

# BASIS GROBNER DAN ALGORITMA BUCHBERGER

M. Zaki Riyanto<sup>1</sup> dan Sri Wahyuni<sup>2</sup>

**Abstract:** Let  $F[x_1, \dots, x_n]$  be a polynomial ring with variables  $x_1, \dots, x_n$  over a field  $F$ . Suppose  $I$  is an ideal of  $F[x_1, \dots, x_n]$ . A subset  $S \subset F[x_1, \dots, x_n]$  is said to be a basis for  $I$  if it's finitely generated by  $S$ . Fix a monomial order relation. We denote by  $\text{LT}(f)$  the leading term of  $f \in F[x_1, \dots, x_n]$  and  $\text{LT}(I)$  the set of all leading term of all elements in  $I$ . A subset  $\{g_1, \dots, g_t\} \subset F[x_1, \dots, x_n]$  is said to be Grobner basis for  $I$  if  $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$ . In this paper we discussed the motivation of construction of the Grobner basis and a method to find the Grobner basis using Buchberger algorithm.

**Kata Kunci:** Buchberger Algorithm, Grobner Basis, Ideal, Monomial Ordering, Polynomial Ring.

## PENDAHULUAN

Konsep basis Grobner untuk ring polinomial pertama kali dikemukakan oleh Bruno Buchberger pada tahun 1965. Basis Grobner telah digunakan untuk menyelesaikan berbagai macam masalah dalam kajian di aljabar komutatif dan geometri aljabarik, seperti masalah keanggotaan ideal, dekomposisi ideal, penyelesaian sistem persamaan polinomial, dan sebagainya. Sampai saat ini, basis Grobner telah digunakan secara luas dalam berbagai bidang, seperti dalam mekanika, kimia, teori pengkodean, dan kriptografi [1].

Pengembangan dari konsep basis Grobner pada awalnya muncul dari masalah-masalah berikut ini. Diberikan ring polinomial  $F[x_1, \dots, x_n]$  atas field  $F$ .

- Masalah Deskripsi Ideal: Jika  $I$  ideal  $F[x_1, \dots, x_n]$ , bagaimana mengecek bahwa  $I$  dibangun secara hingga, yaitu  $I = \langle f_1, \dots, f_s \rangle$ , untuk suatu  $f_i \in F[x_1, \dots, x_n]$ .
- Masalah Keanggotaan Ideal: Jika diberikan  $f \in F[x_1, \dots, x_n]$  dan suatu ideal  $I = \langle f_1, \dots, f_s \rangle$ , bagaimana mengecek bahwa  $f \in I$ .
- Masalah Penyelesaian Sistem Persamaan Polinomial: Tentukan semua solusi bersama di  $F^n$  dari sistem persamaan polinomial berikut:

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_s(x_1, \dots, x_n) &= 0. \end{aligned}$$

---

<sup>1</sup> S2 Matematika FMIPA UGM, E-mail: [zaki@mail.ugm.ac.id](mailto:zaki@mail.ugm.ac.id)

<sup>2</sup> Jurusan Matematika FMIPA UGM, E-mail: [swahyuni@ugm.ac.id](mailto:swahyuni@ugm.ac.id)

Dalam paper ini dibahas mengenai konstruksi dari basis Grobner dan metode atau teknik untuk menghitung basis Grobner menggunakan suatu algoritma. Dalam [1] dan [2] telah dijelaskan motivasi dari pembentukan basis Grobner. Secara khusus dalam [1] dijelaskan lebih detail mengenai komputasi basis Grobner. Secara umum, pembahasan dalam paper ini didasarkan pada [1].

## AFFINE VARIETY DAN IDEAL

Diberikan  $F[x_1, \dots, x_n]$  adalah ring polinomial atas field  $F$  dengan variabel  $x_1, \dots, x_n$ . Diberikan  $f_1, \dots, f_s \in F[x_1, \dots, x_n]$ . Misalkan  $I$  adalah ideal yang dibangun secara hingga oleh  $\{f_1, \dots, f_s\}$ , maka  $I = \{c_1 f_1 + \dots + c_s f_s \mid c_i \in F[x_1, \dots, x_n]\}$  dan ditulis  $I = \langle f_1, \dots, f_s \rangle$ . Misalkan  $F^n = \{(a_1, \dots, a_n) \mid a_i \in F, i = 1, \dots, n\}$ .

Berikut ini dibahas mengenai salah satu masalah dalam geometri aljabarik, yaitu mencari pembuat nol bersama di  $F^n$  dari polinomial-polinomial  $f_1, \dots, f_s$ . Masalah ini dapat memotivasi pembentukan basis Grobner yang diberikan pada pembahasan selanjutnya.

**Definisi 1.** Misalkan  $S = \{f_1, \dots, f_s\} \subset F[x_1, \dots, x_n]$ . Maka *affine variety* dari  $S$  adalah himpunan  $V(S) = \{(a_1, \dots, a_n) \in F^n \mid f_i(a_1, \dots, a_n) = 0, i = 1, \dots, s\}$ .

