



**CİSİM VE BAZI MODÜLLER ÜZERİNDE
GRÖBNER TABAN İNCELEMESİ**

Mehmet ARVAS

Yüksek Lisans Tezi

Matematik Anabilim Dalı

Dr. Öğr. Üyesi Abdullah ÇAĞMAN

AĞRI-2019

(Her Hakkı Saklıdır.)

T.C.
AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

Mehmet ARVAS

CİSİM VE BAZI MODÜLLER ÜZERİNDE
GRÖBNER TABAN İNCELEMESİ
YÜKSEK LİSANS TEZİ

TEZ YÖNETİCİSİ
Dr. Öğr. Üyesi Abdullah ÇAĞMAN

AĞRI-2019

ÖZET
YÜKSEK LİSANS TEZİ
CİSİM VE BAZI MODÜLLER ÜZERİNDE
GRÖBNER TABAN İNCELEMESİ

Tez Danışmanı: Dr. Öğr. Üyesi Abdullah ÇAĞMAN

2019, 60 sayfa

Jüri: Dr. Öğr. Üyesi Sait TAŞ

Dr. Öğr. Üyesi Abdullah ÇAĞMAN

Doç. Dr. Ahmet Ocak AKDEMİR

Bu tezde Gröbner tabanları incelenerek modüllerde Gröbner tabanı yardımıyla polinom indirgemesinin nasıl yapılacağı hakkında bilgi verilmiştir. Tezin ilk bölümünde giriş yapılmış ve ikinci bölümünde cisimler üzerinde tek değişkenli ve çok değişkenli polinomların indirgemesi, terim sıralamaları ve bölme algoritması üzerinde durulmuştur. Üçüncü bölüm Gröbner taban tanımı, S-Polinomları, Buchberger Algoritması ve İndirgenmiş Gröbner tabanlarına ayrılmıştır. Son olarak dördüncü bölümünde Modül teori hakkında bazı bilgiler verilerek Modüllerde Gröbner tabanları incelenmiştir.

2019, 60 sayfa

Anahtar Kelimeler: Polinom Halkası, İdeal, Gröbner Taban, Modül.

ABSTRACT
MASTER’S THESIS
GROBNER BASIS EXAMINATION ON
FIELDS AND SOME MODULES

Advisor Of Thesis: Assist. Prof. Dr. Abbdullah ÇAĞMAN

2019, 60 Pages

Jury : Assist. Prof. Dr. Sait TAŞ

Assist. Prof. Dr. Abdullah ÇAĞMAN

Assoc. Prof. Dr. Ahmet Ocak AKDEMİR

In this thesis, Gröbner bases were examined and some information was given about how to make polynomial reduction by using Gröbner basis in modules. In the first part of the thesis, introduction was made and reduction of univariate and multivariate polynomials, term ordering and division algorithm over fields are emphasized in the second section. The third section is attributed to the Gröbner basis definition, S-Polynomials, Buchberger Algorithm and Reduced Gröbner bases. Finally, in the fourth chapter, some information about Module theory is given and Gröbner bases in Modules are discussed.

2019, 60 Pages

Key Words: Polynomial Ring, Ideal, Gröbner Basis, Module.

TEŞEKKÜR

Bu tez çalışması Ağrı İbrahim Çeçen Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında hazırlanmıştır.

Yüksek lisans eğitimim boyunca, benden bilgi ve deneyimlerini esirgemeyen, çalışmalarımın tamamlanabilmesi için her türlü şartı sağlayan ve bana her zaman her türlü desteği sunan çok değerli danışman hocam Sayın Dr. Öğr. Üyesi Abdullah ÇAĞMAN' a teşekkürlerimi sunarım.

Öğrenim hayatım boyunca kendilerinden görmüş olduğum maddi ve manevi destek den dolayı aileme ve her zaman her türlü desteği ile yanımda olan sevgili eşim Saime ARVAS' a teşekkürlerimi sunarım.

04/07/2019

Mehmet ARVAS

İÇİNDEKİLER

ÖZET.....	ii
ABSTRACT.....	iii
TEŞEKKÜR.....	iv
SİMGELER ve KISALTMALAR DİZİNİ.....	vi
1. GİRİŞ.....	1
2. KURAMSAL TEMELLER.....	3
2.1. Temel Tanım ve Teoremler.....	3
2.2. Tek Değişkenli Polinomlar İçin İndirgenme.....	8
2.3. Çok Değişkenli Doğrusal Polinomlar İçin İndirgenme.....	15
2.4. Terim Sıralamaları.....	16
2.5. Bölme Algoritması ile Polinomların İndirgenmesi.....	17
3. MATERYAL VE YÖNTEM.....	24
3.1. Gröbner Tabanları.....	24
3.2. S-Polinomları ve Buchberger Algoritması.....	28
3.3. İndirgenmiş Gröbner Tabanlar.....	35
4. ARAŞTIRMA BULGULAR.....	37
4.1. Modüller.....	37
4.2. Modüller İçin Gröbner Tabanları.....	40
4.3. Modüller İçin Gröbner Tabanların Basit Uygulamaları.....	52
5. SONUÇLAR.....	58
KAYNAKLAR.....	59
ÖZGEÇMİŞ.....	60

SİMGELER ve KISALTMALAR DİZİNİ

$<$	Küçüktür
$>$	Büyüktür
$\leq$	Küçük veya Eşittir
$\geq$	Büyük veya Eşittir
$\subset$	Alt Küme
$\subseteq$	Alt Kümesi veya Eşit
$\not\subseteq$	Alt Küme ve Eşit Değil
$\cong$	Yaklaşık Olarak Eşit
$\ni$	Eleman Olarak Kapsar
$\mathbb{Z}^+$	Pozitif Tamsayılar Kümesi
$\cup$	Birleşim
$\cap$	Kesişim
$\in$	Elemanıdır
$\notin$	Elemanı Değildir
$\mathbb{N}$	Doğal Sayılar Kümesi
$\mathbb{R}$	Reel Sayılar Kümesi
max	Maksimum
Σ	Toplam Sembolü
$\mathbb{Q}$	Rasyonel Sayılar Kümesi
$\emptyset$	Boş Küme
$\forall$	Her
$\exists$	En az bir
$=$	Eşit
$\neq$	Eşit Değil
gcd	En Büyük Ortak Bölen
lcm	En Küçük Ortak Kat
∞	Sonsuz

1. GİRİŞ

Gröbner tabanları teorik olarak 1899 yılında Gordan, daha sonra 1964 yılında Hironaka tarafından kullanılmıştır. Fakat Gröbner tabanlarının gerçek önemi, hesaplanabilmeleri gerçeğidir. Bu bağlamda 1965 yılında Bruno Buchberger tarafından Gröbner tabanlarının hesaplanmasını sağlayan bir algoritma geliştirildi.

F bir cisim olmak üzere $F[x_1, x_2, \dots, x_n]$ polinom halkasında bir ideal için tanımlanan Gröbner tabanı ile birlikte bu idealin üreteç kümesi daha basit hale getirildi. $F[x_1, x_2, \dots, x_n]$ polinom halkasının bir idealinin Gröbner tabanını elde etmek için $F[x_1, x_2, \dots, x_n]$ üzerinde bir terim sıralaması ve bir bölme algoritmasına ihtiyaç vardır. Terim sıralaması yardımıyla indirgenme işlemi ifade edilerek, çok değişkenli polinom halkalarında bölme algoritması oluşturulmuştur. $I, F[x_1, x_2, \dots, x_n]$ polinom halkasının bir ideali ve $G = \{g_1, g_2, \dots, g_t\}$ sıfırdan farklı polinomların bir kümesi olmak üzere $G \subseteq I$ olsun. Her $f \in I - \{0\}$ için $lp(g_i), lp(f)$ yi bölecek şekilde en az bir $i \in \{1, 2, \dots, t\}$ varsa G kümesine I ideali için bir Gröbner tabanı denir. $F[x_1, x_2, \dots, x_n]$ polinom halkasının sıfırdan farklı her idealin bir Gröbner tabanına sahip olduğunu gözlemlenmiştir. Gröbner tabanı tanımı yardımıyla bir çok teorem elde edilmişse de bu teoremler sadece bir kümenin bir idealin Gröbner tabanı olup olmadığını incelemek için kullanılmış, fakat bu teoremler bir ideal için Gröbner tabanı bulmak için yeterli olmamıştır.

Buchberger'in amacı bir cisim üzerindeki bir polinom halkasında herhangi bir ideal için bir Gröbner tabanını oluşturmak için S-Polinomu kavramını tanımlamış ve bu tabanı elde etmek için kendi adıyla Buchberger Algoritmasını oluşturmuştur. S-Polinomu, iki polinom kullanılarak bulunan yeni bir polinomdur. Algoritmaya göre bir ideale Gröbner tabanı bulmak için önce bu idealin üreteç kümesi alınır. Daha sonra bu üreteç kümesi içindeki polinomların ikişer ikişer S-Polinomları bulunur ve bulunan bütün S-Polinomları üreteç kümesine göre indirgenir. Sıfıra indirgenemeyen S-Polinomları üreteç kümesine eklenerek, sıfıra indirgenene kadar bu işlem devam eder ve sonunda istenilen Gröbner tabanı elde edilmiş olur. Bu işlem sonunda bulunan küme içinde birbiri cinsinden yazılabilen polinomlar kümeden atılarak, minimal ve ardından indirgenmiş Gröbner tabanı elde edilmiştir. İndirgenmiş

Gröbner tabanının tek olduğu da ispatlanmıştır. Bu sayede oluşturulan indirgenmiş Gröbner tabanı verilen ideal için bulunabilecek en uygun üreteç kümesi olarak elde edilmiştir.

Tezimizin ilk bölümleri yukarıda bahsedilen konular için ayrılmış olup, son bölümde katsayılar halkası olarak farklı bir cebirsel yapı olan Modüller alınarak Gröbner tabanları incelenmiştir.



2. KURAMSAL TEMELLER

2.1. Temel Tanım ve Teoremler

Bu çalışmada kullanılacak bazı temel tanım ve teoremler aşağıda verilmiştir.

Tanım 2.1.1. $F \neq \emptyset$ kümesi üzerinde tanımlı iki ikili işlem $+$ ve $\cdot$ olsun. Aşağıdaki aksiyomları sağlayan $(F, +, \cdot)$ cebirsel yapısına bir **halka** denir (Çallıalp 2013).

H1: $(F, +)$ bir değişmeli gruptur.

H2: $\cdot$ işleminin F de birleşme özelliği vardır.

H3: $\cdot$ işleminin $+$ işlemi üzerine sağdan ve soldan dağılma özellikleri vardır:

$$\forall a, b, c \in F \text{ için } a(b + c) = ab + ac \text{ ve } (a + c)b = ac + bc.$$

F halkasının $+$ işlemine göre etkisiz (birim) elemanına halkanın **sıfır elemanı** denir ve 0_F ile gösterilir. Halkanın $\cdot$ işlemine göre etkisiz elemanı olmayabilir. Eğer ikinci işleme göre de etkisiz elemanı varsa bu elemana, halkanın **birim elemanı** denir ve 1_F ile gösterilir. Böyle bir halkaya da **birimli halka** denir. Ayrıca halka ikinci işleme göre değişme özelliğine sahip ise halkaya **değişmeli halka** denir.

Grup, tek işlemli cebirsel bir yapı iken, halka, iki işlemli cebirsel bir yapıdır.

Tanım 2.1.2. F halkasında, $0_F \neq a \in F$ elemanı için; $ab = 0_F$ ($ba = 0_F$) olacak şekilde $\exists 0_F \neq b \in F$ bulunabilirse a ya, F halkasının bir **sol sıfır böleni** (**sağ sıfır böleni**) denir. Eğer a hem sol sıfır bölen hem de sağ sıfır bölen ise kısaca sıfır bölen olarak adlandırılır (Çallıalp 2013).

Tanım 2.1.3. Sıfır bölensiz bir halkaya **tam halka** denir. Birimli, değişmeli ve sıfır bölensiz halkaya da bir **tamlık bölgesi** denir (Çallıalp 2013).

Tanım 2.1.4. F birimli ve değişmeli bir halka olsun. $F - \{0_F\} = F^*$ ifadesi ikinci işleme $(\cdot)$ göre bir grup ise F ye bir **cisim** denir. Yani cisim; birimli, değişmeli ve sıfırdan farklı her elemanın tersi olan özel bir halkadır (Çallıalp 2013).

Tanım 2.1.5. F bir halka ve $\emptyset \neq S \subset F$ olsun. F deki işlemlere göre S alt kümesi kendi başına bir halka ise S ye F halkasının bir **alt halkası** denir (Çallıalp 2013).

Önerme 2.1.6. F bir halka ve $\emptyset \neq S \subset F$ olsun. S nin, F nin bir alt halkası olması için gerek ve yeter şart $\forall a, b \in S$ için, $a - b \in S$ ve $ab \in S$ olmasıdır (Çallıalp 2013).

Tanım 2.1.7. K, F halkasının bir alt kümesi olsun. F nin K yı kapsayan bütün alt halkalarının arakesitine **K nın ürettiği alt halka** denir ve $\langle K \rangle$ ile gösterilir. K nın elemanlarına da $\langle K \rangle$ nın **üretecileri** denir (Çallıalp 2013).

Örnek 2.1.8. $\mathbb{Q}$ da, $K = \left\{ \frac{1}{2} \right\}$ nin ürettiği alt halka;

$$\left\{ a_0 + \frac{a_1}{2} + \frac{a_2}{2^2} + \dots + \frac{a_r}{2^r} \mid r \geq 0, r, a_i \in \mathbb{Z}, i = 0, 1, 2, \dots, r \right\}$$

dir.

Tanım 2.1.9. F bir halka ve $\emptyset \neq I \subset F$ olsun.

i) $\forall a, b \in I$ için $a - b \in I$ ve

ii) $\forall a \in I$ ve $\forall r \in F$ için, $ra \in I$ (veya $ar \in I$)

ise I ya F nin bir **sol** (veya **sağ**) **ideali** denir. Hem sol, hem de sağ bir ideale **iki taraflı ideal** veya kısaca **ideal** denir (Çallıalp 2013).

Tanım 2.1.10. K, F halkasının bir alt kümesi olsun. F nin K yı kapsayan bütün ideallerinin arakesitine **K nın ürettiği ideal** denir ve $\langle K \rangle$ ile gösterilir. Eğer $K = \{a\}$ tek elemanlı bir küme ise K nın ürettiği ideale **temel ideal** denir ve $\langle a \rangle$ ile gösterilir (Çallıalp 2013).

Önerme 2.1.11. F değişmeli bir halka ve $\emptyset \neq K \subset F$ ise K nın ürettiği ideal

$$\langle K \rangle = \left\{ \sum_{i=1}^s r_i a_i + \sum_{j=1}^t n_j b_j \mid r_i \in F, n_j \in \mathbb{Z}, a_i, b_j \in K, s, t \in \mathbb{N} \right\}$$

dir (Çallıalp 2013).

Sonuç 2.1.12. F birimli ve değişmeli bir halka ve $\emptyset \neq K \subset F$ ise K nın ürettiği ideal

$$\langle K \rangle = \left\{ \sum_{i=1}^s r_i a_i \mid r_i \in F, a_i \in K, s \in \mathbb{N}, 1 \leq i \leq s \right\}$$

dir (Çallıalp 2013).

Sonuç 2.1.13. F birimli ve değişmeli bir halka ve $a \in F$ ise

$$\langle a \rangle = aF = \{ar | r \in F\}$$

dir (Çallıalp 2013).

Tanım 2.1.14. F halkasının, bir I idealine göre tanımlanan denklik sınıfları arasında;

$$(a + I) \oplus (b + I) = (a + b) + I, (a + I) \odot (b + I) = (ab) + I$$

ile tanımlanan $\oplus$ ve $\odot$ işlemlerine göre F/I bir halkadır. Bu halkaya F nin I idealine göre **bölüm halkası** denir ve F/I veya $\frac{F}{I}$ şeklinde gösterilir (Çallıalp 2013).

Tanım 2.1.15. $x_1, x_2, \dots, x_n$ 'ler bilinmeyen ve $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$, $\beta_i \in \mathbb{N}$, $i = 1, 2, \dots, n$ olmak üzere $\mathbf{x}^\beta = x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n}$ ifadesine **kuvvet çarpımı** denir (Adams and Loustaunau 1994).

Tanım 2.1.16. F bir halka, x bir bilinmeyen ve F halkasından seçilen $a_0, a_1, \dots, a_k$ katsayıları olmak üzere, $a_0 + a_1x + \dots + a_kx^k$ şeklindeki bir ifadeye F den katsayılı bir **polinom** denir. F den katsayılı tüm polinomlar halkası $F[x]$ ile gösterilir. $x_1, x_2, \dots, x_n$ bilinmeyenler içinde yine katsayıları F den seçilerek oluşturulan $F[x_1, x_2, \dots, x_n]$ ifadesine n değişkenli **polinom halkası** denir (Çallıalp 2013).

Örnek 2.1.17. $f = 2x_1 - x_2^3 + 5$ iki değişkenli, $f = x_1^2 + x_2 - x_3^3x_4 + 1$ dört değişkenli polinom halkasının birer elemanıdır.

Tanım 2.1.18. $F[x_1, x_2, \dots, x_n]$, F üzerinde n değişkenli polinom halkası olsun. $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ polinomları, $i = 1, 2, \dots, n$ için $\beta_i \in \mathbb{N}$ ve $r \in F$ olmak üzere $r \cdot x_i^{\beta_i}$ terimlerinin sonlu toplamıdır (Adams and Loustaunau 1994).

Önerme 2.1.19. Bütün kuvvet çarpımlarının kümesi

$$\mathbb{T}^n = \{x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} | \beta_i \in \mathbb{N}, i = 1, 2, \dots, n\}$$

olmak üzere $F[x_1, x_2, \dots, x_n]$ polinom halkası tabanı $\mathbb{T}^n$ olan bir F –vektör uzayıdır (Adams and Loustaunau 1994).

Tanım 2.1.20. $n \in \mathbb{Z}^+$ için

$$F^n = \{(r_1, r_2, \dots, r_n) | r_i \in F, i = 1, 2, \dots, n\}$$

ifadesine **afin n –uzayı** denir (Taşçı 2018).

Örnek 2.1.21. $F = \mathbb{R}$ ise $F^n = \mathbb{R}^n$ ye **Öklid n –uzayı** denir.

Önerme 2.1.22. F bir halka ise $F[x]$ de bir halkadır (Taşçı 2018).

Önerme 2.1.23. F bir halka olsun.

i) F birimli ise $F[x]$ de birimli,

ii) F değişmeli ise $F[x]$ de değişmeli ve

iii) F tamlik bölgesi ise $F[x]$ de tamlik bölgesidir (Taşçı 2018).

Tanım 2.1.24. $f \in F[x_1, x_2, \dots, x_n]$ için $f = 0$ denkleminin çözümlerinin kümesi

$$V(f) = \{(r_1, r_2, \dots, r_n) \in F^n \mid f(r_1, r_2, \dots, r_n) = 0\} \subseteq F^n$$

şeklinde olup $V(f)$ kümesine f tarafından tanımlanan varyete (variety) denir (Adams and Lousaunau 1994).

