BASIS GRÖBNER UNTUK IDEAL DI GELANGGANG POLINOMIAL

RIDWAN SETIAWAN

0305010513

UNIVERSITAS INDONESIA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

DEPARTEMEN MATEMATIKA

DEPOK

2009

BASIS GRÖBNER UNTUK IDEAL DI GELANGGANG POLINOMIAL

Skripsi diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains

Oleh:

RIDWAN SETIAWAN

0305010513

DEPOK

2009

SKRIPSI : BASIS GRÖBNER UNTUK IDEAL DI GELANGGANG POLINOMIAL

NAMA : RIDWAN SETIAWAN

NPM : 0305010513

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

DEPOK, 14 DESEMBER 2009

Dr. SRI MARDIYATI, M.Kom	HELEN BURHAN, M.Si
PEMBIMBING I	PEMBIMBING II

Tanggal lulus Ujian Sidang Sarjana: 23 Desember 2009

PENGUJI I : Dr. Sri Mardiyati, M.Kom.

PENGUJI II : Mila Novita, S.Si, M.Si.

PENGUJI III : Prof. Dr. Belawati H Widjaja

KATA PENGANTAR

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan begitu banyak nikmat dan rahmat-Nya sehingga tugas akhir ini dapat terselesaikan. Sehubungan dengan kemampuan penulis yang masih sangat terbatas, maka penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna. Masih banyak kekurangan baik dalam penyajian materi maupun penyusunannya.

Dalam penyusunan tugas akhir ini penulis banyak menerima bantuan, bimbingan, dukungan serta doa dari berbagai pihak yang telah mau dan bersedia meluangkan waktunya bagi penulis untuk memberikan arahan yang berhubungan dengan penyusunan tugas akhir ini. Untuk itu penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam penulisan tugas akhir ini, khususnya penulis sampaikan kepada:

1. Bu Sri Mardiyati dan Bu Helen Burhan, selaku pembimbing I dan II. Terima kasih atas bimbingan, saran, kritik, serta kesabaran yang luar biasa dalam membimbing penulis.
2. Bu Rustina, pembimbing akademik yang selalu memberi nasihat dan arahan kepada penulis selama kuliah di departemen Matematika UI.
3. Bu Kiki, Bu Nora, Pak Alhaji, Pak Djati. Terima kasih atas saran serta masukannya.

4. Karyawan & staf departemen Matematika UI, terima kasih atas segala bantuannya.
5. Orang tua penulis Bapak Wawan Hermawan & Ibu Afia Damayanti, serta The Brother Rio Nurmawan, Deni Heriawan & Adam Dewa Andhika. Terima kasih atas segala dukungan dan doanya. Semoga penulis dapat menjadi orang yang berguna untuk kalian.
6. Lya Chikmatul Maula, terimakasih untuk segala motivasi, semangat dan perhatian yang tiada hentinya.
7. Bapak Ponidi (Alm) & Ibu Istiqomah, serta anak-anaknya, Usama, Aisyah, Asyafah, Atikah, Umar. Terima kasih untuk tempat tinggal yang penulis tempati selama hampir 4 tahun.
8. Anak-anak kontrakan, mulai dari Arif Wirawan satu-satunya playboy yang belum pernah punya pacar, kemudian Dimas Trisnadi yang kabar nikahnya tiba-tiba, Moh Abdul Latief yang sering kena sial di kota yang keras ini, Ashari Hidayat yang super sibuk, juga Sigap Pamungkas yang betul-betul sigap. Terima kasih juga untuk temen-temen yang sempat tinggal di kontrakan bareng, yaitu Hairu, Nunug, Imba dll.
9. The Abelian gank: Maul sang ketua Abel nonaktif, Uun, Rifkos, Dimas, Udin, Hamdan, Aris, Trian, Hairu, Asep, Imba, dan Cupliz.
10. Teman-teman Math ’05: Ardibian (makasih pinjaman kartu perpusnya), Fika, Akmal & Maria (temen seperjuangan nyuci PM), g4ul gank: Othe, khuri, Nisma & Melati. Kemudian juga temen-temen seperjuangan Anggi, Puji, Desti, Mia, Nurma, Teha, Inul, Yuni serta teman-teman lain yang

tidak bisa disebutkan satu persatu. Terima kasih atas kebersamaan, dukungan dan do'anya.

11. The BigBos '06: Aliman, Budiono, Rendy, Oza, Billy dkk yang selalu meramaikan suasana di depan gedung Matematik.
12. Semua teman-teman yang pernah mengucapkan kata "SEMANGAT" dengan lantang.
13. Terima kasih juga untuk gitar kopong butut merk Allegro yang sudah menemani selama lebih dari 10 tahun dan akhirnya hancur juga. Semoga nanti ada Ibanez elektrik yang bisa menggantikanmu.

Penulis mengucapkan banyak terima kasih pada semua pihak yang tidak dapat penulis sebutkan yang telah memberi bantuan, dorongan dan semangat yang sangat berarti.

Penulis

2009

ABSTRAK

Ideal I dari suatu gelanggang R adalah himpunan bagian dari R yang memiliki sifat tertentu. Setiap ideal yang bukan ideal nol memiliki basis yang tidak unik. Untuk suatu ideal di gelanggang polinomial $F[X]$, terdapat basis yang dikenal dengan basis Gröbner. Dalam tugas akhir ini akan dibahas bagaimana cara memeriksa suatu basis yang diberikan berupa basis Gröbner atau bukan. Jika bukan basis Gröbner, akan ditunjukkan cara membentuk basis Gröbner berdasarkan basis tersebut. Untuk suatu basis sembarang $G = \{g_1, ..., g_s\} \subset F[X]$ di ideal I (dapat ditulis sebagai $I = (g_1, ..., g_s)$), diperlukan S-polinomial dari g_i dan g_j di I untuk $1 \le i < j \le s$ melakukan pemeriksaan dan atau pembentukan basis Gröbner

Kata kunci : Gelanggang polinomial, ideal, S-polinomial, pereduksian polinomial, basis Gröbner.

vi + 54 hlm.

Bibliografi: 6 (1975-2009)

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Aljabar abstrak adalah suatu bidang di matematika yang mempelajari struktur aljabar seperti grup, gelanggang, lapangan, modul dan ruang vektor. Struktur aljabar adalah suatu stuktur yang terdiri atas suatu himpunan dan operasi biner pada himpunan tersebut beserta sifat-sifatnya. Grup, gelanggang dan lapangan adalah struktur aljabar yang banyak digunakan pada aplikasi seperti teori bilangan, coding theory atau kriptografi.

Untuk suatu gelanggang atau lapangan, dapat didefinisikan suatu polinomial dengan koefisien-koefisiennya merupakan anggota dari gelanggang atau lapangan tersebut. Jika R adalah gelanggang, maka himpunan semua polinomial dalam X dengan koefisien di R dinotasikan dengan $R[X]$. Jika F adalah lapangan, maka himpunan semua polinomial dalam X dengan koefisien di F dinotasikan dengan $F[X]$. $R[X]$ dan $F[X]$ merupakan suatu gelanggang dan disebut sebagai gelanggang polinomial.

Dalam gelanggang, terdapat himpunan bagian yang memiliki sifat tertentu dan dikenal dengan sebutan ideal. Jika R adalah gelanggang, maka ideal yang dibangun oleh elemen-elemen $a_1,...,a_n$ di R dinotasikan dengan $I=(a_1,...,a_n)$. Hal yang sama juga berlaku untuk gelanggang polinomial. Jika $R[X]$ adalah gelanggang polinomial, maka ideal yang dibangun oleh elemen-elemen $f_1,...,f_n$ di $R[X]$ dinotasikan dengan $I=(f_1,...,f_n)$.

Berdasarkan pengertian ideal di gelanggang polinomial, maka setiap elemen di I bisa ditulis sebagai kombinasi linier dari himpunan pembangunnya dengan koefisiennya di gelanggang $R[X]$. Himpunan pembangun itu disebut sebagai *basis* dari ideal, walaupun representasi dari setiap elemen di I sebagai R-kombinasi linier dari f_i tidak selalu unik.

Misalkan $I=(f_1,...,f_s)$ adalah ideal di suatu gelanggang polinomial $R[X]$. Untuk memeriksa apakah suatu elemen f di $R[X]$ merupakan elemen di I, maka harus ditunjukkan representasi f sebagai R-kombinasi linier dari f_i. Selanjutnya jika diberikan $I=(f_1,...,f_s)$ dan $I'=(f_1',...,f_s')$, apakah $I=I'$? Jika kita mempunyai basis Gröbner dari suatu ideal, akan lebih mudah untuk menjawab pertanyaan-pertanyaan tersebut.

Berdasarkan uraian diatas, maka pembahasan mengenai basis Gröbner menjadi sangat menarik. Teori mengenai basis Gröbner telah diperkenalkan pada tahun 1965 oleh Bruno Buchberger dan sampai saat ini

berbagai aplikasi dalam bidang matematika abstrak maupun dalam sains dan teknik telah menggunakan teori tentang basis Gröbner.

