BAB III

BASIS GRÖBNER

A. Algotritma pembagian Polinomial Variabel Banyak

Algoritma pembagian pada polinomial variabel banyak adalah perumuman dari algoritma pembagian polinomial variabel satu yang telah dijelaskan di bab sebelumnya. Secara umum tujuannya adalah untuk membagi $f \in K[x_1, \ldots, x_n]$ oleh $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ sehingga f dapat dituliskan dalam bentuk $f = a_1 f_1 + \cdots + a_s f_s + r$ dengan $a_1, \ldots, a_s, r \in K[x_1, \ldots, x_n]$. Konsep tentang pengurutan monomial digunakan pada algoritma pembagian di $K[x_1, \ldots, x_n]$ yaitu untuk menentukan suku utama dari suatu $f \in K[x_1, \ldots, x_n]$.

Sama seperti algoritma pembagian pada polinomial variabel satu, algoritma pembagian pada polinomial variabel banyak juga digunakan untuk mengetahui apakah suatu polinomial $f \in K[x_1, \ldots, x_n]$ merupakan elemen ideal atau bukan.

Sebelum membahas lebih jauh tentang algoritma pembagian di $K[x_1, \ldots, x_n]$, terlebih dahulu diperkenalkan definisi membagi habis polinomial.

Definisi 3.1

Misalkan diberikan monomial $x^\alpha, x^\beta \in K[x_1, \ldots, x_n]$ dan $\mathbb{Z}^n_{\geq 0} = \{(\alpha_1, \ldots, \alpha_n) | \alpha_1, \ldots, \alpha_n \geq 0, \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}$. Monomial x^α membagi habis x^β

jika dan hanya jika $\alpha_i \leq \beta_i$ untuk $1 \leq i \leq n$, yaitu $x^{\beta} = x^{\alpha}.x^{\gamma}$ untuk suatu $\gamma \in \mathbb{Z}^n_{\geq 0}$.

Di bawah ini adalah algoritma pembagian pada polinomial variabel banyak.

Algoritma 3.2: Algoritma Pembagian pada Polinomial Variabel Banyak

Input:$f_1, f_2, \ldots, f_s, f \in K[x_1, \ldots, x_n]$ dan relasi urutan monomial " $>$ " pada $K[x_1, \ldots, x_n]$.

Output:$q_1, q_2, \ldots, q_s, r \in K[x_1, \ldots, x_n]$ dengan $f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r$.

1. Diketahui $p = f$
2. Jika $p = 0$ maka algoritma berhenti, jika $p \neq 0$ lanjutkan ke langkah 3
3. (i). Jika terdapat $f_i \in \{f_1, \ldots, f_s\}$ dengan $LT(f_i)$ membagi habis $LT(p)$, maka lanjutkan ke langkah 4.

   (ii). Jika untuk setiap $f_i \in \{f_1, \ldots, f_s\}$, $LT(f_i)$ tidak membagi habis $LT(p)$, maka lanjutkan ke langkah 5.
4. Dibentuk

   $$q_i = q_i + \frac{LT(p)}{LT(f_i)}$$

   dan

   $$p = p - \left(\frac{LT(p)}{LT(f_i)}\right) f_i.$$

   Kemudian kembali ke langkah 3

5. Dibentuk $r = r + LT(p)$ dan $p = p - LT(p)$. Kemudian kembali ke langkah 2.

Untuk lebih memahami algoritma pembagian di polinomial variabel banyak, perhatikan contoh berikut:

Misalkan $f = x^2y + y^2 \in R[x,y]$ dan $F = \{f_1, f_2\} = \{xy - 1, y - 1\} \subset R[x,y]$. Akan dicari $q_1, q_2, r \in R[x,y]$ sehingga $f = q_1f_1 + q_2f_2 + r$ dengan menggunakan algoritma pembagian pada polinomial variabel banyak dan relasi urutan monomial yang digunakan adalah relasi urutan *lexicographic*.

