Astérisque

JEAN-PIERRE SERRE

Groupes de Galois sur Q

Astérisque, tome 161-162 (1988), Séminaire Bourbaki,
exp. n° 689, p. 73-85

<http://www.numdam.org/item?id=SB_1987-1988__30__73_0>

Séminaire BOURBAKI
40ème année, 1987-88, n° 689

Novembre 1987

GROUPES DE GALOIS SUR $\mathbf{Q}$

par Jean-Pierre SERRE

Soit G un groupe fini. Existe-t-il une extension galoisienne finie E de $\mathbf{Q}$ dont le groupe de Galois $\mathrm{Gal}(E/\mathbf{Q})$ soit isomorphe à G ?

Ce problème classique n'est toujours pas résolu. Toutefois, comme on va le voir, il y a de nombreux groupes G pour lesquels la réponse est "oui".

Remarque.- On peut se poser la même question en remplaçant $\mathbf{Q}$ par une extension finie K quelconque. En fait, cette généralisation n'est guère utile : si le problème initial a une réponse positive pour toutes les puissances $G \times \ldots \times G$ de G, on dispose d'une famille infinie d'extensions galoisiennes disjointes $E_i/\mathbf{Q}$ de groupe de Galois G ; pour presque tout i, E_i est linéairement disjointe de K, de sorte que $\mathrm{Gal}(E_iK/K) \simeq G$: le problème sur K a une réponse positive.

1. LE CAS RÉSOLUBLE

Lorsque G est *abélien*, il n'y a pas de difficulté. On choisit un entier $N \geq 1$ tel que G soit isomorphe à un quotient du groupe multiplicatif $(\mathbf{Z}/N\mathbf{Z})^*$, ce qui est possible (d'une infinité de façons) en vertu du théorème de la progression arithmétique. Ceci fait, on prend pour E un sous-corps convenable de $\mathbf{Q}(z_N)$, où z_N est une racine primitive N-ème de l'unité. (Exemple : si G est d'ordre 3, on peut prendre $N = 7,9,13,\ldots$.)

On pourrait croire qu'à partir du cas abélien il est facile de traiter, par extensions successives, le cas d'un groupe résoluble quelconque. En fait, ce n'est pas facile du tout, pour la raison suivante : si G a un quotient G/H tel qu'il existe une extension galoisienne $E^H/\mathbf{Q}$ de groupe de Galois G/H, il n'est pas vrai en général que E^H puisse se plonger dans une extension galoisienne $E/\mathbf{Q}$ de groupe de Galois G ; ce "problème de plongement" a une obstruction de nature cohomologique (cf. § 7). On ne peut donc procéder par extensions successives que si l'on arrive à "tuer" ces obstructions, ce qui est difficile.

C'est pourtant ce qu'a réussi à faire Šafarevič, qui a démontré (cf. [26]) :

THÉORÈME 1.- *Tout groupe fini résoluble est groupe de Galois sur* $\mathbf{Q}$.

Il serait intéressant de reprendre la démonstration de Šafarevič, et de voir si l'on peut en tirer davantage de renseignements (existence d'extensions à comportement local imposé, par exemple). Pour les groupes d'ordre impair, cela a été fait par Neukirch [25].

Pour les groupes non résolubles (par exemple les groupes simples non abéliens), il faut procéder autrement. Jusqu'à présent, la méthode la plus efficace a consisté à exploiter les relations entre extensions de $\mathbf{Q}(T)$ et de $\mathbf{Q}$. Rappelons en quoi cela consiste :

2. EXTENSIONS DE $\mathbf{Q}(T)$ ET EXTENSIONS DE $\mathbf{Q}$

Soit E_T une extension galoisienne finie du corps $\mathbf{Q}(T)$ des fonctions rationnelles sur $\mathbf{Q}$, et soit G son groupe de Galois. Si l'on donne à T une valeur $t \in \mathbf{Q}$ n'appartenant pas à un certain ensemble fini $S = S(E_T)$, on peut "spécialiser" E_T (cf. ci-dessous), et l'on obtient une $\mathbf{Q}$-algèbre étale E_t (i.e. un produit de corps), de rang $r = [E_T:\mathbf{Q}(T)] = |G|$, sur laquelle opère G . Lorsque E_t est un *corps*, c'est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois G .

Exemple.- Si $r = 2$ et si $E_T = \mathbf{Q}(T,X)$ avec $X^2 = T$, on peut prendre $S = \{0\}$. Si $t \in \mathbf{Q}$ n'appartient pas à S , l'algèbre E_t est $\mathbf{Q}[X]/(X^2 - t)$; elle est isomorphe à $\mathbf{Q} \times \mathbf{Q}$ si t est un carré dans $\mathbf{Q}$; sinon, c'est le corps quadratique $\mathbf{Q}(\sqrt{t})$.

Notons $\mathrm{Irr}(E_T)$ l'ensemble des $t \in \mathbf{Q} - S$ tels que E_t soit un corps.

