T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yusuf ÖZENİR

TRAKYA ÜNİVERSİTESİ
FEN FAKÜLTESİ
MATEMATİK BÖLÜMÜ

YÜKSEK LİSANS TEZİ
CEBİR VE SAYILAR TEORİSİ
ANABİLİM DALI

2011
EDİRNE

T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GRÖBNER TABANLARI

Yusuf ÖZENİR

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Tez Yöneticisi : Yrd. Doç. Dr. Figen ÖKE

2011
EDİRNE

T.C
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GRÖBNER TABANLARI

Yusuf ÖZENİR

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Bu Tez **24 / 08 / 2011** Tarihinde Aşağıdaki Jüri Tarafından Kabul Edilmiştir.

Prof. Dr. Hülya İŞCAN

Üye

Doç. Dr. Şaban AKTAŞ

Üye

Yrd. Doç. Dr. Figen ÖKE

Danışman

ÖZET

"Gröbner Tabanları" olarak adlandırılan bu çalışmada izlenen plan aşağıdaki biçimdedir.

I. Bölümde çok değişkenli polinomlar ile ilgili genel bilgiler verilmiştir.

II. Bölümde terim sıralamaları ve indirgemeler çalışılmıştır.

III. Bölümde Gröbner tabanının genel tanımı verilerek, S-Polinomları ve Buchberger Algoritması incelenmiştir.

IV. Bölümde katsayıları cisim dışındaki farklı cebirsel yapılarda olan polinom halkalarında Gröbner tabanları çalışılmıştır.

SUMMARY

The plan followed in this work which is entitled as "Gröbner Basis" may be as below.

In Chapter I pertinent background are given.

In Chapter II term orders and reductions are studied.

In Chapter III general definition of Gröbner base is given, S-Polynomials and Buchberger Algorithm are investigated.

In Chapter IV Gröbner bases in polynomial rings which have not coefficent in a field are studied.

ÖNSÖZ

Çalışmalarımın her aşamasında her türlü yardım ve destekte bulunup matematiksel bakış açısını, bilgisini ve deneyimini benimle paylaşan değerli hocam Yrd. Doç. Dr. Figen ÖKE 'ye en içten teşekkürlerimi sunarım.

Çalışmam boyunca her türlü yardımlarından ve telkinlerinden dolayı değerli hocam Prof. Dr. Hülya İŞCAN 'a en içten teşekkürlerimi sunarım.

Ayrıca tez çalışmam boyunca maddi ve manevi desteklerini esirgemeyen sevgili aileme ve nişanlım Sevsen'e en içten teşekkürlerimi sunarım.

Yusuf ÖZENİR

GÖSTERİMLER

$lp(f)$: f polinomunun en büyük kuvvet çarpımı

$lc(f)$: f polinomunun baş katsayısı

$lt(f)$: f polinomunun baş terimi

$<_{lex}$: Lexicographical sıralama

$<_{\deg lex}$: Degree Lexicographical sıralama

$<_{\deg revlex}$: Degree Reverse Lexicographical sıralama

lcm : En küçük ortak kat

gcd : En büyük ortak bölen

$mdeg(f)$: f polinomunun multiderecesi

İÇİNDEKİLER

ÖZET.....i
SUMMARY.....ii
ÖNSÖZ.....iii
GÖSTERİMLER.....iv
GİRİŞ.....1

I. BÖLÜM / ÖN BİLGİLER.....3

1.1 Çok Değişkenli Polinomlar.....3

1.2 Çok Değişkenli Doğrusal Polinomlar İçin İndirgeme.....12

1.3 Tek Değişkenli Polinomlar İçin İndirgeme.....15

II. BÖLÜM / TERİM SIRALAMALARI VE İNDİRGEMELER.....23

2.1 Terim Sıralamaları.....23

2.2 Polinomların İndirgenmesi ve Bölme Algoritması.....27

III. BÖLÜM / GRÖBNER TABANLARI.....34

3.1 Genel Tanımı.....34

3.2 S-Polinomları ve Buchberger Algoritması.....42

3.3 İndirgenmiş Gröbner Tabanları.....57

IV. BÖLÜM / ESAS İDEAL BÖLGESİ ÜZERİNDE GRÖBNER TABANLARI VE DİNAMİK GRÖBNER TABANLARI.....66

4.1 Değerlendirme Bölgesi Üzerinde Gröbner Tabanı.....66

4.2 Esas İdeal Bölgesi Üzerinde İdeale Ait Olma Problemi.....73

4.3 Esas İdeal Bölgesi Üzerinde Gröbner Tabanı.....75

4.4 Dinamik Gröbner Tabanı.....78

4.5 Esas İdeal Bölgesi Üzerinde Dinamik Gröbner Tabanı.....80

4.6 Buchberger Algoritmasının Dinamik Versiyonu.....83

KAYNAKLAR.....89

ÖZGEÇMİŞ.....90

GİRİŞ

Gröbner tabanı kavramı 1965 yılında Bruno BUCHBERGER tarafından ortaya atılmıştır. k bir cisim olmak üzere $k[x_1, x_2, ..., x_n]$ polinom halkasında bir I ideali için tanımlanan Gröbner tabanı, idealin üreteç kümesini daha basit hale getirerek, ideale ait olma probleminin çözülmesini de kolaylaştırmıştır. $k[x_1, x_2, ..., x_n]$ halkasının bir I idealinin Gröbner tabanını elde edebilmek için $k[x_1, x_2, ..., x_n]$ üzerinde bir terim sıralamasına ve bir bölme algoritmasına ihtiyaç vardır. Terim sıralaması yardımıyla indirgeme işlemi tanımlanmış, çok değişkenli polinom halkalarında bölme algoritması oluşturulmuştur. I , $k[x_1, x_2, ..., x_n]$ halkasının bir ideali ve $G = \{g_1, g_2, ..., g_t\}$ sıfırdan farklı polinomların bir kümesi olmak üzere $G \subseteq I$ olsun. $f \neq 0$ sağlayan her $f \in I$ için $lp(g_i)$, $lp(f)$ yi bölecek şekilde $i \in \{1, 2, ..., t\}$ varsa G kümesine I ideali için bir Gröbner tabanı denir. $k[x_1, x_2, ..., x_n]$ halkasında sıfırdan farklı her idealin bir Gröbner tabanına sahip olduğu kanıtlanmıştır. Gröbner tabanı tanımı yardımıyla bir çok teorem elde edilmişse de bu teoremler sadece bir kümenin bir idealin Gröbner tabanı olup olmadığını incelemek için kullanılmış, fakat bu teoremler bir ideal için Gröbner tabanı elde etmek için yeterli olmamıştır.

Amacı, bir cisim üzerindeki bir polinom halkasında herhangi bir ideal için bir Gröbner tabanı oluşturmak olan Bruno BUCHBERGER S-Polinomu kavramını tanımlamış ve Gröbner tabanı elde edebilmek için kendi adıyla anılan Buchberger Algoritmasını oluşturmuştur. S-Polinomu, iki polinom kullanılarak bulunan yeni bir polinomdur. Algoritmaya göre bir ideale Gröbner tabanı bulmak için önce bu idealin üreteç kümesi alınır. Daha sonra bu üreteç kümesi içindeki polinomların ikişer ikişer S-Polinomları bulunur ve bulunan bütün S-Polinomları üreteç kümesine göre indirgenir. Sıfıra indirgenemeyen S-Polinomları üreteç kümesine eklenerek istenilen Gröbner tabanı elde edilmiş olur. Bu işlem sonunda bulunan küme içinde birbiri cinsinden yazılabilen polinomlar kümeden atılarak, minimal ve ardından indirgenmiş Gröbner tabanı elde edilmiş olur. İndirgenmiş Gröbner tabanının tek olduğu da kanıtlanmıştır. Bu sayede oluşturulan indirgenmiş Gröbner tabanı verilen ideal için bulunabilecek en uygun üreteç kümesi olarak elde edilmiş olur.

İlk olarak bir cisim üzerindeki polinom halkalarında çalışılan Gröbner tabanı, daha sonra katsayıları esas ideal bölgelerinde, değerlendirme bölgelerinde olan polinom halkalarında çalışılmıştır. Bu yüzden bu çalışmanın III. Bölümünde k bir cisim olmak üzere $k[x_1, x_2, ..., x_n]$ polinom halkasındaki bir ideal için Gröbner tabanları çalışılmıştır. IV. Bölümde de katsayıları bir esas ideal bölgesinde seçilen polinom halkalarında ve ardından katsayıları bir değerlendirme halkasında seçilen polinom halkalarında Gröbner tabanları çalışılmıştır.

I . BÖLÜM

ÖN BİLGİLER

.

1.1. Çok Değişkenli Polinomlar

k bir cisim ve $k[x_1, x_2, ..., x_n]$ k cismi üzerindeki n değişkenli polinom halkası olsun.

Tanım1.1.1: $x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot ... \cdot x_n^{\beta_n}$ ifadesine **kuvvet çarpımı** denir.

k bir cisim olsun. $f(x_1, x_2, ..., x_n) \in k[x_1, x_2, ..., x_n]$ polinomları $i = 1, 2, ..., n$ için $\beta_i \in \mathbb{N}$ ve $a \in k$ olmak üzere $a \cdot x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot ... \cdot x_n^{\beta_n}$ terimlerinin sonlu toplamıdır.

Örneğin; $f = x_1^2 + x_2^2 - 1$ ve $g = x_1 - 3x_2^2 + \frac{1}{2} x_1 x_3$ üç değişkenli polinomlardır.

$k[x_1, x_2, ..., x_n]$ ile katsayıları k cisminde olan n değişkenli polinomların kümesi gösterilsin. $k[x_1, x_2, ..., x_n]$, polinomların toplamı ve çarpımı işlemlerine göre değişmeli bir halkadır.

Bütün kuvvet çarpımlarının kümesi $T^n = \left\{ x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot ... \cdot x_n^{\beta_n} \mid \beta_i \in \mathbb{N},\ i = 1, 2, ..., n \right\}$ olmak üzere $k[x_1, x_2, ..., x_n]$ halkası tabanı T^n olan bir $k-$vektör uzayıdır.

$n \in \mathbb{Z}^+$ için $k^n = \left\{ (a_1, a_2, ..., a_n) \mid a_i \in k,\ i = 1, 2, ..., n \right\}$ şeklindedir.

Örneğin; $k = \mathbb{R}$ ise $k^n = \mathbb{R}^n$ dir.

Tanım1.1.2: $f \in k[x_1, x_2, ..., x_n]$ polinomu ile

$$\begin{aligned} \psi : k^n &\longrightarrow k \\ (a_1, a_2, ..., a_n) &\mapsto \psi(a_1, a_2, ..., a_n) = f(a_1, a_2, ..., a_n) \end{aligned}$$

biçiminde bir fonksiyon tanımlanır. Bu fonksiyona **değer fonksiyonu** denir.

Tanım1.1.3: $f \in k[x_1, x_2, ..., x_n]$ için $f = 0$ denkleminin çözümlerinin kümesi $V(f) = \{ (a_1, a_2, ..., a_n) \in k^n \mid f(a_1, a_2, ..., a_n) = 0 \} \subseteq k^n$ şeklindedir. $V(f)$ kümesine f tarafından tanımlanan **variety** denir.

Örneğin; $V(x^2 + y^2 - 1) = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \} \subseteq \mathbb{R}^2$ olup, $xy-$koordinat sisteminde $(0,0)$ merkezli ve $r = 1$ yarıçaplı bir çember belirtir.

Tanım1.1.4: f_1 , f_2 ,..., $f_s \in k[x_1, x_2, ..., x_n]$ polinomları verilsin.

$$f_1 = 0 , \ f_2 = 0 \ , ..., \ f_s = 0 \qquad (1.1.1)$$

sisteminin bütün çözümleri $V(f_1, f_2, ..., f_s)$ **variety kümesi** olarak tanımlanır ve $V(f_1, f_2, ..., f_s) = \{ (a_1, a_2, ..., a_n) \in k^n \mid f_i(a_1, a_2, ..., a_n) = 0 , i = 1, 2, ..., s \}$ şeklindedir.

Burada

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

Örneğin; $V(x^2 + y^2 - 1, \ x - 3y^2) \subseteq \mathbb{R}^2$ variety kümesi $x^2 + y^2 = 1$ çemberi ile $x = 3y^2$ parabolünün $xy-$koordinat düzlemindeki kesişimidir.

Bununla beraber genel olarak;

$S = \{ f \mid \ f \in k[x_1, x_2, ..., x_n] \} \subseteq k[x_1, x_2, ..., x_n]$ ise,

$V(S) = \{ (a_1, a_2, ..., a_n) \in k^n \mid \ \forall f \in S \ \text{için} \ f(a_1, a_2, ..., a_n) = 0 \ \}$ kümesi tanımlanır.

Tanım1.1.5: $(R,+,\bullet)$ bir halka $I \subseteq R$, $I \neq \varnothing$ olsun. Eğer;

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

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

$I = \langle f_1, f_2, ..., f_s \rangle = \left\{ \sum_{i=1}^{s} u_i f_i \mid u_i \in k[x_1, x_2, ..., x_n], i = 1,2,...,s \right\}$, $k[x_1, x_2, ..., x_n]$ nin bir idealidir. Bu durumda $\{ f_1, f_2, ..., f_s \}$, I idealinin bir üreteç kümesidir. Variety kümesini daha basit yazabilmek için $I = \langle f_1, f_2, ..., f_s \rangle$ ideali göz önüne alınsın. $V(f_1, f_2, ..., f_s)$ variety kümesi için istenilen daha basit gösterim, $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için daha iyi bir üreteç kümesi olacaktır.

Bunun nasıl olacağını görmek için $V(I)$ variety kümesini göz önüne alalım.

$f \in I$ olmak üzere $f = 0$ şeklinde verilen (1.1.2) denklem sisteminin çözümleri ile

$$f_1 = 0,\ f_2 = 0,\ ...,\ f_s = 0 \qquad (1.1.3)$$

sisteminin çözümlerini karşılaştıralım.

$i = 1,2,...,s$ için $f_i \in I$ olduğundan (1.1.2) sisteminin çözümünün, (1.1.3) sisteminin çözümü olacağı açıktır. Tersine $(a_1, a_2, ..., a_n) \in k^n$, (1.1.3) sisteminin bir çözümüdür ve f polinomu I idealinin herhangi bir elemanı ise $\exists\, u_i \in k[x_1, x_2, ..., x_n]$ için $f = \sum_{i=1}^{s} u_i f_i$ olduğundan $f(a_1, a_2, ..., a_n) = 0$ bulunur. Buradan $(a_1, a_2, ..., a_n) \in k^n$, (1.1.2) sisteminin bir çözümü ve dolayısıyla $V(I) = V(f_1, f_2, ..., f_s)$ olur. Yani I idealinin variety kümesini bulmak için $\{ f_1, f_2, ..., f_s \}$ üreteç kümesinin variety kümesini bulmak yeterli olacaktır. O halde $I = \langle f_1, f_2, ..., f_s \rangle = \langle f_1', f_2', ..., f_t' \rangle$ ise, yani I idealinin birden fazla üreteç kümesi varsa bu üreteç kümelerinin variety kümeleri aynıdır.

Böylece $V(f_1, f_2, ..., f_s) = V(I) = V\left(f_1', f_2', ..., f_t'\right)$ eşitliği yazılır. Bunun anlamı $f_1 = 0$, $f_2 = 0$, ..., $f_s = 0$ sistemi ile $f_1' = 0$, $f_2' = 0$, ..., $f_s' = 0$ sisteminin çözümleri aynı demektir. Bu da şöyle bir soruyu akla getirmektedir. I idealinin variety kümesini bulmak için hangi üreteç kümesinin variety kümesini bulmak yerinde olacaktır? Dolayısıyla $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için 'daha iyi' bir üreteç kümesi elde edilirse $V(f_1, f_2, ..., f_s)$ variety kümesi için de daha basit bir gösterime sahip olunacaktır.

Şimdi probleme farklı bir bakış açısıyla bakalım. k^n nin bir V alt kümesini göz önüne alalım.

$\mathrm{I}(\mathrm{V}) \subseteq k[x_1, x_2, ..., x_n]$ kümesi;

$\mathrm{I}(\mathrm{V}) = \{ f \in k[x_1, x_2, ..., x_n] \mid \forall (a_1, a_2, ..., a_n) \in \mathrm{V} \ için \ f(a_1, a_2, ..., a_n) = 0 \}$ şeklinde tanımlanır. $\mathrm{I}(\mathrm{V})$ kümesi $k[x_1, x_2, ..., x_n]$ nin bir idealdir.

Yukarıdaki $\mathrm{I}(\mathrm{V})$ idealinin kuruluşu çok önemlidir.

$$\{k[x_1, x_2, ..., x_n] \text{ nin alt kümeleri}\} \to \{k^n \text{ nin variety kümeleri}\}$$
$$S \mapsto V(S)$$

dönüşümüne ek olarak,

$$\{k^n \text{ nin alt kümeleri}\} \to \{k[x_1, x_2, ..., x_n] \text{ nin idealleri}\}$$
$$\mathrm{V} \mapsto \mathrm{I}(\mathrm{V})$$

dönüşümü vardır.

Özellikle I ideali ve $\mathrm{I}(V(I))$ ideali arasındaki ilişkiye bakalım. $I \subseteq \mathrm{I}(V(I))$ olduğunu görmek kolaydır, fakat eşitlik her zaman sağlanmaz.

Herhangi bir $f \in I$ alalım. $f \in \mathrm{I}(V(I))$ mı?

$f \notin \mathrm{I}(V(I))$ olduğunu varsayalım.

$$f \notin \mathrm{I}(V(I)) \Rightarrow f \in k[x_1, x_2, ..., x_n] \text{ , } \exists (a_1, a_2, ..., a_n) \in V(I) \text{ için } f(a_1, a_2, ..., a_n) \neq 0 \quad (*)$$
$$\Rightarrow \forall f \in I \text{ için } f(a_1, a_2, ..., a_n) = 0 \quad (**)$$

(*) ile (**) ifadeleri birbiriyle çelişir. Buradan $f \in \mathrm{I}(V(I))$ olur. Böylece $I \subseteq \mathrm{I}(V(I))$ olur.

Örneğin; $I = \langle x^2, y^2 \rangle \subseteq k[x, y]$ ise $V(I) = V(x^2, y^2) = \{(0,0)\}$ bulunur. Dolayısıyla x, $y \in \mathrm{I}(V(I))$ olmasına rağmen x, $y \notin I$ olur. Böylece eşitliğin her zaman olmadığı görülür.

Yukarıda bahsettiğimiz 'daha iyi' üreteç kümesini bulmak için önce $k[x_1, x_2, ..., x_n]$ deki polinomların sonlu iki kümesinin aynı ideali üretip üretmediğini belirlemek gerekir.

Başka bir ifadeyle $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ ve $f_1', f_2', ..., f_t' \in k[x_1, x_2, ..., x_n]$ verildiğinde $\langle f_1, f_2, ..., f_s \rangle = \langle f_1', f_2', ..., f_t' \rangle$ olup olmadığı belirlemek gerekir. Bu nedenle aşağıdaki adımların gerçeklenmesi gerekir.

Adım1: $I = \langle f_1, f_2, ..., f_s \rangle$ ve $f \in k[x_1, x_2, ..., x_n]$ verildiğinde f polinomunun I idealinde olup olmadığının belirlenmesi. Bu probleme ideale ait olma problemi denir.

Adım2: f polinomu I idealinde ise $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s$ olacak şekilde $u_1, u_2, ..., u_s \in k[x_1, x_2, ..., x_n]$ polinomlarının belirlenmesi.

$I \subseteq k[x_1, x_2, ..., x_n]$ bir ideal ve $f \in k[x_1, x_2, ..., x_n]$ olsun. Daha önce

$$\psi : k^n \longrightarrow k$$
$$(a_1, a_2, ..., a_n) \mapsto \psi(a_1, a_2, ..., a_n) = f(a_1, a_2, ..., a_n)$$

ile tanımlanan bir değer fonksiyonunun f ile belirlendiği söylenmişti.

Şimdi $\varphi = \psi\big|_{V(I)}$ fonksiyonu her $(a_1, a_2, ..., a_n) \in V(I)$ için

$$\varphi : V(I) \longrightarrow k$$
$$(a_1, a_2, ..., a_n) \mapsto \varphi(a_1, a_2, ..., a_n) = f(a_1, a_2, ..., a_n)$$

biçiminde tanımlansın.

$f, g \in k[x_1, x_2, ..., x_n]$ için f ve g polinomları ile belirlenen $V(I) \longrightarrow k$ değer fonksiyonlarının ne zaman eşit olduğuna bakalım.

$f - g \in \mathrm{I}(V(I))$ ise $\forall (a_1, a_2, ..., a_n) \in V(I)$ için $(f - g)(a_1, a_2, ..., a_n) = 0$ olur. Buradan $f(a_1, a_2, ..., a_n) - g(a_1, a_2, ..., a_n) = 0$ dır.

Dolayısıyla $f(a_1, a_2, ..., a_n) = g(a_1, a_2, ..., a_n)$ bulunur. Böylece $f = g$ dir.

Sonuç olarak $f - g \in \mathrm{I}(V(I))$ ise f ve g polinomları ile belirlenen $\varphi : V(I) \longrightarrow k$ değer fonksiyonları eşittir.

Tanım1.1.6: $k[x_1, x_2, ..., x_n]$ nin bir J ideali ve $f, g \in k[x_1, x_2, ..., x_n]$ verilsin. $f - g \in J$ ise modülo J ye göre f, g ye **denktir** denir ve $f \equiv g \pmod{J}$ ile gösterilir. Bu biçimde tanımlanan "$\equiv$", $k[x_1, x_2, ..., x_n]$ üzerinde bir denklik bağıntısıdır.

Bu bağıntıya göre denklik sınıflarının kümesi $k\left[x_1, x_2, ..., x_n\right]/J$ ile gösterilir. Aynı zamanda $k\left[x_1, x_2, ..., x_n\right]/J$, denklik sınıflarının toplama ve çarpma işlemleri ile değişmeli bir halkadır.

Teorem1.1.7 (Hilbert Taban Teoremi) :

(i) I **,** $k\left[x_1, x_2, ..., x_n\right]$ halkasının herhangi bir ideali ise $I = \langle f_1, f_2, ..., f_s \rangle$ olacak şekilde $f_1, f_2, ..., f_s \in k\left[x_1, x_2, ..., x_n\right]$ polinomları vardır.

(ii) Eğer $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$, $k\left[x_1, x_2, ..., x_n\right]$ halkasındaki ideallerin artan bir zinciri ise $I_N = I_{N+1} = I_{N+2} = ...$ olacak şekilde bir $N \in \mathbb{N}$ vardır.

Tanım1.1.8: R bir halka I **,** R halkasının herhangi bir ideali olsun. R nin $I = \langle a_1, a_2, ..., a_s \rangle$ olacak şekilde $a_1, a_2, ..., a_s$ elemanları varsa I idealine **sonlu üretilmiş ideal** denir.

Tanım1.1.9 R değişmeli bir halka ve $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$, R nin ideallerinin artan bir zinciri olsun. $I_N = I_{N+1} = I_{N+2} = ...$ olacak şekilde bir $N \in \mathbb{N}$ varsa R halkasına **Noetherian Halka** denir.

Teorem1.1.10: Aşağıdaki koşullar değişmeli bir R halkası için denktir.

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

(ii) Eğer $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...,$ R nin ideallerinin artan bir zinciri ise $I_N = I_{N+1} = I_{N+2} = ...$ olacak şekilde $N \in \mathbb{N}$ vardır.

Kanıt: (i)$\Rightarrow$(ii):

$I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...,$ R nin ideallerinin artan bir zinciri olsun. Böylece $I = \bigcup_{n=1}^{\infty} I_n$ kümesi R nin idealidir.

Bu durumda $i = 1, 2, ..., s$ için $f_i \in I$ olduğundan $f_i \in I_{N_i}$ olacak şekilde $N_i \in \mathbb{N}$ vardır. $N = \max_{1 \le i \le s} N_i$ olsun.

Dolayısıyla her $i = 1, 2, ..., n$ için $f_i \in I_N$ dir. $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$ artan bir zincir ve $I = \bigcup_{n=1}^{\infty} I_n$ olduğundan $I_N \subseteq I = \bigcup_{n=1}^{\infty} I_n$ olur. $\therefore I = I_N$ dir.

(ii)$\Rightarrow$(i):

(ii) nin sağlandığını fakat (i) nin sağlanmadığını varsayalım. Yani I, R nin elemanlarının sonlu bir kümesi tarafından üretilmesin. Bu durumda $I = \langle f_1, f_2, ..., f_s, f_{s+1}, ... \rangle$ olur.

$f_1 \in I$ olsun. O zaman $f_2 \notin \langle f_1 \rangle$ olacak şekilde bir $f_2 \in I$ vardır. Yani $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle$ olur. Benzer şekilde $f_3 \notin \langle f_1, f_2 \rangle$ olacak şekilde bir $f_3 \in I$ vardır. Buradan $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle$ olur. Bu şekilde devam edilirse

$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle \subsetneq .... \subsetneq \langle f_1, f_2, f_3, ..., f_s \rangle \subsetneq \langle f_1, f_2, f_3, ..., f_s, f_{s+1} \rangle \subsetneq ....$ şeklinde artan bir zincir bulunur. Bu (ii) ile çelişir. Dolayısıyla (i) sağlanmalıdır. □

Bu durumda R nin Noetherian Halka olması için gerekli ve yeterli koşul R halkasındaki her idealin sonlu bir üreteç kümesinin olmasıdır.

Teorem1.1.11: R bir Noetherian Halka ise $R[x]$ bir Noetherian Halkadır.

Kanıt: R bir Noetherian Halka ve J, $R[x]$ in bir ideali olsun. önceki teoremden J idealinin sonlu üretilmiş olduğunu görmek yeterlidir. Her bir $n \geq 0$ için; $I_n = \{r \in R \mid r,\ J \text{ deki } n.\text{dereceden bir polinomun başkatsayısı}\} \cup \{0\}$ kümesini tanımlayalım.