Dari algoritma 3.2 di atas, pertama diketahui bahwa $p = f$, p merupakan polinomial yang akan dibagi oleh f_1 dan f_2, kemudian algoritma akan berhenti jika didapat $p = 0$, artinya tidak ada lagi polinomial p yang dapat dibagi oleh f_1 dan f_2, sehingga didapatkan $q_1, q_2, r \in R[x,y]$ dan didapatkan bentuk $f = q_1f_1 + q_2f_2 + r$.

Langkah-langkah pada algoritma 3.2 dapat ditulis seperti di bawah ini. Perhatikan pada langkah pertama belum dipunyai q_1 dan q_2, karena algoritma belum berjalan, oleh karena itu, langkah pertama dapat ditulis seperti di bawah ini.

$$q_1 =$$
$$q_2 =$$

$$\begin{array}{r|l} f_1 = xy - 1 & \\ f_2 = y - 1 & \overline{x^2y + y^2} \end{array}$$

Karena $LT(f_1) = xy$ membagi habis $LT(f) = LT(p) = x^2y$, maka $q_1 = \frac{LT(p)}{LT(f_1)} = x$ dan didapatkan p yang baru yaitu $p = p - \frac{LT(p)}{LT(f_1)} f_1 = x^2y + y^2 - (x)(xy - 1) = y^2 + x$, seperti di bawah ini

$$\begin{array}{r l}
 & q_1 = x \\
 & q_2 = \\
f_1 = xy - 1 & \sqrt{x^2y + y^2} \\
f_2 = y - 1 & \quad \underline{x^2y - x} \\
 & \qquad\quad y^2 + x
\end{array}$$

Perhatikan untuk p yang baru, $LT(p) = y^2$ tidak dapat dibagi oleh $LT(f_1) = xy$, akan tetapi dapat dibagi oleh $LT(f_2) = y$, sehingga didapatkan $q_2 = \frac{LT(p)}{LT(f_2)} = \frac{y^2}{y} = y$ dan didapatkan p berikutnya yaitu $p = p - \frac{LT(p)}{LT(f_2)} f_2 = y^2 + x - y(y - 1) = x + y$

$$\begin{array}{r l}
 & q_1 = x \\
 & q_2 = y \\
f_1 = xy - 1 & \sqrt{x^2y + y^2} \\
f_2 = y - 1 & \quad \underline{x^2y - x} \\
 & \qquad\quad y^2 + x \\
 & \qquad\quad \underline{y^2 - y} \\
 & \qquad\qquad\quad x + y
\end{array}$$

Untuk $p = x + y$, $LT(p) = x$ tidak dapat dibagi oleh $LT(f_1) = xy$ atau oleh $LT(f_2) = y$, maka menurut langkah 3 (ii) pada algoritma pembagian pada polinomial variabel banyak di atas dibentuk $r = LT(p) = x$ dan dibentuk $p = p - LT(p) = y$.

$$q_1 = x$$
$$q_2 = y$$

$$
\begin{array}{lllll}
f_1 = xy - 1 & \sqrt{x^2y + y^2} & & & \\
f_2 = y - 1 & \underline{\ x^2y - x\ } & & & \\
 & \quad y^2 + x & & & \\
 & \quad \underline{y^2 - y} & & & \\
 & & \underline{x + y} & & r = x \\
 & & \quad y & & \\
\end{array}
$$

Karena $LT(p) = y$ dapat dibagi oleh $LT(f_2) = y$, maka $q_2 = q_2 + \frac{LT(p)}{LT(f_2)} = \frac{y}{y} = 1$

dan didapatkan p berikutnya yaitu $p = p - \frac{LT(p)}{LT(f_2)} f_2 = y - 1(y - 1) = 1$

$$q_1 = x$$
$$q_2 = y + 1$$

$$
\begin{array}{lllll}
f_1 = xy - 1 & \sqrt{x^2y + y^2} & & & \\
f_2 = y - 1 & \underline{\ x^2y - x\ } & & & \\
 & \quad y^2 + x & & & \\
 & \quad \underline{y^2 - y} & & & \\
 & & \underline{x + y} & & r = x \\
 & & \quad y & & \\
 & & \quad \underline{y - 1} & & \\
 & & \qquad \underline{1} & & r = x + 1 \\
 & & \qquad 0 & & \\
\end{array}
$$

