

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.

A 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 tel. 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 ([G-G] par exemple). Les prérequis en programmation sont minimaux (procédures, boucles et branchements).

Le logiciel de calcul formel retenu est MAPLE¹, 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 : GAP² pour les groupes et PARI/GP³ pour la théorie des nombres, par exemple. Mentionnons également MAXIMA⁴, XCAS/GIAC⁵ et SAGE⁶ qui partagent la même vocation généraliste que MAPLE. Le lecteur notera que tous les logiciels cités sont libres sous licence GNU-GPL⁷... 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, 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'heuristique, 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

¹pour « érable » ou M A thematical PLEasure, 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>

⁵http://www-fourier.ujf-grenoble.fr/~parisse/gia_fr.html

⁶<http://www.sagemath.org>

⁷General Public Licence, cf. http://www.april.org/gnu/gpl_french.html

⁸Le 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).

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 ([PR]). Un des auteurs a également tiré parti de sa participation au sein du groupe IREM FODESIT-ACCESSIT de Montpellier qui a mené une réflexion 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 expérimentés dans le cadre des enseignements de Mathématiques de l'Université Montpellier 2.

Enfin, des (éléments de) corrigés pour l'ensemble des TP sont disponibles en ligne à l'adresse

<http://www.math.univ-montp2.fr/~hausberg/ens/livre-algebre-t1.html>.

On y trouvera des documents destinés à faciliter la prise en main de MAPLE (notes de cours, feuilles de prise en main) et surtout des solutions aux questions posées, sous forme de feuilles de calcul MAPLE. La version utilisée est la 9.0. C'est à cette version que font référence les commandes mentionnées dans les énoncés de TP, la

compatibilité ascendante avec des versions plus récentes étant en principe assurée. Toute contribution dans un autre logiciel de calcul formel (mentionné plus haut), sous forme d'une ressource correctement documentée et correspondant à un TP complètement résolu, est la bienvenue. Elle pourra être mise en ligne en faisant dûment référence au contributeur.

Les exercices, les TR et les TP de ce tome 1 représentent près de 600 questions, dont la résolution permettra au lecteur d'acquérir une bonne maîtrise des concepts de base concernant les groupes, les corps et la théorie de Galois.

Les démonstrations intègrent de fréquentes références à des résultats contenus dans ce livre. Celles qui commencent par un chiffre romain, renvoient à un résultat contenu dans le chapitre correspondant à ce chiffre. Les autres renvoient à un résultat contenu dans le chapitre en cours. Le symbole \diamond indique la fin, ou l'absence, d'une démonstration.