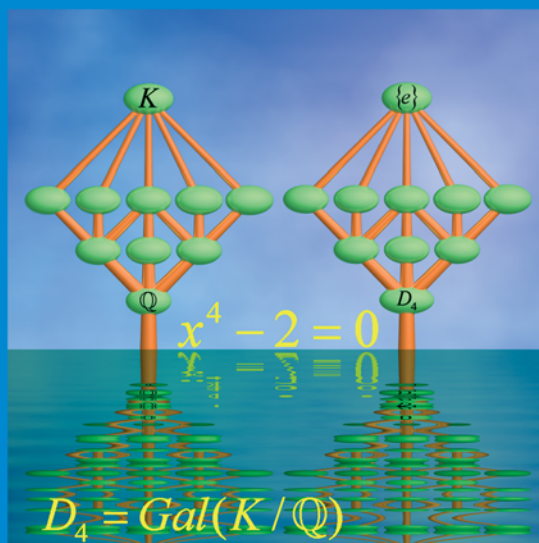


L3M1

Algèbre I

GROUPES, CORPS ET THÉORIE DE GALOIS



Daniel Guin et Thomas Hausberger

ALGÈBRE
Tome 1
GROUPES, CORPS
ET THÉORIE DE GALOIS

Daniel Guin – Thomas Hausberger

Collection dirigée par Daniel Guin



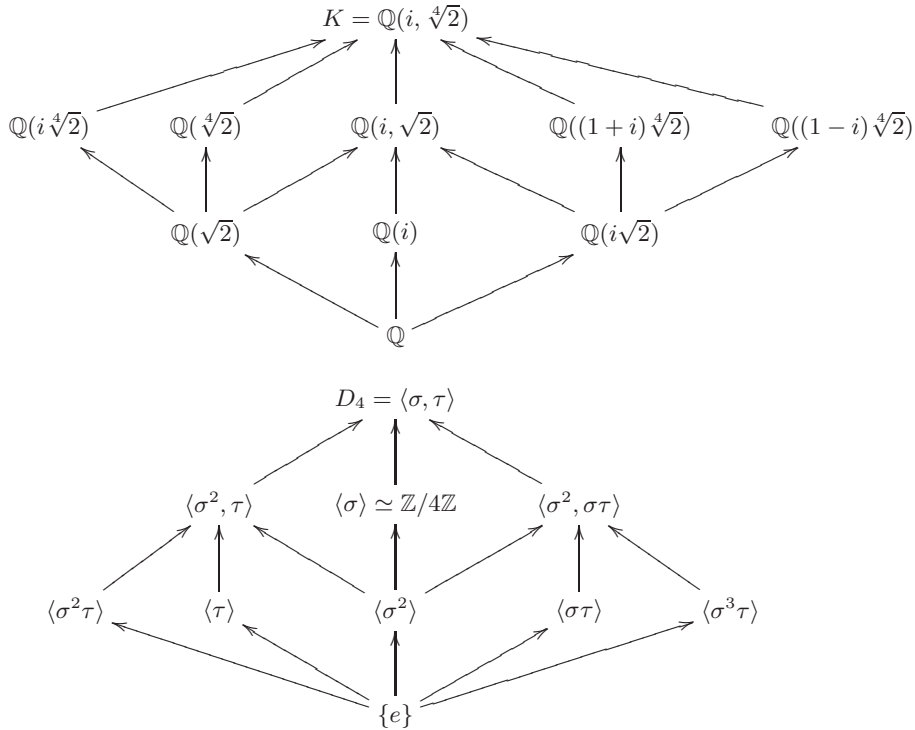
17, avenue du Hoggar
Parc d'activités de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

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.

