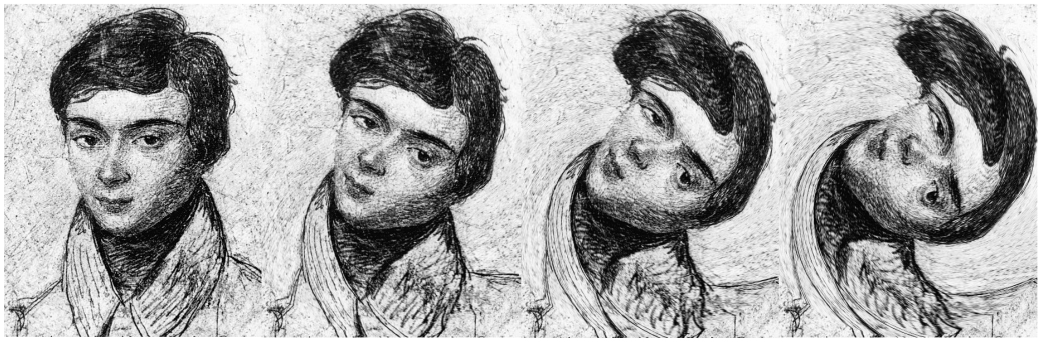

TIGaNoCo

Théorie Inverse de Galois Non Commutative

Projet financé par l'Union européenne dans le cadre du programme opérationnel FEDER/ FSE

Objectifs de recherche

La Théorie Inverse de Galois trouve son origine avec le problème de Hilbert–Noether qui demande s'il est vrai que tout groupe fini se réalise comme le groupe de Galois d'une extension galoisienne du corps des rationnels. Ce problème, toujours ouvert aujourd'hui, a engendré une forte activité mathématique, au point que la théorie est maintenant clairement reconnue comme théorie à part entière. Depuis les années 2000, la classification AMS lui a même réservé un code, le 12F12, témoignant ainsi de son importance. La théorie fédère un nombre substantiel de mathématiciens, sur trois générations actives à travers le monde, et est toujours très prolifique. Les principaux pays concernés sont la France (Caen, Grenoble, Lille, Paris), Israël (Beer-Sheva, Haïfa, Ra'anana, Tel-Aviv), l'Allemagne (Bayreuth, Dresde, Würzburg), le Luxembourg, l'Espagne (Barcelone, Séville), les États-Unis (Philadelphie par exemple), la Corée du Sud (Daejeon) et l'Angleterre (Oxford). La théorie puise ses idées dans deux principaux domaines : la géométrie arithmétique (avec l'interprétation du problème en terme de revêtements de la droite projective) et l'arithmétique des groupes profinis (description du groupe de Galois absolu d'un corps et de ses sous-groupes fermés). Elle a connu ces 40 dernières années de grands succès et a permis une bien meilleure compréhension de la nature galoisienne. Nous renvoyons aux livres [Ser], [Vol], [FJ], [MM] et aux articles de survol [DD1], [Deb1] pour un panorama de la théorie.

Le premier problème général de la théorie est le

Problème Inverse de Galois sur le corps k ($\mathbf{PIG}_k$) : *Tout groupe fini se réalise t-il comme le groupe de Galois d'une extension galoisienne de k ?*

On remarquera que ce problème prend un sens dès que l'on possède une notion d'extension galoisienne de corps. Or, il existe bel et bien une théorie de Galois générale qui inclut le cas des corps gauches, théorie où l'on retrouve tous les éléments de la théorie dans le cas commutatif (correspondances galoisiennes par exemple). Dans le cas général, la notion d'extension galoisienne est celle donnée par Artin : une extension H/k est dite *galoisienne* si le corps des invariants de H par l'action de $\mathrm{Aut}(H/k)$ est égal à k. Nous renvoyons au livre [Coh] pour un panorama de cette théorie.

