BAB II

TEORI PENUNJANG

Pada bab ini akan membahas tentang ring $R[x_1,\ldots,x_n]$ atas lapangan R, urutan monomial dalam $K[x_1,\ldots,x_n]$, algoritma pembagian dan reduksi modulo dalam $K[x_1,\ldots,x_n]$, serta KPK dalam $K[x_1,\ldots,x_n]$.

2. 1 Ring $R[x_1,\ldots,x_n]$ atas Lapangan R

Definisi 2. 1. 1

Operasi Biner $*$ pada himpunan S adalah suatu fungsi dari S x S ke S, yang didefinisikan sebagai $*((a, b)) = a * b$, untuk setiap $(a, b) \in S \times S$.

Contoh: Operasi penjumlahan pada $Z_{\geq 0}$.

Definisi 2. 1. 2

Suatu ring $\langle R,+,\cdot\rangle$ adalah himpunan $R \neq \varnothing$ dengan dua operasi biner yaitu operasi '+' dan operasi '.' , sedemikian sehingga aksioma – aksioma berikut terpenuhi :

1. Terhadap operasi '+' merupakan group abelian :

i. Assosiatif, $(\forall a,b,c \in R)\ (a + b) + c = a + (b + c)$.

ii. Mempunyai elemen netral, $(\exists 0 \in R)(\forall a \in R)\ 0 + a = a + 0 = a$.

iii. Setiap elemen dalam R mempunyai invers didalam R,

$(\forall a \in R)(\exists (-a) \in R)\ a + (-a) = (-a) + a = 0$

iv. Komutatif, $(\forall\ a, b \in R)\ a + b = b + a$.

2. Assosiatif terhadap operasi '.', $(\forall\ a, b, c \in R)(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. i. Distributif kiri : $(\forall\ a, b, c \in R)\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

   ii. Distributif kanan : $(\forall\ a, b, c \in R)\ (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Contoh : $\langle Z,+,\cdot \rangle$

Definisi 2. 1. 3

Suatu ring yang komutatif terhadap perkalian disebut ring komutatif, yaitu $(\forall a, b \in R) a \cdot b = b \cdot a$.

Definisi 2. 1. 4

Suatu ring yang mempunyai elemen identitas terhadap perkalian disebut ring dengan elemen identitas. Elemen identitas terhadap perkalian adalah 1, yaitu $(\exists 1 \in R)(\forall a \in R)\ 1 \cdot a = a \cdot 1 = a$.

Definisi 2. 1. 5

b disebut invers terhadap '.' dari a apabila $b \cdot a = a \cdot b = 1$, untuk selanjutnya dinyatakan $b = a^{-1}$.

Definisi 2. 1. 6

Jika R adalah ring, maka R lapangan apabila memenuhi :

1. R adalah ring komutatif.
2. R mempunyai elemen identitas 1.
3. Setiap elemen dari R yang tidak sama dengan nol, mempunyai invers terhadap '.', yaitu $(\forall a \neq 0 \in R)(\exists a^{-1} \in R)\, a^{-1} \cdot a = a \cdot a^{-1} = 1$.

Contoh : $\langle R,+,\cdot\rangle$ adalah lapangan.

Definisi 2. 1. 7

Diketahui R adalah ring, suatu polinomial f(x) dengan koefisien – koefisien didalam R merupakan penjumlahan tak terbatas berbentuk :

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots$$

dimana $a_i \in R$ merupakan koefisien dari f(x), dan $a_i = 0$ untuk beberapa nilai i. Untuk suatu $i \geq 0$ dengan $a_i \neq 0$ nilai i yang terbesar merupakan derajat dari f(x). Jika semua $a_i = 0$, maka derajatnya tidak terdefinisi. x disebut sebagai indeterminate.

Definisi 2. 1. 8

Jika R ring komutatif dengan elemen identitas dan $f(x)=\sum_{i=0}^{n}a_i x^i$, $g(x)=\sum_{i=0}^{m}b_i x^i$ adalah polinomial - polinomial dengan indeterminatex serta koefisien - koefisien didalam ring R, maka f(x) = g(x) dengan $a_i = b_i$, untuk setiap i.

