Henri Lombardi & Claude Quitté

Algèbre commutative Méthodes constructives

Modules projectifs de type fini

Cours et exercices

Deuxième édition

Calvage & Mounet

Henri Lombardi est Maître de conférences honoraire à l'Université de Franche-Comté.
Ses recherches concernent les mathématiques constructives, l'algèbre réelle et la complexité algorithmique.
Il est l'un des initiateurs du groupe international M.A.P. (Mathematics, Algorithms, Proofs), créé en 2003 : voir le site `https://mapcommunity.github.io/`
Il a publié les ouvrages suivants.

- ▷ *Un cours d'algèbre constructive*, Presses Universitaires de Franche-Comté, 2020. Traduction du livre *A course in constructive algebra* de Mines, Richman et Ruitenburg (Springer 1988), révisée par Stefan Neuwirth.
- ▷ *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem.* avec Perrucci D. et Roy M.-F. Memoirs of the AMS, vol. 1277. Providence, RI : American Mathematical Society (AMS) (2020).
- ▷ *Modules sur les anneaux commutatifs*, Calvage & Mounet, 2014, en collaboration avec Gema Díaz-Toca et Claude Quitté.
- ▷ *Épistémologie mathématique*, Ellipse, 2011.
- ▷ *Méthodes matricielles. Introduction à la complexité algébrique*, Springer, 2003, en collaboration avec Jounaïdi Abdeljaoued.
- ▷ *Géométries élémentaires*, Presses Universitaires de Franche-Comté. 1999.

`henri.lombardi@univ-fcomte.fr` `http://hlombardi.free.fr`

Claude Quitté est Maître de conférences honoraire à l'Université de Poitiers.
Ses recherches concernent l'algèbre commutative effective et le calcul formel.
Il a programmé en `Magma` de très nombreux algorithmes en relation directe avec le présent ouvrage (cours et/ou exercices).
En collaboration avec Patrice Naudin, il a publié l'ouvrage *Algorithmique algébrique*, Masson, 1991.
Avec Henri Lombardi, il a participé à la rédaction de l'ouvrage collectif *Mathématiques L3 Algèbre*. Pearson Education, 2009.
Il a publié *Modules sur les anneaux commutatifs*, Calvage & Mounet, 2014, en collaboration avec Gema Díaz-Toca et Henri Lombardi.

`claude.quitte@math.univ-poitiers.fr`

Mathematics Subject Classification (2010)
– Primary : 13 Commutative Algebra.
– Secondary :
03F Proof theory and constructive mathematics.
06D Distributive lattices.
14Q Computational aspects of algebraic geometry.

ISBN 978-2-91-635286-2

⊛ Imprimé sur papier permanent

à James Brewer

Préface de la première édition

Ce livre est un cours d'introduction à l'algèbre commutative de base, avec un accent particulier mis sur les modules projectifs de type fini, qui constituent la version algébrique des fibrés vectoriels en géométrie différentielle.

Nous adoptons le point de vue constructif, avec lequel tous les théorèmes d'existence ont un contenu algorithmique explicite. En particulier, lorsqu'un théorème affirme l'existence d'un objet, solution d'un problème, un algorithme de construction de l'objet peut toujours être extrait de la démonstration qui est donnée.

Nous revisitons avec un regard nouveau et souvent simplificateur plusieurs théories classiques abstraites. En particulier, nous revenons sur des théories qui n'avaient pas de contenu algorithmique dans leur cadre naturel général, comme la théorie de Galois, celle des anneaux de Dedekind, celle des modules projectifs de type fini ou celle de la dimension de Krull.

L'algèbre constructive est en fait une vieille discipline, développée entre autres par Gauss et Kronecker. Nous nous situons dans la lignée de la «bible» moderne sur le sujet, qu'est le livre *A Course in Constructive Algebra* de Ray Mines, Fred Richman et Wim Ruitenburg, paru en 1988. Nous le citerons sous forme abrégée [MRR].

L'ouvrage correspond à un niveau de Master 2, du moins jusqu'au chapitre XIV, mais ne réclame comme prérequis que les notions de base concernant la théorie des groupes, l'algèbre linéaire sur les corps, les déterminants, les modules sur les anneaux commutatifs, ainsi que la définition des anneaux quotients et localisés. Une familiarité avec les anneaux de polynômes, les propriétés arithmétiques de $\mathbb{Z}$ et des anneaux euclidiens est également souhaitable.

Signalons enfin que nous considérons les exercices et problèmes (un peu plus de 320 en tout) comme une partie essentielle de l'ouvrage.

Nous essaierons de publier le maximum de corrigés manquants, ainsi que des exercices supplémentaires, sur la page web de l'un des auteurs :
`http://hlombardi.free.fr/publis/LivresBrochures.html`.

Remerciements

Nous remercions tou(te)s les collègues qui nous ont encouragés dans notre projet, nous ont apporté quelques sérieux coups de main ou fourni de précieuses informations. Et tout particulièrement MariEmi Alonso, Thierry Coquand, Gema Díaz-Toca, Lionel Ducos, M'hammed El Kahoui, Marco Fontana, Sarah Glaz, Laureano González-Vega, Emmanuel Hallouin, Hervé Perdry, Jean-Claude Raoult, Fred Richman, Marie-Françoise Roy, Peter Schuster et Ihsen Yengui. Last but not least, une mention toute spéciale pour notre expert Latex, François Pétiard.

Enfin, nous ne saurions oublier le Centre international de recherches mathématiques à Luminy et le Mathematisches Forschungsinstitut Oberwolfach, qui nous ont accueillis pour des séjours de recherche pendant la préparation de ce livre, nous offrant des conditions de travail inappréciables.

Henri Lombardi, Claude Quitté
Août 2011

Préface de la deuxième édition

Dans cette deuxième édition, nous avons corrigé les erreurs que nous avons débusquées ou qui nous ont été signalées. Voir `http://hlombardi.free.fr/publis/ErrataPTF-CM.pdf`

Nous avons ajouté des solutions d'exercices ainsi que quelques compléments. La plupart des compléments sont des corrections d'exercices ou de nouveaux exercices ou problèmes.

Les ajouts dans le cours sont les suivants.

Dans le chapitre II, on a précisé le principe local-global concret 3.5 et l'on a ajouté la proposition 3.8.

Dans le chapitre III, on a incorporé à l'énoncé du théorème 9.5 tout ce qui résulte du calcul de la mise en position de Noether, que le corps de base soit supposé contenu dans un corps algébriquement clos ou pas. Cela fait l'objet des points *1*, *2* et *3*. Les conséquences dans le cas où l'on connaît un corps algébriquement clos qui contient le corps de base sont décrites dans les points *4*, *5* et *6*. Dans la remarque qui suit le théorème, on introduit la notion de *dimension de Noether* d'un système polynomial sur un corps discret, qui s'avérera plus tard être égale à la dimension de Krull de l'algèbre quotient.

Dans le chapitre IV, un paragraphe sur les tenseurs nuls a été ajouté à la fin de la section 4. On a précisé la démonstration du lemme 7.1 (Bézout toujours trivial pour un anneau local).

Dans le chapitre VI, on a ajouté le théorème 2.6 de la base normale (démonstration d'Artin). On a ajouté quelques exemples pour le module des différentielles de Kähler après le théorème 6.7. À la fin de la section 6, on a ajouté une sous-section *Structure des algèbres nettes sur un corps discret* page 381. Le but est ici de donner une démonstration plus élémentaire de l'important résultat établi auparavant dans le corollaire 6.15. Concernant les algèbres galoisiennes, on a fait suivre la définition 7.2 par un théorème de même numéro qui donne l'exemple fondamental des algèbres galoisiennes libres, confirmé dans le corollaire 7.12.

Il y a plusieurs ajouts dans le chapitre VII. Des précisions sont apportées dans le théorème 5.3 (gestion dynamique d'un corps de racines) et la remarque qui suit. Des précisions sont apportées dans le théorème 5.4 (unicité du corps de racines, version dynamique). À la fin de la section 5, ajout d'un paragraphe : *Corps de racines, peut-on toujours se ramener au cas d'un polynôme séparable ?* Ajout d'une section 7 : *Clôture séparable dynamique d'un corps discret.*

Dans le chapitre VIII, le paragraphe sur les quotients de modules plats à la fin de la section 1 a été étoffé. On a ajouté une section 7 : *Polynômes non ramifiables.*

Dans le chapitre IX, on a ajouté une section 7 : *Anneau local séparablement clos.*

Dans le chapitre X, la sous-section *Groupe de Picard et groupe des classes d'idéaux* a été renommée *Diviseurs de Cartier, groupe de Picard et groupe des classes d'idéaux* : on a introduit ici la terminologie « groupe des diviseurs de Cartier » qui est la version additive du groupe des idéaux fractionnaires inversibles ; il s'agit d'une simple convention, mais qui s'avère souvent intuitivement efficace.

Dans le chapitre XI, la section 2 consacrée aux groupes réticulés a connu quelques améliorations notables. L'important principe de recouvrement par quotients 2.10 est un peu mieux formulé. La démonstration du théorème 2.16 (un groupe réticulé noethérien est à décomposition partielle) a été simplifiée. À la fin de la section, on a ajouté un paragraphe *Groupes réticulés de dimension* $\leqslant 1$ avec de nombreux résultats intéressants, notamment le principe de recouvrement 2.21, qui simplifient dans le chapitre suivant le sujet des anneaux de Prüfer cohérents de dimension $\leqslant 1$. L'ancien lemme 2.17 se retrouve plus loin en point *1* du théorème 2.20. On a aussi ajouté une section 6 : *Constructions de treillis distributifs.*

Dans le chapitre XII, on a transformé le lemme 1.4 en une proposition pour mettre en valeur dans le point *4* tout ce que l'on sait concernant les idéaux de type fini d'un anneau arithmétique. Le théorème 1.6 est légèrement amélioré. Dans le théorème 1.10, on a ajouté un point *3* dans le langage des diviseurs de Cartier. La démonstration du théorème 3.5 a été rectifiée. Dans la section 7, le théorème 7.2 sur les factorisations en dimension 1 a été considérablement développé, la relation avec le groupe des diviseurs de Cartier a été complètement explicitée. Le lemme 7.6 a été remplacé par un théorème qui contient beaucoup plus de résultats (l'ancien lemme est le point *1b* du théorème) : notamment le fait qu'une factorisation partielle d'une famille finie d'idéaux de type fini relève d'un principe local-global. Le principe local-global concret pour les anneaux de Dedekind 7.14 a été enrichi. Une sous-section *Norme d'un diviseur et applications* a été ajoutée page 795. Elle démontre le théorème 7.16 sur les extensions d'anneaux de

Dedekind, qui n'était pas disponible dans la première édition. Enfin, on a ajouté la section 8, *Anneau intègre versus anneau sans diviseur de zéro*, pour discuter d'un problème intéressant de décryptage des démonstrations classiques, insensibles à la distinction entre anneaux sans diviseur de zéro et anneaux intègres, pertinente du point de vue constructif.

Dans le chapitre XIII, la section 9, *Lying over, going up, going down*, a été un peu étoffée et les exercices 22 à 25 ont été ajoutés ou corrigés.

Enfin, dans le chapitre XV consacré aux principes local-globals, on a ajouté deux sections : 8, *Principes local-globals en profondeur* 1, et 9, *Principes local-globals en profondeur* 2.

Notons aussi que nous avons en général remplacé l'expression « relation de dépendance linéaire » par le terme plus court et plus usuel aujourd'hui « syzygie ».

Aucune numérotation n'a changé, sauf le principe local-global XII-7.13 devenu XII-7.14. Le nombre de pages a augmenté d'une centaine.

Il y a maintenant 319 exercices et 50 problèmes.

L'édition anglaise chez Springer en 2015 correspond à très peu près à cette version corrigée et augmentée française. Il manque cependant dans l'édition anglaise les sections VII-7, VIII-7, IX-7, XI-6 et XII-8, l'étude des groupes réticulés de dimension $\leqslant 1$ et de plusieurs conséquences dans la théorie des anneaux de Prüfer cohérents, ainsi que l'étude de la norme des diviseurs de Cartier dans le chapitre XII. Il manque aussi plusieurs nouveaux exercices ou solutions d'anciens exercices.

Toutes précisions utiles sur le site :

`http://hlombardi.free.fr/publis/LivresBrochures.html`

Remerciements

Aux remerciements figurant dans la préface de la première édition, nous tenons à ajouter des plus récents à l'intention de Darij Grinberg, Gerhard Angermüller et Matthé van der Lie pour leurs conseils avisés.

Enfin, nous n'oublierons pas de remercier tout particulièrement les éditions Calvage & Mounet pour leur travail remarquable concernant la très bonne lisibilité et la soigneuse mise en page du présent ouvrage.

Henri Lombardi, Claude Quitté
9 juin 2021

Table des matières

Avant-propos

Quant à moi, je proposerais de s'en tenir aux règles suivantes :

1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;

2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;

3. Éviter les classifications et les définitions non prédicatives.

Henri Poincaré,

dans *La logique de l'infini* (Revue de Métaphysique et de Morale, 1909).
Réédité dans *Dernières pensées*, Flammarion.

Ce livre est un cours d'introduction à l'algèbre commutative de base, avec un accent particulier mis sur les modules projectifs de type fini, qui constituent la version algébrique des fibrés vectoriels en géométrie différentielle.

Comme indiqué dans la préface, nous adoptons la méthode constructive, avec laquelle tous les théorèmes d'existence ont un contenu algorithmique explicite. Les mathématiques constructives peuvent être regardées comme la partie la plus théorique du calcul formel (computer algebra en anglais), qui s'occupe des mathématiques qui « tournent sur ordinateur ». Notre cours se distingue cependant des cours de calcul formel usuels sous deux aspects essentiels.

Tout d'abord, nos algorithmes sont le plus souvent seulement implicites, sous-jacents à la démonstration, et ne sont en aucune manière optimisés pour s'exécuter le plus rapidement possible, comme il est naturel lorsque l'on vise une implémentation efficace.

Ensuite, notre approche théorique est entièrement constructive, alors que les cours de calcul formel usuels se préoccupent peu de cette question. La philosophie n'est donc pas ici, comme il est d'usage « blanc ou noir, le bon chat est celui qui attrape la souris [1] », mais plutôt la suivante « le moyen fait partie de la recherche de la vérité, aussi bien que le résultat. Il faut que la recherche de la vérité soit elle-même vraie ; la recherche vraie, c'est la vérité déployée, dont les membres épars se réunissent dans le résultat [2] ».

Nous sommes amenés à parler souvent des deux points de vue, classique et constructif, sur un même sujet. En particulier, nous avons mis une étoile pour signaler les énoncés (théorèmes, lemmes...) qui sont vrais en mathématiques

1. Proverbe chinois.

2. Karl Marx, Remarques à propos de la récente instruction prussienne sur la censure, 1843 (cité par Georges Perec dans *Les Choses*).

classiques, mais dont nous ne donnons pas de démonstration constructive, et qui souvent ne peuvent pas en avoir. Ces énoncés « étoilés » ne seront donc probablement jamais implémentés sur machine, mais ils sont bien souvent utiles comme guides pour l'intuition, et au moins pour faire le lien avec les exposés usuels écrits dans le style des mathématiques classiques.

Pour ce qui concerne les définitions, nous donnons généralement en premier une variante constructive, la lectrice [3] voudra bien nous le pardonner, quitte à montrer en mathématiques classiques l'équivalence avec la définition usuelle. Le lecteur constatera que dans les démonstrations « étoilées » nous utilisons librement le lemme de Zorn et le principe du tiers exclu, tandis que les autres démonstrations ont toujours une traduction directe sous forme d'algorithme.

L'algèbre constructive est en fait une vieille discipline, développée en particulier par Gauss et Kronecker. Comme précisé également dans la préface, nous nous situons dans la lignée de la « bible » moderne sur le sujet, qu'est le livre *A Course in Constructive Algebra* de Ray Mines, Fred Richman et Wim Ruitenburg, paru en 1988. Nous le citerons sous forme abrégée [MRR]. Notre ouvrage est cependant autocontenu et nous ne réclamons pas [MRR] comme prérequis. Les livres de Harold M. Edwards de mathématiques constructives [Edwards89, Edwards05] et celui de Ihsen Yengui [Yengui] sont aussi à recommander.

Le contenu de l'ouvrage

Nous commençons par un bref commentaire sur les choix qui ont été faits concernant les thèmes traités.

La théorie des modules projectifs de type fini est un des thèmes unificateurs de l'ouvrage. Nous voyons cette théorie sous forme abstraite comme une théorie algébrique des fibrés vectoriels, et sous forme concrète comme celle des matrices idempotentes. La comparaison des deux points de vue est esquissée dans le chapitre introductif.

La théorie des modules projectifs de type fini proprement dite est traitée dans les chapitres V (premières propriétés), VI (algèbres qui sont des modules projectifs de type fini), X (théorie du rang et exemples), XIV (Splitting Off de Serre) et XVI (modules projectifs de type fini étendus).

Un autre thème unificateur est fourni par les principes local-globals, comme dans [Kunz] par exemple. Il s'agit d'un cadre conceptuel très efficace, même s'il est un peu vague. D'un point de vue constructif, on remplace la localisation en un idéal premier arbitraire par un nombre fini de localisations

3. La personne qui lit ce livre subit la règle inexorable de l'alternance des sexes. Espérons que les lecteurs n'en seront pas plus affectés que les lectrices. En tout cas, cela nous économisera bien des « ou » et bien des « (e) ».

en des monoïdes comaximaux. Les notions qui respectent le principe local-global sont «de bonnes notions», en ce sens qu'elles sont mûres pour le passage des anneaux commutatifs aux schémas de Grothendieck, que nous ne pourrons malheureusement pas aborder dans l'espace restreint de cet ouvrage.

Enfin, un dernier thème récurrent est donné par la méthode, tout à fait familière en calcul formel, dite de *l'évaluation paresseuse*, ou dans sa forme la plus aboutie, la méthode de *l'évaluation dynamique*. Cette méthode est expliquée dans les sections VII-2 et XV-5. Elle nous semble indispensable lorsque l'on veut mettre en place un traitement algorithmique des questions qui requièrent a priori la solution d'un problème de factorisation. Cette méthode a également permis la mise au point des machineries constructives locales-globales que l'on trouve dans les chapitres IV (pages 226 et 235), VIII (page 503), XI (principe XI-2.10) et XV (sections 5, 6 et 7). Elle est aussi à la source de la théorie constructive de la dimension de Krull (chapitre XIII), avec d'importantes applications dans les derniers chapitres.

Nous passons maintenant à une description plus détaillée du contenu de l'ouvrage.

Dans le chapitre I, nous expliquons les liens étroits que l'on peut établir entre la notion de fibré vectoriel en géométrie différentielle et celle de module projectif de type fini en algèbre commutative. Cela fait partie du processus général d'algébrisation en mathématiques, processus qui permet souvent de simplifier, d'abstraire et de généraliser de manière surprenante des concepts provenant de théories particulières.

Le chapitre II est consacré aux systèmes linéaires sur un anneau commutatif, traités sous forme élémentaire. Il ne requiert presqu'aucun appareillage théorique, mis à part la question de la localisation en un monoïde, dont nous donnons un rappel dans la section 1. Nous entrons ensuite dans notre sujet en mettant en place le principe local-global concret pour la résolution des systèmes linéaires (section 2), un outil simple et efficace qui sera repris et diversifié sans cesse. D'un point de vue constructif, la résolution des systèmes linéaires fait immédiatement apparaître comme central le concept d'anneau cohérent que nous traitons dans la section 3. Les anneaux cohérents sont ceux pour lesquels on a une prise minimale sur la solution des systèmes linéaires homogènes. De manière très étonnante, ce concept n'apparaît pas dans les traités classiques d'algèbre commutative. C'est qu'en général cette notion est complètement occultée par celle d'anneau noethérien. Cette occultation n'a pas lieu en mathématiques constructives où la noethérianité n'implique pas nécessairement la cohérence. Nous développons dans la section 4 la question des produits finis d'anneaux, avec la notion de système fondamental d'idempotents orthogonaux et le théorème des restes chinois.

La longue section 5 est consacrée à de nombreuses variations sur le thème des déterminants. Enfin, la section 6 revient sur le principe local-global de base, dans une version un peu plus générale consacrée aux suites exactes de modules.

Le chapitre III développe la méthode des coefficients indéterminés, développée par Gauss. De très nombreux théorèmes d'existence en algèbre commutative reposent sur des « identités algébriques sous conditions » et donc sur des appartenances $g \in \langle f_1, \ldots, f_s \rangle$ dans un anneau $\mathbb{Z}[c_1, \ldots, c_r, X_1, \ldots, X_n]$, où les X_i sont les variables et les c_j les paramètres du théorème considéré. En ce sens, on peut considérer que l'algèbre commutative est une vaste théorie des identités algébriques, qui trouve son cadre naturel dans la méthode des coefficients indéterminés, c'est-à-dire la méthode dans laquelle les paramètres du problème à traiter sont pris comme des indéterminées. Forts de cette certitude, nous sommes, autant que faire se pouvait, systématiquement « partis à la chasse des identités algébriques », ceci non seulement dans les chapitres II et III « purement calculatoires », mais dans tout l'ouvrage. En bref, plutôt que d'affirmer en filigrane d'un théorème d'existence « il existe une identité algébrique qui certifie cette existence », nous avons tâché de donner chaque fois l'identité algébrique elle-même.

Ce chapitre III peut être considéré comme un cours d'algèbre de base avec les méthodes du 19e siècle. Les sections 1, 2 et 3 donnent quelques généralités sur les polynômes, avec notamment l'algorithme de factorisation partielle, la « théorie des identités algébriques » (qui explique la méthode des coefficients indéterminés), les polynômes symétriques élémentaires, le lemme de Dedekind-Mertens et le théorème de Kronecker. Ces deux derniers résultats sont des outils de base qui donnent des informations précises sur les coefficients du produit de deux polynômes ; ils sont souvent utilisés dans le reste de l'ouvrage. La section 4 introduit l'algèbre de décomposition universelle d'un polynôme unitaire sur un anneau commutatif arbitraire, qui est un substitut efficace au corps des racines d'un polynôme sur un corps. La section 5 est consacrée au discriminant et explique en quel sens précis une matrice générique est diagonalisable. Avec ces outils en mains, on peut traiter la théorie de Galois de base dans la section 6. La théorie élémentaire de l'élimination via le résultant est donnée dans la section 7. On peut alors donner les bases de la théorie algébrique des nombres, avec le théorème de décomposition unique en facteurs premiers pour un idéal de type fini d'un corps de nombres (section 8). La section 9 donne la mise en position de Noether et le Nullstellensatz de Hilbert comme applications du résultant. En particulier le théorème 9.5 donne un algorithme qui traite un système polynomial sur un corps discret infini et fournit sa mise en position de Noether grâce à un changement de variables linéaire. Enfin, la section 10 sur la méthode de Newton en algèbre termine le chapitre III.

Le chapitre IV est consacré à l'étude des propriétés élémentaires des modules de présentation finie. Ces modules jouent un peu le même rôle pour les anneaux que les espaces vectoriels de dimension finie pour les corps : la théorie des modules de présentation finie est une manière un peu plus abstraite, et souvent profitable, d'aborder la question des systèmes linéaires. Les sections 1 à 4 donnent les propriétés de stabilité de base ainsi que l'exemple important de l'idéal d'un zéro pour un système polynomial (sur un anneau commutatif arbitraire). On s'intéresse ensuite au problème de classification des modules de présentation finie sur un anneau donné. Sur le chemin des anneaux principaux, pour lesquels le problème de classification est complètement résolu (section 7), nous rencontrons les anneaux quasi intègres (section 6), qui sont les anneaux où l'annulateur d'un élément est toujours engendré par un idempotent. C'est l'occasion de mettre en place une *machinerie locale-globale élémentaire* qui permet de passer d'un résultat établi constructivement pour les anneaux intègres au même résultat, convenablement reformulé, pour les anneaux quasi intègres. Cette machinerie de transformation de preuves est élémentaire, car fondée sur la décomposition d'un anneau en produit fini d'anneaux. La chose intéressante est que cette décomposition est obtenue par relecture de la démonstration constructive écrite dans le cas intègre : on voit ici qu'en mathématiques constructives la démonstration est souvent encore plus importante que le résultat. De la même manière, on a une machinerie locale-globale élémentaire qui permet de passer d'un résultat établi constructivement pour les corps discrets au même résultat, convenablement reformulé, pour les anneaux zéro-dimensionnels réduits (section 8). Les anneaux zéro-dimensionnels, ici définis de manière élémentaire, constituent une clé importante de l'algèbre commutative, comme étape intermédiaire pour généraliser certains résultats des corps discrets aux anneaux commutatifs arbitraires. Dans la littérature classique, ils apparaissent souvent sous leur forme noethérienne, c'est-à-dire celle des anneaux artiniens. La section 9 introduit les invariants très importants que sont les idéaux de Fitting d'un module de présentation finie. Enfin, la section 10 applique cette notion pour introduire l'idéal résultant d'un idéal de type fini dans un anneau de polynômes quand l'idéal en question contient un polynôme unitaire, et démontrer un théorème d'élimination algébrique sur un anneau arbitraire.

Le chapitre V est une première approche de la théorie des modules projectifs de type fini. Les sections 2 à 5 donnent les propriétés de base ainsi que l'exemple important des modules projectifs de type fini sur les anneaux zéro-dimensionnels. La section 6 donne le théorème de structure locale : un module est projectif de type fini si, et seulement si, il devient libre après localisation en des éléments comaximaux convenables. Sa démonstration constructive est une relecture d'un résultat établi dans le chapitre II

pour les systèmes linéaires « bien conditionnés » (théorème II-5.26). La section 7 développe l'exemple des modules projectifs localement monogènes. La section 8 introduit le déterminant d'un endomorphisme d'un module projectif de type fini. Cela donne accès à la décomposition d'un tel module en somme directe de ses composants de rang constant. Enfin, la section 9, que l'on ne savait pas bien où mettre dans l'ouvrage, héberge quelques considérations supplémentaires sur les *propriétés de caractère fini*, une notion introduite au chapitre II pour discuter les rapports entre principes local-globals concrets et principes local-globals abstraits.

Le chapitre VI est consacré aux algèbres de type fini, avec une insistance particulière sur les algèbres qui sont des modules projectifs de type fini sur leur anneau de base, que nous appelons algèbres strictement finies. La section 1 traite le cas où l'anneau de base est un corps discret. Elle donne des versions constructives pour les théorèmes de structure obtenus en mathématiques classiques. Le cas des algèbres étales (quand le discriminant est inversible) est particulièrement éclairant. On découvre que les théorèmes classiques supposent toujours implicitement que l'on sache factoriser les polynômes séparables sur le corps de base. La démonstration constructive du théorème de l'élément primitif 1.9 est significative par son écart avec la démonstration classique. La section 2 applique les résultats précédents pour terminer la théorie de Galois de base commencée dans la section III-6 en caractérisant les extensions galoisiennes de corps discrets comme les extensions étales et normales. La section 3 est une brève introduction aux algèbres de présentation finie, en insistant sur le cas des algèbres entières, avec un Nullstellensatz faible et le lemme lying over dans des versions constructives. La section 4 introduit les algèbres strictement finies sur un anneau arbitraire. Dans les sections 5 et 6, sont introduites les notions voisines d'algèbre strictement étale et d'algèbre séparable qui généralisent la notion d'algèbre étale sur un corps discret. Un théorème particulièrement important (théorème 6.18) est celui qui dit que toute algèbre nette sur un corps discret est étale. Dans la section 7, nous donnons un exposé constructif des bases de la théorie des algèbres galoisiennes pour les anneaux commutatifs. Il s'agit en fait d'une théorie d'Artin-Galois, puisqu'elle reprend l'approche qu'Artin avait développée pour le cas des corps, en partant directement d'un groupe fini d'automorphismes d'un corps, le corps de base n'apparaissant que comme un sous-produit des constructions qui s'ensuivent.

Dans le chapitre VII, la méthode dynamique, une pierre angulaire des méthodes modernes en algèbre constructive, est mise en œuvre pour traiter d'un point de vue constructif le corps des racines d'un polynôme et la théorie de Galois dans le cas séparable, lorsque la proie s'échappe pour laisser place à son ombre, c'est-à-dire lorsque l'on ne sait pas factoriser les polynômes sur le corps de base que l'on considère. À titre d'entraînement,

la section 1 commence par établir des résultats sous forme constructive pour le Nullstellensatz lorsque l'on ne sait pas factoriser les polynômes sur le corps de base. Des considérations d'ordre général sur la méthode dynamique sont développées dans la section 2. On ne doit pas considérer le corps de racines d'un polynôme comme un objet usuel «statique», mais comme un objet «dynamique». Ce phénomène est inévitable, car il faut gérer une double ambiguïté. Celle qui résulte de la théorie de Galois classique à travers l'indiscernabilité des racines d'un polynôme irréductible. Et celle qui résulte de l'impossibilité de connaître le groupe de Galois d'un polynôme par une méthode infaillible. Par ailleurs, le dépaysement produit par cette mise en perspective dynamique n'est qu'un exemple de la méthode générale dite d'évaluation paresseuse : *rien ne sert de trop se fatiguer pour connaître toute la vérité quand une vérité partielle est suffisante pour les enjeux du calcul en cours.* La section 5 donne une approche constructive et dynamique du corps de racines d'un polynôme sur un corps discret, sans hypothèse de séparabilité pour le polynôme. La théorie de Galois dynamique d'un polynôme séparable sur un corps discret est développée dans la section 6. Enfin la section 7 explique comment traiter de manière dynamique la clôture séparable d'un corps discret sans utiliser ni le principe du tiers exclu (c'est-à-dire ici sans prétendre connaître la factorisation des polynômes sur ce corps), ni le lemme de Zorn.

Le chapitre VIII est une brève introduction aux modules plats et aux algèbres plates et fidèlement plates. En langage intuitif, une $\mathbf{A}$-algèbre $\mathbf{B}$ est plate lorsque les systèmes linéaires sur $\mathbf{A}$ sans second membre n'ont «pas plus» de solutions dans $\mathbf{B}$ que dans $\mathbf{A}$, et elle est fidèlement plate si cette affirmation est vraie également des systèmes linéaires avec second membre. Ces notions cruciales de l'algèbre commutative ont été introduites par Serre dans [177, GAGA,1956]. Nous ne donnons que les résultats vraiment fondamentaux. C'est également l'occasion d'introduire les notions d'anneau localement sans diviseur de zéro, de module sans torsion (pour un anneau arbitraire), d'anneau arithmétique et d'anneau de Prüfer. Nous insistons comme toujours sur le principe local-global quand il s'applique. Enfin, la section 7, *Polynômes non ramifiables*, répond à la question suivante : étant donné un polynôme unitaire $f \in \mathbf{k}[X]$ pour un anneau arbitraire $\mathbf{k}$, quand la $\mathbf{k}$-algèbre $(\mathbf{k}[X]/\langle f\rangle)[1/f']$ est-elle fidèlement plate ?

Le chapitre IX parle des anneaux locaux et de quelques généralisations. La section 1 introduit la terminologie constructive pour quelques notions classiques usuelles, dont la notion importante de radical de Jacobson. Une notion connexe est celle d'anneau résiduellement zéro-dimensionnel (un anneau $\mathbf{A}$ tel que $\mathbf{A}/\operatorname{Rad}\mathbf{A}$ est zéro-dimensionnel). C'est une notion robuste, qui n'utilise jamais les idéaux maximaux, et la plupart des théorèmes de la littérature concernant les anneaux semi-locaux (en mathématiques classiques ce sont les

anneaux qui n'ont qu'un nombre fini d'idéaux maximaux) s'appliquent aux anneaux résiduellement zéro-dimensionnels. La section 2 répertorie quelques résultats qui montrent que sur un anneau local on ramène la solution de certains problèmes au cas des corps. Les sections 3 et 4 établissent sur des exemples géométriques (c'est-à-dire concernant l'étude de systèmes polynomiaux) un lien entre la notion d'étude locale au sens intuitif topologique et l'étude de certaines localisations d'anneaux (dans le cas d'un corps discret à la base, ces localisations sont des anneaux locaux). On introduit notamment les notions d'espaces tangent et cotangent en un zéro d'un système polynomial. La section 5 fait une brève étude des anneaux décomposables, dont un cas particulier en mathématiques classiques sont les anneaux décomposés (produits finis d'anneaux locaux), qui jouent un rôle important dans la théorie des anneaux locaux henséliens. La section 6 traite la notion d'anneau local-global, qui généralise à la fois celle d'anneau local et celle d'anneau zéro-dimensionnel. Ces anneaux vérifient des propriétés locales-globales très fortes, par exemple les modules projectifs de rang constant sont toujours libres, et ils sont stables par extensions entières. Dans la section 7, *Anneau local séparablement clos*, nous continuons la section VIII-7 sur les polynômes non ramifiables pour le cas des anneaux locaux, et nous faisons une brève discussion de la notion d'anneau local hensélien séparablement clos.

Le chapitre X poursuit l'étude des modules projectifs de type fini commencée dans le chapitre V. Dans la section 1, nous reprenons la question de la caractérisation des modules projectifs de type fini comme modules localement libres, c'est-à-dire du théorème de structure locale. Nous en donnons une version matricielle (théorème 1.7), qui résume et précise les différents énoncés du théorème. La section 2 est consacrée à l'anneau des rangs sur $\mathbf{A}$. En mathématiques classiques, le rang d'un module projectif de type fini est défini comme une fonction localement constante sur le spectre de Zariski. Nous donnons ici une théorie élémentaire du rang qui ne fait pas appel aux idéaux premiers. Dans la section 3, nous donnons quelques applications simples du théorème de structure locale. La section 4 est une introduction aux grassmanniennes, et dans la section 5, nous introduisons le problème général de la classification complète des modules projectifs de type fini sur un anneau $\mathbf{A}$ fixé. Cette classification est un problème fondamental et difficile, qui n'admet pas de solution algorithmique générale. La section 6 présente un exemple non trivial pour lesquels cette classification peut être obtenue.

Le chapitre XI est consacré aux treillis distributifs et aux groupes réticulés. Les deux premières sections décrivent ces structures algébriques ainsi que leurs propriétés de base. Ces structures sont importantes en algèbre commutative pour plusieurs raisons.

▷ Une première raison de s'intéresser aux treillis distributifs est que la théorie de la divisibilité a comme « modèle idéal » la théorie de la divisibilité des entiers naturels. La structure du monoïde multiplicatif $(\mathbb{N}^*, \times, 1)$ est reliée au fait qu'il s'agit de la partie positive d'un groupe réticulé. Cela se généralise en algèbre commutative dans deux directions. La première généralisation est la théorie des anneaux intègres dont les idéaux de type fini forment un treillis distributif, appelés des domaines de Prüfer, que nous étudions dans le chapitre XII : leurs idéaux de type fini non nuls forment la partie positive d'un groupe réticulé. La deuxième est la théorie des anneaux à pgcd étudiée dans la section 3. La section 2 est consacrée aux groupes réticulés. Elle comporte l'important principe de recouvrement par quotients 2.10, qui est une sorte d'analogue du principe local-global concret en algèbre commutative. À la fin de la section, le paragraphe *Groupes réticulés de dimension* $\leqslant 1$ contient de nombreux résultats intéressants qui simplifient dans le chapitre suivant le traitement des anneaux de Prüfer cohérents de dimension $\leqslant 1$. Signalons la première apparition dans la section 3 de la dimension de Krull $\leqslant 1$ des anneaux commutatifs avec le résultat suivant (théorème 3.12) : un anneau à pgcd intègre de dimension $\leqslant 1$ est un anneau de Bézout. La section 6, *Constructions de treillis distributifs*, s'appuie sur la version des treillis distributifs basée sur les relations implicatives, développée dans la section 5.

▷ Une deuxième raison de s'intéresser aux treillis distributifs est que ces derniers interviennent comme la contrepartie constructive des espaces spectraux divers et variés qui se sont imposés comme des outils puissants de l'algèbre abstraite. Les rapports entre treillis distributifs et espaces spectraux seront abordés dans la section XIII-1. Dans la section XI-4, nous mettons en place le treillis de Zariski d'un anneau commutatif $\mathbf{A}$, qui est la contrepartie constructive du fameux *spectre de Zariski*. Notre but ici est d'établir le parallèle entre la construction de la clôture zéro-dimensionnelle réduite d'un anneau (notée $\mathbf{A}^\bullet$) et celle de l'algèbre de Boole engendrée par un treillis distributif (qui fait l'objet du théorème 4.26). L'objet $\mathbf{A}^\bullet$ ainsi construit contient essentiellement la même information que le produit des anneaux $\mathrm{Frac}(\mathbf{A}/\mathfrak{p})$ pour tous les idéaux premiers $\mathfrak{p}$ de $\mathbf{A}$ [4]. Ce résultat est en relation étroite avec le fait que le treillis de Zariski de $\mathbf{A}^\bullet$ est l'algèbre de Boole engendrée par le treillis de Zariski de $\mathbf{A}$.

▷ Une troisième raison de s'intéresser aux treillis distributifs est la logique constructive (ou intuitionniste). Dans cette logique, l'ensemble des valeurs de vérité de la logique classique, à savoir $\{\mathsf{Vrai}, \mathsf{Faux}\}$, qui est une algèbre de Boole à deux éléments, est remplacé par un treillis distributif assez mystérieux. La logique constructive sera abordée de manière informelle dans

4. Ce produit n'est pas accessible en mathématiques constructives, $\mathbf{A}^\bullet$ en est un substitut constructif tout à fait efficace.

l'annexe. Dans la section 5, nous mettons en place les outils qui servent de cadre à une étude algébrique formelle de la logique constructive : les relations implicatives et les algèbres de Heyting. Par ailleurs, relations implicatives et algèbres de Heyting ont leur utilité propre dans l'étude générale des treillis distributifs. Par exemple, le treillis de Zariski d'un anneau noethérien cohérent est une algèbre de Heyting (proposition 6.9).

Le chapitre XII traite les anneaux arithmétiques, les anneaux de Prüfer et les anneaux de Dedekind. Il commence par quelques remarques d'ordre épistémologique sur l'intérêt intrinsèque d'aborder les problèmes de factorisation avec le théorème de factorisation partielle plutôt qu'avec celui de factorisation totale. Les anneaux arithmétiques sont les anneaux dont le treillis des idéaux de type fini est distributif. Un anneau de Prüfer est un anneau arithmétique réduit et il est caractérisé par le fait que tous ses idéaux sont plats. Un anneau de Prüfer cohérent est la même chose qu'un anneau arithmétique quasi intègre. Il est caractérisé par le fait que ses idéaux de type fini sont projectifs. Un anneau de Dedekind est un anneau de Prüfer cohérent noethérien et fortement discret (en mathématiques classiques avec le principe du tiers exclu tout anneau est fortement discret et tout anneau noethérien est cohérent). Ces anneaux sont apparus tout d'abord avec les anneaux d'entiers de corps de nombres. Le paradigme dans le cas intègre est la décomposition unique en facteurs premiers de tout idéal de type fini non nul. Les propriétés arithmétiques du monoïde multiplicatif des idéaux de type fini sont pour l'essentiel vérifiées par les anneaux arithmétiques. Pour les propriétés les plus subtiles concernant la factorisation des idéaux de type fini, et notamment la décomposition en facteurs premiers, une hypothèse noethérienne, ou au moins de dimension $\leqslant 1$, est indispensable. Dans ce chapitre, nous avons voulu montrer la progression des propriétés satisfaites par les anneaux au fur et à mesure que l'on renforce les hypothèses, depuis les anneaux arithmétiques jusqu'aux anneaux de Dedekind à factorisation totale. Nous insistons sur le caractère algorithmique simple des définitions dans le cadre constructif. Certaines propriétés ne dépendent que de la dimension $\leqslant 1$, et nous avons voulu rendre justice aux anneaux quasi intègres de dimension $\leqslant 1$. Nous avons également développé une étude du problème de la décomposition en facteurs premiers plus progressive et plus fine que dans les exposés qui s'autorisent le principe du tiers exclu. Par exemple, les théorèmes 4.10 et 7.12 donnent des versions constructives précises du théorème concernant les extensions finies séparables d'anneaux de Dedekind, avec ou sans la propriété de factorisation totale. Dans la sous-section *Norme d'un diviseur et applications*, la notion introduite permet d'établir le théorème 7.16 général sur les extensions d'anneaux de Dedekind.

La section finale 8, *Anneau intègre versus anneau sans diviseur de zéro*, discute un problème intéressant de décryptage des démonstrations classiques, insensibles à la distinction entre anneaux sans diviseur de zéro et anneaux intègres, pertinente du point de vue constructif.

Le chapitre XIII est consacré à la dimension de Krull des anneaux commutatifs, à celle de leurs morphismes, à celle des treillis distributifs et à la dimension valuative des anneaux commutatifs. Plusieurs notions importantes de dimension en algèbre commutative classique sont des dimensions d'espaces spectraux. Ces espaces topologiques très particuliers jouissent de la propriété d'être entièrement décrits (au moins en mathématiques classiques) par leurs ouverts quasi-compacts, qui forment un treillis distributif. Il s'avère que le treillis distributif correspondant a en général une interprétation simple, sans recours aucun aux espaces spectraux. En 1974, André Joyal a montré comment définir constructivement la dimension de Krull d'un treillis distributif. Depuis ce jour faste, la théorie de la dimension qui semblait baigner dans des espaces éthérés, invisibles lorsque l'on ne fait pas confiance à l'axiome du choix, est devenue (au moins en principe) une théorie de nature élémentaire, sans plus aucun mystère. La section 1 décrit l'approche de la dimension de Krull en mathématiques classiques. Elle explique aussi comment on peut interpréter la dimension de Krull d'un tel espace en termes du treillis distributif de ses ouverts quasi-compacts. La section 2 donne la définition constructive de la dimension de Krull d'un anneau commutatif, notée $\mathsf{Kdim}\,\mathbf{A}$, et en tire quelques conséquences. La section 3 donne quelques propriétés plus avancées, et notamment le principe local-global et le principe de recouvrement fermé pour la dimension de Krull. La section 4 traite la dimension de Krull des extensions entières et la section 5 celle des anneaux géométriques (correspondant aux systèmes polynomiaux) sur les corps discrets. La section 6 donne la définition constructive de la dimension de Krull d'un treillis distributif et montre que la dimension de Krull d'un anneau commutatif et celle de son treillis de Zariski coïncident. La section 7 est consacrée à la dimension des morphismes entre anneaux commutatifs. La définition utilise la clôture zéro-dimensionnelle réduite de l'anneau source du morphisme. Pour démontrer la formule qui majore $\mathsf{Kdim}\,\mathbf{B}$ à partir de $\mathsf{Kdim}\,\mathbf{A}$ et $\mathsf{Kdim}\,\rho$ (lorsque l'on a un morphisme $\rho : \mathbf{A} \to \mathbf{B}$), nous devons introduire la clôture quasi intègre minimale d'un anneau commutatif. Cet objet est une contrepartie constructive du produit de tous les $\mathbf{A}/\mathfrak{p}$, lorsque $\mathfrak{p}$ parcourt les idéaux premiers minimaux de $\mathbf{A}$. La section 8 introduit la dimension valuative d'un anneau commutatif et utilise cette notion notamment pour démontrer le résultat important suivant : pour un anneau arithmétique non nul $\mathbf{A}$, on a $\mathsf{Kdim}\,\mathbf{A}[X_1, \ldots, X_n] = n + \mathsf{Kdim}\,\mathbf{A}$. La section 9 donne des versions constructives des théorèmes Going up et Going down.

Dans le chapitre XIV, intitulé *Nombre de générateurs d'un module*, on établit la version élémentaire, non noethérienne et constructive de « grands » théorèmes d'algèbre commutative, dus dans leurs versions originales à Kronecker, Bass, Serre, Forster et Swan. Ces résultats concernent le nombre de générateurs radicaux d'un idéal de type fini, le nombre de générateurs d'un module, la possibilité de produire un sous-module libre en facteur direct dans un module, et la possibilité de simplifier des isomorphismes, dans le style suivant : si $M \oplus N \simeq M' \oplus N$ alors $M \simeq M'$. Ils font intervenir la dimension de Krull ou d'autres dimensions plus sophistiquées, introduites par R. Heitmann ainsi que par Thierry Coquand et les auteurs de cet ouvrage. La section 1 est consacrée au théorème de Kronecker et à ses extensions (la plus aboutie, non noethérienne, est due à R. Heitmann [104]). Le théorème de Kronecker est usuellement énoncé sous la forme suivante : une variété algébrique dans $\mathbb{C}^n$ peut toujours être définie par $n+1$ équations. La forme due à Heitmann affirme que dans un anneau de dimension de Krull inférieure ou égale à n, pour tout idéal de type fini $\mathfrak{a}$, il existe un idéal $\mathfrak{b}$ engendré par au plus $n+1$ éléments de $\mathfrak{a}$ tel que $\sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a}}$. La démonstration donne aussi le théorème de Bass, dit « stable range ». Ce dernier théorème a été amélioré en faisant intervenir des dimensions « meilleures » que la dimension de Krull. Cela fait l'objet de la section 2, où est définie la *dimension de Heitmann*, découverte en lisant avec attention les démonstrations de Heitmann (Heitmann utilise une autre dimension, a priori un peu moins bonne, que nous expliquons également en termes constructifs). Dans la section 3, nous expliquons quelles sont les propriétés matricielles d'un anneau qui permettent de faire fonctionner les théorèmes de Serre (Splitting Off), de Forster-Swan (contrôle du nombre de générateurs d'un module de type fini en fonction du nombre de générateurs local) et le théorème de simplification de Bass. La section 4 introduit les notions de support (une application d'un anneau dans un treillis distributif vérifiant certains axiomes) et de n-stabilité. Cette dernière notion a été définie par Thierry Coquand, après avoir analysé une démonstration de Bass qui établit que les modules projectifs de type fini sur un anneau $\mathbf{V}[X]$, où $\mathbf{V}$ est un anneau de valuation de dimension de Krull finie, sont libres. Dans la dernière section, on démontre que la propriété matricielle cruciale introduite dans la section 3 est satisfaite, d'une part, par les anneaux n-stables, d'autre part par les anneaux de dimension de Heitmann $< n$ (et a fortiori par les anneaux de dimension de Krull $< n$).