Dans le cas des corps gauches, la présence d'automorphismes intérieurs perturbe un peu les choses et l'on peut obtenir des situations surprenantes. Par exemple, dans le travail [Des2], il est construit une extension galoisienne H/k de groupe fini G et telle que $[H:K] < |G|$... On trouvera dans l'article [Des1] la preuve du fait que le corps des nombres complexes ne possède pour extensions finies que des extensions de degré 2 et que les classes d'isomorphismes de ces extensions sont en nombre infini. Ainsi, on voit que la notion de compositum d'extensions finies d'un corps gauche est à manipuler avec beaucoup plus de précautions que dans le cas commutatif. La principale difficulté dans le cas non commutatif est que la notion de polynôme, et donc d'élément algébrique, n'a pas de sens inné. Bien sûr, il existe des constructions d'anneaux de polynômes, mais les applications d'évaluation ne sont alors plus des morphismes et toute tentative d'approche de la théorie de Galois au moyen de la séparabilité/normalité devient ainsi vaine. La théorie de Galois des corps gauches s'entend uniquement par actions galoisiennes, ce qui rend les choses bien plus compliquées.

Jusqu'à très récemment, personne ne s'était aventuré dans cette forêt des corps gauches du point de vue de la théorie inverse de Galois. Dans le travail [DL] qui paraîtra prochainement, B. Deschamps et F. Legrand montrent qu'une promenade dans cette forêt peut être très fructueuse. Plus précisément, ils s'intéressent aux corps de fractions tordus à indéterminée centrale. Etant donné un corps gauche H, le corps $H(t)$ de fractions tordu à indéterminée centrale et à coefficients dans H est le corps de fractions de l'anneau de polynômes tordu de Ore $H[t] = H[t,\alpha,\delta]$ où α est l'automorphisme identité et δ la dérivation nulle (voir [Ore]). Moralement, dans $H[t]$, l'indéterminée t commute avec tout le monde. Le résultat principal de l'article [DL] est le

Théorème.— *Si H désigne un corps de dimension finie sur son centre k et si k contient un corps ample, alors le $\mathbf{PIG}_{H(t)}$ admet une réponse positive.*

La notion de corps ample fut introduite par F. Pop dans les années 90 pour résoudre un certain nombre de questions de théorie inverse de Galois, il s'agit là d'une notion centrale du domaine (voir [Pop1], [Jar], [Pop2]). Ce théorème s'applique notamment au corps $H = \mathbb{H}$ des quaternions d'Hamilton. La stratégie mise en oeuvre pour démontrer ce théorème ouvre de nombreuses perspectives et ce sont ces perspectives qui constituent le coeur de ce projet de recherche.

Le projet que nous présentons ici est résolument précurseur, puisque personne ne s'est jamais penché sur l'aspect non commutatif de la théorie inverse de Galois. Le fait que de premiers résultats sur ces questions soient publiés montre que cet aspect n'est pas du tout fantaisiste. Enfin, de par la forme parlante des résultats déjà obtenus (par exemple, le fait que le problème inverse de Galois possède une réponse positive sur le corps $\mathbb{H}(t)$) et ceux escomptés, il y a fort à parier que cette nouvelle branche de la théorie inverse de Galois intéressera beaucoup de mathématiciens à l'avenir.

Parmi les pistes à étudier, il conviendra de s'intéresser plus particulièrement aux questions suivantes, dont chacune constituera une tâche dans le programme.

A/ **f-hilbertianité.** Le théorème d'irréductibilité de Hilbert sur la conservation de l'irréductibilité de polynômes à coefficients dans $\mathbb{Q}$ par spécialisation joue un rôle fondamental en théorie inverse de Galois. Il permet notamment de passer du problème inverse de Galois sur un corps de fractions $k(t)$ au problème inverse de Galois sur le corps des constantes k lui-même. Il est d'ailleurs conjecturé que la propriété d'hilbertianité (i.e. le fait qu'un corps k satisfasse au théorème d'irréductibilité de Hilbert) est suffisante pour assurer une réponse positive au problème inverse de Galois sur k (voir [DD1]). L'article [DL] montre qu'en dépit du fait que le théorème d'irréductibilité de Hilbert n'a a priori aucun sens pour un corps gauche, la notion d'hilbertianité reste centrale pour l'étude de l'implication $\mathbf{PIG}_{H(t)} \Longrightarrow \mathbf{PIG}_H$ dans le cas des corps gauches. Sans trop rentrer dans le détail, voilà en quelques mots la notion de f-hilbertianité qui va rentrer en jeu et qu'il conviendra d'étudier.