1.2 PERUMUSAN MASALAH

Dalam tugas akhir ini, masalah yang akan dibahas adalah:

- Bagaimana kita mengetahui suatu basis dari suatu ideal dari gelanggang polinomial adalah basis Gröbner?
- Bagaimana membentuk suatu basis Gröbner dari suatu basis yang bukan Gröbner?

1.3 TUJUAN PENULISAN

Tujuan penelitian yang dilakukan dalam tugas akhir ini adalah:

- Memeriksa apakah basis dari ideal dari gelanggang polinomial yang diberikan merupakan basis Gröbner atau bukan.
- Membentuk sebuah basis Gröbner dari suatu basis yang bukan Gröbner.

1.4 METODE PENELITIAN

Metode penelitian yang digunakan dalam proses pembuatan tugas akhir ini adalah studi literatur, yaitu dengan cara mempelajari buku-buku referensi, jurnal, ataupun materi penunjang lain dari website yang berhubungan dengan topik tugas akhir ini.

1.5 SISTEMATIKA PENULISAN

Penulisan tugas akhir ini akan dibagi dalam empat bab, yang dimulai dengan pendahuluan pada bab I, yang berisi tentang latar belakang, tujuan penulisan, rumusan masalah, metode penelitian dan sistematika penulisan.

Selanjutnya, Bab II berisi tentang pengertian dasar dalam struktur aljabar, serta sifat-sifat yang akan digunakan dalam pembahasan tugas akhir ini.

Bab III yang merupakan isi dari tugas akhir ini membahas tentang algoritma Euclid untuk polinomial, pereduksian polinomial, definisi basis Gröbner, serta cara pembentukan basis Gröbner dari suatu basis yang bukan Gröbner.

Bab IV merupakan penutup, berisi kesimpulan yang diambil dari pembahasan mengenai topik tugas akhir dan juga saran.

BAB II

LANDASAN TEORI

Pada bab ini, akan dibahas definisi-definisi dasar yang diperlukan untuk lebih memahami isi pembahasan yang akan diberikan pada bab selanjutnya, sekaligus juga untuk menyamakan notasi dan terminologi di seluruh tulisan dalam tugas akhir ini.

Berikut ini akan diberikan pengertian grup, gelanggang, serta definisi lain yang berkaitan.

Definisi 2.1

Suatu *grup* $(G,*)$ adalah suatu himpunan G dengan satu operasi biner $*$ yang memenuhi sifat-sifat berikut:

1. Tertutup : $a*b \in G$, untuk setiap $a,b \in G$.
2. Assosiatif : $a*(b*c)=(a*b)*c$, untuk setiap $a,b,c \in G$.
3. Terdapat elemen identitas $e \in G$ sedemikian sehingga $a*e=e*a=a$, untuk setiap $a \in G$.

4. Untuk setiap $a \in G$, terdapat suatu invers dari a di G (dinotasikan dengan a^{-1}), sedemikian sehingga $a * a^{-1} = a^{-1} * a = e$.

(I. N. Herstein, 1996)

Definisi 2.2

Suatu grup $(G,*)$ disebut grup *komutatif* (atau grup *abel*) apabila memenuhi hukum komutatif, yaitu : $a * b = b * a$ untuk setiap $a, b \in G$.

(I. N. Herstein, 1996)

Definisi 2.3

Suatu himpunan bagian tak kosong H dari grup G disebut *subgrup* dari G, bila H itu sendiri merupakan grup dengan operasi yang sama seperti pada G.

(I. N. Herstein, 1996)

Definisi 2.4

Suatu himpunan R dengan 2 operasi $+$ dan $\bullet$ disebut *gelanggang* jika memenuhi:

1. $(R,+)$ adalah grup komutatif.
2. $(R,\bullet)$ bersifat tertutup dan assosiatif.
3. $(R,+,\bullet)$ memenuhi sifat distributif, yaitu untuk setiap $a,b,c \in R$, berlaku $a\bullet(b+c)=a\bullet b+a\bullet c$ dan $(b+c)\bullet a=b\bullet a+c\bullet a$.

(I. N. Herstein, 1996)

Suatu gelanggang R disebut *gelanggang komutatif* jika operasi $\bullet$ bersifat komutatif. Suatu gelanggang R disebut *gelanggang dengan unsur satuan* jika terdapat elemen $1\in R$ sedemikian sehingga $a\bullet 1=1\bullet a=a$, untuk setiap $a\in R$

Definisi 2.5

Suatu gelanggang komutatif R disebut *daerah integral* jika $a\bullet b=0$ mengakibatkan $a=0$ atau $b=0$.

(I. N. Herstein, 1996)

Definisi 2.6

Suatu himpunan F dengan 2 operasi $+$ dan $\bullet$ disebut *lapangan* bila memenuhi:

2 $(F,+)$ merupakan grup komutatif.

3 $(F-\{0\},\bullet)$ merupakan grup komutatif.

4 $(F,+,\bullet)$ memenuhi sifat distributif, artinya $a\bullet(b+c)=a\bullet b+a\bullet c$ untuk setiap $a,b,c\in F$.

(I. N. Herstein, 1996)

Untuk selanjutnya, $a\bullet b$ dinyatakan dengan ab.

Definisi 2.7

Himpunan semua bilangan bulat yang menghasilkan sisa a jika dibagi dengan $n\in N$ disebut kelas a modulo n, dinotasikan $[a]_n$.

Dengan kata lain, $[a]_n = \{a+nk \mid k\in Z\}$.

(Alexander Bogomolny, 1996)

Pandang $Z_n=\{[a]_n \mid a\in Z\}$ dengan dua operasi penjumlahan dan perkalian sebagai berikut:

$$+:[a]_n+[b]_n=[a+b]_n$$

$$\bullet : [a]_n \bullet [b]_n = [a \bullet b]_n$$

maka

1. $(Z_n, +)$ merupakan grup komutatif.
2. $(Z_n, \bullet)$ memenuhi sifat assosiatif dan komutatif.
3. $(Z_n, +, \bullet)$ memenuhi sifat distributif, karena

   $[a]_n \bullet \left([b]_n + [c]_n\right) = [a]_n \bullet [b]_n + [a]_n \bullet [c]_n$ untuk setiap $[a]_n, [b]_n, [c]_n \in Z_n$.

Jadi, Z_n merupakan suatu *gelanggang komutatif*.

Jika $n = p$, dimana p prima, maka $\left(Z_p - \{[0]\}, \bullet\right)$ dapat dibuktikan sebagai grup komutatif dengan menggunakan teorema Fermat berikut ini.

Teorema *2*.8 (*Teorema Fermat*)

Jika p adalah prima dan $p \nmid a$, maka $a^{p-1} \equiv 1 \mod p$.

Untuk suatu bilangan bulat b, jika $p \mid b$ maka $b^p \equiv b \mod p$.

(I. N. Herstein, 1996)

Teorema 2.9

Misalkan $Z_p^* = Z_p - \{[0]\}$. Maka $(Z_p^*, \bullet)$ dengan p bilangan prima merupakan grup komutatif.

Bukti:

Untuk p prima, $(Z_p^*, \bullet)$ memenuhi sifat assosiatif dan komutatif. Elemen identitas dalam $(Z_p^*, \bullet)$ adalah $[1]_p$, karena $[a]_p \bullet [1]_p = [a \bullet 1]_p = [a]_p$ untuk setiap $[a]_p \in Z_p^*$. Selanjutnya akan dibuktikan bahwa setiap elemen di Z_p^* mempunyai invers yang juga merupakan elemen dari Z_p^*. Perhatikan jika $[a]_p \in Z_p^*$, berarti $p \nmid a$.

Dengan demikian, berdasarkan Teorema Fermat,

$$a^{p-1} \equiv 1 \text{ mod } p$$

Dari definisi kelas $[.]$ didapatkan

$$\left[a^{p-1}\right]_p = [1]_p$$

Karena

$$\left[a^{p-1}\right]_p = [a]_p^{\,p-1}$$

maka

$$[a]_p{}^{p-1} = [1]_p .$$

Sehingga

$$[a]_p{}^{p-2} \bullet [a]_p = [1]_p$$

yang berarti bahwa terdapat invers dari $[a]_p \in Z_p^*$ yaitu $[a]_p{}^{p-2}$. Terbukti bahwa $(Z_p^*, \bullet)$ dengan p bilangan prima merupakan grup komutatif.

Karena $(Z_p, +)$ grup komutatif dan $(Z_p^*, \bullet)$ juga grup komutatif, maka $(Z_p, +, \bullet)$ merupakan suatu lapangan.

Selanjutnya akan diberikan pengertian tentang ideal.

Definisi 2.10

Jika (R,+,●) adalah gelanggang, maka suatu himpunan bagian tak kosong I dari R disebut *ideal* di R jika memenuhi:

i. I membentuk subgrup terhadap operasi $+$ di R.

ii. Untuk setiap $r \in R$ dan $a \in I$, maka $ra \in I$ dan $ar \in I$.