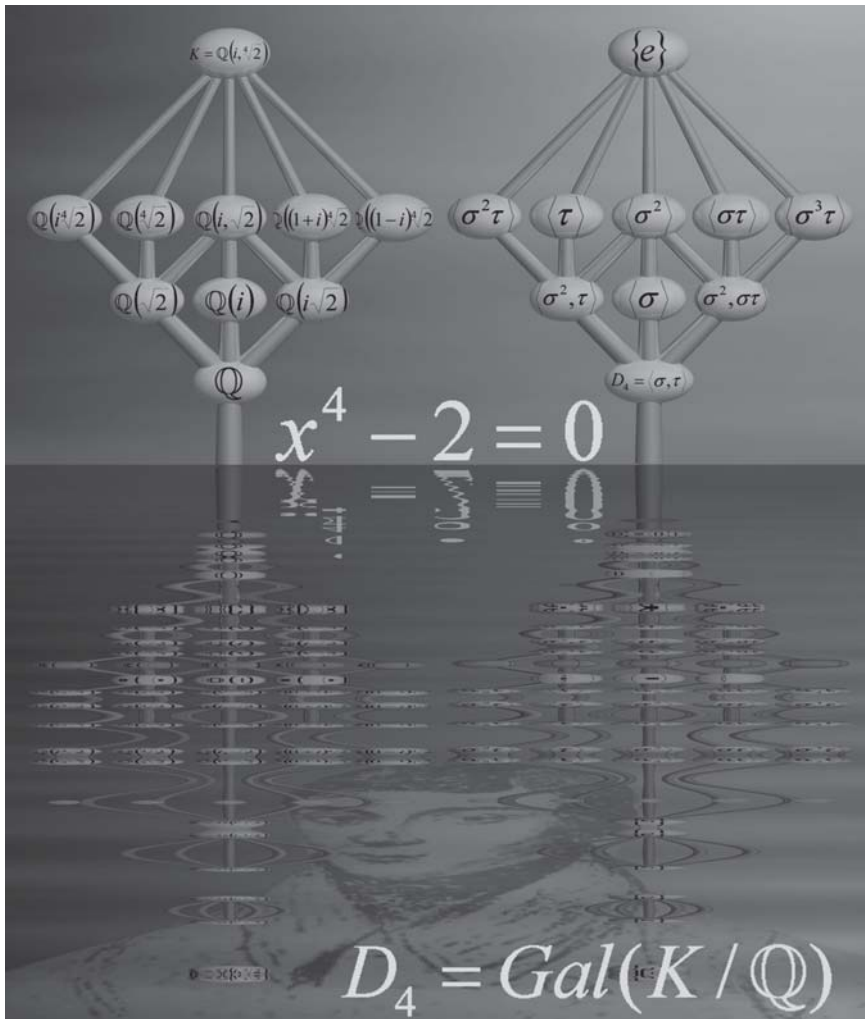


Cette correspondance renverse le sens des inclusions, donc celui des flèches. On peut se représenter les deux diagrammes comme deux arbres qui seraient reflet l'un de l'autre, dans l'esprit de la gravure « les 3 mondes » d'Escher. L'équation $x^4 - 2 = 0$ est le trait d'union entre le monde des groupes 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 $G \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$ 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 : $D_4 \triangleright \mathbb{Z}/4\mathbb{Z} \triangleright \{e\}$.

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

Tous droits de traduction, d'adaptation et de reproduction par tous procédés réservés pour tous pays. Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, des pages publiées dans le présent ouvrage, faite sans l'autorisation de l'éditeur est illicite et constitue une contrefaçon. Seules sont autorisées, d'une part, les reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, et d'autre part, les courtes citations justifiées par le caractère scientifique ou d'information de l'œuvre dans laquelle elles sont incorporées (art. L. 122-4, L. 122-5 et L. 335-2 du Code de la propriété intellectuelle). Des photocopies payantes peuvent être réalisées avec l'accord de l'éditeur. S'adresser au : Centre français d'exploitation du droit de copie, 3, rue Hautefeuille, 75006 Paris. Tél. : 01 43 26 95 35.

