Теорія та застосування баз Грьобнера до некомутативних поліноміальних алгебр

Віктор Левандовський *
Київський Національний Університет
імені Тараса Шевченка
та
Centre for Computer Algebra,
University of Kaiserslautern
E–mail : brand@ukrsat.com

Abstract

We give a generalization of Gröbner bases theory for modules over a wide class of noncommutative associative polynomial algebras, namely G–algebras, whose definition and properties we shortly investigate. For left and two–sided ideals and modules we provide many algorithms with implementations in Computer Algebra System. Applications of the theory, including computation of a free resolution of a given module, are discussed in details.

1 G–алгебри та їх властивості

Нехай $<$ є тотальним впорядкуванням на $\mathbb{N}^n$. Воно зветься **гарним впорядкуванням**, якщо $\forall a \in \mathbb{N}^n$ існує скінчена кількість $b \in \mathbb{N}^n$, так що $b < a$.

Нехай A є $\mathbb{K}$–алгеброю, породженою $x_1, \dots, x_n$ із деякими співвідношеннями. Ми кажемо, що A має **PBW (Poincaré–Birkhoff–Witt) базу** тоді і тільки тоді, коли $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{N}\}$ є $\mathbb{K}$–базою A. В такому випадку, ця база може бути ідентифікованою з $\mathbb{N}^n$ через $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mapsto (\alpha_1, \alpha_2, \dots, \alpha_n) = \alpha$, й ми називаємо елементи бази **мономами**. Ми кажемо, що A є алгеброю **PBW типу**, якщо $\mathbb{K}$–база алгебри є підмножиною $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$.

Definition 1.1. Нехай ми маємо дві множини $C = \{c_{ij}\}$ та $D = \{d_{ij}\}$. Означимо $\mathcal{NDC}_{ijk}$ (**умова невиродженості для** $i < j < k$) наступним чином

$$\mathcal{NDC}_{ijk} = c_{ik}c_{jk} \cdot d_{ij}x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_i d_{jk}.$$

Definition 1.2. Нехай $<$ є тотальним впорядкуванням на $\mathbb{N}^n$, A є PBW алгеброю.

1) Впорядкування $<=<_A$ зветься **мономіальним впорядкуванням на** A, якщо виконуються наступні умови:

- $\forall\ \alpha, \beta \in \mathbb{N}^n\ \alpha < \beta \Rightarrow x^\alpha <_A x^\beta$
- $\forall\ \alpha, \beta, \gamma \in \mathbb{N}^n$, з $x^\alpha <_A x^\beta$ випливає $x^{\alpha+\gamma} <_A x^{\beta+\gamma}$.

2) Довільне $f \in A \setminus \{0\}$ може бути записаним єдиним чином як сума $f = cx^\alpha + f'$, де $c \in K^*$ та $x^{\alpha'} <_A x^\alpha$ для довільного ненульового одночлену $c'x^{\alpha'}$ з запису f'. Ми означимо $\mathrm{lm}(f) := x^\alpha$, **ведучий моном** f, $\mathrm{lc}(f) := c$, **ведучий коефіцієнт** f, $\mathrm{lt}(f) := cx^\alpha$, **ведучий одночлен** f.

Ми досліджуємо певні асоціативні алгебри, а саме, ті, співвідношення яких є типу *переписування*, як то $\forall\ 1 \le i < j \le n\ \ x_j x_i = c_{ij} \cdot x_i x_j + d_{ij}(\underline{x})$, де $c_{ij} \in \mathbb{K}^*$ та $d_{ij} \in A$. Зрозуміло, що алгебра A є алгеброю типу PBW. Значить, ми можемо використовувати мономіальні впорядкування на A, хоча, не без певних додаткових обмежень.

*Автор частково підтриманий грантом CRDF UM2-2094

Definition 1.3. Розглянемо $\mathbb{K}$–алгебру $A = \mathbb{K}\langle x_1, \ldots, x_n \mid f_{j,i} = 0 \ \ 1 \le i < j \le n\rangle$, де

$$\forall\ i < j \ \ f_{j,i} = -x_j x_i + c_{ij} \cdot x_i x_j + d_{ij}(\underline{x}),\ \ c_{ij} \in \mathbb{K}^*, d_{ij} \in A.$$

A зветься G**–алгеброю (від n змінних)**, якщо виконуються наступні умови:

- Існує таке мономіальне впорядкування $<_A$, що $\forall\ i < j \ \ \mathrm{lm}(d_{ij}(\underline{x})) <_A x_i x_j$,
- $\forall\ 1 \le i < j < k \le n \ \ \mathcal{NDC}_{ijk} = 0$ для множин $C = \{c_{ij}\} \subset \mathbb{K}^*$ та $D = \{d_{ij}\} \subset A$.

Theorem 1.4. Нехай A є G–алгеброю від n змінних. Тоді

- A має PBW базу,
- A є нетеровою зліва й справа,
- A є областю (тобто не містить дільників нуля),
- A має двостороннє кільце часток $\mathrm{Quot}(A)$.

Remark 1.5. Нехай A є G–алгеброю від n змінних. Тоді, $\forall\ \alpha, \beta \in \mathbb{N}^n$ ведучий одночлен $x^\alpha x^\beta$ дорівнює $c(\alpha,\beta) x^{\alpha+\beta}$, $c(\alpha,\beta) \in \mathbb{K}^*$, значить

$$\forall\ f, g \in A \quad \mathrm{lm}(f \cdot g) = \mathrm{lm}(\mathrm{lm}(f) \cdot \mathrm{lm}(g)) = \mathrm{lm}(g \cdot f).$$

Більш того, легко побачити, що $\mathrm{lm}(f+g) \le \max_<(\mathrm{lm}(f), \mathrm{lm}(g))$, й нерівність досягається тоді й лише тоді, коли $\mathrm{lm}(g) = \mathrm{lm}(f)$, $\mathrm{lc}(f) = -\,\mathrm{lc}(g)$.

Example 1.6 (Приклади G–алгебр)**.** Квазікомутативні кільця поліномів (наприклад, квантова площина Маніна $YX = q \cdot XY,\ q \in \mathbb{K}^*$), універсальні обгортуючі алгебри скінченовимірних алгебр Лі ([AP],[LV]), додатні (та від'ємні) частини квантизованих обгортуючих алгебр, алгебри розв'язного типу ([KW]), деякі ітеровані розширення Оре, нестандартні квантові деформації ([HKP]), алгебри Вейля та q–алгебри Вейля; Віттенівська деформація $\mathfrak{sl}_2$, алгебри Сміта, конформні $\mathfrak{sl}_2$–алгебри ([BR]), дифузійні алгебри ([IPR]) та багато інших.

Обгортуючі алгебри

Нехай $\mathfrak{g}$ є скінченовимірною алгеброю Лі та $A := U(\mathfrak{g})$ її універсальна обгортуюча алгебра (детальніше в [Dix]). A може бути заданою наступним чином : нехай $x_1, \ldots, x_n$ є породжуючими із співвідношеннями $\forall j > i \quad x_j x_i = x_i x_j - \sum_{k=1}^{n} c_{ijk} x_k$, де $c_{ijk} \in \mathbb{K}$ — структурні константи алгебри Лі. По-перше, довільне степеневе гарне впорядкування є допустимим на A. По-друге, обраховуючи умови невиродженості (які, до речі виглядають наступним чином в усіх алгебрах, де має місце $\forall i < j \ \ \mathrm{lc}(x_j x_i) = \mathrm{lc}(x_i x_j)$), ми отримаємо

$$\mathcal{NDC}^{Lie}_{ijk} = d_{ij}x_k - x_k d_{ij} + x_j d_{ik} - d_{ik} x_j + d_{jk} x_i - x_i d_{jk} = [x_k, [x_i, x_j]] + [x_j, [x_k, x_i]] + [x_i, [x_j, x_k]].$$

Ми бачимо, що $\mathcal{NDC}^{Lie}_{ijk} = 0$ співпадає із тотожністю Якобі, записаної в обгортуючій алгебрі, де $[x,y] = xy - yx$. Таким чином, ми можемо розглядати $\mathcal{NDC}_{ijk}$ як *узагальнену тотожність Якобі.* Отже, $U(\mathfrak{g})$ є G–алгеброю від n змінних для довільного степеневого гарного впорядкування, й наявність PBW бази гарантована умовами невиродженості. Докладніше про умови невиродженості, їх зв'язок із PBW базами та базами Грьобнера буде написано в наступних статтях.