Definisi 2. 1. 9

Jika $f(x)=\sum_{i=0}^{n}a_i x^i$ dan $g(x)=\sum_{i=0}^{m}b_i x^i$ merupakan polinomial – polinomial dengan koefisien – koefisien dalam ring R, maka penjumlahan dan perkalian polinomial didefinisikan sebagai :

$$f(x)+g(x)=\sum_{i=0}^{p}(a_i+b_i)x^i$$ dengan p bilangan yang terbesar antara n atau m.

$$f(x)\cdot g(x)=\sum_{i=0}^{n+m}c_i x^i \text{ dengan } c_i=\sum_{j=0}^{i}a_j b_{i-j}$$

$$c_i=\sum_{j=0}^{i}a_j b_{i-j}=a_0b_1+a_1b_{i-1}+\ldots+a_{i-1}b_1+a_ib_0=\sum_{p+q=i}a_p b_q$$

Teorema 2. 1. 10

R[x] adalah himpunan semua polinomial dengan indeterminate x dan koefisien – koefisien dalam ring R. Dengan operasi penjumlahan dan perkalian polinomial seperti Definisi 2.1.9, R[x] merupakan ring.

Jika R ring komutatif dan mempunyai elemen identitas 1, maka R[x] ring komutatif dan mempunyai elemen identitas $1x^0$.

Bukti :

Misal $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $h(x) = \sum_{i=0}^{p} c_i x^i$ merupakan elemen – elemen sebarang dalam R[x]. R[x] merupakan ring komutatif dengan elemen identitas apabila memenuhi aksioma – aksioma :

1. Terhadap operasi penjumlahan merupakan group abelian :

i. Assosiatif,

$$(f(x) + g(x)) + h(x) = \sum_{i=0}^{r} (a_i + b_i) x^i + \sum_{i=0}^{p} c_i x^i = \sum_{i=0}^{s} [(a_i + b_i) + c_i] x^i$$

$$= \sum_{i=0}^{s} [a_i + (b_i + c_i)] x^i = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{r} (b_i + c_i) x^i = f(x) + (g(x) + h(x)).$$

ii. Mempunyai elemen identitas yaitu $0x^0$,

$$0x^0 + f(x) = f(x) + 0x^0 = f(x).$$

iii. Setiap elemen dalam R mempunyai invers didalam R,

$$\sum_{i=0}^{n} (-a_i) x^i + \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} (-a_i) x^i = 0x^0.$$

iv. Komutatif,

$$f(x) + g(x) = \sum_{i=0}^{r} (a_i + b_i) x^i = \sum_{i=0}^{r} (b_i + a_i) x^i = g(x) + f(x)$$

2. Terhadap operasi perkalian :

i. Assosiatif.

$$(f(x)\cdot g(x))\cdot h(x)=\left(\sum_{i=0}^{n+m}\left(\sum_{r+q=i}a_r b_q\right)x^i\right)\left(\sum_{i=0}^{p}c_i x^i\right)=\sum_{i=0}^{n+m+p}\left(\sum_{r+q+s=i}(a_r b_q)c_s\right)x^i$$

$$=\sum_{i=0}^{n+m+p}\left(\sum_{r+q+s=i}a_r(b_q c_s)\right)x^i=\sum_{i=0}^{n}a_i x^i\left(\sum_{i=0}^{m+p}\left(\sum_{q+s=i}b_q c_s\right)x^i\right)=f(x)\cdot(g(x)\cdot h(x))$$

ii. Komutatif.

$$f(x)\cdot g(x)=\sum_{i=0}^{n+m}\left(\sum_{r+q=i}a_r b_q\right)x^i=\sum_{i=0}^{m+n}\left(\sum_{q+r=i}b_q a_r\right)x^i=g(x)\cdot f(x)$$

3. i. Distributif kiri :

$$f(x)\cdot(g(x)+h(x))=\sum_{i=0}^{n}a_i x^i\left(\sum_{i=0}^{t}(b_i+c_i)x^i\right)=\sum_{i=0}^{n+t}\left(\sum_{r+q=i}a_r(b_q+c_q)\right)x^i$$

$$=\sum_{i=0}^{n+t}\left(\sum_{r+q=i}(a_r b_q+a_r c_q)\right)x^i=\sum_{i=0}^{n+t}\left(\sum_{r+q=i}a_r b_q\right)x^i+\sum_{i=0}^{n+t}\left(\sum_{r+q=i}a_r c_q\right)x^i$$

$$=\sum_{i=0}^{n+m}\left(\sum_{r+q=i}a_r b_q\right)x^i+\sum_{i=0}^{n+p}\left(\sum_{r+q=i}a_r c_q\right)x^i=f(x)\cdot g(x)+f(x)\cdot h(x)$$

