

**UKUROVA NİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ**

**YÜKSEK LİSANS TEZİ**

**Orhan SÖNMEZ**

**SONLU DOĞURAYLI DEĞİŞMELİ MONOİDLER VE UYGULAMALARI**

**MATEMATİK ANABİLİM DALI**

**ADANA, 2005**

**ÇUKUROVA ÜNİVERSİTESİ**  
**FEN BİLİMLERİ ENSTİTÜSÜ**

**SONLU DOĞURAYLI DEĞİŞMELİ MONOİDLER VE UYGULAMALARI**

**Orhan SÖNMEZ**  
**YÜKSEK LİSANS TEZİ**  
**MATEMATİK ANABİLİM DALI**

Bu tez ..... tarihinde aşağıdaki jüri üyeleri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

İmza.....  
Prof.Dr. Yusuf ÜNLÜ  
DANIŞMAN

İmza.....  
Doç.Dr. Hayrullah AYIK  
ÜYE

İmza.....  
Yrd.Doç.Dr. Ersin KIRAL  
ÜYE

Bu tez Enstitümüz Matematik Anabilim Dalında hazırlanmıştır.  
Kod No:

Prof.Dr. Aziz ERTUNÇ  
Enstitü Müdürü  
İmza ve Mühür

Bu Çalışma Ç.Ü. Bilimsel Araştırma Projeleri Birimi Tarafından Desteklenmiştir.

Proje No: FEF2003YL58

**Not:** Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

ÖZ  
YÜKSEK LİSANS TEZİ

SONLU DOĞURAYLI DEĞİŞMELİ MONOİDLER VE UYGULAMALARI

Orhan SÖNMEZ

ÇUKUROVA ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ  
MATEMATİK ANABİLİM DALI

Danışman: Prof.Dr. Yusuf ÜNLÜ

Yıl: 2005, Sayfa: 60

Jüri: Prof.Dr. Yusuf ÜNLÜ

Doç.Dr. Hayrullah AYIK

Yrd.Doç.Dr. Ersin KIRAL

Bu tezde abelyen monoid teorisinin klasik sonuçlarının bir derlemesi yapılmıştır. Ayrıca bu derlemede yer alan temel algoritmaların program olarak hayata geçirilebilmeleri için MS Visual Basic dilinde bir nesnel yapı önerilmiştir. Bu derlemede yer alan başlıca teorem ve algoritmalar şunlardır:

$M, \mathbb{Z}^n$  nin invaryant faktörleri  $d_1, \dots, d_r$  olan bir alt grubu ise

$$\mathbb{Z}^n / M \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

olduğu ve  $M$  nin bir doğuray kümesinden veya denklemlerinden bir bazının nasıl hesaplandığı gösterilmiştir.

Sonlu doğuraylı monoidlerin sadeleşmeli olma, burulmasız olma, indirgenmiş olma ve sonlu olma gibi özellikleri ve buna bağlı bazı sonuçlar incelenmiştir. Grillet'in, sonlu doğuraylı monoidler üzerindeki bir teoremine de değinilmiştir.

Minkowski-Farkas lemma ve bunun sonlu doğuraylı monoidler üzerindeki uygulamalarından bahsedilmiştir. Bu lemma kullanılarak,  $\mathbb{Q}^n$  nin bir alt uzayının; eğer varsa, belirli özellikteki negatif olmayan elemanlarını veya kuvvetli pozitif elemanlarını bulacak algoritmalar ile  $\mathbb{N}^n / \sim_M$  nin bir grup olup olmadığına veya bir afin yarıgrubu olup olmadığına karar veren algoritmalar verilmiştir.  $U(\mathbb{N}^n / \sim_M)$  nin hesaplanması için yine bir algoritma verilmiştir. Rasyonel katsayılı bir homojen lineer denklem sisteminin, tüm koordinatları negatif olmayan tamsayı olacak şekilde bir aşık olmayan çözüme sahip olup olmadığının kontrolü için bir algoritma verilmiştir.  $\mathbb{N}^n$  nin iki sonlu doğuraylı alt monoidinin kesişiminin aşık olup olmadığının belirlenmesi, eğer aşık değilse kesişimindeki bir elemanın bulunması için bir metod verilmiştir.

**Anahtar Kelimeler:** Sonlu doğuraylı değişmeli monodiler, sadeleşmeli olma, burulmasız olma, indirgenmiş olma, kuvvetli pozitif eleman.

## ABSTRACT

### MSc THESIS

# FINITELY GENERATED COMMUTATIVE MONOIDS AND ITS APPLICATIONS

Orhan SÖNMEZ

DEPARTMENT OF MATHEMATICS  
INSTITUTE OF NATURAL AND APPLIED SCIENCES  
UNIVERSITY OF ÇUKUROVA

Supervisor: Prof.Dr. Yusuf ÜNLÜ

Year: 2005, Pages: 60

Jury: Prof.Dr. Yusuf ÜNLÜ

Assoc.Prof.Dr. Hayrullah AYIK

Assist.Prof.Dr. Ersin KIRAL

In this thesis we give an exposition of the fundamental results in abelian monoid theory. In addition to this we give a description of some classes in MS Visual Basic that can be used to implement the algorithms which take place in this exposition. Following is a list of some important theorems and algorithms in this thesis.

If  $M$  is a subgroup of  $\mathbb{Z}^n$  with invariant factors  $d_1, \dots, d_r$  then it is shown that

$$\mathbb{Z}^n/M \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}.$$

Furthermore, we give an algorithm to compute a basis of a subgroup of  $\mathbb{Z}^n$  from one of its systems of generators or its defining equations.

We discuss the properties of finitely generated monoids such as of being cancellative, torsion free, reduced and finite and give some results. We mention a result by Grillet on finitely generated monoids.

Minkowski-Farkas lemma and some of its consequences on finitely generated monoids are given. Especially we apply this lemma to decide when a subspace of  $\mathbb{Q}^n$  has a non negative or strongly positive elements, if any. We give algorithms to find out whether  $\mathbb{N}^n / \sim_M$  is a group or an affine semigroup. We describe an algorithm to calculate  $U(\mathbb{N}^n / \sim_M)$ . An algorithmic method deciding whether a linear homogeneous system of equations has a nontrivial nonnegative solution and another algorithmic method deciding whether two submonoids of  $\mathbb{N}^n$  have nontrivial intersection and if so then finding an element in intersection is given.

**Key Words:** Finitely generated commutative monoids, being cancellative, being torsion free, being reduced, strongly positive element.

## TEŞEKKÜR

Gerek bu çalışmanın hazırlanması sırasında gerekse bu bölüme lisans öğrenci olarak geldiğim 1998 yılından bu yana yardımlarını hiç bir zaman esirgemeyen, sürekli destek olan, fikirleriyle her zaman örnek aldığım değerli danışmanım Prof. Dr. Yusuf ÜNLÜ'ye çok teşekkür ederim.

Genel olarak çalışmalarım sırasında bana her zaman destek olan Doç. Dr. Hayrullah AYIK ve Yrd. Doç. Dr. Gonca AYIK'a da teşekkürlerimi bir borç bilirim. Ayrıca Ç.Ü. Fizik bölümü öğretim elemanı Güzide ÜNLÜ'ye, Ç.Ü. Matematik Bölümü emekli öğretim üyesi Prof. Dr. Melih BORAL'a, Tez Jüri üyesi Yrd. Doç. Dr. Ersin KIRAL'a ve Ç.Ü. Matematik bölümünün diğer tüm öğretim elemanlarına destekleri için teşekkür ederim.

Yaşamım boyunca, gerek maddi gerekse manevi her türlü zorlukla mücadele ederek, yetişmemde büyük emeği olan değerli ailem; babam Ahmet SÖNMEZ'e, annem Naile SÖNMEZ'e ve kardeşim Nurhan SÖNMEZ'e de çok teşekkür ederim.

## İÇİNDEKİLER

## SAYFA

|                                                                                                                                                                                                                                                                               |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ÖZ . . . . .                                                                                                                                                                                                                                                                  | I   |
| ABSTRACT . . . . .                                                                                                                                                                                                                                                            | II  |
| TEŞEKKÜR . . . . .                                                                                                                                                                                                                                                            | III |
| İÇİNDEKİLER . . . . .                                                                                                                                                                                                                                                         | IV  |
| 1 TEMEL TANIMLAR VE SONUÇLAR . . . . .                                                                                                                                                                                                                                        | 1   |
| 2 SONLU DOĞURAYLI DEĞİŞMELİ GRUPLAR . . . . .                                                                                                                                                                                                                                 | 8   |
| 2.1 $\mathbb{Z}^n$ nin Alt Gruplarının Bazları ve Rankı . . . . .                                                                                                                                                                                                             | 8   |
| 2.2 Tamsayı Bileşenli Matrislerin Denkliği ve İnvariant Faktörleri . . . . .                                                                                                                                                                                                  | 11  |
| 2.3 Bazların Hesaplanması İle İlgili Bazı Kullanışlı Sonuçlar . . . . .                                                                                                                                                                                                       | 22  |
| 2.3.1 $\mathbb{Z}^n$ nin Bir Alt Grubunun Bir Doğuray Kümesinden Bir Bazının Hesaplanması . . . . .                                                                                                                                                                           | 22  |
| 2.3.2 $\mathbb{Z}^n$ nin Bir Alt Grubunun Denklemlerinden Bir Bazının Hesaplanması . . . . .                                                                                                                                                                                  | 23  |
| 3 SONLU DOĞURAYLI SADELEŞMELİ MONOİDLER . . . . .                                                                                                                                                                                                                             | 26  |
| 3.1 Sonlu Doğuraylı Sadeleşmeli Burulmasız Monoidler . . . . .                                                                                                                                                                                                                | 28  |
| 3.2 Sonlu Doğuraylı Sadeleşmeli İndirgenmiş Monoidler . . . . .                                                                                                                                                                                                               | 30  |
| 3.3 Sonlu Sadeleşmeli Monoidler . . . . .                                                                                                                                                                                                                                     | 34  |
| 4 MINKOWSKI-FARKAS LEMMASI VE MONOİDLERDEKİ UYGULAMALARI . . . . .                                                                                                                                                                                                            | 36  |
| 4.1 Temel Sonuçlar ve Algoritmalar . . . . .                                                                                                                                                                                                                                  | 36  |
| 4.2 Monoidlere Uygulanışları . . . . .                                                                                                                                                                                                                                        | 45  |
| 4.2.1 $\mathbb{N}^n / \sim_M$ Formundaki Bir Monoidin Grup Olup Olmadığının Kontrolü . . . . .                                                                                                                                                                                | 45  |
| 4.2.2 $\mathbb{N}^n / \sim_M$ Formundaki Bir Monoidin Afın Olup Olmadığının Saptanması, Eğer Afın İse $S \simeq \mathbb{N}^n / \sim_M$ Olacak Şekilde Bir $k \in \mathbb{N} \setminus \{0\}$ ve $\mathbb{N}^k$ nin Bir Sonlu Doğuraylı $S$ Alt Monoidinin Bulunması . . . . . | 45  |
| 4.2.3 $\mathbb{N}^n / \sim_M = U(\mathbb{N}^n / \sim_M) + C$ ve $U(\mathbb{N}^n / \sim_M) \cap C = \{0\}$ Olacak Şekilde $\mathbb{N}^n / \sim_M$ nin Birimlerinin Kümesi İle Bir $C$ Alt Monoidinin Hesaplanması . . . . .                                                    | 47  |

|       |                                                                                                                                                                                          |    |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.2.4 | Rasyonel Katsayılı Bir Homojen Lineer Denklem Sisteminin, Tüm Koordinatları Negatif Olmayan Tamsayı Olacak Şekilde Bir Aşık Olmayan Çözüme Sahip Olup Olmadığının Belirlenmesi . . . . . | 50 |
| 4.2.5 | $\mathbb{N}^n$ nin İki Sonlu Doğuraylı Alt Monoidinin Kesişiminin Aşık Olup Olmadığının Belirlenmesi, Eğer Aşık Değilse Kesişimindeki Bir Elemanın Bulunması . . . . .                   | 51 |
| 5     | ALGORİTMALAR VE ARİTMETİK İŞLEMLER İÇİN                                                                                                                                                  |    |
|       | NESNEL YAPI . . . . .                                                                                                                                                                    | 52 |
|       | KAYNAKLAR . . . . .                                                                                                                                                                      | 59 |
|       | ÖZGEÇMİŞ . . . . .                                                                                                                                                                       | 60 |

## 1. TEMEL TANIMLAR VE SONUÇLAR

Gruplarda bölüm grubunu elde etmek için onun bir normal altgrubuna, halkalarda ise onun bir idealine gerek vardır. Monoidlerde ise bu gereksinimi kongruanslar karşılar. Gerekli bütün tanımları yaptıktan sonra dikkatimizi sonlu doğuraylı monoidler üzerinde yoğunlaştıracğıız ve her sonlu doğuraylı monoidin  $\mathbb{N}^n$  nin bir bölümü olduğı durumlarda bir temsil vereceğıız.

Bu tezde  $\mathbb{Z}$  ile tamsayılar ve  $\mathbb{N}$  ile negatif olmayan tamsayıların kümesi gösterilecektir.

Denklik bağıntıları ile ilgili temel bilgileri burada kısaca hatırlayalım.  $X$  herhangi bir küme ise  $X \times X$  nin  $\sigma$  gibi bir alt kümesine  $X$  üzerinde bir *bağıntı* denir.  $(a, b) \in \sigma$  yerine  $a\sigma b$  gösterimini de kullanacağız.

$X$  üzerindeki bir  $\sigma$  bağıntısına; her  $a \in X$  için  $a\sigma a$  oluyorsa *yansımali*, her  $a, b \in X$  için  $a\sigma b$  iken  $b\sigma a$  oluyorsa *simetrik*, her  $a, b, c \in X$  için  $a\sigma b$  ve  $b\sigma c$  iken  $a\sigma c$  oluyorsa *geçişmeli* denir. Eğer  $X$  üzerindeki bir  $\sigma$  bağıntısı yansımali, simetrik ve geçişken ise  $\sigma$  ya bir *denklik bağıntısı* denir.  $\sigma$  bir denklik bağıntısı ve  $a \in X$  ise  $[a]_\sigma = \{b \in X \mid a\sigma b\}$  ya  $a$  nın *denklik sınıfı* denir. Yanlış anlaşılmaya yol açmayan durumlarda  $[a]_\sigma$  yerine  $[a]$  kullanacağız. Bilindiğı gibi  $a, b \in X$  ise  $[a] \cap [b] \neq \emptyset$  olması için gerek ve yeter koşul  $[a] = [b]$  olmasıdır. O halde denklik sınıfları  $X$  in bir parçalanışını verir. Herhangi iki elemanın denk olması için gerek ve yeter koşul elemanların bu parçalanışın aynı kümesi içinde olmasıdır.