2 Бази Грьобнера в G–алгебрах

Детальна інформація про бази Грьобнера викладена в роботах [GPa], [GPb] (комутативні поліноміальні кільця), [AP], [Gr] (тензорні алгебри та алгебри шляхів), [KW] (алгебри розв'язного типу), [AP], [LV] (універсальні обгортуючі алгебри скінченовимірних алгебр Лі).

Нехай A є G–алгеброю від n змінних.

Definition 2.1. 1) **Анулятором (лівого) модуля** M є двосторонній ідеал $\mathrm{Ann}_A\, M := \{a \in A \mid aM = 0\} \subseteq A$.

2) Для деякого елементу $v \in M$, **анулятором** v є лівий ідеал $\mathrm{Ann}_A\, v := \{a \in A \mid a \cdot v = 0\} \subseteq A$.

3) **Примітивний ідеал** є анулятором простого лівого A–модуля. Примітивні ідеали відіграють важливу роль в теорії зображень ([AJ], [Dix]) та є, відповідно, головними об'єктами досліджень.

Перехід від деякого модуля до його ідеалу–анулятора дозволяє нам зосередитися на теорії баз Грьобнера для (лівих) ідеалів та (лівих) підмодулів вільних модулів скінченого рангу, які є скінченопородженними, так як G–алгебри є нетеровими.

Домовленості та позначення: Відтепер, вживаючи поняття *модуль*, ми розумітимемо під цим лівий підмодуль вільного модулю деякого скінченого рангу, а під *одночленом* розумітимемо моном, помножений на коефіцієнт. Припустимо, що $<$ є гарним впорядкуванням. Ми використовуватимемо символи $|$ (відповідно $<$) замість $|_A$ (відповідно $<_A$), для подільності (відповідно для мономіального впорядкування).

2.1 Впорядкування на модулях

Definition 2.2. Нехай $m_1 = x^\alpha$ та $m_2 = x^\beta$ є мономами. Ми кажемо $m_1|m_2$ (m_1 **ділить** m_2), якщо $\alpha_i \leq \beta_i \ \forall i = 1 \ldots n$. Тоді існують такі $p, r \in A$, що $r <_A m_1$ та $m_2 = p \cdot m_1 + r$.

Розширимо тепер поняття мономіального впорядкування на вільний модуль $A^r = Ae_1 \oplus \cdots \oplus Ae_r$, де $e_i = (0, \ldots, 1, \ldots, 0)$. Ми називаємо $x^\alpha e_i \in A^r$ а **мономом (включаючим і–ту компоненту)**.

Definition 2.3. Нехай $<$ є мономіальним впорядкуванням на A. **Мономіальним** (**модульним**) **впорядкуванням** на A^r є тотальне впорядкування $<_m$ на множині мономів $\{x^\alpha e_i \mid \alpha \in \mathbb{N}^n, 1 \leq i \leq r\}$, що задовольняє наступні умови:

$$1)\ x^\alpha e_i <_m x^\beta e_j \Rightarrow x^{\alpha+\gamma} e_i <_m x^{\beta+\gamma} e_j, \quad \text{та} \quad 2)\ x^\alpha < x^\beta \Rightarrow x^\alpha e_i <_m x^\beta e_i,$$

для всіх $\alpha, \beta, \gamma \in \mathbb{N}^n$, $1 \leq i, j \leq r$ та $x^{\alpha+\gamma} \neq 0,\ x^{\beta+\gamma} \neq 0$.

Так як довільний $f \in A^r \setminus \{0\}$ може бути єдиним чином записаний як $f = cx^\alpha e_i + g$, $c \in \mathbb{K}^*$ та $x^\alpha e_i > x^\beta e_j$ для довільного ненульового одночлену $dx^\beta e_j$ з g, назвемо $\mathrm{lm}(f) = x^\alpha e_i$, **ведучим мономом** f та $\mathrm{lc}(f) = c$, **ведучим коефіцієнтом** f.

Для $S \subset A^r$, нехай $\ell(S) = \langle \alpha \mid \exists s \in S, \mathrm{lm}(s) = x^\alpha \rangle \subseteq \mathbb{N}^n$ є моноїдом ведучих експонент. Тоді існують такі $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^n$, що $\ell(S) := \langle \alpha_1, \ldots, \alpha_m \rangle$; ми звемо $L(S) := \{x^\alpha \mid \alpha \in \ell(S)\}$ **множиною ведучих мономів** S.

Нехай $<$ є фіксованим мономіальним впорядкуванням на G–алгебрі A.

Definition 2.4. Нехай $I \subset A^r$ є підмодулем. Скінчена множина $G \subset I$ зветься **базою Грьобнера** (або **стандартною базою**) підмодулю I тоді і тільки тоді, коли $L(G) = L(I)$, тобто для довільного $f \in I \setminus \{0\}$ існує таке $g \in G$, що $\mathrm{lm}(g)|\,\mathrm{lm}(f)$.

В комутативному випадку (наприклад, в [GPa], [GPb]), назва *база Грьобнера* використовується, як правило для гарних впорядкувань, в той час як *стандартна база* — для всіх інших (наприклад, для локальних впорядкувань, за допомогою яких ми можемо працювати із локалізацією кільця в його максимальному ідеалі). В цій роботі ми не торкаємося інших, ніж гарні, впорядкувань, та використовуємо обидві назви, які, зрозуміло, у випадку гарних впорядкувань співпадають. До речі, нам здається вірогідною можливість розширення теорії на деякі впорядкування, в першу чергу, в зв'язку із дослідженням локалізацій G–алгебр в певних максимальних ідеалах. Можливо, це буде зроблено в наступних роботах.

Множина $G \subset A^r$ зветься **мінімальною**, якщо $0 \notin G$ та якщо $\mathrm{lm}(g) \notin \langle lm(h), h \in G \setminus \{g\} \rangle$. Зрозуміло, що довільну стандартну базу може буде мінімізовано шляхом послідовного видалення тих елементів g, для яких $\mathrm{lm}(h)|\,\mathrm{lm}(g)$ для деякого $h \in G \setminus \{g\}$.

Для $f \in A^r$ та $G \subset A^r$ ми кажемо, що f є **зведеним (редукованим) відносно G**, якщо жодний моном з f не належить до $L(G)$. Множина $G \subset A^r$ зветься **зведеною**, якщо $0 \notin G$ та довільне $g \in G$ є зведеним відносно $G \setminus \{g\}$ та якщо, більш того, $g - \mathrm{lc}(g)\,\mathrm{lm}(g)$ є зведеним відносно G. Це означає, що для довільного $g \in G \subset A^r$, $\mathrm{lm}(g)$ не ділить жодного моному жодного елементу з $G \setminus \{g\}$ за винятком себе.

2.2 Нормальна форма та зведення

Definition 2.5. Нехай $\mathcal{G}$ позначає множину всіх скінчених та впорядкованих підмножин $G \subset A^r$.

1. Відображення $\mathrm{NF} : A^r \times \mathcal{G} \to A^r,\ (f, G) \mapsto \mathrm{NF}(f|G)$,
   зветься **нормальною формою** на A^r, якщо для всіх f та G,
   (i) $\mathrm{NF}(f|G) \neq 0 \Rightarrow \mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G)$,

(ii) $f - \mathrm{NF}(f|G) \in \langle G \rangle$.

NF зветься **зведеною нормальною формою**, якщо $\mathrm{NF}(f|G)$ є зведеною відносно G.

2. Нехай $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$. Зображення $f \in \langle G \rangle_l$,

$$f = \sum_{i=1}^{s} a_i g_i, \quad a_i \in R,$$

що задовольняє $\mathrm{lm}(f) \geq \mathrm{lm}(a_i g_i)$, $a_i g_i \neq 0 \ \forall \ i = 1 \ldots s$, якщо обидві сторони визначені, зветься **стандартним (лівим) зображенням** f (відносно G).