Le chapitre XV est consacré au principe local-global et à ses variantes. La section 1 introduit la notion de recouvrement d'un monoïde par une famille finie de monoïdes, ce qui généralise la notion de monoïdes comaximaux. Le lemme de recouvrement 1.5 sera décisif dans la section 5. La section 2 donne des principes local-globals concrets. Il s'agit de dire que certaines propriétés

sont vraies globalement dès qu'elles le sont localement. Ici, « localement » est pris au sens constructif : après localisation en un nombre fini de monoïdes comaximaux. La plupart des résultats ont été établis dans les chapitres précédents. Leur regroupement fait voir la portée très générale de ces principes. La section 3 reprend certains de ces principes sous forme de principes local-globals abstraits. Ici, « localement » est pris au sens abstrait, c'est-à-dire après localisation en n'importe quel idéal premier. C'est surtout la comparaison avec les principes local-globals concrets correspondants qui nous intéresse. La section 4 explique la construction d'objets « globaux » à partir d'objets de même nature définis uniquement de manière locale, comme il est usuel en géométrie différentielle. C'est l'impossibilité de cette construction lorsque l'on cherche à recoller certains anneaux qui est à l'origine des schémas de Grothendieck. En ce sens, les sections 2 et 4 constituent la base à partir de laquelle on peut développer la théorie des schémas dans un cadre complètement constructif. Les sections suivantes sont d'une autre nature. D'ordre méthodologique, elles sont consacrées au décryptage de différentes variantes du principe local-global en mathématiques classiques. Par exemple, la localisation en tous les idéaux premiers, le passage au quotient par tous les idéaux maximaux ou la localisation en tous les idéaux premiers minimaux, qui s'appliquent chacune dans des situations particulières. Un tel décryptage présente un caractère certainement déroutant dans la mesure où il prend pour point de départ une démonstration classique qui utilise des théorèmes en bonne et due forme, mais où le décryptage constructif de cette démonstration n'est pas seulement donné par l'utilisation de théorèmes constructifs en bonne et due forme. Il faut aussi regarder ce que fait la démonstration classique avec ses objets purement idéaux (des idéaux maximaux par exemple) pour comprendre comment elle nous donne le moyen de construire un nombre fini d'éléments qui vont être impliqués dans un théorème constructif (un principe local-global concret par exemple) pour aboutir au résultat souhaité. En décryptant une telle démonstration, nous utilisons la méthode dynamique générale exposée au chapitre VII. Nous décrivons ainsi des *machineries locales-globales* nettement moins élémentaires que celles du chapitre IV : la machinerie locale-globale constructive de base à idéaux premiers (section 5), la machinerie locale-globale constructive à idéaux maximaux (section 6) et la machinerie locale-globale constructive à idéaux premiers minimaux (section 7). En réalisant « le programme de Poincaré » cité en exergue de cet avant-propos, nos machineries locales-globales prennent en compte une remarque essentielle de Lakatos, à savoir que la chose la plus intéressante et robuste dans un théorème, c'est toujours sa démonstration, même si elle est critiquable à certains égards (voir [Lakatos]). Dans les sections 8 et 9, nous examinons dans quelle mesure certains principes local-globals restent valides lorsque l'on remplace dans les énoncés les listes d'éléments comaximaux par des listes de profondeur $\geqslant 1$ ou de profondeur $\geqslant 2$.

Dans le chapitre XVI, nous traitons la question des modules projectifs de type fini sur les anneaux de polynômes. La question décisive est d'établir pour quelles classes d'anneaux les modules projectifs de type fini sur un anneau de polynômes proviennent par extension des scalaires d'un module projectif de type fini sur l'anneau lui-même (éventuellement en posant certaines restrictions sur les modules projectifs de type fini considérés ou sur le nombre de variables dans l'anneau de polynômes). Quelques généralités sur les modules étendus sont données dans la section 1. Le cas des modules projectifs de rang constant 1, complètement éclairci par le théorème de Traverso-Swan-Coquand, est traité dans la section 2. La démonstration constructive de Coquand utilise de manière cruciale la machinerie locale-globale constructive à idéaux premiers minimaux. La section 3 traite les théorèmes de recollement de Quillen (Quillen patching) et Vaserstein, qui disent que certains objets sont obtenus par extension des scalaires (depuis l'anneau de base à un anneau de polynômes) si, et seulement si, cette propriété est vérifiée localement. Nous donnons aussi une sorte de réciproque du Quillen patching, due à Roitman, sous forme constructive. La section 4 est consacrée aux théorèmes de Horrocks. La démonstration constructive du théorème de Horrocks global fait subir à la démonstration du théorème de Horrocks local la machinerie locale-globale de base et se conclut avec le Quillen patching constructif. La section 5 donne plusieurs preuves constructives du théorème de Quillen-Suslin (les modules projectifs de type fini sur un anneau de polynômes sur un corps discret sont libres), fondées sur différentes démonstrations classiques. La section 6 établit le théorème de Lequain-Simis (les modules projectifs de type fini sur un anneau de polynômes sur un anneau arithmétique sont étendus). La démonstration utilise la méthode dynamique exposée au chapitre VII, cela permet d'établir le théorème d'induction de Yengui, une variante constructive de l'induction de Lequain-Simis.

Dans le chapitre XVII, nous démontrons le « Suslin Stability Theorem » dans le cas particulier des corps discrets. Ici aussi, pour obtenir une démonstration constructive, nous utilisons la machinerie locale-globale de base exposée au chapitre XV.

L'annexe décrit la théorie des ensembles constructive à la Bishop. Elle peut être vue comme une introduction à la logique constructive. On y explique la sémantique de Brouwer-Heyting-Kolmogorov pour les connecteurs et quantificateurs. On discute certaines formes faibles du principe du tiers exclu ainsi que plusieurs principes problématiques en mathématiques constructives.

Quelques remarques d'ordre épistémologique

Nous espérons dans cet ouvrage montrer que des livres classiques d'algèbre commutative comme [Atiyah & Macdonald], [Eisenbud], [Gilmer], [Glaz], [Kaplansky], [Knapp, 1], [Knapp, 2], [Kunz], [Lafon & Marot], [Lam06] (dont la lecture est vivement recommandée), [Matsumura], [Northcott], ou même [Bourbaki] et le remarquable ouvrage [Stacks-Project] disponible sur le réseau, pourront entièrement être récrits avec un point de vue constructif, dissipant le voile de mystère qui entoure les théorèmes d'existence non explicites des mathématiques classiques. Naturellement, nous espérons que les lectrices profiteront de notre ouvrage pour jeter un regard nouveau sur les livres de calcul formel classiques, comme par exemple [Cox, Little & O'Shea], [COCOA], [SINGULAR], [Ene & Herzog], [Elkadi & Mourrain], [Mora], [TAPAS] ou [von zur Gathen & Gerhard].

Dans la mesure où nous voulons un traitement algorithmique de l'algèbre commutative, nous ne pouvons pas utiliser toutes les facilités que donnent l'usage systématique du lemme de Zorn et du principe du tiers exclu en mathématiques classiques. Sans doute, le lecteur comprend bien qu'il est difficile d'implémenter le lemme de Zorn en calcul formel. Le refus du principe du tiers exclu doit par contre lui sembler plus dur à avaler. Ce n'est de notre part qu'une constatation pratique. Si dans une démonstration classique, vous trouvez un raisonnement qui conduit à un calcul du type : « si x est inversible, faire ceci, sinon faire cela », il est bien clair que cela ne se traduit directement sous forme d'un algorithme que dans le cas où l'on dispose d'un test d'inversibilité dans l'anneau en question. C'est pour insister sur cette difficulté, que nous devons contourner en permanence, que nous sommes amenés à parler souvent des deux points de vue, classique et constructif, sur un même sujet.

On peut discuter indéfiniment pour savoir si les mathématiques constructives sont une partie des mathématiques classiques, la partie qui s'occupe exclusivement des aspects explicites des choses, ou si au contraire ce sont les mathématiques classiques qui sont une partie des mathématiques constructives, la partie dont les théorèmes sont « étoilés », c'est-à-dire qui rajoutent systématiquement dans leurs hypothèses le principe du tiers exclu et l'axiome du choix. Un de nos objectifs est de faire pencher la balance dans la deuxième direction, non par le débat philosophique, mais par la pratique.

Signalons enfin deux traits marquants de cet ouvrage par rapport aux ouvrages classiques d'algèbre commutative.

Le premier est la mise au second plan de la noethérianité. L'expérience prouve en effet que la noethérianité est bien souvent une hypothèse trop forte, qui cache la vraie nature algorithmique des choses. Par exemple, tel théorème habituellement énoncé pour les anneaux noethériens et les modules de type fini, lorsque l'on met sa démonstration à plat pour en extraire

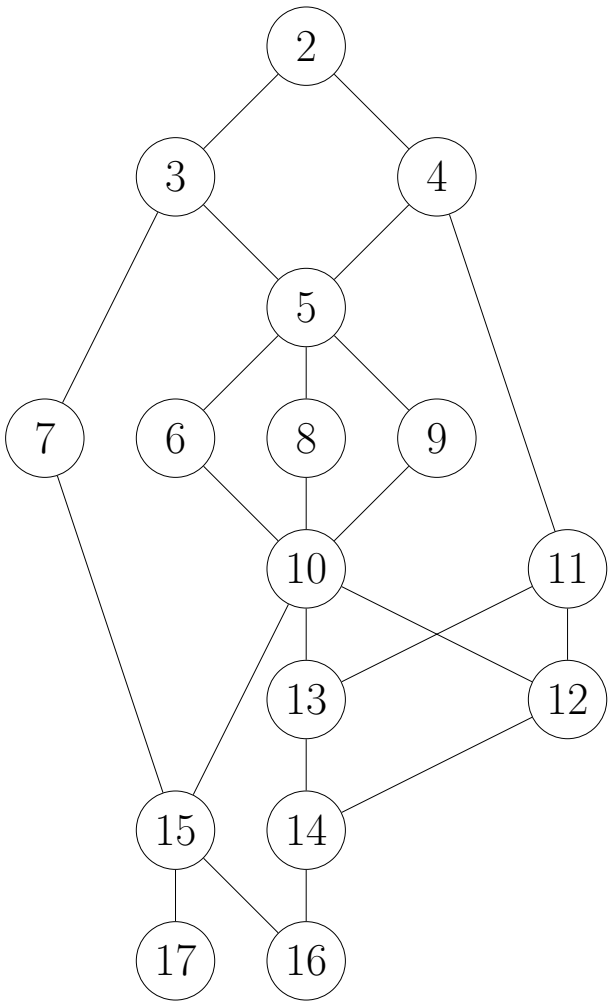
un algorithme, s'avère être un théorème sur les anneaux cohérents et les modules de présentation finie. Le théorème habituel n'est qu'un corollaire du bon théorème, mais avec deux arguments non constructifs qui permettent de déduire en mathématiques classiques la cohérence et la présentation finie de la noethérianité et du type fini. Une démonstration dans le cadre plus satisfaisant de la cohérence et des modules de présentation finie se trouve bien souvent déjà publiée dans des articles de recherche, quoique rarement sous forme entièrement constructive, mais « le bon énoncé » est en général absent dans les ouvrages de référence [5].

Le deuxième trait marquant de l'ouvrage est l'absence presque totale de la négation dans les énoncés constructifs. Par exemple, au lieu d'énoncer que pour un anneau $\mathbf{A}$ non trivial, deux modules libres de rang m et n avec $m > n$ ne peuvent pas être isomorphes, nous préférons dire, sans aucune hypothèse sur l'anneau, que si ces modules sont isomorphes, alors l'anneau est trivial (proposition II-5.2). Cette nuance peut sembler bien mince au premier abord, mais elle a une importance algorithmique. Elle va permettre de remplacer une démonstration en mathématiques classiques utilisant un anneau $\mathbf{A} = \mathbf{B}/\mathfrak{a}$, qui conclurait que $1 \in \mathfrak{a}$ au moyen d'un raisonnement par l'absurde, par une démonstration pleinement algorithmique qui construit 1 en tant qu'élément de l'idéal $\mathfrak{a}$ à partir d'un isomorphisme entre $\mathbf{A}^m$ et $\mathbf{A}^n$.

Pour une présentation générale des idées qui ont conduit aux nouvelles méthodes utilisées en algèbre constructive dans cet ouvrage, on pourra lire l'article de synthèse [45, Coquand & Lombardi, 2006].

Henri Lombardi, Claude Quitté
mai 2021

5. Cette déformation professionnelle noethérienne a produit un travers linguistique dans de nombreux ouvrages et articles de la littérature anglaise qui consiste à prendre « local ring » dans le sens de « Noetherian local ring ».


2
3
4
5
7
6
8
9
10
11
13
12
15
14
17
16

L'organigramme de la page ci-contre donne les liens de dépendance entre les différents chapitres

2. Principe local-global de base et systèmes linéaires
   Anneaux et modules cohérents. Un peu d'algèbre extérieure.
3. La méthode des coefficients indéterminés
   Lemme de Dedekind-Mertens et théorème de Kronecker. Théorie de Galois de base. Nullstellensatz classique.
4. Modules de présentation finie
   Catégorie des modules de présentation finie. Anneaux zéro-dimensionnels. Machineries locales-globales élémentaires. Idéaux de Fitting.
5. Modules projectifs de type fini (1)
   Théorème de structure locale. Déterminant. Rang.
6. Algèbres de type fini
7. La méthode dynamique
   Nullstellensatz général (sans clôture algébrique). Théorie de Galois générale (sans algorithme de factorisation).
8. Modules plats
   Algèbres plates et fidèlement plates.
9. Anneaux locaux, ou presque
   Anneau décomposable. Anneau local-global.
10. Modules projectifs de type fini (2)
11. Treillis distributifs, groupes réticulés
    Anneaux à pgcd. Treillis de Zariski d'un anneau commutatif. Relations implicatives.
12. Anneaux de Prüfer et de Dedekind
    Extensions entières. Dimension $\leqslant 1$. Factorisation d'idéaux de type fini.
13. Dimension de Krull
    Dimension de Krull. Dimension des morphismes. Dimension valuative. Dimension des extensions entières et polynomiales.
14. Nombre de générateurs d'un module
    Théorèmes de Kronecker, Bass et Forster-Swan. Splitting Off de Serre. Dimension de Heitmann.
15. Le principe local-global
16. Modules projectifs étendus
    Théorèmes de Traverso-Swan-Coquand, Quillen-Suslin, Bass-Lequain-Simis.
17. Théorème de stabilité de Suslin

II. Principe local-global de base et systèmes linéaires

Sommaire

Dans ce chapitre, comme dans tout l'ouvrage sauf mention expresse du contraire, les anneaux sont commutatifs et unitaires, et les homomorphismes entre anneaux respectent les 1. En particulier, un sous-anneau a le même 1 que l'anneau.

Introduction

La théorie de la résolution des systèmes linéaires est un thème omniprésent en algèbre commutative (sa forme la plus évoluée est l'algèbre homologique). Nous donnons dans ce chapitre un rappel de quelques résultats classiques sur ce sujet. Nous y reviendrons souvent.

Nous n'utilisons presqu'aucun appareillage théorique, mis à part la question de la localisation en un monoïde, dont nous donnons un rappel dans la section 1. Nous mettons en place le principe local-global concret pour la résolution des systèmes linéaires dans la section 2. Cet outil simple et efficace sera repris et diversifié sans cesse. D'un point de vue constructif, la résolution des systèmes linéaires fait immédiatement apparaître comme central le concept d'anneau cohérent que nous traitons dans la section 3. Les anneaux cohérents sont ceux pour lesquels on a une prise minimale sur la solution des systèmes linéaires homogènes.

Dans la section 4, nous développons la question des produits finis d'anneaux, avec la notion de système fondamental d'idempotents orthogonaux et le théorème des restes chinois.

La longue section 5 est consacrée à de nombreuses variations sur le thème des déterminants. On y traite notamment la question des matrices localement simples, dont le noyau et l'image sont des facteurs directs. Elles sont caractérisées par leurs idéaux déterminantiels (voir le théorème 5.26), des objets importants qui seront très présents dans toute la suite du livre.

Enfin, la section 6 revient sur le principe local-global de base, dans une version un peu plus générale consacrée aux suites exactes de modules.

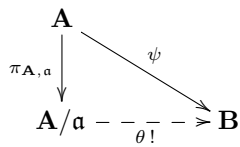
Les premiers pas en algèbre homologique sont traités dans les exercices 33 à 35.

1. Quelques faits concernant les quotients et les localisations

Commençons par un rappel sur les quotients. Soit $\mathfrak{a}$ un idéal de $\mathbf{A}$. En cas de besoin, on notera l'application canonique par $\pi_{\mathbf{A},\mathfrak{a}} : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$.

L'anneau quotient $(\mathbf{A}/\mathfrak{a}\,, \pi_{\mathbf{A},\mathfrak{a}})$ est caractérisé, *à isomorphisme unique près*, par la propriété universelle suivante.

1.1. Fait. (Propriété caractéristique du quotient par l'idéal $\mathfrak{a}$)
Un homomorphisme d'anneaux $\psi : \mathbf{A} \to \mathbf{B}$ se factorise par $\pi_{\mathbf{A},\mathfrak{a}}$ si, et seulement si, $\mathfrak{a} \subseteq \operatorname{Ker}\psi$, c'est-à-dire encore si $\psi(\mathfrak{a}) \subseteq \{0_{\mathbf{B}}\}$. Dans ce cas, la factorisation est unique.



homomorphismes nuls sur $\mathfrak{a}$.

Explication concernant la figure. *Dans une figure du type ci-dessus, tout est donné, sauf le morphisme θ correspondant à la flèche en traits tiretés. Le point d'exclamation signifie que θ fait commuter le diagramme et qu'il est* l'unique *morphisme possédant cette propriété.*

On note $M/\mathfrak{a}M$ le $\mathbf{A}/\mathfrak{a}$-module quotient du $\mathbf{A}$-module M par le sous-module engendré par les ax pour $a \in \mathfrak{a}$ et $x \in M$. Ce module peut aussi être défini par extension des scalaires à $\mathbf{A}/\mathfrak{a}$ du $\mathbf{A}$-module M (voir page 218, et l'exercice IV-5).

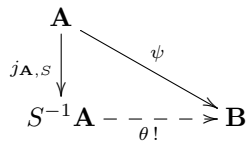
Passons aux localisations, qui sont très analogues aux quotients (nous reviendrons plus en détail sur cette analogie, en page 710). Dans cet ouvrage, lorsque l'on parle d'un *monoïde* contenu dans un anneau, on entend toujours une partie contenant 1 et stable pour la multiplication.

Pour un anneau $\mathbf{A}$, nous noterons $\mathbf{A}^\times$ le groupe multiplicatif des éléments inversibles, encore appelé *groupe des unités*.

Si S est un monoïde, on note $\mathbf{A}_S$ ou $S^{-1}\mathbf{A}$ le localisé de $\mathbf{A}$ en S. Tout élément de $\mathbf{A}_S$ s'écrit x/s avec $x \in \mathbf{A}$ et $s \in S$.
Par définition on a $x_1/s_1 = x_2/s_2$ s'il existe $s \in S$ tel que $ss_2x_1 = ss_1x_2$. En cas de besoin, on notera $j_{\mathbf{A},S} : \mathbf{A} \to \mathbf{A}_S$ l'application canonique $x \mapsto x/1$.

Le localisé $(\mathbf{A}_S, j_{\mathbf{A},S})$ est caractérisé, *à isomorphisme unique près*, par la propriété universelle suivante.

1.2. Fait. (Propriété caractéristique de la localisation en S)
Un homomorphisme d'anneaux $\psi : \mathbf{A} \to \mathbf{B}$ se factorise par $j_{\mathbf{A},S}$ si, et seulement si, $\psi(S) \subseteq \mathbf{B}^\times$, et dans ce cas la factorisation est unique.



homomorphismes qui envoient S dans $\mathbf{B}^\times$.

De même, on note $M_S = S^{-1}M$ le $\mathbf{A}_S$-module localisé du $\mathbf{A}$-module M en S. Tout élément de M_S s'écrit x/s avec $x \in M$ et $s \in S$. Par définition, on a $x_1/s_1 = x_2/s_2$ s'il existe $s \in S$ tel que $ss_2x_1 = ss_1x_2$. Ce module M_S peut aussi être défini par extension des scalaires à $\mathbf{A}_S$ du $\mathbf{A}$-module M (voir page 218, et l'exercice IV-5).

Un monoïde S dans un anneau $\mathbf{A}$ est dit *saturé* lorsque l'implication

$$\forall s, t \in \mathbf{A}, \qquad (st \in S \ \Rightarrow \ s \in S)$$

est satisfaite. Un monoïde saturé est également appelé un *filtre*. Nous appellerons *filtre principal* un filtre engendré par un élément : il est constitué de l'ensemble des diviseurs d'une puissance de cet élément.

On note S^{sat} le saturé du monoïde S ; il est obtenu en rajoutant tous les éléments qui divisent un élément de S. Si l'on sature un monoïde S, on ne change pas la localisation [1]. Deux monoïdes S_1 et S_2 sont dits *équivalents* s'ils ont le même saturé. Dans ce cas, on écrit $\mathbf{A}_{S_1} = \mathbf{A}_{S_2}$.

Nous gardons la possibilité de localiser en un monoïde qui contient 0. Le résultat est alors l'anneau *trivial* (rappelons qu'un anneau est trivial s'il est réduit à un seul élément, c'est-à-dire encore si $1 = 0$).

Dans un anneau le *transporteur* d'un idéal $\mathfrak{a}$ dans un idéal $\mathfrak{b}$ est l'idéal

$$(\mathfrak{b} : \mathfrak{a})_{\mathbf{A}} = \{\, a \in \mathbf{A} \mid a\mathfrak{a} \subseteq \mathfrak{b} \,\}.$$

Plus généralement, si N et P sont deux sous-modules d'un $\mathbf{A}$-module M, on définit le *transporteur* de N dans P comme l'idéal

$$(P : N)_{\mathbf{A}} = \{\, a \in \mathbf{A} \mid aN \subseteq P \,\}.$$

Rappelons aussi que *l'annulateur* d'un élément x d'un $\mathbf{A}$-module M est l'idéal $\mathrm{Ann}_{\mathbf{A}}(x) = (\langle 0_{\mathbf{A}} \rangle : \langle x \rangle) = \{\, a \in \mathbf{A} \mid ax = 0 \,\}$.

L'*annulateur du module* M est l'idéal $\mathrm{Ann}_{\mathbf{A}}(M) = (\langle 0_M \rangle : M)_{\mathbf{A}}$. Un module ou un idéal est *fidèle* si son annulateur est réduit à 0.

1. En fait, selon la construction précise que l'on choisit pour définir une localisation, on aura ou bien égalité, ou bien isomorphisme canonique, entre les deux localisés.

Si S est engendré par $s \in \mathbf{A}$, c'est-à-dire si $S = s^{\mathbb{N}} \stackrel{\text{déf}}{=} \{ s^k \mid k \in \mathbb{N} \}$, on note $\mathbf{A}_s$ ou $\mathbf{A}[1/s]$ le localisé $S^{-1}\mathbf{A}$, qui est isomorphe à $\mathbf{A}[T]/\langle sT-1\rangle$.
Les notations suivantes sont également utiles pour un sous-module N de M.

$$\begin{aligned}(N : \mathfrak{a})_M &= \{ x \in M \mid x\,\mathfrak{a} \subseteq N \}\\ (N : \mathfrak{a}^\infty)_M &= \{ x \in M \mid \exists n,\, x\,\mathfrak{a}^n \subseteq N \}\,.\end{aligned}$$

Ce dernier module s'appelle le *saturé de N par $\mathfrak{a}$*.

Nous disons qu'un élément x d'un $\mathbf{A}$-module M est *régulier* (si $M = \mathbf{A}$, on dit aussi que x est *non diviseur de zéro*, en un seul mot) si la suite

$$0 \longrightarrow \mathbf{A} \xrightarrow{.x} M$$

est exacte, autrement dit si $\mathrm{Ann}(x) = 0$. Si $0_{\mathbf{A}}$ est non diviseur de zéro dans $\mathbf{A}$, l'anneau est trivial.

En général, pour alléger les notations précédentes concernant les transporteurs, on omet l'indice $\mathbf{A}$ ou M lorsqu'il est clair d'après le contexte.

L'*anneau total de fractions* de $\mathbf{A}$, que nous notons $\mathrm{Frac}\,\mathbf{A}$, est l'anneau localisé $\mathbf{A}_S$, où S est le monoïde des éléments réguliers de $\mathbf{A}$, que nous notons $\mathrm{Reg}\,\mathbf{A}$.

1.3. Fait

1. *Le noyau de l'homomorphisme naturel $j_{\mathbf{A},s} : \mathbf{A} \to \mathbf{A}_s = \mathbf{A}[1/s]$ est l'idéal $(0 : s^\infty)_{\mathbf{A}}$. Il est réduit à 0 si, et seulement si, s est régulier.*
2. *Le noyau de l'homomorphisme naturel de M dans $M_s = M[1/s]$ est le sous-$\mathbf{A}$-module $(0 : s^\infty)_M$.*
3. *L'homomorphisme naturel $\mathbf{A} \to \mathrm{Frac}\,\mathbf{A}$ est injectif.*

1.4. Fait. *Si $S \subseteq S'$ sont deux monoïdes de $\mathbf{A}$ et M un $\mathbf{A}$-module, on a des identifications naturelles $(\mathbf{A}_S)_{S'} \simeq \mathbf{A}_{S'}$ et $(M_S)_{S'} \simeq M_{S'}$.*

2. Principe local-global de base

Nous étudierons le fonctionnement général du principe local-global en algèbre commutative dans le chapitre XV. Nous le rencontrerons cependant à tous les détours de notre chemin sous des formes particulières, adaptées à chaque situation. Une instance essentielle de ce principe est donnée dans cette section parce qu'elle est tellement simple qu'il serait bête de se priver plus longtemps de ce petit plaisir et de cette machinerie si efficace.

Le principe local-global affirme que certaines propriétés sont vraies si, et seulement si, elles sont vraies après des localisations «en quantité suffisante». En mathématiques classiques, on invoque souvent la localisation en tous les idéaux maximaux. C'est beaucoup, et un peu mystérieux, surtout d'un

point de vue algorithmique. Nous utiliserons des versions plus simples, et moins effrayantes, dans lesquelles seulement un nombre fini de localisations sont mises en œuvre.

Localisations comaximales et principe local-global

La définition qui suit correspond à l'idée intuitive que certains systèmes de localisés d'un anneau $\mathbf{A}$ sont «en quantité suffisante» pour récupérer à travers eux toute l'information contenue dans $\mathbf{A}$.

2.1. Définition

1. Des éléments $s_1, \ldots, s_n$ sont dits *comaximaux* si $\langle 1\rangle = \langle s_1, \ldots, s_n\rangle$. Deux éléments comaximaux sont aussi appelés *étrangers*.
2. Des monoïdes $S_1, \ldots, S_n$ sont dits *comaximaux* si chaque fois que l'on a des éléments $s_1 \in S_1$, …, $s_n \in S_n$, ces s_i sont comaximaux.

Deux exemples fondamentaux

1) Si $s_1, \ldots, s_n$ sont comaximaux, les monoïdes qu'ils engendrent sont comaximaux. En effet, considérons des $s_i^{m_i}$ $(m_i \geqslant 1)$ dans les monoïdes $s_i^{\mathbb{N}}$, en élevant l'égalité $\sum_{i=1}^n a_i s_i = 1$ à la puissance $1 - n + \sum_{i=1}^n m_i$, on obtient, en regroupant convenablement les termes de la somme obtenue, l'égalité souhaitée $\sum_{i=1}^n b_i s_i^{m_i} = 1$.

2) Si $a = a_1 \cdots a_n \in \mathbf{A}$, alors les monoïdes $a^{\mathbb{N}}$, $1 + a_1\mathbf{A}$, …, $1 + a_n\mathbf{A}$ sont comaximaux. Prenons en effet un élément $b_i = 1 - a_i x_i$ dans chaque monoïde $1 + a_i\mathbf{A}$ et un élément a^m dans le monoïde $a^{\mathbb{N}}$. On doit montrer que l'idéal $\mathfrak{m} = \langle a^m, b_1, \ldots, b_n\rangle$ contient 1. Or, modulo $\mathfrak{m}$ on a $1 = a_i x_i$, donc $1 = a\prod_i x_i = ax$, et enfin $1 = 1^m = a^m x^m = 0$. ∎

Voici une caractérisation en mathématiques classiques.

2.2. Fait*. Soient des monoïdes $S_1, \ldots, S_n$ dans un anneau non trivial $\mathbf{A}$ (i.e., $1 \neq_{\mathbf{A}} 0$). Les monoïdes S_i sont comaximaux si, et seulement si, pour tout idéal premier (resp. pour tout idéal maximal) $\mathfrak{p}$ l'un des S_i est contenu dans $\mathbf{A} \setminus \mathfrak{p}$.

◗ Soit $\mathfrak{p}$ un idéal premier. Si aucun des S_i n'est contenu dans $\mathbf{A} \setminus \mathfrak{p}$, il existe, pour chaque i, un $s_i \in S_i \cap \mathfrak{p}$; alors, $s_1, \ldots, s_n$ ne sont pas comaximaux.
Inversement, supposons que pour tout idéal maximal $\mathfrak{m}$ l'un des S_i est contenu dans $\mathbf{A} \setminus \mathfrak{m}$ et soient $s_1 \in S_1$, …, $s_n \in S_n$, l'idéal $\langle s_1, \ldots, s_n\rangle$ n'est alors contenu dans aucun idéal maximal, et il contient donc 1. □

Nous notons $\mathbf{A}^{m\times p}$ ou $\mathbb{M}_{m,p}(\mathbf{A})$ le $\mathbf{A}$-module des matrices à m lignes et p colonnes à coefficients dans $\mathbf{A}$, et $\mathbb{M}_n(\mathbf{A})$ désigne $\mathbb{M}_{n,n}(\mathbf{A})$. Le groupe formé par les matrices inversibles est noté $\mathbb{GL}_n(\mathbf{A})$, le sous-groupe des matrices de déterminant 1 est noté $\mathbb{SL}_n(\mathbf{A})$. Le sous-ensemble de $\mathbb{M}_n(\mathbf{A})$ formé par

les matrices de projection (c'est-à-dire les matrices F telles que $F^2 = F$) est noté $\mathbb{GA}_n(\mathbf{A})$. L'explication des acronymes est la suivante : $\mathbb{GL}$ pour groupe linéaire, $\mathbb{SL}$ pour groupe linéaire spécial et $\mathbb{GA}$ pour grassmannienne affine.

2.3. Principe local-global concret. (Principe local-global de base, recollement concret de solutions d'un système linéaire)
Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$, B une matrice de $\mathbf{A}^{m\times p}$ et C un vecteur colonne de $\mathbf{A}^m$. Alors, les propriétés suivantes sont équivalentes.

1. *Le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^p$.*
2. *Pour $i \in [\![1..n]\!]$, le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^p_{S_i}$.*

Ce principe vaut également pour les systèmes linéaires à coefficients dans un $\mathbf{A}$-module M.

D *1 $\Rightarrow$ 2.* Clair.
2 $\Rightarrow$ 1. Pour chaque i, on a $Y_i \in \mathbf{A}^p$ et $s_i \in S_i$ tels que $B(Y_i/s_i) = C$ dans $\mathbf{A}^m_{S_i}$. Cela signifie que l'on a un $t_i \in S_i$ tel que $t_i\, BY_i = s_i t_i\, C$ dans $\mathbf{A}^m$. En utilisant $\sum_i a_i s_i t_i = 1$, on a une solution dans $\mathbf{A}$: $X = \sum_i a_i t_i Y_i$. □

Remarque. Quant au fond, ce principe local-global concret se ramène à la remarque suivante dans le cas d'un anneau intègre (un anneau est dit *intègre* si tout élément est nul ou régulier [2]). Si les s_i sont réguliers et si

$$\frac{x_1}{s_1} = \frac{x_2}{s_2} = \cdots = \frac{x_n}{s_n},$$

la valeur commune de cette fraction, lorsque $\sum_i s_i u_i = 1$, est aussi égale à

$$\frac{x_1u_1 + \cdots + x_nu_n}{s_1u_1 + \cdots + s_nu_n} = x_1u_1 + \cdots + x_nu_n.$$

Ce principe pourrait donc s'appeler aussi «l'art de chasser astucieusement les dénominateurs». La chose la plus remarquable est sans doute que cela fonctionne en toute généralité, même si l'anneau n'est pas intègre. Merci donc à Claude Chevalley d'avoir introduit les localisations arbitraires. Dans certains ouvrages savants, on trouve la même chose formulée ainsi (au prix d'une perte d'information sur le caractère très concret du résultat) : le $\mathbf{A}$-module $\bigoplus_{\mathfrak{m}} \mathbf{A}_{1+\mathfrak{m}}$ (où $\mathfrak{m}$ parcourt tous les idéaux maximaux de $\mathbf{A}$) est fidèlement plat. ■

2. La notion est discutée plus en détail page 224.

2.4. Corollaire. *Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$, $x \in \mathbf{A}$ et $\mathfrak{a}, \mathfrak{b}$ deux idéaux de type fini de $\mathbf{A}$. Alors, on a les équivalences suivantes.*

1. *$x = 0$ dans $\mathbf{A}$ si, et seulement si, pour $i \in [\![1..n]\!]$, $x = 0$ dans $\mathbf{A}_{S_i}$.*
2. *x est régulier dans $\mathbf{A}$ si, et seulement si, pour $i \in [\![1..n]\!]$, x est régulier dans $\mathbf{A}_{S_i}$.*
3. *$\mathfrak{a} = \langle 1 \rangle$ dans $\mathbf{A}$ si, et seulement si, pour $i \in [\![1..n]\!]$, $\mathfrak{a} = \langle 1 \rangle$ dans $\mathbf{A}_{S_i}$.*
4. *$\mathfrak{a} \subseteq \mathfrak{b}$ dans $\mathbf{A}$ si, et seulement si, pour $i \in [\![1..n]\!]$, $\mathfrak{a} \subseteq \mathfrak{b}$ dans $\mathbf{A}_{S_i}$.*

▷ La démonstration est laissée au lecteur. □

Remarque. En fait, comme nous le verrons dans le principe local-global 6.7, les idéaux n'ont pas besoin d'être de type fini. ■

Exemples

Donnons des exemples simples d'application du principe local-global concret de base. Un cas d'application typique du premier exemple (fait 2.5) est celui où le module M dans l'énoncé est un idéal non nul d'un anneau de Dedekind. Un module M est dit *localement monogène* si, après chaque localisation en des monoïdes comaximaux $S_1, \ldots, S_n$, il est engendré par un seul élément.

2.5. Fait. *Soit $M = \langle a, b \rangle = \langle c, d \rangle$ un module avec deux systèmes générateurs. On suppose que ce module est fidèle et localement monogène. Alors, il existe une matrice $A \in \mathbb{SL}_2(\mathbf{A})$ telle que $[\,a\ b\,]\,A = [\,c\ d\,]$.*

▷ Si $A = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$, la matrice cotransposée doit être égale à

$$B = \operatorname{Adj} A = \begin{bmatrix} t & -y \\ -z & x \end{bmatrix}.$$

En particulier, on cherche à résoudre le système linéaire suivant :

$$[\,a\ b\,]\,A = [\,c\ d\,], \qquad [\,c\ d\,]\,B = [\,a\ b\,] \tag{$*$}$$

dont les inconnues sont x, y, z, t. Notons que $A\,B = \det(A)\,\mathrm{I}_2$.
Inversement, si ce système linéaire est résolu, on aura $[\,a\ b\,] = [\,a\ b\,]\,A\,B$, donc $\big(1 - \det(A)\big)[\,a\ b\,] = [\,0\ 0\,]$, et puisque le module est fidèle, $\det(A) = 1$.
On a des monoïdes comaximaux S_i tels que M_{S_i} est engendré par $g_i/1$ pour un $g_i \in M$. Pour résoudre le système linéaire, il suffit de le résoudre après localisation en chacun des S_i.
Dans l'anneau $\mathbf{A}_{S_i}$, on a les égalités $a = \alpha_i g_i$, $b = \beta_i g_i$, $g_i = \mu_i a + \nu_i b$, et donc $\big(1 - (\alpha_i\mu_i + \beta_i\nu_i)\big)\, g_i = 0$.

Le module $M_{S_i} = \langle g_i \rangle$ reste fidèle, donc $1 = \alpha_i\mu_i + \beta_i\nu_i$ dans $\mathbf{A}_{S_i}$. Ainsi :

$$[\,a\ b\,]\,E_i = [\,g_i\ 0\,], \quad \text{avec } E_i = \begin{bmatrix} \mu_i & -\beta_i \\ \nu_i & \alpha_i \end{bmatrix} \text{ et } \det(E_i) = 1.$$

De même, on obtiendra $[\,c\ d\,]\,C_i = [\,g_i\ 0\,]$ avec une matrice C_i de déterminant 1 dans $\mathbf{A}_{S_i}$. En prenant $A_i = E_i\ \mathrm{Adj}(C_i)$, on obtient $[\,a\ b\,]\,A_i = [\,c\ d\,]$ et $\det(A_i) = 1$ dans $\mathbf{A}_{S_i}$. Le système linéaire $(*)$ admet dès lors une solution dans $\mathbf{A}_{S_i}$. □

Notre deuxième exemple est donné par le lemme de Gauss-Joyal : le point *1* dans le lemme suivant est prouvé en application du principe local-global de base. Nous devons d'abord rappeler quelques définitions.

Un élément a d'un anneau est dit *nilpotent* si $a^n = 0$ pour un entier $n \in \mathbb{N}$. Les éléments nilpotents dans un anneau $\mathbf{A}$ forment un idéal appelé *nilradical*, ou encore *radical nilpotent* de l'anneau. Un anneau est *réduit* si son nilradical est égal à 0. Plus généralement, le nilradical d'un idéal $\mathfrak{a}$ de $\mathbf{A}$ est l'idéal formé par les $x \in \mathbf{A}$ dont une puissance est dans $\mathfrak{a}$. Nous le noterons $\sqrt{\mathfrak{a}}$ ou $\sqrt[\mathbf{A}]{\mathfrak{a}}$ ou $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$. Nous notons aussi $\mathrm{D}_{\mathbf{A}}(x)$ pour $\mathrm{D}_{\mathbf{A}}(\langle x \rangle)$. Un idéal $\mathfrak{a}$ est appelé *un idéal radical* lorsqu'il est égal à son nilradical. L'anneau $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0) = \mathbf{A}_{\mathrm{red}}$ est *l'anneau réduit associé* à $\mathbf{A}$.

Pour un polynôme f de $\mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, on appelle *contenu* de f et l'on note $\mathrm{c}_{\mathbf{A},\underline{X}}(f)$ ou $\mathrm{c}(f)$ l'idéal engendré par les coefficients de f. Le polynôme f est dit *primitif* (en $\underline{X}$) lorsque $\mathrm{c}_{\mathbf{A},\underline{X}}(f) = \langle 1 \rangle$.

Lorsqu'un polynôme f de $\mathbf{A}[X]$ est donné sous la forme $f(X) = \sum_{k=0}^{n} a_k X^k$, on dit que n est le *degré formel* de f, et a_n est son *coefficient formellement dominant*. Enfin, si f est donné comme nul, son degré formel est -1.

2.6. Lemme

1. (Gauss-Joyal du pauvre) *Le produit de deux polynômes primitifs est un polynôme primitif.*
2. (Gauss-Joyal) *Pour f, $g \in \mathbf{A}[\underline{X}]$, il existe un entier $p \in \mathbb{N}$ tel que $\big(\mathrm{c}(f)\mathrm{c}(g)\big)^p \subseteq \mathrm{c}(fg)$.*
3. (Éléments nilpotents dans $\mathbf{A}[\underline{X}]$) *Un élément f de $\mathbf{A}[\underline{X}]$ est nilpotent si, et seulement si, tous ses coefficients sont nilpotents. Autrement dit, on a l'égalité $(\mathbf{A}[\underline{X}])_{\mathrm{red}} = \mathbf{A}_{\mathrm{red}}[\underline{X}]$.*
4. (Éléments inversibles dans $\mathbf{A}[\underline{X}]$) *Un élément f de $\mathbf{A}[\underline{X}]$ est inversible si, et seulement si, $f(\underline{0})$ est inversible et $f - f(\underline{0})$ est nilpotent. Autrement dit, $\mathbf{A}[\underline{X}]^\times = \mathbf{A}^\times + \mathrm{D}_{\mathbf{A}}(0)[\underline{X}]$ et en particulier pour les inversibles $(\mathbf{A}_{\mathrm{red}}[\underline{X}])^\times = (\mathbf{A}_{\mathrm{red}})^\times$.*

▷ Notez que l'on a a priori l'inclusion $\mathrm{c}(fg) \subseteq \mathrm{c}(f)\mathrm{c}(g)$.

1. Pour des polynômes f, $g \in \mathbf{A}[X]$ en une variable. On a $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1\rangle$. On considère l'anneau quotient $\mathbf{B} = \mathbf{A}/\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big)$. On doit démontrer que cet anneau est trivial. Il suffit de le faire après localisation en des éléments comaximaux, par exemple les coefficients de f. Autrement dit, on peut supposer qu'un coefficient de f est inversible. Faisons la preuve sur un exemple suffisamment général, en supposant que

$$f(X) = a + bX + X^2 + cX^3 + \dots \quad \text{et} \quad g(X) = g_0 + g_1X + g_2X^2 + \dots$$

Dans l'anneau $\mathbf{B}$ on a $ag_0 = 0$, $ag_1 + bg_0 = 0$, $ag_2 + bg_1 + g_0 = 0$, donc $bg_0^2 = 0$, puis $g_0^3 = 0$, donc $g_0 = 0$. On a alors $g = Xh$ et $c(fg) = c(fh)$, et puisque le degré formel de h est plus petit que celui de g, on peut conclure par récurrence sur le degré formel que $g = 0$. Comme $\mathrm{c}(g) = \langle 1\rangle$, l'anneau est trivial.

2. Pour des polynômes en une variable. On considère un coefficient a de f et un coefficient b de g. Montrons que ab est nilpotent dans $\mathbf{B} = \mathbf{A}/\mathrm{c}(fg)$. Cela revient à démontrer que $\mathbf{C} = \mathbf{B}[1/(ab)]$ est trivial. Or, dans $\mathbf{C}$, f et g sont primitifs, donc le point *1* implique que $\mathbf{C}$ est trivial.

2 et *1. Cas général.* Le point *2* se démontre par récurrence sur le nombre de variables à partir du cas univarié. En effet, pour $f \in \mathbf{A}[X][Y]$, on a l'égalité

$$\mathrm{c}_{\mathbf{A},X,Y}(f) = \big\langle \mathrm{c}_{\mathbf{A},X}(h) \mid h \in \mathrm{c}_{\mathbf{A}[X],Y}(f)\big\rangle\,.$$

Ensuite, on en déduit le point *1.*

3. On note que $f^2 = 0$ implique $\mathrm{c}(f)^p = 0$ pour un certain p d'après le point *2.*

4. La condition est suffisante : dans un anneau si x est nilpotent, $1 - x$ est inversible parce que $(1 - x)(1 + x + \cdots + x^n) = 1 - x^{n+1}$, donc si u est inversible et x nilpotent, $u + x$ est inversible. Pour voir que la condition est nécessaire, il suffit de traiter le cas en une variable (on conclut par récurrence sur le nombre de variables). Écrivons $fg = 1$ avec $f = f(0) + XF(X)$ et $g = g(0) + XG(X)$. On a $f(0)g(0) = 1$. Soit n le degré formel de F et m celui de G. On doit montrer que F et G sont nilpotents.
Si $n = -1$ ou $m = -1$, le résultat est clair. On raisonne par récurrence sur $n + m$ en supposant n, $m \geqslant 0$, F_n et G_m étant les coefficients formellement dominants. Par hypothèse de récurrence, le résultat est obtenu pour les anneaux $(\mathbf{A}/\langle F_n\rangle)[X]$ et $(\mathbf{A}/\langle G_m\rangle)[X]$. Puisque $F_nG_m = 0$, on peut conclure par le lemme qui suit.

NB : on donne des précisions dans l'exercice VII-8. □

2.7. Lemme. *Soient a, b, $c \in \mathbf{A}$. Si c est nilpotent modulo a et modulo b, et si $ab = 0$, alors c est nilpotent.*

▷ On a $c^n = xa$ et $c^m = yb$, donc $c^{n+m} = xyab = 0$. □

Remarque. On peut formuler ce lemme de manière plus structurelle en considérant pour deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ le morphisme canonique $\mathbf{A} \to \mathbf{A}/\mathfrak{a} \times \mathbf{A}/\mathfrak{b}$ de noyau $\mathfrak{a} \cap \mathfrak{b}$. Si un élément de $\mathbf{A}$ est nilpotent modulo $\mathfrak{a}$ et modulo $\mathfrak{b}$, il l'est modulo $\mathfrak{a} \cap \mathfrak{b}$, donc aussi modulo $\mathfrak{ab}$, car $(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{ab}$. On touche ici au «principe de recouvrement fermé», voir page 715. ∎

Propriétés de caractère fini

Le principe local-global concret de base peut être reformulé comme un «principe de transfert».

2.8. Principe de transfert de base
Pour un système linéaire dans un anneau $\mathbf{A}$*, les éléments* s *tels que le système linéaire ait une solution dans* $\mathbf{A}[1/s]$ *forment un idéal de* $\mathbf{A}$*.*

Nous proposons tout d'abord à la lectrice de démontrer que ce principe de transfert est équivalent au principe local-global concret de base.

Nous faisons maintenant une analyse détaillée de ce qui se passe. L'équivalence repose en fait sur la notion suivante.

2.9. Définition. Une propriété P concernant les anneaux commutatifs et les modules est dite *de caractère fini* si elle est conservée par localisation (par passage de $\mathbf{A}$ à $S^{-1}\mathbf{A}$) et si, lorsqu'elle est vérifiée avec $S^{-1}\mathbf{A}$, alors elle est vérifiée avec $\mathbf{A}[1/s]$ pour un certain $s \in S$.

2.10. Fait. *Soit* P *une propriété de caractère fini. Alors, le principe local-global concret pour* P *est équivalent au principe de transfert pour* P*. Autrement dit, les principes suivants sont équivalents.*

1. *Si la propriété* P *est vraie après localisation en une famille de monoïdes comaximaux, alors elle est vraie.*
2. *L'ensemble des éléments* s *de l'anneau pour lesquels la propriété* P *est vraie après localisation en* s *forme un idéal.*

▷ Soit $\mathbf{A}$ un anneau qui fournit le contexte pour la propriété P. Considérons alors l'ensemble $I = \{\, s \in \mathbf{A} \mid \mathsf{P} \text{ est vraie pour } \mathbf{A}_s \,\}$.

