ENS Rennes
Année 2023-2024
Jade Nardi

Groupes de lecture : Bases de Gröbner et applications

Créneau mercredi 10h15–12h15 du 06/09/2023 au 25/10/2023. Deux séances le 04/10 (13h45-15h45).
Présence obligatoire !

1 Déroulé d'un exposé

Les orateurs et oratrices devront prévoir un exposé de **40 minutes**, questions **non comprises**.
Un exposé trop court ou trop long sera pénalisé.

Pauses programmées

Prévoir **deux** moments de pause dans votre exposé pour laisser vos collègues poser des questions. Vous êtes libres de décider du moment où vous faites vos pauses (après une démonstration, un exemple...)
Ces temps de question ne seront pas comptés dans les 40 minutes d'exposé.

Questions obligatoires

Pour chaque paire (A, B) ci-dessous, le groupe A doit poser **deux** questions au groupe B. Chaque question compte pour 1pt dans la note finale du groupe A (pertinence, niveau...).

$$\{(1,12),(2,10),(3,8),(4,9),(5,1),(6,11),(7,2),(8,4),(9,5),(10,7),(11,3),(12,6)\}$$

Conseils de préparation

Vous construisez un cours ensemble. Une préparation soignée prend du **temps** et de la **coordination** avec le binôme de la même séance. N'oubliez pas de faire référence aux séances précédentes si vous utilisez un résultat présenté auparavant.

Je vous demande une **attention toute particulière pour les démonstrations**, même les plus simples et celles que les auteurs éludent par une phrase du type « on voit bien que », ou qu'ils renvoient en exercice. Profitez-bien de vos deux semaines de préparation : vous pouvez m'envoyer une semaine avant vos notes. Passé ce délai, je ne garantis aucune réponse.

Je vous conseille très fortement de **répéter** votre exposé au moins une fois avant le jour J. Si votre exposé vous semble trop court, **n'hésitez surtout pas à faire des exemples** ! Tout effort pour modifier les exemples donnés dans les références sera apprécié.

Si vous préparez des transparents avec Beamer [1], faites-en bon usage et évitez l'effet doublon. Ne réécrivez pas au tableau ce qui est déjà écrit dessus. Pour les preuves, je vous conseille de privilégier le tableau. Mais vous pouvez utiliser les transparents pour y noter ce que vous n'avez pas le temps (ou l'envie) d'écrire au tableau (longs énoncés, formules un peu lourdes, rappel d'un résultat utile...).

Interactions avec les autres

Soyez polis et bienveillants envers vos collègues, que ce soit votre binôme ou le reste de la classe.

On ne coupe pas la parole de son binôme et on l'écoute pendant qu'il/elle parle. S'il fait une faute qu'il ne remarque pas rapidement, vous pouvez la lui signaler aimablement.

On ne juge pas des questions des camarades. Vous avez passé plusieurs jours à travailler votre sujet ; ce n'est pas leur cas. **Il n'y a pas de question bête.**

2 Références

- [CLOS94] : référence principale. On choisira cette référence pour les notations.
- [AL94] pour une autre référence générique, avec beaucoup d'exemples et d'exercices.
- [FHP03], [Gei08] : exemples d'application des bases de Gröbner.
- [Bro22] : thèse récente utilisant des bases de Gröbner pour des attaques sur des systèmes cryptographiques. Beaucoup d'exemples et très discursif.

1. Astuce de pro : `\documentclass[aspectratio=169]beamer` pour des transparents en 16 : 9.

Programme des séances

Possibilité de transvaser des parties d'un binôme à l'autre mais demandez-moi avant tout changement !

Le symbole ⌨ signale une utilisation attendue/conseillée d'un logiciel de calcul formel (SageMath, COCOA, Magma, Macaulay2...).

- **1^e séance (20/09/2023) :** Préliminaires

1. *Ordre monomiaux.* Référence : [CLOS94] §2.2
   Groupe : Sylvain Marie-Victoire & Mathis Preault
   Définition et ordres classiques (lex, grlex, grevlex) avec une preuve complète que l'un d'eux est un ordre monomial (sauf lex). Exemples dans l'esprit des exercices 1 et 2.
   Exercice 7 (a) et (b)
   Si le temps le permet, contre-exemples d'ordres monomiaux.
   Terme/monôme dominant, degré (Def. 7 et Lem. 8) et leur propriétés (exercices 11 et 12)
2. *Algorithme de division.* Référence : [CLOS94] §2.3
   Groupe : Manon Branchereau & Matteo Soreda
   Exemples et lien avec le cas univarié. Déterminer les ordres monomiaux sur $k[x]$.
   Division : algorithme et preuve (Thm 4 [CLOS94])
   ⌨ Dépendance du reste selon l'ordre de la famille de polynômes (Exercice 5)

- **2^e séance (27/10/2023) :** Bases de Gröbner : définitions et caractérisation

3. *Idéaux monomiaux.* Référence : [CLOS94] §2.4
   Groupe : Wael El Khaledi & Millan Huppe
   Définition et propriétés d'un idéal monomial (Preuve du Lem. 3 dans l'ex. 2), base minimale.
   Lemme de Dickson avec preuve (Thm 5)
   Ex. 3, si le temps le permet.
4. *Bases de Gröbner.* Références : [CLOS94] §2.5
   Groupe : Axel Mauroy & Killian Le Milbeau
   Théorème de la base de Hilbert avec preuve (Thm 4 et ses prérequis)
   Définition base de Gröbner et exemples (dans l'esprit des exercices 7 et 8)
   Condition de chaîne ascendante avec preuve (Thm 7 + Exercice 12)