Karena untuk $LT(p) = 1$, tidak dapat dibagi oleh $LT(f_1) = xy$ ataupun oleh $LT(f_2) = y$, maka menurut langkah 3 (ii) pada algoritma pembagian pada polinomial variabel banyak di atas dibentuk $r = r + LT(p) = x + 1$ dan dibentuk

$p = 1 - 1 = 0$. Karena $p = 0$ maka algoritma berhenti dan didapatkan $q_1 = x$, $q_2 = y + 1$ dan $r = x + 1$,sehingga $f = x(xy - 1) + (y + 1)(y - 1) + (x + 1)$.

Perhatikan bahwa pada langkah 1 tidak hanya $LT(f_1)$ yang dapat membagi habis $LT(f)$ karena $LT(f_2) = y$ juga membagi habis $LT(f)$. Apabila pada langkah 1 $LT(f_2)$ digunakan menggantikan $LT(f_1)$ hasil akhir yang diperoleh adalah $f = (0)f_1 + (x^2 + y + 1)f_2 + (x^2 + 1)$, sehingga dengan demikian output dari algoritma pembagian pada polinomial variabel banyak tidak tunggal untuk suatu input yang sama. Output dari algoritma juga dapat berbeda-beda, tergantung dari relasi urutan monomial yang digunakan.

Perhatikan bahwa r yang dihasilkan merupakan kombinasi linier monomial atas lapangan K yang tidak dapat dibagi habis oleh $LT(f_1)$ dan $LT(f_2)$. Polinomial r disebut sisa pembagian polinomial f dengan himpunan polinomial F.

Algoritma pembagian di $K[X]$ bisa dijadikan cara untuk membuktikan suatu $f \in K[X]$ merupakan elemen di $I \subset K[X]$ atau bukan, yaitu jika sisa pembagian f oleh $g \in K[X]$ adalah nol. Sehingga f dapat ditulis dalam bentuk $f = qg + 0$, berdasarkan corollary 2.25, $I \subset K[X]$ dapat ditulis dalam bentuk $I = \langle g \rangle$ dan karena $f = qg$ maka f merupakan elemen dari I. Apakah hal yang sama juga berlaku untuk polinomial variabel banyak? Untuk menjawabnya perhatikan contoh di bawah ini.

Contoh

Misalkan $f = xy^2 - x$ dan $F = \{xy + 1, y^2 - 1\}$, dengan menggunakan relasi urutan *lexicographic*, dan dengan menggunakan algoritma pembagian pada polinomial variabel banyak didapatkan

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

sehingga $f \notin I = \langle xy + 1, y^2 - 1 \rangle$. Akan tetapi jika diubah $F = \{xy + 1, y^2 - 1\}$ menjadi $F = \{y^2 - 1, xy + 1\}$ didapatkan

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

Sehingga f merupakan elemen dari I.

Ternyata hal yang sama tidak berlaku pada polinomial variabel banyak. Jika sisa pembagian $f \in K[x_1, \ldots, x_n]$ oleh $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ adalah nol, maka belum tentu f elemen $I \subset K[x_1, \ldots, x_n]$, karena masih ada kemungkinan sisa pembagian f oleh $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ yang tidak menghasilkan nol. Oleh karena itu, akan dicari basis yang lain yang masih membagun I yang sama akan tetapi bisa menghasilkan sisa pembagian selalu nol. Basis tersebut dinamakan basis Gröbner.