1 ⇒ *2.* Supposons *1.* Soient $s, t \in I$, $a, b \in \mathbf{A}$ et $u = as + bt$. Les éléments s et t sont comaximaux dans $\mathbf{A}_u$. Puisque P est stable par localisation, P est vraie pour $(\mathbf{A}_u)_s = (\mathbf{A}_s)_u$ et $(\mathbf{A}_u)_t = (\mathbf{A}_t)_u$. En appliquant *1*, P est vraie pour $\mathbf{A}_u$, i.e., $u = as + bt \in I$.

2 ⇒ *1.* Supposons *2* et soit (S_i) la famille de monoïdes comaximaux considérée. Puisque la propriété est de caractère fini, on trouve dans chaque S_i un élément s_i tel que P soit vraie après localisation en s_i. Puisque les S_i sont comaximaux, les s_i sont des éléments comaximaux. En appliquant *2*, on obtient $I = \langle 1 \rangle$. Ainsi, la localisation en 1 donne la réponse. □

La plupart des principes local-globals concrets que nous considérerons dans cet ouvrage s'appliquent pour des propriétés de caractère fini. Si le lecteur le préfère, il a tout le loisir de remplacer alors le principe local-global concret par le principe de transfert correspondant.

En mathématiques classiques, on a pour les propriétés de caractère fini l'équivalence de deux notions, l'une concrète et l'autre abstraite, comme expliqué dans le fait suivant.

2.11. Fait***.** *Soit* P *une propriété de caractère fini. Alors, en mathématiques classiques, les propriétés suivantes sont équivalentes.*

1. *Il existe des monoïdes comaximaux tels que la propriété* P *soit vraie après localisation en chacun des monoïdes.*
2. *La propriété* P *est vraie après localisation en tout idéal maximal.*

D *1* $\Rightarrow$ *2.* Soit (S_i) la famille de monoïdes comaximaux considérée. Puisque la propriété est de caractère fini, on trouve dans chaque S_i un élément s_i tel que P soit vraie après localisation en s_i. Puisque les S_i sont comaximaux, les s_i sont des éléments comaximaux. Soit $\mathfrak{m}$ un idéal maximal. L'un des s_i n'est pas dans $\mathfrak{m}$. La localisation en $1+\mathfrak{m}$ est une localisation de la localisation en s_i. Donc, P est vraie après localisation en $1+\mathfrak{m}$.
2 $\Rightarrow$ *1.* Pour chaque idéal maximal $\mathfrak{m}$ sélectionnons un $s_{\mathfrak{m}} \notin \mathfrak{m}$ tel que la propriété P soit vraie après localisation en $s_{\mathfrak{m}}$. L'ensemble des $s_{\mathfrak{m}}$ engendre un idéal qui n'est contenu dans aucun idéal maximal, donc c'est l'idéal $\langle 1\rangle$. Une famille finie de certains de ces $s_{\mathfrak{m}}$ est donc un système d'éléments comaximaux. La famille des monoïdes engendrés par ces éléments convient.□

On a le corollaire immédiat suivant.

2.12. Fait***.** *Soit* P *une propriété de caractère fini. Alors, le principe local-global concret pour* P *est équivalent (en mathématiques classiques) au principe local-global abstrait pour* P*. Autrement dit, les principes suivants sont équivalents.*

1. *Si la propriété* P *est vraie après localisation en une famille de monoïdes comaximaux, alors elle est vraie.*
2. *Si la propriété* P *est vraie après localisation en tout idéal maximal, alors elle est vraie.*

Remarque. Donnons une démonstration directe de l'équivalence en mathématiques classiques du principe de transfert et du principe local-global abstrait pour la propriété P (supposée de caractère fini).
Transfert $\Rightarrow$ *Abstrait.* Supposons la propriété vraie après localisation en tout idéal maximal. L'idéal donné par le principe de transfert ne peut pas

être strict [3] car sinon il serait contenu dans un idéal maximal $\mathfrak{m}$, ce qui est en contradiction avec le fait que la propriété est vraie après localisation en un $s \notin \mathfrak{m}$.

Abstrait $\Rightarrow$ *Transfert.* Pour tout idéal maximal $\mathfrak{m}$, sélectionnons un $s_{\mathfrak{m}} \notin \mathfrak{m}$ tel que la propriété P soit vraie après localisation en $s_{\mathfrak{m}}$. L'ensemble des $s_{\mathfrak{m}}$ engendre un idéal qui n'est contenu dans aucun idéal maximal, donc c'est l'idéal $\langle 1 \rangle$. On peut conclure par le principe de transfert : la propriété est vraie après localisation en 1 ! ∎

Commentaire. L'avantage de la localisation en un idéal premier est que le localisé est un anneau local, lequel a de très bonnes propriétés (voir le chapitre IX). Le désavantage est que les preuves qui utilisent un principe local-global abstrait en lieu et place du principe local-global concret correspondant sont non constructives dans la mesure où le seul accès que l'on a (dans une situation générale) aux idéaux premiers est donné par le lemme de Zorn. En outre, même le fait 2.2 est obtenu au moyen d'un raisonnement par l'absurde, qui enlève tout caractère algorithmique à la « construction » correspondante.

Certains principes local-globals concrets n'ont pas de correspondant abstrait, parce que la propriété concernée n'est pas de caractère fini. Ce sera le cas des principes local-globals concrets 3.6 pour les modules de type fini et 3.5 pour les anneaux cohérents.

Nous ferons un usage systématique efficace et constructif du principe local-global concret de base et de ses conséquences. Souvent, nous nous inspirerons d'une démonstration d'un principe local-global abstrait en mathématiques classiques.

Dans la section XV-5, nous mettrons au point une machinerie locale-globale générale pour exploiter à fond de manière constructive les preuves classiques de type local-global. Nous généraliserons cette technique à d'autres situations semblables dans les sections suivantes du chapitre XV.

Nous reviendrons sur les propriétés de caractère fini dans la section V-9. Une discussion du cas où le principe local-global concret « après localisation en des éléments comaximaux » fonctionne pour une propriété qui n'est pas de caractère fini, comme la propriété pour un module d'être de type fini, est faite dans le paragraphe « Localisation au voisinage de tout idéal premier » page 949 de la section XV-3. ∎

3. Rappelons qu'un idéal est dit *strict* lorsqu'il ne contient pas 1. Nous ferons usage de cette notion essentiellement dans nos commentaires au sujet des mathématiques classiques.

Version abstraite du principe local-global de base

Vu que la propriété considérée est de caractère fini, on obtient en mathématiques classiques la version abstraite suivante pour le principe local-global de base.

2.13. Principe local-global abstrait*. (Principe local-global abstrait de base : recollement abstrait de solutions d'un système linéaire)
Soient B une matrice $\in \mathbf{A}^{m\times p}$ et C un vecteur colonne de $\mathbf{A}^m$. Alors, les propriétés suivantes sont équivalentes.

1. *Le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^p$.*
2. *Pour tout idéal maximal $\mathfrak{m}$, le système linéaire $BX = C$ admet une solution dans $(\mathbf{A}_{1+\mathfrak{m}})^p$.*

Rendre des éléments comaximaux par force

La localisation en un élément $s \in \mathbf{A}$ est une opération fondamentale en algèbre commutative pour rendre s inversible par force.

Il arrive que l'on ait besoin de rendre comaximaux des éléments $a_1, \ldots, a_n$ d'un anneau $\mathbf{A}$. On introduit à cet effet l'anneau

$$\mathbf{B} = \mathbf{A}[X_1, \ldots, X_n]\big/\big\langle 1 - \textstyle\sum_i a_i X_i\big\rangle = \mathbf{A}[x_1, \ldots, x_n].$$

2.14. Lemme. *Le noyau de l'homomorphisme naturel $\psi : \mathbf{A} \to \mathbf{B}$ est l'idéal $(0 : \mathfrak{a}^\infty)$, où $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$. En particulier, l'homomorphisme est injectif si, et seulement si,* $\operatorname{Ann}\mathfrak{a} = 0$.

◗ Soit c un élément du noyau, vu l'isomorphisme $\mathbf{B}/\langle (x_j)_{j\neq i}\rangle \simeq \mathbf{A}[1/a_i]$, on a $c =_{\mathbf{A}[1/a_i]} 0$, donc $c \in (0 : a_i^\infty)$. On en déduit $c \in (0 : \mathfrak{a}^\infty)$. Inversement, si $c \in (0 : \mathfrak{a}^\infty)$, il existe un r tel que $ca_i^r = 0$ pour chaque i, et donc $\psi(c) = \psi(c)(\sum a_i x_i)^{nr} = 0$. □

3. Anneaux et modules cohérents

Une notion fondamentale

Un $\mathbf{A}$-module M est dit *de type fini* si l'on a $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in M$ tels que $M = x_1\mathbf{A} + \cdots + x_n\mathbf{A}$ (noté $\langle x_1, \ldots, x_n\rangle$ ou $\langle x_1, \ldots, x_n\rangle_{\mathbf{A}}$). On dit aussi que M est *un $\mathbf{A}$-module fini*.

Un anneau $\mathbf{A}$ est dit *cohérent* si toute équation linéaire

$$LX = 0, \quad \text{avec } L \in \mathbf{A}^{1\times n} \text{ et } X \in \mathbf{A}^{n\times 1}$$

admet pour solutions les éléments d'un sous-$\mathbf{A}$-module de type fini de $\mathbf{A}^{n\times 1}$.

Autrement dit :

$$\begin{cases} \forall n \in \mathbb{N},\ \forall L \in \mathbf{A}^{1\times n},\ \exists m \in \mathbb{N},\ \exists G \in \mathbf{A}^{n\times m},\ \forall X \in \mathbf{A}^{n\times 1}\,, \\ \qquad LX = 0 \quad \Longleftrightarrow \quad \exists Y \in \mathbf{A}^{m\times 1},\ X = GY\ . \end{cases} \tag{1}$$

Cela signifie que l'on maîtrise un peu l'ensemble des solutions du système linéaire homogène $LX = 0$.

Il est clair qu'un produit fini d'anneaux est cohérent si, et seulement si, chaque facteur est cohérent.

Plus généralement, si $V = (v_1, \ldots, v_n) \in M^n$, où M est un $\mathbf{A}$-module, on appelle *module des relations entre les* v_i le sous-$\mathbf{A}$-module de $\mathbf{A}^n$ noyau de l'application linéaire

$$\check{V} : \mathbf{A}^n \to M, \qquad (x_1, \ldots, x_n) \mapsto \sum\nolimits_i x_i v_i.$$

On dira aussi de manière plus précise qu'il s'agit du *module des relations pour (le vecteur)* V, ou encore *du module des syzygies pour (le vecteur)* V. Un élément $(x_1, \ldots, x_n)$ de ce noyau est appelé une *relation de dépendance linéaire*, ou encore une *syzygie* entre les v_i.

Par abus de langage on parle indifféremment de *la syzygie* $\sum_i x_i v_i = 0$ ou de *la syzygie* $(x_1, \ldots, x_n) \in \mathbf{A}^n$. Le $\mathbf{A}$-module M est dit *cohérent* si pour tout $V \in M^n$, le module des syzygies est de type fini, autrement dit si l'on a :

$$\begin{cases} \forall n \in \mathbb{N},\ \forall V \in M^{n\times 1},\ \exists m \in \mathbb{N},\ \exists G \in \mathbf{A}^{m\times n},\ \forall X \in \mathbf{A}^{1\times n}\,, \\ \qquad XV = 0 \quad \Longleftrightarrow \quad \exists Y \in \mathbf{A}^{1\times m},\ X = YG\ . \end{cases} \tag{2}$$

Un anneau $\mathbf{A}$ est donc cohérent si, et seulement si, il est cohérent en tant que $\mathbf{A}$-module.

Notez que nous avons utilisé dans la formule (2) une notation transposée par rapport à la formule (1). C'est pour ne pas avoir la somme $\sum_i x_i v_i$ écrite sous forme $\sum_i v_i x_i$ avec $v_i \in M$ et $x_i \in \mathbf{A}$. Dans la suite, nous ne ferons généralement plus cette transposition, car il nous semble préférable de garder la forme usuelle $AX = V$ pour un système linéaire, même si les matrices A et V sont à coefficients dans M.

3.1. Proposition. *Soit* M *un* $\mathbf{A}$*-module cohérent. Tout système linéaire sans second membre,* $BX = 0$ *(avec* $B \in M^{k\times n}$, $X \in \mathbf{A}^{n\times 1}$*), admet pour solutions les éléments d'un sous-*$\mathbf{A}$*-module de type fini de* $\mathbf{A}^{n\times 1}$.

D Faisons la démonstration par exemple pour $k = 2$ (la démonstration générale fonctionne par récurrence de la même manière). Le principe est le suivant : on résout la première équation et l'on porte la solution générale dans la seconde. Voyons ceci plus précisément.

La matrice B est constituée des lignes L et L'. On a une matrice G telle que

$$LX = 0 \quad \Longleftrightarrow \quad \exists Y \in \mathbf{A}^{m\times 1},\ X = GY.$$

Il reste à résoudre l'équation $L'GY = 0$, ce qui équivaut à l'existence d'un vecteur colonne Z tel que $Y = G'Z$ pour une matrice G' convenable. Donc, $BX = 0$ si, et seulement si, X peut s'écrire sous forme $GG'Z$. □

La proposition précédente est particulièrement importante pour les systèmes linéaires sur $\mathbf{A}$ (c'est-à-dire lorsque $M = \mathbf{A}$).

Commentaire. La notion d'anneau cohérent est donc fondamentale du point de vue algorithmique en algèbre commutative. Dans les traités usuels, cette notion est rarement mise en avant parce que l'on préfère la notion d'anneau *noethérien* [4]. En mathématiques classiques, tout anneau noethérien $\mathbf{A}$ est cohérent parce que tous les sous-modules de $\mathbf{A}^n$ sont de type fini, et tout module de type fini est cohérent pour la même raison. En outre, on a le théorème de Hilbert qui dit que *si* $\mathbf{A}$ *est noethérien, toute* $\mathbf{A}$*-algèbre de type fini est également un anneau noethérien,* tandis que la même affirmation est en défaut si l'on remplace « noethérien » par « cohérent ».

D'un point de vue algorithmique cependant, il semble impossible de trouver une formulation constructive satisfaisante de la noethérianité qui implique la cohérence (voir l'exercice 8). Et la cohérence est souvent la propriété la plus importante du point de vue algorithmique. Comme conséquence, la cohérence ne peut pas être sous-entendue (comme c'est le cas en mathématiques classiques) lorsque l'on parle d'un anneau ou d'un module noethérien.

Le théorème classique disant que sur un anneau noethérien tout $\mathbf{A}$-module de type fini est noethérien est souvent avantageusement remplacé par le théorème constructif suivant [5].

Sur un anneau cohérent (resp. noethérien cohérent), tout $\mathbf{A}$*-module de présentation finie est cohérent (resp. noethérien cohérent).*

En fait, comme le montre cet exemple, la noethérianité est souvent une hypothèse inutilement forte. ∎

La définition suivante d'un module noethérien est équivalente à la définition usuelle en mathématiques classiques, mais elle est beaucoup mieux adaptée à l'algèbre constructive (seul l'anneau trivial satisfait constructivement la définition usuelle).

---

4. Nous donnons après ce commentaire une définition constructive de cette notion.

5. Pour la version non noethérienne, voir le théorème IV-4.3, et pour la version noethérienne, voir [MRR, corollary III-2.8 p. 83].

3.2. Définition. *(Noethérianité à la Richman-Seidenberg, [164, 175])*
Un **A**-module est dit *noethérien* s'il vérifie la *condition de chaîne ascendante* suivante : toute suite croissante de sous-modules de type fini possède deux termes consécutifs égaux. Un anneau **A** est dit *noethérien* s'il est noethérien en tant que **A**-module.

Voici un corollaire de la proposition 3.1.

3.3. Corollaire. (Transporteurs et cohérence)
Soit **A** *un anneau cohérent. Alors, le transporteur d'un idéal de type fini dans un autre est un idéal de type fini. Plus généralement, si N et P sont deux sous-modules de type fini d'un* **A***-module cohérent, alors $(P : N)$ est un idéal de type fini.*

3.4. Théorème. *Un* **A***-module M est cohérent si, et seulement si, sont vérifiées les deux conditions suivantes.*

1. *L'intersection de deux sous-modules de type fini arbitraires est un module de type fini.*
2. *L'annulateur d'un élément arbitraire est un idéal de type fini.*

$\triangleright$ *La première condition est nécessaire.* Soient $g_1, \ldots, g_n$ des générateurs du premier sous-module et $g_{n+1}, \ldots, g_m$ des générateurs du second. Se donner un élément de l'intersection revient à se donner une relation $\sum_{i=1}^{m} \alpha_i g_i = 0$ entre les g_i : à une telle relation $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbf{A}^m$, correspond l'élément $\varphi(\alpha) = \alpha_1 g_1 + \cdots + \alpha_n g_n = -(\alpha_{n+1} g_{n+1} + \cdots + \alpha_m g_m)$ dans l'intersection. Donc, si S est un système générateur pour les relations entre les g_i, $\varphi(S)$ engendre l'intersection des deux sous-modules.

La deuxième condition est nécessaire par définition.

Les deux conditions mises ensemble sont suffisantes. Nous donnons l'idée essentielle de la démonstration et laissons les détails à la lectrice. Nous considérons le module des relations pour un $L \in M^n$. On raisonne par récurrence sur n. Pour $n = 1$, la deuxième condition s'applique et donne un système générateur pour les relations liant l'unique élément de L.
Supposons que le module des relations pour tout $L \in M^n$ soit de type fini et considérons un $L' \in M^{n+1}$. Soit un entier $k \in [\![1..n]\!]$; on écrit $L' = L_1 \bullet L_2$, où $L_1 = (a_1, \ldots, a_k)$ et $L_2 = (a_{k+1}, \ldots, a_{n+1})$. Posons $M_1 = \langle a_1, \ldots, a_k \rangle$ et $M_2 = \langle a_{k+1}, \ldots, a_{n+1} \rangle$. Se donner une relation $\sum_{i=1}^{n+1} \alpha_i a_i = 0$ revient à se donner un élément de l'intersection $M_1 \cap M_2$ (comme ci-dessus). On obtiendra donc un système générateur pour les relations entre les a_i en prenant la réunion des trois systèmes de relations suivants : celui des relations entre les éléments de L_1, celui des relations entre les éléments de L_2, et celui qui provient du système générateur de l'intersection $M_1 \cap M_2$. $\square$

En particulier, *un anneau est cohérent si, et seulement si, d'une part l'intersection de deux idéaux de type fini est toujours un idéal de type fini, et d'autre part l'annulateur d'un élément est toujours un idéal de type fini.*

Exemples. Si **K** est un corps discret, toute algèbre de présentation finie sur **K** est un anneau cohérent (théorème VII-1.10). Il est clair aussi que tout anneau de Bézout intègre (cf. page 228) est un anneau cohérent. ∎

Caractère local de la cohérence

On a d'abord la constatation suivante.

Fait. (Les modules de syzygies se comportent bien par localisation.)
On considère un anneau **A**, *M un* **A***-module, $a = (a_1, \dots, a_m) \in M^m$ et N le module des syzygies pour le vecteur des a_i. Soit S un monoïde et soit N' le module des syzygies pour le vecteur des a_i vus dans M_S. Alors, $N' = N_S$.*

▷ L'inclusion $N_S \subseteq N'$ est claire. Inversement, si $\sum_{j=1}^m \frac{x_j}{s_j} a_j = 0$ dans M_S, posons $u = \prod_i s_i$ et $u_j = \prod_{i \neq j} s_i$, de sorte que $\sum_{j=1}^m x_j u_j a_j = 0$ dans M_S et $\sum_{j=1}^m s x_j u_j a_j = 0$ dans M pour un $s \in S$. On a $y = (y_1, \dots, y_m)$ i.e. $y = (s x_1 u_1, \dots, s x_m u_m) \in N$ et $\big(\frac{x_1}{s_1}, \dots, \frac{x_m}{s_m}\big) = \frac{1}{su}\, y$ dans $\mathbf{A}_S^m$. □

La cohérence est une notion locale, au sens suivant.

3.5. Principe local-global concret. (Syzygies, modules cohérents)
On considère un anneau **A**, $S_1, \dots, S_n$ *des monoïdes comaximaux, M un* **A***-module et $a = (a_1, \dots, a_m) \in M^m$.*

0. Le module $N \subseteq \mathbf{A}^m$ des syzygies du vecteur des a_i vus dans M est de type fini si, et seulement si, chaque module $N_i \subseteq \mathbf{A}_{S_i}^m$ des syzygies du vecteur des a_i vus dans M_{S_i} est de type fini.

1. Le module M est cohérent si, et seulement si, chacun des M_{S_i} est cohérent.

2. L'anneau **A** *est cohérent si, et seulement si, chacun des $\mathbf{A}_{S_i}$ est cohérent.*

▷ *0.* La condition est nécessaire d'après le fait énoncé précédemment.
Vu ce même fait, la condition est suffisante d'après le principe local-global concret qui suit.
2. Cas particulier du point *1*, qui résulte clairement du point *0*. □

3.6. Principe local-global concret. (Modules de type fini)
Soient $S_1, \dots, S_n$ des monoïdes comaximaux de $\mathbf{A}$ et M un $\mathbf{A}$-module. Alors, M est de type fini si, et seulement si, chacun des M_{S_i} est de type fini.

D Supposons que M_{S_i} soit un $\mathbf{A}_{S_i}$-module de type fini pour chaque i. Montrons que M est de type fini. Soient $g_{i,1}, \dots, g_{i,q_i}$ des éléments de M qui engendrent M_{S_i}. Soit $x \in M$ arbitraire. Pour chaque i, on a un $s_i \in S_i$ et des $a_{i,j} \in \mathbf{A}$ tels que :

$$s_i x = a_{i,1} g_{i,1} + \cdots + a_{i,q_i} g_{i,q_i}, \quad \text{dans} \quad M.$$

En écrivant $\sum_{i=1}^{n} b_i s_i = 1$, on voit que x est combinaison linéaire des $g_{i,j}$. □

Remarque. Considérons le sous-$\mathbb{Z}$-module M de $\mathbb{Q}$ engendré par les éléments $1/p$, où p parcourt l'ensemble des nombres premiers. On vérifie facilement que M n'est pas de type fini mais qu'il devient de type fini après localisation en n'importe quel idéal premier. Cela signifie que le principe local-global concret 3.6 n'admet pas de version « abstraite » correspondante, dans laquelle la localisation en des monoïdes comaximaux serait remplacée par la localisation en tous les idéaux premiers. En fait la propriété P pour un module d'être de type fini n'est pas une propriété de caractère fini, comme on peut le voir avec le module M ci-dessus et les monoïdes $\mathbb{Z} \setminus \{0\}$ ou $1 + p\mathbb{Z}$. La propriété vérifie par ailleurs le principe de transfert, mais en l'occurrence, cela n'est d'aucune utilité. ∎

Au sujet du test d'égalité et du test d'appartenance

Nous introduisons maintenant quelques notions constructives relatives au test d'égalité et au test d'appartenance.

Un ensemble E est bien défini lorsque l'on a indiqué comment construire ses éléments et lorsque l'on a construit une relation d'équivalence qui définit l'égalité de deux éléments dans l'ensemble. On note $x = y$ l'égalité dans E, ou $x =_E y$ si nécessaire. L'ensemble E est appelé *discret* lorsque l'axiome suivant est vérifié

$$\forall x, y \in E, \qquad x = y \ \text{ ou } \ \neg(x = y).$$

Classiquement, tous les ensembles sont discrets, car le « ou » présent dans la définition est compris de manière « abstraite ». Constructivement, le « ou » présent dans la définition est compris selon la signification du langage usuel : une des deux alternatives au moins doit avoir lieu de manière certaine. Il s'agit donc d'un « ou » de nature algorithmique. En bref un ensemble est discret si l'on a un test pour l'égalité de deux éléments arbitraires de cet ensemble.

Si l'on veut être plus précis et expliquer en détail ce qu'est un test d'égalité dans l'ensemble E, on dira qu'il s'agit d'une construction qui, à partir de

deux éléments de E donnés en tant que tels, fournit une réponse « oui » ou « non » à la question posée (ces éléments sont-ils égaux ?). Mais on ne pourra guère aller plus loin. En mathématiques constructives les notions de nombre entier et de construction sont des concepts de base. Elles peuvent être expliquées et commentées, mais pas à proprement parler « définies ». La signification constructive du « ou » et celle du « il existe » sont ainsi directement dépendantes de la notion de construction [6], que l'on ne tente pas de définir.

Un *corps discret* (en un seul mot) est un anneau où est vérifié l'axiome suivant :

$$\forall x \in \mathbf{A}, \qquad x = 0 \ \text{ ou } \ x \in \mathbf{A}^{\times}. \tag{3}$$

L'anneau trivial est un corps discret.

Remarque. La méthode chinoise du pivot (souvent appelée méthode du pivot de Gauss) fonctionne de façon algorithmique avec les corps discrets. Cela signifie que l'algèbre linéaire de base est explicite sur les corps discrets. ∎

Notons qu'un corps discret $\mathbf{A}$ est un ensemble discret si, et seulement si, le test « $1 =_{\mathbf{A}} 0$? » est explicite [7]. Il arrive cependant que l'on sache qu'un anneau construit au cours d'un algorithme est un corps discret sans savoir s'il est trivial ou non.

Si $\mathbf{A}$ est un corps discret non trivial, l'affirmation « M est un espace vectoriel libre de dimension finie » est plus précise que l'affirmation « M est un espace vectoriel de type fini », car dans le dernier cas, savoir extraire une base du système générateur revient à disposer d'un test d'indépendance linéaire dans M. Un espace vectoriel de type fini est aussi dit *fini*, un espace vectoriel libre de dimension finie est aussi dit *strictement fini*.

Une partie P d'un ensemble E est dite *détachable* lorsque la propriété suivante est vérifiée :

$$\forall x \in E, \qquad x \in P \ \text{ ou } \ \neg(x \in P).$$

Il revient au même de se donner une partie détachable de E ou sa fonction caractéristique $\chi_P : E \to \{0, 1\}$.

En mathématiques constructives, on considère que si deux ensembles E et F sont correctement définis, il en va de même pour l'*ensemble des*

6. En mathématiques classiques on peut vouloir définir la notion de construction à partir de la notion de « programme correct ». Mais ce que l'on définit ainsi est plutôt la notion de « construction mécanisable ». Et surtout dans la notion de « programme correct », il y a le fait que le programme doit s'arrêter après un nombre fini d'étapes. Cela cache un « il existe », qui en mathématiques constructives renvoie de manière irréductible à la notion de construction. Voir à ce sujet la section A-4 de l'Annexe.

7. La notion générale de corps en mathématiques constructives sera définie page 533. Nous verrons que, si un corps est un ensemble discret, c'est un corps discret.

fonctions de E vers F, que l'on note F^E. En conséquence l'*ensemble des parties détachables* d'un ensemble E est lui-même correctement défini car il s'identifie à l'ensemble $\{0,1\}^E$ des fonctions caractéristiques de source E.

Anneaux et modules cohérents fortement discrets

Un anneau (resp. un module) est dit *fortement discret* lorsque les idéaux de type fini (resp. les sous-modules de type fini) sont détachables, c'est-à-dire encore si les quotients par les idéaux de type fini (resp. par les sous-modules de type fini) sont discrets.

Cela revient à dire que l'on a un test pour décider si une équation linéaire $LX = c$ admet ou non une solution, et en calculer une en cas de réponse positive.

Un résultat essentiel pour l'algèbre constructive et le calcul formel affirme que $\mathbb{Z}[X_1, \ldots, X_n]$ est un anneau cohérent fortement discret.
Plus généralement, on a la version constructive suivante du théorème de Hilbert (voir [MRR, Adams & Loustaunau]).

Si $\mathbf{A}$ est un anneau noethérien cohérent fortement discret, il en va de même pour toute $\mathbf{A}$-algèbre de présentation finie.

La proposition suivante se démontre comme la proposition 3.1.

3.7. Proposition. *Sur un module cohérent fortement discret M, tout système linéaire $BX = C$ ($B \in M^{k\times n}$, $C \in M^{k\times 1}$, $X \in \mathbf{A}^{n\times 1}$) peut être testé. En cas de réponse positive, une solution particulière X_0 peut être calculée. En outre, les solutions X sont tous les éléments de $X_0 + N$, où N est un sous-$\mathbf{A}$-module de type fini de $\mathbf{A}^{n\times 1}$.*

Il est clair que le quotient d'un module cohérent fortement discret par un sous-module de type fini est encore cohérent fortement discret.

En revanche, un localisé d'un module cohérent fortement discret, toujours cohérent, n'est pas nécessairement fortement discret. Le théorème XII-7.2 donne un exemple important où $\mathbf{A}[1/s]$ reste fortement discret.

De manière générale, on a au moins le résultat suivant.

3.8. Proposition. *Soient $\mathbf{A}$ un anneau cohérent fortement discret, $\mathfrak{a}$ un idéal de type fini et M un $\mathbf{A}$-module cohérent fortement discret. Alors, $\mathbf{A}_{1+\mathfrak{a}}$ et $M_{1+\mathfrak{a}}$ sont cohérents fortement discrets.*

▷ On prend $\mathfrak{a} = \langle a_1, \ldots, a_m\rangle$ et l'on considère $N = \langle u_1, \ldots, u_n\rangle$ un sous-module de type fini de M. Pour un $y \in M$ arbitraire, on a $y \in N$ dans $M_{1+\mathfrak{a}}$ si, et seulement si, il existe $x_1, \ldots, x_m$ et $z_1, \ldots, z_n \in \mathbf{A}$ tels que l'on ait $y(1 + \sum_i x_i a_i) = \sum_j z_j u_j$. Il s'agit donc de résoudre une équation linéaire à inconnues dans $\mathbf{A}$ et à coefficients dans M. □

4. Systèmes fondamentaux d'idempotents orthogonaux

Un élément e d'un anneau est dit *idempotent* si $e^2 = e$. Dans ce cas, $1-e$ est aussi un idempotent, appelé l'*idempotent complémentaire de* e, ou encore le *complément de* e. Pour deux idempotents e_1 et e_2, on a

$$\langle e_1\rangle \cap \langle e_2\rangle = \langle e_1e_2\rangle\,, \quad \langle e_1\rangle + \langle e_2\rangle = \langle e_1, e_2\rangle = \langle e_1 + e_2 - e_1e_2\rangle\,,$$

avec e_1e_2 et $e_1 + e_2 - e_1e_2$ idempotents. Deux idempotents e_1 et e_2 sont dits *orthogonaux* lorsque $e_1e_2 = 0$. On a alors $\langle e_1\rangle + \langle e_2\rangle = \langle e_1 + e_2\rangle$.

Un anneau est dit *connexe* si tout idempotent est égal à 0 ou 1.

Dans la suite nous utilisons implicitement le fait évident suivant : pour un idempotent e et un élément x, e divise x si, et seulement si, $x = ex$.

La présence d'un idempotent $\neq 0, 1$ signifie que l'anneau $\mathbf{A}$ est isomorphe à un produit de deux anneaux $\mathbf{A}_1$ et $\mathbf{A}_2$, et que tout calcul dans $\mathbf{A}$ peut être scindé en deux calculs « plus simples » dans $\mathbf{A}_1$ et $\mathbf{A}_2$. On décrit cette situation comme suit.

4.1. Fait. *Pour tout isomorphisme $\lambda : \mathbf{A} \to \mathbf{A}_1 \times \mathbf{A}_2$, il existe un unique élément $e \in \mathbf{A}$ satisfaisant les propriétés suivantes.*

1. *L'élément e est idempotent (on note son complément $f = 1 - e$).*
2. *L'homomorphisme $\mathbf{A} \to \mathbf{A}_1$ identifie $\mathbf{A}_1$ avec $\mathbf{A}/\langle e\rangle$ et avec $\mathbf{A}[1/f]$.*
3. *L'homomorphisme $\mathbf{A} \to \mathbf{A}_2$ identifie $\mathbf{A}_2$ avec $\mathbf{A}/\langle f\rangle$ et avec $\mathbf{A}[1/e]$.*

Réciproquement, si e est un idempotent et f son complément, l'homomorphisme canonique $\mathbf{A} \to \mathbf{A}/\langle e\rangle \times \mathbf{A}/\langle f\rangle$ est un isomorphisme.

⊳ L'élément e est défini par $\lambda(e) = (0, 1)$. □

On peut apporter quelques précisions souvent utiles.

4.2. Fait. *Soit e un idempotent de $\mathbf{A}$, et soient $f = 1-e$ et M un $\mathbf{A}$-module.*

1. *Les monoïdes $e^{\mathbb{N}} = \{1, e\}$ et $1 + f\mathbf{A}$ ont le même saturé.*
2. *En tant que $\mathbf{A}$-module, $\mathbf{A}$ est somme directe de $\langle e\rangle = e\mathbf{A}$ et $\langle f\rangle = f\mathbf{A}$. L'idéal $e\mathbf{A}$ est un anneau si l'on prend e comme élément neutre pour la multiplication. On a alors trois anneaux isomorphes*

$$\mathbf{A}[1/e] = (1 + f\mathbf{A})^{-1}\mathbf{A} \;\simeq\; \mathbf{A}/\langle f\rangle \;\simeq\; e\mathbf{A}.$$

Ces isomorphismes proviennent des trois applications canoniques

$$\begin{array}{lll} \mathbf{A} \to \mathbf{A}[1/e] & : & x \mapsto x/1, \\ \mathbf{A} \to \mathbf{A}/\langle f\rangle & : & x \mapsto x \bmod \langle f\rangle\,, \\ \mathbf{A} \to e\mathbf{A} & : & x \mapsto e\,x, \end{array}$$

qui sont surjectives et ont même noyau.

3. On a trois $\mathbf{A}$*-modules isomorphes* $M[1/e] \simeq M/fM \simeq eM$*. Ces isomorphismes proviennent des trois applications canoniques*

$$\begin{array}{lll} M \to M[1/e] & : & x \mapsto x/1, \\ M \to M/fM & : & x \mapsto x \bmod \langle f \rangle, \\ M \to eM & : & x \mapsto e\,x, \end{array}$$

qui sont surjectives et ont même noyau.

Par ailleurs, il faut prendre garde que l'idéal $e\mathbf{A}$, qui est un anneau avec e pour élément neutre, n'est pas un sous-anneau de $\mathbf{A}$ (sauf si $e = 1$).

Dans un anneau $\mathbf{A}$ un *système fondamental d'idempotents orthogonaux* est une liste $(e_1, \ldots, e_n)$ d'éléments de $\mathbf{A}$ qui satisfait les égalités suivantes :

$$e_i e_j = 0, \ \text{ pour } \ i \neq j \quad \text{ et } \quad \textstyle\sum_{i=1}^{n} e_i = 1.$$

Cela implique que les e_i sont idempotents. Nous ne réclamons pas qu'ils soient tous non nuls [8].

4.3. Théorème. (Système fondamental d'idempotents orthogonaux)
Soit $(e_1, \ldots, e_n)$ *un système fondamental d'idempotents orthogonaux d'un anneau* $\mathbf{A}$*, et* M *un* $\mathbf{A}$*-module. Notons* $\mathbf{A}_i = \mathbf{A}/\langle 1 - e_i \rangle \simeq \mathbf{A}[1/e_i]$*. Alors :*

$$\begin{array}{rl} \mathbf{A} \simeq & \mathbf{A}_1 \times \cdots \times \mathbf{A}_n, \\ M = & e_1 M \oplus \cdots \oplus e_n M. \end{array}$$

Notez que $e_1 M$ est un $\mathbf{A}$-module et un $\mathbf{A}_1$-module, mais que ce n'est pas un $\mathbf{A}_2$-module (sauf s'il est nul).

Le lemme suivant donne une réciproque du théorème 4.3

4.4. Lemme. *Soient* $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ *des idéaux de* $\mathbf{A}$*. On a* $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$ *si, et seulement si, il existe un système fondamental d'idempotents orthogonaux* $(e_i)_{i \in [\![1..n]\!]}$ *tel que* $\mathfrak{a}_i = \langle e_i \rangle$ *pour* $i \in [\![1..n]\!]$*. Dans ce cas le système fondamental d'idempotents orthogonaux est déterminé de manière unique.*

D Supposons $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$. On a des $e_i \in \mathfrak{a}_i$ tels que $\sum_i e_i = 1$, et comme $e_i e_j \in \mathfrak{a}_i \cap \mathfrak{a}_j = \{0\}$ pour $i \neq j$, on obtient bien un système fondamental d'idempotents orthogonaux.
En outre si $x \in \mathfrak{a}_j$, on a $x = x \sum_i e_i = x e_j$ et donc $\mathfrak{a}_j = \langle e_j \rangle$.
L'implication réciproque est immédiate. L'unicité résulte de celle d'une écriture d'un élément dans une somme directe. □

Voici maintenant deux lemmes très utiles.

8. C'est beaucoup plus confortable pour obtenir des énoncés uniformes. En outre, c'est pratiquement indispensable lorsque l'on ne sait pas tester l'égalité à zéro des idempotents dans l'anneau avec lequel on travaille.

4.5. Lemme. (Lemme de l'idéal engendré par un idempotent)
Un idéal $\mathfrak{a}$ est engendré par un idempotent si, et seulement si,

$$\mathfrak{a} + \operatorname{Ann}\mathfrak{a} = \langle 1\rangle\,.$$

▷ Tout d'abord, si e est idempotent, on a $\operatorname{Ann}\langle e\rangle = \langle 1-e\rangle$. Pour l'implication réciproque, soit $e \in \mathfrak{a}$ tel que $1-e \in \operatorname{Ann}\mathfrak{a}$. Alors, $e(1-e)=0$, donc e est idempotent. Et, pour tout $y \in \mathfrak{a}$, $y = ye$, donc $\mathfrak{a} \subseteq \langle e\rangle$. □

4.6. Lemme. (Lemme de l'idéal de type fini idempotent)
Si $\mathfrak{a}$ est un idéal de type fini idempotent (i.e., $\mathfrak{a} = \mathfrak{a}^2$) dans $\mathbf{A}$, alors $\mathfrak{a} = \langle e\rangle$ avec $e^2 = e$ entièrement déterminé par $\mathfrak{a}$.

▷ On utilise le truc du déterminant. On considère un système générateur $(a_1, \dots a_q)$ de $\mathfrak{a}$ et le vecteur colonne $\underline{a} = {}^{\mathrm{t}}[\,a_1\ \cdots\ a_q\,]$.
Puisque $a_j \in \mathfrak{a}^2$ pour $j \in [\![1..q]\!]$, il existe $C \in \mathbb{M}_q(\mathfrak{a})$ telle que $\underline{a} = C\,\underline{a}$, donc $(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$ et $\det(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$. Or, $\det(\mathrm{I}_q - C) = 1 - e$ avec $e \in \mathfrak{a}$.
Donc, $(1-e)\mathfrak{a} = 0$, et l'on applique le lemme 4.5.
Enfin, l'unicité de e est déjà dans le lemme 4.4. □

Rappelons enfin le théorème chinois, outil très efficace, qui cache un système fondamental d'idempotents orthogonaux. Des idéaux $\mathfrak{b}_1$, …, $\mathfrak{b}_\ell$ d'un anneau $\mathbf{A}$ sont dit *comaximaux* lorsque $\mathfrak{b}_1 + \cdots + \mathfrak{b}_\ell = \langle 1\rangle$.

4.7. Théorème des restes chinois
Soient dans $\mathbf{A}$ des idéaux $(\mathfrak{a}_i)_{i\in[\![1..n]\!]}$ deux à deux comaximaux et $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$.

1. *On a l'égalité $\mathfrak{a} = \prod_i \mathfrak{a}_i$,*
2. *l'application canonique $\mathbf{A}/\mathfrak{a} \to \prod_i \mathbf{A}/\mathfrak{a}_i$ est un isomorphisme,*
3. *il existe e_1, …, e_n dans $\mathbf{A}$ tels que $\mathfrak{a}_i = \mathfrak{a} + \langle 1 - e_i\rangle$ et les $\pi_{\mathbf{A},\mathfrak{a}}(e_i)$ forment un système fondamental d'idempotents orthogonaux de $\mathbf{A}/\mathfrak{a}$.*

Comme corollaire on obtient le lemme des noyaux.

4.8. Lemme. (Lemme des noyaux)
Soit $P = P_1 \cdots P_\ell \in \mathbf{A}[X]$ et une application $\mathbf{A}$-linéaire $\varphi : M \to M$ vérifiant $P(\varphi) = 0$. On suppose que les P_i sont deux à deux comaximaux. Notons $K_i = \operatorname{Ker}\big(P_i(\varphi)\big)$, $Q_i = \prod_{j\neq i} P_j$. On a alors :

$$K_i = \operatorname{Im}\big(Q_i(\varphi)\big),\ M = \bigoplus_{j=1}^{\ell} K_j \quad \text{et} \quad \operatorname{Im}\big(P_i(\varphi)\big) = \operatorname{Ker}\big(Q_i(\varphi)\big) = \bigoplus_{j\neq i} K_i.$$

▷ On considère l'anneau $\mathbf{B} = \mathbf{A}[X]/\langle P\rangle$. Le module M peut être vu comme un $\mathbf{B}$-module pour la loi $(Q, y) \mapsto Q \cdot y = Q(\varphi)(y)$. On applique alors le théorème des restes chinois et le théorème de structure 4.3.
Cette démonstration résume le calcul plus classique suivant. À partir des égalités $U_{ij}P_i + U_{ji}P_j = 1$, on obtient des égalités $U_iP_i + V_iQ_i = 1$, ainsi qu'une égalité $\sum_i W_iQ_i = 1$. Notons $p_i = P_i(\varphi)$, $q_i = Q_i(\varphi)$, etc.

Alors, tous les endomorphismes obtenus commutent et l'on obtient des égalités $p_i q_i = 0$, $u_i p_i + v_i q_i = \mathrm{Id}_M$, $\sum_i w_i q_i = \mathrm{Id}_M$. Le lemme en découle facilement. □

5. Un peu d'algèbre extérieure

Qu'un système linéaire homogène de n équations à n inconnues
admette (sur un corps discret) une solution non triviale
si, et seulement si, le déterminant du système est nul,
voilà un fait d'une importance capitale dont on
n'aura jamais fini de mesurer la portée.
Anonyme

Éliminons, éliminons, éliminons
les éliminateurs de l'élimination !
Poème mathématique (extrait)
S. Abhyankar

Quelques exemples simples illustrent ces idées dans la section présente.

Sous-modules libres en facteur direct (Splitting Off)

Soit $k \in \mathbb{N}$. Un *module libre de rang k* est par définition un $\mathbf{A}$-module isomorphe à $\mathbf{A}^k$. Si k n'est pas précisé, on dira *module libre de rang fini*.

Lorsque $\mathbf{A}$ est un corps discret on parle indifféremment d'*espace vectoriel de dimension finie* ou *de rang fini* ou *strictement fini*.

Les modules dont la structure est la plus simple sont les modules libres de rang fini. On est donc intéressé par la possibilité d'écrire un module arbitraire M sous la forme $L \oplus N$, où L est un module libre de rang fini. Une réponse (partielle) à cette question est donnée par l'algèbre extérieure.

5.1. Proposition. (Splitting Off)
Soient $a_1, \ldots, a_k$ des éléments d'un $\mathbf{A}$-module M, alors les propriétés suivantes sont équivalentes.

1. *Le sous-module $L = \langle a_1, \ldots, a_k \rangle$ de M est libre de base $(a_1, \ldots, a_k)$ et il est facteur direct de M.*
2. *Il existe une forme k-linéaire alternée $\varphi : M^k \to \mathbf{A}$ qui satisfait l'égalité $\varphi(a_1, \ldots, a_k) = 1$.*

D *1 ⇒ 2.* Si $L \oplus N = M$, si $\pi : M \to L$ est la projection parallèlement à N, et si $\theta_j : L \to \mathbf{A}$ est la j-ième forme coordonnée pour la base $(a_1, \ldots, a_k)$, on définit

$$\varphi(x_1, \ldots, x_k) = \det\Big(\big(\theta_j\big(\pi(x_i)\big)\big)_{i,j \in [\![1..k]\!]}\Big).$$

2 ⇒ 1. On définit l'application linéaire $\pi : M \to M$ par

$$\pi(x) = \sum_{j=1}^{k} \varphi(\underbrace{a_1, \ldots, x, \ldots, a_k}_{(x \text{ est en position } j)})\, a_j.$$

On a immédiatement $\pi(a_i) = a_i$ et $\operatorname{Im}\pi \subseteq L := \langle a_1, \ldots, a_k\rangle$, donc $\pi^2 = \pi$ et $\operatorname{Im}\pi = L$. Enfin, si $x = \sum_j \lambda_j a_j = 0$, alors $\varphi(a_1, \ldots, x, \ldots, a_k) = \lambda_j = 0$ (avec x en position j). □

Cas particulier : pour $k = 1$ on dit que l'élément a de M est *unimodulaire* lorsqu'il existe une forme linéaire $\varphi : M \to \mathbf{A}$ tel que $\varphi(a) = 1$. Dire que le vecteur $b = (b_1, \ldots, b_n) \in \mathbf{A}^n$ est unimodulaire revient à dire que les b_i sont comaximaux. On dit aussi dans ce cas que la suite $(b_1, \ldots, b_n)$ est *unimodulaire*.

Le rang d'un module libre

Comme nous allons le voir, le rang d'un module libre est un entier bien déterminé si l'anneau n'est pas trivial. Autrement dit, deux $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ et $P \simeq \mathbf{A}^p$ avec $m \neq p$ ne peuvent être isomorphes que si $1 =_{\mathbf{A}} 0$.

Nous utiliserons la notation $\operatorname{rg}_{\mathbf{A}}(M) = k$ (ou $\operatorname{rg}(M) = k$ si $\mathbf{A}$ est clair d'après le contexte) pour indiquer qu'un module (supposé libre) est de rang k.

Une démonstration savante consiste à dire que, si $m > p$, la puissance extérieure m-ième de P est $\{0\}$ tandis que celle de M est isomorphe à $\mathbf{A}$ (c'est pour l'essentiel la preuve faite dans le corollaire 5.23).