I_n kümesinin R nin bir ideali olduğu açıktır.

$\forall n \geq 0$ için $I_n \subseteq I_{n+1}$ dir. Gerçekten;

$r_1 \in I_n$ ise r_1, J deki $n.$ dereceden bir $p(x)$ polinomunun başkatsayısıdır. Yani $p(x) = r_1 x^n + p_1(x)$ olarak yazılır. Buradan $x \cdot p(x) = r_1 x^{n+1} + x \cdot p_1(x)$ olur. Böylece $t(x) = x \cdot p(x) \in J$ bulunur ve r_1, J deki $(n+1).$ dereceden bir $t(x)$ polinomunun başkatsayısıdır.

O halde $r_1 \in I_{n+1}$ ve $I_n \subseteq I_{n+1}$ olur.

R bir Noetherian Halka olduğundan $\forall n \geq N$ için $I_n = I_N$ olacak şekilde bir $N \in \mathbb{N}$ vardır. Aynı zamanda Teorem1.1.10 den her bir $i \in \{1, 2, ..., n\}$ için I_i sonlu üretilmiştir.

$I_i = \langle r_{i1}, r_{i2}, ..., r_{it_i} \rangle$ diyelim. Şimdi $i = 1, 2, ..., N$ ve $j = 1, 2, ..., t_i$ için f_{ij}, J idealindeki deki $i.$ dereceden ve başkatsayısı r_{ij} olan bir polinom olsun. $J^* = \langle f_{ij} \mid 1 \leq i \leq N,\ 1 \leq j \leq t_i \rangle$, $R[x]$ halkasında sonlu üretilmiş bir ideal olsun. Teoremi kanıtlamak için $J = J^*$ olduğunu görmek yeterlidir. $J^* \subseteq J$ olduğu açıktır.

$f \in J$ ve f $n.$ dereceden bir polinom olsun. n üzerinden tümevarımla $f \in J^*$ olduğu kanıtlanabilir. $f = 0$ veya $n = 0$ ise $f \in I_0$ dir. Buradan $f \in J^*$ olur.

$n > 0$ olsun. Derecesi n den küçük olan tüm polinomların J^* da olduğunu varsayalım. f nin başkatsayısı r olsun.

Eğer $n \le N$ ise; $r \in I_n$ olacağından $\exists\, s_j \in R$ için $r = \sum_{j=1}^{t_n} s_j \cdot r_{nj}$ dir. Bu durumda f_{nj} polinomunun başkatsayısı r_{nj} olduğundan $n.$dereceden $g = \sum_{j=1}^{t_n} s_j \cdot f_{nj}$ polinomunun başkatsayısı r dir ve $g \in J^*$ dır. $f-g$ nin derecesi en fazla $n-1$ olacağından $f-g \in J$ dir. Varsayımdan $f-g \in J^*$ elde edilir. Buradan $f \in J^*$ bulunur. Eğer $n > N$ ise $r \in I_n = I_N$ olacağından $\exists\, s_j \in R$ için $r = \sum_{j=1}^{t_N} s_j \cdot r_{Nj}$ dir. O zaman $g = \sum_{j=1}^{t_N} s_j \cdot x^{n-N} \cdot f_{Nj}$ polinomunun derecesi n, başkatsayısı r olup $g \in J^*$ dır. $f-g$ nin derecesi en fazla $n-1$ olacağından $f-g \in J$ olur. Varsayımdan $f-g \in J^*$ elde edilir. Buradan $f \in J^*$ bulunur. Sonuç olarak $J = J^*$ olur. □

Yukarıdaki teorem ve n üzerinden tümevarım kullanılırsa $k[x_1, x_2, ..., x_n]$ nin bir Noetherian Halka olduğu görülür. Bu, Teorem1.1.7 in kanıtıdır.

1.2. Çok Değişkenli Doğrusal Polinomlar İçin İndirgeme

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

$$f_1 = 0\,,\ f_2 = 0\,, ...,\ f_s = 0 \tag{1.2.1}$$

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

Örnek1.2.1: $f_1 = x + y - z$, $f_2 = 2x + 3y + 2z \in \mathbb{R}[x, y, z]$ doğrusal polinomlar olsun. $I = \langle f_1, f_2 \rangle$ idealini ve

$$\begin{cases} x + y - z = 0 \\ 2x + 3y + 2z = 0 \end{cases} \tag{1.2.2}$$

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

Bu sistemin katsayılar matrisi üzerinde satır indirgeme metodu kulanılırsa $\begin{bmatrix} 1 & 1 & -1 \\ 2 & 3 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & -1 \\ 0 & 1 & 4 \end{bmatrix}$ olur. (1.2.2) sisteminin çözümleri,

$$\begin{cases} x+y-z=0 \\ y+4z=0 \end{cases} \tag{1.2.3}$$

sisteminin çözümleri ile aynıdır. Satır indirgeme yöntemi $I=\langle f_1, f_2 \rangle$ ideali için üreteç kümesini değiştirme yoludur. Yapılan satır indirgemesi ile $f_3 = y+4z$ polinomunun f_1 ve f_2 polinomlarının doğrusal bileşimi olarak yazıldığı görülür.

$f_3 = f_2 - 2f_1$ olduğundan $f_3 \in \langle f_1, f_2 \rangle = I$ dır. Diğer taraftan $f_2 = 2f_1 + f_3$ olduğundan $f_2 \in \langle f_1, f_3 \rangle$ olur. Sonuç olarak $I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ elde edilir.

Bu yöntem I idealinin üreteç kümesini sadeleştirir ve (1.2.2) sisteminin bir çözümünün bulunması için kolaylık sağlar. Bunlar birlikte düşünüldüğü zaman $V(I)$ variety kümesinin belirlenmesi daha kolay olur.

Tanım1.2.2: Yukarıdaki gibi f_1 polinomu kullanılarak f_2 polinomu yerine f_3 polinomunun yazılması yöntemi; f_2 nin f_1 tarafından indirgenmesi olarak adlandırılır ve $f_2 \xrightarrow{f_1} f_3$ ile gösterilir.

Aslında üretilen yeni f_3 polinomu bir bölme işleminin kalanıdır.

Örnek1.2.3: $f_1 = y-z,\ f_2 = x+2y+3z,\ f_3 = 3x-4y+2z \in \mathbb{Q}[x,y,z]$ doğrusal polinomlar olsun. $I = \langle f_1, f_2, f_3 \rangle$ ideali ve

$$\begin{cases} y-z=0 \\ x+2y+3z=0 \\ 3x-4y+2z=0 \end{cases} \tag{1.2.4}$$

sisteminin çözümü olan $V(f_1, f_2, f_3)$ variety kümesi güz önüne alınsın.

Bu sistemin katsayılar matrisinin satır indirgemesi yapılırsa

$\begin{bmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 3 & -4 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 0 & -10 & -7 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 0 & 0 & -17 \end{bmatrix}$ olur. Böylece yapılan satır indirgemesi ile $f_4 = -17z$ polinomu üretilmiş olur.

İndirgemeler;

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z \tag{1.2.5}$$

ile gösterilebilir. Bu f_3 ün sırasıyla f_2 ve f_1 ile bölünmesi anlamına gelir.

$$f_3 = -10f_1 + 3f_2 - 17z \tag{1.2.6}$$

olarak elde edilir. Dolayısıyla $I = \langle f_1, f_2, f_3 \rangle$ ideali için yeni üreteç kümesi $\{f_1, f_2, f_4\}$ olarak elde edilir.

Yukarıdaki örneğin çözümünde:

İlk Olarak; (1.2.4) sisteminin üçüncü denkleminden, önce x değişkeninin sonra da yeni üçüncü denklemden y değişkeninin yok edilmesi yolu seçilmiştir.

Polinomlardaki değişkenler farklı sırada yazılarak $f_1 = -z + y$, $f_2 = 3z + 2y + x$, $f_3 = 2z - 4y + 3x$ şeklinde yazılabilir. Yine satır indirgeme metodu kullanılır, fakat önce z değişkeni sonra da y değişkeni yok edilebilir. Dolayısıyla değişkenlerin hangi sırada yazıldığı önemli değildir. Ancak değişkenleri belli bir sırada yazmak zorunludur. Değişkenler polinom içinde ve matriste farklı sıralanmamalıdır. Örneğimizde değişken sırası x, y, z şeklindedir.

İkinci Olarak; (1.2.5) deki indirgemeler önce f_3 polinomundan f_2 polinomunun bir katı sonrada $-10y - 7z$ polinomundan f_1 polinomunun bir katı çıkarılarak elde edildi. f_3 ve $-10y - 7z$ polinomlarındaki bazı terimlerin yok edilmesinde f_1 ve ve f_2 polinomlarının baş terimlerinin kullanılmasının etkisi olmuştur. Burada $-17z$ polinomu f_1 ve f_2 polinomları kullanılarak indirgenemez.

Bir $f \in k[x,y,z]$ polinomunun I idealinde olup olmadığı problemine geri dönelim. Eğer $f \in I$ ise f polinomu I idealinin üreteç kümesindeki elemanların bir doğrusal bileşimi şeklinde ifade edilir. Bu durumda f_1 polinomunun baş terimi x ve f_3 polinomunun baş terimi y olduğundan (1.2.5) deki gibi benzer bir yolla hem f_1 hem de f_3 ile bölme kullanılarak herhangi bir f polinomu sadece z değişkenine bağlı bir polinoma indirgenebilir. Ancak sadece z ye bağlı herhangi bir polinom bölme kullanılarak f_1 ve f_3 ile indirgenemez.

Bölme, f polinomunu (1.2.6) daki gibi f_1 ve f_3 polinomlarının doğrusal bileşimi ve bir kalanın toplamı olarak yazılmasını sağlar. Böylece;

$f \in I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ olması için gerekli ve yeterli koşul bu kalanın sıfır olmasıdır.

1.3. Tek Değişkenli Polinomlar İçin İndirgeme

Bu kısımda $k[x]$ polinom halkasındaki polinomlar göz önüne alınacaktır ve ilk kısımda bahsedilen problemleri çözmek için **Euclide Algoritması** kullanılacaktır. Bunu yaparken de $k[x]$ ile ilgili bazı temel tanımlar ve gösterimler verilecektir. Daha sonra bu tanım ve gösterimler çok değişkenli polinomlara genelleştirilecektir.

Tanım1.3.1: $0 \neq f \in k[x]$ için f polinomundaki x değişkeninin en büyük kuvvetine f polinomunun **derecesi** denir ve $\deg f$ ile gösterilir.

Tanım1.3.2: $0 \neq f \in k[x]$ için f polinomundaki en büyük dereceli terime f polinomunun **baş terimi** denir ve $lt(f)$ ile gösterilir.

Tanım1.3.3: $0 \neq f \in k[x]$ için f polinomundaki baş terimin katsayısına f polinomunun **baş katsayısı** denir ve $lc(f)$ ile gösterilir.

Dolayısıyla $a_0, a_1, ..., a_n \in k$ ve $a_n \neq 0$ olmak üzere $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ ise $\deg(f) = n$, $lt(f) = a_n x^n$, $lc(f) = a_n$ olur.

Tanım1.3.4: $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ ve $g = b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0$, $n = \deg(f) \geq m = \deg(g)$ olmak üzere iki polinom ise f nin g ile bölünmesinde ilk adım $\frac{a_n}{b_m} x^{n-m} \cdot g$ çarpımını f polinomundan çıkarmaktır. Verilen gösterim kullanılarak bu çarpımda g polinomunun çarpanının $\frac{lt(f)}{lt(g)}$ olduğu söylenebilir. Dolayısıyla $h = f - \frac{lt(f)}{lt(g)} \cdot g$ nin ilk kalan olduğu görülür. Bu işleme f polinomunun g polinmu tarafından h polinomuna **indirgenmesi** denir ve $f \xrightarrow{g} h$ ile gösterilir.

Örnek1.3.5: $f = x^3 - 2x^2 + 2x + 8$ ve $g = 2x^2 + 3x + 1 \in \mathbb{Q}[x]$ olsun. f polinomunun g ile bölümünden elde edilen bölüm $q = \frac{1}{2}x - \frac{7}{4}$ ve kalan $r = \frac{27}{4}x + \frac{39}{4}$ olarak bulunur. Dolayısıyla $f = \left(\frac{1}{2}x - \frac{7}{4}\right)g + \left(\frac{27}{4}x + \frac{39}{4}\right)$ olur.

Yukarıda yapılan bölme adımlarını inceleyelim. Önce $\frac{1}{2}x$ ile g polinomu çarpıldı ve elde edilen çarpım f polinomundan çıkarıldı. Böylece f polinomunu baş terimi yok edilmiş oldu. Sonra elde edilen ilk kalan olan $h = f - \left(\frac{1}{2}x\right)g = -\frac{7}{2}x^2 + \frac{3}{2}x + 8$ polinomunun baş terimi yok edilip $r = \frac{27}{4}x + \frac{39}{4}$ kalanı elde edildi.

Az önceki indirgeme gösterimi kullanılarak $f \xrightarrow{g} h \xrightarrow{g} r$ şeklinde yazılabilir. Yukarıdaki gibi tekrarlanan indirgeme adımlarının kullanımı $f \xrightarrow{g}_{+} r$ ile gösterilir.

Teorem1.3.6 k değişmeli bir cisim ve $0 \neq g$, $f \in k[x]$ olsun. Bu durumda $f = q \cdot g + r$ ve $r = 0$ ya da $\deg(r) < \deg(g)$ olacak şekilde tek şekilde belirli $q, r \in k[x]$ vardır. (William W. Adams, Philippe Loustaunau 1994)

GİRİŞ: $g \neq 0$ olmak üzere $f, g \in k[x]$ alınsın.

ÇIKIŞ: $\exists\, q, r \in k[x]$ ∋ $f = q \cdot g + r$, $r = 0$ veya $\deg(r) < \deg(g)$

BAŞLANGIÇ: $q := 0$; $r := f$

DÖNGÜ: $r \neq 0$ ve $\deg(g) \leq \deg(r)$ olduğu sürece aşağıdaki işlemler yapılır

$$q := q + \frac{lt(r)}{lt(g)} \quad , \qquad r := r - \frac{lt(r)}{lt(g)} \cdot g$$

ALGORİTMA 1.3.1Tek Değişkenli Polinomlar İçin Bölme Algoritması

Algoritmadaki r polinomu $r = 0$ veya g polinomunun derecesinden kesinlikle daha küçük bir dereceye sahip oluncaya kadar döngüdeki adımlar tekrarlanır.

Örnek1.3.7: $f = x^3 - 2x^2 + 2x + 8$ ve $g = 2x^2 + 3x + 1 \in \mathbb{Q}[x]$ olsun. f polinomunun g polinomu ile bölümünden oluşan bölüm ve kalan Algoritma1.3.1 ile bulunabilir.

BAŞLANGIÇ: $q := 0$, $r := f = x^3 - 2x^2 + 2x + 8$

1. ADIM:

$$q := q + \frac{lt(r)}{lt(g)} = 0 + \frac{x^3}{2x^2} = \frac{1}{2}x$$

$$r := r - \frac{lt(r)}{lt(g)} \cdot g = \left(x^3 - 2x^2 + 2x + 8\right) - \frac{x^3}{2x^2} \cdot \left(2x^2 + 3x + 1\right) = -\frac{7}{2}x^2 + \frac{3}{2}x + 8$$

2.ADIM:

$$q := q + \frac{lt(r)}{lt(g)} = \frac{1}{2}x + \frac{-\frac{7}{2}x^2}{2x^2} = \frac{1}{2}x - \frac{7}{4}$$

$$r := r - \frac{lt(r)}{lt(g)} \cdot g = \left(-\frac{7}{2}x^2 + \frac{3}{2}x + 8\right) - \frac{-\frac{7}{2}x^2}{2x^2} \cdot \left(2x^2 + 3x + 1\right) = \frac{27}{4}x + \frac{39}{4}$$

$\deg(r) = 1 < 2 = \deg(g)$ olduğundan algoritma tamamlanır.

Bölüm $q = \frac{1}{2}x - \frac{7}{4}$ ve kalan $r = \frac{27}{4}x + \frac{39}{4}$ olarak elde edilir.

- İki polinom tarafından üretilen idealin üreteç elemanlarından birinin diğerine göre indirgenerek üreteç kümesinin nasıl değiştirilebileceğine bakalım.

$I = \langle f, g \rangle$ olsun. $f \xrightarrow{g} h$ olduğunu varsayalım. $I = \langle h, g \rangle$ olacağını görelim.

$f \xrightarrow{g} h \Rightarrow h = f - \frac{lt(f)}{lt(g)} \cdot g$ (*)dir.

$f \in \langle f, g \rangle \underset{(*)dan}{\Rightarrow} f \in \langle h, g \rangle$ ve $g \in \langle f, g \rangle \Rightarrow g \in \langle h, g \rangle$ dir. Böylece $\langle f, g \rangle \subseteq \langle h, g \rangle$ olur.

$h \in \langle h, g \rangle \underset{(*)dan}{\Rightarrow} h \in \langle f, g \rangle$ ve $g \in \langle h, g \rangle \Rightarrow g \in \langle f, g \rangle$ dir. Buradan $\langle h, g \rangle \subseteq \langle f, g \rangle$ olur.

Sonuç olarak $I = \langle f, g \rangle = \langle h, g \rangle$ bulunur.

Dolayısıyla I idealinin üreteç kümesinde f yerine h yazılabilir ve bu sayede I idealinin üreteç kümesi değiştirilmiş olur.

Teorem1.3.8: k bir cisim olmak üzere $k[x]$ polinom halkasındaki her ideal tek bir g elemanı tarafından üretilmiştir. (William W. Adams, Philippe Loustaunau 1994)

Dikkat edilmelidir ki Teorem1.3.8 deki g polinomu sıfırdan farklı sabit bir çarpan yakınlığında tektir. Aynı zamanda burada $\{g\}$ kümesi $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için 'daha iyi' bir üreteç kümesidir.

Örneğin; $f_1 = 0, f_2 = 0, ..., f_s = 0$, $i = 1, 2, ..., s$, $f_i \in k[x]$, denklem sisteminin çözüm kümesi, tam olarak $g = 0$ denkleminin çözüm kümesi ile aynıdır. Dolayısıyla $\langle f_1, f_2, ..., f_s \rangle = \langle g \rangle$ dir.

Teorem1.3.8 deki g polinomunun nasıl bulunacağını araştıralım.

İlk olarak; İki polinom tarafından üretilen $I \subseteq k[x]$ idealini göz önüne alalım. $I = \langle f_1, f_2 \rangle$ olsun. $\gcd(f_1, f_2) = g$ ise;

- g, f_1 *ve* f_2 *yi böler*
- Eğer $h \in k[x]$ f_1 *ve* f_2 *yi bölüyorsa* $h \mid g$ *dir*
- $lc(g) = 1$ dir.

Önerme1.3.9: $f_1, f_2 \neq 0$ olmak üzere $f_1, f_2 \in k[x]$ olsun. O zaman $\gcd(f_1, f_2)$ vardır ve $\langle f_1, f_2 \rangle = \langle \gcd(f_1, f_2) \rangle$ dir.

Kanıt: Teorem1.3.8 den $\langle f_1, f_2 \rangle = \langle g \rangle$ olacak şekilde bir $g \in k[x]$ vardır. g sıfırdan farklı bir sabit çarpan yakınlığında tek olduğundan $lc(g) = 1$ varsayılabilir.

$\langle f_1, f_2 \rangle = \langle g \rangle$ olduğundan $\gcd(f_1, f_2) = g$ olduğunu göstermeliyiz. $f_1, f_2 \in \langle f_1, f_2 \rangle = \langle g \rangle \Rightarrow g \mid f_1$ *ve* $g \mid f_2$ dir. h polinomu f_1 ve f_2 yi bölen başka bir polinom olsun.

$g \in \langle f_1, f_2 \rangle \Rightarrow g = u_1 f_1 + u_2 f_2$ olacak şekilde $u_1, u_2 \in k[x]$ vardır.

$h \mid f_1$, $h \mid f_2 \Rightarrow h \mid u_1 f_1$, $h \mid u_2 f_2 \Rightarrow h \mid u_1 f_1 + u_2 f_2 \Rightarrow h \mid g$. Buradan $g = \gcd(f_1, f_2)$ dir.

$\therefore \langle f_1, f_2 \rangle = \langle g \rangle = \langle \gcd(f_1, f_2) \rangle$. □

Sonuç olarak eğer en büyük ortak bölenin bulunması için bir algoritmaya sahipsek aslında $\langle f_1, f_2 \rangle$ ideali için tek elemanlı bir üreteç kümesi bulabiliriz.

Lemma1.3.10: $f_1, f_2 \in k[x]$ ve $f_1, f_2 \neq 0$ olsun. O zaman $\forall q \in k[x]$ için $\gcd(f_1, f_2) = \gcd(f_1 - q \cdot f_2, f_2)$ dir. (William W. Adams, Philippe Loustaunau, 1994)

İki polinomun en büyük ortak bölenini bulmak için aşağıda bir algoritma verilmiştir.

GİRİŞ: $f_1, f_2 \neq 0$ olmak üzere $f_1, f_2 \in k[x]$ alınsın.

ÇIKIŞ: $f = \gcd(f_1, f_2)$

BAŞLANGIÇ: $f := f_1$, $g := f_2$

DÖNGÜ: $g \neq 0$ olduğu sürece aşağıdaki işlemler yapılır

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

$f := g$, $g := r$, $f := \frac{1}{lc(f)} \cdot f$

ALGORİTMA 1.3.2

Örnek1.3.11: $f_1 = x^3 - 3x + 2$ ve $f_2 = x^2 - 1 \in \mathbb{Q}[x]$ olsun. $\gcd(f_1, f_2)$ Algoritma1.3.2 ile bulunabilir.

BAŞLANGIÇ: $f := x^3 - 3x + 2$, $g := x^2 - 1$

1.ADIM:

$x^3 - 3x + 2 \xrightarrow{x^2-1} -2x + 2$

$f := x^2 - 1$, $g := -2x + 2$

2.ADIM:

$x^2 - 1 \xrightarrow{-2x+2} x - 1 \xrightarrow{-2x+2} 0$

$f := -2x + 2$, $g := 0$

$f := \frac{1}{lc(f)} \cdot f = -\frac{1}{2} f = x - 1$

$g = 0$ olduğundan algoritma tamamlanır.

Dolayısıyla $\gcd(f_1, f_2) = x - 1$ dir.

İkinci Olarak; f_i ler $i = 1, 2, ..., s$ ve $s \geq 2$ için sıfırdan farklı polinomlar olmak üzere $I = \langle f_1, f_2, ..., f_s \rangle$ idealini göz önüne alalım. $f_1, f_2, ..., f_s$ polinomlarının $\gcd(f_1, f_2, ..., f_s)$ ile gösterilen en büyük ortak bölenini hatırlayalım. $\gcd(f_1, f_2, ..., f_s) = g$ ise;

- $\forall\, i = 1, 2, ..., s \;\; için \;\; g \mid f_i$ dir
- Eğer $h \in k[x]$ ve $\forall\, i = 1, 2, ..., s \;\; için \;\; h \mid f_i \;\; ise \;\; h \mid g$ dir
- $lc(g) = 1$ dir.

Önerme1.3.12: $f_1, f_2, ..., f_s \in k[x]$ olsun. O zaman

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

(ii) Eğer $s \geq 3$ ise $\gcd(f_1, f_2, ..., f_s) = \gcd(f_1, \gcd(f_2, f_3, ..., f_s))$ dir.

Kanıt: (i): Teorem1.3.8 den $\langle f_1, f_2, ..., f_s \rangle = \langle g \rangle$ olacak şekilde bir $g \in k[x]$ vardır. g sabit bir çarpan yakınlığında tek olduğundan $lc(g) = 1$ olduğu varsayılabilir. $\langle f_1, f_2, ..., f_s \rangle = \langle g \rangle$ olduğundan $\gcd(f_1, f_2, ..., f_s) = g$ olduğu gösterilmelidir. $f_1, f_2, ..., f_s \in \langle f_1, f_2, ..., f_s \rangle \Rightarrow \forall\, i = 1, 2, ..., s \;\; için \;\; g \mid f_i$ dir.

h , $i = 1, 2, ..., s \;\; için \; h \mid f_i$ sağlayan başka bir polinom olsun.

$g \in \langle g \rangle = \langle f_1, f_2, ..., f_s \rangle \Rightarrow g = u_1 f_1 + u_2 f_2 + ... + u_s f_s$ olacak şekilde $u_1, u_2, ..., u_s \in k[x]$ vardır.

$$\begin{aligned}\forall i=1,2,...,s \ \ için \ \ h\,|\,f_i &\Rightarrow \forall i=1,2,...,s \ \ için \ \ h\,|\,u_i f_i \\ &\Rightarrow h\,|\,u_1 f_1+u_2 f_2+...+u_s f_s \\ &\Rightarrow h\,|\,g\end{aligned}$$

Buradan $g=\gcd(f_1, f_2,..., f_s)$ dir. $\therefore \langle f_1, f_2,..., f_s\rangle=\langle g\rangle=\langle \gcd(f_1, f_2,..., f_s)\rangle$.

(ii): $h=\gcd(f_2, f_3,..., f_s)$ olsun. O zaman (i) den $\langle f_2, f_3,..., f_s\rangle=\langle h\rangle$ olur. Buradan $\langle f_1, f_2,..., f_s\rangle=\langle f_1, h\rangle$ bulunur.