- **3^e séance (04/10/2023 matin) :** Algorithme de Buchberger

5. *S-polynôme.* Références : [CLOS94] §2.6
   Groupe : Coline Fournier & Tiphaine Vaisson
   Preuve de l'unicité de reste de la division par une base de Gröbner (Prop. 1 avec ajout de l'Ex. 1)
   Exercice 2 pour non–unicité des quotients
   Definition et propriétés du S-polynôme
   Critère de Buchberger avec preuve et exemples d'application (dans l'esprit des exercices 9 et 10)
6. *Algorithme de Buchberger.* Références : [CLOS94] §2.7
   Groupe : Romain Azam & Romaric Batisse
   Thm. 2 avec preuve.
   Relation avec l'algorithme d'Euclide pour les polynômes univarés (Exercice 11)
   ⌨ Exemple d'application de l'algorithme (idéal engendré par 2 polynômes bivariés)

- **4^e séance (04/10/2023 après-midi) :** Applications I

7. *Preuves de théorèmes en géométrie.* Références : [CLOS94] §1.2 et §6.4 ([RV99] pour d'autres exemples)
   Groupe : Pierre Sarre & Dimitri Bergeault
   Prérequis (§1.2) : langage des variétés algébriques, union et intersection de variétés en termes d'idéaux (Lem. 2), exemples dans l'esprit des premiers exercices de §1.2.
   Traduction des propriétés mathématiques en polynômes (Prop. 2 §6.4)
   ⌨ Au moins un exemple de théorème détaillé
   Gestion des cas dégénérés, si le temps le permet. On pourra admettre le théorème des zéros de Hilbert si besoin.
8. *Exemple en biophysique.* Références : [FHP03] jusqu'à Prop. 4.6.
   Groupe : Sylvain Chaurand & Thibault Brasseur
   ⌨ Comprendre la preuve du Thm. 1.1, en particulier Prop 3.1.
   Utilisation de la symétrie du problème pour réduire la complexité.

◆ **5^e séance (11/10/2023)**

9. *Bases de Gröbner homogènes et linéarisation.* Références : [CLOS94] §8.3 et §10.1 + [Bro22] §2.3.2
   Groupe : Pierre Beuchot & Kylian Prigent
   Polynômes et idéaux homogènes Def. 1 et Thm 2 de §8.3
   Lemme 7 avec preuve
   Définition matrices de Macaulay et lien avec les S-polynômes
   Exemple §2.3.2.2 [Bro22]
   Complexité
10. *Variétés algébriques.* Références : [CLOS94] §4.1 & 4.2
    Groupe : Sarah Carrier & Rachel Ruelle
    Rappels (si nécessaires) sur le vocabulaire des variétés
    Théorème faible des zéros de Hilbert (Nullstellensatz) [§4.1 Thm 1]
    Application au problème de cohérence des systèmes polynomiaux (*consistency algorithm*)
    Théorème fort des zéros de Hilbert [§4.1 Thm 2]
    Radical d'un idéal avec exemples (§4.2 exercices 1 et 2)
    Correspondance idéaux radicaux ↔ variétés (admis si manque de temps)
    Exemple cas non algébriquement clos (§4.2 exercice 3)
    Application au 3-coloriage de graphe (Tutorial 26 [KR00] : ⌨ pour (d)-(f))

◆ **6^e séance (25/10/2023) :** Applications II

11. *Quotient par un idéal et applications au codes d'évaluation.* Références : [Gei08] jusqu'à §4 comprise et [CLOS94] §5.3.
    Groupe : Mahe Ambert & Noan Botcazou-Brasse
    Prérequis : code correcteurs linéaires (longueur, dimension, distance minimale)
    Définition d'un code d'évaluation
    Empreinte (*footprint* en anglais) d'un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ (Def.2 [Gei08])
    Borne de l'empreinte ([CLOS94] §5.3. Prop. 4)
    Application au calcul de la longueur et de la distance minimale d'un code d'évaluation
    ⌨ Exemples
12. *Application à la cryptographie : le problème MinRank* Référence : [Bro22]
    Groupe : Maxence Michot & Gurwan Pape
    Présentation du problème MinRank (Definition 16)
    Ancienne attaque du problème et complexité
    Factorisation d'une matrice de rang r (admise dans la thèse, à démontrer)
    Modélisation algébrique du problème §3.1.1

Références

[AL94] William W Adams and Philippe Loustaunau. *An introduction to Gröbner bases*, volume 3. 1994.

[Bro22] Maxime Bros. *Algebraic cryptanalysis and contributions to post-quantum cryptography based on error-correcting codes in the rank-metric*. PhD thesis, 2022. Thèse de doctorat dirigée par Gaborit, Philippe et Neiger, Vincent Informatique Limoges 2022.

[CLOS94] David Cox, John Little, Donal O'Shea, and Moss Sweedler. Ideals, varieties, and algorithms. *American Mathematical Monthly*, 101(6) :582–586, 1994.

[FHP03] Jean-Charles Faugere, Milena Hering, and Jeff Phan. The membrane inclusions curvature equations. *Advances in Applied Mathematics*, 31(4) :643–658, 2003.

[Gei08] Olav Geil. *Evaluation Codes from an Affine Variety Code Perspective*, pages 153–180. 2008.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra*, volume 1. Springer, 2000.

[RV99] Tomas Recio and M. Vélez. Automatic discovery of theorems in elementary geometry. *Journal of Automated Reasoning*, 23 :63–82, 07 1999.