THÉORÈME 2 (Hilbert).- a) *L'ensemble* $\mathrm{Irr}(E_T)$ *est infini.*

b) *Supposons que* E_T *soit une extension régulière de* $\mathbf{Q}(T)$, i.e. (Bourbaki, A.V. 136) *que* $\mathbf{Q}$ *soit algébriquement fermé dans* E_T . *Il existe alors une suite infinie* $t_1,\ldots,t_n,\ldots$ *d'éléments de* $\mathrm{Irr}(E_T)$ *tels que les corps* E_{t_i} *correspondants soient linéairement disjoints sur* $\mathbf{Q}$.

Cela résulte du théorème d'irréductibilité de Hilbert, cf. [8], [12], [14]. La démonstration montre en outre que "la plupart" des $t \in \mathbf{Q} - S$ appartiennent à $\mathrm{Irr}(E_T)$. Par exemple, si l'on se restreint à $t \in \mathbf{Z}$, le nombre des t avec $|t| \leq N$ qui n'appartiennent pas à $\mathrm{Irr}(E_T)$ est $O(N^{1/2})$ pour $N \longrightarrow \infty$.

Interprétation géométrique des E_t . Le corps $\mathbf{Q}(T)$ est le corps des fonctions rationnelles de la *droite projective* P_1 sur $\mathbf{Q}$. De même, E_T est le corps des fonctions d'une courbe projective lisse irréductible E sur $\mathbf{Q}$, qui est absolument irréductible si et seulement si E_T est une extension régulière de $\mathbf{Q}(T)$. Le groupe G opère fidèlement sur E , et le quotient E/G s'identifie à P_1 .

On peut donc voir E comme un revêtement $\pi : E \longrightarrow P_1$, de groupe de Galois G . Si $\Sigma \subset P_1$ est l'ensemble des points de ramification de π (ensemble qui est non vide si $r > 1$), on peut prendre pour S l'ensemble des $t \in Q$ qui appartiennent à Σ . Si $t \notin S$, la fibre $\pi^{-1}(t)$ de t est un Q-schéma étale fini dont l'algèbre est E_t . Dire que t appartient à $\mathrm{Irr}(E_T)$ signifie que cette fibre est réduite à un seul point (du point de vue des schémas), ou encore que les différents points géométriques de $\pi^{-1}(t)$ sont conjugués entre eux (autre formulation : il n'existe aucun sous-groupe propre H de G tel que t soit l'image d'un point rationnel de E/H).

Application aux groupes de Galois sur Q . Si G est un groupe fini, notons $\mathrm{Gal}_T(G)$ et $\mathrm{Gal}_\infty(G)$ les deux propriétés suivantes de G :

$\mathrm{Gal}_T(G)$ - *Il existe une extension galoisienne régulière de* $Q(T)$ *de groupe de Galois* G .

$\mathrm{Gal}_\infty(G)$ - *Il existe une infinité d'extensions galoisiennes de* Q *de groupe de Galois* G *qui sont deux à deux disjointes.*

Le th. 2 b) entraîne :

THÉORÈME 3.- $\mathrm{Gal}_T(G) \Longrightarrow \mathrm{Gal}_\infty(G)$.

(Plus généralement, $\mathrm{Gal}_T(G)$ entraîne que G est groupe de Galois sur tout *corps hilbertien* ([14], chap. 9) de caractéristique 0 .)

On peut se demander si $\mathrm{Gal}_T(G)$ est vraie pour tout groupe fini G : on ne connaît aucun contre-exemple. Signalons à ce sujet :

a) $\mathrm{Gal}_T(G_1)$ et $\mathrm{Gal}_T(G_2)$ entraînent $\mathrm{Gal}_T(G_1 \times G_2)$: c'est facile.

b) $\mathrm{Gal}_T(G)$ est vraie si G est abélien, cf. [27]. (*Exemple* : si G est d'ordre 3 , on peut prendre pour E_T l'extension définie par l'équation $X^3 - TX^2 + (T-3)X + 1 = 0$, de discriminant $\Delta = (T^2 - 3T + 9)^2$; c'est même là une extension *universelle* au sens de [27].)

c) On ignore si $\mathrm{Gal}_T(G)$ est vraie pour tout groupe résoluble G ; c'est le cas pour certains groupes de Frobenius, cf. [4].

d) $\mathrm{Gal}_T(G)$ est vraie pour $G = S_n$ ou A_n (Hilbert [12]).

e) $\mathrm{Gal}_T(G)$ est vraie pour la plupart des vingt-six groupes simples sporadiques, cf. § 5. C'est une conséquence de la théorie de la "rigidité" résumée au § 4 ci-après.

3. RAPPELS SUR LES EXTENSIONS FINIES DE $C(T)$

Avant de chercher à construire des extensions finies de $Q(T)$, il est bon de s'occuper de celles de $C(T)$.

Ces dernières, on le sait, se décrivent de façon purement topologique :

Fixons un sous-ensemble fini $\Sigma = \{t_1,\ldots,t_k\}$ de la droite projective complexe $\mathbf{P}_1(\mathbf{C}) \simeq \mathbf{S}_2$. Les objets suivants se correspondent bijectivement (modulo isomorphismes) :

i) extensions finies de $\mathbf{C}(T)$ non ramifiées en dehors de Σ ;

ii) revêtements finis connexes non vides de $\mathbf{P}_1(\mathbf{C}) - \Sigma$.