ii. Distributif kanan :

$$(f(x)+g(x))\cdot h(x)=h(x)\cdot(f(x)+g(x))=h(x)\cdot f(x)+h(x)\cdot g(x)$$

$$=f(x)\cdot h(x)+g(x)\cdot h(x)$$

4. Mempunyai elemen identitas, yaitu $1x^0$ karena

$(1x^0)f(x) = f(x)(1x^0) = f(x)$ ♦

Jika R lapangan, maka R[x] bukan lapangan, sebab setiap elemen dari R[x] yang tidak sama dengan nol tidak mempunyai invers, dalam hal ini R[x] merupakan ring komutatif dengan elemen identitas.

Jika R ring dan x, y adalah indeterminate, maka dapat dibentuk ring (R[x])[y] yang merupakan ring dari polinomial – polinomial dengan indeterminate y dan koefisien – koefisien dalam ring polinomial R[x]. Ring ini dapat juga ditulis sebagai ring polinomial dengan indeterminate x dan koefisien – koefisien dalam ring polinomial R[y], yaitu (R[y])[x]. Sehingga ring diatas bisa ditulis sebagai R[x, y] yang merupakan ring polinomial dengan indeterminate x, y dan koefisien – koefisien dalam ring R. Dengan cara sama didapatkan ring $R[x_1,\ldots,x_n]$ yaitu ring polinomial dengan n indeterminate x_i dan koefisien – koefisien dalam ring R. Ring polinomial dengan koefisien – koefisien dalam ring R juga disebut ring polinomial atas ring R. Biasanya digunakan indeterminate x, y, z daripada x_1, x_2, x_3.

Contoh :

Polinomial $f(x, y) = 3x^2y + 2x^2y^2 - 4xy - 8$ merupakan polinomial dengan indeterminate x dan y atas ring R, dapat ditulis sebagai :

$(f(x))(y) = (2x^2)y^2 + (3x^2 - 4x)y - 8$ yang merupakan polinomial dengan indeterminate y atas ring polinomial R[x], atau

$(f(y))(x) = (2y^2 + 3y)x^2 - (4y)x - 8$ yaitu polinomial dengan indeterminate x atas ring polinomial R[y].

Definisi 2. 2. 11

Suatu Monomial dalam $x_1,\ldots,x_n$ adalah suatu perkalian berbentuk $x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\cdots\cdot x_n^{\alpha_n}$ dengan semua eksponen $\alpha_1,\ldots,\alpha_n$ merupakan bilangan bulat non negatif. Derajat dari monomial adalah $\alpha_1+\ldots+\alpha_n$ yang dinotasikan sebagai

$|\alpha| = \alpha_1+\ldots+\alpha_n$.

Jika $\alpha=(\alpha_1,\ldots,\alpha_n)$ adalah tuple-n bilangan bulat non negatif, maka

$x^\alpha = x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\cdots\cdot x_n^{\alpha_n}$.

Contoh : x^4y^2 merupakan monomial dalam indeterminate x, y dan derajat 6.

Suatu polinomial merupakan kombinasi linear dari monomial – monomial.

Definisi 2. 1. 12

Diketahui $f=\sum_\alpha a_\alpha x^\alpha$ adalah polinomial dalam $K[x_1,\ldots,x_n]$

1. a_α adalah koefisien dari monomial x^α.
2. Jika $a_\alpha \neq 0$, maka $a_\alpha x^\alpha$ adalah suku dari f.
3. Derajat dari f dinotasikan sebagai der(f), yang merupakan nilai $|\alpha|$ yang terbesar dengan $a_\alpha \neq 0$.

Contoh :

Polinomial $f(x, y, z) = 2x^3y^2z + 3/2y^3z^3 - 3xyz + y^2$ mempunyai 4 suku dan derajat 6. Dapat dilihat ada 2 suku yang mempunyai derajat terbesar yaitu $2x^3y^2z$ dan $3/2y^3z^3$ yang tidak mungkin terjadi pada polinomial dengan 1 indeterminate.

2. 2. Urutan Monomial dalam $K[x_1,...,x_n]$

Urutan monomial mempunyai peran penting dalam mencari basis Groebner, karena dengan urutan monomial berbeda, akan didapatkan basis yang berbeda. Suatu urutan dari monomial – monomial x^α, x^β akan memenuhi salah satu dari 3 pernyataan berikut : $x^\alpha > x^\beta$ $\quad$ $x^\alpha = x^\beta$ $\quad$ $x^\alpha < x^\beta$.