La même démonstration peut être présentée de façon plus élémentaire comme suit. Rappelons tout d'abord la formule de Cramer de base. Si B est une matrice carrée d'ordre n, nous notons $\widetilde{B}$ ou $\operatorname{Adj} B$ la matrice *cotransposée* (on dit parfois, *adjointe*). La forme élémentaire des identités de Cramer s'écrit alors :

$$A\ \operatorname{Adj}(A) = \operatorname{Adj}(A)\, A = \det(A)\, \mathrm{I}_n. \tag{4}$$

Cette formule, jointe à la formule du produit « $\det(AB) = \det(A)\det(B)$ », implique qu'une matrice carrée A est inversible si, et seulement si, son déterminant est inversible, ou encore si elle est inversible d'un seul côté, et que son inverse est alors égal à $(\det A)^{-1} \operatorname{Adj} A$.

On considère maintenant deux $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ et $P \simeq \mathbf{A}^p$ avec $m \geqslant p$ et une application linéaire surjective $\varphi : P \to M$. Il existe donc une application linéaire $\psi : M \to P$ telle que $\varphi \circ \psi = \mathrm{Id}_M$. Cela correspond à deux matrices $A \in \mathbf{A}^{m\times p}$ et $B \in \mathbf{A}^{p\times m}$ avec $AB = \mathrm{I}_m$. Si $m = p$, la matrice A est inversible d'inverse B et φ et ψ sont des isomorphismes réciproques. Si $m > p$, on a $AB = A_1B_1$ avec A_1 et B_1 carrées obtenues à partir de A et B en complétant par des zéros ($m - p$ colonnes pour A_1, $m - p$ lignes pour B_1).

$$A_1 = \left[\begin{array}{c|c} 0 & \\ \vdots & A \\ 0 & \end{array}\right], \qquad B_1 = \left[\begin{array}{c|c} 0 \quad \cdots \quad 0 & \\ \hline & B \end{array}\right], \qquad A_1 B_1 = \mathrm{I}_m.$$

Ainsi, $1 = \det \mathrm{I}_m = \det(AB) = \det(A_1 B_1) = \det(A_1)\det(B_1) = 0$.
Dans cette démonstration, on voit clairement apparaître la commutativité de l'anneau (qui est vraiment nécessaire). Résumons.

5.2. Proposition. *Soient deux* $\mathbf{A}$*-modules* $M \simeq \mathbf{A}^m$ *et* $P \simeq \mathbf{A}^p$*, et soit une application linéaire surjective* $\varphi : P \to M$*.*

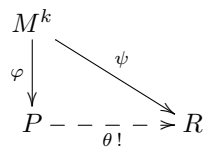
1. *Si* $m = p$*, alors* φ *est un isomorphisme. Autrement dit, dans un module* $\mathbf{A}^m$ *tout système générateur de* m *éléments est une base.*
2. *Si* $m > p$*, alors* $1 =_{\mathbf{A}} 0$*. Et si l'anneau n'est pas trivial,* $m > p$ *est impossible.*

Dans la suite, ce théorème de classification important apparaîtra souvent comme corollaire de théorèmes plus subtils, comme par exemple le théorème IV-5.1 ou le théorème IV-5.2.

Puissances extérieures d'un module

Terminologie. Rappelons que l'on appelle *mineur* d'une matrice A tout déterminant d'une matrice carrée extraite de A sur certaines lignes et certaines colonnes. On parle de *mineur d'ordre* k lorsque la matrice carrée extraite est dans $\mathbb{M}_k(\mathbf{A})$. Lorsque A est une matrice carrée, un *mineur principal* est un mineur correspondant à une matrice extraite pour le même ensemble d'indices sur les lignes et sur les colonnes. Par exemple si $A \in \mathbb{M}_n(\mathbf{A})$, le coefficient de X^k dans le polynôme $\det(\mathrm{I}_n + XA)$ est la somme des mineurs principaux d'ordre k de A. Enfin, on appelle *mineur principal dominant* un mineur principal en position nord-ouest, c'est-à-dire obtenu en extrayant la matrice sur les premières lignes et les premières colonnes. ∎

Soit M un $\mathbf{A}$-module. Une application k-linéaire alternée $\varphi : M^k \to P$ est appelée une *puissance extérieure* k*-ième du* $\mathbf{A}$*-module* M si toute application k-linéaire alternée $\psi : M^k \to R$ s'écrit de manière unique sous la forme $\psi = \theta \circ \varphi$, où θ est une application $\mathbf{A}$-linéaire de P vers R.



applications k-linéaires alternées

applications linéaires.

Il est clair que $\varphi : M^k \to P$ est unique au sens catégorique, c'est-à-dire que pour toute autre puissance extérieure $\varphi' : M^k \to P'$ il y a une application linéaire unique $\theta : P \to P'$ qui rend le diagramme convenable commutatif, et que θ est un isomorphisme.

On note alors $\bigwedge^k M$ ou $\bigwedge^k_{\mathbf{A}} M$ pour P et $\lambda_k(x_1, \ldots, x_k)$ ou $x_1 \wedge \cdots \wedge x_k$ pour $\varphi(x_1, \ldots, x_k)$.

L'existence d'une puissance extérieure k-ième pour tout module M résulte de considérations générales analogues à celles que nous détaillerons pour le produit tensoriel page 213 de la section IV-4.

La théorie la plus simple des puissances extérieures, analogue à la théorie élémentaire du déterminant, démontre que si M est un module libre ayant une base de n éléments $(a_1, \ldots, a_n)$, alors $\bigwedge^k M$ est nul si $k > n$, et sinon c'est un module libre ayant pour base les $\binom{n}{k}$ k-vecteurs $a_{i_1} \wedge \cdots \wedge a_{i_k}$, où $(i_1, \ldots, i_k)$ parcourt l'ensemble des k-uplets strictement croissants d'éléments de $[\![1..n]\!]$.

En particulier, $\bigwedge^n M$ est libre de rang 1 avec pour base $a_1 \wedge \cdots \wedge a_n$.

À toute application $\mathbf{A}$-linéaire $\alpha : M \to N$ correspond une unique application $\mathbf{A}$-linéaire $\bigwedge^k \alpha : \bigwedge^k M \to \bigwedge^k N$ vérifiant l'égalité

$$\Big(\bigwedge^k \alpha\Big)(x_1 \wedge \cdots \wedge x_k) = \alpha(x_1) \wedge \cdots \wedge \alpha(x_k),$$

pour tout k-vecteur $x_1 \wedge \cdots \wedge x_k$ de $\bigwedge^k M$. L'application linéaire $\bigwedge^k \alpha$ s'appelle la *puissance extérieure* k-ième de l'application linéaire α.

En outre, on a $\big(\bigwedge^k \alpha\big) \circ \big(\bigwedge^k \beta\big) = \bigwedge^k (\alpha \circ \beta)$ quand $\alpha \circ \beta$ est défini. En bref, chaque $\bigwedge^k(\bullet)$ est un foncteur.

Si M et N sont libres de bases respectives $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_m)$, et si α admet la matrice H sur ces bases, alors $\bigwedge^k \alpha$ admet la matrice notée $\bigwedge^k H$ sur les bases correspondantes de $\bigwedge^k M$ et $\bigwedge^k N$. Les coefficients de cette matrice sont tous les mineurs d'ordre k de la matrice H.

Idéaux déterminantiels

5.3. Définition. Soient $G \in \mathbf{A}^{n \times m}$ et $k \in [\![1.. \min(m, n)]\!]$. *L'idéal déterminantiel d'ordre k de la matrice G* est l'idéal, noté $\mathcal{D}_{\mathbf{A},k}(G)$ ou $\mathcal{D}_k(G)$, engendré par les mineurs d'ordre k de G. Pour $k \leqslant 0$, on pose par convention $\mathcal{D}_k(G) = \langle 1 \rangle$, et pour $k > \min(m, n)$, $\mathcal{D}_k(G) = \langle 0 \rangle$.

Ces conventions sont naturelles car elles permettent d'obtenir en toute généralité les égalités suivantes.

— Si $H = \begin{array}{|c|c|}\hline \mathrm{I}_r & 0 \\ \hline 0 & G \\ \hline \end{array}$, pour tout $k \in \mathbb{Z}$, on a $\mathcal{D}_k(G) = \mathcal{D}_{k+r}(H)$.

— Si $H = \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & G \\ \hline \end{array}$, pour tout $k \in \mathbb{Z}$, on a $\mathcal{D}_k(H) = \mathcal{D}_k(G)$.

5.4. Fait. *Pour toute matrice G de type $n \times m$ on a les inclusions*

$$\{0\} = \mathcal{D}_{1+\min(m,n)}(G) \subseteq \cdots \subseteq \mathcal{D}_1(G) \subseteq \mathcal{D}_0(G) = \langle 1 \rangle = \mathbf{A}. \tag{5}$$

Plus précisément, pour tout $k, r \in \mathbb{N}$, on a une inclusion

$$\mathcal{D}_{k+r}(G) \subseteq \mathcal{D}_k(G)\,\mathcal{D}_r(G). \tag{6}$$

En effet, tout mineur d'ordre $h+1$ s'exprime comme combinaison linéaire de mineurs d'ordre h. Et l'inclusion (6) s'obtient avec le développement de Laplace du déterminant.

5.5. Fait. *Soient $G_1 \in \mathbf{A}^{n\times m_1}$, $G_2 \in \mathbf{A}^{n\times m_2}$ et $H \in \mathbf{A}^{p\times n}$.*

1. *Si $\operatorname{Im} G_1 \subseteq \operatorname{Im} G_2$, alors pour tout entier k on a $\mathcal{D}_k(G_1) \subseteq \mathcal{D}_k(G_2)$.*
2. *Pour tout entier k, on a $\mathcal{D}_k(HG_1) \subseteq \mathcal{D}_k(G_1)$.*
3. *Les idéaux déterminantiels d'une matrice $G \in \mathbf{A}^{n\times m}$ ne dépendent que de la classe d'équivalence du sous-module image de G (i.e., ils ne dépendent que de $\operatorname{Im} G$, à automorphisme près du module $\mathbf{A}^n$).*
4. *En particulier, si φ est une application linéaire entre modules libres de rangs finis, les idéaux déterminantiels d'une matrice de φ ne dépendent pas des bases choisies. On les note $\mathcal{D}_k(\varphi)$ et on les appelle les* idéaux déterminantiels de l'application linéaire φ.

▷ *1.* Chaque colonne de G_1 est une combinaison linéaire de colonnes de G_2. On conclut par la multilinéarité du déterminant.
2. Même raisonnement en remplaçant les colonnes par les lignes.
Enfin, *3* implique *4* et résulte des deux points précédents. □

Remarque. Un idéal déterminantiel est donc attaché essentiellement à un sous-module de type fini M d'un module libre L. Mais c'est la structure de l'inclusion $M \subseteq L$ et non pas seulement la structure de M qui intervient pour déterminer les idéaux déterminantiels. Par exemple $M = 3\mathbb{Z} \times 5\mathbb{Z}$ est un sous-$\mathbb{Z}$-module libre de $L = \mathbb{Z}^2$ et ses idéaux déterminantiels sont $\mathcal{D}_1(M) = \langle 1 \rangle$, $\mathcal{D}_2(M) = \langle 15 \rangle$. Si l'on remplace 3 et 5 par 6 et 10 par exemple, on obtient un autre sous-module libre, mais la structure de l'inclusion est différente puisque les idéaux déterminantiels sont maintenant $\langle 2 \rangle$ et $\langle 60 \rangle$. ■

5.6. Fait. *Si G et H sont des matrices telles que GH est définie, alors pour tout $n \geqslant 0$ on a*
$$\mathcal{D}_n(GH) \subseteq \mathcal{D}_n(G)\,\mathcal{D}_n(H). \tag{7}$$

▷ Le résultat est clair pour $n = 1$. Pour $n > 1$, on se ramène au cas $n = 1$ en notant que les mineurs d'ordre n de G, H et GH représentent les coefficients des matrices « puissance extérieure n-ième de G, H et GH » (en tenant compte de l'égalité $\bigwedge^n(\varphi\psi) = \bigwedge^n \varphi \circ \bigwedge^n \psi$). □

L'égalité suivante est immédiate.
$$\mathcal{D}_n(\varphi \oplus \psi) = \sum\nolimits_{k=0}^{n} \mathcal{D}_k(\varphi)\,\mathcal{D}_{n-k}(\psi). \tag{8}$$

Rang d'une matrice

5.7. Définition
Une application linéaire φ entre modules libres de rangs finis est dite
- *de rang $\leqslant k$* si $\mathcal{D}_{k+1}(\varphi) = 0$;
- *de rang $\geqslant k$* si $\mathcal{D}_k(\varphi) = \langle 1\rangle$;
- *de rang k* si elle est à la fois de rang $\geqslant k$ et de rang $\leqslant k$.

Nous utiliserons les notations $\mathrm{rg}(\varphi) \geqslant k$ et $\mathrm{rg}(\varphi) \leqslant k$, conformément à la définition précédente, sans présupposer que $\mathrm{rg}(\varphi)$ soit défini. Seule l'écriture $\mathrm{rg}(\varphi) = k$ signifiera que le rang est défini.

Nous généraliserons plus loin cette définition au cas d'applications linéaires entre modules projectifs de type fini : voir les exercices X-21, X-22 et X-23.

Commentaire. Le lecteur doit prendre garde qu'il n'existe pas de définition universellement acceptée pour « matrice de rang k » dans la littérature. En lisant un autre ouvrage, il doit d'abord s'assurer de la définition adoptée par l'auteur. Par exemple, dans le cas d'un anneau intègre $\mathbf{A}$, on trouve souvent le rang défini comme celui de la matrice vue dans le corps de fractions de $\mathbf{A}$. Néanmoins, une matrice de rang k au sens de la définition 5.7 est généralement de rang k au sens des autres auteurs. ■

Le principe local-global concret suivant est une conséquence immédiate du principe local-global de base.

5.8. Principe local-global concret. (Rang d'une matrice)
Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$ et B une matrice $\in \mathbf{A}^{m\times p}$. Alors les propriétés suivantes sont équivalentes.

1. *La matrice est de rang $\leqslant k$ (resp. de rang $\geqslant k$) sur $\mathbf{A}$.*
2. *Pour $i \in [\![1..n]\!]$, la matrice est de rang $\leqslant k$ (resp. de rang $\geqslant k$) sur $\mathbf{A}_{S_i}$.*

Méthode du pivot généralisée

Terminologie

1) Deux matrices sont dites *équivalentes* lorsque l'on passe de l'une à l'autre en multipliant à droite et à gauche par des matrices inversibles.

2) Deux matrices carrées dans $\mathbb{M}_n(\mathbf{A})$ sont dites *semblables* lorsqu'elles représentent le même endomorphisme de $\mathbf{A}^n$ sur deux bases (distinctes ou non), autrement dit lorsqu'elles sont conjuguées pour l'action $(G, M) \mapsto GMG^{-1}$ de $\mathbb{GL}_n(\mathbf{A})$ sur $\mathbb{M}_n(\mathbf{A})$.

3) Une *manipulation élémentaire de lignes* sur une matrice de n lignes consiste en le remplacement d'une ligne L_i par la ligne $L_i + \lambda L_j$ avec $i \neq j$. On la note aussi $L_i \leftarrow L_i + \lambda L_j$.

Cela correspond à la multiplication à gauche par une matrice, dite *élémentaire*, notée $\mathrm{E}_{i,j}^{(n)}(\lambda)$ (ou, si le contexte le permet, $\mathrm{E}_{i,j}(\lambda)$). Cette matrice est obtenue à partir de I_n par la même manipulation élémentaire de lignes.
La multiplication à droite par la même matrice $\mathrm{E}_{i,j}(\lambda)$ correspond, elle, à la *manipulation élémentaire de colonnes* (pour une matrice qui possède n colonnes) qui transforme la matrice I_n en $\mathrm{E}_{i,j}(\lambda)$: $C_j \leftarrow C_j + \lambda C_i$.

4) Le sous-groupe de $\mathbb{SL}_n(\mathbf{A})$ engendré par les matrices élémentaires est appelé le *groupe élémentaire* et il est noté $\mathbb{E}_n(\mathbf{A})$. Deux matrices sont dites *élémentairement équivalentes* lorsque l'on peut passer de l'une à l'autre par des manipulations élémentaires de lignes et de colonnes. ∎

5.9. Lemme du mineur inversible. (Pivot généralisé)
Si une matrice $G \in \mathbf{A}^{q\times m}$ possède un mineur d'ordre $k \leqslant \min(m, q)$ inversible, elle est équivalente alors à une matrice

$$\begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix},$$

avec $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G)$ pour tout $r \in \mathbb{Z}$.

▷ En permutant éventuellement les lignes et les colonnes, on ramène le mineur inversible en haut à gauche. Puis, en multipliant à droite (ou à gauche) par une matrice inversible, on se ramène à la forme

$$G' \;=\; \begin{bmatrix} \mathrm{I}_k & A \\ B & C \end{bmatrix},$$

puis par des manipulations élémentaires de lignes et de colonnes, on obtient

$$G'' \;=\; \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix}.$$

Enfin, $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G'') = \mathcal{D}_{k+r}(G)$ pour tout $r \in \mathbb{Z}$. □

Comme conséquence immédiate, on obtient le lemme de la liberté.

5.10. Lemme de la liberté. *Considérons une matrice $G \in \mathbf{A}^{q\times m}$ de rang $\leqslant k$ avec $1 \leqslant k \leqslant \min(m,q)$. Si la matrice G possède un mineur d'ordre k inversible, alors elle est équivalente à la matrice*

$$\mathrm{I}_{k,q,m} \;=\; \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & 0_{q-k,m-k} \end{bmatrix}.$$

Dans ce cas, l'image, le noyau et le conoyau de G sont libres, respectivement de rangs k, $m-k$ et $q-k$. En outre, l'image et le noyau possèdent des supplémentaires libres.
Si $i_1,\dots,i_k$ (resp. $j_1,\dots,j_k$) sont les numéros de lignes (resp. de colonnes) du mineur inversible, alors les colonnes $j_1,\dots,j_k$ forment une base du module $\operatorname{Im} G$*, et* $\operatorname{Ker} G$ *est le sous-module défini par l'annulation des formes linéaires correspondant aux lignes $i_1,\dots,i_k$.*

▷ Avec les notations du lemme précédent on a $\mathcal{D}_1(G_1) = \mathcal{D}_{k+1}(G) = \langle 0\rangle$, donc $G_1 = 0$. Le reste est laissé à la lectrice. □

La matrice $\mathrm{I}_{k,q,m}$ est appelée une *matrice simple standard*. On note $\mathrm{I}_{k,n}$ pour $\mathrm{I}_{k,n,n}$ et on l'appelle une *matrice de projection standard*.

5.11. Définition. Une application linéaire entre modules libres de rangs finis est dite *simple* si elle peut être représentée par une matrice $\mathrm{I}_{k,q,m}$ sur des bases convenables. De même, une matrice est dite *simple* lorsqu'elle est équivalente à une matrice $\mathrm{I}_{k,q,m}$.

Formule de Cramer généralisée

Nous étudions dans ce paragraphe quelques généralisations des formules de Cramer usuelles. Nous les exploiterons dans les paragraphes suivants.

Pour une matrice $A \in \mathbf{A}^{m\times n}$ nous notons $A_{\alpha,\beta}$ la matrice extraite sur les lignes $\alpha = \{\alpha_1,\dots,\alpha_r\} \subseteq [\![1..m]\!]$ et les colonnes $\beta = \{\beta_1,\dots,\beta_s\} \subseteq [\![1..n]\!]$.

Supposons la matrice A de rang $\leqslant k$. Soit $V \in \mathbf{A}^{m\times 1}$ un vecteur colonne tel que la matrice bordée $[\,A \,|\, V\,]$ soit aussi de rang $\leqslant k$. Appelons A_j la j-ième colonne de A. Soit $\mu_{\alpha,\beta} = \det(A_{\alpha,\beta})$ le mineur d'ordre k de la matrice A extrait sur les lignes $\alpha = \{\alpha_1,\dots,\alpha_k\}$ et les colonnes $\beta = \{\beta_1,\dots,\beta_k\}$. Pour $j \in [\![1..k]\!]$ soit $\nu_{\alpha,\beta,j}$ le déterminant de la même matrice extraite, à ceci près que la colonne j a été remplacée par la colonne extraite de V sur les lignes α. Alors, on obtient pour chaque couple (α,β) de multi-indices une identité de Cramer :

$$\mu_{\alpha,\beta}\, V = \sum\nolimits_{j=1}^{k} \nu_{\alpha,\beta,j}\, A_{\beta_j} \tag{9}$$

due au fait que le rang de la matrice bordée $[\,A_{1..m,\beta} \,|\, V\,]$ est $\leqslant k$.

Cela peut se relire comme suit :

$$\begin{aligned}\mu_{\alpha,\beta}\, V &= \begin{bmatrix} A_{\beta_1} & \dots & A_{\beta_k} \end{bmatrix} \cdot \begin{bmatrix} \nu_{\alpha,\beta,1} \\ \vdots \\ \nu_{\alpha,\beta,k} \end{bmatrix} \\ &= \begin{bmatrix} A_{\beta_1} & \dots & A_{\beta_k} \end{bmatrix} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot \begin{bmatrix} v_{\alpha_1} \\ \vdots \\ v_{\alpha_k} \end{bmatrix} \\ &= A \cdot (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m} \cdot V \qquad (10)\end{aligned}$$

Cela nous conduit à introduire la notation suivante.

5.12. Notation. Nous notons $\mathcal{P}_\ell$ l'ensemble des parties de $[\![1..\ell]\!]$ et $\mathcal{P}_{k,\ell}$ l'ensemble des parties à k éléments de $[\![1..\ell]\!]$.
Pour $A \in \mathbf{A}^{m\times n}$ et $\alpha \in \mathcal{P}_{k,m}$, $\beta \in \mathcal{P}_{k,n}$, nous notons

$$\mathrm{Adj}_{\alpha,\beta}(A) = (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m}.$$

Par exemple, avec la matrice

$$A = \begin{bmatrix} 5 & -5 & 7 & 4 \\ 9 & -1 & 2 & 7 \\ 13 & 3 & -3 & 10 \end{bmatrix}$$

et les parties $\alpha = \{1, 2\}$ et $\beta = \{2, 3\}$, on obtient

$$A_{\alpha,\beta} = \begin{bmatrix} -5 & 7 \\ -1 & 2 \end{bmatrix},\ \mathrm{Adj}(A_{\alpha,\beta}) = \begin{bmatrix} 2 & -7 \\ 1 & -5 \end{bmatrix} \text{ et } \mathrm{Adj}_{\alpha,\beta}(A) = \begin{bmatrix} 0 & 0 & 0 \\ 2 & -7 & 0 \\ 1 & -5 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

L'égalité (10) s'écrit comme suit, sous l'hypothèse que $\mathcal{D}_{k+1}([\, A \,|\, V \,]) = 0$.

$$\mu_{\alpha,\beta}\, V \;=\; A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V\,. \qquad (11)$$

On obtient donc l'égalité ci-dessous, sous l'hypothèse que A est de rang $\leqslant k$.

$$\mu_{\alpha,\beta}\, A \;=\; A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A\,. \qquad (12)$$

Les identités de Cramer (11) et (12) fournissent des congruences qui ne sont soumises à aucune hypothèse : il suffit par exemple de lire (11) dans l'anneau quotient $\mathbf{A}/\mathcal{D}_{k+1}([\, A \,|\, V \,])$ pour obtenir la congruence (13).

5.13. Lemme. (Formule de Cramer généralisée)
Sans aucune hypothèse sur la matrice A ou le vecteur V, on a pour $\alpha \in \mathcal{P}_{k,m}$ et $\beta \in \mathcal{P}_{k,n}$ les congruences suivantes.

$$\mu_{\alpha,\beta}\, V \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V \qquad \mod \ \mathcal{D}_{k+1}([\, A \,|\, V \,]) \qquad (13)$$

$$\mu_{\alpha,\beta}\, A \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A \qquad \mod \ \mathcal{D}_{k+1}(A). \qquad (14)$$

Un cas particulier simple est le suivant avec $k = m \leqslant n$.

$$\mu_{1..m,\beta}\, \mathrm{I}_m \;=\; A \cdot \mathrm{Adj}_{1..m,\beta}(A), \qquad (\beta \in \mathcal{P}_{m,n}). \qquad (15)$$

Cette égalité est d'ailleurs une conséquence directe de l'identité de Cramer

de base (4). De la même manière, on obtient

$$\mu_{\alpha,1..n}\,\mathrm{I}_n \;=\; \mathrm{Adj}_{\alpha,1..n}(A)\cdot A, \qquad (\alpha\in\mathcal{P}_{n,m},\, n\leqslant m). \tag{16}$$

Une formule magique

Une conséquence immédiate de l'identité de Cramer (12) est l'identité (17) moins usuelle donnée dans le théorème suivant. De même les égalités (18) et (19) résultent facilement de (15) et (16).

5.14. Théorème. *Soit $A\in\mathbf{A}^{m\times n}$ une matrice de rang k. On a donc une égalité $\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\,\mu_{\alpha,\beta}=1$. Posons*

$$B \;=\; \textstyle\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\;\mathrm{Adj}_{\alpha,\beta}(A).$$

1. *On a*
$$A\cdot B\cdot A = A. \tag{17}$$
En conséquence, $A\,B$ est une projection de rang k et le sous-module $\mathrm{Im}\,A=\mathrm{Im}\,AB$ est facteur direct dans $\mathbf{A}^m$.

2. *Si $k=m$, alors*
$$A\cdot B=\mathrm{I}_m. \tag{18}$$

3. *Si $k=n$, alors*
$$B\cdot A=\mathrm{I}_n. \tag{19}$$

L'identité suivante, que nous n'utiliserons pas dans la suite, est encore plus miraculeuse.

5.15. Proposition. (Prasad et Robinson)
Avec les hypothèses et les notations du théorème 5.14, si l'on a

$$\forall\alpha,\alpha'\in\mathcal{P}_{k,m},\ \forall\beta,\beta'\in\mathcal{P}_{k,n},\quad c_{\alpha,\beta}\,c_{\alpha',\beta'}=c_{\alpha,\beta'}\,c_{\alpha',\beta}\,,$$

alors
$$B\cdot A\cdot B=B. \tag{20}$$

Inverses généralisés et applications localement simples

Soient E et F deux $\mathbf{A}$-modules, et une application linéaire $\varphi:E\to F$. On peut voir cette donnée comme une sorte de système linéaire généralisé (un système linéaire usuel correspond au cas de modules libres de rang fini). De manière informelle, un tel système linéaire est considéré comme «bien conditionné» s'il y a une façon systématique de trouver une solution à l'équation en x, $\varphi(x)=y$, à partir de la donnée y, lorsqu'une telle solution existe. Plus précisément, on se demande s'il existe une application linéaire $\psi:F\to E$ vérifiant $\varphi\big(\psi(y)\big)=y$ chaque fois qu'il existe une solution x. Cela revient à demander $\varphi\Big(\psi\big(\varphi(x)\big)\Big)=\varphi(x)$ pour tout $x\in E$.

Cela éclaire l'importance de l'équation (17) et conduit à la notion d'inverse généralisé.

La terminologie concernant les inverses généralisés ne semble pas entièrement fixée. Nous adoptons celle de [Lancaster & Tismenetsky].
Dans le livre [Bhaskara Rao], l'auteur utilise le terme « reflexive g-inverse ».

5.16. Définition. Soient E et F deux $\mathbf{A}$-modules, et une application linéaire $\varphi : E \to F$. Une application linéaire $\psi : F \to E$ est appelée un *inverse généralisé* de φ si l'on a

$$\varphi \circ \psi \circ \varphi = \varphi \quad \text{et} \quad \psi \circ \varphi \circ \psi = \psi. \tag{21}$$

Une application linéaire est dite *localement simple* lorsqu'elle possède un inverse généralisé. Une matrice est dite *localement simple* lorsque l'application linéaire qu'elle définit est localement simple.

Le fait suivant est immédiat.

5.17. Fait. *Lorsque ψ est un inverse généralisé de φ, on a :*

- *$\varphi\,\psi$ et $\psi\,\varphi$ sont des projections,*
- *$\operatorname{Im}\varphi = \operatorname{Im}\varphi\,\psi$, $\operatorname{Im}\psi = \operatorname{Im}\psi\,\varphi$, $\operatorname{Ker}\varphi = \operatorname{Ker}\psi\,\varphi$, $\operatorname{Ker}\psi = \operatorname{Ker}\varphi\,\psi$,*
- *$E = \operatorname{Ker}\varphi \oplus \operatorname{Im}\psi$ et $F = \operatorname{Ker}\psi \oplus \operatorname{Im}\varphi$,*
- *$\operatorname{Ker}\varphi \simeq \operatorname{Coker}\psi$ et $\operatorname{Ker}\psi \simeq \operatorname{Coker}\varphi$.*

En outre, φ et ψ donnent par restriction des isomorphismes réciproques φ_1 et ψ_1 entre $\operatorname{Im}\psi$ et $\operatorname{Im}\varphi$. Matriciellement, on obtient :

$$\begin{array}{c} \\ \operatorname{Im}\varphi \\ \operatorname{Ker}\psi \end{array} \begin{array}{c} \begin{array}{cc} \operatorname{Im}\psi & \operatorname{Ker}\varphi \end{array} \\ \begin{bmatrix} \varphi_1 & 0 \\ 0 & 0 \end{bmatrix} \end{array} = \varphi, \qquad \begin{array}{c} \\ \operatorname{Im}\psi \\ \operatorname{Ker}\varphi \end{array} \begin{array}{c} \begin{array}{cc} \operatorname{Im}\varphi & \operatorname{Ker}\psi \end{array} \\ \begin{bmatrix} \psi_1 & 0 \\ 0 & 0 \end{bmatrix} \end{array} = \psi.$$

Remarques

1) Si l'on a une application linéaire ψ_0 vérifiant comme dans le théorème 5.14 l'égalité $\varphi\,\psi_0\,\varphi = \varphi$, on obtient un inverse généralisé de φ en posant $\psi = \psi_0\,\varphi\,\psi_0$. Autrement dit, une application linéaire φ est localement simple si, et seulement si, il existe ψ vérifiant $\varphi\,\psi\,\varphi = \varphi$.

2) Une application linéaire simple entre modules libres de rangs finis est localement simple (vérification immédiate).

3) Le théorème 5.14 nous dit qu'une application linéaire qui possède un rang k au sens de la définition 5.7 est localement simple. ∎

5.18. Fait. *Soit une application linéaire $\varphi : \mathbf{A}^n \to \mathbf{A}^m$. Les propriétés suivantes sont équivalentes.*

1. *L'application linéaire φ est localement simple.*
2. *Il existe $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$ telle que*
$$\mathbf{A}^n = \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi^\bullet \quad \text{et} \quad \mathbf{A}^m = \operatorname{Ker}\varphi^\bullet \oplus \operatorname{Im}\varphi.$$
3. *Le sous-module $\operatorname{Im}\varphi$ est facteur direct dans $\mathbf{A}^m$.*

D *1 ⇒ 2.* Si ψ est un inverse généralisé de φ, on peut prendre $\varphi^\bullet = \psi$.
2 ⇒ 3. Évident.
3 ⇒ 1. Si $\mathbf{A}^m = P \oplus \operatorname{Im}\varphi$, notons $\pi : \mathbf{A}^m \to \mathbf{A}^m$ la projection sur $\operatorname{Im}\varphi$ parallèlement à P. Pour chaque vecteur e_i de la base canonique de $\mathbf{A}^m$, il existe un élément a_i de $\mathbf{A}^n$ tel que $\varphi(a_i) = \pi(e_i)$. On définit $\psi : \mathbf{A}^m \to \mathbf{A}^n$ par $\psi(e_i) = a_i$. Alors, $\varphi \circ \psi = \pi$ et $\varphi \circ \psi \circ \varphi = \pi \circ \varphi = \varphi$. Et $\psi \circ \varphi \circ \psi$ est un inverse généralisé de φ. □

La notion d'application linéaire localement simple est une notion locale au sens suivant.

5.19. Principe local-global concret. (Applications linéaires localement simples) *Soient S_1, …, S_n des monoïdes comaximaux d'un anneau $\mathbf{A}$. Soit une application linéaire $\varphi : \mathbf{A}^m \to \mathbf{A}^q$. Si les $\varphi_{S_i} : \mathbf{A}^m_{S_i} \to \mathbf{A}^q_{S_i}$ sont simples, alors φ est localement simple. Plus généralement, φ est localement simple si, et seulement si, les φ_{S_i} sont localement simples.*

D Voyons la deuxième affirmation. Montrer que φ est localement simple revient à trouver ψ vérifiant $\varphi\,\psi\,\varphi = \varphi$. Cela est un système linéaire en les coefficients de la matrice de ψ et l'on peut donc appliquer le principe local-global concret de base (principe 2.3). □

La terminologie d'application linéaire localement simple est justifiée par le principe local-global précédent et par la réciproque donnée au point *8* du théorème 5.26 (voir aussi le lemme de l'application localement simple dans le cas des anneaux locaux, page 539).

Grassmanniennes

Le théorème suivant sert d'introduction aux variétés grassmanniennes. Il résulte du fait 5.18 et du théorème 5.14.

5.20. Théorème. (Sous-modules de type fini en facteur direct dans un module libre) *Soit $M = \langle C_1, \ldots, C_m\rangle$ un sous-module de type fini de $\mathbf{A}^n$ et $C = [\,C_1\ \cdots\ C_m\,] \in \mathbf{A}^{n\times m}$ la matrice correspondante.*

1. *Les propriétés suivantes sont équivalentes.*
   a. *La matrice C est localement simple.*
   b. *Le module M est en facteur direct dans $\mathbf{A}^n$.*
   c. *Le module M est l'image d'une matrice $F \in \mathbb{GA}_n(\mathbf{A})$.*
2. *Les propriétés suivantes sont équivalentes.*
   a. *La matrice C est de rang k.*
   b. *Le module M est l'image d'une matrice $F \in \mathbb{GA}_n(\mathbf{A})$ de rang k.*

La « variété » des droites vectorielles dans un $\mathbf{K}$-espace vectoriel de dimension $n+1$ est, intuitivement, de dimension n, car une droite dépend pour l'essentiel de n paramètres (un vecteur non nul, à une constante multiplicative près, cela fait $(n+1)-1$ paramètres indépendants). On appelle cette variété l'espace projectif de dimension n sur $\mathbf{K}$.
Par ailleurs, en passant d'un corps $\mathbf{K}$ à un anneau arbitraire $\mathbf{A}$, la bonne généralisation d'une « droite vectorielle dans $\mathbf{K}^{n+1}$ » est « l'image d'une matrice de projection de rang 1 dans $\mathbf{A}^{n+1}$ ». Cela conduit aux définitions suivantes.

5.21. Définition

1. On définit l'espace $\mathbb{GA}_{n,k}(\mathbf{A}) \subseteq \mathbb{GA}_n(\mathbf{A})$ comme l'ensemble des matrices de projection de rang k et $\mathbb{G}_{n,k}(\mathbf{A})$ comme l'ensemble des sous-modules de $\mathbf{A}^n$ qui sont images de matrices de $\mathbb{GA}_{n,k}(\mathbf{A})$ [9].
2. L'espace $\mathbb{G}_{n+1,1}(\mathbf{A})$ est encore noté $\mathbb{P}^n(\mathbf{A})$, et on l'appelle l'*espace projectif de dimension n sur $\mathbf{A}$*.
3. On note $\mathbb{G}_n(\mathbf{A})$ l'espace de tous les sous-modules en facteur direct dans $\mathbf{A}^n$ (c'est-à-dire images d'une matrice de projection).

Naturellement, la définition ci-dessus est peu satisfaisante, dans la mesure où on n'explique pas comment est structuré l'ensemble $\mathbb{G}_{n,k}(\mathbf{A})$. Seule cette structure lui fait mériter son nom d'« espace ».
Une réponse partielle est donnée par la constatation que $\mathbb{G}_{n,k}$ est un foncteur. Plus précisément, à tout homomorphisme $\varphi : \mathbf{A} \to \mathbf{B}$ on associe une application naturelle $\mathbb{G}_{n,k}(\varphi) : \mathbb{G}_{n,k}(\mathbf{A}) \to \mathbb{G}_{n,k}(\mathbf{B})$, avec notamment

$$\mathbb{G}_{n,k}(\mathrm{Id}_{\mathbf{A}}) = \mathrm{Id}_{\mathbb{G}_{n,k}(\mathbf{A})} \quad \text{et} \quad \mathbb{G}_{n,k}(\psi \circ \varphi) = \mathbb{G}_{n,k}(\psi) \circ \mathbb{G}_{n,k}(\varphi),$$

lorsque $\psi \circ \varphi$ est défini.

Critères d'injectivité et de surjectivité

Deux propositions célèbres sont contenues dans le théorème suivant.

5.22. Théorème. *Soit $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ une application linéaire de matrice A.*

1. *L'application φ est surjective si, et seulement si, φ est de rang m, c'est-à-dire ici $\mathcal{D}_m(\varphi) = \langle 1 \rangle$ (on dit alors que A est* unimodulaire*).*
2. (Théorème de McCoy) *L'application φ est injective si, et seulement si, l'idéal $\mathcal{D}_n(\varphi)$ est fidèle, c'est-à-dire si* $\mathrm{Ann}_{\mathbf{A}}\big(\mathcal{D}_n(\varphi)\big) = 0$.

9. L'ensemble $\mathbb{G}_{n,k}(\mathbf{A})$ est appelé une *grassmannienne*, ou une *grassmanienne projective*. Nous appelons $\mathbb{GA}_{n,k}(\mathbf{A})$ une *grassmannienne affine*. Nous avons malencontreusement opté pour une notation peu usuelle en choisisssnt de mettre n, k au lieu de k, n.

1. Si φ est surjective, elle admet une inverse à droite ψ, et le fait 5.6 donne $\langle 1\rangle = \mathcal{D}_m(\mathrm{I}_m) \subseteq \mathcal{D}_m(\varphi)\mathcal{D}_m(\psi)$, donc $\mathcal{D}_m(\varphi) = \langle 1\rangle$. Réciproquement, si A est de rang m, l'équation (18) montre que A admet une inverse à droite, et φ est surjective.

2. Supposons que $\mathcal{D}_n(A)$ est fidèle. D'après l'égalité (16), si $AV = 0$, alors $\mu_{\alpha,1..n}V = 0$ pour tous les générateurs $\mu_{\alpha,1..n}$ de $\mathcal{D}_n(A)$, et donc $V = 0$.
Pour la réciproque [10], nous montrons par récurrence sur k la propriété suivante : *si k vecteurs colonnes $x_1, \dots, x_k$ sont linéairement indépendants, alors l'annulateur du vecteur $x_1 \wedge \cdots \wedge x_k$ est réduit à* 0. Pour $k = 1$, c'est trivial. Pour passer de k à $k+1$, nous raisonnons comme suit. Soit z un scalaire annulant $x_1 \wedge \cdots \wedge x_{k+1}$. Pour $\alpha \in \mathcal{P}_{k,m}$, nous notons $d_\alpha(y_1, \dots, y_k)$ le mineur extrait sur les lignes indices de α pour les vecteurs colonnes $y_1, \dots, y_k$ de $\mathbf{A}^m$.
Puisque $z(x_1 \wedge \cdots \wedge x_{k+1}) = 0$, et vu les formules de Cramer, on a l'égalité

$$z\left(d_\alpha(x_1, \dots, x_k)x_{k+1} - d_\alpha(x_1, \dots, x_{k-1}, x_{k+1})x_k + \dots\right) = 0,$$

donc $z\, d_\alpha(x_1, \dots, x_k) = 0$.
Comme ceci est vrai pour tout α, cela donne $z(x_1 \wedge \cdots \wedge x_k) = 0$. Et, par l'hypothèse de récurrence, $z = 0$. □

Remarque. Le théorème 5.22 peut se relire sous la forme suivante.

1. L'application linéaire $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ est surjective si, et seulement si, l'application $\bigwedge^m \varphi : \mathbf{A}^{\binom{n}{m}} \to \mathbf{A}$ est surjective.
2. L'application linéaire $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ est injective si, et seulement si, l'application $\bigwedge^n \varphi : \mathbf{A} \to \mathbf{A}^{\binom{m}{n}}$ est injective. ∎

5.23. Corollaire. *Soit une application $\mathbf{A}$-linéaire $\varphi : \mathbf{A}^n \to \mathbf{A}^m$.*

1. *Si φ est surjective et $n < m$, l'anneau est alors trivial.*
2. *Si φ est injective et $n > m$, l'anneau est alors trivial.*

Remarque. Une formulation plus positive, équivalente, mais sans doute encore plus déroutante, pour les résultats du corollaire précédent est la suivante.

1. Si φ est surjective, alors X^m divise X^n dans $\mathbf{A}[X]$.
2. Si φ est injective, alors X^n divise X^m dans $\mathbf{A}[X]$.

D'une certaine manière, cela se rapproche plus de la formulation en mathématiques classiques : si l'anneau est non trivial, alors $m \leqslant n$ dans le premier cas (resp. $n \leqslant m$ dans le deuxième cas).
L'avantage de nos formulations est qu'elles fonctionnent dans tous les cas, sans avoir besoin de présupposer que l'on sache décider si l'anneau est trivial ou pas. ∎

10. Voir aussi la démonstration alternative donnée en XV-8.7.

5.24. Corollaire. *Si $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ est injective, il en va alors de même pour toute puissance extérieure de φ.*

$\mathbb{D}$ L'annulateur de $\mathcal{D}_n(\varphi)$ est réduit à 0 d'après le théorème précédent. Il existe un anneau $\mathbf{B} \supseteq \mathbf{A}$ tel que les générateurs de $\mathcal{D}_n(\varphi)$ deviennent comaximaux dans $\mathbf{B}$ (lemme 2.14). L'application $\mathbf{B}$-linéaire $\varphi_1 : \mathbf{B}^n \to \mathbf{B}^m$ obtenue en étendant φ à $\mathbf{B}$, est donc de rang n et admet un inverse à gauche ψ (point *3* du théorème 5.14), c'est-à-dire $\psi \circ \varphi_1 = \mathrm{Id}_{\mathbf{B}^n}$. Par suite,

$$\textstyle\bigwedge^k \psi \circ \bigwedge^k \varphi_1 = \mathrm{Id}_{\bigwedge^k \mathbf{B}^n}.$$

Ainsi, la matrice de $\bigwedge^k \varphi_1$, est injective. Et, puisque c'est la même matrice que celle de $\bigwedge^k \varphi$, l'application linéaire $\bigwedge^k \varphi$ est injective. □

Caractérisation des applications localement simples

Le lemme suivant met en correspondance bijective les systèmes fondamentaux d'idempotents orthogonaux et les suites finies d'idempotents croissantes pour la divisibilité.

5.25. Lemme. *Soit une liste d'idempotents $(e_{q+1} = 0, e_q, \ldots, e_1, e_0 = 1)$ telle que e_i divise e_{i+1} pour $i = 0, \ldots, q$. Alors, les éléments $r_i := e_i - e_{i+1}$ pour $i \in [\![0..q]\!]$, forment un système fondamental d'idempotents orthogonaux. Réciproquement, tout système fondamental d'idempotents orthogonaux $(r_0, \ldots, r_q)$ définit une telle liste d'idempotents en posant*

$$e_j = \textstyle\sum_{k \geqslant j} r_k, \quad \text{pour } j \in [\![0..q+1]\!].$$

$\mathbb{D}$ Il est clair que $\sum_i r_i = 1$. Pour $0 \leqslant i < q$, on a $e_{i+1} = e_i e_{i+1}$.
D'où, $(e_i - e_{i+1})e_{i+1} = 0$, c'est-à-dire $(r_q + \cdots + r_{i+1}) \cdot r_i = 0$. On en déduit facilement que $r_i r_j = 0$ pour $j > i$. □

On note $\mathrm{Diag}(a_1, \ldots, a_n)$ la matrice diagonale d'ordre n dont le coefficient en position (i, i) est l'élément a_i.

Dans le théorème qui suit, certains des idempotents r_i dans le système fondamental d'idempotents orthogonaux peuvent très bien être nuls. Par exemple si l'anneau est connexe et non trivial ils sont tous nuls sauf un.

5.26. Théorème. (Matrice localement simple) *Soit $G \in \mathbf{A}^{m \times n}$ la matrice d'une application linéaire $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ et $q = \inf(m, n)$. Les propriétés suivantes sont équivalentes.*

1. *L'application linéaire φ est localement simple.*
2. *Le sous-module $\mathrm{Im}\,\varphi$ est facteur direct dans $\mathbf{A}^m$.*
3. *$\mathrm{Im}\,\varphi$ est facteur direct dans $\mathbf{A}^m$ et $\mathrm{Ker}\,\varphi$ est facteur direct dans $\mathbf{A}^n$.*
4. *Il existe une application linéaire $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$, avec $\mathbf{A}^n = \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\varphi^\bullet$ et $\mathbf{A}^m = \mathrm{Ker}\,\varphi^\bullet \oplus \mathrm{Im}\,\varphi$.*

5. *Chaque idéal déterminantiel $\mathcal{D}_k(\varphi)$ est idempotent.*
6. *Il existe un (unique) système fondamental d'idempotents orthogonaux $(r_0, r_1, \ldots, r_q)$ tel que sur chaque localisé $\mathbf{A}[1/r_k]$ l'application φ est de rang k.*
7. *Chaque idéal déterminantiel $\mathcal{D}_k(\varphi)$ est engendré par un idempotent e_k. Soit alors $r_k = e_k - e_{k+1}$. Les r_k forment un système fondamental d'idempotents orthogonaux. Pour tout mineur μ d'ordre k de la matrice G, l'application linéaire φ devient simple de rang k sur le localisé $\mathbf{A}[1/(r_k\,\mu)]$.*
8. *L'application linéaire φ devient simple après localisation en des éléments comaximaux convenables.*
9. *Chaque idéal déterminantiel $\mathcal{D}_k(\varphi)$ est engendré par un idempotent e_k et la matrice de φ devient équivalente à la matrice diagonale $\mathrm{Diag}(e_1, e_2, \ldots, e_q)$, éventuellement complétée par des lignes ou colonnes nulles, après localisation en des éléments comaximaux convenables.*
10.* *L'application linéaire φ devient simple après localisation en n'importe quel idéal maximal.*

D L'équivalence des points *1*, *2*, *3*, *4* est déjà claire (voir les faits 5.17 et 5.18). Par ailleurs, on a trivialement $7 \Rightarrow 6 \Rightarrow 5$ et $9 \Rightarrow 5$.

Puisque $q = \inf(m, n)$, on a $\mathcal{D}_{q+1}(\varphi) = 0$.

1 $\Rightarrow$ *5.* On a $GHG = G$ pour une certaine matrice H, et l'on applique le fait 5.6.