[Si $E/\mathbf{C}(T)$ est non ramifiée en dehors de Σ , on lui associe le revêtement fourni par la courbe correspondante $E_{\mathbf{C}} \longrightarrow \mathbf{P}_1$, dont on retire les points au-dessus de Σ . D'où un foncteur i) $\longrightarrow$ ii). Le "théorème d'existence de Riemann" dit que c'est une équivalence, cf. par exemple [11], exposé XII.]

Quant aux objets de type ii), ils se classifient au moyen du groupe fondamental $\pi_1 = \pi_1(\mathbf{P}_1(\mathbf{C}) - \Sigma; t_o)$, où t_o est un point de base choisi en dehors de Σ . Plus précisément, ils correspondent aux objets suivants :

iii) ensembles finis non vides munis d'une action transitive de π_1 .

[La correspondance se fait en associant à un revêtement sa fibre au-dessus de t_o , munie de l'action naturelle de π_1 dessus, cf. [11], exposé V .]

Il reste à décrire π_1 . Pour cela, choisissons un chemin c_i joignant t_o à t_i $(1 \leq i \leq k)$ et ne passant par aucun des t_j , $j \neq 0,i$. En suivant c_i , puis tournant autour de t_i dans le sens positif, et suivant c_i en sens inverse, on obtient un élément $s_i \in \pi_1$, qui dépend de c_i (mais sa classe de conjugaison n'en dépend pas). *Si les c_i sont bien choisis, le groupe π_1 est défini par la présentation :*

$$\pi_1 = \{s_1,\ldots,s_k \ ; \ s_1 \ldots s_k = 1\} \ .$$

En particulier π_1 est un groupe libre de base $\{s_1,\ldots,s_{k-1}\}$.

(Attention : si les c_i ne sont pas bien choisis, il se peut que les s_i n'engendrent pas π_1 !)

Ces diverses équivalences montrent qu'un groupe fini G est groupe de Galois d'une extension de $\mathbf{C}(T)$ non ramifiée en dehors de $\Sigma = \{t_1,\ldots,t_k\}$ si et seulement si il peut être engendré par k éléments $g_1,\ldots,g_k$ satisfaisant à la relation $g_1 \ldots g_k = 1$ (i.e. s'il peut être engendré par $k-1$ éléments). Ce n'est pas là une condition bien restrictive : il suffit de prendre k assez grand. Le problème sérieux est de descendre de $\mathbf{C}(T)$ à $\mathbf{Q}(T)$. On ne sait pas grand-chose là-dessus en général, mais on va voir qu'il y a au moins un cas, le cas "rigide", où cette descente se fait sans difficulté.

4. RIGIDITÉ

Soit G un groupe fini *de centre trivial*, et soient $C_1,\ldots,C_k$ $(k \geq 3)$ des classes de conjugaison de G . Notons $P = P(C_1,\ldots,C_k)$ l'ensemble des

$(g_1,\dots,g_k) \in C_1 \times \dots \times C_k$ tels que

$$g_1 \dots g_k = 1 ,$$

et notons P' le sous-ensemble de P formé des $(g_1,\dots,g_k) \in P$ qui *engendrent* G. Le groupe G opère par conjugaison sur P et sur P'.

DÉFINITION.- *La famille* $(C_1,\dots,C_k)$ *est dite* rigide *si* G *opère transitivement sur* P' *et si* P' *est non vide. Elle est dite* strictement rigide *si l'on a en outre* $P = P'$.

Noter que G opère librement sur P'. Il y a donc rigidité si et seulement si $|P'| = |G|$, et cela entraîne $|P| \geq |G|$ (avec égalité s'il y a stricte rigidité). L'entier $|P|$ peut d'ailleurs se calculer à partir de la table des caractères de G : si l'on choisit $c_i \in C_i$, et si l'on pose $z_i = |Z_G(c_i)| = |G|/|C_i|$, on a

$$(1) \qquad |P| = \frac{|G|^{k-1}}{z_1 \dots z_k} \sum_{\chi} \chi(c_1) \dots \chi(c_k) / \chi(1)^{k-2} ,$$

où χ parcourt l'ensemble des caractères irréductibles de G.

(*Exercice* : si $c_0,\dots,c_k$ sont des éléments d'un groupe fini G quelconque, montrer que le nombre des $x_1,\dots,x_k \in G$ tels que

$$x_1 c_1 x_1^{-1} \cdot x_2 c_2 x_2^{-1} \dots x_k c_k x_k^{-1} = c_0$$

est égal à $|G|^{k-1} \sum_{\chi} \chi(c_1) \dots \chi(c_k) \bar{\chi}(c_0) / \chi(1)^{k-1}$.
En déduire (1) en prenant $c_0 = 1$.)

