

ŞUBAT 2017

YÜKSEK LİSANS - MATEMATİK BÖLÜMÜ

SERAP GÜNGÖR KUTLU

T.C.

GAZİANTEP ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GRÖBNER TABAN VE POLİNOM HALKALARI

MATEMATİK BÖLÜMÜ
YÜKSEK LİSANS TEZİ

SERAP GÜNGÖR KUTLU
ŞUBAT 2017

Gröbner Taban ve Polinom Halkaları

Gaziantep Üniversitesi

Matematik Bölümü

Yüksek Lisans Tezi

Danışman

Doç. Dr. Necati OLGUN

Serap GÜNGÖR KUTLU

Şubat 2017



© 2017 [Serap GÜNGÖR KUTLU]



T.C.
GAZİANTEP ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
MATEMATİK ANA BİLİM DALI

Tezin Adı: Gröbner Taban ve Polinom Halkaları

Öğrencinin, Adı Soyadı: Serap GÜNGÖR KUTLU

Tez Savunma Tarihi: 06/02/2017

Fen Bilimleri Enstitüsü onayı


Prof. Dr. Ahmet Necmeddin YAZICI

FBE Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.


Prof. Dr. Adil KILIÇ

Enstitü ABD Başkanı

Bu tez tarafımda okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.


Doç. Dr. Necati OLGUN

Tez Danışmanı

Bu tez tarafımızca okunmuş, kapsam ve niteliği açısından bir Yüksek Lisans tezi olarak oy birliği ile kabul edilmiştir.

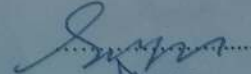
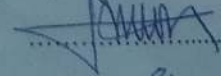
Jüri Üyeleri:

Prof. Dr. İsmet YILDIZ

Doç. Dr. Memet ŞAHİN

Doç. Dr. Necati OLGUN

İmzası


İlgili tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin referans gösterilerek ilgili tezde yer aldığını beyan ederim.

Serap GÜNGÖR KUTLU



ÖZET

GRÖBNER TABANI VE POLİNOM HALKALARI

GÜNGÖR KUTLU, Serap

Yüksek Lisans, Matematik Bölümü

Tez Yöneticisi: Doç.Dr.Necati OLGUN

Şubat 2017

Bu çalışma beş bölümden oluşmaktadır. Birinci bölüm, Bernd Sturmfels'in Gröbner taban ile ilgili çalışmasını içermektedir. Bu çalışmada Gröbner taban nedir ve Gröbner taban için üzerinde durulması gereken birkaç teorem verildi. Ayrıca terim sıralaması ve indirgenemezlik ile ilgili bilgi verildi. Gröbner tabanın niçin önemli olduğu ve amacının ne olduğu ile ilgili bilgi verildi. İlk olarak Buchberger 1965-1985 yıllarında;

$R = k[x_1, x_2, \dots, x_n]$ Gröbner taban kavramını verdi. Tezin ikinci bölümünde bu çalışmalar incelendi. R 'de sıfırdan farklı her idealin bir Gröbner tabana sahip olduğu ispatlandı ve bu tabanı veren Buchberger Algoritması inşa edildi. Bir ideal için Gröbner tabanın tek olmak zorunda olmadığı ve R 'deki bir idealin Gröbner tabanındaki elemanlar tarafından üretildiği görüldü. R 'nin bir I idealinin bir Gröbner tabanından minimal ve indirgenmiş Gröbner tabanların nasıl elde edildiği gösterildi. Minimal Gröbner tabanların da tek olmak zorunda olmadığı, fakat indirgenmiş Gröbner tabanın tek olduğu verildi.

Buchberger'den sonra Mora 1986-1994 yıllarında serbest k-cebiri üzerinde Gröbner taban tanımını verdi. Böylece "Değişmeli Olmayan Gröbner Taban Teorisi" üzerindeki çalışmalar için ilk adım atılmış oldu. Tezin dördüncü bölümünde de bu çalışmaya yer verilmiştir.

Beşinci bölümde, Gröbner tabanların iki uygulaması olarak, ideale ait olma ve radikale ait olma problemleri ele alındı.

Anahtar Kelimeler: Gröbner Taban, İdeal, Polinom Halkaları

ABSTRACT

GRÖBNER BASIS AND POLYNOMIAL RINGS

GÜNGÖR KUTLU, Serap

M.Sc.Thesis, Mathematics Department

Adviser: Doç.Dr.Necati OLGUN

February 2017

This work consists of five chapters. The first chapter consists works of Bernd Sturmfels about Gröbner basis. Some theory are proved in this study. For example; “What is a Gröbner basis?” Also, monomial orders and irreducibility are investigated. Importance of Gröbner basis and purpose of Gröbner basis are investigated.

Firstly; Buchberger, in the years 1965-1985, defined the notion of Gröbner basis on $R = k[x_1, x_2, \dots, x_n]$. In Chapter 2, these studies are investigated. It is proved that every non-zero ideal of R has a Gröbner basis and Buchberger’s Algorithm which gives this basis is constructed. It is seen that the Gröbner basis for an ideal need not be unique and any ideal in R is generated by the elements in the Gröbner basis of that ideal. It is shown how minimal and reduced Gröbner basis can be obtained from any Gröbner basis of an ideal of R . It is proved that also minimal Gröbner basis need not be unique although reduced Gröbner basis is unique.

After Buchberger, Mora, in the years 1986-1994, gave the notion of Gröbner basis on the free k -algebra. Therefore the first studies were given for Noncommutative Gröbner Basis Theory. In Chapter 4, these studies are considered respectively.

In Chapter 5, as two applications of Gröbner basis, Ideal Membership Problem and Radikal Membership Problem are considered.

Key Words: Gröbner Basis, Ideals, Polynomial Rings



Çok kıymetli aileme...

TEŞEKKÜR

Bu çalışma süresince desteğini, deneyimini ve emeğini hiçbir zaman benden esirgemeyen ve aynı zamanda kişiliğiyle de bana örnek olan Gaziantep Üniversitesi öğretim üyelerinden saygıdeğer hocam Doç. Dr. Necati OLGUN'a minnettarlığımı sunarım.

Maddi ve manevi destekleriyle her zaman yanımda bulunarak bu günlere gelmemde en büyük pay sahibi olan aileme ve eşime sonsuz şükranları borç bilirim.



İÇİNDEKİLER

ÖZET.....	v
ABSTRACT.....	vi
TEŞEKKÜR.....	viii
İÇİNDEKİLER	ix
SEMBOLLER LİSTESİ	x
BÖLÜM 1 - GİRİŞ	1
1.1. Bir Gröbner Taban Nedir?	1
1.2. Bir Gröbner Taban Niçin Önemlidir?	3
1.3.Gröbner Taban Teorisinin Amacı Nedir?.....	3
BÖLÜM 2- GRÖBNER TABAN ÇALIŞMALARI.....	4
2.1.Tam Sıralı ve İyi Sıralı Kümeler.....	4
2.2. Polinom Halkaları.....	5
2.3. Serbest (Free) Cebiri	9
BÖLÜM 3 - TERİM SIRALAMALARI VE BÖLME ALGORİTMASI	10
3.1.Temel Tanım ve Sonuçlar	10
3.2.Terim Sıralamaları.....	12
3.3. $k[x_1, x_2, \dots, x_n]$ Polinomlar Halkası Üzerinde Bölme Algoritması.....	14
BÖLÜM 4 - DEĞİŞMELİ GRÖBNER TABAN TEORİSİ	19
4.1.Değişmeli Gröbner Tabanlar.....	19
4.2.S- Polinomu ve Buchberger Algoritması	20
4.3.İndirgenmiş Gröbner Tabanlar.....	23
BÖLÜM 5 - GRÖBNER TABANLARIN UYGULAMALARI.....	25
5.1.İdeale Ait Olma Problemi.....	25
5.2.Radikale Ait Olma Problemi.....	28
KAYNAKLAR.....	31

SEMBOLLER LİSTESİ

$\mathbb{N}$	: Doğal sayılar kümesi
$\mathbb{Q}$	: Rasyonel sayılar kümesi
Γ_0	: Noktalar kümesi
Γ_1	: Ayrıklar kümesi
Γ	: Sonlu direk çizgesi
$<_{lex}$	: Sözlük sıralaması
$<_{deg\,lex}$	: Derece-sözlük sıralaması
$\sqrt{I}$	: I idealinin radikali



1. GİRİŞ

1.1 Bir Gröbner Taban Nedir?

Bir Gröbner taban, uygun algoritmik özelliklere sahip çok değişkenli polinomların kümesidir. Her polinom kümesi bir Gröbner tabana çevrilebilir. Bu yöntem, 3 bilinen yöntemi genelleştirir:

- Lineer denklem sistemleri çözümü için Gauss Eliminasyon yöntemi
- Tek değişkenli iki polinomun en büyük ortak bölenini bulmak için Öklid Algoritması
- Ve lineer programlama için Simplex Algoritması (Metodu)

Örneğin; Gauss Eliminasyon lineer formların şu şekilde toplamıdır :

$$F = \{2x + 3y + 4z - 5, 3x + 4y + 5z - 2\},$$

Ve F algoritması Gröbner tabana dönüşür.

$$G = \{\underline{x} - z + 14, \underline{y} + 2z - 11\}$$

Bir cisim alalım, örneğin reel sayılar ($K = \mathbb{R}$), kompleks (karmaşık) sayılar ($K = \mathbb{C}$), rasyonel sayılar ($K = \mathbb{Q}$) veya sonlu bir cisim $K = F_p$ alalım. n değişken α_i 'lerden oluşan ve katsayılarını K cisminden alan bir $K[x_1, \dots, x_n]$ polinom halkası yazarız. Eğer F bir polinom kümesi ise, o hâlde F tarafından üretilen ideal, tüm polinom lineer kombinasyonların kümesi olan $\langle F \rangle$ dir.

$$\langle F \rangle = \{p_1 f_1 + \dots + p_r f_r; f_1, \dots, f_r \in F; p_1, p_2, \dots, p_r \in K[x_1, x_2, \dots, x_n]\}$$

Örneğimizdeki F ve onun Gröbner tabanı G aynı ideali üretir :

$$\langle G \rangle = \langle F \rangle$$

Teorem 1.1.1 ; $K[x_1, \dots, x_n]$ deki her ideal $I = \langle F \rangle$ şeklindeki forma sahipse F polinomunun sonlu birkaç kümesinden üretilir.

