Séminaire BOURBAKI Juin 2003
55e année, 2002-2003, nº 923, p. 403 à 431

GROUPES DE GALOIS DE CORPS DE TYPE FINI
[d'après Pop]

par **Tamás SZAMUELY**

Le but de cet exposé est de montrer que le groupe de Galois absolu d'un corps de fonctions est un invariant très fin : d'une part, il détermine le corps de fonctions à isomorphisme près ; d'autre part, il est possible d'en extraire des informations très riches et variées sur l'arithmétique et la géométrie du corps en question.

1. ÉNONCÉS

Les deux résultats principaux qui nous intéressent ici sont les suivants. Ici, et dans la suite, pour un corps F on fixe toujours une clôture séparable F^s, et on note G_F le groupe de Galois absolu $\mathrm{Gal}(F^s|F)$.

THÉORÈME 1.1 (Florian Pop, [30], [32]). — *Soient K, L deux corps infinis, de type fini sur le corps premier. Supposons qu'il existe un isomorphisme $\Phi : G_K \xrightarrow{\sim} G_L$ de groupes profinis. Alors il existe des extensions purement inséparables $K'|K, L'|L$ avec $K' \cong L'$. De plus, il existe un isomorphisme $\phi : L'^s \xrightarrow{\sim} K'^s$ de clôtures séparables tel que pour tout élément $g \in G_{K'}$ on ait $\Phi(g) = \phi^{-1} \circ g \circ \phi$.*

Remarques 1.2

(1) En particulier, tout corps de type fini sur $\mathbf{Q}$ est déterminé à isomorphisme près par son groupe de Galois absolu. Un tel énoncé ne vaut pas en caractéristique positive, car si $K'|K$ est une extension purement inséparable de corps, alors l'homomorphisme de restriction $G_K \to G_{K'}$ est un isomorphisme. La formulation ci-dessus tient compte de ce contre-exemple évident.

(2) Pop démontre en fait un énoncé plus précis : pour L, K comme ci-dessus, considérons la règle qui associe à tout isomorphisme $\phi : L^i \xrightarrow{\sim} K^i$ entre leurs clôtures parfaites l'isomorphisme $\Phi : G_K \xrightarrow{\sim} G_L$ donné par la formule $\Phi(g) = \phi^{-1} \circ g \circ \phi$. En caractéristique 0, c'est une bijection entre l'ensemble des isomorphismes de corps $L \xrightarrow{\sim} K$ et le *quotient* de l'ensemble des isomorphismes de groupes

profinis $G_K \xrightarrow{\sim} G_L$ par l'action intérieure naturelle de G_L. En caractéristique positive on a une bijection analogue, mais il faut y identifier les isomorphismes $L^i \xrightarrow{\sim} K^i$ qui sont les mêmes « quitte à tordre par un automorphisme de Frobenius ».

Dans un travail en préparation, Pop obtient l'amplification remarquable que voici. Pour un groupe profini G et un nombre premier ℓ, notons G^ℓ le pro-ℓ-quotient maximal de G.

Théorème 1.3 (Florian Pop, [33], [34]). — *Soient ℓ un nombre premier, K et L deux corps de type fini sur la* clôture algébrique *du corps premier dont le degré de transcendance est au moins 2 et dont la caractéristique est différente de ℓ. Supposons qu'il existe un isomorphisme $\Phi : G_K^\ell \xrightarrow{\sim} G_L^\ell$ de groupes profinis. Alors il existe des extensions purement inséparables $K'|K, L'|L$ avec $K' \cong L'$. De plus, il existe un isomorphisme $\phi : L'^s \xrightarrow{\sim} K'^s$ de clôtures séparables tel que pour tout élément $g \in G_K^\ell$ on ait $\Phi(g) = \phi^{-1} \circ g \circ \phi$.*

Remarques 1.4

(1) Bien entendu, on a encore un énoncé plus précis comme dans la remarque ci-dessus.