Rappelons d'autre part qu'une classe de conjugaison C de G est dite *rationnelle sur* $\mathbf{Q}$ (ou simplement *rationnelle*) si elle satisfait aux conditions équivalentes suivantes :

(2) *Tout caractère de* G *prend sur* C *des valeurs rationnelles.*

(3) *Si* $c \in C$ *et si* $i \in \mathbf{Z}$ *est premier à l'ordre de* c, *alors* c^i *appartient à* C (i.e. si un générateur d'un sous-groupe cyclique de G appartient à C, il en est de même des autres générateurs).

(*Exemple* : toutes les classes de conjugaison d'un groupe symétrique - ou plus généralement d'un groupe de Weyl - sont rationnelles.)

Nous pouvons maintenant énoncer le théorème principal de cet exposé ; à quelques variations près, il est dû à Belyi, Fried, Matzat et Thompson (*cf.* [2], [9], [10], [18], [22], [23], [30]).

THÉORÈME 4.- *Soient* G *un groupe fini de centre trivial et* $C_1,\dots,C_k$ *des classes de conjugaison de* G. *Faisons les hypothèses suivantes :*

a) *les* C_i *sont rationnelles ;*

b) *la famille* $(C_1,\dots,C_k)$ *est rigide.*

Soient d'autre part $t_1,\dots,t_k$ *des points de* $P_1(\mathbf{Q})$ *, deux à deux distincts.*

Il existe alors une (et une seule) *extension galoisienne finie régulière* $E_T/\mathbf{Q}(T)$ *, de groupe de Galois* G *, ramifiée seulement en les* t_i *, et telle que les générateurs des groupes d'inertie correspondants appartiennent aux* C_i *.*

(Noter que l'on ne précise pas quels sont les générateurs des groupes d'inertie que l'on prend : cela n'a pas d'importance, puisque les classes C_i sont rationnelles.)

Compte tenu du th. 3, ceci entraîne :

COROLLAIRE.- *Si* G *possède une famille rigide de classes rationnelles, alors* $\mathrm{Gal}_T(G)$ *est vraie, et a fortiori* $\mathrm{Gal}_\infty(G)$ *. En particulier,* G *est groupe de Galois d'une extension de* $\mathbf{Q}$ *.*

Démonstration du th. 4.- On se place d'abord sur $\mathbf{C}$. On montre :

i) qu'il existe une extension galoisienne E de $\mathbf{C}(T)$, de groupe de Galois G, ayant les propriétés imposées (i.e. non ramifiée en dehors des t_i , et avec les générateurs des groupes d'inertie dans les C_i) ;

ii) qu'une telle extension est unique, à isomorphisme unique près (i.e. si E et E' sont deux telles extensions, il existe un unique isomorphisme $E \longrightarrow E'$ qui commute à l'action de G et est l'identité sur $\mathbf{C}(T)$).

[Pour prouver i), on choisit $g_1 \in C_1,\dots,g_k \in C_k$ engendrant G et tels que $g_1 \dots g_k = 1$. D'après le § 3, il existe un homomorphisme $\varphi : \pi_1 \longrightarrow G$ qui envoie s_i sur g_i pour tout i . Comme cet homomorphisme est surjectif, cela entraîne i).

De plus, l'hypothèse de rigidité montre que φ est unique, à un automorphisme intérieur de G près. On en déduit que, si E et E' sont deux extensions de type i), il existe un isomorphisme $E \longrightarrow E'$ compatible avec l'action de G ; l'unicité d'un tel isomorphisme résulte de l'hypothèse suivant laquelle le centre de G est trivial.]

Une fois i) et ii) acquis, l'unicité de E (munie de l'action de G) montre que E provient par extension des scalaires d'une extension galoisienne de $\mathbf{Q}(T)$ de groupe de Galois G : il suffit d'appliquer le critère de descente du corps de base de Weil [34]. (Ce critère dit en effet que tout problème "raisonnable" sur un corps K qui a une solution unique, à isomorphisme unique près, sur une extension algébriquement close de K , a déjà une solution sur K .)

Remarques.- 1) La méthode de démonstration esquissée ci-dessus m'a été indiquée par Deligne ; elle est voisine de celle utilisée dans Shih [29], § 2. On aurait pu aussi se servir de la suite exacte liant le π_1 algébrique sur $\mathbf{Q}$ au π_1 géométrique (*cf.* Grothendieck [11], exposé X, p. 253) ; c'est ce que fait Belyi [2].

2) Il y a un énoncé analogue au th. 4 dans lequel on supprime l'hypothèse de rationalité des C_i mais l'on remplace Q par son extension cyclotomique maximale Q^{cycl}. La démonstration est la même.