Örnek 2.1.25. $V((x-1)^2 + y^2 + z^2 - 4) = \{(x, y, z) \in \mathbb{R}^3 \mid (x-1)^2 + y^2 + z^2 = 4\} \subseteq \mathbb{R}^3$ olup, xyz –koordinat sisteminde $(1,0,0)$ merkezli ve $r = 2$ yarıçaplı bir küre belirtir.

Tanım 2.1.26. $f_1, f_2, \dots, f_s \in F[x_1, x_2, \dots, x_n]$ polinomları verilsin.

$$f_1 = 0, f_2 = 0, \dots, f_s = 0 \quad (2.1.1)$$

sisteminin bütün çözümleri $V(f_1, f_2, \dots, f_s)$ **varyete kümesi** olarak tanımlanır ve

$$V(f_1, f_2, \dots, f_s) = \{(r_1, r_2, \dots, r_n) \in F^n \mid f_i(r_1, r_2, \dots, r_n) = 0, i = 1, 2, \dots, s\}$$

şeklindedir. Burada

$$V(f_1, f_2, \dots, f_s) = \bigcap_{i=1}^s V(f_i)$$

şeklindedir (Adams and Lousaunau 1994).

Örnek 2.1.27. $V(x^2 + y^2 - 16, x - y^2 + 4) \subseteq \mathbb{R}^2$ varyete kümesi $x^2 + y^2 = 4$ çemberi ile $x = y^2 - 4$ parabolünün xy –koordinat düzleminde kesişimidir.

Bununla birlikte genel olarak;

$$S = \{f \mid f \in F[x_1, x_2, \dots, x_n]\} \subseteq F[x_1, x_2, \dots, x_n]$$

ise,

$$V(S) = \{(r_1, r_2, \dots, r_n) \in F^n \mid \forall f \in S \text{ için } f(r_1, r_2, \dots, r_n) = 0\}$$

kümesi tanımlanır.

$$I = \langle f_1, f_2, \dots, f_s \rangle = \left\{ \sum_{i=1}^s u_i f_i \mid u_i \in F[x_1, x_2, \dots, x_n], i = 1, 2, \dots, s \right\},$$

$F[x_1, x_2, \dots, x_n]$ nin bir idealidir. Burada $\{f_1, f_2, \dots, f_s\}$, I idealinin bir üreteç kümesidir. Varyete kümesini daha basit yazabilmek için $I = \langle f_1, f_2, \dots, f_s \rangle$ ideali göz önüne alınırsa, $V(f_1, f_2, \dots, f_s)$ varyete kümesi için istenilen daha basit gösterim, $I = \langle f_1, f_2, \dots, f_s \rangle$ ideali için daha iyi bir üreteç kümesidir.

Teorem 2.1.28. (Hilbert Taban Teoremi)

i) I , $F[x_1, x_2, \dots, x_n]$ polinom halkasının herhangi bir ideali ise $I = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in F[x_1, x_2, \dots, x_n]$ polinomları vardır.

ii) Eğer $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, $F[x_1, x_2, \dots, x_n]$ polinom halkasındaki ideallerin artan bir zinciri ise $I_N = I_{N+1} = I_{N+2} = \dots$ olacak şekilde bir $N \in \mathbb{N}$ vardır (Özenir 2011).

Tanım 2.1.29. F değişmeli bir halka ve $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, F nin ideallerinin artan bir zinciri olsun. $I_N = I_{N+1} = I_{N+2} = \dots$ olacak şekilde bir $N \in \mathbb{N}$ varsa F halkasına **Noetherian Halka** denir (Özenir 2011).

Teorem 2.1.30. Değişmeli bir F halkası için aşağıdaki koşullar denktir.

i) I, F nin herhangi bir ideali ise $I = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in F$ elemanları vardır.

ii) Eğer $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, F nin ideallerinin artan bir zinciri ise $I_N = I_{N+1} = I_{N+2} = \dots$ olacak şekilde bir $N \in \mathbb{N}$ vardır (Özenir 2011).

İspat: $(i) \Rightarrow (ii)$: $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, F nin ideallerinin artan bir zinciri olsun. Böylece $I = \bigcup_{n=1}^{\infty} I_n$ kümesi F nin bir idealidir. Bu durumda $i = 1, 2, \dots, s$ için $f_i \in I$ olduğundan $f_i \in I_{N_i}$ olacak şekilde $N_i \in \mathbb{N}$ vardır. $N = \max_{1 \leq i \leq s} N_i$ olsun. Dolayısıyla her $i = 1, 2, \dots, s$ için $f_i \in I_N$ dir. $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$ artan bir zincir ve

$$I = \bigcup_{n=1}^{\infty} I_n$$

olduğundan

$$I_N \subseteq I = \bigcup_{n=1}^{\infty} I_n$$

olur. Buradan $I = I_N$ ifadesi elde edilir.

(ii) $\Rightarrow$ (i): (ii) nin sağladığını fakat (i) nin sağlamadığı varsayalım. Yani I, F nin elemanlarının sonlu bir kümesi tarafından üretilmesin. Bu durumda $I = \langle f_1, f_2, \dots, f_s, f_{s+1}, \dots \rangle$ olur. $f_1 \in I$ olsun. O zaman $f_2 \notin \langle f_1 \rangle$ olacak şekilde bir $f_2 \in I$ vardır. Yani $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle$ olur. Benzer şekilde $f_3 \notin \langle f_1, f_2 \rangle$ olacak şekilde bir $f_3 \in I$ vardır. Buradan $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle$ olur. Bu şekilde devam edilirse

$$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle \subsetneq \dots \subsetneq \langle f_1, f_2, \dots, f_s \rangle \subsetneq \langle f_1, f_2, \dots, f_s, f_{s+1} \rangle \subsetneq \dots$$

şeklinde artan bir zincir bulunur. Bu (ii) ile çelişir. Dolayısıyla (i) sağlanmalıdır.

Teorem 2.1.31. F bir Noetherian Halka ise $F[x]$ bir Noetherian halkadır (Adams and Lousaunau 1994).

Yukarıdaki Teorem ve n üzerinden tümevarım kullanılırsa $F[x_1, x_2, \dots, x_n]$ polinom halkasının bir Noetherian halka olduğu görülür. Bu ise Teorem 2.1.28 in kanıtıdır.

2.2. Tek Değişkenli Polinomlar İçin İndirgenme

İlk etapta $F[x]$ polinom halkası ile ilgili bazı temel tanım ve bilgileri verilecektir. Daha sonra bu tanım ve bilgileri çok değişkenli polinomlara genelleştirilecektir.

Tanım 2.2.1. $0 \neq f \in F[x]$ için f polinomundaki x değişkeninin en büyük kuvvetine f polinomunun **derecesi** denir ve $\deg f$ ile gösterilir (Adams and Lousaunau 1994).

Tanım 2.2.2. $0 \neq f \in F[x]$ için f polinomundaki en büyük dereceli terime f polinomunun **baş terimi** denir ve $lt(f)$ ile gösterilir (Adams and Lousaunau 1994).

Tanım 2.2.3. $0 \neq f \in F[x]$ için f polinomundaki baş terimin katsayısına f polinomunun **baş katsayısı** denir ve $lc(f)$ ile gösterilir. $a_0, a_1, \dots, a_n \in F$ ve $a_n \neq 0$ olmak üzere

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

ise

$$\deg f = n, lt(f) = a_n x^n, lc(f) = a_n$$

olur (Adams and Loustaunau 1994).

Tanım 2.2.4. $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ve

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0, \quad n = \deg(f) \geq m = \deg(g)$$

iki polinom olmak üzere f nin g ile bölünmesinde ilk adım $\frac{a_n}{b_m} x^{n-m} \cdot g$ çarpımını f polinomundan çıkarmaktır. Burada $\frac{a_n}{b_m} x^{n-m} = \frac{lt(f)}{lt(g)}$ olup, $h = f - \frac{lt(f)}{lt(g)} g$ nin ilk kalan olduğu görülür. Bu işlem f polinomunun g polinomu tarafından h polinomuna **indirgenmesi** denir ve $f \xrightarrow{g} h$ ile gösterilir. Burada kalan polinomunun derecesi bölen polinomdan küçük çıkana kadar indirgenme işlemi devam eder ve

$$f \xrightarrow{g} h_1 \xrightarrow{g} h_2 \xrightarrow{g} \dots \xrightarrow{g} h_k$$

şeklinde yazılabilir. Bu tekrarlanan indirgenme adımları kısaca

$$f \xrightarrow{+g} h_k$$

ile gösterilir (Adams and Loustaunau 1994).

Örnek 2.2.5. $f = x^4 + 2x^3 - 4$ ve $g = 2x^2 + x \in \mathbb{Q}[x]$ olsun. f polinomunun g polinomu ile bölümünden elde edilen bölüm $q = \frac{x^2}{2} + \frac{3x}{4} - \frac{3}{8}$ ve kalan $r = \frac{3x}{8} - 4$ olarak bulunur. Bölüm ve kalanı kullanarak $f = \left(\frac{x^2}{2} + \frac{3x}{4} - \frac{3}{8}\right)g + \left(\frac{3x}{8} - 4\right)$ ifadesi elde edilir. Şimdide Tanım 2.2.4 e göre indirgenme işlemi yapılacaktır. $h = f - \frac{lt(f)}{lt(g)}g$ formülünden $h_1 = x^4 + 2x^3 - 4 - \frac{x^4}{2x^2}(2x^2 + x) = \frac{3x^3}{2} - 4$ ilk kalan elde edilir. İkinci adımda $h_2 = h_1 - \frac{lt(h_1)}{lt(g)} \cdot g = \left(\frac{3x^3}{2} - 4\right) - \frac{\frac{3x^3}{2}}{2x^2}(2x^2 + x) = -\frac{3x^2}{4} - 4$ elde edilir. h_2 polinomunun derecesi g polinomunun derecesine eşit olduğu için son

bir indirgenme işlemi daha yapılacaktır. O halde;

$$h_3 = h_2 - \frac{lt(h_2)}{lt(g)} \cdot g = -\frac{3x^2}{4} - 4 - \frac{-\frac{3x^2}{4}}{2x^2} (2x^2 + x) = \frac{3x}{8} - 4 \text{ ifadesi elde edilir ve}$$

$f \xrightarrow{g}_+ h_3$ şeklinde gösterilir.

Teorem 2.2.6. F bir cisim ve $0 \neq f, g \in F[x]$ olsun. Bu durumda

$$f = q \cdot g + r \text{ ve } r = 0 \text{ ya da } \deg(r) < \deg(g)$$

olacak şekilde tek türlü belirli $q, r \in F[x]$ vardır (Adams and Loustaunau 1994).

Aşağıda Bölme Algoritması olarak bilinen Algoritma 2.2.1 verilmiştir.

Girdi: $g \neq 0$ olmak üzere $f, g \in F[x]$ alınsın

Çıktı: $\exists q, r \in F[x] \ni f = q \cdot g + r, r = 0$ veya $\deg(r) < \deg(g)$

1 **Başlat:** $q := 0 ; r := f$

2 **Tekrar et:** $r \neq 0$ ve $\deg(g) \leq \deg(r)$ olduğu sürece aşağıdaki işlemler yapılır

3 $q := q + \frac{lt(r)}{lt(g)}$

4 $r := r - \frac{lt(r)}{lt(g)} g$

Algoritma 2.2.1. Tek Değişkenli Polinomlar İçin Bölme Algoritması

Örnek 2.2.7. $f = x^4 + 2x^3 - 4$ ve $g = 2x^2 + x \in \mathbb{Q}[x]$ olsun. f polinomunun g polinomu ile bölümünden oluşan bölüm ve kalan Algoritma 2.2.1 ile bulunur.

Başlat: $q := 0 ; r := f = x^4 + 2x^3 - 4$

1.ADİM: $q := q + \frac{lt(r)}{lt(g)} = 0 + \frac{x^4}{2x^2} = \frac{x^2}{2}$

$$r := r - \frac{lt(r)}{lt(g)} \cdot g = x^4 + 2x^3 - 4 - \frac{x^4}{2x^2} (2x^2 + x) = \frac{3x^3}{2} - 4$$

2.ADİM: $q := q + \frac{lt(r)}{lt(g)} = \frac{x^2}{2} + \frac{\frac{3x^3}{2}}{2x^2} = \frac{x^2}{2} + \frac{3x}{4}$

$$r := r - \frac{lt(r)}{lt(g)} \cdot g = \frac{3x^3}{2} - 4 - \frac{\frac{3x^3}{2}}{2x^2} (2x^2 + x) = \frac{3x^3}{2} - 4 - \frac{3x^3}{2} - \frac{3x^2}{4} = -\frac{3x^2}{4} - 4$$

$$\mathbf{3.ADIM:} \quad q := q + \frac{lt(r)}{lt(g)} = \frac{x^2}{2} + \frac{3x}{4} + \frac{\frac{-3x^2}{4}}{2x^2} = \frac{x^2}{2} + \frac{3x}{4} - \frac{3}{8}$$

$$r := r - \frac{lt(r)}{lt(g)} \cdot g = -\frac{3x^2}{4} - 4 - \frac{\frac{-3x^2}{4}}{2x^2} (2x^2 + x) = \frac{3x}{8} - 8$$

olup, $\deg(r) = 1 < 2 = \deg(g)$ olduğundan algoritma tamamlanarak bölüm $q = \frac{x^2}{2} + \frac{3x}{4} - \frac{3}{8}$ ve kalan $r = \frac{3x}{8} - 8$ şeklinde bulunur.

İki polinom tarafından üretilen idealin üreteç kümesi şu şekilde değiştirilebilir: $I = \langle f, g \rangle$ olsun. $f \xrightarrow{g} h$ olduğu varsayalım. $h = f - \frac{lt(f)}{lt(g)} g$ olduğundan $I = \langle h, g \rangle$ dir. Dolayısıyla I idealinin üreteç kümesinde f yerine h yazılabilir ve bu sayede I idealinin üreteç kümesi değiştirilmiş olur. Bu fikir tekrarlanarak kullanılırsa aşağıdaki sonuç elde edilir.

Teorem 2.2.8. F bir cisim olmak üzere $F[x]$ polinom halkasındaki her ideal tek bir eleman tarafından üretilir (Adams and Loustaunau 1994).

İspat: $I, F[x]$ in sıfırdan farklı bir ideali olsun. $g \neq 0$ ve $n = \deg(g)$ en az olacak şekilde $g \in I$ olsun. Herhangi bir $f \in I$ için, Teorem 2.2.6 dan $q, r \in F[x]$ ve $r = 0$ veya $\deg(r) < \deg(g) = n$ olacak şekilde $f = qg + r$ elde edilir. Eğer $r \neq 0$ ise $r = f - qg \in I$ olup bu ise g nin seçimi ile çelişir. Böylece

$$r = 0, f = qg \text{ ve } I \subseteq \langle g \rangle$$

olur. g, I nın elemanı olduğu için ters kapsama da sağlanır ve dolayısıyla eşitlik durumu elde edilir.

Dikkat edilmelidir ki Teorem 2.2.8 deki g polinomu sıfırdan farklı sabit bir çarpan farkıyla tektir. Yani eğer $I = \langle g_1 \rangle = \langle g_2 \rangle$ ise g_1 böler g_2 ve g_2 böler g_1 dir. Aynı zamanda burada $\{g\}$ kümesi $I = \langle f_1, f_2, \dots, f_s \rangle$ ideali için ‘daha iyi’ bir üreteç kümesidir. Burada g polinomunun nasıl bulunacağına bakılacaktır. İki polinom tarafından üretilen $I \subseteq F[x]$ ideali için $I = \langle f_1, f_2 \rangle$ olsun. f_1 ve f_2 polinomlarının en büyük ortak böleni $\gcd(f_1, f_2) = g$ ise;

- g, f_1 ve f_2 yi böler,
- Eğer $h \in F[x], f_1$ ve f_2 yi bölüyorsa $h|g$,
- $lc(g) = 1$ (yani g moniktir)

dir.

Önerme 2.2.9. f_1 ve f_2 den bir tanesi sıfırdan farklı olmak üzere $f_1, f_2 \in F[x]$ olsun. Bu durumda, $\gcd(f_1, f_2)$ vardır ve $\langle f_1, f_2 \rangle = \langle \gcd(f_1, f_2) \rangle$ dir (Adams and Loustaunau 1994).

İspat: Teorem 2.2.8 den $\langle f_1, f_2 \rangle = \langle g \rangle$ olacak şekilde bir $g \in F[x]$ vardır. g sıfırdan farklı bir sabit çarpan farkıyla tek olduğundan $lc(g) = 1$ olduğu kabul edilebilir. $g = \gcd(f_1, f_2)$ olduğu gösterilecektir. $f_1, f_2 \in \langle g \rangle$ olduğundan $g|f_1$ ve $g|f_2$ dir. Şimdi, h polinomu f_1 ve f_2 yi bölen başka bir polinom olsun. $g \in \langle f_1, f_2 \rangle$ olduğundan

$$g = u_1 f_1 + u_2 f_2$$

olacak şekilde $u_1, u_2 \in F[x]$ vardır. Dolayısıyla, $h|g$ olup istenen elde edilir.

Sonuç olarak eğer en büyük ortak bölenin bulunması için bir algoritmaya sahip ise aslında $\langle f_1, f_2 \rangle$ ideali için tek elemanlı bir üreteç kümesi bulunabilir. Öklid Algoritması yukarıda bahsedilen Bölme Algoritmasına bağlı olan bir en büyük ortak bölen bulma algoritmasıdır.

Lemma 2.2.10. f_1 ve f_2 den bir tanesi sıfırdan farklı olmak üzere $f_1, f_2 \in F[x]$ olsun. Bu durumda, $\forall q \in F[x]$ için

$$\gcd(f_1, f_2) = \gcd(f_1 - q \cdot f_2, f_2)$$

dir (Adams and Loustaunau 1994).

İspat: $\langle f_1, f_2 \rangle = \langle f_1 - q f_2, f_2 \rangle$ olduğunu görmek kolaydır. Böylece Önerme 2.2.9 dan

$$\langle \gcd(f_1, f_2) \rangle = \langle f_1, f_2 \rangle = \langle f_1 - q f_2, f_2 \rangle = \langle \gcd(f_1 - q f_2, f_2) \rangle$$

dir. Böylece, bir esas idealin üretici sabit bir çarpan farkıyla tek olduğundan ve iki polinomun en büyük ortak böleninin baş katsayısı 1 olarak tanımlandığından,

$$\gcd(f_1, f_2) = \gcd(f_1 - q f_2, f_2)$$

elde edilir.

Aşağıda verilen Öklid Algoritmasında dikkat edilmesi gereken durum, algoritma döngüsündeki r nin derecesi, bir önceki r olan g nin derecesinden

kesinlikle daha küçüktür ve dolayısıyla algoritma ilerledikçe r nin derecesi kesinlikle azaldığından algoritma sonlanır. Aynı zamanda Algoritma $gcd(f_1, f_2)$ yi bir çıktı olarak verir çünkü, her bir döngü içinden geçildikçe, $g \neq 0$ olduğu sürece Lemma 2.2.10 dan

$$gcd(f_1, f_2) = gcd(f, g) = gcd(r, g)$$

ifadesi elde edilir. $g = 0$ olduğunda ise,

$$gcd(f_1, f_2) = gcd(f, 0) = \frac{1}{lc(f)} f$$

dir. Algoritmanın son adımı ise sonuç polinomunun monik olduğunu garanti eder.

