Topics in Galois Theory

J.-P. Serre: Research Notes in Mathematics
(1992) Jones and Bartlett Publ, 116 pages

Ce livre de Serre touche à un ensemble de sujets. Il contient les origines historiques et les applications du problème inverse de la théorie de Galois. Il s'adresse aux mathématiciens qui connaissent l'omniprésence des groupes de Galois en théorie des nombres. Ces mathématiciens savent que le problème inverse de la théorie de Galois a connu dernièrement des progrès importants. Serre a dressé une carte de ces avancées, en s'attachant à celles qui ne perdent pas de vue les repères classiques. Nous allons décrire ce nouvel horizon vu par Serre et ajouter quelques commentaires sur certains développements qu'il a laissés de côté. Le livre de Serre est désormais noté [Se].

La théorie de Galois est le sujet suprême dans un domaine qu'on appelait autrefois *la Théorie des Polynômes*. Le problème inverse de la théorie de Galois a des applications immédiates en théorie algébrique des nombres, en géométrie, en théorie des codes. Ceci inclut des applications provenant de la théorie des corps finis. Jusque récemment cependant, les approches du problème étaient *ad hoc*. Même quand des méthodes générales ont commencé à se faire jour à la fin des années soixante-dix, leur reconnaissance prit un certain temps. On continuait de croire en des méthodes plus particulières. On dispose aujourd'hui d'exemples qui expliquent pourquoi les méthodes plus anciennes ne résoudront pas le problème dans sa totalité.

Pourtant, certains gardent espoir. Par exemple, Colliot-Thélène fait la conjecture suivante [Se; Conjecture 3.5.8]. Si K est un corps de nombres, alors une variété K-unirationnelle a une propriété d'approximation que Serre appelle *weak-weak approximation*. Serre montre qu'une telle propriété entraine une propriété type Hilbert. Il retrouve ainsi — de manière conjecturale — le programme initial de Noether. Celui-ci demandait si tout groupe $G \leq S_n$ agissant sur $K(x_1, \ldots, x_n)$ a comme corps d'invariants une extension transcendante pure. Bien qu'il y ait un contre-exemple bien connu de Swann, Serre demande si sous quelque forme le théorème d'irréductibilité de Hilbert ne s'applique pas quand même à l'extension ci-dessus. Cette question, et plus généralement la conjecture de Colliot-Thélène, est certes naturelle et fondamentale, mais pouvons-nous raisonnablement en attendre une réponse prochaine? Serre pense que non.

Pourquoi le problème inverse de la théorie de Galois a-t-il connu cet essor récent? La classification des groupes finis simples a eu un gros impact psychologique. Beaucoup ont été séduits par la réalisation du Monstre par Thompson, grâce à la méthode de *rigidité* (§5). Il y avait un sentiment répandu: réaliser tous les groupes simples comme groupes de Galois suffisait pour réaliser tous les groupes. Si on pouvait réaliser le Monstre, le cas des autres groupes simples ne devait-il pas suivre et donc aussi le problème inverse de la théorie de Galois dans sa totalité? La section 8 explique pourquoi cela était naïf. Cela a cependant déclenché un regain d'intérêt.

Le livre fait un peu plus de cent pages. Avec des démonstrations complètes, il aurait dépassé les trois-cents pages. Il n'aurait pas été publié aussi vite. La plupart des algébristes y trouveront de l'intérêt.

Les corps seront supposés de caractéristique 0, en général des sous-corps de $\mathbb{C}$, le corps des complexes.

§0. LE PROBLEME INVERSE DE LA THEORIE DE GALOIS: Soit $L/\mathbb{Q}$ une extension finie de corps. Alors il y a $n = [L : \mathbb{Q}]$ plongements de L dans le corps $\overline{\mathbb{Q}}$ des nombres algébriques. Si $L = \mathbb{Q}(\alpha)$, chaque plongement correspond à une racine du polynôme minimal de α sur $\mathbb{Q}$. Quand tous ces plongements sont des automorphismes de L, L est une extension *galoisienne* de $\mathbb{Q}$. Le groupe $G(L/\mathbb{Q})$ des automorphismes de l'extension est le *groupe de Galois* de $L/\mathbb{Q}$. Pour toute extension $L/\mathbb{Q}$, il y a une extension galoisienne minimale $\hat{L}/\mathbb{Q}$ contenant L: la clôture galoisienne de $L/\mathbb{Q}$. Considérons les groupes $G^L = G(\hat{L}/\mathbb{Q})$ quand L décrit toutes les extensions finies de $\mathbb{Q}$. Si $L \subset L'$, l'homomorphisme de restriction $G(\hat{L}'/\mathbb{Q}) \xrightarrow{\text{rest}} G(\hat{L}/\mathbb{Q})$ transforme chaque automorphisme de $\hat{L}'$ en un automorphisme de $\hat{L}$. Le groupe $G_{\mathbb{Q}} = G(\overline{\mathbb{Q}}/\mathbb{Q})$ est défini comme le sous-groupe de $\mathcal{G} = \prod_L G^L$ constitué de tous les ∞-uplets $(\ldots, \alpha_L, \ldots)$ tels que $\text{rest}(\alpha_{L'}) = \alpha_L$ pour toute extension $L \subset L'$. Le groupe $G_{\mathbb{Q}}$ est le *groupe de Galois absolu* de $\mathbb{Q}$; on le considère comme l'objet le plus important en géométrie arithmétique. Cependant qu'en connaissons-nous?

Par construction, $G_{\mathbb{Q}}$ est un très gros groupe topologique compact possédant un nombre dénombrable de générateurs topologiques. S'il possédait des générateurs *indépendants*, c'est-à-dire, si c'était un groupe (profini) libre, nous en saurions énormément. Par exemple, tout groupe fini en serait un quotient. C'est-à-dire, étant donné un groupe fini G, il existerait L tel que $G(\hat{L}/\mathbb{Q}) = G$. Ceci est la forme la plus simple du *problème inverse de la théorie de Galois*.

On sait que $G_{\mathbb{Q}}$ n'est pas un groupe libre. Par exemple, un groupe libre n'a pas d'éléments d'ordre fini. Or $G_{\mathbb{Q}}$ contient un élément d'ordre 2, la conjugaison complexe. Le groupe symétrique S_n et le groupe alterné A_n font partie des quotients connus de $G_{\mathbb{Q}}$ (Hilbert: 1896). On sait aussi que parmi ses quotients figurent tous les groupes simples sporadiques (Feit, Matzat and Thompson) — sauf peut-être M_{23}, le groupe de Mathieu de degré 23, ainsi que tous les groupes résolubles (Shafarevich). Voir [Se] pour des références plus précises.

