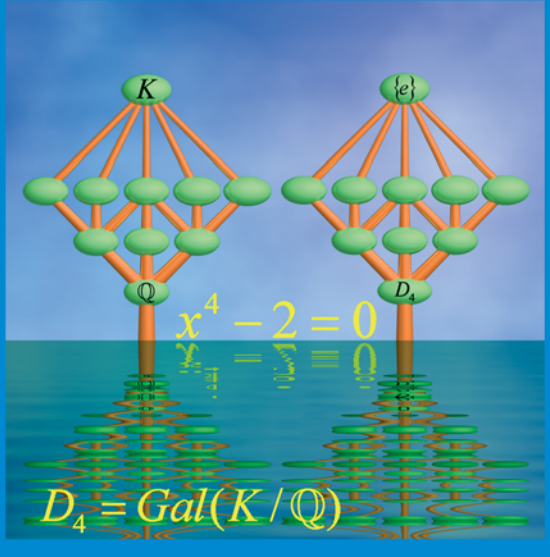
COLLECTION ENSEIGNEMENT SUP //// Mathématiques

L3M1

Algèbre I

GROUPES, CORPS ET THÉORIE DE GALOIS



Daniel Guin et Thomas Hausberger

EDP SCIENCES

ALGÈBRE

Tome 1

GROUPES, CORPS ET THÉORIE DE GALOIS

Daniel Guin – Thomas Hausberger

Collection dirigée par Daniel Guin

EDP SCIENCES

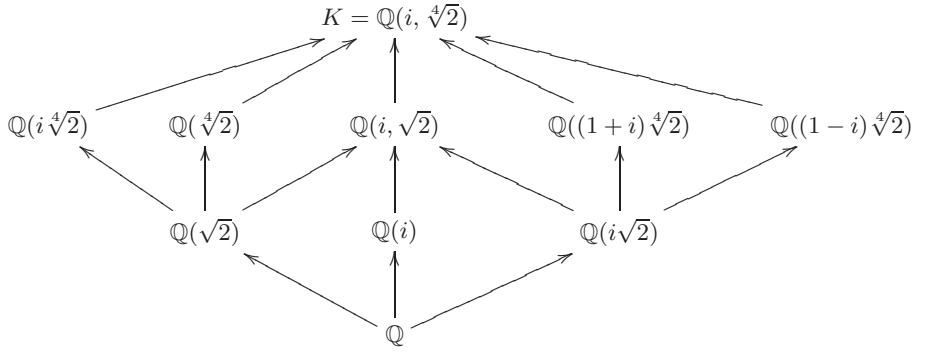
17, avenue du Hoggar
Parc d'activités de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

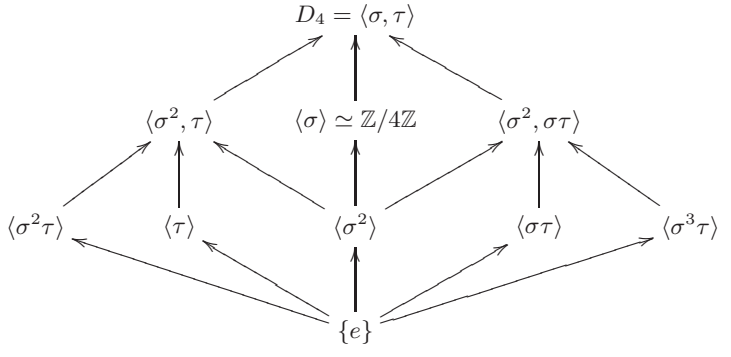
À propos de la couverture :

Le groupe de Galois de l'équation $x^4 - 2 = 0$ est le groupe de Galois $G = Gal(K/\mathbb{Q})$ du corps $K = \mathbb{Q}(i, \sqrt[4]{2})$ engendré sur $\mathbb{Q}$ par les racines complexes $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ du polynôme $x^4 - 2$.

Il existe un élément σ de G défini par $\sigma(i) = i$ et $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ et un élément τ défini par $\tau(i) = -i$ et $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$. Ces deux éléments engendrant G, on voit que le groupe de Galois est isomorphe au groupe diédral D_4 des isométries du carré.

Les sous-corps de K correspondent aux sous-groupes de G par la correspondance de Galois : par exemple, à $H = \langle\sigma\rangle$ correspond le sous-corps $\mathbb{Q}(i)$ des invariants de K sous l'action de H. On peut représenter les inclusions entre les groupes et les extensions de corps par les diagrammes ci-dessous, où chaque flèche représente une inclusion.