(2) L'énoncé est *faux* pour les corps de degré de transcendance un. En effet, si K est le corps de fonctions de n'importe quelle courbe propre lisse X de genre $g > 0$ sur un corps algébriquement clos, et ℓ est premier à la caractéristique de K, alors G_K^ℓ est la limite projective des groupes fondamentaux ℓ-complétés $\pi_1(U, u)^\ell$ pour les sous-schémas ouverts $U \subset X$. Or la présentation d'un tel $\pi_1(U, u)^\ell$ est bien connue d'après les travaux de Riemann, Poincaré et Grothendieck (voir [15]) : elle est de la forme $\langle a_1, b_1, \ldots, a_g, b_g, i_1, \ldots, i_r | [a_1, b_1] \ldots [a_g, b_g] i_1 \ldots i_r = 1\rangle$, où r est le nombre des points de $X \smallsetminus U$. Ainsi, G_K^ℓ ne dépend que de g et du cardinal du corps de base.

(3) Le th. 1.1 ne semble pas découler de manière évidente du th. 1.3. Toutefois, après avoir fait une bonne partie de la démonstration du th. 1.1, on peut conclure par une application de 1.3 (voir la remarque 8.6).

2. HISTORIQUE

Bien que la caractérisation galoisienne des corps réels clos par Artin et Schreier [2] puisse être regardée comme un précurseur des résultats ci-dessus, l'histoire commence réellement avec des travaux de Neukirch à la fin des années 1960. Celui-ci a été amené par son étude de la structure du groupe de Galois absolu d'un corps p-adique (un sujet de recherche florissant à l'époque) à une caractérisation cohomologique des sous-groupes de décomposition associés aux idéaux premiers dans une extension galoisienne de corps de nombres. De là il a pu déduire, par une application du théorème de densité de Chebotarev, le th. 1.1 dans le cas où L et K sont des extensions *finies galoisiennes* de **Q** (voir [26]). En plus, il a remarqué que l'on pourrait étendre son résultat au cas de corps de nombres arbitraires via la solution d'un « problème de plongement » en théorie de Galois inverse. Ce travail a été mené à bien par Iwasawa (non publié) et Uchida [40] (voir aussi [27], [28]). Ce dernier a également étendu dans [41] la méthode de Neukirch au cas des corps de fonctions à une variable sur un corps fini.

L'histoire semblait donc arriver à une conclusion satisfaisante, mais l'intérêt pour ce genre de questions a été réalimenté vers le milieu des années 1980 par la « vision anabélienne » de Grothendieck, exposée dans sa célèbre lettre à Faltings [17]. Ce programme, qui vise la reconstitution de certains schémas définis sur des corps de type fini (dits *schémas anabéliens*) ainsi que leurs morphismes dominants à partir de leur groupe fondamental géométrique muni de l'action extérieure du groupe de Galois du corps de base, a donné lieu à de spectaculaires développements ces dernières années dont la plupart ont été rapportés dans ce séminaire par Faltings [13] (voir aussi les survols [24], [28], [31], [39] et [18]). Grothendieck énonce dans sa lettre le th. 1.1 comme une variante birationnelle de ses conjectures sur les groupes fondamentaux, avec toutefois une différence notable : il considère les groupes de Galois des corps de fonctions munis d'augmentations naturelles vers le groupe de Galois absolu d'un corps de base k (qui peut être le corps premier, supposé le même pour K et L, ou plus généralement un corps de type fini sur le corps premier contenu dans chacun de ces deux corps) et par suite les k-isomorphismes entre K et L. En revanche, il prédit que les k-homomorphismes $K \to L$ devraient également être reconstituables à partir des G_k-morphismes induits sur les groupes de Galois. Or le th. 1.1 et surtout le th. 1.3 montrent que, du moins en ce qui concerne la reconstruction des isomorphismes, l'action du groupe de Galois d'un corps de base n'est pas essentielle. Les travaux récents de Tamagawa, Raynaud et autres sur les groupes fondamentaux des courbes sur un corps algébriquement clos de caractéristique positive témoignent d'ailleurs du même phénomène.