(I. N. Herstein, 1996)

Ideal dapat dibedakan menjadi beberapa jenis berdasarkan elemen-elemen yang ada di ideal tersebut.

Definisi 2.11

- *Ideal unit* I dari gelanggang R adalah ideal yang mengandung semua elemen dari R.
- *Ideal sejati* adalah ideal yang bukan merupakan ideal unit.
- *Ideal nol* adalah ideal yang elemennya hanya {0}.
- *Ideal nontrivial* adalah ideal selain ideal nol dan ideal unit.

(Neal Koblitz, 2004)

Definisi 2.12

Suatu ideal I dari gelanggang R disebut *ideal maksimal* jika dan hanya jika $I \neq R$ dan tidak ada ideal J dari gelanggang R dengan $I \subset J \subset R$.

(I. N. Herstein, 1975)

Definisi 2.13

Suatu ideal I dari gelanggang R disebut *ideal prima* jika dan hanya jika untuk setiap $a,b \in R$ berlaku jika $ab \in I$ maka $a \in I$ atau $b \in I$.

(I. N. Herstein, 1975)

Selanjutnya akan diberikan definisi tentang himpunan pembangun untuk suatu ideal.

Definisi 2.14

Himpunan $A = \{a_1, a_2, ...\} \subseteq I$ disebut *himpunan pembangun* dari suatu ideal I di gelanggang R jika setiap elemen x di I dapat dituliskan sebagai kombinasi linier dari elemen-elemen di A dengan koefisien di R, yaitu $x = \sum_{i=1} ra_i$, dengan $r \in R$.

(Neal Koblitz, 2004)

Ideal dapat juga dibedakan berdasarkan jumlah elemen dari himpunan pembangunnya.

Definisi 2.15

Suatu ideal dikatakan "*dibangun secara hingga*" jika ideal tersebut mempunyai berhingga banyaknya elemen dalam himpunan pembangunnya.

(Neal Koblitz, 2004)

Jika ideal I di gelanggang R dibangun oleh himpunan berhingga elemen-elemen $\{a_1,...,a_n\} \subseteq I$, maka ditulis $I = (a_1,...,a_n)$.

Definisi 2.16

Ideal yang dibangun oleh satu elemen disebut *ideal utama*.

(I. N. Herstein, 1975)

Jika ideal I dari suatu gelanggang R dibangun oleh satu elemen a, maka setiap elemen di I dapat ditulis sebagai kelipatan dari a. Dengan kata lain, $x = ra$ untuk setiap $x \in I$ dengan $r \in R$.

Definisi 2.17

Suatu daerah integral dikatakan *daerah ideal utama* jika semua idealnya adalah ideal utama.

(Neal Koblitz, 2004)

Berikut ini diberikan pengertian tentang polinomial, gelanggang polinomial, serta istilah dan notasi penting yang berkaitan dengan polinomial.

Definisi 2.18

$f(X) = \sum_{i=0}^{n} a_i X^i$, untuk beberapa $a_i \neq 0$ disebut *polinomial*.

Indeks n dengan n bilangan bulat terbesar untuk $a_n \neq 0$ disebut derajat polinomial, dan dinotasikan dengan $\deg(f)$

(I. N. Herstein, 1975)

Definisi 2.19

Jika $\deg f(X) = n$ dan $a_n = 1$, maka $f(X)$ disebut polinomial monik.

(I. N. Herstein, 1996)

Definisi 2.20

Pandang polinomial $f(X) = a_0 + a_1X + ... + a_nX^n$ dengan $\deg(f) = n$, Maka

14. a_n disebut *koefisien utama* dari $f(X)$, dinotasikan dengan $lc(f)$,
15. a_nx^n disebut *suku utama* dari $f(X)$, dinotasikan dengan $lt(f)$,
16. a_0 disebut *suku konstan* dari $f(X)$,

(Jimmie Gilbert, 1996)

Selanjutnya akan diberikan pengertian tentang gelanggang polinomial.

Misalkan R adalah gelanggang, himpunan semua polinomial dalam X atas R dinotasikan dengan $R[X]$. Jika $f(X) \in R[X]$, maka ditulis $f(X) = a_0 + a_1X + ... + a_nX^n$, $n \geq 0$ dengan $a_i \in R$, $i = 0,1,...,n$.

Dalam $R[X]$ dapat didefinisikan operasi penjumlahan dan perkalian polinomial. Misalkan $p(X) = \sum_{i=0}^{n} a_iX^i$, $q(X) = \sum_{i=0}^{m} b_iX^i \in R[X]$, maka operasi penjumlahan dan perkaliannya didefinisikan sebagai berikut:

$+ : p(X) + q(X) = \sum_{i=0}^{\text{maks}(m,n)} c_iX^i$, dengan $c_i = a_i + b_i$, untuk setiap i.

$\bullet : p(X) \bullet q(X) = \sum_{i=0}^{m+n} c_i X^i$, dengan $c_i = a_i b_0 + a_{i-1} b_1 + ... + a_1 b_{i-1} + a_0 b_i$, untuk setiap i.

$R[X]$ dengan operasi penjumlahan dan perkalian ini memenuhi sifat-sifat berikut:

- $(R[X], +)$ membentuk grup komutatif, dengan $0(X) = 0$ sebagai elemen identitas dan $-f(X)$ sebagai invers penjumlahan dari $f(X)$ di $R[X]$.
- $(R[X], \bullet)$ bersifat tertutup dan assosiatif
- $(R[X], +, \bullet)$ memenuhi sifat distributif

Jadi, $R[X]$ membentuk suatu gelanggang yang disebut sebagai gelanggang polinomial.

Untuk F suatu lapangan, maka himpunan polinomial dalam X atas F dinotasikan sebagai $F[X]$, dan elemen-elemen di $F[X]$ berbentuk $f(X) = a_0 + a_1 X + ... + a_n X^n$, $n \geq 0$ dimana $a_i \in F$, $i = 0, 1, ..., n$.

Himpunan $F[X]$ dengan operasi penjumlahan dan perkalian polinomial seperti yang didefinisikan diatas juga membentuk suatu gelanggang.

Selanjutnya akan diberikan definisi tentang gelanggang polinomial dalam m variabel. Misalkan R adalah gelanggang, himpunan semua polinomial dalam m variabel $X = \{X_1,...,X_m\}$ atas R dinotasikan dengan $R[X_1,...,X_m]$. Elemen-elemen di $R[X_1,...,X_m]$ berbentuk $\sum a_{i_1,...,i_m} X_1^{i_1}...X_m^{i_m}$ dengan $a_{i_1,...,i_m} \in R$ dan i_j bilangan bulat nonnegatif.

Dalam $R[X_1,...,X_m]$ juga dapat didefinisikan operasi penjumlahan dan perkalian polinomial. Misalkan $p(x) = \sum_{i=1}^{s} a_{i_1,...,i_m} X_1^{i_1}...X_m^{i_m}$, $q(x) = \sum_{i=1}^{t} b_{i_1,...,i_m} X_1^{i_1}...X_m^{i_m} \in R[X]$, maka operasi penjumlahan dan perkaliannya didefinisikan sebagai berikut:

$+ : p(X) + q(X) = \sum_{i=0}^{\text{maks}(s,t)} c_{i_1,...,i_m} X_1^{i_1}...X_m^{i_m}$, dengan $c_{i_1,...,i_m} = a_{i_1,...,i_m} + b_{i_1,...,i_m}$

$\bullet : p(X) \bullet q(X) = \sum_{j=0}^{s+t} c_{j_1,...,j_m} X_1^{j_1}...X_m^{j_m}$, dengan $c_{j_1,...,j_m} = \sum_{i=1}^{n} a_{i_1,...,i_m} b_{j_1-i_1,...,j_m-i_m}$,

$0 \le i_k \le j_k$, $k = 1,...,m$.

$R[X_1,...,X_m]$ dengan operasi penjumlahan dan perkalian seperti diatas memenuhi sifat-sifat berikut:

- $(R[X_1,...,X_m],+)$ membentuk grup komutatif.

- $\left(R[X_1,...,X_m],\bullet\right)$ bersifat tertutup dan assosiatif
- $\left(R[X_1,...,X_m],+,\bullet\right)$ memenuhi sifat distributif.

Sehingga diperoleh bahwa $R[X_1,...,X_m]$ merupakan suatu gelanggang, dan disebut sebagai gelanggang polinomial dengan m variabel.

Definisi 2.21

- Bentuk $a_{i_1,...,i_m}X_1^{i_1}...X_m^{i_m}$ disebut sebagai *monomial*, dan bentuk monomial tanpa koefisiennya, yaitu $X_1^{i_1}...X_m^{i_m}$, disebut sebagai *power product*.
- Derajat total dari bentuk monomial $a_{i_1,...,i_m}X_1^{i_1}...X_m^{i_m}$ adalah $i_1+...+i_m$.
- Derajat total dari suatu polinomial adalah maksimum derajat total dari monomial yang koefisiennya tidak nol.