Urutan yang berhubungan dengan bilangan dalam himpunan bilangan bulat non negatif merupakan urutan total. Suatu urutan dalam bilangan bulat non negatif merupakan urutan yang baik apabila untuk setiap himpunan bagian yang tidak kosong dari himpunan bilangan bulat non negatif mempunyai elemen terkecil apabila diurutkan.

Definisi 2. 2. 1

Urutan monomial pada $K[x_1,...,x_n]$ adalah suatu relasi ">" didalam $Z^n_{\geq 0}$ atau ekuivalen dengan suatu relasi pada himpunan monomial x^α, $\alpha \in Z^n_{\geq 0}$ yang memenuhi :

i. Relasi ">" didalam $Z^n_{\geq 0}$ adalah urutan total.

ii. Jika $\alpha > \beta$ dan $\gamma \in Z^n_{\geq 0}$, maka $\alpha + \gamma > \beta + \gamma$.

iii. Relasi ">" dalam $Z^n_{\geq 0}$ adalah urutan yang baik .

Lemma 2. 2. 2

Relasi ">" dalam $Z^n_{\geq 0}$ merupakan urutan yang baik jika hanya jika setiap barisan yang turun murni didalam $Z^n_{\geq 0}$ yaitu $\alpha(1) > \alpha(2)$... pasti mempunyai elemen terkecil (terbatas).

Bukti :

Akan dibuktikan dengan kontrapositif dari lemma diatas yaitu : relasi ">" bukan urutan yang baik jika hanya jika ada barisan yang turun murni tak terbatas dalam $Z^n_{\geq 0}$.

($\Rightarrow$) Jika relasi ">" bukan urutan yang baik, maka ada himpunan bagian dari $Z^n_{\geq 0}$ yang tidak kosong yaitu S, dan S tidak mempunyai elemen terkecil. Ambil $\alpha(1) \in S$, karena $\alpha(1)$ bukan elemen terkecil, maka ada $\alpha(2) \in S$, sehingga $\alpha(1) > \alpha(2)$, selanjutnya $\alpha(2)$ juga bukan elemen terkecil sehingga ada $\alpha(3) \in S$, sedemikian sehingga $\alpha(1) > \alpha(2) > \alpha(3)$. Begitu seterusnya sampai didapatkan barisan turun murni yang tak terbatas $\alpha(1) > \alpha(2) > \alpha(3)$....

($\Leftarrow$) Sebaliknya jika diberikan barisan tak terbatas { $\alpha(1)$, $\alpha(2)$, $\alpha(3)$,... } yang merupakan himpunan bagian tidak kosong dari $Z^n_{\geq 0}$ tanpa elemen terkecil , maka dari Definisi 2.2.1, relasi ">" bukan urutan yang baik. ♦

Akan didefinisikan 3 urutan monomial yaitu :

1. Urutan Lex (Lexicografic Order).
2. Urutan Grlex (Graded Lexicografic Order).
4. Urutan Grevlex (Graded Reverse Lexicografic Order).

Definisi 2. 2. 3 (Urutan lex)

Misalkan $\alpha = (\alpha_1,\ldots,\alpha_n)$, $\beta = (\beta_1,\ldots,\beta_n)$ dalam $Z^n_{\geq 0}$, maka $\alpha >_{lex} \beta$, apabila $\alpha - \beta \in Z^n$, entri paling kiri yang tidak sama dengan nol adalah positif. Selanjutnya kita tulis $x^\alpha >_{lex} x^\beta$, jika $\alpha >_{lex} \beta$.

Contoh :

a. $\alpha = (1, 2, 0) >_{lex} \beta = (0, 3, 4)$ karena $\alpha - \beta = (1, -1, -4)$.

b. $\alpha = (3, 2, 4) >_{lex} \beta = (3, 2, 1)$ karena $\alpha - \beta = (0, 0, 3)$.

Definisi 2. 2. 4 (Urutan grlex)

Misalkan $\alpha, \beta \in Z^n_{\geq 0}$, maka $\alpha >_{grlex} \beta$, apabila memenuhi:

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

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

Contoh :

a. $(1, 2, 3) >_{grlex} (3, 2, 0)$ karena $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.

b. $(1, 2, 4) >_{grlex} (1, 1, 5)$ karena $|(1, 2, 4)| = 7 = |(1, 1, 5)|$ dan

$(1, 2, 4) >_{lex} (1, 1, 5)$.

