

IDENTIFIKASI BASIS GRÖBNER DALAM IDEAL RING POLINOMIAL

Melky M. Romsery¹, Henry W. M. Patty², Mozart W. Talakua³

^{1,2,3} Jurusan Matematika FMIPA Universitas Pattimura
Jl. Ir. M. Putuhena, KampusUnpatti, Poka-Ambon, Indonesia
e-mail: ²henrywmpatty81@gmail.com

Abstrak

Dalam suatu ring atau lapangan, dapat didefinisikan suatu polinomial yang koefisien-koefisiennya merupakan elemen dari ring atau lapangan tersebut. $R[X]$ dan $F[X]$ merupakan suatu ring yang disebut ring polinomial. Misalkan $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq F[X]$, dengan $f_i \neq 0$ untuk setiap $i = \{1, 2, 3, \dots, s\}$. Suatu polinomial $f \in F[X]$ merupakan elemen di I jika f dapat ditulis sebagai kombinasi linier dari f_i yaitu $f = q_1 f_1 + q_2 f_2 + \dots + q_s f_s$ dengan $q_i \in F[X]$. Untuk mengubah f menjadi kombinasi linier, maka dapat digunakan algoritma pembagian polinomial bervariabel banyak tetapi dengan syarat sisa pembagian adalah nol. Pada polinomial bervariabel banyak, sisa pembagiannya tidak tunggal tergantung pada urutan f_1, f_2, \dots, f_s . Dikatakan tidak tunggal karena jika sisa pembagiannya nol, tetapi setelah merubah urutan f_1, f_2, \dots, f_s akan dihasilkan sisa pembagian yang bukan nol. Oleh karena itu, untuk menyelesaikan masalah keanggotaan ideal tersebut, maka harus dicari himpunan pembangun yang lain dari I yang disebut basis Gröbner. Basis Gröbner pada I adalah himpunan semua polinomial $\{g_1, g_2, \dots, g_s\}$ dalam I sedemikian sehingga untuk sebarang $f \in I$ terdapat $LT(g_i)$ habis membagi $LT(f)$ dengan $i = 1, 2, \dots, s$. Dari hasil penelitian dapat disimpulkan bahwa setiap ideal yang merupakan ideal polinomial dalam $F[X]$ mempunyai basis Gröbner. Untuk mengetahui apakah suatu basis merupakan basis Gröbner maka digunakan kriteria Buchberger. Sedangkan untuk mendapatkan basis Gröbner dari suatu ideal polinomial digunakan algoritma Buchberger.

Kata Kunci: Algoritma Buchberger, basis Gröbner, himpunan pembangun, ideal, kriteria Buchberger, ring, ring polinomial.

IDENTIFY GROBNER BASES IN IDEAL OF POLYNOMIAL RING

Abstract

In a ring or field, it was able to define a polynomial which all coefficients are elements of the ring or field. The set of all polynomials with indeterminate X and coefficient in ring R denoted by $R[X]$. It was same with $F[X]$, the set of polynomials which coefficient in field F . $R[X]$ and $F[X]$ is a ring which called polynomial ring. Let $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq F[X]$, with $f_i \neq 0$ for every $i = \{1, 2, \dots, s\}$. A polynomial $f \in F[X]$ is element in I if f could form linier combination of f_i such that $f = q_1 f_1 + q_2 f_2 + \dots + q_s f_s$ with $q_i \in F[X]$. To transform f such a linier combination, then used division algorithm for multivariable polynomials with condition Methe reminder must be zero. But, in multivariable polynomials, the reminder is not unique depends the order of f_1, f_2, \dots, f_s . That is not unique since if the reminder has zero, but after change the order of f_1, f_2, \dots, f_s will obtain the nonzero reminder. Thus, to solving it, must find another generating set of I called Grobner bases. Grobner bases in I is a set of all polynomials $\{g_1, g_2, \dots, g_s\}$ in I such that for any $f \in I$, there is $LT(g_i)$ divides $LT(f)$ with $i = 1, 2, \dots, s$. By the result of this research showed that every polynomial ideal has Grobner bases. To know that whether an in ideal has Grober bases then used Buchberger criterion. While to obtain a Grobner bases of an ideal of polynomial ring can use Buchberger algorithm.

Keywords: Buchberger algorithm, Buchberger criterion, generating set, Grobner bases, ideal, polynomial ring, ring.

1. Pendahuluan

Dalam suatu ring atau lapangan, dapat didefinisikan suatu polinomial yang koefisien-koefisiennya merupakan elemen dari ring atau lapangan tersebut. Himpunan semua polinomial dengan *indeterminate* X dengan koefisien di ring R dinotasikan dengan $R[X]$. Begitu pula dengan $F[X]$ yang merupakan himpunan semua polinomial dengan koefisien di lapangan F . $R[x]$ dan $F[X]$ merupakan suatu ring yang disebut ring polinomial [1]. Dalam teori ring, terdapat himpunan bagian yang memiliki sifat tertentu yang dikenal dengan sebutan ideal. Jika $F[X]$ adalah ring polinomial, maka ideal polinomial akan dibangun oleh elemen-elemen f_1, f_2, \dots, f_n di $F[X]$ dan dinotasikan dengan $I = \langle f_1, f_2, \dots, f_n \rangle$. Elemen-elemen yang membangun ideal tersebut untuk selanjutnya dinamakan basis [2].