Нижче буде показано, що $\mathrm{NF}(f|G)$ не є єдиною, а зведена нормальна форма єдина. В застосуваннях нормальні форми є найбільш корисними тоді, коли G є стандартною базою для $\langle G \rangle$.

Lemma 2.6. Нехай $I \subset A^r$ є підмодулем, $G \subset I$ є стандартною базою I та $\mathrm{NF}(-|G)$ — нормальна форма на A^r відносно G.

1. Для довільного $f \in A^r$ маємо $f \in I \Leftrightarrow \mathrm{NF}(f|G) = 0$.
2. Якщо $J \subset A^r$ є підмодулем та $I \subset J$, тоді з $L(I) = L(J)$ випливає $I = J$. Зокрема, G породжує I як лівий A–модуль.
3. Зведена нормальна форма єдина.

Доведення. 1. Якщо $\mathrm{NF}(f|G) = 0$, тоді $f \in I$. Коли $\mathrm{NF}(f|G) \neq 0$, маємо $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G) = L(I)$, значить $\mathrm{NF}(f|G) \notin I$, з чого випливає $f \notin I$.

2. Нехай $f \in J$, припустимо, що $\mathrm{NF}(f|G) \neq 0$. Тоді $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G) = L(I) = L(J)$ —маємо протиріччя до $\mathrm{NF}(f|G) \in J$. Значить, $f \in I$ за 1).
3. Нехай $f \in A^r$; припустимо, що h, h' — дві зведені нормальні форми f відносно G. Тоді $h - h' \in \langle G \rangle_l = I$. Якщо $h - h' \neq 0$, маємо $\mathrm{lm}(h - h') \in L(I) = L(G)$ – протиріччя, так як $\mathrm{lm}(h - h')$ є мономом з h або h'.

$\square$

Для опису узагальненого алгоритму нормальної форми Бухбергера, введемо поняття s–поліному.

Definition 2.7. Нехай $f, g \in A^r \setminus \{0\}$ із $\mathrm{lm}(f) = x^\alpha e_i$ та $\mathrm{lm}(g) = x^\beta e_j$. Покладемо

$$\gamma := \big(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n)\big)$$

та означимо **лівий s–поліном** від f та g таким чином

$$\mathrm{spoly}(f, g) := \begin{cases} x^{\gamma-\alpha} f - \dfrac{\mathrm{lc}(x^{\gamma-\alpha} f)}{\mathrm{lc}(x^{\gamma-\beta} g)} x^{\gamma-\beta} g, & \text{якщо } i = j, \\ 0, & \text{якщо} i \neq j. \end{cases}$$

Зрозуміло, що $\mathrm{spoly}(f, g) \in A^r$ є поліномом тоді й тільки тоді, коли $r = 1$ та $f, g \in A$ й векторним поліномом в усіх інших випадках.

Remark 2.8. Легко побачити (з 1.5), що виконується $\mathrm{lm}(\mathrm{spoly}(f, g)) < \mathrm{lm}(f \cdot g)$.
Якщо $\mathrm{lm}(g) | \mathrm{lm}(f)$, тобто, скажімо, $\mathrm{lm}(g) = x^\beta e_i$, $\mathrm{lm}(f) = x^\alpha e_i$, тоді s–поліном має простішу форму, а саме

$$\mathrm{spoly}(f, g) = f - \frac{lc(f)}{lc(x^{\alpha-\beta} g)} x^{\alpha-\beta} g,$$

причому $\mathrm{lm}\big(\mathrm{spoly}(f, g)\big) < \mathrm{lm}(f)$. Для алгоритму нормальної форми, s–поліном буде використано саме в цій формі, в той час для алгоритму стандартної бази нам потрібна загальна формула. Задля того, щоб використовувати той самий вираз в обох алгоритмах, ми означили s–поліном саме так, а не в більш симетричній формі
$\mathrm{lc}(x^{\gamma-\beta} g) x^{\gamma-\alpha} f - \mathrm{lc}(x^{\gamma-\alpha} f) x^{\gamma-\beta} g$. Обидві форми є, зрозуміло, еквівалентними.

Припустимо, що в даній G–алгебрі, всі визначаючі коефіцієнти c_{ij} дорівнюють 1 (як приклад можна взяти універсальні обгортуючі алгебри скінченовимірних алгебр Лі). Тоді, коефіцієнти узагальненого s–поліному співпадають з їхніми прототипами комутативного випадку.

Algorithm 2.9. Нехай $<$ є гарним впорядкуванням на A^r.

LeftNF($f|G$)

Input: $f \in A^r,\ G \in \mathcal{G}$.

Output: $h \in A^r$, ліва нормальна форма f відносно G.

- $h = f$;
- WHILE ($h \neq 0$ та $G_h = \{g \in G \mid \operatorname{lm}(g) \mid \operatorname{lm}(h)\} \neq \emptyset$)
  вибрати довільний $g \in G_h$;
  $h = \operatorname{spoly}(h, g)$;
- return h;

Доведення. Скінченість та коректність алгоритму : Ми бачимо, що кожний специфічний вибір "довільного"в алгоритмі може давати нам нову нормальну форму. Нехай $h_0 := f$, та на i–му кроці WHILE–циклу ми обраховуємо $h_i = \operatorname{spoly}(h_{i-1}, g)$. Так як $\operatorname{lm}(h_i) = \operatorname{lm}(\operatorname{spoly}(h_{i-1}, g)) < \operatorname{lm}(h_{i-1})$ (за властивістю s–поліному), ми отримуємо множину $\{\operatorname{lm}(h_i)\}$ ведучих мономів h_i, де $\forall i$ ведучий моном h_{i+1} є строго меншим за ведучий моном h_i. Так як $<$ є гарним впорядкуванням, ця множина має мінімум, значить алгоритм є скінченим (тобто закінчує свою роботу за скінчену кількість кроків). Припустимо, цей мінімум досягнуто на m–му кроці. Нехай $h = h_m$, a_i є одночленом та $g_i \in G$. Після рекурсивних замін ми отримаємо наступний вираз:

$$h = f - \sum_{i=1}^{m-1} a_i g_i,$$

разом із властивістю $\operatorname{lm}(f) = \operatorname{lm}(a_1 g_1) > \operatorname{lm}(a_i g_i) > \operatorname{lm}(h_m)$.

Більш того, за побудовою, $\operatorname{lm}(h) \notin L(G)$. Це й доводить коректність, незалежно від специфічного вибору "довільного"в циклі WHILE. $\square$

Трансформуємо алгоритм LeftNF до алгоритму зведеної нормальної форми.

Algorithm 2.10. Нехай $<$ є гарним впорядкуванням на A^r.

redLeftNF

Input: $f \in A^r$, $G \in \mathcal{G}$

Output: $h \in A^r$, зведена нормальна форма f відносно G

- $h := 0,\ g = f$;
- WHILE ($g \neq 0$)
  $g = \operatorname{LeftNF}(g|G)$;
  $h = h + \operatorname{lc}(g)\operatorname{lm}(g)$;
  $g = g - \operatorname{lc}(g)\operatorname{lm}(g)$;
- return h;

Так як "хвіст"$g - \operatorname{lc}(g)\operatorname{lm}(g)$ поліному g має строго меншого ведучого моному ніж g, алгоритм є скінченим. Твердження про коректність цього алгоритму випливає з коректності LeftNF.

Аналогічним чином можна визначити поняття правих нормальних форм (red)RightNF. Тепер ми викладемо узагальнений Лівий Алгоритм Бухбергера.

Algorithm 2.11. Нехай $<$ є гарним впорядкуванням на A^r, припустимо, що дано алгоритм лівої нормальної форми LeftNF на A^r.

LeftStandard(G,LeftNF)

Input: Множина лівих породжуючих $G \in \mathcal{G}_l$

Output: Множина $S \in \mathcal{G}_l$, така що S є стандартною базою лівого підмодуля $I = \langle G \rangle \subset A^r$.