**Tanım 1.1**  $S$  boştan farklı bir küme ve  $+$ ,  $S$  üzerinde birleşme özelliğini sağlayan bir ikili işlem ise  $(S, +)$  ikilisine bir *yarıgrup* denir.

**Tanım 1.2** Bir  $(S, +)$  yarıgrubunda her  $a \in S$  için  $a + 0 = 0 + a = a$  olacak şekilde bir  $0 \in S$  varsa  $(S, +)$  ikilisine bir *monoid* denir.

**Not 1.3** Aksi belirtilmedikçe bu tezdeki bütün monoidleri ve yarıgrupları değişmeli olarak alacağız.

**Tanım 1.4** Bir  $S$  monoidinde her  $a, b, c \in S$  için  $a + c = b + c$  olduğunda  $a = b$  oluyorsa  $S$  monoidi *sadeleşmelidir* denir.

**Tanım 1.5** Bir  $(S, +)$  monoidinde her  $a \in S$  için  $a + b = 0$  olacak şekilde bir  $b \in S$  varsa  $(S, +)$  ikilisine bir *grup* denir.



Eğer bir monoidde bir elemanın tersi varsa tektir. Bu yüzden bir  $a$  elemanın tersini  $-a$  ile göstereceğiz. Bir grubun daima sadeleşmeli bir monoid olacağı açıktır.

**Tanım 1.6**  $S$  bir monoid ve  $H \subseteq S$  olsun.  $0 \in H$  ve her  $a, b \in H$  için  $a + b \in H$  ise  $H$  ye  $S$  nin bir *alt monoidi* denir.

Verilen bir  $S$  monoidinin bütün alt monoidlerinin kesişiminin de,  $S$  nin bir alt monoidi olduğu açıktır. Bir  $S$  monoidinin bir  $A$  alt kümesi verilsin. O halde  $S$  nin  $A$  yı içeren tüm alt monoidlerinin arakesiti de bir monoiddir. Bu monoide  $A$  tarafından doğurulan monoid denir ve  $\langle A \rangle$  ile gösterilir.  $\langle A \rangle$  monoidi  $S$  nin  $A$  yı içeren (kapsamaya göre) en küçük alt monoididir. Dahası eğer  $0a = 0$  ve  $0 \leq n$  için  $(n+1)a = na + a$  ise

$$\langle A \rangle = \left\{ \sum_{i=1}^r n_i a_i \mid r \in \mathbb{N} \text{ ve her } 1 \leq i \leq r \text{ için } n_i \in \mathbb{N}, a_i \in A \right\}$$

olduğu kolayca ispatlanabilir. Aşağıda aksi söylenmedikçe  $S$  sembolü bir monoidi gösterecektir.

**Tanım 1.7**  $S = \langle A \rangle$  ise  $S$  ye  $A$  tarafından doğurulmuş ve  $A$  ya da  $S$  nin bir *doğuray kümesi* denir.

$S = \langle S \rangle$  olacağı açıktır.

**Tanım 1.8**  $S = \langle A \rangle$  ve  $A$  nın  $S$  yi doğuracak şekilde hiçbir özalt kümesi yok ise  $S$  ye  $A$  tarafından *minimal olarak doğurulmuş* ve  $A$  ya da  $S$  nin bir *minimal doğuray kümesi* denir.

**Tanım 1.9** Eğer  $S$  nin,  $S = \langle A \rangle$  olacak şekilde sonlu bir  $A$  alt kümesi varsa  $S$  ye *sonlu doğuraylı* denir.

$A, S$  grubunun bir alt kümesi ise  $\langle A \rangle$  monoidi aslında  $S$  nin bir alt grubudur.  $A$  tarafından doğurulan bu alt grubu  $\mathbf{G}(A)$  ile göstereceğiz. Eğer her  $n \in \mathbb{N}$  ve  $a \in A$  için  $n(-a)$  elemanını  $(-n)a$  şeklinde gösterirsek,

$$\mathbf{G}(A) = \left\{ \sum_{i=1}^r z_i a_i \mid r \in \mathbb{N} \text{ ve her } 1 \leq i \leq r \text{ için } z_i \in \mathbb{Z}, a_i \in A \right\}$$

olduğu kolayca gösterilebilir.

**Tanım 1.10** Eğer  $A$  sonlu ve  $S = \mathbf{G}(A)$  ise  $S$  ye *sonlu doğuraylı grup* denir.

$S_1, \dots, S_n$  bir monoidler (gruplar) dizisi olsun.  $S_1, \dots, S_n$  kümelerinin kartezyen çarpımı olan  $S_1 \times \dots \times S_n$  kümesi üzerinde

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

şeklinde bir işlem tanımlarsak  $(S_1 \times \dots \times S_n, +)$  bir monoid (grup) olur. Buna  $S_1, \dots, S_n$  nin *direk çarpımı* denir. Eğer  $S_i$  ler sadeleşmeli monoid ise  $S_1 \times \dots \times S_n$  de sadeleşmeli monoiddir.  $S_i$  ler sonlu doğuraylı ise  $S_1, \dots, S_n$  nin direk çarpımı da sonlu doğuraylıdır.

**Gösterim 1.11**  $S \times \dots \times S$  yi  $S^n$  ile göstereceğiz.

**Tanım 1.12**  $\sigma$ ,  $S$  üzerinde bir bağıntı olsun. Eğer her  $a\sigma b$  ve her  $c \in S$  için  $(a+c)\sigma(b+c)$  oluyorsa  $\sigma$  ya  $S$  üzerinde *uyumlu bir bağıntı* denir.

$\sigma$ ,  $S$  üzerinde uyumlu bir bağıntı ise, kolayca görüleceği gibi her  $a\sigma b$ ,  $c\sigma d$  için  $(a+c)\sigma(b+d)$  dir.

**Tanım 1.13**  $S$  üzerindeki uyumlu bir  $\sigma$  denklik bağıntısına  $S$  üzerinde bir *kongruans* denir.

**Gösterim 1.14** Bir  $S$  monoidi üzerindeki verilen bir  $\sigma$  kongruansı için  $S/\sigma$  ile  $S$  nin tüm elemanlarının denklik sınıflarının kümesini göstereceğiz.

$S/\sigma$  üzerinde  $+$  işlemi  $[a] + [b] = [a+b]$  olarak tanımlanırsa  $(S/\sigma, +)$  nin bir değişmeli monoid olduğu kolayca gösterilebilir.  $S/\sigma$  monoidine  $S$  nin  $\sigma$  modülüne göre *bölüm monoidi* denir. Benzer şekilde  $S$  bir grup ise  $S/\sigma$  nin bir grup ve  $S$  sonlu doğuraylı ise  $S/\sigma$  nin de sonlu doğuraylı olduğu kolayca görülebilir.

**Tanım 1.15**  $S, S'$  iki monoid olsun.  $f : S \rightarrow S'$  bir fonksiyon ve  $f(0) = 0$ ,  $\forall a, b \in S$  için  $f(a+b) = f(a) + f(b)$  ise  $f$  ye monoid *morfizmi* denir. Eğer  $f$  bire-bir {örten [hem bire-bir hem örten]} ise  $f$  ye monomorfizm {epimorfizm [izomorfizm]} denir.

Eğer  $f : S \rightarrow S'$  izomorfizm ise  $f : S \simeq S'$  veya kısaca  $S \simeq S'$  yazılır.

Eğer  $f$  izomorfizm ise  $f$  nin  $f^{-1}$  tersi de izomorfizmdir. Eğer herhangi iki monoid arasında bir izomorfizm varsa bu iki monoid *izomorftir* denir. Sadeleşmeli olma, grup olma, sonlu doğuraylı olma özellikleri izomorfizmalar altında korunur.

$f : S \rightarrow S'$  bir monoid morfizmi olsun.  $S$  üzerinde  $\ker(f)$  bağıntısını

$$\ker(f) = \{(a, b) \in S \times S \mid f(a) = f(b)\}$$

şeklinde tanımlayalım.  $f$  bir monoid morfizmi olduğundan  $\ker(f)$  nin bir kongruans olduğu kolayca gösterilebilir. Bu kongruans  $f$  nin *çekirdek kongruansı* olarak bilinir.

$f$  nin görüntü kümesi

$$\text{Im}(f) = \{f(a) \mid a \in S\}$$

ile gösterilir.  $f$  bir monoid morfizmi olduğundan  $\text{Im}(f)$  de bir monoid olur.

**Teorem 1.16**  $f : S \rightarrow S'$  bir monoid morfizmi olsun. O zaman

$$\bar{f} : S/\ker(f) \rightarrow \text{Im}(f)$$

$$\bar{f}([a]) = f(a)$$

bir izomorfizmdir. □

**Teorem 1.17**  $S, \{s_1, \dots, s_n\}$  tarafından doğurulan bir monoid olsun. O zaman  $\mathbb{N}^n$  monoidi üzerinde,  $S \simeq \mathbb{N}^n/\sigma$  olacak şekilde bir  $\sigma$  kongruansı vardır.

**İspat:**  $f : \mathbb{N}^n \rightarrow S, f(a_1, \dots, a_n) = \sum_{i=1}^n a_i s_i$  fonksiyonunu tanımlayalım. Bu fonksiyon bir epimorfizmdir.  $\sigma$  yı  $\ker(f)$  olarak alırsak bir önceki teoremden  $\bar{f}$  izomorfizm olur. ■

$\mathbb{N}^n$  üzerindeki kongruansların özelliklerini çalışmak, sonlu doğuraylı monoidlerin özelliklerini çalışmakla hemen hemen aynıdır.

Önce sadeleşme özelliği ile başlayalım. Bu amaçla  $\mathbb{Z}^n$  nin her alt grubuna bir kongruans, her kongruansa da  $\mathbb{Z}^n$  nin bir alt grubunu karşılık getireceğiz.

**Tanım 1.18**  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olsun.  $M_\sigma = \{a - b \mid (a, b) \in \sigma\} \subseteq \mathbb{Z}^n$  tanımlayalım. Burada  $a - b \in \mathbb{Z}^n, a \in \mathbb{N}^n$  den  $b \in \mathbb{N}^n$  nin bileşen bileşen çıkarılması sonucu elde edilen elemandır.  $\sigma$  bir kongruans olduğundan  $M_\sigma, \mathbb{Z}^n$  nin bir alt grubu olur.

**Tanım 1.19**  $H, \mathbb{Z}^n$  nin bir alt grubu olsun.  $\sim_H = \{(a, b) \in \mathbb{N}^n \times \mathbb{N}^n \mid a - b \in H\}$  tanımlayalım.  $\sim_H, \mathbb{N}^n$  üzerinde bir kongruansdır.

Öncelikle  $M_{\sim_H}$  in yapısını inceleyelim.

$x \in M_{\sim_H}$  olsun. Bu durumda en az bir  $(a, b) \in \sim_H$  için  $x = a - b$  olur. O halde  $(a, b) \in \mathbb{N}^n \times \mathbb{N}^n$  ve  $x = a - b \in H$  dir. Karşıt olarak  $x = a - b \in H$  ise  $(a, b) \in \sim_H$  olup,  $x \in M_{\sim_H}$  olur. O halde  $M_{\sim_H} = H$  dir. Fakat  $\sigma$  ile  $\sim_{M_\sigma}$  her zaman birbirine eşit değildir.

**Lemma 1.20**  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olsun. O halde;

1.  $\sigma \subseteq \sim_{M_\sigma}$  dır,

2. Her  $(a, b) \in \sim_{M_\sigma}$  için  $(a + c, b + c) \in \sigma$  olacak şekilde  $c \in \mathbb{N}^n$  vardır.

**İspat:**  $(a, b) \in \sigma$  ise  $M_\sigma$  nın tanımından  $a - b \in M_\sigma$  olur. Dolayısıyla  $(a, b) \in \sim_{M_\sigma}$  olur. Şimdi  $(a, b) \in \sim_{M_\sigma}$  alalım.  $a - b \in M_\sigma$  olup  $M_\sigma$  nın tanımından bir  $(x, y) \in \sigma$  için  $x - y = a - b$  dir.  $\sigma$  bir kongruans olduğundan  $(x + a, y + a) \in \sigma$  olur.  $x + b = y + a$  olup  $(x + a, x + b) \in \sigma$  elde edilir.  $x = c$  alırsak istenen elde edilmiş olur. ■

Bu sonuç sadeleşmeli olmayla  $\sigma$  nın  $\sim_{M_\sigma}$  ya eşit olması arasındaki ilişkiyi ortaya koymaktadır.

**Önerme 1.21**  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olsun. O zaman

$$\mathbb{N}^n / \sigma \text{ sadeleşmelidir} \iff \sigma = \sim_{M_\sigma}$$

**İspat:**  $\implies$ :  $\mathbb{N}^n / \sigma$  sadeleşmeli olsun.  $\sigma \subseteq \sim_{M_\sigma}$  olduğunu zaten biliyoruz.  $(a, b) \in \sim_{M_\sigma}$  alalım. Bir önceki lemmadan bir  $c \in \mathbb{N}^n$  için  $(a + c, b + c) \in \sigma$  dir. Böylece  $[a + c] = [a] + [c]$  ile  $[b + c] = [b] + [c]$  nin  $\mathbb{N}^n / \sigma$  da birbirine eşit olduğu görülür. Sadeleşme özelliğinden  $[a] = [b]$  yani  $(a, b) \in \sigma$  elde edilir. Dolayısıyla  $\sigma = \sim_{M_\sigma}$  dır.