Misalkan $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq F[X]$, dengan $f_i \neq 0$ untuk setiap $i = \{1, 2, \dots, s\}$. Suatu polinomial $f \in F[X]$ merupakan elemen di I jika f dapat ditulis sebagai kombinasi linier dari f_i yaitu $f = q_1 f_1 + q_2 f_2 + \dots + q_s f_s$ dengan $q_i \in F[X]$. Untuk mengubah f menjadi kombinasi linier, maka dapat digunakan algoritma pembagian polinomial bervariasi banyak tetapi dengan syarat sisa pembagian adalah nol. Umumnya pada algoritma pembagian polinomial satu variabel, sisa pembagian selalu tunggal. Hal ini berbeda dengan algoritma pembagian pada polinomial bervariasi banyak dimana sisa pembagiannya tidak tunggal tergantung pada urutan f_1, f_2, \dots, f_s . Dikatakan tidak tunggal karena jika sisa pembagiannya nol, tetapi setelah merubah urutan f_1, f_2, \dots, f_s akan dihasilkan sisa pembagian yang bukan nol. Oleh karena itu, untuk menyelesaikan masalah keanggotaan ideal tersebut, maka akan dicari himpunan pembangun yang lain dari I yang disebut basis Gröbner.

Dalam penelitian ini akan dibahas tentang bagaimana menentukan suatu himpunan pembangun ideal suatu ring polinomial merupakan basis Gröbner dan bagaimana cara mendapatkannya. Akan dibahas beberapa definisi, teorema dan algoritma yang berhubungan dengan basis Gröbner.

2. Tinjauan Pustaka

Basis Gröbner pertama kali diperkenalkan oleh Bruno Buchberger dalam tesisnya pada tahun 1970. Nama "Basis Gröbner" dipilih oleh Buchberger sebagai penghargaan terhadap W. Gröbner sebagai pembimbingnya. Untuk mencari basis Gröbner dikembangkan pula suatu algoritma yang dikenal sebagai Algoritma Buchberger. Sampai saat ini berbagai aplikasi dalam bidang matematika abstrak, sains dan teknik yang telah banyak menggunakan teori tentang basis Gröbner.

Definisi 1. Suatu grup $(G, *)$ merupakan himpunan G bersama dengan satu operasi biner $*$ yang didefinisikan pada G dan memenuhi sifat-sifat berikut:

- i. Tertutup : $a * b \in G$ untuk setiap $a, b \in G$;
- ii. Asosiatif : $(a * b) * c = a * (b * c)$ untuk setiap $a, b, c \in G$;
- iii. Elemen identitas : terdapat $e \in G$ sedemikian sehingga $e * a = a * e = a$ untuk setiap $a \in G$;
- iv. Invers: untuk setiap $a \in G$ terdapat $a^{-1} \in G$ sedemikian sehingga $a * a^{-1} = a^{-1} * a = e$.

Suatu grup $(G, *)$ disebut grup komutatif jika $a * b = b * a$ untuk setiap $a, b \in G$.

Definisi 2. Suatu ring $(R, +, \bullet)$ adalah himpunan tak kosong R yang dilengkapi dua operasi biner yaitu penjumlahan dan perkalian yang memenuhi sifat-sifat berikut:

- i. $(R, +)$ merupakan grup komutatif;
- ii. (R, \bullet) merupakan semigrup;
- iii. Memenuhi sifat distributif kiri dan kanan, yaitu:
 - a. untuk setiap $a, b, c \in R$ berlaku $a \bullet (b + c) = a \bullet b + a \bullet c$ dan
 - b. $(a + b) \bullet c = a \bullet c + b \bullet c$.

Suatu ring R disebut ring komutatif apabila pada operasi \bullet berlaku sifat komutatif yaitu $a \bullet b = b \bullet a$ untuk semua $a, b \in R$. Jika pada R terdapat $1 \in R$ sedemikian sehingga $a \bullet 1 = 1 \bullet a = a$ untuk setiap $a \in R$ maka R disebut ring dengan elemen satuan [3].

Contoh 1. Himpunan semua bilangan bulat terhadap operasi penjumlahan dan perkalian biasa yang dinotasikan dengan $(\mathbb{Z}, +, \bullet)$ merupakan ring.

Definisi 3. Suatu himpunan F disebut lapangan (*field*) jika memenuhi sifat-sifat berikut:

- $(F, +, \cdot)$ adalah ring komutatif;
- F terhadap operasi pergandaan mempunyai elemen satuan e dan $e \neq 0$;
- Setiap elemen tak nol di F mempunyai invers terhadap operasi pergandaan.

Contoh 2. Himpunan bilangan-bilangan riil \mathbb{R} dan himpunan bilangan kompleks \mathbb{C} merupakan lapangan tetapi himpunan bilangan bulat \mathbb{Z} bukan suatu lapangan karena setiap elemen di \mathbb{Z} tidak mempunyai invers terhadap pergandaan.