İki polinomun en büyük ortak bölenini bulmak için aşağıda verilen Öklid Algoritmasına bakılacaktır.

Girdi: $f_1, f_2 \in F[x]$, f_1, f_2 nin biri sıfırdan farklı

Çıktı: $f = gcd(f_1, f_2)$

1 **Başlat:** $f := f_1, g := f_2$

2 **Tekrar et:** $g \neq 0$ olduğu sürece aşağıdaki işlemler yapılır

3 $f \xrightarrow{g}_+ r$, burada r , f nin g ile bölümünden kalandır

4 $f := g$

5 $g := r$

6 $f := \frac{1}{lc(f)} f$

Algoritma 2.2.2. Öklid Algoritması

Örnek 2.2.11. $f_1 = x^4 + x^3 - 13x^2 - x + 12$ ve $f_2 = x^2 - 9 \in \mathbb{Q}[x]$ olsun. $gcd(f_1, f_2)$ Algoritma 2.2.2 ile bulunur.

Başlat: $f := x^4 + x^3 - 13x^2 - x + 12, g := x^2 - 9$

1.ADIM: $x^4 + x^3 - 13x^2 - x + 12 \xrightarrow{x^2-9} x^3 - 4x^2 - x + 12$

$$\xrightarrow{x^2-9} -4x^2 + 8x + 12$$

$$\xrightarrow{x^2-9} 8x - 24$$

$$f := x^2 - 9, \quad g := 8x - 24$$

$$\mathbf{2.ADIM:} \quad x^2 - 9 \xrightarrow{8x-24} 3x - 9 \xrightarrow{8x-24} 0$$

$$f := 8x - 24, \quad g := 0$$

$$f := \frac{1}{lc(f)} \cdot f = \frac{1}{8}(8x - 24) = x - 3$$

$g = 0$ bulunduğundan dolayı algoritma tamamlanmış olur ve $gcd(f_1, f_2) = x - 3$ ifadesi elde edilir.

Önerme 2.2.12. $f_1, f_2, \dots, f_s \in F[x]$ olsun. O zaman

$$i) \langle f_1, f_2, \dots, f_s \rangle = \langle gcd(f_1, f_2, \dots, f_s) \rangle,$$

$$ii) \text{ Eğer } s \geq 3 \text{ ise } gcd(f_1, f_2, \dots, f_s) = gcd(f_1, gcd(f_2, \dots, f_s))$$

dir (Adams and Loustaunau 1994).

$f_1 = 0, f_2 = 0, \dots, f_s = 0, i = 1, 2, \dots, s, f_i \in F[x]$ denklem sistemini çözmek için ilk önce $g = gcd(f_1, f_2, \dots, f_s)$ bulunur. Böylece $g = 0$ tek denklemini çözmek yeterli olur.

Herhangi bir f polinomunun $I = \langle f_1, f_2, \dots, f_s \rangle$ idealinde olup olmadığına karar vermek için ilk önce $g = gcd(f_1, f_2, \dots, f_s)$ bulunmalıdır. Sonra Bölme Algoritması kullanılarak f polinomu g polinomuna bölünür. Bu bölmede kalanın sıfır olması için gerek ve yeter şart f polinomunun $I = \langle f_1, f_2, \dots, f_s \rangle = \langle g \rangle$ idealinde olmasıdır. Bu ifade

$$f \in I = \langle g \rangle \Leftrightarrow f \xrightarrow{g}_+ 0$$

şeklinde gösterilir.

Örnek 2.2.13. $f_1 = x^2 - x - 6, f_2 = x^4 + x^3 - 13x^2 - x + 12$ ve $f_3 = x^2 - 9 \in \mathbb{Q}[x]$ olsun. $gcd(f_1, f_2, f_3)$ ifadesi bulunabilir. Önerme 2.2.12 den

$$gcd(f_1, f_2, f_3) = gcd(f_1, gcd(f_2, f_3))$$

olur. Örnek 2.2.11 den $gcd(f_2, f_3) = x - 3$ olup $gcd(f_1, x - 3)$ ifadesi Algoritma 2.2.2 ile bulunur.

Başlat: $f := x^2 - x - 6$, $g := x - 3$

1.ADIM: $x^2 - x - 6 \xrightarrow{x-3} 2x - 6 \xrightarrow{x-3} 0$

$f := x - 3$, $g := 0$

$f := \frac{1}{lc(f)} \cdot f = x - 3$, $g = 0$ bulunduğundan dolayı algoritma tamamlanmış olur ve

$gcd(f_1, gcd(f_2, f_3)) = gcd(f_1, f_2, f_3) = x - 3$ ifadesi elde edilir.

2.3. Çok Değişkenli Doğrusal Polinomlar İçin İndirgenme

Bu bölümde her bir $i = \{1, 2, \dots, s\}$ için f_i doğrusal polinom olmak üzere

$$f_1 = 0, f_2 = 0, \dots, f_s = 0 \quad (2.3.1)$$

denklem sistemi göz önüne alınacaktır. Satır eşelon form indirgeme metodu kullanılacaktır.

Örnek 2.3.1. $f_1 = x + 2y - z$, $f_2 = 3x + y + 2z \in \mathbb{R}[x, y, z]$ doğrusal polinomlar olsun. $I = \langle f_1, f_2 \rangle$ idealini ve

$$\begin{cases} x + 2y - z = 0 \\ 3x + y + 2z = 0 \end{cases} \quad (2.3.2)$$

sisteminin çözümü olan $V = (f_1, f_2)$ variety kümesi göz önüne alalım.

Bu sistemin katsayılar matrisi üzerinde satır indirgeme metodu kullanılırsa

$$\begin{bmatrix} 1 & 2 & -1 \\ 3 & 1 & 2 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 2 & -1 \\ 0 & -5 & 5 \end{bmatrix}$$

olur. (2.3.2) sisteminin çözümleri,

$$\begin{cases} x + 2y - z = 0 \\ -5y + 5z = 0 \end{cases} \quad (2.3.3)$$

sisteminin çözümleri ile aynıdır. Satır indirgeme yöntemi $I = \langle f_1, f_2 \rangle$ ideali için üreteç kümesini değiştirme yoludur. Yapılan satır indirgemesi ile $f_3 = -5y + 5z$ polinomunun f_1 ve f_2 polinomlarının doğrusal bileşimi olarak yazıldığı görülür.

$f_3 = f_2 - 3f_1$ olduğundan $f_3 \in \langle f_1, f_2 \rangle = I$ dır. Diğer taraftan $f_2 = f_3 + 3f_1$ olduğundan $f_2 \in \langle f_1, f_3 \rangle$ olur. Sonuç olarak $I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ elde edilir ve $I = \langle f_1, f_2 \rangle$ ideali için yeni üreteç kümesi $\{f_1, f_3\}$ şeklinde elde edilir. Elde edilen bu

f_3 polinomunda sadece y ve z değişkenleri var iken f_1 ve f_2 polinomlarında y ve z değişkenleri ile birlikte x değişkeni de bulunduğu için f_3 polinomu, f_1 ve f_2 polinomları kullanılarak indirgenemez.

2.4. Terim Sıralamaları

Tanım 2.4.1. Tanım 2.1.15 de $x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n}$ ifadesini kuvvet çarpımı olarak tanımlamıştı ve bütün kuvvet çarpımlarının kümesi

$$\mathbb{T}^n = \{x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} | \beta_i \in \mathbb{N}, i = 1, 2, \dots, n\}$$

şeklinde ifade edilir. ‘Tam sıralama’ olması için, $x^\alpha, x^\beta \in \mathbb{T}^n$ olmak üzere $x^\alpha < x^\beta, x^\alpha > x^\beta$ veya $x^\alpha = x^\beta$ ifadelerinden biri olması gerekir. İşte bu sıralamalara **terim sıralaması** denir (Adams and Loustaunau 1994).

Tek değişkenli polinomlarda terim sıralaması için derecesi büyük olan değişken ilk terim olarak alınır, birden fazla değişkenli polinomlarda terim sıralaması içinde bazı tanımlar verilecektir. Terim sıralamaları için değişkenler arasındaki sıralamanın mutlaka verilmesi gerekiyor.

Tanım 2.4.2. $\mathbb{T}^n$ üzerinde aşağıdaki şartları sağlayan “ $<$ ” tam sıralamasına $\mathbb{T}^n$ üzerinde bir **terim sıralaması** denir (Adams and Loustaunau 1994).

i) $x^\alpha \neq 1, \forall x^\alpha \in \mathbb{T}^n$ için $1 < x^\alpha$ dır.

ii) Eğer $x^\alpha < x^\beta$ ise $\forall x^p \in \mathbb{T}^n$ için $x^\alpha \cdot x^p < x^\beta \cdot x^p$ dır.

Örneğin tek değişkenli durumda $1 < x < x^2 < x^3 < \dots < x^n < \dots$ şeklinde sıralanır.

Tanım 2.4.3. $\mathbb{T}^n$ üzerinde $x_1 > x_2 > \dots > x_n$ ve $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$,

$\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ olmak üzere iki farklı α_i ve β_i koordinatlarından soldan ilk bileşenden başlayarak $\alpha_i < \beta_i$ koşulu sağlanırsa $x^\alpha < x^\beta$ ifadesine **alfabetik sıralama** (lexicographical) denir ve lex ile gösterilir (Adams and Loustaunau 1994).

Örneğin üç değişkenli durumda $x > y > z$ olmak üzere

$$1 < z < yz < y^2 < y^2z < x < xyz < x^2 < x^2z^5 < x^2y < x^3$$

şeklinde sıralanır.

Tanım 2.4.4. $\mathbb{T}^n$ üzerinde $x_1 > x_2 > \dots > x_n$ ve $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ olmak üzere terimlerin kuvvetleri olan α_i ve β_i lerin toplamında büyük olanın terimi daha büyük olur, kuvvetler toplamı eşit olan terimlerin sıralaması içinde alfabetik sıralama kullanılır, buna göre $x^\alpha < x^\beta$ ifadesine **dereceye göre alfabetik sıralama** (degree lexicographical) denir ve deglex ile gösterilir (Adams and Lousaunau 1994).

Örneğin üç değişkenli durumda $x > y > z$ olmak üzere

$$1 < z < x < xz < xy < xy^2 < y^2z^2 < x^2y^2 < xyz^3 < xy^2z^2$$

şeklinde sıralanır.

Tanım 2.4.5. $\mathbb{T}^n$ üzerinde $x_1 > x_2 > \dots > x_n$ ve $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ olmak üzere terimlerin kuvvetleri olan α_i ve β_i lerin toplamında büyük olanın terimi daha büyük olur, kuvvetler toplamı eşit olan terimler α ve β için sağdan itibaren farklı ilk α_i ve β_i koordinatları için $\alpha_i > \beta_i$ sıralaması sağlanır, buna göre $x^\alpha < x^\beta$ ifadesine **dereceye göre ters alfabetik sıralama** (degree reverse lexicographical) denir ve degrevlex ile gösterilir (Adams and Lousaunau 1994).

Örneğin üç değişkenli durumda $x > y > z$ olmak üzere

$$1 < y < z^2 < xyz < y^2z^2 < xyz^2 < x^2yz < xy^3$$

şeklinde sıralanır.

2.5. Bölme Algoritması ile Polinomların İndirgenmesi

Tanım 2.5.1. F bir cisim olmak üzere $F[x_1, x_2, \dots, x_n]$ polinom halkası üzerindeki bölme algoritması ile indirgenme işlemi yapılacaktır.

$$X^{n_i} \in T^n, r_i \in F, i = 1, 2, \dots, k, X^{n_1} > X^{n_2} > \dots > X^{n_k}$$

için $f \in F[x_1, x_2, \dots, x_n]$ polinomu

$$f = r_1X^{n_1} + r_2X^{n_2} + \dots + r_kX^{n_k}$$

olarak yazılır.

- f nin en büyük dereceli teriminin kuvvet çarpımı $lp(f) = X^{n_1}$
- f nin en büyük dereceli teriminin katsayısı $lc(f) = r_1$

- f nin en büyük dereceli terimi $lt(f) = r_1 X^{n_1}$

olarak tanımlanır (Adams and Lousaunau 1994).

Örnek 2.5.2. $f = 3xyz^2 - 5x^2yz + xy^3 + xy^2 + 7x - 6$ ve $x > y > z$ olsun.

- lex sıralamasına göre

$$lp(f) = x^2yz$$

$$lc(f) = -5$$

$$lt(f) = -5x^2yz$$

- deglex sıralamasına göre

$$lp(f) = x^2yz$$

$$lc(f) = -5$$

$$lt(f) = -5x^2yz$$

- degrevlex sıralamasına göre

$$lp(f) = xy^3$$

$$lc(f) = 1$$

$$lt(f) = xy^3$$

dır.

Tanım 2.5.3. $g \neq 0$ ve $f, g, h \in F[x_1, x_2, \dots, x_n]$ için $f \xrightarrow{g} h$ ile gösterilen f nin tek adımda g modülüne göre h ya indirgenmesi için gerek ve yeter şart $lp(g)$ nin f polinomunun sıfırdan farklı bir X terimini bölmesidir. Burada, $h = f - \frac{X}{lt(g)} \cdot g$ dir (Adams and Lousaunau 1994).

Örnek 2.5.4. $f = 3x^2y - 5xy + 7x - 6, g = 2x + y \in \mathbb{Q}[x, y]$ ve $x > y$ için deglex sıralaması ve Tanım 2.5.3 kullanılarak f polinomu, g polinomu yardımıyla indirgensin.

$$lp(g) = x, lt(g) = 2x, lp(g) = x | 3x^2y \text{ olduğundan } X = 3x^2y \text{ olsun}$$

$$h_1 = f - \frac{X}{lt(g)} \cdot g = 3x^2y - 5xy + 7x - 6 - \frac{3x^2y}{2x} (2x + y)$$

$$= -5xy + 7x - \frac{3xy^2}{2} - 6$$

$$lp(g) = x, lt(g) = 2x, lp(g) = x \mid -\frac{3xy^2}{2} \text{ olduğundan } X = -\frac{3xy^2}{2} \text{ olsun.}$$

$$\begin{aligned} h_2 &= h_1 - \frac{X}{lt(g)} \cdot g = -5xy + 7x - \frac{3xy^2}{2} - 6 - \frac{\frac{3xy^2}{2}}{2x} (2x + y) \\ &= -5xy + 7x + \frac{3y^3}{4} - 6 \end{aligned}$$

$$lp(g) = x, lt(g) = 2x, lp(g) = x \mid -5xy \text{ olduğundan } X = -5xy \text{ olsun.}$$

$$\begin{aligned} h_3 &= h_2 - \frac{X}{lt(g)} \cdot g = -5xy + 7x + \frac{3y^3}{4} - 6 - \frac{-5xy}{2x} (2x + y) \\ &= 7x + \frac{3y^3}{4} - 6 + \frac{5y^2}{2} \end{aligned}$$

$$lp(g) = x, lt(g) = 2x, lp(g) = x \mid 7x \text{ olduğundan } X = 7x \text{ olsun.}$$

$$h_4 = h_3 - \frac{X}{lt(g)} \cdot g = 7x + \frac{3y^3}{4} - 6 + \frac{5y^2}{2} - \frac{7x}{2x} (2x + y) = \frac{3y^3}{4} - 6 + \frac{5y^2}{2} - \frac{7y}{2}$$

olur. Elde edilen bu h_4 polinomundaki hiçbir terim $lp(g) = x$ e bölünmediğinden dolayı indirgenme işlemi burada bitmiştir ve f polinomu, g polinomu yardımıyla indirgenme basamaklarından geçerek h_4 polinomuna indirgenmiştir yani,

$$\begin{aligned} f &\xrightarrow{g} -5xy + 7x - \frac{3xy^2}{2} - 6 \xrightarrow{g} -5xy + 7x + \frac{3y^3}{4} - 6 \xrightarrow{g} 7x + \frac{3y^3}{4} - 6 + \frac{5y^2}{2} \\ &\xrightarrow{g} \frac{3y^3}{4} - 6 + \frac{5y^2}{2} - \frac{7y}{2} \end{aligned}$$

olur. Burada dikkat edilmesi gereken durum, indirgenme basamaklarında indirgenecek her polinomdan alınacak keyfi bir terim $lp(g)$ ye bölünmek zorundadır, hiçbir terim bölünmediği zaman indirgenme işlemi tamamlanmış olur.

Tanım 2.5.5. $f, h \in F[x_1, x_2, \dots, x_n]$, ve $i = 1, 2, \dots, s$ için $f_i \neq 0$, olmak üzere $F[x_1, x_2, \dots, x_n]$ polinom halkasındaki polinomların bir kümesi $G = \{f_1, f_2, \dots, f_s\}$, olsun. Eğer

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} h_3 \dots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

olacak şekilde $i_1, i_2, \dots, i_t \in \{1, 2, \dots, s\}$ indislerin bir dizisi ve $h_1, h_2, \dots, h_{t-1} \in F[x_1, x_2, \dots, x_n]$ polinomlarının bir dizisi varsa f polinomu, G kümesine göre h **polinomuna indirgenir** denir ve $f \xrightarrow{G}_+ h$ ile gösterilir (Adams and Lousaunau 1994).

Örnek 2.5.6. $f = xy^3 + 1, f_1 = x - y, f_2 = y^2 \in \mathbb{Q}[x, y], G = \{f_1, f_2\}$ ve $x > y$ için deglex sıralaması kullanılarak $f \xrightarrow{G}_+ 1$ olduğunu gösterilecektir.

$lp(f_1) = x, lt(f_1) = x, lp(f_1) = x|xy^3$ olduğundan $X = xy^3$ olsun.

$$h_1 = f - \frac{X}{lt(f_1)} \cdot f_1 = xy^3 + 1 - \frac{xy^3}{x}(x - y) = 1 + y^4$$

$lp(f_2) = y^2, lt(f_2) = y^2, lp(f_2) = y^2|y^4$ olduğundan $X = y^4$ olsun.

$$h_2 = h_1 - \frac{X}{lt(f_2)} \cdot f_2 = 1 + y^4 - \frac{y^4}{y^2} \cdot y^2 = 1$$

Böylece $xy^3 + 1 \xrightarrow{f_1} 1 + y^4 \xrightarrow{f_2} 1$ ifadesinden $f \xrightarrow{G}_+ 1$ olduğu görülür.

Aynı örnek için f_2 ye göre ilk önce işlem yapalım.

$lp(f_2) = y^2, lt(f_2) = y^2, lp(f_2) = y^2|xy^3$ olduğundan $X = xy^3$ olsun.

$$h_1 = f - \frac{X}{lt(f_2)} \cdot f_2 = xy^3 + 1 - \frac{xy^3}{y^2} y^2 = 1$$

$lp(f_1) = x, lt(f_1) = x, lp(f_1) = x \nmid 1$ olduğu için $f \xrightarrow{f_2} 1$ ifadesinden $f \xrightarrow{G}_+ 1$ olduğu görülür.