$\impliedby$ :  $\sigma = \sim_{M_\sigma}$  olsun. Eğer  $[a] + [c] = [b] + [c]$  ise  $(a + c, b + c) \in \sigma$  dır. Buradan  $(a + c) - (b + c) \in M_\sigma$  dolayısıyla  $a - b \in M_\sigma$  elde edilir. Böylece  $(a, b) \in \sim_{M_\sigma} = \sigma$  olur. O halde  $[a] = [b]$  dir. Böylece  $\mathbb{N}^n / \sigma$  nin sadeleşmeli olduğu görülür. ■

**Tanım 1.22**  $\mathbb{Z}^n$  nin bir  $H$  alt grubu verilsin.  $\mathbb{Z}^n$  üzerinde

$$a \equiv_H b \iff a - b \in H$$

olarak tanımlayalım.  $\equiv_H$  bağıntısı daha açık olarak

$$\equiv_H = \{(a, b) \in \mathbb{Z}^n \times \mathbb{Z}^n \mid a - b \in H\}$$

dir.

$\sim_H$  da olduğu gibi  $\equiv_H$  nin de bir kongruans olduğu kolayca gösterilebilir. Böylece  $\mathbb{Z}^n / \equiv_H$  bir monoid olur. Ayrıca  $[a - a]_{\equiv_H} = [a]_{\equiv_H} + [-a]_{\equiv_H} = [0]_{\equiv_H}$  olduğundan  $\mathbb{Z}^n / \equiv_H$  bir grup olur. Genellikle bu grup  $\mathbb{Z}^n / H$  ile gösterilir ve  $\mathbb{Z}^n$  nin  $H$  üzerindeki *bölüm grubu* olarak adlandırılır. Bu gruba bir örnek olarak  $n = 1$  ve  $1 < d \in \mathbb{N}$  için  $H = (d) = \mathbf{G}(\{d\})$  olsun.  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  için  $a \equiv_H b$  olması için gerek ve yeter koşul  $a - b \in H = (d)$  veya

$d \mid a - b$  olmasıdır. O halde  $\equiv_H$  bağıntısının eşdeğerlik sınıfları,  $d$  modülüne göre kalan sınıflarıdır.  $\mathbb{Z}/\equiv_H$  de toplamanın tanımı göz önüne alınırsa  $\mathbb{Z}/\equiv_H = \mathbb{Z}_d$  olduğu görülür.

Aşağıdaki sonuç  $\sim_M$  ile  $\equiv_H$  arasındaki bağıntıyı vermektedir.

**Önerme 1.23**  $H, \mathbb{Z}^n$  nin bir alt grubu olsun.  $i([a]_{\sim_H}) = [a]_{\equiv_H}$  olarak tanımlanan

$$i : \mathbb{N}^n / \sim_H \rightarrow \mathbb{Z}^n / \equiv_H$$

dönüşümü bir monoid monomorfizmidir.

**İspat:**  $[a]_{\sim_H} = [b]_{\sim_H}$  olsun. O zaman  $a - b \in H$  olup  $[a]_{\equiv_H} = [b]_{\equiv_H}$  dir. O halde  $i$ , iyi tanımlıdır.

$i$  nin monoid morfizmi olduğu açıktır. O halde  $i$  nin birebir olduğunu gösterelim.  $a, b \in \mathbb{N}^n$  olmak üzere  $[a]_{\equiv_H} = [b]_{\equiv_H}$  olsun. O halde  $a - b \in H$  ve buradan  $[a]_{\sim_H} = [b]_{\sim_H}$  elde edilir. Böylece  $i$  nin bir monomorfizm olduğu görülür. ■

**Sonuç 1.24**  $S$  sonlu doğuraylı bir monoid olsun. O zaman,  $S$  nin sadeleşmeli olması için gerek ve yeter koşul  $S$  nin, bir grubun alt monoidine izomorfik olmasıdır.

**İspat:** Teorem 1.17 den  $n \in \mathbb{N}$  ve  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olmak üzere,  $S, \mathbb{N}^n/\sigma$  ya izomorfiktir. Önerme 1.21 den de  $\sigma = \sim_{M_\sigma}$  elde edilir. O zaman  $S, \mathbb{N}^n/\sim_{M_\sigma}$  ya izomorfiktir. Önerme 1.23 ise  $\mathbb{N}^n/\sim_{M_\sigma}$  nın  $\mathbb{Z}^n/\equiv_{M_\sigma} = \mathbb{Z}^n/M_\sigma$  nın bir alt monoidine izomorfik olduğunu söyler ki bu da ispatı bitirir. ■

**Tanım 1.25**  $x \in \mathbb{Z}^n$  nin her koordinatı pozitif ise  $x$  'e *kuvvetli pozitif* denir. Benzer şekilde  $x \in \mathbb{Z}^n$  nin her koordinatı sıfır yada sıfırdan büyükse  $x$  'e *negatif olmayan* denir.

**Önerme 1.26**  $S$ , sonlu doğuraylı bir monoid olsun. O halde aşağıdakiler birbirine denktir.

1.  $S$  bir gruptur.
2.  $n \in \mathbb{N}$  ve  $\mathbb{Z}^n$  nin kuvvetli pozitif eleman içeren bir  $H$  alt grubu için  $S \simeq \mathbb{N}^n / \sim_H$  dir.
3.  $n \in \mathbb{N}$  ve  $\mathbb{Z}^n$  nin bir  $H$  alt grubu için  $S \simeq \mathbb{Z}^n / H = \mathbb{Z}^n / \equiv_H$  dir.

**İspat:**  $1 \implies 2$ :  $S$  bir grup ise  $S$  sadeleşmeli bir monoiddir. Sonuç 1.24 nın ispatından  $n \in \mathbb{N}$  ve  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olmak üzere  $S \simeq \mathbb{N}^n / \sim_{M_\sigma}$  dir.  $S$  grup olduğundan

$\mathbb{N}^n / \sim_{M_\sigma}$  da gruptur. O zaman  $[(1, \dots, 1)]_{\sim_{M_\sigma}}$  nin tersi vardır.  $[(a_1, \dots, a_n)]_{\sim_{M_\sigma}}$  tersi olsun. O halde

$$[(a_1 + 1, \dots, a_n + 1)]_{\sim_{M_\sigma}} = [(1, \dots, 1)]_{\sim_{M_\sigma}} + [(a_1, \dots, a_n)]_{\sim_{M_\sigma}} = [(0, \dots, 0)]_{\sim_{M_\sigma}}$$

olur. Sonuç olarak  $(a_1 + 1, \dots, a_n + 1) \sim_{M_\sigma} (0, \dots, 0)$  dır. Tanımdan dolayı

$$(a_1 + 1, \dots, a_n + 1) - (0, \dots, 0) \in M_\sigma$$

olur. Dolayısıyla  $(a_1 + 1, \dots, a_n + 1) \in M_\sigma$  olur ki zaten bu bir kuvvetli pozitif elemandır. O halde istenen elde edilmiş olur. Çünkü  $M_\sigma, \mathbb{Z}^n$  nin bir alt grubudur.

2  $\implies$  3: Önerme 1.23 deki  $i$  dönüşümünün örten olduğunu göstermemiz yeterlidir.  $a \in H$  bir kuvvetli pozitif eleman olsun.  $[x]_{\equiv_H} \in \mathbb{Z}^n / H$  alalım.  $a$  nın bütün koordinatları pozitif olduğu için  $ka + x \in \mathbb{N}^n$  olacak şekilde  $k \in \mathbb{N}$  vardır.  $ka \in H$  olduğundan

$$[ka + x]_{\equiv_H} = [x]_{\equiv_H}$$

elde edilir.  $i([ka + x]_{\sim_H}) = [ka + x]_{\equiv_H} = [x]_{\equiv_H}$  olduğundan  $i$  örtendir.

3  $\implies$  1:  $\mathbb{Z}^n / H$  bir grup olduğu için  $S$  de bir gruptur. ■

## 2. SONLU DOĞURAYLI DEĞİŞMELİ GRUPLAR

Burada Grup teorisinin klasik sonuçlarından biri olan sonlu doğuraylı değişmeli grupların temel teoremi ile ilgileneceğiz. Önce bu teoremi ifade edelim.

**Teorem 2.1** Sonlu doğuraylı her değişmeli grup,  $d_1, \dots, d_r, k$  her  $1 \leq i \leq r-1$  için  $d_i, d_{i+1}$  i bölecek şekilde bir takım pozitif tamsayılar olmak üzere  $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$  grubuna izomorftur.

Burada da  $\mathbb{Z}_n$  ile  $n$  modülüne göre kalan sınıflarının toplama altındaki grubu gösterilmektedir.

Temel teoremin kanıtında kullanılan fikirler şunlardır:

1.  $H, \mathbb{Z}^n$  nin bir alt grubu olmak üzere her sonlu doğuraylı grup  $\mathbb{Z}^n/H$  formundadır.
2.  $\{f_1, \dots, f_n\}, \mathbb{Z}^n$  nin bir bazı olsun. Her  $i \in \{1, \dots, r\}$  için  $d_i$  pozitif bir tamsayı olmak üzere  $H = \mathbf{G}(\{d_1 f_1, \dots, d_r f_r\})$  olsun. O zaman  $\mathbb{Z}^n/H \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$  dir.
3.  $\{f_1, \dots, f_n\}, \mathbb{Z}^n$  nin bir bazı olsun. O zaman  $\mathbb{Z}^n$  nin her alt grubunun  $\{d_1 f_1, \dots, d_r f_r\}$  formunda bir bazı vardır.

### 2.1 $\mathbb{Z}^n$ nin Alt Gruplarının Bazları ve Rankı

**Tanım 2.2**  $M, \mathbb{Z}^n$  nin bir alt grubu olsun. Eğer  $M$  deki her eleman,  $z_1, \dots, z_r \in \mathbb{Z}$  olmak üzere  $m = \sum_{i=1}^r z_i m_i$  şeklinde tek türlü yazılabiliyorsa  $\{m_1, \dots, m_r\} \subset M$  kümesine  $M$  nin bir bazı denir.  $(z_1, \dots, z_r) \in \mathbb{Z}^r$  ye de  $m$  nin  $\{m_1, \dots, m_r\}$  sıralı bazına göre koordinatları denir.

**Sonuç 2.3**  $\{m_1, \dots, m_r\}$  nin  $M$  nin bir bazı olması için gerek ve yeter koşul

1. Her  $m \in M$  için  $z_1, \dots, z_r \in \mathbb{Z}$  olmak üzere  $m = \sum_{i=1}^r z_i m_i$  şeklinde yazılabilir,
2. Eğer  $z_1, \dots, z_r \in \mathbb{Z}$  olmak üzere  $\sum_{i=1}^r z_i m_i = 0$  ise her  $i \in \{1, \dots, r\}$  için  $z_i = 0$  olmasıdır.

Birinci koşul  $\{m_1, \dots, m_r\}$  kümesinin  $M$  için bir doğuray kümesi olduğunu yani  $M = \mathbf{G}(\{m_1, \dots, m_r\})$  olduğunu, ikinci koşul ise bir bakımdan lineer bağımsızlığı ifade

etmektedir. Bu son ifadeye kesinlik kazandırmak için

$$m_1, \dots, m_r \in \mathbb{Z}^n \text{ lineer bağımsızdır} \iff m_1, \dots, m_r, \mathbb{Q}^n \text{ de lineer bağımsızdır}$$

olduğuna dikkat edelim.

**Gösterim 2.4**  $e_i, \mathbb{N}^n$  nin  $i$ -inci koordinatı 1, diğer bütün koordinatları 0 olan elemanıdır.

$\{e_1, \dots, e_n\}$  nin  $\mathbb{Z}^n$  nin bir bazı olduğuna dikkat edelim.

**Önerme 2.5**  $M, \mathbb{Z}$  nin bir alt grubu ise  $M = \mathbf{G}(\{z\})$  olacak şekilde bir  $z \in M$  vardır.

**İspat:**  $M = \{0\}$  ise  $M = \mathbf{G}(\{0\})$  dır.

$M \neq \{0\}$  varsayalım.

$M$  bir grup olduğundan  $M$  de pozitif elemanlar vardır. O halde  $\{h \in M \mid h > 0\}$  kümesi boştan farklıdır. Bu yüzden bu kümenin bir minimum elemanı vardır. Buna  $z$  diyelim. Şimdi  $M = \mathbf{G}(\{z\})$  olduğunu gösterelim.  $\mathbf{G}(\{z\}) \subseteq M$  olduğu aşikar. O zaman  $h \in M$  alalım.  $\mathbb{Z}$  deki bölme algoritması gereği;  $q, r \in \mathbb{Z}$  vardır öyleki  $h = qz + r$ ,  $0 \leq r < z$ . Dolayısıyla  $0 \leq r = h - qz < z$  dir. Fakat  $M$  deki sıfırdan büyük elemanların en küçüğü  $z$  idi. O halde  $r = 0$  dir. Dolayısıyla  $h = qz \in \mathbf{G}(\{z\})$  dir. ■

$\{0\} \subseteq \mathbb{Z}^n$  in bir bazının boş küme olduğuna dikkat edelim. Şimdi  $\mathbb{Z}^n$  nin bir alt grubunun bir bazının eleman sayısının en fazla ne olabileceğini söyleyeceğiz.

**Önerme 2.6**  $M, \mathbb{Z}^n$  nin bir alt grubu olsun. O zaman  $M$  nin bir bazı en fazla  $n$  eleman içerir.

**İspat:** Her  $j \in \{1, \dots, n\}$  için  $M_j = M \cap \mathbf{G}(\{e_1, \dots, e_j\})$  tanımlayalım.

$$M_n = M, M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

ve  $M_j$  lerin  $\mathbb{Z}^n$  nin birer alt grubu olduğuna dikkat edelim. Tümevarım kullanarak  $M_i$  nin bir bazının en fazla  $i$  eleman içerebileceğini gösterelim.

$M_1 = \{0\}$  ise  $M_1$  in bazı boş kümedir.

$M_1 \neq \{0\}$  ise  $H = \{k \in \mathbb{Z} \mid ke_1 \in M_1\}$  kümesini düşünelim.  $H, \mathbb{Z}$  nin alt grubudur ve önerme 2.5 den  $z \in \mathbb{Z} \setminus \{0\}$  için  $H = \mathbf{G}(\{z\})$  dir. Buradan  $M_1 = \mathbf{G}(\{ze_1\})$  olacağı açıktır. Sonuç olarak  $\{ze_1\}, M_1$  için bir baz olur. O halde Önerme  $i = 1$  için doğru olur.