(i) den $\gcd(f_1, f_2,..., f_s)=\gcd(f_1, h)=\gcd(f_1, \gcd(f_2, f_3,..., f_s))$ olur. □

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

- $I=\langle f_1, f_2,..., f_s\rangle$ idealinde olup olmadığına karar vermek için ilk önce $g=\gcd(f_1, f_2,..., f_s)$ bulunmalıdır. Sonra Bölme algoritması kullanılarak f polinomu g polinomuna bölünür. Bu bölmede f polinomunun $I=\langle f_1, f_2,..., f_s\rangle=\langle g\rangle$ idealinde olması için gerekli ve yeterli koşul f polinomunun g polinomu ile bölümünden kalanın sıfır olmasıdır. Bu

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

II .BÖLÜM

TERİM SIRALAMALARI VE İNDİRGEMELER

2.1. Terim Sıralamaları

Terim sıralaması kuvvet çarpımları üzerinde bir sıralama belirtmek için önemlidir. Sıralama değişebilir. Fakat hangi sıralamanın kullanıldığı belirtilmek zorundadır. Tek değişkenli durumda en büyük dereceli ilk terim kullanılır. Birden fazla değişkende benzer bir sıralamaya ihtiyaç vardır.

$T^n = \left\{ x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \ldots \cdot x_n^{\beta_n} \mid \beta_i \in \mathbb{N}, i = 1,2,\ldots,n \right\}$ ile gösterilen kuvvet çarpımları kümesini hatırlayalım. X^β ile $x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \ldots \cdot x_n^{\beta_n}$ kuvvet çarpımını gösterilecektir ve burada $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$ şeklinde olacaktır.

Bu çalışma boyunca **'kuvvet çarpımı'** x_i değişkenlerinin bir çarpımını ifade edecektir. **'Terim'** ise kuvvet çarpımının bir katsayı katını ifade edecektir. Aynı zamanda bir polinomda farklı terimlerin farklı kuvvet çarpımlarına sahip olduğu varsayılacaktır. Dolayısıyla $3x^2y$ olarak asla $2x^2y + x^2y$ yazılmayacaktır.

T^n kümesini sıralamak için bazı yollar vardır. Örneğin tek değişkenli ve doğrusal polinom durumunda sıralama; bir bölme (veya indirgeme) algoritması tanımlamak için kullanılır.

$X^\alpha \mid X^\beta$ ise $X^\alpha \leq X^\beta$ dır. Aynı zamanda $\forall\, i = 1,2,\ldots,n \quad için \quad \alpha_i \leq \beta_i \quad ise \quad X^\alpha \leq X^\beta$ dır.

Doğrusal durumda ve tek değişkenli durumda tanımlanan bölmelerde polinomların terimleri artan veya azalan sırada düzenlenmişti. Bu durumdan herhangi iki kuvvet çarpımı karşılaştırabilir. Böylece bir tam sıralama olmak zorundadır. Dolayısıyla $X^\alpha,\ X^\beta \in T^n$ verildiğinde aşağıdakilerden biri gerçeklenmek zorundadır.

$$X^\alpha < X^\beta, \quad X^\alpha = X^\beta, \quad X^\alpha > X^\beta$$

Tanım2.1.1: T^n üzerinde aşağıdaki iki koşulu sağlayan "$<$" tam sıralamasına **terim sıralaması** denir.

(i) $X^\beta \neq 1$ olan her $X^\beta \in T^n$ için $1 < X^\beta$ dır.

(ii) $X^\alpha < X^\beta$ ise her $X^\nu \in T^n$ için $X^\alpha \cdot X^\nu < X^\beta \cdot X^\nu$ dir.

Aşağıda terim sıralamasının üç örneği verilecektir.

Örnek2.1.2: $x_1 > x_2 > x_3 > ... > x_n$ olmak üzere T^n üzerinde

$\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\beta = (\beta_1, \beta_2, ..., \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \alpha \text{ ve } \beta \text{ içinde soldan itibaren farklı ilk} \\ \alpha_i \text{ ve } \beta_i \text{ koordinatlarının } \alpha_i < \beta_i \text{ sağlamasıdır.} \end{cases}$$

biçiminde tanımlanan terim sıralaması **lexicographical** sıralama olarak adlandırılır ve **lex** ($<_{lex}$) ile gösterilir.

Örneğin iki değişkenli durumda $x_1 > x_2$ olmak üzere

$1 <_{lex} x_2 <_{lex} x_2^2 <_{lex} x_2^3 <_{lex} x_1 <_{lex} x_1 x_2$ şeklinde sıralanır.

Değişkenler üzerindeki sıralamanın belirtilmesi gerektiği unutulmamalıdır.

Örneğin iki değişkenli durumda $x_2 > x_1$ olmak üzere

$1 <_{lex} x_1 <_{lex} x_2 <_{lex} x_2 x_1 <_{lex} x_2 x_1^2 <_{lex} x_2^2$ şeklinde sıralanır. Bu örnekte değişkenler üzerindeki sıralamanın önemini vurgulamak için x_1 ve x_2 nin sırası değiştirilmiştir.

Örnek2.1.3: $x_1 > x_2 > x_3 > ... > x_n$ olmak üzere T^n üzerinde

$\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\beta = (\beta_1, \beta_2, ..., \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{I=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \quad ya\ da \\ \sum_{I=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \quad ise \quad x_1 > x_2 > x_3 > ... > x_n \ olmak\ üzere \\ lex\ sıralamasına\ göre \quad X^\alpha < X^\beta \quad olmalıdır. \end{cases}$$

biçiminde tanımlanan terim sıralaması **degree lexicographical** sıralama olarak adlandırılır ve **deglex** ($<_{deglex}$) ile gösterilr.

Örneğin iki değişkenli durumda $1 <_{deglex} x_2 <_{deglex} x_1 <_{deglex} x_2^2 <_{deglex} x_1 x_2 <_{deglex} x_1^2$ şeklinde sıralananır.

Örnek2.1.4: $x_1 > x_2 > x_3 > ... > x_n$ olmak üzere T^n üzerinde

$\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\beta = (\beta_1, \beta_2, ..., \beta_n) \in \mathbb{N}^n$ için;

$$X^\alpha < X^\beta \Leftrightarrow \begin{cases} \sum_{I=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \quad ya\ da \\ \sum_{I=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \quad ise\ \alpha\ ve\ \beta\ içinde\ sağdan\ itibaren \\ farklı\ ilk\ \alpha_i\ ve\ \beta_i\ koordinatları\ için\ \alpha_i > \beta_i\ sağlanmalıdır. \end{cases}$$

biçiminde tanımlanan terim sıralaması **degree reverse lexicographical** sıralama olarak adlandırılır ve **degrevlex** ($<_{degrevlex}$) ile gösterilir.

Örnek2.1.5: $k[x, y]$ halkasında deglex ve degrevlex sıralamaları aynı sıralamalardır.

Tanım2.1.6: Her teriminin toplam derecesi aynı olan $f \in k[x_1, x_2, ..., x_n]$ polinomuna **homojen polinom** denir.

Örneğin; $f = x^2y^2z + xy^4 - z^5$ polinomunun her bir teriminin toplam derecesi 5 olduğundan f homojen polinomdur.

Önerme2.1.7: $X^\alpha, X^\beta \in T^n$ için $X^\alpha \mid X^\beta$ ise $X^\alpha \le X^\beta$ olur. (William W. Adams, Philippe Loustaunau, 1994)

Teorem2.1.8: T^n üzerindeki her terim sıralaması bir iyi sıralamadır. Her $A \subseteq T^n$ ve her $X^\beta \in A$ için $X^\alpha \le X^\beta$ olacak şekilde $X^\alpha \in A$ vardır.

Kanıt: Verilen terim sıralamasının iyi sıralama olmadığını varsayalım. $X^{\alpha_1} > X^{\alpha_2} > X^{\alpha_3} > \ldots$ olacak şekilde $X^{\alpha_i} \in T^n$ vardır. $(i = 1,2,3,\ldots)$ $\langle X^{\alpha_1} \rangle \subset \langle X^{\alpha_1}, X^{\alpha_2} \rangle \subset \langle X^{\alpha_1}, X^{\alpha_2}, X^{\alpha_3} \rangle \subset \ldots.$ olduğu açıktır. $X^{\alpha_1} > X^{\alpha_2}$ olduğundan ve Önerme2.1.7 dan $X^{\alpha_1} \nmid X^{\alpha_2}$ dir. Öyleyse $X^{\alpha_2} \notin \langle X^{\alpha_1} \rangle \Rightarrow \langle X^{\alpha_1} \rangle \subsetneq \langle X^{\alpha_1}, X^{\alpha_2} \rangle$

$X^{\alpha_1} > X^{\alpha_3}$, $X^{\alpha_2} > X^{\alpha_3}$ ve Önerme2.1.7 dan $X^{\alpha_1} \nmid X^{\alpha_3}$ ve $X^{\alpha_2} \nmid X^{\alpha_3}$ dir. Bu durumda $X^{\alpha_3} \notin \langle X^{\alpha_1}, X^{\alpha_2} \rangle \Rightarrow \langle X^{\alpha_1}, X^{\alpha_2} \rangle \subsetneq \langle X^{\alpha_1}, X^{\alpha_2}, X^{\alpha_3} \rangle$ dir.

Bu şekilde devam edilirse $k[x_1, x_2, \ldots, x_n]$ halkasında $\langle X^{\alpha_1} \rangle \subsetneq \langle X^{\alpha_1}, X^{\alpha_2} \rangle \subsetneq \langle X^{\alpha_1}, X^{\alpha_2}, X^{\alpha_3} \rangle \subsetneq \ldots.$ biçiminde ideallerin bir artan zinciri elde edilir. Bu ideal zincirinde eşitlik olmadığı için zincirde belli bir yerden sonra eşit ifadelerin gelmesi mümkün değildir. Bu da Hilbert Taban Teoremi ile çelişir.

Böylece T^n deki her terim sıralaması bir iyi sıralamadır. □

2.2. Polinomların İndirgenmesi Ve Bölme Algoritması

Bu kısımda $k[x_1, x_2, ..., x_n]$ üzerindeki bölme algoritması ile çalışılacaktır. $k[x_1, x_2, ..., x_n]$ üzerinde bir terim sıralaması seçilsin.

$0 \neq a_i \in k$, $X^{\alpha_i} \in T^n$ $(i = 1, 2, ..., r)$, $X^{\alpha_1} > X^{\alpha_2} > ... > X^{\alpha_r}$ ve $f \neq 0$ olmak üzere $f \in k[x_1, x_2, ..., x_n]$ polinomu $f = a_1 X^{\alpha_1} + a_2 X^{\alpha_2} + ... + a_r X^{\alpha_r}$ olarak yazılır.

Tanım2.2.1: Yukarıdaki f polinomu ifadesinde ;

f polinomunun **en büyük kuvvet çarpımı,** $lp(f) = X^{\alpha_1}$

f polinomunun **baş katsayısı,** $lc(f) = a_1$

f polinomunun **baş terimi,** $lt(f) = a_1 X^{\alpha_1}$ olarak tanımlanır.

Not: $f, g \in k[x_1, x_2, ..., x_n]$ için;

$lp(0) = lc(0) = lt(0) = 0$
$lp(f \cdot g) = lp(f) \cdot lp(g)$
$lc(f \cdot g) = lc(f) \cdot lc(g)$
$lt(f \cdot g) = lt(f) \cdot lt(g)$

şeklindedir. Aynı zamanda terim sıralaması değiştirilirse $lp(f), lc(f), lt(f)$ değişebilir.

Örnek2.2.2: $x > y > z$ olmak üzere $f = 2x^2yz + 3xy^3 - 2x^3$ olsun.

Lex sıralamasına göre $lp(f) = x^3$, $lc(f) = -2$, $lt(f) = -2x^3$ dir.

Deglex sıralamasına göre $lp(f) = x^2yz$, $lc(f) = 2$, $lt(f) = 2x^2yz$ dir.

Degrevlex sıralamasına göre $lp(f) = xy^3$, $lc(f) = 3$, $lt(f) = 3xy^3$ dir.

Tanım2.2.3: $g \neq 0$ olmak üzere; verilen $f, g, h \in k[x_1, x_2, ..., x_n]$ için $lp(g)$, f polinomunun sıfırdan farklı bir X terimini bölüyorsa ve $h = f - \frac{X}{lt(g)} \cdot g$ ise f polinomu modülo g ye göre **bir adımda** h **polinomuna indirgenir** denir ve $f \xrightarrow{g} h$ ile gösterilir.

Örnek2.2.4: $f = y^2x + 4yx - 3x^2$, $g = 2y + x + 1 \in \mathbb{Q}[x, y]$ ve $y > x$ olmak üzere sıralama deglex olsun.

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

$lp(g) = y$, $lt(g) = 2y$, $lp(g) \mid y^2x$, $X = y^2x$

$$h_1 = f - \frac{X}{lt(g)} \cdot g = y^2x + 4yx - 3x^2 - \frac{y^2x}{2y} \cdot (2y + x + 1) = -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2$$

$lp(g) = y$, $lt(g) = 2y$, $lp(g) \mid -\frac{1}{2}yx^2$, $X = -\frac{1}{2}yx^2$

$$h_2 = h_1 - \frac{X}{lt(g)} \cdot g = -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2 - \frac{-\frac{1}{2}yx^2}{2y} \cdot (2y + x + 1) = \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2$$

$lp(g) = y$, $lt(g) = 2y$, $lp(g) \mid \frac{7}{2}yx$, $X = \frac{7}{2}yx$

$$h_3 = h_2 - \frac{X}{lt(g)} \cdot g = \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2 - \frac{\frac{7}{2}yx}{2y} \cdot (2y + x + 1) = \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$$

$lp(g) = y$, $lp(g) \nmid \frac{1}{4}x^3$, $lp(g) \nmid -\frac{9}{2}x^2$, $lp(g) \nmid -\frac{7}{4}x$ olduğundan indirgeme burada biter.

Çok değişkenli durumda bir seferde birden fazla polinom tarafından bölme yapılabilir. Dolayısıyla yukarıdaki indirgeme yöntemini içeren daha genel bir tanım verilebilir.

Tanım2.2.5: f, $h \in k[x_1, x_2, ..., x_n]$ ve $1 \le i \le s$ için $f_i \neq 0$ olmak üzere $k[x_1, x_2, ..., x_n]$ halkasındaki polinomların bir kümesi $F = \{f_1, f_2, ..., f_s\}$ olsun. Eğer;

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

olacak şekilde $h_1, h_2, ..., h_{t-1} \in k[x_1, x_2, ..., x_n]$ polinomların bir dizisi ve $i_1, i_2, ..., i_t \in \{1, 2, ..., s\}$ indislerin bir dizisi varsa f polinomu modülo F ye göre h **polinomuna indirgenir** denir ve $f \xrightarrow{F}_{+} h$ ile gösterilir.

Örnek2.2.6: $f_1 = yx - y$, $f_2 = y^2 - x \in \mathbb{Q}[x, y]$ ve $y > x$ olmak üzere sıralama deglex olsun. $f = y^2x \in \mathbb{Q}[x, y]$, $F = \{f_1, f_2\}$ alalım. $f \xrightarrow{F}_{+} x$ olacağını gösterelim.

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

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

Böylece $y^2x \xrightarrow{f_1} y^2 \xrightarrow{f_2} x$ dir. Buradan $f \xrightarrow{F}_{+} x$ olur.

Tanım2.2.7: $F = \{f_1, f_2, ..., f_s\}$, $k[x_1, x_2, ..., x_n]$ deki sıfırdan farklı polinomların bir kümesi ve $r \in k[x_1, x_2, ..., x_n]$ bir polinom olsun.

$r = 0$ veya r polinomunda ortaya çıkan hiçbir terim $i = 1, 2, ..., s$ olmak üzere $lp(f_i)$ lerin herhangi biri tarafından bölünmüyorsa r polinomuna F **kümesine göre indirgenmiştir** denir. Diğer bir değişle r modülo F ye göre **indirgenemezdir** denir.

Tanım2.2.8: $f \xrightarrow{F}_{+} r$ (f modülo F ye göre indirgenmiş) ise ve r polinomu da F kümesine göre indirgenmişse r polinomuna F kümesine göre f polinomu için **kalan** denir.

İndirgeme yöntemi tek değişkenli polinom halkalarındaki bölme algoritmasına benzer bir bölme algoritması tanımlanmasını sağlar.

• $1 \le i \le s$ için $f_i \neq 0$ olmak üzere $f, f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ verildiğinde bu algoritma ile $u_1, u_2, ..., u_s \in k[x_1, x_2, ..., x_n]$ bölümler ve $r \in k[x_1, x_2, ..., x_n]$ kalan olmak üzere $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r$ bulunur.

GİRİŞ: $1 \le i \le s$ için $f_i \neq 0$ olmak üzere $f, f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ alınsın.

ÇIKIŞ: $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r$ ve $\max(lp(u_1) \cdot lp(f_1), ..., lp(u_s) \cdot lp(f_s), lp(r)) = lp(f)$ olacak şekilde $\{f_1, f_2, ..., f_s\}$ kümesine göre indirgenmiş bir r polinomu ve $u_1, u_2, ..., u_s$ polinomları istenmektedir.

BAŞLANGIÇ: $u_1 := 0$, $u_2 := 0$,..., $u_s := 0$, $r := 0$, $h := f$

DÖNGÜ: $h \neq 0$ olduğu sürece:

$lp(f_i) \mid lp(h)$ olacak şekilde i varsa o zaman $lp(f_i) \mid lp(h)$ olacak şekildeki en küçük i indisi seçilir ve

$u_i := u_i + \frac{lt(h)}{lt(f_i)}$, $h := h - \frac{lt(h)}{lt(f_i)} \cdot f_i$ işlemleri yapılır

$lp(f_i) \mid lp(h)$ olacak şekilde i yoksa aşağıdaki işlemler yapılır

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

ALGORİTMA 2.2.1 Çok Değişkenli Polinomlar İçin Bölme Algoritması

Algoritma2.2.1 de $\{f_1, f_2, ..., f_s\}$ kümesinde polinomlar arasında bir sıralama olduğu varsayılsın. O zaman $lp(f_i) \mid lp(h)$ olacak şekildeki en küçük i indisini seçeriz. Bu önemli bir noktadır ve Örnek2.2.11 de bunu göreceğiz.

Algoritma2.2.1 Çok Değişkenli Bölme Algoritması ve Algoritma1.3.1 Tek Değişkenli Bölme Algoritması arasındaki benzerlikler dikkat çekicidir. Algoritma2.2.1 deki $u_1, u_2, ..., u_s$ bölüm polinomları Algoritma1.3.1 deki tek q bölüm polinomuna karşılık gelmektedir. Algoritma2.2.1'de s tane farklı bölüm polinomu vardır. Çünkü Algoritma1.3.1'de f polinomu tek g polinomuna bölünürken Algoritma2.2.1'de f polinomu s tane farklı $f_1, f_2, ..., f_s$ polinomlarına bölünmektedir.

Her iki algoritmada kalan r olarak adlandırılır ve r polinomunun herhangi bir bölenin baş terimi tarafından bölünebilen hiçbir terimi yoktur.

Örnek2.2.9: $f_1 = yx - y$, $f_2 = y^2 - x \in \mathbb{Q}[x, y]$ olmak üzere $F = \{f_1, f_2\}$ olsun. $y > x$ olmak üzere sıralama deglex ve $f = y^2x$ olsun. $f \xrightarrow{F}_{+} r$ deki r polinomunu Algoritma2.2.1'i kullanarak bulalım.

BAŞLANGIÇ: $u_1 := 0$, $u_2 := 0$, $r := 0$, $h := f = y^2x$

1.ADIM:

$lp(f_1) = lp(yx - y) = yx$, $lp(h) = lp(y^2x) = y^2x$ ifadesini böler

$$u_1 := u_1 + \frac{lt(h)}{lt(f_1)} = 0 + \frac{y^2x}{yx} = y \qquad h := h - \frac{lt(h)}{lt(f_1)} \cdot f_1 = y^2x - \frac{y^2x}{yx}(yx - y) = y^2$$

2.ADIM:

$lp(f_1) = yx$, $lp(h) = lp(y^2) = y^2$ yi bölmez

$lp(f_2) = lp(y^2 - x) = y^2$, $lp(h) = lp(y^2) = y^2$ yi böler

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

3.ADIM:

$lp(f_1) = yx$, $lp(h) = lp(x) = x$ ifadesini bölmez

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

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

$h=0$ olduğundan algoritma tamamlanır.

$f \xrightarrow{F}_{+} r=x$ ve $f=u_1f_1+u_2f_2+r=y\cdot(yx-y)+1\cdot(y^2-x)+x$ dir. Ayrıca

$$lp(f)=\max\left(lp(u_1)\cdot lp(f_1), lp(u_2)\cdot lp(f_2), lp(r)\right)$$
$$=\max\left(y\cdot yx, 1\cdot y^2, x\right)=\max\left(y^2x, y^2, x\right)=y^2x$$

olur.

Teorem2.2.10: $F=\{f_1, f_2, ..., f_s\}\subseteq k[x_1, x_2, ..., x_n]$ sıfırdan farklı polinomların bir kümesi ve $f\in k[x_1, x_2, ..., x_n]$ verilsin. Algoritma2.2.1 den dolayı r polinomu F kümesine göre indirgenmiş olacak şekilde $\exists\, u_1, u_2, ..., u_s, r\in k[x_1, x_2, ..., x_n]$ $\ni f=u_1f_1+u_2f_2+...+u_sf_s+r$ dir. Bu durumda

$lp(f)=\max\left(\max\left(lp(u_i)\cdot lp(f_i)\right), lp(r)\right)$ olur.

(WilliamW.Adams, Philippe Loustaunau, 1994)

Örnek2.2.11: $f=y^2x-x\in\mathbb{Q}[x,y]$ polinomunu göz önüne alalım. $f_1=yx-y$, $f_2=y^2-x\in\mathbb{Q}[x,y]$ olmak üzere $I=\langle f_1, f_2\rangle\subseteq\mathbb{Q}[x,y]$ olsun. $y>x$ olmak üzere deglex sıralaması ve Algoritma2.2.1 kullanılarak $f\xrightarrow{f_1}y^2-x\xrightarrow{f_2}0$ ve $f\xrightarrow{F}_{+}0$ elde edilir.

Gerçekten $f=y\cdot f_1+f_2$ dir ve buradan $f\in I$ olur.

Ancak Algoritma2.2.1'de f_1 ve f_2 nin sırası değiştirilirse (algoritmada önce f_2 kullanılırsa) o zaman sadece $f\xrightarrow{f_2}x^2-x$ olur.

Gerçekten;

BAŞLANGIÇ: $u_1 := 0$, $u_2 := 0$, $r := 0$, $h := f = y^2x - x$

1.ADIM:

$lp(f_2) = lp(y^2 - x) = y^2$, $lp(h) = lp(y^2x - x) = y^2x$ ifadesini böler

$u_2 := u_2 + \dfrac{lt(h)}{lt(f_2)} = 0 + \dfrac{y^2x}{y^2} = x$, $h := h - \dfrac{lt(h)}{lt(f_2)} \cdot f_2 = y^2x - x - \dfrac{y^2x}{y^2}(y^2 - x) = x^2 - x$

2.ADIM:

$lp(f_2) = y^2$, $lp(h) = lp(x^2 - x) = x^2$ yi bölmez

$lp(f_1) = lp(yx - y) = yx$, $lp(h) = lp(x^2 - x) = x^2$ yi bölmez

$r := r + lt(h) = 0 + x^2 = x^2$, $h := h - lt(h) = (x^2 - x) - x^2 = -x$

3.ADIM:

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

$lp(f_1) = yx$, $lp(h) = lp(-x) = x$ ifadesini bölmez

$r := r + lt(h) = x^2 + (-x) = x^2 - x$, $h := h - lt(h) = -x - (-x) = 0$

$h = 0$ olduğundan algoritma tamamlanır.

$f = u_2 f_2 + u_1 f_1 + r = x(y^2 - x) + 0(yx - y) + (x^2 - x) = x(y^2 - x) + (x^2 - x)$

$(x^2 - x)$, F kümesine göre indirgenmiştir. Dolayısıyla $(x^2 - x)$ F kümesine göre f polinomu için bir kalandır ve sıfır değildir. Böylece f polinomunun f_1, f_2 ile bölümünden kalan sıfır olmamasına rağmen $f \in \langle f_1, f_2 \rangle = I$ dir. Dolayısıyla en küçük indisli polinomdan başlamak daha akılcı olacaktır.

III .BÖLÜM

GRÖBNER TABANLARI

3.1.Genel Tanımı

Tanım3.1.1: I , $k[x_1, x_2, ..., x_n]$ halkasının bir ideali ve $G = \{g_1, g_2, ..., g_t\}$ sıfırdan farklı polinomların bir kümesi olmak üzere $G \subseteq I$ olsun. $f \neq 0$ sağlayan her $f \in I$ için $lp(g_i)$, $lp(f)$ yi bölecek şekilde $i \in \{1, 2, ..., t\}$ varsa G kümesine I ideali için bir **Gröbner tabanı** denir.

Diğer bir değişle G , I ideali için bir Gröbner tabanı ise I idealinde G kümesine göre indirgenmiş sıfırdan farklı polinom yoktur.

Tanım3.1.2: Herhangi bir $S \subseteq k[x_1, x_2, ..., x_n]$ için $Lt(S) = \langle \{lt(s) |\ s \in S\} \rangle$ ideali tanımlanır. Bu ideale S kümesinin **baş terim ideali** denir.

Teorem3.1.3: I , $k[x_1, x_2, ..., x_n]$ halkasının sıfırdan farklı bir ideali olsun. Sıfırdan farklı polinomların bir kümesi $G = \{g_1, g_2, ..., g_t\} \subseteq I$ için aşağıdaki durumlar denktir.

(i) G , I ideali için bir Gröbner tabanıdır.

(ii) $f \in I$ olması için gerekli ve yeterli koşul $f \xrightarrow{G}_{+} 0$ olmasıdır.

(iii) $f \in I$ olması için gerekli ve yeterli koşul $lp(f) = \max_{1 \le i \le t} \left(lp(h_i) \cdot lp(g_i) \right)$ olmak üzere $f = \sum_{i=1}^{t} h_i \cdot g_i$ olmasıdır.