Etant donné un corps gauche H de dimension finie sur son centre k, on peut associer à l'extension H/k une k-forme f relativement à la norme réduite de cette extension. Si G est groupe de Galois sur $H(t)$, on peut alors considérer un certain polynôme irréductible $P(t,X) \in k(t)[X]$ dont le corps de décomposition L sur $k(t)$ est une extension galoisienne de $k(t)$ de groupe G et qui jouit de la propriété suivante : la forme f ne possède que le zéro trivial sur L. S'il existe des spécialisations

$t = t_0 \in k$ telles que le polynôme $P(t_0, X) \in k[X]$ reste irréductible sur k <u>et</u> telles que la forme f ne possède que le zéro trivial sur le corps de décomposition de $P(t_0, X)$ sur k, alors G est groupe de Galois sur H. La *f-hilbertianité* est la propriété que le corps k a de vérifier cette qualité pour tout polynôme irréductible $P(t, X)$.

Donnons un exemple simple, mais déjà instructif, pour illustrer la difficulté du passage hilbertien $\longrightarrow$ f-hilbertien : le corps $\mathbb{H}_k$ des quaternions sur un corps commutatif k de niveau au moins 4. La forme f à considérer ici est la forme quadratique

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Si l'on considère le polynôme $P(t, X) = X^2 - t$, on voit que f ne possède aucun zéro non trivial sur le corps de décomposition $k(\sqrt{t})$ de $X^2 - t$ sur $k(t)$. Les bonnes spécialisations de t pour l'hilbertianité sont les $t_0 \in k$ qui ne sont pas des carrés dans k. Pour la f-hilbertianité, les spécialisations acceptables sont les $t_0 \in k$ qui ne sont pas des carrés dans k <u>et</u> pour lesquels le corps $k(\sqrt{t_0})$ possède un niveau ≥ 4. On voit donc sur cet exemple simple que la notion de f-hilbertianité est liée à l'anisotropie de la forme quadratique f sur les extensions quadratiques de k, et est donc en lien avec la validité d'éventuels principes "local-global" sur ces corps.

Il conviendra d'étudier dans cette partie du programme de recherche d'éventuels analogues de résultats sur les corps hilbertiens. Par exemple, pour quel type de forme f les corps de nombres sont-ils f-hilbertiens ? A t-on des théorèmes de transition du genre "k est f-hilbertien $\Longrightarrow$ L est f-hilbertien pour toute extension finie séparable L/k", ou encore un théorème de Weissauer : toute extension finie séparable stricte d'une extension galoisienne d'un corps f-hilbertien est-elle un corps f-hilbertien ? Existe-t-il des ensembles universels de Hilbert pour la f-hilbertianité ?

Par ailleurs, la notion de f-spécialisation évoquée ci-dessus permet de définir des analogues de questions portant sur les spécialisations déjà étudiées dans le cas commutatif. On peut par exemple citer le *problème de Beckmann-Black* (voir [Bec], [Bla], [Deb2]) ou la notion plus récente d'*extension paramétrique* (voir [Leg], [Deb3], [KL]). Comme pour les éventuels résultats sur les corps f-hilbertiens évoqués ci-dessus, l'on envisage d'étudier ces variantes et d'obtenir d'éventuels analogues des résultats existant dans le cas commutatif. Par exemple, le problème de Beckmann-Black pour les groupes abéliens admet-il une réponse positive sur n'importe quel corps gauche de dimension finie sur son centre ? Ou encore : existe t-il des groupes finis G et des corps gauches H de dimension finie sur leurs centres k tels que k soit un corps de nombres et tels qu'aucune extension galoisienne de $H(t)$ de groupe G ne soit paramétrique ?