Varsayalım ki  $r \leq k$  olmak üzere  $\{m_1, \dots, m_r\}, M_k$  için bir baz olsun. Eğer  $M_{k+1} = \{0\}$  ise  $M_k = \{0\}$  dır. Dolayısıyla  $r = 0$  ve  $M_{k+1}$  in bazı boş küme olur.



$M_{k+1} \neq \{0\}$  varsayalım ve  $H = \{z \in \mathbb{Z} \mid y + ze_{k+1} \in M_{k+1}, y \in \mathbf{G}(\{e_1, \dots, e_k\})\}$  tanımlayalım. Yine  $H, \mathbb{Z}$  nin alt grubu olur. O zaman bir  $z \in \mathbb{Z}$  için  $H = \mathbf{G}(\{z\})$  olur. Eğer  $z = 0$  ise  $M_{k+1} = M_k$  olur. Böylece  $M_{k+1}, r$  elemanlı bir baza sahiptir ve  $r \leq k < k+1$  dir.

Eğer  $z \neq 0$  ise  $w = y + ze_{k+1} \in M_{k+1}$  olacak şekilde  $y \in \mathbf{G}(\{e_1, \dots, e_k\})$  vardır. Şimdi  $\{m_1, \dots, m_r, w\}$  nun  $M_{k+1}$  için bir baz olduğunu gösterelim.  $m \in M_{k+1}$  alalım.

i)  $m \in \mathbf{G}(\{e_1, \dots, e_{k+1}\})$  olduğundan  $z_1, \dots, z_{k+1} \in \mathbb{Z}$  için  $m = \sum_{i=1}^{k+1} z_i e_i$  dir. O halde  $z_{k+1} \in H$  olur. Dolayısıyla  $z_{k+1} = zt$  olacak şekilde bir  $t \in \mathbb{Z}$  vardır. Buradan

$$m = \sum_{i=1}^k z_i e_i - ty + tw$$

ve sonuç olarak

$$m - tw \in M \cap \mathbf{G}(\{e_1, \dots, e_k\}) = M_k$$

elde edilir.  $\{m_1, \dots, m_r\}, M_k$  nın bir bazı olduğundan dolayı

$$m - tw = \sum_{i=1}^r t_i m_i$$

olacak şekilde  $t_1, \dots, t_r \in \mathbb{Z}$  vardır. O halde  $m = \sum_{i=1}^r t_i m_i + tw$  dir.

ii)  $s_1, \dots, s_{r+1} \in \mathbb{Z}$  olmak üzere  $\sum_{i=1}^r s_i m_i + s_{r+1} w = 0$  olsun.  $\sum_{i=1}^r s_i m_i \in \mathbf{G}(\{e_1, \dots, e_k\})$  ve  $w, (k+1)$ -inci koordinatı sıfırdan farklı olan tek eleman olduğundan  $s_{r+1} = 0$  elde edilir. Dolayısıyla  $\sum_{i=1}^r s_i m_i = 0$  dir ve böylece  $s_1 = \dots = s_r = 0$  elde edilir (çünkü  $\{m_1, \dots, m_r\}, M_k$  nın bazı). Dolayısıyla  $s_1 = \dots = s_r = s_{r+1} = 0$  dir.

$\{m_1, \dots, m_r, w\}$  nun  $M_{k+1}$  için bir baz olduğunu gösterdik ( $r+1 \leq k+1$ ). ■

**Tanım 2.7**  $\mathbb{Q}^n$  nin  $A$  tarafından gerilen alt uzayı

$$\mathbf{L}_{\mathbb{Q}}(A) = \left\{ \sum_{i=1}^n q_i a_i \mid n \in \mathbb{N} \text{ ve her } 1 \leq i \leq n \text{ için } q_i \in \mathbb{Q}, a_i \in A \right\}$$

şeklinde tanımlanır.

**Önerme 2.8**  $M, \mathbb{Z}^n$  nin alt grubu olsun. O zaman  $M$  nin bütün bazlarında aynı sayıda eleman bulunur.

**İspat:**  $B = \{m_i \mid i \in I\}$  ve  $B' = \{n_i \mid i \in I'\}$ ,  $M$  nin iki farklı bazı olsun.  $B$  nin elemanları  $\mathbb{Q}^n$  de lineer bağımsız olduklarından  $|B|$  en fazla  $n$  olabilir. Benzer şey  $|B'|$  içinde geçerlidir.  $B, V = \mathbf{L}_{\mathbb{Q}}(B)$  nin bir bazı ve

$$B' \subset M = \mathbf{G}(\{m_1, \dots, m_r\}) \subset \mathbf{L}_{\mathbb{Q}}(B)$$

$V$  nin lineer bağımsız vektörlerinin kümesi olduğundan  $|B'| \leq |B|$  olmak zorundadır. Tersini de benzer şekilde söyleyebiliriz. ■

**Tanım 2.9**  $\mathbb{Z}^n$  nin bir  $M$  alt grubunun *rankı*,  $M$  nin herhangi bir bazındaki eleman sayısı olarak tanımlanır ve  $\text{rank}(M)$  ile gösterilir.  $\text{rank}(M) \leq n$  olduğuna dikkat edelim.

**Önerme 2.10**  $M, \mathbb{Z}^n$  nin rankı  $k$  olan bir alt grubu ise  $M \simeq \mathbb{Z}^k$  dır.

**İspat:**  $B = \{m_1, \dots, m_k\}$ ,  $M$  nin bir bazı olsun.  $M$  nin her elemanının  $B$  sıralı bazına göre koordinatı tek olduğundan

$$f: \mathbb{Z}^k \rightarrow M$$

$$f(z_1, \dots, z_k) = \sum_{i=1}^k z_i m_i$$

dönüşümü bir izomorfizmdir. ■

**Sonuç 2.11**  $M$  ve  $M', \mathbb{Z}^n$  nin iki alt grubu olsun. O zaman

$$M \simeq M' \iff \text{rank}(M) = \text{rank}(M')$$

dir.

## 2.2 Tamsayı Bileşenli Matrislerin Denkliği ve İnvaryant Faktörleri

Daha önce belirttiğimiz amaçlara ulaşmak için, bileşenleri tamsayı olan matrislerle ilgili bir kaç sonucu tekrar ele almamız gerekiyor. Temel fikir;  $\mathbb{Z}^n$  nin verilen bir alt grubunun bazını, elementer işlemlerle, bu konunun başındaki şekilde olan bir baza dönüştürmektir. Satırları, verilen bir alt grubun bazının elemanları olan matrislerin transformasyonundan bahsedeceğiz. Bu prosese Gauss eliminasyonu diyoruz.

Verilen bir  $n$  tamsayısı için  $1 \leq i, j \leq n$ , ( $i \neq j$ ) olmak üzere şunları tanımlayalım.

1.  $R_{i \leftrightarrow j}, I_n$  nin  $i$ -inci satırı ile  $j$ -inci satırının yer değiştirmesiyle elde edilen matristir.

2.  $R_{i \leftarrow -i}, I_n$  nin  $i$ -inci satırının  $-1$  ile çarpılmasıyla elde edilen matristir.
3.  $R_{j \leftarrow j+zi}, I_n$  nin  $i$ -inci satırının  $z \in \mathbb{Z}$  ile çarpılıp  $j$ -inci satırına eklenmesiyle elde edilen matristir.

$C_{i \leftrightarrow j}, C_{i \leftarrow -i}, C_{j \leftarrow j+zi}$  de yukarıdakine benzer şekilde sadece satır yerine sütun yazmakla tanımlanmış olur.

**Tanım 2.12**  $R_{i \leftrightarrow j}, R_{i \leftarrow -i}, R_{j \leftarrow j+zi}$  matrislerine *elementer satır matrisleri*,  $C_{i \leftrightarrow j}, C_{i \leftarrow -i}, C_{j \leftarrow j+zi}$  matrislerine de *elementer sütun matrisleri* denir.

**Önerme 2.13**  $i, j$  iki pozitif tamsayı,  $z \in \mathbb{Z}$ ,  $A$  bileşenleri tamsayı olan  $n \times n$  tipinde bir matris ve  $\det(B)$  de  $B$  matrisinin determinantını gösterebilirsin. O zaman

1.  $\det(R_{i \leftrightarrow j}) = \det(C_{i \leftrightarrow j}) = -1$ ,
2.  $(R_{i \leftrightarrow j})^{-1} = R_{j \leftrightarrow i}$  ve  $(C_{i \leftrightarrow j})^{-1} = C_{j \leftrightarrow i}$ ,
3.  $\det(R_{i \leftarrow -i}) = \det(C_{i \leftarrow -i}) = -1$ ,
4.  $(R_{i \leftarrow -i})^{-1} = R_{i \leftarrow -i}$  ve  $(C_{i \leftarrow -i})^{-1} = C_{i \leftarrow -i}$ ,
5.  $\det(R_{j \leftarrow j+zi}) = \det(C_{j \leftarrow j+zi}) = 1$ ,
6.  $(R_{j \leftarrow j+zi})^{-1} = R_{j \leftarrow j-zi}$  ve  $(C_{j \leftarrow j+zi})^{-1} = C_{j \leftarrow j-zi}$ ,
7.  $R_{i \leftrightarrow j}A$  matrisi,  $A$  matrisinin  $i$ -inci satırı ile  $j$ -inci satırının yer değiştirilmesi sonucu elde edilen matristir.  $AC_{i \leftrightarrow j}$  matrisi de,  $A$  matrisinin  $i$ -inci sütunu ile  $j$ -inci sütununun yer değiştirilmesi sonucu elde edilen matristir.
8.  $R_{i \leftarrow -i}A$  matrisi,  $A$  matrisinin  $i$ -inci satırının  $-1$  ile çarpılması ile elde edilen matristir.  $AC_{i \leftarrow -i}$  matrisi de,  $A$  matrisinin  $i$ -inci sütununun  $-1$  ile çarpılması ile elde edilen matristir.
9.  $R_{j \leftarrow j+zi}A$  matrisi,  $A$  matrisinin  $i$ -inci satırının  $z$  ile çarpımının  $j$ -inci satırına eklenmesiyle elde edilen matristir.  $AC_{j \leftarrow j+zi}$  matrisi de  $A$  matrisinin  $i$ -inci sütununun  $z$  ile çarpımının  $j$ -inci sütununa eklenmesiyle elde edilen matristir.

**Tanım 2.14** Bileşenleri tamsayı olan  $A$  ve  $B$  gibi iki matris verildiğinde

$$B = P_1 \dots P_r A Q_1 \dots Q_s$$

olacak şekilde  $P_1, \dots, P_r$  elementer satır matrisleri ve  $Q_1, \dots, Q_s$  elementer sütun matrisleri varsa  $A$  ve  $B$  ye *denktirler* denir.

Önerme 2.13 kullanılarak

$$A \sim B \iff A \text{ ve } B \text{ denktirler}$$

bağıntısının bir denklik bağıntısı olduğu kolayca gösterilebilir.

**Not 2.15**  $R_*$  tipindeki matrisler çarpılırken verilen matrisin satırları üzerinde elementer işlemler yapılır.  $C_*$  tipindeki matrisler çarpılırken de verilen matrisin sütunları üzerinde elementer işlemler yapılır.

Tamsayılar ve rasyonel sayılar veya herhangi bir cisim üzerinde çalışırkenki temel fark şudur;  $q$ , cisimin sıfırdan farklı bir elemanı olmak üzere  $R_{i \leftarrow qi}$  ve  $C_{i \leftarrow qi}$  de elementer matrisler olur.

Gauss-Jordan eliminasyon metodunu bileşenleri cisimden gelen matrisler üzerinde şöyle yaparız.

İlk adım olarak matrisin sol üst köşesinin sıfırdan farklı olacak şekilde işlem yaparız. Bunu  $R_{i \leftrightarrow j}$  ve  $C_{i \leftrightarrow j}$  elementer matrislerinin kullanarak yaparız. Yani matrisimizin sol üst köşesi sıfırdan farklı olacak şekilde satır ve sütun değişimleri yaparız. Sonra birinci satırı veya birinci sütunu bu sol üst köşedeki sayıya bölerek sol üst köşeyi 1 yaparız. Bu kez sadece  $R_{j \leftarrow j+z1}$  ve  $C_{j \leftarrow j+z1}$  elementer matrislerini kullanarak orjinal matrisimize denk olan sol üst köşesi hariç birinci satırdaki ve sütundaki diğer bütün bileşenleri sıfır olan bir matris elde ederiz. Birinci satırı ve birinci sütunu kapatıp bu prosedürü yeni matrise de uyguluyoruz. Bu prosese bu şekilde devam ederiz.

Fakat tamsayılarda bu prosedür bu kadar kolay işlemiyor. Çünkü genellikle bir satırı veya sütunu 1 veya  $-1$  den farklı bir tamsayıya bölemiyor ve dolayısıyla denk matrisi elde edemiyoruz.

Bu prosedürün tamsayılardaki halini aşağıdaki şekilde tanımlayabiliriz.

**Önerme 2.16**  $A$ , bileşenleri tamsayı olan  $s \times t$  tipinde bir matris olsun.  $r \leq \min\{s, t\}$ ,  $\{d_1, \dots, d_r\} \subset \mathbb{N} \setminus \{0\}$  ve her  $i \in \{1, \dots, r-1\}$  için  $d_i \mid d_{i+1}$  olmak üzere  $A$  matrisi

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

matrisine denktir.