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

Kanıt: (i)$\Rightarrow$(ii):

G, I ideali için bir Gröbner tabanı ve $f \in k\left[x_1, x_2, ..., x_n\right]$ olsun. Teorem2.2.10 dan $f \xrightarrow{G}_{+} r$ olacak şekilde G kümesine göre indirgenmiş bir $r \in k\left[x_1, x_2, ..., x_n\right]$ elemanı vardır. Böylece $f - r \in I$ olur. Dolayısıyla $f \in I$ olması için gerekli ve yeterli koşul $r \in I$ olmasıdır. $r = 0$ ise $f \xrightarrow{G}_{+} 0$ dir. Tersine $f \in I$ ve $r \neq 0$ ise $r \in I$ olur.

(i) den $lp(g_i) \mid lp(r)$ olacak şekilde bir $i \in \{1, 2, ..., n\}$ vardır. Bu r polinomunun G kümesine göre indirgenmiş olması ile çelişir. Böylece $r = 0$ olmalıdır. Yani $f \xrightarrow{G}_{+} 0$ dır.

(ii)$\Rightarrow$(iii):

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

$$f \in I \Leftrightarrow f \xrightarrow{G}_{+} 0 \underset{Teorem2.2.10}{\Leftrightarrow} f = \sum_{i=1}^{t} h_i \cdot g_i \,,\; lp(f) = \max_{1 \le i \le t} \left(lp(h_i) \cdot lp(g_i) \right)$$

(iii)$\Rightarrow$(iv):

$$x \in Lt(G) \Rightarrow \forall\, g_i \in G \;\; ve \;\; \exists\, a_i \in k \;\; için \;\; x = \sum_{i=1}^{t} a_i \cdot lt(g_i)$$

$$\underset{G \subseteq I}{\Rightarrow} \exists\, g_i \in I \;\; ve \;\; \exists\, a_{i \in} k \;\; için \;\; x = \sum_{i=1}^{t} a_i \cdot lt(g_i) \Rightarrow x \in Lt(I)$$

$Lt(G) \subseteq Lt(I)$ olur.

Diğer taraftan $f \in I$ için $lt(f)$ ler $Lt(I)$ nın üreteçleri olduğundan her $f \in I$ için $lt(f) \in Lt(G)$ olduğunu göstermek yeterlidir. Varsayımımızdaki gibi $f = \sum_{i=1}^{t} h_i \cdot g_i$ olarak yazılan her f polinomu için $lt(f) = \sum_{i=1}^{t} lt(h_i) \cdot lt(g_i)$ dir. Buradan $lt(f) \in Lt(G)$ olur. Böylece $Lt(I) \subseteq Lt(G)$ dir. $Lt(G) = Lt(I)$ bulunur.

(iv)$\Rightarrow$(i):

$f \in I$ ise $lt(f) \in Lt(G)$ dir. Buradan $lt(f) = \sum_{i=1}^{t} h_i \cdot lt(g_i)$, $h_i \in k[x_1, x_2, ..., x_n]$ olur. Toplam ifadesi açılırsa toplamdaki her bir terimin en az bir $lp(g_i)$ tarafından bölündüğü görülür. Böylece eşitliğin sol tarafındaki tek terim olan $lt(f)$ en az bir $lp(g_i)$ tarafından bölünür. Buradan Gröbner tabanı tanımına gelinmiş olur. Sonuç olarak G kümesi I idealinin bir Gröbner tabanı olur. □

Sonuç3.1.4: $G = \{g_1, g_2, ..., g_t\}$ kümesi I ideali için bir Gröbner tabanı ise $I = \langle g_1, g_2, ..., g_t \rangle$ dir.

Kanıt: $G \subseteq I$ olduğu açıktır. Her bir $i = 1, 2, ..., t$ için $g_i \in I$ olduğundan $\langle g_1, g_2, ..., g_t \rangle \subseteq I$ dır.

$f \in I$ olsun. Teorem3.1.3 den $f \xrightarrow{G}_{+} 0$ dır. Buradan $f \in \langle g_1, g_2, ..., g_t \rangle$ olur. Böylece $I \subseteq \langle g_1, g_2, ..., g_t \rangle$ dir. Dolayısıyla $I = \langle g_1, g_2, ..., g_t \rangle$ bulunur. □

Lemma3.1.5: $f \in k[x_1, x_2, ..., x_n]$ ve I ideali sıfırdan farklı terimlerin bir S kümesi tarafından üretilmiş olsun.

$f \in I$ olması için gerekli ve yeterli koşul f polinomunda ortaya çıkan her X terimi için $Y \mid X$ olacak şekilde bir $Y \in S$ var olmasıdır. Ayrıca $I = \langle S_0 \rangle$ olacak şekilde S kümesinin sonlu bir S_0 alt kümesi vardır.

Kanıt: $\Rightarrow$: $I = \langle S \rangle$ olsun.

$f \in I \Rightarrow f = \sum_{i=}^{t} h_i \cdot X_i$, $i = 1, 2, ..., t$ *için* $h_i \in k[x_1, x_2, ..., x_n]$, $X_i \in S$ dir. Toplam ifadesi açılırsa toplam ifadesindeki her terimin S kümesindeki en az bir X_i terimi tarafından bölünebildiği görülür. Bu durumda aynı zamanda eşitliğin sol tarafındaki polinomun her terimi en az bir $X_i \in S$ tarafından bölünmek zorunda kalır.

$\Leftarrow$: f polinomunda ortaya çıkan her bir X terimi için $Y|X$ olacak şekilde bir $Y \in S$ terimi var olsun.

$Y|X \Rightarrow \exists\, Z \in k[x_1, x_2, ..., x_n]$ ə $X = Y.Z \underset{Y \in S}{\Rightarrow} X \in I = \langle S \rangle$ olur. Buradan $f \in I$ bulunur.

Son durumu kanıtlamak için; Hilbert Taban Teoremi'nden I sonlu bir üreteç kümesine sahiptir. Lemma'nın birinci kısmından üreteç kümesinin elemanı olan her bir terim S kümesinin bir elemanı tarafından bölünür. Bölenlerin sonlu kümesi S_0 olmak üzere $I = \langle S_0 \rangle$ olur. □

Sonuç3.1.6: $k[x_1, x_2, ..., x_n]$ halkasının sıfırdan farklı her ideali bir Gröbner tabanına sahiptir.

Kanıt: Lemma3.1.5 den baş terim ideali $Lt(I)$ sonlu bir üreteç kümesine sahiptir. $g_1, g_2, ..., g_t \in I$ olmak üzere bu kümenin $\{lt(g_1), lt(g_2), ..., lt(g_t)\}$ olduğunu varsayalım. $G = \{g_1, g_2, ..., g_t\}$ ise $Lt(G) = Lt(I)$ dır. Teorem3.1.3 den G kümesi I ideali için bir Gröbner tabanıdır. □

Önerme3.1.7: $G = \{g_1, g_2, ..., g_t\} \subseteq k[x_1, x_2, ..., x_n]$ kümesinin bir Gröbner tabanı olması için gerekli ve yeterli koşul $\langle G \rangle$ ideali için bir Gröbner tabanı olmasıdır.

(William W. Adams, Philipe Loustaunau, 1994)

Teorem3.1.8: $G = \{g_1, g_2, ..., g_t\}$, $k[x_1, x_2, ..., x_n]$ halkasındaki sıfırdan farklı polinomların bir kümesi olsun.

G nin bir Gröbner tabanı olması için gerekli ve yeterli koşul $\forall f \in k[x_1, x_2, ..., x_n]$ için f polinomunun G kümesine bölümünden kalanın tek olmasıdır.

Kanıt: $\Rightarrow$: G bir Gröbner tabanı olsun.

r_1 ve r_2 polinomları G kümesine göre indirgenmiş olmak üzere $f \xrightarrow{G}_+ r_1$ ve $f \xrightarrow{G}_+ r_2$ olsun. Buradan $f - r_1, f - r_2 \in \langle G \rangle = \langle g_1, g_2, ..., g_t \rangle$ olur.

Böylece $f-r_2-(f-r_1)=r_2-r_1\in\langle G\rangle$ dir. G kümesi $\langle G\rangle$ ideali için Gröbner tabanı olduğundan $r_2-r_1\in\langle G\rangle$ dir.

$r_2-r_1\in\langle G\rangle$ olduğundan Teorem3.1.3'ten $r_2-r_1\xrightarrow{G}_+0$ dir.

Ayrıca r_2-r_1 polinomu G kümesine göre indirgenmiştir. Buradan $r_2-r_1=0$ olmalıdır. Böylece $r_2=r_1$ bulunur.

$\Leftarrow:\forall f\in k[x_1,x_2,...,x_n]$ için f polinomunun G kümesine bölümünden kalan tek olsun. Şimdi G kümesinin $\langle G\rangle$ ideali için bir Gröbner tabanı olduğu gösterilecektir. Bunun için Teorem3.1.3 (ii) durumu kanıtlanacaktır.

$f\in\langle G\rangle$ olsun. r polinomu G kümesine göre indirgenmiş olmak üzere $f\xrightarrow{G}_+r$ olduğunu varsayalım. $r=0$ olduğu gösterilmelidir.

İddia: $0\neq c\in k$, $X\in T^n$ bir kuvvet çarpımı ve r polinomu $G=\{g_1,g_2,...,g_t\}$ kümesine göre indirgenmiş bir polinom olmak üzere $g\in k[x_1,x_2,...,x_n]$ polinomu $g\xrightarrow{G}_+r$ sağlıyorsa her bir $i\in\{1,2,...,t\}$ için $g-c\cdot X\cdot g_i\xrightarrow{G}_+r$ dir.

İddianın doğru olduğu varsayılarak aşağıdaki işlemler yapılabilir.

$f\in\langle G\rangle$ olduğundan $f=\sum_{\nu=1}^{l}c_\nu\cdot X_\nu\cdot g_{i_\nu}$ yazılabilir. Burada $0\neq c_\nu\in k$, $X_\nu\in T^n$ ve her bir $i_\nu\in\{1,2,...,t\}$ dir. O zaman $g=f$ ye iddia uygulansın.

$f-c_1\cdot X_1\cdot g_{i_1}\xrightarrow{G}_+r$ olduğu iddiadan görülür.

Şimdi $f-c_1\cdot X_1\cdot g_{i_1}-c_2\cdot X_2\cdot g_{i_2}\xrightarrow{G}_+r$ yi elde etmek için iddia $q=f-c_1\cdot X_1\cdot g_{i_1}$ polinomuna uygulanabilir.

Aynı şekilde $f - c_1 \cdot X_1 \cdot g_{i_1} - c_2 \cdot X_2 \cdot g_{i_2} - c_3 \cdot X_3 \cdot g_{i_3} \xrightarrow{G}_+ r$ olduğunu görmek için iddia $h = f - c_1 \cdot X_1 \cdot g_{i_1} - c_2 \cdot X_2 \cdot g_{i_2}$ polinomuna uygulanabilir. Bu şekilde devam edilerek $f - c_1 \cdot X_1 \cdot g_{i_1} - c_2 \cdot X_2 \cdot g_{i_2} - ... - c_l \cdot X_l \cdot g_{i_l} \xrightarrow{G}_+ r$ olduğu elde edilir.

Yani $f - \sum_{\nu=1}^{l} c_\nu \cdot X_\nu \cdot g_{i_\nu} \xrightarrow{G}_+ r$ dir. Buradan $f - f = 0 \xrightarrow{G}_+ r$ olur. Böylece $r = 0$ olarak bulunur.

Sonuç olarak $f \in \langle G \rangle \Rightarrow f \xrightarrow{G}_+ 0$ olduğu görülür. Tersine $f \xrightarrow{G}_+ 0$ ise $f \in \langle G \rangle$ dir. O halde G Gröbner tabanıdır. □

İddianın Kanıtı: g polinomunda $X \cdot lp(g_i)$ nin katsayısı olarak $d \cdot lc(g_i)$ sağlayan $d \in k$ tanımlansın. Üç durum göz önüne alınacaktır.

1.Durum: $d = 0$ ise;

Bu durumda $g - c \cdot X \cdot g_i$ deki $X \cdot lp(g_i)$ nin katsayısı $-c \cdot lc(g_i)$ dir. $c \neq 0$ olduğundan $-c \cdot lc(g_i) \neq 0$ dır. Dolayısıyla $g - c \cdot X \cdot g_i \xrightarrow{g_i} g \xrightarrow{G}_+ r$ olur.

2.Durum: $d = c$ ise;

r_1 polinomu G ye göre indirgenmiş olsun. $g - c \cdot X \cdot g_i \xrightarrow{G}_+ r_1$ olduğunu varsayalım. O zaman $d = c \neq 0$ olduğundan $g \xrightarrow{g_i} g - c \cdot X \cdot g_i \xrightarrow{G}_+ r_1$ olduğu görülür.(Bir f polinomunu indirgerken $f \xrightarrow{f_1} h = f - \frac{X}{lt(f_1)} \cdot f_1$ yazılışından esinlenilmiştir). Aynı zamanda $g \xrightarrow{G}_+ r$ olduğundan ve kalan tek olduğundan $r = r_1$ bulunur. Dolayısıyla $g - c \cdot X \cdot g_i \xrightarrow{G}_+ r$ olur.

3.Durum: $d \neq 0$ ve $d \neq c$ ise;

$h = g - d \cdot X \cdot g_i$ olsun. O zaman g deki $X \cdot lp(g_i)$ nin katsayısı $d \cdot lc(g_i)$ ve $d \cdot X \cdot g_i$ deki $X \cdot lp(g_i)$ nin katsayısı $d \cdot lc(g_i)$ olduğundan h daki $X \cdot lp(g_i)$ nin katsayısı sıfırdır.

$h = g - d \cdot X \cdot g_i$ ise $g = h + d \cdot X \cdot g_i$ dir. $d \neq 0$ olduğundan $g \xrightarrow{g_i} h$ dir. Aynı zamanda $d \neq c$ olduğundan $g - c \cdot X \cdot g_i \xrightarrow{g_i} h$ olur. Dolayısıyla r_2 polinomu G kümesine göre indirgenmiş olacak şekilde $h \xrightarrow{G}_+ r_2$ ise $g \xrightarrow{g_i} h \xrightarrow{G}_+ r_2$ olur. Buradan $g \xrightarrow{G}_+ r_2$ kalanın tek olduğu varsayımından $r_2 = r$ olur. O halde $h \xrightarrow{G}_+ r$ dir.

Buradan $g - c \cdot X \cdot g_i \xrightarrow{g_i} h \xrightarrow{G}_+ r$ bulunur ve iddianın kanıtı biter. □

Örnek3.1.9: $f = y^2x - x$, $f_1 = yx - x$, $f_2 = y^2 - x \in \mathbb{Q}[x, y]$ olsun. $F = \{f_1, f_2\}$ ve $y > x$ olmak üzere sıralama deglex olsun.

Örnek2.2.11'de $f \xrightarrow{F}_+ 0$ ve $f \xrightarrow{F}_+ x^2 - x$ olduğu gösterilmişti. $x^2 - x$ polinomu F kümesine göre indirgenmiştir. Böylece Teorem3.1.8 den F kümesi Gröbner tabanı değildir. Bunu başka yolla da gösterebiliriz.

$f = y \cdot f_1 + f_2 \in \langle f_1, f_2 \rangle$ olduğu biliniyor.

Ayrıca $f \xrightarrow{F}_+ x^2 - x$ olduğundan $f = x \cdot f_2 + (x^2 - x)$ dir. Buradan $x^2 - x = f - x \cdot f_2$ olur. $x^2 - x = f - x \cdot f_2 \in \langle f_1, f_2 \rangle$ bulunur. Fakat $lp(x^2 - x) = x^2$ ifadesi $lp(f_1) = xy$ veya $lp(f_2) = y^2$ terimlerinin herhangi biri tarafından bölünemez. Böylece Gröbner tabanı tanımından F kümesi $\langle f_1, f_2 \rangle$ ideali için bir Gröbner tabanı değildir.

Örnek3.1.10: $g_1 = z + x$, $g_2 = y - x$, $\in \mathbb{Q}[x, y, z]$ polinomlarını göz önüne alalım. $G = \{g_1, g_2\}$ ve $I = \langle g_1, g_2 \rangle$ olsun. $\mathbb{Q}[x, y, z]$ üzerinde $z > y > x$ olmak üzere lex sıralamasını kullanalım. G kümesinin I ideali için Gröbner tabanı olduğunu gösterelim.

$lt(g_1) = z$, $lt(g_2) = y$ ve $Lt(G) = \langle lt(g_1), lt(g_2) \rangle$ dir. $Lt(G) = Lt(I)$ eşitliğini görmemiz gerekir. $Lt(G) \subseteq Lt(I)$ olduğu açıktır.

$f \in I$ için herhangi bir $lt(f) \in Lt(I)$ alalım.

$lt(f) \notin Lt(G) = \langle lt(g_1), lt(g_2) \rangle = \langle z, y \rangle$ olacak şekilde bir $f \in I$ olduğunu varsayalım. O zaman $lt(f)$ ifadesi z ve y değişkenleri tarafından bölünemez. Böylece terim sıralaması lex olduğundan dolayı z ve y değişkenleri f polinomunun hiçbir teriminde gözükmez. Dolayısıyla f, sadece x değişkenine bağlı bir polinom olur. Yani $f \in \mathbb{Q}[x]$ olur.

$f \in I = \langle g_1, g_2 \rangle$ olduğundan

$\exists\, h_1(x,y,z), h_2(x,y,z) \in \mathbb{Q}[x,y,z]$ ∋ $f = (z+x) \cdot h_1(x,y,z) + (y-x) \cdot h_2(x,y,z)$ dir. f polinomunda y değişkeni olmadığından yukarıdaki f polinomu ifadesinde y değişkeni yerine x değişkenini yazmak sorun yaratmaz. Böylece $f = (z+x) \cdot h_1(x,x,z) + (x-x) \cdot h_2(x,x,z)$ olur. Buradan $f = (z+x) \cdot h_1(x,x,z)$ ve $(z+x) \mid f$ dir. Bu ifade f polinomunun sadece x değişkenine bağlı olması ile çelişir. Bu $lt(f) \in Lt(I)$ iken $lt(f) \notin Lt(G)$ olmasından kaynaklanır. O halde $Lt(I) \subseteq Lt(G)$ olur.

Böylece $Lt(I) = Lt(G)$ dir ve G kümesi I ideali için bir Gröbner tabanıdır.

•• Herhangi bir I idealinin $G = \{g_1, g_2, ..., g_t\}$ gibi bir Gröbner tabanı olduğunu varsayalım. Bir f polinomunun I idealinde olup olmadığına karar vermek için Algoritma2.2.1 kullanılarak f polinomu G kümesine göre indirgenir(bölünür) ve bir kalan bulunur. $f \in I$ olması için gerekli ve yeterli koşul bu kalanın sıfır olmasıdır.

$f \in I$ ise Teorem2.2.10'daki gibi $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s$ olacak şekilde $u_1, u_2, ..., u_s \in k[x_1, x_2, ..., x_n]$ polinomlarını Algoritma2.2.1 yardımıyla bulunur.

Not: Bir terim sıralamasına göre Gröbner tabanı olan küme farklı bir terim sıralamasına göre Gröbner tabanı olmayabilir.

Örneğin; Örnek3.1.10'da $x > y > z$ olmak üzere lex sıralaması kullanılırsa G kümesi I ideali için Gröbner tabanı olmaz.

Bu kısımdaki sonuçlar Gröbner tabanının varlığını kanıtlamak içindi. Bu sonuçların kanıtları Gröbner tabanlarını bulmak için herhangi bir metod olduğu anlamına gelmez. Gelecek kısımda Gröbner tabanının nasıl hesaplanacağı gösterilecektir.

3.2 S-Polinomları Ve Buchberger Algoritması

Bu bölümde S-Polinomları tanımlanacak, ardından Buchberger Teoremi verilecektir. Bunlar yardımıyla da Gröbner tabanı elde etmek için bir algoritma belirlenecektir.

Tanım3.2.1: $0 \neq f$, $g \in k[x_1, x_2, ..., x_n]$ ve $L = lcm(lp(f_1), lp(f_2))$ olsun.

$S(f,g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$ polinomuna f ve g nin **S-Polinomu** denir.

Örnek3.2.2: $f = 2yx - y, g = 3x^2 - x \in \mathbb{Q}[x,y]$ ve $y > x$ olmak üzere sıralama deglex olsun.

$lp(f) = yx$, $lt(f) = 2yx$, $lp(g) = y^2$, $lt(g) = 3y^2$ ve $L = lcm(yx, y^2) = y^2x$ dir.

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

$S(f,g) = \frac{1}{2}y^2 + \frac{1}{3}x^2$ olur. Burada $lp\left(\frac{1}{2}y \cdot f\right) = y^2x = lp\left(\frac{1}{3}x \cdot g\right)$ terimi $S(f,g)$ de yok edilmiştir.

S-Polinomlarını elde etmenin başka bir yolu daha vardır. Yani; f polinomunun $f_1, f_2, ..., f_s$ tarafından bölünmesinde f polinomunda $i \neq j$ için $lp(f_i)$ ve $lp(f_j)$ nin her ikisi tarafından bölünebilen bazı X terimleri ortaya çıkabilir. Buradan X, $L = (lp(f_i), lp(f_j))$ tarafından bölünebilir.

f polinomu f_i kullanılarak indirgenirse $h_1 = f - \frac{X}{lt(f_i)} \cdot f_i$ elde edilir.

f polinomu f_j kullanılarak indirgenirse $h_2 = f - \frac{X}{lt(f_j)} \cdot f_j$ elde edilir.

$h_2 - h_1 = \frac{X}{lt(f_j)} \cdot f_j - \frac{X}{lt(f_i)} \cdot f_i = \frac{X}{L} \cdot S(f_i, f_j)$ olur.

Örnek3.2.3: $f = y^2x + 1$, $f_1 = yx - y$, $f_2 = y^2 - x \in \mathbb{Q}[x, y]$ ve $y > x$ olmak üzere sıralama deglex olsun. f polinomundaki $X = y^2x$ terimini göz önüne alalım.

$f \xrightarrow{f_1} y^2 + 1 = f - y \cdot f_1$ ve $f \xrightarrow{f_2} x^2 + 1 = f - x \cdot f_2$ dir.

$X = L = lcm(lp(f_1), lp(f_2)) = lcm(yx, y^2) = y^2x$ dir.

$(x^2 + 1) - (y^2 + 1) = -y^2 + x^2 = y \cdot f_1 - x \cdot f_2 = S(f_1, f_2)$ dir.

Aynı zamanda $S(f_1, f_2) \in \langle f_1, f_2 \rangle$ dir. $S(f_1, f_2) \xrightarrow{f_2} x^2 - x$ olur ve $x^2 - x$ polinomu $\{f_1, f_2\}$ kümesine göre indirgenmiştir.

Lemma3.2.4: $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$ ve $\forall i = 1, 2, ..., s$ için $lp(f_i) = X \neq 0$ olsun. $\forall i = 1, 2, ..., s$ için $c_i \in k$ olmak üzere $f = \sum_{i=1}^{s} c_i \cdot f_i$ olsun. Eğer $lp(f) < X$ ise f polinomu, k cismindeki katsayılar ve $1 \leq i < j \leq s$ için $S(f_i, f_j)$ polinomlarının bir doğrusal kombinasyonudur.

Kanıt: $lp(f) < X$ olsun. $a_i \in k$ olmak üzere $f_i = a_i X + daha\ küçük\ terimler$ şeklinde yazılır. O zaman hipotezden

$$\left.\begin{aligned} f_1 &= a_1 X + daha\ küçük\ terimler \\ f_2 &= a_2 X + daha\ küçük\ terimler \\ &\vdots \\ f_s &= a_s X + daha\ küçük\ terimler \end{aligned}\right\} (*)$$

$$f=\sum_{i=1}^{s}c_i\cdot f_i=c_1\cdot f_1+c_2\cdot f_2+\ldots+c_s\cdot f_s$$

$$\underset{(*)dan}{\Rightarrow}\quad f=c_1\left(a_1X+\textit{daha küçük terimler}\right)+\ldots+c_s\left(a_sX+\textit{daha küçük terimler}\right)$$

$$\Rightarrow f=c_1a_1X+\ldots+c_sa_sX+\textit{daha küçük terimler}$$

$$\Rightarrow f=\left(c_1a_1+\ldots+c_sa_s\right)X+\textit{daha küçük terimler}$$

$lp(f)<X$ olduğundan X teriminin katsayısı $c_1a_1+\ldots+c_sa_s=0$ olmalıdır. Dolayısıyla $\forall i=1,2,\ldots,s$ için $c_i\in k$ olmak üzere $\sum_{i=1}^{s}c_i\cdot a_i=0$ olur.

$lp(f_i)=lp(f_j)=X$ olduğundan $L=lcm\left(lp(f_i),lp(f_j)\right)=X=lp(f_i)=lp(f_j)$ dir.

$$S(f_i,f_j)=\frac{L}{lt(f_i)}\cdot f_i-\frac{L}{lt(f_j)}\cdot f_j=\frac{lp(f_i)}{lt(f_i)}\cdot f_i-\frac{lp(f_j)}{lt(f_j)}\cdot f_j$$

$$=\frac{lp(f_i)}{a_i\cdot lp(f_i)}\cdot f_i-\frac{lp(f_j)}{a_j\cdot lp(f_j)}\cdot f_j$$

$$=\frac{1}{a_i}\cdot f_i-\frac{1}{a_j}\cdot f_j$$

bulunur.