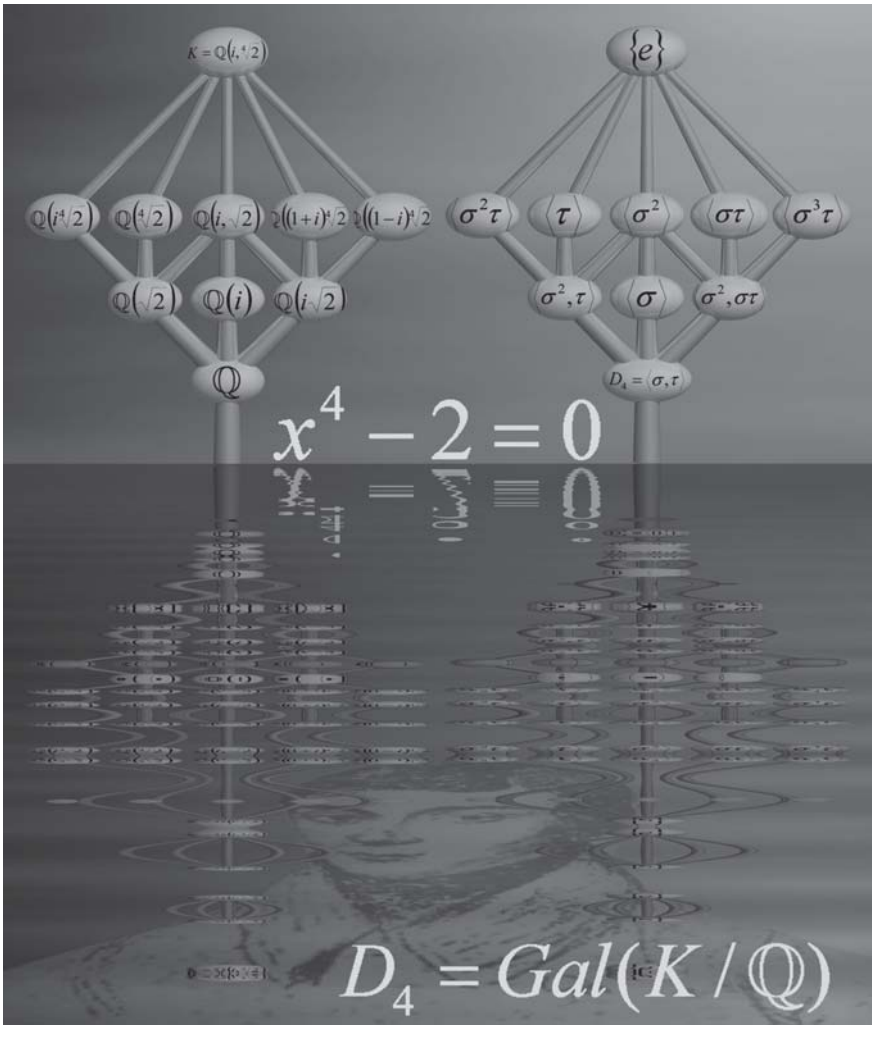


Cette correspondance renverse le sens des inclusions, donc celui des flèches. On peut se représenter les deux diagrammes comme deux arbres qui seraient reflet l'un de l'autre, dans l'esprit de la gravure « les 3 mondes » d'Escher. L'équation $x^4 - 2 = 0$ est le trait d'union entre le monde des groupes et celui des corps. Peut-être le troisième monde est-il celui de l'esprit du mathématicien dont l'inspiration et la raison ont fait naître les concepts, en se heurtant aux contingences de l'univers mathématique ?

Le groupe de Galois est le groupe des relations rationnelles entre les racines, par rapport au corps de base $\mathbb{Q}$. Il est trivial lorsque toutes les racines sont différenciées sur la base. Faire une extension, par exemple adjoindre le nombre imaginaire i, permet de regrouper les racines en catégories, selon qu'elles sont invariantes sous σ ou pas. C'est l'idée qui a guidé Galois lors de l'élaboration de son traité sur la résolution des équations : briser progressivement les symétries entre les racines. Ces travaux ont permis de faire émerger les structures contemporaines de groupe et de corps.