Pour les groupes de Chevalley, même sur les corps finis d'ordre premier, c'est un autre problème. Une grande part du livre de Serre repose sur la théorie des *formes modulaires* et sur la *rigidité*. Avec ces outils, il obtient de nombreux groupes de Chevalley comme groupes de Galois à partir de $\mathrm{GL}_2(p)$, $\mathrm{PSL}_2(p)$ and $\mathrm{PGL}_2(p)$ (Belyi, Malle, Shih en particulier). Ce sont des groupes de Chevalley de rang 1 sur le corps premier $\mathbb{F}_p$.

En revanche, sur des corps finis non premiers, Serre ne fait mention de résultats que pour une poignée de groupes de Chevalley [Se; p. 53]. Aucun d'eux n'a un rang strictement plus grand que 1. Dans le même temps pourtant, Völklein [V1, V2] a réalisé plusieurs familles de groupes de Chevalley de rang plus élevé sur des corps finis non premiers. Ces résultats utilisent des généralisations de la rigidité qui ne figurent pas dans [Se] (voir §1).

Si $G_{\mathbb{Q}}$ était un groupe libre, il en serait de même pour de nombreux sous-groupes normaux d'indice infini, en particulier son groupe des commutateurs $[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$. Ce groupe est le groupe de Galois absolu de l'extension abélienne maximale $\mathbb{Q}^{\mathrm{ab}}$ de $\mathbb{Q}$. Kronecker a montré au siècle dernier que $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$, le corps obtenu à partir de $\mathbb{Q}$ par adjonction de toutes les racines de l'unité. La conjecture suivante permettrait de coincer $G(\overline{\mathbb{Q}}/\mathbb{Q})$ entre deux groupes profinis bien connus, le groupe profini libre à un nombre dénombrable de générateurs $\hat{F}_\omega$ et le groupe profini $\hat{\mathbb{Z}}^*$ des entiers inversibles.

Conjecture de Shafarevich: *$G(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}})$ est un groupe profini libre. On a donc la suite exacte suivante:*

$$1 \to \hat{F}_\omega \to G_{\mathbb{Q}} \to G(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \to 1.$$

§1. RESULTATS CLASSIQUES: [Se] illustre bien l'importance de la théorie de Galois dans divers domaines. Il passe assez vite de la période classique — le théorème de Shafarevich et les méthodes de théorie algébrique des nombres — à l'ère moderne. Celle-ci commence au début des années 80 au moment où les réalisations régulières prennent le dessus. En effet, après les deux premiers chapitres, le livre se concentre sur les *extensions régulières* $L/\mathbb{Q}(x)$, *i.e.*, les extensions $L/\mathbb{Q}(x)$ telles que $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Ici x désigne une indéterminée fixée dans toute la suite.

Pour la plupart des applications, il vaut mieux s'intéresser aux réalisations régulières. Voici pourquoi. Les applications nécessitent souvent de réaliser un groupe avec en plus certaines conditions annexes, comme celles qui apparaissent pour la réalisation des ℓ-groupes [Se; Chap. 2]. Une réalisation régulière offre une plus grande lattitude pour garantir de telles conditions. Voici deux types de conditions dont on peut avoir besoin quand on réalise un groupe G sur un corps K.

Au cours d'une construction sur un corps K, on peut être amené à réaliser G comme $G(M/\mathbb{Q})$ avec $M \cap K = \mathbb{Q}$: une *condition d'indépendance*. Ou bien, on peut demander à M de satisfaire des conditions locales — en certaines places.

Hilbert a lui-même énoncé l'application suivante de son théorème d'irréductibilité. On obtient par spécialisation d'une extension régulière de G sur K une infinité d'extensions galoisiennes linéairement disjointes de K de groupe G. Ce corollaire est un exercice facile sur les *groupes de décomposition* — une technique bien connue de beaucoup d'algébristes. Le théorème de Hilbert permet également d'obtenir comme groupes de Galois sur $\mathbb{Q}$ des produits en couronne de G avec un autre groupe déjà réalisé comme groupe de Galois sur $\mathbb{Q}$. Cette dernière réalisation n'a pas à être régulière. ([Se; p. 36] se contente d'une remarque sur ce corollaire précieux).

Le théorème d'irréductibilité de Hilbert tient une place de choix dans le livre de Serre. Son énoncé semble anodin: tout corps de nombres L est un corps hilbertien, c'est-à-dire, tout polynôme irréductible $f(x,y) \in L[x,y]$ (de degré > 0 en y) reste irréductible pour une infinité de spécialisations de x dans L. [Se] en propose diverses variantes et conséquences, parfois sans citer leurs auteurs (par exemple [Se;§4.6] où il donne les grandes lignes de [FrJ; Theorem 12.7]). Une réalisation régulière rend plus de services, mais leur recherche est plus difficile; on peut donc être surpris qu'elle ait rencontré plus de succès que la recherche de simples réalisations.

La *rigidité* dans sa forme première est au centre des chapitres suivants (voir §4). Cependant le livre n'analyse pas les limites de cette méthode. Ainsi il y a des raisons sérieuses pour lesquelles on ne peut pas — comprendre il n'est pas possible de — réaliser la plupart des groupes comme groupes de Galois par la méthode de rigidité. De fait, depuis plusieurs années maintenant, ce sont des généralisations de la rigidité et non la rigidité elle-même, qui ont permis d'obtenir de nouveaux groupes comme groupes de Galois sur $\mathbb{Q}$. Le livre de Serre ne fait aucun commentaire sur ces généralisations. (Celles-ci existaient bien avant la rigidité dans [Fr].) Ces résultats généraux nécessitent un cadre théorique important où la rigidité seule perd sa place centrale sinon son intérêt.

Nous faisons quelques commentaires sur ces généralisations au §3. La section 7 comprend un exemple lié au sous-thème des courbes modulaires de [Se; Chap. 5]. Les courbes modulaires sont des revêtements $\varphi : X \to \mathbb{P}^1$ de la sphère ramifiés en trois points $\mathbb{Q}$-rationnels de $\mathbb{P}^1$. De façon classique, la fonction j uniformise ici la copie de la sphère. Les points de ramification de φ peuvent être pris égaux à 0, 1 et ∞. Ces courbes particulières apparaissent cependant comme compactifications du demi-plan de Poincaré modulo des *sous-groupes de congruence* de $\mathrm{PSL}_2(\mathbb{Z})$. Serre consacre un grand nombre de pages au théorème de Shih sur la réalisation régulière de $\mathrm{PSL}_2(\mathbb{F}_p)$ (sur $\mathbb{Q}$). Le paragraphe suivant décrit comment il exploite la théorie des formes modulaires pour la mettre au service du problème inverse de la théorie de Galois.