Böylece $f=c_1\cdot f_1+c_2\cdot f_2+\ldots+c_s\cdot f_s$

$$f=c_1a_1\left(\frac{1}{a_1}\cdot f_1\right)+c_2a_2\left(\frac{1}{a_2}\cdot f_2\right)+\ldots+c_sa_s\left(\frac{1}{a_s}\cdot f_s\right)$$

$$f=c_1a_1\left(\frac{1}{a_1}\cdot f_1-\frac{1}{a_2}\cdot f_2\right)+\left(c_1a_1+c_2a_2\right)\left(\frac{1}{a_2}\cdot f_2-\frac{1}{a_3}\cdot f_3\right)+\ldots$$

$$+\left(c_1a_1+c_2a_2+\ldots+c_{s-1}a_{s-1}\right)\left(\frac{1}{a_{s-1}}\cdot f_{s-1}-\frac{1}{a_s}\cdot f_s\right)+\left(c_1a_1+c_2a_2+\ldots+c_sa_s\right)\left(\frac{1}{a_s}\cdot f_s\right)$$

$c_1a_1 + c_2a_2 + ... + c_sa_s = 0$ olduğundan

$$f = c_1a_1\left(\frac{1}{a_1}\cdot f_1 - \frac{1}{a_2}\cdot f_2\right) + \left(c_1a_1 + c_2a_2\right)\left(\frac{1}{a_2}\cdot f_2 - \frac{1}{a_3}\cdot f_3\right) + ...$$
$$+ \left(c_1a_1 + c_2a_2 + ... + c_{s-1}a_{s-1}\right)\left(\frac{1}{a_{s-1}}\cdot f_{s-1} - \frac{1}{a_s}\cdot f_s\right)$$

$$f = c_1a_1S\left(f_1, f_2\right) + \left(c_1a_1 + c_2a_2\right)S\left(f_2, f_3\right) + ... + \left(c_1a_1 + c_2a_2 + ... + c_{s-1}a_{s-1}\right)S\left(f_{s-1}, f_s\right)$$
$$f = \underbrace{c_1a_1}_{\in k}\, S\left(f_1, f_2\right) + \underbrace{\left(c_1a_1 + c_2a_2\right)}_{\in k}S\left(f_2, f_3\right) + ... + \underbrace{\left(c_1a_1 + c_2a_2 + ... + c_{s-1}a_{s-1}\right)}_{\in k}S\left(f_{s-1}, f_s\right)$$

elde edilir.

Teorem3.2.5 (BUCHBERGER): $G = \{g_1, g_2, ..., g_t\}$, $k[x_1, x_2, ..., x_n]$ halkasındaki sıfırdan farklı polinomların bir kümesi ve $I = \langle g_1, g_2, ..., g_t\rangle$, $k[x_1, x_2, ..., x_n]$ nin sıfırdan farklı bir ideali olsun.

G kümesi I ideali için Gröbner tabanıdır. $\Leftrightarrow \forall i \neq j$ için $S\left(g_i, g_j\right) \xrightarrow{G}_{+} 0$ dir.

Kanıt: $\Rightarrow$:

$G = \{g_1, g_2, ..., g_t\}$ kümesi $I = \langle g_1, g_2, ..., g_t\rangle$ idealinin Gröbner tabanı olsun.

S-Polinomu tanımından $\forall i \neq j$ için $S\left(g_i, g_j\right) \in I = \langle g_1, g_2, ..., g_t\rangle$ dir. Böylece Teorem3.1.3 (ii) den $\forall i \neq j$ için $S\left(g_i, g_j\right) \xrightarrow{G}_{+} 0$ olur.

$\Leftarrow$: $\forall i \neq j$ için $S\left(g_i, g_j\right) \xrightarrow{G}_{+} 0$ olsun. G nin $I = \langle g_1, g_2, ..., g_t\rangle$ için bir Gröbner tabanı olduğu gösterilecektir. Bunun için Teorem3.1.3 kullanacağız.

$f \in I$ olsun. O zaman f polinomu g_i polinomlarının bir doğrusal bileşimi olarak yazılır. G nin Gröbner tabanı olması için $X = \max_{1\le i\le t}\left(lp\left(h_i\right)\cdot lp\left(g_i\right)\right)$ olduğu gösterilmelidir.

$lp\left(f\right) = X$ ise Teorem3.1.3 den G kümesi, $I = \langle g_1, g_2, ..., g_t\rangle$ için Gröbner tabanıdır.

Aksi takdirde $lp(f) < X$ dir.

$S = \{i \mid lp(h_i) \cdot lp(g_i) = X\}$ olsun. $i \in S$ için $h_i = c_i \cdot X_i + \textit{daha küçük terimler}$

olmak üzere

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

$\forall i \in S$ için $lp(X_i \cdot g_i) = lp(X_i) \cdot lp(g_i) = lp(h_i) \cdot lp(g_i) = X$ dir. Fakat $lp(g) < X$ dir.

Lemma3.2.4 den $g = \sum_{\substack{i,j \in s \\ i \neq j}} d_{ij} \cdot S(X_i \cdot g_i, X_j \cdot g_j)$ olacak şekilde $d_{ij} \in k$ vardır.

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

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X}{lt(X_i \cdot g_i)} \cdot X_i \cdot g_i - \frac{X}{lt(X_j \cdot g_j)} \cdot X_j \cdot g_j$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X}{lt(X_i) lt(g_i)} \cdot X_i \cdot g_i - \frac{X}{lt(X_j) lt(g_j)} \cdot X_j \cdot g_j$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X}{X_i lt(g_i)} \cdot X_i \cdot g_i - \frac{X}{X_j lt(g_j)} \cdot X_j \cdot g_j \qquad \begin{pmatrix} lt(X_i) = X_i \text{ , } lt(X_j) = X_j \\ \textit{olduğundan} \end{pmatrix}$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X}{lt(g_i)} \cdot g_i - \frac{X}{lt(g_j)} \cdot g_j$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = X \left(\frac{1}{lt(g_i)} \cdot g_i - \frac{1}{lt(g_j)} \cdot g_j \right)$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X_{ij} \cdot X}{X_{ij}} \left(\frac{1}{lt(g_i)} \cdot g_i - \frac{1}{lt(g_j)} \cdot g_j \right)$$

$$S(X_i \cdot g_i, X_j \cdot g_j) = \frac{X}{X_{ij}} \left(\frac{X_{ij}}{lt(g_i)} \cdot g_i - \frac{X_{ij}}{lt(g_j)} \cdot g_j \right)$$

$S\left(X_i \cdot g_i, X_j \cdot g_j\right) = \frac{X}{X_{ij}} \cdot S\left(g_i, g_j\right)$ bulunur. Burada $X_{ij} = lcm\left(lp\left(g_i\right), lp\left(g_j\right)\right)$ dir.

Böylece $S\left(g_i, g_j\right) \xrightarrow{G}_{+} 0$ olduğundan $S\left(X_i \cdot g_i, X_j \cdot g_j\right) \xrightarrow{G}_{+} 0$ olur. Bu $S\left(X_i \cdot g_i, X_j \cdot g_j\right) = \sum_{\nu=1}^{t} h_{ij\nu} \cdot g_\nu$ olarak gösterilebilir.

Teorem2.2.10 dan $lp\left(S\left(X_i \cdot g_i, X_j \cdot g_j\right)\right) = \max_{1 \le \nu \le t}\left(lp\left(h_{ij\nu}\right) \cdot lp\left(g_\nu\right)\right)$ dir.

$$\max_{1 \le \nu \le t}\left(lp\left(h_{ij\nu}\right) \cdot lp\left(g_\nu\right)\right) = lp\left(S\left(X_i \cdot g_i, X_j \cdot g_j\right)\right) < \max\left(lp\left(X_i \cdot g_i\right), lp\left(X_j \cdot g_j\right)\right) = X$$

$f = \sum_{i=1}^{t} h_i' \cdot g_i$ ve $lp(f) = \max_{1 \le \nu \le t}\left(lp\left(h_i'\right) \cdot lp\left(g_i\right)\right) < X$ dir.□

Sonuç3.2.6: $\forall i = 1,2,..,t$ için $g_i = 0$ olmak üzere $G = \{g_1, g_2, ..., g_t\}$ olsun. O zaman

$$G \text{ bir Gröbner tabanıdır} \Leftrightarrow \begin{cases} \forall i \neq j \ \ (1 \le i, j \le t) \ \ için \ \ S\left(g_i, g_j\right) = \sum_{\nu=1}^{t} h_{ij\nu} \cdot g_\nu \\ lp\left(S\left(g_i, g_j\right)\right) = \max_{1 \le \nu \le t}\left(lp\left(h_{ij\nu}\right) \cdot lp\left(g_\nu\right)\right) \ \ olmasıdır. \end{cases}$$

(William W. Adams, Philipe Loustaunau, 1994)

Not: Buchberger teoremi Gröbner tabanlarını hesaplamak için bir yol verir:

Bu yolla önce S-Polinomları indirgenir ve bir kalan bulunur. Bu kalan sıfır değilse üreteç kümesindeki polinomların yanına eklenir. Bu işlem tüm S-Polnomlarının indirgenmesinden sıfır polinomu bulunana kadar yapılır.

Örnek3.2.7: $f_1 = xy - x$, $f_2 = x^2 - y \in \mathbb{Q}[x, y]$ ve $x < y$ olmak üzere terim sıralaması deglex olsun. $F = \{f_1, f_2\}$ olsun. $\langle f_1, f_2 \rangle$ ideali için bir Gröbner tabanı bulalım.

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

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

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

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

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

f_3 polinomu F kümesine göre indirgenmiştir ve sıfırdan farklıdır. Dolayısıyla F kümesine eklenir. $F' = \{f_1, f_2, f_3\}$ olur. Bu durumda $S(f_1, f_2) \xrightarrow{F'}_{+} 0$ olur.

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

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

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

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

$lp(f_1) = xy$, $x^2 y$ yi böler

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

$lp(f_2) = x^2$, x^2 yi böler

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

$lp(f_3) = y^2$, $-y^2$ yi böler

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

$lp(f_3) = y^2$, $-y^2$ yi böler

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

Böylece $S(f_2, f_3) \xrightarrow{F'}_{+} 0$ olur. Bütün S-Polinomları sıfıra indirgenmiştir. Dolayısıyla $F' = \{f_1, f_2, f_3\}$ kümesi $\langle f_1, f_2 \rangle$ ideali için bir Gröbner tabanı olur.

GİRİŞ: $F = \{f_1, f_2, ..., f_s\} \subseteq k[x_1, x_2, ..., x_n]$, $f_i = 0$ $(1 \le i \le s)$ alınsın.

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

BAŞLANGIÇ: $G := F$, $\mathfrak{G} = \{\{f_i, f_j\} | \ f_i \neq f_j \ , \ f_i, f_j \in G\}$

DÖNGÜ: $\mathfrak{G} :\neq \varnothing$ olduğu sürece aşağıdaki işlemler yapılır

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

$\mathfrak{G} := \mathfrak{G} - \{\{f, g\}\}$

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

$h \neq 0$ ise aşağıdaki işlemler yapılır

$\mathfrak{G} := \mathfrak{G} \cup \{\{u, h\} | \ \forall u \in G \ için\}$

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

ALGORİTMA 3.2.1 Gröbner Tabanları İçin Buchberger Algoritması

Teorem3.2.8: $\forall i = 1, 2, ..., s$ için $f_i \neq 0$ olmak üzere $F = \{f_1, f_2, ..., f_s\}$ verisin. Buchberger Algoritması(Algoritma3.2.1) $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için bir Gröbner tabanı verir.

Kanıt: Öncelikle bu algoritmanın sonlu olduğunu görmek gerekir. Algoritmanın sonlu olmadığını varsayalım. O zaman algoritmanın aşamalarından G_{i-1} den daha büyük olan G_i kümeleri oluşturulur. Böylece $G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq .....$ artan sonsuz dizisini elde edilir.

Her bir G_i kümesi, G_{i-1} kümesine bazı $h \in I$ polinomları eklenerek G_{i-1} kümesinden elde edilen kümedir.

Burada $h \neq 0$ polinomu, G_{i-1} kümesinin iki elemanının S-Polinomunun G_{i-1} kümesine göre indirgenmesiyle elde edilen bir polinomdur. $\left(S(f_1, f_2) \xrightarrow{G_{i-1}} h \neq 0 \right)$

h polinomu G_{i-1} kümesine göre indirgenmiş olduğundan $lt(h) \notin Lt(G_{i-1})$ olur. Böylece $Lt(G_1) \underset{\neq}{\subset} Lt(G_2) \underset{\neq}{\subset} Lt(G_3) \underset{\neq}{\subset} .....$ elde edilir. Bu, ideallerin artan bir zinciridir. Bu zincir Hilbert Taban Teoremi ile çelişir. Dolayısıyla bu algoritma sonludur.

$F \subseteq G \subseteq I$ olduğu biliniyor.

$F = \{f_1, f_2, ..., f_s\} \subseteq \{g_1, g_2, ..., g_t\} = G$ olduğundan $\langle f_1, f_2, ..., f \rangle \subseteq \langle g_1, g_2, ..., g_t \rangle$ olur. $G \subseteq I$ olduğundan $\langle g_1, g_2, ..., g_t \rangle \subseteq I$ olur.

Buradan $I = \langle f_1, f_2, ..., f \rangle \subseteq \langle g_1, g_2, ..., g_t \rangle \subseteq I$ dır. Böylece $I = \langle g_1, g_2, ..., g_t \rangle$ olur. Sonuç olarak G kümesi I ideali için bir üreteç kümesidir.

Ayrıca, $g_i, g_j \in G$ ise S-Polinomunun oluşturulma şeklinden $S(g_1, g_2) \xrightarrow{G}_{+} 0$ dir. Dolayısıyla Buchberger Teoreminden G kümesi I ideali için bir Gröbner tabanıdır. □

Örnek3.2.9: $f_1 = y^2 + yx + x^2$, $f_2 = y + x$, $f_3 = y \in \mathbb{Q}[x, y]$ $y > x$ olmak üzere sıralama lex olsun. $I = \langle f_1, f_2, f_3 \rangle$ ideali için bir Gröbner tabanı bulalım.

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

1.ADIM:

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

$\left[lt(f_1) = y^2 \text{ , } lt(f_2) = y \text{ , } L = lcm(lp(f_1), lp(f_2)) = lcm(y^2, y) = y^2 \right]$

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

$S(f_1, f_2) = x^2 \xrightarrow{G}_{+} x^2 = h$ $[h, G \text{ ye göre indirgenmiş}]$

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

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

2.ADIM:

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

$\left[lt(f_3) = y \text{ , } lt(f_3) = y \text{ , } L_1 = lcm(lp(f_1), lp(f_3)) = lcm(y^2, y) = y^2 \right]$

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

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

3.ADIM:

$\mathfrak{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$, $\left[L_2 = lcm(lp(f_2), lp(f_3)) = lcm(y, y) = y \right]$

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

$S(f_2, f_3) = x \xrightarrow{G}_{+} x = h$ $\quad [h, G \text{ ye göre indirgenmiş}]$

$h \neq 0$ olduğundan $f_5 := x$ olsun.

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

4.ADIM:

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

$\left[lt(f_4) \text{ , } L_3 = lcm(lp(f_1), lp(f_4)) = lcm(y^2, x^2) = y^2 x^2 \right]$

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

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

5.ADIM:

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

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

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

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

6.ADIM:

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

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

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

7.ADIM:

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

$$\left[lt(f_5) = x, \ L_5 = lcm\left(lp(f_1), lp(f_5)\right) = lcm\left(y^2, x\right) = y^2 x \right]$$

$$S(f_1, f_5) = \frac{L_5}{lt(f_1)} f_1 - \frac{L_5}{lt(f_5)} f_5 = \frac{y^2 x}{y^2}\left(y^2 + yx + x^2\right) - \frac{y^2 x}{x}(x) = yx^2 + x^3$$

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

8.ADIM:

$$\mathfrak{G} := \{\{f_3, f_5\}, \{f_4, f_5\}\}, \quad \left[L_6 = lcm\left(lp(f_2), lp(f_5)\right) = lcm\left(y, x\right) = yx \right]$$

$$S(f_2, f_5) = \frac{L_6}{lt(f_2)} f_2 - \frac{L_6}{lt(f_5)} f_5 = \frac{yx}{y}(y+x) - \frac{yx}{x}(x) = x^2$$

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

9.ADIM:

$\mathfrak{G} := \{\{f_4, f_5\}\}$, $\left[L_7 = lcm(lp(f_3), lp(f_5)) = lcm(y,x) = yx \right]$

$$S(f_3, f_5) = \frac{L_7}{lt(f_3)} f_3 - \frac{L_7}{lt(f_5)} f_5 = \frac{yx}{y}(y) - \frac{yx}{x}(x) = 0$$

10.ADIM:

$\mathfrak{G} := \varnothing$, $\left[L_8 = lcm(lp(f_4), lp(f_5)) = lcm(x^2, x) = x^2 \right]$

$$S(f_4, f_5) = \frac{L_8}{lt(f_4)} f_4 - \frac{L_8}{lt(f_5)} f_5 = \frac{x^2}{x^2}(x^2) - \frac{x^2}{x}(x) = 0$$

$\mathfrak{G} := \varnothing$ olduğundan algoritma tamamlanır.

Böylece $G = \{f_1, f_2, f_3, f_4, f_5\}$ kümesi $I = \langle f_1, f_2, f_3 \rangle$ ideali için bir Gröbner tabanıdır.

Şimdiye kadar örneklerimizde $\mathbb{Q}$ cismini kullandık. Aslında teori herhangi bir k cismi için geçerlidir. Bu noktayı açıklamak için bir sonraki örneğimizde k nın sonlu bir cisim olması durumunda bir Gröbner tabanı bulacağız.

Örnek3.2.10: Bu örnekte $k = \mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$ cismini göz önüne alalım.

$f_1 = x^2 + y^2 + 1$, $f_2 = x^2 y + 2xy + x \in \mathbb{Z}_5[x, y]$ ve $x > y$ olmak üzere sıralama lex olsun. $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Z}_5[x, y]$ ideali için bir Gröbner tabanı bulalım.

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

1.ADIM:

$\mathfrak{G} := \varnothing$, $\left[lt(f_1) = x^2, lt(f_2) = x^2 y, L = lcm(lp(f_1), lp(f_2)) = lcm(x^2, x^2 y) = x^2 y \right]$

$$S(f_1, f_2) = \frac{L}{lt(f_1)} f_1 - \frac{L}{lt(f_2)} f_2 = \frac{x^2 y}{x^2}(x^2 + y^2 + 1) - \frac{x^2 y}{x^2 y}(x^2 y + 2xy + x)$$
$$= y^3 + y - 2xy - x = 3xy + 4x + y^3 + y$$

$S(f_1, f_2) = 3xy + 4x + y^3 + y = h \quad [h, G \text{ ye göre indirgenmiş}]$

$h \neq 0$ olduğundan $f_3 := 3xy + 4x + y^3 + y$ olsun.

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

2.ADIM:

$\mathbb{G} := \{\{f_2, f_3\}\}, \qquad \left[lt(f_3) = 3xy,\ L_1 = lcm(lp(f_1), lp(f_3)) = lcm(x^2, xy) = x^2y\right]$

$$S(f_1, f_3) = \frac{L_1}{lt(f_1)} f_1 - \frac{L_1}{lt(f_3)} f_3 = \frac{x^2y}{x^2}(x^2 + y^2 + 1) - \frac{x^2y}{3xy}(3xy + 4x + y^3 + y)$$
$$= -5x^2y - 8x^2 - 2xy^3 - 2xy + y^3 + y = 2x^2 + 3xy^3 + 3xy + y^3 + y$$

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

$$3xy^3 + 3xy + y^3 + 3y^2 + y + 3 \xrightarrow{f_3} xy^2 + 3xy + 4y^5 3y^2 + y + 3$$

$$xy^2 + 3xy + 4y^5 3y^2 + y + 3 \xrightarrow{f_3} 4y^5 + 3y^4 + y^2 + y + 3$$

$$S(f_1, f_3) \xrightarrow{G}_{+} 4y^5 + 3y^4 + y^2 + y + 3 = h \quad [h, G \text{ ye göre indirgenmiş}]$$

$h \neq 0$ olduğundan $f_4 := 4y^5 + 3y^4 + y^2 + y + 3$ olsun.

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

3.ADIM:

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

$\left[lt(f_4) = 4y^5,\ L_2 = lcm(lp(f_2), lp(f_3)) = lcm(x^2y, xy) = x^2y\right]$

$$S(f_2, f_3) = \frac{L_2}{lt(f_2)} f_2 - \frac{L_2}{lt(f_3)} f_3 = \frac{x^2y}{x^2y}(x^2y + 2xy + x) - \frac{x^2y}{3xy}(3xy + 4x + y^3 + y)$$
$$= 10x^2y + 12x^2 + 3xy^3 + 5xy + x = 2x^2 + x + 3xy^3$$

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

$$x + 3xy^3 + 3y^2 + 3 \xrightarrow{f_3} x + xy^2 + 4y^5 + 4y^3 + 3y^2 + 3$$

$$x+xy^2+4y^5+4y^3+3y^2+3 \xrightarrow{f_3} 4y^5+3y^4+y^2+y+3$$

$$x+xy^2+4y^5+4y^3+3y^2+3 \xrightarrow{f_4} 0,\quad S(f_2,f_3) \xrightarrow{G}_{+} 0$$

4.ADIM:

$$\mathbb{G} := \{\{f_2,f_4\},\{f_3,f_4\}\},\quad \left[L_3 = lcm(lp(f_1),lp(f_4)) = lcm(x^2,y^5) = x^2y^5\right]$$

$$S(f_1,f_4) = \frac{L_3}{lt(f_1)}f_1 - \frac{L_3}{lt(f_4)}f_4 = \frac{x^2y^5}{x^2}(x^2+y^2+1) - \frac{x^2y^5}{4y^5}(4y^5+3y^4+y^2+y+3)$$

$$= 5x^2y^5+3x^2y^4+x^2y^2+x^2y+3x^2+y^7+y^5 = 3x^2+3x^2y^4+x^2y^2+x^2y+y^7+y^5$$

$$3x^2+3x^2y^4+x^2y^2+x^2y+y^7+y^5 \xrightarrow{f_1} 3x^2y^4+x^2y^2+x^2y+y^7+y^5+2y^2+2$$

$$3x^2y^4+x^2y^2+x^2y+y^7+y^5+2y^2+2 \xrightarrow{f_1} x^2y^2+x^2y+y^7+2y^6+y^5+2y^4+2y^2+2$$

$$x^2y^2+x^2y+y^7+2y^6+y^5+2y^4+2y^2+2 \xrightarrow{f_1} x^2y+y^7+2y^6+y^5+y^4+y^2+2$$

$$x^2y+y^7+2y^6+y^5+y^4+y^2+2 \xrightarrow{f_1} y^7+2y^6+y^5+y^4+4y^3+y^2+4y+2$$

$$y^7+2y^6+y^5+y^4+4y^3+y^2+4y+2 \xrightarrow{f_4} y^5+2y^4+4y^2+4y+2$$

$$y^5+2y^4+4y^2+4y+2 \xrightarrow{f_4} 0,\quad S(f_1,f_4) \xrightarrow{G}_{+} 0$$

5.ADIM:

$$\mathbb{G} := \{\{f_3,f_4\}\},\quad \left[L_4 = lcm(lp(f_2),lp(f_4)) = lcm(x^2y,y^5) = x^2y^5\right]$$

$$S(f_2,f_4) = \frac{L_4}{lt(f_2)}f_2 - \frac{L_4}{lt(f_4)}f_4 = \frac{x^2y^5}{x^2y}(x^2y+2xy+x) - \frac{x^2y^5}{4y^5}(4y^5+3y^4+y^2+y+3)$$

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

$$= 2x^2+2x^2y^5+2x^2y^4+4x^2y^2+4x^2y+2xy^5+xy^4$$

$$S(f_2,f_4) \xrightarrow{f_1} 2x^2y^5+2x^2y^4+4x^2y^2+4x^2y+2xy^5+xy^4+3y^2+3 = h_1$$

$$h_1 \xrightarrow{f_1} 2x^2y^4+4x^2y^2+4x^2y+2xy^5+xy^4+3y^7+3y^5+3y^2+3 = h_2$$

$$h_2 \xrightarrow{f_1} 4x^2y^2+4x^2y+2xy^5+xy^4+3y^7+3y^6+3y^5+3y^4+3y^2+3 = h_3$$

$$h_3 \xrightarrow{f_1} 4x^2y+2xy^5+xy^4+3y^7+3y^6+3y^5+4y^4+4y^2+3 = h_4$$

$$h_4 \xrightarrow{f_1} 2xy^5+xy^4+3y^7+3y^6+3y^5+4y^4+y^3+4y^2+y+3 = h_5$$

$$h_5 \xrightarrow{f_3} 4y^7+3y^6+4y^5+4y^4+y^3+4y^2+y+3=h_6$$

$$h_6 \xrightarrow{f_4} 4y^5+3y^4+y^2+y+3=h_7$$

$$h_7 \xrightarrow{f_4} 0,\ \ S(f_2,f_4) \xrightarrow{G}_{+} 0$$

6.ADIM:

$$\mathfrak{G} := \varnothing,\ \ \left[L_5 = lcm\left(lp(f_3), lp(f_4)\right) = lcm\left(xy, y^5\right) = xy^5\right]$$

$$S(f_3,f_4) = \frac{L_5}{lt(f_3)} f_3 - \frac{L_5}{lt(f_4)} f_4 = \frac{xy^5}{3xy}\left(3xy+4x+y^3+y\right) - \frac{xy^5}{4y^5}\left(4y^5+3y^4+y^2+y+3\right)$$
$$= xy^4+xy^2+xy+3x+2y^7+2y^5$$

$$S(f_3,f_4) \xrightarrow{f_3} 2xy^3+xy^2+xy+3x+2y^7+3y^6+2y^5+3y^4=h_8$$

$$h_8 \xrightarrow{f_3} xy+3x+2y^7+3y^6+3y^5+3y^4+y^3=h_9$$

$$h_9 \xrightarrow{f_3} 2y^7+3y^6+3y^5+3y^4+4y^3+3y=h_{10}$$

$$h_{10} \xrightarrow{f_4} 4y^6+3y^5+y^3+y^2+3y=h_{11}$$

$$h_{11} \xrightarrow{f_4} 0$$

$$S(f_3,f_4) \xrightarrow{G}_{+} 0$$

$\mathfrak{G} := \varnothing$ olduğundan algoritma tamamlanır. Böylece $G=\{f_1, f_2, f_3, f_4\}$ kümesi $I=\langle f_1, f_2\rangle \subseteq \mathbb{Z}_5[x,y]$ ideali için bir Gröbner tabanı olur.