B/ **ψ-liberté.** Au début des années 2000, P. Dèbes et B. Deschamps ont introduit dans l'article [DD2] la notion de corps *ψ-libre* : il s'agit des corps qui possèdent tous les groupes profinis de rang dénombrable pour groupes de Galois, c'est-à-dire les corps qui satisfont au problème inverse de Galois lorsque l'on remplace l'hypothèse "groupe fini" par "groupe profini de rang dénombrable". S'il est conjecturé que le corps $\mathbb{Q}$ satisfait au PIG, ce dernier n'est certainement pas ψ-libre (la théorie d'Iwasawa montrant, par exemple, que $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ n'est pas groupe de Galois sur $\mathbb{Q}$). Dans le travail [DD2], il est montré que, si k désigne un corps hensélien, alors le corps $k(t)$ est ψ-libre. La preuve repose sur une astucieuse construction de tours d'extensions galoisiennes à contraintes de ramification fixées. Cette notion de ψ-liberté a un sens dans le cas des corps gauches. En combinant les résultats de [DD2] et [DL], il semble possible d'envisager le résultat suivant : si H désigne un corps de dimension finie sur son centre k et si k est hensélien, alors le corps $H(t)$ est ψ-libre (par exemple, $\mathbb{H}(t)$ serait ψ-libre). Cette voie constitue le coeur du travail de recherche de la thèse d'Angelot Behajaina (étudiant en deuxième année de thèse sous la direction de B. Deschamps et F. Legrand) et est très prometteuse. Si elle aboutit, elle constituera l'extension naturelle au cas profini du cas fini traité dans [DL].

C/ **Problèmes de plongement.** La notion de problème de plongement joue un rôle capital en théorie inverse de Galois. Rappelons brièvement de quoi il s'agit. On se donne un groupe profini Γ, deux groupes finis G et H, et deux épimorphismes π et φ

$$\begin{tikzcd} & \Gamma \arrow[dl, "?"'] \arrow[d, "\pi"] \\ G \arrow[r, "\varphi"'] & H \end{tikzcd}$$

et l'on cherche à savoir s'il existe un morphisme $\Gamma \longrightarrow G$ qui fasse commuter le diagramme. Lorsque c'est le cas pour tous G, H, π et φ, le groupe Γ est dit *projectif* (notion qui est en fait caractérisée par le fait que sa dimension cohomologique soit ≤ 1). Si l'on peut à chaque fois choisir $\Gamma \longrightarrow G$ surjectif, alors Γ est dit *ω-libre* (un profond théorème du à Iwasawa montre que, lorsque Γ est de rang dénombrable, cette propriété équivaut à être prolibre).

Du point de vue galoisien, on peut considérer, pour un corps commutatif k donné, le groupe de Galois absolu $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ de k. Un problème de plongement revient donc à se donner un épimorphisme $\alpha : G \to \mathrm{Gal}(L/k)$, où G désigne un groupe fini et L/k une extension galoisienne, et à trouver une extension galoisienne M/k et un isomorphisme $\beta : \mathrm{Gal}(M/k) \to G$ tels que $L \subset M$ et $\alpha \circ \beta$ soit l'application de restriction $\mathrm{Gal}(M/k) \to \mathrm{Gal}(L/k)$:

$$\begin{tikzcd} M \arrow[d, dash, dashed] \arrow[dd, dash, dashed, bend left=60, "G"] \\ L \arrow[d, dash] \\ k \end{tikzcd}$$

Dans le cas des corps gauches, la notion de groupe de Galois absolu n'a pas de sens, mais la notion de problème de plongement, telle que l'on vient de la traduire en termes galoisiens, en a un et est particulièrement intéressante, notamment en raison du théorème d'Iwasawa rappelé plus haut. Le cas qui nous intéressera en premier lieu est celui des corps gauches de dimensions finies sur leurs centres, puisqu'il permettra d'utiliser les résultats de [DL]. De jolies choses pourraient bien être montrées, en particulier en relation avec la tâche B : on s'attend à pouvoir donner des exemples de corps gauches ψ-libres qui ne pourraient être abordés avec les idées développées dans [DD2]. Un autre résultat envisagé ici, et qui constituerait une autre généralisation du résultat principal de l'article [DL], est le suivant : étant donné un corps H de dimension finie sur son centre k, si k est ample, alors tout problème de plongement fini scindé et constant sur $H(t)$ admet une solution.