Definisi 2. 2. 5 (Urutan grevlex)

Misalkan $\alpha, \beta \in Z^n_{\geq 0}$. Maka $\alpha >_{grevlex} \beta$, apabila memenuhi :

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

ii. $|\alpha| = |\beta|$ dan untuk $\alpha - \beta \in Z^n$, entri paling kanan yang tidak sama dengan nol adalah negatif.

Contoh :

a. $(4, 7, 1) >_{grevlex} (4, 2, 3)$ karena $|(4, 7, 1)| = 12 > |(4, 2, 3)| = 9$

b. $(1, 5, 2) >_{grevlex} (4, 1, 3)$ karena $|(1, 5, 2)| = 8 = |(4, 1, 3)|$ dan

(1, 5, 2) - (4, 1, 3) = (-3, 4, -1).

Dibawah ini diberikan contoh penggunaan ketiga urutan monomial diatas pada polinomial $f(x, y z) = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ dalam K[x, y, z]

Dengan urutan lex : $-5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$

Dengan urutan grlex : $7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$

Dengan urutan grevlex : $4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$

Definisi 2. 2. 6

Jika $f = \sum_{\alpha} a_\alpha x^\alpha \in K[x_1,\ldots,x_n]$, f polinomial tidak sama dengan nol dan relasi "$>$" merupakan urutan monomial , maka

i. Multiderajat dari f adalah multider (f) = maks ($\alpha \in Z^n_{\geq 0} \mid a_\alpha \neq 0$)

(maksimum dari f tergantung pada urutan yang dipakai).

ii. Koefisien awal dari f adalah LC (f) = $a_{\text{multider}(f)} \in K$

iii. Monomial awal dari f adalah LM (f) = $x^{\text{multider}(f)}$

iv. Suku awal dari f adalah LT (f) = LC (f) LM (f)

Contoh :

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$ dengan urutan lex menjadi

$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$ dan didapatkan :

multider (f) = (3, 0, 0)

LC (f) = -5

LM (f) = x^3

LT (f) = $-5x^3$

Lemma 2. 2. 7

Jika f, g$\in$K[$x_1,\ldots,x_n$] adalah polinomial tidak sama dengan nol, maka :

i. Multider ($f \cdot g$) = multider (f) + multider (g)

ii. Jika $f + g \neq 0$, maka

multider (f + g) $\leq$ maks { multider (f), multider (g) }.

2. 3. Algoritma Pembagian dan Reduksi Modulo dalam K[$x_1,\ldots,x_n$]

Terlebih dahulu akan diberikan teorema tentang algoritma pembagian dalam K[$x_1,\ldots,x_n$].

Teorema 2. 3. 1

Jika urutan monomial ">" didalam $Z^n_{\geq 0}$, dan F = ($f_1,\ldots,f_s$) adalah urutan dari tuple-s polinomial – polinomial dalam K[$x_1,\ldots,x_n$], maka untuk setiap f$\in$K[$x_1,\ldots,x_n$] dapat ditulis $f = a_1f_1 + \ldots + a_sf_s + r$, dimana a_i, r$\in$K[$x_1,\ldots,x_n$] dengan r = 0 atau monomial dari r tidak dapat dibagi oleh suatu LT (f_1), ... LT (f_s). Selanjutnya jika $a_if_i \neq 0$, maka multider (f) $\geq$ multider (a_if_i).

Bukti :

Untuk membuktikan keberadaan $a_1, ..., a_s$ dan r akan diberikan algoritma dan juga ditunjukkan bahwa dengan masukan yang diberikan algoritmanya akan berjalan.