§**2. SHIH'S THEOREM:** Note: Un élément d'ordre 2 et un élément d'ordre 3 engendrent $\mathrm{PSL}_2(\mathbb{Z})$ sans relations. Considérons un revêtement quelconque de la sphère ramifié en trois points. Supposons que sa clôture galoisienne ait un groupe de Galois engendré par un élément d'ordre 2 et un élément d'ordre 3. Ce revêtement peut donc être présenté comme un quotient du demi-plan de Poincaré par un sous-groupe d'indice fini de $\mathrm{PSL}_2(\mathbb{Z})$. Pour la plupart, de telles courbes ne sont pourtant pas des courbes modulaires. Chaque point d'une courbe modulaire a une signification géométrique. Expliquons brièvement comment [Sh] a tiré parti de cela.

Soit $N > 0$ un entier. Considérons le sous-groupe $\Gamma_0(N)$ de $\mathrm{PSL}_2(\mathbb{Z})$ des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec $c \equiv 0 \bmod N$. Nous nous intéressons surtout au cas où la compactification naturelle $X = X_N$ de $H/\Gamma_0(N)$ est de genre 0. D'après la théorie classique, on obtient une courbe définie sur $\mathbb{Q}$; cela se déduit aussi de la rigidité (§4), étendue au cas des revêtements non nécessairement galoisiens. On voit apparaître divers groupes $\mathrm{PSL}_2(\mathbb{F}_p)$ en interprétant les points rationnels sur des *twists* de ce revêtement quand X_N est de genre 0. Serre rappelle, sans référence, que cela ne peut se produire que pour $N \leq 18, N \neq 4, 9, 11, 14$–$17$. Il y a une involution naturelle w sur X_N. Considérons les points sur X_N comme des paires (E, E') de courbes elliptiques données avec une isogénie cyclique $E \to E'$ de degré N. L'isogénie duale fournit une flèche $E' \to E$. On peut définir w par $w(E, E') = (E', E)$.

Considérons une extension quadratique $K/\mathbb{Q}$. Notons σ le générateur de son groupe de Galois. Identifions les groupes de Galois $G(\mathbb{Q}(X_N)/\mathbb{Q}(X_N/\langle w\rangle))$ et $G(K/\mathbb{Q})$ avec $\mathbb{Z}/2$. Donc $G(K(X_N)/\mathbb{Q}(X_N/\langle w\rangle))$ est $\mathbb{Z}/2 \times \mathbb{Z}/2$. La diagonale a ici comme corps des invariants le corps des fonctions d'une courbe X_N^K de genre 0 définie sur $\mathbb{Q}$.

Intéressons nous au cas où $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)$ et $\left(\frac{N}{p}\right) = -1$ avec p un nombre premier. Considérons une courbe elliptique E définie sur K et telle que E et E^σ soient isogènes. Alors:

(*) $G_{\mathbb{Q}}$ opère sur les points de p-division de E avec image dans $\mathrm{PSL}_2(\mathbb{F}_p)$ (au lieu de $\mathrm{PGL}_2(\mathbb{F}_p)$).

Quand $X_N^K = X_N^p$ possède un point rationnel, son corps des fonctions est $\mathbb{Q}(x)$ pour un certain x. Dans ce cas, (*) fournit une représentation régulière de $\mathrm{PSL}_2(\mathbb{F}_p)$. Quand $N = 2, 3$ ou 7, Serre explique rapidement comment une interprétation modulaire permet de voir que les points fixes de w sont rationnels. On obtient donc un point rationnel sur X_N^p. Ainsi les nombres premiers p pour lesquels on obtient une réalisation régulière de $\mathrm{PSL}_2(\mathbb{F}_p)$ sont ceux pour lesquels $\left(\frac{N}{p}\right) = -1$, où $N = 2, 3$ ou 7. Il est manifeste que Serre apprécierait tout progrès dans cette direction.

§3. L'ARGUMENT DES CYCLES DE RAMIFICATION — PRELUDE A LA RIGIDITE: [Se; Chap. 6] est consacré au *théorème d'existence de Riemann*. Plusieurs versions y sont données, avec de nombreuses références. Ce résultat est au cœur de la rigidité et de ses généralisations. Nous allons en énoncer une version simple, dépourvue de toute la sophistication qui l'accompagne habituellement. (Cette sophistication, inutile ici, est importante en d'autres circonstances). Soit $L/\mathbb{C}(x)$ une extension finie de degré n. Soit $\hat{L}/\mathbb{C}(x)$ sa clôture galoisienne (§0). Alors, $G(\hat{L}/\mathbb{C}(x))$ peut-être envoyé fidèlement dans S_n. Ce plongement est unique à conjugaison près de l'image par un élément de S_n.

Pour tout $x' \in \mathbb{C} \cup \{\infty\}$, considérons le corps $\mathbb{C}((x-x'))$ des séries de Laurent formelles en $x-x'$. La variable $x-x'$ doit être remplacée par $1/x$ si $x' = \infty$. La clôture algébrique de $\mathbb{C}((x-x'))$ est $\cup_{e=1}^{\infty}\mathbb{C}(((x-x')^{\frac{1}{e}}))$. Le groupe de Galois absolu de $\mathbb{C}((x-x'))$ est donc pro-cyclique. Son générateur $\sigma_{x'}$ envoie $(x-x')^{\frac{1}{e}}$ sur $\zeta_e(x-x')^{\frac{1}{e}}$, $e = 2, 3, \ldots$, où $\zeta_e = e^{2\pi i/e}$. Comme l'extension $\hat{L}\mathbb{C}((x-x'))/\mathbb{C}((x-x'))$ est galoisienne, il existe un plus petit entier e tel que $\hat{L}$ se plonge dans $\mathbb{C}(((x-x')^{\frac{1}{e}}))$ (en prolongeant l'identité sur $\mathbb{C}(x)$). Tout plongement $\hat{L} \to \mathbb{C}(((x-x')^{\frac{1}{e}}))$ s'obtient en composant un plongement fixé quelconque $\psi_{x'} : \hat{L} \to \mathbb{C}(((x-x')^{\frac{1}{e}}))$ avec les automorphismes de $\hat{L}$. La restriction de $\sigma_{x'}$ à $\hat{L}$ définit donc une classe de conjugaison du groupe $G(\hat{L}/\mathbb{C}(x))$.