$1 \leq i \leq s$ için $f_i \neq 0$ olmak üzere $f, f_1, f_2, \dots, f_s \in F[x_1, x_2, \dots, x_n]$ verilsin.

Aşağıda verilen algoritma ile $u_1, u_2, \dots, u_s \in F[x_1, x_2, \dots, x_n]$ bölümler ve $r \in F[x_1, x_2, \dots, x_n]$ kalan olmak üzere

$$f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$$

bulunur.

Girdi: $f, f_1, f_2, \dots, f_s \in F[x_1, x_2, \dots, x_n], f_i \neq 0 (1 \leq i \leq s)$.

Çıktı: $u_1, u_2, \dots, u_s, r$. Burada, $f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$, $r, \{f_1, f_2, \dots, f_s\}$ ye göre indirgenmiş ve $\max(lp(u_1)lp(f_1), lp(u_2)lp(f_2), \dots, lp(u_s)lp(f_s), lp(r)) = lp(f)$ dir.

1 **Başlat:** $u_1 := 0, u_2 := 0, \dots, u_s := 0, r := 0, h := f$

2 **Tekrar et:** $h \neq 0$ olduğu sürece:

3 **Eğer** $lp(f_i)|lp(h)$ olacak şekilde i varsa **bu durumda**

$lp(f_i)|lp(h)$ olacak şekilde en küçük i indisi seçilir ve

4 $u_i := u_i + \frac{lt(h)}{lt(f_i)}$

5 $h := h - \frac{lt(h)}{lt(f_i)} f_i$ işlemleri yapılır

6 **Aksi halde**

7 $r := r + lt(h)$

8 $h := h - lt(h)$

Algoritma 2.5.1. Çok Değişkenli Polinomlar İçin Bölme Algoritması

Örnek 2.5.7. $f = xy^3 + 1, f_1 = x - y, f_2 = y^2 \in \mathbb{Q}[x, y], G = \{f_1, f_2\}$ ve $x > y$ için deglex sıralaması ve Algoritma 2.5.1 i kullanılarak $f \xrightarrow{+}_G r$ deki r polinomu bulunmaya çalışılsın.

Başlat: $u_1 := 0, u_2 := 0, r := 0, h := f = xy^3 + 1$

1.ADİM: $lp(f_1) = x, lp(h) = lp(xy^3 + 1) = xy^3$ ifadesini böler

$$\begin{aligned} u_1 := u_1 + \frac{lt(h)}{lt(f_1)} &= 0 + \frac{xy^3}{x} = y^3, h := h - \frac{lt(h)}{lt(f_1)} f_1 = xy^3 + 1 - \frac{xy^3}{x} (x - y) \\ &= y^4 + 1 \end{aligned}$$

2.ADİM: $lp(f_1) = x, lp(h) = lp(y^4 + 1) = y^4$ ifadesini bölmez

$lp(f_2) = y^2, lp(h) = lp(y^4 + 1) = y^4$ ifadesini böler

$$u_2 := u_2 + \frac{lt(h)}{lt(f_2)} = 0 + \frac{y^4}{y^2} = y^2, h := h - \frac{lt(h)}{lt(f_2)} f_2 = y^4 + 1 - \frac{y^4}{y^2} (y^2) = 1$$

3.ADIM: $lp(f_1) = x, lp(h) = lp(1) = 1$ ifadesini bölmez

$lp(f_2) = y^2, lp(h) = lp(1) = 1$ ifadesini bölmez

$$r := r + lt(h) = 0 + 1 = 1, h := h - lt(h) = 1 - 1 = 0$$

$h = 0$ olduğundan algoritma tamamlanır.

$f \xrightarrow{+}_G r = 1$ ve $f = u_1 f_1 + u_2 f_2 + r = y^3 \cdot (x - y) + y^2 \cdot y^2 + 1$ olup

$$\begin{aligned} lp(f) &= \max(lp(u_1)lp(f_1), lp(u_2)lp(f_2), lp(r)) \\ &= \max(y^3 \cdot x, y^2 \cdot y^2, 1) \\ &= \max(y^3 x, y^4, 1) \\ &= y^3 x \end{aligned}$$

dir.

Teorem 2.5.8. Algoritma 2.5.1, sıfırdan farklı polinomlardan oluşan bir $G = \{f_1, f_2, \dots, f_s\}$ kümesi ve $f \in F[x_1, x_2, \dots, x_n]$ için r kalan polinomu G ye göre indirgenmiş ve

$$lp(f) = \max(\max_{1 \leq i \leq s}(lp(u_i)lp(f_i)), lp(r))$$

olmak üzere

$$f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$$

olacak şekilde

$$u_1, u_2, \dots, u_s, r \in F[x_1, x_2, \dots, x_n]$$

polinomları üretir (Adams and Lousaunau 1994).

f polinomu Teorem 2.5.8 deki gibi olmak üzere, $f - r \in \langle f_1, f_2, \dots, f_s \rangle$ dir. Dolayısıyla, eğer $r = 0$ ise f polinomu $\langle f_1, f_2, \dots, f_s \rangle$ idealinin bir elemanıdır. Ancak, bu durumun tersinin doğru olması gerekmez. Yani, f polinomu $\langle f_1, f_2, \dots, f_s \rangle$ idealinin elemanı olabilir ancak f nin $\{f_1, f_2, \dots, f_s\}$ ile bölümünden kalan sıfır olmayabilir.

Örnek 2.5.9. $f = y^2 x - x \in \mathbb{Q}[x, y]$ polinomu göz önüne alınsın. $f_1 = yx - y, f_2 = y^2 - x \in \mathbb{Q}[x, y]$ olmak üzere $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ olsun. $y > x$ olmak

üzere deglex sıralaması ve Algoritma 2.5.1 kullanılarak $f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$ ve $f \xrightarrow{+} 0$ elde edilir. Gerçekten $f = yf_1 + f_2$ dir ve buradan $f \in I$ olur. Ancak Algoritma 2.5.1 de f_1 ve f_2 nin sırası değiştirilirse (algoritmada önce f_2 kullanılırsa) $f \xrightarrow{f_2} x^2 - x$ olup $x^2 - x$ polinomu $\{f_1, f_2\}$ ye göre indirgenmiştir. Böylece, f nin $\{f_1, f_2\}$ ile bölümünden kalan sıfır olmamasına rağmen f polinomu $\langle f_1, f_2 \rangle$ idealinin bir elemanıdır.

Burada karşılaşılan bu sıkıntılı durum, tek değişkenli polinom halkalarında, daha iyi bir üreteç kümesi olan en büyük ortak bölen bulunarak aşılmıştı. Çok değişkenli polinom halkalarında ise bu sıkıntı Gröbner taban kavramı ile aşılacaktır.

3. MATERYAL VE YÖNTEM

3.1. Gröbner Tabanlar

Tanım 3.1.1. Bir I idealindeki sıfırdan farklı polinomlardan oluşan $G = \{g_1, g_2, \dots, g_s\}$ kümesinin I nin **Gröbner tabanı** olması için gerek ve yeter şart her $0 \neq f \in I$ için $lp(g_i)$ böler $lp(f)$ olacak şekilde $i \in \{1, 2, \dots, s\}$ olmasıdır (Adams and Loustaunau 1994).

Tanım 3.1.2. $S \subseteq F[x_1, x_2, \dots, x_n]$ için

$$Lt(S) = \langle lt(f) \mid f \in S \rangle$$

idealine S nin baş terim ideali denir (Adams and Loustaunau 1994).

Teorem 3.1.3. $F[x_1, x_2, \dots, x_n]$ polinom halkasının sıfırdan farklı bir ideali I ve $G = \{g_1, g_2, \dots, g_s\} \subseteq I$ sıfırdan farklı polinomların bir kümesi olmak üzere aşağıdaki ifadeler denktir.

i) G, I ideali için bir Gröbner tabanıdır.

ii) $f \in I \Leftrightarrow f \xrightarrow{+}_G 0$ olmasıdır.

iii) $f \in I \Leftrightarrow lp(f) = \max_{1 \leq i \leq s} (lp(h_i)lp(g_i))$ olmak üzere $f = \sum_{i=1}^s h_i g_i$ olmasıdır.

iv) $Lt(G) = Lt(I)$ (Dummit and Foote 2003).

İspat: (i) $\Rightarrow$ (ii) G, I ideali için bir Gröbner tabanı ve $f \in F[x_1, x_2, \dots, x_n]$ olsun. Teorem 2.5.8 den $f \xrightarrow{+}_G r$ olacak şekilde G kümesine göre indirgenmiş bir $r \in F[x_1, x_2, \dots, x_n]$ elemanı vardır. Böylece $f - r \in I$ olur. Dolayısıyla $f \in I$ olması için gerek ve yeter şart $r \in I$ olmasıdır. $r = 0$ ise (yani $f \xrightarrow{+}_G 0$) $f \in I$ olduğu açıktır. Tersine $f \in I$ ve $r \neq 0$ ise $r \in I$ ve (i) den $lp(g_i) \mid lp(r)$ olacak şekilde bir $i \in \{1, 2, \dots, s\}$ vardır. Bu ise r polinomunun G kümesine göre indirgenmiş olması ile çelişir. Böylece $r = 0$ olmalıdır. Yani $f \xrightarrow{+}_G 0$ dir.

(ii) $\Rightarrow$ (iii) $f \in I \Leftrightarrow f \xrightarrow{+}_G 0$ olsun. Bu durumda,

$$f \in I \Leftrightarrow f \xrightarrow[+]{G} 0 \underset{\text{Teorem 2.5.8}}{\Leftrightarrow} f = \sum_{i=1}^t h_i g_i, lp(f) = \max_{1 \leq i \leq t} (lp(h_i)lp(g_i))$$

dir.

(iii) $\Rightarrow$ (iv) $G \subseteq I$ olduğundan $Lt(G) \subseteq Lt(I)$ dir. Diğer taraftan her $f \in I$ için $lt(f) \in Lt(G)$ olduğunu göstermek $lt(f)$ ler $Lt(I)$ nin üreteçleri olduğundan ters kapsama için yeterlidir. f polinomu hipotezdeki gibi yazılırsa

$$lt(f) = \sum_i lt(h_i)lt(g_i)$$

dir. Burada toplam $lp(f) = lp(h_i)lp(g_i)$ olan bütün i ler üzerinden hesaplanır. Buradan $lt(f) \in Lt(G)$ olur. Böylece $Lt(I) \subseteq Lt(G)$ olup $Lt(G) = Lt(I)$ bulunur.

(iv) $\Rightarrow$ (i) $f \in I$ ise $lt(f) \in Lt(G)$ dir. Buradan

$$lt(f) = \sum_{i=1}^s h_i lt(g_i), h_i \in F[x_1, x_2, \dots, x_n]$$

olur. Toplam ifadesi açılırsa her bir terimin bazı $lp(g_i)$ ler tarafından bölündüğü görülür. Böylece eşitliğin sol tarafındaki tek terim olan $lp(f)$ de, bazı $lp(g_i)$ ler tarafından bölünür. Dolayısıyla, G kümesi I idealinin bir Gröbner tabanı olur.

Sonuç 3.1.4. $G = \{g_1, g_2, \dots, g_s\}$ kümesi I ideali için bir Gröbner tabanı ise

$$I = \langle g_1, g_2, \dots, g_s \rangle$$

dir (Dummit and Foote 2003).

Lemma 3.1.5. I ideali sıfırdan farklı terimlerin bir S kümesi tarafından üretilmiş ve $f \in F[x_1, x_2, \dots, x_n]$ olsun. $f \in I$ olması için gerekli ve yeterli koşul f polinomundaki her X terimi için $Y|X$ olacak şekilde bir $Y \in S$ var olmasıdır. Ayrıca, $I = \langle S_0 \rangle$ olacak şekilde S kümesinin sonlu bir S_0 alt kümesi vardır (Dummit and Foote 2003).

Sonuç 3.1.6. $F[x_1, x_2, \dots, x_n]$ polinom halkasının sıfırdan farklı her idealin bir Gröbner tabanı vardır (Dummit and Foote 2003).

İspat: Lemma 3.1.5 den $Lt(I)$ baş terim ideali sonlu bir üreteç kümesine sahiptir. $g_1, g_2, \dots, g_s \in I$ olmak üzere bu kümenin $\{lt(g_1), lt(g_2), \dots, lt(g_s)\}$ olduğu varsayalım. $G = \{g_1, g_2, \dots, g_s\}$ ise

$$Lt(G) = Lt(I)$$

dır. Dolayısıyla, Teorem 3.1.3 den G kümesi I ideali için bir Gröbner tabanıdır.

Önerme 3.1.7. $F[x_1, x_2, \dots, x_n]$ polinom halkasının bir $G = \{g_1, g_2, \dots, g_s\}$ alt kümesinin Gröbner tabanı olması için gerek ve yeter şart $\langle G \rangle$ ideali için bir Gröbner tabanı olmasıdır (Adams and Lousaunau 1994).

Teorem 3.1.8. $G = \{g_1, g_2, \dots, g_s\}$ kümesi sıfırdan farklı polinomlardan oluşan $F[x_1, x_2, \dots, x_n]$ nin bir alt kümesi olsun. G nin bir Gröbner tabanı olması için gerek ve yeter şart her $f \in F[x_1, x_2, \dots, x_n]$ için f nin G ye bölümünden kalanın tek olmasıdır (Adams and Lousaunau 1994).

Örnek 3.1.9. $f = xy^2 - x, f_1 = xy - x, f_2 = y^2 - x \in \mathbb{Q}[x, y]$, $R = \{f_1, f_2\}$ ve $x > y$ için deglex sıralaması kullanılarak $f \xrightarrow{R}_+ 0$ ve $f \xrightarrow{R}_+ x^2 - x$ ifadeleri elde edilir. $x^2 - x$ polinomu R kümesine göre indirgenmiş bir polinomdur. Dolayısıyla kalanlar eşit olmadığından $R = \{f_1, f_2\}$ kümesi $\langle f_1, f_2 \rangle$ ideali için bir Gröbner taban değildir.

Örnek 3.1.10. $f_1 = x + z, f_2 = y - x \in \mathbb{Q}[x, y, z]$ polinomları göz önüne alınsın. $R = \{f_1, f_2\}$ ve $I = \langle f_1, f_2 \rangle$ olsun. $\mathbb{Q}[x, y, z]$ üzerinde $z > y > x$ olmak üzere lex sıralamasını kullanarak R polinomlar kümesinin I ideali için bir Gröbner taban olduğu gösterilecektir. $lt(f_1) = z, lt(f_2) = y$ ve $Lt(R) = \langle lt(f_1), lt(f_2) \rangle$ dir. $Lt(R) = Lt(I)$ olduğu gösterilmesi lazım. $Lt(R) \subseteq Lt(I)$ olduğu açıktır. $f \in I$ için herhangi bir $lt(f) \in Lt(I)$ alınsın. $lt(f) \notin Lt(R) = \langle lt(f_1), lt(f_2) \rangle = \langle z, y \rangle$ olacak şekilde bir $f \in I$ olduğu varsayılınsın. O zaman $lt(f)$ ifadesi z ve y değişkenleri tarafından bölünemez. Böylece terim sıralaması lex olduğundan dolayı z ve y değişkenleri f polinomunun hiçbir teriminde gözükmez. Dolayısıyla f , sadece x değişkenine bağlı bir polinom olur. Yani $f \in \mathbb{Q}[x]$ olur. $f \in I = \langle f_1, f_2 \rangle$ olduğundan $\exists h_1(x, y, z), h_2(x, y, z) \in \mathbb{Q}[x, y, z] \ni f = (x + z) \cdot h_1(x, y, z) + (y - x)h_2(x, y, z)$ dir. f polinomunda y değişkeni olmadığından yukarıdaki f polinomu ifadesinde y değişkeni yerine x değişkenini yazmak sorun yaratmaz. Böylece

$$f = (x + z) \cdot h_1(x, x, z) + (x - x)h_2(x, x, z)$$

olur. Buradan

$$f = (x + z) \cdot h_1(x, x, z) \text{ ve } (x + z)|f$$

dir. Bu ifade f polinomunun sadece x değişkenine bağlı olması ile çelişir. Bu $lt(f) \in Lt(I)$ iken $lt(f) \notin Lt(R)$ olmasından kaynaklanır. O halde $Lt(I) \subseteq Lt(R)$ olur. Böylece $Lt(R) = Lt(I)$ dir ve R kümesi I ideali için bir Gröbner tabanıdır.

Örnek 3.1.11. $f_1 = x + z$, $f_2 = y - x \in \mathbb{Q}[x, y, z]$ polinomları göz önüne alınsın. $R = \{f_1, f_2\}$ ve $I = \langle f_1, f_2 \rangle$ olsun. $\mathbb{Q}[x, y, z]$ üzerinde $x > y > z$ olmak üzere lex sıralamasını kullanarak R polinomlar kümesinin I ideali için bir Gröbner taban olmadığı gösterilecektir. $lt(f_1) = x$, $lt(f_2) = -x$ ve $Lt(R) = \langle lt(f_1), lt(f_2) \rangle$ dir. R polinomlar kümesinin I ideali için bir Gröbner taban olmadığını göstermek için $Lt(R) \neq Lt(I)$ olduğunu göstermek lazım. $Lt(R) = Lt(I)$ olduğunu kabul edilsin, dolayısıyla $Lt(R) \subseteq Lt(I)$ olduğu açıktır. $f \in I$ için herhangi bir $lt(f) \in Lt(I)$ alınsın.

$$lt(f) \notin Lt(R) = \langle lt(f_1), lt(f_2) \rangle = \langle x, -x \rangle$$

olacak şekilde bir $f \in I$ olduğu varsayılınsın. O zaman $lt(f)$ ifadesi x değişkeni tarafından bölünemez. Böylece terim sıralaması lex olduğundan dolayı x değişkeni f polinomunun hiçbir teriminde gözükmez. Dolayısıyla f , sadece y, z değişkenlerinden biri ya da ikisine bağlı bir polinom olur. Yani $f \in \mathbb{Q}[y]$, $f \in \mathbb{Q}[z]$ veya $f \in \mathbb{Q}[y, z]$ olur. $f \in I = \langle f_1, f_2 \rangle$ olduğundan

$\exists h_1(x, y, z), h_2(x, y, z) \in \mathbb{Q}[x, y, z] \exists f = (x + z) \cdot h_1(x, y, z) + (y - x)h_2(x, y, z)$ dir. f polinomunda x değişkeni olmadığından yukarıdaki f polinomu ifadesinde x değişkeni yerine y değişkenini yazmak sorun oluşturmaz. Böylece

$$f = (y + z) \cdot h_1(y, y, z) + (y - y)h_2(y, y, z)$$

olur. Buradan

$$f = (y + z) \cdot h_1(x, y, z) \text{ ve } (y + z)|f$$

dir. Bu ifade f polinomunun sadece y, z değişkenlerinden biri ya da ikisine bağlı olmasını doğrular. Bu $lt(f) \in Lt(I)$ iken $lt(f) \notin Lt(R)$ olarak alınmasından kaynaklanır. O halde $Lt(I) \not\subseteq Lt(R)$ olur. Buda $Lt(R) = Lt(I)$ eşitliği ile çelişir. Dolayısıyla $Lt(R) \neq Lt(I)$ olup R kümesi I ideali için bir Gröbner tabanı değildir.

