



**GRÖBNER TABAN VE
BİLGİSAYARDAKİ UYGULAMALARI
YÜKSEK LİSANS TEZİ**

Merve ALGI

Danışman
Dr. Öğr. Üyesi Fatma KAYNARCA

MATEMATİK ANABİLİM DALI

Haziran 2023

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

GRÖBNER TABAN VE BİLGİSAYARDAKİ
UYGULAMALARI

Merve ALGI

Danışman

Dr. Öğr. Üyesi Fatma KAYNARCA

MATEMATİK ANABİLİM DALI

Haziran 2023

TEZ ONAY SAYFASI

Merve ALGI tarafından hazırlanan “Gröbner Taban ve Bilgisayardaki Uygulamaları” adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 21.06.2023 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **Matematik Anabilim Dalı’nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Dr. Öğr. Üyesi Fatma KAYNARCA

Başkan : Prof. Dr. Nil ORHAN ERTAŞ
Bursa Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fak.

Üye : Dr. Öğr. Üyesi Esra GÜLLE
Afyon Kocatepe Üniv. Fen Edebiyat Fak.

Üye : Dr. Öğr. Üyesi Fatma KAYNARCA
Afyon Kocatepe Üniv. Fen Edebiyat Fak.

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu’nun
...../...../ 2023 tarih ve
..... sayılı kararıyla onaylanmıştır.

Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

21/06/2023

Merve ALGI

ÖZET

Yüksek Lisans Tezi

GRÖBNER TABAN VE BİLGİSAYARDAKİ UYGULAMALARI

Merve ALGI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Fatma KAYNARCA

Bu tez, Gröbner taban teorisinin cebirsel yapısının incelenmesinin yanısıra farklı programlama dillerindeki kullanımını da içermektedir. İlk bölümde, Gröbner taban teorisinin tarihsel gelişim sürecinin anlatıldığı giriş kısmı yer almaktadır. İkinci bölümde, tez çalışması için gerekli olan temel tanımlar ve özellikler verilmiştir. Üçüncü bölümde, ilk olarak Gröbner taban kavramı tanıtılarak karakterizasyonları verilmiş, daha sonra Gröbner taban hesaplamaya yarayan bir metod olan Buchberger algoritması örneklerle açıklanmıştır. Ayrıca bir Gröbner tabandan indirgenmiş ve minimum adı altında iki farklı Gröbner tabanın daha yazılabildiği gösterilmiştir. Dördüncü bölümde ise, bazı programlama dillerinde Gröbner tabanın nasıl hesaplandığı ifade edilmiş ve örnekler verilmiştir.

2023, v+58 sayfa

Anahtar Kelimeler: n değişkenli polinom halkası, Terim sıralaması, Bölme algoritması, Gröbner taban, Buchberger algoritması.

ABSTRACT

M.Sc. Thesis

GRÖBNER BASIS AND ITS APPLICATIONS ON THE COMPUTER

Merve ALGI

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Mathematics

Supervisor: Asst. Prof. Fatma KAYNARCA

This thesis includes the analysis of the algebraic structure of Gröbner's basis theory as well as its use in different programming languages. In the first chapter, there is the introduction part in which the historical development process of Gröbner basis theory is explained. In the second part, the basic definitions and features required for the thesis work are given. In the third chapter, firstly the Gröbner basis concept is introduced and its characterizations are given, then the Buchberger algorithm, which is a method for calculating the Gröbner basis, is explained with examples. In addition, it has been shown that two different Gröbner bases can be written under the name of a minimum and reduced from a Gröbner base. In the fourth chapter, how the Gröbner base is calculated in some programming languages is explained and examples are given.

2023, v+58 pages

Key Words: Polynomials ring with n variables, Term ordering, Division algorithm, Gröbner basis, Buchberger algorithm.

TEŞEKKÜR

Tez çalışmam sürecinde; değerli danışman hocamın bana sağlamış olduğu rehberlik, destek ve motivasyon sayesinde tezimi bugün ki haline getirme şansına sahip oldum. Bilgi birikimi ve tecrübesi sayesinde tez çalışmamı daha sağlam temeller üzerinde yürütme fırsatı yakaladığım; her zaman anlayışlı, sabırlı ve bana iyi bir mentor olan saygı değer hocam Sayın Dr. Öğr. Üyesi Fatma KAYNARCA'ya sonsuz teşekkürlerimi sunarım.

Tez çalışmamın değerlendirilmesinde, kıymetli vaktini ayırarak yaptığı incelemeler ve düzeltmeler sayesinde tezimi geliştirmem ve daha iyi bir hale getirme noktasında yardımlarından dolayı Prof. Dr. Nil ORHAN ERTAŞ hocama, teşekkürü bir borç bilirim.

Her zaman beni destekleyen ve tez çalışmam sürecinde özellikle moral veren, benim arkamda olduklarını sonuna kadar hissettiren annem ve babam siz benim en büyük şanslısınız. Hayatımın her alanında olduğu gibi, bu süreçte bana destek veren aileme ve sevdiklerime de en içten teşekkürlerimi sunmak istiyorum.

Merve ALGI

Afyonkarahisar 2023

İÇİNDEKİLER DİZİNİ

ÖZET	i
ABSTRACT	ii
TEŞEKKÜR	iii
İÇİNDEKİLER DİZİNİ	iv
SİMGELER DİZİNİ	v
ŞEKİLLER DİZİNİ	vi
1 GİRİŞ	1
2 ÖN BİLGİLER	7
2.1 Temel Kavramlar	7
2.2 Tek Değişkenli Polinomlar Halkası	9
2.3 Çok Değişkenli Polinomlar Halkası	16
3 GRÖBNER TABANLARI	30
3.1 Klasik Gröbner Taban Teorisi	30
3.2 Minimal Gröbner Taban	42
3.3 İndirgenmiş Gröbner Taban	44
4 GRÖBNER TABANIN BİLGİSAYARDAKİ UYGULAMALARI	47
4.1 Maple’da Gröbner Taban	47
4.2 Mathematica’da Gröbner Taban	49
4.3 CoCoA’da Gröbner Taban	51
4.4 Çizge Boyama	52
5 KAYNAKLAR	57
ÖZGEÇMİŞ	59

SİMGELER DİZİNİ

Simgeler

$\subseteq$	Altküme
$\subset$	Öz altküme
$a b$	a böler b
$\preceq$	Herhangi bir kısmi sıralama bağıntısı
$\prec$	Herhangi bir terim sıralaması
$\prec_l$	Sözlüksel sıralama
$\prec_{dl}$	Derece sözlüksel sıralama
$\prec_{rl}$	Ters sözlüksel sıralama
$\prec_{drl}$	Derece ters sözlüksel sıralama
$\prec_{grl}$	Dereceli ters sözlüksel sıralama
$\mathbb{N}$	Doğal sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
R	Herhangi bir halka
K	Herhangi bir cisim
I	Herhangi bir ideal
$\langle G \rangle$	Bir G kümesi tarafından üretilen ideal
$R[x]$	R üzerindeki tek değişkenli polinomlar halkası
$R[x_1, x_2, \dots, x_n]$	R üzerindeki n değişkenli polinomlar halkası

ŞEKİLLER DİZİNİ

Sayfa

Şekil 2.1	Tek Değişkenli Polinomlar Halkasında Bölme Algoritması	13
Şekil 2.2	Tek Değişkenli Polinomlar Halkasında Öklid Algoritması	14
Şekil 2.3	n Değişkenli Polinomlar Halkasında Bölme Algoritması	26
Şekil 3.1	Buchberger Algoritması	41
Şekil 4.1	Çizge Boyama Örneği	55
Şekil 4.2	Çizge Boyama Örneği 1	56
Şekil 4.3	Çizge Boyama Örneği 2	56
Şekil 4.4	Çizge Boyama Örneği 3	56

1. GİRİŞ

Matematikte, özellikle bilgisayar cebirinde, hesaplamalı cebirsel geometride ve hesaplamalı değişmeli cebirde önemli rol oynayan Gröbner taban kavramı; 1965 yılında Bruno Buchberger'in doktora tezinde tanıttığı ve adını tez danışmanı olan Wolfgang Gröbner'e ithaf ettiği bir kavramdır. Buchberger; doktora tezinde sadece Gröbner taban kavramını tanıtmakla kalmamış aynı zamanda bu tabanı bulmaya yarayan kendi adıyla adlandırdığı bir algoritma geliştirmiş ve bu algoritmanın doğruluğunun ve sonlandırılmasının dayandığı temel teoremi kanıtlamıştır. Uzun yıllar boyunca Buchberger'in çalışmasının önemi tam olarak anlaşılamamış olup 1980'lerde matematik ve bilgisayar bilimlerindeki gelişmeler sayesinde araştırmacılar bu yeni teori hakkında derin bir araştırma başlatmışlardır. İlerleyen zamanda Gröbner taban teorisi, matematiğin ve diğer bilimlerin birçok alanında, çok çeşitli teorik ve hesaplamalı yöntemler sağlayan, cebirin temel bir alanı haline gelmiştir. Bu alanda birçok genelleme ve çok çeşitli uygulamalar geliştirilmiştir (Kreuzer ve Robbiano 2000).

Temel fikirlerinin basitliği; uygulamalarının genişliği ve gücü ile taban tabana zıt olan Gröbner taban teorisinin günümüzde pek çok uygulama alanı bulunmaktadır. Kreuzer ve Robbiano (2000)'ya göre bazı uygulama alanları aşağıda listelenmiştir:

Cebirsel Geometrideki Uygulamaları: Hilbert'in Sıfır Teoremi (Hilbert's Nullstellensatz), afin çeşitlemleri (affine varieties), projektif uzaylar ve Grasmannianlar (Projective spaces and Grassmannians), bir projektif çeşitlemin homojen kaybolan idealinin hesaplanması için doygunluk (saturation for computing the homogeneous vanishing ideal of a projective variety), polinom denklem sistemleri (systems of polynomial equations), çeşitlemlerin indirgenmez bileşenlerinin hesaplanması için ilkel ayrışmalar (primary decompositions for computing irreducible components of varieties), projektif çeşitlemler (projective varieties), projektif kapanışların hesaplanması için homojenleştirme (homogenization for computing projective closures), küme-teoritik tam kesişimler (set-theoretic complete intersections), afin ve projektif çeşitlemlerin boyutları (dimensions of affine and projective varieties), noktaların

idealleri (ideals of points).

Sayı Teorisindeki Uygulamaları: Modüler aritmetik (modular arithmetic) ve sonlu cisimler üzerindeki polinomların çarpanlara ayrılması (factoring polynomials over finite fields), cebirsel sayılar cisminde hesaplamalar (computations in the field of algebraic numbers), sihirli kareler (magic squares).

Homoloji Cebirdeki Uygulamaları: Syzygy modüllerin hesaplanması (computation of syzygy modules), modül homomorfizmlerinin çekirdekleri, görüntüleri ve yükseltmeleri (kernels, images and liftings of module homomorphisms), Hom-modüllerinin hesaplanması (computation of Hom-modules), Ext-modülleri ve bir modülün derinliği (Ext-modules and the depth of a module), dereceli serbest çözücüler (graded free resolutions).

Kombinatorikteki Uygulamaları: Monomial idealler ve modüller (monomial ideals and modules), çizge boyama (graph colourings), torik idealleri (toric ideals).

Diğer Uygulamaları: Şeritler (Splines), Diophantine Sistemleri ve Tamsayı Programlama (Diophantine Systems and Integer Programming), tuhaf polinomlar (strange polynomials), Matematiksel Finans: Modern Portfolyo Teorisi (Mathematical Finance: Modern Portfolio Theory), Fotogrametri (Photogrammetry), Satranç Bulmacaları (Chess Puzzles), İstatistik: Deney Tasarımı (Statistics: Design of Experiments), Otomatik Teorem Kanıtlama (Automatic Theorem Proving).

Gröbner taban teorisinin en çok kullanıldığı alanlardan biri olan cebirsel geometrideki uygulamaları Cox vd. (1992) tarafından incelenmiştir. Polinom denklemleriyle tanımlanan eğriler, yüzeyler ve daha yüksek boyutlu nesneler olan afin çeşitlemelerin geometrisinin incelenmesinde veya çok değişkenli polinomlar halkasındaki ideallerin cebirsel yapısıyla ilgili karşılaşılan problemlerin çözümünde Gröbner taban kavramı önemli rol oynar. Aşağıda verilen problemlerin son ikisi cebirsel geometriyle ilgili olup, tez çalışmasında; cebirsel olan ilk iki problemle ilgileneceğiz.

İdeal Belirleme Problemi (The Ideal Description Problem): $K[x_1, x_2, \dots, x_n]$ 'nin her I ideali bir sonlu üreteç kümesine sahip midir? Diğer bir deyişle; $I = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in K[x_1, x_2, \dots, x_n]$ polinomları nasıl belirlenir?

İdeal Üyelik Problemi (The Ideal Membership Problem): Bir $f \in K[x_1, x_2, \dots, x_n]$ polinomu ve bir $I = \langle f_1, f_2, \dots, f_s \rangle$ ideali verildiğinde $f \in I$ olup olmadığı nasıl belirlenir?

Polinom Denklemlerinin Çözüm Problemi (The Problem of Solving Polynomial Equations): n değişkenli polinomların oluşturduğu bir

$$f_1(x_1, x_2, \dots, x_n) = \dots = f_s(x_1, x_2, \dots, x_n) = 0$$

denklem sisteminin k^n afin uzayında tüm ortak çözümleri nasıl bulunur?

Örtükleştirme Problemi (The Implicitization Problem): g_i 'ler t_j değişkenli polinomlar (ya da rasyonel fonksiyonlar) olmak üzere V , aşağıdaki parametrik denklemle verilen k^n 'in bir altkümesi olsun.

$$\begin{aligned} x_1 &= g_1(t_1, t_2, \dots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, t_2, \dots, t_m). \end{aligned}$$

Bu durumda V bir afin çeşitlemdir ya da onun bir parçasıdır. Bu çeşitlemi belirleyen (x_i değişkenli) bir polinom denklem sistemi nasıl bulunur?

Ayrıca Gröbner taban; tek değişkenli polinomlar halkasında iki polinomun en büyük ortak bölenini bulmak için kullanılan Öklid (Euclidean) Algoritmasını (ve dolayısıyla bölme algoritmasını), lineer denklem sistemlerini çözmek için kullanılan Gauss Eliminasyon Yöntemini ve doğrusal programlama için kullanılan Simplex Algoritmasını genelleştiren bir kavramdır. Buchberger'in bu teoriyi yaratmasının altında yatan temel fikrin, tek değişkenli polinomlar teorisini çok değişkenli polinomlar teorisine

genelleştirmek olduğunu gözönüne alarak, adı geçen genelleştirmelerin sırasıyla nasıl yapıldığını açıklayalım.

Hilbert'in Taban Teoremi (Hilbert's Basis Theorem) gereğince, K bir cisim olmak üzere $K[x]$ polinomlar halkasının herhangi bir I ideali sonlu üretilmiştir, özel olarak bir temel idealdir, öyle ki: $\{f_1, f_2, \dots, f_s\}$ kümesi $K[x]$ 'in bir I ideali için bir üreteç kümesi ise, Öklid algoritması kullanılarak bulunan, üreteçlerin en büyük ortak böleni olan $\text{ebob}(f_1, f_2, \dots, f_s) = d$ polinomu I 'yı üretir. Ayrıca bir $f \in K[x]$ polinomunun I 'da olup olmadığına karar vermek için f 'nin d ile bölümünden kalanın sıfır olup olmadığına bakılır, yani; $f \in I$ olması için gerek ve yeter koşul f 'nin d ile bölümünden kalanın sıfır olmasıdır. Buchberger bu durumu; tek değişkenli polinomlar halkasındaki bölme algoritmasını çok değişkenli polinomlar halkasına taşıyarak, şu şekilde genelleştirmiştir: Gröbner taban; $K[x_1, x_2, \dots, x_n]$ çok değişkenli polinomlar halkasının bir I ideali için bir üreteç kümesidir ve $f \in I$ olması için gerek yeter koşul f 'nin Gröbner tabandaki polinomlar ile bölümünden kalanın sıfır olmasıdır. Böylece Gröbner taban kavramının tanımlanmasıyla hem “İdeal Belirleme” hem de “İdeal Üyelik” problemlerine bir çözüm getirilmiş olur. Burada *bölme* (*division*) kavramının, Gröbner taban teorisinde merkezi bir rol oynadığına dikkat edilmelidir. Bundan başka Hilbert'in Taban Teoremi ve onun daha genel bir versiyonu olan “ R Noether bir halka ise, $R[x]$ Noetherdir” ifadesi çok değişkenli polinomlar halkasında da gerçekleşmiş olur. Yani; $K[x_1, x_2, \dots, x_n]$ 'nin her ideali sonlu bir üreteç kümesine sahiptir ve Noether bir halka üzerine kurulan çok değişkenli polinomlar halkası Noetherdir.

Şimdi, bir lineer denklem sisteminin çözümü için kullanılan, genişletilmiş katsayılar matrisinin satırca basamak (eşelon) matrisine indirgenmesini esas alan, Gauss Eliminasyon Metodundaki düşüncenin, $K[x_1, x_2, \dots, x_n]$ 'nin bir I idealinin cebirsel yapısının anlaşılabilmesini sağlayan “en iyi” üreteç kümesinin bulunmasında kullanılan *indirgeme yöntemi* (*reduction process*) olarak adlandırılan yönteme nasıl genelleştirildiğini bir örnekle açıklayalım: $\mathbb{R}[x, y, z]$ 'de $f_1 = x + y - z$ ve $f_2 = 2x + 3y + 2z$ doğrusal polinomları ve $I = \langle f_1, f_2 \rangle$ ideali verilsin. f_1 ve f_2 'nin oluşturduğu aşağıdaki homo-

jen lineer denklem sistemini gözönüne alalım.

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

Lineer denklem sisteminin çözümü için Gauss yoketme yöntemi kullanılırsa

$$\begin{bmatrix} 1 & 1 & -1 & 0 \\ 2 & 3 & 2 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 4 & 0 \end{bmatrix}$$

satırca eşelon matrisi elde edilir. Böylece yukarıda verilen lineer denklem sistemi ile

$$\begin{cases} x + y - z = 0 \\ y + 4z = 0 \end{cases}$$

lineer denklem sistemi aynı parametrik $y = -4z$ ve $x = 5z$ çözümüne sahiptir. Buradaki satır indirgeme işlemi, aslında I ideali için yeni bir üreteç kümesi bulunmasını sağlar. Yani; satırı indirgemek için yapılan işlemin polinomlara uygulandığı düşünülürse, yeni bir $f_3 = f_2 - 2f_1 = y + 4z \in I = \langle f_1, f_2 \rangle$ polinomu bulunmuş olur. Diğer yandan $f_2 = 2f_1 + f_3$ olduğundan $f_2 \in \langle f_1, f_3 \rangle$ olup I için yeni bir üreteç kümesi, yani; $I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ elde edilir. Burada f_1 kullanılarak f_2 'nin f_3 ile değiştirilmesine f_2 'nin f_1 ile indirgenmesi (*reduction*) denir ve $f_2 \xrightarrow{f_1} f_3$ ile gösterilir. Burada indirgeme işlemi yapılırken, ilk terim olarak x 'in gözönüne alınması ve buna göre sadeleştirme yapılması sonucunda $f_2 \xrightarrow{f_1} f_3 = y + 4z$ bulunduğu dikkat edilir. Eğer yukarıdaki lineer denklem sistemi

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

biçiminde yazılıp ilk terim olarak y gözönüne alınsaydı, farklı bir parametrik çözümle birlikte, f_2 'nin f_1 ile indirgenmesinden farklı bir $f_3 = f_2 - 3f_1 = -x + 5z \in I = \langle f_1, f_2 \rangle$ polinomu var olup $f_2 \xrightarrow{f_1} f_3 = -x + 5z$ ve $I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ bulunurdu. Benzer olarak z değişkenine göre indirgeme yapılsaydı farklı bir kalan polinomu, dolayısıyla I ideali için farklı bir üreteç kümesi bulunmuş olurdu. Her bir durumda değişkenler üzerinde yapılan farklı bir sıralamaya göre elde edilen kalan polinomun değiştiği ve dolayısıyla I için farklı üreteç kümelerinin bulunabildiği açık bir biçimde görülmektedir. Yukarıda üç değişkenli iki tane (lineer) polinom

tarafından üretilen bir ideal için açıkladığımız durum, n değişkenli sonlu sayıda lineer polinom tarafından üretilen bir ideal için de geçerlidir. Buchberger lineer polinomlardaki değişkenlerin sıralamasını, lineer olmayan polinomlarda monomilerin sıralamasına genelleştirerek, lineer polinomlar tarafından üretilen bir ideal için gerçekleşen bu durumu, çok değişkenli polinomlar halkasında sonlu sayıda lineer olmayan polinom tarafından üretilen bir I idealinin üreteçlerinin bulunmasına genelleştirmiştir. $K[x_1, x_2, \dots, x_n]$ 'nin bir I idealinin sonlu bir üreteç kümesi verildiğinde, Buchberger algoritması olarak adlandırılan bir çeşit indirgeme yöntemi kullanılarak, bulunan “en iyi” üreteç kümesi I idealinin bir Gröbner tabanı olarak karşımıza çıkar. Ayrıca yukarıdaki açıklamalar gözönüne alındığında Gröbner taban teorisinin merkezinde rol oynayan diğer önemli bir kavram da *sıralama* (*ordering*) kavramıdır.