© 2008, **EDP Sciences**, 17, avenue du Hoggar, BP 112, Parc d'activités de Courtabœuf,
91944 Les Ulis Cedex A

TABLE DES MATIÈRES

Avant-propos	xiii
Avertissement	xvii
Première partie – GROUPES	1
I Généralités sur les groupes	3
I.1 Définitions — exemples	3
I.2 Sous-groupes — morphismes	8
A - Sous-groupes	8
B - Sous-groupes engendrés	11
C - Ordre d'un groupe, d'un élément	13
D - Morphismes	13
I.3 Produit direct de groupes	19
Thèmes de réflexion	25
TR.I.A. Étude du groupe symétrique S_n	25
TR.I.B. Groupes cycliques	27
TR.I.C. Détermination des groupes d'ordre n , pour $1 \leq n \leq 9$	30
Travaux pratiques	33
TPI. Étude de quelques groupes de permutations	33
II Groupes quotients	37
II.1 Classes modulo un sous-groupe	37
II.2 Compatibilité avec la structure	41
II.3 Groupes quotients	42

II.4	Caractérisation des sous-groupes normaux	45
II.5	Sous-groupes normaux et morphismes	47
II.6	Sous-groupes d'un groupe quotient	48
Thèmes de réflexion		53
TR.II.A.	Sous-groupes dérivés et abélianisation	53
TR.II.B.	Étude des sous-groupes normaux de S_n	54
TR.II.C.	Étude des automorphismes de S_n	57
Travaux pratiques		59
TP.II.	Classes, structure quotient et systèmes générateurs forts	59
III	Présentation d'un groupe par générateurs et relations	65
III.1	Groupes libres	65
III.2	Générateurs et relations	72
Thèmes de réflexion		75
TR.III.A.	Présentation du groupe quaternionique \mathcal{H}	75
TR.III.B.	Groupes de présentation finie	75
TR.III.C.	Quelques propriétés des groupes libres	76
TR.III.D.	Produit libre de groupes	77
IV	Groupes opérant sur un ensemble	81
IV.1	Définitions – Exemples	81
IV.2	Stabilisateurs – Orbites	84
IV.3	Produit semi-direct	87
	A - Groupes opérant sur un groupe	87
	B - Produit semi-direct de sous-groupes	87
	C - Produit semi-direct de groupes	88
IV.4	Opérations transitives, fidèles	90
IV.5	Points fixes	91
Thèmes de réflexion		93
TR.IV.A.	Groupes diédraux D_n	93
TR.IV.B.	Groupe des isométries du cube	94
TR.IV.C.	Produits et extensions de groupes	94
TR.IV.D.	Groupes libres de rang 2	96
Travaux pratiques		99
TP.IV.A.	Générateurs et relations, autour de l'algorithme de Todd-Coxeter	99

TP.IV.B	Actions k -transitives, formule de Burnside et énumérations de Polya	108
V	Les théorèmes de Sylow	117
V.1	Le premier théorème de Sylow	117
V.2	Le second théorème de Sylow	119
V.3	Applications	122
	Thèmes de réflexion	125
TR.V.A.	$\text{Int}(S_6) \neq \text{Aut}(S_6)$	125
TR.V.B.	Détermination des groupes d'ordre n , $n \leq 15$	126
TR.V.C.	Détermination des groupes d'ordre pq	127
VI	Groupes abéliens	129
VI.1	Somme directe de groupes abéliens	129
	A - Somme directe de sous-groupes d'un groupe abélien .	129
	B - Somme directe de groupes abéliens	131
	C - Facteur direct d'un groupe abélien	132
VI.2	Groupes abéliens libres	133
	A - Définition - Propriété universelle	133
	B - Rang d'un groupe abélien libre	137
	C - Sous-groupes d'un groupe abélien libre	140
VI.3	Groupes abéliens de torsion	142
VI.4	Structure des groupes abéliens de type fini	145
	Thèmes de réflexion	155
TR.VI.A.	Rang d'un groupe libre	155
TR.VI.B.	Groupes divisibles	156
TR.VI.C.	Calcul des facteurs invariants	158
	Travaux pratiques	161
TP.VI.A.	Algorithmes de Gauss-Jordan, de Hermite et de Smith . .	161
TP.VI.B.	Courbes elliptiques et groupe de Mordell	166
VII	Groupes résolubles	177
VII.1	Suites de composition	177
VII.2	Suites de Jordan-Hölder	179
VII.3	Groupes résolubles	181
VII.4	Applications	183