Il n'y a qu'un nombre fini de x' tels que $e = e_{x'} > 1$. Notons les $x_1, \ldots, x_r$, ce sont les *points de ramification* du revêtement. Notons $\sigma_1, \ldots, \sigma_r$ les automorphismes correspondant aux plongements ψ associés aux points $x_1, \ldots, x_r$. Soit e_i l'entier e associé à x_i: c'est *l'indice de ramification* en x_i.

Théorème d'existence de Riemann: *Pour un certain choix des plongements ψ, on a*

(i) $\sigma_1 \cdots \sigma_r = 1$, *et*

(ii) $\sigma_1, , \ldots \sigma_r$ *engendrent* G.

Réciproquement, supposons donnés $x_1, \ldots, x_r$, et $\sigma_1, \ldots, \sigma_r \in S_n$ satisfaisant (i) et (ii) avec G un sous-groupe transitif de S_n. Alors il existe une extension $L/\mathbb{C}(x)$ pour laquelle ces données soient les invariants construits ci-dessus.

Nous pouvons maintenant expliquer l'*argument des cycles de ramification* donné dans [Fr; prelude to Th.5.1]. Supposons que $L/\mathbb{Q}(x)$ soit une extension régulière. Soit $\hat{L}/\mathbb{Q}(x)$ sa clôture galoisienne. Notons $\hat{\mathbb{Q}}$ le corps des constantes de $\hat{L}/\mathbb{Q}(x)$. Par définition, le *groupe de monodromie arithmétique* est $\hat{G} = G(\hat{L}/\mathbb{Q}(x))$ et le *groupe de monodromie géométrique* est $G = G(\hat{L}/\hat{\mathbb{Q}}(x))$. Le groupe $G_{\mathbb{Q}}$ permute les points de ramification $x_1, \ldots, x_r$ de $L/\mathbb{Q}(x)$. Cette permutation est un invariant précieux de l'extension.

Fixons un plongement $\hat{L} \subset \overline{\mathbb{Q}}(((x-x_i)^{\frac{1}{e_i}}))$. Comme en §0, soit $\mathbb{Q}^{\mathrm{cyc}}$ le corps obtenu en adjoignant à $\mathbb{Q}$ les racines de l'unité. L'image de tout élément $\tau \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ par la restriction $G(\overline{\mathbb{Q}}/\mathbb{Q}) \to G(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ est donnée par l'action de τ sur les racines de l'unité. On peut donc voir l'image de τ comme un entier supernaturel $n_\tau \in \mathbb{Z}^*$. Identifions également l'action of τ sur $x_1, \ldots, x_r$ avec la permutation correspondante de $1, \ldots, r$. Etant donnée une famille $\mathrm{C}_1, \ldots, \mathrm{C}_t$ de classes de conjugaisons de $\hat{G}$, on dit que $C_1 \cup \cdots \cup C_t$ est une *réunion rationnelle* si elle contient les puissances m-ièmes de ses éléments, pour tout entier m premier avec les ordres de tous ses éléments.

Argument des Cycles de Ramification: *Sous les hypothèses ci-dessus sur $L/\mathbb{Q}(x)$ et sur $x_1, \ldots, x_r$, la classe de conjugaison dans $\hat{G}$ de $\sigma_{\tau(i)}^{n_\tau}$ est la même que la classe de conjugaison de σ_i, $1, \ldots, r$. En particulier, pour chaque $i = 1, \ldots, r$, la réunion des classes de conjugaison de $\sigma_{\tau(i)}$ où τ décrit $G(\overline{\mathbb{Q}}/\mathbb{Q})$, est une réunion rationnelle de classes de conjugaison dans $\hat{G}$.*

Cas particulier: Supposons en plus que $x_1 \in \mathbb{Q}$. Soit m un entier premier à l'ordre de σ_1. Le résultat dit que σ_1^m est conjugué à σ_1 dans $\hat{G}$. En voici la raison. Choisissons un $\tau \in G_{\mathbb{Q}}$ tel que $\tau(\zeta_{e_1}) = \zeta_{e_1}^m$. L'élément τ a une action naturelle sur $\overline{\mathbb{Q}}(((x-x_1)^{\frac{1}{e_1}}))$: on agit sur chacun des coefficients. Cette action induit par restriction un automorphisme de $\hat{L}$. Calculons maintenant l'effet de la conjugaison de τ sur σ_1: $\tau\sigma_1\tau^{-1}((x-x_1)^{\frac{1}{e_1}}) = \tau(\zeta_{e_1}(x-x_1)^{\frac{1}{e_1}}) = \zeta_{e_1}^m(x-x_1)^{\frac{1}{e_1}}$. L'action est la même que celle de σ_1^m.

La section 7 contient plusieurs exemples montrant comment utiliser l'argument des cycles de ramification.

§4. **LA RIGIDITE ET SES GENERALISATIONS:** Le Théorème 5.1 de [Fr] constitue une réciproque partielle de l'argument des cycles de ramification. Ce résultat, qui s'énonce en termes d'espaces de modules, est relatif aux extensions $L/\mathbb{Q}(x)$ ayant comme groupes de monodromie géométrique et arithmétique des groupes G et $\hat{G}$ donnés. Si $[L : \mathbb{Q}(x)] = n$, ces deux groupes sont naturellement des sous-groupes de S_n. De plus G est un sous-groupe normal de $\hat{G}$. En vue des applications, commençons par nous donner G et l'ensemble $\mathbf{C}$ des classes de conjugaisons respectives des générateurs $\sigma_1, \ldots, \sigma_r \in G$. Supposons que

(iii) La réunion de ces classes est rationnelle, comme indiqué dans l'argument des cycles de ramification.

Alors il existe un groupe maximal G^* qui contient tous les groupes possibles $\hat{G}$. Considérons un groupe H quelconque compris entre G et G^*. Sous certaines conditions sur G—principalement G n'a pas de centre—on peut construire un ensemble algébrique $\mathcal{H}(\mathbf{C}, G, H)$, défini sur $\mathbb{Q}$. De plus il existe des morphismes (finis) $\mathcal{H}(\mathbf{C}, G, G^*) \to \mathcal{H}(\mathbf{C}, G, H)$, également définis sur $\mathbb{Q}$.