$K[x_1, \dots, x_n]$ için;

“<” terim sıralaması $x^a = x_1^{a_1} \dots x_n^{a_n}$ şeklindedir. Bu sıralama iki özelliğe sahiptir;

$$(1) \ x^a < x^b \Rightarrow x^{a+c} < x^{b+c} \quad (\forall a, b, c \in \mathbb{N}^n)$$

(2) Sabit değişken en küçüktür.

$$1 < x^a \quad (\forall a \in \mathbb{N}) \quad (a \neq 0)$$

$n = 2$ için derece-sözlük sıralaması aşağıdaki gibidir;

$$1 < x_1 < x_2 < x_1^2 < x_1x_2 < x_2^2 < x_1^3 < x_1^2x_2 < \dots$$

Eğer “<” terim sıralamasını düzenlersek, her f polinomu $f = x^a$ ya sahiptir. “<” terim sıralamasında x^a en büyük değişkendir. f polinomunun azalan sıralamasını yazdığımızda ilk terimin altını çizimiz. Örneğin, kuadratik polinom için;

$$f = \underline{3x_2^2} + 5x_1x_2 + 7x_1^2 + 11x_1 + 13x_2 + 17$$

$K[x_1, \dots, x_n]$ polinomunda bir I ideali alalım. O hâlde $K[x_1, \dots, x_n]$ nin ilk ideali I daki tüm ilk idealleri tarafından üretilmiş olsun. İlk ideali “ $in_{<}(I)$ ” şeklinde gösterelim.

İlk ideali üretmek için G deki elemanlar ilk terim ise I nın sonlu kümesi olan G terim sıralamasına uyan Gröbner tabandır.

$$in_{<}(I) = \langle in_{<}(g) : g \in G \rangle$$

Gröbner taban için indirgenemezliğe ihtiyaç yoktur. Eğer I ideali için G Gröbner taban ise o hâlde I nın her sonlu kümesi G yi içerir. Bu indirgenemezliği çözmek için G yi Gröbner tabana indirgeriz;

(1) $\forall g \in G$, g deki ilk terimin $(in_{<}(g))$ katsayısı 1 dir.

(2) $\{in_{<}(g) : g \in G\}$ kümesi, $in_{<}(I)$ yı üretir.

(3) “<” terim sıralamasını düzenlersek, $K[x_1, \dots, x_n]$ deki her ideal tek indirgenmiş tabana sahiptir.

1.2 Gröbner Taban Niçin Önemlidir?

Gröbner taban teorisi önemlidir çünkü;

- ✓ Ana problem, bu teori ile beş dakikada çözülür. (Polinomlarda çarpma ve bölme işlemleri uzun zaman alır.)
- ✓ Matematiğin farklı alanlarındaki çoğu problemler Gröbner tabana indirgenip hesaplanabilir.
- ✓ Gröbner tabanları polinom halkaları teorisinde kullanılan çok önemli bir araçtır. Gröbner tabanları teorik olarak 1964 yılında Hironaka, daha önce de 1899 yılında Gordan tarafından kullanılmıştı. 1965 yılında Buchberger Gröbner tabanlarının hesaplanmasını sağlayan bir algoritma buldu. Buchberger algoritmasının polinom sistemleri açısından önemi lineer cebirdeki Gauss yoketme yöntemiyle karşılaştırılabilir. Bu algoritmanın polinom denklemlerinin köklerinin bulunması, bir polinomun verilen başka polinomlar cinsinden ifade edilmesi gibi pek çok uygulaması vardır.
- ✓ Gröbner taban, parametrik gösterimden örtük çok terimli gösterime geçiş için kullanılan en kolay yöntemlerden biridir.

1.3 Gröbner Taban Teorisinin Amacı Nedir?

Gröbner Taban Metodu, çok değişkenli polinomlarda hızlı işlem yapmamızı sağlar. Gröbner tabanın uygulandığı alanlar ;

- Cebirsel Geometri, Değiştirilebilen Cebir, Polinom ideal teori
- “Automated Geometrical” teoreminin çözümü
- Kod Teori
- Tamsayı Programlama
- Kısmî Diferansiyel Denklemler
- Hipergeometrik Fonksiyonlar
- İstatistik
- Nümerik
- Sistemler Teorisi
- Sembolik Toplam

- Değişirilemeyen Cebir
- Denklemlerin Cebirsel Çözümü
- Hilbert Fonksiyonları
- Polinomlar Arasındaki Cebirsel İlişkiler

Ayrıca parametrik gösterimden örtük çok terimli gösterime geçiş için literatürde birçok yöntem bulunabilir. Bunlardan birisi de Gröbner Taban Teorisidir.

2. GRÖBNER TABAN ÇALIŞMALARI

İlk olarak Buchberger 1965-1985 yıllarında $R = k[x_1, \dots, x_n]$ üzerinde Gröbner taban kavramını tanımladı ve bazı denklemleri verdi. Daha sonraki çalışmalarda Gröbner tabanı veren Buchberger Algoritması inşa edildi. Bir ideal için Gröbner tabanın tek olmak zorunda olmadığı ve R ’deki bir idealin Gröbner tabandaki elemanlar tarafından üretildiği görüldü. R ’nin bir I idealinin bir Gröbner tabanından minimal ve indirgenmiş Gröbner tabanların nasıl olduğu üzerinde çalışıldı. Minimal Gröbner tabanların da tek olmak zorunda olmadığı, fakat indirgenmiş Gröbner tabanın tek olduğu ispatlandı.

Buchberger’den sonra Mora 1986-1994 yıllarında $k \langle x_i \rangle_{i \in I}$ serbest k -cebiri üzerinde Gröbner taban tanımını verdi. Böylece “Değişmeli Olmayan Gröbner Taban Teorisi” üzerindeki çalışmalar için ilk adım atılmış oldu. Mora’dan sonra Green 1993’te herhangi bir k -cebiri için, cebirin k -tabanı üzerine bazı koşullar koyarak, Gröbner tanımını verdi. Green’in çalışmaları değişmeli durumda Buchberger’in çalışmaları ile çakışmaktadır. Ayrıca Green’in çalışmaları $k \langle x_i \rangle_{i \in I}$ serbest k -cebirine uygulanırsa Mora’nın çalışmaları elde edilebilmektedir.

Bu çalışmada k keyfi karakteristikli herhangi bir cismi ve R değişmeli, birimli bir halkayı gösterecektir.

2.1 Tam Sıralı ve İyi Sıralı Kümeler

Tanım 2.1.1 A boştan farklı bir küme olsun. $\leq$, A üzerinde bir bağıntı olsun.

Eğer

- Her $x \in A$ için $x \leq x$ (Yansıma Özelliği)
- Her $x, y \in A$ için $x \leq y$ ve $y \leq x$ iken $x = y$ (Ters Simetri Özelliği)

- Her $x, y, z \in A$ için $x \leq y$ ve $y \leq z$ iken $x \leq z$ (Geçişme Özelliği)

koşulları sağlanırsa $\leq$ bağıntısına A üzerinde **kısmen sıralama bağıntısı**, $(A, \leq)$ ' ya da **kısmen sıralı küme** denir.

Tanım 2.1.2 $(A, \leq)$ kısmen sıralı bir küme ve $B \subset A$ olsun. Eğer her $x, y \in B$ için $x \leq y$ ya da $y \leq x$ olursa B ' ye A ' nın bir zinciri denir. Eğer her $x, y \in A$ için $x \leq y$ ya da $y \leq x$ olursa $\leq$ bağıntısına **tam sıralama bağıntısı** ve $(A, \leq)$ ye **tam sıralı küme** denir. (Dummit and Foote, 1999)

Tanım 2.1.3 $(A, \leq)$ kısmen sıralı küme olsun. Eğer A 'nın boştan farklı her altkümesi bir en küçük elemana sahipse $\leq$ bağıntısına **iyi sıralama bağıntısı** ve $(A, \leq)$ 'ya da **iyi sıralama küme** denir.

2.2 Polinom Halkaları

Tanım: R birimli ve değişmeli bir halka ve x bilinmeyen olsun. Buna göre $n \geq 0$ olacak şekilde bir tamsayı ve $a_0, a_1, a_2, \dots, a_n \in R$ olmak üzere

$$a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_nx^n$$

şeklindeki bir ifadeye katsayıları R de olan x bilinmeyenine bağlı bir polinom denir. Burada a_ix^i lere polinomun terimleri ve a_ix^i terimlerindeki a_i ' ye x^i nin katsayısı denir.

R halkası üzerinde x ' e bağlı bütün polinomların kümesini $R[x]$ ile göstereceğiz.