Concernant la conjecture birationnelle de Grothendieck, le premier pas est franchi par Pop [29], où le th. 1.1 est démontré dans le cas des corps de fonctions à une variable sur un corps de nombres, en combinant la stratégie de Neukirch avec des considérations en théorie des valuations utilisant des techniques de logique. Spiess [38] a ensuite trouvé une démonstration purement arithmético-géométrique encore plus proche de l'esprit original de Neukirch. En combinant ces idées avec des arguments de géométrie birationnelle, Pop a ensuite réussi à démontrer le th. 1.1.

Entretemps, dans ses articles [4], [5], Bogomolov a esquissé un programme pour démontrer un résultat similaire au th. 1.3, mais pour des corps de type fini au-dessus d'un corps algébriquement clos quelconque. D'après son point de vue, le corps de fonctions K devrait être déterminé par le deuxième quotient $G_K^\ell/[[G_K^\ell, G_K^\ell], G_K^\ell]$ de la suite centrale descendante de G_K^ℓ. Dans leurs articles récents [6], [7], Bogomolov et Tschinkel fournissent des détails de cette démonstration dans le cas des corps de fonctions de certaines surfaces au-dessus de $\overline{\mathbf{F}}_p$. Certaines idées de Bogomolov ont inspiré Pop dans sa démonstration du théorème 1.3. Pour un complément intéressant, voir [35].

Cet aperçu ne serait pas complet si on ne mentionnait pas un résultat très important de Mochizuki [23] : il y est démontré que si K et L sont deux corps de type fini sur un corps k qui peut lui-même être plongé dans une extension de type fini de $\mathbf{Q}_p$ (Mochizuki appelle un tel corps *sous-p-adique*), alors tout G_k-morphisme $G_K \to G_L$ de groupes profinis à image ouverte est induit par un k-morphisme $L \to K$ de corps. Mochizuki dérive ce théorème de son résultat anabélien fondamental d'après lequel tout G_k-morphisme $\pi_1(X) \to \pi_1(Y)$ à image ouverte entre les groupes fondamentaux de deux k-courbes hyperboliques X et Y est induit par un k-morphisme dominant $X \to Y$ (voir l'exposé [13] de Faltings). La stratégie est alors la suivante (pour les détails, *cf.* [23], §§15, 16) : on montre d'abord que si K est le corps de fonctions de X, alors tout G_k-morphisme $G_K \to \pi_1(Y)$ se factorise à travers $\pi_1(X)$, d'où on conclut aisément en utilisant le résultat précédent qu'il est induit par un morphisme $\operatorname{Spec} K \to Y$. Un argument (non trivial) de fibration en courbes permet alors d'en déduire un résultat similaire pour K corps de type fini quelconque sur k. Ensuite, étant donné un G_k-morphisme $G_K \to G_L$, où L est le corps de fonctions de Y, on peut le composer par le G_k-morphisme naturel $G_L \to \pi_1(Y)$ et ainsi récupérer par ce qui précède le morphisme dominant $\operatorname{Spec} K \to Y$; il se factorise à travers $\operatorname{Spec} L$. Enfin, le résultat pour L général s'en suit à nouveau par un argument de fibration (facile cette fois).

Noter que dans cette preuve l'action de G_k joue un rôle essentiel ; la variante « absolue » du théorème, ainsi que son analogue en caractéristique positive, ne sont pas connues à ce jour.

3. STRATÉGIE

Nous donnons maintenant un survol parallèle des démonstrations des théorèmes 1.1 et 1.3, laissant les détails aux chapitres suivants. Nous ignorons ici les complications causées par les extensions inséparables en caractéristique positive.

On va appeler la situation du th. 1.1 le *cas arithmétique* et celle du th. 1.3 le *cas géométrique.* Le corps de base k est le corps premier de K dans le premier cas et sa clôture algébrique dans le second ; de même pour l et L.

