Domaines de Recherche

Mon domaine de recherche mathématique concerne l'arithmétique des corps et des revêtements, la théorie de Galois et la théorie inverse, l'arithmétique des groupes profinis, la cohomologie galoisienne, l'arithmétique des corps gauches et la théorie additive des nombres.

a.— *Théorie inverse de Galois, géométrie-arithmétique.* Mots clés : *Problème Inverse de Galois, arithmétique des revêtements algébriques, espace de Hurwitz, arithmétique des groupes profinis.*

Il s'agit de mon domaine originel de recherche. La théorie inverse de Galois a pour objectif de regarder la possibilité de réaliser des groupes (pro)finis comme groupes de Galois sur des corps fixés. Plus généralement, l'objectif est de mieux comprendre la structure arithmétique des groupes de Galois absolus (i.e. des groupes de Galois d'extensions galoisiennes maximales). L'approche moderne à ce problème utilise la géométrie arithmétique, en particulier, la théorie des revêtements algébriques.

Après avoir travaillé sur la théorie des espaces de modules de revêtements (espaces d'Hurwitz) pendant ma thèse sous la direction de Pierre Dèbes, j'ai obtenu plusieurs résultats de théorie inverse de Galois (voir 1/ et 2/) sur ce sujet. En particulier, j'ai montré que pour un groupe fini donné il existe des espaces de Hurwitz paramétrés par G et possédant pour tout p des points $\mathbb{Q}_p$-rationnels (rappelons à ce sujet que l'existence d'un point $\mathbb{Q}$-rationnel assure la réalisation du groupe comme groupe de Galois sur $\mathbb{Q}$). Il convient de signaler que dans l'article 2/ a été énoncé une conjecture maintenant appelée internationalement " Conjecture de Dèbes-Deschamps " et qui constitue la conjecture la plus générale (et donc la plus risquée) du domaine puisqu'elle contient plusieurs des plus fameuses conjectures (Shafarevich, Fried-Volklein, PIG et PIGR etc.). Cette conjecture est régulièrement citée et elle a même été le sujet d'un programme de recherche israélo-américain.

Un autre important travail sur ce sujet est une collaboration avec P. Dèbes. Il s'agit de l'article 9/ dans lequel nous introduisons une nouvelle notion : celle de corps ψ-libre. L'idée fut d'utiliser les méthodes existantes pour la construction de revêtements à paramètres arithmétiques fixés (groupe de Galois, ramification etc.) et de les appliquer à la construction de tours infinies cohérentes de revêtements. Ces constructions permettent de réaliser sur certains corps, le groupe profini libre de rang dénombrable $\widehat{F}_\omega$ comme groupe de Galois (c'est ce que nous appelons être ψ-libre). En particulier, nous montrons que si k est un corps valué hensélien de caractéristique résiduelle nulle et contenant les racines de l'unité alors le corps $k(T)$ est (régulièrement) ψ-libre (i.e. $\widehat{F}_\omega$ est groupe de Galois d'une extension régulière de $k(T)$). Ce résultat s'applique par exemple pour le corps $k = \mathbb{Q}^{ab}((T))$.

Cette notion de psi-liberté est proprement nouvelle puisqu'elle vient s'intercaler strictement entre la propriété d'ω-liberté et le fait pour un corps de vérifier Galois Inverse. Des perspectives intéressantes s'ouvrent à partir de cette notion, par exemple pour la conjecture de Shafarevich (qui prévoit au total beaucoup plus que la ψ-liberté de la clôture abélienne de $\mathbb{Q}$) ainsi que vers des perspectives modulaires comme l'indique la dernière partie de l'article mentionné.

Dans l'article 17/ je m'intéresse aux extensions abéliennes et projectives de $\mathbb{Q}$ en relation avec les conjectures de Shafarevich, Fried-Völklein et Dèbes-Deschamps en théorie inverse de Galois. Dans ce travail on classifie complètement les sous-corps projectifs minimaux de $\mathbb{Q}^{ab}$ et l'on indique comment assurer l'existence et exhiber des corps "abyssaux " (des corps qui ne sont extensions d'aucun sous-corps projectif minimal de $\mathbb{Q}^{ab}$). On propose deux nouvelles conjectures, intermédiaires à celles citées précédemment et l'on montre comment, sous ces conjectures on peut obtenir une description simple du monstre $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sous forme de produits semi-directs.