Réciproque de l'argument des cycles de ramification ([Fr] ou [FrV] sous une forme plus précise): *La condition suivante est une condition diophantienne équivalente à l'existence d'une extension $L/\mathbb{Q}(x)$ ayant G et H comme groupes de monodromie et pour laquelle l'ensemble des classes de conjugaison des cycles de ramification soit l'ensemble* $\mathbf{C}$ *donné. Il existe un point $\boldsymbol{p}^* \in \mathcal{H}(\mathbf{C}, G, G^*)$ dont l'image dans $\mathcal{H}(\mathbf{C}, G, H)$ a des coordonnées dans $\mathbb{Q}$ et $[\mathbb{Q}(\boldsymbol{p}^*)/\mathbb{Q}] = (G^* : H)$. (Comme les espaces $\mathcal{H}$ sont des espaces de modules, ces résultats s'appliquent avec n'importe quel corps K à la place de $\mathbb{Q}$.)*

Pour le problème inverse, considérons un groupe G plongé S_n par sa représentation régulière et prenons $H = G^*$.

La forme régulière du problème inverse de la théorie de Galois est équivalente à l'existence d'un point $\mathbb{Q}$-rationnel sur l'un des espaces $\mathcal{H}(\mathbf{C}, G, G^*)$ où $\mathbf{C}$ vérifie (iii).

Dans la section 7 on s'intéresse au cas lié aux formes modulaires rencontré dans la section 2. Les espaces $\mathcal{H}$ sont $G_{\mathbb{Q}}$-invariants et lisses. Donc ils ne peuvent avoir de points rationnels que s'ils ont des $\mathbb{Q}$-composantes *absolument* irréductibles sur $\mathbb{Q}$. Pour examiner cette question, revenons au cas particulier de la rigidité [Se; §7.3]. La condition de rigidité est rarement satisfaite en dehors du cas $r = 3$. Quand $r = 3$, les espaces $\mathcal{H}$ sont soit $(\mathbb{P}^1)^3$ privé des hyperplans diagonaux, ou bien un de ses quotients par un sous-groupe de S_3. Ces espaces ont évidemment un ensemble dense de points rationnels. Dans les sections suivantes, nous reprenons quelques exemples historiques donnés dans [Se].

Soient $\mathbf{C} = (\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3)$ trois classes de conjugaisons de G. Soit $\Sigma(\mathbf{C})$ l'ensemble des triplets $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ satisfaisant les conditions (i) et (ii) de §3 et tels que $\sigma_i \in \mathrm{C}_i$, $i = 1, 2, 3$. Le groupe G opère sur $\Sigma(\mathbf{C})$ par conjugaison: $g\boldsymbol{\sigma}g^{-1} = (g\sigma_1 g^{-1}, g\sigma_2 g^{-1}, g\sigma_3 g^{-1})$.

Condition de rigidité: *En plus de (iii), un groupe G de centre trivial est dit rigide sur* $\mathbf{C}$*, s'il agit transitivement sur $\Sigma(\mathbf{C})$. Pour $r > 3$, ceci est remplacé par une condition plus générale où la transitivité de G est remplacée par la transitivité d'une action du groupe des tresses d'Artin ([Fr; Theorem 5.1] et [FrV]).*

§5. LA RIGIDITE APPLIQUEE AU MONSTRE: L'Atlas [At] contient un abrégé sur les groupes simples sporadiques. [Se,§7.4.4-§7.4.7] montre comment utiliser les tables de caractères contenues dans [At] pour vérifier la condition de rigidité. La section 7.4.7 notamment, inspirée de [Th], explique comment cela a permis de réaliser le *Monstre de Fischer-Griess*.

Le Monstre M a des classes de conjugaison rationnelles notées $2A$, $3B$ et $29A$ dans l'Atlas. Leurs éléments sont d'ordre, respectivement 2, 3 et 29. Pour montrer que cet ensemble de classes de conjugaison est rigide, on commence par montrer qu'il y a $|M|$ triplets $(\sigma_1, \sigma_2, \sigma_3)$ à composantes dans chacune de ces 3 classses vérifiant (i). Pour un groupe ordinaire, ce serait un calcul classique de caractères basé sur la *formule des constantes de structure* [Se,p.70]. Pour le groupe M, ce calcul a été fait sur ordinateur — par un collaborateur de Thompson. (Ce calcul peut être réalisé aujourd'hui grâce au logiciel GAP qui contient la table de caractères du Monstre.)

Il faut ensuite montrer que de tels triplets engendrent le Monstre tout entier (condition (ii)). L'affaire se corse. [At] ne donne pas la liste des sous-groupes maximaux du Monstre; on ne les connaît pas encore. On a donc recours à un argument indirect. Un quotient simple du groupe engendré par $(\sigma_1, \sigma_2, \sigma_3)$ aurait un ordre de la forme $2 \cdot 3 \cdot 29 \cdot k$ divisant M. D'après la classification des groupes simples, il n'existe pas de tels groupes. A cet endroit [Se; p. 79] s'interrompt pour faire le commentaire suivant sur la classification:

> "Bien que la preuve de la classification ait été annoncée, décrite et largement commentée depuis 1980, il n'est pas clair qu'elle soit complète: la partie sur les groupes *quasi-minces* n'a jamais été publiée."

Il existe des manuscrits de Mason (autour de 1979) et d'Aschbacher (1992) qui, réunis, démontrent les résultats relatifs aux groupes quasi-minces. Il se peut qu'on obtienne une démonstration complète de la classification en regroupant l'ensemble de tous les travaux sur la question. Cela dit, considérons l'énoncé affirmant qu'il n'y a pas de groupes simples avec un ordre satisfaisant les conditions ci-dessus. On peut souhaiter plus de détails. Pour le moment, il faut se contenter du fait que cela est en accord avec la liste des groupes simples et de leus ordres donnée par l'Atlas. Avec la mort de Daniel Gorenstein, qui va prendre en charge le projet de *révision*? Plus encore que de mener la classification à son terme, l'objectif de Gorenstein était de la rendre accessible à tout chercheur, même non expert en théorie des groupes.

§6. GROUPES RESOLUBLES ET REALISATIONS REGULIERES: Le théorème de Shafarevich énonce que tout groupe résoluble est groupe de Galois sur $\mathbb{Q}$. Mais en connaît-on des réalisations régulières? On ne le sait même pas pour les ℓ-groupes [Se; p. 9]. Le chapitre 2 de [Se] contient une preuve de ce que les ℓ-groupes sont groupes de Galois sur $\mathbb{Q}$. Serre poursuit ensuite de la façon suivante [Se; p. 17].

Proposition [Se; Prop. 2.2.4]: *Tout groupe résoluble G est quotient du produit semi-direct d'un groupe nilpotent par un groupe résoluble d'ordre strictement plus petit que $|G|$.*

Ce résultat pourrait figurer dans un cours d'algèbre de Licence. Le résultat suivant, attribué à Shafarevich, Serre ne l'énonce que comme assertion.