- $S = G$;
- $P = \{(f, g) | f, g \in S\} \subset S \times S$;
- WHILE ($P \neq \emptyset$)
  вибрати $(f, g) \in P$;
  $P = P \setminus \{(f, g)\}$;
  $h = \operatorname{LeftNF}\big(\operatorname{LeftSpoly}(f, g)|S\big)$;
  If ($h \neq 0$)
  $P = P \cup \{(h, f) | f \in S\}$;
  $S = S \cup h$;

- return S;

Remark 2.12. Якщо LeftNF є зведеною нормальною формою та G є зведеною множиною, тоді S є зведеною стандартною базою. Якщо G не є зведеною, ми можемо застосувати LeftNF після закінчення роботи алгоритму до $(f, S - \{f\})$ для всіх $f \in S$, щоб отримати зведену стандартну базу.

Задля доведення скінченості LeftStandard, нагадаємо, що якщо $h \neq 0$, тоді $\mathrm{lm}(h) \notin L(S)$ за властивістю 2.6.1). Значить, ми отримаємо строго спадаючу послідовність мономіальних підмодулів A^r, яка стабілізується завдяки нетеровості алгебри A. Це означає, що за скінченну кількість кроків ми матимемо $\mathrm{LeftNF}\big(\mathrm{spoly}(f,g)|S)\big) = 0$ для $(f,g) \in P$ й, після ще певної скінченої кількості кроків, множина пар P спорожніє.

Коректність випливає з застосування узагальненого фундаментального критерію Бухбергера стандартних баз.

Theorem 2.13 (Лівий Критерій Бухбергера)**.** Нехай $I \subset A^r$ є лівим підмодулем та $G = \{g_1, \dots, g_s\} \subset I$. Нехай $\mathrm{LeftNF}(-|G)$ є лівою нормальною формою на A^r відносно G.

Тоді наступні твердження еквівалентні:

1. G є лівою стандартною базою для I,
2. $\mathrm{LeftNF}(f|G) = 0$ для всіх $f \in I$,
3. кожний $f \in I$ має стандартне ліве зображення відносно G,
4. G породжує I як лівий модуль та $\mathrm{LeftNF}\big(\mathrm{LeftSpoly}(g_i, g_j)|G\big) = 0$ для $i, j = 1, \dots, s$.

Доведення. Імплікація ($1 \Rightarrow 2$) випливає з Леми 2.6, ($2 \Rightarrow 3$) — з відповідних означень. Доведемо імплікацію ($3 \Rightarrow 1$), з якої випливатиме еквівалентність ($1 \Leftrightarrow 3$). Припускаючи 3), ми бачимо, що $\mathrm{lm}(f)$ мусить виникати як ведучий моном $a_i g_i$ для деякого i. Це означає, що $\mathrm{lm}(g_i) | \mathrm{lm}(f)$ й, відповідно, випливає 1).

В доведенні 3) $\Rightarrow$ 4), відмітимо, що $h = \mathrm{LeftNF}\big(\mathrm{LeftSpoly}(f_i, f_j)|G\big) \in I$ й, значить, за 3), якщо $h \neq 0$, $\mathrm{lm}(h) \in L(G)$ за 3) — протиріччя зі властивістю (ii) нормальної форми. В Лемі 2.6 ми вже показали, що G породжує I.

Імплікація 4) $\Rightarrow$ 1) є важливим критерієм, що дозволяє перевірку й побудову стандартних баз за скінчену кількість кроків. Доведення використовує сизигії й тому перенесено до наступної секції (Теорема 4.3). $\square$

2.3 Алгоритм Двосторонніх Баз Грьобнера

Нехай $G = \{g_1, \dots, g_n\} \subset A$ є скінченою множиною елементів.

Lemma 2.14. Нехай $I = \langle G \rangle_2$ є двостороннім ідеалом, породженим G. Тоді, взагалі кажучи, існує певне $g \in I$, що не має стандартного двостороннього зображення типу 2.5.

Доведення. Іншими словами, ми не можемо записати

$$g = \sum_{i=1}^{n} l_i g_i r_i, \; l_i, r_i \in A, \text{ але } g = \sum_{i \in \Lambda} l_i g_i r_i \text{ для деякої множини індексів } \Lambda \text{ з } \#\Lambda \geq n.$$

Про справедливість твердження говорить очевидний контрприклад — розглянемо стандартне зображення універсальної обгортуючої алгебри Лі $U(\mathfrak{sl}_2)$, тобто, $\langle e, f, h \mid [e,f] = h, \; [h,e] = 2e, \; [h,f] = -2f \; \rangle$. Візьмемо ідеал $I = \langle f \rangle_2$ та поліном $f + efh \in U(\mathfrak{sl}_2)$. Тоді не існує таких $a, b \in U(\mathfrak{sl}_2)$, що $f + efh = afb$, а значить, в сумі мусить стояти більш ніж один доданок. $\square$

Remark 2.15. Ліві та праві ідеали в G–алгебрах мають стандартні ліві та, відповідно, праві зображення, як це було показано в 2.5. Це зображення є узагальненням відповідного зображення в комутативному випадку. Попередня Лема показує, що для таких важливих об'єктів, якими є двосторонні ідеали, не існує безпосереднього аналогу. Треба зазначити, що нетривіальні двосторонні ідеали, визначені множиною двосторонніх породжуючих, приховують важливу структурну інформацію. Наша ідея полягає в тому, щоб розглядати двосторонні структури як ліві (чи праві), еквівалентні даним. Алгоритм, наведений нижче, обраховує ліву стандартну базу даного двостороннього модуля. Ще раз ми засвідчуємося, що техніка баз Грьобнера допомагає нам виявити багато з прихованих даних. Велика кількість обрахованих прикладів підтвердила, що наші ідеї працюють як і очікувалося.

Algorithm 2.16. Нехай $<$ є гарним впорядкуванням на A^r та припустимо, що дано деякий алгоритм лівої нормальної форми NF = LeftNF на A^r.

StandardTwoSided(G,NF)

Input: Множина двосторонніх породжуючих $T \in \mathcal{G}_{two}$

Output: $L \in \mathcal{G}_l$, так що L є лівою стандартною базою двостороннього модуля $I = \langle T \rangle_2 \subset A^r$.

- L =LeftStandard$(T, \mathrm{NF}) = \{f_1, \ldots, f_m\}$;
- $W = \emptyset$; $Z = L$;
- LOOP

  For $i = 1$ to $\#Z$

  For $j = 1$ to n

  * g_i є i–м елементом Z
  * $g = g_i \cdot x_j$;
  * $h = NF\big(\mathrm{spoly}(g, g_i)|L\big)$;
  * IF $(h \neq 0)$

    $L = L \cup h$;

    $W = W \cup h$;

  If $W = \emptyset$ BREAK;

  $Z = W$;

  $W = \emptyset$;

  END LOOP
- L =LeftStandard(L, NF);
- return (L);

Доведення. Скінченість та коректність:

Так як A є нетеровою, довільний модуль є скінченопородженим, значить "вічний"цикл в алгоритмі буде перервано за скінчену кількість кроків. Ми почали з множини двосторонніх породжуючих T, порахували ліву стандартну базу її, як множини лівих породжуючих $Z = L$. Задля ефективності ми вимагаємо, щоб ця стандартна база була мінімальною. Тоді в циклі LOOP ... END LOOP ми додаємо в порожню спочатку множину W нові породжуючі, помножуючи справа елементи з Z на породжуючі $x_1, \ldots, x_n$, й зводячи результат відносно відомої бази L. Після того, як цикл LOOP ... END LOOP вперше завершено, ми вже порахували та додали до L всі ненульові нормальні форми $\{r_{ij}\}$ добутків $\{f_i x_j, f_i \in Z\}$. Для довільного $f_i \in Z$ та $x := x_j, y := x_k$ ми маємо наступне:

$$f_i \cdot xy = (\sum_p a_p f_p + r_{ij})y = \sum_q \left(\sum_p a_p b_q f_q + \sum_k a_p r_{ik} \right) + r_{ij} y.$$

Отже, єдиний елемент, що має бути зведено, це $r_{ij}y$, тобто достатньо продовжити подальшу роботу тільки з множиною W, яка складається на цьому кроці з $\{r_{ij}\}$. Ми виходимо з "вічного"циклу, коли $W = \emptyset$, тобто тоді, коли всі обраховані на поточному кроці "кандидати"(h в алгоритмі) є зведеними до нуля відносно бази L. Це означає, що L є повною базою. Останній підрахунок стандартної бази має скоріше косметичне значення — база L може мати досить багато зайвих (себто продубльованих) елементів, й тому є сенс її мінімізувати. □

2.4 Застосування

Нехай $\mathbb{K}$ є полем, $A = \langle x_1, \ldots, x_n \mid x_j x_i = c_{ij} x_i x_j + d_{ij}(x) \rangle$ є G–алгеброю від n змінних та $<$ є мономіальним впорядкуванням на A^r.