Tez çalışmasının ikinci bölümünde, tez çalışmasında kullanılacak temel kavramların yanısıra, tek değişkenli ve çok değişkenli polinomlar halkasının yapısı ve özellikleri verilmiştir. Gröbner taban teorisinin temelini oluşturan bölme algoritması ve sıralama kavramları çeşitli örneklerle detaylı bir biçimde açıklanmıştır.

Üçüncü bölümde Gröbner taban kavramının tanımı ve karakterizasyonları örneklerle açıklanarak sunulmuştur. Gröbner tabanın hesaplanmasında kullanılan Buchberger algoritması ve bu algoritmanın temel araçlarından biri olan S -polinomları örneklerle tanıtılmıştır. Bir idealin üreteç kümesi kullanılarak Buchberger algoritması yardımıyla Gröbner tabanın nasıl elde edildiği ve elde edilen bir Gröbner tabandan daha az elemana sahip fakat tek olmayan minimal Gröbner tabanın nasıl bulunduğu örneklerle açıklanmıştır. Ayrıca minimal Gröbner tabandan elde edilen ve tek türlü tanımlı olan indirgenmiş Gröbner taban kavramı ile bu tabanların birbiriyle ilişkileri incelenmiş olup bölüm sonunda Gröbner tabanın tüm karakterizasyonlarını içeren bir özet yapılmıştır.

Dördüncü bölümde bazı bilgisayar programlarında Gröbner tabanın bulunuşuna dair bilgilere ve bir uygulama alanı olarak çizge boyamaya yer verilmiştir.

2. ÖN BİLGİLER

Bu bölümde tez çalışması için gerekli olan bazı temel kavramlar tanıtılarak kullanılacak olan bazı özellikler ifade edilecektir. Bu bölümde Malik vd. (1997), Hungerford (1974), Dummit ve Foote (2020), Adams ve Loustaunau (1994) kullanılan temel kaynaklardır.

2.1. Temel Kavramlar

Tanım 2.1.1 $\preceq$; boştan farklı bir A kümesi üzerinde bir bağıntı olsun.

- (i) Her $a \in A$ için $a \preceq a$ oluyorsa, $\preceq$ 'e *yansıyan* (*reflexive*),
- (ii) $a \preceq b$ ve $b \preceq a$ iken $a = b$ oluyorsa, $\preceq$ 'e *ters-simetrik* (*anti-symmetric*),
- (ii.) $a \preceq b$ ve $b \preceq c$ iken $a \preceq c$ oluyorsa, $\preceq$ 'e *geçişmeli* (*transitive*)

bağıntı denir. Yansıyan, ters-simetrik ve geçişmeli bir $\preceq$ bağıntısına bir *kısmi sıralama bağıntısı* (*partial order relation*) adı verilir. $(A, \preceq)$ ikilisi de bir *kısmi sıralı küme* (*partial ordered set* ya da *poset*) olarak adlandırılır.

Tanım 2.1.2 $(A, \preceq)$ kısmi sıralı bir küme olsun. Her $a, b \in A$ için $a \preceq b$ veya $b \preceq a$ oluyorsa, $\preceq$ bir *tam sıralı bağıntı* (*totally order relation*), $(A, \preceq)$ ikilisi de bir *tam sıralı küme* (*total ordered set*) ya da bir *zincir* (*chain*) olarak adlandırılır.

Tanım 2.1.3 $(A, \preceq)$ kısmi sıralı bir küme olsun. A 'nın her boştan farklı altkümesinin bir en küçük elemanı varsa $\preceq$ 'e *iyi sıralı bağıntı* (*well order relation*), A 'ya da *iyi sıralı küme* (*well ordered set*) denir.

Tamsayılar kümesi üzerinde aşağıda verilen bölme algoritması, önce tek değişkenli polinomlar halkasına daha sonra da çok değişkenli polinomlar halkasına taşınacak ve tez çalışmasında kullanılan en temel araçlardan biri olacaktır.

Teorem 2.1.4 ($\mathbb{Z}$ 'de Bölme Algoritması) $a, b \in \mathbb{Z}$ ve $b \neq 0$ olsun. Bu durumda $a = qb + r$ ve $0 \leq r < |b|$ olacak şekilde $q, r \in \mathbb{Z}$ tamsayıları vardır. Burada q 'ya *bölüm* (*quotient*) r 'ye *kalan* (*remainder*) denir. Eğer $r = 0$ ise, $a = qb$ olacak şekilde $q \in \mathbb{Z}$ var olup, b ; a 'yı *böler* (*divide*) ya da b 'ye; a 'nın bir *böleni* (*divisor*) denir ve $b|a$ ile gösterilir.

Tanım 2.1.5 Aşağıdaki özellikleri sağlayan sıfırdan farklı bir d tamsayısına a ve b tamsayılarının *en büyük ortak böleni* (*great common divisor*) denir:

- (i) $d|a$ ve $d|b$;
- (ii) $c|a$ ve $c|b$ iken, $c|d$.

Herhangi iki tamsayının en büyük ortak böleni Öklid (Euclidean) algoritması kullanılarak bulunur. Aşağıdaki teoremden sıfırdan farklı iki tamsayının en büyük ortak böleninin, her zaman var olduğu ve bu sayıların bir lineer bileşimi olarak yazıldığı ifade edilmiştir.

Teorem 2.1.6 a ve b sıfırdan farklı tamsayılar olsun. Bu durumda a ve b 'nin bir pozitif d en büyük ortak böleni vardır. Ayrıca, $d = xa + yb$ olacak şekilde $x, y \in \mathbb{Z}$ vardır.

Tanım 2.1.7 Bir *halka* (*ring*); $(R, +)$ bir toplamsal abel grup, $(R, \cdot)$ bir semigrup ve her $a, b, c \in R$ için

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

dağılma özellikleri sağlanacak şekilde bir $(R, +, \cdot)$ sistemidir. Bir R halkasında her $a, b \in R$ için $a \cdot b = b \cdot a$ oluyorsa R 'ye *değişmeli halka* (*commutative ring*) denir. Ayrıca, her $a \in R$ için $a \cdot 1 = 1 \cdot a = a$ olacak şekilde $1 \in R$ varsa R 'ye *birimli halka* (*ring with unity*) adı verilir. Birimli ve değişmeli bir R halkasında sıfırdan farklı her elemanın çarpımsal tersi varsa R bir *cisim* (*field*) olarak adlandırılır.

Tez çalışmasında R birimli bir halka olacaktır.

Tanım 2.1.8 R bir halka ve I , R 'nin boştan farklı bir altkümesi olsun. Her $a, b \in I$ için $a - b \in I$ ve her $r \in R$ için

- $ar \in I$ olursa, I 'ya *sağ ideal* (*right ideal*);
- $ra \in I$ olursa, I 'ya *sol ideal* (*left ideal*);
- hem $ar \in I$ hem de $ra \in I$ olursa, I 'ya *iki-yanlı ideal* (*two-sided ideal*)

adı verilir.

Tanım 2.1.9 R bir halka olmak üzere R 'nin sol (sağ) idealleri üzerinde *artan zincir şartı* (*ascending chain condition*) (kısaca ACC) sağlanırsa, yani; R 'nin sol (sağ) ideallerinin her artan $I_1 \subset I_2 \subset I_3 \subset \dots$ zinciri ve her $i \geq n$ için $I_i = I_n$ oluyorsa, R 'ye *sol (sağ) Noether halka* denir. Hem sol hem de sağ Noether olan bir halka Noether olarak adlandırılır.

Tanım 2.1.10 R bir halka ve S ; R 'nin boştan farklı bir altkümesi olsun. R 'nin S 'yi kapsayan tüm sağ (sol veya iki-yanlı) ideallerinin arakesatine S tarafından üretilen *sağ (sol veya iki-yanlı) ideal* (*right (left or two-sided) ideal generated by S*) denir ve $\langle S \rangle_r$ ($\langle S \rangle_l$ veya $\langle S \rangle$) ile gösterilir. R birimli bir halka ise,

$$\begin{aligned}\langle S \rangle_r &= \left\{ \sum_{i=1}^n s_i r_i \mid r_i \in R, s_i \in S, n \in \mathbb{N} \right\} \\ \langle S \rangle_l &= \left\{ \sum_{i=1}^n r_i s_i \mid r_i \in R, s_i \in S, n \in \mathbb{N} \right\} \\ \langle S \rangle &= \left\{ \sum_{i=1}^n r_i s_i t_i \mid r_i, t_i \in R, s_i \in S, n \in \mathbb{N} \right\}\end{aligned}$$

ile tanımlanır. $S = \{s_1, s_2, \dots, s_n\}$ olması durumunda $\langle S \rangle$ 'ye *sonlu üretilmiş ideal* (*finitely generated ideal*) denir. $S = \{a\}$ olması durumunda $\langle S \rangle$ 'ye *a tarafından üretilen temel ideal* (*principal ideal generated by a*) adı verilir. Her ideali bir tek eleman tarafından üretilen bir tamlık bölgesi (birimli, değişmeli ve sıfır bölensiz bir halka) bir *temel ideal bölgesi* (*principal ideal domain*), kısaca *TİB* (*PID*) olarak adlandırılır. Tanım 2.1.9'a denk olarak, her ideali sonlu üretilmiş olan birimli ve değişmeli bir halka Noether olarak adlandırılır.

2.2. Tek Değişkenli Polinomlar Halkası

Bu bölümde bir R halkası üzerine kurulan tek değişkenli polinomlar halkası ve bazı temel özellikleri tanıtılacaktır.

Tanım 2.2.1 R bir halka olmak üzere sonlu sayıdaki i dışında tüm $a_i = 0$ olacak şekilde R 'nin elemanlarının oluşturduğu tüm $(a_0, a_1, \dots)$ sıralılarının kümesi $R[x]$

olsun. $(a_0, a_1, \dots), (b_0, b_1, \dots) \in R[x]$ olmak üzere

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

ve

$$c_n = \sum_{i=0}^n a_{n-i}b_i = a_nb_0 + a_{n-1}b_1 + \dots + a_1b_{n-1} + a_0b_n = \sum_{k+j=n} a_kb_j \text{ olmak üzere,}$$

$$(a_0, a_1, \dots)(b_0, b_1, \dots) = (c_0, c_1, \dots)$$

ile tanımlanan toplama ve çarpma işlemleriyle birlikte $R[x]$ bir halkadır. Bu halkaya R üzerindeki *polinomlar halkası* (*ring of polynomials*), elemanlarına da *polinom* (*polynomial*) denir.

Uyarı 2.2.2

- (i) Her bir $r \in R$ için $f(r) = (r, 0, \dots)$ ile tanımlı bir $f : R \rightarrow R[x]$ halka monomorfizması vardır. Bundan dolayı R halkası $R[x]$ içine gömülür, yani; R halkasının her bir elemanı $R[x]$ 'de bir polinom olur.
- (ii) R birimli bir halka ise $R[x]$ 'de birimli bir halkadır.
- (iii) R değişmeli bir halka ise, $R[x]$ 'de değişmeli bir halkadır.
- (iv) R bir tamlık bölgesi ise $R[x]$ 'de bir tamlık bölgesidir.

Teorem 2.2.3 $R[x]$ 'de $(0, 1_R, 0, \dots)$ elemanı *değişken* (*indeterminate*) olarak adlandırılıp x ile gösterilsin. Buna göre;

- (i) $1_R, (n+1)$. bileşende olmak üzere $x^n = (0, 0, \dots, 0, 1_R, 0, \dots)$ biçimindedir.
- (ii) $r \in R$ olmak üzere her bir $n \geq 0$ için $r, (n+1)$. bileşende olmak üzere $rx^n = x^n r = (0, 0, \dots, 0, r, 0, \dots)$ biçimindedir.
- (iii) $R[x]$ 'deki sıfırdan farklı her f polinomu $n \in \mathbb{N}$ ve $a_0, a_1, \dots, a_n \in R$ olmak üzere $f = a_0 + a_1x^1 + \dots + a_nx^n$ biçiminde tek türlü yazılır.

Uyarı 2.2.4 Bir R halkası üzerindeki bir f polinomu $f = a_0 + a_1x^1 + \cdots + a_nx^n$ biçiminde gösterilir. Bu durumda $R[x]$ 'deki toplama ve çarpma işlemleri:

$$f + g = \left(\sum_{i=0}^n a_i x^i \right) + \left(\sum_{j=0}^m b_j x^j \right) = \sum_{i=0}^n (a_i + b_i) x^i, \quad (n > m \text{ iken})$$

ve $c_k = \sum_{i+j=k} a_i b_j$ olmak üzere

$$fg = \left(\sum_{i=0}^n a_i x^i \right) \left(\sum_{j=0}^m b_j x^j \right) = \sum_{k=0}^{m+n} c_k x^k$$

ile tanımlanır.

Tanım 2.2.5 $R[x]$ 'deki bir $f = \sum_{i=0}^n a_i x^i$ polinomu için,

- $a_i \in R$ 'lere f 'nin *katsayıları* (*coefficients*) denir.
- $a_0 \in R$ 'a f 'nin *sabit terimi* (*constant term*) adı verilir.
- $a_n \neq 0$ ise, a_n 'e f 'nin *baş katsayısı* (*leading coefficient*) denir ve $\text{lc}(f)$ ile gösterilir.
- $a_n \neq 0$ ise, $a_n x^n$ 'e f 'nin *baş terimi* (*leading term*) denir ve $\text{lt}(f)$ ile gösterilir.
- $a_n \neq 0$ ise, n 'ye f 'nin *derecesi* (*degree*) denir ve $\text{deg}(f)$ ile gösterilir. 0 polinomunun derecesi $-\infty$ olarak alınır.
- f 'nin başkatsayısı 1 ise, f 'ye *monik* (*monic*) polinom denir.

Teorem 2.1.4'de tamsayılar kümesi üzerinde ifade edilen bölme algoritması tek değişkenli polinomlar halkası üzerinde aşağıdaki biçimde ifade edilir.

Teorem 2.2.6 ($R[x]$ 'de Bölme Algoritması) R bir halka olsun. g 'nin başkatsayısı R 'de tersinir olacak şekilde sıfırdan farklı $f, g \in R[x]$ polinomları için

$$f = qg + r \quad \text{ve} \quad \text{deg}(r) < \text{deg}(g)$$

olacak şekilde bir tek $q, r \in R[x]$ polinomları vardır. Burada r 'ye f 'nin g ile bölümünden *kalan* (*remainder*), q 'ya da *bölüm* (*quotient*) denir. $r = 0$ olması durumunda g , f 'yi *böler* (*divide*) denir ve $g|f$ ile gösterilir.

Örnek 2.2.7 $\mathbb{Q}[x]$ 'de verilen $f = x^3 - 2x^2 + 2x + 8$ ve $g = 2x^2 + 3x + 1$ polinomlarına bölme algoritmasını uygulayalım.

$$\begin{array}{r|l}
 x^3 - 2x^2 + 2x + 8 & 2x^2 + 3x + 1 \\
 -x^3 - \frac{3}{2}x^2 - \frac{1}{2}x & \frac{1}{2}x - \frac{7}{4} \\
 \hline
 -\frac{7}{2}x^2 + \frac{3}{2}x + 8 & \\
 \frac{7}{2}x^2 + \frac{21}{4}x + \frac{7}{4} & \\
 \hline
 \frac{27}{4}x + \frac{39}{4} &
 \end{array}$$

Böylece $f = \left(\frac{1}{2}x - \frac{7}{4}\right)g + \left(\frac{27}{4}x + \frac{39}{4}\right)$ biçiminde yazılır.

Uyarı 2.2.8 Tek değişkenli polinom halkasında, bir f polinomu ile derecesi f 'nin derecesinden küçük veya eşit olan bir g polinomuna bölme algoritması uygulandığında, r 'nin derecesi g 'nin derecesinden küçük oluncaya kadar ya da $r = 0$ oluncaya kadar süreç tekrarlanır. Bu durum, sembolik olarak

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

ile ifade edilir ve f polinomu g 'ye göre r 'ye indirgenir denir.

Örnek 2.2.9 Yukarıdaki örnekte

$$\begin{aligned}
 h &= f - \frac{lt(f)}{lt(g)}g = -\frac{7}{2}x^2 + \frac{3}{2}x + 8 \\
 r &= h - \frac{lt(h)}{lt(g)}g = \frac{27}{4}x + \frac{39}{4}
 \end{aligned}$$

olmak üzere

$$f \xrightarrow{g} h \xrightarrow{g} r$$

biçiminde ifade edilir.

Uyarı 2.2.10 Tek değişkenli polinom halkasında bölme algoritmasının bilgisayardaki akış şeması Şekil 2.1'deki gibi ifade edilir.

GİRİDİ (INPUT)	: $f, g \in K[x], g \neq 0$
ÇIKTI (OUTPUT)	: $r = 0$ ya da $\deg(r) < \deg(g)$ ve $f = qg + r$ olacak şekilde q, r vardır.
BAŞLANGIÇ (INITIALIZATION)	: $q := 0; r := f$
DÖNGÜ (WHILE)	$r \neq 0$ VE (AND) $\deg(g) \leq \deg(r)$ YAP (DO) $q := q + \frac{\text{lt}(r)}{\text{lt}(g)}$ $r := r - \frac{\text{lt}(r)}{\text{lt}(g)}g$

Şekil 2.1 Tek Değişkenli Polinomlar Halkasında Bölme Algoritması

Teorem 2.2.11 $R[x]$ 'in sıfırdan farklı her ideali bir temel idealdir.

İspat $I, R[x]$ 'in sıfırdan farklı bir ideali olsun. $\deg(g) = n$ en küçük olacak şekilde sıfırdan farklı bir $g \in I$ alalım. Herhangi $f \in I$ polinomu ile g 'ye bölme algoritması uygulanırsa $f = qg + r$ ve $r = 0$ veya $\deg(r) < \deg(g)$ olacak şekilde $q, r \in R[x]$ polinomları vardır. $r \neq 0$ olması durumunda $r = f - qg \in I$ olması g 'nin seçimi ile çelişir. Böylece $r = 0$ olmalıdır. Bu durumda $f = qg$ olup $f \in \langle g \rangle$ ve buradan $I \subseteq \langle g \rangle$ bulunur. Diğer yandan $g \in I$ olduğundan $\langle g \rangle \subseteq I$ olduğu açıktır. Sonuç olarak $I = \langle g \rangle$ olup I bir temel idealdir.

Tanım 2.1.10 ve Teorem 2.2.11 gereğince, n değişkenli polinomlar halkasında da geçerli olan, Hilbert'in Taban Teoreminin daha genel bir ifadesi aşağıda verilmiştir.

Teorem 2.2.12 R bir Noetherian halka ise, $R[x]$ Noetheriandır.

Uyarı 2.2.13 Teorem 2.2.11 gereğince $R[x]$ bir TİB olur. $R[x]$ 'deki bir ideali üreten polinom bir sabitle çarpım bakımından tek türlü belirlidir. Yani; $I = \langle g_1 \rangle = \langle g_2 \rangle$ biçiminde ise, $g_1|g_2$ veya $g_2|g_1$ dir. O halde tek değişkenli polinom halkasında sıfırdan farklı bir ideali üreten tek elemanı bulma problemi doğal olarak ortaya çıkar. Bunun için gerekli olan polinomlarda en büyük ortak bölen kavramı aşağıda verilmiştir.