**Contoh 2.** Misalkan  $S = \{2x + y - 2\} \subset \mathbb{R}[x, y]$ , maka affine variety dari  $S$  adalah suatu garis lurus yang memotong sumbu- $x$  di 1 dan memotong sumbu- $y$  di 2, atau dapat ditulis  $V(S) = V(2x + y - 2) = \{(a, b) \in \mathbb{R}^2 \mid 2a + b = 2\}$ .

Selanjutnya, diberikan konsep mengenai basis dari suatu ideal. Tidak seperti pada aljabar linear, pada definisi basis untuk ideal tidak menggunakan sifat-sifat basis pada umumnya seperti sifat bebas linear.

**Definisi 3.** Diberikan  $I$  adalah suatu ideal di  $F[x_1, \dots, x_n]$ . Suatu subset  $\{f_1, \dots, f_s\} \subset I$  disebut *basis* untuk  $I$  jika  $I = \langle f_1, \dots, f_s \rangle$ .

Berikut ini diberikan sebuah teorema yang mengaitkan hubungan antara variety dari basis suatu ideal dengan variety dari ideal yang dibangun oleh basis tersebut.

**Teorema 4.** Diberikan  $S = \{f_1, \dots, f_s\} \subset F[x_1, \dots, x_n]$ , maka  $V(S) = V(\langle f_1, \dots, f_s \rangle)$ .

**Teorema 5. (Teorema Basis Hilbert)** Jika  $I$  adalah ideal di  $F[x_1, \dots, x_n]$ , maka  $I$  dibangun secara hingga, yaitu  $I = \langle f_1, \dots, f_s \rangle$ , untuk suatu  $f_1, \dots, f_s \in I$ .

Teorema Basis Hilbert menyatakan bahwa setiap ideal di  $F[x_1, \dots, x_n]$  dibangun secara hingga. Misal diberikan suatu basis untuk suatu ideal  $I$  di  $F[x_1, \dots, x_n]$ . Apakah basis tersebut dapat dimodifikasi sehingga strukturnya menjadi lebih sederhana, sehingga dapat mempermudah dalam menghitung  $V(I)$ ? Salah satu caranya adalah menggunakan algoritma pembagian.

**Teorema 6.** *Diberikan polinomial  $f, g, q, r \in F[x_1, \dots, x_n]$  sedemikian hingga  $f = gq + r$ . Maka pembuat nol bersama di  $F^n$  dari  $f$  dan  $g$  sama dengan pembuat nol bersama dari  $g$  dan  $r$ . Lebih lanjut, pembagi bersama di  $F[x_1, \dots, x_n]$  dari  $f$  dan  $g$  sama dengan pembagi bersama dari  $g$  dan  $r$ . Jika  $f$  dan  $g$  elemen dari suatu basis untuk ideal  $I$  di  $F[x_1, \dots, x_n]$ , maka dengan mengganti  $f$  dengan  $r$  juga merupakan basis untuk  $I$ .*

Dalam aljabar linear, salah satu teknik dasar untuk menyelesaikan solusi dari suatu sistem persamaan linear berhingga adalah dengan mencari pembuat nol bersama dari persamaan-persamaan tersebut. Cara yang dapat digunakan adalah metode eliminasi yang berguna untuk menyederhanakan sistem. Berikut ini diberikan sebuah contoh dalam  $\mathbb{R}[x]$  dengan satu variabel.

**Contoh 7.** Diberikan  $f = x^4 + x^3 - 3x^2 - 5x - 2$  dan  $g = x^3 + 3x^2 - 6x - 8$  di  $\mathbb{R}[x]$ . Akan ditentukan variety atau himpunan semua pembuat nol bersama  $V(\{f, g\})$  di  $\mathbb{R}$ . Dibentuk ideal  $I = \langle f, g \rangle$ . Berdasarkan Teorema 5, maka akan dicari basis dari  $\langle f, g \rangle$  dengan derajat yang lebih kecil. Menggunakan algoritma pembagian pada  $\mathbb{R}[x]$ , maka terdapat dengan tunggal  $q, r \in \mathbb{R}[x]$  sedemikian hingga  $f = gq + r$  dengan  $\deg(r) \leq 2$ , yaitu  $g = x - 2$  dan  $r = 9x^2 - 9x - 18$ . Karena pembuat nol dari  $9x^2 - 9x - 18$  sama dengan pembuat nol dari  $x^2 - x - 2$ , maka ditentukan  $r = x^2 - x - 2$ . Oleh karena itu, basis  $\{f, g\}$  dapat diganti dengan  $\{g, r\}$ . Selanjutnya, dilakukan proses yang sama yaitu  $g$  dibagi dengan  $r$ , diperoleh sisa  $r_1 = 0$  sehingga diperoleh basis baru yaitu  $\{r, r_1\} = \{x^2 - x - 2\}$ . Diperoleh  $I = \langle f, g \rangle = \langle x^2 - x - 2 \rangle = \langle (x - 2)(x + 1) \rangle$  dan  $V(\{f, g\}) = \{-1, 2\}$ .