Definisi 4. Misalkan R suatu ring, $S \neq \emptyset$, $S \subseteq R$, disebut subring dari ring R jika S terhadap operasi yang sama di R merupakan ring.

Sifat 1. Misalkan R suatu ring, $S \neq \emptyset$, $S \subseteq R$, disebut subring dari ring R jika memenuhi:

- $a, b \in S \Rightarrow a - b \in S$
- $a, b \in S \Rightarrow ab \in S$

Definisi 5. Misalkan I subring R , maka:

- I disebut ideal kanan jika $a \in I, r \in R$ maka $ar \in I$.
 I disebut ideal kiri jika $a \in I, r \in R$, maka $ra \in I$.
- I disebut ideal dalam R jika I memenuhi ideal kiri dan kanan dalam R .

Contoh 3. Didefinisikan $S = \{2k | k \in \mathbb{Z}\}$ merupakan subring dari \mathbb{Z} .

- Ambil $r \in \mathbb{Z}$ dan $a \in S$ dengan $a = 2k, k \in \mathbb{Z}$

$$ra = r(2k) = 2(rk) \in S$$

karena $r \in \mathbb{Z}$ dan $k \in \mathbb{Z}$ maka $rk \in \mathbb{Z}$ maka S ideal kiri

$$ar = (2k)r = 2(kr) \in S$$

karena $r \in \mathbb{Z}$ dan $k \in \mathbb{Z}$ maka $kr \in \mathbb{Z}$ maka S ideal kanan

- S disebut ideal karena memenuhi ideal kiri dan ideal kanan

Definisi 6. Diketahui R ring komutatif dengan elemen satuan dan $P \subseteq R$ dengan $P \neq 0$. Himpunan $I = \left\{ \sum_{i=1}^n p_i r_i \mid p_i \in P, r_i \in R, n \in \mathbb{N} \right\}$ disebut ideal yang dibangun oleh P dan dinotasikan dengan $\langle P \rangle$. Himpunan P disebut pembangun (*generator*).

Contoh 4.

- Untuk sebarang R ring komutatif dengan elemen satuan, berlaku $\langle 1_R \rangle = R$
- Diketahui $\mathbb{R}[X]$ himpunan semua polinomial peubah tunggal dengan *indeterminate* X atas bilangan riil. Diketahui $\mathbb{R}[X]$ merupakan ring terhadap operasi penjumlahan dan pergandaan biasa. Jika dipilih $\{1, X\} \subset \mathbb{R}[X]$, maka $\langle 1, X \rangle = \{a + bx \mid a, b \in \mathbb{R}\} \subset \mathbb{R}[X]$.

Definisi 7. Misalkan R adalah ring, himpunan semua polinomial dengan *indeterminate* X atas R dinotasikan dengan $R[X]$. Jika $(x) \in R[X]$, maka ditulis $f(X) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0$, $n \geq 0$ dengan $a_i \in R, i = 0, 1, \dots, n$. Misalkan $f(X) = \sum_{i=0}^n a_i x^i, q(X) = \sum_{i=0}^m b_i x^i \in R[x]$, maka operasi penjumlahan dan pergandaan pada $R[x]$ dapat didefinisikan sebagai berikut :

$$+ : f(X) + q(X) = \sum_{i=0}^{\max(m,n)} c_i x^i, \quad \text{dengan } c_i = a_i + b_i$$

$$\cdot : f(X) \cdot q(X) = \sum_{i=0}^{m+n} c_i x^i,$$

dengan $c_i = a_i b_0 + a_{i-1} b_1 + \dots + a_1 b_{i-1} + a_0 b_i$, untuk setiap i .

Definisi 8. Diberikan suatu polinomial $f(X) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0 x^0$ dengan $a_n = 1$, maka $f(X)$ disebut polinomial monik.

Contoh 5. Diberikan ring R dan $f(x) = x^2 + 5x + 1$ suku banyak di $R[x]$. Polinomial $f(x)$ disebut polinomial monik karena koefisien utama $a_n = 1$.

Jika R ring dengan indeterminatenya x, y , maka dapat dibentuk ring $(R[x])[y]$ yang merupakan ring dari polinomial-polinomial dengan indeterminate y dan dengan koefisien-koefisien dalam ring polinomial $R[x]$. Ring ini juga dapat tulis sebagai ring polinomial dengan indeterminate x dan koefisien-koefisien dalam ring polinomial $R[y]$, yaitu $(R[y])[x]$.

2.1. Pengurutan Monomial

Suatu monomial dalam x_1, \dots, x_n adalah suatu perkalian berbentuk $x^a = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ dengan $a = a_1, a_2, \dots, a_n \in \mathbb{Z}_{\geq 0}^n$. Terdapat tiga cara pengurutan monomial, yaitu:

- Pengurutan Lex (*Lexicographic order*)
- Pengurutan Grlex (*Graded Lexicographic order*)
- Pengurutan Grevlex (*Graded Reverse Lexicographic*)

Definisi 9. Diberikan $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ dan $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. Dikatakan $\alpha >_{lex} \beta$ jika $\alpha - \beta \in \mathbb{Z}^n$, entri paling kiri yang tak nol adalah positif. Ditulis $x^\alpha >_{lex} x^\beta$ jika $\alpha >_{lex} \beta$. Pengurutan lexicographic analog dengan pengurutan pada kamus.