NOT : $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_nx^n$ polinomunu kısaca

$$f(x) = \sum_{i=0}^n a_ix^i$$

şeklinde göstermek mümkündür.

R bir halka olsun. $i \geq 0$ için $s_i \in R$ ve $t_i \in R$ olmak üzere;

$\sigma = (s_0, \dots, s_i, \dots)$ ve $\tau = (t_0, \dots, t_i, \dots)$ dizileri alınsın. O zaman

$$\tau = \sigma \Leftrightarrow \forall i \text{ için } \tau(i) = t_i = \sigma(i) = s_i \quad (i \geq 0)$$

dır.

Tanım 2.2.1 $\sigma = (s_0, \dots, s_i, \dots)$ R ' de bir dizi olsun. Eğer $\forall n < i$ için $s_i = 0$ olacak şekilde bir $n \geq 0$ tamsayısı varsa σ 'ye kısa dizi denir.

Tanım 2.2.2 $\sigma = (s_0, s_1, \dots, s_n, \dots)$ bir kısa dizi ve $s_n = 0$ olsun.

- s_n ' ye σ ' nin başkatsayısı ve
- n ' ye de σ ' nin derecesi denir.

Tanım 2.2.3 $x = (0, 1, 0, \dots)$ olsun. R ' deki bütün kısa diziler $R[x]$ ile gösterilsin. O zaman $x \in R[x]$ olur.

$\sigma = (s_0, \dots, s_i, \dots)$ ve $\tau = (t_0, \dots, t_i, \dots)$ olsun.

$\sigma + \tau$ ' nun toplamı;

$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \dots, s_i + t_i, \dots) = \tau + \sigma$ ile çarpımı da

$\tau \cdot \sigma = (s_0 t_0, s_0 t_1 + s_1 t_0, s_2 t_0 + s_1 t_1 + s_0 t_2, \dots) = \sigma \cdot \tau$

$= (a_0, a_1, a_2, \dots, a_k, \dots)$

Öyle ki

$a_k = \sum_{i=0}^k s_i t_{k-i}$ ile tanımlansın.

O zaman $R[x]$ bu “+” ve “.” işlemleri ile birimli ve değişmeli bir halka olur.

$x = (0, 1, 0, \dots)$ olsun. Dolayısıyla $R[x]$ 'deki “.” işlemi gereğince;

$x^2 = (0, 0, 1, 0, \dots), \dots, x^n = (0, 0, \dots, 0, 1, 0, \dots)$ olur.

$x \cdot \sigma = (0, s_0, s_1, \dots, s_i, \dots) = \sigma \cdot x$ dir ve $\tau \in R$ olmak üzere $(\tau, 0, \dots)$ dizisi için

$$(\tau, 0, \dots) \cdot (s_0, \dots, s_i, \dots) = (\tau s_0, \dots, \tau s_i, \dots)$$

olur ve $(\tau, 0, \dots)$ dizisi τ olarak görülebilir.

$$\begin{aligned}
\sigma &= (s_0, \dots, s_n, \dots) \\
&= (s_0, 0, \dots) + (0, s_1, 0, \dots) + \dots + (0, 0, \dots, s_n, \dots) \\
&= s_0(1, 0, 0, \dots) + s_1(0, 1, 0, \dots) + \dots + s_n(0, 0, \dots, 0, 1, 0, \dots) \\
&= s_0 + s_1x + \dots + s_nx^n
\end{aligned}$$

Bu şekilde elde edilen $R[x]$ halkasına x bilinmeyenli R katsayılı değişmeli polinomlar halkası denir. $R[x]$ in elemanlarına da x bilinmeyenli R katsayılı polinomlar denir. Eğer,

$$f(x) = s_0 + s_1x + \dots + s_nx^n \quad (s_n \neq 0)$$

ise o zaman;

- $s_0, s_1, \dots, s_n$; polinomun katsayıları,
 - s_0 ; polinomun sabiti,
 - s_nx^n ; polinomun başterimi ($lt(f)$),
 - s_n ; polinomun başkatsayısı ($lc(f)$),
 - n ; polinomun derecesi ($der(f(x))$)
- olarak adlandırılır.

Not: Bir sabit polinom ya sıfır ya da derecesi sıfır olan bir polinomdur. Tümevarım yardımıyla $R[x_1][x_2] \dots [x_n] = R[x_1, \dots, x_n]$ değişmeli polinomlar halkası inşa edilir. (Rotman, 1996)

Önteorem 2.2.4 R tamlık bölgesi ve $p(x), q(x) \in R[x]$ olsun. Bu durumda ;

- $der(p(x)q(x)) = der(p(x)) + der(q(x))$
- $R[x]$ 'in tersinir elemanları sadece R 'nin tersinir elemanlarıdır.
- $R[x]$ tamlık bölgesidir.

Teorem: Bir R halkasının tamlık bölgesi olması için gerek ve yeter şart $R[x]$ 'in bir tamlık bölgesi olmasıdır.

İspat $\Rightarrow$: R bir tamlık olsun. Buna göre göstereceğiz ki $R[x]$ de bir tamlık bölgesidir. R tamlık bölgesi olduğundan birimli, değişmeli ve sıfır bölensiz bir hal-kadır. R birimli ve değişmeli ise $R[x]$ de birimli ve değişmelidir.

O hâlde $R[x]$ 'in tamlık bölgesi olduğunu göstermek için geriye sadece sıfır bölensiz olduğunu göstermek kalır. $f(x)$ ve $g(x)$ ' in $R[x]$ in sıfırdan farklı olduğunu kabul edelim. Eğer $\deg(f(x)) = n$ ve $\deg(g(x)) = m$ ise o zaman $f(x)$ ve $g(x)$ in sırası ile a_n ve b_m başkatsayıları R nin sıfırdan farklı elemanları olur. Oysa R bir tamlık bölgesi olduğundan $a_n b_m \neq 0$ dır. Halbuki $a_n b_m$, $f(x)g(x)$ çarpımındaki x^{m+n} katsayısı olduğundan buradan $f(x)g(x) = 0$ sonucu elde edilir. Böylece $R[x]$ sıfır bölensizdir. O hâlde sonuç olarak $R[x]$ birimli, değişmeli ve sıfır bölensiz olduğundan bir tamlık bölgesidir.

$\Leftarrow$: $R[x]$ bir tamlık bölgesi olsun. Buna göre R nin bir tamlık bölgesi olduğunu göstermeliyiz. Eğer a, b R halkasının sıfırdan farklı iki elemanı ise bu durumda a ve b elemanları $R[x]$ de iki sabit polinom olarak düşünülebilir. Böylece $R[x]$ de $ab \neq 0$ olup aynı zamanda R çarpma işlemine göre kapalı olduğundan $a, b \neq 0 \in R$ dir. O hâlde R bir tamlık bölgesidir.

Not: Eğer R tamlık bölgesi değilse o takdirde $R[x]$ de bir tamlık bölgesi değildir.

Örneğin ; $\mathbb{Z}_6$ bir tamlık bölgesi olmadığından $\mathbb{Z}_6[x]$ de bir tamlık bölgesi değildir.

Gerçekten $2, 3 \in \mathbb{Z}_6$ için $2.3 = 0$ olduğundan $\mathbb{Z}_6$ tamlık bölgesi değildir. Diğer taraftan ; $f(x) = 2x$ ve $g(x) = 3x$ $\mathbb{Z}_6$ de sıfırdan farklı polinomlar olmak üzere

$$f(x)g(x) = (2x)(3x) = 6x^2 = 0$$

yazarız. Bu da $\mathbb{Z}_6[x]$ in bir tamlık bölgesi olmadığını gösterir. Yani $R[x]$ bir tamlık bölgesi değilse bu durumda R de bir tamlık bölgesi değildir.

Önteorem 2.2.5 $f_1, f_2, \dots, f_s \in k[x]$ olmak üzere;

$g = \text{ebob}(f_1, f_2, \dots, f_s)$ ifadesi $f_1, f_2, f_3, \dots, f_s$ polinomlarının en büyük

ortak bölenini gösterebilirsin. ($lc(g) = 1$)

- (i) $\langle f_1, f_2, \dots, f_s \rangle = \langle ebob(f_1, f_2, \dots, f_s) \rangle$
- (ii) Eğer $s \geq 3$ ise $ebob(f_1, f_2, \dots, f_s) = ebob(f_1, ebob(f_2, \dots, f_s))$

Tanım 2.2.6 A bir halka ve x bir değişken olmak üzere ;

$\sum a_i x^i$ formunda tek türlü yazılabilen elemanlardan oluşan ve $a_i x = x a_i$ olması gerekmeyen halka düşünölsün.

σ ve $\delta : A \rightarrow A$ grup homomorfizmaları olsunlar ve $xa = \sigma(a)x + \delta(a)$

eşitliği sağlansın. O zaman ;

$$\begin{aligned}
 x(ab) &= \sigma(ab)x + \delta(ab) \\
 (xa)b &= [\sigma(a)x + \delta(a)]b = (\sigma(a)x)b + \delta(a)b \\
 &= \sigma(a)(xb) + \delta(a)b \\
 &= \sigma(a)(\sigma(b)x + \delta(b)) + \delta(a)b \\
 &= \sigma(a)\sigma(b)x + \sigma(a)\delta(b) + \delta(a)b
 \end{aligned}$$

elde edilir ve böylece $\sigma(ab) = \sigma(a)\sigma(b)$ ve $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ olur.