5 $\Rightarrow$ *7.* Le fait que chaque $\mathcal{D}_k(\varphi)$ est engendré par un idempotent e_k résulte du fait 4.6. Le fait que $(r_0, \ldots, r_q)$ est un système fondamental d'idempotents orthogonaux résulte du lemme 5.25 (et du fait 5.4).
Comme $r_k e_{k+1} = 0$, sur l'anneau $\mathbf{A}[1/r_k]$, et donc sur l'anneau $\mathbf{A}[1/(\mu r_k)]$, où μ est un mineur d'ordre k, tous les mineurs d'ordre $k+1$ de la matrice G sont nuls. Donc, par le lemme de la liberté, G est simple de rang k.

7 $\Rightarrow$ *9.* Sur $\mathbf{A}[1/r_k]$ et donc sur $\mathbf{A}[1/(\mu r_k)]$ (μ un mineur d'ordre k), on a $\mathrm{Diag}(e_1, \ldots, e_q) = \mathrm{Diag}(1, \ldots, 1, 0, \ldots, 0)$ avec k fois 1.

7 $\Rightarrow$ *8.* Notons $t_{k,j}$ les mineurs d'ordre k de G. Les localisations sont celles en les $t_{k,j} r_k$. Nous devons vérifier qu'elles sont comaximales. Chaque e_k s'écrit sous forme $\sum t_{k,j} v_{k,j}$, donc $\sum_{k,j} v_{k,j}(t_{k,j} r_k) = \sum_k e_k r_k = \sum r_k = 1$.

8 $\Rightarrow$ *1.* Par application du principe local-global 5.19 puisque toute application simple est localement simple.

8 $\Rightarrow$ *10.* (En mathématiques classiques) Parce que le complémentaire d'un idéal maximal contient toujours au moins un élément dans un système d'éléments comaximaux (on peut supposer l'anneau non trivial).

10 $\Rightarrow$ *8.* (En mathématiques classiques) Pour chaque idéal maximal $\mathfrak{m}$ on obtient un $s_{\mathfrak{m}} \notin \mathfrak{m}$ et une matrice $H_{\mathfrak{m}}$ tels que l'on ait $GH_{\mathfrak{m}}G = G$ dans $\mathbf{A}[1/s_{\mathfrak{m}}]$. L'idéal engendré par les $s_{\mathfrak{m}}$ n'est contenu dans aucun idéal maximal donc c'est l'idéal $\langle 1\rangle$. Il y a donc un nombre fini de ces $s_{\mathfrak{m}}$ qui sont comaximaux.

Terminons en donnant une preuve directe pour l'implication *6* $\Rightarrow$ *1.*
Sur l'anneau $\mathbf{A}[1/r_k]$, la matrice G est de rang k donc il existe une matrice B_k vérifiant $GB_kG = G$ (théorème 5.14). Cela signifie sur l'anneau $\mathbf{A}$ que l'on a une matrice H_k dans $\mathbf{A}^{n\times m}$ vérifiant $r_kH_k = H_k$ et $r_kG = GH_kG$. On prend alors $H = \sum_k H_k$ et l'on obtient $G = GHG$. □

L'équivalence des points *1* à *9* a été établie de manière constructive, tandis que le point *10* implique les précédents uniquement en mathématiques classiques.

Trace, norme, discriminant, transitivité

Nous notons $\mathrm{Tr}(\varphi)$ et $\mathrm{C}_\varphi(X)$ la trace et le *polynôme caractéristique* d'un endomorphisme φ d'un module libre de rang fini (nous prenons pour *polynôme caractéristique d'une matrice* $F \in \mathbb{M}_n(\mathbf{A})$ le polynôme $\det(X\mathrm{I}_n - F)$, qui a l'avantage d'être unitaire).

5.27. Notation

- Si $\mathbf{A} \subseteq \mathbf{B}$ et si $\mathbf{B}$ est un $\mathbf{A}$-module libre de rang fini, on note $[\,\mathbf{B} : \mathbf{A}\,]$ pour $\mathrm{rg}_{\mathbf{A}}(\mathbf{B})$.
- Pour $a \in \mathbf{B}$, on note alors $\mathrm{Tr}_{\mathbf{B/A}}(a)$, $\mathrm{N}_{\mathbf{B/A}}(a)$ et $\mathrm{C}_{\mathbf{B/A}}(a)(X)$ la trace, le déterminant et le polynôme caractéristique de la multiplication par a, vue comme endomorphisme du $\mathbf{A}$-module $\mathbf{B}$.
  On les appelle la *trace*, la *norme* et le *polynôme caractéristique de* a *sur* $\mathbf{A}$.

5.28. Lemme. *Supposons que* $\mathbf{A} \subseteq \mathbf{B}$ *et que* $\mathbf{B}$ *est un* $\mathbf{A}$*-module libre de rang fini* m*.*

1. *Soit* E *un* $\mathbf{B}$*-module libre de rang fini* n*. Si* $\underline{e} = (e_i)_{i\in[\![1..m]\!]}$ *est une base de* $\mathbf{B}$ *sur* $\mathbf{A}$ *et* $\underline{f} = (f_j)_{j\in[\![1..n]\!]}$ *une base de* E *sur* $\mathbf{B}$*, alors* $(e_if_j)_{i,j}$ *est une base de* E *sur* $\mathbf{A}$*. En conséquence,* E *est libre sur* $\mathbf{A}$ *et*
$$\mathrm{rg}_{\mathbf{A}}(E) = \mathrm{rg}_{\mathbf{B}}(E)\times \mathrm{rg}_{\mathbf{A}}(\mathbf{B}).$$
2. *Si* $\mathbf{B} \subseteq \mathbf{C}$ *et si* $\mathbf{C}$ *est un* $\mathbf{B}$*-module libre de rang fini, on a*
$$[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,]\times[\,\mathbf{B} : \mathbf{A}\,].$$

Remarque. Soit $\mathbf{C} = \mathbf{A}[Y]/\langle Y^3\rangle = \mathbf{A}[y]$, c'est une $\mathbf{A}$-algèbre libre de rang 3. Puisque $y^4 = 0$, $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}y^2$ est une sous-algèbre de $\mathbf{C}$ libre sur $\mathbf{A}$ dont le rang (égal à 2) ne divise pas le rang de $\mathbf{C}$ (égal à 3).

L'égalité $[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,]\times[\,\mathbf{B} : \mathbf{A}\,]$ ne s'applique pas car $\mathbf{C}$ n'est pas libre sur $\mathbf{B}$. ∎

5.29. Théorème. (Formules de transitivité pour la trace, le déterminant et le polynôme caractéristique) *Sous les mêmes hypothèses, soit $u_{\mathbf{B}} : E \to E$ une application $\mathbf{B}$-linéaire. On note $u_{\mathbf{A}}$ cette application considérée comme une application $\mathbf{A}$-linéaire. On a alors les égalités :*

$$\begin{aligned} \det(u_{\mathbf{A}}) &= \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big),\\ \mathrm{Tr}(u_{\mathbf{A}}) &= \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{Tr}(u_{\mathbf{B}})\big),\\ \mathrm{C}_{u_{\mathbf{A}}}(X) &= \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{u_{\mathbf{B}}}(X)\big). \end{aligned}$$

▷ On prend les notations du lemme 5.28. Soient u_{kj} les éléments de $\mathbf{B}$ définis par $u(f_j) = \sum_{k=1}^{n} u_{kj} f_k$.

Alors, la matrice M de $u_{\mathbf{A}}$ sur la base $(e_i f_j)_{i,j}$ s'écrit comme une matrice par blocs

$$M = \begin{bmatrix} M_{11} & \cdots & M_{1n} \\ \vdots & & \vdots \\ M_{n1} & \cdots & M_{nn} \end{bmatrix},$$

où M_{kj} représente l'application $\mathbf{A}$-linéaire $b \mapsto bu_{kj}$ de $\mathbf{B}$ dans $\mathbf{B}$ sur la base $\underline{e}$. Cela fournit la relation sur la trace puisque :

$$\begin{aligned} \mathrm{Tr}(u_{\mathbf{A}}) &= \sum\nolimits_{i=1}^{n} \mathrm{Tr}(M_{ii}) = \sum\nolimits_{i=1}^{n} \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(u_{ii})\\ &= \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\sum\nolimits_{i=1}^{n} u_{ii}\big) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{Tr}(u_{\mathbf{B}})\big). \end{aligned}$$

Quant à l'égalité pour le déterminant, remarquons que les matrices M_{ij} commutent deux à deux (M_{ij} est la matrice de la multiplication par u_{ij}). On peut donc appliquer le lemme 5.30 qui suit, ce qui nous donne :

$$\det(M) = \det(\Delta), \qquad \text{avec} \quad \Delta = \textstyle\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) M_{1\sigma_1} M_{2\sigma_2} \cdots M_{n\sigma_n}.$$

Or, Δ n'est autre que la matrice de la multiplication par l'élément

$$\textstyle\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) u_{1\sigma_1} u_{2\sigma_2} \cdots u_{n\sigma_n},$$

i.e., par $\det(u_{\mathbf{B}})$, donc :

$$\det(u_{\mathbf{A}}) = \det(M) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big).$$

Enfin, l'égalité sur le polynôme caractéristique se déduit de celle sur les déterminants en utilisant le fait que $\mathrm{C}_{u_{\mathbf{A}}}(X)$ est le déterminant de l'endomorphisme $X\mathrm{Id}_{E[X]} - u_{\mathbf{A}}$ du $\mathbf{A}[X]$-module $E[X]$ tandis que $\mathrm{C}_{u_{\mathbf{B}}}(X)$ est celui de la même application vue comme endomorphisme du $\mathbf{B}[X]$-module $E[X]$.□

Dans un anneau non commutatif, deux éléments a et b sont dits *permutables* si $ab = ba$.

5.30. Lemme. *Soit $(N_{ij})_{i,j}$ une famille de n^2 matrices carrées $\in \mathbb{M}_m(\mathbf{A})$, deux à deux permutables, et N la matrice carrée d'ordre mn :*

$$N = \begin{bmatrix} N_{11} & \cdots & N_{1n} \\ \vdots & & \vdots \\ N_{n1} & \cdots & N_{nn} \end{bmatrix}.$$

Alors : $\det(N) = \det\big(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\, N_{1\sigma_1} N_{2\sigma_2} \cdots N_{n\sigma_n}\big)$.

𝔇 Notons Δ la matrice $n\times n$ définie par $\Delta = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) N_{1\sigma_1} N_{2\sigma_2} \cdots N_{n\sigma_n}$. Il faut donc démontrer que $\det(N) = \det(\Delta)$.

Traitons les cas particuliers $n = 2$ puis $n = 3$. On remplace $\mathbf{A}$ par $\mathbf{A}[Y]$ et N_{ii} par $N_{ii} + Y\mathrm{I}_m$, ce qui a l'avantage de rendre certains déterminants réguliers dans $\mathbf{A}[Y]$. Il suffit d'établir les égalités avec ces nouvelles matrices, car on termine en faisant $Y = 0$.

Le point-clef de la démonstration pour $n = 2$ réside dans l'égalité suivante :

$$\begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix} \begin{bmatrix} N_{22} & 0 \\ -N_{21} & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} N_{11}N_{22} - N_{12}N_{21} & N_{12} \\ 0 & N_{22} \end{bmatrix}.$$

On considère ensuite le déterminant des deux membres :

$$\det(N)\det(N_{22}) = \det(N_{11}N_{22} - N_{12}N_{21})\det(N_{22}),$$

puis on simplifie par $\det(N_{22})$ (qui est régulier) pour obtenir le résultat.

Le cas $n = 3$ passe par l'égalité :

$$\begin{bmatrix} N_{11} & N_{12} & N_{13} \\ N_{21} & N_{22} & N_{23} \\ N_{31} & N_{32} & N_{33} \end{bmatrix} \begin{bmatrix} N_{22}N_{33} - N_{23}N_{32} & 0 & 0 \\ N_{31}N_{23} - N_{21}N_{33} & \mathrm{I}_m & 0 \\ N_{21}N_{32} - N_{22}N_{31} & 0 & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \Delta & N_{12} & N_{13} \\ 0 & N_{22} & N_{23} \\ 0 & N_{32} & N_{33} \end{bmatrix},$$

qui conduit à

$$\det(N)\det(N_{22}N_{33} - N_{23}N_{32}) = \det(\Delta)\det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}.$$

Le cas $n = 2$ fournit $\det(N_{22}N_{33} - N_{23}N_{32}) = \det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}$. On simplifie par ce déterminant et l'on obtient $\det(N) = \det(\Delta)$.

Le cas général est laissé au lecteur (voir l'exercice 28). □

5.31. Corollaire. *Soient $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$ trois anneaux avec $\mathbf{C}$ libre de rang fini sur $\mathbf{B}$ et $\mathbf{B}$ libre de rang fini sur $\mathbf{A}$. On a les égalités suivantes :*

$$\mathrm{N}_{\mathbf{C}/\mathbf{A}} = \mathrm{N}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{N}_{\mathbf{C}/\mathbf{B}}, \quad \mathrm{Tr}_{\mathbf{C}/\mathbf{A}} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{Tr}_{\mathbf{C}/\mathbf{B}},$$

$$\mathrm{C}_{\mathbf{C}/\mathbf{A}}(c)(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{\mathbf{C}/\mathbf{B}}(c)(X)\big), \quad \textit{pour } c \in \mathbf{C}.$$

Déterminants de Gram et discriminants

5.32. Définition. Soit M un $\mathbf{A}$-module, $\varphi : M \times M \to \mathbf{A}$ une forme bilinéaire symétrique et $\underline{x} = x_1, \dots, x_k$ une liste d'éléments de M. On appelle *matrice de Gram de* $(x_1, \dots, x_k)$ *pour* φ la matrice

$$\mathrm{Gram}_{\mathbf{A}}(\varphi, \underline{x}) \overset{\text{déf}}{=} \big(\varphi(x_i, x_j)\big)_{i,j \in [\![1..k]\!]}.$$

Son déterminant est appelé le *déterminant de Gram de* $(x_1, \dots, x_k)$ *pour* φ, il est noté $\mathrm{gram}_{\mathbf{A}}(\varphi, \underline{x})$.

Si $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$, on a une égalité

$$\mathrm{gram}(\varphi, y_1, \dots, y_k) = \det(A)^2 \,\mathrm{gram}(\varphi, x_1, \dots, x_k),$$

où A est une matrice $k \times k$ qui exprime les y_j en fonction des x_i.

Nous introduisons maintenant un cas important de déterminant de Gram, le discriminant. Rappelons que deux éléments a, b d'un anneau $\mathbf{A}$ sont dits *associés* s'il existe $u \in \mathbf{A}^\times$ tels que $a = ub$.

5.33. Proposition et définition. *Soit* $\mathbf{C} \supseteq \mathbf{A}$ *une* $\mathbf{A}$*-algèbre qui est un* $\mathbf{A}$*-module libre de rang fini et soient* $x_1, \dots, x_k, y_1, \dots, y_k \in \mathbf{C}$.

1. *On appelle discriminant de* $(x_1, \dots, x_k)$ *le déterminant de la matrice*
$$\big(\mathrm{Tr}_{\mathbf{C}/\mathbf{A}}(x_i x_j)\big)_{i,j \in [\![1..k]\!]}.$$
On le note $\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(x_1, \dots, x_k)$ *ou* $\mathrm{disc}(x_1, \dots, x_k)$.
2. *Si* $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$, *on a*
$$\mathrm{disc}(y_1, \dots, y_k) = \det(A)^2 \,\mathrm{disc}(x_1, \dots, x_k),$$
où A *est une matrice* $k \times k$ *qui exprime les* y_j *en fonction des* x_i.
3. *En particulier, si* $(x_1, \dots, x_n)$ *et* $(y_1, \dots, y_n)$ *sont deux bases de* $\mathbf{C}$ *comme* $\mathbf{A}$*-module, les éléments* $\mathrm{disc}(x_1, \dots, x_n)$ *et* $\mathrm{disc}(y_1, \dots, y_n)$ *sont congrus multiplicativement modulo les carrés de* $\mathbf{A}^\times$. *On appelle discriminant de l'extension* $\mathbf{C}/\mathbf{A}$ *la classe d'équivalence correspondante. On le note* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$.
4. *Si* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *est régulier et* $n = [\,\mathbf{C} : \mathbf{A}\,]$, *un système* $u_1, \dots, u_n$ *dans* $\mathbf{C}$ *est une* $\mathbf{A}$*-base de* $\mathbf{C}$ *si, et seulement si,* $\mathrm{disc}(u_1, \dots, u_n)$ *et* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *sont associés.*

Par exemple, dans le cas où $\mathbf{A} = \mathbb{Z}$, le discriminant de l'extension est un entier bien défini, tandis que si $\mathbf{A} = \mathbb{Q}$, le discriminant est caractérisé d'une part par son signe, d'autre part par la liste des nombres premiers qui y figurent avec une puissance impaire.

5.34. Proposition. *Soient* $\mathbf{B}$ *et* $\mathbf{C}$ *deux* $\mathbf{A}$*-algèbres libres de rangs* m *et* n*. Soit l'algèbre produit* $\mathbf{B}\times\mathbf{C}$*. Étant données une liste* $(\underline{x})=(x_1,\dots,x_m)$ *d'éléments de* $\mathbf{B}$ *et une liste* $(\underline{y})=(y_1,\dots,y_n)$ *d'éléments de* $\mathbf{C}$*, on a :*

$$\mathrm{disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}}(\underline{x},\underline{y})=\mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{x})\times\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(\underline{y}).$$

En particulier, $\mathrm{Disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}}=\mathrm{Disc}_{\mathbf{B}/\mathbf{A}}\times\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$.

▷ La démonstration est laissée à la lectrice. □

5.35. Proposition. *Soit* $\mathbf{B}\supseteq\mathbf{A}$ *une* $\mathbf{A}$*-algèbre libre de rang fini* p*.*
On considère

- *un* $\mathbf{B}$*-module* E *;*
- *une forme* $\mathbf{B}$*-bilinéaire symétrique* $\varphi_{\mathbf{B}}:E\times E\to\mathbf{B}$ *;*
- *une base* $(\underline{b})=(b_i)_{i\in[\![1..p]\!]}$ *de* $\mathbf{B}$ *sur* $\mathbf{A}$ *;*
- *une famille* $(\underline{e})=(e_j)_{j\in[\![1..n]\!]}$ *de* n *éléments de* E*.*

Notons $(\underline{b}\star\underline{e})$ *la famille* (b_ie_j) *de* np *éléments de* E *et* $\varphi_{\mathbf{A}}:E\times E\to\mathbf{A}$ *la forme* $\mathbf{A}$*-bilinéaire symétrique définie par :*

$$\varphi_{\mathbf{A}}(x,y)=\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(x,y)\big).$$

On a alors la formule de transitivité suivante :

$$\mathrm{gram}(\varphi_{\mathbf{A}},\underline{b}\star\underline{e})=\mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{b})^n\times\mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{gram}(\varphi_{\mathbf{B}},\underline{e})\big).$$

▷ Dans la suite, les indices i, i', k, j, j' satisfont à i, i', $k\in[\![1..p]\!]$ et j, $j'\in[\![1..n]\!]$. Convenons de ranger $\underline{b}\star\underline{e}$ dans l'ordre

$$\underline{b}\star\underline{e}=b_1e_1,\dots,b_pe_1,b_1e_2,\dots,b_pe_2,\dots,b_1e_n,\dots,b_pe_n.$$

Pour $x\in\mathbf{B}$, notons $\mu_x:\mathbf{B}\to\mathbf{B}$ la multiplication par x et $m(x)$ la matrice de μ_x dans la base $(b_i)_{i\in[\![1..p]\!]}$ de $\mathbf{B}$ sur $\mathbf{A}$. On définit ainsi un isomorphisme m de l'anneau $\mathbf{B}$ vers un sous-anneau commutatif de $\mathbb{M}_p(\mathbf{A})$. Si l'on note $m_{ki}(x)$ les coefficients de la matrice $m(x)$, on a donc :

$$\mu_x(b_i)=b_ix=\textstyle\sum_{k=1}^p m_{ki}(x)b_k,$$

avec $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(x)=\det\big(m(x)\big)$. En posant $\varphi_{jj'}=\varphi_{\mathbf{B}}(e_j,e_{j'})\in\mathbf{B}$, on a

$$\varphi_{\mathbf{A}}(b_ie_jb_{i'}e_{j'})=\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(b_ie_jb_{i'}e_{j'})\big)=\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_ib_{i'}\varphi_{jj'}).$$

En utilisant l'égalité $b_{i'}\varphi_{jj'}=\sum_{k=1}^p m_{ki'}(\varphi_{jj'})\,b_k$, il vient avec $\mathrm{Tr}=\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}$:

$$\mathrm{Tr}(b_ib_{i'}\varphi_{jj'})=\mathrm{Tr}\Big(\sum\nolimits_{k=1}^p b_i\,m_{ki'}(\varphi_{jj'})\,b_k\Big)=\sum\nolimits_{k=1}^p Tr(b_ib_k)\,m_{ki'}(\varphi_{jj'}).\quad(*)$$

On définit $\beta\in\mathbb{M}_p(\mathbf{A})$ par $\beta_{ik}=\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_ib_k)$. La somme de droite dans $(*)$ n'est autre que le coefficient d'un produit de matrices : $\big(\beta\cdot m(\varphi_{jj'})\big)_{ii'}$. Le déterminant de Gram de $\underline{b}\star\underline{e}$ pour $\varphi_{\mathbf{A}}$ est donc une matrice $np\times np$ constituée de n^2 blocs de matrices $p\times p$.

Voici cette matrice en notant $\phi_{jj'} = m(\varphi_{jj'})$ pour alléger l'écriture :

$$\begin{bmatrix} \beta\phi_{11} & \beta\phi_{12} & \dots & \beta\phi_{1n} \\ \beta\phi_{21} & \beta\phi_{22} & \dots & \beta\phi_{2n} \\ \vdots & & & \vdots \\ \beta\phi_{n1} & \beta\phi_{n2} & \dots & \beta\phi_{nn} \end{bmatrix} = \begin{bmatrix} \beta & 0 & \dots & 0 \\ 0 & \beta & \dots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & & \dots & \beta \end{bmatrix} \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

En prenant les déterminants, on obtient

$$\operatorname{gram}(\varphi_{\mathbf{A}}, \underline{b} \star \underline{e}) = \det(\beta)^n \times \det \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

En utilisant le fait que les matrices ϕ_{jl} commutent deux à deux, on obtient que le déterminant de droite est égal à

$$\det\Big(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\phi_{1\sigma_1}\phi_{2\sigma_2}\cdots\phi_{n\sigma_n}\Big) = \det m\big(\det(\varphi_{jl})\big) = \mathrm{N}_{\mathbf{B/A}}\big(\operatorname{gram}(\varphi_{\mathbf{B}}, \underline{e})\big),$$

ce qui démontre le résultat. □

5.36. Théorème. (Formule de transitivité pour les discriminants)
Soient $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$, *avec* $\mathbf{B}$ *libre sur* $\mathbf{A}$, $\mathbf{C}$ *libre sur* $\mathbf{B}$, $[\,\mathbf{C} : \mathbf{B}\,] = n$ *et* $[\,\mathbf{B} : \mathbf{A}\,] = m$. *Soit* $(\underline{b}) = (b_i)_{i\in[\![1..m]\!]}$ *une base de* $\mathbf{B}$ *sur* $\mathbf{A}$, $(\underline{c}) = (c_j)_{j\in[\![1..n]\!]}$ *une base de* $\mathbf{C}$ *sur* $\mathbf{B}$ *et notons* $(\underline{b} \star \underline{c})$ *la base* $(b_i c_j)$ *de* $\mathbf{C}$ *sur* $\mathbf{A}$.
Alors :

$$\operatorname{disc}_{\mathbf{C/A}}(\underline{b} \star \underline{c}) = \operatorname{disc}_{\mathbf{B/A}}(\underline{b})^{[\,\mathbf{C}:\mathbf{B}\,]}\ \mathrm{N}_{\mathbf{B/A}}\big(\operatorname{disc}_{\mathbf{C/B}}(\underline{c})\big),$$

et donc $$\operatorname{Disc}_{\mathbf{C/A}} = \operatorname{Disc}_{\mathbf{B/A}}^{[\,\mathbf{C}:\mathbf{B}\,]}\ \mathrm{N}_{\mathbf{B/A}}(\operatorname{Disc}_{\mathbf{C/B}}).$$

▷ Application directe de la proposition 5.35. □

6. Principe local-global de base pour les modules

Les résultats de cette section ne seront pas utilisés avant le chapitre V.

Nous allons donner une version un peu plus générale du principe local-global de base 2.3, version qui concerne des $\mathbf{A}$-modules et des applications linéaires arbitraires, tandis que le principe de base peut être considéré comme le cas particulier où les modules sont libres de rang fini. La preuve est essentiellement la même que celle du principe de base.
Auparavant, nous commençons par un bref rappel sur les suites exactes et nous établissons quelques propriétés élémentaires de la localisation pour les modules.

Complexes et suites exactes

Lorsque l'on a des applications linéaires successives

$$M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q\ ,$$

on dit qu'elles forment un *complexe* si la composée de deux applications qui se suivent est nulle.

On dit que la suite est *exacte en* N si $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. La suite toute entière est dite exacte si elle est exacte en N et P. On dit alors que *le complexe est exact*. Cela s'étend à des suites de longueur arbitraire.

Une application linéaire $\varphi : E \to F$ est appelée une *surjection scindée*, si l'on dispose d'une application linéaire $\psi : F \to E$ telle que $\varphi \circ \psi = \mathrm{Id}_F$. Dans ce cas, on dit que ψ est une *section* de φ, et l'on a $E = \operatorname{Ker}\varphi \oplus \psi(F) \simeq \operatorname{Ker}\varphi \oplus F$.

Une *suite exacte courte* est une suite exacte du type

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0\ .$$

Dans ce cas, le module M s'identifie à un sous-module M' de N, et P s'identifie à N/M'.

Une suite exacte courte est dite *scindée* si sa surjection est scindée.

Ce langage « abstrait » a une contrepartie immédiate en termes de systèmes linéaires lorsque l'on a affaire à des modules libres de rang fini. Par exemple, si $N = \mathbf{A}^n$, $P = \mathbf{A}^m$ et si l'on a une suite exacte

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0\ ,$$

l'application linéaire β est représentée par une matrice associée à un système linéaire de m équations à n inconnues, le module M, isomorphe à $\operatorname{Ker}\beta$, représente le défaut d'injectivité de β et le module Q, isomorphe à $\operatorname{Coker}\beta$, représente son défaut de surjectivité.

Il est important de noter qu'une suite exacte du type

$$0 \ \to\ M_m \ \xrightarrow{u_m}\ M_{m-1} \ \longrightarrow\ \cdots\cdots\cdots \ \xrightarrow{u_1}\ M_0 \ \to\ 0\ ,$$

(avec $m \geqslant 3$) « se décompose » en $m-1$ *suites exactes courtes* selon le schéma suivant.

$$\begin{array}{ccccccccc}
0 & \to & E_2 & \xrightarrow{\iota_2} & M_1 & \xrightarrow{u_1} & M_0 & \to & 0 \\
0 & \to & E_3 & \xrightarrow{\iota_3} & M_2 & \xrightarrow{v_2} & E_2 & \to & 0 \\
 & & \vdots & & & & & & \vdots \\
0 & \to & E_{m-1} & \xrightarrow{\iota_{m-1}} & M_{m-2} & \xrightarrow{v_{m-2}} & E_{m-2} & \to & 0 \\
0 & \to & M_m & \xrightarrow{u_m} & M_{m-1} & \xrightarrow{v_{m-1}} & E_{m-1} & \to & 0\ ,
\end{array}$$

avec $E_i = \operatorname{Im} u_i \subseteq M_{i-1}$ pour $i \in [\![2..m-1]\!]$, les ι_k des injections canoniques, et les v_k obtenus à partir des u_k en restreignant le module image à $\operatorname{Im} u_k$.

Un thème important de l'algèbre commutative est fourni par les transformations qui conservent, ou ne conservent pas, les suites exactes.

Nous allons donner deux exemples de base, qui utilisent les modules d'applications linéaires.

Nous notons $\mathrm{L}_{\mathbf{A}}(M,P)$ le $\mathbf{A}$-module des applications $\mathbf{A}$-linéaires de M dans P et $\mathrm{End}_{\mathbf{A}}(M)$ désigne $\mathrm{L}_{\mathbf{A}}(M,M)$ (avec sa structure d'anneau généralement non commutatif). Le *module dual* de M, $\mathrm{L}_{\mathbf{A}}(M,\mathbf{A})$, sera en général noté $M^\star$.

6.1. Fait. *Si $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ est une suite exacte de $\mathbf{A}$-modules, et si F est un $\mathbf{A}$-module, alors la suite*

$$0 \to \mathrm{L}_{\mathbf{A}}(F,M) \longrightarrow \mathrm{L}_{\mathbf{A}}(F,N) \longrightarrow \mathrm{L}_{\mathbf{A}}(F,P)$$

est exacte.

D *Exactitude en* $\mathrm{L}_{\mathbf{A}}(F,M)$. Soit $\varphi \in \mathrm{L}_{\mathbf{A}}(F,M)$ telle que $\alpha \circ \varphi = 0$. Alors, puisque la première suite est exacte en M, pour tout $x \in F$, $\varphi(x) = 0$, donc $\varphi = 0$.

Exactitude en $\mathrm{L}_{\mathbf{A}}(F,N)$. Soit $\varphi \in \mathrm{L}_{\mathbf{A}}(F,N)$ telle que $\beta \circ \varphi = 0$. Alors, puisque la première suite est exacte en N, pour tout $x \in F$, $\varphi(x) \in \mathrm{Im}\,\alpha$. Soient $\alpha_1 : \mathrm{Im}\,\alpha \to M$ la bijection réciproque de α (lorsque l'on regarde α comme à valeurs dans $\mathrm{Im}\,\alpha$) et $\psi = \alpha_1\,\varphi$.
On obtient alors les égalités $\mathrm{L}_{\mathbf{A}}(F,\alpha)(\psi) = \alpha\,\alpha_1\,\varphi = \varphi$. □

6.2. Fait. *Si $N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0$ est une suite exacte de $\mathbf{A}$-modules et si F est un $\mathbf{A}$-module, alors la suite*

$$0 \to \mathrm{L}_{\mathbf{A}}(Q,F) \longrightarrow \mathrm{L}_{\mathbf{A}}(P,F) \longrightarrow \mathrm{L}_{\mathbf{A}}(N,F)$$

est exacte.

D *Exactitude en* $\mathrm{L}_{\mathbf{A}}(Q,F)$. Si $\varphi \in \mathrm{L}_{\mathbf{A}}(Q,F)$ vérifie $\varphi \circ \gamma = 0$, alors, puisque γ est surjective, $\varphi = 0$.

Exactitude en $\mathrm{L}_{\mathbf{A}}(P,F)$. Si $\varphi : P \to F$ vérifie $\varphi \circ \beta = 0$, alors $\mathrm{Im}\,\beta \subseteq \mathrm{Ker}\,\varphi$ et φ se factorise par $P/\mathrm{Im}\,\beta \simeq Q$, i.e. $\varphi = \psi \circ \gamma$ pour une application linéaire $\psi : Q \to F$, c'est-à-dire $\varphi \in \mathrm{Im}\,\mathrm{L}_{\mathbf{A}}(\gamma,F)$. □

6.3. Fait. *Soit $\beta : N \to P$ une application linéaire et $\gamma : P \to \mathrm{Coker}\,\beta$ la projection canonique.*

1. *L'application canonique ${}^{\mathrm{t}}\gamma : (\mathrm{Coker}\,\beta)^\star \to P^\star$ induit un isomorphisme de $(\mathrm{Coker}\,\beta)^\star$ sur $\mathrm{Ker}\,{}^{\mathrm{t}}\beta$.*
2. *Si les applications linéaires canoniques $N \to N^{\star\star}$ et $P \to P^{\star\star}$ sont des isomorphismes, alors la surjection canonique de $N^\star$ dans $\mathrm{Coker}\,{}^{\mathrm{t}}\beta$ fournit par dualité un isomorphisme de $(\mathrm{Coker}\,{}^{\mathrm{t}}\beta)^\star$ sur $\mathrm{Ker}\,\beta$.*

▷ *1.* On applique le fait 6.2 avec $F = \mathbf{A}$.
2. On applique le point *1* à l'application linéaire ${}^{\mathrm{t}}\beta$ en identifiant N et $N^{\star\star}$, ainsi que P et $P^{\star\star}$, et donc aussi β et ${}^{\mathrm{t}}({}^{\mathrm{t}}\beta)$. □

Remarque. Il est possible d'affaiblir légèrement l'hypothèse en demandant pour l'application linéaire $P \to P^{\star\star}$ qu'elle soit injective. ▪

Localisation et suites exactes

6.4. Fait. *Soit S un monoïde d'un anneau $\mathbf{A}$.*

1. *Si M est un sous-module de N, on a l'identification canonique de M_S avec un sous-module de N_S et de $(N/M)_S$ avec N_S/M_S.*
   En particulier, pour tout idéal $\mathfrak{a}$ de $\mathbf{A}$, le $\mathbf{A}$-module $\mathfrak{a}_S$ s'identifie canoniquement avec l'idéal $\mathfrak{a}\mathbf{A}_S$ de $\mathbf{A}_S$.
2. *Si $\varphi : M \to N$ est une application $\mathbf{A}$-linéaire, alors :*
   a. $\mathrm{Im}(\varphi_S)$ *s'identifie canoniquement à* $\big(\mathrm{Im}(\varphi)\big)_S$,
   b. $\mathrm{Ker}(\varphi_S)$ *s'identifie canoniquement à* $\big(\mathrm{Ker}(\varphi)\big)_S$,
   c. $\mathrm{Coker}(\varphi_S)$ *s'identifie canoniquement à* $\big(\mathrm{Coker}(\varphi)\big)_S$.
3. *Si l'on a une suite exacte de $\mathbf{A}$-modules*
   $$M \xrightarrow{\varphi} N \xrightarrow{\psi} P\,,$$
   alors la suite de $\mathbf{A}_S$-modules
   $$M_S \xrightarrow{\varphi_S} N_S \xrightarrow{\psi_S} P_S$$
   est également exacte.

6.5. Fait. *Si M_1, …, M_r sont des sous-modules de N et $M = \bigcap_{i=1}^{r} M_i$, alors en identifiant les modules $(M_i)_S$ et M_S à des sous-modules de N_S on obtient $M_S = \bigcap_{i=1}^{r} (M_i)_S$.*

6.6. Fait. *Soient M et N deux sous-modules d'un $\mathbf{A}$-module P, avec N de type fini. Alors, l'idéal transporteur $(M_S : N_S)$ s'identifie à $(M : N)_S$, via les applications naturelles de $(M : N)$ dans $(M_S : N_S)$ et $(M : N)_S$.*

Cela s'applique en particulier pour l'annulateur d'un idéal de type fini.

Principe local-global pour les suites exactes de modules

6.7. Principe local-global concret. (Pour les suites exactes)
Soient S_1, …, S_n des monoïdes comaximaux de $\mathbf{A}$, M, N, P des $\mathbf{A}$-modules et deux applications linéaires $\varphi : M \to N$, $\psi : N \to P$. On note $\mathbf{A}_i$ pour $\mathbf{A}_{S_i}$, M_i pour M_{S_i} etc. Les propriétés suivantes sont équivalentes.

1. *La suite $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ est exacte.*
2. *Pour chaque $i \in [\![1..n]\!]$, la suite $M_i \xrightarrow{\varphi_i} N_i \xrightarrow{\psi_i} P_i$ est exacte.*

Comme conséquence, φ est injective (resp. surjective) si, et seulement si, pour chaque $i \in [\![1..n]\!]$, φ_i est injective (resp. surjective).

$\mathbb{D}$ Nous avons vu que *1* $\Rightarrow$ *2* dans le fait 6.4.
Supposons *2*. Notons $\mu_i : M \to M_i$, $\nu_i : N \to N_i$, $\pi_i : P \to P_i$ les homomorphismes canoniques. Soit $x \in M$ et $z = \psi\big(\varphi(x)\big)$, on a

$$0 = \psi_i\Big(\varphi_i\big(\mu_i(x)\big)\Big) = \pi_i\Big(\psi\big(\varphi(x)\big)\Big) = \pi_i(z),$$

donc pour un $s_i \in S_i$, $s_i z = 0$ dans P. On conclut que $z = 0$ en utilisant la comaximalité des S_i : $\sum_i u_i s_i = 1$. Soit maintenant $y \in N$ tel que $\psi(y) = 0$. Pour chaque i il existe un $x_i \in M_i$ tel que $\varphi_i(x_i) = \nu_i(y)$.
On écrit $x_i =_{M_i} a_i/s_i$ avec $a_i \in M$ et $s_i \in S_i$. L'égalité $\varphi_i(x_i) = \nu_i(y)$ signifie que pour un certain $t_i \in S_i$ on a $t_i\varphi(a_i) = t_i s_i y$ qui est dans N. Si $\sum_i v_i t_i s_i = 1$, on en déduit que $\varphi\big(\sum_i v_i t_i a_i\big) = y$. Ainsi, $\operatorname{Ker}\psi$ est bien inclus dans $\operatorname{Im}\varphi$. □

6.8. Principe local-global abstrait*. (Pour les suites exactes)
Soient M, N, P des $\mathbf{A}$-modules, et deux applications linéaires $\varphi : M \to N$ et $\psi : N \to P$. Les propriétés suivantes sont équivalentes.

1. *La suite $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ est exacte.*
2. *Pour tout idéal maximal $\mathfrak{m}$, la suite $M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{\psi_{\mathfrak{m}}} P_{\mathfrak{m}}$ est exacte.*

Comme conséquence, φ est injective (resp. surjective) si, et seulement si, pour tout idéal maximal $\mathfrak{m}$, $\varphi_{\mathfrak{m}}$ est injective (resp. surjective).

$\mathbb{D}$ La propriété $x = 0$ pour un élément x d'un module est une propriété de caractère fini. De même pour la propriété $y \in \operatorname{Im}\varphi$. Ainsi, même si la propriété « la suite est exacte » n'est pas de caractère fini, c'est une conjonction de propriétés de caractère fini, et l'on peut appliquer le fait* 2.11 pour déduire le principe local-global abstrait du principe local-global concret. □

Signalons enfin un principe local-global concret pour les monoïdes.

6.9. Principe local-global concret. (Pour les monoïdes)
Soient S_1, …, S_n des monoïdes comaximaux de $\mathbf{A}$, V un monoïde. Les propriétés suivantes sont équivalentes.

1. *Le monoïde V contient 0.*
2. *Pour $i \in [\![1..n]\!]$, le monoïde V vu dans $\mathbf{A}_{S_i}$ contient 0.*

$\mathbb{D}$ Pour chaque i on a un $v_i \in V$ et un $s_i \in S_i$ tels que $s_i v_i = 0$. On pose $v = \prod_i v_i \in V$. Alors, v est nul dans les $\mathbf{A}_{S_i}$, donc dans $\mathbf{A}$. □

Exercices et problèmes

Exercice 1. Il est recommandé de faire les démonstrations non données, esquissées, laissées au lecteur, etc. On pourra notamment traiter les cas suivants.

— Vérifier les affirmations des faits 1.2 à 1.4.
— Démontrer le corollaire 2.4.
— Dans le lemme 2.6 calculer des exposants convenables dans les points *2*, *3*, et *4*, en explicitant complètement la démonstration.
— Démontrer le corollaire 3.3. Donner une preuve plus détaillée du théorème 3.4. Vérifiez les détails dans la preuve du principe local-global 3.5. Démontrer la proposition 3.7.
— Vérifier les affirmations des faits 6.4 à 6.6. Pour le fait 6.5 on utilisera la suite exacte $0 \to M \to N \to \bigoplus_{i=1}^{r} N/M_i$, qui est préservée par localisation.

Exercice 2. (Voir aussi l'exercice VII-8)

1. *(Inversibles dans* $\mathbf{B}[T]$*, cf. lemme 2.6)*
   Soient deux polynômes $f = \sum_{i=0}^{n} a_i T^i$, $g = \sum_{j=0}^{m} b_j T^j$ avec $fg = 1$. Montrer que les coefficients a_i, $i \geqslant 1$, b_j, $j \geqslant 1$ sont nilpotents et que $a_n^{m+1} = 0$.
2. *(Polynôme caractéristique d'une matrice nilpotente)*
   Soit $A \in \mathbb{M}_n(\mathbf{B})$ une matrice nilpotente et soit $\mathrm{C}_A(T) = T^n + \sum_{k=0}^{n-1} a_k T^k$ son polynôme caractéristique.
   a. Montrer que les coefficients a_i sont nilpotents.
   b. Précisément, si $A^e = 0$, alors $\mathrm{Tr}(A)^{(e-1)n+1} = 0$ et
   $$a_i^{e_i} = 0, \quad \text{avec} \quad e_i = (e-1)\tbinom{n}{i} + 1, \quad (i = 0, \dots, n-1).$$

Exercice 3. On considère un vecteur $x = (x_1, \dots, x_n) \in \mathbf{A}^n$ et $s \in \mathbf{A}$.

1. Si x est unimodulaire dans $\mathbf{A}/\langle s \rangle$ et dans $\mathbf{A}[1/s]$, il est unimodulaire dans $\mathbf{A}$.
2. Soient $\mathfrak{b}$ et $\mathfrak{c}$ deux idéaux de $\mathbf{A}$; si x est unimodulaire modulo $\mathfrak{b}$ et modulo $\mathfrak{c}$, il l'est modulo $\mathfrak{bc}$.

Exercice 4. *(Une application typique du principe local-global de base)*
Soit $x = (x_1, \dots, x_n) \in \mathbf{A}^n$, *unimodulaire*. Pour $d \geqslant 1$, on note $\mathbf{A}[X_1, \dots, X_n]_d$ le sous-$\mathbf{A}$-module des polynômes homogènes de degré d et
$$I_{d,x} = \left\{ f \in \mathbf{A}[\underline{X}]_d \mid f(x) = 0 \right\}, \quad \text{sous-}\mathbf{A}\text{-module de } \mathbf{A}[\underline{X}].$$

1. Si $x_1 \in \mathbf{A}^\times$, tout $f \in I_{d,x}$ est combinaison linéaire des $x_1 X_j - x_j X_1$ avec pour coefficients des polynômes homogènes de degré $d-1$.
2. En général, tout $f \in I_{d,x}$ est une combinaison linéaire des $(x_k X_j - x_j X_k)$ avec pour coefficients des polynômes homogènes de degré $d-1$.
3. Soit $I_x = \bigoplus_{d \geqslant 1} I_{d,x}$. Montrer que $I_x = \{ F \mid F(tx) = 0 \}$ (où t est une nouvelle indéterminée). Montrer que I_x est *saturé*, i.e., si $X_j^m F \in I_x$ pour un m et pour chaque j, alors $F \in I_x$.

Exercice 5. *(Variations sur le lemme de Gauss-Joyal 2.6)*
Montrer que les affirmations suivantes sont équivalentes (chacune des affirmations est universelle, i.e., valable pour tous polynômes et tout anneau commutatif $\mathbf{A}$) :

1. $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1\rangle \;\Rightarrow\; \mathrm{c}(fg) = \langle 1\rangle$,
2. $(\exists i_0, j_0 \;\; f_{i_0} = g_{j_0} = 1) \;\Rightarrow\; \mathrm{c}(fg) = \langle 1\rangle$,
3. $\exists p \in \mathbb{N}, \;\; \big(\mathrm{c}(f)\mathrm{c}(g)\big)^p \subseteq \mathrm{c}(fg)$,
4. *(Gauss-Joyal)* $\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(f)\mathrm{c}(g)\big) = \mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big)$.

Exercice 6. *(Norme d'un polynôme primitif via l'utilisation d'un anneau nul)*
Soient $\mathbf{B}$ une $\mathbf{A}$-algèbre libre de dimension finie, $\underline{X} = (X_1, \ldots, X_n)$ des indéterminées. On pose $Q \in \mathbf{B}[\underline{X}]$ et $P = \mathrm{N}_{\mathbf{B}[\underline{X}]/\mathbf{A}[\underline{X}]}(Q) \in \mathbf{A}[\underline{X}]$. Montrer que si Q est primitif, alors P l'est aussi.
Indication : vérifier l'égalité $\mathbf{A} \cap \mathrm{c}_{\mathbf{B}}(P) = \mathrm{c}_{\mathbf{A}}(P)$ et considérer ensuite le sous-anneau $\mathbf{A}' = \mathbf{A}/\mathrm{c}_{\mathbf{A}}(P)$ du quotient $\mathbf{B}' = \mathbf{B}/\mathrm{c}_{\mathbf{B}}(P)$ et l'application $\mathbf{A}'$-linéaire « multiplication par Q », $m_Q : \mathbf{B}'[\underline{X}] \to \mathbf{B}'[\underline{X}],\; R \mapsto QR$.

Exercice 7. Montrer qu'un anneau $\mathbf{A}$ cohérent est fortement discret si, et seulement si, le test « $1 \in \langle a_1, \ldots, a_n\rangle$? » est explicite pour toute suite finie $(a_1, \ldots, a_n)$ dans $\mathbf{A}$.

Exercice 8. *(Un exemple d'anneau noethérien cohérent avec un quotient non cohérent)*
On considère l'anneau $\mathbb{Z}$ et un idéal $\mathfrak{a}$ engendré par une suite infinie d'éléments, tous nuls sauf éventuellement un, qui est alors égal à 3 (par exemple on met un 3 la première fois, si cela arrive, qu'un zéro de la fonction zéta de Riemann n'a pas sa partie réelle égale à 1/2). Si l'on est capable de donner un système fini de générateurs pour l'annulateur de 3 dans $\mathbb{Z}/\mathfrak{a}$, on est capable de dire si la suite infinie est identiquement nulle ou pas. Cela signifierait qu'il existe une méthode sûre pour résoudre les conjectures du type de celle de Riemann.
Commentaire. Comme toute définition constructive raisonnable de la noethérianité semble réclamer qu'un quotient d'un anneau noethérien reste noethérien, et vu le « contre-exemple » précédent, on ne peut espérer avoir une preuve constructive du théorème de mathématiques classiques qui affirme que tout anneau noethérien est cohérent. ∎

Exercice 9. *(Idempotents de $\mathbf{A}[X]$)*
Montrer que tout idempotent de $\mathbf{A}[X]$ est un idempotent de $\mathbf{A}$.