Variantes : L'existence dans G d'une famille rigide de classes rationnelles est une condition très restrictive (elle n'est même pas satisfaite pour le groupe A_5). Il est utile de l'affaiblir. Cela peut se faire de plusieurs manières. Je me borne à en indiquer deux, particulièrement simples :

1) *Passage d'un groupe à un groupe deux fois plus grand*

Supposons que G soit un sous-groupe d'indice 2 d'un groupe G' de centre trivial, possédant un triplet rigide rationnel (C_1,C_2,C_3). (*Exemple* : $G = A_n$, $G' = S_n$, $n \geq 3$.) Montrons que $Gal_T(G)$ *est vraie.*

D'après le th. 4, il existe une extension galoisienne régulière E de $Q(T)$, de groupe de Galois G', qui est non ramifiée en dehors de trois points rationnels t_1,t_2,t_3 de la droite projective. Soit K le sous-corps de E fixé par G. C'est une extension quadratique de $Q(T)$, non ramifiée en dehors de t_1,t_2,t_3, donc ramifiée en exactement deux de ces points, disons en t_1 et t_2. Un argument élémentaire montre alors que K est une extension transcendante pure de Q : on a $K = Q(U)$, avec $U^2 = c(T-t_1)/(T-t_2)$, $c \in Q^*$. Comme E est une extension galoisienne régulière de K, de groupe de Galois G, cela montre bien que $Gal_T(G)$ est vraie.

2) *Affaiblissement de l'hypothèse de rationalité*

Supposons que G possède un triplet rigide (C_1,C_2,C_3) avec :

C_1 rationnelle sur Q,

C_2 et C_3 rationnelles, non sur Q, mais sur un corps quadratique $Q(\sqrt{d})$, et conjuguées entre elles.

(*Exemple* : $G = A_5$; C_1 = classe des éléments d'ordre 2 ; C_2 et C_3 = classes des éléments d'ordre 5 ; $d = 5$.)

Alors $Gal_T(G)$ *est vraie.*

Cela se voit en reprenant la méthode de démonstration du th. 4, avec la différence suivante : au lieu de choisir les points de ramification t_2 et t_3 rationnels sur Q, on les choisit rationnels sur $Q(\sqrt{d})$, et conjugués l'un de l'autre sur Q.

Pour d'autres variantes (et en particulier pour celles qui utilisent l'action du *groupe des tresses* sur π_1), je renvoie à Fried [9], [10] et Matzat [21], [23].

5. EXEMPLES

5.1 (facile).- On prend $G = S_n$, $n \geq 3$ et l'on choisit pour C_1,C_2 et C_3 les classes de conjugaison des cycles de longueur 2, $n-1$ et n. Montrons que l'on obtient ainsi un triplet *strictement rigide* :

La donnée d'un élément $g_3 \in C_3$ équivaut à celle d'un ordre circulaire sur n lettres. Pour qu'une transposition $g_1 = (ab)$ soit telle que $g_1 g_3$ soit un cycle d'ordre $n-1$, il faut et il suffit que les lettres a et b soient consécutives dans l'ordre en question :

On sait qu'alors g_1 et g_3 engendrent G ; d'où $P = P'$. Quant à la rigidité, elle se voit en remarquant que, si l'on a deux figures du type ci-dessus, il existe un isomorphisme unique de l'une sur l'autre :

(*Exercice* : vérifier que $|P| = |G|$ en utilisant la formule (1) du § 4, et en montrant que tous les termes de la somme de droite sont nuls, à l'exception de ceux provenant des deux caractères χ de degré 1.)

5.2 (difficile).- On prend $G = M$ (le groupe simple de Griess-Fischer, i.e. le "Monstre"). On prend pour C_1, C_2, C_3 les classes de type 2A, 3B et 29A avec les notations de l'ATLAS [5]. D'après Thompson [30], ce triplet est strictement rigide. Cela se voit en deux étapes :

i) En utilisant la formule (1) du § 4, ainsi que la table des caractères de M donnée dans [5], on vérifie (sur ordinateur) que l'on a bien $|P| = |G|$.

ii) Il reste alors à prouver que $P' = P$, i.e. que, si $(g_1, g_2, g_3) \in P$, le sous-groupe engendré par les g_i est égal à M. S'il ne l'était pas, il serait contenu dans un sous-groupe maximal de M. Faute de connaître une liste complète de ces sous-groupes (ou même seulement de ceux dont l'ordre est divisible par 29), on invoque la classification des groupes finis simples pour tirer de là une contradiction (cf. [13], [30]). Inutile de dire que l'on aimerait avoir une démonstration plus aisément vérifiable[1].

5.3. Groupes simples

La liste des groupes simples G pour lesquels la propriété $\mathrm{Gal}_T(G)$ a été démontrée s'accroît régulièrement. Sauf erreur, elle contient :

5.3.1. les groupes alternés A_n, $n \geq 5$ (Hilbert [12]) : ils se déduisent du cas de S_n traité ci-dessus, grâce à la variante 1) du § 4 (c'était à peu de

[1] La démonstration du théorème de classification des groupes finis simples a été souvent décrite, mais jamais écrite (complètement) : l'une de ses étapes n'a pas été publiée. Le "théorème" en question n'est donc pas vérifiable au sens habituel du terme : il réclame un acte de foi.

chose près la méthode de Hilbert lui-même) ;