**İspat:**  $A$  bir sıfır matrisi ise  $r = 0$  olduğuna dikkat edelim.  $(i, j)$ ;  $i$ -inci satır,  $j$ -inci sütunda bulunan elemanı gösterebiliriz.  $A$  matrisine elementer işlemler uygulanması sonucu  $(1, 1)$  deki elemanı mutlak değerce en küçük olacak şekilde ayarlayabiliriz. Elde ettiğimiz  $B$  matrisi  $A$  ya denk bir matristir. Şimdi birinci satırda bu eleman tarafından bölünemeyen bir eleman var mı ona bakalım. Eğer varsa genelliği kaybetmeksizin bu eleman  $(1, 2)$  deki eleman olsun. Euclid algoritmasından dolayı  $\gcd\{b_{11}, b_{12}\} = d$  ( $b_{11}$  ile  $b_{12}$  nin en büyük ortak böleni) bulabiliriz.  $d$  hesaplanırkenki işlemleri elementer operasyonlara çevirebilir ve matrisimizi önce  $C_{1 \leftarrow 1 + z2}$  ve sonra  $C_{1 \leftrightarrow 2}$  ile çarparak yine orjinal matrisimize denk olan bir matris elde ederiz ve elde ettiğimiz bu matriste  $(1, 1)$  deki eleman  $(1, 2)$  deki elemanı böler. Bu prosedürü devam ettirdiğimizde her  $i$  için  $c_{11} \mid c_{1i}$  olacak şekilde  $A$  ya denk bir  $C$  matrisi elde ederiz. Birinci sütunu uygun sayılarla çarpıp diğer sütunlara eklediğimizde  $(1, 1)$  deki bileşen hariç birinci satırdaki tüm bileşenleri sıfırlamış oluruz. Benzer prosedürü birinci sütun için de uygulayabiliriz. Fakat bu sırada birinci satır bozulabilir (sıfırların bir kısmı kaybolabilir). Bu durumda prosedür birinci satır için tekrarlanmalıdır. Benzer şey birinci sütun içinde geçerlidir. Sonlu adım sonunda

$$\begin{pmatrix} f_{11} & 0 & \cdots & 0 \\ 0 & f_{22} & \cdots & f_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & f_{s2} & \cdots & f_{st} \end{pmatrix}$$

matrisini elde ederiz.

$f_{11} \nmid f_{ij}$  olacak şekilde  $i, j$  varsa  $i$ -inci satırı birinci satıra ekleyip biraz önce uyguladığımız prosedürü tekrarlırsak her  $i, j$  için  $f_{11} \mid f_{ij}$  elde ederiz. Sonlu adım sonunda  $(1, 1)$  deki eleman  $A$  nın bütün bileşenlerinin en büyük ortak böleni olur. Şimdi  $d_1 = \gcd\{g_{ij} \mid \forall i, j \text{ için}\}$  olmak üzere orjinal matrisimize denk

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & g_{22} & \cdots & g_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & g_{s2} & \cdots & g_{st} \end{pmatrix}$$

matrisini elde etmiş olduk. Benzer yolla

$$\begin{pmatrix} g_{22} & \cdots & g_{2t} \\ \vdots & \ddots & \vdots \\ g_{s2} & \cdots & g_{st} \end{pmatrix}$$

alt matrisini de bu forma getirebiliriz.

Sonlu adım sonunda istediğimiz sonuca ulaşmış oluruz. ■

**Tanım 2.17**  $d_1, \dots, d_r$  elemanlarına  $A$  nın *invariant faktörleri* denir.

Bunların tek (unique) olduğunu kanıtlayacağız.

**Tanım 2.18** Bir  $A$  matrisinin  $k \times k$  tipindeki bir alt matrisinin determinantına  $A$  nın bir  $k$ -minörü denir.  $A$  nın bütün  $k$ -minörlerinin en büyük ortak bölenini  $D_k(A)$  ile göstereceğiz.

**Önerme 2.19**  $A$  bileşenleri tamsayı olan bir matris olsun. O zaman

1.  $D_k(R_{i \leftrightarrow j}A) = D_k(A) = D_k(AC_{i \leftrightarrow j})$ ,
2.  $D_k(R_{i \leftarrow -i}A) = D_k(A) = D_k(AC_{i \leftarrow -i})$ ,
3.  $D_k(R_{j \leftarrow j+zi}A) = D_k(A) = D_k(AC_{j \leftarrow j+zi})$  dir.

Bunun bir sonucu olarak şunu elde ederiz: “ $A$  ve  $B$  matrisleri denk ise her  $k$  için  $D_k(A) = D_k(B)$  dir.”

**Önerme 2.20**  $A$  ve  $B$  bileşenleri tamsayı olan iki matris olsun. O zaman  $A$  ile  $B$  nin denk olması için gerek ve yeter koşul  $A$  ile  $B$  nin aynı invariant faktörlere sahip olmasıdır.

**İspat:**  $\sim$  bağıntısı bir denklik bağıntısı olduğundan önerme 2.16 kullanılarak

$$\delta_1 = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}, \delta_2 = \begin{pmatrix} d'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d'_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

ve  $\{d_1, \dots, d_r, d'_1, \dots, d'_s\} \subset \mathbb{N} \setminus \{0\}$ , her  $i$  için  $d_i \mid d_{i+1}$ ,  $d'_i \mid d'_{i+1}$  olmak üzere

$$\delta_1 \text{ ve } \delta_2 \text{ denktir} \iff r = s \text{ ve her } i \text{ için } d_i = d'_i$$

olduğunu göstermek yeterlidir.

Eğer  $r = s$  ve her  $i$  için  $d_i = d'_i$  ise  $\delta_1$  ve  $\delta_2$  denktir. Tersine eğer  $\delta_1$  ve  $\delta_2$  denk iseler

$$d_1 \cdots d_r = D_k(\delta_1) = D_k(\delta_2) = d'_1 \cdots d'_s$$

den dolayı sonuç açıktır. ■

Şimdi bütün bu sonuçları  $\mathbb{Z}^n$  nin alt gruplarına uygulayabiliriz.

**Önerme 2.21**  $\{m_1, \dots, m_i, \dots, m_j, \dots, m_r\}$ ,  $\mathbb{Z}^n$  nin bir  $M$  alt grubunun bir bazı olsun. O zaman

1.  $\{m_1, \dots, m_j, \dots, m_i, \dots, m_r\}$  de  $M$  nin bir bazıdır.
2.  $\{m_1, \dots, -m_i, \dots, m_j, \dots, m_r\}$  de  $M$  nin bir bazıdır.
3.  $\{m_1, \dots, m_i, \dots, m_j + zm_i, \dots, m_r\}$  de  $M$  nin bir bazıdır.

Bu işlemler, bazlar için elementer işlemler olarak bilinir.

**Önerme 2.22** Bileşenleri tamsayı olan

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

matrisi verilsin.  $b_i = (b_{i1}, \dots, b_{in}) \in \mathbb{Z}^n$  alalım. O zaman  $\{b_1, \dots, b_n\}$  nin  $\mathbb{Z}^n$  nin bir bazı olması için gerek ve yeter koşul  $\det(B) \in \{-1, 1\}$  olmasıdır.

**İspat:**  $\implies$ : Her  $i \in \{1, \dots, n\}$  için  $\sum_{j=1}^n z_{ij} b_j = e_i$  olacak şekilde  $z_{i1}, \dots, z_{in} \in \mathbb{Z}$  vardır.

$$\begin{pmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & \ddots & \vdots \\ z_{n1} & \cdots & z_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

dir. Böylece  $\det((z_{ij})) \det(B) = 1$ , dolayısıyla  $\det(B) \in \{-1, 1\}$  dir.

$\Leftarrow$ :  $\det(B) \in \{-1, 1\}$  olsun. O halde  $B$  tersinirdir ve buradan

$$(x_1, \dots, x_n)B = z$$

denklem sistemi tek bir çözüme sahiptir ve o da (her  $z \in \mathbb{Z}^n$  için)  $zB^{-1}$  dir. Yani her eleman  $\{b_1, \dots, b_n\}$  sırasında tek bir koordinata sahiptir. Dolayısıyla  $\{b_1, \dots, b_n\}$ ,  $\mathbb{Z}^n$  nin bazıdır. ■

**Teorem 2.23**  $M$ ,  $\text{rank}(M) = r$  olacak şekilde  $\mathbb{Z}^n$  nin bir alt grubu olsun. O zaman her  $i$  için  $d_i \mid d_{i+1}$  ve  $\{d_1 f_1, \dots, d_r f_r\}$ ,  $M$  için bir baz olacak şekilde  $\mathbb{Z}^n$  nin bir  $\{f_1, \dots, f_r, \dots, f_n\}$  bazı ve  $\{d_1, \dots, d_r\} \subset \mathbb{N} \setminus \{0\}$  kümesi vardır.

**İspat:** Her  $i$  için  $m_i = (m_{i1}, \dots, m_{in})$  olmak üzere  $\{m_1, \dots, m_r\}$ ,  $M$  için bir baz olsun. Önerme 2.16 den  $0 \leq s \leq \min\{r, n\}$  ve her  $i$  için  $d_i \mid d_{i+1}$  ve  $\{d_1, \dots, d_r\} \subset \mathbb{N} \setminus \{0\}$  olmak üzere

$$P \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix} Q = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$



olacak şekilde  $P$  ve  $Q$  matrisleri vardır.  $P$  ve  $Q$  tersinir olduklarından

$$\begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix} \text{ ile } \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

nin rankı aynı olur (önerme 2.21 den).

Dolayısıyla  $s = r$  dir. Ek olarak

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rn} \end{pmatrix} = P \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix}$$

alalım ve  $c_i = (c_{i1}, \dots, c_{in})$  koyalım.  $\{c_1, \dots, c_r\}$  kümesi,  $\{m_1, \dots, m_r\}$  bazından sonlu elementer işlemler uygulanarak elde edilmiştir. O halde  $\{c_1, \dots, c_r\}$  de  $M$  için bir bazdır.

Son olarak  $Q^{-1}$  i hesaplar ve

$$Q^{-1} = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}$$

şeklinde gösterirsek  $f_i = (f_{i1}, \dots, f_{in})$  olmak üzere  $\{f_1, \dots, f_n\}$ ,  $\mathbb{Z}^n$  için bir baz olur (önerme 2.22 den), ve

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rn} \end{pmatrix} = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}$$

bulunur. Dolayısıyla her  $i \in \{1, \dots, r\}$  için  $c_i = d_i f_i$  dir. ■

$\{d_1, \dots, d_r\}$  invariant faktörlerin kümesi beklendiği gibi  $M$  nin bir alt grubudur.

$\{f_1, \dots, f_r, \dots, f_n\}$ ,  $\mathbb{Z}^n$  nin bir bazı ve  $\{d_1 f_1, \dots, d_r f_r\}$  de  $M$  nin bir bazı olduğundan  $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$  nin  $M$  nin elemanı olması için gerek ve yeter koşul  $x$  in  $\{f_1, \dots, f_n\}$

sıralı bazına göre koordinatları olan  $(z_1, \dots, z_n)$  nin

$$\begin{aligned} z_1 &\equiv 0 \pmod{d_1} \\ &\vdots \\ z_r &\equiv 0 \pmod{d_r} \\ z_{r+1} &= 0 \\ &\vdots \\ z_n &= 0 \end{aligned}$$

denklemlerini sağlamasıdır.

Teorem 2.23 nin ispatında olduğu gibi her  $i$  için  $f_i = (f_{i1}, \dots, f_{in})$  alalım.  $(z_1, \dots, z_n)$ ,  $x$  in  $\{f_1, \dots, f_n\}$  sıralı bazına göre koordinatları olduğundan

$$x = (x_1, \dots, x_n) = \sum_{i=1}^n z_i f_i$$

ve buradan

$$(x_1, \dots, x_n) = (z_1, \dots, z_n) \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}$$

yazabiliriz. Dolayısıyla

$$(z_1, \dots, z_n) = (x_1, \dots, x_n) \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

dir (buradaki  $(b_{ij})$  matrisi Teorem 2.23 nin ispatındaki  $(f_{ij})$  matrisinin tersi olan matris yani  $Q$  matrisidir).

Buradan,

$$\begin{aligned} x = (x_1, \dots, x_n) \in \mathbb{Z}^n, M \text{ dedir} &\iff \begin{aligned} b_{11}x_1 + \cdots + b_{n1}x_n &\equiv 0 \pmod{d_1} \\ &\vdots \\ b_{1r}x_1 + \cdots + b_{nr}x_n &\equiv 0 \pmod{d_r} \\ b_{1(r+1)}x_1 + \cdots + b_{n(r+1)}x_n &= 0 \\ &\vdots \\ b_{1n}x_1 + \cdots + b_{nn}x_n &= 0 \end{aligned} \end{aligned}$$

elde edilir. Bu denklemler genellikle  $\{e_1, \dots, e_n\}$  sıralı bazına göre  $M$  nin denklemleri yada daha basitçe  $M$  nin denklemleri olarak bilinir.

Eğer  $d_i = 1$  ise bu  $d_i$  nin geçtiği denklem elimine edilebilir (çünkü her tamsayının 1 ile bölümünden kalan 0 dır).

$M$  nin tüm invaryant faktörleri 1 ise  $M$  ye *homojendir* denir.

**Örnek 2.24**  $M = \mathbf{G}(\{(2, -1, 1), (3, 2, -1)\}) \subseteq \mathbb{Z}^3$  alalım. Sütunlarında yaptığımız elementer işlemleri sağdaki matrise, satırlarında yaptığımız elementer işlemleri soldaki matrise uyguluyoruz.

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

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

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

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \rightarrow$$

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

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -5 \\ 1 & 1 & -7 \end{pmatrix}$$

elde edilir. Buradan

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & 1 \\ 3 & 2 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -5 \\ 1 & 1 & -7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

elde edilir. Bu nedenle  $M$  nin denklemleri

$$x_3 \equiv 0 \pmod{1}$$

$$x_2 + x_3 \equiv 0 \pmod{1}$$

$$x_1 - 5x_2 - 7x_3 = 0$$

dir. İlk iki denklemi elimine edebileceğimizden

$$(x_1, x_2, x_3) \in M \iff x_1 - 5x_2 - 7x_3 = 0$$

elde ederiz. ◇

Aşağıdaki teorem, sonlu doğuraylı değişmeli grupların temel teoremini göstermek için gerekli son kısmı verir.

**Teorem 2.25**  $M, \mathbb{Z}^n$  nin invaryant faktörleri  $d_1, \dots, d_r$  olan bir alt grubu ise

$$\mathbb{Z}^n / M \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

dir.