(Neal Koblitz, 2004)

Pada polinomial dengan satu variabel penulisan polinomial tersebut bisa dimulai dengan variabel dengan pangkat tertinggi sampai terendah, atau sebaliknya. Akan tetapi untuk polinomial dengan lebih dari satu variabel, diperlukan suatu aturan untuk mengurutkan monomial-monomialnya agar bisa ditentukan koefisien utama dan suku utamanya.

Ada 2 cara pengurutan monomial yang banyak digunakan, yaitu:

1. Pengurutan *lexicographical*

   Secara bahasa, lexicographic berarti pengurutan kata atau huruf seperti pada penyusunan kamus. Misalkan diberikan $f(X,Y,Z)$, maka X disebut sebagai variabel pertama, Y disebut sebagai variabel kedua, dan Z disebut variabel ketiga.

   Pengurutan dilakukan dari monomial yang variabel pertamanya berderajat lebih tinggi. Jika ada monomial yang variabel pertamanya berderajat sama, maka dilihat variabel kedua yang derajatnya lebih tinggi.

   Contoh polinomial dengan pengurutan lexicographical adalah

   $$f(X,Y,Z) = X^3 - X^2Y^2Z + X^2YZ^2 - X^2Z^4 + XY^2 - XZ^3 + Y^3Z^3 + Y^2Z + Z^4$$

   dan suku utama dari f adalah X^3.

2. Pengurutan *lexicographical derajat total*

   Yaitu, monomialnya diurutkan berdasarkan derajat total dari yang terbesar sampai terkecil, dan monomial yang mempunyai derajat total yang sama diurutkan berdasarkan pengurutan lexicographical.

   Untuk polinomial yang diberikan diatas, pengurutan lexicographical derajat totalnya adalah

   $$f(X,Y,Z) = -X^2Z^4 + Y^3Z^3 - X^2Y^2Z + X^2YZ^2 - XZ^3 + Z^4 + X^3 + XY^2 + Y^2Z$$

dan suku utama dari f adalah $-X^2Z^4$.

Untuk pembahasan selanjutnya, pengurutan monomial yang akan digunakan adalah pengurutan lexicographical derajat total.

BAB III

BASIS GRÖBNER

Pada Bab II telah dibahas mengenai himpunan pembangun dari suatu ideal I di gelanggang R. Himpunan pembangun ini disebut juga sebagai basis. Untuk suatu gelanggang polinomial $F[X]$ atau $F[X_1,...,X_m]$, elemen-elemen basis dari idealnya berbentuk polinomial, dimana setiap elemen di ideal tersebut dapat dinyatakan sebagai kombinasi linier dari basisnya dengan koefisien di $F[X]$ atau $F[X_1,...,X_m]$.

Misalkan $I=(f_1,...,f_n)$ adalah ideal di $F[X_1,...,X_m]$ dan diberikan $k \in F[X_1,...,X_m]$, permasalahan yang selalu muncul adalah ketika menentukan apakah k merupakan elemen di I atau tidak. Jika ya, bagaimana merepresentasikan setiap elemen di I ke dalam bentuk $k = g_1 f_1 + g_2 f_2 + ... + g_s f_s$, dimana $g_i \in F[X_1,...,X_m]$. Untuk menjawab pertanyaan tersebut maka digunakan teori Basis Gröbner.

Pada bab ini akan dibahas mengenai basis Gröbner, cara memeriksa suatu basis apakah merupakan basis Gröbner atau bukan, serta pembentukan basis Gröbner dari suatu basis yang bukan Gröbner. Namun sebelum membahas itu semua, perlu diketahui beberapa teori yang

diperlukan untuk pembahasan lebih lanjut mengenai basis Gröbner. Pertama-tama akan dibahas tentang algoritma euclid, gelanggang Noetherian, serta pereduksian suatu polinomial.

3.1 ALGORITMA EUCLID UNTUK POLINOMIAL

Algoritma Euclid untuk polinomial digunakan untuk mencari faktor persekutuan terbesar dari dua buah polinomial $f, g \in F[X]$. Berikut diberikan definisi formal dari faktor persekutuan terbesar dari dua buah polinomial $f, g \in F[X]$.

Definisi 3.1.1

Faktor persekutuan terbesar dari dua buah polinomial $f, g \in F[X]$ adalah polinomial monik dengan derajat tertinggi yang membagi keduanya. Faktor persekutuan terbesar dari $f, g \in F[X]$ dinotasikan dengan $\text{g.c.d.}(f, g)$.

(Neil Koblitz, 2004)

Sebelum membahas pencarian g.c.d dari dua buah polinomial, diperlukan algoritma pembagian untuk kedua polinomial tersebut.

Teorema 3.1.2 (Algoritma Pembagian)

Misalkan $f(x)$, $g(x) \in F[X]$ dengan $g(x) \neq 0$. Maka ada elemen-elemen $q(x)$, $r(x) \in F[X]$ yang unik sedemikian sehingga

$$f(x) = q(x)g(x) + r(x)$$

dengan $r(x) = 0$ atau $\deg r(x) < \deg g(x)$.

(I. N. Herstein, 1996)

Algoritma Euclid adalah suatu algoritma yang merupakan pengulangan algoritma pembagian sampai diperoleh faktor persekutuan terbesar dari dua polinomial. Misalkan $f(x)$, $g(x) \in F[X]$ dengan $g(x) \neq 0$. Untuk mencari $\text{g.c.d.}(f, g)$, digunakan algoritma Euclid dengan langkah-langkah sebagai berikut:

$$
\begin{aligned}
f(x) &= q_0(x)g(x) + r_1(x), && \deg r_1(x) < \deg g(x)\\
g(x) &= q_1(x)r_1(x) + r_2(x), && \deg r_2(x) < \deg r_1(x)\\
r_1(x) &= q_2(x)r_2(x) + r_3(x), && \deg r_3(x) < \deg r_2(x)\\
&\vdots && \vdots\\
r_{n-2}(x) &= q_{n-1}(x)r_{n-1}(x) + r_n(x), && \deg r_n(x) < \deg r_{n-1}(x)
\end{aligned}
$$

$$r_{n-1}(x) = q_n(x)r_n(x)$$

misalkan a adalah koefisien utama dari $r_n(x) \neq 0$, maka $\text{g.c.d.}(f, g)$ adalah $a^{-1}r_n(x)$.

Berikut ini akan diberikan contoh untuk mencari faktor persekutuan terbesar dari dua polinomial yang diberikan.

Contoh 3.1.3:

Pandang $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ dan $g(x) = 3x^3 + 5x^2 + 6x$ di $Z_7[X]$. Untuk mencari $\text{g.c.d.}(f, g)$ dengan menggunakan algoritma Euclid, dilakukan langkah-langkah berikut:

$$
\begin{aligned}
f(x) &= (6x)g(x) + (5x^2 + 4x + 5),\\
g(x) &= (2x + 5)(5x^2 + 4x + 5) + (4x + 3),\\
(5x^2 + 4x + 5) &= (3x + 4)(4x + 3)
\end{aligned}
$$

Jadi, $(4x+3)$ adalah sisa pembagian terakhir yang tidak nol, dan faktor persekutuan terbesar dari $f(x)$ dan $g(x)$ di $Z_7[X]$ adalah

$$d(x) = 4^{-1}(4x+3)$$

$$= 2(4x+3)$$
$$= x+6$$

Selanjutnya $d(x)$ akan diekspresikan dalam bentuk kombinasi linier dari $f(x)$ dan $g(x)$ yaitu

$$d(x) = u(x)f(x) + v(x)g(x)$$

Dengan $u(x)$, $v(x) \in Z_7[X]$.

$$4x+3 = g(x) - (2x+5)(5x^2+4x+5)$$

$$= g(x) - (2x+5)[f(x) - (6x)g(x)]$$
$$= g(x) + g(x)(6x)(2x+5) - f(x)(2x+5)$$
$$= g(x)[1+(6x)(2x+5)] + f(x)(-2x-5)$$
$$= g(x)(5x^2+2x+1) + f(x)(5x+2)$$

Karena $d(x) = 4^{-1}(4x+3) = 2(4x+3)$, maka

$$d(x) = (2)g(x)(5x^2+2x+1) + (2)f(x)(5x+2)$$
$$d(x) = g(x)(3x^2+4x+2) + f(x)(3x+4)$$
$$d(x) = (3x+4)f(x) + (3x^2+4x+2)g(x)$$

Bentuk terakhir adalah ekspresi $\text{g.c.d.}(f, g)$ dalam bentuk kombinasi linier dari $f(x)$ dan $g(x)$.

3.2 GELANGGANG NOETHERIAN

Berikut ini akan didefinisikan suatu gelanggang yang mempunyai sifat tertentu.

Definisi 3.2.1

Suatu gelanggang R disebut gelanggang *Noetherian* jika setiap idealnya dibangun secara hingga.

(Neil Koblitz, 2004)

Dari definisi tersebut, jelas bahwa setiap lapangan dan setiap daerah ideal utama adalah gelanggang Noetherian karena keduanya dibangun oleh satu elemen. Berkaitan dengan definisi diatas, didapatkan teorema berikut.