Exercice 10. Soient u et v deux idempotents et x un élément de $\mathbf{A}$.
L'élément $1 - (1-u)(1-v) = u + v - uv$ est noté $u \vee v$.

1. Montrer que $x \in u\mathbf{A} \;\Leftrightarrow\; ux = x$. En particulier, $u\mathbf{A} = v\mathbf{A} \;\Leftrightarrow\; u = v$.
2. L'élément uv est le plus petit commun multiple de u et v parmi les idempotents de $\mathbf{A}$ (i.e., si w est un idempotent, $w \in u\mathbf{A} \cap v\mathbf{A} \;\Leftrightarrow\; w \in uv\mathbf{A}$). En fait, on a même $u\mathbf{A} \cap v\mathbf{A} = uv\mathbf{A}$. On note $u \wedge v = uv$.
3. Démontrer l'égalité $u\mathbf{A} + v\mathbf{A} = (u \vee v)\mathbf{A}$. En déduire que $u \vee v$ est le plus grand commun diviseur de u et v parmi les idempotents de $\mathbf{A}$ (en fait un élément arbitraire de $\mathbf{A}$ divise u et v si, et seulement si, il divise $u \vee v$).

4. À l'aide d'une suite de manipulations élémentaires, transformer la matrice $\mathrm{Diag}(u, v)$ en la matrice $\mathrm{Diag}(u \vee v, u \wedge v)$.
   En déduire que les deux $\mathbf{A}$-modules $u\mathbf{A} \oplus v\mathbf{A}$ et $(u \vee v)\mathbf{A} \oplus (u \wedge v)\mathbf{A}$ sont isomorphes.
5. Montrer que les deux anneaux $\mathbf{A}/\langle u\rangle \times \mathbf{A}/\langle v\rangle$ et $\mathbf{A}/\langle u \vee v\rangle \times \mathbf{A}/\langle u \wedge v\rangle$ sont isomorphes.

Exercice 11. Soit $\mathbf{A}$ un anneau et $(e_1, \dots, e_n)$ un système fondamental d'idempotents orthogonaux de $\mathrm{Frac}\,\mathbf{A} = \mathbf{K}$. On écrit $e_i = a_i/d$ avec $a_i \in \mathbf{A}$ et $d \in \mathrm{Reg}\,\mathbf{A}$. On a alors $a_i a_j = 0$ pour $i \neq j$ et $\sum_i a_i$ régulier.
1. Établir une réciproque.
2. Montrer que $\mathbf{K}[1/e_i] \simeq \mathrm{Frac}\left(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\right)$ et $\mathbf{K} \simeq \prod_i \mathrm{Frac}\left(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\right)$.

Exercice 12. *(Séparer les composantes irréductibles)*
1. Soit $\mathbf{A} = \mathbb{Q}[x, y, z] = \mathbb{Q}[X, Y, Z]/\langle XY, XZ, YZ\rangle$ et $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$. Quels sont les zéros de $\mathbf{A}$ dans $\mathbb{Q}^3$ (i.e. $(x, y, z) \in \mathbb{Q}^3$ tels que $xy = yz = zx = 0$) ? Donner une forme réduite pour les éléments de $\mathbf{A}$. Montrer que $x+y+z \in \mathrm{Reg}\,\mathbf{A}$. Montrer que les éléments $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ et $\dfrac{z}{x+y+z}$ forment un système fondamental d'idempotents orthogonaux dans $\mathbf{K}$. Montrer que $\mathbf{K} \simeq \mathbb{Q}(X) \times \mathbb{Q}(Y) \times \mathbb{Q}(Z)$.
2. Soit $\mathbf{B} = \mathbb{Q}[u, v, w] = \mathbb{Q}[U, V, W]/\langle UVW\rangle$ et $\mathbf{L} = \mathrm{Frac}\,\mathbf{B}$.
Quels sont les zéros de $\mathbf{B}$ dans $\mathbb{Q}^3$? Donner une forme réduite pour les éléments de $\mathbf{B}$. Montrer que $\mathbf{L} \simeq \mathbb{Q}(U, V) \times \mathbb{Q}(V, W) \times \mathbb{Q}(W, U)$.

Exercice 13. *(Idempotent et groupe élémentaire)*
Soit $a \in \mathbf{A}$ un idempotent. Pour $b \in \mathbf{A}$, expliciter une matrice $A \in \mathbb{E}_2(\mathbf{A})$ et un élément $d \in \mathbf{A}$ tels que $A \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$. En particulier, $\langle a, b\rangle = \langle d\rangle$.
En outre, si b est régulier (resp. inversible) modulo a, alors d est régulier (resp. inversible). Enfin si b est idempotent, $d = a \vee b = a + b - ab$.

Exercice 14. Soit $(r_1, \dots, r_m)$ une famille finie d'idempotents dans un anneau $\mathbf{A}$. Posons $s_i = 1 - r_i$ et, pour une partie I de $[\![1..m]\!]$, notons $r_I = \prod_{i\in I} r_i \prod_{i\notin I} s_i$.
1. Montrer que la matrice diagonale $D = \mathrm{Diag}(r_1, \dots, r_m)$ est semblable à une matrice $D' = \mathrm{Diag}(e_1, \dots, e_m)$, où les e_i sont des idempotents qui vérifient : e_i divise e_j si $j > i$. On pourra commencer par le cas $n = 2$ et utiliser l'exercice 10. Montrer que $\langle e_k\rangle = \mathcal{D}_k(D)$ pour tout k.
2. Montrer que l'on peut écrire $D' = PDP^{-1}$ avec P une *matrice de permutation généralisée*, c'est-à-dire une matrice qui s'écrit $\sum_j f_j P_j$, où les f_j forment un système fondamental d'idempotents orthogonaux et chaque P_j est une matrice de permutation. Suggestions :

— Les r_I forment un système fondamental d'idempotents orthogonaux. La matrice diagonale $r_I D$ a pour coefficient en position (i, i) l'élément r_I si $i \in I$ et 0 sinon. La matrice P_I correspond alors à une permutation ramenant les coefficients r_I en tête de la liste. Enfin, $P = \sum_I r_I P_I$. Notez que le test « $r_I = 0$? » n'est pas nécessaire !

— On peut aussi traiter le cas $m = 2$: on trouve $P = e\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + f\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, avec $f = r_2 s_1$, $e = 1 - f$, et $D' = \mathrm{Diag}(r_1 \vee r_2, r_1 \wedge r_2)$.
Ensuite, on traite le cas $m > 2$ de proche en proche.

Exercice 15. Rappeler une preuve du théorème des restes chinois (page 38) et expliciter les idempotents.

Exercice 16. *(Groupe élémentaire : premiers pas)* Cas de $\mathbb{M}_2(\mathbf{A})$.

1. Soit $a \in \mathbf{A}$. Déterminer une matrice $P \in \mathbb{E}_2(\mathbf{A})$ telle que $P\begin{bmatrix} a \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ a \end{bmatrix}$. Même chose pour $\begin{bmatrix} \varepsilon a \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} a \\ 0 \end{bmatrix}$, où $\varepsilon \in \mathbf{A}^\times$.

2. Écrire comme éléments de $\mathbb{E}_2(\mathbf{A})$ les matrices $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

3. Toute matrice triangulaire de $\mathbb{SL}_2(\mathbf{A})$ est dans $\mathbb{E}_2(\mathbf{A})$.

4. Soient $u = \begin{bmatrix} x \\ y \end{bmatrix}$, $v = \begin{bmatrix} y \\ x \end{bmatrix}$, $w = \begin{bmatrix} -y \\ x \end{bmatrix}$ avec $x, y \in \mathbf{A}$. Montrer que $v \in \mathbb{GL}_2(\mathbf{A}) \cdot u$ et $w \in \mathbb{E}_2(\mathbf{A}) \cdot u$, mais pas nécessairement $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$. Par exemple, si x, y sont deux indéterminées sur un anneau $\mathbf{k}$, $\mathbf{A} = \mathbf{k}[x, y]$ et $v = Au$, avec $A \in \mathbb{GL}_2(\mathbf{A})$, alors $\big(\det(A)\big)(0, 0) = -1$. En conséquence, on a $\det(A) \in -1 + \mathrm{D}_{\mathbf{k}}(0)\,\langle x, y\rangle$ (lemme 2.6), donc $\det(A) = -1$ si $\mathbf{k}$ est réduit. De plus, si $\det(A) = 1$, alors $2 = 0$ dans $\mathbf{k}$. Par suite, $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$ si, et seulement si, $2 = 0$ dans $\mathbf{k}$.

Exercice 17. *(Groupe élémentaire : deuxièmes pas)*
1. Soit $A \in \mathbb{M}_{n,m}(\mathbf{A})$ avec un coefficient inversible et $(n, m) \neq (1, 1)$. Déterminer des matrices $P \in \mathbb{E}_n(\mathbf{A})$ et $Q \in \mathbb{E}_m(\mathbf{A})$ telles que $PAQ = \begin{bmatrix} 1 & 0_{1,m-1} \\ 0_{n-1,1} & A' \end{bmatrix}$.
Exemple : avec $a \in \mathbf{A}^\times$ donner P pour $P\begin{bmatrix} a \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (exercice 16 point *1*).

2. Soit $A \in \mathbb{M}_2(\mathbf{A})$ avec un coefficient inversible. Calculer des matrices P et $Q \in \mathbb{E}_2(\mathbf{A})$ telles que : $PAQ = \begin{bmatrix} 1 & 0 \\ 0 & \delta \end{bmatrix}$ avec $\delta = \det(A)$.
Toute matrice $A \in \mathbb{SL}_2(\mathbf{A})$ ayant un coefficient inversible appartient à $\mathbb{E}_2(\mathbf{A})$. Expliciter les cas suivants :

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \qquad \begin{bmatrix} 0 & a \\ -a^{-1} & 0 \end{bmatrix}, \qquad \text{avec } a \in \mathbf{A}^\times.$$

Écrire les matrices suivantes (avec $a \in \mathbf{A}^\times$) dans $\mathbb{E}_2(\mathbf{A})$:

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}, \qquad \begin{bmatrix} a & 0 \\ b & a^{-1} \end{bmatrix}, \qquad \begin{bmatrix} 0 & a \\ -a^{-1} & b \end{bmatrix}, \qquad \begin{bmatrix} b & a \\ -a^{-1} & 0 \end{bmatrix}.$$

3. Si $A = \mathrm{Diag}(a_1, a_2, \ldots, a_n) \in \mathbb{SL}_n(\mathbf{A})$, alors $A \in \mathbb{E}_n(\mathbf{A})$.

4. Toute matrice triangulaire $A \in \mathbb{SL}_n(\mathbf{A})$ appartient à $\mathbb{E}_n(\mathbf{A})$.

Exercice 18. *(Les matrices de division D_q de déterminant 1)*
Une « division générale » $a = bq - r$ peut s'écrire matriciellement :

$$\begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ r \end{bmatrix}.$$

Cela conduit à introduire la matrice $D_q = \begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \in \mathbb{SL}_2(\mathbf{A})$.

Montrer que $\mathbb{E}_2(\mathbf{A})$ est le monoïde engendré par les matrices D_q.

Exercice 19. Soient $\mathbf{A}$ un anneau et A, $B \in \mathbb{M}_n(\mathbf{A})$. On suppose que l'on a un $i \in \mathbf{A}$ avec $i^2 = -1$ et que $2 \in \mathbf{A}^\times$. Montrer que les matrices de $\mathbb{M}_{2n}(\mathbf{A})$

$$M = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \text{ et } M' = \begin{bmatrix} A+iB & 0 \\ 0 & A-iB \end{bmatrix}$$

sont *élémentairement semblables*, (i.e., $\exists P \in \mathbb{E}_{2n}(\mathbf{A}),\ PMP^{-1} = M'$).
Indication : traiter d'abord le cas $n = 1$.

Exercice 20. Pour $d \in \mathbf{A}^\times$ et $\lambda \in \mathbf{A}$ calculer la matrice

$$\mathrm{Diag}(1, \dots, d, \dots, 1) \cdot \mathrm{E}_{ij}(\lambda) \cdot \mathrm{Diag}(1, \dots, d^{-1}, \dots, 1).$$

Montrer que le sous-groupe des matrices diagonales de $\mathbb{GL}_n(\mathbf{A})$ normalise $\mathbb{E}_n(\mathbf{A})$.

Exercice 21. *(Un lemme de liberté, ou un Splitting Off, au choix de la lectrice)*
Soit $F \in \mathbb{GA}_n(\mathbf{A})$ un projecteur possédant un mineur principal d'ordre k inversible. Montrer que F est semblable à une matrice $\begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & F' \end{bmatrix}$, où $F' \in \mathbb{GA}_{n-k}(\mathbf{A})$.

Le module projectif de type fini $P \overset{\text{déf}}{=} \operatorname{Im} F \subseteq \mathbf{A}^n$ admet un facteur direct libre ayant pour base k colonnes de F.

Exercice 22. Soit $A \in \mathbf{A}^{n\times m}$ de rang 1. Construire $B \in \mathbf{A}^{m\times n}$ telle que $ABA = A$ et vérifier que AB est un projecteur de rang 1. Comparez votre solution à celle qui résulterait de la preuve du théorème 5.14.

Exercice 23. Cet exercice constitue une abstraction des calculs qui ont mené au théorème 5.14. On considère un $\mathbf{A}$-module E « ayant assez de formes linéaires », i.e. si $x \in E$ vérifie $\mu(x) = 0$ pour tout $\mu \in E^\star$, alors $x = 0$. Cela signifie que l'application canonique de E dans son bidual, $E \to E^{\star\star}$, est injective. Lorsque cette application linéaire est un isomorphisme, on dit que le module est *réflexif* ; c'est le cas pour un module libre de rang fini ou un module projectif de type fini.

Pour $x_1, \dots, x_n \in E$, on note $\bigwedge_r(x_1, \dots, x_n)$ l'idéal de $\mathbf{A}$ engendré par les évaluations de toutes les formes r-linéaires alternées de E en tous les r-uplets d'éléments de $\{x_1, \dots, x_n\}$.

On suppose que $1 \in \bigwedge_r(x_1, \dots, x_n)$ *et* $\bigwedge_{r+1}(x_1, \dots, x_n) = 0$.

On veut montrer que le sous-module $\sum \mathbf{A}x_i$ est facteur direct dans E en explicitant un projecteur $\pi : E \to E$ dont l'image est ce sous-module.

1. *(Formules de Cramer)* Soit f une forme r-linéaire alternée sur E. Montrer, pour $y_0, \ldots, y_r \in \sum \mathbf{A}x_i$, que
$$\sum\nolimits_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, y_i = 0.$$
Ou encore, pour $y, y_1, \ldots, y_r \in \sum \mathbf{A}x_i$
$$f(y_1, \ldots, y_r)\, y = \sum\nolimits_{i=1}^{r} f(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_r)\, y_i.$$
2. Donner n formes linéaires $\alpha_i \in E^\star$ telles que l'application linéaire
$$\pi : E \to E, \quad x \mapsto \textstyle\sum_i \alpha_i(x) x_i$$
soit un projecteur d'image $\sum \mathbf{A}x_i$.
On notera $\psi : \mathbf{A}^n \to E$ définie par $e_i \mapsto x_i$, et $\varphi : E \to \mathbf{A}^n$ définie par $\varphi(x) = \big(\alpha_1(x), \ldots, \alpha_n(x)\big)$. On s'arrangera pour que $\pi = \psi \circ \varphi$ et $\pi \circ \psi = \psi$, ce qui donne $\psi \circ \varphi \circ \psi = \psi$.
3. *(Nouvelle démonstration du théorème 5.14)* Soit $A \in \mathbf{A}^{m\times n}$ une matrice de rang r. Montrer qu'il existe $B \in \mathbf{A}^{n\times m}$ telle que $A\,B\,A = A$.

Exercice 24. Soient $A \in \mathbf{A}^{n\times m}$ et $B \in \mathbf{A}^{m\times n}$.

1. On a la formule de commutativité suivante : $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB)$.

Première démonstration. Traiter d'abord le cas où $m = n$, par exemple par la méthode des coefficients indéterminés. Si $m \neq n$, on peut compléter A et B par des lignes et des colonnes de 0 pour en faire des matrices carrées A_1 et B_1 de taille $q = \max(m, n)$ comme dans la démonstration donnée page 40.

On vérifie alors que
$$\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_q + XB_1A_1) \quad \text{et} \quad \det(\mathrm{I}_n + XAB) = \det(\mathrm{I}_q + XA_1B_1).$$

Deuxième démonstration. On considère une indéterminée X et les matrices
$$B' = \begin{bmatrix} XB & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{bmatrix} \quad \text{et} \quad A' = \begin{bmatrix} A & \mathrm{I}_n \\ \mathrm{I}_m & -XB \end{bmatrix}.$$
Calculer $A'B'$ et $B'A'$ et conclure.

2. Qu'en déduit-on pour les polynômes caractéristiques de $A\,B$ et $B\,A$?

Exercice 25. *(Formule de Binet-Cauchy)*
On utilise les notations page 47. Si $A \in \mathbf{A}^{n\times m}$ et $B \in \mathbf{A}^{m\times n}$ sont deux matrices de formats transposés, on a la formule de Binet-Cauchy :
$$\det(BA) = \sum\nolimits_{\alpha \in \mathcal{P}_{m,n}} \det(B_{1..m,\alpha}) \det(A_{\alpha,1..m}).$$

Première démonstration. On utilise la formule $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB)$ (exercice 24). On considère alors le coefficient de X^m dans chacun des polynômes $\det(\mathrm{I}_m + XBA)$ et $\det(\mathrm{I}_n + XAB)$.

Deuxième démonstration. Les matrices A et B représentent des applications linéaires $u : \mathbf{A}^m \to \mathbf{A}^n$ et $v : \mathbf{A}^n \to \mathbf{A}^m$.

On considère alors les matrices de $\bigwedge^m u$, $\bigwedge^m v$ et $\bigwedge^m(v \circ u)$ sur les bases naturellement associées aux bases canoniques de $\mathbf{A}^n$ et $\mathbf{A}^m$.
On conclut en écrivant que $\bigwedge^m(v \circ u) = \bigwedge^m v \circ \bigwedge^m u$.

Troisième démonstration. Dans le produit BA on intercale entre B et A une matrice diagonale D ayant pour coefficients des indéterminées λ_i, et l'on regarde quel est le coefficient de $\lambda_{i_1} \cdots \lambda_{i_m}$ dans le polynôme $\det(BDA)$ (pour cela on prend $\lambda_{i_1} = \cdots = \lambda_{i_m} = 1$ et les autres nuls). On conclut en prenant tous les λ_i égaux à 1.

Exercice 26. Soit $u \in \mathrm{End}_{\mathbf{A}}(\mathbf{A}^n)$. Pour $k \in [\![0..n]\!]$, on note $u_k = \bigwedge^k(u)$.
Montrer que $\det(u_k) = \det(u)^{\binom{n-1}{k-1}}$ et que

$$\det(u_k)\det(u_{n-k}) = \det(u)^{\binom{n}{k}} .$$

Exercice 27. Pour $A \in \mathbf{A}^{n\times r}$ les propriétés suivantes sont équivalentes.

1. La matrice A est injective et localement simple.
2. Il existe une matrice $B \in \mathbf{A}^{r\times n}$ telle que $B\,A = \mathrm{I}_r$.
3. L'idéal déterminantiel $\mathcal{D}_r(A) = \langle 1\rangle$.

Indication : voir les théorèmes 5.14, 5.22 et 5.26.

Exercice 28. Traiter le cas général dans la démonstration du lemme 5.30.

Exercice 29. Si $\mathrm{gram}_{\mathbf{A}}(\varphi,x_1,\ldots,x_n)$ est inversible, le sous-module $\mathbf{A}x_1+\cdots+\mathbf{A}x_n$ est libre avec $(x_1,\ldots,x_n)$ pour base.

Exercice 30. Soient $A \in \mathbf{A}^{m\times n}$, $B \in \mathbf{A}^{n\times p}$, et r, s avec $r + s > n$.

1. Si $AB = 0$ alors $\mathcal{D}_r(A)\mathcal{D}_s(B) = 0$.
2. En général, $\mathcal{D}_r(A)\mathcal{D}_s(B) \subseteq \mathcal{D}_1(AB)$.
3. Plus généralement, si $r + s \geqslant n + q$, alors pour tout mineur μ d'ordre r de A on a l'inclusion $\mu^q\mathcal{D}_s(B) \subseteq \mathcal{D}_q(AB)$.

Exercice 31. On considère un $\mathbf{A}$-module M et deux sous-$\mathbf{A}$-modules N_1 et N_2. On a une suite exacte courte :

$$0 \longrightarrow N_1 \cap N_2 \xrightarrow{\ j\ } N_1 \times N_2 \xrightarrow{\ \pi\ } N_1 + N_2 \longrightarrow 0 ,$$

avec $j(x) = (x, -x)$ et $\pi(y, z) = y + z$.

1. Qu'est-ce que cela donne en termes de dimensions d'espaces vectoriels lorsque $\mathbf{A}$ est un corps discret et M un espace vectoriel de dimension finie ?
2. Étudier la signification du caractère scindé de cette suite exacte.

Exercice 32. On considère un $\mathbf{A}$-module M et deux sous-$\mathbf{A}$-modules N_1 et N_2. On définit un complexe comme suit :

$$0 \longrightarrow M/(N_1 \cap N_2) \xrightarrow{\ j\ } M/N_1 \times M/N_2 \xrightarrow{\ \pi\ } M/(N_1 + N_2) \longrightarrow 0 ,$$

avec $j(\widehat{x}) = (\widetilde{x}, \overset{\circ}{-x})$ et $\pi(\widetilde{y}, \overset{\circ}{z}) = \overline{y + z}$.

1. Montrer qu'il s'agit d'une suite exacte.
2. Qu'est-ce que cela donne en termes de dimensions d'espaces vectoriels lorsque $\mathbf{A}$ est un corps discret et M un espace vectoriel de dimension finie ?
3. Donner des exemples où cette suite exacte est scindée et d'autres où elle ne l'est pas.

Exercice 33. On considère deux sous-modules E et F' d'un $\mathbf{A}$-module F.
On note $E' = E \cap F'$, $G = F/E$, $G' = F'/E'$, $S = E+F'$, $E'' = E/E'$, $F'' = F/F'$ et $G'' = F/S$.

1. Montrer que l'on a un diagramme commutatif comme ci-dessous dans lequel
   — ι, ι', ι_E et ι_F sont les injections canoniques ;
   — π, π', π_E et π_F sont les surjections canoniques ;
   — et toutes les suites horizontales et verticales sont exactes.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E' & \xrightarrow{\iota'} & F' & \xrightarrow{\pi'} & G' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \iota_E} & & \downarrow{\scriptstyle \iota_F} & & \downarrow{\scriptstyle \iota_G} & & \\
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_E} & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \pi_G} & & \\
0 & \longrightarrow & E'' & \xrightarrow[\iota'']{} & F'' & \xrightarrow[\pi'']{} & G'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

   Faites le lien avec les théorèmes de Noether concernant les quotients de sous-modules.
2. Le diagramme construit est-il le seul diagramme commutatif satisfaisant les conditions requises au point *1* ?

Exercice 34

1. On considère un diagramme commutatif comme ci-dessous dans lequel toutes les suites horizontales et verticales sont supposées exactes

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & E_0 & \xrightarrow{\iota_0} & F' & \xrightarrow{\pi_0} & G_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \jmath_E} & & \downarrow{\scriptstyle \iota_F} & & & & \\
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0.
\end{array}$$

   À isomorphismes et renommages près, on peut supposer que E, F' et E_0 sont des sous-modules de F et que toutes les injections et surjections sont canoniques (donc $G_0 = F'/E_0$ et $G = F/E$). Nous le supposons désormais et nous notons $E' = E \cap F'$.
   a. Montrer qu'il existe une unique application linéaire $\jmath_G : G_0 \to G$ qui rend le diagramme commutatif (i.e., telle que $\jmath_G \circ \pi_0 = \pi \circ \iota_F$).

b. Montrer que l'image de $\jmath_G$ est le sous-module $(E + F')/E = S/E$ de $G = F/E$.

c. Montrer que $\jmath_G$ est injective si, et seulement si, $E_0 = E'$. Dans ce cas $\jmath_G$ réalise un isomorphisme de F'/E' sur S/E. Et l'on est ramené à la situation de l'exercice 33.

2. On étudie maintenant la situation « duale » de celle du point *1.*
Précisément, on suppose que l'on a un diagramme commutatif comme ci-dessous dans lequel les suites horizontales et verticales sont exactes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \theta_G} & & \\
0 & \longrightarrow & E_3 & \xrightarrow[\iota_3]{} & F'' & \xrightarrow[\pi_3]{} & G_3 & \longrightarrow & 0. \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

À isomorphisme et renommage près, on peut supposer que E est un sous-module de F et que l'injection ι est canonique. Nous le supposons désormais et nous notons $F' = \operatorname{Ker} \pi_F$.
Notons S_3 le noyau de l'application linéaire $\theta_G \circ \pi = \pi_3 \circ \pi_F$. On a donc une inclusion $S_3 \supseteq \operatorname{Ker} \pi + \operatorname{Ker} \pi_F = E + F'$.

a. Montrer qu'il existe une unique application linéaire $\beta : E \to E_3$ qui rend le diagramme commutatif (i.e., telle que $\iota_3 \circ \beta = \pi_F \circ \iota$).

b. Montrer que $\operatorname{Ker} \beta = E \cap F'$.

c. Montrer que β est surjective si, et seulement si, $S_3 = E + F'$.
Préciser dans ce cas en quoi on retrouve la situation correspondant à l'exercice 33.

Exercice 35. On suppose que dans le diagramme commutatif ci-dessous, les suites verticales sont exactes, et que la suite $0 \to E \to F \to G \to 0$ est exacte.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1 & \xrightarrow{\iota_1} & F_1 & \xrightarrow{\pi_1} & G_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \iota_E} & & \downarrow{\scriptstyle \iota_F} & & \downarrow{\scriptstyle \iota_G} & & \\
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_E} & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \pi_G} & & \\
0 & \longrightarrow & E_2 & \xrightarrow[\iota_2]{} & F_2 & \xrightarrow[\pi_2]{} & G_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

1. Montrer que la suite $0 \to E_1 \to F_1 \to G_1 \to 0$ est exacte si, et seulement si, la suite $0 \to E_2 \to F_2 \to G_2 \to 0$ exacte.

2. Dans ce cas, à renommages et isomorphismes près, on retrouve le diagramme de l'exercice 33.

En particulier, si les quatre injections ι, ι_1, ι_E et ι_F sont canoniques (ce qui n'est pas restrictif), on a $E_1 = E \cap F_1$ et $\mathrm{Ker}(\pi_G \circ \pi) = E + F_1$ (donc $G_2 \simeq F/(E + F_1)$).

Exercice 36. *(Dualité exacte et endomorphisme cotransposé)*
On considère un application bilinéaire $\Psi : E \times F \to G$, où G est un $\mathbf{k}$-module libre de rang 1. On dit que Ψ *est une dualité exacte entre* E *et* F lorsque les applications linéaires correspondantes

$$E \to \mathrm{L}(F,G),\ x \mapsto \big(y \mapsto \varphi(x,y)\big) \quad \text{et} \quad F \to \mathrm{L}(E,G),\ y \mapsto \big(x \mapsto \varphi(x,y)\big)$$

sont des isomorphismes. On en déduit que $E^\star \simeq F$ et $F^\star \simeq E$.

1. Lorsque l'on a une dualité exacte Ψ entre E et F, pour tout $\varphi \in \mathrm{End}(F)$ on a une Ψ-transposée $\varphi^{\star\Psi} : E \to E$ qui est l'unique application $\mathbf{k}$-linéaire satisfaisant

$$\Psi\big(\varphi^{\star\Psi}(x), y\big) = \Psi\big(x, \varphi(y)\big), \quad \text{pour tous } x \in E \text{ et } y \in F.$$

On a comme pour la transposition usuelle $\varphi_1^{\star\Psi} \circ \varphi_2^{\star\Psi} = (\varphi_2 \circ \varphi_1)^{\star\Psi}$. Et aussi, avec la définition symétrique et une notation légèrement ambivalente $(\varphi^{\star\Psi})^{\star\Psi} = \varphi$.

2. Soit E un $\mathbf{k}$-module libre de rang n et $k \in [\![1..n-1]\!]$.
Montrer qu'une dualité exacte entre $\bigwedge^k E$ et $\bigwedge^{n-k} E$ est donnée par

$$\Psi_k : \bigwedge^k E \times \bigwedge^{n-k} E \longrightarrow \bigwedge^n E, \quad (x,y) \longmapsto x \wedge y.$$

Montrer aussi que le cotransposé d'un endomorphisme $\varphi \in \mathrm{L}_{\mathbf{k}}(E)$ au sens usuel est égal à $\big(\bigwedge^{n-1} \varphi\big)^{\star\Psi_1}$. Ainsi, est expliqué le fait que la matrice de $\widetilde{\varphi}$ sur une base donnée est la transposée de la matrice des cofacteurs. Cela donne aussi une « bonne » raison pour laquelle l'endomorphisme cotransposé est intrinsèque.

Problème 1. *(Pivot de Gauss, $A\,B\,A = A$, et rationalité linéaire)*
Soit $\mathbf{K}$ un corps discret. Si $x \in \mathbf{K}^n$ est un vecteur non nul, son *indice pivot* i est le plus petit indice i tel que $x_i \neq 0$. On dit que le coefficient x_i est le *pivot* de x. La *hauteur* $h(x)$ de x est l'entier $n - i + 1$ et l'on convient que $h(0) = 0$.

Par exemple, pour $n = 4$ et $x = \begin{bmatrix} 0 \\ 1 \\ * \\ * \end{bmatrix}$, l'indice pivot de x est $i = 2$, et $h(x) = 3$.

Les notions d'échelonnement qui suivent sont relatives à cette hauteur h.

On dit qu'une matrice $A \in \mathbb{M}_{n,m}(\mathbf{K})$ est *échelonnée en colonnes* si les colonnes non nulles de A ont des hauteurs distinctes ; on dit qu'elle est *strictement échelonnée* si de plus les lignes passant par les indices pivot sont des vecteurs de la base canonique de $\mathbf{K}^m$ (ces vecteurs sont nécessairement distincts).

Voici une matrice strictement échelonnée (0 a été remplacé par un point) :

$$\begin{bmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & a_{24} & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & a_{43} & a_{44} & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ a_{71} & a_{72} & a_{73} & a_{74} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{91} & a_{92} & a_{93} & a_{94} & a_{95} & \cdot \end{bmatrix}.$$

1. Soit $A \in \mathbb{M}_{n,m}(\mathbf{K})$ strictement échelonnée ; on définit $\overline{A} \in \mathbb{M}_{n,m}(\mathbf{K})$ en annulant les coefficients non pivots (les a_{ij} dans l'exemple ci-dessus) et $B = {}^{\mathrm{t}}\overline{A} \in \mathbb{M}_{m,n}(\mathbf{K})$. Vérifier que $ABA = A$.
Décrire les projecteurs AB, BA et la décomposition $\mathbf{K}^n = \operatorname{Im} AB \oplus \operatorname{Ker} AB$.

2. Soit $A \in \mathbb{M}_{n,m}(\mathbf{K})$ une matrice quelconque. Comment obtenir $Q \in \mathbb{GL}_m(\mathbf{K})$ telle que $A' = AQ$ soit strictement échelonnée ? Comment calculer $B \in \mathbb{M}_{m,n}(\mathbf{K})$ vérifiant $ABA = A$?

3. Soient $A \in \mathbb{M}_{n,m}(\mathbf{K})$ et $y \in \mathbf{K}^n$. On suppose que le système linéaire $Ax = y$ admet une solution x sur un sur-anneau de $\mathbf{K}$. Montrer qu'il admet une solution sur $\mathbf{K}$.

4. Soient $\mathbf{K}_0 \subseteq \mathbf{K}$ un sous-corps et E, F deux sous-espaces vectoriels supplémentaires de $\mathbf{K}^n$. On suppose que E et F sont engendrés par des vecteurs à composantes dans $\mathbf{K}_0$. Montrer que $\mathbf{K}_0^n = (E \cap \mathbf{K}_0^n) \oplus (F \cap \mathbf{K}_0^n)$.

Soit $E \subseteq \mathbf{K}^n$ un sous-$\mathbf{K}$-espace vectoriel. On dit que E *est* $\mathbf{K}_0$*-rationnel* s'il est engendré par des vecteurs à composantes dans $\mathbf{K}_0$.

5. Soit F un supplémentaire de E dans $\mathbf{K}^n$ engendré par des vecteurs de la base canonique de $\mathbf{K}^n$: $\mathbf{K}^n = E \oplus F$ et $\pi : \mathbf{K}^n \twoheadrightarrow E$ la projection associée.

a. Montrer que E est $\mathbf{K}_0$-rationnel si, et seulement si, $\pi(e_j) \in \mathbf{K}_0^n$ pour tout vecteur e_j de la base canonique.

b. En déduire l'existence d'un plus petit corps de rationalité pour E.

c. Quel est le corps de rationalité de l'image dans $\mathbf{K}^n$ d'une matrice strictement échelonnée en colonnes ?

Problème 2

1. Algorithme de factorisation partielle. Étant donnés deux entiers a et b montrer que l'on peut calculer « rapidement » une famille finie d'entiers positifs p_i premiers entre eux deux à deux tels que $a = \pm\prod_{i=1}^n p_i^{\alpha_i}$ et $b = \pm\prod_{i=1}^n p_i^{\beta_i}$.

2. On considère un système linéaire $AX = B$ dans $\mathbb{Z}$ qui admet une infinité de solutions dans $\mathbb{Q}^m$. Pour savoir s'il admet une solution dans $\mathbb{Z}^m$ on peut essayer une méthode locale-globale. On commence par déterminer une solution dans $\mathbb{Q}$, qui est un vecteur $X \in \mathbb{Q}^m$. On trouve un entier d tel que $dX \in \mathbb{Z}^m$, de sorte que X est à coefficients dans $\mathbb{Z}[1/d]$. Il suffit ensuite de construire une solution dans chaque localisé $\mathbb{Z}_{1+p\mathbb{Z}}$ pour les p premiers qui divisent d et d'appliquer le principe local-global concret 2.3.

Pour savoir s'il y a une solution dans $\mathbb{Z}_{1+p\mathbb{Z}}$ et en construire une, on peut utiliser la méthode du pivot, à condition de prendre pour pivot un élément de la matrice (ou plutôt de la partie restant à traiter de la matrice) qui divise tous les autres coefficients, c'est-à-dire un coefficient dans lequel p figure avec un exposant minimum. L'inconvénient de cette méthode est qu'elle nécessite de factoriser d, ce qui peut la rendre impraticable.
Cependant, on peut légèrement modifier la méthode de façon à ne pas avoir à factoriser complètement d. On utilisera l'algorithme de factorisation partielle. On commence par faire comme si d était un nombre premier. Plus précisément on travaille avec l'anneau $\mathbb{Z}_{1+d\mathbb{Z}}$. On cherche si un coefficient de la matrice est étranger à d. Si l'on en trouve un, on le choisit comme pivot. Dans le cas contraire aucun coefficient de la matrice n'est étranger à d et (en utilisant si nécessaire l'algorithme de factorisation partielle) on est dans l'un des trois cas suivants :

- l'entier d divise tous les coefficients de la matrice, auquel cas, ou bien il divise aussi les coefficients de B et l'on est ramené à un problème plus simple, ou bien il ne divise pas un coefficient de B et le système linéaire n'admet pas de solution ;
- l'entier d s'écrit sous forme d'un produit de facteurs deux à deux étrangers $d = d_1 \cdots d_k$ avec $k \geqslant 2$, auquel cas on peut travailler ensuite avec les localisations en les monoïdes $(1 + d_1\mathbb{Z})$, …, $(1 + d_k\mathbb{Z})$;
- l'entier d s'écrit comme une puissance pure d'un d' divisant d, ce qui nous ramène, avec d' à la place de d, à un problème du même type mais plus simple.

Vérifier que l'on peut exploiter récursivement l'idée exprimée ci-dessus. Écrire un algorithme et l'expérimenter. Examiner si l'algorithme obtenu s'exécute en temps raisonnable.

Quelques solutions, ou esquisses de solutions

Exercice 2. *1.* On suppose sans perte de généralité $a_0 = b_0 = 1$. Lorsque l'on écrit que $fg = 1$, il vient

$$0 = a_n b_m,\ 0 = a_n b_{m-1} + a_{n-1} b_m, \quad 0 = a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m,$$

et ainsi de suite jusqu'au degré 1.
On montre alors par récurrence sur j que $\deg(a_n^j g) \leqslant m - j$.
En particulier, pour $j = m + 1$, on obtient $\deg(a_n^{m+1} g) \leqslant -1$, i.e. $a_n^{m+1} g = 0$. D'où, $a_n^{m+1} = 0$. Enfin en raisonnant modulo $\mathrm{D}_{\mathbf{B}}(0)$, on obtient a_j nilpotent successivement pour $j = n - 1$, …, 1.

2a. On considère les polynômes sur l'anneau commutatif $\mathbf{B}[A]$:

$$f(T) = \det(\mathrm{I}_n - TA) \ \text{ et } \ g(T) = \det(\mathrm{I}_n + TA + T^2A^2 + \cdots + T^{e-1}A^{e-1}).$$

On a $f(T)g(T) = \det(\mathrm{I}_n - T^e A^e) = 1$. Le coefficient de degré $n-i$ de f est $\pm a_i$. On applique *1.*

2b. Il suffit de montrer que $\mathrm{Tr}(A)^{(e-1)n+1} = 0$, car $a_i = \pm \mathrm{Tr}\left(\bigwedge^{n-i}(A)\right)$.
On considère le déterminant défini par rapport à une base fixée $\mathcal{B}$ de $\mathbf{A}^n$. Si l'on prend la base canonique formée par les e_i, on a une égalité évidente

$$\mathrm{Tr}(f) = \det_{\mathcal{B}}(f(e_1), e_2, \dots, e_n) + \cdots + \det_{\mathcal{B}}\left(e_1, e_2, \dots, f(e_n)\right).$$

Elle peut être vue sous la forme suivante :

$$\mathrm{Tr}(f)\det_{\mathcal{B}}(e_1,\dots,e_n) = \det_{\mathcal{B}}(f(e_1),e_2,\dots,e_n) + \cdots + \det_{\mathcal{B}}\left(e_1,e_2,\dots,f(e_n)\right).$$

Sous cette forme on peut remplacer les e_i par n'importe quel système de n vecteurs de $\mathbf{A}^n$: les deux membres sont des formes n-linéaires alternées (en les e_i) sur $\mathbf{A}^n$, donc sont égales parce qu'elles coïncident sur une base.
Ainsi, multiplier un déterminant par $\mathrm{Tr}(f)$ revient à le remplacer par une somme de déterminants dans lesquels on a fait opérer f sur chacun des vecteurs.
On en déduit que l'expression $\mathrm{Tr}(f)^{n(e-1)+1}\det_{\mathcal{B}}(e_1,\dots,e_n)$ est égale à une somme dont chaque terme est un déterminant de la forme

$$\det_{\mathcal{B}}\left(f^{m_1}(e_1), f^{m_2}(e_2), \dots, , f^{m_n}(e_n)\right),$$

avec $\sum_i m_i = n(e-1)+1$, donc au moins l'un des exposants m_i est $\geqslant e$.

Remarque. Cette solution pour la borne $n(e-1)+1$ est due à Gert Almkvist. Voir à ce sujet : Zeilberger D. *Gert Almkvist's generalization of a mistake of Bourbaki.* Contemporary Mathematics **143** (1993), p. 609–612. ∎

Exercice 3. *1.* Posons $\mathfrak{a} = \langle x_1, \dots, x_n\rangle$. On obtient $s^r \in \mathfrak{a}$ (pour un certain r), et $1 - as \in \mathfrak{a}$ (pour un certain a). On écrit $1 = a^r s^r + (1-as)(1+as+\cdots) \in \mathfrak{a}$.
2. $\mathfrak{a}+\mathfrak{b} = \langle 1\rangle$, $\mathfrak{a}+\mathfrak{c} = \langle 1\rangle$ et $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{c}) \subseteq \mathfrak{a}+\mathfrak{bc}$, donc $\mathfrak{a}+\mathfrak{bc} = \langle 1\rangle$.

Exercice 4. *1.* Puisque f est homogène, on a $f(tx) = 0$ pour une nouvelle indéterminée t. D'où, des $U_i \in \mathbf{A}[X_1, \dots, X_n, t]$ tels que $f = \sum_{i=1}^n (X_i - tx_i)U_i$.
En faisant $t := x_1^{-1}X_1$, on obtient des $v_i \in \mathbf{A}[X_1, \dots, X_n]$ tels que

$$f = \textstyle\sum_{i=2}^n (x_1X_i - x_iX_1)v_i.$$

Enfin, puisque f est homogène de degré d, on peut remplacer v_i par sa composante homogène de degré $d-1$.
2. Considérons l'égalité $f = \sum_{k,j}(x_kX_j - x_jX_k)u_{kj}$, où les u_{kj} sont des polynômes homogènes de degré $d-1$. Il s'agit d'un système linéaire en les coefficients des u_{kj}. Puisque ce système admet une solution sur chaque localisé $\mathbf{A}_{x_i}$ et que les x_i sont comaximaux, il admet une solution sur $\mathbf{A}$.
3. Si $F = \sum_d F_d$ est la décomposition de $F \in \mathbf{A}[X_1, \dots, X_n]$ en composantes homogènes, on a $F(tx) = 0$ si, et seulement si, $F_d(x) = 0$ pour tout d, d'où le premier point de la question. Pour la saturation, montrons que si $X_iF \in I_x$ pour tout i, alors $F \in I_x$. Or, on a $x_iF(tx) = 0$ donc, par comaximalité des x_i, on obtient $F(tx) = 0$, i.e. $F \in I_x$.

Exercice 6. Le polynôme Q, vu comme un polynôme à coefficients dans $\mathbf{B}'$, reste primitif donc régulier (Gauss-Joyal, point 2 du lemme 2.6). Puisque m_Q est injective, son déterminant $\det(m_Q) = P \in \mathbf{A}'[\underline{X}]$ est régulier (théorème 5.22, point *2*). Mais P est également nul dans $\mathbf{A}'[\underline{X}]$. Donc, $\mathbf{A}'$ est l'anneau nul, autrement dit $1 \in \mathrm{c}_{\mathbf{A}}(P)$.

Exercice 7. La condition est évidement nécessaire. Supposons qu'elle est satisfaite et soient $b, b_1, \dots, b_n \in \mathbf{A}$. On considère le module des syzygies pour $(b, b_1, \dots, b_n)$, c'est l'image d'une matrice $M \in \mathrm{Mat}_{n+1,p}(\mathbf{A})$. Alors, $b \in \langle b_1, \dots, b_n\rangle$ si, et seulement si, les coefficients de la première ligne de M sont comaximaux.

Exercice 9. Soit $f(X)$ un idempotent de $\mathbf{A}[X]$. Il est clair que $e = f(0)$ est idempotent. On veut montrer que $f = e$. Pour cela on peut raisonner séparément modulo e et modulo $1 - e$.
Si $e = 0$, alors $f = Xg$. On a $(Xg)(1-Xg) = 0$, or $1-Xg$ est régulier, donc $g = 0$.
Si $e = 1$, on considère l'idempotent $1 - f$ et l'on est ramené au cas précédent.

Exercice 10. Pour la question *5* on montre d'abord le résultat lorsque $uv = 0$. Dans la situation générale, on note $u' = 1 - u$ et $v' = 1 - v$. On a alors un système fondamental d'idempotents orthogonaux $(uv, uv', u'v, u'v')$ et en appliquant le cas particulier précédent on voit que les deux anneaux sont isomorphes au produit $\mathbf{A}/\langle uv'\rangle \times (\mathbf{A}/\langle uv\rangle)^2 \times \mathbf{A}/\langle u'v\rangle$.

Exercice 11. *2.* On a $\mathbf{K}[1/e_i] \simeq \mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ et $\mathrm{Ann}_{\mathbf{K}}(e_i) = \mathrm{Ann}_{\mathbf{A}}(a_i)\mathbf{K}$. Pour un élément x de $\mathbf{A}$, on écrit $dx = \sum_{i\in[\![1..n]\!]} x_i$ dans $\mathbf{K}$, avec $x_i = e_i dx = a_i x$. La décomposition est donc entièrement dans $\mathbf{A}$. Et $dx \equiv x_i \bmod \mathrm{Ann}_{\mathbf{A}}(a_i)$, donc la composante $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ du produit, quand on la voit comme l'idéal $e_i\mathbf{K}$, est formée des éléments de la forme $a_i x/y$ avec $x \in \mathbf{A}$ et y régulier dans $\mathbf{A}$. Mais y est régulier dans $\mathbf{A}$ si, et seulement si, chaque $y_i = a_i y$ est régulier modulo $\mathrm{Ann}_{\mathbf{A}}(a_i)$, de sorte $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ s'identifie à $\mathrm{Frac}\big(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\big)$.

Exercice 12. *1.* Les zéros de $\mathbf{A}$ sont les trois « axes de coordonnées ».
Tout élément de $\mathbf{A}$ s'écrit de manière unique sous forme

$$u = a + xf(x) + yg(y) + zh(z),$$

avec f, g, $h \in \mathbb{Q}[T]$. Cela implique que $x + y + z$ est régulier car

$$(x + y + z)u = x\big(a + xf(x)\big) + y\big(a + yg(y)\big) + z\big(a + zh(z)\big).$$

Donc, les éléments $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ et $\dfrac{z}{x+y+z}$ forment un système fondamental d'idempotents orthogonaux de $\mathbf{K}$. On conclut avec l'exercice 11 en notant que $\mathrm{Ann}_{\mathbf{A}}(x) = \langle y, z\rangle$, et donc que

$$\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(x) \simeq \mathbb{Q}[X].$$

2. Les zéros de $\mathbf{B}$ sont les trois « plans de coordonnées ». Le système fondamental d'idempotents orthogonaux dans $\mathbf{L}$ est donné par $\dfrac{uv}{uv+vw+wu}$, $\dfrac{vw}{uv+vw+wu}$ et $\dfrac{wu}{uv+vw+wu}$.