Tanım 2.2.14 $f_1, f_2 \in R[x]$ olsun. Aşağıdaki özellikleri sağlayan bir $g \in R[x]$ polinomuna f_1 ve f_2 polinomlarının *en büyük ortak böleni* (*great common divisor*) denir ve $\text{ebob}(f_1, f_2) = g$ ile gösterilir:

- (i) g ; f_1 ve f_2 'yi böler,
- (ii) h ; f_1 ve f_2 'yi bölen başka bir polinom ise, bu durumda h , g 'yi böler,
- (iii) g monik polinomdur.

Lemma 2.2.15 f_1 ve f_2 en az biri sıfırdan farklı polinomlar olsun. Bu durumda her $q \in R[x]$ için $\text{ebob}(f_1, f_2) = \text{ebob}(f_1 - qf_2, f_2)$ dir.

Uyarı 2.2.16 Verilen f_1 ve f_2 polinomlarının en büyük ortak böleni ve böylece Uyarı 2.2.13 gereğince $\langle f_1, f_2 \rangle$ idealinin tek üretici bulunurken, Lemma 2.2.15'i ve bölme algoritmasını temel alan, Şekil 2.2'deki Öklid (Euclidean) algoritması kullanılır.

GİRDİ (INPUT)	$: f_1, f_2$ 'den biri sıfırdan farklı; $f_1, f_2 \in K[x]$
ÇIKTI (OUTPUT)	$: f = \text{ebob}(f_1, f_2)$
BAŞLANGIÇ (INITIALIZATION)	$: f := f_1, g := f_2$
DÖNGÜ (WHILE)	YAP (DO)
	$g \neq 0$
	$f \xrightarrow{g} r$; burada r , f 'nin g 'ye bölümünden kalandır
	$f := g$
	$g := r$
	$f := \frac{1}{\text{lc}(f)}f$

Şekil 2.2 Tek Değişkenli Polinomlar Halkasında Öklid Algoritması

Bilgisayardaki akış şeması yukarıdaki biçimde olan Öklid algoritması şu şekilde uygulanır: ilk adımda verilen polinomlardan biri, daha küçük dereceli olan diğer polinoma bölünür. İkinci adımda; ilk adımdaki bölen rolündeki polinom birinci adımda elde edilen kalana bölünür. Her bir adımda, bir önceki adımın böleni elde edilen kalana bölünür ve bu süreç 0 kalanı bulununcaya kadar tekrarlanır. Sıfır kalanı bulunmadan önceki son kalan monik polinom verilen polinomların en büyük ortak böleni olur. Şimdi bunu bir örnekle açıklayalım:

Örnek 2.2.17 $\mathbb{Q}[x]$ 'de verilen $f_1 = x^3 - 3x + 2$ ve $f_2 = x^2 - 1$ polinomlarının en büyük ortak bölenini bulalım. $f := x^3 - 3x + 2$ ve $g := x^2 - 1$ polinomlarına bölme

algoritması uygulanırsa

$$\begin{array}{r|l} x^3 - 3x + 2 & x^2 - 1 \\ -x^3 & +x \\ \hline & -2x + 2 \end{array}$$

olup $x^3 - 3x + 2 \xrightarrow{x^2-1} -2x + 2$ bulunur. $f := x^2 - 1$ ve $g := -2x + 2$ olmak üzere tekrar bölme algoritması uygulanırsa

$$\begin{array}{r|l} x^2 & -1 \\ -x^2 & +x \\ \hline & x - 1 \\ & -x + 1 \\ \hline & 0 \end{array}$$

olup $x^2 - 1 \xrightarrow{-2x+2} 0$ ve buradan $\text{ebob}(f_1, f_2) = -\frac{1}{2}(-2x + 2) = x - 1$ olarak bulunur.

Uyarı 2.2.13'te ifade edildiği gibi, ikiden daha fazla polinom tarafından üretilen bir idealin, bu polinomların en büyük ortak böleni olan bir tek polinom tarafından üretildiği aşağıdaki önermede gösterilmiştir.

Önerme 2.2.18 $R[x]$ 'de $I = \langle f_1, f_2, \dots, f_n \rangle$ ideali verilsin. Bu durumda,

- (i) $I = \langle \text{ebob}(f_1, f_2, \dots, f_n) \rangle$.
- (ii) $n \geq 3$ ise, $\text{ebob}(f_1, f_2, \dots, f_n) = \text{ebob}(f_1, \text{ebob}(f_2, \dots, f_n))$.

Uyarı 2.2.19 Adına *ideal üyelik problemi* (*ideal membership problem*) denilen “bir f polinomunun bir $I = \langle f_1, f_2, \dots, f_n \rangle$ idealinde olup olmadığının belirlenmesi” probleminin çözümü için öncelikle $g = \text{ebob}(f_1, f_2, \dots, f_n)$ bulunur. Daha sonra f ile g polinomlarına bölme algoritması uygulanır. Bölme işleminde kalanın sıfır olması için gerek ve yeter koşul $f \in I = \langle f_1, f_2, \dots, f_n \rangle = \langle g \rangle$ olmasıdır. Bu durum aşağıdaki biçimde de ifade edilebilir:

$$f \in I = \langle g \rangle \text{ olması için gerek ve yeter koşul } f \xrightarrow{+g} 0 .$$

Bu bölümde verilen bilgiler özetlenecek olursa, tek değişkenli polinomlar halkasında şu iki probleme vurgu yapılmıştır:

- Sıfırdan farklı bir I idealini üreten tek polinomun bulunması,
- Bir polinomun bir ideale ait olup olmadığına karar verilmesi.

Bu sorulara bölme algoritması kullanılarak cevap verilmiştir. Ancak bölme algoritması yapılırken derecesi büyük olan polinom derecesi küçük veya eşit olan bir polinoma bölünerek, yani $n \geq m$ özelliğine sahip doğal sayılar için $x^n \succeq x^m$ biçiminde bir tür sıralama kullanılmıştır. Bu iki kavram (bölme algoritması ve sıralama) çok değişkenli polinomların halkasında da önemli rol oynamaktadır.

2.3. Çok Değişkenli Polinomlar Halkası

Birimli bir R halkası üzerine kurulan $R[x]$ tek değişkenli polinomlar halkasının inşası Tanım 2.2.1’de verilmiştir. Bu tanımda $R[x]$ ’in elemanları öncelikle bir $\mathbb{N} \rightarrow R$ fonksiyonu altında oluşan görüntülerin sıralısı olarak alınmış daha sonra bu küme üzerinde tanımlanan ikili işlemlerle bir halka yapısı oluşturularak tek değişkenli polinomlar halkası inşa edilmiştir. Bu yaklaşıma benzer biçimde, bu bölümde n değişkenli polinomlar halkası tanımlanacaktır. Bunun için, bileşensel toplama işlemine göre bir toplamsal değişmeli monoid olan ve elemanları doğal sayıların oluşturduğu n -liler olan $\mathbb{N}^n = \mathbb{N} \times \dots \times \mathbb{N}$ kümesi ve $\mathbb{N}^n \rightarrow R$ fonksiyonları kullanılacaktır.

Tanım 2.3.1 R birimli bir halka olmak üzere $u \in \mathbb{N}^n$ için en fazla sonlu sayıda $f(u) \neq 0$ olacak şekildeki tüm $f : \mathbb{N}^n \rightarrow R$ fonksiyonlarının kümesi $R[x_1, x_2, \dots, x_n]$ olsun. $u \in \mathbb{N}^n$ ve $f, g \in R[x_1, x_2, \dots, x_n]$ olmak üzere

$$(f + g)(u) = f(u) + g(u) \quad \text{ve} \quad (fg)(u) = \sum_{\substack{v + w = u \\ v, w \in \mathbb{N}^n}} f(v)g(w)$$

ile tanımlanan toplama ve çarpma işlemleriyle birlikte $R[x_1, x_2, \dots, x_n]$ bir halkadır. Bu halkaya R üzerindeki n *değişkenli polinomlar halkası* (*ring of polynomials in n indeterminates*) denir. Bu tanımda $n = 1$ için $R[x]$ tek değişkenli polinomlar halkası elde edilir.

Uyarı 2.3.2

- (i) Her bir $r \in R$ için $f_r(0, 0, \dots, 0) = r$ ve diğer tüm $u \in \mathbb{N}^n$ için $f(u) = 0$ olmak üzere, $\varphi(r) = f_r$ ile tanımlanan bir $\varphi : R \rightarrow R[x_1, x_2, \dots, x_n]$ halka monomorfizması vardır. Böylece R halkasının her bir elemanı n değişkenli polinomlar halkasında bir sabit polinom olarak düşünülebilir.
- (ii) R birimli bir halka ise $R[x_1, x_2, \dots, x_n]$ de birimli bir halkadır.
- (iii) R değişmeli bir halka ise, $R[x_1, x_2, \dots, x_n]$ de değişmeli bir halkadır.
- (iv) R bir tamlık bölgesi ise $R[x_1, x_2, \dots, x_n]$ de bir tamlık bölgesidir.

Uyarı 2.3.3 n pozitif bir tamsayı olmak üzere her bir $i = 1, 2, \dots, n$ için, $\mathbb{N}^n$ 'nin i . bileşeni 1 olan elemanı

$$\varepsilon_i = (0, \dots, 0, 1, 0, \dots, 0)$$

olsun. Bu durumda her $k = (k_1, k_2, \dots, k_n) \in \mathbb{N}^n$ elemanı

$$k = (k_1, k_2, \dots, k_n) = k_1\varepsilon_1 + k_2\varepsilon_2 + \dots + k_n\varepsilon_n$$

biçiminde yazılır.

Teorem 2.3.4 R birimli bir halka ve n bir pozitif tamsayı olmak üzere her bir $i = 1, 2, \dots, n$ için $x_i \in R[x_1, x_2, \dots, x_n]$ elemanı

$$x_i(u) = \begin{cases} 1_R, & u = \varepsilon_i; \\ 0_R, & u \neq \varepsilon_i. \end{cases}$$

ile tanımlansın. Bu durumda

- (i) Her bir k pozitif tamsayısı sayısı için $x_i^k(k\varepsilon_i) = 1_R$ ve $u \neq k\varepsilon_i$ için $x_i^k(u) = 0$ olur.
- (ii) Her bir $(k_1, k_2, \dots, k_n) \in \mathbb{N}^n$ için $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}(k_1\varepsilon_1 + k_2\varepsilon_2 + \dots + k_n\varepsilon_n) = 1_R$ ve $u \neq k_1\varepsilon_1 + k_2\varepsilon_2 + \dots + k_n\varepsilon_n$ iken $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}(u) = 0$ olur.
- (iii) Her $s, t \in \mathbb{N}$ ve her $i, j = 1, 2, \dots, n$ için $x_i^s x_j^t = x_j^t x_i^s$ olur.

(iv) Her $r \in R$ ve her $t \in \mathbb{N}$ için $x_i^t r = r x_i^t$ dir.

(v) $R[x_1, x_2, \dots, x_n]$ 'deki her f polinomu, en fazla sonlu sayıda sıfırdan farklı $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ fonksiyonlarının lineer bileşimi olarak yazılır. Yani,

$$f = \sum_{(k_1, k_2, \dots, k_n) \in \mathbb{N}^n} a_{k_1, k_2, \dots, k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$$

olacak şekilde $(k_1, k_2, \dots, k_n) \in \mathbb{N}^n$ ile indislenen tek türlü belirli $a_{k_1, k_2, \dots, k_n} \in R$ elemanları vardır.

Tanım 2.3.5 n değişkenli polinomların $R[x_1, x_2, \dots, x_n]$ halkasında $x_1, x_2, \dots, x_n$ elemanlarına *değişkenler* (*indeterminates*), $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ elemanına *tekterimli* (*monomial*) ya da *kuvvet çarpımı* (*power product*), herhangi $c \in R$ için $c x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ elemanına bir *terim* (*term*) adı verilir. Teorem 2.3.4(v)'den n değişkenli polinomlar halkasındaki her polinom tekterimlilerin bir lineer bileşimi olarak ifade edilir.

Uyarı 2.3.6 R herhangi bir halka olmak üzere $\sum_{i=0}^m a_i x_1^i \mapsto \sum_{i=0}^m a_i x_1^i x_2^0 \dots x_n^0$ ile tanımlı bir $R[x_1] \rightarrow R[x_1, x_2, \dots, x_n]$ monomorfizması var olduğundan tek değişkenli polinomlar halkası, n değişkenli polinomlar halkasının bir althalkası olarak düşünülebilir.

Uyarı 2.3.7 Tez çalışması boyunca K bir cisim olmak üzere K üzerine kurulan n değişkenli polinomlar halkası $K[x_1, x_2, \dots, x_n] = S$ ile, S 'deki tüm tekterimlilerin kümesi ise

$$\text{Mon}(S) = \{x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \mid a_i \in \mathbb{N}, i = 1, 2, \dots, n\}$$

ile gösterilecektir. $\text{Mon}(S)$ 'de bir $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ elemanı $a = (a_1, a_2, \dots, a_n) \in \mathbb{N}^n$ olmak üzere x^a ile gösterilecektir.

Tanım 2.3.8 $\text{Mon}(S)$ 'de sıfırdan farklı bir $x^a = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ tekterimlinin *derecesi* (*degree*);

$$\deg(x^a) = \sum_{i=1}^n a_i = a_1 + a_2 + \dots + a_n$$

ile tanımlanır. S 'de bir f polinomunun *bütünsel* ya da *çoklu derecesi* (*total* ya da *multi degree*); katsayısı sıfırdan farklı olan f 'yi oluşturan tekterimlilerin derecelerinin

maksimumu olarak tanımlanır. Sıfırdan farklı bir f polinomunun derecesinin 0 olması için gerek ve yeter koşul $f = c = cx_1^0x_2^0 \dots x_n^0$ biçiminde bir sabit polinom olmasıdır. Böylece 0 sabit polinomunun derecesinin 0 olduğu açıktır. Her biri i . dereceden olan tekterimlilerin toplamı olan bir polinoma *i. dereceden homojen (homogeneous of degree i)* polinom denir.

Örnek 2.3.9 $f = 2x_1x_3 + 3x_1x_2^2x_3 - x_1^4x_2^2 \in K[x_1, x_2, x_3]$ polinomu verilsin.

- f polinomunun x_1x_3 tekterimlinin derecesi 2'dir.
- f polinomunun $x_1x_2^2x_3$ tekterimlinin derecesi 4'dür.
- f polinomunun $x_1^4x_2^2$ tekterimlinin derecesi 6'dır.
- f polinomunun çoklu derecesi 6'dır.

f polinomunu oluşturan tekterimlilerin dereceleri farklı olduğundan f bir homojen polinom değildir. Fakat $g = x_1x_3 - x_2x_3 + 2x_1x_2$ polinomu her biri 2. dereceden tekterimlilerin toplamı olduğundan 2. dereceden homojen bir polinomdur.

Tanım 2.3.10 Mon S 'de $x^a = x_1^{a_1}x_2^{a_2} \dots x_n^{a_n}$ ve $x^b = x_1^{b_1}x_2^{b_2} \dots x_n^{b_n}$ tekterimleri verilsin. Her $i = 1, 2, \dots, n$ için $a_i \leq b_i$ ise, $x^a; x^b$ 'yi *böler* denir ve $x^a|x^b$ ile gösterilir. x^a ve x^b tekterimlerinin sırasıyla *en büyük ortak böleni (greatest common divisor)* ve *en küçük ortak katı (least common multiple)*

$$ebob(x^a, x^b) = x_1^{\min\{a_1, b_1\}} x_2^{\min\{a_2, b_2\}} \dots x_n^{\min\{a_n, b_n\}}$$

$$ekok(x^a, x^b) = x_1^{\max\{a_1, b_1\}} x_2^{\max\{a_2, b_2\}} \dots x_n^{\max\{a_n, b_n\}}$$

ile tanımlıdır.

Tez çalışmasının en önemli iki kavramı: bölme algoritması ve terim sıralamasıdır. Teorem 2.2.6'da verilen bölme algoritması bir tekterim sıralaması olan derecelerin küçük/büyük olması esas alınarak yapılmıştır. S 'de bölme algoritması uygulayabilmek için bir sıralama kavramına ihtiyaç duyulur. Tekterim sıralaması kavramının tanımı ve bazı örnekleri aşağıda verilmiştir.

Tanım 2.3.11 $\text{Mon}(S)$ üzerinde bir *tekterim sıralaması* (*monomial order*) aşağıdaki şartları sağlayan bir “ $\prec$ ” tam sıralama bağıntısıdır öyle ki:

- (i) $1 \neq x^a$ olacak şekilde her $x^a \in \text{Mon}(S)$ için $1 \prec x^a$,
- (ii) $x^a \prec x^b$ iken her $x^c \in \text{Mon}(S)$ için $x^a x^c \prec x^b x^c$ dir.

Uyarı 2.3.12 Bölme algoritması uygulanırken polinomların terimleri artan/azalan sırada düzenlenmelidir. Bundan dolayı herhangi iki tekterim karşılaştırılabilir. Böylece tekterim sıralaması bir tam sıralı bağıntı olmak zorundadır. Yani; verilen herhangi $x^a, x^b \in \text{Mon}(S)$ monomialleri için

$$x^a \prec x^b, \quad x^a = x^b, \quad x^b \prec x^a$$

durumlarından biri sağlanmalıdır.

Uyarı 2.3.13 Bölme algoritması uygulanırken indirgeme işlemi sonlu adımda durmak zorundadır. Bundan dolayı $\text{Mon}(S)$ ’de tanımlanan her tekterim sıralaması iyi sıralı olmalıdır. Yani; $\text{Mon}(S)$ ’nin her A altkümesi ve her $x^b \in A$ için $x^a \prec x^b$ olacak şekilde bir $x^a \in A$ var olmalıdır.

$\text{Mon}(S)$ ’de farklı tekterim sıralamaları tanımlanabilir. Tanım 2.3.10’da

$$x^a \prec x^b \Leftrightarrow x^a | x^b$$

ile tanımlanan bölünebilme bağıntısı, tek değişkenli polinomlar halkasında bölme algoritması uygulanırken kullanılan sıralama olup, n değişkenli polinomlar halkasında bir tekterim sıralamasıdır. Farklı şekillerde tanımlanan çok sayıda tekterim sıralaması olmasına rağmen, tez çalışmasında kullanılacak olan tekterim sıralamalarının tanımları ve her birinin örneği aşağıda verilmiştir.

Uyarı 2.3.14 Aşağıda verilen sıralama örneklerinde aksi belirtilmedikçe

$$x_n \prec \dots \prec x_2 \prec x_1$$

sıralaması geçerli olacaktır.

Tanım 2.3.15 $x^a, x^b \in \text{Mon}(S)$ tekterimlileri için,

$$x^a \prec_l x^b \Leftrightarrow a \text{ ve } b \text{ 'nin soldan farklı ilk } a_i \text{ ve } b_i \text{ koordinatları için } a_i < b_i \text{ dir}$$

ile tanımlanan bağıntıya *sözcüksel sıralama* (*lexicographic order*) adı verilir ve kısaca l harfi ile gösterilir. Diğer bir deyişle;

$$x^a \prec_l x^b \Leftrightarrow a - b \text{ nin sıfırdan farklı soldaki ilk bileşeninin negatif olmasıdır.}$$

Örnek: Uyarı 2.3.14 gözönüne alındığında, değişkenleri x_1, x_2 olan iki değişkenli polinomlar halkasında sözlüksel sıralama:

$$1 \prec_l x_2 \prec_l x_2^2 \prec_l x_2^3 \prec_l \dots \prec_l x_1 \prec_l x_2 x_1 \prec_l x_2^2 x_1 \prec_l \dots \prec_l x_1^2 \prec_l \dots ,$$

biçimindedir.

Tanım 2.3.16 $x^a, x^b \in \text{Mon}(S)$ tekterimlileri için,

$$x^a \prec_{dl} x^b \Leftrightarrow \begin{cases} \deg(x^a) < \deg(x^b) \text{ ise, aksi takdirde} \\ \deg(x^a) = \deg(x^b) \text{ ise, } \prec_l \text{'e göre sıralama yapılır.} \end{cases}$$

ile tanımlanan bağıntı *derece sözcüksel sıralama* (*degree lexicographic order*) olarak adlandırılır ve kısaca dl ile gösterilir. Bu sıralama, aynı zamanda *derecelendirilmiş sözlüksel sıralama* (*graded lexicographic order*) olarak ta adlandırılır ve kısaca gl ile gösterilir. Tez çalışmasında ilk gösterim kullanılacaktır.