Dolayısıyla σ bir halka homomorfizması ve δ , $\forall a, b \in A$ için;

$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ eşitliğini sağlar.

Tersine, A bir halka ; $\sigma : A \rightarrow A$ bir halka homomorfizması, $\delta : A \rightarrow A$ bir grup homomorfizması ve $\forall a, b \in A$ için;

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b \text{ olsun.}$$

2.3 Serbest (Free) Cebiri

Tanım 4.3.1 F bir grup, X boştan farklı bir küme ve $\sigma : X \rightarrow F$ bir fonksiyon olsun. Eğer X 'den bir G grubuna olan $\forall \alpha$ fonksiyonu için bir tek $\beta : F \rightarrow G$ grup homomorfizması varsa ve $\beta \circ \sigma = \alpha$ ise, F 'ye X üzerinde **serbesttir** denir. Herhangi bir küme üzerinde serbest olan gruba **serbest-grup** denir. [Hungerford,1974]

Tanım 4.3.2 $X = \{x_i\}_{i \in I}$ olsun. X üzerinde çarpma işlemi aşağıdaki biçimde tanımlansın.

$$(x_{i_1}, \dots, x_{i_t})(x_{j_1}, \dots, x_{j_k}) = x_{i_1} \dots x_{i_t} x_{j_1} \dots x_{j_k}$$

Bu durumda

$$S = \langle X \rangle = \{x_{i_1} \dots x_{i_t} \mid x_{i_j} \in X, t \in \mathbb{N}\} \cup \{1\}$$

X tarafından üretilen serbest yarı-grup olur. Böylece

$$k \langle S \rangle = k \langle X \rangle = k \langle x_i \rangle_{i \in I} = \left\{ \sum_{\text{sonlu}} \mu(i_1, \dots, i_t) x_{i_1} \dots x_{i_t} \mid \mu(i_1, \dots, i_t) \in k, x_{i_1} \dots x_{i_t} \in S \right\}$$

ile tanımlanan ve tabanı S olan k -cebire X üzerindeki serbest (free) cebir denir.

[Hungerford , 1974]

Teorem 2.3.3 $i: X \rightarrow k \langle X \rangle$ dönüşüm ve $A = k[a_i]_{i \in I}$ bir k -cebiri olsun. $\varphi: X \rightarrow A$ bir fonksiyon olmak üzere;

$k \langle X \rangle$ 'den A 'ya bir tek ϕ k -cebiri homomorfizması vardır öyle ki $\phi \circ i = \varphi$ olur.

3. TERİM SIRALAMALARI VE BÖLME ALGORİTMASI

Bu bölümde Gröbner tabanlar için gerekli olan bazı temel kavramlar, tek ve çok değişkenli bölme algoritmaları ve terim sıralamaları hakkında bilgi verilecektir.

3.1 Temel Tanım ve Sonuçlar

k herhangi bir cisim olmak üzere;

$k[x_1, x_2, \dots, x_n]$ değişmeli polinomlar halkası olsun.

$\beta = \{x^a = x_1^{a_1} \dots x_n^{a_n} \mid a = (a_1, \dots, a_n) \in \mathbb{N}^n\}$ nin $k[x_1, x_2, \dots, x_n]$ için bir k -taban olduğu açıktır.

Tanım 3.1.1 $(R, +, \cdot)$ bir halka $I \subseteq R, I \neq \emptyset$ olsun. Eğer,

- (i) Her $a, b \in I$ için $a - b \in I$ ve
- (ii) Her $a \in I$ ve her $r \in R$ için $r \cdot a \in I$ (veya $a \cdot r \in I$) ise, I, R halkasının bir sol (veya sağ) idealidir denir. $(R, +, \cdot)$ değişmeli ise sağ ve sol kavramları çakışır ve I kümesine **ideal** denir.

Teorem 3.1.2 (Hilbert Taban Teoremi) : R deđişmeli bir halka olsun. Aşağıdakiler birbirlerine denktir.

- i) Eğer I , R nin bir ideali ise $I = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in R$ polinomları vardır.
- ii) Eğer $I_1 \subseteq I_2 \subseteq \dots \subseteq I_k \subseteq \dots$ dizisi R nin ideallerinin bir artan dizisi ise öyle bir N vardır ki, $I_N = I_{N+1} = \dots$ dir.

İspat : I , R nin bir ideali ve $I = \langle f_1, f_2, \dots, f_s \rangle$ olsun.

$J = \bigcup_{i=1}^{\infty} I_i$ idealini alalım.

(i) den dolayı $J = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in R$ dir. O zaman bir N için $f_1, f_2, \dots, f_s \in I_N$ dir. Böylece $I_N = I_{N+1} = I_{N+2} = \dots$ olur. Şimdi tersine $I_1 \subseteq I_2 \subseteq \dots \subseteq I_N \subseteq \dots$ R de artan idealler zinciri ve bir N için $I_N = I_{N+1} = I_{N+2} = \dots$ olsun. I 'nın, R 'de sonsuz üreteçli bir ideali olduğunu varsayalım. $f_1 \in I$ alalım. $\langle f_1 \rangle \neq I$ dır.

$f_2 \in \left(\frac{I}{\langle f_1 \rangle} \right)$ alalım. $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \neq I$ dır.

$f_3 \in \left(\frac{I}{\langle f_1, f_2 \rangle} \right)$ alalım. $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle \neq I$ dır.

$\vdots$

Bu şekilde sonsuz artan zinciri elde edilir. Hipotezden bir s için $I = \langle f_1, f_2, \dots, f_s \rangle$ olup I 'nın sonlu üreteçli olduğu görülür.

Tanım 3.1.3 R , birim elemanlı ve deđişmeli bir halka olsun. Eğer R , Teorem 2.1.1 deki koşulları sağlıyorsa R 'ye bir **Noetherian halkası** denir.

Teorem 3.1.4 R , **Noetherian halka** (artan zincir şartını sağlayan halka) ise $R[x]$ de Noether halkadır.

İspat:

Sonuç 3.1.5 K bir cisim ise $K[x_1, x_2, \dots, x_n]$ Noetherian halkasıdır.

Teorem 3.1.6 Eğer $a(x), b(x) \in k[x]$ ve $b(x) \neq 0$ ise o zaman tek $q(x)$ ve $r(x) \in k[x]$ vardır öyle ki,

$$a(x) = q(x)b(x) + r(x)$$

$r(x) = 0$ ya da $\deg(r(x)) < \deg(b(x))$ dir.

3.2 Terim Sıralamaları

Tanım 3.2.1 β üzerinde $x_1 > x_2 > \dots > x_n$ sırasında $<$ derece-sözlük sıralaması aşağıdaki gibi tanımlanır:

$\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ için,

$$x^\alpha < x^\beta \Leftrightarrow \left\{ \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \right\} \text{ ya da } x^\alpha < x^\beta \Leftrightarrow \left\{ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \right\} \text{ ve } x_1 > x_2 > \dots > x_n$$

sırasında $x^\alpha < \text{lex}(x^\beta)$ dir. Böylece bu sıralamaya göre iki değişkenli durumda yani $x_2 < x_1$ sırasında,

$$1 < x_2 < x_1 < (x_2)^2 < x_1 x_2 < (x_1)^2 < (x_2)^3 < x_1 (x_2)^2 < (x_1)^2 x_2 < (x_1)^3 < \dots$$

elde edilir. $<$ derece-sözlük sıralaması “deglex” ile gösterilir ve $<$ deglex bir terim sıralamasıdır.

i) $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ için, $1 \neq x^\alpha \in \beta$ olsun.

$$1 = (x_1)^0 \dots (x_n)^0 \neq (x_1)^{\alpha_1} \dots (x_n)^{\alpha_n} \text{ olduğundan } \sum_{i=1}^n \alpha_i > 0 \text{ dir.}$$

Dolayısıyla $1 < \text{deglex}(x^\alpha)$ olur.

ii) $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$ için $x^\alpha, x^\beta \in \beta$ ve

$$x^\alpha < \text{deglex}(x^\beta) \text{ olsun. } x^\gamma \in \beta \text{ alınsın.}$$

Tanım 3.2.2 $x^\alpha, x^\beta \in \beta$ olsun. Eğer $x^\beta = x^\alpha x^\gamma$ olacak şekilde bir $x^\gamma \in \beta$ varsa x^α, x^β yı böler denir.

Önerme $x^\alpha, x^\beta \in \beta$ ve $<, \beta$ üzerinde bir terim sıralaması olsun. Eğer x^α, x^β yı bölerse $x^\alpha \leq x^\beta$ olur.

İspat ; x^α, x^β yı bölerse, Tanım 2.2.2 gereğince $x^\beta = x^\alpha x^\gamma$ olacak şekilde bir $x^\gamma \in \beta$ vardır. $<$ terim sıralaması olduğu için $x^\gamma \geq 1$ dir ve sonuç olarak

$$x^\beta = x^\alpha x^\gamma \geq x^\alpha$$

elde edilir.

Teorem 3.2.3 β üzerindeki her terim sıralaması bir iyi sıralamadır.

Tanım 3.2.4 $k[x_1, x_2, \dots, x_n]$ üzerinde terim sıralaması $<$ olsun. $f \in k[x_1, x_2, \dots, x_n]$ alındığında

$$f = \alpha_1 x^{\alpha_1} + \alpha_2 x^{\alpha_2} + \dots + \alpha_r x^{\alpha_r} \text{ ve } x^{\alpha_1} > x^{\alpha_2} > \dots > x^{\alpha_r}$$

olacak şekilde $x^{\alpha_i} \in \beta$ ($1 \leq i \leq r \leq n$) ve $0 \neq \alpha_i \in k$ vardır. Ayrıca f için aşağıdaki tanım ve gösterimler kullanılacaktır.