## URUTAN MONOMIAL DAN ALGORITMA PEMBAGIAN

Dalam penyelesaian Contoh 7 di atas digunakan algoritma pembagian pada  $\mathbb{R}[x]$ . Masalah yang kemudian muncul adalah bagaimana dengan algoritma pembagian pada  $F[x_1, \dots, x_n]$ . Pada kasus dengan satu variabel  $F[x]$ , koefisien utama dari suatu polinomial ditentukan oleh pangkat tertinggi dari  $x$ . Oleh karena itu, perlu didefinisikan suatu urutan monomial pada  $F[x_1, \dots, x_n]$ .

Dalam  $F[x_1, \dots, x_n]$ , variabel atau indeterminat dinyatakan sebagai monomial yang berbentuk  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  dengan  $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ . Misalkan  $M$  adalah himpunan semua monomial di  $F[x_1, \dots, x_n]$ , maka  $\varphi: M \rightarrow \mathbb{N}_0^n$  dengan  $\varphi(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = (\alpha_1, \dots, \alpha_n)$  merupakan pemetaan injektif. Lebih lanjut, dapat diperoleh sifat bahwa  $\varphi((x_1^{\alpha_1} \cdots x_n^{\alpha_n})(x_1^{\beta_1} \cdots x_n^{\beta_n})) = \varphi(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) + \varphi(x_1^{\beta_1} \cdots x_n^{\beta_n})$ . Untuk selanjutnya, dapat ditulis  $x = x_1 \cdots x_n$ ,  $\alpha = (\alpha_1, \dots, \alpha_n)$ , dan  $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ .

**Definisi 8.** *Relasi urutan monomial pada  $F[x_1, \dots, x_n]$  adalah relasi  $>$  pada  $\mathbb{N}_0^n$  yang memenuhi tiga aksioma berikut:*

- (i) *Relasi  $>$  merupakan relasi urutan total, yaitu untuk setiap  $\alpha, \beta \in \mathbb{N}_0^n$  berlaku salah satu:  $\alpha > \beta$ ,  $\alpha = \beta$ , atau  $\beta > \alpha$ .*
- (ii) *Jika  $\alpha > \beta$  dan  $\gamma \in \mathbb{N}_0^n$ , maka  $\alpha + \gamma > \beta + \gamma$ .*
- (iii) *Relasi  $>$  merupakan relasi urutan balik (well ordering), yaitu setiap subset tidak kosong dari  $\mathbb{N}_0^n$  mempunyai elemen minimal terhadap relasi  $>$ .*

Suatu relasi  $>$  pada  $F[x_1, \dots, x_n]$  merupakan relasi urutan balik jika dan hanya jika untuk setiap barisan turun tegas  $x^{\alpha(1)} > x^{\alpha(2)} > x^{\alpha(3)} > \dots$  terbatas. Berikut ini diberikan beberapa relasi urutan monomial pada  $F[x_1, \dots, x_n]$ .

**Definisi 9. (Urutan Lexicographic)** *Relasi urutan lexicographic pada  $\mathbb{N}_0^n$  adalah suatu relasi  $>_{\text{lex}}$  dengan definisi untuk setiap  $\alpha, \beta \in \mathbb{N}_0^n$  berlaku  $\alpha >_{\text{lex}} \beta$  jika dan hanya jika terdapat  $1 \leq j \leq n$  dengan  $\alpha_j > \beta_j$  dan  $\alpha_i = \beta_i$  untuk setiap  $1 \leq i \leq j-1$ .*

**Contoh 10.** Diberikan polinomial  $f = xyz^2 + 2y^4z^2 - xy^2z \in \mathbb{Q}[x, y, z]$ . Diketahui  $(1, 1, 2), (0, 4, 2), (1, 2, 1) \in \mathbb{N}_0^3$ . Menggunakan relasi urutan lexicographic  $>_{\text{lex}}$  diperoleh  $(1, 1, 2) >_{\text{lex}} (0, 4, 2)$  dan  $(1, 2, 1) >_{\text{lex}} (1, 1, 2)$ . Jadi,  $f = -xy^2z + 2y^4z^2 + xyz^2$ .

Relasi urutan lexicographic merupakan relasi urutan monomial. Selanjutnya, diberikan konsep mengenai derajat total dari suatu monomial. *Derajat total* dari suatu monomial  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  didefinisikan sebagai jumlahan  $\alpha_1 + \cdots + \alpha_n$ , dan dinotasikan dengan  $|\alpha|$ . Definisi ini dapat digunakan untuk mendefinisikan urutan monomial baru berdasarkan urutan lexicographic.

**Definisi 11. (Urutan Lexicographic Derajat Total)** *Relasi urutan lexicographic derajat total pada  $\mathbb{N}_0^n$  adalah relasi  $>_{\text{deglex}}$  dengan definisi untuk setiap  $\alpha, \beta \in \mathbb{N}_0^n$  berlaku  $\alpha >_{\text{deglex}} \beta$  jika dan hanya jika  $|\alpha| > |\beta|$  atau  $|\alpha| = |\beta|$  dan  $\alpha >_{\text{lex}} \beta$ .*

**Contoh 12.** Berdasarkan Contoh 10 sebelumnya, menggunakan relasi lexicographic derajat total  $>_{\text{deglex}}$  diperoleh bahwa  $(0,4,2) >_{\text{deglex}} (1,2,1)$  dan  $(1,2,1) >_{\text{deglex}} (1,1,2)$ . Jadi,  $f = 2y^4z^2 - xy^2z + xyz^2$ .