Teorema 3.2.2

Jika R adalah gelanggang Noetherian, maka gelanggang polinomial dalam satu variabel $R[X]$ juga merupakan gelanggang Noetherian.

(Neil Koblitz, 2004)

Bukti:

Karena R adalah gelanggang, maka berdasarkan pembahasan pada Bab II, $R[X]$ juga merupakan gelanggang. Selanjutnya akan dibuktikan bahwa $R[X]$ adalah gelanggang Noetherian.

Misal I adalah ideal dari $R[X]$. Maka akan ditunjukkan bahwa I dibangun secara hingga.

Untuk $n = 0,1,2,\ldots$ misalkan $J_n \subset R$ adalah himpunan yang mengandung 0 dan semua koefisien utama dari polinomial di I yang berderajat n.

J_n jelas tertutup terhadap operasi penjumlahan karena jika $p, q \in I$ adalah polinomial berderajat n, maka polinomial $p+q$ juga berderajat n dan ada di I. Jadi koefisien utama dari polinomial $p+q$ juga ada di J_n. Jika polinomial berderajat n dikalikan suatu konstanta maka akan dihasilkan juga polinomial berderajat n, sehingga untuk $a \in I$ dan $r \in R$, maka $ar \in I$. Koefisien utama dari ar ada di J_n. Dengan memandang 0 sebagai elemen

identitas terhadap penjumlahan di J_n, dan $-a$ sebagai invers dari a terhadap penjumlahan di J_n, maka J_n adalah ideal dari R.

Untuk setiap elemen $a \in J_n$, terdapat polinomial $f \in I$ berderajat n yang koefisien utamanya adalah a. Karena polinomial $Xf \in I$ berderajat $(n+1)$ juga memiliki koefisien utama yang sama, maka a juga elemen J_{n+1}. Sehingga diperoleh bahwa $J_n \subset J_{n+1}$ untuk $n = 0,1,2,\ldots$.

Bentuk $J = \bigcup_{n=0}^{\infty} J_n$. J adalah ideal di R. Karena setiap ideal di R dibangun secara hingga, berarti J dibangun oleh himpunan hingga elemen r_i yang masing-masing terdapat di suatu J_{n_i}. Jika kita ambil N sebagai maksimum dari n_i, maka seluruh himpunan pembangunnya terkandung di J_N. Dan didapatkan bahwa $J = J_N$ (dengan kata lain, $J_{n+1} = J_N$ untuk $n \geq N$).

Karena diketahui R Noetherian, masing-masing ideal J_n mempunyai berhingga himpunan pembangun $\{r_{n,1},\ldots,r_{n,l_n}\}$ dengan $n = 0,1,\ldots,N$. Gabungan himpunan-himpunan itu membangun J. Untuk setiap $r_{n,i}$ misalkan $f_{n,i}$ adalah polinomial berderajat n di I yang koefisien utamanya adalah $r_{n,i}$. Akan ditunjukkan bahwa gabungan himpunan-himpunan $\{f_{n,i},\ldots,f_{n,l_n}\}$ membangun I dengan $n = 0,1,\ldots,N$.

Untuk melihatnya, misalkan $f \in I$ mempunyai derajat n. $lc(f) \in J_n$ dapat ditulis dalam bentuk $\sum_i a_i r_{n,i}$ untuk $n \leq N$, $a_i \in R$. Jika $n > N$, maka $J_n = J_N$, dan $lc(f)$ bisa dituliskan sebagai kombinasi linier dari $r_{N,i}$. Berarti, polinomial $f - \sum_i a_i f_{n,i}$ (atau $f - \sum_i a_i f_{N,i}$ pada kasus $n > N$) adalah elemen dari I yang berderajat kurang dari n. Nyatakan $f - \sum_i a_i f_{n,i} = \hat{f}$.

Dengan kata lain, f bisa ditulis sebagai kombinasi linier dari $f_{n,i}$ ditambah sebuah polinomial $\hat{f} \in I$ yang berderajat lebih kecil dari f. Jika dilakukan cara yang sama untuk $\hat{f}$, yaitu jika $\hat{f}$ diekspresikan sebagai kombinasi linier dari $f_{n,i}$ ditambah sebuah polinomial di I yang berderajat lebih kecil dari $\hat{f}$ dan proses ini terus dilanjutkan, maka pada akhirnya akan didapatkan suatu ekspresi f dalam bentuk kombinasi linier dari $f_{n,i}$, $n = 0,1...,N$, $i = 1,2,...,l_n$. Jadi terbukti bahwa setiap elemen $f \in I$ dapat dituliskan dalam bentuk kombinasi linier dari $f_{n,i}$, sehingga I dibangun secara hingga. Karena I adalah ideal sembarang di $R[X]$, maka terbukti bahwa $R[X]$ merupakan gelanggang Noetherian.

Akibat 3.2.3

Jika F adalah lapangan, dan $\bar{X} = \{X_1, ..., X_n\}$ adalah himpunan hingga variabel, maka $F\left[\bar{X}\right]$ adalah gelanggang Noetherian.

(Neil Koblitz, 2004)

Bukti:

Pertama-tama akan dibuktikan bahwa F adalah Noetherian. Karena F adalah lapangan, maka ideal di F hanyalah $\{0\}$ dan F itu sendiri. Jelas bahwa $\{0\}$ dibangun secara hingga, dan F dibangun oleh satu elemen. Jadi semua ideal di F dibangun secara hingga. Dengan kata lain, F Noetherian.

Selanjutnya pembuktian bahwa $F\left[\bar{X}\right]$ adalah gelanggang Noetherian akan dilakukan dengan induksi. Berdasarkan Teorema 3.2.2, jika F gelanggang Noetherian maka $F[X_1]$ juga gelanggang Noetherian. Jadi, Akibat 3.2.3 terpenuhi untuk $n = 1$.

Misalkan untuk $n = k$ terpenuhi, yaitu jika F adalah lapangan, maka $F[X_1, ..., X_k]$ adalah gelanggang Noetherian. Akan dibuktikan untuk $k+1$ juga terpenuhi. Dengan kata lain akan dibuktikan bahwa jika F adalah lapangan, maka $F[X_1, ..., X_{k+1}]$ adalah gelanggang Noetherian.

Misalkan $F' = F[X_1,...,X_k]$. F' adalah gelanggang Noetherian. Berdasarkan Teorema 3.2.2, jika F' gelanggang Noetherian, maka $F'[X_{k+1}]$ juga gelanggang Noetherian. $F'[X_{k+1}]$adalah gelanggang polinomial dalam X_{k+1} dengan koefisien di F'. Kemudian karena $F' = F[X_1,...,X_k]$, maka $F'[X_{k+1}] = F[X_1,...,X_k][X_{k+1}] = F[X_1,...,X_{k+1}]$. Didapat bahwa jika $F[X_1,...,X_k]$ adalah gelanggang Noetherian maka $F[X_1,...,X_{k+1}]$ juga gelanggang Noetherian. Sehingga diperoleh jika F adalah lapangan, maka $F[X_1,...,X_{k+1}]$ adalah gelanggang Noetherian. Terbukti bahwa jika F adalah lapangan, maka $F[X_1,...,X_n]$ adalah gelanggang Noetherian.

Akibat 3.2.4

Setiap barisan naik dari ideal $I_1 \subset I_2 \subset \cdots$ di $F[X_1,...,X_m]$ selalu berhingga.

(Neil Koblitz, 2004)

Bukti:

Akan dibuktikan dengan kontradiksi. Andaikan ada barisan naik yang tak hingga dari suatu ideal $I_1 \subset I_2 \subset \cdots$ dalam $F[X_1,...,X_m]$.

Misalkan $I = \bigcup_{i=1}^{\infty} I_i$. Jelas bahwa I juga merupakan ideal di $F[X_1,...,X_m]$. Berdasarkan Akibat 3.2.3 yang menyatakan bahwa $F[X_1,...,X_m]$ gelanggang Noetherian, maka I dibangun oleh berhingga elemen yang masing-masingnya adalah elemen dari suatu I_i. Misalkan n adalah maksimum dari i, maka $I = I_n$, dan tidak bisa ditemukan ideal I_{n+1} yang lebih besar dari I. Hal ini kontradiksi dengan pemisalan awal. Terbukti bahwa setiap barisan naik dari ideal $I_1 \subset I_2 \subset \cdots$ selalu berhingga.

3.3 PEREDUKSIAN POLINOMIAL

Misalkan $f, g \in F[\overline{X}]$ dan $lt(g)$ membagi $lt(f)$. Dalam kasus ini, $lt(f)$ dapat dihilangkan dengan cara mengurangkan f dengan kelipatan dari g. Secara umum, setiap suku dari f yang dapat dibagi oleh $lt(g)$ dapat diganti dengan suku yang lebih kecil dengan cara yang sama. Hal ini berdasarkan definisi berikut.