- $lp(f) = x^{\alpha_1}$; f 'nin başpolinomu
- $lc(f) = \alpha_1$; f 'nin başkatsayısı
- $lt(f) = \alpha_1 x^{\alpha_1}$; f 'nin başterimidir.

Not : $lp(0) = lc(0) = lt(0) = 0$ olarak alınacaktır.

$f, g \in k[x_1, x_2, \dots, x_n]$ olmak üzere ;

$$lp(fg) = lp(f)lp(g)$$

$$lc(fg) = lc(f)lc(g)$$

$$lt(fg) = lt(f)lt(g)$$

dir.

Örnek 3.2.5 $f = 2x^2yz + 3xy^3 - 2x^3$ ve $x > y > z$ olsun.

(i) *lex* sıralamasına göre ;

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

$$lc(f) = -2$$

$$lt(f) = -2x^3$$

dır.

(ii) *deg lex* sıralamasına göre ;

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

$$lc(f) = 2$$

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

dır.

3.3 $k[x_1, x_2, \dots, x_n]$ Polinomlar Halkası Üzerinde Bölme Algoritması

Tanım 3.3.1 $f, g, h \in k[x_1, x_2, \dots, x_n]$ ve $g \neq 0$ olsun. Eğer $lp(g), f$ 'de gözüken sıfırdan farklı bir X terimini bölerse ve

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

ise “ f, g yardımıyla h 'ye indirgenir” denir ve “ $f \xrightarrow{g} h$ ” ile gösterilir.

Örnek 3.3.2 $f = y^2x + 4yx - 3x^2$ ve $g = 2y + x + 1$ $Q[x, y]$ 'de iki polinom olsun.

$Q[x, y]$ üzerinde $y > x$ sırasında derece-sözlük sıralaması olsun.

O zaman $lp(g) = y$ dir. y hem y^2x hem de $4yx$ i böler. X olarak bunlardan

birisi seçilebilir. $X = y^2x$ olsun.

$$h = f - \frac{X}{lt(g)} g = f - \frac{y^2 x}{2y} (2y + x + 1)$$

$$h = \frac{7}{2} yx - 3x^2 - \frac{1}{2} yx^2$$

olur. Böylece $f \xrightarrow{g} h = \frac{7}{2} yx - 3x^2 - \frac{1}{2} yx^2$ elde edilir. $X = 4yx$ seçilseydi başka bir h polinomu bulunacaktı. Dolayısıyla bir f polinomu için indirgeme işlemi tek değildir.

İndirgeme işlemine devam edelim:

$$h_1 = h = \frac{7}{2} yx - 3x^2 - \frac{1}{2} yx^2 \text{ olsun.}$$

$$lp(g) = y \text{ hem } \frac{7}{2} yx \text{ i hem de } -\frac{1}{2} yx^2 \text{ yi böler.}$$

$$X = -\frac{1}{2} yx^2 \text{ olsun.}$$

$$h_2 = h_1 - \frac{X}{lt(g)} g = \frac{7}{2} yx - 3x^2 - \frac{1}{2} yx^2 - \frac{-\frac{1}{2} yx^2}{2y} (2y + x + 1)$$

$$h_2 = \frac{7}{2} yx + \frac{1}{4} x^3 - \frac{11}{4} x^2$$

olur. Böylece

$$f \xrightarrow{g} \frac{7}{2} yx - 3x^2 - \frac{1}{2} yx^2 \xrightarrow{g} \frac{7}{2} yx + \frac{1}{4} x^3 - \frac{11}{4} x^2$$

elde edilir. Tekrar h_2, g yardımıyla bir h_3 polinomuna indirgenebilir.

$$lp(g) = y, \frac{7}{2} yx \text{ i böldüğünden } X = \frac{7}{2} yx \text{ olsun.}$$

$$h_3 = h_2 - \frac{X}{lt(g)} g = \frac{1}{4} x^3 - \frac{9}{2} x^2 - \frac{7}{4} x$$

elde edilir. Bu son h_3 polinomundaki hiçbir terim artık $lp(g) = y$ ile bölünmediği için işlem bu adımda durur.

$$f \xrightarrow{g} \frac{7}{2}yx - 3x^2 - \frac{1}{2}yx^2 \xrightarrow{g} \frac{7}{2}yx + \frac{1}{4}x^3 - \frac{11}{4}x^2 \xrightarrow{g} \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$$

indirgeme işlemleri elde edilir.

Örnek 3.3.3 $Q[x, y]$ 'de $f = 6x^2y - x + 4y^3 - 1$ ve $g = 2xy + y^3$ polinomlarını alalım. $Q[x, y]$ üzerinde $x > y$ sırasında derece-sözlük sıralaması var olsun.

O zaman $lp(g) = xy$ 'dir. xy , $6x^2y$ 'yi böler. Dolayısıyla $X = 6x^2y$ olur.

$$h = f - \frac{X}{lt(g)} g = f - \frac{6x^2y}{2yx} (2xy + y^3)$$

$$h = f - 3xg$$

$$h = 6x^2y - x + 4y^3 - 1 - 3x(2xy + y^3)$$

$$h = -x + 4y^3 - 1 - 3xy^3$$

Böylece $f \xrightarrow{g} h = -x + 4y^3 - 1 - 3xy^3$ elde edilir. İndirgeme işlemini devam ettirelim :

$h_1 = h = -x + 4y^3 - 1 - 3xy^3$ olsun. $lp(g) = xy$, $-3xy^3$ 'ü böler. $X = -3xy^3$ olsun.

$$h_2 = h_1 - \frac{X}{lt(g)} g = -x + 4y^3 - 1 - 3xy^3 - \left(\frac{-3xy^3}{2xy} (2xy + y^3) \right)$$

$$h_2 = -x + 4y^3 - 1 - 3xy^3 + 3xy^3 + \frac{3}{2}y^5$$

$$h_2 = -x + 4y^3 - 1 + \frac{3}{2}y^5$$

h_2 polinomundaki hiçbir terim artık $lp(g) = xy$ ile bölünmediği için işlem bu adımda durur. Dolayısıyla,

$$f \xrightarrow{g} -x + 4y^3 - 1 - 3xy^3 \xrightarrow{g} -x + 4y^3 - 1 + \frac{3}{2}y^5$$

indirgeme işlemleri elde edilir.

Tanım 3.3.4 $f, h, f_1, f_2, \dots, f_s \in k[x_1, \dots, x_n]$ ve $f_i \neq 0$ olsun. $F = \{f_1, \dots, f_s\}$ olsun.

Eğer $i_1, i_2, \dots, i_t \in \{1, \dots, s\}$ indislerinin ve $h_1, h_2, \dots, h_{t-1} \in k[x_1, x_2, \dots, x_n]$ polinomlarının bir dizisi varsa ve

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

ise “ f, F yardımıyla h 'ye indirgenir.” denir ve “ $f \xrightarrow{F} +h$ ” ile gösterilir.

Örnek 3.3.5 $f_1 = yx - y$ ve $f_2 = y^2 - x \in Q[x, y]$ olsun. $y > x$ sırasında derece-sözlük sırası alınsın. $F = \{f_1, f_2\}$ ve $f = y^2x$ olsun.

1.DURUM $X = y^2x$ olsun. $lp(f_1) = yx$, y^2x i böler. Böylece

$$h_1 = f - \frac{X}{lt(f_1)} f_1 = y^2x - \frac{y^2x}{yx}(yx - y) = y^2$$

elde edilir. Yani;

$$f \xrightarrow{f_1} y^2$$

dir.

$lp(f_2) = y^2$, $X = y^2$ yi böler. Böylece

$$h_2 = h_1 - \frac{X}{lt(f_2)} f_2 = y^2 - \frac{y^2}{y^2}(y^2 - x) = x$$

Dolayısıyla ;

$$f \xrightarrow{f_1} y^2 \xrightarrow{f_2} x \text{ ve sonuç olarak } f \xrightarrow{F} +x \text{ elde edilir.}$$

2.DURUM $X = y^2x$ olsun. $lp(f_2) = y^2$, y^2x i böler. Böylece

$$h_1 = f - \frac{X}{lt(f_2)} f_2 = y^2x - \frac{y^2x}{y^2}(y^2 - x) = x^2$$

elde edilir. Yani $f \xrightarrow{f_2} x^2$ dir. $lp(f_1)$ ve $lp(f_2)$, x^2 yi bölmediği için $f \xrightarrow{F} +x^2$ olur.

Tanım 3.3.6 Bir τ polinomuna, sıfırdan farklı polinomların kümesi

$F = \{f_1, f_2, \dots, f_s\}$ 'ye göre indirgenmiş denir, eğer $\tau = 0$ ya da τ de gözükün

terimlerin hiçbirisi $lp(f_i), i = \{1, \dots, s\}$ tarafından bölünmez ise, yani τ 'ye F 'ye göre f için kalan denir.

Örnek 3.3.7 $Q[x, y]$ 'de $f = y^2x, f_1 = yx - y, f_2 = y^2 - x$, derece-sözlük sıralamasına göre $x < y$ ve $F = \{f_1, f_2\}$ olsun.