Deuxième partie – THÉORIE DES CORPS	185
VIII Anneaux de polynômes	187
VIII.1 Définitions - Exemples	187
VIII.2 Idéaux – Morphismes	190
VIII.3 Idéaux maximaux, idéaux premiers	194
VIII.4 Produit d’anneaux - Théorème chinois	196
VIII.5 Corps des fractions d’un anneau intègre	198
VIII.6 Anneaux de polynômes	199
VIII.7 Anneaux principaux	205
VIII.8 Divisibilité	210
VIII.9 Irréductibilité des polynômes	212
VIII.10 Racines – Ordre de multiplicité	217
VIII.11 Polynômes symétriques	220
Thèmes de réflexion	225
TR.VIII.A. Critère d’irréductibilité par extension	225
TR.VIII.B. Critère d’irréductibilité par réduction	226
TR.VIII.C. Résultant - Discriminant	227
TR.VIII.D. Algèbres - Algèbres de polynômes	228
Travaux pratiques	231
TP.VIII. Entiers de Gauss et sommes de deux carrés	231
IX Généralités sur les extensions de corps	237
IX.1 Corps premiers – Caractéristique d’un corps	237
IX.2 Extensions	239
Thèmes de réflexion	243
TR.IX.A. Corps finis	243
TR.IX.B. Corps des quaternions et théorème des quatre carrés	244
Travaux pratiques	249
TP.IX.A. Factorisation des polynômes	249
TP.IX.B. Les quaternions de Hamilton	259
X K-morphisms et groupe de Galois d’une extension	263
X.1 K -morphisms	263
X.2 Groupe de Galois	264

X.3	Degré d'une extension et ordre du groupe de Galois . . .	266
X.4	Corps intermédiaires et sous-groupes du groupe de Galois	268
XI	Extensions algébriques – extensions transcendentes	271
XI.1	Extensions algébriques	271
XI.2	Extensions transcendentes	276
XI.3	Appendice	281
	Thèmes de réflexion	285
TR.XI.A.	Constructions à la règle et au compas	285
TR.XI.B.	Théorème de Lüroth	287
	Travaux pratiques	289
TP.XI.	Nombres algébriques et polynôme minimal	289
XII	Décomposition des polynômes – Clôtures algébriques	299
XII.1	Corps de rupture et corps de décomposition d'un polynôme	299
XII.2	Clôtures algébriques	304
	Thèmes de réflexion	311
TR.XII.	Plongements dans une clôture algébrique	311
	Travaux pratiques	315
TP.XII.	Calculs dans les corps de nombres	315
XIII	Extensions normales, séparables	321
XIII.1	Extensions et éléments conjugués	321
XIII.2	Extensions normales	322
XIII.3	Extensions séparables	326
XIII.4	Éléments primitifs	331
XIII.5	Norme et trace	333
	Thèmes de réflexion	337
TR.XIII.A.	Corps parfaits	337
TR.XIII.B.	Extensions inséparables et radicielles	337
TR.XIII.C.	Dérivations et extensions séparables	339

Troisième partie – THÉORIE DE GALOIS ET APPLICATIONS 343

XIV Extensions galoisiennes – Théorie de Galois des extensions finies		345
XIV.1	Extensions galoisiennes	345
XIV.2	Clôture galoisienne d’une extension séparable	348
XIV.3	Théorèmes fondamentaux de la théorie de Galois	348
XIV.4	Étude d’un exemple	350
Thèmes de réflexion		355
TR.XIV.	Théorie de Galois des extensions infinies	355
Travaux pratiques		359
TP.XIV.	Autour de la correspondance de Galois	359
XV Racines de l’unité – Corps finis – Extensions cycliques		367
XV.1	Racines de l’unité	367
XV.2	Corps des racines n -ième de l’unité	369
XV.3	Polynômes cyclotomiques	371
XV.4	Corps finis	373
XV.5	Extensions cycliques	376
Thèmes de réflexion		381
TR.XV.A.	Symboles de Legendre. Loi de réciprocité quadratique	381
TR.XV.B.	Interprétation cohomologique du théorème « Hilbert 90 »	383
TR.XV.C.	Irréductibilité du polynôme $X^n - a$	384
Travaux pratiques		387
TP.XV.	Racines de l’unité dans un corps fini et codes <i>BCH</i>	387
XVI Résolubilité par radicaux des équations polynomiales		399
XVI.1	Extensions radicales	399
XVI.2	Résolubilité des polynômes	402
XVI.3	Caractérisation des polynômes résolubles	406
Thèmes de réflexion		409
TR.XVI.	Résolution des équations polynomiales de degrés 3 et 4	409
Travaux pratiques		413
TP.XVI.	Théorie de Galois constructive	413