Masukan : $f_1, ..., f_s, f$

Hasil : $a_1, ..., a_s, r$

$a_1 := 0$; ... ; $a_s := 0$; $r := 0$

$p := f$

Ketika $p \neq 0$ hitung

  $i := 1$

  Terjadi pembagian := salah

  Ketika $i \leq s$ dan terjadi pembagian := salah hitung

    Jika LT (f_i) membagi LT (p), maka

      $a_i := a_i + LT(p) / LT(f_i)$

      $p := p - \{ LT(p) / LT(f_i) \} f_i$

      Terjadi pembagian := benar

    Yang lain

      $i := i + 1$

  Jika terjadi pembagian := salah, maka

    $r := r + LT(p)$

    $p := p - LT(p)$

Terjadi pembagian berarti ketika suatu LT (f_i) membagi LT (p). Setiap melewati "Ketika $p \neq 0$ hitung", tepat satu dari dua hal dibawah ini terjadi :

1. (Langkah pembagian) jika suatu LT (f_i) membagi LT (p), maka

$$a_i := a_i + LT(p) / LT(f_i)$$

$$p := p - \{ LT(p) / LT(f_i) \} f_i$$

2. (Langkah sisa) jika tidak ada LT (f_i) membagi LT (p), maka LT (p) ditambahkan ke sisa.

Algoritma berjalan karena nilai awal dari $a_1, ..., a_s$, p dan r memenuhi :

$$f = a_1f_1 + ... + a_sf_s + p + r \qquad ...(2.3.i)$$

Sekarang akan ditunjukkan bahwa nilai $a_1, ..., a_s$, p dan r yang baru juga memenuhi (2.3.i). Andai (2. 3. i) benar pada awal algoritma, maka untuk langkah berikutnya :

Jika langkah pembagian, maka :

$a_if_i + p = \{ a_i + LT(p) / LT(f_i) \} f_i + [p - \{ LT(p) / LT(f_i) \} f_i]$

karena semua variabel yang lain tidak berpengaruh, maka dapat dilihat $a_if_i + p$ tidak berubah, sehingga (2. 3. i) tetap terpenuhi.

Jika langkah sisa, maka :

$p + r = \{ p - LT(p)) + r + LT(p) \}$.

Disini p dan r akan berubah, tapi penjumlahan p + r tidak berubah dan tetap memenuhi (2. 3. i).

Selanjutnya algoritma akan berhenti ketika p = 0, dalam hal ini (2. 3.i) menjadi $f = a_1f_1 + ... + a_sf_s + r$. Untuk melihat algoritama berhenti maka harus ditunjukkan bahwa setiap mendefinisikan kembali variabel p, multiderajatnya akan turun atau p menjadi nol. Selama langkah pembagian, p didefinisikan menjadi

$$p' = p - \{ LT(p) / LT(f_i) \} f_i$$

Sekarang akan dicari suku awal dari $\{ LT(p) / LT(f_i) \} f_i$ yaitu

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

dapat dilihat p dan $\{ LT(p) / LT(f_i) \} f_i$ mempunyai suku awal yang sama, oleh karena itu untuk $p' \neq 0$ maka p' harus mempunyai multiderajat yang lebih kecil. Sekarang selama langkah sisa p didefinisikan menjadi :

$$p' = p - LT(p)$$

dari sini jelas bahwa multider (p') < multider (p) untuk $p' \neq 0$. Jadi multiderajat dari p pasti menurun. Apabila algoritma tidak pernah berhenti, maka akan didapatkan barisan multiderajat yang turun tak terbatas, hal ini bertentangan dengan syarat urutan yang baik, sehingga pasti akan didapatkan $p = 0$.

Selanjutnya akan dicari hubungan antara multider (f) dan multider ($a_i f_i$). Algoritma dimulai dengan $p = f$ dan diselesaikan dengan membuktikan bahwa multider (p) menurun. Hal ini menunjukkan bahwa $LT(p) \leq LT(f)$ sehingga multider ($a_i f_i$) ≤ multider (f) untuk $a_i f_i \neq 0$. ♦

Contoh :

Akan dibagi $f = x^2y + xy^2 + y^2$ dengan $f_1 = xy - 1$ dan $f_2 = y^2 - 1$ serta menggunakan urutan lex : $x > y$

$a_1 : x + y$

$a_2 : 1$

$$\begin{array}{l} xy-1 \\ y^2-1 \end{array} \sqrt{x^2y + xy^2 + y^2}$$

$$\underline{x^2y - x}$$

$$xy^2 + x + y^2$$

$$\underline{xy^2 - y}$$

$$\underline{x + y^2 + y}$$

$$y^2 + y \quad \rightarrow \quad x$$

$$\underline{y^2 - 1}$$

$$\underline{y + 1}$$

$$\underline{1} \quad \rightarrow \quad x + y$$

$$0 \quad \rightarrow \quad x + y + 1$$

kita dapatkan sisa = $x + y + 1$ sehingga

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

Untuk selanjutnya sisa dari f dibagi oleh F ditulis sebagai $\overline{f}^{F}$. Sekarang akan dibahas tentang reduksi modulo dalam $K[x_1,\ldots,x_n]$.