Relasi urutan lexicographic derajat total  $>_{\text{deglex}}$  juga merupakan relasi urutan monomial. Setelah diberikan konsep urutan monomial, berikut ini diberikan definisi mengenai beberapa komponen dari polinomial setelah dilakukan pengurutan berdasarkan suatu relasi urutan monomial.

**Definisi 13.** Diberikan  $f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha \in F[x_1, \dots, x_n]$  adalah suatu polinomial tidak nol dan suatu relasi urutan monomial  $>$  pada  $F[x_1, \dots, x_n]$ .

- **Derajat bersama** (multidegree) dari  $f$  didefinisikan sebagai  $\max\{\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0\}$  terhadap relasi  $>$ , dan dinotasikan dengan  $\text{mdeg}(f)$ .
- **Koefisien utama** (leading coefficient) dari  $f$  didefinisikan sebagai  $a_{\text{mdeg}(f)}$ , dan dinotasikan dengan  $\text{LC}(f)$ .
- **Monomial utama** (leading monomial) dari  $f$  didefinisikan sebagai monomial  $x^{\text{mdeg}(f)}$ , dan dinotasikan dengan  $\text{LM}(f)$ .
- **Suku utama** (leading term) dari  $f$  didefinisikan sebagai  $\text{LC}(f)\text{LM}(f)$ , dan dinotasikan dengan  $\text{LT}(f)$ .

**Contoh 14.** Diberikan  $f = xyz^2 + 2y^4z^2 - xy^2z \in \mathbb{Q}[x, y, z]$  dan relasi urutan monomial lexicographic. Berdasarkan Contoh 10 diperoleh  $f = -xy^2z + 2y^4z^2 + xyz^2$ . Sehingga diperoleh  $\text{mdeg}(f) = (1,2,1)$ ,  $\text{LC}(f) = -1$ ,  $\text{LM}(f) = xy^2z$ , dan  $\text{LT}(f) = -xy^2z$ .

Pada Contoh 10 di atas, dapat dikatakan bahwa variabel  $x$  dianggap lebih besar dari  $y$  dan  $z$ . Oleh karena itu, relasi urutan lexicographic dapat juga dinyatakan dengan definisi  $z < y < x$ . Berikut ini diberikan konsep mengenai perbandingan dari dua variabel dan konsep membagi habis pada monomial.

**Definisi 15.** Diberikan suatu relasi urutan monomial  $>$  pada  $F[x_1, \dots, x_n]$ . Variabel  $x_i$  dikatakan **lebih besar** dari variabel  $x_j$ , dinotasikan dengan  $x_i \gg x_j$  jika  $x_i > x_j^n$ , untuk setiap  $n \in \mathbb{N}_0$ .

**Definisi 16. (Membagi Habis pada Monomial)** Diberikan monomial  $x^\alpha, x^\beta \in F[x_1, \dots, x_n]$  dengan  $\alpha = (\alpha_1, \dots, \alpha_n)$  dan  $\beta = (\beta_1, \dots, \beta_n)$ . Monomial  $x^\alpha$  dikatakan **membagi habis**  $x^\beta$  jika  $\alpha_i \leq \beta_i$  untuk setiap  $1 \leq i \leq n$ , atau dengan kata lain  $x^\beta = x^\alpha x^\gamma$  untuk suatu  $\gamma \in \mathbb{N}_0^n$ .

Sebagai contoh, monomial  $xy^2$  membagi habis  $x^5y^3$ , sebab  $x^5y^3 = (xy^2)(x^4y)$ . Setelah diberikan berbagai konsep mengenai monomial pada  $F[x_1, \dots, x_n]$ , maka dari sini dapat dibentuk suatu algoritma pembagian pada  $F[x_1, \dots, x_n]$ . Pada algoritma pembagian ini perhitungannya relatif terhadap suatu relasi urutan monomial.

Prinsip dasar dari algoritma pembagian pada  $F[x_1, \dots, x_n]$  adalah sebagai berikut. Diberikan polinomial tidak nol  $f_1, \dots, f_s \in F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Diberikan polinomial  $f \in F[x_1, \dots, x_n]$ . Ditentukan nilai awal  $q_1 = \dots = q_s = r = 0$ . Selanjutnya, dilakukan iterasi sebagai berikut:

- (i) Jika  $LT(f)$  habis dibagi  $LT(f_i)$  untuk setiap  $i$ , maka  $LT(f) = a_i LT(f_i)$ . Ditentukan  $q_i \leftarrow a_i$  dan  $f \leftarrow (f - a_i g_i)$ .
- (ii) Jika  $LT(f)$  tidak habis dibagi oleh setiap  $LT(f_i)$ , maka ditentukan  $r \leftarrow LT(f)$  dan  $f \leftarrow (f - LT(f))$ .