En général, les formules donnant les racines ne sont pas connues. La connaissance du groupe de Galois nous renseigne sur leur expression. Lorsque le groupe est résoluble, c'est-à-dire lorsqu'il existe une suite $G \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$ formée de sous-groupes normaux emboîtés tels que les quotients successifs soient abéliens, alors les solutions sont exprimables par radicaux. C'est le cas sur notre exemple : $D_4 \rhd \mathbb{Z}/4\mathbb{Z} \rhd \{e\}$.

Le dessin de la couverture a été réalisé par Jos Leys[1], ingénieur passionné d'imagerie mathématique, reconnu internationalement dans le monde de l'édition scientifique pour la qualité de ses illustrations, en relation directe avec le « substrat » mathématique. Les auteurs le remercient chaleureusement.



[1] http://www.josleys.com

Imprimé en France

ISBN : 978-2-86883-974-9

TABLE DES MATIÈRES

This page intentionally left blank

AVANT-PROPOS

La très longue histoire de l'étude des nombres, puis des équations, a permis de remarquer des analogies entre certaines propriétés vérifiées par des objets mathématiques de natures différentes, par exemple, les nombres et les polynômes. Cela a conduit les mathématiciens, en particulier au XIX^{e} siècle, à tenter de dégager une axiomatique qui rende compte des raisons profondes de ces analogies. Il est alors apparu que ces objets, de natures différentes, possédaient les mêmes « structures » algébriques, par exemple, groupe, espace vectoriel, anneau, etc.

Il devint alors évident qu'il était plus efficace d'étudier ces structures pour elles-mêmes, indépendamment de leurs réalisations concrètes, puis d'appliquer les résultats obtenus dans les divers domaines que l'on considérait antérieurement.

L'algèbre « abstraite » était née.

La notion de ***groupe*** (chapitres I à VII) est apparue dans l'étude des équations. Elle a notamment permis d'apporter, *via* la ***théorie de Galois*** (chapitre XIV), une réponse définitive à la non résolubilité, par radicaux, des équations polynomiales de degré supérieur ou égal à cinq (chapitre XVI).

Ensuite, l'introduction des groupes en géométrie a été à l'origine de développements féconds, qui ont complètement modifié l'essence même de cette discipline ancestrale. Dans un premier temps, ils sont intervenus comme groupes de déplacements dans l'espace euclidien pour affiner l'étude des figures classiques. Plus tard, d'outils dans l'étude de la géométrie, les groupes en sont devenus le cœur : une géométrie, euclidienne ou non, est l'étude des notions et propriétés qui restent invariantes par un groupe donné de transformations. La géométrie est donc devenue une branche de la théorie des groupes.

Enfin, l'existence de groupes a été mise en évidence, non seulement dans la quasi-totalité des mathématiques, mais également en physique, où cette structure algébrique joue un rôle très important dans les développements contemporains, en mécanique, en chimie, en biologie, en linguistique, en psychologie.

L'étude des nombres entiers remonte à la plus haute antiquité, mais c'est l'étude des nombres algébriques, au XIX^{e} siècle, qui a conduit aux notions d'***anneau*** et de ***corps***.

L'étude de la divisibilité dans les nombres entiers est basée sur la propriété fondamentale suivante : tout nombre entier s'écrit, de « manière unique », comme produit de nombres premiers. Comme pour toutes les structures algébriques importantes, la structure d'anneau apparaît dans de nombreuses situations dans lesquelles les éléments ne sont plus des nombres entiers. C'est en particulier le cas des polynômes. Il est donc utile d'étudier le notion de divisibilité dans des anneaux généraux et de voir si l'analogue de la décomposition en produit de nombres premiers existe : on l'appelle alors « décomposition en produit d'éléments irréductibles ».

L'idée essentielle, pour cela, a été l'introduction de la notion d'idéal : elle permet de formuler des énoncés qui généralisent ceux des propriétés usuelles de la divisibilité des nombres entiers. En particulier, la généralisation aux idéaux de la propriété de « décomposition en produit d'irréductibles », associée à la notion d'extension de corps, a permis de faire de très grands progrès en arithmétique.

Comme dans le cas des groupes, la structure d'anneau a donné naissance à une approche algébrique de la géométrie, en particulier des courbes et des surfaces : la géométrie algébrique. Cette démarche « algébrique » a été également appliquée, avec beaucoup d'efficacité, en analyse — groupes topologiques, espaces vectoriels normés, algèbres de Banach.