Contoh 6

- $xy^2 >_{lex} y^5z^6$ karena $\alpha - \beta = (1, -3, -6)$
- $x^2y^3z^5 >_{lex} x^2yz^5$ karena $\alpha - \beta = (0, 2, 0)$

Definisi 10. Misalkan $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Dikatakan $\alpha >_{grlex} \beta$ jika

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$$

atau $|\alpha| = |\beta|$ dan $\alpha >_{lex} \beta$.

Contoh 7.

- $xy^3z^2 >_{grlex} x^4y$ karena $|(1, 3, 2)| = 6 > |(4, 1, 0)| = 5$.
- $xy^3z^2 >_{grlex} xyz^4$ karena $|(1, 3, 2)| = |(1, 1, 4)|$ dan $(1, 3, 2) >_{lex} (1, 1, 4)$.

Pengurutan grlex dilakukan berdasarkan total derajat terbesar dan digunakan pengurutan lex ketika ada dua monomial memiliki total derajat yang sama.

Definisi 11. Misalkan $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Dikatakan $\alpha >_{grevlex} \beta$ jika

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$$

atau $|\alpha| = |\beta|$ dan entri paling kanan yang tak nol dari $\alpha - \beta \in \mathbb{Z}^n$ adalah negatif.

Contoh 8.

- $x^4y >_{grevlex} xy^3z$ karena $|(1, 3, 1)| = |(4, 1, 0)|$ dan $(4, 1, 0) - (1, 3, 1) = (3, -2, -1)$.
- $xy^3z^2 >_{grevlex} xyz^4$ karena $|(1, 3, 2)| = |(1, 1, 4)|$ dan $(1, 3, 2) - (1, 1, 4) = (0, 2, -2)$.

Definisi 12. Diberikan $f = \sum_{\alpha} c_{\alpha} x^{\alpha} \in F[X]$ suatu polinomial yang tak nol dan $>$ merupakan pengurutan monomial, maka

- Multidegree f

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0);$$

- Leading koefisien f

$$\text{LC}(f) = a_{\text{multideg}(f)} \in k;$$

- Leading monomial f

$$\text{LM}(f) = x^{\text{multideg}(f)};$$

- Leading term f

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Contoh 9. Diberikan polinomial $f = 4x^2y^2z^3 + 5xy^2z + 2y^3z^4$ dengan pengurutan lex diperoleh: $\text{multideg}(f) = (2,2,3)$, $\text{LC}(f) = 4$, $\text{LM}(f) = x^2y^2z^3$, dan $\text{LT}(f) = 4x^2y^2z^3$.

3. HASIL DAN PEMBAHASAN

3.1. Algoritma Pembagian Polinomial Multivariabel

Misalkan $I = \langle f_1, f_2, \dots, f_s \rangle$ adalah ideal di $F[X]$. Permasalahan yang muncul adalah ketika menentukan apakah suatu $f \in F[X]$ merupakan elemen di I atau tidak. Untuk mengatakan bahwa $f \in I$ maka harus ditunjukkan bahwa f merupakan kombinasi linier dari himpunan pembangun idealnya. Agar memperoleh kombinasi linier dimaksud maka digunakan algoritma pembagian polinomial multivariabel.

Algoritma pembagian pada polinomial multivariabel umumnya untuk membagi $f \in F[X]$ oleh $f_1, f_2, \dots, f_s \in F[X]$ sehingga dapat dinyatakan dalam bentuk $f = q_1f_1 + q_2f_2 + \dots + q_sf_s + r$ dengan $q_i, r \in F[X]$ dengan $r = 0$ atau tidak ada $\text{LT}(f_i)$ untuk $i = 1, 2, \dots, s$ yang habis membagi sebarang suku di r , dimana r merupakan sisa pembagian.

Contoh 10. Diberikan $f = -xy + y^3$, $I = \langle f_1, f_2 \rangle$ dimana $f_1 = y - 1$, $f_2 = xy - 1$ dan menggunakan pengurutan lex. Akan ditunjukkan bahwa f merupakan kombinasi linier dari f_1 dan f_2 .

Penyelesaian.

$$\begin{array}{r} q_1 = \\ q_2 = \\ \hline f_1 = y-1 \quad -xy + y^3 \\ f_2 = xy-1 \end{array}$$

Karena $\text{LT}(f_1) = y$ dan $\text{LT}(f_2) = xy$ keduanya membagi $\text{LT}(f) = -xy$, maka langkah awal bagi f oleh f_1 sehingga diperoleh :

$$\begin{array}{r} q_1 = -x \\ q_2 = 0 \\ \hline f_1 = y-1 \quad -xy + y^3 \\ f_2 = xy-1 \quad -xy + x \\ \hline -x + y^3 \end{array}$$

Karena $\text{LT}(f_1)$ dan $\text{LT}(f_2)$ tidak membagi $-x$, maka dihilangkan sebagai sisa.