O halde bir terim sıralamasına göre Gröbner taban olan küme farklı bir terim sıralamasına göre Gröbner taban olmayabilir. Bu kısımda sadece Gröbner tabanın varlığı hakkında bilgi verilmiştir. Bir sonraki kısımda ise bu tabanların nasıl bulunacağına değinilecektir.

3.2. S-Polinomları ve Buchberger Algoritması

Tanım 3.2.1. f ve g , $F[x_1, x_2, \dots, x_n]$ de sıfırdan farklı iki polinom ve $L = \text{lcm}(lp(f), lp(g))$ olsun.

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

polinomuna f ve g nın **S-Polinomu** denir (Adams and Loustaunau 1994).

Örnek 3.2.2. $f = 4x^2 - y$, $g = 3y^3 - x \in \mathbb{Q}[x, y]$ ve $y > x$ olmak üzere deglex sıralaması alınsın.

$$lp(f) = x^2, lt(f) = 4x^2, lp(g) = y^3, lt(g) = 3y^3 \text{ ve}$$

$$L = \text{lcm}(lp(f), lp(g)) = \text{lcm}(x^2, y^3) = x^2y^3 \text{ elde edilir.}$$

$$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g = \frac{x^2y^3}{4x^2} (4x^2 - y) - \frac{x^2y^3}{3y^3} (3y^3 - x) = \frac{x^3}{3} - \frac{y^4}{4}$$

olur.

Lemma 3.2.3. $f_1, f_2, \dots, f_s \in F[x_1, x_2, \dots, x_n]$ ve her $i = 1, 2, \dots, s$ için $lp(f_i) = X \neq 0$ olsun. $i = 1, 2, \dots, s$ için $c_i \in F$ olmak üzere $f = \sum_{i=1}^s c_i f_i$ olsun. Eğer $lp(f) < X$ ise f polinomu, katsayıları F cisminde olmak üzere $1 \leq i < j \leq s$ için $S(f_i, f_j)$ polinomlarının bir lineer kombinasyonudur (Adams and Loustaunau 1994).

Teorem 3.2.4. (Buchberger) $G = \{g_1, g_2, \dots, g_t\}$, $F[x_1, x_2, \dots, x_n]$ de sıfırdan farklı polinomlardan oluşan bir küme olsun. G nin I idealinin bir Gröbner tabanı olması için gerek ve yeter şart her $i \neq j$ için

$$S(g_i, g_j) \xrightarrow{+}_G 0$$

olmasıdır (Adams and Loustaunau 1994).

İspat: $\Rightarrow$: $G = \{g_1, g_2, \dots, g_t\}$ kümesi $I = \langle g_1, g_2, \dots, g_t \rangle$ idealinin bir Gröbner tabanı olsun. S-Polinomu tanımından $\forall i \neq j$ için $S(g_i, g_j) \in I = \langle g_1, g_2, \dots, g_t \rangle$ dir. Böylece Teorem 3.1.3 (ii) den $\forall i \neq j$ için $S(g_i, g_j) \xrightarrow{+}_G 0$ olur.

$\Leftarrow$: $\forall i \neq j$ için $S(g_i, g_j) \xrightarrow{+}_G 0$ olsun. G nin $I = \langle g_1, g_2, \dots, g_t \rangle$ için bir Gröbner taban olduğunu göstereceğiz. Bunun için Teorem 3.1.3 kullanılacaktır.

$f \in I$ olsun. O zaman f polinomu g_i polinomlarının bir lineer kombinasyonu olarak yazılabilir.

$$X = \max_{1 \leq i \leq s} (lp(h_i) \cdot lp(g_i))$$

en küçük olacak şekilde

$$f = \sum_{i=1}^t h_i g_i$$

şeklinde yazılsın (burada terim sıralamasının iyi sıralı olma özelliği kullanılmıştır).

$X = lp(f)$ ise Teorem 3.1.3 den G kümesi, $I = \langle g_1, g_2, \dots, g_t \rangle$ için bir Gröbner tabanıdır. Aksi takdirde $lp(f) < X$ dir. f nin X den daha küçük bir terimle temsili bulunacağından bu bir çelişki olacaktır. $S = \{i \mid lp(h_i) \cdot lp(g_i) = X\}$ olsun. $i \in S$ için $h_i = c_i \cdot X_i + \text{"daha küçük terimler"}$ yazılsın.

$$g = \sum_{i \in S} c_i \cdot X_i \cdot g_i$$

olarak ayarlansın. Bu durumda, her $i \in S$ için

$$lp(X_i \cdot g_i) = lp(X_i) \cdot lp(g_i) = lp(h_i) \cdot lp(g_i) = X$$

dir. Fakat $lp(g) < X$ dir. Lemma 3.2.3 den

$$g = \sum_{\substack{i,j \in S \\ i \neq j}} d_{ij} \cdot S(X_i \cdot g_i, X_j \cdot g_j)$$

olacak şekilde $d_{ij} \in F$ vardır. Burada,

$$X = lcm(lp(X_i \cdot g_i), lp(X_j \cdot g_j))$$

dir. Dolayısıyla, $X_{ij} = lcm(lp(g_i), lp(g_j))$ olmak üzere,

$$\begin{aligned}
S(X_i \cdot g_i, X_j \cdot g_j) &= \frac{X}{lt(X_i \cdot g_i)} \cdot X_i \cdot g_i - \frac{X}{lt(X_j \cdot g_j)} \cdot X_j \cdot g_j \\
&= \frac{X}{lt(X_i)lt(g_i)} \cdot X_i \cdot g_i - \frac{X}{lt(X_j)lt(g_j)} \cdot X_j \cdot g_j \\
&= \frac{X}{X_i lt(g_i)} \cdot X_i \cdot g_i - \frac{X}{X_j lt(g_j)} \cdot X_j \cdot g_j \left(\begin{array}{l} lt(X_i) = X_i, lt(X_j) = X_j \\ \text{olduğundan} \end{array} \right) \\
&= \frac{X}{lt(g_i)} \cdot g_i - \frac{X}{lt(g_j)} \cdot g_j \\
&= X \left(\frac{1}{lt(g_i)} \cdot g_i - \frac{1}{lt(g_j)} \cdot g_j \right) \\
&= \frac{X_{ij}X}{X_{ij}} \left(\frac{1}{lt(g_i)} \cdot g_i - \frac{1}{lt(g_j)} \cdot g_j \right) \\
&= \frac{X}{X_{ij}} \left(\frac{X_{ij}}{lt(g_i)} \cdot g_i - \frac{X_{ij}}{lt(g_j)} \cdot g_j \right) \\
&= \frac{X}{X_{ij}} S(g_i, g_j)
\end{aligned}$$

bulunur. Hipotezden,

$$S(g_i, g_j) \xrightarrow{+}_G 0$$

olup $S(X_i \cdot g_i, X_j \cdot g_j) \xrightarrow{+}_G 0$ olur. Bu ifade

$$S(X_i \cdot g_i, X_j \cdot g_j) = \sum_{v=1}^t h_{ijv} \cdot g_v$$

şeklinde gösterilebilir. Burada Teorem 2.5.8 den

$$\begin{aligned}
\max_{1 \leq v \leq t} (lp(h_{ijv}) \cdot lp(g_v)) &= lp(S(X_i \cdot g_i, X_j \cdot g_j)) \\
&< \max(lp(X_i g_i), lp(X_j g_j)) = X
\end{aligned}$$

dir. Bu ifadeler yukarıda g de yerine koyulur ve g de f de yerine yazılırsa

$\max_{1 \leq i \leq t} (lp(h'_i) \cdot lp(g_i)) < X$ olmak üzere

$$f = \sum_{i=1}^t h'_i g_i$$

elde edilir. Bu ise bir çelişkidir.

Sonuç 3.2.5. $G = \{g_1, g_2, \dots, g_t\}$ sıfırdan farklı polinomların bir kümesi olsun. G nin bir Gröbner taban olması için yeter ve gerek şart her $i \neq j$ ($1 \leq i, j \leq t$) için

$$lp(S(g_i, g_j)) = \max_{1 \leq v \leq t} (lp(h_{ijv}) \cdot lp(g_v)) \text{ olmak üzere}$$

$$S(g_i, g_j) = \sum_{v=1}^t h_{ijv} \cdot g_v$$

olmasıdır (Adams and Lousstaunau 1994).

Örnek 3.2.6. $f_1 = xy - x, f_2 = x^2 - y \in \mathbb{Q}[x, y]$ ve $x < y$ olmak üzere terim sıralaması deglex olsun. $R = \{f_1, f_2\}$ olsun. $\langle f_1, f_2 \rangle$ ideali için bir Gröbner taban bulunmaya çalışılsın.

$$lp(f_1) = xy, lp(f_2) = x^2, lt(f_1) = xy, lt(f_2) = x^2$$

$$L = lcm(lp(f_1), lp(f_2)) = (xy, x^2) = x^2y$$

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

$$S(f_1, f_2) = y^2 - x^2 \xrightarrow{+}_R h_1$$

$$y^2 - x^2 \xrightarrow{f_2} h_1 = y^2 - x^2 - \frac{-x^2}{lt(f_2)} \cdot f_2 = y^2 - x^2 - \frac{-x^2}{x^2} \cdot (x^2 - y) = y^2 - y = f_3$$

dir. f_3 polinomu R kümesine göre ve sıfırdan farklıdır. Dolayısıyla R kümesine

eklenir. Yani $R' = \{f_1, f_2, f_3\}$ olur. Bu durumda $S(f_1, f_2) \xrightarrow{+}_{R'} 0$ olur.

$$lp(f_3) = y^2, lt(f_3) = y^2, L = lcm(lp(f_1), lp(f_3)) = (xy, y^2) = xy^2$$

$$S(f_1, f_3) = \frac{L}{lt(f_1)} \cdot f_1 - \frac{L}{lt(f_3)} \cdot f_3 = \frac{xy^2}{xy} \cdot (xy - x) - \frac{xy^2}{y^2} \cdot (y^2 - y) = 0$$

Buradan $S(f_1, f_3) \xrightarrow{R'} 0$ olur. $L = lcm(lp(f_2), lp(f_3)) = (x^2, y^2) = x^2y^2$

$$S(f_2, f_3) = \frac{L}{lt(f_2)} \cdot f_2 - \frac{L}{lt(f_3)} \cdot f_3 = \frac{x^2y^2}{x^2} \cdot (x^2 - y) - \frac{x^2y^2}{y^2} \cdot (y^2 - y) = -y^3 + x^2y$$

$$lp(f_1) = xy, x^2y \text{ yi böler}$$

$$-y^3 + x^2y \xrightarrow{f_1} h_2 = -y^3 + x^2y - \frac{x^2y}{lt(f_1)} \cdot f_1 = -y^3 + x^2y - \frac{x^2y}{xy} (xy - x)$$

$$= -y^3 + x^2$$

$lp(f_2) = x^2, x^2$ yi böler

$$-y^3 + x^2 \xrightarrow{f_2} h_3 = -y^3 + x^2 - \frac{x^2}{lt(f_2)} \cdot f_2 = -y^3 + x^2 - \frac{x^2}{x^2} (x^2 - y) = -y^3 + y$$

$lp(f_3) = y^2, -y^3$ ü böler

$$-y^3 + y \xrightarrow{f_3} h_4 = -y^3 + y - \frac{-y^3}{lt(f_3)} \cdot f_3 = -y^3 + y - \frac{-y^3}{y^2} (y^2 - y) = -y^2 + y$$

$lp(f_3) = y^2, -y^2$ yi böler

$$-y^2 + y \xrightarrow{f_3} h_5 = -y^2 + y - \frac{-y^2}{lt(f_3)} \cdot f_3 = -y^2 + y - \frac{-y^2}{y^2} (y^2 - y) = 0$$

Böylece $S(f_2, f_3) \xrightarrow{R'}_+ 0$ olur. Bütün S-Polinomları sıfıra indirgenmiştir. Dolayısıyla

$R' = \{f_1, f_2, f_3\}$ kümesi $\langle f_1, f_2 \rangle$ ideali için bir Gröbner tabanı olur.

Girdi: $R = \{f_1, f_2, \dots, f_s\} \subseteq F[x_1, x_2, \dots, x_n], f_i = 0 \ (1 \leq i \leq s)$ alınsın.

Çıktı: $G = \{g_1, g_2, \dots, g_t\}, \langle f_1, f_2, \dots, f_s \rangle$ için bir Gröbner tabanı istenmektedir.

1 **Başlat:** $G := R, \mathcal{G} = \{\{f_i, f_j\} \mid f_i \neq f_j, f_i, f_j \in G\}$

2 **Tekrar et:** $\mathcal{G} \neq \emptyset$ olduğu sürece aşağıdaki işlemler yapılır

3 Herhangi bir $\{f, g\} \in \mathcal{G}$ seçilir

4 $\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$

5 $S(f, g) \xrightarrow{G}_+ h$ burada h polinomu G ye göre indirgenmiştir.

6 $h \neq 0$ ise aşağıdaki işlemler yapılır

7 $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid \forall u \in G \text{ için}\}$

8 $G := G \cup \{h\}$

Algoritma 3.2.1. Gröbner Tabanlar İçin Buchberger Algoritması

Teorem 3.2.7. $i = 1, 2, \dots, s$ için $f_i \neq 0$ olmak üzere $R = \{f_1, f_2, \dots, f_s\}$ verilsin. Buchberger Algoritması (Algoritma 3.2.1) $I = \langle f_1, f_2, \dots, f_s \rangle$ ideali için bir Gröbner tabanı üretir (Adams and Loustaunau 1994).

Örnek 3.2.8. $f_1 = y^2 + xy + x^2$, $f_2 = x + y$, $f_3 = y \in \mathbb{Q}[x, y]$ ve $x < y$ olmak üzere terim sıralaması lex olsun. $I = \langle f_1, f_2, f_3 \rangle$ ideali için bir Gröbner tabanı bulunmaya çalışılsın.

Başlat: $G := \{f_1, f_2, f_3\}$ $\mathcal{G} := \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$

1.ADİM: $\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$$[lt(f_1) = y^2, lt(f_2) = y, L = lcm(lp(f_1), lp(f_2)) = lcm(y^2, y) = y^2]$$

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

$$S(f_1, f_2) = x^2 \xrightarrow{+}_G x^2 = h$$

$h \neq 0$ olduğundan $f_4 := x^2$ olsun.

$$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}, G := \{f_1, f_2, f_3, f_4\}$$

2.ADİM: $\mathcal{G} := \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$$[lt(f_1) = y^2, lt(f_3) = y, L_1 = lcm(lp(f_1), lp(f_3)) = lcm(y^2, y) = y^2]$$

$$S(f_1, f_3) = \frac{L_1}{lt(f_1)} f_1 - \frac{L_1}{lt(f_3)} f_3 = \frac{y^2}{y^2} (y^2 + xy + x^2) - \frac{y^2}{y} (y) = yx + x^2$$

$$S(f_1, f_3) = yx + x^2 \xrightarrow{f_2}_G 0, S(f_1, f_3) \xrightarrow{+}_G 0$$

3.ADİM: $\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\},$

$$[L_2 = lcm(lp(f_2), lp(f_3)) = lcm(y, y) = y]$$

$$S(f_2, f_3) = \frac{L_2}{lt(f_2)} f_2 - \frac{L_2}{lt(f_3)} f_3 = \frac{y}{y} (y + x) - \frac{y}{y} (y) = x$$

$$S(f_2, f_3) = x \xrightarrow{+}_G x = h, h \neq 0 \text{ olduğundan } f_5 := x \text{ olsun.}$$

$$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}, G := \{f_1, f_2, f_3, f_4, f_5\}$$

4.ADİM: $\mathcal{G} := \{\{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$$[lt(f_4) = x^2, L_3 = lcm(lp(f_1), lp(f_4)) = lcm(y^2, x^2) = y^2 x^2]$$

$$S(f_1, f_4) = \frac{L_3}{lt(f_1)} f_1 - \frac{L_3}{lt(f_4)} f_4 = \frac{y^2 x^2}{y^2} (y^2 + xy + x^2) - \frac{y^2 x^2}{x^2} (x^2) = yx^3 + x^4$$

$$S(f_1, f_4) = yx^3 + x^4 \xrightarrow{f_2} 0, S(f_1, f_4) \xrightarrow{+}_G 0$$

$$\mathbf{5.ADIM:} \mathcal{G} := \{\{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

$$[L_4 = lcm(lp(f_2), lp(f_4)) = lcm(y, x^2) = yx^2]$$

$$S(f_2, f_4) = \frac{L_4}{lt(f_2)} f_2 - \frac{L_4}{lt(f_4)} f_4 = \frac{yx^2}{y} (y + x) - \frac{yx^2}{x^2} (x^2) = x^3$$

$$S(f_2, f_4) = x^3 \xrightarrow{f_4} 0, S(f_2, f_4) \xrightarrow{+}_G 0$$

$$\mathbf{6.ADIM:} \mathcal{G} := \{\{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

$$[L_5 = lcm(lp(f_3), lp(f_4)) = lcm(y, x^2) = yx^2]$$

$$S(f_3, f_4) = \frac{L_5}{lt(f_3)} f_3 - \frac{L_5}{lt(f_4)} f_4 = \frac{yx^2}{y} (y) - \frac{yx^2}{x^2} (x^2) = 0$$

$$\mathbf{7.ADIM:} \mathcal{G} := \{\{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$$

$$[lt(f_5) = x, L_6 = lcm(lp(f_1), lp(f_5)) = lcm(y^2, x) = y^2x]$$

$$S(f_1, f_5) = \frac{L_6}{lt(f_1)} f_1 - \frac{L_6}{lt(f_5)} f_5 = \frac{y^2x}{y^2} (y^2 + xy + x^2) - \frac{y^2x}{x} (x) = yx^2 + x^3$$

$$S(f_1, f_5) = yx^2 + x^3 \xrightarrow{f_2} 0, S(f_1, f_5) \xrightarrow{+}_G 0$$

$$\mathbf{8.ADIM:} \mathcal{G} := \{\{f_3, f_5\}, \{f_4, f_5\}\}$$

$$[L_7 = lcm(lp(f_2), lp(f_5)) = lcm(y, x) = yx]$$

$$S(f_2, f_5) = \frac{L_7}{lt(f_2)} f_2 - \frac{L_7}{lt(f_5)} f_5 = \frac{yx}{y} (y + x) - \frac{yx}{x} (x) = x^2$$

$$S(f_2, f_5) = x^2 \xrightarrow{f_4} 0, S(f_2, f_5) \xrightarrow{+}_G 0$$

$$\mathbf{9.ADIM:} \mathcal{G} := \{\{f_4, f_5\}\}$$

$$[L_8 = lcm(lp(f_3), lp(f_5)) = lcm(y, x) = yx]$$

$$S(f_3, f_5) = \frac{L_8}{lt(f_3)} f_3 - \frac{L_8}{lt(f_5)} f_5 = \frac{yx}{y} (y) - \frac{yx}{x} (x) = 0$$

$$\mathbf{10.ADIM:} \mathcal{G} := \emptyset$$

$$[L_9 = lcm(lp(f_4), lp(f_5)) = lcm(x^2, x) = x^2]$$

$$S(f_4, f_5) = \frac{L_9}{lt(f_4)} f_4 - \frac{L_9}{lt(f_5)} f_5 = \frac{x^2}{x^2} (x^2) - \frac{x^2}{x} (x) = 0$$

$\mathcal{G} := \emptyset$ olduğundan algoritma tamamlanır. Böylece $G = \{f_1, f_2, f_3, f_4, f_5\}$ kümesi $I = \langle f_1, f_2, f_3 \rangle$ ideali için bir Gröbner tabanıdır.