1) Еквівалентність модулів

Припустимо RedMinStd(module I) — це алгоритм, що обчислює зведену мінімальну стандартну базу I. Якщо для двох модулів I та J RedMinStd(I)=RedMinStd(J), тоді I та J

належать до одного й того ж класу ізоморфізму. (Дивись також 2.6,2).

2) Належність елемента підмодулю

Нехай $I \subseteq A^r$ є підмодулем, $f \in A^r$ та $S = \{f_1, \ldots, f_m\}$ стандартна база I, тоді $f \in I$ тоді й тільки тоді, коли $\mathrm{NF}(f|S) = 0$. (Дивись також 2.6,1).

3) Перетин із підалгебрами

На відміну від комутативного випадку, не кожна підмножина множини породжуючих G–алгебри породжує нетривіальну підалгебру (тобто ту, що не співпадає з усією алгеброю). Таким чином, замість поняття "виключення"(англ. elimination), ми використовуємо скоріше "перетин із підалгеброю", так як взагалі виключення класичного типу може й не мати місця. Хоча, ми можемо "виключати"довільні комутативні підалгебри, породжені підмножиною множини породжуючих, наприклад довільні однопороджені підалгебри такого типу.

Definition 2.17. Нехай $A = A_x \otimes_{\mathbb{K}} A_y$, де A_x (відп. A_y) є G–алгебра від n (відп. m) змінних $\mathbf{x} = (x_1, \ldots, x_n)$ (відп. $\mathbf{y} = (y_1, \ldots, y_m)$). Тоді, за 3.5, A є G–алгеброю від $n + m$ змінних. Припустимо ми маємо гарне впорядкування $>_1$ на $\mathbf{x}$ та деяке довільне впорядкування $>_2$ на $\mathbf{y}$. Блокове впорядкування $(>_1, >_2)$ на A зветься **впорядкуванням виключення** відносно $x_1, \ldots, x_n$, якщо для $g \in A$ та $\mathrm{lm}(g) \in A_y$ має місце $g \in A_y$.

Lemma 2.18. Нехай $I \subseteq A$ є ідеалом. Припустимо, що $B = \langle x_{r+1}, \ldots, x_n \mid x_j x_i = c_{ij} x_i x_j + d_{ij}(x) \rangle$ є нетривіальною підалгеброю A, та $<$ є впорядкуванням виключення на A відносно $x_1, \ldots, x_r$. Якщо $S = \{f_1, \ldots, f_m\}$ є стандартною базою I, тоді $S \cap B$ є стандартною базою $I \cap B$.

Доведення. Проаналізуємо

$$L(I \cap B) = \langle \{L(f) | f \in I \cap B\} \rangle = L(I) \cap \langle \{L(f) | f \in B\} \rangle.$$

Так як $<$ є впорядкуванням виключення відносно B, $\langle \{L(f) | f \in B\} \rangle = B$ та

$$L(I \cap B) = L(I) \cap B = \langle L(f_1), \ldots, L(f_m) \rangle \cap B = S \cap B.$$

□

4) Перетин із підмодулями

Нехай $I \subseteq A^r = \sum_{i=1}^{r} A e_i$ є підмодулем. Припустимо, що впорядкування на A^r означено таким чином: $x^\alpha e_i < x^\beta e_j \Leftrightarrow j < i$ або $j = i$ та $x^\alpha < x^\beta$. Нехай $S = \{f_1, \ldots, f_m\}$ є стандартною базою I, тоді $S \cap \sum_{i=s}^{r} A e_i$ є стандартною базою $I \cap \sum_{i=s}^{r} A e_i$.

5) Перетин ідеалів

Нехай $I = \langle f_1, \ldots, f_r \rangle$, $J = \langle g_1, \ldots, g_s \rangle$ є ліві (чи праві) ідеали з A. Розглянемо ідеал $D := t \cdot I + (1 - t) \cdot J \subseteq A[t]$, де $A[t]$ є G–алгеброю, породженою $x_1 \ldots x_n, t$, причому t комутує з A. Тоді $I \cap J = D \cap A$.

Доведення. Припустимо, що $\{f_i\}$ та $\{g_i\}$ є стандартними базами I та, відповідно, J. Нехай $f \in D \cap A$. Тоді ми можемо представити його як суму

$$f = \sum_{i=1}^{r} a_i t f_i + \sum_{i=1}^{s} b_i (1 - t) g_i,$$

Надаючи t деяке значення, ми отримуємо :

$$t = 0 \Rightarrow f = \sum_{i=1}^{s} b_i g_i \in J, \; t = 1 \Rightarrow f = \sum_{i=1}^{r} a_i f_i \in I.$$

Значить, $f \in I \cap J$ та $I \cap J \supseteq D \cap A$.
З іншого боку, нехай $f \in I \cap J$. Тоді f може бути представлено двома варіантами :

$$f = \sum_{i=1}^{r} a_i f_i = \sum_{i=1}^{s} b_i g_i.$$

Так як t комутує з A, розглянемо

$$f = tf + (1-t)f = \sum_{i=1}^{r} t a_i f_i + \sum_{i=1}^{s} (1-t) b_i g_i = \sum_{i=1}^{r} a_i t f_i + \sum_{i=1}^{s} b_i (1-t) g_i.$$

Звідси $f \in D \cap A$ та $I \cap J = D \cap A$. $\square$

3 GR–алгебри та бази Грьобнера в факторалгебрах

Definition 3.1. Алгебра A зветься **алгеброю Грьобнера** чи просто GR–**алгеброю**, якщо існує деяка невироджена заміна змінних $\phi : A \to A$ та гарне впорядкування $<_A$, такі, що $\phi(A)$ є або G–алгеброю від n змінних для певного $n \in \mathbb{N}$,
або для певного $m \in \mathbb{N}$ існує G–алгебра від m змінних B та двосторонній ідеал $I \subset B$, так що $\phi(A) \cong B/I$.

Зрозуміло, що довільна GR–алгебра є нетеровою алгеброю PBW типу.
Довільному класу $[f] \in A \setminus \{[0]\}$ поставимо у відповідність його *канонічного представника* $\overline{f} := \mathrm{RedNF}_B(f \mid I)$. Так як зведена нормальна форма є єдиною, ототожнюватимемо клас $[f]$ з його канонічним представником $\overline{f}$. Працюючи з GR–алгебрами $A = B/I$, завжди припускатимемо, що нетривіальний двосторонній ідеал I подано в його лівій стандартній базі (яка може бути обчисленою за допомогою алгоритму StandardTwoSided).

Definition 3.2. Нехай $A = B/I$ є GR–алгеброю із n змінними.

1) Для деякого $\alpha \in \mathbb{N}^n$, x^α зветься **мономом** в A , якщо $\overline{x^\alpha} \neq 0$ та $x^\alpha = \overline{x^\alpha}$. Множиною мономів A є підмножина PBW бази B, а саме $\mathrm{Mon}(A) = \{\mathrm{lm}_B(\overline{x^\alpha}) \mid \alpha \in \mathbb{N}^n\} \setminus \{0\}$.

2) Впорядкування $<=<_A$ зветься **мономіальним впорядкуванням на** A, якщо виконуються наступні умови:

- $\forall\ \alpha, \beta \in \mathbb{N}^n$ таких, що x^α та x^β є мономами, $\alpha < \beta \Rightarrow x^\alpha <_A x^\beta$
- $\forall\ \alpha, \beta, \gamma\ \in \mathbb{N}^n$, таких, що x^α та x^β є мономами, та мають місце нерівності $x^\alpha <_A x^\beta$, $\overline{x^{\alpha+\gamma}} \neq 0$, $\overline{x^{\beta+\gamma}} \neq 0$, тоді $\overline{x^{\alpha+\gamma}} <_A \overline{x^{\beta+\gamma}}$.