L'étude de la résolubilité et de la résolution des équations algébriques, c'est-à-dire des équations du type

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

a été une épopée, certainement la plus longue de l'histoire des mathématiques, qui s'est déroulée sur plus de 3500 ans.

Les premières traces écrites de problèmes se ramenant à la résolution d'une équation du second degré, $ax^2 + bx + c = 0$, apparaissent sur des tablettes babyloniennes 1700 ans avant notre ère et ces documents montrent que les babyloniens savaient résoudre ces équations lorsque les racines sont positives (et les coefficients dans un certain sous-anneau de $\mathbb{R}$). Ce furent ensuite les problèmes géométriques de duplication du cube et de trisection de l'angle (*cf.* chapitre XI) qui conduisirent les mathématiciens grecs à s'intéresser, dès le IV^{e} siècle avant J.-C., aux équations du troisième degré, mais il fallut attendre l'école mathématique italienne de la renaissance, au XVI^{e} siècle, pour que des formules explicites donnent les solutions de ces équations et, dans la foulée, celles des équations du quatrième degré.

Le fait, remarquable, que ces formules expriment les solutions de l'équation en fonction de ses coefficients aux moyens des quatre opérations élémentaires (addition, soustraction, multiplication, division) et de l'extraction de racines (carrées, cubiques) incita les mathématiciens du XVII^{e} et du XVIII^{e} siècles à rechercher des formules analogues pour les équations de degré supérieur ou égal à 5. Ce n'est qu'au XIX^{e} siècle que le point final fut mis à cette étude, en montrant l'impossibilité de l'existence générale de telles formules et en caractérisant les équations pour lesquelles cela était possible (*cf.* chapitre XVI).

Cette œuvre gigantesque mobilisa les mathématiciens parmi les plus grands de l'Histoire : Pythagore, Euclide, Diophante, Eratosthène, Al-Khowarizmi, Brahmagupta, Khayyam, Tartaglia, Cardan, Bombelli, Ferrari, Descartes, d'Alembert, Euler, Vandermonde, Lagrange, Gauss, pour s'achever par les travaux d'Abel et de Galois.

C'est l'étude des équations algébriques qui est à l'origine de la création et du développement de l'algèbre, dont le nom provient du titre d'un traité d'Al-Khowarizmi. D'abord exclusivement dévolue au calcul, à l'introduction des outils (nombres négatifs, extraction de racines, nombres complexes) et à l'élaboration des règles d'utilisation de ces objets, l'algèbre a évolué vers ce qu'elle est maintenant, l'étude des structures. Bien que non explicitement formulées, les structures de groupe et de corps sont présentes dans les travaux de Galois, dont l'apport le plus significatif a été de montrer que l'étude de la résolubilité des équations algébriques se ramenait à l'étude d'un groupe associé à chacune des équations. Comme c'est souvent le cas, l'apport d'idées nouvelles profondes pour étudier un problème d'envergure irradie l'ensemble des mathématiques. C'est ainsi qu'on retrouve, encore maintenant, cette idée féconde de Galois dans de nombreux domaines, en algèbre évidemment, mais aussi, par exemple, en géométrie et topologie (théorie des revêtements) et en analyse (théorie de Galois différentielle).

La notion de corps n'a été formalisée qu'au début du XX^{e} siècle par Dedekind. Cette notion, dont l'intérêt dépasse largement le cadre des équations algébriques, permet de donner une présentation conceptuelle et générale de l'étude de ces dernières. De plus, la notion d'extension de corps et son degré (qui n'est rien d'autre que la dimension d'un espace vectoriel) a permis, par exemple, de donner, après plus de vingt-trois siècles d'efforts, une réponse définitive aux problèmes de la duplication du cube ou de la trisection de l'angle (chapitre XI).

Ceci est l'un des nombreux exemples de la puissance des idées et des méthodes algébriques et illustre la nécessité de dégager les concepts fondamentaux qui permettent de formaliser, à un niveau convenable de généralité, des problèmes dont

la résolution résiste à toutes les investigations qui restent internes au cadre dans lequel ces problèmes sont posés.