Une collaboration avec François Legrand a été initiée lors des JA2017. Dans l'article 21/ nous expliquons comment construire des familles de corps k sur lesquels le problème inverse Galois est faux (il existe des groupes finis qui n'apparaissent pas comme groupes de Galois sur k) mais pour lesquels le problème inverse Galois faible est vrai (tous les groupes finis apparaissent comme

groupes d'automorphismes d'une extension séparable de k). Il s'agit là d'un article qui complète et généralise une série d'articles sur l'étude du sujet, étude initiée dans les années 70.

b.— *Arithmétique des corps et des groupes profinis.* Mots clés : *Théorie de Galois*, *arithmétique des corps ordonnables et théorie d'Artin-Schreier*, *valuations et corps henséliens*, *groupes profinis*, *cohomologie galoisienne.*

Vers la fin de ma thèse je me suis plus spécialement intéressé aux corps ordonnables et à la théorie d'Artin et Schreier. Synthétisant plusieurs idées de théorie inverse de Galois, j'ai obtenu des résultats arithmétiques et cohomologiques sur les clôtures totalement réelles, qui sont présentés dans l'article 3/. Nommé Maître de conférence à Saint-Étienne en 1999, j'ai continué mon travail sur l'arithmétique des corps. J'ai repris des travaux de Ribenboim sur les corps fermatiens et j'ai montré que, sous certaines conditions, la clôture p-fermatienne d'un corps, a un groupe de Galois qui est un pro-p-groupe sans torsion. Ce résultat est l'objet principal de l'article 4/. Parallèlement, j'ai décrit dans l'article 5/, pour un corps K de caractéristique 0, le plus petit corps complet et algébriquement clos contenant $K((X))$: le corps des séries de Puiseux généralisées qui, comme son nom l'indique, étend la notion de série de Puiseux. L'article 7/ aborde une question relative aux corps gauches de dimension finie sur $\mathbb{R}$. Dans cet article, je montre notamment qu'un corps gauche de dimension finie sur un corps algébriquement clos $\overline{K}$ (sans aucune condition de centralité) est en fait un corps de quaternions sur un sous-corps réel clos de $\overline{K}$. Ce résultat étend, sur ce point, le fameux théorème de Frobenius.

Un travail de fond a été fait sur l'étude des automorphismes continus d'un corps de série de Puiseux. Dans l'article 10/, je donne une décomposition en un produit semi-direct à quatre facteurs du groupe des K-automorphismes du corps des séries de Puiseux à coefficients dans la clôture algébrique de K (K étant un corps de caractéristique nulle). Les facteurs de ce produit semi-direct sont intrinsèquement donnés par l'arithmétique du corps, on y retrouve d'ailleurs de manière naturelle le groupe de Galois absolu de $\overline{K}((X))$. En application de ce résultat structurel, je décris les classes de conjugaisons des sous-corps réels clos de ce corps de séries de Puiseux. Elles sont paramétrées finalement par les ordres compatibles sur K. Une autre application de ce travail vise à décrire certains sous-groupes du monstre $\mathbf{Aut}(\mathbb{C})$. Je montre, en particulier, que pour tout corps K de caractéristique nulle et de cardinal au plus la puissance du dénombrable, le groupe de Galois absolu de K est un sous-groupe de $\mathbf{Aut}(\mathbb{C})$. En particulier, le groupe $\mathbf{Aut}(\mathbb{C})$ contient en son sein tous les groupes prolibres de rang plus petit que la puissance du continu.