XVII Polygones réguliers constructibles et nombres de Fermat	431
XVII.1 Points constructibles	431
XVII.2 Constructibilité des polygones réguliers	434
Appendice	439
1 Ensembles ordonnés	439
2 Cardinaux – Ensembles infinis	442
Bibliographie	449
Index terminologique	451

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 la 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 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>

⁽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 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

produit semi-direct de sous-groupes
 définition IV.3.2
 produit tensoriel (d'espaces vectoriels,
 d'algèbres) TR.XII.A
 propre (idéal) définition VIII.2.2
 propre (sous-groupe) définition I.2.2
 propriété universelle d'un anneau de polynômes
 théorème VIII.6.1
 propriété universelle de groupe abélien libre
 théorème VI.2.2
 propriété universelle de produit d'anneaux
 théorème VIII.4.1
 propriété universelle de produit direct
 de groupe) théorème I.3.1
 propriété universelle de somme directe
 de groupes théorème VI.1.1
 puissance du continu remarque A.2.3
 pur (quaternion) TR.IX.B
 pure (base, extension transcendante)
 définition XI.2.3

Q

quadratique (résidu) TR.XV.A
 quadratique (loi de réciprocité) TR.XV.A
 quadrature (du cercle) TR.III.A
 quaternion conjugué TR.IX.B
 quaternions (corps des) TR.IX.B - TP.IX.B
 quaternion d'Hurwitz TR.IX.B
 quaternion pur TR.IX.B
 quaternionique (groupe) exercice I.2 - TR.I.C -
 TR.III.A
 quotient (d'un anneau) VIII.2
 quotient (d'une suite de composition)
 définition VII.1.1
 quotient (groupe) définition II.3.1

R

racine de l'unité définition XV.1.1
 racine (d'un polynôme) définition VIII.10.1
 racine multiple (d'un polynôme)
 définition VIII.10.2
 racines n -ième de l'unité définition XV.1.1
 racines n -ième de l'unité (corps des)
 définition XV.2.1
 racines primitive n -ième de l'unité
 définition XV.1.2
 racine simple (d'un polynôme)
 définition VIII.10.2
 radicale (extension) définition XVI.1.1

radicaux (suite de) définition XVI.1.1
 radicielle (clôture, élément, extension)
 TR.XIII.B
 raffinement (d'une suite de composition)
 définition VII.1.2
 raffinement propre (d'une suite de composition)
 définition VII.1.2
 rang (d'un groupe) définition III.1.5
 rang (d'un groupe abélien) définition VI.2.3
 réciprocité quadratique (loi de) TR.XV.A
 relation compatible avec une loi définition II.2.1
 relation d'équivalence modulo un sous-groupe
 définition II.1.1
 relation d'ordre définition A.1.1
 relation d'ordre totale définition A.1.5
 réduit (mot) définition III.1.4
 réduite (forme) proposition III.1.2.1
 réduit (groupe) TR.VI.B
 résidu quadratique TR.XV.A
 résoluble (groupe) définition VII.3.1
 résoluble par radicaux (équation)
 définition XVI.2.1
 résolvante TR.XVI.A - TP.XVI
 résolvante (H -) TP.XVI
 résultant TR.VIII.C
 réunion disjointe définition A.2.1
 rupture (corps de) définition XII.1.1