Première étape : Correspondance locale. — Soit X un k-schéma normal intègre de type fini ayant K pour corps de fonctions, et soit P un point de codimension 1 de X. Notons D_P un sous-groupe de décomposition de G_K (resp. G_K^ℓ) associé à P, i.e. le stabilisateur d'un point $\overline{P}$ au-dessus de P du normalisé de X dans la clôture algébrique $\overline{K}$ de K. Alors on montre que $D_Q := \Phi(D_P)$ est un groupe de décomposition associé à un point Q de codimension 1 d'un k-schéma normal intègre de type fini Y ayant L pour corps de fonctions. En plus, on obtient ainsi une bijection entre les sous-groupes de décomposition de G_K et de G_L (resp. leurs pro-ℓ-quotients maximaux) du type décrit ci-dessus.

On démontre ensuite que Φ transforme le sous-groupe d'inertie de D_P en celui de D_Q, d'où un isomorphisme $\Phi_P : G_{k(P)} \to G_{k(Q)}$ entre les groupes de Galois des corps résiduels de P et de Q (resp. leurs pro-ℓ-quotients maximaux).

Les résultats locaux esquissés ci-dessus permettent déjà de reconstituer beaucoup d'invariants arithmétiques et géométriques des corps K et L.

En particulier, dans le cas arithmétique, l'utilisation des résultats précédents permet d'établir que les corps de base $k \subset K$ et $l \subset L$ sont isomorphes, et que Φ transforme la projection canonique $G_K \to G_k$ en la projection $G_L \to G_l$; par le théorème de Neukirch/Uchida, on a donc $k \cong l$. Dans le cas géométrique ces deux projections sont bien entendu triviales.

Une fois la projection $G_K \to G_k$ (ou même la projection $G_K^\ell \to G_k^\ell$) connue, il est possible de déduire le cas arithmétique du cas géométrique (*cf.* la remarque 8.6). On va opter pour ce procédé en caractéristique positive ; en revanche, en caractéristique 0, l'approche directe au th. 1.1 est plus simple.

Deuxième étape : Correspondance kummérienne. — Soit maintenant n un entier positif que l'on suppose toujours premier à la caractéristique de K et de L ; dans le cas géométrique, on suppose de plus que c'est une puissance de ℓ.

Dans le cas arithmétique, le groupe G_K agit sur le groupe μ_n des racines n-ièmes de l'unité à travers son quotient G_k qui est préservé par Φ par ce qui précède ; dans le cas géométrique cette action est triviale. Donc, par application de la théorie de Kummer, on obtient une suite d'isomorphismes

$$K^\times/K^{\times n} \cong H^1(G_K, \mu_n) \cong H^1(G_L, \mu_n) \cong L^\times/L^{\times n}$$

où $K^\times$ (resp. $L^\times$) est le groupe multiplicatif de K (resp. L), les deux groupes au milieu sont des groupes de cohomologie galoisienne et leur isomorphisme est induit par Φ. Notons ici que Φ est également applicable dans le cas géométrique : comme l'action de G_K sur μ_n est triviale, les éléments de $H^1(G_K, \mu_n)$ sont alors des homomorphismes $G_K \to \mu_n$; ils se factorisent à travers G_K^ℓ car on a supposé que n est une puissance de ℓ.

Par passage à la limite projective sur les puissances de ℓ, on obtient également un isomorphisme

$$\Phi^{(\ell)} : K^{\times(\ell)} \cong L^{\times(\ell)}$$

entre les *complétés ℓ-adiques* des groupes multiplicatifs des deux corps.

Le noyau du morphisme $K^\times \to K^{(\ell)}$ est le sous-groupe ℓ-divisible maximal de $K^\times$. Dans le cas arithmétique on peut montrer que ce sous-groupe est trivial ; en revanche, dans le cas géométrique, ce sous-groupe est égal à $k^\times$.