Iterasi ini pasti akan berhenti karena  $LT(f)$  selalu berkurang sampai akhirnya diperoleh pembagi 0, dan akhirnya dapat diperoleh  $f = q_1 f_1 + \dots + q_s f_s + r$ . Jika ditulis lebih detail ke dalam suatu algoritma, maka dapat ditulis sebagai berikut.

**Algoritma 1:** Algoritma Pembagian pada  $F[x_1, \dots, x_n]$

**Input** : Polinomial tidak nol  $f_1, \dots, f_s, f \in F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial  $>$  pada  $F[x_1, \dots, x_n]$

**Output** : Polinomial  $q_1, \dots, q_s, r \in F[x_1, \dots, x_n]$  dengan  $f = q_1 f_1 + \dots + q_s f_s + r$ .

**Langkah-langkah:**

- (1)  $q_1 \leftarrow 0, \dots, q_s \leftarrow 0, r \leftarrow 0$ .
- (2) Jika terdapat  $f_i$  dengan  $LT(f_i)$  membagi habis  $LT(f)$ , ke langkah (4)
- (3) Jika untuk setiap  $f_i$ ,  $LT(f_i)$  tidak membagi habis  $LT(f)$ , ke langkah (5)
- (4)  $q_i \leftarrow q_i + \frac{LT(f)}{LT(f_i)}$  dan  $f \leftarrow f - \frac{LT(f)}{LT(f_i)} \cdot f_i$ , ke langkah (2).
- (5)  $r \leftarrow r + LT(f)$  dan  $f \leftarrow f - LT(f)$ , ke langkah (2).

**Contoh 17.** Diberikan  $f_1, f_2, f \in F[x, y]$  dengan  $f_1 = xy + 1$ ,  $f_2 = x + y$ ,  $f = x^2 + x - y^2 + y$ , dan suatu relasi urutan lexicographic dengan definisi  $x > y$ . Menggunakan algoritma pembagian diperoleh:

- (1) **Iterasi ke-1:**  $LT(f) = x^2$  tidak habis dibagi  $LT(f_1) = xy$ , tetapi habis dibagi  $LT(f_2) = x$ . Maka  $q_2 \leftarrow x$  dan  $f \leftarrow f - x f_2 = -xy + x - y^2 + y$ .

(2) **Iterasi ke-2:**  $LT(f) = xy$  habis dibagi  $LT(f_1) = xy$  dengan hasil bagi  $-1$ , sehingga ditentukan  $q_1 \leftarrow (-1)$  dan  $f \leftarrow f - (-1)f_1 = x - y^2 + y + 1$ .

(3) **Iterasi ke-3:**  $LT(f) = x$  tidak habis dibagi  $LT(f_1)$ , tetapi habis dibagi  $LT(f_2)$  dengan hasil bagi  $1$ ,  $q_2 \leftarrow 1$ , yaitu  $q_2 = x + 1$ , dan  $f \leftarrow f - 1f_2 = -y^2 + 1$ .

Dari sini diperoleh bahwa  $LT(f) = y^2$ , tidak habis dibagi  $LT(f_1) = xy$  dan  $LT(f_2) = x$ , sehingga hasil baginya  $0$  dan sisanya  $r = -y^2 + 1$ . Jadi,  $f = x^2 + x - y^2 + y = (-1)(xy + 1) + (x + 1)(x + y) + (-y^2 + 1)$ , dengan  $q_1 = -1$ ,  $q_2 = x + 1$ , dan  $r = -y^2 + 1$ .

**Akibat 18. (Akibat dari Algoritma Pembagian)** Diberikan  $I = \langle f_1, \dots, f_s \rangle$  ideal di  $F[x_1, \dots, x_n]$ ,  $f \in F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Maka terdapat  $q_1, \dots, q_s, r \in F[x_1, \dots, x_n]$  sedemikian hingga  $f = q_1f_1 + \dots + q_sf_s + r$  dengan  $LT(f_i)$  tidak membagi habis  $r$ , untuk setiap  $1 \leq i \leq s$ . Jika  $r = 0$ , maka  $f \in I$ .

## BASIS GROBNER DAN ALGORITMA BUCHBERGER

Pada bagian ini dibahas mengenai konstruksi dari basis Grobner. Basis Grobner merupakan basis dari suatu ideal yang memenuhi beberapa aksioma tertentu. Motivasi dari aksioma tersebut didasarkan pada masalah yang telah diberikan sebelumnya di atas, yaitu untuk menyederhanakan basis awal dari suatu ideal, sehingga diharapkan perhitungan untuk mencari variety dari basis tersebut akan menjadi lebih mudah. Sebelumnya diberikan terlebih dahulu mengenai konsep dari ideal monomial. Suatu ideal  $I$  di  $F[x_1, \dots, x_n]$  disebut *ideal monomial* jika  $I$  dibangun oleh suatu himpunan monomial.

**Lemma 19.** Diberikan ideal monomial  $I = \langle x^\alpha \mid \alpha \in \mathbb{N}_0^n \rangle$  di  $F[x_1, \dots, x_n]$ . Suatu monomial  $x^\beta$  termuat dalam  $I$  jika dan hanya jika terdapat  $1 \leq i \leq n$  sedemikian hingga  $x^{\alpha^{(i)}}$  membagi habis  $x^\beta$ .