Definisi 2. 3. 2

Misalkan polinomial-polinomial $f \neq 0$ dan $g \neq 0$ dalam $K[x_1,\ldots,x_n\}$. f tereduksi modulo g jika ada monomial dari f yang dapat dibagi oleh monomial awal dari g. Jika $f = ap + r$ dimana $a \in K\text{-}\{0\}$, $p \in x^{\alpha}$, $r \in K[x_1,\ldots,x_n]$, maka

$$f \rightarrow_g f - \left\{\frac{ap}{LT(g)}\right\} g = f'$$

yang berarti f tereduksi modulo g menjadi f'.

Jika p tereduksi modulo suatu polinomial dalam $G = \{g_1,\ldots,g_m\}$ menjadi p', maka $p \rightarrow_G p'$. Apabila tidak ada monomial dari p yang dapat dibagi oleh suatu monomial awal dari G, maka dikatakan p tidak tereduksi.

Contoh :

$f = 2y^2z - xz^2$ dan $g = 7y^2 + yz$

$$f \rightarrow_g \left(2y^2z - xz^2\right) - \frac{2y^2z}{7y^2}\left(7y^2 + yz\right) = -xz^2 - \frac{2}{7}yz^2.$$

Definisi 2. 3. 3

Misalkan $G = \{g_1,\ldots,g_s\} \subset K[x_1,\ldots,x_n]$ dengan urutan monomial tertentu dan $f \in K[x_1,\ldots,x_n]$. Apabila f dapat ditulis dalam bentuk $f = a_1g_1 + \ldots + a_tg_t$ dengan $a_ig_i \neq 0$ dan multider (f) $\geq$ multider(a_ig_i), maka f dikatakan tereduksi modulo G menjadi nol dan dinyatakan dengan $f \rightarrow_G 0$.

Pada algoritma pembagian apabila f dibagi f_i didapatkan $r = 0$, maka f dapat ditulis $f = a_1f_1 + \ldots + a_tf_t$ dengan $a_if_i \neq 0$ dan multider(f) $\geq$ multider(a_if_i), sedangkan untuk f tereduksi modulo f_i menjadi nol ditulis $f = a_1f_1 + \ldots + a_tf_t$ dengan $a_if_i \neq 0$ dan multider(f) $\geq$ multider(a_if_i). Jadi apabila $f_i \mid f$, maka reduksi modulo dan algoritma pembagian ekuivalen.

Contoh :

$f = x^4y + x^2$ dan $F = (x^2y + 1, y + 1)$,digunakan urutan lex dalam $K[x, y]$.

Dengan algoritma pembagian :

$x^4y + x^2 = x^2(x^2y + 1) + 0(y + 1)$ dan multider$(x^4y + x^2) \geq$ multider$(x^2(x^2y + 1))$.

Dengan reduksi modulo :

$x^4y + x^2 \to_F (x^4y + x^2) - x^2(x^2y + 1) = 0$ sehingga $x^4y + x^2 = x^2(x^2y + 1) + 0(y + 1)$ dengan multider$(x^4y + x^2) \geq$ multider$(x^2(x^2y + 1))$.

2. 4. Kelipatan Persekutuan Terkecil (KPK) dalam $K[x_1,\ldots,x_n]$

Definisi 2. 4. 1

Misalkan polinomial – polinomial f, g, h $\in K[x_1,\ldots,x_n]$, h disebut kelipatan persekutuan terkecil dari f dan g, selanjutnya dinotasikan dengan h = KPK(f, g) apabila :

1. $f \mid h$ dan $g \mid h$.
2. $f \mid r$ dan $g \mid r \Rightarrow h \mid r$, $r \in K[x_1,\ldots,x_n]$.

Contoh :

Misalkan $f = x^3yz + x^3 = x^3(yz + 1)$ dan $g = x^2y^2 + x^2z = x^2(y^2 + z)$, dengan menggunakan urutan lex didapatkan KPK dari f, g yaitu

$\text{KPK}(f, g) = x^3(yz + 1)(y^2 + z) = (x^3yz + x^3)(y^2 + z) = x^3y^3z + x^3y^2 + x^3yz^2 + x^3z$