$$\begin{array}{r} q_1 = -x \\ q_2 = 0 \\ \hline f_1 = y-1 \quad -xy + y^3 \\ f_2 = xy-1 \quad -xy + x \\ \hline y^3 \quad r = -x \end{array}$$

$\text{LT}(f_1)$ dapat membagi y^3 maka diperoleh

$$\begin{array}{r} q_1 = -x + y^2 + y + 1 \\ q_2 = 0 \\ \hline f_1 = y-1 \quad -xy + y^3 \\ f_2 = xy-1 \quad -xy + x \\ \hline y^3 \\ y^3 - y^2 \\ \hline y^2 \\ y^2 - y \\ \hline y \\ y-1 \\ \hline 1 \quad r = -x+1 \end{array}$$

Karena $LT(f_1)$ dan $LT(f_2)$ tidak membagi 1, maka ditambahkan pada sisa pembagian yaitu $r = -x + 1$. Jadi diperoleh $q_1 = -x + y^2 + y + 1$ dan $q_2 = 0$.

Jadi, f dapat ditulis sebagai kombinasi linier dari f_1, f_2 yaitu

$$f = (-x + y^2 + y + 1)(y - 1) + 0(xy - 1) + (-x + 1)$$

Pada langkah awal, dapat dilihat bahwa $LT(f_1) = y$ dan $LT(f_2) = xy$ keduanya dapat membagi $LT(f) = -xy$. Apabila pada langkah tersebut $LT(f_2) = xy$ menggantikan $LT(f_1) = y$, maka dengan menggunakan algoritma pembagian maka hasil akhir yang diperoleh adalah

$$f = (y^2 + y + 1)(y - 1) + (-1)(xy - 1).$$

Algoritma pembagian di $F[X]$ bisa dijadikan cara untuk membuktikan apakah suatu $f \in F[X]$ merupakan elemen di I atau bukan, yaitu jika sisa pembagiannya nol. Akan tetapi berdasarkan contoh 10 di atas, dapat dilihat bahwa sisa pembagiannya tidak tunggal (sisa pembagiannya berbeda) tergantung pengurutan elemen di himpunan pembangun idealnya, sehingga tidak dapat ditentukan apakah $f \in I$.

Sifat penting pada sisa r dari algoritma pembagian di $F[X]$ harus sama, yaitu $r = 0$, walaupun diubah urutan dari elemen pada himpunan pembangun idealnya. Contoh berikut ini dapat akan menunjukkan bagaimana memperoleh sisa yang tidak tunggal tersebut jika urutan elemen pembangunnya diubah.

Contoh 11. Misalkan $f = xy^2 - x \in F[X]$ dengan pengurutan lex. Diberikan $I = \langle f_1, f_2 \rangle$ dimana $f_1 = xy + 1$, $f_2 = y^2 - 1$. Dengan membagi f oleh $\{f_1, f_2\}$ diperoleh:

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

Sedangkan jika dilakukan pembagian f oleh $\{f_2, f_1\}$ maka kombinasi liniernya berbentuk

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$$

Pada persamaan (1) dapat dilihat bahwa $r = -x - y$, sedangkan pada persamaan (2) diperoleh $r = 0$.

Secara umum algoritma pembagian polinomial multivariabel tidak akan menghasilkan sisa yang sama yaitu $r = 0$. Untuk menyelesaikan masalah tersebut, maka diperlukan himpunan pembangun khusus lain yang masih membangun ideal suatu polinomial. Himpunan pembangun tersebut dinamakan basis Gröbner.

3.2. Basis Gröbner

Pada bagian ini akan diberikan definisi dari basis Gröbner dan beberapa teorema yang berkaitan serta beberapa contoh.

Definisi 13. Diberikan $F[X]$ ring polinomial atas lapangan F dengan suatu pengurutan monomial. Misalkan I suatu ideal pada $F[X]$. Himpunan semua polinomial $G = \{g_1, g_2, \dots, g_s\}$ dalam I disebut basis Gröbner jika dan hanya jika untuk setiap polinomial tak nol $f \in I$, terdapat $LT(g_i)$ yang habis membagi $LT(f)$ untuk suatu $i = 1, 2, \dots, s$.

Contoh 12. Diberikan polinomial $y - 1$ dan $xy - 1$ dengan pengurutan lex. Apakah himpunan $\{y - 1, xy - 1\}$ adalah suatu basis Gröbner untuk ideal $I = \langle y - 1, xy - 1 \rangle$?

Penyelesaian. Misalkan $f = x - 1 \in I$ karena $x - 1 = xy - xy + x - 1 = (xy - 1) - x(y - 1)$. Himpunan $\{y - 1, xy - 1\}$ bukan suatu basis Gröbner karena berdasarkan definisi basis Gröbner, $LT(y - 1) = y$ dan $LT(xy - 1) = xy$ tidak habis membagi $LT(x - 1) = x$.

Pada contoh 11 dapat dilihat bahwa permasalahan yang muncul adalah kondisi dimana suatu polinomial f dapat menjadi elemen suatu ideal. Akan tetapi ketika dilakukan algoritma pembagian untuk membagi f dengan elemen pembangunnya tidak diperoleh sisa 0 seperti yang diharapkan. Untuk itu teorema berikut ini dapat menjamin sisa pembagian f oleh suatu basis Gröbner menghasilkan sisa 0.