**İspat:** Teorem 2.23 den,  $\{f_1, \dots, f_r, \dots, f_n\}$ ,  $\mathbb{Z}^n$  nin bazı olacak şekilde,  $M$  nin  $\{d_1 f_1, \dots, d_r f_r\}$  formunda bir bazı olduğunu biliyoruz. Notasyonu basitleştirmek için  $\mathbb{Z}_{d_i} = \mathbb{Z} / \mathbf{G}(\{d_i\})$  deki  $[z_i]_{\equiv_{\mathbf{G}(\{d_i\})}}$  elemanını  $[z_i]_{d_i}$  ile gösterip

$$\begin{aligned} \varphi : \mathbb{Z}^n / M &\rightarrow \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r} \\ \varphi \left( \left[ \sum_{i=1}^n z_i f_i \right]_{\equiv M} \right) &= ([z_1]_{d_1}, \dots, [z_r]_{d_r}, z_{r+1}, \dots, z_n) \end{aligned}$$

dönüşümünü tanımlayalım.

$\varphi$  iyi tanımlıdır ve  $\varphi$  bir izomorfizmdir. ■

### 2.3 Bazların Hesaplanması İle İlgili Bazı Kullanışlı Sonuçlar

#### 2.3.1 $\mathbb{Z}^n$ nin Bir Alt Grubunun Bir Doğuray Kümesinden Bir Bazının Hesaplanması

Eğer  $Q$ , bileşenleri tamsayı ve determinantı sıfırdan farklı olan bir matris ve  $f$

$$f : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$$

$$f(x_1, \dots, x_n) = (x_1, \dots, x_n)Q$$

şeklinde tanımlanan bir fonksiyon ise  $m_1, \dots, m_r$  nin lineer bağımsız olması için gerek ve yeter koşul  $f(m_1), \dots, f(m_r)$  nin lineer bağımsız olmasıdır.

$$g : \mathbb{Q}^n \rightarrow \mathbb{Q}^n$$

$$g(x) = xQ$$

dönüşümü bir izomorfizmdir. Dolayısıyla  $g$ , lineer bağımsızlığı korur.

Her  $i \in \{1, \dots, s\}$  için  $m_i = (m_{i1}, \dots, m_{in})$  olmak üzere  $\mathbb{Z}^n$  nin  $\{m_1, \dots, m_s\}$  tarafından doğurulan  $M$  alt grubunu alalım.  $A$ , satırları  $m_1, \dots, m_s$  olan bir matris olsun.  $d_1, \dots, d_r \in \mathbb{N} \setminus \{0\}$  olmak üzere  $A$  matrisinin

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

diagonal matrisine denk olduğunu biliyoruz. Dolayısıyla  $PAQ = D$  olacak şekilde  $P$  ve  $Q$  matrisleri vardır. Üstelik  $P$  nin satır elementer matrislerin bir çarpımı ve  $Q$  nun da sütun elementer matrislerin bir çarpımı olduğunu biliyoruz. Böylece  $PA = DQ^{-1}$  olduğuna ve buradan aşağıdakilerin sağlandığına dikkat edelim.

1.  $Q$  sadece  $D$  nin sütunları üzerinde elementer işlemler yaptığından ve  $PA = DQ^{-1}$  olduğundan ve de  $D$  nin son  $s - r$  satırındaki bütün bileşenler sıfır olduğundan  $PA$  nın son  $s - r$  satırındaki bütün bileşenler sıfırdır.

2.  $P$  matrisi sadece  $A$  nın satırları üzerinde elementer işlemler yaptığından  $PA$  nın satırları  $M$  nin bir doğuray kümesi olur. Buradan  $PA$  nın ilk  $r$  satırının  $M$  nin bir doğuray kümesi olduğunu söylemiş oluruz.
3.  $D$  nin ilk  $r$  satırı lineer bağımsız ve  $\det(Q) \neq 0$  olduğundan  $PA$  nın ilk  $r$  satırı lineer bağımsız olur.

Buradan,  $PA$  yı hesaplayıp onun ilk  $r$  satırını alarak,  $M$  nin bir bazını elde etmiş oluruz.

### 2.3.2 $\mathbb{Z}^n$ nin Bir Alt Grubunun Denklemlerinden Bir Bazının Hesaplanması

Önce homojen olma durumunu (yani bütün invaryant faktörlerin 1 olduğu durumu) inceleyeceğiz. Sonra genel duruma bakacağız (aslında genel durumun homojen olma durumuna indirgenebileceğini göreceğiz).

$M, \mathbb{Z}^n$  nin homojen bir alt grubu ve  $A$ , bileşenleri tamsayı olan bir matris olsun. Varsayalımki

$$x \in M \iff Ax = 0$$

olsun.  $P, Q$  sırasıyla elementer satır matrislerinin ve elementer sütun matrislerinin çarpımları olmak üzere  $PAQ = D$  olacak şekilde  $P$  ve  $Q$  matrislerini bulabiliriz ( $D$  bir önceki sayfada verilen diagonal  $D$  matrisidir). Dolayısıyla  $AQ = P^{-1}D$  dir ve böylece  $AQ$  matrisinin son  $n - r$  sütunundaki tüm bileşenler sıfırdır. O halde  $Q$  nun son  $n - r$  sütunu  $Ax = 0$  denklemini sağlar. Böylece bu son  $n - r$  sütun  $M$  nin elemanıdır. Bu elemanlar determinantı sıfır olmayan bir matrisin bir parçası olduklarından lineer bağımsızdır. O halde,  $Q$  nun son  $n - r$  sütunu  $M$  nin lineer bağımsız elemanlarıdır demiş olduk. Şimdi bunların  $M$  yi doğurduğunu gösterelim.  $x \in M$  alalım. O zaman  $Ax = 0$  dir. Dolayısıyla  $P^{-1}DQ^{-1}x = 0$  dir.  $\det(P) \neq 0$  olduğundan  $D(Q^{-1}x) = 0$  dir. Böylece  $Q^{-1}x$  in ilk  $r$  koordinatı sıfırdır. O halde  $Q^{-1}x$

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_{r+1} \\ \vdots \\ y_n \end{pmatrix}$$

formundadır ve buradan

$$x = Q \begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_{r+1} \\ \vdots \\ y_n \end{pmatrix}$$

olur. Dolayısıyla  $x$ ,  $Q$  nun son  $n - r$  sütununun bir lineer kombinasyonu şeklinde yazılabilir.

Özetle,  $Q$  nun son  $n - r$  sütununun  $M$  için bir baz olduğunu göstermiş olduk.

Şimdi genel duruma bakalım.  $M$  kümesi,  $\mathbb{Z}^n$  nin

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &\equiv 0 \pmod{b_1} \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &\equiv 0 \pmod{b_k} \\ a_{(k+1)1}x_1 + \cdots + a_{(k+1)n}x_n &= 0 \\ &\vdots \\ a_{s1}x_1 + \cdots + a_{sn}x_n &= 0 \end{aligned}$$

denklemlerini sağlayacak şekildeki elemanlarının kümesi olsun.

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n - b_1x_{n+1} &= 0 \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n - b_kx_{n+k} &= 0 \\ a_{(k+1)1}x_1 + \cdots + a_{(k+1)n}x_n &= 0 \\ &\vdots \\ a_{s1}x_1 + \cdots + a_{sn}x_n &= 0 \end{aligned}$$

denklemlerini sağlayacak şekildeki  $(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+k}) \in \mathbb{Z}^{n+k}$  elemanlarının oluşturduğu kümeye  $M'$  diyelim.  $M'$  homojen olduğu için  $B' = \{m'_1, \dots, m'_r\}$  gibi bir bazını bulabiliriz.  $m'_i = (m_{i1}, \dots, m_{i(n+k)})$  olarak varsayalım ve  $m_i = (m_{i1}, \dots, m_{in})$  alalım. Şimdi  $B = \{m_1, \dots, m_r\}$  nin  $M$  için bir baz olduğunu gösterelim.

- $x = (x_1, \dots, x_n) \in M$  alalım. Her  $i \in \{1, \dots, k\}$  için

$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv 0 \pmod{b_i}$$

olduğunu biliyoruz. Bu nedenle

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_ix_{n+i}$$

olacak şekilde  $x_{n+i} \in \mathbb{Z}$  vardır. Dolayısıyla  $x' = (x_1, \dots, x_n, x_{n+1}, \dots, x_{n+k}) \in M'$  dir ve böylece  $a_1, \dots, a_r \in \mathbb{Z}$  için  $x' = \sum_{i=1}^r a_i m'_i$  dir. Buradan  $x = \sum_{i=1}^r a_i m_i$  olacağı açıktır. O halde  $B, M$  için bir doğuray kümesidir.

- $a_1, \dots, a_r \in \mathbb{Z}$  nin  $\sum_{i=1}^r a_i m_i = 0$  denklemini sağladığını varsayalım.

$$a_1 = \cdots = a_r = 0$$

olduğunu göstermek için,  $B'$  baz olduğundan,  $\sum_{i=1}^r a_i m'_i = 0$  olduğunu göstermek yeterlidir.  $\sum_{i=1}^r a_i m_i = 0$  olduğundan sadece, her  $j \in \{1, \dots, k\}$  için  $\sum_{i=1}^r a_i m_{i(n+j)} = 0$  olduğunu göstermeliyiz.  $m'_1, \dots, m'_r \in M'$  olduğundan bunlar  $M'$  nin denklemlerini sağlar.

Dolayısıyla

$$b_j m_{i(n+j)} = a_{j1} m_{i1} + \cdots + a_{jn} m_{in}$$

dir. O halde

$$m_{i(n+j)} = \frac{(a_{j1} m_{i1} + \cdots + a_{jn} m_{in})}{b_j}$$

dir. Böylece

$$\begin{aligned} \sum_{i=1}^r a_i m_{i(n+j)} &= \sum_{i=1}^r a_i \left( \sum_{l=1}^n a_{jl} m_{il} \right) / b_j \\ &= \left( \sum_{l=1}^n a_{jl} \left( \sum_{i=1}^r a_i m_{il} \right) \right) / b_j \\ &= \left( \sum_{l=1}^n a_{jl} 0 \right) / b_j \\ &= 0 \end{aligned}$$

dır. Dolayısıyla  $B$  deki vektörler lineer bağımsızdır.



### 3. SONLU DOĞURAYLI SADELEŞMELİ MONOİDLER

Birinci bölümde, sonlu doğuraylı sadeleşmeli bir monoidin, sonlu doğuraylı bir grubun bir alt monoidine izomorfik olduğunu gösterdik. İkinci bölümde de sonlu doğuraylı değişmeli gruplar için temel teoremi ispatladık. Bunları kullanarak  $d_1, \dots, d_r, k \in \mathbb{N} \setminus \{0\}$  olmak üzere her sonlu doğuraylı sadeleşmeli monoidin  $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$  nin bir alt monoidi olduğunu söyleyebiliriz.

Sonlu doğuraylı sadeleşmeli monoidleri burulmasız olanlar, indirgenmiş olanlar ve sonlu olanlar olmak üzere kendi içinde üç sınıfa ayıracağız. Bu bölümde aşağıdaki üç temel sonucu ispatlayacağız.

1. Her sonlu doğuraylı sadeleşmeli burulmasız monoid,  $n$  bir pozitif tamsayı olmak üzere,  $\mathbb{Z}^n$  nin bir alt monoidine izomorfiktir.
2. Her sonlu doğuraylı sadeleşmeli burulmasız indirgenmiş monoid,  $n$  bir pozitif tamsayı olmak üzere,  $\mathbb{N}^n$  nin bir alt monoidine izomorfiktir.
3. Her sonlu sadeleşmeli monoid bir gruptur.

Teorem 1.17 ve önerme 1.21 den,  $M, \mathbb{Z}^n$  nin bir alt grubu olmak üzere her sonlu doğuraylı sadeleşmeli monoid  $\mathbb{N}^n / \sim_M$  ye izomorfiktir. Sonraki sonuç ise  $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$  nin  $S$  ye izomorfik bir alt monoidinin  $M$  nin denklemlerinin “sütunları” tarafından doğurulmuş olduğunu söyler.

**Önerme 3.1**  $\mathbb{Z}^n$  nin

$$\begin{aligned}
 (x_1, \dots, x_n) \in M &\iff \begin{aligned}
 &a_{11}x_1 + \dots + a_{1n}x_n \equiv 0 \pmod{d_1} \\
 &\vdots \\
 &a_{r1}x_1 + \dots + a_{rn}x_n \equiv 0 \pmod{d_r} \\
 &a_{(r+1)1}x_1 + \dots + a_{(r+1)n}x_n = 0 \\
 &\vdots \\
 &a_{(r+k)1}x_1 + \dots + a_{(r+k)n}x_n = 0
 \end{aligned}
 \end{aligned}$$

olacak şekilde bir  $M$  alt grubu verilsin. O zaman;  $[a]_d$ ,  $a$  nın  $\mathbb{Z}_d$  deki denklik sınıfını göstermek üzere  $\mathbb{N}^n / \sim_M, \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$  nin

$$S = \langle \{ ([a_{11}]_{d_1}, \dots, [a_{r1}]_{d_r}, a_{(r+1)1}, \dots, a_{(r+k)1}), \dots, ([a_{1n}]_{d_1}, \dots, [a_{rn}]_{d_r}, a_{(r+1)n}, \dots, a_{(r+k)n}) \} \rangle$$

olacak şekilde alt monoidine izomorfiktir.

**İspat:**

$$\begin{aligned} \varphi &: \mathbb{N}^n / \sim_M \rightarrow \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k \\ \varphi([(a_1, \dots, a_n)]_{\sim_M}) &= \left( \left[ \sum_{i=1}^n a_i a_{1i} \right]_{d_1}, \dots, \left[ \sum_{i=1}^n a_i a_{ri} \right]_{d_r}, \sum_{i=1}^n a_i a_{(r+1)i}, \dots, \sum_{i=1}^n a_i a_{(r+k)i} \right) \end{aligned}$$

fonksiyonunu tanımlayalım. Bu fonksiyon iyi tanımlı bir monomorfizmdir. O halde  $S = \text{Im}(\varphi)$  alınırsa  $\mathbb{N}^n / \sim_M \simeq S$  dir. ■

**Örnek 3.2**  $M = \mathbf{G}(\{(2, 0, 0), (0, 1, -1)\}) \subseteq \mathbb{Z}^3$  verilsin.  $M$  nin invaryant faktörlerini bulalım.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

olur. Dolayısıyla

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

dir. O halde  $M$  nin denklemleri

$$\begin{aligned} y &\equiv 0 \pmod{1} \\ x &\equiv 0 \pmod{2} \\ y+z &= 0 \end{aligned}$$

olur. Böylece

$$(x, y, z) \in M \iff \begin{aligned} x &\equiv 0 \pmod{2} \\ y+z &= 0 \end{aligned}$$

elde edilir. O halde  $\mathbb{N}^3 / \sim_M, \mathbb{Z}_2 \times \mathbb{Z}$  nin

$$\{([1]_2, 0), ([0]_2, 1), ([0]_2, 1)\} = \{([1]_2, 0), ([0]_2, 1)\}$$

tarafından doğurulan alt monoidine izomorftir.  $\diamond$

### 3.1 Sonlu Doğuraylı Sadeleşmeli Burulmasız Monoidler

**Tanım 3.3** Her  $a, b \in S$  ve  $k \in \mathbb{N} \setminus \{0\}$  için  $ka = kb$  iken  $a = b$  oluyorsa  $S$  monoidine *burulmasız* denir.