$f \xrightarrow{F} x$ olduğunu gösterelim.

$$y^2x \xrightarrow{f_1} y^2 \xrightarrow{f_2} x$$

$$h_1 = y^2x - \frac{y^2x}{yx}(yx - y) = y^2$$

$$h = y^2 - \frac{y^2}{y^2}(y^2 - x) = x$$

dir.

Örnek 3.3.8 $Q[x, y]$ 'de $f = y^2x, f_1 = yx - y, f_2 = y^2 - x, F = \{f_1, f_2\}$ derece-sözlük sıralamasına göre $x < y$ olsun.

$lp(f_1) = yx, lp(f_2) = y^2$ olup aşağıdaki indirgemeleri düşünelim.

$$f \xrightarrow{f_1} h_1$$

ile

$$f - \frac{y^2x}{yx}(yx - y) = -x + y^2 = h_1$$

elde edilir.

$$f \xrightarrow{f_1} -x + y^2 \xrightarrow{f_2} h_2 = 0$$

ile

$$h_1 - \frac{y^2}{y^2}(y^2 - x) = 0$$

elde edilir. O hâlde $f - yf_1 - 1.f_2 = 0$ olup

$$f = yf_1 + f_2, f \in \langle f_1, f_2 \rangle \text{ dir.}$$

Sonuç 0 ise $f \in \langle f_1, f_2 \rangle$ dir.

Örnek 3.3.9 $f = y^2x - x \in Q[x, y], I = \langle f_1, f_2 \rangle \subseteq Q[x, y],$

$f_1 = yx - y, f_2 = y^2 - x, F\{f_1, f_2\}$ ve derece-sözlük sıralamasına göre $x < y$ olsun.

$f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$ böylece $f \xrightarrow{F} 0$, indirgemelerine göre $f = yf_1 + f_2$ ve

$r = 0$ olduğundan $f \in I = \langle f_1, f_2 \rangle$ dır.

4. DEĞİŞMELİ GRÖBNER TABAN TEORİSİ

4.1 Değişmeli Gröbner Tabanlar

İlk olarak Buchberger, $k[x_1, x_2, \dots, x_n]$ değişmeli polinomlar halkası üzerinde Gröbner taban tanımını verdi ve $k[x_1, x_2, \dots, x_n]$ 'nin bir I ideali alındığında bu I ideali için bir Gröbner taban üreten algoritmayı geliştirdi. Buchberger' in bu çalışmaları “Klasik Gröbner Taban Teorisi” ya da “Değişmeli Gröbner Taban Teorisi” olarak bilinmektedir.

Tanım 4.1.1 $G = \{g_1, g_2, \dots, g_s\}, k[x_1, x_2, \dots, x_n]$ 'nin sıfırdan farklı polinomlarının bir kümesi olsun. $I, k[x_1, x_2, \dots, x_n]$ 'in bir ideali ve $G \subseteq I$ olsun. Eğer $\forall f \in I$ için $(f \neq 0)$ $lp(f)$ 'yi bölen bir $lp(g_i)$ $1 \leq i \leq s$ varsa G 'ye göre indirgenmiş olan sıfırdan farklı hiçbir polinom yoktur.

G bir Gröbner taban olsun demekle ; G 'nin G tarafından üretilen $\langle G \rangle$ ideali için bir Gröbner taban olduğu anlaşılabacaktır.

Tanım 4.1.2 $S \subseteq k[x_1, \dots, x_n]$ olsun.

$$LT(S) = \langle lt(s) \mid s \in S \rangle$$

İdeale S 'nin **başterim ideali** denir.

Teorem 4.1.3 $I, k[x_1, x_2, \dots, x_n]$ 'nin bir ideali olsun. Sıfırdan farklı polinomların bir kümesi $G = \{g_1, g_2, \dots, g_t\}$ ve $G \subseteq I$ olsun. Aşağıdaki ifadeler denktir.

i) G, I için bir Gröbner tabandır.

ii) $f \in I \Leftrightarrow f \xrightarrow{G} +0$

$$\text{iii)} \quad f \in I \Leftrightarrow f = \sum_{i=1}^t h_i g_i, lp(f) = \max(lp(h_i)lp(g_i)) \quad (1 < i < t)$$

$$\text{iv)} \quad LT(G) = LT(I)$$

Sonuç 4.1.4 Eğer $G = \{g_1, g_2, \dots, g_t\}, I$ ideali için bir Gröbner taban ise $\langle g_1, \dots, g_t \rangle = I$ olur.

İspat Herbir g_i I 'ya ait olduğu için, $\langle g_1, g_2, \dots, g_t \rangle \subset I$ dır. $f \in I$ olsun. Teorem

3.1.3'den $f = \sum_{i=1}^t h_i g_i$ olacak şekilde $h_i \in k[x_1, \dots, x_n]$ vardır. Böylece

$f \in \langle g_1, \dots, g_t \rangle$ elde edilir. O hâlde $I = \langle g_1, \dots, g_t \rangle$ olur.

Sonuç 4.1.5 $I = \langle f_1, f_2, \dots, f_s \rangle, k[x]$ polinomlar halkası üzerinde bir ideal ve $G = \{g = ebob\{f_1, f_2, \dots, f_s\}\}$ olsun. $I = \langle g \rangle$ olduğu için G, I için Gröbner tabandır.

Not ; $k[x_1, \dots, x_n]$ 'in sıfırdan farklı her I ideali bir Gröbner tabana sahiptir.

Teorem 4.1.6 $G = \{g_1, \dots, g_t\}, k[x_1, \dots, x_n]$ 'de sıfırdan farklı polinomların kümesi olsun.

G , Gröbner tabandır $\Leftrightarrow \forall f \in k[x_1, \dots, x_n]$ polinomu için f 'nin G 'ye bölümündeki kalan tektir.

4.1.7 Örnek $f = y^2x - x, f_1 = yx - y$ ve $f_2 = y^2 - x \in Q[x, y]$ olsun. $F = \{f_1, f_2\}$ ve $y > x$ sırasında derece-sözlük sıralaması alınsın.

$$f \xrightarrow{F} +0 \text{ ve } f \xrightarrow{F} +x^2 - x$$

Bu yüzden f polinomunun F 'ye göre bölümündeki kalan tek olmadığından, F bir Gröbner taban değildir.

4.2 S-Polinomu ve Buchberger Algoritması

Tanım 4.2.1 $k[x_1, \dots, x_n]$ 'deki sıfırdan farklı her f, g polinomları için;

$L = ekok\{lp(f), lp(g)\}$ olsun.

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

polinomuna f ve g polinomunun S-polinomu denir. Herhangi iki f ve g polinomu için $S(f, g) \in \langle f, g \rangle$ olduğu açıktır.

Örnek 4.2.2 $f = 2yx - y$, $g = 3y^2 - x \in Q[x, y]$ ve $y > x$ sırasında derece-sözlük sıralaması alınsın. O zaman;

$$L = \text{ekok}\{lp(f), lp(g)\} = \text{ekok}\{yx, y^2\} = y^2x \quad \text{ve}$$

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g = \frac{y^2x}{2yx} f - \frac{y^2x}{3y^2} g = -\frac{1}{2}y^2 + \frac{1}{3}x^2$$

olur.

Teorem 4.2.3 (Buchberger) $k[x_1, \dots, x_n]$ 'deki sıfırdan farklı polinomların bir kümesi $G = \{g_1, \dots, g_t\}$ olsun. O zaman $G, I = \langle g_1, \dots, g_t \rangle$ için bir Gröbner tabandır ancak ve ancak $\forall i \neq j$ için $S(g_i, g_j) \xrightarrow{G} +0$ dır.

Örnek 4.2.4 $f_1 = xy - x, f_2 = x^2 - y \in Q[x, y]$ ve $x < y$ sırasında derece-sözlük sıralaması alınsın. $F = \{f_1, f_2\}$ olsun.

$$S(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{F} +y^2 - y$$

olur ve $y^2 - y$ F 'e göre indirgenmiştir.

$$f_3 = y^2 - y \text{ ve } F' = \{f_1, f_2, f_3\} \text{ olsun.}$$

O zaman $S(f_1, f_2) \xrightarrow{F'} +0, S(f_1, f_3) = yf_1 - xf_3 = 0$ ve

$$S(f_2, f_3) = y^2f_2 - x^2f_3 = -y^3 + x^2y \xrightarrow{F'} x^2y - y^2 \xrightarrow{F'} 0$$

elde edilir. Dolayısıyla $F' = \{f_1, f_2, f_3\}$ $I = \langle F' \rangle$ için bir Gröbner tabanı olur. O hâlde bir G tabanı elde etmek için aşağıdaki algoritma verilebilir.

Buchberger Algoritması

INPUT : $F = \{f_1, \dots, f_s\} \subseteq k[x_1, \dots, x_n], 1 \leq i \leq s$ için $f_i \neq 0$

OUTPUT : $G = \{g_1, \dots, g_t\}, \langle f_1, \dots, f_s \rangle$ için bir Gröbner taban

INITIALIZATION : $G := F, \beta := \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$

WHILE $\beta \neq \emptyset$ **DO**

Herhangi bir $\{f, g\} \in \beta$ 'yi seç.

$$\beta := \beta \cap \{\{f, g\}\}'$$

$$S(f, g) \xrightarrow{G} +h ; h, G \text{ 'ye göre indirgenmiş}$$

IF $h \neq 0$ **THEN**

$$\beta := \beta \cup \{\{u, h\} \mid u \in G\}$$

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

Bu tabloya göre ; $0 \neq f_i (1 \leq i \leq s)$ için $F = \{f_1, \dots, f_s\}$ olsun. Buchberger Algoritması $I = \langle f_1, \dots, f_s \rangle$ ideali için bir Gröbner taban üretir.