Teorema 1. Diberikan $F[X]$ suatu ring polinomial atas lapangan F dengan suatu pengurutan monomial. Misalkan I ideal pada $F[X]$ dan $G = \{g_1, g_2, \dots, g_s\}$ merupakan basis Gröbner untuk I . Maka suatu polinomial $f \in F[X]$ ditulis sebagai $f = q_1g_1 + q_2g_2 + \dots + q_s g_s + r$, dimana $r = 0$ atau tidak ada *leading term* untuk suatu g_1, g_2, \dots, g_s yang habis membagi sebarang suku di polinomial r diperoleh, $f \in I$ jika dan hanya jika $r = 0$.

Bukti.

\Leftarrow) Diketahui $r = 0$

Akan ditunjukkan $f \in I$

Jika $r = 0$, maka sesuai algoritma pembagian diperoleh $f = q_1g_1 + q_2g_2 + \dots + q_sg_s$ yang berarti $f \in I$.

\Rightarrow) Diketahui $f \in I$

Akan ditunjukkan $r = 0$

Akan dibuktikan dengan kontradiksi. Andaikan $r \neq 0$ maka berdasarkan algoritma pembagian

$$f = q_1g_1 + q_2g_2 + \dots + q_sg_s + r$$

$$f - r = q_1g_1 + q_2g_2 + \dots + q_sg_s$$

yang berarti $f - r \in I$, maka menurut definisi ideal diperoleh $r \in I$. Berdasarkan definisi basis Gröbner, maka terdapat $LT(g_1)$ yang habis membagi $LT(r)$ terjadi kontradiksi sehingga seharusnya $r = 0$. ■

Teorema 1 di atas dapat digunakan untuk menjawab pertanyaan utama yang diangkat penelitian ini yaitu bagaimana menentukan $f \in I$. Jawabannya adalah dapat digunakan algoritma pembagian dengan membagi f oleh polinomial dalam basis Gröbner. Jika sisa yang dihasilkan adalah nol, maka dapat disimpulkan $f \in I$ dan sebaliknya. Pada teorema ini hipotesis yang menyatakan $G = \{g_1, g_2, \dots, g_s\}$ merupakan suatu basis Gröbner hanya digunakan dalam pembuktian. Jadi, $r = 0$ merupakan syarat yang cukup untuk $f \in I$, tetapi basis Gröbner juga merupakan syarat perlu. Hal ini memunculkan teorema berikut yang menjamin bahwa basis Gröbner merupakan himpunan pembangun suatu ideal I .

Teorema 2. Jika I suatu ideal $F[X]$ dan $G = \{g_1, g_2, \dots, g_s\} \subset I$ suatu basis Gröbner untuk ideal I , maka $\langle g_1, g_2, \dots, g_s \rangle = I$

Bukti. Akan ditunjukkan bahwa

i. $\langle g_1, g_2, \dots, g_s \rangle \subseteq I$.

Karena $g_1, g_2, \dots, g_s \in I$ maka jelas bahwa $\langle g_1, g_2, \dots, g_s \rangle \subseteq I$.

ii. $I \subseteq \langle g_1, g_2, \dots, g_s \rangle$.

Ambil sebarang $f \in I$

Akan ditunjukkan bahwa $f \in \langle g_1, g_2, \dots, g_s \rangle$.

Dengan menggunakan algoritma pembagian untuk membagi f oleh $\langle g_1, g_2, \dots, g_s \rangle$ maka f dapat ditulis dalam bentuk

$$f = q_1g_1 + q_2g_2 + \dots + q_sg_s + r,$$

dimana tidak ada suku di r yang habis dibagi oleh sebarang $LT(g_i)$.

Andaikan $r \neq 0$ maka

$$f - r = q_1g_1 + q_2g_2 + \dots + q_sg_s \in I,$$

maka, diperoleh $r \in I$ sehingga terdapat $LT(g_i)$ habis membagi $LT(r)$.

Terjadi kontradiksi dimana r merupakan sisa pembagian sehingga tidak ada suku di r yang habis dibagi oleh sebarang $LT(g_i)$. Pengandaian salah, maka diperoleh $r = 0$, sehingga dapat ditulis $f = q_1g_1 + q_2g_2 + \dots + q_sg_s + 0 \in \langle g_1, g_2, \dots, g_s \rangle$ yang berarti $f \in \langle g_1, g_2, \dots, g_s \rangle$.

Jadi, $I \subseteq \langle g_1, g_2, \dots, g_s \rangle$

Berdasarkan i) dan ii), maka terbukti bahwa bahwa $I = \langle g_1, g_2, \dots, g_s \rangle$. ■

Pada suatu basis Gröbner sisa pembagian $f \in F[X]$ selalu menghasilkan sisa pembagian yang tunggal yang termuat dalam teorema berikut.

Teorema 3. Diberikan I suatu ideal pada ring polinomial $F[X]$ dan $G = \{g_1, g_2, \dots, g_s\}$ suatu basis Gröbner. Misalkan $f \in F[X]$, maka pembagian f oleh polinomial G menghasilkan sisa r yang tunggal.