Burulmasız olmanın izomorfizmalar altında korunduğunu ve bir burulmasız monoidin alt monoidinin de yine burulmasız olduğu kolayca gösterilebilir. O halde özel olarak  $\mathbb{Z}^n$  nin her alt monoidi burulmasızdır. İzomorfizmalar altında, mümkün olan bütün sonlu doğuraylı sadeleşmeli ve burulmasız monoidlerin bunlardan ibaret olduğunu göstereceğiz. Bunu yapmak için önce,  $\mathbb{N}^n / \sim_M$  formundaki bir monoid burulmasız ise  $M$  nin homojen olmak zorunda kaldığını gösterelim.

**Önerme 3.4**  $M, \mathbb{Z}^n$  nin bir alt grubu olsun. O halde aşağıdakiler birbirine denktir.

1.  $M$  homojendir.
2.  $\mathbb{N}^n / \sim_M$ ,  $k$  pozitif bir tamsayı olmak üzere,  $\mathbb{Z}^k$  nin bir alt monoidine izomorftir.
3.  $\mathbb{N}^n / \sim_M$  burulmasızdır.

**İspat:**  $1 \implies 2$ : Tanımdan dolayı  $M$  nin denklemleri

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

şeklindedir ve önerme 3.1 den,  $\mathbb{N}^n / \sim_M, \langle (a_{11}, \dots, a_{m1}), \dots, (a_{1n}, \dots, a_{mn}) \rangle \subseteq \mathbb{Z}^m$  ye izomorfiktir.

$2 \implies 3$ :  $\mathbb{Z}^n$  nin her alt monoidi burulmasız olduğundan ve burulmasız olma özelliği izomorfizmalar altında korunduğundan  $\mathbb{N}^n / \sim_M$  de burulmasız olur.

$3 \implies 1$ :  $M$  nin homojen olduğunu yani  $M$  nin bütün invaryant faktörlerinin 1 olduğunu gösterelim.  $d_1, \dots, d_r$ ,  $M$  nin invaryant faktörleri olsun. Teorem 2.23 den  $\{d_1 f_1, \dots, d_r f_r\}$ ,  $M$  nin bazı olacak şekilde  $\mathbb{Z}^n$  nin bir  $\{f_1, \dots, f_r, \dots, f_n\}$  bazı vardır.  $d_i > 1$  olacak şekilde  $i \in \{1, \dots, r\}$  olduğunu varsayalım ve  $f_i = (f_{i1}, \dots, f_{in})$  koyalım.

$$\begin{aligned} f_i^+ &= (\max\{f_{i1}, 0\}, \dots, \max\{f_{in}, 0\}) \\ f_i^- &= (\max\{-f_{i1}, 0\}, \dots, \max\{-f_{in}, 0\}) \end{aligned}$$

alalım.  $f_i = f_i^+ - f_i^-$  ve  $f_i^+, f_i^- \in \mathbb{N}^n$  olduğuna dikkat edelim.  $d_i > 1$  olduğundan  $f_i^+ - f_i^- = f_i \notin M$  ve buradan  $[f_i^+]_{\sim_M} \neq [f_i^-]_{\sim_M}$  elde edilir. Bununla birlikte  $d_i f_i = d_i f_i^+ - d_i f_i^- \in M$  ve buradan  $d_i [f_i^+] = d_i [f_i^-]$  elde edilir. Bu ise  $\mathbb{N}^n / \sim_M$  nin burulmasız olması ile çelişir. O halde her  $i$  için  $d_i = 1$  dir. Dolayısıyla  $M$  homojendir. ■

**Sonuç 3.5**  $S$  sonlu doğuraylı bir monoid olsun. O zaman  $S$  nin sadeleşmeli ve burulmasız olması için gerek ve yeter koşul  $k$  bir pozitif tamsayı olmak üzere  $S$  nin  $\mathbb{Z}^k$  nin bir alt monoidine izomorfik olmasıdır.

**İspat:**  $\implies$ :  $S$  sonlu doğuraylı olduğundan  $n \in \mathbb{Z}^+$  ve  $\sigma, \mathbb{N}^n$  üzerinde bir kongruans olmak üzere,  $S \simeq \mathbb{N}^n / \sigma$  dir (teorem 1.17 den).  $S$  sadeleşmeli olduğundan, önerme 1.21 den dolayı  $\sigma \sim_{M_\sigma}$  dir.  $S$  burulmasız olduğundan önerme 3.4 den dolayı pozitif bir  $k$  tamsayısı için  $\mathbb{N}^n / \sim_{M_\sigma}$  dolayısıyla  $S, \mathbb{Z}^k$  nin bir alt monoidine izomorfiktir.

$\Leftarrow$ : Aşıkardır. ■

**Örnek 3.6**  $M = \mathbf{G}(\{(4, 1, -3), (1, -2, 1)\}) \subseteq \mathbb{Z}^3$  verilsin.  $M$  nin invaryant faktörlerini hesaplırsak

$$\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 4 & 1 & -3 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 \\ 0 & -3 & 7 \\ 0 & -4 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

olduğunu görürüz.  $M$  nin denklemleri sadece  $5x + 7y + 9z = 0$  dir. Dolayısıyla  $\mathbb{N}^3 / \sim_M, \mathbb{Z}$  nin  $\{5, 7, 9\}$  tarafından doğurulan alt monoidine izomorfiktir. ◇

### 3.2 Sonlu Doğuraylı Sadeleşmeli İndirgenmiş Monoidler

**Tanım 3.7**  $S$  bir monoid olsun.  $a \in S$  için  $a + b = 0$  olacak şekilde  $b \in S$  varsa  $a$  ya bir *birim* denir.  $S$  nin birimlerinin kümesini  $U(S)$  ile göstereceğiz.

$U(S)$  nin,  $S$  nin bir alt monoidi; dahası bir grup olduğuna dikkat edelim.

**Tanım 3.8** Eğer  $U(S) = 0$  ise  $S$  ye *indirgenmiş* denir.

İndirgenmiş olmak izomorfizmalar altında korunan bir özelliktir. Bir indirgenmiş monoidin her alt monoidinin de indirgenmiş olduğu kolayca gösterilebilir. Özel olarak  $n$  bir pozitif tamsayı olmak üzere  $\mathbb{N}^n$  nin tüm alt monoidleri indirgenmiştir. Bu bölümdeki amaç; her sonlu doğuraylı sadeleşmeli burulmasız indirgenmiş monoidin,  $n$  bir pozitif tamsayı olmak üzere  $\mathbb{N}^n$  nin sonlu doğuraylı bir alt monoidine izomorfik olduğunu göstermektir.

**Önerme 3.9**  $M, \mathbb{Z}^n$  nin  $M \cap \{e_1, \dots, e_n\} = \emptyset$  olacak şekildeki bir alt grubu olsun. O zaman  $\mathbb{N}^n / \sim_M$  nin indirgenmiş olması için gerek ve yeter koşul  $M \cap \mathbb{N}^n = \{0\}$  olmasıdır.

**İspat:**  $\implies$ :  $(a_1, \dots, a_n) \in M \cap \mathbb{N}^n$  alalım. Bir  $i \in \{1, \dots, n\}$  için  $a_i > 0$  varsayalım.  $(a_1, \dots, a_n) \in M$  olduğundan

$$[(a_1, \dots, a_n)] = [0] = [e_i] + [(a_1, \dots, a_i - 1, \dots, a_n)]$$

olur.  $e_i \notin M$  olduğundan  $[e_i] \neq [0]$  olur ki bu da  $\mathbb{N}^n / \sim_M$  nin indirgenmiş olması ile çelişir. O halde  $M \cap \mathbb{N}^n = \{0\}$  dir.

$\impliedby$ :  $\mathbb{N}^n / \sim_M$  nin indirgenmiş olmadığını varsayalım. O zaman

$$[a + b] = [a] + [b] = [0]$$

olacak şekilde  $[a], [b] \in \mathbb{N}^n / \sim_M \setminus \{[0]\}$  vardır.  $a, b \in \mathbb{N}^n \setminus \{0\}$  olduğundan  $0 \neq a + b \in M$  olur ki bu  $M \cap \mathbb{N}^n = \{0\}$  olmasından dolayı imkansızdır. O halde  $\mathbb{N}^n / \sim_M$  indirgenmiştir. ■

O halde  $S$  sonlu doğuraylı ve sadeleşmeli ise  $\mathbb{N}^n / \sim_M$  formundadır. Eğer  $S$  nin indirgenmiş olup olmadığını bilmek istiyorsak  $M \cap \{e_1, \dots, e_n\} = \emptyset$  koşulu altında  $M \cap \mathbb{N}^n = \{0\}$  olup olmadığını kontrol etmek zorundayız. Bir sonraki bölümde bunun kontrolü için bir prosedür vereceğiz. Her ne kadar  $M \cap \{e_1, \dots, e_n\} = \emptyset$  koşulu garip gibi görünse de, bu koşulun  $S$  nin doğurayları cinsinden bir anlamı vardır. Eğer bir  $i$  için  $e_i \in M$  ise  $\mathbb{N}^n / \sim_M = \langle [e_1], \dots, [e_n] \rangle$  nin  $[e_i]$  doğurayı sıfıra eşittir. O halde bunu dikkate almayabiliriz. Bu fikri aşağıdaki sonuçta açıklayacağız.

**Önerme 3.10**  $M, \mathbb{Z}^n$  nin  $M \cap \{e_1, \dots, e_n\} = \{e_{r+1}, \dots, e_n\}$  olacak şekildeki bir alt grubu olsun.

$$M' = \{(x_1, \dots, x_r) \in \mathbb{Z}^r \mid (x_1, \dots, x_r, x_{r+1}, \dots, x_n) \in M\}$$

alalım. O zaman

1.  $M', \mathbb{Z}^r$  nin alt grubudur.

2.  $\mathbb{N}^n / \sim_M \simeq \mathbb{N}^r / \sim_{M'}$  dir.

3. Eğer

$$M = \mathbf{G}(\{(m_{11}, \dots, m_{1n}), \dots, (m_{k1}, \dots, m_{kn})\})$$

ise

$$M' = \mathbf{G}(\{(m_{11}, \dots, m_{1r}), \dots, (m_{k1}, \dots, m_{kr})\})$$

dir.

**İspat:**

$$\varphi : \mathbb{N}^n / \sim_M \rightarrow \mathbb{N}^r / \sim_{M'}$$

$$\varphi([(a_1, \dots, a_n)]_{\sim_M}) = [(a_1, \dots, a_r)]_{\sim_{M'}}$$

dönüşümünün bir izomorfizm olduğunu söylemek ispat için yeterlidir. ■

**Örnek 3.11**  $M = \mathbf{G}(\{(1, -1, 1, 1), (0, 1, -1, -1), (-1, 1, 0, -1)\}) \subseteq \mathbb{Z}^4$  verilsin.  $M$  nin invariant faktörlerini hesaplırsak hepsinin 1 olduğunu ve  $M$  nin sadece  $x_2 + x_4 = 0$  denkleminin sahip olduğunu görebiliriz. Bu denklemden  $M \cap \{e_1, e_2, e_3, e_4\} = \{e_1, e_3\}$  olduğu sonucuna varırız. Dolayısıyla  $M', \mathbb{Z}^2$  nin  $\{(-1, 1), (1, -1), (1, -1)\}$  tarafından doğurulan alt grubudur.  $(-1, 1) = -(1, -1)$  olduğundan  $M' = \mathbf{G}(\{(1, -1)\})$  dir. O halde  $M'$  nin denklemleri olarak  $x_1 + x_2 = 0$  elde edilir. Önerme 3.1 den  $\mathbb{N}^2 / \sim_{M'}, \mathbb{Z}$  nin  $\{1, 1\} = \{1\}$  tarafından doğurulan alt monoidine izomorfiktir ( $M$  nin denklemlerinin kolonlarındaki katsayılar 1 olduğu için). Dolayısıyla  $\mathbb{N}^2 / \sim_{M'}$ ,  $\mathbb{N}$  ye izomorfiktir. O halde  $\mathbb{N}^4 / \sim_M \simeq \mathbb{N}$  dir. ◇

Şimdi,  $\mathbb{N}^n / \sim_M$  indirgenmiş olduğunda  $M$  nin denklemlerinin formuna bakalım. Bu durumda bütün katsayıları sıfırdan büyük bir denklem elde edebileceğimizi göreceğiz. Bu sayede  $k$  pozitif bir tamsayı olmak üzere her sonlu doğuraylı sadeleşmeli burulmasız indirgenmiş monoidin  $\mathbb{N}^k$  nın bir sonlu doğuraylı alt monoidine izomorfik olduğunu göstereceğiz.

**Tanım 3.12**  $\mathbb{Q}^n$  nin bir  $V$  alt uzayının *ortogonal uzayı*

$$V^\perp = \left\{ (x_1, \dots, x_n) \in \mathbb{Q}^n \mid \text{Her } (y_1, \dots, y_n) \in V \text{ için } \sum_{i=1}^n x_i y_i = 0 \right\}$$

dır.

$\mathbb{Q}^n$  nin negatif olmayan elemanı bütün koordinatları 0 yada 0 dan büyük olan elemandır.

$\mathbb{Q}^n$  nin kuvvetli pozitif elemanı bütün koordinatları 0 dan büyük olan elemandır.

**Lemma 3.13**  $V, \mathbb{Q}^n$  nin bir alt uzayı olsun. O zaman  $V^\perp$  in bir kuvvetli pozitif elemanı olması için gerek ve yeter koşul  $V$  nin negatif olmayan elemanının sadece 0 olmasıdır.