3.3. İndirgenmiş Gröbner Tabanları

Önceki kısımda Gröbner tabanlarının nasıl bulunacağı görülmüştü. Ancak Buchberger Algoritmasından elde edilen Gröbner tabanı tek olmayabilir. Bu kısımda Gröbner tabanındaki polinomlar üzerine bazı şartlar konularak teklik özelliğinin sağlanabileceği gösterilecektir.

Buchberger Algoritmasında seçimlerin yapıldığı iki yer vardır. İlki; Bölme Algoritmasının uygulamasının etkilendiği yer olan polinomların girişinin sıralamasıdır. İkincisi; Algoritmada S-Polinomlarının hesaplandığı döngüdeki $\{f,g\}\in G$ lerin rastgele seçimidir.

Dolayısıyla bu seçimlerin ikisi değiştirilirse farklı bir Gröbner tabanı ile karşılaşılabilir.

Örneğin; Örnek3.2.9'da ilk olarak $S(f_2,f_3)=x$ hesaplansaydı $S(f_1,f_2)$ polinomu sıfıra indirgenebilmiş olurdu. Böylece $S(f_1,f_2)$ polinomu Gröbner tabanında ortaya çıkmazdı. Dolayısıyla farklı bir Gröbner tabanı elde edilirdi. Unutulmamalıdır ki; $I=\langle f_1,f_2,f_3\rangle$ ideali için $G=\{f_1,f_2,f_3,f_4,f_5\}$ Gröbner tabanı sonra hesaplansa bile G kümesinden $f_4=x^2$ polinomunun kaldırılabileceğini gözlemlenebilir. Aynı zamanda $G=\{f_1,f_2,f_3,f_5\}$ kümesi $I=\langle f_1,f_2,f_3\rangle$ için bir Gröbner tabanıdır. Çünkü $lt(f_4)=x^2$ tarafından bölünebilen herhangi bir terim $lt(f_5)=x$ tarafından da bölünebilir. Dolayısıla $G=\{f_1,f_2,f_3,f_5\}$ kümesi $I=\langle f_1,f_2,f_3\rangle$ için bir Gröbner tabanıdır.

Örnek3.3.1: Örnek3.2.9 örneğinde $S(f_1,f_2)$den önce $S(f_2,f_3)$ polinomunu hesaplayarak görülebilir.

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

1.ADIM:

$$\left[lt(f_1)=y^2,\ lt(f_2)=y,\ lt(f_3)=y,\ L=lcm(lp(f_2),lp(f_3))=lcm(y,y)=y\right]$$

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

$S(f_2, f_3) = x \xrightarrow{G}_{+} x = h \quad [h, G \text{ ye göre indirgenmiş}]$

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

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

2.ADIM:

$\mathbb{G} := \{\{f_1, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}, \left[L_1 = lcm(lp(f_1), lp(f_2)) = lcm(y^2, y) = y^2\right]$

$$S(f_1, f_2) = \frac{L_1}{lt(f_1)} f_1 - \frac{L_1}{lt(f_2)} f_2 = \frac{y^2}{y^2}(y^2 + yx + x^2) - \frac{y^2}{y}(y + x) = x^2$$

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

3.ADIM:

$\mathbb{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}, \left[L_2 = lcm(lp(f_1), lp(f_3)) = lcm(y^2, y) = y^2\right]$

$$S(f_1, f_3) = \frac{L_2}{lt(f_1)} f_1 - \frac{L_2}{lt(f_3)} f_3 = \frac{y^2}{y^2}(y^2 + yx + x^2) - \frac{y^2}{y}(y) = yx + x^2$$

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

4.ADIM:

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

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

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

$S(f_1, f_4) = yx^2 + x^3 \xrightarrow{f_2} 0 \;\; , \;\; S(f_1, f_4) \xrightarrow{G}_{+} 0$

5.ADIM:

$\mathfrak{G} := \{\{f_3, f_4\}\}$, $\left[L_4 = lcm(lp(f_2), lp(f_4)) = lcm(y,x) = yx \right]$

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

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

6.ADIM:

$\mathfrak{G} := \varnothing$ $\left[L_5 = lcm(lp(f_3), lp(f_4)) = lcm(y,x) = yx \right]$

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

$\mathfrak{G} := \varnothing$ olduğundan algoritma tamamlanır. Böylece $\langle f_1, f_2, f_3 \rangle$ ideali için $G := \{f_1, f_2, f_3, f_4\}$ kümesi bir Gröbner tabanı olur.

Tanım3.3.2: Her i için $lc(g_i) = 1$ ve her $i \neq j$ için $lp(g_i)$, $lp(g_j)$ yi bölmüyor ise $G = \{g_1, g_2, ..., g_t\}$ Gröbner tabanına **minimal** denir.

Lemma3.3.3: $G = \{g_1, g_2, ..., g_t\}$ kümesi I ideali için bir Gröbner tabanı olsun. Eğer $lp(g_2)$, $lp(g_1)$ ifadesini bölüyor ise $G = \{g_2, g_3, ..., g_t\}$ kümesi de aynı zamanda I için Gröbner tabanıdır.

Kanıt: $lp(g_2)$, $lp(g_1)$ ifadesini bölüyor olsun. f polinomu $lp(g_1)$, $lp(f)$ yi bölecek biçimde ise aynı zamanda $lp(g_2)$, $lp(f)$ yi böler. Bu nedenle Tanım3.1.1 den $G = \{g_2, g_3, ..., g_t\}$ kümesi I için bir Gröbner tabanıdır. □

Bu lemmanın doğrudan bir sonucu olarak herhangi bir Gröbner tabanından bir minimal Gröbner tabanının nasıl elde edileceğini göreceğiz.

Sonuç3.3.4: $G=\{g_1,g_2,...,g_t\}$ I ideali için bir Gröbner tabanı olsun. G kümesinden bir minimal Gröbner tabanı elde etmek için;

$lp(g_j)|lp(g_i)$ olacak şekilde $j\neq i$ indisleri var olduğunda g_i polinomları elenir(kümeden çıkarılır) ve geri kalan g_i polinomları da $lc(g_i)$ katsayılarına bölünür. (William W. Adams, Philippe Loustaunau, 1994)

Örnek3.2.9'da f_1, f_2, f_4 polinomları kaldırılarak $\{f_1, f_2, f_3, f_4, f_5\}$ kümesinden I için bir minimal Gröbner tabanı elde edilebilir. Aynı zamanda f_1, f_3, f_4 polinomları kaldırılarak da $\{f_1, f_2, f_3, f_4, f_5\}$ kümesinden I için bir minimal Gröbner tabanı elde edilebilir. Dolayısıyla minimal Gröbner tabanları da tek değildir. Fakat aşağıdaki önermede gösterileceği gibi bir I ideali için bütün minimal Gröbner tabanları aynı eleman sayısına sahiptir. Aynı zamanda baş terimleri aynıdır.

Önerme3.3.5: $G=\{g_1,g_2,...,g_t\}$ ve $F=\{f_1, f_2,..., f_s\}$ kümeleri bir I ideali için minimal Gröbner tabanları olsun. O zaman $s=t$ dir ve gerekirse yeniden numaralandırılarak $\forall i=1,2,...,t$ için $lt(f_i)=lt(g_i)$ elde edilir.

(William W. Adams, Philipe Loustaunau, 1994)

Az önce bahsedildiği gibi minimal Gröbner tabanları tek değildir. Teklik elde etmek için Gröbner tabanındaki polinomlar üzerine daha güçlü bir koşul eklenmesi gerekir.

Tanım3.3.6: Her i için $lc(g_i)=1$ ve g_i polinomu $G-\{g_i\}$ kümesine göre indirgenmiş ise $G=\{g_1,g_2,...,g_t\}$ Gröbner tabanına **indirgrnmiş Gröbner tabanı** denir.

Bunun anlamı her i için ;

Herhangi bir $j\neq i$ için g_i polinomu içinde herhangi bir $lp(g_j)$ tarafından bölünebilen sıfırdan farklı bir terim yoktur.

Not: Her indirgenmiş Gröbner tabanı aynı zamanda minimal Gröbner tabanıdır.

Sonuç3.3.7: $G=\{g_1,g_2,...,g_t\}$, I ideali için bir minimal Göbner tabanı olsun. Aşağıdaki indirgeme işlemlerini göz önüne alalım.

$g_1 \xrightarrow{H_1}_{+} h_1$ Burada h_1 polinomu $H_1=\{g_2,g_3,...,g_t\}$ kümesine göre indirgenmiş.

$g_2 \xrightarrow{H_2}_{+} h_2$ Burada h_2 polinomu $H_2=\{h_1,g_3,...,g_t\}$ kümesine göre indirgenmiş.

$g_3 \xrightarrow{H_3}_{+} h_3$ Burada h_3 polinomu $H_3=\{h_1,h_2,g_4,g_5,...,g_t\}$ kümesine göre indirgenmiş.

$\vdots$

$g_t \xrightarrow{H_t}_{+} h_t$ Burada h_t polinomu $H_t=\{h_1,h_2,...,h_{t-1}\}$ kümesine göre indirgenmiş.

O zaman $H=\{h_1,h_2,...,h_t\}$ kümesi I ideali için indirgenmiş Gröbner tabanıdır.

Kanıt: $H=\{h_1,h_2,...,h_t\}$ indirgenmiş Gröbner tabanı olduğundan aynı zamanda minimal Gröbner tabanıdır. G kümesi de minimal Gröbner tabanı olduğundan her bir $i=1,2,...,t$ için $lp(h_i)=lp(g_i)$ dir. Şimdi bunun nasıl olduğunu görelim.

G minimal Gröbner tabanı olduğundan $i\neq j$ için $lp(g_i)$, $lp(g_j)$ yi bölmez.

$i=1$ için için ele alırsak;

$j\neq 1$ için $lp(g_1)$, $lp(g_j)$ yi bömez. Hipotezdeki indirgeme işleminden g_1 polinomu içinde g_1 polinomu olmayan bir kümeye göre indirgeniyor. Dolayısıyla $j\neq 1$ için $lp(g_1)$, $lp(g_j)$ bölmediğinden g_1 polinomunun $lp(g_1)$ ifadesi yok olmaz(sadeleşmez). Böylece h_1 polinomunun $lp(h_1)$ ifadesi için $lp(h_1)=lp(g_1)$ olur. Benzer şekilde diğer i indisleri için aynı işlemler yapılır. Dolayısıyla her bir $i=1,2,...,t$ için $lp(h_i)=lp(g_i)$ bulunur.

g_i polinomlarının $h_1, h_2, ..., h_{i-1}, g_{i+1}, ..., g_t$ polinomları ile bölünmesi;

$lp(h_1), lp(h_2), ..., lp(h_{i-1}), lp(g_{i+1}), ..., lp(g_t)$ kullanılarak g_i polinomunun terimlerinin yok edilmesi ile yapıldığından ve her j için $lp(h_j) = lp(g_j)$ olduğundan H bir indirgenmiş Gröbner tabanıdır. □

Teorem3.3.8 (BUCHBERGER): Belirli bir terim sıralaması alalım. O zaman sıfırdan farklı her I ideali bu terim sıralamasına göre bir tek indirgenmiş Gröbner tabanına sahiptir.

Kanıt: Sonuç3.3.7'de her idealin bir indirgenmiş Gröbner tabanına sahip olduğunu kanıtladık. Böylece sadece tekliği kanıtlamamız yeterli olacaktır.

$G = \{g_1, g_2, ..., g_t\}$ ve $H = \{h_1, h_2, ..., h_t\}$ kümeleri I ideali için indirgenmiş Gröbner tabanları olsun.

Önerme3.3.5 den ve indirgenmiş Gröbner tabanının aynı zamanda minimal Gröbner tabanı olmasından G ve H kümelerinin ikisi de aynı eleman sayılarına sahiptirler.

Her bir i için $lt(g_i) = lt(h_i)$ olduğunu varsayalım. $1 \le i \le t$ olsun.

Eğer $g_i \neq h_i$ ise;

$g_i - h_i \in I$ ise $lp(h_j) \mid lp(g_i - h_i)$ olacak şekilde bir j vardır. (Gröbner tabanı tanımından). Buradan $lp(g_i - h_i) < lp(h_i)$ olduğundan $j \neq i$ olur.

$lt(g_i) = lt(h_i)$ olduğunu biliyoruz. Buradan $g_i - h_i$ polinomunda $lt(h_i)$ veya $lt(g_i)$ yok olur. Dolayısıyla $lp(g_i - h_i) < lp(h_i)$ olur.

$$lp(h_j) \mid lp(g_i - h_i) \Rightarrow lp(h_j) < lp(g_i - h_i) \Rightarrow lp(h_j) < lp(g_i - h_i) < lp(h_i)$$

$$\Rightarrow lp(h_j) < lp(h_i) \Rightarrow i \neq j \text{ olur.}$$

Fakat o zaman $lt(g_j) = lt(h_j)$, g_i nin veya h_i nin bir terimini böler.

Bu G *ve* H nin indirgenmiş Gröbner tabanı olması ile çelişir.

Dolayısıyla $g_i = h_i$ dir. Böylece $G = H$ olur. Teklik kanıtlanır. □

Örnek3.3.9: Örnek3.2.9'i tekrar ele alalım.

Sonuç3.3.4den sonra $\{f_3, f_5\}$ *ve* $\{f_2, f_5\}$ kümelerinin her ikisinin $I = \langle f_1, f_2, f_3 \rangle$ ideali için minimal Gröbner tabanı olduğunun doğruluğunu göstermiştik.

$f_3 = y$ *ve* $f_5 = x$ olduğundan $\{f_3, f_5\}$, I için bir indirgenmiş Gröbner tabanıdır. $f_2 = y + x$ olduğundan f_5 kullanılarak f_2 polinomunu y polinomuna indirgeyebiliriz.

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

Dolayısıyla $\{f_2, f_5\}$ indirgenmiş bir Gröbner tabanıdır. Tabi ki indirgenmiş Gröbner tabanı tek olduğundan $\{f_2, f_5\}$ den elde edilen indirgenmiş Gröbner tabanı aslında $\{f_3, f_5\}$ dir.

Örnek3.3.10: Örnek3.2.10'i ele alalım.

$x > y$ olmak üzere lex sıralamasına göre $I = \langle x^2 + y^2 + 1, x^2 y + 2xy + x \rangle \subseteq \mathbb{Z}_5[x, y]$ ideali için

$\{g_1 = x^2 + y^2 + 1,\ g_2 = x^2 y + 2xy + x,\ g_3 = 3xy + 4x + y^3 + y,\ g_4 = 4y^5 + 3y^4 + y^2 + y + 3\}$ kümesinin bir Gröbner tabanı olduğunu göstedik.

Sonuç3.3.4 kullanılarak; $lp(g_1) \mid lp(g_2)$ olduğundan g_2 kümeden atılır. Şimdi artık her $i \neq j$ için $lp(g_i)$, $lp(g_j)$ yi bölmez.

Kalan g_1, g_3, g_4 polinomları için $lc(g_1) = 1, lp(g_3) = 3$, $lp(g_4) = 4$ dir. g_3 *ve* g_4 polinomlarında $lp(g_3) \neq 1, lp(g_4) \neq 1$ olduğundan g_3 *ve* g_4 polinomları sırasıyla $lp(g_3) = 3$, $lp(g_4) = 4$ katsayılarına bölünür.

Böylece $g_3 = xy+3x+2y^3+2y$, $g_4 = y^5+2y^4+4y^2+4y+2$ olur. Sonuç3.3.4 den $F=\{x^2+y^2+1,\ xy+3x+2y^3+2y,\ y^5+2y^4+4y^2+4y+2\}$ kümesi, I için minimal Gröbner tabanıdır. Bu kümenin I için indirgenmiş Gröbner tabanı olduğunu görmek kolaydır. Bunun için;

$f_1 = x^2+y^2+1$, $f_2 = xy+3x+2y^3+2y$, $f_3 = y^5+2y^4+4y^2+4y+2$ olarak

F kümesindeki polinomları yeniden adlandırılsın.

Buradan $lc(f_1)=1, lc(f_2)=1, lc(f_3)=1$ dir.

f_1 polinomu $F-\{f_1\}$ kümesine göre indirgenmiştir.

f_2 polinomu $F-\{f_2\}$ kümesine göre indirgenmiştir.

f_3 polinomu $F-\{f_3\}$ kümesine göre indirgenmiştir.

Böylece F kümesi I ideali için indirgenmiş bir Gröbner tabanıdır.

Şimdiye kadar gördüğümüz en önemli sonuçların bir özetini vererek bu kısım sonlandırılacaktır

Teorem3.3.11: Sıfırdan farklı polinomların bir kümesi $G=\{g_1,g_2,...,g_t\}$ ve $I=\langle G\rangle=\langle g_1,g_2,...,g_t\rangle$ ideali için aşağıdaki durumlar denktir.

(i) $\forall\ f\in I$ için $lp(g_i)\,|\,lp(f)$ olacak şekilde $i\in\{1,2,...,t\}$ vardır. Yani G kümesi I ideali için bir Gröbner tabanıdır.

(ii) $Lt(G)=Lt(I)$ dir.

(iii) $f\in I \Leftrightarrow f \xrightarrow{G}_{+} 0$ dir.

(iv) $\forall\ f\in k[x_1,x_2,...,x_n]$ için $f \xrightarrow{G}_{+} r_1$, $f \xrightarrow{G}_{+} r_2$ ve r_1, r_2 polinomları G

kümesine göre indirgenmiş ise $r_1=r_2$ dir.

(v) $\forall i \neq j$ için $S\left(g_i, g_j\right) \xrightarrow{G}_{+} 0$ dir .

(vi) $\forall f \in I$ için $f = h_1 g_1 + h_2 g_2 + ... + h_t g_t$ ve $lp(f) = \max_{1 \leq \nu \leq t} \left(lp(h_\nu) \cdot lp(g_\nu) \right)$ olacak şekilde $h_1, h_2, ..., h_t \in k\left[x_1, x_2, ..., x_n\right]$ elemanları vardır.

(vii) $\forall i \neq j \ (1 \leq i, j \leq t)$ için $lp\left(S\left(g_i, g_j\right)\right) = \max_{1 \leq \nu \leq t} \left(lp\left(h_{i j \nu}\right) lp\left(g_\nu\right) \right)$ olacak şekilde $S\left(g_i, g_j\right) = h_{i j 1} \cdot g_1 + h_{i j 2} \cdot g_2 + ... + h_{i j t} \cdot g_t$ vardır.

Teorem3.3.12: $k\left[x_1, x_2, ..., x_n\right]$ üzerinde bir sabit terim sıralaması olsun. O zaman her I ideali bu terim sıralamasına göre indirgenmiş bir Gröbner tabanına sahiptir. I ideali polinomların sonlu bir kümesi tarafından üretiliyor ise bu Gröbner tabanı hesaplanabilir.

Ayrıca verilen terim sıralamasına göre, I ideali için elde edilen bu indirgenmiş Gröbner tabanı tek şekilde belirlidir.

IV .BÖLÜM

ESAS İDEAL BÖLGESİ ÜZERİNDE GRÖBNER TABANLARI VE DİNAMİK GRÖBNER TABANLARI

4.1 Değerlendirme Bölgesi Üzerinde Gröbner Tabanı

Tanım4.1.1: R bir halka, $f=\sum_{\alpha} a_{\alpha}X^{\alpha}$, $R[x_1,x_2,...,x_n]$ halkasında sıfırdan farklı bir polinom, $\varnothing \neq E \subseteq R[x_1,x_2,...,x_n]$ ve $">"$ bir terim sıralaması olsun.

(i) X^{α} ifadelerine f polinomunun **kuvvet çarpımları (monomialleri)** ve

$a_{\alpha}X^{\alpha}$ ifadelerine f polinomunun **terimleri** denir.

(ii) f polinomunun **multiderecesi** $m\deg(f)=\max\{\alpha\in\mathbb{N}^n \mid a_{\alpha}\neq 0\}$ dir.

(iii) f polinomunun **baş katsayısı** $lc(f)=a_{m\deg(f)}\in R$ dir.

(iv) f polinomunun **baş kuvvet çarpımı (baş monomiali)** $lp(f)=X^{m\deg(f)}$ dir.

(v) f polinomunun **baş terimi** $lt(f)=lc(f)\cdot lp(f)$ dir.

(vi) $Lt(E)=\langle\{lt(g)\mid g\in E\}\rangle$

(vii) $Lt(S)$, $R[x_1,x_2,...,x_n]$ halkasının bir idealidir.

(viii) $g,h\in R[x_1,x_2,...,x_n]-\{0\}$ için $lp(g)\mid lp(h)$ ve $lc(g)\mid lc(h)$ ise $lt(g)\mid lt(h)$ dir.

Tanım4.1.2:

(i) k bir cisim ve G toplamsal bir sıralı grup olsun. $v: k \longrightarrow G \cup \{\infty\}$ dönüşümü, $\forall a,b \in k$ için;

1) $v(a) = \infty \Leftrightarrow a = 0$

2) $v(a \cdot b) = v(a) + v(b)$

3) $v(a+b) \geq \min\{v(a), v(b)\}$

özellikleri sağlanıyorsa v ye k cismi üzerinde bir **değerlendirme** denir.

(ii) k bir cisim, v k cisminin bir değerlendirmesi olsun. v nin değer grubu tek bir elemanla üretilmiş sonsuz devirli grup ise v ye **ayrık değerlendirme** denir.

Tanım4.1.3

(i) R bir halka olsun. Her $a, b \in R$ için $a \mid b$ veya $b \mid a$ ise R halkasına **değerlendirme halkası** denir.

(ii) R bir tamlık bölgesi ve her $a, b \in R$ için $a \mid b$ veya $b \mid a$ ise R tamlık bölgesine **değerlendirme bölgesi** denir.

Tanım4.1.4: R bir değerlendirme bölgesi, $f, g \in R[x_1, x_2, ..., x_n] - \{0\}$, $I = \langle f_1, f_2, ..., f_s \rangle$ ideali $R[x_1, x_2, ..., x_n]$ halkasının sıfırdan farklı sonlu üretilmiş bir ideali ve "$>$" bir terim sıralaması olsun.

(i) $m\deg(f) = \alpha$ ve $m\deg(g) = \beta$ ise her bir $i = 1, 2, ..., n$ için $\gamma_i = \max(\alpha_i, \beta_i)$ olmak üzere $\gamma = (\gamma_1, \gamma_2, ..., \gamma_n)$ olsun. f ve g polinomlarının S-Polinomu kombinasyonu;

$lc(g) \mid lc(f)$ ise $S(f,g) = \dfrac{X^{\gamma}}{lp(f)} \cdot f - \dfrac{lc(f)}{lc(g)} \cdot \dfrac{X^{\gamma}}{lp(g)} \cdot g$ dir.

$lc(g)$, $lc(f)$ yi bölmüyor ve $lc(f)|lc(g)$ ise

$S(f,g)=\frac{lc(g)}{lc(f)}\cdot\frac{X^{\gamma}}{lp(f)}\cdot f-\frac{X^{\gamma}}{lp(g)}\cdot g$ dir.

(ii) $Lt(I)=\langle lt(f_1),lt(f_2),...,lt(f_s)\rangle$ ise $G=\{f_1,f_2,...,f_s\}$ kümesi I ideali için bir **Gröbner tabanı**dır.

(iii) F cisim iken $F[x_1,x_2,...,x_n]$ polinom halksındaki klasik Bölme Algoritması gibi, her bir $h,h_1,h_2,...,h_m\in R[x_1,x_2,...,x_n]$ polinomları için;

$h=h_1\cdot q_1+h_2\cdot q_2+...+h_m\cdot q_m+r$ olacak şekilde $q_1,q_2,...,q_m,r\in R[x_1,x_2,...,x_n]$ vardır. Burada ya $r=0$ ya da r polinomunun her bir terimi $lt(h_1),lt(h_2),...,lt(h_m)$ lerin hiçbiri tarafından bölünmez. r polinomuna h polinomunun $H=\{h_1,h_2,...,h_m\}$ kümesi ile bölümünden **kalan** denir. $h\xrightarrow{H}_{+} r$ ile gösterilir.

Lemma4.1.5: R bir değerlendirme bölgesi, $I=\langle a_\alpha X^\alpha \mid \alpha\in A\rangle$, $R[x_1,x_2,...,x_n]$ halkasının bir ideali olsun. Herhangi bir $b\cdot X^\beta$ için;

$b\cdot X^\beta\in I$ olması için gerekli ve yeterli koşul $X^\alpha|X^\beta$ ve $\exists\alpha\in A$ için $a_\alpha|b$ olmasıdır.

Kanıt: $\Rightarrow$:

$X^\alpha|X^\beta$ ve $\exists\alpha\in A$ için $a_\alpha|b$ olsun.

$X^\alpha|X^\beta\Rightarrow\exists t\in T^n$ için $X^\beta=t\cdot X^\alpha$ dir.

$\exists\alpha\in A$ için $a_\alpha|b\Rightarrow\exists\alpha\in A$ ve $\exists k\in R$ için $b=k\cdot a_\alpha$ dır.

Bu durumda $b\cdot X^\beta=b\cdot t\cdot X^\alpha=k\cdot t\cdot a_\alpha\cdot X^\alpha$ dır. Böylece $b\cdot X^\beta\in I=\langle a_\alpha X^\alpha\mid\alpha\in A\rangle$ olur.

$\Leftarrow$: $b \cdot X^{\beta} \in I$ olsun.

Bu durumda $\gamma_i \in \mathbb{N}^n$, $c_i, a_{\alpha_i} \in R - \{0\}$ ve $\alpha_1, \alpha_2, ..., \alpha_s \in A$ için

$b \cdot X^{\beta} = \sum_{i=1}^{s} c_i \cdot a_{\alpha_i} \cdot X^{\gamma_i} \cdot X^{\alpha_i}$ yazılır.