Bukti. Misalkan dengan menggunakan algoritma pembagian diperoleh dua kombinasi linier dari f yaitu:

$$f = q_1g_1 + q_2g_2 + \dots + q_sg_s + r$$

$$f = p_1g_1 + p_2g_2 + \dots + p_sg_s + t$$

dengan sisa pembagian r dan t .

Akan ditunjukkan bahwa $r = t$. Berdasarkan algoritma pembagian, diperoleh $r = 0$ atau $t = 0$ atau tidak ada $LT(g_i)$ yang habis membagi suku di r atau t . Karena $r - t \in I$, maka berdasarkan definisi basis Gröbner, jika $r - t \neq 0$, maka terdapat suatu $LT(g_i)$ habis membagi $LT(r - t)$. Muncul kontradiksi karena r dan t merupakan sisa pembagian sehingga tidak ada $LT(g_i)$ yang habis membagi suku di r ataupun t . Sehingga seharusnya $r - t = 0$ atau $r = t$. ■

Contoh 13. Diberikan $G = \{x + z, y - z\}$ suatu basis Gröbner di lapangan $F[x, y, z]$ dengan pengurutan lex. Misalkan $f = xyz \in F[x, y, z]$. Akan ditunjukkan dengan Teorema 3, pembagian f oleh G menghasilkan sisa tunggal.

$$xyz = yz(x + z) - z^2(y - z) - z^3.$$

Selanjutnya jika urutan pembagiannya diubah menjadi $G = \{g_2, g_1\}$, maka diperoleh

$$xyz = xz(x + z) + z^2(y - z) - z^3.$$

Jadi, sisa pembagian yang diperoleh adalah $-z^3$.

3.3. Kriteria Buchberger dan Algoritma Buchberger

Pada bagian ini akan dibahas tentang cara memeriksa apakah suatu basis merupakan basis Gröbner dan bagaimana membentuk suatu basis Gröbner. Tetapi sebelumnya diberikan definisi dari S -Polinomial berikut ini.

Definisi 14. Diberikan $f, g \in F[X]$ polinomial tak nol, maka S -Polinomial dari f dan g didefinisikan sebagai:

$$S(f, g) = \frac{L}{LT(f)}f - \frac{L}{LT(g)}g$$

dengan $L = lcm(LM(f), LM(g))$.

Contoh 14. Misalkan $I = \langle f_1, f_2 \rangle \subset F[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$. S -Polinomial dari f_1 dan f_2 adalah:

$$\begin{aligned} S(f_1, f_2) &= \frac{x^2y^3}{x^2y}(x^2y + x) - \frac{x^2y^3}{xy^3}(xy^3 - y) \\ &= xy + xy^2 \end{aligned}$$

Definisi S -Polinomial di atas dapat digunakan untuk memeriksa apakah suatu himpunan pembangun ideal merupakan basis Gröbner atau tidak. Dikatakan basis Gröbner jika pembagian setiap $S(g_i, g_j)$ oleh G menghasilkan sisa nol.

3.3.1. Kriteria Buchberger

Misalkan I suatu ideal polinomial pada suatu ring polinomial $F[X]$. Maka $G = \{g_1, g_2, \dots, g_s\}$ merupakan basis Gröbner untuk I jika dan hanya jika untuk semua $i \neq j$ dengan $i > j$ berlaku $\overline{S(g_i, g_j)}^G = 0$. Dimana $\overline{S(g_i, g_j)}^G$ adalah sisa pembagian $S(g_i, g_j)$ oleh G .

Contoh 15. Misalkan $I = \langle f_1, f_2 \rangle \subseteq F[X]$ dengan $f_1 = x + z$, $f_2 = y - z$. Akan ditunjukkan $I = \langle f_1, f_2 \rangle$ merupakan basis Gröbner dengan menggunakan kriteria Buchberger.

Penyelesaian.

$$\begin{aligned} S(f_1, f_2) &= \frac{xy}{x}(x + z) - \frac{xy}{y}(y - z) \\ &= xy + yz - xy + xz \\ &= xz + yz \end{aligned}$$

Karena $xz + yz = z(x + z) + z(y - z)$ yang berarti sisa pembagiannya nol, maka $I = \langle f_1, f_2 \rangle$ merupakan suatu basis Gröbner.

Dari contoh 15 dapat dilihat bahwa $I = \langle f_1, f_2 \rangle$ merupakan basis Gröbner. Pertanyaan selanjutnya adalah bagaimana jika pembagian $S(g_1, g_2)$ oleh G menghasilkan sisa tak nol. Untuk itu, salah satu tujuan dari penelitian ini adalah membentuk suatu basis Gröbner dari basis yang bukan Gröbner. Dengan menggunakan algoritma Buchberger berikut, dapat dibentuk basis Gröbner dari suatu ideal I .