Un autre travail (cf. 11/), qui est en collaboration avec Gérard Leloup (logicien, MCF au Mans) a porté sur la structure algébrique du groupe des unités d'un anneau de séries entières à coefficients dans un anneau commutatif unitaire fini. Ce groupe est en fait profini. Le résultat principal de l'étude montre qu'il s'agit d'une somme directe du sous-groupe des éléments de torsion et d'une partie constituée de groupes (pro)-libres. Plus exactement, pour un anneau de coefficients A fixé, ce groupe est isomorphe en tant que groupe topologique (pour la topologie profinie liée à la presque-valuation usuelle) au produit direct $A^*\times\Gamma\times\prod_{p\nmid\sharp A}\mathbb{Z}_p^{\aleph_0}$ où Γ est un groupe profini abélien d'exposant. L'étude de la torsion de ce groupe a été faite dans un cas assez large et nous montrons que sous certaines conditions sur A (incluant le cas des produits directs) on a $\Gamma\simeq N^{\aleph_0}$ où $N=\sqrt{\{0\}}$ désigne le nilradical de A.

En 2008-2009 j'ai travaillé avec Ivan Suarez (jeune MCF recruté en 2008 au Mans) sur un sujet de combinatoire des groupes profinis. L'idée de départ fut de généraliser au cas profini le célèbre résultat de structure qui assure qu'un groupe abstrait est libre si et seulement si il agit librement sur un arbre. Pour ce faire, j'ai introduit un nouveau concept : les prographes sylvestres, et avec Suarez nous avons donné un analogue profini au résultat ci-dessus mentionné. L'analogue, dans ce cas, de la liberté est ce que nous appelons la *presque liberté* et qui est la qualité qu'un groupe profini a de posséder un sous-groupe abstrait libre et dense. Le résultat principal de notre article (cf. 14/) est qu'un groupe profini est presque libre si et seulement si il agit prolibrement sur un proarbre. Un proarbre est un système projectif de graphes duquel on peut extrairement inductivement un arbre. La notion d'action prolibre correspond au fait qu'il existe une filtration du groupe profini

considéré pour laquelle les quotients finis associés agissent librement sur chaque étage du système inductif qui définit le proarbre. La notion de presque liberté est difficile a appréhender, par exemple c'est une propriété qui n'est pas forcément stable par passage aux sous-groupes ni par passage aux quotients. Il me semble raisonnable d'envisager que les groupes projectifs sont presque libres (penser déjà au cas des pro-p-groupes), ce théorème que nous avons établi avec Suarez sera surement un moyen d'aborder cette question sur les groupes projectifs lors d'un prochain travail.

En 2009, je me suis aussi intéressé à une pure question d'arithmétique des corps sur le groupe circulaire. Etant donné un corps algébriquement clos $\overline{K}$ et c une involution de ce corps, on définit le *groupe circulaire* de $\overline{K}$ relatif à c comme étant l'ensemble

$$U = \{z \in \overline{K} / \ zc(z) = 1\}$$

Il s'agit en fait du groupe des éléments de norme 1 de l'extension $\overline{K}/R$ où R désigne le corps réel clos des invariants de $\overline{K}$ par c. Dans le cas où $\overline{K} = \mathbb{C}$ et c est la conjugaison complexe, il est célèbre que U est topologiquement isomorphe au groupe quotient $\mathbb{R}/\mathbb{Z}$. Dans l'article 15/ on se pose la question de savoir si cette propriété algébrique et topologique reste vraie dans le cas général. Je montre dans cette article que l'isomorphisme algébrique reste vrai pour n'importe quel sous-corps algébriquement clos de $\mathbb{C}$ (c restant la conjugaison complexe). Ce résultat n'est pas tout à fait trivial si l'on pense par exemple au cas $\overline{K} = \overline{\mathbb{Q}}$ et au fait que l'application $x \longmapsto e^{ix}$ n'envoie pas $\overline{\mathbb{Q}} \cap \mathbb{R}$ dans $\overline{\mathbb{Q}}$ (théorème de Lindemann). Je démontre dans une autre partie de cet article que si, pour un corps algébriquement clos $\overline{K}$ et une involution c donnés, il existe un isomorphisme algébrique de U sur $R/\mathbb{Z}$ alors il existe un isomorphisme de groupes topologiques entre le groupe circulaire relatif à Puis($\overline{K}$) et Puis(R)/$\mathbb{Z}$ (l'involution considérée sur Puis($\overline{K}$) étant celle obtenu de c par action sur les coefficients des séries). Ce résultat de structure permet alors d'exhiber un exemple d'involution c_0 de $\mathbb{C}$ qui n'est pas conjuguée dans Aut($\mathbb{C}$) à la conjugaison complexe et pour laquelle l'isomorphisme topologique $U \simeq R/\mathbb{Z}$ reste vrai.