S

Schreier-Sims (algorithme de) TP.II
 scindé (polynôme) définition XII.1.3
 section TR.IV.C - remarque VI.2.2
 semi-direct (produit) proposition-définition
 VI.3.1 - proposition VI.3.3
 séparable (degré) définition XIII.3.2
 séparable (élément, extension, polynôme)
 définition XIII.3.1
 signature d'une permutation TR.I.A
 signature (morphisme) TR.I.A
 simple (groupe) TR.II.B
 simple (racine d'un polynôme)
 définition VIII.10.2
 Smith (algorithme de) TP.VI.A
 somme d'idéaux proposition-définition VIII.2.1
 somme de cardinaux définition A.2.5
 somme de Gauss TR.XV.A
 somme de sous-groupes définition VI.1.1
 somme directe de groupes abéliens
 proposition-définition VI.1.3
 somme directe de sous-groupes définition VI.1.2

sous-anneau définition VIII.1.3
 sous-anneau (-corps) engendré
 proposition-définition VIII.1.3 - IX.2.8
 sous-corps définition VIII.1.3 - IX.1.1
 sous-corps premier définition IX.1.2
 sous-groupe définition I.2.1
 sous-groupe de Sylow (p -) définition V.1.1
 sous-groupe de torsion proposition-définition VI.3.1
 sous-groupe dérivé TR.II.A
 sous-groupe engendré définition I.2.3
 sous-groupe normal définition II.3.1
 sous-groupe normal engendré définition III.2.1
 sous-groupe propre définition I.2.2
 stabilisateur proposition-définition IV.2.1
 suite de composition définition VII.1.1
 suite de Jordan-Hölder définition VII.2.1
 suite de radicaux XVI.1.1
 suite exacte (de groupes) TR.IV.C
 suites de composition équivalentes définition VII.1.2
 support d'une permutation TR.I.A
 symbole de Legendre TR.XV.A
 Sylow (p -sous-groupe de) définition V.1.1
 Sylow (théorème de) théorème V.1.1 - théorème V.2.1
 symétrique (élément) définition I.1.1
 symétrique (différence) exercice VIII.1
 symétrique (groupe) exemple I.1.2 - TR.I.A
 symétrique (polynôme) définition VIII.11.2
 système générateur fort TP.II

T

table d'un groupe I.1.4
 tensoriel (produit) TR.XII.A
 théorème chinois théorème VIII.4.2
 théorème de Bezout VIII.5.8
 théorème de Cantor-Bernstein A.2.1

théorème de Cayley théorème I.2.1
 théorème "Hilbert 90" XV.5.1 - exercice XV.5
 théorème de Kronecker-Weber TR.XV.A
 théorème de Lagrange théorème II.1.1
 théorème de Lüroth TR.XI.B
 théorème de Mazur TP.VI.B
 théorème de Nagell-Lutz TP.VI.B
 théorème de passage au quotient II.6.2 - VIII.2.2
 théorème de Zermelo A.1.2
 théorème de Zorn A.1.1
 Todd-Coxeter (algorithme de) TP.IV.A
 topologique (groupe) TR.XIV.A
 torsion (groupe de) définition VI.3.1
 torsion (groupe sans) définition VI.3.1
 total (ordre) définition A.1.5
 totalement ordonné (ensemble) définition A.1.5
 trace (d'un élément) définition XIII.5.1
 transcendance (base de) définition XI.2.4
 transcendance (degré de, élément) définition XI.2.5
 transcendant (élément) définition XI.2.1
 transcendante (extension) définition XI.2.1
 transcendante pure (extension) définition XI.2.3
 transitive (opération) définition IV.4.1
 trisection (de l'angle) TR.III.A
 type (d'un groupe) définition VI.4.3
 type fini (extension) IX.2.11
 type fini (groupe de) définition III.1.1 - TR.III.B - définition VI.2.2

U - Z

unitaire (polynôme) VIII.1
 unité (élément) définition VIII.1.1
 unité (racine de, racine n -ième de) définition XV.1.1
 Zermelo (théorème de) A.1.2
 zéro (d'un polynôme) définition VIII.10.1
 Zorn (théorème de) A.1.1