D/ **Arithmétique des corps de dimensions infinies sur leurs centres.** Il s'agit là de la question la plus prospective de ce programme de recherche. Les résultats déjà obtenus ainsi que les questions précédentes se situent tous dans le cadre d'un corps gauche H de dimension finie sur son centre k, avec pour application le corps $H(t)$ des fractions tordu à indéterminée centrale. L'hypothèse d'être de dimension finie sur son centre est cruciale dans la méthode développée pour aborder les tâches A, B et C. Dans la tâche D, on s'intéressera à deux situations qui ne rentrent pas dans ce contexte :

a) Un des points techniques utilisés dans les preuves est que le centre de $H(t)$ est précisément $k(t)$ et que dès lors, le corps $H(t)$ est de dimension finie sur son centre. La question naturelle est de savoir si les résultats persistent sur d'autres corps de fractions tordus. Plus précisément, on se donne un anneau de polynômes tordu de Ore $H[t, \alpha, \delta]$, H étant un corps (éventuellement de dimension finie sur son centre, voire même simplement commutatif), $\alpha \in \mathrm{Aut}(H)$ un automorphisme et δ une α-dérivation du corps H. On travaille alors sur le corps de fractions $H(t, \alpha, \delta)$ de l'anneau $H[t, \alpha, \delta]$ et l'on se demande s'il existe une condition sur H (du genre de celle présente dans le cas de l'indéterminée centrale) pour que le $\mathbf{PIG}_{H(t,\alpha,\delta)}$ admette une réponse positive. Ici, les méthodes précédentes ne marchent plus dès que $\alpha \neq \mathrm{Id}$ puisque, dans ces circonstances, le corps $H(t, \alpha, \delta)$ n'est plus une algèbre simple centrale. Si le cas $\delta \neq 0$ semble assez inaccessible, on peut espérer obtenir des résultats significatifs dans le cas des corps $H(t,\alpha) = H(t,\alpha,0)$, en particulier pour la description du groupe $\mathrm{Aut}(H(t,\alpha)/k)$ (dont on sait que, lorsque le corps $H = k$ est commutatif infini et α=Id, il est isomorphe au groupe $\mathrm{PGL}_2(k)$). Un autre champ d'investigation pour ces corps de fractions tordus sera de donner l'analogue de la méthode de Noether pour des corps de fractions itérés $H(t_1,\dots,t_n,\alpha_1,\dots,\alpha_n)$. Une première étude de cette question a déjà été faite dans [Des1], dans une situation simple.

b) La théorie du groupe de Brauer permet de décrire, à corps commutatif k fixé, l'ensemble des corps gauches de centre k et de dimension finie sur k. Puisque l'on sait aborder la problématique inverse de Galois sur ces corps, on s'intéressera à des extensions L/k filtrées par ces corps. Plus précisément, on considèrera une suite croissante $k \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$ où chaque L_n est une k-algèbre simple centrale et le corps $L = \bigcup_n L_n$. Sous certaines hypothèses sur k, on tentera de déduire des informations galoisiennes sur L. La première étape consistera à bien comprendre comment l'inclusion $L_n \subset L_{n+1}$ peut s'interpréter dans le groupe de Brauer de k.

Il convient de signaler pour finir ce paragraphe que, publicité des premiers résultats de cette nouvelle théorie ayant été faite lors des XXIXèmes Rencontres Arithmétiques de Caen à Tatihou en 2019, plusieurs mathématiciens ont signalé leur intérêt pour ces questions. C'est notamment le cas d'Elad Paran (The Open University of Israel) et Pierre Dèbes (Université de Lille) qui souhaitent vivement collaborer à ce programme (voir leurs lettres d'intention jointes en annexe) et qui seront associés comme partenaire au projet. Un travail en commun avec Paran a d'ailleurs déjà débuté : dans une note qu'il a écrite, il remarque très astucieusement que le corps des fractions $H(x)$ de l'anneau des fonctions polynomiales (fonctions de H dans H qui s'écrivent comme sommes de produits non commutatifs de constantes et de puissances de la variable x, par exemple $f(x) = ax + xb + ux^2vxwx$) à coefficients dans un corps gauche H de dimension finie sur son centre k est en fait isomorphe à un corps de fractions tordu $H(t_1,\dots,t_n)$ en n variables et à indéterminées centrales. La conséquence de cette observation est que, d'après [DL], si k contient un corps ample, alors le $\mathbf{PIG}_{H(x)}$ admet une réponse positive. Pierre Dèbes est quant à lui un spécialiste des questions hilbertiennes et nous allons initier une collaboration avec lui sur la question de la f-hilbertianité.