Örnek 4.2.5 $f_1 = xy - x, f_2 = -y + x^2 \in Q[x, y]$ ve $Q[x, y]$ üzerinde $y > x$ sırasında sözlük sıralaması olsun. $I = \langle f_1, f_2 \rangle$ ideali için Gröbner taban aşağıdaki şekilde bulunur.

INITIALIZATION :

$$G := \{f_1, f_2\},$$

$$\beta := \{\{f_1, f_2\}\}$$

1.WHILE İŞLEMİ : $\{f_1, f_2\}$ 'yi seç.

$$\beta := \beta \cap \{\{f_1, f_2\}\}' = \emptyset$$

$$S(f_1, f_2) = x^3 - x \xrightarrow{G} +x^3 - x = h \quad (x^3 - x, G \text{ 'ye göre indirgenmiştir.})$$

$$h \neq 0 \text{ olduğu için } f_3 := x^3 - x$$

$$\beta := \{\{f_1, f_3\}, \{f_2, f_3\}\} \neq \emptyset$$

$$\beta := \{f_1, f_2, f_3\}$$

2.WHILE İŞLEMİ $\{f_1, f_3\}$ 'ü seç.

$$\beta := \{\{f_2, f_3\}\}$$

$$S(f_1, f_3) = xy - x^3 \xrightarrow{G} +0 = h$$

3.WHILE İŞLEMİ $\{f_2, f_3\}$ 'ü seç.

$$\beta := \emptyset$$

$$S(f_2, f_3) = -x^5 + xy \xrightarrow{G} +0 = h$$

$\beta = \emptyset$ olduğu için algoritma durur. Böylece $\{f_1, f_2, f_3\}$, $\langle f_1, f_2 \rangle$ ideali için bir Gröbner taban olur.

4.3 İndirgenmiş Gröbner Tabanlar

Buchberger Algoritması ile $k[x_1, \dots, x_n]$ 'deki sıfırdan farklı bir idealin bir Gröbner tabanı elde edilmektedir. Ancak bu Gröbner taban tek değildir. Buchberger Algoritmasında sonucu etkileyecek olan iki durum vardır. Bunlardan biri; test etmeye başlanan polinomların sırası değiştirilirse bu sıra Bölme Algoritmasını etkileyecek ve farklı kalanlar elde edileceği için başka bir Gröbner taban bulunacaktır. İkinci olarak; S-polinomları hesaplanan polinomların sırası değiştirilirse yine farklı bir Gröbner taban elde edilecektir. Bu yüzden;

Tanım 4.3.1 $G = \{g_1, \dots, g_t\}$, I ideali için bir Gröbner taban olsun. Eğer bütün i 'ler için $lc(g_i) = 1$ ve bütün $i \neq j$ için $lp(g_i), lp(g_j)$ ' yi bölmez ise G 'ye **minimal Gröbner taban** denir.

Sonuç 4.3.2 $G = \{g_1, \dots, g_t\}$ bir ideali için bir Gröbner taban olsun. G ' den bir minimal Gröbner taban elde etmek için ; $g_i \in G$ olmak üzere herhangi bir $i \neq j$ için $lp(g_i), lp(g_j)$ tarafından bölünürse g_i, G 'den çıkartılır. Bu şekilde tüm g_i 'ler incelenir ve geriye kalan tüm $g_i \in G$ elemanları $lc(g_i)$ 'ye bölünerek $lc(g_i)=1$ olması sağlanır.

Eğer $G = \{g_1, \dots, g_t\}$ ve $F = \{f_1, \dots, f_s\}$ bir ideali için iki minimal Gröbner taban ise $t = s$ ve $i = 1, \dots, t$ için;

$$lp(f_i) = lp(g_i) \quad \text{dir.}$$

Tanım 4.3.3 $G = \{g_1, \dots, g_t\}$ bir I ideali için bir Gröbner taban olsun. Eğer tüm $lc(g_i)=1$ ve g_i 'ler $G - \{g_i\}$ 'ye göre indirgenmiş iseler G 'ye indirgenmiş Gröbner Taban denir. Dolayısıyla indirgenmiş Gröbner tabanlar minimal Gröbner tabanlardır.

$G = \{g_1, \dots, g_t\}$ bir I ideali için bir minimal Gröbner taban olsun.

Aşağıdaki indirgeme işlemleri düşünölsün.

$$g_1 \xrightarrow{H_1} +h_1 \quad ; \quad H_1 = \{g_2, \dots, g_t\} \text{ 'e göre indirgenmiş}$$

$$g_2 \xrightarrow{H_2} +h_2 \quad ; \quad H_2 = \{h_1, g_3, \dots, g_t\} \text{ 'e göre indirgenmiş}$$

.

.

$$g_t \xrightarrow{H_t} +h_t \quad ; \quad H_t = \{h_1, h_2, \dots, h_{t-1}\} \text{ 'e göre indirgenmiş}$$

O zaman $H = \{h_1, h_2, \dots, h_t\}$ indirgenmiş Gröbner tabandır.

5. GRÖBNER TABANLARIN UYGULAMALARI

Bu bölümde ; $k[x_1, \dots, x_n]$ içinde bazı basit hesaplamalar yapmak için Gröbner taban yardımıyla geliştirilmiş metodlar verilecektir.

5.1 İdeale Ait Olma Problemi

$I = \langle f_1, \dots, f_s \rangle, k[x_1, \dots, x_n]$ 'nin bir ideali olsun. Eğer $f \in k[x_1, \dots, x_n]$ ise f 'nin I ya ait olup olmadığını belirleme problemi “ideale ait olma problemi” olarak bilinir. Eğer $f \in I$ ise $f = v_1 f_1 + \dots + v_s f_s$ olacak şekildeki $v_1, \dots, v_s \in k[x_1, \dots, x_n]$ nasıl hesaplanır? Amaç , f 'nin hangi şartlarda I 'ya ait olduğunu belirlemek ve $f = v_1 f_1 + \dots + v_s f_s$ 'yi sağlayan $v_1, \dots, v_s \in k[x_1, \dots, x_n]$ polinomları elde etmek olacaktır. $F = \{f_1, \dots, f_s\}$ olsun. Herhangi bir terim sıralamasına göre;

$$G = \{g_1, \dots, g_t\}, I = \langle F \rangle \text{ için}$$

$$f \in I \Leftrightarrow f \xrightarrow{G} +0$$

olup böylece ideale ait olma problemi çözülmüş olur. f 'nin G 'ye bölümü gerçekleştirilirse $f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t$ olacak şekilde $u_1, \dots, u_t \in k[x_1, \dots, x_n]$ polinomları elde edilir.

Buchberger Algoritması, sadece bir $I = \langle f_1, \dots, f_s \rangle$ ideali için bir $\{g_1, \dots, g_t\}$ Gröbner tabanı elde etmekle kalmaz, ayrıca polinomların $t \times s$ tipinden bir μ matrisini inşa eder öyle ki,

$$\begin{bmatrix} g_1 \\ \vdots \\ g_t \end{bmatrix} = \mu \begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix}$$

olur.

Örnek 5.1.1 $f_1 = x^2 y - y + x$ ve $f_2 = xy^2 - x$ $\mathbb{Q}[x, y]$ 'de iki polinom ve $I = \langle f_1, f_2 \rangle$ olsun. $x < y$ sırasında derece – sözlük terim sıralaması düşünölsün. Algoritma yardımıyla üreteç kümesindeki yeni polinomların inşasını veren doğrusal kombinasyonlar izlenecektir.

INITIALIZATION: $G := \{f_1, f_2\}$

$$G := \{\{f_1, f_2\}\}$$

1.WHILE İŞLEMİ: $\{f_1, f_2\}$ 'yi seç.

$$G := G \cap \{\{f_1, f_2\}\}' = \emptyset$$

$$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + xy + x^2$$

$$f_3 := -y^2 + xy + x^2, f_3 = yf_1 - xf_2$$

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

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

2.WHILE İŞLEMİ: $\{f_1, f_3\}$ 'ü seç.

$$G := G \cap \{\{f_1, f_2\}\}' = \{\{f_2, f_3\}\}$$

$$S(f_1, f_3) = yf_1 + x^2 f_3 = x^3 y + x^4 - y^2 + xy$$

$$\xrightarrow{f_1} x^4 - y^2 + 2xy - x^2 \quad (G' \text{ ye göre indirgenmiştir.})$$

$$f_4 := x^4 - y^2 + 2xy - x^2$$

$$f_4 = (yf_1 + x^2 f_3) - xf_1$$

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

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

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

3.WHILE İŞLEMİ: $\{f_2, f_3\}$ 'ü seç.