3.3. İndirgenmiş Gröbner Tabanlar

Önceki konularda Gröbner tabanın olup olmadığını ve nasıl bulunacağını, bulunan Gröbner tabanı için değişkenlerin veya polinomların sırası değiştirildiği zaman Gröbner tabanın değiştiğini ya da bulunamadığı ifade edilmişti. Bu bölümde Gröbner tabanındaki polinomlara belirli koşullar koyarak bu Gröbner tabanının tekliği ifade edilmeye çalışılacaktır.

Tanım 3.3.1. $I, F[x_1, x_2, \dots, x_n]$ polinom halkasının bir ideali ve $G = \{g_1, g_2, \dots, g_s\}$, I ideali için bir Gröbner taban olsun. Eğer her i için $lc(g_i) = 1$ ve her $i \neq j$ için $lp(g_i), lp(g_j)$ yi bölmüyorsa G Gröbner tabanına **minimal Gröbner tabanı** denir (Adams and Loustaunau 1994).

Lemma 3.3.2. $G = \{g_1, g_2, \dots, g_s\}$, I ideali için bir Gröbner taban olsun. Eğer $lp(g_2)$ böler $lp(g_1)$ ise $\{g_2, \dots, g_s\}$ kümesi de I için bir Gröbner tabandır (Adams and Loustaunau 1994).

Sonuç 3.3.3. $G = \{g_1, g_2, \dots, g_s\}$, I ideali için bir Gröbner taban olsun. G polinomlar kümesinden bir minimal Gröbner taban elde etmek için, $j \neq i$ iken $lp(g_j)$ böler $lp(g_i)$ olacak şekildeki bütün g_i ler çıkarılır ve geriye kalan tüm g_i ler $lc(g_i)$ ye bölünür (Adams and Loustaunau 1994).

Tanım 3.3.4. $G = \{g_1, g_2, \dots, g_s\}$ bir Gröbner taban olsun. Her i için $lc(g_i) = 1$ ve g_i polinomu $G - \{g_i\}$ kümesine göre indirgenmiş ise $G = \{g_1, g_2, \dots, g_s\}$ Gröbner tabanına **indirgenmiş Gröbner tabanı** denir. Yani, her i için g_i nin $j \neq i$ iken $lp(g_j)$ ye bölünen sıfırdan farklı bir terimi olmamalıdır (Adams and Loustaunau 1994).

Sonuç 3.3.5. $G = \{g_1, g_2, \dots, g_s\}$, I ideali için bir minimal Gröbner taban olsun. Aşağıdaki indirgeme işlemleri göz önüne alınsın:

$$g_1 \xrightarrow{+}_{H_1} h_1, h_1 \text{ polinomu } H_1 = \{g_2, g_3, \dots, g_s\} \text{ kümesine göre indirgenmiş}$$

$g_2 \xrightarrow[+]{H_2} h_2$, h_2 polinomu $H_2 = \{h_1, g_3, \dots, g_s\}$ kümesine göre indirgenmiş

$g_3 \xrightarrow[+]{H_3} h_3$, h_3 polinomu $H_3 = \{h_1, h_2, g_4, \dots, g_s\}$ kümesine göre indirgenmiş

$\vdots$

$g_s \xrightarrow[+]{H_s} h_s$, h_s polinomu $H_s = \{h_1, h_2, \dots, h_{s-1}\}$ kümesine göre indirgenmiş.

Bu durumda, $H = \{h_1, h_2, \dots, h_s\}$ kümesi I ideali için bir indirgenmiş Gröbner tabanıdır (Adams and Lousaunau 1994).

Teorem 3.3.6 (Buchberger). Belirli bir terim sıralaması alınsın. O zaman sıfırdan farklı her I ideali bu terim sıralamasına göre bir tek indirgenmiş Gröbner tabanına sahiptir (Adams and Lousaunau 1994).

Örnek 3.3.7. Örnek 3.2.8 e tekrar bakalım. Sonuç 3.3.3 e göre $\{f_3, f_5\}$ ve $\{f_2, f_5\}$ kümelerinin her ikisinin $I = \{f_1, f_2, f_3\}$ ideali için bir minimal Gröbner tabanı olduğu görülür. $f_3 = y$ ve $f_5 = x$ olduğundan $\{f_3, f_5\}$, I ideali için bir indirgenmiş Gröbner tabanıdır. $f_2 = y + x$ olduğundan f_5 i kullanarak f_2 polinomu y polinomuna indirgenebilir. O halde

$$y + x \xrightarrow{f_5} y + x - \frac{x}{x}(x) = y$$

olup $\{f_2, f_5\}$ kümesi indirgenmiş Gröbner taban değildir. İndirgenmiş Gröbner tabanı tek olduğundan $\{f_2, f_5\}$ kümesinden elde edilen Gröbner tabanı $\{f_3, f_5\}$ kümesidir.

4. ARAŞTIRMA BULGULARI

4.1. Modüller

Bu kısımda A değişmeli bir halka ve $A^t = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix} \mid a_i \in A, i = 1, 2, \dots, t \right\}$ de A

kümesinin t . dereceden kartezyen çarpımı olsun. Buradaki $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix}$ sütun vektörleri sadelik olması açısından $(a_1, a_2, \dots, a_t)$ şeklinde yazılacaktır.

Tanım 4.1.1. M toplamsal değişmeli bir grup olmak üzere eğer M nin elemanlarının A nın elemanları ile çarpımı (skaler çarpım) aşağıdaki şartları sağlıyorsa M ye bir A -modül denir (Adams and Loustaunau 1994).

$$i) \forall x \in A \text{ ve } \forall m \in M \text{ için } x \cdot m \in M$$

$$ii) \forall x \in A \text{ ve } \forall m, m' \in M \text{ için } x(m + m') = x \cdot m + x \cdot m'$$

$$iii) \forall x, x' \in A \text{ ve } \forall m \in M \text{ için } (x + x') \cdot m = x \cdot m + x' \cdot m$$

$$iv) \forall x, x' \in A \text{ ve } \forall m \in M \text{ için } x \cdot (x' \cdot m) = (x \cdot x')m$$

$$v) \forall m \in M \text{ için } 1 \cdot m = m$$

Tanım 4.1.2. $x \in A$ ve $(a_1, a_2, \dots, a_t) \in A^t$ olmak üzere

$$x \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} xa_1 \\ xa_2 \\ \vdots \\ xa_t \end{bmatrix} \text{ ya da } x(a_1, a_2, \dots, a_t) = (xa_1, xa_2, \dots, xa_t)$$

ifadesine A^t de skaler çarpımı denir. A^t modülü, bir tabana yani lineer bağımsız vektörlerden oluşan bir üreteç kümesine sahip olduğu için serbest modül olarak adlandırılır (Adams and Loustaunau 1994).

Örneğin;

$$e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0), \dots, e_t = (0, 0, \dots, 1)$$

vektörleri A^t modülü için standart tabandır.

Tanım 4.1.3. M bir A -modül olsun. M nin herhangi bir S alt kümesi M deki işlemlere göre kendi başına bir A -modül oluyorsa S ye M nin bir alt modülü denir. Örneğin, eğer $a_1, a_2, \dots, a_s$ ler A^t de vektörler iseler

$$M = \{b_1 a_1 + b_2 a_2 + \dots + b_s a_s \mid b_i \in A, i = 1, 2, \dots, s\} \subseteq A^t$$

kümesi A^t nin bir alt modülüdür. Bu alt modül $\langle a_1, a_2, \dots, a_s \rangle \subseteq A^t$ şeklinde gösterilir ve $\{a_1, a_2, \dots, a_s\}$ kümesi M nin üreteç kümesi olarak adlandırılır (Adams and Loustaunau 1994).

Tanım 4.1.4. $M = \langle a_1, a_2, \dots, a_s \rangle \subseteq A^t$ olsun. Eğer a_i vektörlerini bir $m \times s$ S matrisinin sütunları olarak düşünülürse, M matrisine S nin sütun uzayı denir (Adams and Loustaunau 1994). Yani;

$$M = \left\{ Sb \mid b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{bmatrix} \in A^s \right\}$$

olup verilen bir $a \in A^t$ için,

$$Sb = a \tag{4.1.1}$$

matris denklemiyle belirlenen t lineer denklem sistemi ($b \in A^s$ nin koordinatları olan bilinmeyenlerle birlikte) a vektörünün M de olup olmadığı sorusuna dönüştürülebilir.

$t = 1$ olması durumunda, yani M nin A nın bir ideali ve (4.1.1) denkleminin sadece bir denkleme sahip olması halinde bu problem “İdeal ait olma problemi” dir. A^t deki diğer lineer cebir problemleri de bu yolla modül teorik sorulara dönüştürülebilir. Bu bölümde bu sorulara $A = F[x_1, x_2, \dots, x_n]$ durumunda cevap verebilmek için bazı algoritmalar bahsedilecektir.

İlk olarak genel modül teorisi ile ilgili bazı konulara değinilecektir. Esasen Hilbert Taban Teoreminden (Teorem 2.1.28) Noetherian halkası olduğu bilinen $F[x_1, x_2, \dots, x_n]$ ile ilgilenildiği göz önüne alındığında A halkasının Noetherian olduğu kabul edilecektir.

Teorem 4.1.5. A^t nın her bir M alt modülü sonlu bir üreteç kümesine sahiptir (Adams and Loustaunau 1994).

Tanım 4.1.6. Bir M A –modülünün Noetherian olarak adlandırılması için gerek ve yeter şart M nin her bir alt modülünün sonlu üretilmiş olmasıdır (Adams and Loustaunau 1994).

Eğer A bir Noetherian halka ise Teorem 4.1.5 ten her $t \geq 1$ için A^t bir Noetherian modüldür. Ayrıca, A^t nin her alt modülü de yine bir Noetherian modüldür.

M bir A –modül ve N de M nin bir alt modülü olsun.

$$M/N = \{m + N | m \in M\}$$

şeklinde tanımlansın. M/N kümesi yan kümelerin bilinen toplama işlemine göre değişmeli bölüm grubudur. M/N grubu her $x \in A$ ve her $m \in M$ için;

$$x \cdot (m + N) = xm + N$$

işlemine göre bir A -modüldür. Bu M/N modülü M nin N ile bölüm modülü olarak adlandırılır.

Tanım 4.1.7. M ve M' iki A –modül olsun. $\phi: M \rightarrow M'$ fonksiyonu aşağıdaki şartları sağlıyorsa A -modül homomorfizmi olarak adlandırılır (Adams and Loustaunau 1994).

$$i) \forall m, m' \in M \text{ için } \phi(m + m') = \phi(m) + \phi(m')$$

$$ii) \forall x \in A \text{ ve } \forall m \in M \text{ için } x\phi(m) = \phi(xm) \text{ dir.}$$

Tanım 4.1.8. $\phi: M \rightarrow M'$ modül homomorfizması $1 - 1$ ve örten ise ϕ fonksiyonuna **izomorfizmi** denir ve $M \cong M'$ şeklinde gösterilir (Adams and Loustaunau 1994).

Tanım 4.1.9. $\phi: M \rightarrow M'$ modül homomorfizma ise ϕ nin **çekirdeği**

$$N = \text{Çek}(\phi) = \{m \in M | \phi(m) = 0\}$$

ile tanımlanır (Adams and Loustaunau 1994). Burada N , M modülünün $\phi(M)$ de M' modülünün birer alt modülüdür. Abelyan grup teorisinden,

$$M/N \rightarrow \phi(M)$$

$$m + N \rightarrow \phi(m)$$

dönüşümü altında $M/N \cong \phi(M)$ olduğu bilinmektedir. Bu dönüşüm aslında bir A –modül izomorfizmidir. Bu durum modüller için Birinci İzomorfizm Teoremi olarak bilinir.

Abelyan grup teorisinde olduğu gibi M/N nin alt modülleri L , M nin N yi içeren alt modülü olmak üzere L/N şeklindedir.

Lemma 4.1.10. Her sonlu üretilmiş M A –modülü, herhangi bir s pozitif tamsayısı ve A^s nin herhangi bir N alt modülü için A^s/N ye izomorftur (Adams and Lousaunau 1994).

Tanım 4.1.11. Eğer $M \cong A^s/N$ ise A^s/N ye M nin bir takdimi denir (Adams and Lousaunau 1994).

Sonuç 4.1.12. Her sonlu üretilmiş A –modül M , Noetherian modüldür (Adams and Lousaunau 1994).

4.2. Modüller İçin Gröbner Tabanlar

F bir cisim olmak üzere $A = F[x_1, x_2, \dots, x_n]$ olsun. Bu kısımda Gröbner tabanlarının A^t nin alt modüllerine genelleştirilmesi hakkında bazı bilgiler verilecektir.

$$e_1 = (1, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_t = (0, 0, \dots, 0, 1)$$

A^t nin standart tabanı olsun. Bu durumda, A^t deki bir monomiyal olarak X , A da bir kuvvet çarpımı olmak üzere Xe_i ($1 \leq i \leq t$) tipindeki bir vektör anlaşılabacaktır. Yani monomiyal, A nın bir kuvvet çarpımı olan bir girdisi hariç diğer girdileri sıfır olan bir sütun vektörüdür. A^t deki monomiyallar A halkasındaki kuvvet çarpımı kavramının yerine kullanılacaktır. Böylece örneğin, $(0, x_1^2 x_3, 0)$ ve $(0, 0, x_2)$ A^3 de monomiyaldir. Fakat $(0, x_1 + x_2, 0)$ ve $(0, x_2, x_1)$ monomiyal değildir. Eğer $X = Xe_i$ ve $Y = Ye_j$ A^t de monomiyal iseler, $i = j$ ve X böler Y ise X böler Y denir. Böylece, A^3 de $(0, x_1^2 x_3, 0)$, $(0, x_1^2 x_3^3, 0)$ ı böler fakat $(0, x_1 x_3, 0)$ veya $(x_1^2 x_3^3, 0, 0)$ ı bölmez. Eğer, X böler Y ise $Y = ZX$ olacak şekilde A halkasında Z kuvvet çarpımı vardır. Bu durumda

$$\frac{Y}{X} = \frac{Y}{X} = Z$$

olarak tanımlanır. Böylece, örneğin

$$\frac{(0, x_1^2 x_3^2, 0)}{(0, x_1^2 x_3, 0)} = \frac{x_1^2 x_3^2}{x_1^2 x_3} = x_3$$

yazılabilir.

Benzer şekilde, $c \in F - \{0\}$ ve X bir monomiyal olmak üzere cX tipindeki bir vektör terim olarak adlandırılacaktır. Böylece $X = (0, x_1^2 x_3^4, 0, 0) = x_1^2 x_3^4 e_2$ olmak üzere $(0, 5x_1^2 x_3^4, 0, 0) = 5X$, A^4 de bir terimdir fakat bir monomiyal değildir. Ayrıca eğer $X = cX e_i$ ve $Y = dY e_j$, A^t nin terimleri ise $i = j$ ve X böler Y ise X böler Y denir.

$$\frac{Y}{X} = \frac{dY}{cX}$$

şeklinde yazılır. Böylece örneğin,

$$\frac{(0, 5x_1^2 x_3^2, 0)}{(0, 2x_1^2 x_3, 0)} = \frac{5x_1^2 x_3^2}{2x_1^2 x_3} = \frac{5}{2} x_3$$

yazılabilir.

Şimdi A^t nin monomiyalları üzerinde terim sıralamasının nasıl tanımlandığı hakkında bazı bilgiler verilecektir.

Tanım 4.2.1. A^t nin monomiyalleri üzerinde aşağıdaki şartları sağlayan $<$ tam sıralamasına bir terim sıralaması denir (Adams and Loustaunau 1994).

i) A^t nin her X monomiyali ve A nın her $Z \neq 1$ kuvvet çarpımı için $X < ZX$ dir.

ii) $\forall X, Y \in A^t$ ve $\forall Z \in A$ kuvvet çarpımı için eğer $X < Y$ ise $ZX < ZY$ dir.

Eğer A üzerinde bir terim sırası verilirse, A^t üzerinde terim sıralaması oluşturmanın iki doğal yolu vardır. Bunlar aşağıdaki tanımlarda verilmiştir.

Tanım 4.2.2. A^t nin $X = X e_i$ ve $Y = Y e_j$ monomiyalları için,

$$X < Y \Leftrightarrow \begin{cases} X < Y \\ \text{veya} \\ X = Y \text{ ve } i < j \end{cases}$$

olduğu söylenebilir. Bu sıralama, A üzerindeki terim sıralaması vektördeki pozisyonundan daha önemli olduğu için “terim pozisyonundan önce” sıralaması olarak adlandırılacak ve kısaca TPÖ ile gösterilecektir (Adams and Lousaunau 1994).

Böylece, örneğin iki değişken ve $m = 2$ durumunda A nın kuvvet çarpımları üzerinde $x < y$ olmak üzere deglex sıralaması kullanılırsa,

$$(x, 0) < (0, x) < (y, 0) < (xy, 0)$$

olduğu görülür.

Tanım 4.2.3. A^t nin $X = Xe_i$ ve $Y = Ye_j$ monomiyalları için

$$X < Y \Leftrightarrow \begin{cases} i < j \\ \text{veya} \\ i = j \text{ ve } X < Y \end{cases}$$

olduğu söylenebilir. Bu sıralama, vektördeki pozisyon A daki terim sıralamasından daha önemli olduğu için “pozisyon terimden önce” sıralaması olarak adlandırılacak ve kısaca PTÖ ile gösterilecektir (Adams and Lousaunau 1994).

Böylece, yine örneğin iki değişken ve $m = 2$ durumunda A nın kuvvet çarpımları üzerinde $x < y$ olmak üzere deglex sıralaması kullanılırsa,

$$(x, 0) < (y, 0) < (xy, 0) < (0, x)$$

dir.

Elbette bu iki sıralamanın her biri $\{1, 2, \dots, t\}$ alt indislerinin farklı bir sıralaması ile de tanımlanmış olabilir. Hangi sıralamanın kullanıldığını göstermek için örneğin $e_1 < e_2 < \dots < e_t$ yazılacaktır.

“ $<$ ” sembolü hem A daki kuvvet çarpımları üzerindeki terim sıralamasında hem de A^t deki monomiyallerin terim sıralamasında kullanılmaktadır. Hangi sıralama için kullanıldığı metinden açık olarak anlaşılabilmektedir.