**Lemma 20.** Diberikan ideal monomial  $I = \langle x^\alpha \mid \alpha \in \mathbb{N}_0^n \rangle$  di  $F[x_1, \dots, x_n]$ . Maka ketiga pernyataan berikut ini ekuivalen:

- (1)  $f \in I$ .
- (2) Setiap suku dari  $f$  termuat dalam  $I$ .
- (3)  $f \in F[x_1, \dots, x_n]$  dapat dinyatakan sebagai kombinasi linear dari monomial-monomial pada  $I$  atas  $F$ .

Diberikan ideal tidak nol  $I$  di  $F[x_1, \dots, x_n]$ . Maka dapat dibentuk himpunan semua suku utama dari elemen-elemen di  $I$ , yaitu  $LT(I) = \{cx^\alpha \mid (\exists f \in I) LT(f) = cx^\alpha\}$ . Ideal yang dibangun oleh  $LT(I)$  dinotasikan dengan  $\langle LT(I) \rangle$ .

**Lemma 21.** *Diberikan  $I$  adalah ideal di  $F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Maka  $\langle LT(I) \rangle$  merupakan ideal monomial. Lebih lanjut, terdapat  $g_1, \dots, g_t \in I$  sedemikian hingga  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ .*

**Teorema 22.** *Diberikan  $I$  adalah ideal di  $F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Diberikan  $G = \{g_1, \dots, g_t\} \subset I$  dengan  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ . Maka  $I = \langle g_1, \dots, g_t \rangle$ .*

**Akibat 23.** *Diberikan  $I$  adalah ideal di  $F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Diberikan  $G = \{g_1, \dots, g_t\} \subset I$  sedemikian hingga  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ . Maka  $f \in I$  jika dan hanya jika pembagian  $f$  dengan  $g_1, \dots, g_t$  menghasilkan sisa  $r = 0$ .*

Diberikan  $I$  adalah suatu ideal di  $F[x_1, \dots, x_n]$ . Dari sini dapat didefinisikan suatu himpunan sebagai basis untuk ideal  $I$ . Pendefinisian himpunan ini termotivasi dari Teorema 22 yang selanjutnya disebut dengan basis Grobner. Berikut ini diberikan definisi selengkapnya.

**Definisi 24. (Basis Grobner)** *Diberikan  $I$  adalah ideal di  $F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Suatu subset  $G = \{g_1, \dots, g_t\} \subset F[x_1, \dots, x_n]$  disebut dengan **basis Grobner** untuk  $I$  jika  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ .*

Sama halnya dengan pengertian basis untuk ideal, pengertian basis Grobner berbeda dengan pengertian basis pada modul atau ruang vektor di aljabar linear, sebab tidak digunakan sifat bebas linear dan sifat-sifat yang dimiliki juga berbeda. Dari definisi basis Grobner di atas, diperoleh bahwa  $\{g_1, \dots, g_t\}$  merupakan basis Grobner untuk ideal  $I = \langle g_1, \dots, g_t \rangle$  jika dan hanya jika untuk setiap polinomial tidak nol  $f \in I$  terdapat  $1 \leq i \leq t$  sedemikian hingga  $LT(g_i)$  membagi habis  $LT(f)$ .

Setiap ideal tidak nol  $I$  di  $F[x_1, \dots, x_n]$  selalu mempunyai suatu basis Grobner. Basis Grobner untuk  $I$  tidak selalu sama, tergantung dari relasi urutan monomial yang digunakan. Berikut ini diberikan sebuah teorema yang merupakan sifat dari basis Grobner.

**Teorema 25.** *Diberikan  $I$  ideal tidak nol di  $F[x_1, \dots, x_n]$  dan suatu relasi urutan monomial. Diberikan  $f \in F[x_1, \dots, x_n]$  dan  $\{g_1, \dots, g_t\}$  adalah basis Grobner untuk  $I$ , maka:*

- (1) Setiap  $f \in F[x_1, \dots, x_n]$  dapat dinyatakan secara tunggal sebagai  $f = f_i + r$ , dengan  $f_i \in I$  dan tidak ada monomial dari  $r$  yang habis dibagi oleh setiap  $LT(g_1), \dots, LT(g_t)$ .
- (2) Polinomial  $f_i \in I$  dan  $r$  dapat dihitung menggunakan algoritma pembagian.

Basis Grobner harus memuat suatu polinomial dengan derajat total yang lebih kecil dari polinomial pada basis semula. Diberikan  $\{f_1, \dots, f_s\} \subset F[x_1, \dots, x_n]$ . Cara yang paling mudah untuk menentukan basis Grobner dari ideal  $I = \langle f_1, \dots, f_s \rangle$  dapat dilakukan dengan melakukan eliminasi dan pembagian pada  $\{f_1, \dots, f_s\}$ , dan jika tidak dimungkinkan karena masalah derajat, maka perlu ditambahkan suatu polinomial khusus yang disebut dengan S-polinomial. Untuk mencari basis Grobner dari suatu ideal dapat digunakan suatu algoritma yang disebut dengan algoritma Buchberger. Konsep S-polinomial dan algoritma Buchberger akan diberikan pada pembahasan selanjutnya. Sebelumnya, terlebih dahulu diberikan konsep mengenai kelipatan persekutuan terkecil pada monomial.