5.3.2. les groupes sporadiques M_{11} , M_{12} , J_1 , M_{22} , J_2 , HS , M_{24} , Suz , ON , Co_3 , Co_2 , Fi_{22} , HN , F_3 , Fi_{23} , Co_1 , Fi'_{24} , $F_2 = BM$ et $F_1 = M$, cf. [13], [20], [23] (aux dernières nouvelles, les groupes J_3 , M^cL , He , Ru , Ly et J_4 auraient été obtenus par H. Pahlings - seul M_{23} résiste) ;

5.3.3. les groupes de Chevalley de type :

$PSL_2(\mathbf{F}_p)$, $p \geq 5$, si $(\frac{2}{p}) = -1$, ou $(\frac{3}{p}) = -1$, ou $(\frac{7}{p}) = -1$: Shih [29] ;

$PSL_3(\mathbf{F}_p)$, $p \equiv 1 \pmod 4$: Thompson [31] ;

$PSp_4(\mathbf{F}_p)$, $p \geq 3$, $p \equiv 2,3 \pmod 5$: Dentzer [6] ;

$G_2(\mathbf{F}_p)$, $p \geq 5$: Thompson [32] ;

$E_8(\mathbf{F}_p)$ pour une infinité de p : Malle [16], Kap. 9.

(Noter l'absence dans cette liste de groupes de Chevalley sur $\mathbf{F}_q$, pour q non premier.)

5.4. Exemples sur $\mathbf{Q}^{cycl}$

Il y en a bien davantage : il n'y a plus à s'occuper de la rationalité des classes de conjugaison considérées. On trouve (sauf erreur) tous les groupes sporadiques, tous les groupes de Chevalley classiques (Belyi [2], [3]) et la plupart des groupes de Chevalley exceptionnels (Malle [16]).

5.5. Exemples numériques

Supposons G réalisé comme sous-groupe transitif de S_n . On peut se proposer de décrire explicitement, non pas une extension galoisienne $E_T/\mathbf{Q}(T)$ de groupe G , mais au moins la sous-extension $K/\mathbf{Q}(T)$ de degré n correspondant à l'action de G sur n lettres. Le cas le plus simple est celui de S_n lui-même : l'extension K associée aux triplets rigides de 5.1 ci-dessus peut être définie par l'équation

$$X^n + X^{n-1} + T = 0 .$$

En particulier, il existe une infinité de $t \in \mathbf{Z}$ tels que l'équation spécialisée $X^n + X^{n-1} + t$ soit irréductible sur $\mathbf{Q}$, et de groupe de Galois S_n . (*Exercice* : montrer que l'on peut prendre $t = -1$.)

Pour le groupe $PSL_2(\mathbf{F}_7)$ d'ordre 168 , plongé dans S_7 , Malle et Matzat [17] donnent l'équation suivante :

$$X^7 - 56\,X^6 + 609\,X^5 + 1190\,X^4 + 6356\,X^3 + 4536\,X^2 - 6804\,X - 5832 - TX^3(X+1) = 0 .$$

Ils montrent également que, si l'on spécialise T en un entier t avec $t \equiv 1 \pmod{35}$, l'équation obtenue est irréductible et de groupe de Galois $PSL_2(\mathbf{F}_7)$. On ne peut rien rêver de plus explicite !

Les cas de $PSL_2(F_{11})$ et $PSL_2(F_{13})$ sont également traités dans [17], le cas de $SL_2(F_8)$ dans [18] et [22], et celui du groupe de Mathieu M_{12} dans [24]. Voici par exemple une équation de degré 12 donnant M_{12} :

$$X^{12} + 100\,X^{11} + 4050\,X^{10} + 83700\,X^9 + 888975\,X^8 + 3645000\,X^7$$
$$- 10570500\,X^6 - 107163000\,X^5 + 100875375\,X^4 + 1131772500\,X^3$$
$$- 319848750\,X^2 + 1328602500\,X + 332150625 - 9765625\,TX^2 = 0 .$$

6. RÉALITÉ

On peut se demander quelles sont les propriétés *locales* (sur Q_p ou sur R) des extensions de Q fabriquées par la méthode de rigidité.

Il y a un cas où l'on peut répondre à cette question : celui où le corps local est R, et où l'extension $E_T/Q(T)$ est construite par le procédé du th. 4, à partir de *trois classes* rationnelles C_1, C_2, C_3 satisfaisant à la condition de rigidité. Dans ce cas, l'extension E_T est non ramifiée en dehors de trois points rationnels t_1, t_2, t_3 de la droite projective P_1. Comme $P_1(R)$ est homéomorphe à un cercle, ces points partagent $P_1(R)$ en trois segments : $[t_1t_2]$, $[t_2t_3]$ et $[t_3t_1]$.

Soit $t \in P_1(R)$ distincts des t_i. Il correspond à t un élément c_t de G, défini à conjugaison près, qui donne la *conjugaison complexe* dans l'algèbre étale E_t associée à t. On a $c_t^2 = 1$. Il s'agit de déterminer la classe de c_t.