Böylece zorunlu olarak; her bir $1 \le i \le s$ için $\gamma_i + \alpha_i = \beta$ ve $b = \sum_{i=1}^{s} c_i \cdot a_{\alpha_i}$ dir. Her bir $1 \le i \le s$ için $X^{\alpha_i} \mid X^{\beta}$ olduğu açıktır. Buradan $X^{\alpha} \mid X^{\beta}$ olur.

$v : R \to (G, \le)$, R halkasına karşılık gelen bir değerlendirme olsun.
$b \mapsto t^m$

$v(b) = v\left(\sum_{i=1}^{s} c_i \cdot a_{\alpha_i} \right) \ge \min_{1 \le i \le s} v\left(c_i \cdot a_{\alpha_i} \right) = \min_{1 \le i \le s} \left(v(c_i) + v\left(a_{\alpha_i} \right) \right) \ge \min_{1 \le i \le s} v\left(a_{\alpha_i} \right)$ olduğundan

$v(b) \ge v\left(a_{\alpha_i} \right)$ olacak şekilde bir $1 \le i \le s$ vardır. Böylece $a_{\alpha_i} \mid b$ olur. □

Lemma4.1.6: (Ayrık Değerlendirme Bölgeleri İçin Dickson Lemması)

R ayrık değerlendirme bölgesi ve $I = \langle a_{\alpha} X^{\alpha} \mid \alpha \in A \rangle$, $R[x_1, x_2, ..., x_n]$ halkasının bir ideali olsun. O zaman $I = \langle a_{\alpha_1} X^{\alpha_1}, a_{\alpha_2} X^{\alpha_2}, ..., a_{\alpha_s} X^{\alpha_s} \rangle$ olacak şekilde $\alpha_1, \alpha_2, ..., \alpha_s \in A$ vardır. (David Cox, John Little, Donal O'Shea, 1997)

Teorem4.1.7: R ayrık değerlendirme halkası, I $R[x_1, x_2, ..., x_n]$ halkasının sıfırdan farklı bir ideali ve "$>$" bir terim sıralaması olsun. O zaman I ideali bir G Gröbner tabanına sahiptir. Aynı zamanda her bir $f \in R[x_1, x_2, ..., x_n]$ için; $f \in I$ olması için gerekli ve yeterli koşul f polinomunun G ile bölümünden kalanın sıfır olmasıdır. (Ihsen Yengui, 2005)

Lemma4.1.8: R bir değerlendirme halkası, "$>$" bir terim sıralaması olsun. Her bir $1 \le i \le s$ için $m\deg(f_i) = \gamma$ olacak şekilde $f_1, f_2, ..., f_s \in R[x_1, x_2, ..., x_n]$ alınsın. Eğer; $a_1, a_2, ..., a_s \in R$ için $m\deg\left(\sum_{i=1}^{s} a_i \cdot f_i\right) < \gamma$ ise $\sum_{i=1}^{s} a_i \cdot f_i$ ifadesi $1 \le i < j \le s$ için $S(f_i, f_j)$ S-Polinomlarının R deki katsayılar ile doğrusal bir kombinasyonudur. Ayrıca herbir $S(f_i, f_j)$ için $m\deg\left(S(f_i, f_j)\right) < \gamma$ dır. (Ihsen Yengui, 2005)

- R ayrık değerlendirme bölgesi, $I = \langle f_1, f_2, ..., f_s \rangle$ $R[x_1, x_2, ..., x_n]$ nin sıfırdan farklı bir ideali ve "$>$" bir terim sıralaması olsun. I ideali için bir Gröbner tabanı aşağıdaki algoritma ile hesaplanabilir.

GİRİŞ: $F = \{f_1, f_2, ..., f_s\} \subseteq k[x_1, x_2, ..., x_n]$, $f_i = 0$ $(1 \le i \le s)$ alınsın.

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

BAŞLANGIÇ: $G := F$, $\mathfrak{G} = \{\{f_i, f_j\} \mid f_i \neq f_j \ , \ f_i, f_j \in G\}$

DÖNGÜ: $\mathfrak{G} :\neq \varnothing$ olduğu sürece aşağıdaki işlemler yapılır

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

$\mathfrak{G} := \mathfrak{G} - \{\{f, g\}\}$

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

$h \neq 0$ ise aşağıdaki işlemler yapılır

$\mathfrak{G} := \mathfrak{G} \cup \{\{u, h\} \mid \forall u \in G \ için\}$

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

BUCHBERGER ALGORİTMASI

Teorem4.1.9: R bir değerlendirme halkası, $I=\langle g_1,g_2,...g_s\rangle$ $R[x_1,x_2,...,x_n]$ halkasının bir ideali ve "$>$" bir terim sıralaması olsun. O zaman $G=\{g_1,g_2,...g_s\}$ kümesinin I ideali için Gröbner tabanı olması için gerekli ve yeterli koşul tüm $i\neq j$ ikilileri için $S(f_i,f_j)$ nin G ile bölümünden kalanın sıfır olmasıdır.(Ihsen Yengui, 2005)

Soru: R bir değerlendirme bölgesi olmak üzere $R[x_1,x_2,...,x_n]$ nin sıfırdan farklı sonlu üretilmiş her ideali için Buchberger Algoritması ile sonlu adımda bir Gröbner tabanı belilemek mümkün mü? Bu soruya cevap bulmak için aşağıdaki örneği inceleyelim.

Örnek4.1.10: R, G grubu ve v değerlendirmesine karşılık gelen bir değerlendirme bölgesi olsun. G nin archimedian olmadığını varsayalım. Bu $v(a)>0$ ve $\forall n\in\mathbb{N}-\{0\}$ için $v(b)>n\cdot v(a)$ olacak şekilde $a,\ b\in R$ elemanlarının var olmasıdır.

$R[x]$ in $g_1=ax+1$ ve $g_2=b$ ile üretilen idealini I ile gösterelim.

$m\deg(g_1)=1, m\deg(g_2)=0, X^{\gamma}=x$

$$S(g_1,g_2)=\frac{lc(g_2)}{lc(g_1)}\frac{X^{\gamma}}{lp(g_1)}g_1-\frac{X^{\gamma}}{lp(g_2)}g_2$$

$S(g_1,g_2)=\frac{b}{a}\frac{x}{x}(ax+1)-\frac{x}{1}(b)=\frac{b}{a}$ olur. $S(g_1,g_2)$ indirgenemediğinden Buchberger Algoritmasını çalıştırdığımızda $g_3=\frac{b}{a}$ eklemeliyiz.

Aynı şekilde $S(g_1,g_3)=\frac{b}{a^2}$ olur. $S(g_1,g_3)$ indirgenemediğinden Buchberger Algoritması uygulanırken $g_4=\frac{b}{a^2}$ eklenmelidir. Bu şekilde devam edersek Buchberger Algoritmasının sonlanmadığını gözlemleriz.

Lex sıralaması ile $G=\mathbb{Z}\times\mathbb{Z}$ durumunu ele alalım. $v(a)=(0,1)$, $v(b)=(1,0)$ olsun.

$I=\langle g_1,g_2\rangle$ sonlu üretilmiş olmasına rağmen $\langle Lt(I)\rangle$ nın sonlu üretilmiş olmadığını kanıtlayabiliriz.

$\langle Lt(I)\rangle$ nın sonlu üretilmiş olduğunu varsayalım. $\langle Lt(I)\rangle=\langle h_1,h_2,...,h_s\rangle$ $h_i\in I-\{0\}$, $s\in\mathbb{N}-\{0\}$ olsun. $h_1,h_2,...,h_s$ terimlerinin her bir $1\le i\le s$ için $h_i=lt(h_i)$ olduğunu varsayabiliriz. Yukarıda S-Polinomları hesaplanırken çıkan ifadelerden $\frac{b}{a^n}\in I$ olur. Lemma4.1.4 den anlaşılacağı gibi her bir $n\in\mathbb{N}$ için $h_{i_n}\left|\frac{b}{a^n}\right.$ olacak şekilde $i_n\in\{1,2,...,s\}$ vardır. h_{i_0} sabit sayı ($h_{i_0}\in R-\{0\}$) ve her $n\in\mathbb{N}$ için $h_{i_0}\left|\frac{b}{a^n}\right.$ olacak şekilde $1\le i_0\le s$ olduğu sonucuna varırız.

$$h_{i_0}\left|\frac{b}{a^n}\Rightarrow v\left(h_{i_0}\right)\le v\left(\frac{b}{a^n}\right)=v(b)-v\left(a^n\right)=v(b)-v\left(\underbrace{a\cdot a\cdot...\cdot a}_{n\text{ tane}}\right)\right.$$

$$=v(b)-\left(\underbrace{v(a)+...+v(a)}_{n\text{ tane}}\right)=v(b)-nv(a)=(1,0)-n(0,1)=(1,-n)$$

Buradan $v\left(h_{i_0}\right)\le(1,-n)$ olur.

Böylece $v\left(h_{i_0}\right)=(0,k)$ olacak şekilde $k\in\mathbb{N}$ olduğu sonucu çıkar.(Lex sıralaması)

$$v\left(h_{i_0}\right)=(0,k)=k\cdot(0,1)=k\cdot v(a)=v\left(a^k\right)$$

$$\Rightarrow v\left(h_{i_0}\right)-v\left(a^k\right)=(0,0)\Rightarrow v\left(\frac{h_{i_0}}{a^k}\right)=(0,0)\Rightarrow\frac{h_{i_0}}{a^k}=u,\quad u\in R$$ terslenebilir. Bu yüzden $h_{i_0}=u\cdot a^k$ olacak şekilde R halkasında terslenebilir bir u elemanı vardır. $h_{i_0}\in I$ olduğundan $a^k\in I$ dır.

$$\begin{cases}a^k\in I\\ ax+1\in I\end{cases}\Rightarrow\begin{cases}a^k\in I\\ a^{k-1}(ax+1)\in I\end{cases}\Rightarrow a^{k-1}\in I\Rightarrow...\Rightarrow a\in I\Rightarrow 1\in I$$ olur. Bu bir çelişkidir.

Bu çelişki $\langle Lt(I)\rangle$ nın sonlu üretilmiş alınmasından kaynaklanır. Dolayısıyla I sonlu üretilmiş olmasına rağmen $\langle Lt(I)\rangle$ sonlu üretilmiş değildir. Literatürde bunu sağlayan bir ideal yoktur.

Sonuç olarak G grubunun archimedian olması gerekir.

Yukarıdaki örnekten anlaşılacağı gibi Buchberger Algoritmasının sonlanması için gerekli koşul G grubunun archimedian olmasıdır.

4.2 Esas İdeal Bölgesi Üzerinde İdeale Ait Olma Problemi

Tanım4.2.1: R esas ideal bölgesi ve $S \subseteq R$ olsun.

$1 \in S$ ve $\forall a,b \in S$ için $a \cdot b \in S$ ise S kümesine R halkasının **çarpımsal alt kümesi** denir.

$a_1, a_2, ..., a_r \in R$ için R nin $a_1, a_2, ..., a_r$ ile üretilen çarpımsal alt kümesi $M(a_1, a_2, ..., a_r)$ ile gösterilir.

$M(a_1, a_2, ..., a_r) = \left\{ a_1^{n_1} \cdot a_2^{n_2} \cdot ... \cdot a_r^{n_r} \mid n_i \in \mathbb{N} \right\}$ şeklindedir.

R nin yukarıda tanımlanan çarpımsal alt kümesine **sonlu üretilmiştir** denir.

Tanım4.2.2: Bir R halkasının çarpımsal bir alt kümesi S ise;

S kümesi üzerinde R nin **yerelleştirmesi,** $S^{-1}R = \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$ şeklinde tanımlanan halkadır. $a \in R$ ise $M(a)$ çarpımsal alt kümesi üzerinde R nin yerelleştirmesi R_a ile gösterilecektir.

Özel Durum: P asal ideal ve $S = R - P$ ise elde edilen yerelleştirme R_P ile gösterilir.

R esas ideal bölgesi ve R nin kesir cismi F olsun.

$R[x_1, x_2, ..., x_n]$ halkasında $f \in \langle f_1, f_2, ..., f_s \rangle$ olması için gerekli ilk durum $F[x_1, x_2, ..., x_n]$ halkasında $f \in \langle f_1, f_2, ..., f_s \rangle$ olmasıdır.

Bu koşul yerine $R[x_1, x_2, ..., x_n]$ de $d \cdot f \in \langle f_1, f_2, ..., f_s \rangle$ olacak şekilde $d \in R - \{0\}$ olduğunu varsayalım….(0)

R esas ideal bölgesi olduğundan $d = u \cdot P_1^{n_1} \cdot ... \cdot P_l^{n_l}$ yazılabilir. Burada P_i ler R halkasında farklı indirgenemez elemanlar, u R de terslenebilir eleman ve $n_i \in \mathbb{N}$ dir. $R[x_1, x_2, ..., x_n]$ de $f \in \langle f_1, f_2, ..., f_s \rangle$ olması için gerekli diğer durumlar her bir $1 \le i \le l$ için $R_{P_i R}[x_1, x_2, ..., x_n]$ de $f \in \langle f_1, f_2, ..., f_s \rangle$ olmasıdır.

Bazı $d_i \in R - P_i R$ için $R[x_1, x_2, ..., x_n]$ halkasında $d_i f \in \langle f_1, f_2, ..., f_s \rangle$ .....(i) yazılır.

$\gcd(d, d_1, d_2, ..., d_l) = 1$ olduğundan (0), (1), …,(l) ifadelerini birleştirerek ve $d, d_1, d_2, ..., d_l$ arasındaki Bezout özdeşliği kullanılarak $R[x_1, x_2, ..., x_n]$ halkasında $f \in \langle f_1, f_2, ..., f_s \rangle$ bulunur.

Q sorusu: $R[x_1, x_2, ..., x_n]$ polinom halkasında f polinomu $\langle f_1, f_2, ..., f_s \rangle$ idealinde midir?

Q_0 sorusu: $F[x_1, x_2, ..., x_n]$ polinom halkasında f polinomu $\langle f_1, f_2, ..., f_s \rangle$ idealinde midir?

Q sorusuna cevap verebilmek için Q_0 sorusuna cevap vermek gerekir. Q_0 sorusuna cevap olumsuz ise o zaman Q sorusuna da cevap olumsuzdur.

Q_0 sorusuna cevap olumlu ise $R[x_1, x_2, ..., x_n]$ de $d \cdot f \in \langle f_1, f_2, ..., f_s \rangle$ olacak şekilde $d \in R - \{0\}$ vardır…..(0)

R esas ideal bölgesi olduğundan $d = u \cdot P_1^{n_1} \cdot ... \cdot P_l^{n_l}$ yazılabilir. Burada P_i ler R halkasında farklı indirgenemez elemanlar, u R de terslenebilir bir eleman ve $n_i \in \mathbb{N}$ dir.

Q_{P_i} sorusu: Her bir $1 \le i \le l$ için $R_{P_iR}[x_1, x_2, ..., x_n]$ de $f \in \langle f_1, f_2, ..., f_s \rangle$ midir?

Q sorusuna cevabı olumlu olması için gerekli ve yeterli koşul her bir $1 \le i \le l$ için Q_{P_i} sorularının cevaplarının olumlu olmasıdır.

Olumlu cevapların durumunda her bir $1 \le i \le l$ için;

Bazı $d_i \in R - P_iR$ için $R[x_1, x_2, ..., x_n]$ halkasında $d_i f \in \langle f_1, f_2, ..., f_s \rangle$ .....(i) yazılır.

$\gcd(d, d_1, d_2, ..., d_l) = 1$ olduğundan (0), (1),…, (l) ifadeleri birleştirilerek ve $d, d_1, d_2, ..., d_l$ arasındaki Bezout özdeşliği kullanılarak $R[x_1, x_2, ..., x_n]$ halkasında $f \in \langle f_1, f_2, ..., f_s \rangle$ bulunur.

Sonuç olarak ideale ait olma Q probleminin çözümü, R halkasının yerelleştirme halkasında sonlu sayıdaki $Q_0, Q_1, ..., Q_{P_l}$ ideale ait olma problemlerinin çözümü anlamına gelir.

4.3 Esas İdeal Bölgesi Üzerinde Gröbner Tabanı

R kesir cismi F olan bir esas ideal bölgesi olsun. $I = \langle f_1, f_2, ..., f_s \rangle$, $R[x_1, x_2, ..., x_n]$ nin bir ideali olsun. $R[x_1, x_2, ..., x_n]$ üzerinde ideale ait olma problemini çözmenin ilk adımının, problemi $F[x_1, x_2, ..., x_n]$ üzerinde çözmektir.

$F[x_1, x_2, ..., x_n]$ halkasında $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için Gröbner tabanı G_0 olsun. $1 \le i \le l$, $R_{P_iR}[x_1, x_2, ..., x_n]$ halkasında $I = \langle f_1, f_2, ..., f_s \rangle$ için Gröbner tabanları sırasıyla $G_{P_1}, G_{P_2}, ..., G_{P_l}$ olsun. $R[x_1, x_2, ..., x_n]$ halkasında $I = \langle f_1, f_2, ..., f_s \rangle$ ideali için

Gröbner tabanı $G=\left\{G_0,G_{P_1},G_{P_2},...,G_{P_l}\right\}$ dir. Bu durumda $f\in R\left[x_1,x_2,...,x_n\right]$ polinomunun I idealinde olması için gerekli ve yeterli koşul f polinomunun $G_0,G_{P_1},G_{P_2},...,G_{P_l}$ ile bölümünden sırasıyla tüm $r_0,r_1,...,r_l$ kalanlarının sıfır olmasıdır. $r=\left\{r_0,r_1,...,r_l\right\}$ kümesi f nin G kümesi ile bölümünden kalan olarak adlandırılır.

Örnek4.3.1: $f=5x^3y+2x^2+3xy^2+4y-7\in\mathbb{Z}\left[x,y\right]$ ve

$f_1=3xy+4$, $f_2=2x^2+3\in\mathbb{Z}\left[x,y\right]$ olsun. $I=\left\langle f_1,f_2\right\rangle$ ve $x>y$ olmak üzere lex sıralaması alınsın.

$\mathbb{Q}\left[x,y\right]$'de Buchberger Algoritması çalıştırılırsa $G_0=\left\{f_1,\ f_2,\ \frac{4}{3}x-\frac{3}{2}y\ ,\ \frac{9}{8}y^2+\frac{4}{3}\right\}$ $\left\langle f_1,f_2\right\rangle$ için bir Gröbner tabanı olarak bulunur.

$f=\left(\frac{5}{3}x^2+y\right)\cdot f_1-\frac{7}{3}f_2$ olduğundan $\mathbb{Q}\left[x,y\right]$'de ideale ait olma probleminin yanıtı olumludur.

Yukarıdaki f polinomu ifadesinde paydalar eşitlenirse;

$3f=\left(5x^2+3y\right)\cdot f_1-7f_2$ .....(*) elde edilir.

Geriye $\mathbb{Z}_{3\mathbb{Z}}\left[x,y\right]=\mathbb{Z}_{(3)}\left[x,y\right]$'de Buchberger Algoritmasını çalıştırmak kalır.

Buradan $\mathbb{Z}_{(3)}\left[x,y\right]$'de $\left\langle f_1,f_2\right\rangle$ ideali için Gröbner tabanı olarak $G_3=\left\{f_1,\ f_2,\ 4x-\frac{9}{2}y\ ,\frac{27}{8}y^2+4\right\}$ elde edilir.

Böylece $G=\left\{\left\{f_1,\ f_2,\ \frac{4}{3}x-\frac{3}{2}y\ ,\ \frac{9}{8}y^2+\frac{4}{3}\right\},\left\{f_1,\ f_2,4x-\frac{9}{2}y\ ,\frac{27}{8}y^2+4\right\}\right\}$ kümesi $\mathbb{Z}\left[x,y\right]$'de $I=\left\langle f_1,f_2\right\rangle$ ideali için bir Göbner tabanıdır.

$f = \left(y - \frac{5}{2} \right) \cdot f_1 + \left(\frac{5}{2} xy + 1 \right) \cdot f_2$ olduğundan $\mathbb{Z}_{(3)}[x, y]$'de ideale ait olma probleminin yanıtı olumludur.

f polinomunun bu ifadesinde paydalar eşitlenirse;

$2f = (2y - 5) \cdot f_1 + (5xy + 2) \cdot f_2$ .....(**) elde edilir.

2 *ve* 3 arasındaki Bezout özdeşliğinden $3 \cdot 1 + 2 \cdot (-1) = 1$ dir. Böylece (*) eşitliğinden (**) eşitliği çıkarılırsa $f = \left(5x^2 + y + 5\right) \cdot f_1 + \left(-5xy - 9\right) \cdot f_2$ bulunur.

Bulunan ifade $\mathbb{Z}[x, y]$'de f polinomunun $I = \langle f_1, f_2 \rangle$ idealinde bulunduğunu gösterir. Yani $\mathbb{Z}[x, y]$ halkasında ideale ait olma probleminin yanıtı olumludur.

4.4. Dinamik Gröbner Tabanları

R Noetherian değerlendirme Halkası, $I=\langle f_1, f_2,..., f_s\rangle$ $R[x_1, x_2,..., x_n]$ nin bir ideali ve ">" bir terim sıralaması olsun. O zaman I ideali için bir Gröbner tabanı aşağıdaki gibi bir algoritma ile sonlu adımda bulunur.

GİRİŞ: $F=\{f_1, f_2,..., f_s\}\subseteq k[x_1, x_2,..., x_n]$, $f_i=0$ $(1\le i\le s)$ alınsın.

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

BAŞLANGIÇ: $G:=F$, $\mathbb{G}=\{\{f_i, f_j\}\mid f_i\neq f_j\ ,\ f_i, f_j\in G\}$

DÖNGÜ: $\mathbb{G}:\neq\varnothing$ olduğu sürece aşağıdaki işlemler yapılır

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

$\mathbb{G}:=\mathbb{G}-\{\{f,g\}\}$

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

$h\neq 0$ ise aşağıdaki işlemler yapılır

$\mathbb{G}:=\mathbb{G}\cup\{\{u,h\}\mid \forall u\in G\ için\}$

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

BUCHBERGER ALGORİTMASI

R Noetherian halka olduğu zaman algoritma sonlanmak zorundadır.

Örnek4.4.1: $R[x,y]=\left(\mathbb{Z}/27\mathbb{Z}\right)[x,y]$ olsun.

$g_1=9$, $g_2=x+1$, $g_3=3y^2$, $g_4=y^3+13y^2-12\in R[x,y]$ ve $G=\{g_1, g_2, g_3, g_4\}$ olsun. $x>y$ olmak üzere lex sıralamasını kullanalım.

$S(g_1,g_2)=xg_1-9g_2=-9\xrightarrow{g_1}0$, $S(g_1,g_3)=y^2g_1-3g_3=0$

$S(g_1,g_4)=y^3g_1-9g_4=-117y^2-108\xrightarrow{g_1}_{+}0,\ S(g_2,g_3)=3y^2g_2-xg_3=3y^2\xrightarrow{g_3}0$

$S(g_2,g_4)=y^3g_2-xg_4=-13xy^2+12x+y^3\xrightarrow{g_2}y^3+13y^2-12\xrightarrow{g_3}0$

$S(g_3,g_4)=yg_3-3g_4=-13y^3+9\xrightarrow{g_3}9\xrightarrow{g_1}0$

Böylece $R[x,y]$'de $\langle g_1,g_2,g_3,g_4\rangle$ ideali için bir Gröbner tabanı $G=\{g_1,g_2,g_3,g_4\}$ kümesidir.

Örnek4.4.2: $R[x,y]=\left(\mathbb{Z}/4\mathbb{Z}\right)[x,y]$ olsun. $f_1=x^4-x$, $f_2=y^3-1$, $f_3=2xy\in R[x,y]$ olsun. $I=\langle f_1,f_2,f_3\rangle$ idealini ve $x>y$ olmak üzere lex sıralamasını alalım.

$S(f_1,f_2)=y^3f_1-x^4f_2=x^4-xy^3\xrightarrow{f_1}x-xy^3\xrightarrow{f_2}0$

$S(f_1,f_3)=2yf_1-x^3f_3=-2xy\xrightarrow{f_3}0$

$S(f_2,f_3)=2xf_2-y^2f_3=-2x=2x:=f_4$ (f_4 *indirgenmiş*)

$S(f_1,f_4)=-2f_1-x^3f_4=2x\xrightarrow{f_4}0$

$S(f_2,f_4)=-2xf_2-y^3f_4=2x\xrightarrow{f_4}0$

$S(f_3,f_4)=-f_3-yf_4=0$ ve $f_3\xrightarrow{f_4}0$

Böylece $G=\{f_1,f_2,f_4\}$ kümesi $R[x,y]$'de I için Gröbner tabanıdır.

Soru: R bir değerlendirme halkası olmak üzere $R[x_1,x_2,...,x_n]$ nin sıfırdan farklı sonlu üretilmiş her ideali için Buchberger Algoritması ile sonlu adımda bir Gröbner tabanı hesaplamak mümkün müdür? (R nin Noetherian olduğunu varsaymadan)

Cevap: Aslında R, G grubu ve v değerlendirmesine karşılık gelen bir değerlendirme halkası iken G grubu Archimedian değilse Örnek4.1.8'de görüldüğü gibi Buchberger Algoritması her zaman sonlu adımda sonlanmaz.

Tanım4.4.3: $R[x_1,x_2,...,x_n]$ halkasının sonlu üretilmiş her bir I ideali için $R[x_1,x_2,...,x_n]$ nin $\langle lt(f)|\ f\in I\rangle$ ideali sonlu üretilmiş ise R halkasına bir **Gröbner halkası** denir.

4.5 Esas İdeal Bölgesi Üzerinde Dinamik Gröbner Tabanı

$a \in R$ ise $M(a)$ çarpımsal alt kümesi üzerinde R nin yerelleştirmesinin R_a ile gösterileceğini söylemiştik.