Avec Ivan Suarez nous nous sommes intéressé à certaines propriétés des sous-groupes Gal($k((t))/k$). Dans l'article 18/ nous montrons deux séries de résultats. La première sur les centralisateurs des éléments Gal($k((t))/k$). La seconde sur la nature des sous-groupes engendrés par deux éléments de torsion. Cette dernière question est très intrigante, car, comme nous le montrons, dans certains cas ces sous-groupes sont des sommes amalgamées de groupes cycliques. Un lien profond existe entre ces questions et la théorie de Serre-Bass sur les arbres.

c.— *Théorie additive des nombres.* Mots clés : *Bases additives*, *essentialités*.

Dans ce domaine le centre d'intérêt est la notion d'essentialité dans une base additive. Une base additive est une partie $A \subset \mathbb{N}$ telle qu'il existe un entier $h \geq 1$ vérifiant que $h.A \sim \mathbb{N}$. Le plus petit entier h vérifiant cette propriété s'appelle alors l'ordre de la base A.

En 2001, un travail en collaboration avec G. Grekos (cf. 6/) et publié au journal de Crelle traitait du problème des éléments essentiels dans une base additive A donnée, c'est-à-dire les éléments $a \in A$ tel que $A - \{a\}$ ne soit plus une base (par exemple 1 dans la base $A = 2.\mathbb{N} \cup \{1\}$). Le résultat principal de cette étude est que le nombre d'éléments essentiels dans une base est fini et que le cardinal de l'ensemble de ces éléments est en $O\left(\sqrt{\frac{h}{\log h}}\right)$ (avec une constante effective = 5.7). Il est par ailleurs montré que cette estimation en O est en fait la meilleure possible asymptotiquement. Cette étude a été complétée ultérieurement par l'article 8/ où il est démontré que l'on peut toujours retirer d'une base additive une infinité d'éléments sans perdre le caractère de basicité.

Une généralisation de la notion d'élément essentiel dans une base est la notion d'essentialité. Une essentialité dans une base A est une partie minimale B de A telle que la partie $A - B$ ne soit plus une base additive. Une collaboration (cf. 12/) avec B.Farhi (ATER au Mans en 2004-2005) a abordé le cas des essentialités finies. Le résultat principal de cette étude montre qu'à l'instar des éléments essentiels, les essensialités finies dans une base sont toujours en nombre fini. Toutefois, leur nombre ne peut être contrôlé par une fonction de l'ordre de la base, comme le montre des exemples assez simples. Dans cet article, nous introduisons un invariant pour l'étude de ce nombre

: la raison d'une base. Il s'agit de la plus grande raison des progressions arithmétiques contenant presque totalement A (l'existence d'une telle progression maximale avec cette propriété n'est pas simple). Etant donné la raison r d'une base on peut alors majorer le nombre d'essentialités finies par la longueur du radical de r. Là encore ce résultat est optimal.

Dans l'article 13/ je me suis intéressé aux bonnes valeurs initiales de la suite de Lucas-Lehmer. Je montre que la détermination des valeurs initiales de la suite de Lucas-Lehmer qui font du test de primalité pour les nombres de Mersennes une condition nécessaire et suffisante se ramène à la recherche de points entiers sur certaines courbes algébriques. En application de ce résultat, j'exhibe deux familles infinies de bonnes valeurs initiales pour cette suite.

Mon dernier travail dans le domaine concerne le fameux théorème Mills qui assure qu'il existe une constante M telle que $[M^{3^n}]$ soit un nombre premiers pour tout entier $n \geq 0$. L'objet de l'article 19/ est de généraliser ce théorème et d'étudier la topologie de l'ensemble des constantes M. J'ai montré, en particulier, que cet ensemble est la limite croissante d'ensembles homéomorphes à l'ensemble triadique de Cantor.

d.— *Arithmétique des corps gauches.* Mots clés : *Algèbre non commutative*, *théorie de Galois généralisée*, *Problème Inverse de Galois*.