Definisi 3.3.1

Misalkan $f, g \in F[\overline{X}]$. f dikatakan *tereduksi ke* h *modulo* g (atau f *tereduksi modulo* g *ke* h) dalam satu langkah jika $a_i X^i$ adalah suku dari f yang dapat dibagi oleh $lt(g)$, dan

$$h = f - \frac{a_i X^i}{lt(g)} g$$

Dapat dituliskan sebagai

$$f \xrightarrow{g} h$$

Jika $lt(f)$ dapat dibagi oleh $lt(g)$ maka berlaku

$$h = f - \frac{lt(f)}{lt(g)} g$$

dan $lt(h)$ kurang dari $lt(f)$.

(Neil Koblitz, 2004)

Contoh 3.3.2:

Misal $f(X,Y,Z) = -X^2Z^4 + Y^3Z^3 - X^2Y^2Z + X^2YZ^2 - XZ^3 + Z^4 + X^3 + XY^2 + Y^2Z$ $\in F[X,Y,Z]$, dimana F menyatakan lapangan Z_3. Dan misal $g_1(X,Y,Z) = XZ^3 - Y^2Z^2$, Maka f tereduksi ke

$$h_1 = f - \frac{lt(f)}{lt(g_1)} g_1$$

$$= f - \frac{-X^2Z^4}{XZ^3} XZ^3 - Y^2Z^2$$

$$= f + XZ\left(XZ^3 - Y^2Z^2\right)$$

$$h_1 = XY^2Z^3 + Y^3Z^3 - X^2Y^2Z + X^2YZ^2 - XZ^3 + Z^4 + X^3 + XY^2 + Y^2Z$$

modulo g_1 dalam satu langkah. Dengan cara yang sama, Proses reduksi dapat dilanjutkan karena $lt(g_1)$ membagi $lt(h_1)$. Kemudian didapatkan bahwa h_1 tereduksi ke

$$h_2(X,Y,Z) = -Y^4Z^2 + Y^3Z^3 - X^2Y^2Z + X^2YZ^2 - XZ^3 + Z^4 + X^3 + XY^2 + Y^2Z$$

modulo g_1. Jadi, f tereduksi ke h_2 modulo g_1 dalam dua langkah.

Definisi 3.3.3

Misal $G = \{g_1,...,g_l\} \subset F[X_1,...,X_m]$, dan $f \in F[X_1,...,X_m]$. Maka f dikatakan *tereduksi ke* h *modulo* himpunan G jika terdapat barisan dari polinomial yang dimulai dengan $h_0 = f$ dan berakhir dengan $h_k = h$ sedemikian sehingga h_j tereduksi ke h_{j+1} modulo suatu $g \in G$ dalam satu langkah, $j = 0,1,...,k-1$

(Neil Koblitz, 2004)

Contoh 3.3.4:

Misal $G=\{g_1,g_2\}$ dimana $g_1=XZ^3-Y^2Z^2$ dan $g_2=Y^2Z-YZ^2$, dan juga misalkan f adalah polinomial pada Contoh 3.3.2. Melanjutkan Contoh 3.3.2, didapat bahwa h_2 tereduksi modulo g_2 ke

$$h_3=h_2-\frac{lt(h_2)}{lt(g_2)}g_2$$

$$=h_2-\frac{-Y^4Z^2}{Y^2Z}Y^2Z-YZ^2$$

$$=h_2+Y^2Z\left(Y^2Z-YZ^2\right)$$

$$h_3=-X^2Y^2Z+X^2YZ^2-XZ^3+Z^4+X^3+XY^2+Y^2Z$$

Dan dengan cara yang sama, h_3 tereduksi modulo g_2 ke

$$h_4(X,Y,Z)=-XZ^3+Z^4+X^3+XY^2+Y^2Z$$

Berikutnya, h_4 tereduksi modulo g_1 ke

$$h_5(X,Y,Z)=-Y^2Z^2+Z^4+X^3+XY^2+Y^2Z$$

Dan h_5 tereduksi modulo g_2 ke

$$h_6(X,Y,Z) = -YZ^3 + Z^4 + X^3 + XY^2 + Y^2Z$$

Dapat dilihat bahwa $lt(h_6)$ tidak dapat dibagi oleh $lt(g_1)$ atau $lt(g_2)$, sehingga $lt(h_6)$ tidak bisa diganti dengan suku yang lebih kecil. Tetapi dapat dilakukan satu langkah reduksi lagi karena $lt(g_2)$ membagi suku terakhir dari h_6, dan menghasilkan

$$h(X,Y,Z) = h_7(X,Y,Z) = -YZ^3 + Z^4 + X^3 + XY^2 + YZ^2$$

Jadi, f tereduksi ke $h = h_7$ modulo G, karena

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_1} h_2 \xrightarrow{g_2} h_3 \xrightarrow{g_2} h_4 \xrightarrow{g_1} h_5 \xrightarrow{g_2} h_6 \xrightarrow{g_2} h .$$

Pada contoh ini, jika kita lebih memilih untuk mereduksi h_1 modulo g_2 (daripada g_1), kemudian mereduksi hasilnya (dinotasikan dengan h_2') modulo g_1 dan melanjutkan seperti contoh diatas, maka akan diperoleh polinomial h yang sama. Yakni, akan diperoleh barisan langkah reduksi berikut:

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2' \xrightarrow{g_1} h_3 \xrightarrow{g_2} h_4 \xrightarrow{g_1} h_5 \xrightarrow{g_2} h_6 \xrightarrow{g_2} h$$

Pada kenyataannya, saat mereduksi $f \in F[\bar{X}]$ modulo $G = \{g_1, ..., g_l\}$, kadang akan menghasilkan perbedaan besar jika g_i yang diambil berbeda. Hal ini dapat dilihat pada contoh berikut:

Contoh 3.3.5:

Misal $f(X,Y,Z) = X^2Y^2 + XY \in F[X,Y,Z]$, dimana F menyatakan lapangan Z_3. Dan misal $G = \{g_1, g_2, g_3\}$, dimana $g_1(X,Y,Z) = Y^2 + Z^2$, $g_2(X,Y,Z) = X^2Y + YZ$, dan $g_3(X,Y,Z) = Z^3 + XY$. Jika f direduksi modulo g_1 kita dapatkan $-X^2Z^2 + XY$ yang tidak dapat direduksi lebih lanjut karena tak satu pun dari sukunya yang dapat dibagi oleh $lt(g_1)$, $lt(g_2)$, ataupun $lt(g_3)$. Akan tetapi, jika pada tahap awal f direduksi modulo g_2 kita dapatkan $-Y^2Z + XY$ yang kemudian bisa direduksi modulo g_1 dan mendapatkan $Z^3 + XY$. Pada akhirnya, hasil terakhir dapat direduksi modulo g_3 dan menghasilkan 0.

3.4 BASIS GRÖBNER

Berdasarkan Contoh 3.3.5 pada Subbab 3.3, dapat diambil kesimpulan bahwa himpunan $G=\{g_1,g_2,g_3\}$ bukan pilihan yang baik sebagai basis untuk ideal yang dibangun oleh g_1,g_2,g_3. Berikut ini akan diberikan definisi yang memberikan suatu gagasan dasar dalam perhitungan aljabar agar diperoleh pilihan yang baik untuk basis ideal pada suatu gelanggang polinomial.

Definisi 3.4.1

Misalkan $G=\{g_1,...,g_s\}\subset F\left[\bar{X}\right]$ dengan $\bar{X}=\{X_1,...,X_m\}$. Dan misalkan I ideal di $F\left[\bar{X}\right]$ yang dibangun oleh G. G disebut *basis Gröbner* untuk ideal I jika setiap $f\in I$, $f\neq 0$, terdapat paling sedikit satu g_i sedemikian sehingga $lt(g_i)$ membagi $lt(f)$.

(Neil Koblitz, 2004)

Berkaitan dengan Definisi 3.4.1, maka didapatkan teorema sebagai berikut.

Teorema 3.4.2

Misalkan $G=\{g_1,...,g_s\}\subset F\left[\bar{X}\right]$ dengan $\bar{X}=\{X_1,...,X_m\}$. Dan misalkan I ideal di $F\left[\bar{X}\right]$ yang dibangun oleh G. G adalah basis Gröbner untuk I jika dan hanya jika setiap $f\in I$ tereduksi ke 0 modulo G.

(Neil Koblitz, 2004)

Bukti:

$(\rightarrow)$

Misalkan G basis Gröbner dan $f\in I$. Akan dibuktikan bahwa setiap $f\in I$ tereduksi ke 0 modulo G. Karena $lt(f)$ dapat dibagi oleh $lt(g_{i_1})$ untuk suatu i_1, maka f dapat direduksi modulo g_{i_1} untuk mendapatkan h_1. Jelas bahwa $h_1\in I$, dan $lt(h_1)$ kurang dari $lt(f)$. Kemudian proses ini dapat dilanjutkan dengan mereduksi h_1 modulo g_{i_2} untuk mendapatkan h_2. Karena dalam setiap proses menghasilkan suatu polinomial yang suku utamanya lebih kecil, maka akan diperoleh 0 pada akhir reduksi.