Assertion 2.2.5: *Tout problème de plongement scindé a une solution sur des corps de nombres.*

A partir de là, un raisonnement par récurrence montre que tout groupe résoluble peut être réalisé sur tout corps de nombres. Le chapitre se termine avec une preuve de l'Assertion 2.2.5 pour les problèmes de plongement scindés à noyau *abélien.* Là se conclut le point de vue de Serre. D'autres soutiennent que l'assertion a été démontrée dans sa totalité. En tout cas, cela montre que le cas des groupes résolubles n'est pas une partie de plaisir.

§**7. GROUPES DIEDRAUX:** Se pourrait-il que les groupes diédraux soient plus difficiles que, par exemple, le Monstre? Pour ce qui est des réalisations régulières, la réponse est "Oui!" Note: Un Monstre va seul faire face à une horde de groupes diédraux. Nous commençons par un exercice extrait du livre de Serre.

Exercice 1 p. 36: Montrer que $\mathbb{Z}_p$ n'est le groupe de Galois d'aucune extension régulière de $\mathbb{Q}(x)$. Rappel: L'ensemble $\mathbb{Z}_p$ des nombres p-adiques est un groupe pro-cyclique qui a des sous-groupes d'indice p^n pour tout entier n. **Solution:** Supposons le contraire. Alors le groupe quotient $\mathbb{Z}/p^n$ est groupe de Galois d'une sous-extension $L_n/\mathbb{Q}(x)$ de cette extension régulière. Parmi les générateurs de cette extension galoisienne, il doit y en avoir au moins un d'ordre p^n. Cela oblige la ramification de l'extension $L_n/\mathbb{Q}(x)$ à être d'ordre p^n en au moins une place. Considérons l'ensemble $\mathbf{C}$ des classes de conjugaison des générateurs des groupes d'inertie de cette extension. D'après l'argument des cycles de ramification (§3), $\mathbf{C}$ est une réunion rationnelle de classes de conjugaison.

Mais, dans un groupe abélien, chaque élément est le seul dans sa classe de conjugaison. Il y a donc au moins $p^n - p^{n-1}$ éléments d'ordre p^n dans $\mathbf{C}$. Or chaque point de ramification de $L_n/\mathbb{Q}(x)$ est également un point de ramification de $L_1/\mathbb{Q}(x)$. Ici L_1 est le corps fixé par le sous-groupe d'indice p du groupe de Galois. On obtient donc que le nombre des points de ramification n'est pas borné, ce qui est absurde.

Soit D_ℓ le *groupe diédral* de degré un nombre premier ℓ. C'est un groupe d'ordre 2ℓ, engendré par deux involutions. En utilisant des produits en couronne, on peut réaliser D_ℓ, pour ℓ premier, comme le groupe de Galois d'une *extension régulière* de $\mathbb{Q}(x)$. Cependant cette réalisation conduit à un revêtement ayant des éléments d'ordre ℓ comme générateurs des groupes d'inertie en les places ramifiées. Appliquons l'*argument des cycles de ramification* comme ci-dessus. Les éléments d'ordre ℓ constituent $(\ell-1)/2$ classes de conjugaison distintes de D_ℓ. Le nombre de points de ramification $L/\mathbb{Q}(x)$ doit être au moins égal à $(\ell-1)/2$.

Existe-t-il des réalisations de D_ℓ, pour *tout* ℓ, pour lesquelles, il n'y ait que des involutions comme cycles de ramification? Nous appelons cela une *réalisation avec involutions* de D_ℓ.

Théorème 1 [DFr; Theorem 5.1]: *Pour tout nombre premier $\ell > 7$, si D_ℓ est le groupe d'une extension régulière de $\mathbb{Q}(x)$, alors l'extension a au moins 6 points de ramification.*

Pour la plupart des cas, il suffit d'invoquer l'argument des cycles de ramification. Il reste un cas essentiel: il faut éliminer la possibilité de réaliser D_ℓ avec involutions avec seulement $r = 4$ points de ramification. Voici l'observation principale. Pour une telle réalisation $L/\mathbb{Q}(x)$, le corps L est un corps de fonctions de genre 1 dont le groupe de Picard contient un point d'ordre ℓ défini sur $\mathbb{Q}$. Il est classique que cela entraîne l'existence d'un point rationnel sur la courbe modulaire $X_1(\ell) \setminus \{\text{pointes}\}$. Comme $\ell > 7$, cela contredit le théorème de Mazur ([M] ou [Se2; Theorem 3]).

Il faut se rappeler qu'en comparaison, le Monstre, lui, est groupe de Galois d'une extension régulière de $\mathbb{Q}(x)$ ayant 3 points de ramification seulement. Nous conjecturons qu'il n'existe pas de borne uniforme pour le nombre de points de ramification nécessaire pour réaliser les groupes diédraux D_ℓ .

Conjecture 2: *Comme ci-dessus, ℓ décrit l'ensemble des nombres premiers impairs. Pour tout entier r_0, il n'existe qu'un nombre fini de groupes D_ℓ qui sont groupes de Galois d'une extension régulière $L/\mathbb{Q}(x)$ ayant au plus r_0 points de ramification.*

Supposons que r_0 contredise la conjecture. La preuve du Théorème 1 montre alors qu'il doit exister une réalisation avec involutions pour une infinité de groupes D_ℓ. On peut reformuler la Conjecture 2.

Conjecture 2': *Pour tout r_0, il n'existe qu'un nombre fini de groupes D_ℓ qui peuvent être réalisés avec involutions avec au plus r_0 points de ramification.*

Soit $L/\mathbb{Q}(x)$ une réalisation avec involutions de D_ℓ. Un automorphisme d'ordre ℓ fixe une extension $T/\mathbb{Q}(x)$ de degré 2 ayant un nombre (pair) r de points de ramification. C'est-à-dire, T est le corps de fonctions d'une courbe hyperelliptique de genre $\frac{r-2}{2}$. D'autre part, L/T est une extension cyclique non-ramifiée de degré ℓ.

Nous cherchons un revêtement $\varphi : \hat{X} \to \mathbb{P}^1$ de degré 2ℓ. Tous ses *cycles de ramification* $(\sigma_1, \ldots, \sigma_r)$ doivent être des involutions. Un calcul combinatoire du nombre de ces r-uplets est facile. On en déduit l'irréductibilité de *l'espace de Hurwitz* $\mathcal{H}(\mathbf{C}) = \mathcal{H}(r, \ell)$ qui paramètre les classes d'équivalence des revêtements cherchés.