Exercice 13. Il suffit de résoudre la question modulo a et modulo $1-a$.
Modulo a : $\left[\begin{array}{c} a \\ b \end{array}\right] = \left[\begin{array}{c} 0 \\ b \end{array}\right] \mapsto \left[\begin{array}{c} b \\ b \end{array}\right] \mapsto \left[\begin{array}{c} b \\ 0 \end{array}\right]$.
Modulo $1-a$, $\left[\begin{array}{c} a \\ b \end{array}\right] = \left[\begin{array}{c} 1 \\ b \end{array}\right] \mapsto \left[\begin{array}{c} 1 \\ 0 \end{array}\right]$. En recollant : $d = (1-a)b + a$ avec par exemple la matrice $A = A_2A_1$, où

$$A_1 = (1-a)\left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right] + a\left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right] = \left[\begin{array}{cc} 1 & 1-a \\ 0 & 1 \end{array}\right],$$

$$A_2 = (1-a)\left[\begin{array}{cc} 1 & 0 \\ -1 & 1 \end{array}\right] + a\left[\begin{array}{cc} 1 & 0 \\ -b & 1 \end{array}\right] = \left[\begin{array}{cc} 1 & 0 \\ a-ab-1 & 1 \end{array}\right] \quad \text{et}$$

$$A = \left[\begin{array}{cc} 1 & 1-a \\ a-ab-1 & a \end{array}\right].$$

Exercice 14. *1* et *2.* Cas $m = 2$. On a par manipulations élémentaires avec

$$e_1 = r_1 \vee r_2 = r_1 + s_1r_2 = r_2 + s_2r_1,$$

en notant que $e_1r_2 = r_2$ et $-r_2(r_2s_1) = -r_2s_1 = r_1r_2 - r_2$.

$$\left[\begin{array}{cc} r_1 & 0 \\ 0 & r_2 \end{array}\right] \longmapsto \left[\begin{array}{cc} r_1 & 0 \\ r_2 & r_2 \end{array}\right] \longmapsto \left[\begin{array}{cc} r_1 + r_2s_1 & r_2s_1 \\ r_2 & r_2 \end{array}\right] = \left[\begin{array}{cc} e_1 & r_2s_1 \\ r_2 & r_2 \end{array}\right]$$
$$\longmapsto \left[\begin{array}{cc} e_1 & 0 \\ 0 & r_1r_2 \end{array}\right].$$

En outre, en posant $f = r_2s_1$, $e = 1-f$ et $P = \left[\begin{array}{cc} e & f \\ f & e \end{array}\right]$, on a $P^2 = \mathrm{I}_2$, $er_1 = r_1$ et $er_2 = r_1r_2$. Finalement,

$$P\left[\begin{array}{cc} r_1 & 0 \\ 0 & r_2 \end{array}\right]P = \left[\begin{array}{cc} er_1 & fr_2 \\ fr_1 & er_2 \end{array}\right]P = \left[\begin{array}{cc} r_1 & f \\ 0 & r_1r_2 \end{array}\right]\left[\begin{array}{cc} e & f \\ f & e \end{array}\right]$$
$$= \left[\begin{array}{cc} r_1e + f & 0 \\ 0 & r_1r_2e \end{array}\right] = \left[\begin{array}{cc} e_1 & 0 \\ 0 & r_1r_2 \end{array}\right].$$

Exercice 15. On pose $\mathfrak{b}_i = \prod_{j:j\neq i} \mathfrak{a}_j$. On note $\varphi : \mathbf{A} \to \prod_{k=1}^n \mathbf{A}/\mathfrak{a}_k$ l'application canonique. Écrivons $a_{ij} + a_{ji} = 1$ pour $i \neq j$ avec $a_{ij} \in \mathfrak{a}_i$, $a_{ji} \in \mathfrak{a}_j$. On écrit

$$1 = \prod\nolimits_{k:k\neq i}(a_{ik} + a_{ki}) = \big(\prod\nolimits_{k:k\neq i} a_{ki}\big) + b_i = e_i + b_i, \qquad (\#)$$

avec $b_i \in \mathfrak{a}_i$ et $e_i \in \mathfrak{b}_i$, donc

$$e_i \equiv 0 \bmod \mathfrak{b}_i \quad \text{et} \quad e_i \equiv 1 \bmod \mathfrak{a}_i. \qquad (+)$$

En conséquence, pour $x_1, \ldots, x_n \in \mathbf{A}$

$$\varphi\big(\sum\nolimits_{i=1}^n e_ix_i\big) = (x_1 \bmod \mathfrak{a}_1, \ldots, x_n \bmod \mathfrak{a}_n),$$

ce qui montre que φ est surjective.

Le théorème de factorisation donne alors l'isomorphisme $\theta : \mathbf{A}/\mathfrak{a} \to \prod_i \mathbf{A}/\mathfrak{a}_i$ car on a évidemment $\operatorname{Ker}\varphi = \bigcap_{k=1}^n \mathfrak{a}_k = \mathfrak{a}$. Les congurences $(+)$ montrent que les $\pi(e_i) \in \mathbf{A}/\mathfrak{a}$ donnent par θ le système fondamental d'idempotents orthogonaux associé à la structure de produit $\prod_i \mathbf{A}/\mathfrak{a}_i$. Vus dans ce produit, les éléments de $\mathfrak{a}_1$ sont ceux dont la première coordonnée est nulle : ils forment donc bien l'idéal engendré par $\varphi(1-e_1)$. Autrement dit, on obtient $\pi(\mathfrak{a}_1) = \pi(\langle 1-e_1\rangle)$ en remontant dans $\mathbf{A}/\mathfrak{a}$, et $\mathfrak{a}_1 = \mathfrak{a} + \langle 1-e_1\rangle$ en remontant dans $\mathbf{A}$.
L'égalité $\bigcap_{k=1}^n \mathfrak{a}_k = \prod_{k=1}^n \mathfrak{a}_k$ se démontre par récurrence sur n pour $n \geqslant 2$ en notant que $(\#)$ implique que $\mathfrak{a}_i$ et $\mathfrak{b}_i$ sont comaximaux. Voyons l'initialisation, c'est-à-dire le cas $n = 2$: si $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ et si $a + b = 1$ avec $a \in \mathfrak{a}_1$ et $b \in \mathfrak{a}_2$, alors $x = ax + bx$, avec $ax \in \mathfrak{a}_1\mathfrak{a}_2$ parce que $x \in \mathfrak{a}_2$ et $bx \in \mathfrak{a}_1\mathfrak{a}_2$ parce que $x \in \mathfrak{a}_1$, donc $x \in \mathfrak{a}_1\mathfrak{a}_2$.

Exercice 18. Pour $q = 0$, la matrice $D_0 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ transforme $\begin{bmatrix} x \\ y \end{bmatrix}$ en $\begin{bmatrix} -y \\ x \end{bmatrix}$, donc $D_0^2 = -\mathrm{I}_2$ et $D_0^3 = -D_0 = D_0^{-1}$.
On a aussi $D_0 = \mathrm{E}_{12}(1)\mathrm{E}_{21}(-1)\mathrm{E}_{12}(1)$, $D_0 D_q = -\mathrm{E}_{12}(q)$ et $D_q D_0 = -\mathrm{E}_{21}(q)$.

Exercice 21. Notons $(e_1, \dots, e_n)$ la base canonique de $\mathbf{A}^n$ et $(f_1, \dots, f_n)$ les n colonnes de F. On peut supposer que le mineur principal inversible est en position nord-ouest de sorte que $(f_1, \dots, f_k, e_{k+1}, \dots, e_n)$ est une base de $\mathbf{A}^n$.
Puisque $F(f_j) = f_j$, la matrice de F dans cette base est $G \overset{\text{def}}{=} \begin{bmatrix} \mathrm{I}_k & * \\ 0 & * \end{bmatrix}$.
La matrice G est idempotente ainsi que sa transposée G'. On applique au projecteur G' l'opération que l'on vient de faire subir à F.
Puisque $G'(e_j) \in \bigoplus_{i \geqslant k+1} \mathbf{A}e_i$ pour $j \geqslant k+1$, la matrice de G' dans la nouvelle base est de la forme $H = \begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & * \end{bmatrix}$, d'où le résultat car F est semblable à ${}^{\mathrm{t}}H$.

Exercice 22. On a des $b_{ji} \in \mathbf{A}$ tels que $1 = \sum_{i,j} b_{ji}a_{ij}$. Soit $B \in \mathbf{A}^{m\times n}$ définie par $B = (b_{ji})$. Vérifions que $ABA = A$: $(ABA)_{ij} = \sum_{l,k} a_{il}b_{lk}a_{kj}$.
Mais $\begin{vmatrix} a_{il} & a_{ij} \\ a_{kl} & a_{kj} \end{vmatrix} = 0$, donc $(ABA)_{ij} = \sum_{l,k} a_{ij}a_{kl}b_{lk} = a_{ij}\sum_{l,k} a_{kl}b_{lk} = a_{ij}$. En conséquence, AB est un projecteur.
Montrons que AB est de rang 1. On a $\operatorname{Tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij}b_{ji} = 1$, donc $\mathcal{D}_1(AB) = 1$. Par ailleurs, $\mathcal{D}_2(AB) \subseteq \mathcal{D}_2(A) = 0$.

Exercice 23. *1.* Fixons une forme linéaire μ. L'application $E^{r+1} \to \mathbf{A}$ définie par
$$(y_0, \dots, y_r) \mapsto \textstyle\sum_{i=0}^r (-1)^i f(y_0, \dots, y_{i-1}, \widehat{y_i}, y_{i+1}, \dots, y_r)\, \mu(y_i),$$
où $\widehat{y_i}$ symbole de l'omission de l'élément, est une forme $(r+1)$-linéaire alternée.
D'après l'hypothèse $\bigwedge_{r+1}(x_1, \dots, x_n) = 0$ et l'injectivité de $E \mapsto E^{\star\star}$, on obtient
$$\textstyle\sum_{i=0}^r (-1)^i f(y_0, \dots, y_{i-1}, \widehat{y_i}, y_{i+1}, \dots, y_r)\, y_i = 0.$$
Notons y au lieu de y_0 et réalisons l'opération suivante : dans l'expression
$$(-1)^i f(y, \dots, y_{i-1}, \widehat{y_i}, y_{i+1}, \dots, y_r),$$
amenons y entre y_{i-1} et y_i. La permutation ainsi réalisée nécessite une multiplication par $(-1)^{i-1}$.
On obtient alors la deuxième égalité dans laquelle tous les signes « ont disparu ».

Par exemple avec $r = 4$, l'expression

$$\begin{aligned} f(\widehat{y}, y_1, y_2, y_3, y_4)y \;&-\; f(y, \widehat{y_1}, y_2, y_3, y_4)y_1 + f(y, y_1, \widehat{y_2}, y_3, y_4)y_2 \\ &-\; f(y, y_1, y_2, \widehat{y_3}, y_4)y_3 + f(y, y_1, y_2, y_3, \widehat{y_4})y_4 \\ = f(y_1, y_2, y_3, y_4)y \;&-\; f(y, y_2, y_3, y_4)y_1 + f(y, y_1, y_3, y_4)y_2 \\ &-\; f(y, y_1, y_2, y_4)y_3 + f(y, y_1, y_2, y_3)y_4 \end{aligned}$$

n'est autre que

$$\begin{aligned} f(y_1, y_2, y_3, y_4)y \;&-\; f(y, y_2, y_3, y_4)y_1 - f(y_1, y, y_3, y_4)y_2 \\ &-\; f(y_1, y_2, y, y_4)y_3 - f(y_1, y_2, y_3, y)y_4. \end{aligned}$$

Une preuve plus expéditive : on applique une forme linéaire μ à la dernière expression ci-dessus, on vérifie que l'application obtenue $(y, y_1, y_2, y_3, y_4) \mapsto \mu(\ldots)$ est 5-linéaire alternée donc nulle d'après les hypothèses.

2. Traitons le cas $r = 3$. On a une hypothèse

$$1 = \sum\nolimits_{ijk} \alpha_{ijk} f_{ijk}(x_i, x_j, x_k), \qquad f_{ijk} \text{ 3-linéaire alternée sur } E.$$

On définit $\pi : E \to E$ par :

$$\pi(x) = \sum\nolimits_{ijk} \alpha_{ijk}[f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k].$$

Il est clair que l'image de p est contenue dans le sous-module $\sum \mathbf{A}x_i$. De plus, pour $x \in \sum \mathbf{A}x_i$, on a

$$f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k = f_{ijk}(x_i, x_j, x_k)x.$$

D'où, $\pi(x) = x$: l'endomorphisme $\pi : E \to E$ est un projecteur d'image $\sum \mathbf{A}x_i$. On voit que p est de la forme $\pi(x) = \sum_i \alpha_i(x)x_i$ i.e. $\pi = \psi \circ \varphi$ et que $\pi \circ \psi = \psi$.

3. Le module E en question est $\mathbf{A}^m$ et les vecteurs $x_1, \ldots, x_n$ sont les colonnes de A. On a $\psi = A : \mathbf{A}^n \to \mathbf{A}^m$, et si l'on note $B \in \mathbf{A}^{n\times m}$ la matrice de $\varphi : \mathbf{A}^m \to \mathbf{A}^n$, on a bien $ABA = A$. Alors, l'application linéaire $AB : \mathbf{A}^m \to \mathbf{A}^m$ est un projecteur de même image que A.

Exercice 26. Voyons d'abord le cas où $u = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. On dispose d'une base (e_I) de $\bigwedge^k(\mathbf{A}^n)$ indexée par les parties $I \subseteq \{1, \ldots, n\}$ de cardinal k :

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}, \qquad I = \{i_1 < \cdots < i_k\}.$$

Alors, u_k est diagonale dans la base (e_I) : $u_k(e_I) = \lambda_I e_I$ avec $\lambda_I = \prod_{i\in I} \lambda_i$. Il s'ensuit que $\det(u_k) = \prod_{\#I=k} \prod_{i\in I} \lambda_i$. Reste à déterminer, pour un j donné dans $[\![1..n]\!]$, le nombre d'occurrences de λ_j dans le produit ci-dessus. Autrement dit, combien de parties I, de cardinal k, contenant j ? Autant que de parties de cardinal $k-1$ contenues dans $\{1, \cdots, n\} \setminus \{j\}$, i.e. $\binom{n-1}{k-1}$. Le résultat est démontré pour une matrice générique. Il est vrai donc pour une matrice quelconque. Le deuxième point résulte des égalités

$$\binom{n-1}{k-1} + \binom{n-1}{n-k-1} = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Exercice 28. Le cas général se traite par récurrence sur n. On considère l'anneau de polynômes $\mathbb{Z}[(x_{ij})]$ à n^2 indéterminées et la matrice universelle $A = (x_{ij})$ à coefficients dans cet anneau. Notons $\Delta_{1k} \in \mathbb{Z}[(x_{ij})]$ le cofacteur de x_{1k} dans A. Ces cofacteurs vérifient les identités :

$$\sum\nolimits_{j=1}^{n} x_{1j}\Delta_{1j} = \det A, \qquad \sum\nolimits_{j=1}^{n} x_{ij}\Delta_{1j} = 0, \quad \text{pour } i > 1.$$

Puisque les N_{kl} commutent deux à deux, la spécialisation $x_{kl} \mapsto N_{kl}$ est légitime. Notons $N'_{1j} = \Delta_{1j}(x_{kl} \mapsto N_{kl})$, alors on a

$$N'_{11} = \textstyle\sum_{\sigma\in\mathfrak{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3} \dots N_{n\sigma_n}.$$

Définissons N' par :

$$N' = \begin{bmatrix} N'_{11} & 0 & \cdots & 0 \\ N'_{12} & \mathrm{I}_m & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ N'_{1n} & 0 & \cdots & \mathrm{I}_m \end{bmatrix}, \quad \text{d'où} \quad NN' = \begin{bmatrix} \Delta & N_{12} & \cdots & N_{1n} \\ 0 & N_{22} & \cdots & N_{2n} \\ \vdots & & & \vdots \\ 0 & N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

En prenant les déterminants, on obtient

$$\det(N)\det(N'_{11}) = \det(\Delta)\det\begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

L'hypothèse de récurrence fournit les égalités

$$\det\begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix} = \det\Big(\sum_{\sigma\in\mathfrak{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3} \cdots N_{n\sigma_n}\Big) = \det(N'_{11}).$$

La simplification par l'élément régulier $\det(N'_{11})$ donne l'égalité $\det(N) = \det(\Delta)$.

Exercice 30

1. On peut supposer $r \leqslant n$. On considère un mineur μ d'ordre r de A, sans perte de généralité on suppose la matrice carrée extraite correspondante A_1 située dans le coin nord-ouest. On écrit

$$A = \left[\begin{array}{c|c} A_1 & X \\ \hline Y & Z \end{array}\right], \quad A' = \left[\begin{array}{c|c} \widetilde{A_1} & 0 \\ \hline 0 & 0 \end{array}\right], \quad A'A = \left[\begin{array}{c|c} \mu\,\mathrm{I}_r & 0 \\ \hline 0 & 0 \end{array}\right]$$

avec $\mu = \det(A_1)$.

On partage ensuite B en $B_1 \in \mathbf{A}^{r\times p}$ et $B_2 \in \mathbf{A}^{(n-r)\times p}$

$$B = \begin{array}{|c|}\hline B_1 \\ \hline B_2 \\ \hline \end{array}, \quad A'AB = \begin{array}{|c|}\hline \mu\, B_1 \\ \hline 0 \\ \hline \end{array} = 0.$$

Un mineur ν d'ordre s de B est le déterminant d'une matrice carrée extraite C dont au moins une ligne est dans B_1. On exprime ce mineur ν au moyen d'un développement de Laplace en partageant C en deux parties, l'une correspondant aux lignes empruntées à B_1, l'autre, éventuellement vide, correspondant aux lignes empruntées à B_2. On voit que $\mu\,\nu$ est dans l'idéal engendré par les coefficients de $\mu\, B_1$, donc $\mu\,\nu = 0$. Ce qu'il fallait démontrer.

2. Il suffit d'appliquer le point *1* avec l'anneau $\mathbf{A}/\mathcal{D}_1(AB)$.

3. Supposons par exemple $r + s \geqslant n + 2$. Le même calcul que dans le point *1* donne cette fois-ci $\mu^2\,\mathcal{D}_2(B_1) = \mathcal{D}_2(\mu\, B_1) \subseteq \mathcal{D}_2(AB)$. On utilise le développement de Laplace pour exprimer $\nu = \text{dét}(C)$, la matrice C a maintenant au moins deux lignes empruntées à B_1, on obtient donc $\mu^2\,\nu \in \mathcal{D}_2(AB)$.

Exercice 31. Notez que l'on est dans le contexte usuel des théorèmes de factorisation de Noether, ici les deux sous-modules sont notés N_1 et N_2, ce qui montre mieux la symétrie de la situation.

1. Si l'anneau est un corps $\mathbf{K}$ avec

$$\dim_{\mathbf{K}}(N_i) = n_i,\ \dim_{\mathbf{K}}(N_1 + N_2) = n \text{ et } \dim_{\mathbf{K}}(N_1 \cap N_2) = n',$$

la suite exacte est automatiquement scindée (théorème de la base incomplète) et l'on obtient l'égalité classique $n + n' = n_1 + n_2$.

2. Notons $N = N_1 \cap N_2$. La suite exacte est scindée si l'on a une section

$$\sigma : N_1 + N_2 \longrightarrow N_1 \times N_2.$$

On écrit $\sigma(x_1 + x_2) = \sigma_1(x_1) + \sigma_2(x_2)$, avec $\sigma_1(x_1) = \big(x_1 - \alpha_1(x_1), \alpha_1(x_1)\big)$ $\big($en effet $\pi\big(\sigma_1(x_1)\big) = x_1\big)$ et $\sigma_2(x_2) = \big(\alpha_2(x_2), x_2 - \alpha_2(x_2)\big)$.

On a donc $\alpha_1 : N_1 \to N$ et $\alpha_2 : N_2 \to N$. L'application σ est bien définie si, et seulement si, pour tout $y \in N$, on a $\sigma_1(y) = \sigma_2(y)$, i.e. $\alpha_1(y) + \alpha_2(y) = y$.

En résumé, la suite est scindée si, et seulement si, on peut trouver $\alpha_1 : N_1 \to N$ et $\alpha_2 : N_2 \to N$ vérifiant $\alpha_1(y) + \alpha_2(y) = y$ pour $y \in N$.

Cette condition est un peu mystérieuse. Elle est satisfaite par exemple si N est facteur direct dans N_1 en prenant $\alpha_2 = 0$ et α_1 une projection de N_1 sur N. Mais en général, le critère n'est pas très parlant.

Prenons par exemple avec un anneau à pgcd $\mathbf{A}$, les sous-modules $N_1 = a_1\mathbf{A}$ et $N_2 = a_2\mathbf{A}$ du module $\mathbf{A}$. Si g est le pgcd et m le ppcm, on a $N = m\mathbf{A}$ avec $a_1 = gc_1$, $a_2 = gc_2$, $m = a_1c_2 = a_2c_1$. Pour obtenir une section il nous faut des $\alpha_i : N_i \to N$. On a alors $\alpha_1(a_1) = mx$, $\alpha_2(a_2) = my$, ce qui donne

$$\alpha_1(m) = c_2mx, \qquad \alpha_2(m) = c_1my,$$

et l'égalité $\alpha_1(m) + \alpha_2(m) = m$ signifie $c_2x + c_1y = 1$. En bref les deux éléments c_1 et c_2 premiers entre eux doivent engendrer l'idéal $\langle 1\rangle$.

Ainsi, la suite sera toujours scindée si $\mathbf{A}$ est un domaine de Bézout, mais pas toujours scindée dans le cas contraire.

Exercice 32. On étudie le complexe :

$$0 \longrightarrow M/(N_1 \cap N_2) \xrightarrow{\ j\ } M/N_1 \times M/N_2 \xrightarrow{\ \pi\ } M/(N_1 + N_2) \longrightarrow 0,$$

où $j(\widehat{x}) = (\widetilde{x}, -\overset{\circ}{x})$ et $\pi(\widetilde{y}, \overset{\circ}{z}) = \overline{y} + \overline{z}$.

1. Le complexe est exact. Tout d'abord $j(\widehat{x}) = 0$ si, et seulement si, $\widetilde{x}$ et $\overset{\circ}{x}$ sont nuls, i.e. $x \in N_1 \cap N_2$. Cela donne l'exactitude en $M/(N_1 \cap N_2)$. Ensuite, $\pi(\widetilde{y}, 0) = \overline{y}$ donc π est surjective. Cela donne l'exactitude en $M/(N_1 + N_2)$.

Soit maintenant un élément arbitraire $(\widetilde{y}, \overset{\circ}{z}) \in \operatorname{Ker}\pi$, i.e. $y + z \in N_1 + N_2$.
On écrit $y + z = y_1 + z_2$ avec $y_1 \in N_1$ et $z_2 \in N_2$, d'où $(y - y_1) = -(z - z_2)$.
Alors, $\widetilde{y} = \widetilde{y - y_1}$, $\overset{\circ}{z} = \overset{\circ}{z - z_2}$, donc $(\widetilde{y}, \overset{\circ}{z}) = j(\widehat{x})$ pour $x = y - y_1$.
Cela donne l'exactitude au milieu.

2. Si l'anneau est un corps $\mathbf{K}$ avec

$$\dim_{\mathbf{K}}(M) = m, \quad \dim_{\mathbf{K}}(N_i) = n_i, \quad \dim_{\mathbf{K}}(N_1 + N_2) = n \ \text{ et } \dim_{\mathbf{K}}(N_1 \cap N_2) = n',$$

la suite exacte est automatiquement scindée (théorème de la base incomplète) et l'on obtient $(m - n) + (m - n') = (m - n_1) + (m - n_2)$, c'est-à-dire l'égalité classique $n + n' = n_1 + n_2$.

3. On prend les mêmes modules $M = \mathbf{A}$, $N_1 = a_1\mathbf{A} \subseteq M$, $N_2 = a_2\mathbf{A} \subseteq M$ que pour la fin de la solution de l'exercice 31. On suppose que $\mathbf{A}$ est un anneau à pgcd, on reprend les mêmes notations.
Une section $\sigma : \mathbf{A}/\langle a_1, a_2\rangle \to \mathbf{A}/\langle a_1\rangle \times \mathbf{A}/\langle a_2\rangle$ est a priori donnée par deux applications linéaires $\sigma_i : \mathbf{A}/\langle a_1, a_2\rangle \to \mathbf{A}/\langle a_i\rangle$. On les définit par

$$\sigma_1(\overline{1}) = \widetilde{uc_2} \qquad \text{et} \qquad \sigma_2(\overline{1}) = \overset{\circ}{vc_1}.$$

Pour que $\pi\big(\sigma(\overline{1})\big) = \overline{1}$, il faut que $uc_2 + vc_1 \equiv 1 \bmod \langle a_1, a_1\rangle$, ce qui signifie que $\langle c_1, c_2\rangle = \langle 1\rangle$ dans $\mathbf{A}$. Ainsi, on retrouve que la suite est scindée si $\mathbf{A}$ est de Bézout, et qu'elle peut ne pas être scindée dans le cas contraire.

Exercice 33. *1.* Rappelons le diagramme que l'on souhaite : les deux premières lignes et les deux premières colonnes sont des suites exactes courtes canoniques et $G'' = F/(E + F')$

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E' & \xrightarrow{\iota'} & F' & \xrightarrow{\pi'} & G' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \iota_E} & & \downarrow{\scriptstyle \iota_F} & & \downarrow{\scriptstyle \iota_G} & & \\
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_E} & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \pi_G} & & \\
0 & \longrightarrow & E'' & \xrightarrow[\iota'']{} & F'' & \xrightarrow[\pi'']{} & G'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Le théorème de factorisation de Noether donne un isomorphisme naturel

$$G' = F'/(E \cap F') \xrightarrow{\ j\ } (E + F')/E, \ \text{ avec } (E + F')/E \subseteq F/E.$$

Cet isomorphisme est défini par $j\big(\pi'(x)\big) = \pi(x) = \pi\big(\iota_F(x)\big)$.

Cela nous dit que l'on a une application linéaire injective $\iota_G : G' \to F/E$ qui vérifie
$$\iota_G\big(\pi'(x)\big) = \pi\big(\iota_F(x)\big),$$
c'est-à-dire qui rend le diagramme commutatif.
Comme π' est surjective, ι_G est même l'unique application **A**-linéaire qui rend le diagramme commutatif.
De même, on a une unique application linéaire
$$E'' = E/(E \cap F') \xrightarrow{\iota''} F'' = F/F' ,$$
qui rend le diagramme commutatif, et ι'' est injective, d'image $(E + F')/F'$.
La surjection canonique $\theta : F \to F/(E + F')$ se factorise de manière unique via π parce que $\operatorname{Ker}\pi = E \subseteq E + F' = \operatorname{Ker}\theta$ et l'on obtient ainsi $\pi_G : G \to G''$ satisfaisant $\pi_G \circ \pi = \theta$.
On obtient de même une application linéaire surjective $\pi'' : F'' \to G''$ satisfaisant l'égalité $\pi'' \circ \pi_F = \theta$.
On a ainsi obtenu un diagramme commutatif complet. Il reste à voir que la troisième suite verticale et la troisième suite horizontale sont exactes.
Or, $\operatorname{Ker}\pi_G = \pi(\operatorname{Ker}\theta) = (E+F')/E = S/E$ et $\operatorname{Im}\iota_G = \operatorname{Im} j = S/E$. Cela montre que la suite verticale est exacte, et l'on vient de redécouvrir le théorème de Noether qui établit un isomorphisme naturel
$$G/\operatorname{Ker}\pi_G = (F/E)/(S/E) \xrightarrow{\alpha} F/S = G''$$
satisfaisant $\alpha\big(\overline{\pi(x)}\big) = \pi(x)$ pour tout $x \in F$.
Symétriquement la troisième suite horizontale est exacte.

2. On a déjà vu que la commutativité du diagramme sur les deux premières lignes (resp. colonnes) impose l'application linéaire ι_G (resp. ι''). Il nous reste à voir si l'affirmation analogue concernant π_G et π'' est correcte. On suppose que l'on a des applications linéaires λ_G et λ'' qui satisfont l'égalité $\lambda_G \circ \pi = \lambda'' \circ \pi_F$ et que toutes les lignes et colonnes sont exactes. On obtient donc $\operatorname{Ker}\lambda_G = \operatorname{Im}\iota_G = E + F'$, mais ceci ne force pas l'égalité $\lambda_G \circ \pi = \theta$. Par exemple, si β est un automorphisme arbitraire de G'', on peut prendre $\lambda_G = \beta \circ \pi_G$ et $\lambda'' = \beta \circ \pi''$.

Remarques

i. Le point *2* montre une certaine absence de symétrie (regrettable) dans la situation. Cela sera élucidé d'une certaine manière dans l'exercice 34.
On peut néanmoins conclure cet exercice comme suit.
Supposons que :

- *les deux premières suites horizontales et les deux premières suites verticales sont des suites exactes courtes canoniques ;*
- *et* $\theta = \pi_G \circ \pi = \pi'' \circ \pi_F$.

Alors, il y a un unique diagramme commutatif de la forme annoncée, et il rend les troisièmes suites horizontale et verticale exactes.

Notons que ceci constitue une forme particulièrement précise des théorèmes de Noether dans la mesure où les isomorphismes de Noether sont ici complètement explicites et déterminés de manière unique.

ii. Remarquons aussi que l'hypothèse selon laquelle certaines injections et surjections sont canoniques est un peu artificielle dans la mesure où ι_G et ι'' ne sont pas des injections canoniques et π_G et π'' ne sont pas des surjections canoniques. Voir à ce sujet la remarque à la fin du corrigé de l'exercice 34. ∎

Exercice 34. *1.* Rappelons le diagramme donné en hypothèse dans le cas (non vraiment restrictif), où les injections et les surjections sont toutes canoniques.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & E_0 & \xrightarrow{\iota_0} & F' & \xrightarrow{\pi_0} & G_0 = F'/E_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \jmath_E} & & \downarrow{\scriptstyle \iota_F} & & & & \\
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G = F/E & \longrightarrow & 0
\end{array}$$

1a. L'application linéaire $\jmath_G$ doit être obtenue en factorisant $\pi\circ\iota_F$. Si elle existe, elle est unique, et elle existe si, et seulement si, $\operatorname{Ker}\pi_0 \subseteq \operatorname{Ker}(\pi\circ\iota_F)$. Or, $\operatorname{Ker}\pi_0 = \operatorname{Im}\iota_0$. La condition équivaut donc à $\pi\circ\iota_F\circ\iota_0 = 0$. Or, $\pi\circ\iota_F\circ\iota_0 = \pi\circ\iota\circ\jmath_E$ et $\pi\circ\iota = 0$.

1b. Puisque π_0 est surjective, on a $\operatorname{Im}\jmath_G = \operatorname{Im}(\jmath_G\circ\pi_0) = \operatorname{Im}(\pi\circ\iota_F) = \pi(F')$. Enfin, $\pi^{-1}\big(\pi(F')\big) = E + F' = S$. Ainsi, $\operatorname{Im}\jmath_G = S/E \subseteq F/E$.

1c. L'application $\jmath_G$ est injective si, et seulement si, le noyau de $\jmath_G\circ\pi_0$ est égal au noyau de π_0, qui est E_0, c'est-à-dire encore si $\operatorname{Ker}(\pi\circ\iota_F) = E_0$.
Or, $\operatorname{Ker}(\pi\circ\iota_F) = \iota_F^{-1}(E) = E\cap F'$. Ainsi, la condition est bien $E_0 = E'$.
Cela nous ramène à la situation de l'exercice 33.

2. Rappelons le diagramme donné en hypothèse dans lequel on peut supposer que ι est une injection canonique et π_F une surjection canonique $F \to F'' = F/F'$ avec $F' = \operatorname{Ker}\pi_F$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \theta_G} & & \\
0 & \longrightarrow & E_3 & \xrightarrow[\iota_3]{} & F'' & \xrightarrow[\pi_3]{} & G_3 & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

2a. Comme ι est une injection canonique, l'application linéaire $\beta : E \to E_3$ que l'on veut définir doit satisfaire pour $x \in E$ l'égalité $\iota_3\big(\beta(x)\big) = \pi_F(x)$, ce qui est possible si $\pi_F(E) \subseteq \iota_3(E_3)$, c'est-à-dire si $\pi_F(E) \subseteq \operatorname{Ker}\pi_3$, c'est-à-dire encore $\pi_3\circ\pi_F\circ\iota = 0$. Or, $\pi_3\circ\pi_F\circ\iota = \theta_G\circ\pi\circ\iota$ et $\pi\circ\iota = 0$.
Ainsi, β est bien définie, et elle est unique parce que ι_3 est injective.

2b. Puisque ι_3 est injective, on a

$$\operatorname{Ker}\beta = \operatorname{Ker}(\iota_3\circ\beta) = \operatorname{Ker}(\pi_F\circ\iota) = \iota^{-1}(\operatorname{Ker}\pi_F) = \iota^{-1}(F') = E\cap F'.$$

2c. L'application linéaire β est surjective si, et seulement si, $\operatorname{Im}(\iota_3\circ\beta) \supseteq \operatorname{Ker}\pi_3$, c'est-à-dire encore si $\pi_F(E) \supseteq \operatorname{Ker}\pi_3$, ou aussi $\pi_F^{-1}\big(\pi_F(E)\big) \supseteq \pi_F^{-1}\big(\operatorname{Ker}\pi_3\big)$, i.e. enfin $E + \operatorname{Ker}\pi_F \supseteq S_3$. Ainsi, β est surjective si, et seulement si, $E + F' = S_3$.

Dans ce cas, en prenant $E' = E\cap F'$ on retrouve à isomorphismes près la situation de l'exercice 33. Voyons ceci précisément.
Tout d'abord puisque β est surjective de noyau E', on a une unique application linéaire $\alpha_E = E/E' \to E_3$ qui satisfait $\alpha_E\circ\pi_E = \beta$ ($\pi_E : E \to E/E'$ surjection canonique). Ainsi, α_E est un isomorphisme.

Ensuite, puisque $F'' = F/F'$ et $\mathrm{Ker}(\pi_3 \circ \pi_F) = E' + F$, on a un unique application linéaire $\alpha_G : F/S = G'' \to G_3$ qui satisfait $\alpha_G \circ \pi'' = \pi_3$ (avec π'' comme dans l'exercice 33), et α_G est un isomorphisme.

Enfin, vu la commutativité du diagramme, on a $\alpha_G \circ \pi_G = \theta_G$ (avec π_G comme dans l'exercice 33).

Ainsi, on retrouve bien, modulo les isomorphismes α_E et α_G, les deux dernières lignes du diagramme de l'exercice 33.

Remarque. En se libérant de l'hypothèse, rajoutée un peu artificiellement pour faciliter la démonstration, selon laquelle les injections et surjections données au départ sont canoniques, le point *1* donnerait l'énoncé suivant.

Un diagramme commutatif de suites exactes du type (I) *peut être complété en un diagramme commutatif complet* (C) *de suites exactes si, et seulement si, on a l'égalité* $\mathrm{Ker}(\iota \circ \iota_E) = \mathrm{Ker}\,\iota_E \cap \mathrm{Ker}\,\iota'$. *Et, dans ce cas,* (C) *est essentiellement unique.*

(I)

$$\begin{array}{ccccc} & & 0 & & 0 \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & E' & \xrightarrow{\iota'} & F' \\ & & \downarrow{\scriptstyle \iota_E} & & \downarrow{\scriptstyle \iota_F} \\ 0 & \longrightarrow & E & \xrightarrow{\iota} & F \end{array}$$

(C)

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E' & \xrightarrow{\iota'} & F' & \xrightarrow{\pi'} & G' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota_E} & & \downarrow{\scriptstyle \iota_F} & & \downarrow{\scriptstyle \iota_G} & & \\ 0 & \longrightarrow & E & \xrightarrow{\iota} & F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_E} & & \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \pi_G} & & \\ 0 & \longrightarrow & E'' & \xrightarrow[\iota'']{} & F'' & \xrightarrow[\pi'']{} & G'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

En outre, le point *2* fournit un théorème dual.

Un diagramme commutatif de suites exactes du type (I') *peut être complété en un diagramme commutatif complet* (C) *de suites exactes si, et seulement si, on a l'égalité* $\mathrm{Ker}(\pi_G \circ \pi) = \mathrm{Ker}\,\pi + \mathrm{Ker}\,\pi_F$. *Et, dans ce cas,* (C) *est essentiellement unique.*

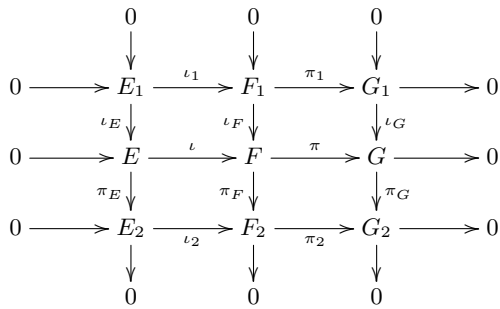
(I')

$$\begin{array}{ccccc} F & \xrightarrow{\pi} & G & \longrightarrow & 0 \\ \downarrow{\scriptstyle \pi_F} & & \downarrow{\scriptstyle \pi_G} & & \\ F'' & \xrightarrow[\pi'']{} & G'' & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ 0 & & 0 & & \end{array}$$

Remarque. La dualité qui apparaît ici entre les points *1* et *2* frise maintenant la perfection. Elle a donné lieu à une abstraction qui permet de mieux la comprendre : la théorie des catégories abéliennes. La catégorie opposée d'une catégorie abélienne

étant elle-ême abélienne, un énoncé du style de *1* prouvé dans une catégorie abélienne fournit ipso facto un énoncé correct tel que *2*. ∎

Exercice 35. On rappelle le diagramme



On suppose sans perte de généralité que ι, ι_1, ι_E et ι_F sont des injections canoniques, et π, π_1, π_E et π_F sont des surjections canoniques.
Notons S_2 le noyau de l'application linéaire $\pi_2 \circ \pi_F = \pi_G \circ \pi$.

1. Supposons tout d'abord la suite $0 \to E_1 \to F_1 \to G_1 \to 0$ exacte. Alors, d'après le point *1* de l'exercice 34, on a

$$E_1 = E \cap F_1, \quad \text{donc} \quad E_2 = E/(E \cap F_1),$$

et

$$\operatorname{Im} \iota_G = (E + F_1)/E \subseteq F/E, \quad \text{donc} \quad G_2 \simeq F/(E + F_1).$$

Cela implique que la troisième ligne est exacte.

Supposons la suite $0 \to E_2 \to F_2 \to G_2 \to 0$ exacte. Alors, d'après le point *2* de l'exercice 34, on a $\operatorname{Ker} \pi_E = E \cap F_1$, donc $E_1 = E \cap F_1$, et le noyau de l'application linéaire $F \to G_2$ doit être égal à $E + F_1$, ce qui implique $\operatorname{Ker} \pi_G = (E + F_1)/E$. Comme $F_1/(E \cap F_1) \simeq (E + F_1)/E$, ceci implique que la première ligne est exacte.

2. Déjà démontré

Exercice 36. Laissé au lecteur.

Problème 1. *1.* Si A_j est une colonne non nulle de A, on a $BA_j = e_j$ donc $ABA_j = A_j$; ainsi, AB est l'identité sur $\operatorname{Im} A$ donc $ABA = A$. La matrice AB est triangulaire inférieure, et ses coefficients diagonaux sont $0, 1$. La matrice BA est diagonale et ses coefficients diagonaux sont $0, 1$. On a, d'une part,

$$B = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}, \qquad BA = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

et, d'autre part,

$$AB = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{24} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{44} & \cdot & a_{43} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ a_{74} & \cdot & a_{73} & \cdot & a_{71} & a_{72} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{94} & \cdot & a_{93} & \cdot & a_{91} & a_{92} & \cdot & a_{95} & \cdot \end{bmatrix}.$$

Le supplémentaire $\operatorname{Ker} AB$ de $\operatorname{Im} A = \operatorname{Im} AB$ dans $\mathbf{K}^n$ admet comme base les e_i pour les indices i de lignes ne contenant pas un indice pivot.
Dans l'exemple, (e_2, e_4, e_7, e_9) est une base de $\operatorname{Ker} AB$.

2. On obtient (Q, A') par la méthode (classique) d'échelonnement de Gauss. Si la matrice $B' \in M_{n,m}(\mathbf{K})$ vérifie $A'B'A' = A'$, alors $AQB'AQ = AQ$, donc la matrice $B = QB'$ vérifie $ABA = A$.

3. Considérons une matrice $B \in \mathbb{M}_{m,n}(\mathbf{K})$ telle que $ABA = A$. Alors, si $y = Ax$ pour un m-vecteur à coefficients dans un sur-anneau de $\mathbf{K}$, on a $A(By) = y$, d'où l'existence d'une solution sur $\mathbf{K}$, à savoir By.

4. Soient $(u_1, \ldots, u_r)$ un système générateur du $\mathbf{K}$-espace vectoriel E, constitué de vecteurs de $\mathbf{K}_0^n$; idem pour $(v_1, \ldots, v_s)$ et F. Soit $z \in \mathbf{K}_0^n$, que l'on cherche à écrire sous la forme $z = x_1u_1 + \cdots + x_ru_r + y_1v_1 + \cdots + y_sv_s$ avec les $x_i, y_j \in \mathbf{K}_0$. On obtient ainsi un système $\mathbf{K}_0$-linéaire en les inconnues x_i, y_j qui admet une solution sur $\mathbf{K}$, donc également sur $\mathbf{K}_0$.

5.a. Si tous les $\pi(e_j)$ sont dans $\mathbf{K}_0^n$, alors le sous-espace E, engendré par les $\pi(e_j)$, est $\mathbf{K}_0$-rationnel. Réciproquement, si E est $\mathbf{K}_0$-rationnel, comme F l'est aussi, on a, d'après la question précédente, $\pi(e_j) \in \mathbf{K}_0^n$ pour tout j.

5b. Facile maintenant : $\mathbf{K}_0$ est le sous-corps engendré par les composantes des vecteurs $\pi(e_j)$.

5c. Le corps de rationalité d'une matrice strictement échelonnée est le sous-corps engendré par les coefficients de la matrice. Par exemple avec $E = \operatorname{Im} A \subset \mathbf{K}^5$:

$$A = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{array} \begin{array}{c} \begin{array}{ccc} w_1 & w_2 & w_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & c & d \end{bmatrix} \end{array},$$

on obtient $E = \mathbf{K}w_1 \oplus \mathbf{K}w_2 \oplus \mathbf{K}w_3$ et l'on a $\mathbf{K}^5 = E \oplus F$ avec $F = \mathbf{K}e_2 \oplus \mathbf{K}e_5$. Puisque

$$e_1 - w_1 \in F, \qquad e_3 - w_2 \in F, \qquad e_4 - w_3 \in F,$$

on a $\pi(e_1) = w_1$, $\pi(e_3) = w_2$, $\pi(e_4) = w_3$ et $\pi(e_2) = \pi(e_5) = 0$. Le corps de rationalité de E est $\mathbf{K}_0 = \mathbf{k}(a, b, c, d)$, où $\mathbf{k}$ est le sous-corps premier de $\mathbf{K}$.

Commentaires bibliographiques

Le lemme de Gauss-Joyal est dans [84], qui lui donne son nom de baptême. Sur le sujet général de la comparaison entre les idéaux $\mathrm{c}(f)\mathrm{c}(g)$ et $\mathrm{c}(fg)$ on peut consulter [41, 99, 151] et, dans cet ouvrage, les sections III-2 et III-3 et la proposition XI-3.14.

Concernant le traitement constructif de la noethérianité on peut consulter les références [MRR, 116, 153, 154, 164, 175, 176, 193].

L'ensemble de la section 5 se trouve plus ou moins dans [Northcott]. Par exemple la formule (12) page 47 se trouve sous une forme voisine dans le théorème 5 page 10. De même, notre formule magique à la Cramer (17) page 48 est très proche du théorème 6 page 11 : Northcott attache une importance centrale à l'équation matricielle $A\,B\,A = A$. Sur ce sujet, voir aussi [Rao & Mitra] et [64, Díaz-Toca & al.].

La proposition 5.15 se trouve dans [Bhaskara Rao] théorème 5.5.

Concernant le théorème 5.26 : dans [Northcott] le théorème 18 page 122 établit l'équivalence des points *1* et *5* par une méthode qui n'est pas entièrement constructive, mais le théorème 5 page 10 permettrait de donner une formule explicite pour l'implication $5 \Rightarrow 1$.

Tables des théorèmes

Méthodes dynamiques

Principes local-globals concrets

Principes de recouvrement fermé

Stabilité par extension des scalaires

Théorèmes

Principe local-global de base et systèmes linéaires

La méthode des coefficients indéterminés

Modules de présentation finie

Modules projectifs de type fini (1)

Algèbres de type fini

La méthode dynamique

Modules plats

Anneaux locaux, ou presque

Modules projectifs de type fini (2)

Treillis distributifs, groupes réticulés

Anneaux de Prüfer et de Dedekind

Dimension de Krull

Nombre de générateurs d'un module

Le principe local-global

Machineries dynamiques et principes local-globals variés sont indiqués pages 1077 et 1078.