**Definisi 26.** Diberikan  $f, g \in F[x_1, \dots, x_n]$  dengan  $\alpha = \text{mdeg}(f)$ ,  $\beta = \text{mdeg}(g)$ , dan  $\gamma = \max\{\alpha, \beta\}$ . Suatu monomial  $x^\gamma$  seperti ini disebut dengan **kelipatan persekutuan terkecil** (least common multiple) dari  $LM(f)$  dan  $LM(g)$ , dan dinotasikan dengan  $\text{lcm}(LM(f), LM(g))$ .

**Contoh 27.** Diberikan  $f = 3x^2y^2z + yz$ ,  $g = 5yz^2 - z \in \mathbb{Q}[x, y, z]$  menggunakan urutan lexicographic. Diperoleh:  $LM(f) = 3x^2y^2z$ ,  $LM(g) = 5yz^2$ ,  $\alpha = (2, 2, 1)$ ,  $\beta = (0, 1, 2)$ . Maka  $\gamma = \max\{(2, 2, 1), (0, 1, 2)\} = (2, 2, 2)$ ,  $\text{lcm}(LM(f), LM(g)) = x^2y^2z^2$ .

**Definisi 28. (S-Polinomial)** Diberikan  $f, g \in F[x_1, \dots, x_n]$ . **S-polinomial** dari  $f$  dan  $g$  didefinisikan sebagai polinomial

$$S(f, g) = \frac{\text{lcm}(LM(f), LM(g))}{LT(f)} f - \frac{\text{lcm}(LM(f), LM(g))}{LT(g)} g.$$

**Contoh 29.** Diberikan polinomial  $f = 3x^2y^2z^2 + yz$  dan  $g = 5yz^2 - z$  di  $\mathbb{Q}[x, y, z]$ . Menggunakan relasi urutan lexicographic diperoleh S-polinomial dari  $f$  dan  $g$  adalah

$$S(f, g) = \frac{x^2y^2z^2}{3x^2y^2z} (3x^2y^2z + yz) - \frac{x^2y^2z^2}{5yz^2} (5yz^2 - z) = \frac{1}{3} yz^2 + \frac{1}{5} x^2yz.$$

Diberikan polinomial  $f \in F[x_1, \dots, x_n]$  dengan  $f = \sum_i^t c_i x^{\alpha(i)} g_i$ ,  $c_i \in F$ ,  $g_i \in F[x_1, \dots, x_n]$ , untuk setiap  $i$ . Jika  $c_i \neq 0$ , maka  $\delta = \alpha(i) + \text{mdeg}(g_i) \in \mathbb{N}_0^n$ .

**Lemma 30.** Jika  $\text{mdeg}\left(\sum_i^t c_i x^{\alpha(i)} g_i\right) < \delta$ , maka terdapat suatu  $c_{jk} \in F$  sehingga

$$\sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} \frac{x^\delta}{x^{\gamma_{jk}}} S(g_j, g_k), \text{ dengan } x^{\gamma_{jk}} = \text{lcm}(\text{LM}(g_j), \text{LM}(g_k)).$$

Lebih lanjut, untuk setiap  $j, k$  berlaku  $\text{mdeg}\left(\frac{x^\delta}{x^{\gamma_{jk}}} S(g_j, g_k)\right)$ .

**Teorema 31. (Kriteria Buchberger)** Diketahui  $I = \langle g_1, \dots, g_t \rangle$  ideal di  $F[x_1, \dots, x_n]$ . Himpunan  $G = \{g_1, \dots, g_t\} \subset F[x_1, \dots, x_n]$  merupakan basis Grobner untuk  $I$  jika dan hanya jika untuk setiap  $1 \leq i \neq j \leq t$  berlaku  $S(g_i, g_j) \text{ mod } G = 0$ .

Berdasarkan kriteria Buchberger, dapat dibentuk suatu algoritma yang dapat digunakan untuk menentukan basis Grobner dari suatu ideal. Berikut ini algoritma selengkapnya. Syarat  $S(g_i, g_j) \text{ mod } G = 0$  menyatakan bahwa S-polinomial dari  $g_i$  dan  $g_j$  habis dibagi oleh  $g_1, \dots, g_t$ .

### Algoritma 2: Algoritma Buchberger

**Input** : Ideal  $I \subset F[x_1, \dots, x_n]$  dengan  $I = \langle f_1, \dots, f_s \rangle$  dan suatu relasi urutan monomial pada  $F[x_1, \dots, x_n]$ .