$(\leftarrow)$

Pembuktian sebaliknya dilakukan dengan kontraposisi. Jika G bukan basis Gröbner, maka ada suatu $f\in I$ sedemikian sehingga $lt(f)$ tidak dapat

dibagi oleh $lt(g_i)$ untuk suatu i. Jadi, f tidak dapat direduksi modulo G ke suatu h yang suku utamanya lebih kecil, sehingga tidak akan mendapatkan 0 di akhir reduksi.

Terbukti bahwa G adalah basis Gröbner untuk I jika dan hanya jika setiap $f \in I$ tereduksi ke 0 modulo G.

Jika suatu basis Gröbner untuk ideal I diperoleh, maka akan lebih mudah untuk mengekspresikan setiap elemen di I sebagai kombinasi linier dari basisnya. Hal itu bisa diperoleh dengan membalikkan proses pereduksian polinomial $p \in I$, dan akhirnya akan didapat kombinasi linier yang mewakili p. Selain itu, jika diberikan sembarang elemen $f \in F\left[\overline{X}\right]$, maka Teorema 3.4.2 dapat digunakan untuk menentukan apakah f ada di I atau tidak. Jika f tereduksi ke 0, maka $f \in I$. Dan jika f tidak tereduksi ke 0, maka $f \notin I$.

Selanjutnya, jika diberikan ideal lain I', dapat diperiksa apakah $I' \subset I$ atau tidak. $I' \subset I$ jika dan hanya jika masing-masing elemen pembangun dari I' ada di I. Lebih jauh lagi, jika kita punya basis Gröbner untuk masing-masing I dan I', maka dapat ditentukan apakah $I' = I$ atau tidak. Persamaan akan didapatkan jika dan hanya jika masing-masing elemen dalam satu basis akan tereduksi ke 0 modulo polinomial di basis lainnya.

Pada kenyataannya, elemen di I tak berhingga banyaknya, sehingga untuk memeriksa suatu basis tidak mungkin dengan cara memeriksa semua elemen $f \in I$ satu persatu berdasarkan Definisi 3.4.1 ataupun Teorema 3.4.2. Dalam teorema berikutnya, untuk memeriksa basis dari I tidak perlu diperiksa setiap elemen $f \in I$. Sebelum itu, akan diberikan definisi mengenai *S-polinomial* dari dua buah polinomial.

Definisi 3.4.3

S-polinomial dari dua polinomial tak kosong $f, g \in F[X_1, ..., X_m]$ (dinotasikan dengan $S(f,g)$) didefinisikan sebagai berikut:

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

dimana L adalah kelipatan persekutuan terkecil dari $lt(f)$ dan $lt(g)$, yaitu monomial dengan derajat total terkecil yang dapat dibagi oleh $lt(f)$ dan $lt(g)$.

(Neil Koblitz, 2004)

Contoh 3.4.4 :

Pada Contoh 3.3.4 dimana $g_1 = XZ^3 - Y^2Z^2$ dan $g_2 = Y^2Z - YZ^2$, diperoleh $L = XY^2Z^3$, dan

$$S(g_1, g_2) = \frac{XY^2Z^3}{XZ^3}(XZ^3 - Y^2Z^2) - \frac{XY^2Z^3}{Y^2Z}(Y^2Z - YZ^2)$$

$$= XYZ^4 - Y^4Z^2$$

Berkaitan dengan definisi diatas, maka diberikan teorema sebagai berikut.

Teorema 3.4.5

Misalkan $G = \{g_1, ..., g_s\} \subset F\left[\bar{X}\right]$ dengan $\bar{X} = \{X_1, ..., X_m\}$. Dan misalkan I ideal di $F\left[\bar{X}\right]$ yang dibangun oleh G. G adalah basis Gröbner untuk I jika dan hanya jika $S(g_i, g_j)$ tereduksi ke 0 modulo G untuk setiap $g_i, g_j \in G$.

(Neil Koblitz, 2004)

Bukti:

$(\rightarrow)$

Misalkan G basis Gröbner untuk I. Berdasarkan definisi ideal, jelas bahwa $S(g_i, g_j) \in I$. Dan berdasarkan teorema 3.4.2, $S(g_i, g_j)$ tereduksi ke 0 modulo G untuk setiap $g_i, g_j \in G$.

$(\leftarrow)$

Misalkan $S(g_i, g_j)$ tereduksi ke 0 modulo G untuk setiap $g_i, g_j \in G$. Berdasarkan definisi 3.4.1, cukup ditunjukkan bahwa untuk setiap $f \in I$, maka terdapat $lt(g_i)$ yang membagi $lt(f)$ untuk suatu i.

Tanpa menghilangkan hal yang berlaku umum, dapat dimisalkan bahwa semua g_i monik karena kedua hipotesis dan kesimpulan pada teorema tersebut tidak berpengaruh jika masing-masing g_i diganti dengan polinomial yang diperoleh dengan mengalikan masing-masing g_i dengan invers dari koefisien utamanya.

Karena $f \in I$, maka f dapat ditulis dalam bentuk $f = \sum_{i=1}^{l} h_i g_i$. Misalkan X^{r} adalah power product terbesar dari masing-masing $h_i g_i$, $i = 1, ..., l$. X^{r} kemungkinan bisa lebih besar dari $lt(f)$ karena X^{r} dapat dihilangkan ketika menjumlahkan semua $h_i g_i$. Misalkan kita telah memilih cara sedemikian sehingga X^{r} minimal.

Jika X^{r} adalah power product di $lt(f)$, maka $lt(g_i)$ membagi $lt(f)$ untuk suatu i, dan pembuktian selesai. Sekarang misalkan bahwa power product di $lt(f)$ kurang dari X^{r}. Untuk membuktikan teorema ini, cukup dibuktikan ada cara untuk menuliskan f dalam bentuk $\sum_{i=1}^{l} h_i' g_i$ dengan semua suku di $h_i' g_i$ lebih kecil dari X^{r}, karena hal itu akan kontradiksi dengan minimalitas dari X^{r}.

Misalkan $h_i g_i$ mempunyai power product X^{r} di suku utamanya. Tanpa menghilangkan hal yang berlaku umum, misalkan bahwa hasil l' pertama pada penjumlahan $f = \sum_{i=1}^{l} h_i g_i$ adalah jumlah $h_i g_i$ yang mengandung X^{r} dalam suku utamanya. Untuk $i = 1,...,l'$, misalkan $h_i = c_i X^{\mathrm{r}_i} + \tilde{h}_i$, dimana $\tilde{h}_i$ adalah polinomial yang lebih kecil dari X^{r_i}. Perhatikan bahwa untuk $i = 1,...,l'$, maka $X^{\mathrm{r}} = X^{\mathrm{r}_i} lt(g_i)$. Untuk $i = 1,...,l'-1$, misalkan X^{s_i} adalah kelipatan persekutuan terkecil dari $lt(g_i)$ dan $lt(g_{i+1})$, dan misalkan juga bahwa $X^{\mathrm{t}_i} = X^{\mathrm{r}-\mathrm{s}_i}$. Pandang penjumlahan berikut,

$$c_1 X^{\mathrm{t}_1} S(g_1, g_2) + (c_1 + c_2) X^{\mathrm{t}_2} S(g_2, g_3)$$

$$+ (c_1 + c_2 + c_3) X^{\mathrm{t}_3} S(g_3, g_4) + \ldots \qquad (1)$$

$$\ldots + (c_1 + c_2 + \ldots + c_{l'-1}) X^{\mathrm{t}_{l'-1}} S(g_{l'-1}, g_l)$$

Jumlah ini sama dengan

$$c_1\left(\frac{X^{\mathrm{r}}}{lt(g_1)}g_1-\frac{X^{\mathrm{r}}}{lt(g_2)}g_2\right)+(c_1+c_2)\left(\frac{X^{\mathrm{r}}}{lt(g_2)}g_2-\frac{X^{\mathrm{r}}}{lt(g_3)}g_3\right)$$

$$+(c_1+c_2+c_3)\left(\frac{X^{\mathrm{r}}}{lt(g_3)}g_3-\frac{X^{\mathrm{r}}}{lt(g_4)}g_4\right)+\ldots$$

(2)

$$\ldots+(c_1+c_2+\ldots+c_{l'-1})\left(\frac{X^{\mathrm{r}}}{lt(g_{l'-1})}g_{l'-1}-\frac{X^{\mathrm{r}}}{lt(g_{l'})}g_{l'}\right)$$

$$+(c_1+c_2+\ldots+c_{l'-1}+c_{l'})\frac{X^{\mathrm{r}}}{lt(g_{l'})}g_{l'},$$

karena koefisien $c_1+c_2+\ldots+c_{l'-1}+c_{l'}$ adalah 0.