Modules projectifs étendus

Théorème de stabilité de Suslin

Bibliographie

[Abdeljaoued & Lombardi] Abdeljaoued A., Lombardi H. *Méthodes Matricielles. Introduction à la Complexité Algébrique*. Springer, (2003). 112

[Aczel & Rathjen] Aczel P., Rathjen M. *Notes on Constructive Set Theory*. `http://www1.maths.leeds.ac.uk/~rathjen/book.pdf`. 1075

[Adams & Loustaunau] Adams W., Loustaunau P. *An Introduction to Gröbner Bases*. American Mathematical Society, (1994). 35

[Apéry & Jouanolou] Apéry F., Jouanolou J.-P. *Élimination. Le cas d'une variable*. Hermann, (2006). 196

[Artin] Artin, E. *Galois theory*. Edited and supplemented with a section on applications by Arthur N. Milgram. Second edition, with additions and revisions. Fifth reprinting. Notre Dame Mathematical Lectures, Number 2, (1959). 419

[Atiyah & Macdonald] Atiyah M.F., Macdonald I.G. *Introduction to Commutative Algebra*. Addison Wesley, (1969). xxxi

[Basu, Pollack & Roy] Basu S., Pollack R. et Roy M.-F. *Algorithms in real algebraic Geometry*. Springer, (2006). `https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.pdf` 196, 197, 242

[Bass] Bass H. *Algebraic K-theory*. W. A. Benjamin, Inc., New York-Amsterdam, (1968). 922, 934, 1039

[Beeson] Beeson M. *Foundations of Constructive Mathematics*. Springer-Verlag, (1985). 215, 1067, 1074

[Bhaskara Rao] Bhaskara Rao K. *Theory of Generalized Inverses over a Commutative Ring*. Taylor & Francis. Londres, (2002). 49, 90

[Bigard, Keimel & Wolfenstein] Bigard A., Keimel K. et Wolfenstein S. *Groupes et anneaux réticulés*. Springer LNM 608, (1977). 749

[Birkhoff] Birkhoff G. *Lattice theory*. Third edition. American Mathematical Society Colloquium Publications, Vol. XXV American Mathematical Society, Providence, R.I., (1967). 748

[Bishop] *Foundations of Constructive Analysis*. McGraw Hill, (1967). Reprint avec une préface de Michael Beeson. 2012. IshiPress New York and Tokyo. 215, 447, 1058, 1074

[Bishop & Bridges] Bishop E., Bridges D. *Constructive Analysis*. Springer-Verlag, (1985). 215, 447, 1058, 1060

[Bourbaki] Bourbaki. *Algèbre Commutative*. Hermann, (1961-2002). xxxi, 675

[Bridges & Richman] Bridges D., Richman F. *Varieties of Constructive Mathematics*. London Math. Soc. LNS 97. Cambridge University Press, (1987). 215, 1067

[Brouwer] Brouwer L. *Brouwer's Cambridge Lectures on Intuitionism, 1951* (Van Dalen ed.) Cambridge University Press, (1981). 1074

[Burris & Sankappanavar] Burris S., Sankappanavar H. *A Course in Universal Algebra*. Springer, (1981). 271

[Cartan & Eilenberg] Cartan H., Eilenberg S. *Homological algebra*. Princeton University Press, (1956). 831

[COCOA] Kreuzer M., Robbiano L. *Computational commutative algebra*. Springer Verlag, Berlin. Vol. 1 (2000), Vol. 2 (2005). xxxi

[Cohn] Cohn P. *Basic Algebra. Groups, rings and fields*. (2nd edition) Springer Verlag, (2002). 271

[Cox] Cox D. *Galois theory*. Wiley-Interscience, (2004). 483

[Cox, Little & O'Shea] Cox D., Little J. et O'Shea D. *Ideals, Varieties, and Algorithms*. (2nd edition) Springer Verlag UTM, (1998). xxxi

[CPMPCS] *Concepts of proof in mathematics, philosophy, and computer science. (Papers based on the research of Humboldt-Kolleg "Proof" held in Bern, September 9–13, 2013)*. Eds : Probst D., Schuster P. Berlin : De Gruyter, (2016). 1096

[CRA] *Commutative ring theory and applications*. Eds : Fontana M., Kabbaj S.-E. et Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002). 1096, 1101

[Curry] Curry H. B. *Foundations of mathematical logic* McGraw-Hill Book Co., Inc., New York-San Francisco, Calif.-Toronto-London, (1963). 749

[David, Nour & Raffalli] David R., Nour K. et Raffalli C. *Introduction à la logique*. Dunod, (2001). 1074

[Demeyer & Ingraham] Demeyer F., Ingraham E. *Separable algebras over commutative rings*. Springer Lecture Notes in Mathematics 181, (1971). 419

[Díaz, Lombardi & Quitté] Díaz-Toca G., Lombardi H. et Quitté C. *Modules sur les anneaux commutatifs*. Calvage & Mounet, (2014). 266

[Dowek1] Dowek G. *La logique*. Flammarion. Collection Dominos, (1995). 1074

[Dowek2] Dowek G. *Les métamorphoses du calcul. Une étonnante histoire de mathématiques*. Le Pommier, (2007). 1074

[Edwards89] Edwards H. *Divisor Theory*. Boston, MA : Birkhäuser, (1989). xviii

[Edwards05] Edwards H. *Essays in Constructive Mathematics*. Springer Verlag, (2005). xviii

[Eisenbud] Eisenbud D. *Commutative Algebra with a view toward Algebraic Geometry*. Springer Verlag, (1995). xxxi, 419, 896

[Ene & Herzog] Ene, V., Herzog, J. *Gröbner bases in commutative algebra*. Graduate Studies in Mathematics n°130, American Mathematical Society, (2012). xxxi

[Elkadi & Mourrain] Elkadi M., Mourrain B. *Introduction à la résolution des systèmes polynomiaux*. Collection Mathématiques & Applications, n°59, Springer Verlag, Berlin, (2007). xxxi

[Feferman] Feferman S. *In the Light of Logic*. Oxford University Press, (1998). 1075

[Frege-Gödel] van Heijenoort J. (ed.), *Frome Frege to Gödel : a source book in mathematical logic*. Harvard University Press, Cambridge, Massachussets, (1967). Troisième réimpression en 2002. 1100

[Freid & Jarden] Freid M. D., Jarden M. *Field Arithmetic*. Springer-Verlag, (1986). 771

[von zur Gathen & Gerhard] von zur Gathen J. Gerhard J. *Modern computer algebra*. Cambridge University Press, Cambridge, (2003). xxxi

[Gilmer] Gilmer R. *Multiplicative Ideal Theory*. Queens papers in pure and applied Math, vol. 90, (1992). xxxi, 529, 831, 896

[Glaz] Glaz S. *Commutative Coherent Rings*. Lecture Notes in Math., vol. 1371, Springer Verlag, Berlin-Heidelberg-New York, second edition, (1990). xxxi

[Grätzer] Grätzer G. *Lattice Theory : foundation*. Birkhäuser/Springer Basel AG, Basel, (2011). 748, 749

[Gupta & Murthy] Gupta S., Murthy M. *Suslin's work on linear groups over polynomial rings and Serre conjecture*. ISI Lecture Notes n°8. The Macmillan Company of India Limited, (1980). 1049, 1052, 1056

[HoTT] *Homotopy Type Theory : Univalent Foundations of Mathematics*. (2014) `http://homotopytypetheory.org/`. 1075

[Infini] Toraldo di Francia G. (ed.), *L'infinito nella scienza*. Istituto della Enciclopedia Italiana, Rome, (1987). 1074

[Ireland & Rosen] Ireland K., Rosen M. *A classical introduction to modern number theory*. Graduate Texts in Mathematics, vol. 84, Springer-Verlag, Berlin-Heidelberg-New York, (1989). 135

[Ischebeck & Rao] Ischebeck F., Rao R. *Ideals and Reality. Projective modules and number of generators of ideals*. Springer Monograph in Mathematics, Berlin-Heidelberg-New York, (2005). 271, 1008

[Jaffard] Jaffard, P. *Théorie de la dimension dans les anneaux de polynômes*. Gauthier-Villars, Paris, (1960). 896

[Jensen, Ledet & Yui] Jensen C., Ledet A. et Yui N. *Generic Polynomials, Constructive Aspects of the Inverse Galois Problem*. Cambrigde University Press, MSRI Publications 45, (2002). 675

[Johnstone] Johnstone P. *Stone spaces*. Cambridges studies in advanced mathematics n°3. Cambridge University Press, (1982). 728, 748, 749, 896

[Kaplansky] Kaplansky I. *Commutative rings*. Boston, Allyn and Bacon, (1970). xxxi

[Kleene & Vesley] Kleene S.C., Vesley R. *The Foundations of intuitionistic mathematics*. Amsterdam (North-Holland), (1965). 1074

[Knapp, 1] Knapp A. *Basic algebra*. Birkhäuser, (2006). xxxi

[Knapp, 2] Knapp A. *Advanced algebra*. Birkhäuser, (2007). xxxi

[Knight] Knight J. *Commutative Algebra*. London Mathematical Society LNS n°5. Cambridge University Press, (1971). 991

[Kunz] Kunz E. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, (1991). xviii, xxxi, 271, 326, 588, 912, 932, 991, 1004

[Lafon & Marot] Lafon J.-P., Marot J. *Algèbre locale*. Hermann, Paris, (2002). xxxi, 555, 588

[Lakatos] Lakatos I. *Preuves et réfutations*. Version française, Hermann, (1984). xxix

[Lam] Lam T.Y. *Serre's conjecture*. Lecture Notes in Mathematics, Vol. 635. Springer Berlin Heidelberg New York, (1978). 1039

[Lam06] Lam T.Y. *Serre's Problem on Projective Modules*. Springer Berlin Heidelberg New York, (2006). xxxi, 271, 987, 1008, 1013, 1014, 1019, 1033, 1038, 1039, 1056

[Lancaster & Tismenetsky] Lancaster P., Tismenetsky M. *The Theory of Matrices, 2/e* Academic Press, (1985). 49

[Lawvere & Rosebrugh] Lawvere W., Rosebrugh R. *Sets for Mathematics*. Cambridge University Press, (2003). 271

[Lorenzen] Lorenzen P. *Métamathématique*. Traduit de l'allemand par J. B. Grize, Gauthier-Villars, Paris, Mouton, Paris La Haye, (1967), édition originale 1962. 1074

[Mac Lane] Mac Lane, S. *Categories for the Working Mathematician*. Second edition, Springer, (1998). 271

[Martin-Löf] Martin-Löf P. *Intuitionistic type theory*. Notes by Giovanni Sambin. Studies in Proof Theory. Lecture Notes, 1. Bibliopolis, Naples, (1984). 1075

[Matsumura] Matsumura H. *Commutative ring theory*. Cambridge studies in advanced mathematics n°8. Cambridge University Press, (1989). xxxi, 912

[MITCA] *Multiplicative Ideal Theory in Commutative Algebra : A tribute to the work of Robert Gilmer*. Eds : Brewer J., Glaz G., Heinzer W. et Olberding B. Springer, (2006). 1094, 1099

[MRR] Mines R., Richman F. et Ruitenburg W. *A Course in Constructive Algebra*. Universitext. Springer-Verlag, (1988). Traduction française *Un cours d'algègre constructive*. Traduction par Henri Lombardi révisée par Stefan Neuwirth. Presses Universitaires de Franche-Comté, (2020). v, xviii, 30, 35, 90, 215, 225, 231, 270, 278, 292, 418, 422, 435, 457, 483, 520, 545, 588, 748, 749, 752, 948, 1058, 1060, 1074

[Mora] Mora T. *Solving Polynomial Equation Systems I : The Kronecker-Duval Philosophy*. Cambridge University Press, (2003). xxxi

[Northcott] Northcott D. *Finite free resolutions*. Cambridge tracts in mathematics No 71. Cambridge University Press, (1976). xxxi, 90, 242, 270, 326, 975

[PFCM] Crosilla L., Schuster P. eds. *From Sets and Types to Analysis and Topology : Towards Practicable Foundations for Constructive Mathematics.* Oxford University Press, (2005). 1096, 1100

[Pohst & Zassenhaus] Pohst M., Zassenhaus H. *Algorithmic algebraic number theory (Encyclopedia of Mathematics and its Applications).* Revised reprint of the 1989 original. Cambridge University Press, (1997). 483, 484

[Rao & Mitra] Rao C., Mitra S. *Generalized Inverses of Matrices and its Applications.* John Wiley & Sons, (1971). 90

[Raynaud] Raynaud M. *Anneaux locaux henséliens.* Springer Lecture Notes in Mathematics n°169, (1970). 555, 588

[SINGULAR] Greuel G.-M., Pfister G. *A Singular Introduction to Commutative Algebra.* Springer, (2002). `http://www.singular.uni-kl.de/` xxxi

[Schwichtenberg & Wainer] Schwichtenberg H., Wainer S. *Proofs and Computations.* Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, (2012). 1074

[Stacks-Project] Stacks-Project. Ouvrage collectif. `http://stacks.math.columbia.edu` xxxi, 270

[TAPAS] Cohen A., Cuypers H. et Sterk H. (eds) *Some Tapas of Computer Algebra.* Springer Verlag, (1999). xxxi

[Tignol] Tignol J.-P. *Galois' theory of algebraic equations.* World Scientific Publishing Co., Inc., River Edge, NJ, (2001). 483

[Yengui] Yengui I. *Constructive commutative algebra. Projective modules over polynomial rings and dynamical Gröbner bases.* Springer LNM n°2138, (2015). xviii, 483

[Zaanen] Zaanen A. *Introduction to Operator Theory in Riesz Spaces.* Springer Verlag, (1997). 749

Articles

[1] Aczel P. *Aspects of general topology in constructive set theory.* Ann. Pure Appl. Logic **137**, (2006), 3–29. 1075

[2] Alonso M.-E., Lombardi, H. et Perdry, H. *Elementary constructive theory of Henselian local rings.* Mathematical Logic Quarterly **54**, (2008), 253–271. 569

[3] Aubry P., Valibouze A. *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation **30**, (2000), 635–651. 484

[4] Auslander M., Goldman, O. *The Brauer group of a commutative ring.* Trans. Amer. Math. Soc. **97**, (1960), 367–409. 419

[5] Avigad J. *Methodology and metaphysics in the development of Dedekind's theory of ideals.* 159–186. Dans : José Ferreirós and Jeremy Gray, editors, The Architecture of Modern Mathematics, Oxford University Press, (2006). 752, 831

[6] Banaschewski B. *Radical ideals and coherent frames.* Comment. Math. Univ. Carolin. **37** 2, (1996), 349–370. 896

[7] Barhoumi S. *Seminormality and polynomial rings.* Journal of Algebra **322** (2009), 1974–1978. 1038

[8] Barhoumi S., Lombardi H. *An Algorithm for the Traverso-Swan theorem on seminormal rings.* Journal of Algebra **320** (2008), 1531–1542. 1004, 1038

[9] Barhoumi S., Lombardi H. et Yengui I. *Projective modules over polynomial rings : a constructive approach.* Math. Nachrichten **282** (2009), 792–799. 1039

[10] Basu R., Rao R. et Khanna R. *On Quillen's Local Global Principle.* Contemporary Mathematics, Commutative Algebra and Algebraic Geometry, Volume 390, (2005), 17–30. 1039

[11] Bass H. *Torsion free and projective modules.* Trans. Amer. Math. Soc. **102**, (1962), 319–327. 949

[12] Bazzoni S., Glaz S. *Prüfer rings.* 55–72. Dans [MITCA]. 530

[13] Berger J. *Constructive Equivalents of the Uniform Continuity Theorem.* Journal of Universal Computer Science **11** (12), (2005), 1878–1883. 1075

[14] Berger J., Bridges D. *A fan-theoretic equivalent of the antithesis of Specker's theorem.* Proc. Koninklijke Nederlandse Akad. Wetenschappen. Indag. Math. **18** (2), (2007), 195-202. 1075

[15] Berger J., Ishihara H. *Brouwer's fan theorem and unique existence in constructive analysis.* Math. Logic Quarterly **51** (2005), 360–364. 1075

[16] Bernstein D. *Factoring into coprimes in essentially linear time.* Journal of Algorithms **54** (2005), 1–30. 752

[17] Bernstein D. *Fast ideal arithmetic via lazy localization.* Cohen, Henri (ed.), Algorithmic number theory. Second international symposium, ANTS-II, Talence, France, May 18-23, 1996. Proceedings. Berlin : Springer. Lect. Notes Comput. Sci. n°1122 (1996), 27–34. 752

[18] Bishop, E. *Mathematics as a numerical language.* in Intuitionism and Proof Theory. Eds. Myhill, Kino, and Vesley, North-Holland, Amsterdam, (1970). 1060

[19] Boniface J., Schappacher N. *"Sur le concept de nombre en mathématique" : cours inédit de Leopold Kronecker à Berlin (1891).* Rev. Histoire Math. **7** (2001), 206–275. 92

[20] Bosma W., Cannon J. et Playoust C. *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24** (1997), 235–265. 484

[21] Brandl R. *Integer polynomials that are reducible modulo all primes.* Amer. Math. Month. **93** (4), (1986), 286–288. 484

[22] Brenner H. *Lifting chains of prime ideals.* J. Pure Appl. Algebra **179** (2003), 1–5. 896

[23] Brewer J., Costa D. *Projective modules over some non-Noetherian polynomial rings.* J. Pure Appl. Algebra **13** (1978) (2), 157–163. 1039

[24] Brewer J., Costa D. *Seminormality and projective modules over polynomial rings.* J. Algebra **58** (1), (1979), 208–216. 1038

[25] Brewer J., Klinger L. *Pole assignability and the invariant factor theorem in Prüfer domains and Dedeking domains.* J. Algebra **111** (1987), 536–545. 831

[26] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6** (2) (1994), 221–260. 752, 753

[27] Cahen, P.-J., *Construction B, I, D et anneaux localement ou résiduellement de Jaffard. (B, I, D construction and locally or residually Jaffard rings).*, Archiv der Mathematik **54**, (1990), 125–141. 896

[28] Caniglia L., Cortinas G., Danón S., Heintz J., Krick T. et Solernó P. *Algorithmic Aspects of Suslin's Proof of Serre's Conjecture.* Computational Complexity **3** (1993), 31–55. 1039

[29] Cannon J., Bosma W. *Handbook of Magma functions.* Version 2.14, Oct. 2007, 4400 pages. 484

[30] Cederquist J., Coquand T. *Entailment relations and Distributive Lattices* Logic Colloquium '98 (Prague), 127–139, Lect. Notes Log., 13. Assoc. Symbol. Logic, Urbana, (2000). 749

[31] Chase S., Harrison D. et Rosenberg A. *Galois theory and Galois cohomology of commutative rings.* Mem. Amer. Math. Soc. **52** (1965), 15–33. 419

[32] Chervov A., Talalaev D. *Hitchin systems on singular curve I.* Theor. Math. Phys. **140** (2004), 1043–1072. 675

[33] Chervov A., Talalaev D. *Hitchin systems on singular curve II. Glueing subschemes.* Int. J. Geom. Meth. Mod. Phys. **4** (2007), 751–787. 675

[34] Coquand T. *La contribution de Kolmogorov en logique intuitionniste.* Dans : L'héritage de Kolmogorov en mathématiques. Charpentier E., Lesne A. et Nikolski N. (eds). Belin, Paris (2004). 1064

[35] Coquand T. *About Brouwer's fan theorem.* Revue internationale de philosophie **230** (2004), 483–489. 1075

[36] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques.* C. R. Acad. Sci. Paris, Ser. I **338** (2004), 291–294. 898

[37] Coquand T. *On seminormality.* Journal of Algebra **305** (1), (2006), 585–602. 991, 996, 1038

[38] Coquand T. *A refinement of Forster's theorem.* Preprint (2007). 898, 934, 1039

[39] Coquand T. *Space of valuations.* Annals of Pure and Applied Logic **157** (2009), 97–109. 896

[40] Coquand T. *Recursive functions and constructive mathematics.* p. 159–167 dans : Bourdeau M., Dubucs J. (Eds.), Calculability and Constructivity. Historical and Philosophical Aspects. Logic, Epistemology and the Unity of Science, Vol. 34. Springer (2014). 1074

[41] Coquand T., Ducos L., Lombardi H. et Quitté C. *L'idéal des coefficients du produit de deux polynômes*. Revue des Mathématiques de l'Enseignement Supérieur **113** (3), (2003), 25–39. 90

[42] Coquand T., Ducos L., Lombardi H. et Quitté C. *Constructive Krull Dimension. I : Integral Extensions*. Journal of Algebra and Its Applications. **8** (2009), 129–138. 896

[43] Coquand T., Lombardi H. *A short proof for the Krull dimension of a polynomial ring*. American Math. Monthly. **112** no. 9 (2005), 826–829. 896

[44] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*. 477–499. Dans [CRA, 2005]. 896

[45] Coquand T., Lombardi H. *A logical approach to abstract algebra*. (survey) Math. Struct. in Comput. Science **16** (2006), 885–900. xxxii

[46] Coquand T., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down*. Rapport technique (2001) `http://hlombardi.free.fr/publis/GoingUpDownFrench.pdf` (version anglaise `http://hlombardi.free.fr/publis/GoingUpDown.pdf`). 896

[47] Coquand T., Lombardi H. *Some remarks on normal rings*. 141–149. Dans [CPMPCS, 2016]. 832

[48] Coquand T., Lombardi H. *Anneaux à diviseurs et anneaux de Krull (une approche constructive)*. Communications in Algebra **44** (2016), 515–567. `https://arxiv.org/abs/1507.02880` 628, 795

[49] Coquand T., Lombardi H. et Neuwirth S. *Lattice-ordered groups generated by an ordered group and regular systems of ideals*. The Rocky Mountain Journal of Mathematics, **49** (2019), 1449–1489. `https://arxiv.org/abs/1701.05115` 483, 749

[50] Coquand T., Lombardi H. et Neuwirth S. *Regular entailment relations*. À paraître dans les Actes de la conférence Paul Lorenzen : Mathematician and Logician, 8-9 mars 2018, Constance, 10 pages. (2020). `https://arxiv.org/abs/1912.09480` 483, 749

[51] Coquand T., Lombardi H. et Quitté C. *Generating non-Noetherian modules constructively*. Manuscripta mathematica **115** (2004), 513–520. 898, 933

[52] Coquand T., Lombardi H. et Quitté C. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs*. Publications Mathématiques de Besançon. Théorie des nombres (2006). 51 pages. Version corrigée : `http://hlombardi.free.fr/publis/AHeitmann.html`. Sur arXiv : `https://arxiv.org/abs/1712.01958` 896, 898, 903, 933, 934

[53] Coquand T., Lombardi H. et Roy M.-F. *An elementary characterization of Krull dimension*. 239–244. Dans [PFCM]. 896

[54] Coquand T., Lombardi H. et Schuster P. *A nilregular element property*. Archiv der Mathematik **85** (2005), 49–54. 848, 896, 932

[55] Coquand T., Persson H. *Valuations and Dedeking Prague theorem*. J. Pure Appl. Algebra **155** (2001), 121–129. 749

[56] Cortiñas G., Haesemayer C., Walker M.E. et Weibel C. *A negative answer to a question of Bass*. Proc. AMS **139** (2011), 1187–1200. 1008

[57] Coste M., Lombardi H. et Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze*. Annals of Pure and Applied Logic **111**, (2001), 203–256. `https://arxiv.org/abs/1701.05794` 570, 990

[58] Couchot F. *Finitely presented modules over semihereditary rings*. Communications in Algebra **35** (9), (2007) 2685–2692. 831

[59] Dedekind R. *Über einen arithmetischen Satz von Gauss*. Mitt. dtsch. math. Ges. Prag. (1892), 1–11. 196

[60] Dedekind R. *Über die Begründung der IdealTheorie*. Nachr. K. Ges. Wiss. Göttingen (1894), 272–277. 752

[61] Della Dora J., Dicrescenzo C. et Duval D. *About a new method for computing in algebraic number fields*. In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985). 434, 466, 990

[62] Díaz-Toca G. *Galois theory, splitting fields and computer algebra*. J. Symbolic Computation **41** (11), (2006), 1174–1186. 483

[63] Díaz-Toca G., Gonzalez-Vega L. et Lombardi H. *Generalizing Cramer's Rule : Solving uniformly linear systems of equations*. SIAM Journal on Matrix Analysis and Applications **27** (3), (2005), 621–637. 588

[64] Díaz-Toca G., Gonzalez-Vega L., Lombardi H. et Quitté C. *Modules projectifs de type fini, applications linéaires croisées et inverses généralisés*. Journal of Algebra **303** (2), (2006), 450–475. 90, 246, 588, 645

[65] Díaz-Toca G., Lombardi H. *A polynomial bound on the number of comaximal localizations needed in order to make free a projective module*. Linear Algebra and its Application **435**, (2011), 354–360. 326

[66] Díaz-Toca G., Lombardi H. et Quitté C. *L'algèbre de décomposition universelle*. Proceedings du colloque TC2006 (Granada), 169–184. 483, 484

[67] Díaz-Toca G., Lombardi H. *Dynamic Galois Theory*. Journal of Symbolic Computation. **45**, (2010), 1316–1329. 483

[68] Drach J. *Essai sur la théorie générale de l'intégration et sur la classification des transcendantes*. Ann. Sci. Ec. Norm. Sup **3** (15), (1898), 243–384. 197, 483

[69] Ducos L. *Effectivité en théorie de Galois. Sous-résultants*. Université de Poitiers, Thèse doctorale. Poitiers (1997). 484

[70] Ducos L. *Construction de corps de décomposition grâce aux facteurs de résolvantes. (French) [Construction of splitting fields in favour of resolvent factors]*. Communications in Algebra **28** (2), (2000), 903–924. 484

[71] Ducos L. *Vecteurs unimodulaires et systèmes générateurs*. Journal of Algebra **297**, (2006), 566–583. 934

[72] Ducos L. *Sur la dimension de Krull des anneaux noethériens.* Journal of Algebra **322**, (2009), 1104–1128. 933, 991

[73] Ducos L. *Polynômes à valeurs entières : un anneau de Prüfer de dimension 2.* (2011) Communications in Algebra **43** (2015), 1146–1155. 784

[74] Ducos L., Lombardi H., Quitté C. et Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra **281** (2004), 604–650. 530, 831

[75] Ducos L., Valibouze A. et Yengui I. *Computing syzygies over $V[X_1, \ldots, X_k]$, V a valuation domain.* Journal of Algebra **425** (2015), 133–145. 483

[76] Edwards H. *The genesis of ideal theory.* Arch. Hist. Exact Sci. **23** (4) (1980/81), 321–378. 831

[77] Eisenbud D., Evans E., Jr. *Generating modules efficiently : theorems from algebraic K-theory.* J. Algebra **27** (1973), 278–305. 933

[78] Eisenbud D., Evans E., Jr. *Every algebraic set in n-space is the intersection of n hypersurfaces.* Inventiones math. **19** (1973), 107–112. 906, 932

[79] Ellouz A., Lombardi H. et Yengui I. *A constructive comparison of the rings $\mathbf{R}(X)$ and $\mathbf{R}\langle X\rangle$ and application to the Lequain-Simis Induction Theorem.* Journal of Algebra **320** (2008), 521–533. 1029, 1039

[80] Español L. *Dimensión en álgebra constructiva.* Thèse doctorale. Université de Zaragoza, Zaragoza, (1978). 896, 934

[81] Español L. *Constructive Krull dimension of lattices.* Rev. Acad. Cienc. Zaragoza (2) **37** (1982), 5–9. 896

[82] Español L. *Le spectre d'un anneau dans l'algèbre constructive et applications à la dimension.* Cahiers de topologie et géométrie différentielle catégorique. **24** (2) (1983), 133–144. 896

[83] Español L. *Dimension of Boolean Valued Lattices and Rings.* Journal of Pure and Applied Algebra **42** (1986), 223–236. 896

[84] Español L. *The spectrum lattice of Baer rings and polynomials.* Categorical algebra and its applications. (Louvain-La-Neuve, 1987), 118–124, Lecture Notes in Math., 1348, Springer, Berlin-New York, (1988). 90, 896

[85] Español L. *Finite chain calculus in distributive lattices and elementary Krull dimension.* Contribuciones cientificas en honor de Mirian Andres Gomez. Eds. L. Lamban, A. Romero y J. Rubio, Servicio de Publicaciones, Universidad de La Rioja, Logrono, Spain, (2010). 883, 896

[86] Estes R., Guralnick R. *Module equivalences : local to global when primitive polynomials represent units.* J. of Algebra **77** (1982), 138–157. 588

[87] Ferrand D. *Les modules projectifs de type fini sur un anneau de polynômes sur un corps sont libres.* Sém. Bourbaki, exposé **484**, (1975-1976), 202–221. 1038

[88] Ferrero M., Paques A. *Galois theory of commutative rings revisited.* Contributions to Algebra and Geometry **38** (1997), 399–410. 419

[89] Fitchas N., Galligo A. *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachr. **149** (1990), 231–253. 1039

[90] Fontana M., Loper A. *An historical overview of Kronecker function rings, Nagata rings and related star and semistar operations.* 169–187. Dans [MITCA]. 197

[91] Forster O. *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring.* Math. Z. **84** (1964), 80–87. 933

[92] Fuchs L. *Über die Ideale arithmetischer ringe.* Math. Helv. **23** (1949), 334–341. 529

[93] Carl Friedrich Gauss *Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse.* Comm. Recentiores (Gottingae) **3** (1816), 107–142. Reproduit dans Werke III, 31–56. Traduction anglaise : `http://www.monad.me.uk/misc/gauss-web.php` sur la page web de Paul Taylor. `http://www.monad.me.uk/` 92

[94] Geissler K., Klüners J. *Galois Group Computation for Rational Polynomials.* J. Symbolic Computation **30** (2000), 653–674. 484

[95] Gillman L., Henriksen M. *Some remarks about elementary divisor rings.* Trans. Amer. Soc. **82**, (1956) 362–365 250

[96] Gilmer R., Heitmann R. *On Pic R[X] for R seminormal.* J. Pure Appl. Algebra **16** (1980), 251–257. 1038

[97] Gilmer R., Hoffmann, J. *A characterization of Prüfer domains in terms of polynomials.* Pacific J. Math. **60** (1) (1975), 81–85. 831

[98] Glaz S. *Finite conductor properties of* $\mathbf{R}(X)$ *and* $\mathbf{R}\langle X\rangle$. Dans : Proceeding of conference in honor to J. Huckaba's retirement, Missouri, Dec. 1999. Marcel Dekker Lecture Notes. 1039

[99] Glaz, S., Vasconcelos W. *Gaussian polynomials.* Marcel Dekker Lecture Notes 186 (1997), 325–337. 90

[100] Goldman O. *Determinants in projective modules.* Nagoya Math. J. **18** (1961), 27–36. 326

[101] Hallouin E. *Parcours initiatique à travers la théorie des valuations.* Rapport technique. Université de Poitiers, (1996). `http://www.picard.ups-tlse.fr/~hallouin/eh-valuation.ps` 159

[102] Hallouin E. *Calcul de fermeture intégrale en dimension 1 et factorisation intégrale.* Thèse. Université de Poitiers, (1998). `http://www.picard.ups-tlse.fr/~hallouin/eh-these.ps` 831

[103] Heitmann R. *Generating ideals in Prüfer domains.* Pacific J. Math. **62** (1976), 117–126. 933

[104] Heitmann R. *Generating non-Noetherian modules efficiently.* Michigan Math. **31** 2 (1984), 167–180. xxviii, 897, 902, 903, 933, 934

[105] Heitmann R., Levy L. *1 1/2 and 2 generator ideals in Prüfer domains.* Rocky Mountain J. Math. **5** 3 (1975), 361–673. 831

[106] Hermida J., Sánchez-Giralda T. *Linear Equations over Commutative Rings and Determinantal Ideals.* Journal of Algebra **99** (1986), 72–79. 502, 529

[107] Hess F. *Computing Riemann-Roch space in algebraic function fields.* Journal of Symbolic Computation **33** (2002), 425–445. 832

[108] Heyting A. *After thirty years.* In : 1962 Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.) pp. 194–197 Stanford Univ. Press, Stanford, Calif. 1074

[109] Hilbert D. *Über das Unendliche.* Math. Annalen **95** (1926), 161–190. (Sur l'infini) traduction anglaise dans [Frege-Gödel] 367–392. 1074

[110] Hochster M. *Prime ideal structure in commutative rings.* Trans. Amer. Math. Soc. **142** (1969), 43–60. 896

[111] Horrocks G. *Projective modules over an extension of a local ring.* Proc. Lond. Math. Soc. **14** (1964), 714–718. 1038

[112] Hulpke A. *Konstruktion transitiver Permutationsgruppen.* Dissertation, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany. (1996). 484

[113] Ishihara H. *Constructive reverse mathematics : compactness properties.* 245–267. Dans [PFCM]. 1075

[114] Ishihara H. *Weak König lemma implies Brouwer's fan theorem : a direct proof.* Notre Dame J. Formal Logic **47** (2006), 249–252. 1075

[115] Ishihara H. *Reverse mathematics in Bishop's constructive mathematics.* Philosophia Scientiae, Cahier Spécial **6** (2006), 43–59. 1075

[116] Jacobsson C., Löfwall C. *Standard Bases for General Coefficient Rings and a New Constructive Proof of Hilbert's Basis Theorem.* J. Symb. Comput. **12** (1991), 337–372. 90

[117] Johnstone, P. *The art of pointless thinking : a student's guide to the category of locales.* Category theory at work (Bremen, 1990), 85–107, Res. Exp. Math., 18, Heldermann, Berlin, 1991. 748

[118] Joyal A. *Spectral spaces and distibutive lattices.* Notices AMS **18** (1971), 393. 896

[119] Joyal A. *Le théorème de Chevalley-Tarski.* Cahiers de topologie et géometrie différentielle catégorique, 1975. 896, 934

[120] van der Kallen W. *The K2 of rings with many units.* Ann. Sci. É.N.S. 4^{e}série **10**, (1977), 473–515. 588

[121] Kaplansky I. *Elementary divisors and modules.* Transactions of the AMS **66**, (1949), 464–491. 250, 271

[122] Kaplansky I. *Modules over Dedekind Rings and Valuation Rings.* Trans. Amer. Math. Soc. **72**, (1952), 327–340. 831

[123] Klüners J., Malle G. *Explicit Galois realization of transitive groups of degree up to 15.* J. Symbolic Comput. **30** (6), (2000), 675–716. 484

[124] Kolmogorov A. *Zur Deutung der intuitionistischen Logik.* Math. Zeitschr. **35** (1932) 58–65. 1064

[125] Kronecker L. *Zur Theorie der Formen höherer Stufen* Ber. K. Akad. Wiss. Berlin (1883), 957–960. (Werke 2, 417–424). 102, 196

[126] Kronecker L. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* J. reine angew. Math. **92**, (1882) 1–123. Réimprimé dans *Leopold Kronecker's Werke*, II, 237–387. 898

[127] Landau, S., Miller, G. *Solvability by radicals is in polynomial time.* J. Comput. Syst. Sci. **30** (1985), 179–208. 484

[128] Lecerf, G. *Fast separable factorization and applications.* Applicable Algebra in Engineering, Communication and Computing **19** (2) (2008), 135–160. 418

[129] Lequain, Y., Simis, A. *Projective modules over $R[X_1, ..., X_n]$, R a Prüfer domain.* J. Pure Appl. Algebra **18** (2) (1980), 165–171. 624, 1030

[130] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besançon. Théorie des nombres. Fascicule (1997), 94–95 & 95–96. 990

[131] Lombardi H. *Platitude, localisation et anneaux de Prüfer : une approche constructive.* 64 pages. Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 530, 831

[132] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift **242**, (2002), 23–46. 896

[133] *Un anneau de Prüfer.* Third International Meeting on Integer-Valued Polynomials. Actes des rencontres du CIRM **2** (2010). `http://acirm.cedram.org/cgi-bin/browse` 784

[134] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global.* 461–476. Dans [CRA]. 1039

[135] Lombardi H., Quitté C. *Seminormal rings (following Thierry Coquand).* Theoretical Computer Science. **392**, (2008), 113–127. 1038

[136] Lombardi H., Quitté C. et Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Journal of Pure and Applied Algebra **212** 7 (2008), 1575–1582. 1039

[137] Lombardi H., Yengui I. *Suslin's algorithms for reduction of unimodular rows.* Journal of Symbolic Computation **39** (2005), 707–717. 1039

[138] Lorenzen, P. *Algebraische und logistische Untersuchungen über freie Verbände.* Journal of Symbolic Logic **16** (1951), 81–106. `http://www.jstor.org/stable/2266681`. Traduction par Stefan Neuwirth : *Algebraic and logistic investigations on free lattices*, `http://arxiv.org/abs/1710.08138`. 749, 1074

[139] Lorenzen, P. *Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen.* Math. Z. **58** (1953), 15–24. `http://eudml.org/doc/169331`. Traduction par Stefan Neuwirth : *Algebraic and logistic investigations on free lattices*, `http://arxiv.org/abs/1710.08138`. 483, 749

[140] Maroscia P. *Modules projectifs sur certains anneaux de polynômes.* C.R.A.S. Paris **285** série A (1977), 183–185. 1039

[141] Per Martin-Löf. *An intuitionistic theory of types : Predicative part.* In H. E. Rose and J. C. Shepherdson, editors, Logic Colloquium Ô73, pages 73–118. North Holland, (1975). 1075

[142] Martin-Löf P. *An intuitionistic theory of types.* 127–172, in : Twenty-five years of constructive type theory (Venice, 1995), Oxford Logic Guides, 36, Oxford Univ. Press, New York, 1998. 1075

[143] Per Martin-Löf *The Hilbert-Brouwer controversy resolved ?* 243–256. Dans : One hundred years of intuitionism (1907-2007), (Cerisy), (Mark Van Atten & al., editors) Publications des Archives Henri Poincaré, Birkhäuser Basel, (2008). 1074

[144] Mertens F. *Über einen algebraischen Satz.* Ber. K. Akad. Wiss. Wien (1892). 196

[145] Mnif A., Yengui I. *An algorithm for unimodular completion over Noetherian rings.* J. Algebra **316** (2007), 483–498. 1039

[146] Mulmuley K. *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field.* Combinatorica **7**/1, (1987), 101–104. 645

[147] Murthy M. *Generators of a general ideal.* in : A tribute to C. S. Seshadri (Chennai, 2002), Trends in Math., Birkhäuser, Basel, (2003), 379–384. 934

[148] Murthy M., Pedrini C. *K_0 and K_1 of polynomial rings.* in Algebraic K-Theory II, Lecture Notes in Math. 342, (1973), 109–121. 1009

[149] Nashier B., Nichols W. *Ideals containing monics.* Proc. Amer. Math. Soc. **99** (1987), 634–636. 1008

[150] Nicholson W. *Lifting idempotents and exchange rings.* Trans. Amer. Math. Soc. **229** (1977), 269–278. 574

[151] Northcott D. *A generalization of a theorem on the content of polynomials.* Proc. Cambridge Philos. Soc. **55** (1959), 282–288. 90, 196

[152] Orange S., Renault G. et Valibouze A. *Calcul efficace de corps de décomposition.* Rapport technique LIP6 2003/005. 484

[153] Perdry H. *Strongly Noetherian rings and constructive ideal theory.* J. Symb. Comput. **37** (2004), 511–535. 90

[154] Perdry H. *Lazy bases : a minimalist constructive theory of Noetherian rings.* Math. Log. Quart. **54** (2008), 70–82. 90

[155] Poincaré H. *La logique de l'infini.* Revue de Métaphysique et de Morale **17**, 461–482, (1909) réédité dans *Dernières pensées*, Flammarion (1913). 1074

[156] Prüfer H. *Untersuchunger uber teilbarkeitseigenschaften in korpen.* Angew. Mat. **168** (1932), 1–36. 529, 831

[157] Quentel Y. *Sur une caractérisation des anneaux de valuation de hauteur 1.* C. R. Acad. Sci., Paris, Ser. A **265** (1967), 659–661. 831

[158] Querré J. *Sur le groupe de classes de diviseurs.* C. R. Acad. Sci. Paris **284** (1977), 397–399. 1038

[159] Quillen D. *Projective modules over polynomial rings.* Invent. Math. **36** (1976), 167–171. 1038, 1039

[160] Rao R. *On projective $R_{f_1,\ldots,f_t}$-modules.* Amer. J. Math. **107** (1985), 387–406. 1050

[161] Rao R. *An elementary transformation of a special unimodular vector to its top coefficient vector.* Proc. Amer. Math. Soc. **93** (1985), 21–24. 1021, 1050

[162] Rao R. *A note on the Serre dimension of polynomial rings.* J. Pure Appl. Algebra **38** (1985), 87–90. 1050

[163] Rao R., Selby J. *Quillen-Suslin theory revisited.* J. Pure Appl. Algebra **211** (2007), 541–546. 1039

[164] Richman F. *Constructive aspects of Noetherian rings.* Proc. Amer. Mat. Soc. **44** (1974), 436–441. 31, 90

[165] Richman F. *Seidenberg's condition P.* in Constructive Mathematics. Springer LNM 873 (1981), 1–11. 418

[166] Richman F. *Finite dimensional algebras over discrete fields.* L. E. J. Brouwer centenary symposium, Troelstra and van Dalen eds., North-Holland Pub. Co. (1982), 397–411. 418

[167] Richman F. *Church Thesis without tears.* Journal of Symbolic Logic **48** (3) (1983), 797–803. 1067

[168] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc. **103** (1988), 1012–1014. 588

[169] Richman F. *Intuitionism as generalization.* Philosophia Mathematica **5** (1990), 124–128. 1074

[170] Roitman M. *On projective modules over polynomial rings.* Journal of Algebra **58** (1979), 51–63. 1038

[171] Roitman M. *On stably extended projective modules over polynomial rings* Proc. Amer. Math. Soc. **97** (1986), 585–589. 1033

[172] Rota Gian Carlo *The many lives of lattice theory.* Notices Amer. Math. Soc. **44** 11 (1997), 1440–1445. 752

[173] Sander T. *Existence and uniqueness of the real closure of an ordered field without Zorn's Lemma.* J. Pure and Applied Algebra **73** (1991), 165–180. 483

[174] Seidenberg A. *A note on the dimension theory of rings.* Pac. J. Math. **3** (1953), 505–512. 896

[175] Seidenberg A. *What is Noetherian ?* Rend. Sem. Mat. e Fis. Milano **44** (1974), 55–61. 31, 90

[176] Seidenberg A. *On the Lasker-Noether decomposition theorem.* Amer. J. Math. **106** (1984), 611–638. 90

[177] Serre J.-P. *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier Grenoble **6** (1955-1956), 1–42. xxiii, 485

[178] Serre J.-P. *Modules projectifs et espaces fibrés à fibre vectorielle.* Séminaire P. Dubreil, Année 1957/1958. 933

[179] Simis A., Vasconcelos W. *Projective modules over $R[X]$, R a valuation ring, are free.* Notices. Amer. Math. Soc. **18** (5), (1971). 1039

[180] Skolem T. *A critical remark on foundational research.* Norske Vid. Selsk. Forh., Trondheim, **28** (1955), 100–105. 1074

[181] Soicher L., McKay J. *Computing Galois groups over the rationals.* J. Number Theory **20**, (1985), 273–281. 484

[182] Stauduhar R. *The determination of Galois groups.* Math. Comp. **27**, (1973), 981–996. 484

[183] Steel A. *A New Scheme for Computing with Algebraically Closed Fields.* Lecture Notes In Computer Science **2369**. Proceedings of the 5th International Symposium on Algorithmic Number Theory, (2002), 491–505. 484

[184] Steel A. *Computing with algebraically closed fields.* Journal of Symbolic Computation **45**, 342–372, (2010). 484

[185] Stone M. H. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, (1937), 1–25. 835, 896

[186] Storch U. *Bemerkung zu einem Satz von M. Kneser.* Arch. Math. **23**, (1972), 403–404. 932

[187] Suslin A. *Projective modules over polynomial rings are free. (Russian).* Dokl. Akad. Nauk SSSR **229** (5), (1976), 1063–1066. 1038

[188] Suslin A. *Stably Free Modules. (Russian).* Mat. Sb. (N.S.) **102** (1977), 537–550. English translation : Math. USSR Sb. **31**, 479–491. 326

[189] Swan R. *Factorization of Polynomials over Finite Fields.* Pacific Journal of Mathematics **12** (3), (1962), 1099–1106. 185

[190] Swan R. *The Number of Generators of a Module.* Math. Z. **102** (1967), 318–322. 933, 934

[191] Swan R. *On Seminormality.* Journal of Algebra **67** (1980), 210–229. 996, 1038

[192] Swan R. *Algebraic vector bundles on the 2-sphere.* Rocky Mountain Journal of Mathematics **23** (1993), 1443–1469. 8

[193] Tennenbaum J. B. *A constructive version of Hilbert's basis theorem.* Dissertation, University of California San Diego, (1973). 90

[194] Traverso C. *Seminormality and the Picard group.* Ann. Scuola Norm. Sup. Pisa **24** (1970), 585–595. 996, 1038

[195] Valibouze A. *Sur le corps des racines d'un polynôme.* Acta Arithmetica **131** (1), (2008), 1–27. 484

[196] Vaserstein L.N. *Serre's problem on projective modules over polynomial rings after Suslin and Quillen*. (1976), Unpublished notes. 1019

[197] Vessiot E. *Sur la théorie de Galois et ses diverses généralisations*. Ann. Sci. E. N. S. 3ème série **21**, (1904), 9–85. 483

[198] Villamayor, O.E., Zelinsky, D. *Galois theory for rings with finitely many idempotents*. Nagoya Math. J. **27**, (1966), 721–731. 419

[199] Van der Waerden. Review Zentralblatt für Math **24**, (1941), 276. 932

[200] Weyl H. *Das Kontinuum, Kritische Untersuchungen über die Grundlagen der Analysis*. Veit, Leipzig (1918). Traduction italienne *Il Continuo. Indagine critiche sui fondamenti dell' Analisi*. par A. B. Veit Riccioli, Bibliopolis, Naples (1977). Traduction anglaise *The Continuum. A critical examination of the foundations of Analysis*. par S. Polard et T. Bole. Thomas Jefferson Press, University Press of America (1987). En français : *Le continu et autres écrits*. Traduits et commentés par Jean Largeault. Librairie Vrin (1994). 1074

[201] Yengui I. *An algorithm for the divisors of monic polynomials over a commutative ring*. Math. Nachr. **260** (2003), 93–99. 989

[202] Yengui I. *Dynamical Gröbner bases*. Journal of Algebra **301** (2006), 447–458. Corrigendum : [203]. 991

[203] Yengui I. Corrigendum to *Dynamical Gröbner bases* [J. Algebra **301** (2) (2006) 447–458] and to *Dynamical Gröbner bases over Dedekind rings* [J. Algebra, 324 (1) (2010) 12–24]. Journal of Algebra **339** (2011), 370–375. 1105

[204] Yengui I. *Making the use of maximal ideals constructive*. Theoretical Computer Science **392**, (2008) 174–178. 991

[205] Yengui I. *The Hermite ring conjecture in dimension one*. Journal of Algebra **320** (2008), 437–441. 1033

[206] Yengui I. *Stably free modules over $R[X]$ of rank $>\dim R$ are free*. Mathematics of Computation **80** (2011), 1093–1098. 1033

Index des notations

page

Exemples

Principe local-global de base et systèmes linéaires

La méthode des coefficients indéterminés

Modules de présentation finie

Modules projectifs de type fini (1)

Algèbres de type fini

La méthode dynamique

Anneaux locaux, ou presque

Modules projectifs de type fini (2)

Treillis distributifs, groupes réticulés

Anneaux de Prüfer et de Dedekind

Dimension de Krull

Nombre de générateurs d'un module

Le principe local-global

Modules projectifs étendus

Théorème de stabilité de Suslin

Annexe : logique constructive

Index des termes