B. Ideal Monomial

Dijelaskan di atas, untuk menjamin bahwa suatu $f \in I \subset K[x_1, \ldots, x_n]$ akan dicari pembangun ideal $I \subset K[x_1, \ldots, x_n]$ yang lain, sehingga sisa pembagian f oleh himpunan pembangun I adalah nol. Berikut ini akan diuraikan suatu konsep ideal $I \subset K[x_1, \dots, x_n]$ yang lain dengan himpunan pembangun I berupa monomial-monomial. Untuk selanjutnya ideal monomial ini mempunyai sifat yang unik sehingga mengakibatkan f dapat dibagi dengan himpunan pembangun I dan mengakibatkan $f \in I$. Berikut ini merupakan definisi ideal monomial.

Definisi 3.3

Suatu ideal $I \subset K[x_1, \dots, x_n]$ adalah ideal monomial jika ada suatu himpunan bagian $A \subset \mathbb{Z}_{\geq 0}^n$ sedemikian sehingga I terdiri dari semua polinomial dalam bentuk $\sum_{\alpha \in A} h_\alpha x^\alpha$, dengan $h_\alpha \in K[x_1, \dots, x_n]$. Tulis $I = \langle x^\alpha | \alpha \in A \rangle$.

Lemma 3.4

Diberikan ideal minomial $I = \langle x^\alpha | \alpha \in A \rangle \subseteq K[x_1, \dots, x_n]$. Monomial x^β termuat dalam I jika dan hanya jika x^β dapat dibagi oleh x^α untuk suatu $\alpha \in A$.

Bukti

($\Rightarrow$)

Jika $x^\beta \in I$, maka x^β dapat disajikan menjadi $x^\beta = \sum_{i=1}^{k} h_i \, x^{\alpha(i)}$ dengan $h_i \in K[x_1, \dots, x_n]$ dan $\alpha(i) \in \mathbb{Z}_{\geq 0}^n$. Jika setiap h_i disajikan sebagai kombinasi linier atas monomial-monomial, maka setiap suku yang berada pada ruas kanan dapat dibagi habis oleh suatu $x^{\alpha(i)}$ dengan $1 \leq i \leq k$. Jadi, ruas kiri juga memiliki sifat yang sama yaitu dapat dibagi habis oleh suatu $x^{\alpha(i)}$ dengan $1 \leq i \leq k$.

($\Leftarrow$)

Jika terdapat suatu $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$ dengan $1 \leq i \leq k$ sehingga $x^{\alpha(i)}$ membagi habis x^β, maka $x^\beta = x^\gamma x^{\alpha(i)}$ untuk suatu $\gamma \in \mathbb{Z}^n_{\geq 0}$ dan akibatnya x^β merupakan kelipatan dari suatu $x^{\alpha(i)}$. Jadi, x^β termuat dalam I. ■

Lemma 3.5

Jika diketahui ideal monomial $I = \langle x^\alpha | \alpha \in A \rangle \subseteq K[x_1, \dots, x_n]$ dan

$f \in K[x_1, \dots, x_n]$, maka ketiga pernyataan berikut ekuivalen.

1. $f \in I$.
2. Setiap suku di f termuat di I.
3. f dapat disajikan sebagai kombinasi linier monomial-monomial atas field K pada I.

Bukti

(1) $\Rightarrow$ (2)

Jika $f \in I$, maka f dapat disajikan sebagai $f = \sum_{i=1}^{k} h_i \, x^{\alpha(i)}$ dengan $h_i \in K[x_1, \dots, x_n]$ dan $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Perhatikan bahwa $x^{\alpha(i)} \in I$, akibatnya $h_i x^{\alpha(i)} \in I$. Dengan demikian setiap suku di f termuat di I.

$(2) \Rightarrow (3)$

Jika setiap suku di f termuat di I, maka kombinasi linier setiap suku pada f juga termuat di I. Jadi, f dapat disajikan sebagai kombinasi linier monomial-monomial pada I.