Lemma 4.2.4. A^t nin monomiyalleri üzerindeki her terim sıralaması bir iyi sıralamadır (Adams and Lousaunau 1994).

Aşağıda önceki bölümlerle adaptasyonu sağlayacak şekilde bazı notasyonlar verilecektir.

İlk olarak A^t deki monomiyaller üzerinde sabit bir “<” terim sıralaması alınsın. Bu durumda, $f \neq 0$ olan her $f \in A^t$ için $1 \leq i \leq r, 0 \neq a_i \in F$ olmak üzere

$$f = a_1 X_1 + a_2 X_2 + \cdots + a_r X_r$$

yazılabilir. Burada $X_i, X_1 > X_2 > \cdots > X_r$ yi sağlayan A^t de bir monomiyaldir.

- $lm(f) = X_1, f$ nin baş monomiyali.
- $lc(f) = a_1, f$ nin baş katsayısı.
- $lt(f) = a_1 X_1, f$ nin baş terimi

şeklinde tanımlanır. Ayrıca, $lt(0) = 0, lm(0) = 0, lc(0) = 0$ olarak kabul edilir.

A daki kuvvetler çarpımı yerine A^t deki monomiyaller kullanıldığından tutarlılık olması için baş kuvvet çarpımları yerine baş monomiyaller kullanılacak olup “lp” yerine “lm” sembolü kullanılacaktır.

Örnek 4.2.5. $x < y$ olmak üzere $A = \mathbb{Q}[x, y]$ üzerinde lex sıralaması alınsın. $f = (2x^3y - y^3 + 5x, 3xy^2 + 4x + y^2) \in A^2$ olsun. Bu durumda yukarıdaki Tanım 4.2.2 nin $e_1 < e_2$ olmak üzere TPÖ sıralamasında

$$f = -y^3e_1 + 3xy^2e_2 + y^2e_2 + 2x^3ye_1 + 4xe_2 + 5xe_1$$

ifadesini elde edilir. Böylece $lm(f) = y^3e_1, lc(f) = -1$ ve $lt(f) = -y^3e_1$ dir. Diğer taraftan yukarıda Tanım 4.2.3 ün $e_1 < e_2$ olmak üzere PTÖ sıralamasında

$$f = 3xy^2e_2 + y^2e_2 + 4xe_2 - y^3e_1 + 2x^3ye_1 + 5xe_1$$

ifadesi elde edilir. Böylece $lm(f) = xy^2e_2, lc(f) = 3$ ve $lt(f) = 3xy^2e_2$ olur.

Şimdi modüller için Gröbner taban inşasında ikinci bileşen olan indirgeme ve Bölme Algoritması ile ilgilenilecektir. Algoritmanın arkasındaki ana fikir polinomlar için olanla aynıdır: f yi $f_1, f_2, \dots, f_s$ ile bölerken f nin monomiyalleri f_i lerin baş terimleri kullanılarak indirgenir ve bu işlem indirgeme yapılamayana kadar devam ettirilir.

Tanım 4.2.6. A^t de verilen f, g, h ($g \neq 0$) için f nin h ya modülo g ye göre tek adımda indirgenmesi için gerek ve yeter şart $lt(g)$ nin f deki bir X terimini bölmesi ve $h = f - \frac{X}{lt(g)}g$ olmasıdır. Bu durum,

$$f \xrightarrow{g} h$$

şeklinde gösterilir (Adams and Lousaunau 1994).

h , Bölüm 2.5 de olduğu gibi f 'nin g ile tek adım bölmesinin kalanı olarak düşünülebilir. f den $\frac{x}{lt(g)}g$ çıkarılarak elde edilen terimler f den çıkarılan X teriminden daha küçüktür. Bu işlem devam ettirilir ve f deki $lt(g)$ ile bölünebilen bütün terimler çıkarılır.

Örnek 4.2.7. $f = (-y^3 + 2x^3y, 3xy^2 + y^2 + 4x)$ ve $g = (x + 1, y^2 + x)$ A^2 nin elemanları olsun. A^2 de $e_1 < e_2$ ile TPÖ ve $x < y$ ile $A = \mathbb{Q}[x, y]$ da lex sıralaması kullanılsın. Bu durumda, $lt(g) = (0, y^2) = y^2e_2$ ve

$$\begin{aligned} f &\xrightarrow{g} (-y^3 + 2x^3y - 3x^2 - 3x, y^2 - 3x^2 + 4x) \\ &\xrightarrow{g} (-y^3 + 2x^3y - 3x^2 - 4x - 1, -3x^2 + 3x) \end{aligned}$$

dir..

Tanım 4.2.8. $f_1, f_2, \dots, f_s$ polinomları sıfırdan farklı olmak üzere f, h ve $f_1, f_2, \dots, f_s$, A^t de birer vektör ve $R = \{f_1, f_2, \dots, f_s\}$ olsun. f nin modülo R ye göre h ya indirgenmesi için gerek ve yeter şart

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots \xrightarrow{f_{i_{p-1}}} h_{p-1} \xrightarrow{f_{i_p}} h$$

olacak şekilde $i_1, i_2, \dots, i_p \in \{1, 2, \dots, s\}$ indislerinin bir dizisi ve $h_1, h_2, \dots, h_{p-1} \in A^t$ vektörlerinin mevcut olmasıdır. Bu durum

$$f \xrightarrow[+]{R} h$$

şeklinde gösterilir (Adams and Lousaunau 1994).

Örnek 4.2.9. $f_1 = (xy - y, x^2), f_2 = (x, y^2 - x) \in A^2$ olsun. A^2 de $e_1 < e_2$ ile TPÖ ve $A = \mathbb{Q}[x, y]$ da $x < y$ ile lex sıralaması kullanılsın. $R = \{f_1, f_2\}$ ve $f = (y^2 + 2x^2y, y^2)$ olsun. Bu durumda,

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

$$\xrightarrow{f_1} (y^2 + 2y - x, -2x^3 - 2x^2 + x)$$

olduğundan

$$f \xrightarrow{+R} (y^2 + 2y - x, -2x^3 - 2x^2 + x)$$

dır. Burada, son vektör olan $h = (y^2 + 2y - x, -2x^3 - 2x^2 + x)$, f_1 ya da f_2 ile daha fazla indirgenemezdir. Çünkü, $lm(f_1) = (xy, 0)$ ve h nin ilk koordinatındaki hiçbir kuvvet çarpımı xy ile bölünemez ve $lm(f_2) = (0, y^2)$ ve h 'nin ikinci koordinatındaki hiçbir kuvvet çarpımı y^2 ile bölünemezdir.

Tanım 4.2.10. r, A^t de bir vektör ve $R = \{f_1, f_2, \dots, f_s\}$ olsun. Eğer $r = 0$ ya da r deki monomiyallerin hiçbiri $i = 1, 2, \dots, s$ için $lm(f_i)$ lerin herhangi biri tarafından bölünmüyorsa r ye R kümesine göre indirgenmiştir denir. Eğer $f \xrightarrow{+R} r$ ve r vektörü R kümesine göre indirgenmiş ise r ye f için R ye göre bir kalan denir (Adams and Lousaunau 1994).

İndirgeme işlemi polinomlar için Bölünme Algoritmasına benzer bir Bölme Algoritması tanımlanmasına imkan verir. Verilen $f, f_1, f_2, \dots, f_s \in A^t$ ($f_1, f_2, \dots, f_s \neq 0$) elemanları için bu algoritma

$$f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r$$

olacak şekilde $a_1, a_2, \dots, a_s \in A = F[x_1, x_2, \dots, x_n]$ bölümlerini ve R ye göre indirgenmiş $r \in A^t$ kalanını geri döndürür. Bu algoritma, Algoritma 4.2.1 olarak verilmiştir.

Girdi: $f, f_1, f_2, \dots, f_s \in A^t$ ile $f_i \neq 0$ ($1 \leq i \leq s$)

Çıktı: $a_1, a_2, \dots, a_s \in A, r \in A^t$ (burada $f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r$ ve $r, \{f_1, f_2, \dots, f_s\}$ ye göre indirgenmiş ve $\max(lp(a_1)lm(f_1), \dots, lp(a_s)lm(f_s), lm(r)) = lm(f)$ dir).

1 **Başlat:** $a_1 := 0, a_2 := 0, \dots, a_s = 0, r := 0, g := f$

2 **Tekrar et:** $g \neq 0$ iken

3 **Eğer** $lm(f_i)$ böler $lm(g)$ olacak şekilde bir i varsa

4 $lm(f_i)$ böler $lm(g)$ olacak şekildeki en küçük i seçilsin.

$$5 \quad a_i := a_i + \frac{lt(g)}{lt(f_i)}$$

$$6 \quad g := g - \frac{lt(g)}{lt(f_i)} f_i$$

7 **Aksi halde**

$$8 \quad r := r + lt(g)$$

$$9 \quad g := g - lt(g)$$

Algoritma 4.2.1. A^t de Bölme Algoritması

Örnek 4.2.11. Algoritma 4.2.1 doğrultusunda adım adım ilerleyerek Örnek 4.2.9 tekrar ele alınmış olsun.

Başlat: $a_1 := 0, a_2 := 0, r := 0, g := (y^2 + 2x^2y, y^2)$

1.ADIM: $(xy, 0) = lm(f_1), lm(g) = (0, y^2)$ yi bölmez.

$(0, y^2) = lm(f_2), lm(g) = (0, y^2)$ yi böler.

$$a_2 := a_2 + \frac{lt(g)}{lt(f_2)} = 1$$

$$\begin{aligned} g &:= g - \frac{lt(g)}{lt(f_2)} f_2 = (y^2 + 2x^2y, y^2) - \frac{(0, y^2)}{(0, y^2)} (x, y^2 - x) \\ &= (y^2 + 2x^2y - x, x) \end{aligned}$$

2.ADIM: Ne $lm(f_1)$ ne de $lm(f_2), lm(g) = (y^2, 0)$ 'ı böler.

$$r := r + lt(g) = (y^2, 0)$$

$$g := g - lt(g) = (2x^2y - x, x)$$

3.ADIM: $(xy, 0) = lm(f_1), lm(g) = (x^2y, 0)$ 'ı böler

$$a_1 := a_1 + \frac{lt(g)}{lt(f_1)} = 2x$$

$$g := (2x^2y - x, x) - \frac{(2x^2y, 0)}{(xy, 0)} (xy - y, x^2) = (2xy - x, -2x^3 + x)$$

4.ADIM: $(xy, 0) = lm(f_1), lm(g) = (xy, 0)$ 'ı böler.

$$a_1 := a_1 + \frac{lt(g)}{lt(f_1)} = 2x + 2$$

$$\begin{aligned}
g &:= (2xy - x, -2x^3 + x) - \frac{(2x^2y, 0)}{(xy, 0)}(xy - y, x^2) \\
&= (2y - x, -2x^3 - 2x^2 + x)
\end{aligned}$$

5.ADIM: Ne $lm(f_1)$ ne de $lm(f_2)$, $lm(g) = (y, 0)$ 'ı böler.

$$r := r + lt(g) = (y^2 + 2y, 0)$$

$$g := g - lt(g) = (-x, -2x^3 - 2x^2 + x)$$

dir. Hem $lm(f_1)$ hem de $lm(f_2)$ g nin geri kalan terimlerini bölmediği için Tekrar et döngüsünün kalan dört adımı son adımla benzerdir. Sonuç olarak, Örnek 4.2.9 da yapıldığı gibi

$$f \xrightarrow{+} (y^2 + 2y - x, -2x^3 - 2x^2 + x) = r$$

ve dahası

$$f = (2x + 2) f_1 + f_2 + r$$

elde edilir.

Teorem 4.2.12. Verilen sıfırdan farklı vektörlerin kümesi $R = \{f_1, f_2, \dots, f_s\}$ ve A^t deki f elemanı için, Bölme Algoritması (Algoritma 4.2.1)

$$f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r$$

olacak şekilde $a_1, a_2, \dots, a_s \in A$ polinomları ve $r \in A^t$ vektörü üretecektir. Burada r vektörü R ye göre indirgenmiş ve

$$lm(f) = \max(lp(a_1)lm(f_1), lp(a_2)lm(f_2), \dots, lp(a_s)lm(f_s), lm(r))$$

dir (Adams and Lousaunau 1994).

Buraya kadar modüllerde Gröbner tabanı tanımlamaya ihtiyaç duyulan temel bilgiler verilmiştir. Şimdi modüllerde Gröbner taban kavramı tanımlanabilir. M, A^t nin bir alt modülü olsun.

Tanım 4.2.13. M alt modülü tarafından kapsanan sıfırdan farklı vektörlerin kümesi $G = \{g_1, g_2, \dots, g_t\}$ nin M nin bir Gröbner tabanı olması için gerek ve yeter şart her $f \in M$ için $lm(g_i)$ böler $lm(f)$ olacak şekilde $i \in \{1, 2, \dots, t\}$ nin mevcut olmasıdır.

Eğer G kümesi $\langle G \rangle$ alt modülü için bir Gröbner taban oluyorsa G ye bir Gröbner taban denir (Adams and Lousaunau 1994).

Şimdi Teorem 3.1.3 ve Teorem 3.1.8 dekine benzer şekilde Gröbner tabanın karakterizasyonu verilecektir. İlk olarak A^t nin bir W alt kümesi için A^t nin bir alt modülü olarak W nin baş terim modülü

$$Lt(W) = \langle lt(w) \mid w \in W \rangle \subseteq A^t$$

şeklinde tanımlansın.

Teorem 4.2.14. Aşağıdaki durumlar $M \subseteq A^t$ alt modülü ve $g_i \neq 0$ ($1 \leq i \leq t$) olmak üzere $G = \{g_1, g_2, \dots, g_t\} \subseteq M$ için denktir.

i) Her $f \in M$ için, $lm(g_i)$ böler $lm(f)$ olacak şekilde i vardır. (yani G, M için bir Gröbner tabandır).

ii) $f \in M$ olması için gerek ve yeter şart $f \xrightarrow{+}_G 0$ olmasıdır.

iii) $\forall f \in M$ için, $f = h_1 g_1 + h_2 g_2 + \dots + h_t g_t$ ve

$lm(f) = \max_{1 \leq i \leq t} (lp(h_i) lm(g_i))$ olacak şekilde $h_1, h_2, \dots, h_t \in A$ vardır.

iv) $Lt(G) = Lt(M)$ dir.

v) $\forall f \in A^t$ için, eğer $f \xrightarrow{+}_G r_1, f \xrightarrow{+}_G r_2$ ve r_1, r_2 G ye göre indirgenmiş ise $r_1 = r_2$ dir (Adams and Lousaunau 1994).

Sonuç 4.2.15. Eğer $G = \{g_1, g_2, \dots, g_t\}$ kümesi A^t nin M alt modülü için bir Gröbner taban ise $M = \langle g_1, g_2, \dots, g_t \rangle$ dir (Adams and Lousaunau 1994).

Sonuç 4.2.16. A^t nin sıfırdan farklı her M alt modülü bir Gröbner tabana sahiptir (Adams and Lousaunau 1994).

Şimdi S-Polinomlarının ele alınan modüllerdeki karşılıkları hakkında bazı bilgiler verilecektir. İki monomiyalin en küçük ortak katının ne olması gerektiği henüz açık olmamakla birlikte polinom durumda yapılanların kopyalanması yeterlidir. Dolayısıyla, $X = X e_i$ ve $Y = Y e_j$, A^t de iki monomiyal olsun. Bu durumda, X ve Y nin en küçük ortak katı ($lcm(X, Y)$ ile gösterilir) olarak

- $0, i \neq j$ ise

- $Le_i, i = j$ ise ($L = lcm(X, Y)$)

anlaşılacaktır.

Örneğin; $lcm((x^2yz, 0), (xy^3, 0)) = (x^2y^3z, 0)$ ve $lcm((x^2y, 0), (0, xy^3)) = (0, 0)$ dır.

Tanım 4.2.17. $0 \neq f, g \in A^t$ ve $L = lcm(lm(f), lm(g))$ olsun.

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

vektörü, f ve g nin S-Polinomu olarak adlandırılır (Adams and Loustaunau 1994).

Bu tanım, Tanım 3.2.1 deki S-Polinom tanımıyla benzerdir. Yani baş monomiyallerin indirgendiği f ve g nin lineer kombinasyonu kullanılmaktadır. Eğer $lm(f)$ ve $lm(g)$ nin sıfırdan farklı kendi bileşenleri farklı koordinatlarda iseler en küçük ortak katları sıfır vektör olacağından S-polinomları da sıfır olur. Diğer taraftan, eğer $lm(f)$ ve $lm(g)$ nin sıfırdan farklı kendi bileşenleri aynı koordinatlarda iseler $S(f, g)$ polinomu baş monomiyalleri indirgemek için en etkili şekilde oluşturulur.

Örnek 4.2.18. A^2 üzerinde $e_1 < e_2$ olmak üzere TPÖ sıralaması ve $A = \mathbb{Q}[x, y]$ üzerinde $x < y$ olmak üzere deglex sıralaması göz önüne alınsın. Bu durumda,

$$\begin{aligned} S((x^2 + 1, 5xy^3 + x), (x^2y, 3x^3y + y)) \\ &= \frac{(0, x^3y^3)}{(0, 5xy^3)}(x^2 + 1, 5xy^3 + x) - \frac{(0, x^3y^3)}{(0, 3x^3y)}(x^2y, 3x^3y + y) \\ &= \frac{x^2}{5}(x^2 + 1, 5xy^3 + x) - \frac{y^2}{3}(x^2y, 3x^3y + y) \\ &= (\frac{1}{5}x^4 + \frac{1}{5}x^2 - \frac{1}{3}x^2y^3, \frac{1}{5}x^3 - \frac{1}{3}y^3) \end{aligned}$$

olur. Burada S-polinomunun baş monomiyali $(x^2y^3, 0) < (0, x^3y^3)$ olmasına rağmen her bir toplam bileşenin baş monomiyali $(0, x^3y^3)$ dir.

Teorem 4.2.19. $G = \{g_1, g_2, \dots, g_t\}$, A^t de sıfırdan farklı vektörlerin bir kümesi olsun. Bu durumda, G kümesinin A^t nin alt modülü olan M nin bir Gröbner tabanı olması için gerek ve yeter şart her $i \neq j$ için

$$S(g_i, g_j) \xrightarrow{+}_G 0$$

olmasıdır (Adams and Lousaunau 1994).

Bu son teorem Gröbner taban hesaplamak için dizayn edilen Buchberger Algoritmasının (Algoritma 3.2.1) benzeri bir algoritmanın oluşturulmasını sağlar. Bu algoritma Algoritma 4.2.2 olarak verilecektir. Aslında bu algoritma Algoritma 3.2.1 ile aynıdır.

Girdi: $R = \{f_1, f_2, \dots, f_s\} \subseteq A^t$, burada $f_i \neq 0$ ($1 \leq i \leq s$) dir.