3) Довільний $\overline{f}$ може бути записаним єдиним чином як сума $\overline{f} = cx^\alpha + f'$, де $c \in K^*$ та $x^{\alpha'} <_A x^\alpha$ для довільного ненульового одночлену $c'x^{\alpha'}$ з запису f'. Ми означимо $\mathrm{lm}([f]) := \mathrm{lm}(\overline{f}) = x^\alpha$, **ведучий моном** $[f]$, відповідно $\mathrm{lc}([f]) := c$, **ведучий коефіцієнт** $[f]$.

Для довільного $[f] \in A$ та ідеалу $J \subset A$ ми обраховуємо нормальну форму наступним чином: $\mathrm{NF}_A([f] \mid J) := \mathrm{NF}_B(f \mid \tilde{J})$, $\tilde{J} :=$LeftStandard$(I + J, \mathrm{NF})$. Відповідно, має місце наступна лема:

Lemma 3.3. Нехай $A = B/I$ є GR–алгеброю та ідеал $J \subset A$. Нехай $F = \{f_1, \ldots, f_k\}$ є стандартною базою ідеалу $I + J \subseteq B$. Тоді множина $\{\mathrm{RedNF}(f_i \mid I) \mid 1 \leq i \leq k\} \setminus \{0\}$ є стандартною базою $J \subset A$.

Example 3.4 (Приклади GR–алгебр)**.** Факторалгебри довільних G–алгебр за нетривіальними двосторонніми ідеалами, й серед них такі важливі алгебри: зовнішні алгебри, алгебри Кліффорда, скінченовимірні асоціативні алгебри задані структурними константами ([DK]) тощо.

Скінченовимірні асоціативні алгебри

Хоча скінченовимірні алгебри не належали до початкових цілей дослідження, вони гарно пасують до розробленої теорії та можуть бути використані в Системі Комп'ютерної Алгебри Singular:Plural.
Розглянемо A, скінченовимірну асоціативну алгебру над полем $\mathbb{K}$, задану структурними константами (докладніше див. [DK]). Нехай $x_1, \ldots, x_n$ є породжуючими алгебри разом із співвідношеннями $\forall i, j\ x_i x_j = \sum_{k=1}^{n} \gamma_{ij}^k x_k$, де γ_{ij}^k є *структурними константами.* subject to relations INSERT.

Спочатку, визначимо асоціативну нескінченовимірну $\mathbb{K}$–алгебру B, породжену $x_1, \dots, x_n$ із співвідношеннями

$$x_j x_i = x_i x_j - \sum_{k=1}^{n} \gamma_{ij}^k x_k + \sum_{k=1}^{n} \gamma_{ji}^k x_k = x_i x_j + \sum_{k=1}^{n} (\gamma_{ji}^k - \gamma_{ij}^k) x_k.$$

Зрозуміло, що довільне степеневе гарне впорядкування є допустимим на B. Умови невиродженості в цьому випадку видають наступні обмеження : INSERT
, які співпадають із оригінальними в означенні скінченовимірних алгебр.

Тому B є G–алгеброю від n змінних. Тепер ми можемо розглянуті співвідношення, що залишились, як двосторонній ідеал $I \subseteq B$, визначений

$$I = \left\langle \{x_i x_j - \sum_{k=1}^{n} \gamma_{ij}^k x_k \mid 1 \le i \le j \le n\} \right\rangle,$$

і зробити висновок, що $A \cong B/I$ є GR–алгеброю.

Lemma 3.5. Категорія GR–алгебр є замкненою відносно операцій тензорного добутку над полем та фактору за модулем двостороннього ідеалу.

4 Сизигії та вільні резольвенти

Нехай $\mathbb{K}$ є полем та $<$ є гарним мономіальним впорядкуванням на A^r.

В цьому розділі ми опишемо узагальнений метод обрахунку сизигій та вільних резольвент модулів, який використовує стандартні бази. Сизигії (англ. syzygies, в однині syzygy) та вільні резольвенти (англ. free resolutions) є доволі важливими об‘єктами та, водночас, базовими інгредієнтами для багатьох конструкцій, зокрема, в гомологічній алгебрі. З іншого боку, використовуючи сизигії, ми отримали елегантне доведення Критерію Стандартних Баз Бухбергера.

Definition 4.1. Ліва (відповідно **права) сизигія** від k елементів $f_1, \dots, f_k \in A^r = \overset{r}{\underset{i=1}{\oplus}} Ae_i$ є набором з k елементів $(g_1, \dots, g_k) \in A^k$, що має місце

$$\sum_{i=1}^{k} g_i f_i = 0 \qquad \Big(\sum_{i=1}^{k} f_i g_i = 0 \Big).$$

Множина лівих (правих) сизигій від $f_1, \dots, f_k$ утворює лівий (правий) підмодуль $S \subseteq A^k$. Враховуючи аналогічність лівих та правих сизигій, надалі працюватимемо із лівими сизигіями. Ми використовуватимемо поняття "сизигія"та NF (нормальна форма), маючи на увазі ліві сизигії та LeftNF (ліва нормальна форма).

Неважко помітити, що S є ядром гомоморфізму вільних A–модулів

$$\varphi_1 : F_1 := \overset{k}{\underset{i=1}{\oplus}} A\varepsilon_i \longrightarrow F_0 := \overset{r}{\underset{i=1}{\oplus}} Ae_i,$$
$$\varepsilon_i \longmapsto f_i,$$

де через e_i (відп. ε_i) позначено канонічну базу A^r (відп. A^k). φ_1 відображається на лівий підмодуль $I = \langle f_1, \dots, f_k \rangle$ та $\operatorname{syz} I = \operatorname{Ker} \varphi_1$ зветься **модулем сизигій** від I відносно породжуючих $f_1, \dots, f_k$. Неважко впевнитися, що клас ізоморфізму $\operatorname{syz} I$ як A–модулю залежить лише від класу ізоморфізму I, зокрема, він є незалежним від обраної множини породжуючих.

Тепер, введемо мономіальне впорядкування на F_1, яке має гарні властивості відносно стандартних баз. Вперше це було введено та використано Ф.-О. Шрайєром.

$$\begin{aligned} x^\alpha \varepsilon_i >_1 x^\beta \varepsilon_j \Leftrightarrow & \operatorname{lm}(x^\alpha f_i) >_0 \operatorname{lm}(x^\beta f_j) \text{ або} \\ & \operatorname{lm}(x^\alpha f_i) = \operatorname{lm}(x^\beta f_j) \text{ та } i < j. \end{aligned}$$

Зліва, $>_1$ позначає нове впорядкування на F_1, з правого боку $>_0$ є впорядкуванням на F_0, які, втім, індукують те й саме впорядкування на A. Впорядкування $>_1$ зветься **Шрайєрівським впорядкуванням**. Зрозуміло, що воно є залежним від $f_1, \dots, f_k$.

Нашою ціллю є доведення Критерію Бухбергера, який стверджує, що множина $G = \{f_1, \ldots, f_k\}$ є стандартною базою I, якщо для всіх $i < j$, $\mathrm{NF}\big(\mathrm{spoly}(f_i, f_j)|G\big) = 0$. Наше доведення використовує сизигії, та містить також вивід узагальнення Шрайєрівського результату про те, що в комутативному кільці сизигії, обчислені зі стандартного зображення $\mathrm{spoly}(f_i, f_j)$ є стандартною базою $\mathrm{syz}\, I$ відносно Шрайєрівського впорядкування.