Örnek: Uyarı 2.3.14 gözönüne alındığında, değişkenleri x_1, x_2 olan iki değişkenli polinomlar halkasında derece sözlüksel sıralama:

$$1 \prec_{dl} x_2 \prec_{dl} x_1 \prec_{dl} x_2^2 \prec_{dl} x_1 x_2 \prec_{dl} x_1^2 \prec_{dl} x_2^3 \prec_{dl} x_1 x_2^2 \prec_{dl} x_1^2 x_2 \prec_{dl} x_1^3 \dots ,$$

biçimindedir.

Tanım 2.3.17 $x^a, x^b \in \text{Mon}(S)$ tekterimlileri için,

$$x^a \prec_{rl} x^b \Leftrightarrow a \text{ ve } b \text{ 'nin sağdan farklı ilk } a_i \text{ ve } b_i \text{ koordinatları için } b_i < a_i \text{ dir}$$

ile tanımlanan bağıntıya *ters sözcüksel sıralama* (*reverse lexicographic order*) adı verilir ve kısaca rl ile gösterilir. Diğer bir deyişle;

$$x^a \prec_{rl} x^b \Leftrightarrow a - b \text{ nin sıfırdan farklı sağdaki ilk bileşeninin pozitif olmasıdır.}$$

Örnek: Uyarı 2.3.14 gözönüne alındığında, değişkenleri x_1, x_2 olan iki değişkenli polinom halkasında ters sözlüksel sıralama:

$$\cdots \prec_{rl} x_1^2 \prec_{rl} \cdots \prec_{rl} x_2^2 x_1 \prec_{rl} x_2 x_1 \prec_{rl} x_1 \prec_{rl} \cdots \prec_{rl} x_2^3 \prec_{rl} x_2^2 \prec_{rl} x_2 \prec_{rl} 1$$

biçimindedir.

Tanım 2.3.18 $x^a, x^b \in \text{Mon}(S)$ tekterimlileri için,

$$x^a \prec_{drl} x^b \Leftrightarrow \begin{cases} \deg(x^a) < \deg(x^b) \text{ ise, aksi takdirde} \\ \deg(x^a) = \deg(x^b) \text{ ise, } \prec_{rl} \text{'e göre sıralama yapılır.} \end{cases}$$

ile tanımlanan bağıntı *derece ters sözcüksel sıralama* (*degree reverse lexicographic order*) olarak adlandırılır ve kısaca *drl* ile gösterilir. Bu bağıntıya, aynı zamanda *derecelendirilmiş ters sözlüksel sıralama* (*graded reverse lexicographic order*) denir ve kısaca *grl* ile gösterilir. Tez çalışmasında ilk gösterim kullanılacaktır.

Uyarı 2.3.19 İki değişkenli polinom halkasında derece sözlüksel sıralama ile derece ters sözlüksel sıralama aynı olur. Fakat en az üç değişkenli polinomlar halkasında bu sıralamaların birbirinden farklı olduğu aşağıdaki örnekte görülebilir.

$$x_1 x_2^3 \prec_{dl} x_1^2 x_2 x_3 \text{ iken } x_1^2 x_2 x_3 \prec_{drl} x_1 x_2^3$$

Ayrıca, yukarıda verilen sıralama örneklerinin her birinin tekterim sıralaması aksiyomlarını sağladığı açıktır.

Tek değişkenli polinomlar halkasındaki bir f polinomu için Tanım 2.2.5'te verilen gösterimler, n değişkenli polinomlar halkasında seçilen bir tekterim sıralamasına göre, sıfırdan farklı bir f polinomu için aşağıdaki biçimde tanımlanır.

Tanım 2.3.20 $\prec; \text{Mon}(S)$ 'de bir tekterim sıralaması, $a_i \in K$, $x^\alpha \in \text{Mon}(S)$ ve $x^{\alpha_r} \prec \cdots \prec x^{\alpha_2} \prec x^{\alpha_1}$ olmak üzere her sıfırdan farklı $f \in S$ polinomu

$$f = c_1 x^{\alpha_1} + c_2 x^{\alpha_2} + \cdots + c_r x^{\alpha_r}$$

biçiminde yazılır. Burada

- $lm(f) = x^{\alpha_1}$; f 'nin baş tekterimi (*leading monomial*),

- $lc(f) = c_1$; f 'nin baş katsayısı (leading coefficient),
- $lt(f) = c_1 x^{\alpha_1}$; f 'nin baş terimi (leading term)

olarak adlandırılır. Özel olarak sıfır polinomu için $lm(0) = lc(0) = lt(0) = 0$ olarak tanımlıdır. Ayrıca $f, g \in S$ polinomları için

$$lm(fg) = lm(f)lm(g)$$

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

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

özellikleri sağlanır.

S 'de sıralama değiştirildiğinde, yukarıdaki tanımda verilen notasyonların değişebileceği aşağıdaki örnekte gösterilmiştir.

Örnek 2.3.21 $f = 3x^4z - 2x^3y^4 + 7x^2y^2z^3 - 8xy^3z^3 \in \mathbb{Q}[x, y, z]$ polinomu için, $z \prec y \prec x$ olmak üzere

- Sözlüksel sıralamaya göre: $lm(f) = x^4z, lc(f) = 3, lt(f) = 3x^4z$,
- Ters sözlüksel sıralamaya göre: $lm(f) = xy^3z^3, lc(f) = -8, lt(f) = -8xy^3z^3$,
- Derece sözlüksel sıralamaya göre: $lm(f) = x^3y^4, lc(f) = -2, lt(f) = -2x^3y^4$,
- Derece ters sözlüksel sıralamaya göre: $lm(f) = xy^3z^3, lc(f) = -8, lt(f) = -8xy^3z^3$ ve $-8xy^3z^3$ ve

$x \prec y \prec z$ olmak üzere

- Sözlüksel sıralamaya göre: $lm(f) = xy^3z^3, lc(f) = -8, lt(f) = -8xy^3z^3$,
- Ters sözlüksel sıralamaya göre: $lm(f) = x^4z, lc(f) = 3, lt(f) = 3x^4z$,
- Derece sözlüksel sıralamaya göre: $lm(f) = xy^3z^3, lc(f) = -8, lt(f) = -8xy^3z^3$,
- Derece ters sözlüksel sıralamaya göre: $lm(f) = x^3y^4, lc(f) = -2, lt(f) = -2x^3y^4$

biçimindedir.

Teorem 2.2.12'de tek değişkenli polinomlar halkası için ifade edilen Hilbert'in Taban Teoreminin n değişkenli polinomlar halkalarındaki ifadesi aşağıda verilmiştir.

Teorem 2.3.22 (Hilbert'in Taban Teoremi)

- (i) S 'nin herhangi bir I ideali için $I = \langle f_1, f_2, \dots, f_n \rangle$ olacak şekilde $f_1, f_2, \dots, f_n \in I$ polinomları vardır.
- (ii) $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$; S 'de ideallerin artan bir dizisi ise, $I_N = I_{N+1} = I_{N+2} = \dots$ olacak şekilde bir N doğal sayısı vardır.

Teorem 2.3.22'nin (i) şıkkı, S 'deki her I idealinin sonlu üretilmiş olması olarak ifade edilir. Buna denk olarak I 'yı üreten sonlu bir üreteç kümesinin bulunması problemi doğal olarak ortaya çıkar. Gröbner taban kavramı bu idealin cebirsel yapısının anlaşılabilmesi için "en iyi" üreteç kümesi olarak tanımlanacaktır. Teorem 2.3.22'nin (ii) şıkkı, S 'de artan zincir şartının sağlandığını, yani S 'nin Noether bir halka olduğunu ifade eder.

Şimdi S 'de, önceki bölümlerde bir indirgeme yöntemi olarak ifade edilen, bölme algoritması tanımlanacaktır. Tek değişkenli polinomlar halkasında bölme algoritması uygulanmasındaki temel fikir; f polinomunu $f_1, f_2, \dots, f_n$ polinomlarına bölerken f_i polinomlarının baş terimlerini kullanarak, sadeleşen terimlerden daha küçük olan yeni terimler elde ederek, f 'nin terimlerini sadeleştirmektir. Bunun için özel olarak S 'de bir terim sıralamasını belirledikten sonra bir f polinomu ile bir g polinomuna bölme algoritmasının uygulanması durumu aşağıda ifade edilmiştir.

Tanım 2.3.23 $g \neq 0$ olmak üzere $f, g \in S$ polinomları verilsin. f 'nin g 'ye göre bir adımda h 'ye indirgenmesi için, yani

$$f \xrightarrow{g} h$$

olması için gerek ve yeter koşul $lm(g)$ 'nin f 'nin sıfırdan farklı bir X terimini kısaltması ve

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

olmasıdır.

Uyarı 2.3.24 Yukarıdaki tanımda f 'den X teriminin tamamının çıkarıldığına ve X 'den daha küçük dereceli terimlerle yer değiştirildiğine dikkat edilmelidir. Burada

indirgeme işlemi yapılırken kullanılan sıralamanın belirlenmesi önemlidir. Sıralama değiştirildiğinde bölme algoritmasından elde edilen h polinomunun değiştiği aşağıdaki örnekte gösterilmiştir.

Örnek 2.3.25 $\mathbb{Q}[x, y]$ 'de $f = 6x^2y - x + 4y^3 - 1$ ve $g = 2xy + y^3$ polinomları verilsin. $y \prec x$ olmak üzere sözlüksel sıralamaya göre, $lt(g) = 2xy$ ve aynı zamanda (f 'nin başterimi olan) $X = 6x^2y$ kullanılarak, f polinomu g 'ye göre $h = -3xy^3 - x + 4y^3 - 1$ polinomuna indirgenir. Şimdi $y \prec x$ olmak üzere derece sözlüksel sıralama gözönüne alınırsa, $lt(g) = y^3$ ve (f 'nin başterimi olmayan) $X = 4y^3$ kullanılarak, f polinomu g 'ye göre $h = 6x^2y - 8xy - x - 1$ polinomuna indirgenir.

Uyarı 2.3.26 Tanım 2.3.23'deki h polinomu, Uyarı 2.2.8'e benzer olarak, f 'nin g ile bir adımdaki bölümünden bir kalan olarak düşünülebilir. Bu yöntem, f 'nin $lt(g)$ ile bölünebilen tüm terimleri sadeleşinceye kadar devam ettirilir.

Örnek 2.3.27 $\mathbb{Q}[x, y]$ 'de verilen $f = y^2 + 4yx - 3x^2$ ve $g = 2y + x + 1$ polinomlarına, $x \prec y$ olmak üzere derece sözlüksel sıralama kullanılarak, bölme algoritması uygulandığında

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

elde edilir. Burada kalan son $\frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$ polinomunun hiçbir teriminin $lm(g) = y$ ile bölünemediği açıktır.

Yukarıda, bir polinomun başka bir polinoma göre indirgenmesi ifade edilmiştir. Aşağıda ise bir polinomun birden fazla polinoma göre indirgenmesi ifade edilmektedir.

Tanım 2.3.28 $1 \leq i \leq s$ için $f_i \neq 0$ olmak üzere $f, h, f_i \in S$ ve $F = \{f_1, f_2, \dots, f_s\}$ olsun. f polinomunun F 'ye göre h polinomuna indirgenmesi, yani

$$f \xrightarrow{F}_+ h$$

olması için gerek ve yeter koşul

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

olacak şekilde indislerin bir $i_1, i_2, \dots, i_t \in \{1, 2, \dots, s\}$ dizisi ve polinomların bir $h_1, h_2, \dots, h_{t-1} \in S$ dizisi vardır.

Örnek 2.3.29 $\mathbb{Q}[x, y]$ 'de $f_1 = yx - y$ ve $f_2 = y^2 - x$ olmak üzere $F = \{f_1, f_2\}$ kümesi verilsin. $x \prec y$ olmak üzere derece sözlüksel sıralamaya göre, $f = y^2x$ polinomu için

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

olup f polinomu F 'ye göre x 'e indirgenir ve $f \xrightarrow{+} x$ ile gösterilir.

Tanım 2.3.28'de ifade edilen indirgeme yöntemi yardımıyla, n değişkenli polinomlar halkasında bölme algoritması aşağıdaki biçimde tanımlanır.

Tanım 2.3.30 (S 'de Bölme Algoritması) $1 \leq i \leq s$ için $f_i \neq 0$ olmak üzere $f, f_i \in S$ olsun. Bu durumda

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

olacak şekilde, *bölüm* (*quotient*) olarak adlandırılan $u_1, u_2, \dots, u_s \in S$ polinomları ve *kalan* (*remainder*) olarak adlandırılan $r \in S$ polinomu vardır.

GİRDİ (INPUT)	: $f, f_1, f_2, \dots, f_s \in K[x_1, \dots, x_n], f_i \neq 0 (1 \leq i \leq s)$
ÇIKTI (OUTPUT)	: $\max\{lm(u_1)lm(f_1), \dots, lm(u_s)lm(f_s), lm(r)\} = lm(f)$ $r : \{f_1, \dots, f_s\}$ 'ye göre indirgenmiş ve $f = u_1 f_1 + \dots + u_s f_s + r$ olacak şekilde $u_1, \dots, u_s, r \in K[x_1, \dots, x_n]$
BAŞLANGIÇ (INITIALIZATION)	: $u_1 := 0, \dots, u_s := 0, r := 0, h := f$
DÖNGÜ (WHILE)	$h \neq 0$
EĞER (IF)	YAP (DO) $lm(h)$ 'yı bölen $lm(f_i)$ 'ler varsa O ZAMAN (THEN) bunlardan en küçük i 'yi seç $u_i := u_i + \frac{lt(h)}{lt(f_i)}$ $h := h - \frac{lt(h)}{lt(f_i)} f_i$
DEĞİLSE (ELSE)	$r := r + lt(h)$ $h := h - lt(h)$

Şekil 2.3 n Değişkenli Polinomlar Halkasında Bölme Algoritması

Uyarı 2.2.10'da tek değişkenli bir f polinomu bir tane g polinomuna bölündüğünde bir tek q bölümü elde edilirken, bilgisayardaki akış şeması yukarıdaki gibi olan bölme

algoritmasında n değişkenli bir f polinomu s tane farklı $f_1, f_2, \dots, f_s$ polinomlarına bölündüğü için s tane $u_1, u_2, \dots, u_s$ bölümleri elde edilir. Her iki durumda da r kalan polinomu aynı özelliğe sahiptir, yani; r 'nin hiçbir terimi, herhangi bir bölen polinomunun başterimi ile bölünemez. Tek değişkenli bölme algoritmasında $r = f$ alınarak algoritma başlatılır. Yukarıdaki durum gerçekleşinceye kadar algoritma devam ettirilir. Fakat n değişkenli polinomlar halkasında bölme algoritması uygulanırken, fazladan bir h polinomuna ihtiyaç duyulduğu için bu yöntem geçerli değildir. Bundan dolayı bölme algoritması başlatılırken $h = f$ ve $r = 0$ alınarak, h 'nin başterimi r 'de görüldüğü sürece h 'nin başterimleri çıkarılır ve böylece r kalanı bulunur. Aynı zamanda, yukarıda verilen bilgisayardaki akış şemasındaki adımların nasıl çalıştığını gösteren, n değişkenli polinomlarda bölme algoritmasının bir uygulamasını aşağıdaki örnekte açıklayalım.

Örnek 2.3.31 $\mathbb{Q}[x, y, z]$ 'de verilen $f_1 = x^2 - 1, f_2 = xy - yz$ polinomları için $F = \{f_1, f_2\}$ olsun. $f = x^3 - x^2y + 2xy^2 + xyz$ polinomunun, $x \prec y \prec z$ olmak üzere sözlüksel sıralamaya göre bölme algoritmasının adımları aşağıdaki biçimdedir.

Başlat: $u_1 := 0, u_2 := 0, r := 0, h := f = x^3 - x^2y + 2xy^2 + xyz$

1. Döngü: $lm(f_1) = x^2, lm(h) = x^3$ 'yi böler

$$\begin{aligned} u_1 &:= u_1 + \frac{lt(h)}{lt(f_1)} = 0 + \frac{x^3}{x^2} = x \\ h &:= h - \frac{lt(h)}{lt(f_1)} f_1 = x^3 - x^2y + 2xy^2 + xyz - x(x^2 - 1) \\ &= -x^2y + 2xy^2 + xyz + x \end{aligned}$$

2. Döngü: $lm(f_1) = x^2, lm(h) = x^2y$ 'yi böler

$$\begin{aligned} u_1 &:= u_1 + \frac{lt(h)}{lt(f_1)} = x + \frac{-x^2y}{x^2} = x - y \\ h &:= h - \frac{lt(h)}{lt(f_1)} f_1 = -x^2y + 2xy^2 + xyz + x + y(x^2 - 1) \\ &= 2xy^2 + xyz + x - y \end{aligned}$$

3. Döngü: $lm(f_1) = x^2, lm(h) = xy^2$ 'yi bölmez

$lm(f_2) = xy$, $lm(h) = xy^2$ 'yi böler

$$u_2 := u_2 + \frac{lt(h)}{lt(f_2)} = 0 + \frac{2xy^2}{xy} = 2y$$

$$\begin{aligned} h &:= h - \frac{lt(h)}{lt(f_2)} f_2 = 2xy^2 + xyz + x - y - 2y(xy - yz) \\ &= xyz + x - y + 2y^2z \end{aligned}$$

4. Döngü: $lm(f_2) = xy$, $lm(h) = xyz$ 'yi böler

$$u_2 := u_2 + \frac{lt(h)}{lt(f_2)} = 2y + \frac{xyz}{xy} = 2y + z$$

$$\begin{aligned} h &:= h - \frac{lt(h)}{lt(f_2)} f_2 = xyz + x - y + 2y^2z - z(xy - yz) \\ &= 2y^2z + yz^2 + x - y \end{aligned}$$

5. Döngü: $lm(f_1) = x^2$ ve $lm(f_2) = xy$, $lm(h) = x$ 'i bölmez

$$r := r + lt(h) = 0 + x = x$$

$$\begin{aligned} h &:= h - lt(h) = 2y^2z + yz^2 + x - y - x \\ &= 2y^2z + yz^2 - y \end{aligned}$$

6. Döngü: $lm(f_1) = x^2$ ve $lm(f_2) = xy$, $lm(h) = y^2z$ 'yi bölmez

$$r := r + lt(h) = x + 2y^2z$$

$$\begin{aligned} h &:= h - lt(h) = 2y^2z + yz^2 - y - 2y^2z \\ &= yz^2 - y \end{aligned}$$

7. Döngü: $lm(f_1) = x^2$ ve $lm(f_2) = xy$, $lm(h) = yz^2$ 'yi bölmez

$$r := r + lt(h) = x + 2y^2z + yz^2$$

$$\begin{aligned} h &:= h - lt(h) = yz^2 - y - yz^2 \\ &= -y \end{aligned}$$

8. Döngü: $lm(f_1) = x^2$ ve $lm(f_2) = xy$, $lm(h) = y$ 'yi bölmez

$$r := r + lt(h) = x + 2y^2z + yz^2 - y$$

$$\begin{aligned} h &:= h - lt(h) = -y + y \\ &= 0 \end{aligned}$$

Algoritma sonlanır. Böylece $u_1 = x - y$, $u_2 = 2y + z$, $r = x + 2y^2z + yz^2 - y$ elde edilir ve $f = u_1f_1 + u_2f_2 + r$ biçiminde yazılır. Sonuç olarak $f \xrightarrow{+} x + 2y^2z + yz^2 - y$ olur.

Aşağıdaki teoremden, Tanım 2.3.30'da bölme algoritmasının tanımında var oldukları ifade edilen bölüm ve kalan polinomlarının sağladığı özellikler verilmiştir.

Teorem 2.3.32 S 'de sıfırdan farklı polinomların bir $F = \{f_1, f_2, \dots, f_s\}$ kümesi ve bir f polinomu verilsin. Bölme algoritmasından

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

ve r kalan polinomu F 'ye göre indirgenmiş olmak üzere

$$f = u_1f_1 + u_2f_2 + \dots + u_sf_s + r$$

olacak şekilde $u_1, u_2, \dots, u_s, r \in S$ vardır.