Un argument de continuité montre que c_t ne dépend que du segment sur lequel se trouve t. Supposons pour fixer les idées que t soit entre t_1 et t_3. Choisissons $(s_1, s_2, s_3) \in P'$. On a

$$s_1s_2s_3 = 1 \quad , \quad s_i \in C_i ,$$

d'où

$$s_1^{-1} \cdot s_3^{-1}s_2^{-1}s_3 \cdot s_3^{-1} = 1 ,$$

et $s_1^{-1} \in C_1$, $s_3^{-1}s_2^{-1}s_3 \in C_2$, $s_3^{-1} \in C_3$ puisque les classes C_i sont rationnelles. Vu l'hypothèse de rigidité, on en conclut qu'il existe un unique élément $c \in G$ tel que

$$cs_1c^{-1} = s_1^{-1} \quad , \quad cs_2c^{-1} = s_3^{-1}s_2^{-1}s_3 \quad \text{et} \quad cs_3c^{-1} = s_3^{-1} .$$

On a $c^2 = 1$, et il n'est pas difficile de montrer que *la classe* (c_t) *cherchée est la classe de* c.

De cette description de c_t on tire par exemple que $c_t \neq 1$ si $|G| > 6$. En particulier, les extensions de Q à groupe de Galois un groupe simple non abélien fournies par un triplet rigide de classes rationnelles *ne sont jamais totalement réelles*. Il serait intéressant de voir ce qui se passe dans d'autres cas.

7. UN AUTRE TYPE D'EXEMPLES : LES GROUPES $\tilde{A}_n$ ($n \geq 4$)

On sait depuis Schur que le groupe alterné A_n possède une unique extension non triviale $\tilde{A}_n$ par $\mathbf{Z}/2\mathbf{Z}$:

$$1 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \tilde{A}_n \longrightarrow A_n \longrightarrow 1 .$$

(On peut l'obtenir, par exemple, en plongeant A_n dans $SO_n(\mathbf{R})$, et en prenant son image réciproque dans le revêtement spinoriel du groupe orthogonal.)

Puisque A_n est groupe de Galois sur $\mathbf{Q}$, et même sur $\mathbf{Q}(T)$, on peut se demander si $\tilde{A}_n$ a la même propriété. Cela conduit au *problème de plongement* suivant : si E/K est une extension galoisienne de groupe de Galois A_n, à quelle condition peut-on plonger E dans une extension galoisienne $\tilde{E}$ de groupe de Galois $\tilde{A}_n$? Si $\bar{K}$ désigne une clôture algébrique de K, cela revient à demander que l'homomorphisme $\mathrm{Gal}(\bar{K}/K) \longrightarrow A_n$ correspondant à E/K se relève en un homomorphisme $\mathrm{Gal}(\bar{K}/K) \longrightarrow \tilde{A}_n$. L'*obstruction* à un tel relèvement est un certain élément $a_n(E)$ du groupe de cohomologie $H^2(\mathrm{Gal}(\bar{K}/K), \mathbf{Z}/2\mathbf{Z})$. Le calcul de $a_n(E)$ est facilité par le résultat suivant :

Supposons que la caractéristique de K soit $\neq 2$, et notons E_n le sous-corps de E fixé par A_{n-1} ; on a $[E_n:K] = n$. L'application $E_n \longrightarrow K$ donnée par $x \longmapsto \mathrm{Tr}_{E_n/K}(x^2)$ est une forme quadratique de rang n sur K *dont l'invariant de Witt est l'obstruction* $a_n(E)$ *définie ci-dessus* ([28], th. 1).

Tout revient donc à trouver des exemples où cet invariant de Witt est 0. Cela a été fait par N. Vila [33] pour certaines extensions galoisiennes de $\mathbf{Q}(T)$ à groupe de Galois A_n. Elle en a déduit que la propriété $\mathrm{Gal}_T(\tilde{A}_n)$ est vraie dans chacun des cas suivants :

$n \equiv 0$ ou $1 \pmod 8$;

$n \equiv 2 \pmod 8$ et n est somme de deux carrés ;

$n \equiv 3 \pmod 8$, et n satisfait à une certaine condition " N " qui est en pratique toujours vérifiée.

On sait également que $\mathrm{Gal}_T(\tilde{A}_n)$ est vraie pour $n = 5$ (Mestre, non publié, améliorant un résultat de Feit [7]).

Signalons enfin que $\mathrm{Gal}_\infty(\tilde{A}_n)$ a été démontrée pour $n = 7$ (Feit) et aussi pour $n = 6$ (Mestre). Dans chaque cas, la famille infinie d'extensions de $\mathbf{Q}$ est paramétrée par les points rationnels d'une *courbe elliptique* sur $\mathbf{Q}$.

BIBLIOGRAPHIE

[1] P. BAYER, P. LLORENTE et N. VILA - $\tilde{M}_{12}$ *comme groupe de Galois sur* $\mathbf{Q}$, C.R. Acad. Sci. Paris 303 (1986), 277-280.

[2] G.V. BELYI - *Extensions galoisiennes du corps cyclotomique maximal* [en russe], Izv. Akad. Nauk SSSR 43 (1979), 267-276 (= Math. USSR Izv. 14 (1980), 247-256).