Bibliographie

[Bec] Sybilla Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?* J. Algebra, 164(2): p.430-451, 1994.

[Bla] Elena V. Black, *Aritmetical lifting of dihedral extensions*. J. Algebra, 203(1): p.12-29, 1998.

[Coh] Paul Moritz Cohn, *Skew fields. Theory of general division rings*. Encyclopedia of Mathematicsand its Applications, 57. Cambridge University Press, Cambridge, 1995.

[Deb1] Pierre Dèbes, *Théorie de Galois et géométrie : une introduction*. Dans "Arithmétique des revêtements algébriques" (Saint-Étienne, 2001), Sémin. Congr. Vol. 5, pages 1-26. Soc.Math. France, Paris, 2001. Editeur : Bruno Deschamps.

[Deb2] Pierre Dèbes, *Galois covers with prescribed fibers: the Beckmann-Black problem*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), 28(2): p.273-286, 1999.

[Deb3] Pierre Dèbes, *Groups with no parametric Galois realizations*. Ann. Sci. Éc. Norm. Supér. (4), 51(1): p.143-179, 2018.

[DD1] Pierre Dèbes et Bruno Deschamps, *The regular inverse Galois problem over large fields*. Geometric Galois actions. 2. The inverse Galois problem, moduli spaces and mapping class groups. Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 243, 119-138, 1997. Schneps, Leila (ed.) et al.

[DD2] Pierre Dèbes et Bruno Deschamps, *Corps ψ-libre et théorie inverse de Galois infinie*, Journal für die Reine und Angewandte Mathematik, 574, 197-218, 2004.

[Des1] Bruno Deschamps, *A propos d'un théorème de Frobenius*. Annales Mathématiques Blaise Pascal, 8-2, 61-66, 2001.

[Des2] Bruno Deschamps, *Des extensions plus petites que leurs groupes de Galois*. Communications in Algebra, 46-10, 4555-4560, 2018.

[Des3] Bruno Deschamps, *Une introduction au groupe de Brauer*. Manuscrit pour un groupe de travail donné à Caen en 2012. http://perso.univ-lemans.fr/~bdesch/BrauerCaen.pdf

[DL] Bruno Deschamps et François Legrand, *Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale*, à paraître, Journal of Pure and Applied Algebra, 2019.

[FJ] Michael D. Fried and Moshe Jarden, *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete.3.Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[Jar] Moshe Jarden, *Algebraic patching*. Springer Monographs in Mathematics. Springer, Heidel-berg, 2011.

[KL] Joachim König and François Legrand, *Non-parametric sets of regular realizations over number fields*. J. Algebra, 497, p.302-336, 2018.

[Leg] François Legrand, *Parametric Galois extensions*. J. Algebra, 422, p.187-222, 2015.

[Ore] Oystein Ore, *Theory of non-commutative polynomials*. Annals of Mathematic (2), 34 (3), 480-508, 1933.

[MM] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*. Springer Monographs in Mathematics. Springer, Berlin, 2018.

[Pop1] Florian Pop, *Embedding problems over large fields*. Annals of Mathematic (2), 144(1), 1-34, 1996.

[Pop2] Florian Pop, *Little survey on large fields - old & new*. Valuation theory in interaction, EMS Ser. Congr. Rep., 432-463. Eur. Math. Soc., Zürich, 2014.

[Ser] Jean-Pierre Serre, *Topics in Galois Theory*, volume 1 of Research Notes in Mathematics. Jones and Bartlett Publishers, Boston, MA, 1992.

[Vol] Helmut Völklein, *Groups as Galois groups. An introduction*, volume 53 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1996.