Ayrıca her bir $a_1, a_2, ..., a_k \in R$ için $R_{a_1 \cdot a_2 \cdot ... \cdot a_k} = \left(R_{a_1 \cdot a_2 \cdot ... \cdot a_{k-1}}\right)_{a_k}$ şeklinde yazılacaktır.

Tanım4.5.1: R halkasının çarpımsal alt kümeleri $S_1, S_2, ..., S_k$ olsun. Her $s_1 \in S_1$, $s_2 \in S_2$,..., $s_k \in S_k$ için $\sum_{i=1}^{k} a_i \cdot s_i = 1$ olacak şekilde $\exists a_1, a_2, ...a_k \in R$ varsa $S_1, S_2, ..., S_k$ kümelerine **comaximal** denir.

Tanım4.5.2: R bir halka, $f, g \in R[x_1, x_2, ..., x_n] - \{0\}$, $">"$ bir terim sıralaması ve $I = \langle f_1, f_2, ..., f_s \rangle$ $R[x_1, x_2, ..., x_n]$ nin sıfırdan farklı sonlu üretilmiş bir ideali olsun. $g_1, g_2, ..., g_t \in R[x_1, x_2, ..., x_n]$ için $I = \langle g_1, g_2, ..., g_t \rangle$, $\{lc(g_1), lc(g_2), ..., lc(g_t)\}$ bölme işlemine göre tam sıralı bir küme ve her bir $i \neq j$ için $S(g_i, g_j) \xrightarrow{G}_{+} 0$ ise $G = \{g_1, g_2, ..., g_t\}$ kümesine I ideali için **özel Gröbner tabanı** denir.

Not: R nin cisim olması durumunda bu tanım Gröbner tabanının klasik tanımı ile çakışır.

Tanım4.5.3: R bir halka, $f, g \in R[x_1, x_2, ..., x_n] - \{0\}$, $">"$ bir terim sıralaması ve $I = \langle f_1, f_2, ..., f_s \rangle$ $R[x_1, x_2, ..., x_n]$ nin sıfırdan farklı sonlu üretilmiş bir ideali olsun. Her bir $\left(S_i^{-1}R\right)[x_1, x_2, ..., x_n]$ yerelleştirmesinde $\langle f_1, f_2, ..., f_s \rangle$ için özel Gröbner tabanı G_i ve $S_1, S_2, ..., S_k$ lar R halkasının sonlu üretilmiş comaximal çarpımsal alt kümeleri ise $G = \{(S_1, G_1), (S_2, G_2), ..., (S_k, G_k)\}$ kümesine I ideali için **dinamik Gröbner tabanı** denir.

Önerme4.5.4: R esas ideal bölgesi, $I=\langle f_1, f_2,..., f_s\rangle$ $R[x_1, x_2,..., x_n]$ nin sıfırdan farklı sonlu üretilmiş ideali, $f \in R[x_1, x_2,..., x_n]$ ve "$>$" bir terim sıralaması olsun. $G=\{g_1, g_2,..., g_t\}$ kümesinin $R[x_1, x_2,..., x_n]$ halkasında I ideali için bir özel Gröbner tabanı olduğunu varsayalım. O zaman $f \in I$ olması için gerekli ve yeterli koşul $f \xrightarrow{G}_{+} 0$ olmasıdır.

Kanıt: $\Leftarrow$: $f \xrightarrow{G}_{+} 0$ ise $f \in \langle g_1, g_2,..., g_t\rangle = I$ olur.

$\Rightarrow$: $f \in I$ olsun.

$R[x_1, x_2,..., x_n]$ halkasında f polinomunun G ile bölümünden kalan r polinomunun sıfırdan farklı olduğunu varsayalım.

Bunun anlamı $lt(r)$; $lt(g_1), lt(g_2),..., lt(g_t)$ nin hiçbiri tarafından bölünememektedir. G kümesi aynı zamanda her bir $P \in R$ indirgenemez elemanı için $R_{PR}[x_1, x_2,..., x_n]$ halkasında $\langle f_1, f_2,..., f_s\rangle$ ideali için bir Gröbner tabanıdır.

R halkasında indirgenemez herhangi bir eleman P olsun. $R_{PR}[x_1, x_2,..., x_n]$ halkasında $\langle f_1, f_2,..., f_s\rangle$ için bir Gröbner tabanı G olduğundan $lp(r)$; $lp(g_1), lp(g_2),..., lp(g_t)$ lerin en az biri tarafından bölünebilir. Fakat $lp(g_i) \mid lp(r)$ olacak şekildeki her bir g_i polinomu için $lc(g_i)$, $lp(r)$ yi bölmemektedir.

$g_{i_1}, g_{i_2},..., g_{i_k}$ ler yukarıdaki koşulu sağlayan polinomlar olsun.

$lc(g_{i_1}) \mid lc(g_{i_2}) \mid ... \mid lc(g_{i_k})$ olduğunu varsayalım. (Özel Gröbner tabanı tanımından bu varsayım yapılabilir.)

R bir esas ideal bölgesi olduğundan $lc(g_{i_1}) = u \cdot P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot ... \cdot P_l^{\alpha_l}$ ve $lc(r) = v \cdot P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot ... \cdot P_l^{\beta_l}$ yazılabilir. Burada P_i ler R deki indirgenemez farklı elemanlar, u, v R halkasında terslenebilir elemanlar ve $\alpha_i, \beta_i \in \mathbb{N}$ dir.

Mutlaka $\alpha_{i_0} > \beta_{i_0}$ olacak şekilde bir $1 \le i_0 \le l$ vardır. Fakat bu $R_{P_{i_0}R}[x_1, x_2, ..., x_n]$ halkasında $\langle f_1, f_2, ..., f_s \rangle$ için G kümesinin Gröbner tabanı olması ile çelişir.

Dolayısıyla r kalan polinomu sıfır olmalıdır. $f \xrightarrow{G}_{+} r = 0$ dır. □

Teorem4.5.5: R esas ideal bölgesi, $I = \langle f_1, f_2, ..., f_t \rangle$ $R[x_1, x_2, ..., x_n]$ nin sıfırdan farklı sonlu üretilmiş bir ideali, $f \in R[x_1, x_2, ..., x_n]$ ve ">" bir terim sıralaması olsun. $G = \{ (S_1, G_1), (S_2, G_2), ..., (S_k, G_k) \}$, $R[x_1, x_2, ..., x_n]$ halkasında I ideali için dinamik Gröbner tabanı olsun. O zaman $f \in I$ olması için gerekli ve yeterli koşul her bir $1 \le i \le k$ için $(S_i^{-1}R)[x_1, x_2, ..., x_n]$ halkasında $f \xrightarrow{G_i}_{+} 0$ olmasıdır.

Kanıt: $\Rightarrow$: Önerme4.5.4 den görülür.

$\Leftarrow$:

Her bir $1 \le i \le k$ için $(S_i^{-1}R)[x_1, x_2, ..., x_n]$ halkasında $f \xrightarrow{G_i}_{+} 0$ olduğundan her $1 \le i \le k$ için $(S_i^{-1}R)[x_1, x_2, ..., x_n]$ halkasında $f \in \langle f_1, f_2, ..., f_t \rangle$ dir.

Bunun anlamı her bir $1 \le i \le k$ için $f = \frac{h_{i,1}}{s_i} \cdot f_1 + \frac{h_{i,2}}{s_i} \cdot f_2 + ... + \frac{h_{i,t}}{s_i} \cdot f_t$ olacak şekilde $\frac{h_{i,1}}{s_i}, \frac{h_{i,2}}{s_i}, ..., \frac{h_{i,t}}{s_i} \in (S_i^{-1}R)[x_1, x_2, ..., x_n]$ olmasıdır.

Burada $h_{i,1}, h_{i,2}, ..., h_{i,t} \in R[x_1, x_2, ..., x_n]$ ve $s_i \in S_i$ dir.

Dolayısıyla her bir $1 \le i \le k$ için $s_i \cdot f = h_{i,1} \cdot f_1 + h_{i,2} \cdot f_2 + ... + h_{i,t} \cdot f_t$ olacak şekilde $h_{i,1}, h_{i,2}, ..., h_{i,t} \in R[x_1, x_2, ..., x_n]$ ve $s_i \in S_i$ vardır.

$S_1, S_2, ..., S_k$ kümeleri comaximal olduğundan $\sum_{i=1}^{k} a_i \cdot s_i = 1$ olacak şekilde $a_1, a_2, ..., a_k \in R$ vardır.

$i=1$ *için* $s_1 \cdot f = h_{1,1} \cdot f_1 + h_{1,2} \cdot f_2 + ... + h_{1,t} \cdot f_t$ .....(1)
$i=2$ *için* $s_2 \cdot f = h_{2,1} \cdot f_1 + h_{2,2} \cdot f_2 + ... + h_{2,t} \cdot f_t$ .....(2)
$\vdots$
$i=k$ *için* $s_k \cdot f = h_{k,1} \cdot f_1 + h_{k,2} \cdot f_2 + ... + h_{k,t} \cdot f_t$ .....(k) olur.

(1) denklemi a_1 ile, (2) denklemi a_2 ile, ... (k) denklemi a_k ile çarpılarak oluşturulan denklemler taraf tarafa toplanıp düzenlenirse

$$f = \underbrace{\left(\sum_{i=1}^{k} a_i \cdot h_{i,1}\right)}_{\in R[x_1,x_2,...,x_n]} f_1 + \underbrace{\left(\sum_{i=1}^{k} a_i \cdot h_{i,2}\right)}_{\in R[x_1,x_2,...,x_n]} f_2 + ... + \underbrace{\left(\sum_{i=1}^{k} a_i \cdot h_{i,t}\right)}_{\in R[x_1,x_2,...,x_n]} f_t \in I \text{ bulunur.}$$

Böylece $R[x_1, x_2, ..., x_n]$ halkasında $f \in I$ bulunur.□

4.6 Buchberger Algoritmasının Dinamik Versiyonu

R bir esas ideal bölgesi, $I = \langle f_1, f_2, ..., f_t \rangle$ $R[x_1, x_2, ..., x_n]$ halkasının sıfırdan farklı sonlu üretilmiş bir ideali ve "$>$" bir terim sıralaması olsun. Amacımız I için bir Gröbner tabanı elde etmektir.

Buradaki Algoritma ayrık değerlendirme halkaları için olan Buchberger Algoritması gibi çalışır. Tek fark R halkasında bölme altında karşılaştırılamaz iki a ve b elemanlarının ele alındığı zaman olur. Bu durumda $d = \gcd(a,b)$ hesaplanır ve $\gcd(a',b') = 1$ olmak üzere $a = d \cdot a'$ ve $b = d \cdot b'$ şeklinde çarpanlara ayrılır. O zaman iki dal açılır: Hesaplamalar $R_{a'}$ ve $R_{b'}$ halkalarında yapılır.

I.Durum: Bölme algoritması yapıldığında karşılaştırılamaz iki a ve b elemanları ile karşılaşılması durumu.

$X^{\beta} \mid X^{\alpha}$ olmak üzere $a \cdot X^{\alpha} = lt(f)$ nın başka bir $b \cdot X^{\beta} = lt(g)$ terimi ile bölünmek istensin.

• $R_{b'}$ halkasında: $f=\frac{a'}{b'}\cdot\frac{X^{\alpha}}{X^{\beta}}\cdot g+r$ $\left(m\deg(r)<m\deg(f)\right)$ ve f yerine r yazılarak bölme devam ettirilir.

• $R_{a'}$ halkasında: $lt(f)$ terimi $lt(g)$ tarafından bölünemez ve böylece $f\xrightarrow{\{g\}}f$ olur.

II.Durum: $lt(f)=a\cdot X^{\alpha}$ ve $lt(g)=b\cdot X^{\beta}$ olmak üzere $S(f,g)$ hesaplandığı zaman karşılaştırılamaz iki a ve b elemanları ile karşılaşılması durumu.

Her bir i için $\gamma_i=\max(\alpha_i,\beta_i)$ olmak üzere $\gamma=(\gamma_1,\gamma_2,...,\gamma_n)$ ile gösterilir.

• $R_{b'}$ halkasında: $S(f,g)=\frac{X^{\gamma}}{X^{\alpha}}\cdot f-\frac{a'}{b'}\cdot\frac{X^{\gamma}}{X^{\beta}}\cdot g$ dır.

• $R_{a'}$ halkasında: $S(f,g)=\frac{b'}{a'}\cdot\frac{X^{\gamma}}{X^{\alpha}}\cdot f-\frac{X^{\gamma}}{X^{\beta}}\cdot g$ dır.

G' her bir yeni dalda kümesi bir Gröbner tabanı olmak üzere $S(f,g)\xrightarrow{G'}h\neq 0$ ise $S(f,g)$ polinomu G' kümesine eklenmek zorundadır.

4.6.1 Açıklamalar:

(1) Bir esas ideal bölgesinin herhangi bir yerelleştirmesi bir esas ideal bölgesidir.

(2) Bu algoritma sonlu adımda bitmek zorundadır.

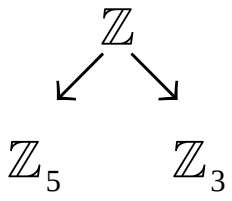
(3) R_i halkasının parçalanışı $\gcd(a',b')=1$ olmak üzere $(R_i)_{a'}$ ve $(R_i)_{b'}$ tipinde iki halka göz önüne alınarak yapılır.

Örnek4.6.2: $f_1=10xy+1$, $f_2=6x^2+3\in\mathbb{Z}[x,y]$ ve sıralama $x>y$ olmak üzere lex olsun. $\mathbb{Z}[x,y]$ halkasında $I=\langle f_1,f_2\rangle$ ideali için bir dinamik Gröbner tabanı oluşturalım.

$lc(f_1)$ ve $lc(f_2)$ bölme altında karşılaştırılamayacağından $S(f_1,f_2)$ hesaplanırken bir sorun ortaya çıkacaktır.

Bunun için;

$\gcd(10,6)=2$, $10=2\times5$, $6=2\times3$ olduğundan iki dal açılmalıdır.



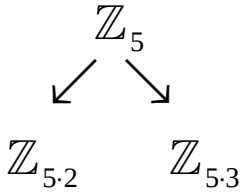
$\mathbb{Z}_5$ ‘de:

$$S(f_1,f_2)=\frac{3}{5}\frac{x^2y}{xy}\cdot f_1-\frac{x^2y}{x^2}\cdot f_2=\frac{3}{5}x\cdot f_1-y\cdot f_2=\frac{3}{5}x-3y:=f_3$$

Fakat $lc(f_1)$ ve $lc(f_3)$ bölme altında karşılaştırılamayacağından $S(f_1,f_3)$ hesaplanırken bir sorun ortaya çıkar.

Bunun için;

$\gcd\left(10,\frac{3}{5}\right)=\gcd(2,3)=1$, $2=1\times2$, $3=1\times3$ olduğundan iki dal açılmalıdır.



$\mathbb{Z}_{5\cdot2}$ ‘de:

$$S(f_1,f_3)=\frac{\frac{3}{5}}{10}\frac{xy}{xy}\cdot f_1-\frac{xy}{x}\cdot f_3=\frac{3}{50}\cdot f_1-y\cdot f_3=3y^2+\frac{3}{50}:=f_4$$

$$S(f_1,f_4)=\frac{3}{10}\frac{xy^2}{xy}\cdot f_1-\frac{xy^2}{y^2}\cdot f_4=\frac{3}{10}y\cdot f_1-x\cdot f_4=-\frac{3}{50}x+\frac{3}{10}=-\frac{1}{10}f_3\xrightarrow{f_3}0$$

$$S(f_2, f_3) = \frac{x^2}{x^2}\cdot f_2 - \frac{6}{\frac{3}{5}}\frac{x^2}{x}\cdot f_3 = f_2 - 10x\cdot f_3 = 30xy + 3 = 3f_1 \xrightarrow{f_1} 0$$

$$S(f_2, f_4) = \frac{x^2y^2}{x^2}\cdot f_2 - \frac{6}{3}\frac{x^2y^2}{y^2}\cdot f_4 = y^2 f_2 - 2x^2\cdot f_4 = -\frac{3}{25}x^2 + 3y^2 \xrightarrow{f_2} f_4 \xrightarrow{f_4} 0$$

$$S(f_3, f_4) = \frac{xy^2}{x}\cdot f_3 - \frac{\frac{3}{5}}{3}\frac{xy^2}{y^2}\cdot f_4 = y^2 f_3 - \frac{1}{5}x\cdot f_4 = -\frac{3}{250}x - 3y^3 \xrightarrow{f_3} -y\cdot f_4 \xrightarrow{f_4} 0$$

Böylece $G_1 = \left\{ 10xy+1,\ 6x^2+3,\ \frac{3}{5}x-3y,\ 3y^2+\frac{3}{50} \right\}$ kümesi $M(5,2)^{-1}\mathbb{Z} = \mathbb{Z}_{5\cdot 2}$ yaprağında $I = \langle f_1, f_2 \rangle$ ideali için bir özel Gröbner tabanıdır.

$\mathbb{Z}_{5\cdot 3}$ 'de:

$$S(f_1, f_3) = \frac{xy}{xy}\cdot f_1 - \frac{10}{\frac{3}{5}}\frac{xy}{x}\cdot f_3 = (10xy+1) - \frac{50}{3}\left(\frac{3}{5}xy - 3y^2\right) = 50y^2 + 1 := g_4$$

$$S(f_1, g_4) = \frac{xy^2}{xy}\cdot f_1 - \frac{10}{50}\frac{xy^2}{y^2}\cdot g_4 = y(10xy+1) - \frac{1}{5}x(50y^2+1) = -\frac{1}{5}x + y \xrightarrow{f_3} 0$$

$$S(f_2, f_3) = \frac{x^2}{x^2}\cdot f_2 - \frac{6}{\frac{3}{5}}\frac{x^2}{x}\cdot f_3 = (6x^2+3) - \frac{30}{3}x\left(\frac{3}{5}x - 3y\right) = 30xy + 3 = 3f_1 \xrightarrow{f_1} 0$$

$$S(f_2, g_4) = \frac{x^2y^2}{x^2}\cdot f_2 - \frac{6}{50}\frac{x^2y^2}{y^2}\cdot g_4 = y^2(6x^2+3) - \frac{3}{25}x^2(50y^2+1)$$
$$= -\frac{3}{25}x^2 + 3y^2 \xrightarrow{f_3} -y\left(\frac{3}{5}x - 3y\right) \xrightarrow{f_3} 0$$

$$S(f_3, g_4) = \frac{\frac{50}{3}}{\frac{3}{5}}\frac{xy^2}{x}\cdot f_3 - \frac{xy^2}{y^2}\cdot g_4 = \frac{250}{3}y^2\left(\frac{3}{5}x - 3y\right) - x(50y^2+1)$$
$$= 250y^3 - x \xrightarrow{f_3} 250y^3 - 5y \xrightarrow{f_3} 0$$

Böylece $G_2 = \left\{ 10xy+1 \text{ , } 6x^2+3 \text{ , } \frac{3}{5}x-3y \text{ , } 50y^2+1 \right\}$ kümesi $M(5,3)^{-1}\mathbb{Z} = \mathbb{Z}_{5\cdot 3}$ yaprağında $I = \langle f_1, f_2 \rangle$ ideali için bir özel Gröbner tabanıdır.

Uyarı! $M(5,3) = M(3,5)$ olduğundan $\mathbb{Z}_{5\cdot 3} = \mathbb{Z}_{3\cdot 5}$ dir. Dolayısıyla G_2 kümesi $\mathbb{Z}_{3\cdot 5}$ yaprağında da $I = \langle f_1, f_2 \rangle$ ideali için bir özel Gröbner tabanıdır.

$\mathbb{Z}_3$ 'de:

$$S(f_1, f_2) = \frac{x^2y}{xy}\cdot f_1 - \frac{5}{3}\frac{x^2y}{x^2}\cdot f_2 = x(10xy+1) - \frac{5}{3}y(6x^2+3) = x-5y := h_3$$

$$S(f_1, h_3) = \frac{xy}{xy}\cdot f_1 - \frac{10}{1}\frac{xy}{x}\cdot h_3 = (10xy+1) - 10y(x-5y) = 50y^2+1 := h_4$$

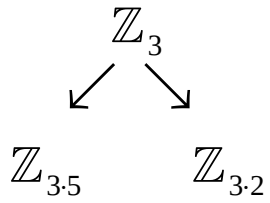
$$S(f_1, h_4) = \frac{50}{10}\frac{xy^2}{xy}\cdot f_1 - \frac{xy^2}{y^2}\cdot h_4 = 5y(10xy+1) - x(50y^2+1) = 5y-x = -h_3 \xrightarrow{h_3} 0$$

$$S(f_2, h_3) = \frac{x^2}{x^2}\cdot f_2 - \frac{6}{1}\frac{x^2}{x}\cdot h_3 = (6x^2+3) - 6x(x-5y) = 30xy+3 = 3f_1 \xrightarrow{f_1} 0$$

$$S(f_2, h_4) = \frac{50}{6}\frac{x^2y^2}{x^2}\cdot f_2 - \frac{x^2y^2}{y^2}\cdot h_4 = \frac{25}{3}y^2(6x^2+3) - x^2(50y^2+1)$$
$$= 25y^2 - x^2 \xrightarrow{h_3} -5xy+25y^2 = -5y(x-5y) = -5yh_3 \xrightarrow{h_3} 0$$

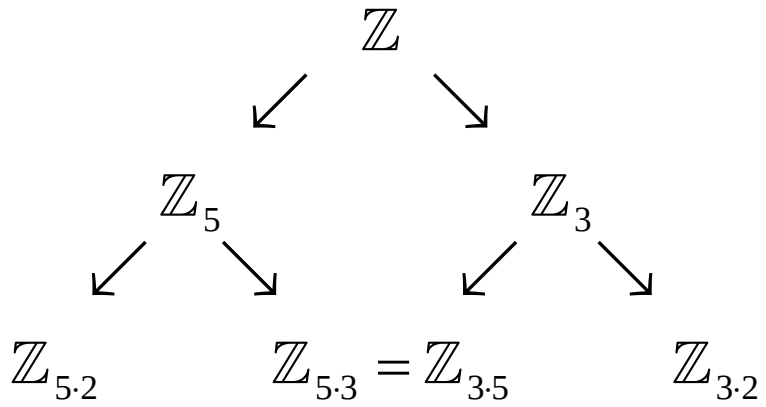
Böylece $G_3 = \{ 10xy+1 \text{ , } 6x^2+3 \text{ , } x-5y \text{ , } 50y^2+1 \}$ kümesi $M(3)^{-1}\mathbb{Z} = \mathbb{Z}_3$ yaprağında $I = \langle f_1, f_2 \rangle$ ideali için bir özel Gröbner tabanıdır.

$M(3) \subseteq M(3,2)$ olduğundan $\mathbb{Z}_3 \subseteq \mathbb{Z}_{3\cdot 5}$ dir. Dolayısıyla G_3 kümesinin $M(3,2)^{-1}\mathbb{Z} = \mathbb{Z}_{3\cdot 2}$ yaprağında $I = \langle f_1, f_2 \rangle$ ideali için bir özel Gröbner tabanı olduğu söylenebilir.



şeklinde ayrılabilir.

Sonuç olarak $I=\langle f_1, f_2\rangle$ ideali için Gröbner tabanı oluşturma probleminin dinamik değerlendirmesi aşağıdaki şekilde bir yapı oluşturur.



$I=\langle f_1, f_2\rangle=\langle 10xy+1,\ 6x^2+3\rangle$ ideali için $\mathbb{Z}[x,y]$ de elde edilen dinamik Gröbner tabanı $\mathbb{G}=\{(M(5,2),G_1),(M(5,3),G_2),(M(3,2),G_3)\}$ olur.

KAYNAKLAR

[1] Adams William W. , Loustaunau Philippe, An Introduction To Gröbner Bases, American Matematical Society, 1994

[2] Aschenbrenner Matthias, Ideal Membership in Polynomial Rings Over The Integers, Journal of the American Mathematical Society. S 0894-0347(04)00451-5 Article Electronically Published on January 15, 2004

[3] Bourbaki N, Algebra Commutative, Herman, Paris, 1964

[4] Çallıalp F, Soyut Cebir I , Hacettepe Üniversitesi Fen Fakültesi Yayınları, Ders Kitapları Dizisi:15, Beytepe, 1981

[5] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, Second Edition Springer-Verlag, New York, 1997

[6] Hungerford Thomas W. , Algebra, Springer-Verlag, New York, 1974

[7] Lang S. , Algebra, Columbia University, New York, 1974

[8] Mc Charty P, Algebraic Extensions of Fields, Blaisdell Publishing Company, Waltham, Massachusetts, Toronto, London, 1996

[9] Yengui Ihsen,Dynamical Gröbner Bases, Journal Of Algebra, Department of Mathematics, Faculty of Sciences of Sfax, Tunisia, Received 26 November 2004

[10] Yengui Ihsen, Computing a Gröbner Basis of a Polynomial Ideal Over a Principal Domain, Preprint, 2005

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı: Yusuf ÖZENİR

Uyruğu:T.C.

Doğum Tarihi ve Yeri: 20.11.1985, Samandağ/Hatay

E-mail: ozeniry@hotmail.com

EĞİTİM DURUMU

İlkokul: Yeşilköy Atatürk İlköğretim Okulu, 1996

Ortaokul: Fatih Sultan Mehmet İlköğretim Okulu, 1999

Lise: Antakya Kurtuluş Lisesi, 2002

Lisans: Trakya Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü, 2008

Yüksek Lisans: Trakya Üniversitesi Fen Bilimleri Enstitüsü, 2011

Yabancı Dil: İngilizce

İŞ TECRÜBESİ

Çalıştığı Yıllar	Çalıştığı Kurum	Görevi
2009-2010	Edirne Havsa Anadolu Lisesi	Matematik Öğretmeni