[3] G.V. BELYI - *On extensions of the maximal cyclotomic field having a given classical Galois group*, J. Crelle 341 (1983), 147-156.

[4] A. BRUEN, C. JENSEN et N. YUI - *Polynomials with Frobenius groups of prime degree as Galois groups* II, J. of Number Theory, 24 (1986), 305-359.

[5] J. CONWAY, R. CURTIS, S. NORTON, R. PARKER et R. WILSON - *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[6] R. DENTZER - *Realisierung von symplektischen Gruppen als Galoisgruppen über* $\mathbf{Q}$, Diplomarbeit, Karlsruhe, 1987.

[7] W. FEIT - $\tilde{A}_5$ *and* $\tilde{A}_7$ *are Galois groups over number fields*, J. of Algebra 104 (1986), 231-260.

[8] M. FRIED - *On Hilbert's irreducibility theorem*, J. of Number Theory 6 (1974), 211-232.

[9] M. FRIED - *Fields of definition of function fields and Hurwitz families, Groups as Galois groups*, Commun. Alg. 5 (1977), 17-82.

[10] M. FRIED - *Rigidity and applications of the classification of simple groups to monodromy*, preprint, 1987.

[11] A. GROTHENDIECK - *Revêtements étales et groupe fondamental* (SGA I), Lect. Notes in Math. 224, Springer-Verlag, 1971.

[12] D. HILBERT - *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Crelle 110 (1892), 104-129 (= *Ges. Abh.* II, 264-286).

[13] D.C. HUNT - *Rational rigidity and the sporadic groups*, J. of Algebra 99 (1986), 577-592.

[14] S. LANG - *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[15] G. MALLE - *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$, M_{22} *and* $PSL_3(F_4) \cdot 2_2$ *over* $\mathbf{Q}$, à paraître.

[16] G. MALLE - *Exzeptionnelle Gruppen vom Lie-typ als Galoisgruppen*, à paraître.

[17] G. MALLE et B.H. MATZAT - *Realisierung von Gruppen* $PSL_2(F_p)$ *als Galoisgruppen über* $\mathbf{Q}$, Math. Ann. 272 (1985), 549-565.

[18] B.H. MATZAT - *Zur Konstruktion von Zahl - und Funktionenkörpern mit vorgegebener Galoisgruppe*, Habilitationsschrift, Karlsruhe, 1980 (voir aussi J. Crelle 349 (1984), 179-220).

[19] B.H. MATZAT - *Zwei Aspekte konstruktiver Galoistheorie*, J. of Algebra 96 (1985), 499-531.

[20] B.H. MATZAT - *Realisierung endlicher Gruppen als Galoisgruppen*, Man. Math. 51 (1985), 253-265.

[21] B.H. MATZAT - *Topologische Automorphismen in der konstruktiven Galoistheorie*, J. Crelle 371 (1986), 16-45.

[22] B.H. MATZAT - *Konstruktive Galoistheorie*, Lect. Notes in Math., 1284, Springer-Verlag, 1987.

[23] B.H. MATZAT - *Rationality criteria for Galois extensions*, 1987, à paraître.

[24] B.H. MATZAT et A. ZEH-MARSCHKE - *Realisierung der Mathieugruppen* M_{11} *und* M_{12} *als Galoisgruppen über* Q , J. of Number Theory 23 (1986), 195-202.

[25] J. NEUKIRCH - *On solvable number fields*, Invent. Math. 53 (1979), 135-164.

[26] I.R. ŠAFAREVIČ - *Construction de corps de nombres algébriques à groupe de Galois résoluble donné* [en russe], Izv. Akad. Nauk SSSR 18 (1954), 525-578 (= Amer. Math. Soc. Transl. 4 (1956), 185-237).

[27] D. SALTMAN - *Generic Galois extensions and problems in field theory*, Adv. in Math. 43 (1982), 250-283.

[28] J.-P. SERRE - *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comm. Math. Helv. 59 (1984), 651-676.

[29] K.-y. SHIH - *On the construction of Galois extensions of function fields and number fields*, Math. Ann. 207 (1974), 99-120.

[30] J.G. THOMPSON - *Some finite groups which appear as* $\mathrm{Gal}(L/K)$, *where* $K \subseteq \mathbf{Q}(\mu_n)$, J. of Algebra 89 (1984), 437-499.

[31] J.G. THOMPSON - PSL_3 *and Galois groups over* Q , Proc. Rutgers groups theory year 1983-1984, Cambridge Univ. Press (1984), 309-319.

[32] J.G. THOMPSON - *Some finite groups of type* G_2 *which appear as Galois groups over* Q , preprint, 1983.

[33] N. VILA - *On central extensions of* A_n *as Galois group over* Q , Arch. Math. 44 (1985), 424-437.

[34] A. WEIL - *The field of definition of a variety*, Amer. J. Math. 78 (1956), 509-524 (= *Oe. Sci.* II, 291-306).

Jean-Pierre SERRE

Collège de France
3, rue d'Ulm
F-75005 PARIS