Домовленості та позначення: Припустимо, дано деяку нормальну форму NF на A^r. Для кожної пари $i < j$, що f_i та f_j мають ведучого монома в одній і тій самій компоненті, скажімо, $\mathrm{lm}(f_i) = x^{\alpha_i} e_\nu$, $\mathrm{lm}(f_j) = x^{\alpha_j} e_\nu$, визначимо моном

$$m_{ji} := x^{\gamma - \alpha_i} \in A,$$

де $\gamma_l = \max(\alpha_{il}, \alpha_{jl})$. Позначивши $c_i = \mathrm{lc}(m_{ji} f_i)$ та $c_j = \mathrm{lc}(m_{ij} f_j)$, тоді

$$m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j = \mathrm{spoly}(f_i, f_j).$$

Припустимо тепер, що $i < j$ та $\mathrm{NF}\big(\mathrm{spoly}(f_i, f_j) \mid G\big) = 0$.

Тоді ми маємо стандартне зображення

$$m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j = \sum_{\nu=1}^{k} a_\nu^{(ij)} f_\nu, \;\; a_\nu^{(ij)} \in A.$$

Для кожної пари $i < j$, що $\mathrm{lm}(f_i)$ та $\mathrm{lm}(f_j)$ мають одну й ту ж компоненту, означимо

$$s_{ij} = m_{ji} \varepsilon_i - \frac{c_i}{c_j} m_{ij} \varepsilon_j - \sum_{\nu} a_\nu^{(ij)} \varepsilon_\nu.$$

Зрозуміло, що тоді $s_{ij} \in \mathrm{syz}\, I$ та вірне наступне твердження:

Lemma 4.2. $\mathrm{lm}(s_{ij}) = m_{ji} \varepsilon_i$.

Доведення. Так як $\mathrm{lm}(m_{ij} f_j) = \mathrm{lm}(m_{ji} f_i)$, за означенням $>_1$ (враховуючи, що $i < j$) маємо $\mathrm{lm}(m_{ji} \varepsilon_i) >_1 \mathrm{lm}(m_{ij} \varepsilon_j)$. З властивості стандартного зображення в свою чергу отримуємо

$$\mathrm{lm}(a_\nu^{(ij)} f_\nu) \leq \mathrm{lm}(m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j) < \mathrm{lm}(m_{ji} f_i),$$

звідки й випливає твердження. □

Theorem 4.3. Нехай $G = \{g_1, \ldots, g_s\}$ є множиною породжуючих підмодулю $I \subset A^r$, що задовольняє, для деякої нормальної форми NF на A^r

$$\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0, \; i < j.$$

Тоді вірні наступні твердження:

1. G є стандартною базою I.
2. $\{s_{ij}\}$, побудовані вище, є стандартною базою $\mathrm{syz}\, I$ відносно Шрайєрівського впорядкування. Зокрема, $\{s_{ij}\}$ породжують $\mathrm{syz}\, I$.

Доведення. Ми доводитимемо 1) та 2) водночас.

Візьмемо довільний $f \in I$ та його прообраз $g \in F_1$,

$$g = \sum_{i=1}^{s} a_i \varepsilon_i, \; f = \varphi(g) = \sum_{i=1}^{s} a_i g_i.$$

Це завжди можливо, так як G породжує I.

У випадку 1), покладемо $f \neq 0$, у випадку 2) $f = 0$. Нехай $h = \sum h_j \varepsilon_j \in F_1$ є нормальною формою g відносно $\{s_{ij}\}$ для деякої нормальної форми на F_1 (нам досить знати, що така існує). Розглянемо стандартне зображення $g - h$,

$$g = \sum a_{ij} s_{ij} + h, \; a_{ij} \in A,$$

Якщо $h \neq 0$, $\mathrm{lm}(h) = \mathrm{lm}(h_\nu) \cdot \varepsilon_\nu$ для деякого ν та $\mathrm{lm}(h) \notin L(\{s_{ij}\}) = \langle\{m_{ji}\varepsilon_i\}\rangle$ за Лемою 4.2. Звідси $m_{j\nu} \nmid \mathrm{lm}(h_\nu)$ для всіх j. Так як $g - h \in \langle\{s_{ij}\}\rangle \subset \mathrm{syz}\, I$, ми отримаємо

$$f = \varphi(g) = \varphi(h) = \sum h_j g_j.$$

Припустимо, що для деякого $j \neq \nu$, $\mathrm{lm}(h_j g_j) = \mathrm{lm}(h_\nu g_\nu)$. Тоді $\mathrm{lm}(h_\nu g_\nu)$ ділиться на $\mathrm{lm}(g_\nu)$ й на $\mathrm{lm}(g_j)$.

Таким чином, ми маємо наступну ситуацію: позначимо мономи $\mathrm{lm}(h_j) = x^c, \mathrm{lm}(g_j) = x^d$, $\mathrm{lm}(h_\nu) = x^a, \mathrm{lm}(g_\nu) = x^b$, тоді $\mathrm{lm}(h_j g_j) = \mathrm{lm}(\mathrm{lm}(h_j)\,\mathrm{lm}(g_j)) = \mathrm{lm}(x^c x^d) = x^{c+d}$, й, за аналогією, $\mathrm{lm}(h_\nu g_\nu) = x^{a+b}$, звідки $x^{a+b} = x^{c+d}$, або $a_i + b_i = c_i + d_i$ для кожної компоненти $i \geq 1$ векторів a, b, c, d. Так як $d_i = a_i + b_i - c_i$, то $e_i := \max(b_i, d_i) \leq a_i + b_i$, значить $x^e | x^{a+b}$ й більш того,

$$x^e = \mathrm{lm}(x^b x^{e-b}) = \mathrm{lm}(\mathrm{lm}(g_\nu) m_{j\nu}) = \mathrm{lm}(g_\nu m_{j\nu}),$$

звідки $\mathrm{lm}(h_\nu g_\nu) = \mathrm{lm}(h_\nu\, \mathrm{lm}(g_\nu))$ ділиться на $\mathrm{lm}(g_\nu m_{j\nu}) = \mathrm{lm}(g_\nu\, \mathrm{lm}(m_{j\nu}))$. В експоненціальному вигляді це означає, що $x^{b'+b} \mid x^{a+b}$, де $x^{b'} = x^{e-b} = m_{j\nu}$, й $b' \leq a$, тобто сам $m_{j\nu}$ ділить $\mathrm{lm}(h_\nu)$, що є протиріччям.

У випадку 1) отримуємо $\mathrm{lm}(f) = \mathrm{lm}(h_\nu g_\nu) \in L(G)$, У випадку 2) це свідчить про те, що припущення $h \neq 0$ веде до протиріччя. В випадку 1) G є, за означенням, стандартною базою. В випадку 2) $\{s_{ij}\}$ є стандартною базою за теоремою 2.13, 2) $\Rightarrow$ 1). ☐

Ще одним аргументом на користь використання методу Шрайєра є те, що за його допомогою ми можемо, наприклад, довести слабку теорему Гільберта про сизигії в G–алгебрах, що стверджує, що довільний A–модуль має вільну резольвенту, довжина якої не перевищує кількості змінних в алгебрі.

Lemma 4.4. Нехай $G = \{g_1, \ldots, g_s\}$ є стандартною базою (з попарно нерівними елементами) підмодулю $I \subset A^r = \sum\limits_{i=1}^{r} Ae_i$, такою що $\mathrm{lm}(g_i) \in \{e_1, \ldots, e_r\}$. Нехай J є множиною індексів j, для яких $e_j \notin \{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\}$. Тоді

$$I = \bigoplus_{i=1}^{s} Ag_i, \quad A^r/I \cong \bigoplus_{j \in J} Ae_j.$$

Доведення. Множина $G \cup \{e_j | j \in J\}$ є лінійно незалежною відносно A, так як такими є ведучі одночлени. Значить, обидві суми в твердженні є прямими. Для $f \in A^r$ розглянемо стандартне зображення

$$f = \sum_{i=1}^{s} a_i g_i + h, \ \mathrm{lm}(h) \notin L(G).$$

Звідси видно, що $h \in \sum\limits_{j \in J} Ae_j$, а значить, результат є вірним. ☐

Lemma 4.5. Нехай $G = \{g_1, \ldots, g_s\}$ є стандартною базою $I \subset A^r$, сортованою таким чином, щоб виконувалося наступне: для $i < j$ та $\mathrm{lm}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{lm}(g_j) = x^{\alpha_j} e_\nu$ для деякого ν, тоді $\alpha_i \geq \alpha_j$ лексикографічно. Нехай s_{ij} позначає сизигії, визначені вище. Припустимо, що $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)$ не залежать від змінних $x_1, \ldots, x_k$. Тоді $\mathrm{lm}(s_{ij})$, взяті відносно Шрайєрівського впорядкування, не залежать від $x_1, \ldots, x_{k+1}$.