Di satu sisi, penjumlahan pada (2) sama dengan

$$c_1X^{\mathrm{r}_1}g_1+c_2X^{\mathrm{r}_2}g_2+\ldots+c_{l'}X^{\mathrm{r}_{l'}}g_{l'} \qquad (3)$$

Di sisi lain, penjumlahan pada (2) sama dengan penjumlahan pada (1). Karena diketahui masing-masing S-polinomial pada (1) dapat direduksi ke 0 modulo F dan suku utama $X^{\mathrm{t}_1}S(g_i,g_{i+1})$ kurang dari X^{r}, proses mereduksi $S(g_i,g_{i+1})$ ke 0 akan menghasilkan sebuah ekspresi $X^{\mathrm{t}_1}S(g_i,g_{i+1})$ dalam bentuk $\sum_{j=1}^{l}h_{ij}g_j$, dimana $lt(h_{ij}g_j)<X^{\mathrm{r}}$ untuk setiap i,j. Jadi, penjumlahan pada (3) dapat diekspresikan dalam bentuk

$$f = \sum_{i=1}^{l} h_i g_i = \sum_{i=1}^{l'} (c_i X^{r_i} + \tilde{h}_i) g_i + \sum_{i=l'+1}^{l} h_i g_i$$

$$= \sum_{i=1}^{l'} (h_i'' + \tilde{h}_i) g_i + \sum_{i=l'+1}^{l} (h_i'' + h_i) g_i = \sum_{i=1}^{l} h_i' g_i ,$$

dimana $h_i' = h_i'' + \tilde{h}_i$ untuk $i = 1, \ldots, l'$, dan $h_i' = h_i'' + h_i$ untuk $i = l'+1, \ldots, l$. Jadi semua power product pada $h_i' g_i$ kurang dari X^r sehingga terbukti bahwa terdapat $lt(g_i)$ yang membagi $lt(f)$ untuk suatu i. Terbukti bahwa G adalah basis Gröbner untuk I jika dan hanya jika $S(g_i, g_j)$ tereduksi ke 0 modulo G untuk setiap $g_i, g_j \in G$.

Selanjutnya akan diberikan contoh yang merepresentasikan Teorema 3.4.5.

Contoh 3.4.6 :

Misal $G = \{g_1, g_2\}$ dimana $g_1 = XZ^3 - Y^2Z^2$ dan $g_2 = Y^2Z - YZ^2$, maka:

$S(g_1, g_2) = XYZ^4 - Y^4Z^2$ terreduksi ke $-Y^4Z^2 + Y^3Z^3$ modulo g_1 dalam satu langkah, dan $-Y^4Z^2 + Y^3Z^3$ terreduksi ke 0 modulo g_2 dalam satu langkah. Jadi G adalah basis Gröbner.

Contoh 3.4.7 :

Misal $G=\{g_1,g_2,g_3\}$, dimana $g_1(X,Y,Z)=Y^2+Z^2$, $g_2(X,Y,Z)=X^2Y+YZ$, dan $g_3(X,Y,Z)=Z^3+XY$. Diperoleh $S(g_1,g_2)$ tidak dapat tereduksi ke 0 modulo G. Jadi G bukan basis Gröbner.

Teorema berikut ini merupakan algoritma untuk memperoleh suatu basis Gröbner dari suatu basis sembarang untuk ideal I.

Teorema 3.4.8

Pandang $I \subset F[X_1,...,X_m]$ adalah ideal yang dibangun oleh $G'=\{g_1,...,g_{l'}\}$. Dan misalkan juga bahwa untuk setiap $1 \le i < j \le l'$ maka $S(g_i,g_j)$ direduksi modulo G' sampai diperoleh polinomial $h_{i,j}$ berupa 0 atau polinomial yang suku utamanya tidak bisa direduksi modulo G'. Dalam kasus yang terakhir, $h_{i,j}$ ditambahkan ke himpunan G'. Dengan melanjutkan cara ini, yaitu menambah $g_{l'+1}, g_{l'+2}, \cdots$ ke himpunan G' sampai didapatkan himpunan $G=\{g_1,...,g_l\}$ sedemikian sehingga $S(g_i,g_j)$ tereduksi ke 0

modulo G untuk setiap $1 \le i < j \le l$. Algoritma ini berakhir dalam berhingga langkah, dan menghasilkan basis Gröbner untuk I.

(Neil Koblitz, 2004)

Bukti:

Untuk setiap j dengan $l' \le j \le l$, dimisalkan J_j adalah ideal yang dibangun oleh $lt(g_1), lt(g_2), ..., lt(g_j)$. Karena $lt(g_j)$ tidak dapat dibagi oleh $lt(g_1)$, $lt(g_2)$, ..., $lt(g_j)$ untuk $j > l'$, maka ideal

$$J_{l'} \subset J_{l'+1} \subset J_{l'+2} \subset ...$$

membentuk barisan naik.

Berdasarkan Akibat 3.2.4, maka banyaknya ideal adalah berhingga, sehingga banyaknya g_j juga berhingga. Jadi algoritma berakhir dalam berhingga langkah. Berdasarkan Teorema 3.4.4, himpunan G yang dihasilkan adalah basis Gröbner.

Contoh 3.4.9 :

Pada Contoh 3.4.7 didapat bahwa himpunan $G' = \{g_1, g_2, g_3\}$ dimana $g_1(X,Y,Z) = Y^2 + Z^2$, $g_2(X,Y,Z) = X^2Y + YZ$, dan $g_3(X,Y,Z) = Z^3 + XY$, bukan basis Gröbner untuk ideal I yang dibangun olehnya, karena

$S(g_1, g_2) = X^2Z^2 - Y^2Z$ tidak bisa direduksi ke 0 modulo G'. Untuk membentuk basis Gröbner dari G', misalkan $g_4 = S(g_1, g_2)$ dan $G = \{g_1, g_2, g_3, g_4\}$. Dapat dengan mudah diperiksa bahwa semua polinomial berikut :

$S(g_1, g_2) = g_4 = X^2Z^2 - Y^2Z$, $S(g_1, g_3) = Z^5 - XY^3$, $S(g_1, g_4) = X^2Z^4 - Y^4Z$, $S(g_2, g_3) = -X^3Y^2 + YZ^4$, $S(g_2, g_4) = Y^3Z + YZ^3$, dan $S(g_3, g_4) = X^3Y + Y^2Z^2$ tereduksi ke 0 modulo G. Jadi, G adalah basis Gröbner untuk I.

BAB IV

PENUTUP

4.1 KESIMPULAN

Misalkan diberikan suatu $I = (g_1, ..., g_{l'})$. Untuk memeriksa $G' = \{g_1, ..., g_{l'}\}$ adalah basis Gröbner atau bukan, dilakukan dengan mencari $S(g_i, g_j)$ untuk setiap $g_i, g_j \in G'$, $1 \le i < j \le l'$. Jika $S(g_i, g_j)$ tereduksi ke 0 modulo G' untuk setiap $g_i, g_j \in G'$, maka G' adalah basis Gröbner untuk I. Jika ada $S(g_i, g_j)$ yang tidak dapat tereduksi ke 0 untuk suatu $g_i, g_j \in G'$, maka G' bukan basis Gröbner untuk I.

Jika $G' = \{g_1, ..., g_{l'}\}$ bukan basis Gröbner untuk I, dapat dibentuk basis Gröbner untuk I dari G' dengan langkah sebagai berikut:

$S(g_i, g_j)$ direduksi modulo G' untuk setiap $g_i, g_j \in G'$, sampai diperoleh 0 atau polinomial h_{ij} pada akhir reduksi. Kemudian h_{ij} dimasukkan ke himpunan G'. Dengan melanjutkan cara ini, yaitu menambah $g_{l'+1}, g_{l'+2}, \cdots$ ke himpunan G' sampai didapatkan himpunan $G = \{g_1, ..., g_l\}$ sedemikian

sehingga $S(g_i, g_j)$ tereduksi ke 0 modulo G untuk setiap $1 \le i < j \le l$.

Himpunan $G = \{g_1, ..., g_l\}$ yang dihasilkan adalah basis Gröbner untuk I.

4.2 SARAN

Dalam tugas akhir ini telah dibahas cara memeriksa suatu basis adalah basis Gröbner atau bukan, serta cara membentuk basis Gröbner. Berdasarkan teori yang ada dalam tugas akhir ini, diharapkan selanjutnya dapat dibentuk basis lain untuk suatu ideal yang dapat diterapkan dalam berbagai aplikasi.

DAFTAR PUSTAKA

Heirstein, I.N. 1975. *Topics in Algebra*, 2nd *edition*. John Wiley&Sons., New York: 120-159.

Herstein, I.N. 1996. *Abstract Algebra*, 3nd *edition*. Prentice-Hall Inc., New Jersey: 40-223.

Koblitz, neil. 1997. *Algebraic Aspects of Cryptography*, *volume* 3. Springer-Verlag, Berlin: 53-60.

Gilbert, Jimmie, G. Linda. 1996. *Elements of Modern Algebra*, 4th *edition*. PWS Publishing Company.

Ajwa, I.A, Z. Liu, P.S. Wang. 2003. *Gröbner Basis Algorithm*. Kent State Uneversity, U.S.A.

http://www.cut-the-knot.org/blue/Modulo.shtml, Oktober 2009.