Çıktı: $G = \{g_1, g_2, \dots, g_t\}, \langle f_1, f_2, \dots, f_s \rangle$ için bir Gröbner taban.

```

1  Başlat:  $G := R, \mathcal{G} = \{\{f_i, f_j\} \mid f_i \neq f_j, f_i, f_j \in G\}$ 
2  Tekrar et:  $\mathcal{G} \neq \emptyset$  iken
3      Herhangi bir  $\{f, g\} \in \mathcal{G}$  seç
4       $\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$ 
5       $S(f, g) \xrightarrow{+}_G h$ , burada  $h$   $G$  ye göre indirgenmiştir.
6      Eğer  $h \neq 0$  ise
7           $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid \text{her } u \in G \text{ için}\}$ 
8           $G := G \cup \{h\}$ 

```

Algoritma 4.2.2. Modüller İçin Buchberger Algoritması

Örnek 4.2.20. $(\mathbb{Q}[x, y])^3$ ün aşağıdaki vektörleri göz önüne alınsın:

$$f_1 = (0, y, x), f_2 = (0, x, xy - x), f_3 = (x, y^2, 0), f_4 = (y, 0, x).$$

$x > y$ olmak üzere $\mathbb{Q}[x, y]$ üzerinde deglex terim sıralaması ve $e_1 > e_2 > e_3$ olmak üzere $(\mathbb{Q}[x, y])^3$ üzerinde TPÖ terim sıralaması kullanılsın. Algoritma 4.2.2 kullanılarak $M = \langle f_1, f_2, f_3, f_4 \rangle$ için bir Gröbner taban hesaplanacaktır. $G = \{f_1, f_2, f_3, f_4\}$ olsun. $\mathcal{G} = \{\{f_1, f_2\}, \{f_1, f_4\}, \{f_2, f_4\}\}$ e sadece Tanım 4.2.17 deki sıfırdan farklı L ile oluşturulan S-Polinomları karşılık gelmektedir.

$$S(f_1, f_2) = yf_1 - f_2 = (0, y^2 - x, x) \xrightarrow{+}_G (-x, -x - y, 0)$$

olarak hesaplanır. Bu vektör G ye göre indirgenir. Böylece $f_5 = (-x, -x - y, 0)$ oluşturulur ve G ye eklenir. Daha sonra

$$S(f_1, f_4) = f_1 - f_4 = (-y, y, 0)$$

olur. Ve yine, bu vektör G ye göre indirgenir. Böylece $f_6 = (-y, y, 0)$ elde edilir ve G ye eklenir. $S(f_2, f_4) \xrightarrow{+}_G 0$ olduğu hemen görülür. Yeni vektörler olan f_5 ve f_6 değerlendirilmesine ihtiyaç olan sadece

$$S(f_5, f_6) = yf_5 - xf_6 = (0, -2xy - y^2, 0) \xrightarrow{+}_G (0, -2xy - x - y, 0)$$

S-Polinomunu oluşturur. Bu vektör G ye göre indirgenmiş olup, $f_7 = (0, -2xy - x - y, 0)$ oluşturulur ve G ye eklenir. Bu yeni vektör ise değerlendirilmek üzere sadece

$$S(f_3, f_7) = 2xf_3 + yf_7 = (2x^2, -xy - y^2, 0) \xrightarrow{+}_G (0, -2x^2 + \frac{1}{2}x + \frac{1}{2}y, 0)$$

S-Polinomunu oluşturur.

$f_8 = (0, -2x^2 + \frac{1}{2x} + \frac{1}{2y}, 0)$ olsun ve f_8 i G ye ekleyelim. Bu yeni vektör değerlendirilmesine gerek olan

$$S(f_3, f_8) = 2x^2f_3 + y^2f_8 = (2x^3, \frac{1}{2}xy^2 + \frac{1}{2}y^3, 0) \xrightarrow{+}_G 0$$

ve

$$S(f_7, f_8) = xf_7 - yf_8 = (0, -x^2 - \frac{3}{2}xy - \frac{1}{2}y^2, 0) \xrightarrow{+}_G 0$$

şeklindeki iki S-Polinomunu üretir. Böylece $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}, M$ için bir Gröbner tabandır.

Son olarak, 3. Bölümde bahsedilen indirgenmiş Gröbner taban kavramının modüllerdeki karşılığı tamamen aynı olup ispat verilmeksizin sadece ifadeler aşağıda yer almaktadır.

Tanım 4.2.21. $G = \{g_1, g_2, \dots, g_t\} \subseteq A^t$ bir Gröbner taban olsun. Eğer her i için g_i ler $G - \{g_i\}$ ye göre indirgenmiş ve her $i = 1, 2, \dots, t$ için $lc(g_i) = 1$ ise G ye indirgenmiş Gröbner taban denir. Böylece her i için g_i nin sıfırdan farklı hiçbir terimi $j \neq i$ olmak üzere herhangi bir $lm(g_j)$ tarafından bölünmez (Adams and Lousaunau 1994).

Teorem 4.2.22. Sabit bir terim sıralaması alınsın. Bu durumda, A^t nin sıfırdan farklı her bir M alt modülü, bu terim sıralamasına göre tek bir indirgenmiş Gröbner tabana sahiptir. Bu Gröbner taban M alt modülü A^t den alınan sonlu sayıdaki vektör ile üretilecek şekilde verildiğinde hemen hesaplanabilir (Adams and Lousaunau 1994).

Örnek 4.2.23. Örnek 4.2.20 tekrar ele alınsın. Bu örnekte $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ kümesinin M için bir Gröbner taban olduğunu söylenmişti. İlk olarak $lm(f_1)$, $lm(f_2)$ ve $lm(f_4)$ ü böldüğü için f_2 ve f_4 vektörleri G den çıkarılır ancak geriye kalan küme hala bir Gröbner tabandır. Dahası

$$f_3 \xrightarrow{+} (0, y^2 - x - y, 0)$$

dır. Bu yüzden, M nin indirgenmiş Gröbner tabanı

$$\left\{ (0, y, x), (0, y^2 - x - y, 0), \left(0, x^2 - \frac{1}{4}x - \frac{1}{4}y, 0\right), \left(0, xy + \frac{1}{2}x + \frac{1}{2}y, 0\right), (y, -y, 0), (x, x + y, 0) \right\}$$

dir.

4.3. Modüller İçin Gröbner Tabanların Basit Uygulamaları

$M = \langle f_1, f_2, \dots, f_s \rangle$, A^t nin bir alt modülü olsun. Aşağıdaki problemlerin nasıl etkili bir şekilde çözüldüğü gösterilecektir.

i) Verilen $f \in A^t$ için f nin M de olup olmadığının belirlenmesi (modül elemanı olma problemi) ve eğer elemanı ise $f = h_1 f_1 + h_2 f_2 + \dots + h_s f_s$ olacak şekilde $h_1, h_2, \dots, h_s \in A$ ların bulunması;

ii) A^t nin verilen diğer bir alt modülü M' için M nin M' nü içerip içermediğinin ve eğer $M' \subseteq M$ ise $M' = M$ olup olmadığının belirlenmesi;

iii) A^m/M nin elemanları için yan küme temsilcilerinin bulunması;

iv) $A^t/M, F$ – vektör uzayı için bir taban bulunması.

$F = \{f_1, f_2, \dots, f_s\}$, A^m de sıfırdan farklı vektörlerin bir kümesi ve $M = \langle f_1, f_2, \dots, f_s \rangle$ olsun. Ayrıca, $G = \{g_1, g_2, \dots, g_t\}$ herhangi bir terim sıralamasına göre M için bir Gröbner taban olsun. İlk olarak (i) deki problem ele alınsın. $f \in A^t$ olsun. Teorem 4.2.14 den

$$f \in M \Leftrightarrow f \xrightarrow{G}_+ 0$$

yazılabilir. Dolayısıyla, $f \in M$ olup olmadığı algoritmik olarak belirlenebilir. Dahası, eğer $f \in M$ ise

$$f = h_1 g_1 + h_2 g_2 + \dots + h_t g_t \quad (4.3.1)$$

eşitliğini elde etmek için Bölüm 4.2 de verilen Bölme Algoritması uygulanabilir. İdeal durumunda olduğu gibi eğer R ve G sütunları sırasıyla f_i ler ve g_j ler olan matrisler olarak ele alınırsa $G = R.T$ olacak şekilde girişleri polinom olan $s \times t$ tipinde bir T matrisi bulunabilir.

Örnek 4.3.1. $A = \mathbb{Q}[x, y]$ olsun.

$$f_1 = (xy, y, x), f_2 = (x^2 + x, y + x^2, y), f_3 = (-y, x, y), f_4 = (x^2, x, y)$$

olmak üzere $R = \{f_1, f_2, f_3, f_4\}$ tarafından üretilen A^3 ün bir M alt modülü ele alınsın. A üzerinde $x < y$ olmak üzere lex sıralaması ve A^3 üzerinde $e_1 > e_2 > e_3$ olmak üzere TPÖ sıralaması kullanılsın. Bir vektörün baş terimi altı çizilerek gösterilecektir. Örneğin;

$$f_1 = (\underline{xy}, y, x), f_2 = (x^2 + x, \underline{y} + x^2, y), f_3 = (\underline{-y}, x, y), f_4 = (x^2, x, \underline{y})$$

dir. M için indirgenmiş Gröbner taban,

$$g_1 = (\underline{x^3} + x, x^2 - x, -x), g_2 = (x, \underline{y} + x^2 - x, 0), g_3 = (\underline{y} + x^2, 0, 0), \\ g_4 = (x^2, x, \underline{y}), g_5 = (x^2, \underline{x^3}, -x^3),$$

$$g_6 = (x^2 - 2x, -x^2 + 2x, x^5 - x^4 - 3x^3 + x^2 + 2x)$$

olmak üzere $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ dir. $f = (-2x, x - 1, \underline{xy} + x)$ vektörü göz önüne alınsın. f nin, M de olup olmadığının belirlenmesi için, Bölüm 4.2 de sunulan Bölme Algoritması uygulanacaktır (Algoritma 4.2.1):

$$f \xrightarrow{x, g_4} (\underline{x^3} - 2x, -x^2 + x - 1, x) \xrightarrow{-1, g_1} (-x, -1, 0)$$

xe_1 ve e_2 herhangi bir $lm(g_i)$ tarafından bölünmediği için $(-x, -1, 0)$ vektörü G ye göre indirgenmiştir ve dolayısıyla f, M de değildir.

Şimdi g vektörü $g = (\underline{yx^5} - yx + x, yx^4 + y + 2x^2 - x, x^5 + yx)$ olarak kabul edilsin. Yine Bölme Algoritması uygulanırsa:

$$\begin{aligned} g &\xrightarrow{x^4, g_3} (-yx - x^7 + x, \underline{yx^4} + y + 2x^2 - x, yx + x^5) \\ &\xrightarrow{x^4, g_2} (\underline{-yx} - x^7 - x^5 + x, y - x^6 + x^5 + 2x^2 - x, xy + x^5) \\ &\xrightarrow{-x, g_3} (-x^7 - x^5 + x^3 + x, y - x^6 + x^5 + 2x^2 - x, \underline{xy} + x^5) \\ &\xrightarrow{x, g_4} (-x^7 - x^5 + x, \underline{y} - x^6 + x^5 + x^2 - x, x^5) \\ &\xrightarrow{1, g_2} (\underline{-x^7} - x^5, -x^6 + x^5, x^5) \\ &\xrightarrow{-x^4, g_1} (0, 0, 0) \end{aligned}$$

bulunur. Böylece g, M dedir. Dahası;

$$\begin{aligned} g &= x^5 g_3 + x^4 g_2 - x g_3 + x g_4 + g_2 - x^4 g_1 \\ &= -x^4 g_1 + (x^4 + 1) g_2 + (x^5 - x) g_3 + x g_4 \end{aligned}$$

elde edilir. Şimdi g , orijinal f_i lerin lineer kombinasyonu olarak ifade edilmek istenilsin. Böylece, G yi R ye dönüştüren T matrisi göz önüne alınsın.

$$\left. \begin{aligned} h_1 &= y^2 + 2x^2y - xy - 2y + x^4 - x^3 - 3x^2 + x + 2 \\ h_2 &= -y^2 - x^2y + 2y + 2x^2 + x - 2 \\ h_3 &= xy^2 + x^3y - x^2y - 3xy - 2x^3 + x^2 + 4x \\ h_4 &= -xy^2 + y^2 - x^3y + 2x^2y + 2xy - 2y - 2x^2 - 3x + 2 \end{aligned} \right\} \quad (4.3.2)$$

olmak üzere

$$[g_1 \ g_2 \ g_3 \ g_4 \ g_5 \ g_6] = [f_1 \ f_2 \ f_3 \ f_4] \underbrace{\begin{bmatrix} -1 & 0 & 0 & 0 & -x^2 - y & h_1 \\ 1 & 1 & 0 & 0 & x + y & h_2 \\ -x & 0 & -1 & 0 & x(1 - y) & h_3 \\ x - 1 & -1 & 1 & 1 & xy - y - x & h_4 \end{bmatrix}}_{\tilde{T}} \quad (4.3.3)$$

ifadesini elde edilir. Böylece;

$$\begin{aligned} g &= -x^4g_1 + (x^4 + 1)g_2 + (x^5 - x)g_3 + xg_4 \\ &= -x^4(-f_1 + f_2 - xf_3 + (x - 1)f_4) + (x^4 + 1)(f_2 - f_4) \\ &\quad + (x^5 - x)(-f_3 + f_4) + xf_4 \\ &= x^4f_1 + f_2 + xf_3 - f_4 \end{aligned}$$

olur.

Şimdi ise (ii) deki problem göz önüne alınsın. M' , A^t nin diğer bir alt modülü olsun. $M' = \langle f_1^i, f_2^i, \dots, f_l^i \rangle$ denilsin. Bu durumda, $M' \subseteq M$ olması için gerek ve yeter şart $i = 1, 2, \dots, l$ için $f_i^i \in M$ olmasıdır. Bu ifade yukarıda tanımlanan metod kullanılarak doğrulanabilir. Ayrıca, eğer $M' \subseteq M$ ise $M' = M$ olması için gerek ve yeter şart $M \subseteq M'$ olmasıdır ve bu ise yine yukarıda tanımlanan metod kullanılarak algoritmik olarak doğrulanabilir. Alternatif olarak M ve M' için indirgenmiş Gröbner taban hesaplanabilir ve $M' = M$ olup olmadığını belirlemek için A^t nin alt modülünün indirgenmiş Gröbner tabanının tekliği (Teorem 4.2.22) kullanılabilir.

Örnek 4.3.2. Örnek 4.3.1 tekrar ele alınsın. M' , A^3 ün $\{f_2, f_3, f_4, g\}$ tarafından üretilen alt modülü olsun. Örnek 4.3.1 de $g \in M$ olduğu gösterildiğinden M', M nin bir alt modülüdür. Ancak, Örnek 4.3.1 de ele alınan sıralama aynen kullanılırsa, M' için indirgenmiş Gröbner taban,

$$g_1^1 = (x, y + x^2 - x, 0), g_2^1 = (y + x^2, 0, 0), g_3^1 = (x^6, x^7, -x^7),$$

$$g_4^1 = (x^7 + x^5, x^6 - x^5, -x^5), g_5^1 = (x^2, x, y),$$

$$g_6^1 = (x^6 - 2x^5, -x^6 + 2x^5, x^9 - x^8 - 3x^7 + x^6 + 2x^5)$$

olmak üzere $\{g_1^1, g_2^1, g_3^1, g_4^1, g_5^1, g_6^1\}$ dir. M' için indirgenmiş Gröbner taban, M nin indirgenmiş Gröbner tabanına eşit olmadığı için, M ve M' modülleri eşit değildir.

Şimdi, $\{f_1, f_2, f_3, g\}$ tarafından üretilen A^3 ün M'' alt modülü göz önüne alınırsa, yine M'' , M' nin bir alt modülüdür. Dahası, M'' nin indirgenmiş Gröbner tabanının, M nin indirgenmiş Gröbner tabanı ile aynı olduğu hesaplanabilir, dolayısıyla $M'' = M$ dir.

(iii) deki problem göz önüne alınsın. Yani, A^t/M bölüm modülü için yan küme temsilcileri bulunacaktır. G, M için Gröbner taban olsun ve $f \in A^t$ olsun. Teorem 4.3.12 ve 4.3.14 den,

$$f \xrightarrow{+}_G r$$

olacak şekilde G ye göre indirgenmiş tek bir $r \in A^t$ vektörünün olduğu bilinmektedir. Bu vektör, f nin G ye göre normal formu olarak adlandırılır ve $N_G(f)$ ile gösterilir.

Önerme 4.3.3. f ve g , A^t de iki vektör olsun. Bu durumda,

$$A^t/M \text{ de } f + M = g + M \Leftrightarrow N_G(f) = N_G(g)$$

olmasıdır. Böylece, $\{N_G(f) \mid f \in A^t\}$, A^t/M bölüm modülü yan küme temsilcilerinin bir kümesidir. Dahası,

$$N_G: A^t \rightarrow A^t$$

$$f \rightarrow N_G(f)$$

dönüşümü bir F – lineer dönüşümdür (Adams and Loustaunau 1994).

Aşağıdaki önerme ise (iv) deki problemi çözer.

Önerme 4.3.4. $A^t/M, F$ – vektör uzayının bir tabanı, hiçbir $lm(g_i)$ bölmez X olacak şekildeki bütün $X \in A^t$ monomiyallerinin yan kümelerinden oluşur (Adams and Lousaunau 1994).

Örnek 4.3.5. Tekrar Örnek 4.3.1 ele alınsın. İndirgenmiş Gröbner tabanın baş terimleri,

$$x^3e_1, ye_2, ye_1, ye_3, x^3e_2, x^5e_3$$

dir. Bu yüzden, $A^3/M, \mathbb{Q}$ –vektör uzayı için bir taban

$$\{e_1, xe_1, x^2e_1, e_2, xe_2, x^2e_2, e_3, xe_3, x^2e_3, x^3e_3, x^4e_3\}$$

dır.

5. SONUÇLAR

Bu tezde öncelikle polinom halkaları üzerinde Gröbner taban kavramı temel tanım ve teoremler yardımıyla açıklanmış ve daha sonra bazı modüller üzerinde Gröbner taban kavramı incelenerek aradaki farklar ortaya konulmuştur.



KAYNAKLAR

Adams, W.W. and Loustaunau, P., 1994. An Introduction To Gröbner Bases. American Mathematical Society, 289 p, ABD.

Çallıalp, F., 2013. Örneklerle Soyut Cebir. Birsen Yayınevi, 343 s, İstanbul.

Dummit, D. S. and Foote, R. S., 2003. Abstract Algebra. Wiley Publication, 944 p.

Özenir, Y., 2011. Gröbner Tabanları. Y. Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Taşçı, D., 2018. Soyut Cebir. Gazi Kitap Evi, 649, Türkiye



ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Mehmet ARVAS
Doğum Yeri ve Tarihi	Diyadin 1982
Eğitim Durumu	
Lisans Öğrenimi	Atatürk Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü
Yüksek Lisans Öğrenimi	Ağrı İbrahim Çeçen Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı
İş Deneyimi	
Çalıştığı Kurumlar	Doğubayazıt Kaymakamlığı Sosyal Yardımlaşma ve Dayanışma Vakfı
İletişim	
E-posta Adresi	mehmetarvas292619@gmail.com