$(3) \Rightarrow (1)$

Karena f dapat disajikan sebagai kombinasi linier monomial-monomial pada I, maka berlaku $f \in I$. ■

Corollary 3.6

Misalkan I dan J adalah ideal monomial, $I = J$ jika dan hanya jika I dan J mempunyai monomial yang sama.

Bukti

$(\Rightarrow)$ Misalkan $I = J$, artinya $\langle x^\alpha | \alpha \in A \rangle = \langle x^\beta | \beta \in B \rangle$. Diambil $x^\alpha \in I$, karena $I = J$, maka $x^\alpha \in J$. Sekarang diambil $x^\beta \in J$, karena $I = J$, maka $x^\beta \in I$. Akibatnya, I dan J mempunyai monomial-monomial yang sama.

$(\Leftarrow)$ Misalkan $I = \langle x^\alpha | \alpha \in A \rangle$ dan $J = \langle x^\beta | \beta \in B \rangle$. Jika I dan J mempunyai monomial-monomial yang sama, maka $x^\beta \in \langle x^\alpha | \alpha \in A \rangle$ dan $x^\alpha \in \langle x^\beta | , \in B \rangle$ sehingga $\langle x^\alpha | \alpha \in A \rangle = \langle x^\beta | \beta \in B \rangle$. ■

Teorema 3.7 menunjukan bahwa semua monomial ideal dari $K[x_1, \ldots, x_n]$ dapat dibangun secara hingga.

Teorema 3.7 Lemma Dickson (Cox 1992:70)

Suatu monomial ideal $I = \langle x^{\alpha} | \alpha \in A \rangle \subseteq K[x_1, \dots, x_n]$ dapat ditulis dalam bentuk $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(k)} \rangle$ dengan $\alpha(i) \in A$, $1 \leq i \leq k$. Dengan kata lain I mempunyai suatu basis yang berhingga.

Bukti

Akan dibuktikan dengan menggukan induksi. Jika $n = 1$, maka I dibangun oleh monomial-monomial x^{α} dengan $\alpha \in A \subset \mathbb{Z}_{\geq 0}^{n}$. Misalkan β adalah elemen terkecil dari $A \subset \mathbb{Z}_{\geq 0}^{n}$, berdasarkan lemma 3.4 x^{β} haruslah membagi setiap generator, atau $I = \langle x^{\beta} \rangle$.

Sekarang asumsikan untuk $n > 1$ dan teorema benar untuk $n - 1$. Dimisalkan variabel-variabel yang akan digunakan adalah $x_1, \dots, x_{n-1}, y$, sehingga monomial-monomial di $K[x_1, \dots, x_{n-1}, y]$ dapat disajikan dalam bentuk $x^{\alpha} y^{m}$, dengan $\alpha = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ dan $m \in N$. Misalkan $I \subset K[x_1, \dots, x_{n-1}, y]$ adalah suatu ideal monomial, dan dimisalkan $J = \langle x^{\alpha} | x^{\alpha} y^{m} \in I \; untuk \; suatu \; m \rangle$ di $K[x_1, \dots, x_{n-1}]$. Kemudian berdasarkan hipotesis induksi, ada $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ $(x^{\alpha(i)} \in \{x^{\alpha} | x^{\alpha} y^{m} \in I \; untuk \; suatu \; m\}$ sedemikian sehingga $J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$ di $K[x_1, \dots, x_{n-1}]$. Dari definisi J, $x^{\alpha(i)} y^{m_i} \in I$ untuk setiap $m_i > 0$, $i = 1, \dots, s$. Misalkan $m = \max\{m_1, \dots, m_s\}$ dan $J_k = \langle x^{\beta} | x^{\beta} y^{k} \in I \rangle$ di $K[x_1, \dots, x_{n-1}]$, $k = 0, \dots, m - 1$. Dari hipotesis induksi, ada $x^{\alpha_k(1)}, \dots, x^{\alpha_k(s_k)}$

sedemikian sehingga $J_k = \langle x^{\alpha_k(1)}, \dots, x^{\alpha_k(s_k)} \rangle$ di $K[x_1, \dots, x_{n-1}]$, dengan $x^{\alpha_k(i)} \in \{x^\beta | x^\beta y^k \in I\}$.