Comme il a été rappelé ci-dessus, l'idée fondamentale de la théorie de Galois est d'associer à une équation (ou une extension de corps), un groupe dont les propriétés rendent compte de celles de l'équation (ou de l'extension). Il faut donc, pour décrire et utiliser la théorie de Galois, avoir une bonne maîtrise de la théorie élémentaire des groupes. C'est pour cette raison que nous avons voulu présenter en un seul livre la théorie des groupes et la théorie de Galois. Dans une première partie nous traitons de la théorie des groupes, dans une deuxième partie de la théorie des corps et dans une troisième de la théorie de Galois. L'objet d'étude principal de la théorie de Galois étant les polynômes, nous avons inséré au début de la deuxième partie un chapitre sur les anneaux de polynômes (chapitre VIII).

Le tome 2 de ce traité sera consacré aux anneaux, dont l'importance capitale, entre autres en arithmétique ou en théorie des nombres, a été soulignée plus haut, ainsi qu'aux modules et à l'algèbre multilinéaire.

Par ce programme, ces deux ouvrages s'adressent aux étudiants de L3 et master, leur contenu faisant partie de la culture normale d'un candidat à l'agrégation de mathématiques.

AVERTISSEMENT

Depuis plusieurs années, l'enseignement de l'algèbre en L1-L2 se limite généralement à l'algèbre linéaire. Cet ouvrage, en deux volumes, donne une présentation des thèmes d'un enseignement d'algèbre générale — groupes, anneaux, corps — et donne une introduction à l'algèbre multilinéaire, sans connaissance préalable nécessaire de ces domaines. On s'est volontairement limité à un exposé simple des concepts fondamentaux qui trouvent leurs places dans un enseignement de L3-M1.

Chaque chapitre comporte, dans le cours du texte, des exemples et des exercices qui illustrent les notions développées, au fur et à mesure qu'elles apparaissent. Les exercices signalés par le symbole (¶) sont plus difficiles que les autres.

À la fin de chacun des chapitres, on trouvera des thèmes de réflexion (TR) et des travaux pratiques (TP).

Les TR se présentent sous forme de questions, dont l'énoncé contient la réponse, qui guident le lecteur dans l'étude d'un objet ou d'une notion particulière, illustration, complément ou approfondissement du cours. Ils sont de trois types :

• Ceux qui sont signalés par le symbole ♡ doivent être considérés comme du cours et doivent être étudiés comme tels. Ils sont utilisés sans rappel dans les chapitres suivants.

• Ceux qui sont signalés par le symbole ♣ sont des problèmes d'application qui utilisent des notions développées dans le chapitre concerné ou dans ceux qui précèdent.

• Ceux qui sont signalés par le symbole ♠ sont des approfondissements plutôt destinés aux étudiants préparant l'agrégation.

Certains de ces TR sont repris dans plusieurs chapitres : on peut ainsi constater comment l'enrichissement de la théorie permet d'étudier, de façon de plus en plus fine, un même objet.

Les travaux pratiques ne sont pas des TP d'informatique, ni d'algorithmique, mais plutôt de « mathématiques assistées par ordinateur », bien que l'on soit naturellement amené à détailler des algorithmes et à discuter de leur pertinence. L'étude formelle de la « complexité » a été volontairement éludée. Au besoin, le lecteur pourra consulter les ouvrages de calcul formel cités en bibliographie ([28] par exemple). Les prérequis en programmation sont minimaux (procédures, boucles et branchements).

Le logiciel de calcul formel retenu est Maple[(1)], conformément aux positions institutionnelles actuelles qui se reflètent au niveau des concours. Cependant, d'autres logiciels sont beaucoup mieux adaptés à certaines questions, en fonction du domaine concerné : gap[(2)] pour les groupes et pari/gp[(3)] pour la théorie des nombres, par exemple. Mentionnons également maxima[(4)], xcas/giac[(5)] et sage[(6)] qui partagent la même vocation généraliste que Maple. Le lecteur notera que tous les logiciels cités sont libres sous licence gnu-gpl[(7)]... à l'exception de Maple.

Le sujet de chaque TP est en relation directe avec le cours du chapitre courant, dont il permet d'aborder les notions par la pratique avec un point de vue effectif. En ce sens, certains TP constituent de véritables compléments de cours, l'expérimentation par le biais du système de calcul formel (SCF) étant le contexte naturel d'élaboration et d'apprentissage de ces méthodes. Signalons que c'est la manipulation des formules qui est à l'origine du *calcul formel*[(8)] ou « computer algebra » en anglais, terminologie qui indique clairement une nature algébrique sous-jacente et désigne une branche disciplinaire des mathématiques qui a pris son essor avec l'avènement des ordinateurs.