Bir f polinomunun Teorem 2.3.32'teki biçimde yazılması $f - r \in \langle f_1, f_2, \dots, f_s \rangle$ olması anlamına gelmektedir. $r = 0$ iken $f \in \langle f_1, f_2, \dots, f_s \rangle$ olup bu ifadenin karşıtı doğru değildir. Yani $f \in \langle f_1, f_2, \dots, f_s \rangle$ olsa bile f 'nin $f_1, f_2, \dots, f_s$ ile bölümünden kalanın 0 olmayabileceği aşağıdaki örnekte ifade edilmiştir.

Örnek 2.3.33 $\mathbb{Q}[x, y]$ 'de $f_1 = yx - y$ ve $f_2 = y^2 - x$ polinomları tarafından üretilen ideal $I = \langle f_1, f_2 \rangle$ olsun. $x \prec y$ olmak üzere derece sözlüksel sıralamaya göre $f = y^2x - x$ polinomuna bölme algoritması uygulanırsa $f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$ bulunur. Böylece $F = \{f_1, f_2\}$ olmak üzere $f \xrightarrow{+} 0$ olup $f = yf_1 + f_2$ biçiminde yazılır. Burada bölme algoritmasından elde edilen kalan sıfırdır ve $f \in I$ olur. Diğer yandan, bölme algoritmasında kullanılan sıralama değiştirilerek f polinomu önce f_2 'ye göre indirgenirse $f \xrightarrow{f_2} x^2 - x$ ve buradan $f \xrightarrow{+} x^2 - x$ bulunur. Burada elde edilen kalan polinomu sıfırdan farklı olduğu halde $f \in I$ dır.

3. GRÖBNER TABANLARI

Çok değişkenli polinomlar halkasındaki bir I ideali için bir Gröbner taban (seçilen sıralamaya göre değişen) idealin cebirsel yapısının en iyi şekilde anlaşılmasını sağlayan bir üreteç kümesidir ve böylece I 'daki her eleman üreteçlerin bir lineer bileşimi olarak yazılır. Tanım 3.1.1'de verilen Gröbner taban; lineer cebirde yer alan vektör uzayının bir tabanı (yani, lineer bileşimlerin tek türlü yazılması) anlamında değildir. Burada bir G kümesinin I idealinin bir Gröbner tabanı olması; I 'da G 'ye göre indirgenmediğinde kalanı sıfırdan farklı olan hiç bir polinomun bulunmaması, yani; I 'daki her polinomun G 'ye göre sıfıra indirgenmesi anlamındadır. Bu tanımdan Gröbner tabanın varlığı açık olmamakla birlikte Sonuç 3.1.6'da Gröbner tabanın her zaman var olduğu gösterilecektir.

İlk olarak, Gröbner taban karakterizasyonlarının ve örneklerinin yer aldığı ve Gröbner taban bulmaya yarayan Buchberger algoritmasının ifade edildiği klasik Gröbner taban teorisi tanıtılacaktır. Daha sonra indirgenmiş Gröbner taban ve minimal Gröbner taban kavramları tanıtılarak özellikleri incelenecektir. Bu bölümde Dummit ve Foote (2004), Adams ve Loustana (2000), Ene ve Herzog (2012), Malik vd. (1997) ve Buchberger (1998) kullanılan temel kaynaklardır.

3.1. Klasik Gröbner Taban Teorisi

Tanım 3.1.1 S 'nin bir I ideali ve sıfırdan farklı polinomlardan oluşan I 'nın bir $G = \{g_1, g_2, \dots, g_t\}$ altkümesi verilsin. Her $0 \neq f \in I$ polinomu için $lm(g_i); lm(f)$ 'yi bölecek şekilde $i \in \{1, 2, \dots, t\}$ varsa G 'ye I için bir *Gröbner taban* ya da *standart taban* (*Gröbner basis*) denir.

Şimdi Gröbner tabanın karakterizasyonları için gerekli olan aşağıdaki tanımları verelim.

Tanım 3.1.2 S 'deki bir G altkümesinde yer alan polinomların başterimleri tarafından üretilen ideale *baş terim ideali* (*leading term ideal*) adı verilir ve

$$Lt(G) = \langle lt(g) \mid g \in G \rangle$$

ile gösterilir.

Bir kümenin Gröbner taban olup olmadığını kontrol etmek için Tanım 3.1.1 kullanışlı olmayabilir. Bunun için aşağıdaki teoremden Gröbner tabanın bazı karakterizasyonları verilmiştir.

Teorem 3.1.3 I, S 'nin sıfırdan farklı bir ideali olsun. I 'nin sıfırdan farklı polinomlarının oluşturduğu bir $G = \{g_1, g_2, \dots, g_t\}$ altkütmesi için aşağıdaki ifadeler birbirine denktir:

- (i) G, I için bir Gröbner tabandır.
- (ii) $f \in I$ olması için gerek ve yeter koşul $f \xrightarrow{+}_G 0$ olmasıdır.
- (iii) $f \in I$ olması için gerek ve yeter koşul $lm(f) = \max_{1 \leq i \leq t}(lm(h_i)lm(g_i))$ olmak üzere $f = \sum_{i=1}^t h_i g_i$ biçiminde yazılmasıdır.
- (iv) $Lt(G) = Lt(I)$ olmasıdır.

İspat (i) $\Rightarrow$ (ii) G, I için bir Gröbner taban olmak üzere $f \in I$ olsun. Kabul edelim ki $f \xrightarrow{+}_G r$ ve $r \neq 0$ olsun. Bu durumda $r \in I$ olup kabulden $lm(g_i)$ böler $lm(r)$ olacak şekilde bir $i \in \{1, 2, \dots, t\}$ vardır. Bu durum r 'nin G 'ye göre indirgenmiş olması ile çelişir. Böylece $r = 0$ olup $f \xrightarrow{+}_G 0$ bulunur. Karşıt olarak $f \in S$ için $f \xrightarrow{+}_G 0$ olduğunu kabul edelim. Teorem 2.3.32 gereğince $f \xrightarrow{+}_G r$ olacak şekilde $r \in S$ polinomu vardır. Böylece $f - r \in I$ ve buradan $f \in I$ olması için gerek ve yeter koşul $r \in I$ olmasıdır. Kabulden $r = 0$ olduğundan $f \in I$ olduğu açıktır.

(ii) $\Rightarrow$ (iii) $f \in I$ polinomu için $f \xrightarrow{+}_G 0$ olduğu kabul edilirse Teorem 2.3.32'teki bölme algoritması gereğince (iii) ifadesi açıktır.

(iii) $\Rightarrow$ (iv) Kabul edelim ki (iii) ifadesi sağlansın. Bu durumda $Lt(G) \subseteq Lt(I)$ olduğu açıktır. Ters kapsama için, kabulden $f = \sum_{i=1}^t h_i g_i$ olacak şekildeki i 'ler üzerinden toplam alınarak

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

biçiminde yazılır. Böylece $lt(f) \in Lt(G)$ olup $Lt(I) \subseteq Lt(G)$ elde edilir.

(iv) $\Rightarrow$ (i) $Lt(G) = Lt(I)$ olduğunu kabul edelim. $f \in I$ alalım. Bu durumda kabulden $lt(f) \in Lt(G)$ olup $lt(f) = \sum_i^t h_i lt(g_i)$ biçiminde yazılır. Böylece $lm(f), lm(g_i)$ 'ler tarafından bölünür. Sonuç olarak G, I için bir Gröbner tabandır.

Tanım 3.1.1'den de anlaşılacağı gibi bir idealin bir tabanı Gröbner taban olmak zorunda değildir. Fakat Teorem 3.1.3'ün bir sonucu olarak, I idealinin bir Gröbner tabanının aynı zamanda bir taban olduğu aşağıda ifade edilmiştir.

Sonuç 3.1.4 $G = \{g_1, g_2, \dots, g_t\}$ kümesi I ideali için bir Gröbner taban ise, bu durumda $I = \langle g_1, g_2, \dots, g_t \rangle$ dir.

İspat $G = \{g_1, g_2, \dots, g_t\}$ kümesi I ideali için bir Gröbner taban olsun. Gröbner tabanın tanımından $\langle g_1, g_2, \dots, g_t \rangle \subseteq I$ olduğu açıktır. $f \in I$ alalım. Teorem 3.1.3 gereğince $f \xrightarrow{+} 0$ olup $f \in \langle g_1, g_2, \dots, g_t \rangle$ elde edilir.

Gröbner tabanın her zaman var olduğu sonucunu ispatlayabilmek için ihtiyacımız olan, baş terim ideallerinin doğal yapısı hakkındaki, bir özellik aşağıdaki lemmada ifade edilmiştir.

Lemma 3.1.5 I sıfırdan farklı terimlerin bir J kümesi tarafından üretilen bir baş terim ideali ve $f \in S$ olsun. $f \in I$ olması için gerek ve yeter koşul f 'de bulunan her X terimi için Y böler X olacak şekilde bir $Y \in J$ 'nin var olmasıdır. Ayrıca $I = \langle J_0 \rangle$ olacak şekilde J 'nin bir sonlu J_0 altkümesi vardır.

İspat $f \in I$ olsun. Bu durumda $i = 1, 2, \dots, l$ için

$$f = \sum_{i=1}^l h_i X_i$$

olacak şekilde $h_i \in S$ ve $X_i \in J$ vardır. Böylece f 'deki her terimi bölen bir $X_i \in J$ var olduğu açıktır. Diğer taraftan f 'de görünen her X terimini bölen bir $Y \in J$ var olsun. Bu durumda $X \in \langle J \rangle = I$ olup $f \in I$ olduğu açıktır. Ayrıca Teorem 2.3.22'de ifade edilen Hilbert'in Taban Teoremi gereğince I sonlu bir üreteç kümesine sahiptir. Lemmanın ilk kısmında ifade edildiği gibi, bu üreteç kümesinin her bir elemanının her bir terimi J 'nin bir elemanı ile bölünür. O halde bu bölenlerin oluşturduğu J 'nin sonlu bir J_0 altkümesi I 'yı üretir.

Aşağıdaki sonuç Gröbner tabanın her zaman var olduğunu ifade eder.

Sonuç 3.1.6 S 'deki sıfırdan farklı her I ideali bir Gröbner tabana sahiptir.

İspat Lemma 3.1.5 gereğince, $g_1, g_2, \dots, g_t \in I$ olmak üzere, $Lt(I)$ baş terim ideali $\{lt(g_1), lt(g_2), \dots, lt(g_t)\}$ formunda bir üreteç kümesine sahiptir. $G = \{g_1, g_2, \dots, g_t\}$ olarak alınırsa $Lt(I) = Lt(G)$ olup Teorem 3.1.3 gereğince G 'nin I için bir Gröbner taban olduğu açıktır.

Aşağıdaki lemmada, Gröbner tabanın Teorem 3.1.3'te verilen karakterizasyonlarına bir yenisi daha eklenecektir. Bunun için S 'de verilen Gröbner taban tanımı şu şekilde genişletilir: S 'nin bir $G = \{g_1, g_2, \dots, g_t\}$ kümesinin bir Gröbner taban olması için gerek ve yeter koşul G kümesinin $\langle G \rangle$ idealinin bir Gröbner taban olmasıdır.

Lemma 3.1.7 $G = \{g_1, g_2, \dots, g_t\}$ sıfırdan farklı polinomların bir kümesi ve r , G 'ye göre indirgenmiş bir polinom olmak üzere $0 \neq c \in K$ ve $X \in \text{Mon}(S)$ için $f \xrightarrow{+}_G r$ olacak şekilde $f \in S$ ise, bu durumda her bir $i \in \{1, 2, \dots, t\}$ için $f - cXg_i \xrightarrow{+}_G r$ dir.

Lemma 3.1.7'de; G 'ye göre indirgendiğinde r kalanını veren bir f polinomundan cXg_i biçimindeki bazı terimler çıkarıldığında, elde edilen polinomun G 'ye göre indirgenmesinden bulunan kalanın hala r olduğu ifade edilir. Daha açık olarak; $f \xrightarrow{+}_G r$ olması durumunda $f = u_1g_1 + u_2g_2 + \dots + u_tg_t + r$ biçiminde yazılır. Bu eşitliğin her iki tarafına $-cXg_i$ eklenirse $f - cXg_i = u_1g_1 + u_2g_2 + \dots + u_i g_i - cXg_i + \dots + u_tg_t + r$ ve buradan yeni elde edilen $f - cXg_i$ polinomu $u_1g_1 + u_2g_2 + \dots + (u_i - cX)g_i + \dots + u_tg_t + r$ biçiminde olup G ile indirgenmesinden elde edilen kalanın r olduğu açıktır.

Teorem 3.1.8 S 'de sıfırdan farklı polinomların bir kümesi $G = \{g_1, g_2, \dots, g_t\}$ olsun. G 'nin bir Gröbner taban olması için gerek ve yeter koşul her $f \in S$ polinomunun G ile bölümünden kalanın bir tek olmasıdır.

İspat G , S 'de bir Gröbner taban olsun. Kabul edelim ki bir $f \in S$ polinomunun G ile bölümünden farklı r_1 ve r_2 kalanları var olsun. Yani; $r_1 \neq r_2$ olmak üzere $f \xrightarrow{+}_G r_1$ ve $f \xrightarrow{+}_G r_2$ olsun. Bu durumda $f - r_1$ ve $f - r_2$ polinomları $\langle G \rangle$ 'de olup buradan $r_1 - r_2 \in \langle G \rangle$ elde edilir. Kabul ve Teorem 3.1.3(ii) gereğince $r_1 - r_2 = 0$ olup $r_1 = r_2$ bulunur.

Tersine her $f \in S$ polinomunun G ile bölümünden kalan bir tek olsun. Teorem 3.1.3(ii)'yi kullanarak G 'nin bir Gröbner taban olduğunu gösterelim. $f \in \langle G \rangle$

olmak üzere $f \xrightarrow{+}_G r$ olduğunu kabul edelim. $r = 0$ olduğunu gösterirsek ispat tamamlanır. $f \in \langle G \rangle$ olduğundan $f = \sum_{v=1}^l c_v X_v g_{i_v}$ olacak şekilde $c_v \in K$, $X_v \in \text{Mon}(S)$ ve $i_v \in \{1, 2, \dots, t\}$ vardır. f 'nin lineer bileşimindeki bir terim yok edildiğinde elde edilen yeni polinomun G ile bölümünden kalan, Lemma 3.1.7 gereğince r 'dir. f 'nin tüm terimleri bu yöntemle yok edildiğinde 0 polinomu elde edilir ve bunun G ile bölümünden kalan r olur. Halbuki 0 polinomu G 'ye göre 0'a indirgendiğinden, kabul gereğince $r = 0$ olmak zorundadır. Sonuç olarak G bir Gröbner tabandır.

Aşağıda bu teoremin bir uygulaması verilmiştir.

Örnek 3.1.9 $f = x^2 + x - y^2 + y, g_1 = xy + 1, g_2 = x + y \in \mathbb{Q}[x, y]$ olmak üzere $G = \{g_1, g_2\}$ olsun. f polinomunu G 'ye göre farklı şekilde indirgenebilir.

I. durum: $x \prec y$ olmak üzere sözlüksel terim sıralamasına göre f polinomunu G 'ye göre indirgendiğinde

$$f \xrightarrow{+}_G -xy + x - y^2 + y \xrightarrow{+}_G x - y^2 + y + 1 \xrightarrow{+}_G -y^2 + 1$$

olup buradan

$$q_1 = -1, \quad q_2 = x + 1, \quad r = -y^2 + 1$$

olmak üzere $f = q_1 g_1 + q_2 g_2 + r$ biçiminde yazılır.

II. durum: $y \prec x$ olmak üzere sözlüksel terim sıralamasına göre f polinomunu G 'ye göre indirgendiğinde

$$f \xrightarrow{+}_G xy + x^2 + x + y \xrightarrow{+}_G xy + x^2 \xrightarrow{+}_G 0$$

olup buradan

$$q_1 = 0, \quad q_2 = -y + 1 + x, \quad r = 0$$

olmak üzere $f = q_1 g_1 + q_2 g_2 + r$ biçiminde yazılır. Bu durumda f 'nin iki farklı gösterimi elde edilir. f 'nin G 'ye bölümünden kalan birinci durumda $-y^2 + 1$, ikinci durumda 0 olup, iki farklı kalan elde edildiği için Teorem 3.1.8 gereğince G bir Gröbner taban olamaz. Ayrıca Teorem 3.1.3(ii) gereğince f 'nin I 'da olup olmadığına karar verilemez (Dummit ve Foote 2004).

Uyarı 3.1.10 Örnek 3.1.9’da görüldüğü gibi, bir sıralamaya göre Gröbner taban olan bir G kümesi başka bir sıralamaya göre Gröbner taban olmayabilir. Şimdi bir polinom kümesinin bir Gröbner taban olup olmadığını kontrol etmek ya da bir idealin bir Gröbner tabanını bulmak için, Bruno Buchberger tarafından tanımlanan ve geliştirilen bir algoritma vereceğiz. Şimdi *Buchberger algoritması* olarak adlandırılan bu algoritmaya neden ihtiyaç duyulduğunu açıklayalım:

$1 \leq i \leq s$ için $g_i \neq 0$ ve $G = \{g_1, g_2, \dots, g_s\}$ olmak üzere I , G tarafından üretilen S ’nin bir ideali olsun. Gröbner taban tanımından; G ’nin bir Gröbner taban olması için gerek yeter koşul her $f \in I$ için $lm(g_i)$; $lm(f)$ ’yi bölecek şekilde bir $i \in \{1, 2, \dots, s\}$ ’nin var olmasıdır. Ancak, baş terimler $lm(g_i)$ ’lerin hiç biriyle bölünemeyen, I ’nin bazı elemanları olabilir ya da $f \in I$ iken $f = \sum_{i=1}^s h_i g_i$ olacak şekilde $h_i \in S$ var olsa bile $lm(h_i g_i) = lm(h_i)lm(g_i)$ ’lerin en büyüğünün sadeleşmesi gibi iki farklı sorunla karşılaşılabilir. Bu gibi sorunların çözümü için, aşağıda tanımı verilen, S -polinomları kullanılır.

Tanım 3.1.11 S ’de sıfırdan farklı f ve g polinomları verilsin. $L = \text{ekok}(lm(f), lm(g))$ olmak üzere

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

ile tanımlı polinoma f ile g ’nin S -polinomu (S -polynomial) denir.

S -polinomlarını hesaplamanın başka bir yolu daha vardır: f polinomu $g_1, g_2, \dots, g_s$ polinomlarına bölündüğünde f ’nin bazı X terimleri $i \neq j$ iken hem $lm(g_i)$ ile hem de $lm(g_j)$ ile (dolayısıyla $L = \text{ekok}(lm(g_i), lm(g_j))$ ile bölünebilir. f polinomu g_i kullanılarak indirgendiğinde $h_1 = f - \frac{X}{lt(g_i)}g_i$ polinomu, g_j kullanılarak indirgendiğinde $h_2 = f - \frac{X}{lt(g_j)}g_j$ polinomu elde edilir. Buradan

$$h_2 - h_1 = \frac{X}{lt(g_i)}g_i - \frac{X}{lt(g_j)}g_j = \frac{X}{L}S(g_i, g_j)$$

olup $S(g_i, g_j) = \frac{L}{X}(h_2 - h_1)$ ile bulunur.

Örnek 3.1.12 $\mathbb{Q}[x, y]$ ’de $f = y^2x + 1$, $g_1 = yx - y$, $g_2 = y^2 - x$ polinomları verilsin. $x \prec y$ olmak üzere derece sözlüksel sıralamaya göre, Tanım 3.1.11 kullanılarak, g_1 ve g_2 ’nin S -polinomunu bulalım. $L = \text{ekok}(yx, y^2) = y^2x$ olmak üzere

$$S(g_1, g_2) = \frac{L}{lt(g_1)}g_1 - \frac{L}{lt(g_2)}g_2 = \frac{y^2x}{yx}g_1 - \frac{y^2x}{y^2}g_2 = yg_1 - xg_2$$

bulunur.

Şimdi, f polinomunun g_1 ve g_2 ile bölümünden kalanlarını kullanarak, g_1 ve g_2 'nin S -polinomunu bulalım. f 'deki X terimi, L ile bölünebilen, y^2x olarak gözönüne alınırsa $f \xrightarrow{g_1} h_1 = y^2 + 1$ ve $f \xrightarrow{g_2} h_2 = x^2 + 1$ ve buradan $h_1 = f - yg_1$ ve $h_2 = f - xg_2$ olup $S(g_1, g_2) = \frac{L}{X}(h_2 - h_1) = yg_1 - xg_2$ elde edilir. Burada $S(g_1, g_2)$ 'de $lm(yg_1) = y^2x = lm(xg_2)$ teriminin sadeleştiğine dikkat edilmelidir.