3.3.2. Algoritma Buchberger

Diberikan $I = \langle f_1, f_2, \dots, f_s \rangle \neq \{0\}$ suatu ideal polinomial. Maka basis Gröbner pada I dapat dibentuk dengan cara seperti berikut:

1. Misalkan $G = \{g_1, g_2, \dots, g_s\}$
2. Hitung S -polinomial untuk setiap pasangan $g_i, g_j \in G$ yaitu $S(g_i, g_j)$ untuk $i < j$.
3. Dilakukan pembagian $S(g_i, g_j)$ dengan G sehingga diperoleh $\overline{S(g_i, g_j)}^G$
4. Jika $\overline{S(g_i, g_j)}^G \neq 0$, maka tambahkan polinomial $\overline{S(g_i, g_j)}^G$ ke G
5. Ulangi langkah 2 dengan $G = G \cup \overline{S(g_i, g_j)}^G$ sampai semua S -polinomial di G menghasilkan sisa 0 setelah pembagian dengan G .

Contoh 16. Diketahui ideal $I = \langle x^2 - x, x - y \rangle \subset F[X]$ dengan $g_1 = x^2 - x$ dan $g_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan pengurutan lex.

Penyelesaian.

1. Misalkan $G = \{x^2 - x, x - y\}$
2. Hitung S -polinomial g_1 dan g_2

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) \\ &= x^2 - x - x(x - y) \\ &= x^2 - x - x^2 + xy \\ &= xy - x \end{aligned}$$

3. Lakukan pembagian $S(g_1, g_2)$ dengan G

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Diperoleh

$$\overline{S(g_1, g_2)}^G = y^2 - y$$

4. Karena $\overline{S(g_1, g_2)}^G = y^2 - y \neq 0$, maka tambahkan $\overline{S(g_1, g_2)}^G$ pada G sebagai pembangun baru $g_3 = y^2 - y$ sehingga diperoleh G yang baru yaitu

$$G = \{g_1, g_2, g_3\}$$

5. Hitung nilai S -polinomial diperoleh

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) \\ &= x^2 - x - x(x - y) \\ &= x^2 - x - x^2 + xy \\ &= xy - x \end{aligned}$$

$$\begin{aligned} S(g_1, g_3) &= \frac{x^2 y^2}{x^2}(x^2 - x) - \frac{x^2 y^2}{y^2}(y^2 - y) \\ &= x^2 y^2 - x y^2 - x^2 y^2 + x^2 y \\ &= x^2 y - x y^2 \\ &= xy - x \end{aligned}$$

$$\begin{aligned} S(g_2, g_3) &= \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) \\ &= xy^2 - y^3 - xy^2 + xy \\ &= xy - y^3 \end{aligned}$$

$$= xy - x$$

Lakukan pembagian setiap pasang S -polinomial dengan $G = \{g_1, g_2, g_3\}$ diperoleh:

$$S(f_1, f_2) = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1)f_2 + f_3 + 0$$

$$S(f_1, f_3) = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y)f_1 + (-x)f_3 + 0$$

$$S(f_2, f_3) = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y)f_2 + (-y)f_3 + 0$$

Karena untuk setiap $i, j = 1, 2, 3$ berlaku $\overline{S(g_i, g_j)}^G = 0$, maka menurut kriteria Buchberger himpunan $G = \{g_1, g_2, g_3\} = \{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

4. Kesimpulan

Dari hasil pembahasan dan uraian pada bab-bab sebelumnya maka dapat diambil beberapa kesimpulan antara lain:

- Untuk menunjukkan apakah sebarang $f \in F[X]$ merupakan elemen di ideal I maka digunakan algoritma pembagian polinomial multivariabel untuk membagi f dengan basis Gröbner dari I . Jika sisa pembagian tersebut adalah nol, maka disimpulkan $f \in I$.
- Untuk memeriksa apakah suatu basis dari ideal I merupakan basis Gröbner G maka digunakan kriteria Buchberger dimana jika pembagian S -polinomial oleh G menghasilkan sisa nol.
- Jika pembagian S -polinomial oleh G menghasilkan sisa yang tak nol maka ideal I bukan suatu basis Gröbner. Untuk membentuk basis Gröbner dari ideal I tersebut maka digunakan algoritma Buchberger.

Daftar Pustaka

- [1] A. Setiawan, Aljabar Abstrak (Teori Grup dan Teori Ring)., Salatiga: PS. Matematika Fakultas Sains dan Matematika, Universitas Kristen Satya Wacana, 2011.
- [2] D. Cox dan J. Little, Ideals, Varieties, and Algorithm: An Introduction to Computational Algebraic Geometry and Commutative Algebra, New York: Springer, 2007.
- [3] D. Malik, S. Mordeson dan M. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, 1997.
- [4] J. A. Gallian, Contemporary Abstract Algebra, Heath and Company, 1990.
- [5] J. Gilbert dan L. Gilbert, Elements of Modern Algebra, Brookscole, 1999.
- [6] I. M. Sulandra, Implementasi Basis Grobner dalam menentukan Keanggotaan Ideal di "Cas Singular", Malang: FMIPA UNM, 2009.
- [7] J. Watkins, Topics in Commutative Ring Theory, Colorado Spring, 2006.
- [8] M. Weiss, Computing Grobner Bases in Python with Buchberger's Algorithm, 2010.