Klaim bahwa I dibangun oleh monomial-monomial seperti dibawah ini:

Dari $J = x^{\alpha(1)}y^m, \dots, x^{\alpha(s)}y^m$,

Dari $J_0 = x^{\alpha_0(1)}, \dots, x^{\alpha_0(s)}$,

Dari $J_1 = x^{\alpha_1(1)}y, \dots, x^{\alpha_1(s)}y$,

$$\vdots$$

Dari $J_{m-1} = x^{\alpha_{m-1}(1)}y^{m-1}, \dots, x^{\alpha_{m-1}(s)}y^{m-1}$.

Perhatikan bahwa setiap monomial di I dapat dibagi dari salah satu monomial dari deretan monomial di atas. Untuk melihatnya, misalkan $x^\alpha y^p \in I$. Jika $p \geq m$, maka $x^\alpha y^p$ dapat dibagi oleh suatu $x^{\alpha(i)}y^m$ hal ini berdasarkan pada konstruksi dari $\sim$. Dengan kata lain, jika $p \leq m - 1$, maka $x^\alpha y^p$ dapat dibagi oleh suatu $x^{\alpha_p(j)}y^p$ hal ini berdasarkan pada konstruksi dari J_p dan berdasarkan lemma 3.4. Berdasarkan corollary 3.6, monomial-monomial di atas membangun suatu ideal yang mempunyai monomial-monomial yang sama sebagai I. Ini mengakibatkan ideal-ideal tersebut sama. Jadi, klaim terbukti.

Sekarang perhatikan $x^{\alpha_k(i)}y^k \in I$, tetapi belum diketahui apakah $x^{\alpha_k(i)}y^k \in \{x^\alpha | \alpha \in A\} \subseteq K[x_1, \dots, x_{n-1}]$ dengan $x_n = y$. Tulis $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle$, dengan $x^{\beta(i)} \in I$, $i = 1, \dots, s$, menurut lemma 3.4, setiap $x^{\beta(i)}$ dapat dibagi habis oleh suatu $x^{\alpha(i)} \in A$ dan $I = \langle x^{\alpha} | \alpha \in A \rangle$. Akibatnya, $I \supseteq \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle \supseteq \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle = I$. Jadi, $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$ ■

C. Basis Gröbner

Definisi 3.8 mengawali pembahasan tentang basis Gröbner.

Definsi 3.8

Misalkan I adalah ideal di $K[x_1, \dots, x_n]$ dan I bukan ideal trivial, himpunan $LT(I) = \{cx^{\alpha} | \exists f \in I, LT(f) = cx^{\alpha}\}$ adalah himpunan semua suku-suku utama dari elemen-elemen di I. Ideal yang dibangun oleh $LT(I)$ dinotasikan dengan $\langle LT(I) \rangle$

Preposisi 3.9 menunjujan bahwa $\langle LT(I) \rangle$ adalah suatu ideal monomial dan dibangun secara hingga.

Preposisi 3.9

Jika I adalah ideal di $K[x_1, \dots, x_n]$, maka:

1. $\langle LT(I) \rangle$ adalah ideal monomial.
2. Ada $g_1, \dots, g_t \in I$ sedemikian sehingga $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$

Bukti

1. Untuk setiap $g \in I$ dengan $g \neq 0$, monomial utama dari g atau $LM(g)$ akan membangun ideal monomial $\langle LM(g)\ | g \neq 0\ dan\ g \in I \rangle$. Karena