**Output** :  $G = \{g_1, \dots, g_t\} \subset F[x_1, \dots, x_n]$  basis Grobner untuk  $I$ .

**Langkah-langkah:**

- (1).  $G \leftarrow \langle f_1, \dots, f_s \rangle$ .
- (2).  $B \leftarrow \left\{ \{g_j, g_k\} \mid g_j, g_k \in G, j \neq k \right\}$ .
- (3). Jika  $B \neq \emptyset$ , ke langkah (4).
- (4). Dipilih sebarang  $\{g_j, g_k\} \in B$ ,  $B \leftarrow B - \{g_j, g_k\}$ ,  $h \leftarrow S(g_j, g_k)$ .
- (5). Jika  $h \text{ mod } G = 0$ , maka  $B \leftarrow B \cup \{g, h\} \mid g \in G$ ,  $G \leftarrow G \cup \{h\}$ . Ke langkah (3).
- (6). Algoritma berhenti jika  $B = \emptyset$ .

**Contoh 32.** Diketahui ideal  $I = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$  dengan  $f_1 = x^2 - x$ ,  $f_2 = x - y$ . Akan dicari basis Grobner  $G$  untuk  $I$  dengan menggunakan urutan lexicographic. S-Polinomial  $f_1$  dan  $f_2$  adalah

$$S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x.$$

dan sisa pembagiannya dengan  $f_1$  dan  $f_2$  adalah :

$$S(f_1, f_2) \text{ mod } \{f_1, f_2\} = y^2 - y.$$

Menurut kriteria Buchberger, karena  $S(f_1, f_2) \bmod \{f_1, f_2\} = y^2 - y \neq 0$ , maka  $\{f_1, f_2\}$  bukan merupakan basis Grobner untuk  $I$ . Namun dengan mengikutsertakan sisa pembagian tersebut, yaitu  $f_3 = y^2 - y$ , pada himpunan basis menjadi  $G = \{f_1, f_2, f_3\}$  sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2.$$

Perhatikan bahwa :

$$S_1 = xy - x = (y-1)(x-y) + (y^2 - y) = (y-1)f_2 + f_3$$

$$S_2 = xy - y^3 = (y)(x-y) + (-y)(y^2 - y) = (y)f_2 + (-y)f_3$$

$$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y)f_1 + (-x)f_3.$$

Karena untuk  $i = 1, 2, 3$  berlaku  $S_i \bmod G = 0$ , menurut kriteria Buchberger, himpunan  $G = \{x^2 - x, x - y, y^2 - y\}$  merupakan basis Grobner untuk  $I = \langle x^2 - x, x - y \rangle$ .

## KESIMPULAN

Basis Grobner merupakan suatu basis dari suatu ideal di  $F[x_1, \dots, x_n]$  yang mempunyai sifat bahwa Hal ini dapat digunakan untuk menghitung suatu affine variety. Konstruksi dari basis Grobner dimulai dari pendefinisian urutan monomial pada  $F[x_1, \dots, x_n]$  dan algoritma pembagian pada  $F[x_1, \dots, x_n]$ . Misalkan  $LT(f)$  menyatakan suku utama dari  $f \in F[x_1, \dots, x_n]$  dan  $LT(I)$  adalah himpunan semua suku utama dari semua elemen-elemen di  $I$ . Suatu subset  $\{g_1, \dots, g_t\} \subset F[x_1, \dots, x_n]$  disebut basis Grobner untuk  $I$  jika  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ . Setiap ideal tidak nol  $I$  di  $F[x_1, \dots, x_n]$  selalu mempunyai suatu basis Grobner. Basis Grobner untuk  $I$  tidak selalu sama, tergantung dari relasi urutan monomial yang digunakan. Untuk menghitung basis Grobner dari suatu ideal dapat digunakan algoritma Buchberger. Algoritma ini didasarkan pada eliminasi dan pembagian, serta konsep kelipatan persekutuan terkecil pada  $F[x_1, \dots, x_n]$ .

## SARAN

Pada paper ini hanya dibahas mengenai konstruksi dari basis Grobner dan metode penghitungannya. Perlu dilakukan pembahasan selanjutnya mengenai aplikasi basis Grobner pada ketiga masalah dalam bagian pendahuluan di atas, yaitu untuk menyelesaikan masalah

deskripsi ideal, masalah keanggotaan ideal, dan masalah penyelesaian sistem persamaan polinomial.

Basis Grobner dalam paper ini didasarkan pada ring polinomial atas field. Dapat diteliti jika digunakan ring polinomial atas suatu ring komutatif. Misalnya ring Noether, sebab setiap ideal di ring Noether dibangun secara hingga. Perlu diadakan pengkajian lebih lanjut apabila ring yang digunakan tidak bersifat komutatif, seperti ring matriks persegi atas field.

## **DAFTAR PUSTAKA**

- [1] D. Cox, J. Little, and O'Shea, *Ideals, Varieties, and Algorithms, Third Edition*, Springer-Verlag, New York, 2006.
- [2] Thomas Becker and Volker Weispfenning, *Grobner Bases*, Springer-Verlag, New York, 1993.
- [3] Fraleigh, John B., *A First Course in Abstract Algebra, Sixth Edition*, Addison-Wesley, New York, 2000.
- [4] David S. Dummit and Richard M. Foote, *Abstract Algebra, Third Edition*, John Wiley and Sons, New Jersey, 2004.