Si l'on obtient rapidement des résultats inaccessibles à la main, après reformulation des nombreux problèmes qui s'y prêtent dans un langage symbolique (très proche de la formulation mathématique) compréhensible par le SCF,

(1) Pour « érable » ou MA*thematical* PLE*asure*, *cf.* `http://www.maplesoft.com/products/maple`
(2) `http://www.gap-system.org`
(3) `http://pari.math.u-bordeaux.fr`
(4) `http://maxima.sourceforge.net` ou `http://michel.gosse.free.fr`
(5) `http://www-fourier.ujf-grenoble.fr/~parisse/gia_fr.html`
(6) `http://www.sagemath.org`
(7) General Public Licence, *cf.* `http://www.april.org/gnu/gpl_french.html`
(8) Le calcul formel, ou calcul symbolique, est l'art de réaliser des calculs algébriques (*i.e.* des manipulations d'expressions) sur des objets généraux représentés en machine et soumis à des règles de transformation bien définies (qui peuvent être prédéfinies dans le logiciel ou bien définies par l'utilisateur). Les algorithmes pour ce type de transformations sont en général basés sur des méthodes exactes, c'est-à-dire qu'il n'y a pas d'erreur due à la méthode, par opposition au calcul numérique qui est l'art de réaliser des calculs approchés où se combinent erreurs de méthode et erreurs d'arrondi (limitation due à la représentation des nombres en machine).

il est important de mettre en garde l'utilisateur contre une tendance à faire une confiance aveugle au SCF et à perdre son esprit critique. Outre une réflexion sur la relation « homme-machine », il est instructif de regarder dans la « boîte noire » afin de prendre conscience qu'il s'agit d'algorithmes implémentés en machine, qui ne donneront une réponse exacte que dans leur contexte strict de validité (voire d'heuristiques, comme pour le calcul des limites, où encore davantage de vigilance est souhaitable de la part de l'utilisateur). Le propos de ces TP ne sera donc pas de faire étalage des possibilités offertes par Maple pour résoudre des problèmes algébriques, mais bien de discuter des notions mathématiques en jeu et, parallèlement, des algorithmes qui se cachent derrière les commandes employées, les deux étant évidemment liés.

Ce faisant, le SCF devient un « assistant de calcul » et un extraordinaire outil d'expérimentation, la « responsabilité scientifique » demeurant entre les mains de l'expérimentateur. Certains auteurs parlent d'« instrumentation raisonnée ». L'expérimentateur est amené à « découvrir » expérimentalement des conjectures-théorèmes, les tester avant de tenter d'en faire la démonstration au papier-crayon. Tout en consolidant bien sûr les connaissances acquises qui sont mobilisées dans l'action...

Certains algorithmes seront étudiés en détail, comme l'algorithme de Todd-Coxeter (calcul de représentants des classes modulo un sous-groupe), de Gauss, Hermite et Smith (algorithmes très importants en algèbre linéaire et dans la théorie des groupes abéliens, c'est-à-dire des $\mathbb{Z}$-modules) ; algorithme de Berlekamp (factorisation des polynômes sur un corps fini) ; algorithmes de recherche des sous-corps d'un corps de nombre, de calcul du groupes de Galois, etc. Si certains sont classiques, d'autres ont été découverts récemment, bien que les notions utilisées soient à la portée d'un étudiant de L3-M1. Figurent également parmi les thèmes traités, les courbes elliptiques (ingrédients essentiels de la preuve du célèbre théorème de Fermat, ces objets fascinants trop souvent réservés à un public averti de Master Recherche deviennent accessibles, par le biais expérimental, grâce aux possibilités de calcul offertes par le SCF) et les codes correcteurs d'erreur, qui font leur apparition dans les manuels contemporains d'algèbre en tant qu'application pertinente (dans le monde de l'industrie) de l'algèbre sur les corps finis. Sans oublier les quaternions de Hamilton, les énumérations de Polya, etc.

Ces TP ont été pour beaucoup inspirés du livre de B. Perrin-Riou [22]. Un des auteurs a également tiré parti de sa participation au sein du groupe IREM Fodesit-Accessit de Montpellier qui a mené une réfexion sur le « bon usage » du calcul formel dans les cursus d'enseignement. Que tous ceux qui ont contribué à cette réflexion pédagogique en soient remerciés. La plupart de ces TP ont été

Q

R

S

T

U - Z