La réciproque de l'argument des cycles de ramification (§3) montre qu'il existe un espace $\mathcal{H}(\mathbf{C})^{\text{in}} = \mathcal{H}(r, \ell)^{\text{in}}$, défini sur $\mathbb{Q}$, qui revêt $\mathcal{H}(r, \ell)$ [FrV]. Les points rationnels sur $\mathcal{H}(r, \ell)^{\text{in}}$ correspondent exactement aux réalisations avec involutions de D_ℓ. Notre problème consiste donc à décider si $\mathcal{H}(r, \ell)^{\text{in}}$ a des points $\mathbb{Q}$-rationnels. On peut relier l'espace $\mathcal{H}(r, \ell)^{\text{in}}$ à des objets plus classiques.

Prenons $\alpha \in D_\ell$ d'ordre ℓ. Formons le quotient $\hat{X}/\langle\alpha\rangle = Y$ de $\hat{X}$ par le groupe engendré par α. Le revêtement $Y \to \mathbb{P}^1$ de degré 2 présente Y comme une courbe hyperelliptique de genre $\frac{r-2}{2}$. De plus, $\hat{X}$ est un revêtement cyclique non-ramifié de Y. [DFr; Lemma 5.3] interprète l'existence de $\hat{X}$ comme une propriété de $\mathrm{Pic}^0(Y)$, *i.e.*, de la Jacobienne de Y. Désignons l'ensemble des points d'ordre ℓ sur $\mathrm{Pic}^0(Y)$ par $T_\ell = T_\ell(Y)$. Le groupe $G(\overline{\mathbb{Q}}/\mathbb{Q}) = G_\mathbb{Q}$ agit sur T_ℓ. Si $\boldsymbol{p} \in T_\ell \setminus \{0\}$ est un point $\mathbb{Q}$-rationnel, alors l'action de $G(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $< \boldsymbol{p} >$ est triviale. Quand un point a cette propriété, désignons le groupe qu'il engendre par $\mathbb{Z}/\ell$. Cela signifie que $G_\mathbb{Q}$ a une action triviale dessus.

Semblablement, $G_\mathbb{Q}$ agit sur les racines ℓ-ièmes de l'unité. C'est une autre copie de $\mathbb{Z}/\ell$, mais pour indiquer que $G_\mathbb{Q}$ a une action non triviale dessus, désignons la par μ_ℓ. Considérons l'ensemble $G_\ell(d)$, où $d = \frac{r-2}{2}$, des réalisations avec involutions de D_ℓ, avec, comme ci-dessus, r points de ramification, et définies sur $\mathbb{Q}$. Soit $\mathrm{Pic}^1(Y)$ l'ensemble des classes de diviseurs de degré 1 sur Y.

Lemme: *L'ensemble des réalisations avec involutions de D_ℓ avec Y comme ci-dessus fixé correspond à un certain sous-ensemble d'injections $G_\mathbb{Q}$-équivariantes de μ_ℓ dans $T_\ell(Y)$. L'image contient toutes les injections $G_\mathbb{Q}$-équivariantes de μ_ℓ dans $T_\ell(Y)$ quand* $\mathrm{Pic}^1(Y)$ *a un point $\mathbb{Q}$-rationnel.*

Cela nous place dans le territoire de [KM]. En fait, la Conjecture $2'$ est plus forte à beaucoup d'égards que les conjectures bornant, pour chaque entier d, la torsion sur F avec $[F : \mathbb{Q}] = d$ sur toutes les courbes elliptiques définies sur $\mathbb{Q}$.

Problème: *Pour ℓ fixé et r grand, est-ce que les espaces de Hurwitz $\mathcal{H}(r,\ell)^{\mathrm{in}}$ sont unirationnels?*

Une réponse affirmative entraînerait ceci. Pour r suffisamment grand, les réalisations avec involutions de D_ℓ avec r points de ramification correspondraient aux points d'une variété unirationnelle. Une variété W est unirationnelle si elle est l'image d'un espace projectif de dimension t pour un certain t. Si W et la flèche provenant de cet espace projectif ont des équations à coefficients dans $\mathbb{Q}$, on dit que W est unirationnelle sur $\mathbb{Q}$. Un espace projectif possède un ensemble dense de points rationnels. Il en serait donc de même pour W. On obtiendrait ainsi des réalisations avec involutions de D_ℓ. On ne connaît même pas, pour tout ℓ, seulement *une*, réalisation avec involutions de D_ℓ.

Voici un analogue du problème de [Se] sur l'absence de réalisations régulières de $\mathbb{Z}_p$. Fixons un nombre premier ℓ et formons la limite projective D_{ℓ^∞} des groupes D_{ℓ^n}. Peut-il exister une réalisation régulière de D_{ℓ^∞}? Premier point: Cela serait une réalisation avec involutions de D_{ℓ^∞}.

Le noyau $\mathbb{Z}_\ell$ du $\mathbb{Z}/2$-quotient de D_{ℓ^∞} correspond à une extension $L/\mathbb{Q}(x)$ de degré 2. Supposons que la réalisation de D_{ℓ^∞} soit ramifiée au-dessus de L. En une place ramifiée, le groupe d'inertie est un sous-groupe cyclique C d'indice fini de $\mathbb{Z}_\ell$. Considérons le point de ramification de $\mathbb{Q}(x)$ ayant C comme groupe d'inertie dans l'extension totale. Pour chaque entier m, il existe une extension régulière $L_m/\mathbb{Q}(x)$ où le groupe d'inertie au-dessus de ce point de ramification est d'ordre ℓ^m. Utilisons l'argument des cycles de ramification. Cette extension a au moins $(\ell^m - \ell^{m-1})/2$ points de ramification. Comme chacun de ces points est aussi un point de ramification de $L_1/\mathbb{Q}(x)$, on obtient une contradiction. Une réalisation régulière de D_{ℓ^∞} est donc une réalisation avec involutions.

On peut conclure que pour chaque n, la Jacobienne A de L est isogène à une variété B_n avec un point $\mathbb{Q}$-rationnel d'ordre ℓ^n. Utilisons maintenant l'appendice de Ribet dans [KL]. On obtient une contradiction en regardant la réduction modulo p. Choisissons un premier $p \neq \ell$ où A a bonne réduction. Comme A et B_n sont isogènes, leurs réductions ont le même nombre de points sur $\mathbb{F}_p$. Donc ℓ^n divise le nombre de points sur A mod p. Comme le nombre de points sur A est fini, on obtient une contradiction en prenant n grand.

Conclusion: *Il n'existe pas de réalisations régulières de D_{ℓ^∞} sur $\mathbb{Q}(x)$.*

Nous terminons par quelques commentaires où nous allons utiliser cette conclusion pour faire le lien avec d'autres questions abordées dans [Se].