$LM(g)$ dan $LT(g)$ hanya berbeda pada koefisiennya saja, maka $\langle LM(g)\ |g \neq 0\ dan\ g \in I\rangle = \langle LT(g)\ |g \neq 0\ dan\ g \in I\rangle = \langle LT(I)\rangle$

2. Seperti pada pembuktian 1, ideal $\langle LT(I)\rangle$ dibangun oleh monomial $LM(g)$ dengan $g \neq 0$ dan $g \in I$ dan teorema 3.7 menyatakan bahwa $\langle LT(I)\rangle = \langle LM(g_1), \dots, LM(g_t)\rangle$ untuk $g_1, \dots, g_t \in I$. Karena $LM(g)$ dan $LT(g)$ berbeda hanya pada koefisiennya saja, maka $\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$ ■

Teorema 3.10 (Teorema Basis Hilbert)

Jika ideal $I \subset K[x_1, \dots, x_n]$ dan $G = \{g_1, \dots, g_t\} \subset I$ dengan $\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$ maka $I = \langle g_1, \dots, g_t\rangle$

Bukti

Akan ditunjukkan bahwa $I = \langle g_1, \dots, g_t\rangle$ yaitu:

1. Akan ditunjukan $\langle g_1, \dots, g_t\rangle \subseteq I$. Karena setiap $g_1, \dots, g_t \in I$, maka jelas bahwa $\langle g_1, \dots, g_t\rangle \subseteq I$.
2. Akan ditunjukan $I \subseteq \langle g_1, \dots, g_t\rangle$ Misalkan $f \in I$ Dengan menggunakan algoritma pembagian pada polinomial variabel banyak untuk membagi f dengan himpunan $G = \{g_1, \dots, g_t\}$ sehingga diperoleh $f = q_1 g_1 + \cdots + q_t g_t + r$, dengan setiap suku pada r tidak dapat dibagi habis oleh $LT(g_1), \dots, LT(g_t)$. Akan ditunjukan bahwa $r = 0$. Perhatikan bahwa $r = f - q_1 g_1 - \cdots - q_t g_t \in I$. Jika $r \neq 0$, maka $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$ sehingga menurut lemma 3.4

berakibat $LT(r)$ dibagi habis oleh suatu $LT(g_i)$ dengan $1 \leq i \leq t$. Hal ini kontradiksi dengan pengandaian di atas, karena r merupakan sisa pembagian yang setiap sukunya tidak dapat dibagi habis oleh $LT(g_1), \dots, LT(g_t)$.

Jadi, berlaku $r = 0$ dan akibatnya $f = q_1 g_1 + \cdots + q_t g_t \in \langle g_1, \dots, g_t \rangle$ atau $I \subseteq \langle g_1, \dots, g_t \rangle$. ■

Himpunan G tersebut merupakan basis Gröbner seperti yang didefinisikan di bawah ini.

Definisi 3.11

Misalkan I ideal di $K[x_1, \dots, x_n]$ dan relasi urutan monomial " $>$ " di $K[x_1, \dots, x_n]$. Himpunan $G = \{g_1, \dots, g_t\} \subset K[x_1, \dots, x_n]$ disebut basis Gröbner untuk ideal I terhadap relasi " $>$ " jika dan hanya jika $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$.

Corollary 3.12 merupakan akibat dari Preposisi 3.9, teorema 3.10 dan definisi 3.11.

Corollary 3.12

Jika I ideal di $K[x_1, \dots, x_n]$, maka setiap ideal non trivial di $K[x_1, \dots, x_n]$ memiliki basis Gröbner. Setiap basis Gröbner untuk I merupakan pembangun ideal I.

Bukti

Misalkan I adalah ideal di $K[x_1, \dots, x_n]$, berdasarkan preposisi 3.9 ada suatu $G = \{g_1, \dots, g_t\} \in I$ sedemikian sehingga $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ dan berdasarkan definisi 3.11 maka G adalah suatu basis Gröbner. Pembuktian bahwa G adalah basis dari I sama seperti pembuktian pada teorema 3.10. ■