Доведення. Розглянемо деякий s_{ij}. Ми знаємо, що тоді $i < j$ та $\mathrm{lm}(g_i)$ й $\mathrm{lm}(g_j)$ мають спільну компоненту, скажімо, e_ν. Згідно припущення, $\mathrm{lm}(g_i) = x^{\alpha_i} e_\nu$ та $\mathrm{lm}(g_j) = x^{\alpha_j} e_\nu$ задовольняють $\alpha_i = (0, \ldots, 0, \alpha_{i,k+1}, \ldots)$ та $\alpha_j = (0, \ldots, 0, \alpha_{j,k+1}, \ldots)$ разом із $\alpha_{i,k+1} \geq \alpha_{j,k+1}$. Таким чином, $\mathrm{lm}(s_{ij}) = m_{ji} e_i$ (де $\exp_t(m_{ji}) = \max(\alpha_{it}, \alpha_{jt}) - \alpha_{it}$) не мають x_{k+1} множником. ☐

Застосовуючи лему до вищих модулів сизигій, отримаємо наступну теорему, яка є вірною для довільного скінченопородженного A–модулю, а не тільки для підмодулів вільних модулів скінченого рангу.

Theorem 4.6. Нехай $>$ є гарним мономіальним впорядкуванням на A. Тоді довільний скінченопороджений A–модуль M має вільну резольвенту

$$0 \longrightarrow F_m \longrightarrow F_{m-1} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

(де F_i — вільні A–модулі) довжини $m \leq n$. Зокрема, $\mathrm{gl.dim}\, A \leq n$.

Доведення. Так як A є нетеровим, M представляється як

$$0 \longrightarrow I \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

де $F_0 = \sum\limits_{i=1}^{r_0} Ae_i$. Нехай $G = \{g_1, \dots, g_s\}$ є стандартною базою I; припустимо $\mathrm{lm}(g_i)$ не залежить від змінних $x_1, \dots, x_k$, $k \geq 0$. За теоремою 4.3, сизигії s_{ij} формують стандартну базу $\operatorname{syz} I$. За лемою 4.5 отримуємо, що $\mathrm{lm}(s_{ij})$ не залежить від $x_1, \dots, x_{k+1}$. Значить, має місце наступна точна послідовність

$$0 \longrightarrow \operatorname{Ker} \varphi_1 = \operatorname{syz} I \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0,$$

де $F_1 = \sum\limits_{i=1}^{r_1} A\varepsilon_i$, $\varphi_1(\varepsilon_i) = g_i$, $r_1 = s$. За індукцією, будуємо точну послідовність

$$0 \longrightarrow \operatorname{Ker} \varphi_{n-k} \longrightarrow F_{n-k} \xrightarrow{\varphi_{n-k}} F_{n-k+1} \longrightarrow \dots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0,$$

де F_i є вільним рангу r_i та $\operatorname{Ker} \varphi_{n-k}$ дано як стандартну базу $\{s_{ij}^{(n-k)}\}$ таким чином, щоб жодна змінна не з'являлася в $\mathrm{lm}(s_{ij}^{(n-k)})$. За Лемою 4.4, $F_{n-k}/\operatorname{Ker} \varphi_{n-k}$ є вільним модулем. Підставляючи $F_{n-k}/\operatorname{Ker} \varphi_{n-k}$ замість F_{n-k}, отримуємо шукану вільну резольвенту. □

Як підсумок цього розділу, подамо алгоритм побудови (не мінімальних) вільних резольвент.

Algorithm 4.7. Нехай $>$ є гарним мономіальним впорядкуванням на A^r.

LeftSResolution

Input: Матриця $G = (g_1, \dots, g_t)$, $g_k \in A^r$ — стандартна база $I = \langle G \rangle \subset A^r$.

Output: Матриці F_i розміру (r_{i-1}, r_i), $i = 1, \dots, n$, такі що

$$0 \longleftarrow A^r/I \longleftarrow A^{r_0} \longleftarrow \dots \longleftarrow A^{r_{i-1}} \xleftarrow{F_i} A^{r_i} \longleftarrow \dots$$

є резольвентою.

- $F_1 = (g_1, \dots, g_t)$;
- Для $i < j$ обрахувати стандартне зображення $\mathrm{spoly}(g_i, g_j) = \sum\limits_{v=1}^{k} a_v^{(ij)} g_v$
  $s_{ij} := m_{ji}\varepsilon_i - \frac{c_i}{c_j} m_{ij}\varepsilon_j - \sum\limits_{v} a_v^{(ij)} \varepsilon_v$;
- $F_2 = (s_{12}, \dots, s_{t-1,t})$;
- Змінити мономіальне впорядкування на Шрайєрівське відносно $g_1, \dots, g_t$;
- result $= \{F_1\} \cup$ LeftSResolution (F_2);
- return(result);

5 Система Комп'ютерної Алгебри

Система Комп'ютерної Алгебри для Некомутативних Поліноміальних Алгебр Singular:Plural розробляється в Центрі Комп'ютерної Алгебри Університету Кайзерслаутерн, Німеччина. Розробка ведеться колективом з Кайзерслаутерну, Києва та Фрайбургу (проф. Г.-М. Гройль,проф. Ю.А. Дрозд, В. Левандовський, А.Хоменко, Х. Шьонеман). Система буде доступна як пакет (розширення ядра) до широко відомої вільно розповсюджуваної Системи Комп'ютерної Алгебри Singular ([GPS]). Багато з описаних вище алгоритмів вже впроваджено, в той час як деякі ще чекають на ефективну реалізацію. Автор пропонує колегам–науковцям надсилати за електронною адресою `brand@ukrsat.com` (чи `levandov@mathematik.uni-kl.de`) запити й обчислювальні проблеми.

Література

[AJ] A. Josef, "Quantum Groups And Their Primitive Ideals", Springer, 1995

[AP] J. Apel, "Gröbnerbasen in nichtkommutativen Algebren und Ihre Anwendung", Dissertation, Universität Leipzig, 1988

[BR] G. Benkart, T.Roby "Down–up algebras", J. Algebra 209, No 1., 305-344 (1998)

[Dix] J. Dixmier "Enveloping Algebras", North-Holland, 1977

[DK] Ю. Дрозд, В. Кириченко, "Конечномернэе алгебрэ", Київ, Вища школа, 1980

[GPS] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 2.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2001). `http://www.singular.uni-kl.de`

[GPa] G.-M. Greuel, G. Pfister: Gröbner bases and algebraic geometry. In: B. Buchberger and F. Winkler (ed.): Gröbner Bases and Applications.,109 - 143, 1998.

[GPb] G.-M. Greuel, G. Pfister, with contributions by O. Bachmann and H. Schönemann, "A SINGULAR Introduction to Commutative Algebra", Springer Verlag, to appear in 2002.

[Gr] Green, E. Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases, Journal of Symbolic Computation Vol.29 No. 4/5, 2000.

[HKP] M. Havlicek, A. Klimyk, S. Posta, "Central elements of the algebras $U_q'(\mathrm{so}_m)$ and $U_q'(\mathrm{iso}_m)$", arXiv.math.QA/9911130

[IPR] A. Isaev, P. Pyatov, V. Rittenberg, "Diffusion algebras", arXiv.math.QA/0103603

[KS] A.Klimyk; K.Schmüdgen, "Quantum groups and their representations", Texts and Monographs in Physics. Berlin: Springer. xix, 552 p. (1997)

[KW] A.Kandri-Rody, V.Weispfenning "Non–commutative Gröbner bases in algebras of solvable type", J. of Symbolic Computation 9, No.1, 1-26 (1990)

[LV] В. Левандовський, "Застосування теорії баз Грьобнера до універсальних обгортуючих алгебр Лі", Київський Університет, 1998

[LV2] V.Levandovskyy, "Gröbner bases of a class of non–commutative algebras", Universität Kaiserslautern, 2000