§**8. ET APRES LES GROUPES SIMPLES?:** Chaque groupe fini G possède une infinité d'extensions totalement non-scindées par des groupes finis. Elles forment un système projectif dont la limite est un groupe profini *projectif* $\tilde{G}$. Les quotients de $\tilde{G}$ compris entre $\tilde{G}$ et G sont les extensions totalement non-scindées de G. Le noyau de la flèche naturelle $\tilde{G} \to G$ est un groupe pro-nilpotent dont l'ordre est un entier (supernaturel) dont les diviseurs sont les nombres premiers divisant $|G|$. Le groupe $\tilde{G}$ est le *revêtement universel de Frattini* de G [FrJ; Chap. 21]. Un groupe profini projectif n'a *aucun* élément d'ordre fini. Cela donne une idée du nombre de ces revêtements.

Pour chaque nombre premier ℓ divisant l'ordre de G, il y a une variante $\tilde{G}_\ell$ de $\tilde{G}$. Quand $G = D_\ell$, alors $\tilde{G}_\ell$ est D_{ℓ^∞}. Même quand G est le groupe alterné A_5 de degré 5, et $\ell = 2$, $\tilde{G}_2$ n'est pas connu. Pour résoudre le problème inverse de la théorie de Galois, il faudra bien réaliser tous les quotients of $\tilde{A}_5$ comme groupes de Galois. Cela ne peut venir que d'une technique un tant soit peu abstraite.

Une partie de ce problème est considérée dans le chapitre 9 (le dernier) de [Se]. Supposons que l'on dispose d'une réalisation régulière $L_n/\mathbb{Q}(x)$ de A_n. On peut alors chercher une réalisation régulière du revêtement spinoriel $\hat{A}_n$ de A_n, qui étende la réalisation $L_n/\mathbb{Q}(x)$. L'extension non-scindée $\hat{A}_n \to A_n$ a pour noyau une copie de $\mathbb{Z}/2$ contenue dans le centre de $\hat{A}_n$. Le livre se termine sur des exercices inspirés de [Me] qui conduisent à une telle réalisation. Serre dit que les groupes simples ne sont pas toute la question. Cela ne considère qu'un petit quotient bien connu de $\tilde{A}_n$.

Les corps cyclotomiques ont les propriétés d'être hilbertien et d'avoir un groupe de Galois absolu projectif. [FrV2] conjecture que ces deux seules propriétés suffisent pour entraîner la conclusion de la conjecture de Shafarevich (§0).

Conjecture: *Si $K \subset \overline{\mathbb{Q}}$ est hilbertien et si G_K est projectif, alors G_K est un groupe profini libre.*

[FrV2] établit cette conjecture sous une condition plus forte que la projectivité. En voici deux corollaires. Le premier: $G_{\mathbb{Q}}$ est une extension du groupe $\prod_{n=1}^{\infty} S_n$, produit de tous les groupes symétriques, par le groupe profini libre (à un nombre dénombrable de générateurs). Le second: Toute extension non réelle du *corps des nombres algébriques totalement réels* a comme groupe de Galois absolu un groupe profini libre. Pour démontrer ces résultats on utilise la réciproque de l'argument des cycles de ramification dans toute sa force: elle permet de résoudre des problèmes de plongement sur de gros sous-corps de $\overline{\mathbb{Q}}$. C'est bien de ce type d'arguments où les problèmes de plongement occupent une place centrale, que l'on aimerait voir découler une solution du problème inverse de la théorie de Galois.

En conclusion, [Se] fait le tour d'un domaine très actif utilisant des outils modernes et prometteurs et dont on peut penser qu'il connaitra prochainement de nouveaux progrès. Il semble bien à propos de conclure par cette déclaration de Serre: "Le problème inverse de la théorie de Galois nous fournit un prétexte pour apprendre beaucoup de nouvelles Mathématiques [Se3]."

BIBLIOGRAPHIE:

[At] Atlas, J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, Atlas of finite groups: maximal subgroups and ordinary characters for simple groups, *Clarendon Press, New York* (1985).

[B] G. V. Belyi, On extensions of the maximal cyclotomic field having a given classical group, *J. Crelle* **341** (1983), 147–156.

[DFr] P. Debes and M. Fried, Nonrigid situations in constructive Galois theory, *Pacific Journal* (1993), 36 page preprint.

[Fr] M. Fried, Fields of Definition of Function Fields and Hurwitz Families and; Groups as Galois Groups, *Communications in Algebra* **5** (1977), 17–82.

[FrJ] M. Fried and M. Jarden, Field Arithmetic, *Springer Ergebnisse series***Vol 11** (1986).

[FrV] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, *Math. Annalen* **290** (1991), 771–800.

[FrV2] M. Fried and H. Völklein, The embedding problem over an Hilbertian-PAC field, *Annals of Math* **135** (1992), 1–13.

[KM] S. Kamienny and B. Mazur, Rational torsion of prime order in elliptic curves over number fields, preprint 6/92, to appear in Asterisque, Columbia University Number Theory Seminar 1992

[KL] N. Katz and S. Lang, Torsion points on abelian varieties in cyclotomic extensions, *Enseignement Mathematique* **27** (1981), K. Ribet's appendix.

[M] B. Mazur, Rational points on modular curves, *Lecture Notes in Math., Springer-Verlag* **601** (1977), 107–148.

[Ma] B. H. Matzat, Konstructive Galoistheorie, *Lect. Notes in Math.* **1284** (1987) Springer-Verlag.

[Mal] G. Malle, Exceptional groups of Lie type as Galois groups, *J. Crelle* **392** (1988), 70–109.

[Me] J.-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$, *J. Alg.* **131** (1990), 483–495.

[Se2] J.-P. Serre, Points rationnels des courbes modulaires, *Séminaire Bourbaki, 30ème année* **n• 511** (1977/78).

[Se3] J.-P. Serre, Conversation at Walter Feit's Birthday Celebration at Oxford in April, 1990.

[Sh] I. R. Shafarevich, The embedding problem for split extensions, *Dokl. Akad. Nauk SSSR* **120** ((1958), 1217–1219.

[S] K. Shih, On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), 99–120.

[Th] J. G. Thompson, Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$, *KJ. Alg.* **89** (1984), 437–499.

[V1] H. Völklein, $\mathrm{GL}_n(q)$ as Galois group over the rationals, *Math. Ann.* **293** (1992), 163–176.

[V2] H. Völklein, Braid group action, embedding problems and the groups $\mathrm{PGL}_n(q)$, $\mathrm{PU}_n(q^2)$, *Forum Math.*, to appear.

Michael Fried
Math Dept: UC Irvine
Home Phone: 714-854-3634
e-mail: mfried@math.uci.edu