1989 ;

— *Problèmes énumératifs sur les coniques, d'après CHASLES*, E.N.S., mai 1989 ;

— *Sommes de trois carrés dans* $\mathbf{F}_q[\mathrm{T}]$, Zurich, mai 1989 ;

— *La moyenne arithmético-géométrique*, Académie des Sciences, juin 1989 ;

— *Réductions supersingulières d'une courbe elliptique, d'après N. ELKIES*, Séminaire de Théorie des Nombres, Paris, juin 1989 ;

— *Automorphic forms* mod *p on quaternion groups*, Durham, juillet 1989 ;

— *Points rationnels et cribles*, Luminy, juillet 1989 ;

— *Motifs*, Luminy, juillet 1989.