Bölme Algoritması uygularken yaşanan belirsizliği ortadan kaldırmanın ve baş terimleri “sadeleştirmenin” bir yolu olarak S -polinomlarının elde edilmesine dair iki farklı yöntem verdik. Şimdi Gröbner tabanlarını, S -polinomları yardımıyla, karakterize etmek için kullanılan bir metod olan Buchberger algoritmasını vermeden önce aşağıdaki lemmayı verelim.

Lemma 3.1.13 Her $i = 1, \dots, s$ için g_i polinomlarının baş tekterimlileri sıfırdan farklı bir X olmak üzere, f polinomu $c_i \in K$ için $f = \sum_{i=1}^s c_i g_i$ biçiminde $g_i \in S$ polinomlarının bir lineer bileşimi olarak yazılsın. Eğer f 'nin baş tekterimlisi X 'den küçük ise, bu durumda f polinomu $1 \leq i < j \leq s$ için $S(g_i, g_j)$ -polinomlarının bir lineer bileşimi olarak yazılır.

İspat Her bir $1 \leq i \leq s$ için g_i polinomlarının baş tekterimlisi X olmak üzere, $f = \sum_{i=1}^s c_i g_i$ biçiminde yazılan bir f polinomunun baş tekterimlisi X 'den küçük olsun. Bu durumda $a_i \in K$ olmak üzere g_i polinomları

$$g_i = a_i X + \{X \text{ 'den daha küçük terimler}\}$$

olarak ifade edilirse $\sum_{i=1}^s c_i a_i = 0$ bulunur. Diğer yandan aşağıdaki lineer bileşimin sağ tarafındaki her bir terimde, g_i polinomlarının baş tekterimlisi olan X terimini sadeleştiren S -polinomları elde edilecek şekilde terim eklenip çıkarılırsa

$$\begin{aligned}
f &= \sum_{i=1}^s c_i g_i \\
&= c_1 g_1 + c_2 g_2 + \cdots + c_s g_s \\
&= c_1 a_1 \left(\frac{1}{a_1} g_1 \right) + c_2 a_2 \left(\frac{1}{a_2} g_2 \right) + \cdots + c_s a_s \left(\frac{1}{a_s} g_s \right) \\
&= c_1 a_1 \left(\frac{1}{a_1} g_1 - \frac{1}{a_2} g_2 \right) + (c_1 a_1 + c_2 a_2) \left(\frac{1}{a_2} g_2 - \frac{1}{a_3} g_3 \right) + \cdots \\
&\quad + (c_1 a_1 + \cdots + c_{s-1} a_{s-1}) \left(\frac{1}{a_{s-1}} g_{s-1} - \frac{1}{a_s} g_s \right) + (c_1 a_1 + \cdots + c_s a_s) \frac{1}{a_s} g_s \\
&= c_1 a_1 S(g_1, g_2) + (c_1 a_1 + c_2 a_2) S(g_2, g_3) + \cdots + (c_1 a_1 + \cdots + c_{s-1} a_{s-1}) S(g_{s-1}, g_s)
\end{aligned}$$

elde edilir. Böylece f polinomu S -polinomlarının bir lineer bileşimi olarak yazılmış olur.

Teorem 3.1.3(iii)'te, bir $G = \{g_1, g_2, \dots, g_s\}$ kümesinin bir I idealinin bir Gröbner tabanı olması için gerek ve yeter koşulun her $f \in I$ için, g_i 'lerin baş tekterimlileri f 'nin baş tekterimlisinden küçük iken, yani;

$$lm(f) = \max_{1 \leq i \leq t} (lm(h_i) lm(g_i))$$

olması durumunda f polinomunun g_i 'lerin bir lineer bileşimi olarak yazılması gerektiği kanıtlanmıştır. Bu durum sağlanmadığında, yani; g_i 'lerin baş tekterimlileri f 'nin baş tekterimlisinden büyük olduğunda f polinomunun g_i 'lerin S -polinomlarının bir lineer bileşimi olarak yazıldığı Lemma 3.1.13'de ifade edilmiştir.

Şimdi Gröbner tabanı hesaplamak için bir yöntem olarak kullanılabilen Buchberger Teoremini ispatlayalım.

Teorem 3.1.14 (Buchberger Teoremi) S 'deki sıfırdan farklı polinomların bir kümesi $G = \{g_1, g_2, \dots, g_t\}$ olsun. G 'nin $I = \langle g_1, g_2, \dots, g_t \rangle$ idealinin bir Gröbner tabanı olması için gerek ve yeter koşul her $i \neq j$ için $S(g_i, g_j) \xrightarrow{+} 0$ olmasıdır.

İspat $(\Rightarrow)$ $G, I = \langle g_1, g_2, \dots, g_t \rangle$ idealinin bir Gröbner tabanı olsun. Bu durumda her $i \neq j$ için $S(g_i, g_j)$ polinomları g_i 'lerin lineer bileşimi olarak yazıldığından, Teorem 3.1.3 gereğince $S(g_i, g_j) \xrightarrow{+} 0$ olduğu açıktır.

($\Leftarrow$) Kabul edelim ki $i \neq j$ için $S(g_i, g_j) \xrightarrow{+}_G 0$ olsun. G 'nin I idealinin bir Gröbner tabanı olduğunu Teorem 3.1.3(iii)'yi kullanarak gösterelim. $f \in I$ alalım. Bu durumda g_i 'ler I ideali için birer üreteç olduğundan f polinomu g_i 'lerin lineer bileşimi olarak yazılabilir. Seçilen herhangi bir terim sıralamasının iyi sıralı olma özelliği kullanılarak

$$X = \max_{1 \leq i \leq t} (lm(h_i)lm(g_i))$$

baş tekterimlisi en küçük olacak şekilde $f = \sum_{i=1}^t h_i g_i$ biçiminde yazıldığını kabul edelim. Eğer $lm(f) = X$ ise, Teorem 3.1.3(iii)'den ispat tamamlanır. Aksi takdirde, seçilen sıralamaya göre $lm(f)$ 'in X 'den küçük olması durumunda ise, f polinomu yukarıda kabul edilen yazılışından daha küçük bir yazılışla ifade edilecek ve çelişki bulunarak ispat tamamlanacaktır. Şimdi baş tekterimlilerinin çarpımı X 'i veren h_i ve g_i polinomlarının indislerinin kümesine $S = \{i \mid lm(h_i)lm(g_i) = X\}$ diyelim. Bu durumda $i \in S$ için h_i polinomları $h_i = c_i X_i + \{\text{küçük terimler}\}$ biçiminde yazılır ve $g = \sum_{i \in S} c_i X_i g_i$ olarak alınırsa her $i \in S$ için $lm(X_i g_i) = X$ olur fakat g 'nin baş tekterimlisi X 'den küçük kalır. Bu durumda Lemma 3.1.13 gereğince

$$g = \sum_{i,j \in S, i \neq j} d_{ij} S(X_i g_i, X_j g_j) \quad (3.1)$$

biçiminde yazılır. Her bir $i \in S$ için $\text{ekok}(lm(X_i g_i), lm(X_j g_j)) = X$ ve $\text{ekok}(lm(g_i), lm(g_j)) = X_{ij}$ olmak üzere

$$\begin{aligned} S(X_i g_i, X_j g_j) &= \frac{X}{lt(X_i g_i)} X_i g_i - \frac{X}{lt(X_j g_j)} X_j g_j \\ &= \frac{X}{lt(g_i)} g_i - \frac{X}{lt(g_j)} g_j \\ &= \frac{X}{X_{ij}} S(g_i, g_j) \end{aligned}$$

elde edilir. Kabulden $S(g_i, g_j) \xrightarrow{+}_G 0$ olduğundan $S(X_i g_i, X_j g_j) \xrightarrow{+}_G 0$ olup Teorem 2.3.32'te ifade edilen bölme algoritması ve Teorem 3.1.3 gereğince

$$\max_{1 \leq v \leq t} (lm(h_{iv})lm(g_v)) = lm(S(X_i g_i, X_j g_j)) \prec X$$

olacak şekilde

$$S(X_i g_i, X_j g_j) = \sum_{v=1}^t h_{iv} g_v \quad (3.2)$$

yazılışı vardır. Böylece (3.1) ve (3.2) eşitlikleri f 'nin gösteriminde yerine yazılırsa $\max_{1 \leq i \leq t} (lm(h'_i lm(g_i))) \prec X$ olmak üzere $f = \sum_{i=1}^t h'_i g_i$ bulunur ki bu durum başlangıçta seçilen f 'nin yazılışı ile çelişir. O halde Teorem 3.1.3(iii) gereğince

$$X = lm(f) = \max_{1 \leq i \leq t} (lm(h_i) lm(g_i))$$

olacak şekilde $f = \sum_{i=1}^t h_i g_i$ biçiminde yazıldığı için G bir Gröbner taban olur.

Bir G kümesinin bir idealin Gröbner tabanı olması için idealdeki herhangi bir polinomun G 'ye göre sıfıra indirgenmesi gerek ve yeter koşul olarak Teorem 3.1.3'te ifade edilmişti. Buchberger yukarıdaki teoremi kanıtlayarak, G 'deki polinomların S -polinomlarının da G 'ye göre sıfıra indirgenmesi durumunda, hem Gröbner taban hesaplamaya yarayan algoritmasını geliştirmeye zemin hazırlamış hem de Gröbner tabanın farklı bir karakterizasyonunu ifade etmiştir. Teorem 3.1.3(iii)'teki karakterizasyona benzer olarak yukarıdaki teoremin bir sonucu aşağıda verilmiştir.

Sonuç 3.1.15 $1 \leq i \leq t$ için sıfırdan farklı polinomların oluşturduğu bir $G = \{g_1, g_2, \dots, g_t\}$ kümesi verilsin. G 'nin bir Gröbner taban olması için gerek ve yeter koşul her $i \neq j$ için $lm(S(g_i, g_j)) = \max_{1 \leq v \leq t} (lm(h_{ijv}) lm(g_v))$ olacak şekilde

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

biçiminde yazılmasıdır.

Gröbner taban hesaplamaya yarayan ve Buchberger tarafından geliştirilen aşağıdaki algoritma, basitçe şu esasa dayanır: Bir G kümesini oluşturan polinomların S -polinomları hesaplanır ve G kümesine göre indirgenir. Bu indirgemedede sıfır kalanını veren S -polinomunu oluşturan polinomlar Gröbner taban olarak alınırken, kalanı sıfır olmayan S -polinomları başka bir eleman olarak kümeye eklenir ve böylece yeni bir küme oluşturulur. Elde edilen yeni kümede, önceki kümenin polinomlarının S -polinomları bu kümeye göre zaten sıfıra indirgenmiş olacağından, en son eklenen polinomun önceki polinomlarla oluşturulan S -polinomlarının bu kümeye göre sıfıra indirgenip indirgenmediğine bakılır. Tüm S -polinomları sıfıra indirgeninceye kadar bu işlem tekrarlanır. Bu yolla elde edilen en son küme, $\langle G \rangle$ ideali için bir Gröbner taban olur. Şimdi Buchberger algoritmasını bir örnek üzerinde açıklayalım.

Örnek 3.1.16 $\mathbb{Q}[x, y]$ 'de $g_1 = x^3y - xy^2 + 1$ ve $g_2 = x^2y^2 - y^3 - 1$ polinomlarından oluşan $G = \{g_1, g_2\}$ kümesi ve $I = \langle g_1, g_2 \rangle$ ideali verilsin. $x \prec y$ olmak üzere sözlüksel sıralamaya göre, I idealinin bir Gröbner tabanını, yukarıda açıklandığı gibi öncelikle G kümesindeki polinomların S -polinomunu hesaplayarak bulalım. $lm(g_1) = x^3y, lm(g_2) = x^2y^2, lt(g_1) = x^3y$ ve $lt(g_2) = x^2y^2$ olmak üzere $L = \text{ekok}(lm(g_1), lm(g_2)) = x^3y^2$ dir. Buna göre

$$S(g_1, g_2) = \frac{L}{lt(g_1)}g_1 - \frac{L}{lt(g_2)}g_2 = yg_1 - xg_2 = x + y$$

biçiminde olup $S(g_1, g_2) \xrightarrow{G} x + y \neq 0$ olduğundan G kümesi I ideali için bir Gröbner taban değildir. Bu durumda $g_3 = x + y$ alınarak $G' = \{g_1, g_2, g_3\}$ kümesi oluşturulur. $S(g_1, g_2) \xrightarrow{+} 0$ olduğu açık olup son eklenen polinom ile önceki polinomların S -polinomlarını hesaplayalım. $lm(g_3) = x, lt(g_3) = x$ olmak üzere $L = \text{ekok}(lm(g_1), lm(g_3)) = x^3y$ için

$$S(g_1, g_3) = \frac{x^3y}{x^3y}g_1 - \frac{x^3y}{x}g_3 = g_1 - x^2yg_3 = -x^2y^2 - xy^2 + 1$$

olup $S(g_1, g_3) \xrightarrow{+} 0$ bulunur. Son olarak $L = \text{ekok}(lm(g_2), lm(g_3)) = x^2y^2$ olmak üzere

$$S(g_2, g_3) = g_2 - xyg_3 = -xy^3 - y^3 - 1$$

olup $S(g_2, g_3) \xrightarrow{+} -xy^3 - y^3 - 1 \neq 0$ olduğundan G' kümesi I ideali için bir Gröbner taban değildir. $g_4 = -xy^3 - y^3 - 1$ alınarak $G'' = \{g_1, g_2, g_3, g_4\}$ kümesi oluşturulur. Buradan $S(g_1, g_2) \xrightarrow{+} 0$, $S(g_1, g_3) \xrightarrow{+} 0$ ve $S(g_2, g_3) \xrightarrow{+} 0$ olduğu açık olup

$$S(g_1, g_4) \xrightarrow{+} 0, \quad S(g_2, g_4) \xrightarrow{+} 0 \quad \text{ve} \quad S(g_3, g_4) \xrightarrow{+} 0$$

olduğu yukarıdaki gibi hesaplanır. Sonuç olarak G'' kümesi I idealinin bir Gröbner tabanı olur.

Aşağıdaki teoremden Gröbner taban hesaplamaya yarayan Buchberger algoritması ve bilgisayardaki akış şeması verilmiştir.

Teorem 3.1.17 $1 \leq i \leq s$ için $g_i \neq 0$ olmak üzere $G = \{g_1, g_2, \dots, g_s\}$ kümesi ve $I = \langle g_1, g_2, \dots, g_s \rangle$ ideali verilsin. I idealinin bir Gröbner tabanı, aşağıda bilgisayardaki akış şeması verilen, Buchberger algoritması ile bulunur.

GİRDİ (INPUT)	$: F = \{f_1, \dots, f_s\} \subseteq K[x_1, \dots, x_n], 1 \leq i \leq s \text{ için } f_i \neq 0$
ÇIKTI (OUTPUT)	$: G = \{g_1, \dots, g_t\}, \langle f_1, \dots, f_s \rangle \text{ için bir Gröbner taban}$
BAŞLANGIÇ (INITIALIZATION)	$: G := F, \mathcal{G} := \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$
DÖNGÜ (WHILE)	$\mathcal{G} \neq \emptyset$ YAP (DO) Herhangi bir $\{f, g\} \in \mathcal{G}$ 'yi seç $\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$ $S(f, g) \xrightarrow{G}_+ h; h, G$ 'ye göre indirgenmiştir.
EĞER (IF)	$h \neq 0$ O ZAMAN (THEN) $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid u \in G\}$ $G := G \cup \{h\}$

Şekil 3.1 Buchberger Algoritması

İspat Buchberger algoritmasının sonlandığını göstermek ispat için yeterlidir. Kabul edelim ki, adımları yukarıdaki akış şemasında verilen, bu algoritma sonlanmasın. Bu durumda, algoritma sürecinde ifade edildiği gibi, her bir G_i kümesi G_{i-1} kümesini öz olarak kapsayacak şekilde, sonsuz artan bir

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \dots \quad (3.3)$$

dizisi elde edilir. Her bir G_i kümesi; G_{i-1} 'e göre indirgendiğinde kalanı sıfırdan farklı olan, iki elemanının S -polinomu olarak belirlenmiş bir $h \in I$ polinomunun, G_{i-1} kümesine eklenmesiyle oluşturulur. Bu şekilde bulunan her bir h polinomu G_{i-1} 'e göre indirgenmiş olduğundan $lt(h) \notin Lt(G_{i-1})$ olur. Böylece başterim ideallerinin sonsuz artan bir

$$Lt(G_1) \subsetneq Lt(G_2) \subsetneq Lt(G_3) \subsetneq \dots$$

dizisi elde edilmiş olur. Bu durum ise Teorem 2.3.22'de ifade edilen Hilbert'in Taban Teoremi ile çelişir. O halde (3.3)'teki artan dizisi bir $G' = \{g'_1, g'_2, \dots, g'_t\}$ kümesinde durur. Ayrıca G' kümesindeki tüm g'_i, g'_j polinomları için $S(g'_i, g'_j) \xrightarrow{G'}_+ 0$ olduğundan Teorem 3.1.14'te ifade edilen Buchberger teoremi gereğince G' kümesi I idealinin bir Gröbner tabanı olur.

Şimdi Örnek 3.1.16'da verilen örneği yukarıdaki akış şemasına göre yeniden inceleyelim.

Örnek 3.1.18 $\mathbb{Q}[x, y]$ 'de $g_1 = x^3y - xy^2 + 1$ ve $g_2 = x^2y^2 - y^3 - 1$ polinomlarından oluşan $G = \{g_1, g_2\}$ kümesi ve $I = \langle g_1, g_2 \rangle$ ideali verilsin. $x \prec y$ olmak üzere sözlüksel sıralamaya göre, I idealinin bir Gröbner tabanını Buchberger algoritmasının bilgisayardaki akış şemasını kullanarak hesaplayalım.

Başlat: $G := \{g_1, g_2\}$, $\mathcal{G} := \{\{g_1, g_2\} \mid g_1 \neq g_2 \in G\}$.

1. Döngü: $\mathcal{G} \neq \emptyset$ ise herhangi $\{g_1, g_2\} \in \mathcal{G}$ seç.

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_2\}\}$ tanımla.

$S(g_1, g_2) = yg_1 - xg_2 = x + y$ belirle ve G 'ye göre indirge.

$$S(g_1, g_2) \xrightarrow{+}_G x + y \quad \text{ve } h = x + y \neq 0 \text{ ise,}$$

$g_3 := h$, $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid \text{her } u \in G \text{ için}\}$ ve $G := G \cup \{h\} = \{g_1, g_2, g_3\}$ tanımla.

2. Döngü: $\mathcal{G} \neq \emptyset$ ise herhangi $\{g_1, g_3\} \in \mathcal{G}$ seç.

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_3\}\}$ tanımla.

$S(g_1, g_3) = g_1 - x^2yg_2 = -x^2y^2 - xy^2 + 1$ belirle ve G 'ye göre indirge.

$$S(g_1, g_3) \xrightarrow{+}_G 0 \quad \text{ve } h = 0.$$

3. Döngü: $\mathcal{G} \neq \emptyset$ ise herhangi $\{g_2, g_3\} \in \mathcal{G}$ seç.

$\mathcal{G} := \mathcal{G} - \{\{g_2, g_3\}\}$ tanımla.

$S(g_2, g_3) = g_2 - xyg_3 = -xy^3 - y^3 - 1$ belirle ve G 'ye göre indirge.

$$S(g_2, g_3) \xrightarrow{+}_G -xy^3 - y^3 - 1 \quad \text{ve } h = -xy^3 - y^3 - 1 \neq 0 \text{ ise,}$$

$g_4 := h$, $\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid \text{her } u \in G \text{ için}\}$ ve $G := G \cup \{h\} = \{g_1, g_2, g_3, g_4\}$ tanımla.

4. Döngü: $\mathcal{G} \neq \emptyset$ ise herhangi $\{g_1, g_4\} \in \mathcal{G}$ seç.

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_4\}\}$ tanımla.