Il s'agit d'une nouvelle théorie que je suis en train de développer depuis 2020. La théorie de Galois admet une généralisation au cas des corps gauches, ce qui justifie l'étude du problème inverse de Galois sur ces corps. Après l'article 20/ où je donne l'exemple (impossible dans le cas commutatif) d'une extension galoisienne à groupe de Galois fini d'ordre plus grand que le degré de l'extension et soulignant ainsi quelques remarquables pathologies dans le cas non commutatif, j'ai attaqué en collaboration avec François Legrand l'analogue du théorème de Pop qui affirme que le problème inverse de Galois admet une réponse positive sur $k(t)$ dès que k est un corps ample. Dans l'article 22/ nous montrons que si H désigne un corps de dimension finie sur son centre k et que si k est un corps ample alors le problème inverse de Galois admet une réponse positive sur le corps des fractions tordu à indéterminée centrale $H(t)$ (l'analogue le plus simple de $k(t)$ dans le cas non commutatif). Par exemple, tout groupe fini est groupe de Galois sur le corps $\mathbb{H}(t)$ où $\mathbb{H}$ désigne le corps des quaternions d'Hamilton. Ce très récent résultat a déjà été utilisé par Paran et Alon qui montrent dans un article à paraitre prochainement, comment à partir du résultat central de 22/ on peut montrer que le problème inverse de Galois admet une réponse positive sur le corps des fonctions rationnelles $H(x)$ (ici l'indéterminée x n'est plus centrale). Mon étudiant A.Behajaina a montré que ce résultat de 22/ reste vrai si l'on ne fait plus d'hypothèse de finitude de H sur k et que l'on tord le corps des fractions par un automorphisme d'ordre fini (il s'agit du corps $H(t,\sigma)$, corps des fractions de l'anneau de polynômes tordu de Ore). Son idée est tout à fait novatrice par rapport à l'approche initiale du problème. J'ai repris dans 24/ cette idée pour généraliser encore le résultat aux cas des corps des fractions $H(t,\sigma,\delta)$ qui sont aussi tordus par une dérivation. Parallèlement, avec Behajaina et Legrand, nous avons dans l'article 23/ exploité ces idées pour aborder la classique question des problèmes de plongement dans le cas des corps gauches.

Ces travaux sur le Problème de Galois Inverse envisagent uniquement le cas des extensions extérieures, c'est-à-dire des extensions de corps gauches qui ne possèdent aucun automorphisme intérieur. La présence d'automorphismes intérieurs perturbe très fortement les choses. Dans l'article 25/ j'étudie l'arithmétique des extensions qui ne possèdent que des automorphismes intérieurs. Dans cette situation de très jolies choses apparaissent, notamment, l'existence d'un " ensemble de Brauer " pour un corps gauche K qui généralise la notion de groupe de Brauer du cas commutatif. Lorsque l'on s'intéresse aux extensions galoisiennes algébriques possédant des automorphismes intérieurs, on perd bien sur la structure profinie du groupe des automorphismes (et les correspondances galoisiennes du théorème de Krull-Jacobson). Dans l'article 26/ je m'attache à montrer que dans la situation intérieure on peut quand même appréhender la structure du monoïde des endomorphismes *via* une complétion projective. Ce résultat généralise d'ailleurs le cas extérieur et constitue une première étape vers une généralisation globale de la théorie de Galois des extensions algébriques.

Cette nouvelle thématique ouvre de très nombreuses pistes de recherche et fédère déjà plusieurs autres mathématiciens. De 2020 à 2022 j'ai organisé et animé un programme de recherche *via* un RIN qui m'a permis de recruter François Legrand sur un postdoc. Ce programme a été particulièrement fécond et nous a permis à Legrand et moi-même d'être recrutés sur cette thématique dans un IRN (voir plus loin).

La dernier sujet d'étude en date sur cette thématique concerne l'arithmétique de l'extension $H(t,\sigma)/H$. En 2024, j'ai montré une généralisation du théorème de Lüroth lorsque σ est un automorphisme complétement kummérien (cf 29/) et j'ai décrit l'ossature galoisienne de cette extension lorsque σ est d'ordre extérieur infini (cf 30/). Ce sujet se révèle lui aussi très fécond et mon étudiant Victor Voisin travaille actuellement sur de possibles généralisations de ces travaux.