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

$$S(f_2, f_3) = f_2 + xf_3 = x^2 y + x^3 - x \xrightarrow{f_1} x^3 + y - 2x$$

(G' ye göre indirgenmiştir.)

$$f_5 := x^3 + y - 2x, f_5 = (f_2 + xf_3) - f_1 = (xy - 1)f_1 + (-x^2 + 1)f_2$$

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

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

Böylece G 'deki her bir çiftin S – polinomları sıfıra indirgenir ve bu durumda $G := \{f_1, f_2, f_3, f_4, f_5\}$ I için bir Gröbner taban olur. Ve $lt(f_3), lt(f_2)$ 'yi ; $lt(f_5), lt(f_4)$ 'ü böldüğünden $\{f_1, f_3, f_5\}$ de I için bir Gröbner tabandır. Yukarıdaki hesaplama işlemleri sonucunda f_1 ve f_2 'nin doğrusal kombinasyonları ile f_3 ve f_5 elde edilmiştir. Böylece

$$\mu = \begin{pmatrix} 1 & 0 \\ y & -x \\ xy-1 & -x^2+1 \end{pmatrix}$$

alınırsa

$$\begin{pmatrix} f_1 \\ f_3 \\ f_5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ y & -x \\ xy-1 & -x^2+1 \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$$

elde edilir. Şimdi,

$$f = x^4 y - 2x^5 + 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^2 y + 2x^3 - y + 2x$$

polinomu alınsın.

$$\begin{aligned} f &\xrightarrow{f_1, x^2} -2x^5 + 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 2x^2 y + x^3 - y + 2x \\ &\xrightarrow{f_5, -2x^2} 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x \\ &\xrightarrow{f_1, 2y} -2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x + 2y^2 - 2xy \\ &\xrightarrow{f_5, -2y} -2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x + 4y^2 - 6xy \\ &\xrightarrow{f_5, -2x} -2y^3 + 4xy^2 - 3x^3 - y + 2x + 4y^2 - 4xy - 4x^2 \\ &\xrightarrow{f_3, 2y} 2xy^2 - 3x^3 - y + 2x + 4y^2 - 4xy - 4x^2 - 2x^2 y \\ &\xrightarrow{f_3, -2x} -x^3 - y + 2x + 4y^2 - 4xy - 4x^2 \\ &\xrightarrow{f_5, -1} 4y^2 - 4xy - 4x^2 \\ &\xrightarrow{f_3, -4} 0 \end{aligned}$$

Buradan $f \xrightarrow{f_i, X} h$; f 'den seçilen bir X terimi ve f_i yardımıyla f 'nin h 'ya indirgenmesi anlamına gelmektedir. Böylece;

$$\begin{aligned} f &= x^2 f_1 - 2x^2 f_5 + 2y f_1 - 2y f_5 - 2x f_5 + 2y f_3 - f_5 - 4f_3 \\ f &= (x^2 + 2y) f_1 + (2y - 2x - 4) f_3 + (-2x^2 - 2y - 2x - 1) f_5 \end{aligned}$$

olur ki, $f \in I$ elde edilir.

$yf_1 - xf_2 = f_3$ ve $(xy-1)f_1 + (-x^2+1)f_2 = f_5$ eşitlikleri kullanılırsa;

$$\begin{aligned} f &= (x^2 + 2y)f_1 + (2y - 2x - 4)(yf_1 - xf_2) + (-2x^2 - 2y - 2x - 1)((xy-1)f_1 + (x^2+1)f_2) \\ f &= (-2x^3y - 2xy^2 - 2x^2y + 2y^2 - 3xy + 3x^2 + 2x + 1)f_1 \\ &+ (2x^4 + 2x^2y + 2x^3 - 2xy + x^2 - 2y + 2x - 1)f_2 \end{aligned}$$

elde edilir.

Her ideal bir tek indirgenmiş Gröbner tabana sahiptir. Dolayısıyla; $I = J$ olması için gerek ve yeter koşul I ve J 'nin aynı indirgenmiş Gröbner tabana sahip olmasıdır.

5.2 Radikale Ait Olma Problemi

İdeale ait olma probleminde olduğu gibi $I = \langle f_1, \dots, f_s \rangle, k[x_1, \dots, x_n]$ 'nin bir ideali olmak üzere herhangi bir $f \in k[x_1, \dots, x_n]$ polinomunun ne zaman $\sqrt{I}$ 'ya ait olduğu sorusu incelenecektir.

Tanım 5.2.1 $I, k[x_1, \dots, x_n]$ 'nin bir ideali olsun.

I 'nın **radikali** $\sqrt{I} = \{f \in k[x_1, \dots, x_n] \mid f^n \in I\}$ {olacak şekilde bir n pozitif tamsayısı vardır.} ile tanımlanır.

Not : $\sqrt{I}, k[x_1, \dots, x_n]$ 'nin bir idealidir.

Teorem 5.2.2 $I = \langle f_1, \dots, f_s \rangle, k[x_1, \dots, x_n]$ 'nin bir ideali ve $f \in k[x_1, \dots, x_n]$ olsun. O zaman $f \in \sqrt{I}$ olması için gerek ve yeter şart koşul w yeni bir bilinmeyen olmak üzere $I \in \langle f_1, \dots, f_s, 1 - wf \rangle \subseteq k[x_1, \dots, x_n, w]$ olmasıdır. [Adams and Loustanau, 1994]

Böylece $f \in \sqrt{I}$ olup olmadığına bakmak için ilk önce $\langle f_1, \dots, f_s, 1 - wf \rangle$ ideali için G indirgenmiş Gröbner taban hesaplanmalıdır. Eğer $I \in G$ ise o zaman $f \in \sqrt{I}$ 'dır , aksi takdirde $f \notin \sqrt{I}$ 'dır.

Örnek5.2.3 $\mathbb{Q}[x, y, z]$ 'de $I = \langle x^2z^2 + x^3, xz^4 + 2x^2z^2 + x^3, y^2z - 2yz^2 + z^3, x^2y + y^3 \rangle$ ve $J = \langle xz^2 + x^2, yz^2 - z^3, x^2y - x^2z, y^4 - x^3, x^4z - x^3z, z^6 + x^4, x^5 - x^4 \rangle$ iki ideal olsun. O zaman $\sqrt{I} = \sqrt{J}$ dir.

$$f_1 = x^2z^2 + x^3, f_2 = xz^4 + 2x^2z^2 + x^3, f_3 = y^2z - 2yz^2 + z^3, f_4 = x^2y + y^3$$

ve

$$g_1 = xz^2 + x^2, g_2 = yz^2 - z^3, g_3 = x^2y - x^2z, g_4 = y^4 - x^3, g_5 = x^4z - x^3z, g_6 = z^6 + x^4, g_7 = x^5 - x^4$$

olsun. w değişken olmak üzere $x < y < z < w$ sırasında derece-sözlük sıralaması göz önüne alınsın.

$$\langle g_1, g_2, g_3, g_4, g_5, g_6, g_7, 1 - wf_1 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } f_1 \in \sqrt{J},$$

$$\langle g_1, g_2, g_3, g_4, g_5, g_6, g_7, 1 - wf_2 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } f_2 \in \sqrt{J},$$

$$\langle g_1, g_2, g_3, g_4, g_5, g_6, g_7, 1 - wf_3 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } f_3 \in \sqrt{J},$$

$$\langle g_1, g_2, g_3, g_4, g_5, g_6, g_7, 1 - wf_4 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } f_4 \in \sqrt{J}$$

Dolayısıyla $I = \langle f_1, f_2, f_3, f_4 \rangle \subseteq \sqrt{J}$ dir. Bu yüzden $\sqrt{I} \subseteq \sqrt{J}$ olur.

$$\langle f_1, f_2, f_3, f_4, 1 - wg_1 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_1 \in \sqrt{I},$$

$$\langle f_1, f_2, f_3, f_4, 1 - wg_2 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_2 \in \sqrt{I},$$

$$\langle f_1, f_2, f_3, f_4, 1 - wg_3 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_3 \in \sqrt{I},$$

$$\langle f_1, f_2, f_3, f_4, 1 - wg_4 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_4 \in \sqrt{I},$$

$$\langle f_1, f_2, f_3, f_4, 1 - wg_5 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_5 \in \sqrt{I},$$

$$\langle f_1, f_2, f_3, f_4, 1 - wg_6 \rangle \text{ için indirgenmiş Gröbner taban } \{1\} \text{ ve } g_6 \in \sqrt{I},$$

$\langle f_1, f_2, f_3, f_4, 1 - wg_7 \rangle$ için indirgenmiş Gröbner taban $\{1\}$ ve $g_7 \in \sqrt{I}$,

$J = \langle g_1, g_2, g_3, g_4, g_5, g_6, g_7 \rangle \subseteq \sqrt{I}$ olur. Dolayısıyla $\sqrt{J} \subseteq \sqrt{I}$ olup sonuç olarak

$\sqrt{I} = \sqrt{J}$ elde edilir.



KAYNAKLAR

Buchberger, B., (1985). *Gröbner bases: an algorithmic method in polynomial ideal theory*, in: N.K. Bose,ed. *Recent Trends in Multidimensional System Theory*, Reidel Dordrecht.

Bergman, G., (1979), *The diamond lemma for ring theory*, *Adv. Math.*, 9(1978), 178-218.

Adams, W. W. and Loustaunau, P., (1994). *An introduction to Gröbner bases*, *Graduate Studies in Math*, Vol. 3, AMS, 1-60.

Dummit, D.S. and Foote , R.M., (1999). *Abstract algebra*, Prentice Hall, Upper Saddle River, N.J. 07458

Green,E.L., (1993). *An introduction to commutative Gröbner bases*, in: *Computational algebra*.

Cox, D., Little, J. and O'shea, D., (1992). *Ideals, Varieties, and Algorithms*, Springer-Verlag.

Orhan N., (2001). *On Gröbner Bases*.

Mansuroğlu N., (2009). *Gröbner Bases and Reduction Techniques*, 1-34.

Sturmfels, B.,(2005).*What is a Gröbner Basis?*

Ünsalan C., Erçil A., (1999). *Parametrik ve Örtük Çokterimli Gösterimler Arası Dönüşümler (Conversions between parametric and implicit forms)*.