$S(g_1, g_4) = g_2 - xyg_3 = -xy^3 - y^3 - 1$ belirle ve G 'ye göre indirge.

$$S(g_1, g_4) \xrightarrow{+}_G 0 \quad \text{ve } h = 0.$$

$$S(g_2, g_4) \xrightarrow{+}_G 0 \quad \text{ve } h = 0.$$

$$S(g_3, g_4) \xrightarrow{+}_G 0 \quad \text{ve } h = 0.$$

Algoritma sonlanır ve $G = \{g_1, g_2, g_3, g_4\}$ kümesi I idealinin bir Gröbner tabanı olarak bulunur.

3.2. Minimal Gröbner Taban

Sonuç 3.1.6 gereğince, n değişkenli polinom halkasındaki her idealin bir Gröbner tabanının var olduğu ve önceki bölümde, Buchberger algoritması yardımıyla bir ide-

alin üreteç kümesi kullanılarak Gröbner tabanının nasıl hesaplandığı ifade edilmiştir. Buchberger algoritmasında yapılan iki seçime göre, farklı Gröbner tabanlar bulunabilir ve bulunan bu Gröbner tabanlarda farklı sayıda eleman olabilir. Bu seçimlerden biri sıralamadır. Polinomların bir üreteç kümesinde, sıralama değiştirildiğinde farklı polinomlardan oluşan Gröbner tabanlar bulunabilir. İkinci seçim, Buchberger algoritmasındaki her bir döngüde S -polinomları belirlenirken yapılan polinomların seçimidir. Bu döngülerde her bir adımda farklı polinom çiftleri seçilerek algoritma sonlandırılırsa, farklı Gröbner tabanlar yazılabilir. Bu bölümde, üreteç kümesindeki polinomlar üzerine bazı koşullar ekleyerek, minimal Gröbner taban olarak adlandırılan daha az elemanlı Gröbner tabanların nasıl elde edildiğini açıklayacağız.

Tanım 3.2.1 $G = \{g_1, g_2, \dots, g_s\}$ bir Gröbner taban olsun. Her i için $lc(g_i) = 1$ ve her $i \neq j$ için $lm(g_i)$; $lm(g_j)$ 'yi bölmez ise, G 'ye *minimal Gröbner taban* adı verilir.

Aşağıdaki lemmada, Buchberger algoritması yardımıyla bulunan bir Gröbner tabandan bazı elemanlar çıkarıldığında, kalan elemanların oluşturduğu kümenin Gröbner taban olmaya devam edeceği ifade edilmiştir.

Lemma 3.2.2 $G = \{g_1, g_2, \dots, g_s\}$ kümesi I ideali için Gröbner taban olsun. $lm(g_2)$; $lm(g_1)$ 'i bölerse $\{g_2, \dots, g_s\}$ kümesi de I ideali için bir Gröbner taban olur.

İspat $G = \{g_1, g_2, \dots, g_s\}$ kümesi I idealinin bir Gröbner tabanı olmak üzere $lm(g_1)$ 'in $lm(g_2)$ ile bölündüğünü kabul edelim. $lm(g_1)$ ile bölünebilen bir f polinomunun, bölünebilme bağıntısının geçişme özelliğinden, $lm(g_2)$ ile bölünebildiği açıktır. Böylece Tanım 3.1.1'den $\{g_2, \dots, g_s\}$ kümesi de I idealinin bir Gröbner tabanı olur.

Bir Gröbner tabandan minimal Gröbner tabanın nasıl elde edildiğini ifade eden, Lemma 3.2.2'nin bir direkt sonucu aşağıda verilmiştir.

Sonuç 3.2.3 $G = \{g_1, g_2, \dots, g_s\}$ kümesi I ideali için Gröbner taban olsun. G 'den bir minimal Gröbner taban elde etmek için, $j \neq i$ iken $lm(g_j)$ böler $lm(g_i)$ ve kalan her g_i için $lc(g_i)$ 'yi böler olacak şekildeki tüm g_i 'ler G kümesinden çıkarılır.

Minimal Gröbner taban tek değildir. Fakat bir I idealinin her minimal Gröbner tabanında aynı sayıda elemanın var olduğu aşağıdaki önermede ifade edilmiştir.

Önerme 3.2.4 $G = \{g_1, g_2, \dots, g_s\}$ ve $F = \{f_1, f_2, \dots, f_t\}$ bir I idealinin minimal Gröbner tabanları olsun. Bu durumda $s = t$ 'dir. Gerekirse yeniden numaralandırılarak $i = 1, 2, \dots, t$ için $lt(f_i) = lt(g_i)$ yapılır.

Örnek 3.2.5 $\mathbb{Q}[x, y]$ 'de $g_1 = y^2 + yx + x^2$, $g_2 = y + x$ ve $g_3 = y$ polinomlarından oluşan $G = \{g_1, g_2, g_3\}$ kümesi ve $I = \langle g_1, g_2, g_3 \rangle$ ideali verilsin. $x \prec y$ olmak üzere sözlüksel sıralamaya göre, I idealinin bir Gröbner tabanını ve bundan yararlanarak bir minimal Gröbner tabanını hesaplayalım. $S(g_1, g_2) \xrightarrow{+} x^2$ olup kalan sıfırdan farklı olduğu için $g_4 = x^2$ polinomu G kümesine eklenir. $G' = \{g_1, g_2, g_3, g_4\}$ olmak üzere $S(g_1, g_3) \xrightarrow{+} 0$ dir fakat $S(g_2, g_3) \xrightarrow{+} x$ olduğundan $g_5 = x$ alınarak, bu polinom G' kümesine eklenir. $G'' = \{g_1, g_2, g_3, g_4, g_5\}$ olmak üzere bu kümedeki tüm polinomların S -polinomlarının G'' 'ye göre sıfıra indirgendiği görülür. Bundan dolayı G'' kümesi I ideali için bir Gröbner taban olur.

Şimdi G'' Gröbner tabanını kullanarak I 'nın bir minimal Gröbner tabanını bulalım. $lm(g_1) = x^2$, $lm(g_2) = x$ ve $lm(g_4) = x^2$ olup bunlar $lm(g_5) = x$ tarafından bölünebildiği için g_1 , g_2 ve g_4 polinomları G'' kümesinden çıkarılır. Böylece G'' den daha az sayıda eleman bulunduran $G_1 = \{g_3, g_5\}$ kümesi I 'nın bir minimal Gröbner tabanı olur. Benzer şekilde $lm(g_2) = x$; $lm(g_1)$, $lm(g_4)$ ve $lm(g_5)$ 'i böldüğü için $G_2 = \{g_2, g_3\}$ kümesi I 'nın başka bir minimal Gröbner tabanıdır. Bu örnekte de görüldüğü gibi minimal Gröbner taban tek olmamasına rağmen, bulundurdıkları eleman sayısı bir tektir.

3.3. İndirgenmiş Gröbner Taban

Önceki bölümde minimal Gröbner tabanın tek olmadığı ifade edilmiştir. Bu bölümde, minimal Gröbner tabandaki polinomların üzerine daha güçlü koşullar eklenerek bir tek Gröbner tabanın elde edilebileceği gösterilmiştir.

Tanım 3.3.1 $G = \{g_1, g_2, \dots, g_s\}$ bir minimal Gröbner taban olsun. Her i için $lc(g_i) = 1$ ve g_i polinomu $G \setminus \{g_i\}$ 'ye göre indirgenmiş ise, yani; her i için g_i 'nin

sıfırdan farklı hiçbir terimi herhangi $j \neq i$ için $lm(g_j)$ ile bölünemiyorsa G 'ye *indirgenmiş* (*reduced*) *Gröbner taban* denir.

Aşağıdaki sonuç indirgenmiş bir Gröbner tabanın her zaman var olduğunu ifade eder.

Sonuç 3.3.2 $G = \{g_1, g_2, \dots, g_t\}$ bir I idealinin bir minimal Gröbner tabanı olsun. Aşağıdaki indirgeme yöntemi kullanılarak

$$\begin{aligned} g_1 &\xrightarrow{+H_1} h_1, h_1; H_1 = \{g_2, g_3, \dots, g_t\}'\text{ye göre indirgenmiştir} \\ g_2 &\xrightarrow{+H_2} h_2, h_2; H_2 = \{h_1, g_3, \dots, g_t\}'\text{ye göre indirgenmiştir} \\ g_3 &\xrightarrow{+H_3} h_3, h_3; H_3 = \{h_1, h_2, g_4, \dots, g_t\}'\text{ye göre indirgenmiştir} \\ &\vdots \\ g_t &\xrightarrow{+H_t} h_t, h_t; H_t = \{h_1, h_2, \dots, h_{t-1}\}'\text{ye göre indirgenmiştir} \end{aligned}$$

elde edilen $H = \{h_1, h_2, \dots, h_t\}$ kümesi I idealinin bir indirgenmiş Gröbner tabanıdır.

Buchberger tarafından ifade ve ispat edilen aşağıdaki teoremden bir tek indirgenmiş Gröbner tabanının var olduğu gösterilmiştir.

Teorem 3.3.3 (Buchberger Teoremi) Seçilen bir terim sıralamasına göre S 'deki sıfırdan farklı her I idealinin bir tek indirgenmiş Gröbner tabanı vardır.

Örnek 3.3.4 Örnek 3.2.5'teki I ideali için bulunan $G_1 = \{g_3, g_5\}$ minimal Gröbner tabanı, $g_3 = y$ ve $g_5 = x$ monik polinomlar olduğundan, aynı zamanda bir indirgenmiş Gröbner tabanıdır.

Örnek 3.3.5 $\mathbb{Z}_5[x, y]$ 'de $g_1 = x^2 + y^2 + 1$ ve $g_2 = x^2 + 2xy + x$ polinomlarından oluşan $G = \{g_1, g_2\}$ kümesi ve $I = \langle g_1, g_2 \rangle$ ideali verilsin. $x \prec y$ olmak üzere sözlüksel sıralamaya göre, I idealinin bir Gröbner tabanını ve indirgenmiş Gröbner tabanını hesaplayalım. $S(g_1, g_2) \xrightarrow{+G} 3xy + 4x + y^3 + y$ olup sıfırdan farklı bir kalan elde edildiği için $g_3 = 3xy + 4x + y^3 + y$ yeni bir polinom olarak G kümesine eklenir.

$G' = \{g_1, g_2, g_3\}$ diyelim. $S(g_1, g_3) \xrightarrow{+} 4y^5 + 3y^4 + y^2 + y + 3$ olup yine sıfırdan farklı bir kalan elde edildiği için $g_4 = 4y^5 + 3y^4 + y^2 + y + 3$ polinomu G' kümesine eklenir. Böylece oluşturulan $G'' = \{g_1, g_2, g_3, g_4\}$ kümesindeki tüm polinomların S -polinomlarının G'' kümesine göre indirgenmesinden elde edilen kalanların sıfır olduğu 6 adımda görülür. Sonuç olarak G'' kümesi I idealinin bir Gröbner tabanı olur. Şimdi G'' Gröbner tabanından yararlanarak I idealinin bir minimal Gröbner tabanını bulalım. $lm(g_1) = x^2, lm(g_2) = x^2, lm(g_3) = xy, lm(g_4) = y^5$ olup Sonuç 3.2.3 gereğince g_2 polinomu kümeden çıkarıldığında $H = \{g_1, g_3, g_4\}$ kümesi I ideali için bir minimal Gröbner tabanı olur. Buradaki polinomlar monik hale getirilerek I 'nın bir indirgenmiş Gröbner tabanı $H' = \{x^2 + y^2 + 1, xy + 3x + 2y^3 + 2y, y^5 + 2y^4 + 4y^2 + 4y + 2\}$ elde edilir.

Şimdi, tez çalışmada ayrı ayrı incelenen Gröbner taban karakterizasyonlarını, aşağıdaki teoremden bir arada ifade edelim.

Teorem 3.3.6 Sıfırdan farklı polinomların bir $G = \{g_1, g_2, \dots, g_t\}$ kümesi ve $I = \langle G \rangle$ ideali için aşağıdaki ifadeler birbirine denktir:

- (i) G kümesi I idealinin bir Gröbner tabanıdır.
- (ii) $Lt(G) = Lt(I)$ dır.
- (iii) $f \in I$ olması için gerek ve yeter koşul $f \xrightarrow{+} 0$ olmasıdır.
- (iv) Her $f \in S$ için $f \xrightarrow{+} r_1$ ve $f \xrightarrow{+} r_2$ olmak üzere r_1 ve r_2 G' ye göre indirgenmiş polinomlar ise, bu durumda $r_1 = r_2$ dir.
- (v) Her $i \neq j$ için $S(g_i, g_j) \xrightarrow{+} 0$ dır.
- (vi) Her $f \in I$ için $lm(f) = \max_{1 \leq i \leq t} (lm(h_i)lm(g_i))$ ve $f = h_1g_1 + \dots + h_tg_t$ olacak şekilde $h_1, h_2, \dots, h_t \in S$ vardır.
- (vii) Her $i \neq j$ ($0 \leq i, j \leq t$) için, $lm(S(g_i, g_j)) = \max_{1 \leq v \leq t} (lm(h_{ijv})lm(g_v))$ olmak üzere $S(g_i, g_j) = h_{ij1}g_1 + \dots + h_{ijt}g_t$ biçiminde yazılır.

4. GRÖBNER TABANIN BİLGİSAYARDAKİ UYGULAMALARI

Matematiği bir araç olarak kullanan tüm bilim dallarındaki hesap işlerini kolaylaştırmak için üretilen ve sembolik biçimdeki matematiksel ifadeleri kolayca işleme yaparak her türlü matematiksel işlemi yapabilen, 2 veya 3 boyutlu grafikler çizebilen programların genel adı *Bilgisayar Cebiri Sistemleri* dir. Bilgisayar Cebiri Sistemleri arasında en yaygın olanlar; Maple, Mathematica, Matlab, CoCoA ve Derive gibi programlardır. Bu programlar, temel özellikleri açısından birbirlerine benzer olup bu bölümde sadece Maple, Mathematica ve CoCoA'da Gröbner tabanın nasıl bulunduğu incelenecektir.

4.1. Maple'da Gröbner Taban

Bu bölümde, Maple programının kısaca nasıl kullanıldığı ve Gröbner tabanın bu programda nasıl hesaplandığı gösterilecektir. Abell ve Braseltan (2005), (İnt. Kyn. 3) ve (İnt. Kyn. 4) bu bölümde kullanılan temel kaynaklardır.

Maple, adını 1981'de bu programı geliştiren ve piyasaya süre Waterloo Maple'dan alan, bilgisayarda matematik yapmak için kullanılan bir sistemdir. Maple programı, matematiksel problemleri analiz etmeyi, keşfetmeyi, görselleştirmeyi ve çözmeyi son derece kolaylaştıran bir arayüzle birleştiren, bir matematik yazılımı olarak ifade edilebilir. Bu programla, matematik, cebir, diferansiyel denklemler, istatistik, kontrol tasarımı, doğrusal cebir, fizik, optimizasyon, grup teorisi, diferansiyel geometri, sinyal işleme, özel fonksiyonlar, sayı teorisi gibi matematiğe dayanan hemen hemen her alanda problemlerin çözülmesi ve finansal modelleme gibi birçok alanda çalışmalar yapılabilen ve, bu program matematik problemlerinin kolay, doğru ve hızlı bir çözümünün elde edilmesinde önemli rol oynar.

Şimdi bir bilgisayara kurulumu yapılan Maple programının işleyişi hakkında kısaca bilgi verelim.

- Maple'da oturumu başlatmak için:

Başlangıç Sayfasından ya da Dosya menüsünden; yeni belge veya yeni çalışma

sayfası seçilerek boş bir belge görüntülenir.

- Maple’da kod yazmak için:

Komut satırının başına [`>` ve satır sonuna `;` işareti eklenir. Maple’da yazılan kodların girdileri ekranda kırmızı renk, çıktıları ise mavi renk ile ifade edilir. Kurallara uygun olarak bir Maple kodu yazılıp *ENTER* tuşuna basıldığında komut satırının hemen altına çıktı yazılır. Eğer komut satırının sonuna `;` işareti yerine `:` işareti eklenirse hesaplama işlemi gerçekleştirilir fakat sonuç ekrana yazdırılmaz, hafızaya kaydedilir. Maple’da hesaplama işlemi gerçekleşmesine rağmen ekrana bir sonuç yazdırılmıyor ise denlemin çözüm kümesi boş küme anlamına gelir. Maple’da bulunan bir komutun yazım şeklini öğrenmek için *?komutadı* ifadesi kullanılır. Örneğin; limit hesaplama işleminin komutunu sorgulamak için *?limit* yazılır. Çok yönlü bir paket programı olan Maple’da bu paketler *with(paket adı)* komutu ile aktif hale getirilir.

- Maple’da Gröbner taban bulmak için:

- Maple da yeni bir çalışma sayfası oluşturulur,
- Çok değişkenli polinom halkası ve sıralama tanımlanır,
- İdealin üretici olan polinomlar tanımlanır,
- Tabanın hesaplanmasında Basis komutu kullanılır,
- GB; komutu ile hesaplanan taban ekrana yazdırılır

adımları uygulanarak hesaplama işlemi tamamlanır. Polinom halkalarına göre kod parçaları düzenlenerek, hesaplaması zor olan, Gröbner taban hızlı ve kolay bir şekilde bulunmuş olur.

Örnek 4.1.1 Maple programında; iki değişkenli bir polinom halkasında, üreticiler aşağıda girdi olarak verilen iki üreteçli bir I idealinin, sözlüksel sıralamaya göre, Gröbner tabanı şu şekilde bulunur:

`with(Groebner):`

`R := PolynomialRing([x,y], 'lex');`

`I := Ideal( $x^3 - y^2$ ,  $xy - 1$ );`

GB:= Basis(I, 'lex'):

GB;

komutları girildiğinde, ekrana

$$GB := [xy - 1, x^3 - y^2, y^3 - x^2]$$

yazdırılır. Böylece, iki değişkenli bir polinomlar halkasında, sözlüksel sıralamaya göre, bir $I = \langle x^3 - y^2, xy - 1 \rangle$ idealinin Gröbner tabanı $G = \{xy - 1, x^3 - y^2, y^3 - x^2\}$ olarak bulunur.

4.2. Mathematica'da Gröbner Taban

Bu bölümde, Mathematica programının nasıl kullanıldığı kısaca ifade edilerek Gröbner tabanın bu programda nasıl hesaplandığı gösterilecektir. Wolfram (2003), (İnt. Kyn. 5), (İnt. Kyn. 6) ve (İnt. Kyn. 7) bu bölümde kullanılan temel kaynaklardır.

Mathematica; Stephen Wolfram tarafından Wolfram programlama dili kullanılarak tasarlanan ve 1988'de Wolfram Araştırma Şirketi tarafından geliştirilen bir programdır. Mathematica; makine öğrenimi, istatistik, sembolik hesaplama, veri manipülasyonu, ağ analizi, zaman serisi analizi, NLP, optimizasyon, çizim işlevleri ve çeşitli veri türleri, algoritmaların uygulanması, kullanıcı arayüzlerinin oluşturulması ve diğer programlama dillerinde yazılmış programlarla arayüz oluşturmaya izin veren çeşitli teknik bilgi işlem alanları için yerleşik kitaplıklara sahip, bir yazılım sistemidir. Şimdi bir bilgisayara kurulumu yapılan Mathematica programının işleyişi hakkında kısaca bilgi verelim.

- Mathematica'da oturumu başlatmak için;
Eğer bilgisayar tamamen grafiksel bir arayüz olarak kullanılıyorsa Mathematica simgesine çift tıklanır, metin tabanlı bir işletim sistemi üzerinde kullanılıyorsa ise *mathematica* komutu yazılır.
- Mathematica çalıştırıldığında açılan ekran boş bir defter şeklindedir. Hesaplanmak istenen komut bu ekrana girilir ve komutun çalışması için *Shift+Enter* tuşlarına basılır. Mathematica'da veri girişi için $In[n]:=$ komutu kullanılır ve

Shift+Enter tuşlarına basıldığında ekranda $Out[n]=$ ifadesi yer alır. Örneğin;

$$In[1] := 2 + 2$$

$$Out[1] = 4$$

- Mathematica’da hesaplamalar yapılırken genellikle önceki sonuçlar kullanılır, bunun için komut satırında % sembolü yazılarak en son hesaplanan değer çağrılır.

(); matematiksel işlemleri gruplandırmak;

[]; fonsiyonların değışkenlerini ve komutları ifade etmek;

{ }; aralıkları ve sayaçları tanımlamak ve liste işlemlerini ifade etmek için kullanılır. Mathematica’yı diğer programlardan farklı kılan; komut satırının okunması için ; sembolünün kullanılmamasıdır. Eğer komut satırının sonuna ; eklenirse program o satırın sonucunu hesaplamaz.

- Mathematica’da Gröbner taban bulmak için;
 - Mathematica programı başlatılır,
 - İdealin üreteçleri olan polinomlar ekrana girilir,
 - Gröbner taban hesaplatmak için GroebnerBasis komutu kullanılır.

Maple programından farklı olarak, elde edilen tabanın bir değışkene atanmasına gerek yoktur, komut satırı yazıldıktan sonra *Shift+Enter* tuşlarına basıldığında sonuç ekrana direkt olarak yazdırılır. Mathematica programında bu adımlar takip edilerek, iki farklı sıralamaya göre, Gröbner tabanın nasıl bulunduğu aşağıdaki örnekte gösterilmiştir.

Örnek 4.2.1 Mathematica programında; üç değışkenli bir polinom halkasında, üreteçleri aşağıda girdi olarak verilen bir I idealinin,

- Sözlüksel sıralamaya göre, Gröbner tabanı:

$$In[1] := polys = \{x^2 + y^2 + z^2 - 1, x - z + 2, z^2 - xy\}$$

$$In[2] := GroebnerBasis[polys, \{x, y, z\}, MonomialOrder \rightarrow Lex]$$

(*Shift+Enter*)

$$Out[3] = \{12 - 28z + 27z^2 - 12z^3 + 3z^4, -6 + 4y + 11z - 6z^2 + 3z^3, 2 + x - z\}$$

- Derece ters sözlüksel sıralamaya göre, Gröbner tabanı:

In[1] := polys = $\{x^2 + y^2 + z^2 - 1, x - z + 2, z^2 - xy\}$

In[2] := GroebnerBasis[polys, $\{x, y, z\}$, MonomialOrder $\rightarrow$ DegRevLex]

(Shift+Enter)

Out[3] = $\{2 + x - z, -2y + yz - z^2, 3 + y^2 - 4z + 2z^2, -6 + 4y + 11z - 6z^2 + 3z^3\}$

biçiminde elde edilir.

4.3. CoCoA'da Gröbner Taban

CoCoA, *Hesaplamalı Değişmeli Cebir* (*Computational Commutative Algebra*) ifadesinin kısaltılmışı olan bir bilgisayar cebir sistemidir. CoCoA programının CoCoA4 sürümü kullanılarak, bu bölümdeki bilgiler verilmiştir. Kreuzer ve Robbiano (2000) ve (İnt. Kyn. 1) bu bölümde kullanılan temel kaynaklardır.

CoCoA, değişmeli cebirde bazı hesaplamalar yapmak için, İtalya'nın Genova Üniversitesi'nde Bilgisayar Cebiri alanında aktif bir araştırma ekibinin projelerinden biri olarak ortaya çıkmıştır. Bu ekibin üyelerinden bazıları: Lorenzo Robbiano (ekip yöneticisi), John Abbott, Anna Bigatti, Massimo Caboara, Martin Kreuzer, David Perkinson, Michael Abshoff, Karsten Hiddeman'dır.

C dilinde yazılmış bir programlama dili olan CoCoA; polinom halkaları üzerindeki idealler ve modüller için Gröbner taban hesaplamaya yarayan Buchberger algoritmasının bilgisayardaki uygulama alanlarından biridir. CoCoA'nın Gröbner tabanı motoru; Gröbner tabanlarını, syzygy'leri, serbest çözücüleri, Hilbert fonksiyonlarını ve minimum üreteç kümelerini hesaplamak için kullanılır.

Örnek 4.3.1 CoCoA programında; iki değişkenli bir polinom halkasında, üreteçleri aşağıda girdi olarak verilen iki üreteçli bir I idealinin, sözlüksel sıralamaya göre, Gröbner tabanı şu şekilde bulunur:

Use $R ::= \mathbb{Q}[x, y, z]$, Lex;

$I := \text{Ideal}(x^3 - y, x^4 - z)$;

Describe I ;

Record[Type = IDEAL, Value = Record[Gens = $[x^3 - y, x^4 - z]$]]

GBasis(I);

$[x^3 - y, -xy + z, x^2z - y^2, y^3 - xz^2]$

Örnek 4.3.2 Dört değişkenli bir polinom halkasında, sözlüksel sıralamaya göre, üreteçleri aşağıdaki gibi verilen bir I idealinin Gröbner tabanı ve indirgenmiş Gröbner tabanı:

Use $R ::= \mathbb{Q}[t, x, y, z]$;

$I := \text{Ideal}(t^3 - x, t^4 - y, t^5 - z)$;

$gb.\text{Start}_G\text{Basis}(I)$; (*Gröbner taban hesaplamayı başlatır*)

$gb.\text{Step}(I)$; (*Gröbner taban hesaplamada bir adım sonrasını verir*)

$I.\text{GBasis}$; (*Buraya kadarki Gröbner taban elemanlarını verir*)

$[t^3 - x]$

$gb.\text{Complete}(I)$; (*Hesaplamayı tamamlar*)

$I.\text{GBasis}$;

$[t^3 - x, -tx + y, -ty + z, -y^2 + xz, -x^2 + tz, t^2z - xy]$

$\text{ReducedGBasis}(I)$; (*İndirgenmiş Gröbner tabanı hesaplatır*)

$[t^3 - x, tx - y, ty - z, y^2 - xz, x^2 - tz, t^2z - xy]$

ile bulunur.

4.4. Çizge Boyama

Çizge (graph) kavramı ilk olarak Leonhard Euler'in (1707-1783) Königsberg'in 7 Köprüsü probleminin çözümü ile ortaya çıkmıştır. *Çizge (graph)*; birbirine *kenarlar (edge)* yardımıyla bağlı *köşelerin (vertex)* oluşturduğu matematiksel bir yapı olarak ifade edilebilir. Çizge teorisi ise, bir problemin kenarlar ve köşeler aracılığıyla modellemesine dayanmaktadır. Günlük hayatta karşılaşılan problemlerin incelenmesi ve analizi için önemli bir araçtır. Bilgisayar bilimi, mühendislik, iletişim ağları, sosyal ağ analizi, lojistik, planlama ve ulaşım da rota belirleme gibi birçok çalışma alanında önemli rol oynar. Seker (2015), Wilson (1996), (İnt. Kyn. 2), Gross vd. (2014) ve Rosen vd. (2000) bu bölümde kullanılan temel kaynaklardır. Şimdi matematiksel olarak çizge kavramının tanımını verelim.

Tanım 4.4.1 Köşelerin bir V kümesi ile, kenarların bir E kümesinin oluşturduğu $\Gamma = (V, E)$ sistemi bir *çizge* (*graph*) olarak adlandırılır.

Köşeleri birbirine bağlayan kenarlara yön verilmiş, yani her bir kenarın bir başlangıç ve bitiş köşesi belirlenmiş ise, bu çizgeye *yönlendirilmiş çizge* (*directed graph*), aksi durumda *yönlendirilmemiş çizge* (*undirected graph*) adı verilir.

Tanım 4.4.2 *Çizge boyama* (*graph coloring*), belirli kurallar çerçevesinde bir çizgenin köşelerine veya kenarlarına farklı renklerin atanması esasına dayanan bir algoritma olarak ifade edilir. Buradaki amaç en az sayıda renk kullanarak komşu köşe veya kenarların farklı renklerle boyanmasıdır.

Çizge boyama problemleri;

- Harita Boyama: Bir haritadaki bölgelerin, komşu bölgelerle farklı renklere boyanması,
- Sınav/Ders Programlama: Sınav veya ders programlarında çakışmaları önlemek amacıyla,
- Frekans Atama: Kablosuz iletişim araçlarında, frekansların birbiriyle çakışmasını önlemek amacıyla baz istasyonlarına renk atamalarının yapılması,
- Sudoku: Sudoku bulmacaları, 9×9 bir kare üzerindeki rakamların belirli kurallara göre renklendirilmesi

gibi farklı alanlarda kullanılmaktadır.

Uyarı 4.4.3 Çizge boyama problemlerinin çözümünde Gröbner taban kavramı doğrudan kullanılmaz. Öncelikle Gröbner taban ile çizgeler arasında ilişki kurmak için, çizgenin köşelerini oluşturan özel polinomlar tanımlanır. 3-Renk Problemi olarak adlandırılan problem; komşu iki köşe aynı renk olmayacak şekilde, bir çizgenin üç renk kullanılarak boyanması esasına dayanır.

Çizge boyama probleminin çözümünde Gröbner taban kavramından yararlanmak için, bir polinom halkasına ihtiyaç duyulmaktadır. Bunun için; üç elemanlı $F_3 = \mathbb{Z}/(3)$ cismi üzerine kurulan, katsayıları mod3'e göre tamsayılar olan, n değişkenli

polinomların $F_3[x_1, x_2, \dots, x_n]$ halkasını gözönüne alalım. Burada $n \geq 2$ doğal sayısı $\Gamma = (V, E)$ çizgesindeki köşe sayısını ve her $1 \leq i \leq n$ için x_i bilinmeyenleri v_i köşelerini göstermektedir. Keyfi olarak seçilen üç rengi göstermek için $\{-1, 0, 1\}$ kümesi kullanılacaktır. Aşağıda verilen teoreme dayanarak her bir $v_i \in V$ köşesinin olası tüm renklendirmeleri belirlenebilir.

Teorem 4.4.4 $I = \langle x_1^3 - x_1, x_2^3 - x_2, \dots, x_n^3 - x_n \rangle \in F_3[x_1, x_2, \dots, x_n]$ idealinin sıfırları, her bir $v_i \in V$ köşesine $\{-1, 0, 1\}$ renklerinden herhangi birini karşılık getirir.

Böylece, Γ 'nın köşelerinin tüm olası renklerini ifade etmek için kullanılacak olan polinomları üreteç olarak kabul eden bir I ideali tanımlanmış olur. Aşağıdaki teoremden, komşu iki köşenin aynı rengi paylaşmasını önlemek için bu polinomlar üzerinde bir koşul verilmiştir.

Teorem 4.4.5 Her $v_i, v_j \in V$ için v_i ve v_j köşelerinin aynı rengi paylaşmaması için gerek ve yeter koşul *komşuluk polinomu* (*adjacency polynomial*) olarak adlandırılan $f(x_i, x_j) = x_i^2 + x_i x_j + x_j^2 - 1$ polinomunun sıfırı olmasıdır.

Renklendirme ideali (*coloring ideal*) olarak adlandırılan

$$I_c = \langle x_i^2 + x_i x_j + x_j^2 - 1 \mid e_{ij} \in E(\Gamma) \rangle$$

ile tanımlı I_c idealinin bir Gröbner tabanı yardımıyla olası tüm renklendirmeler yapılır. Bunun için Γ çizgesinin iki komşu köşesi sabitlenir. Böylece sabitlenmiş iki köşe sayesinde bir veya daha fazla renklendirmeyi hesaplamak çok daha basit hale gelir. Örneğin herhangi bir Γ çizgesinin komşu x_1, x_2 köşelerini sabitleyerek $x_1 = 0$ ve $x_2 = 1$ şeklinde renklendirelim. Böylece I idealinin iki üreteç polinomu $g_1 = x_1$ ve $g_2 = x_2 - 1$ belirlenmiş olur. Çünkü bu polinomların sıfırları istenilen renklendirmelere karşılık gelir. Buradan

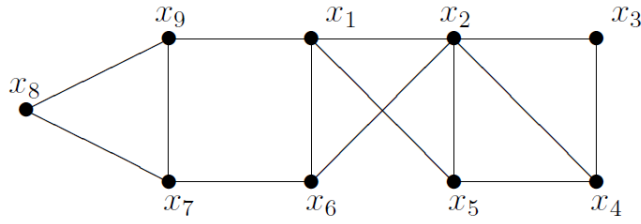
$$I_c = \langle x_1, x_2 - 1, x_i^2 + x_i x_j + x_j^2 - 1 \mid e_{ij} \in E(\Gamma) \rangle$$

idealinin Gröbner tabanı hesaplanarak $x_1 = 0$ ve $x_2 = 1$ olmak üzere Γ 'nın her olası renklendirmesi elde edilmiş olur. Bu idealin Gröbner tabanının 1 'i içermesi durumunda, hiçbir olası 3-renklendirmenin mevcut olmadığı aşağıdaki teoremden ifade edilmiştir.

Teorem 4.4.6 $I_c = \langle x_1, x_2 - 1, x_i^2 + x_i x_j + x_j^2 - 1 | e_{ij} \in E(\Gamma) \rangle$ renklendirme idealine sahip bir Γ çizgesi verilsin. I_c 'nin Gröbner tabanı 1'i içeriyorsa, Γ 'nın hiçbir olası 3-renklendirmesi yoktur.

Şimdi aşağıdaki örnekte bir çizgenin 3-renklendirme probleminin Gröbner taban yardımıyla nasıl çözüldüğünü açıklayalım.

Örnek 4.4.7 9 köşeye ve 13 kenara sahip Γ çizgesi aşağıdaki gibi verilsin.



Şekil 4.1 Çizge Boyama Örneği

Bu çizgedeki köşeleri, komşu köşeler aynı renk olmayacak şekilde üç renk ile boyayalım. Bunun için; bitişik köşeler sabitlenerek, $x_1 = 0$ ve $x_2 = 1$ olarak alınır ve sözlüksel sıralama kullanılarak aşağıdaki komşuluk polinomları belirlenir:

$$\begin{aligned} & x_1^2 + x_1 x_2 + x_2^2 - 1, x_1^2 + x_1 x_6 + x_6^2 - 1, x_1^2 + x_1 x_9 + x_9^2 - 1, \\ & x_1^2 + x_1 x_5 + x_5^2 - 1, x_2^2 + x_3 x_3 + x_3^2 - 1, x_2^2 + x_2 x_4 + x_4^2 - 1, \\ & x_2^2 + x_2 x_5 + x_5^2 - 1, x_2^2 + x_2 x_6 + x_6^2 - 1, x_3^2 + x_3 x_4 + x_4^2 - 1, \\ & x_4^2 + x_4 x_5 + x_5^2 - 1, x_6^2 + x_6 x_7 + x_7^2 - 1, x_7^2 + x_7 x_8 + x_8^2 - 1, \\ & x_7^2 + x_7 x_9 + x_9^2 - 1, x_8^2 + x_8 x_9 + x_9^2 - 1, x_1, x_2 - 1 \end{aligned}$$

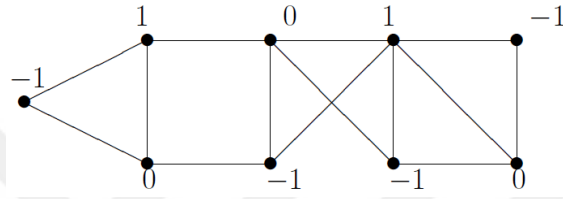
Şimdi bu polinomları üreteç olarak kabul eden $I \subset F_3[x_1, x_2, \dots, x_9]$ idealinin Gröbner tabanını hesaplayalım. Özellikle

$$\begin{aligned} G(I) = & \langle x_1, x_2 - 1, -x_3 - 1, x_4, x_5 + 1, x_6 + 1, -x_7 - x_8 - x_9, \\ & x_8^2 + x_8 x_9 + x_9^2 - 1, -x_8 x_9 - x_8 - x_9 - 1, -x_9^2 + 1 \rangle \end{aligned}$$

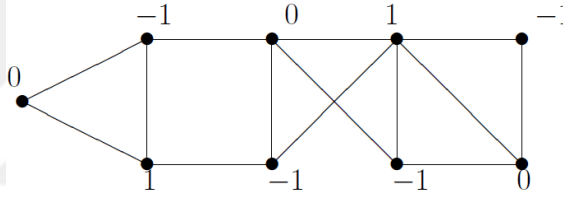
ideali için $1 \notin G(I)$ olduğundan Γ 'nın 3-renklendirilebilir olduğu açıktır. Gröbner tabandaki her polinomun sıfırlarının bulunması sabitlenen x_1 ve x_2 için tüm olası renklendirmeleri verecektir. Bu ise $x_1 = 0, x_2 = 1, x_3 = -1, x_4 = 0, x_5 = -1, x_6 = -1$

ve $x_9 = -1$ veya x_7, x_8, x_9 'un değerine bağlı olarak $x_9 = 1$ olmasını gerektirecektir. Γ çizgesinin 3-renklendirmesi için olası her bir durum aşağıdaki diyagramlarda gösterilmiştir.

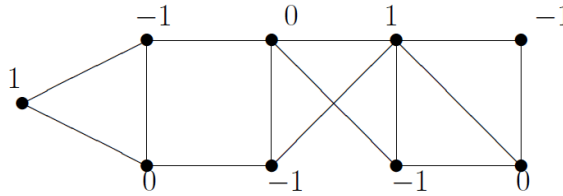
- $x_9 = 1$ iken $x_7 = 0$ ve $x_8 = -1$ alınırsa, Şekil 4.2 elde edilir:
- $x_9 = -1$ iken $x_7 = 1$ ve $x_8 = 0$ alınırsa, Şekil 4.3 elde edilir:
- $x_9 = -1$ iken $x_7 = 0$ ile $x_8 = 1$ alınırsa, Şekil 4.4 elde edilir:



Şekil 4.2 Çizge Boyama Örneği 1



Şekil 4.3 Çizge Boyama Örneği 2



Şekil 4.4 Çizge Boyama Örneği 3

5. KAYNAKLAR

- Abell M L, Braseltan J B, 2005, Maple by Example, Elsevier Academic Press, 563p, Amsterdam.
- Adams W W, Loustau P, 1994, An Intraduction to Gröbner Bases, American Mathematical Society, 303p, Providence Rhode Island.
- Buchberger B, Winkler F, 1998, Gröbner Bases and Applications, Cambridge University Press , 562p, New York.
- Buchberger B, 1965, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes Nach Einem Nulldimensionalen Polynomideal, PhD Thesis, 58p , Innsbruck.
- Cox D Little J O'shea D, 1992, Ideals Varieties and Algorithms, Springer-Verlag.
- Dummit D S, Foote R M, 2004, Maple by Example, Abstract Algebra, John Wiley and Sons Inc, 946p, Danvers.
- Ene V, Herzog J, 2012, Gröbner Bases in Commutative Algebra, American Mathematical Society, 178p, Providence Rhode Island.
- Gross J L, Yellen J, Zhang P, 2014, Handbook Of Graph Theory(Second Edittion), CRC Press ,1630p, New York.
- Hungerford T W, 1974, Algebra, Springer-Verlog, 526p, New York.
- Kreuzer M, Robbiano L, 2000, Computational Commutative Algebra 1, Springer-Verlog, 327p, Berlin Heidelberg New York.
- Malik D S, Mordeson J M, Sen M K , 1997, Fundamentals of Abstract Algebra, The McGraw-Hill Componies Inc, 657p, New York.
- Rosen K H, Michaels J G, Gross J L, Grossman J W, Shier D R, 2000,

Handbook Of Discrete and Combinatorial Mathematics, CRC Press ,1183p,
Boca Raton.

Seker S E, 2015, Çizge Teorisi(Graph Theory), YBS Ansiklopedi 2, 17-29, İstanbul.

Wilson R J, 1996, Introduction to Graph Theory, Longman Group 180p, New York.

Wolfram S, 2003, The Mathematica Book, Wolfram Research Inc, 1301p, Cham-
paign.

İnternet Kaynakları

- 1- <https://cocoa.dima.unige.it/cocoa/download/doc/help.pdf>, 21.06.2023
- 2- [https://www.lakeheadu.ca/sites/default/files/uploads/77/docs/
GallingerFinalr.pdf](https://www.lakeheadu.ca/sites/default/files/uploads/77/docs/GallingerFinalr.pdf), 21.06.2023
- 3- <https://www.maplesoft.com/products/maple/>, 21.06.2023
- 4- <https://www.maplesoft.com/support/help/maple/view.aspx?path=Groebner>,
21.06.2023
- 5- <https://reference.wolfram.com/language/ref/GroebnerBasis.html>, 21.06.2023
- 6- <https://www.wolfram.com/mathematica/>, 21.06.2023
- 7- <https://en.wikipedia.org/wiki/WolframMathematica>, 21.07.2023