**İspat:**  $\implies$ : Her  $i$  için  $a_i > 0$  olmak üzere  $(a_1, \dots, a_n) \in V^\perp$  alalım. Her  $i$  için  $b_i \geq 0$  olacak şekilde  $(b_1, \dots, b_n) \in V$  olduğunu varsayalım.  $\sum_{i=1}^n a_i b_i = 0$  ve her  $i$  için  $a_i b_i \geq 0$  olduğundan her  $i$  için  $a_i b_i = 0$  elde edilir. Dolayısıyla her  $i \in \{1, \dots, n\}$  için  $b_i = 0$  dır.

$\impliedby$ : Bir sonraki bölümde Minkowski-Farkas lemmanın bir sonucu olarak teorem 4.2 de verilecektir. ■

**Önerme 3.14**  $M \cap \mathbb{N}^n = \{0\}$  olacak şekilde  $\mathbb{Z}^n$  nin bir  $M$  alt grubu verilsin. O zaman her  $(x_1, \dots, x_n) \in M$  için  $a_1 x_1 + \dots + a_n x_n = 0$  olacak şekilde bir  $(a_1, \dots, a_n) \in \mathbb{N}^n$  kuvvetli pozitif elemanı vardır.

**İspat:**  $V, \mathbb{Q}^n$  nin  $M$  tarafından gerilen alt uzayı olsun.  $M \cap \mathbb{N}^n = \{0\}$  olduğundan  $V$  nin tek negatif olmayan elemanı 0 dır. Lemma 3.13 ü kullanarak  $V^\perp$  de (paydaları elimine ederek  $\mathbb{N}^n$  üzerinde varsayabiliriz) bir  $(a_1, \dots, a_n)$  kuvvetli pozitif elemanı vardır. O halde her  $(x_1, \dots, x_n) \in M \subset V$  için  $a_1 x_1 + \dots + a_n x_n = 0$  elde etmiş olduk. ■

**Teorem 3.15 (Grillet)**  $S$  sonlu doğuraylı bir monoid olsun.  $S$  nin sadeleşmeli burulmasız ve indirgenmiş olması için gerek ve yeter koşul pozitif bir  $k$  tamsayısı için  $S$  nin  $\mathbb{N}^k$  nin bir alt monoidine izomorfik olmasıdır.

**İspat:**  $\implies$ :  $S$  sadeleşmeli olduğundan,  $\mathbb{Z}^n$  nin bir  $M$  alt grubu için,  $S, \mathbb{N}^n / \sim_M$  formundadır. Önerme 3.4 den dolayı  $M$  homojendir. Önerme 3.1 i kullanarak,  $M$  nin denklemleri

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + \dots + a_{kn}x_n &= 0 \end{aligned}$$

olmak üzere  $S$  nin,  $\mathbb{Z}^k$  nin  $\{(a_{11}, \dots, a_{k1}), \dots, (a_{1n}, \dots, a_{kn})\}$  tarafından doğurulan alt mono-  
idine izomorfik olduğunu söyleriz. Dahası  $S$  indirgenmiş olduğundan dolayı önerme 3.9  
ve önerme 3.14 den eğer  $(x_1, \dots, x_n) \in M$  ise  $a_1x_1 + \dots + a_nx_n = 0$  olacak şekilde  
 $a_1, \dots, a_n \in \mathbb{N} \setminus \{0\}$  vardır. O zaman

$$(x_1, \dots, x_n) \in M \iff \begin{aligned} &a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ &\vdots \\ &a_{k1}x_1 + \dots + a_{kn}x_n = 0 \\ &a_1x_1 + \dots + a_nx_n = 0 \end{aligned}$$

dır. Bu ise şunu söylemeye denktir;

$$(x_1, \dots, x_n) \in M \iff \forall t \in \mathbb{N} \text{ için } \begin{aligned} &(a_{11} + ta_1)x_1 + \dots + (a_{1n} + ta_n)x_n = 0 \\ &\vdots \\ &(a_{k1} + ta_1)x_1 + \dots + (a_{kn} + ta_n)x_n = 0 \\ &a_1x_1 + \dots + a_nx_n = 0 \end{aligned}$$

Yeteri kadar büyük  $t$  için  $a_i > 0$  olduğundan her  $i, j$  için  $a_{ij} + ta_j$  bir pozitif tamsayı olur.

Önerme 3.1 den  $\mathbb{N}^n / \sim_M$  monoidi ve sonuç olarak  $S, \mathbb{Z}^{k+1}$  in

$$\{(a_{11} + ta_1, \dots, a_{k1} + ta_1, a_1), \dots, (a_{1n} + ta_n, \dots, a_{kn} + ta_n, a_n)\}$$

tarafından doğurulan alt monoidine izomorfiktir.

Bütün  $a_{ij} + ta_j$  elemanları pozitif olduğundan bu alt monoid  $\mathbb{N}^{k+1}$  in bir alt monoididir.

$\Leftarrow$ : Aşıkır. ■

**Tanım 3.16**  $\mathbb{N}^k$  nin bir alt monoidine izomorfik olan sonlu doğuraylı bir monoide bir *afin*  
yarıgrubu denir.

O zaman Teorem 3.15,

$S$  monoidi bir afin yarıgruptur  $\iff S$  monoidi sonlu doğuraylı, sadeleşmeli,  
burulmasız ve indirgenmiştir

olur.

**Örnek 3.17**  $M = \mathbf{G}(\{(1, -2, 2, -1), (-3, 1, 1, 1)\}) \subseteq \mathbb{Z}^4$  verilsin. O zaman

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 & 2 & -1 \\ -3 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & -1 & 1 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$



dir. Böylece

$$(x_1, x_2, x_3, x_4) \in M \iff \begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1 - 2x_2 + 5x_4 &= 0 \end{aligned}$$

elde edilir. Birinci denklemi 2 ile çarpıp ikinci denkleme eklersek

$$(x_1, x_2, x_3, x_4) \in M \iff \begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ 3x_1 + 2x_3 + 7x_4 &= 0 \end{aligned}$$

elde ederiz. Dolayısıyla  $\mathbb{N}^4 / \sim_M$ ,  $\mathbb{N}^2$  nin  $\{(1, 3), (1, 0), (1, 2), (1, 7)\}$  tarafından doğurulan alt monoidine izomorftur.  $\diamond$

### 3.3 Sonlu Sadeleşmeli Monoidler

**Önerme 3.18**  $S$  sonlu bir monoid olsun. O zaman  $S$  nin bir grup olması için gerek ve yeter koşul  $S$  nin sadeleşmeli olmasıdır.

**İspat:**  $\implies$ : Aşık.

$\impliedby$ :  $s \in S \setminus \{0\}$  alalım.  $S$  sonlu olduğundan  $\{ns \mid n \in \mathbb{N} \setminus \{0\}\} \subseteq S$  kümesi de sonlu olmak zorundadır. O zaman  $m < n$  için  $ms = ns$  olacak şekilde  $m, n \in \mathbb{N} \setminus \{0\}$  vardır.  $S$  sadeleşmeli olduğundan  $(n - m)s = 0$  olur.  $n - m > 0$  olduğundan  $(n - m - 1)s + s = 0$  olur. Yani  $s$  nin bir tersi vardır. O halde  $S$  bir gruptur. ■

$S$  sadeleşmeli ise bir  $n \in \mathbb{Z}^+$  ve  $\mathbb{Z}^n$  nin bir  $M$  alt grubu için  $S$  nin  $\mathbb{N}^n / \sim_M$  formunda olduğunu biliyoruz. Eğer  $S$  burulmasız veya indirgenmiş ise  $M$  nin denklemlerinin özel formlarda olduğunu gösterdik. Sonlu olma durumunda da benzer bir özelliğin var olduğunu gösterelim.

**Teorem 3.19**  $M, \mathbb{Z}^n$  nin bir alt grubu olsun. O zaman aşağıdakiler birbirine denktir.

1.  $\mathbb{N}^n / \sim_M$  sonludur.
2.  $\text{rank}(M) = n$  dir.
3.  $M$  homojen bir denkleme sahip değildir. Yani  $M$  nin denklemlerinin içinde

$$a_1x_1 + \cdots + a_nx_n = 0$$

formunda bir denklem yoktur.

**İspat:**  $1 \implies 2$ : Önerme 3.18 ün ispatındaki argümanı kullanarak her  $i$  için  $k_i [e_i] = 0$  olacak şekilde  $k_1, \dots, k_n \in \mathbb{N} \setminus \{0\}$  elde edebiliriz. Bunun anlamı ise her  $i$  için  $k_i e_i \in M$  olmasıdır. Bu ise  $\text{rank}(M) = n$  anlamına gelir.

$2 \implies 3$ : Burada ise  $V = \mathbf{L}_{\mathbb{Q}}(M)$  alt uzayı  $\mathbb{Q}^n$  ile çakışır. Eğer  $M$  bir homojen denkleme sahipse buna  $a_1 x_1 + \dots + a_n x_n = 0$  diyelim, o zaman

$$(a_1, \dots, a_n) \in V^{\perp} = (\mathbb{Q}^n)^{\perp} = \{0\}$$

ve böylece her  $i$  için  $a_i = 0$  elde edilir.

$3 \implies 1$ : Eğer  $M$  nin denklemlerini İkinci Bölümdeki gibi hesaplarsak her  $i$  için  $d_i \mid d_{i+1}$  olmak üzere

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &\equiv 0 \pmod{d_1} \\ &\vdots \\ a_{r1}x_1 + \dots + a_{rn}x_n &\equiv 0 \pmod{d_r} \end{aligned}$$

olmak zorunda olduğunu biliyoruz. Her  $i$  için  $d_r e_i \in M$  olduğuna dikkat edelim. Böylece  $\mathbb{N}^n / \sim_M$  de  $d_r [e_i] = [0]$  olur. O zaman  $a_i \in \{0, \dots, d_r - 1\}$  olmak üzere  $\mathbb{N}^n / \sim_M$  nin bütün elemanları  $\sum_{i=1}^n a_i [e_i]$  formunda olmak zorunda olduğundan  $\mathbb{N}^n / \sim_M$  nin eleman sayısı  $(d_r)^n$  den küçük yada  $(d_r)^n$  ye eşittir. ■

**Sonuç 3.20**  $M, \mathbb{Z}^n$  nin rankı  $n$  ve invaryant faktörleri  $d_1, \dots, d_n$  olan bir alt grubu olsun. O zaman;

1.  $\mathbb{N}^n / \sim_M$  sonlu bir gruptur.
2.  $M$ , bir kuvvetli pozitif eleman içerir.
3.  $\mathbb{N}^n / \sim_M \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_n}$  dir. □

**Örnek 3.21**  $M = \mathbf{G}(\{(2, -4, 2), (-6, 2, 2), (-2, 2, 4)\})$  alt grubunun (ki rankı 3 tür) invaryant faktörlerini hesaplarsak  $d_1 = d_2 = 2$  ve  $d_3 = 22$  bulunur. O halde

$$\mathbb{N}^n / \sim_M \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{22}$$

dir. ◇

#### 4. MINKOWSKI-FARKAS LEMMASI VE MONOİDLERDEKİ UYGULAMALARI

Üçüncü bölümde,  $\mathbb{Q}^n$  nin bir  $V$  alt uzayının tek negatif olmayan elemanı  $0$  ise  $V^\perp$  in bir kuvvetli pozitif elemanının var olduğunu gördük. Bu Minkowski-Farkas Lemmanın uygulamalarından biridir. Bu bölümde Minkowski-Farkas Lemmayı ifade ve ispat edeceğiz. Ayrıca bu sonucun daha önce verilen sonuçları elde etmekte nasıl kullanılacağını göstereceğiz. Ek olarak,  $\mathbb{Q}^n$  nin bir alt uzayının aşikar olmayan negatif olmayan elemanlarının olup olmadığını karar vermede kullanılacak bir dizi algoritma vereceğiz. Bu algoritmaların bir kaç uygulamasından da söz edeceğiz. Özellikle aşağıdaki listede verilen hesaplama işlemlerinde uygulamaların nasıl yapılacağını göreceğiz.

1.  $\mathbb{N}^n / \sim_M$  formundaki bir monoidin bir grup olup olmayacağına karar vermek.
2.  $\mathbb{N}^n / \sim_M$  formundaki bir monoidin afin olup olmayacağına karar vermek ve eğer afin ise  $S \cong \mathbb{N}^n / \sim_M$  olacak şekilde bir  $k \in \mathbb{N} \setminus \{0\}$  ve  $\mathbb{N}^k$  nin sonlu doğuraylı bir  $S$  alt monoidini hesaplamak.
3.  $\mathbb{N}^n / \sim_M = U(\mathbb{N}^n / \sim_M) + C$  ve  $U(\mathbb{N}^n / \sim_M) \cap C = \{0\}$  olacak şekilde  $\mathbb{N}^n / \sim_M$  nin birimlerinin grubunu ve  $\mathbb{N}^n / \sim_M$  nin bir  $C$  alt monoidini hesaplamak.
4. Rasyonel katsayılı bir homojen lineer denklem sisteminin, bütün koordinatları negatif olmayan tamsayı olacak şekilde aşikar olmayan bir çözüme sahip olup olmayacağına karar vermek.
5.  $\mathbb{N}^n$  nin iki sonlu doğuraylı alt monoidinin kesişiminin aşikar olup olmayacağına karar vermek, aşikar değilse kesişimde sıfırdan farklı bir eleman bulmak.

##### 4.1 Temel Sonuçlar ve Algoritmalar

Bu bölüm boyunca, verilen bir  $x \in \mathbb{Q}^n$  için  $x \geq 0$  gösterimi  $x$  elemanının her bir koordinatının sıfır yada sıfırdan büyük olduğunu,  $x > 0$  gösterimi de tüm koordinatlarının sıfırdan büyük olduğunu ifade edecektir. Aynı şekilde  $x \leq 0$  ve  $x < 0$  da benzer anlamlara sahiptir.

**Teorem 4.1 (Minkowski-Farkas' lemma)**  $A$  ve  $b$  sırasıyla  $m \times n$  ve  $m \times 1$  tipinde rasyonel katsayılı matrisler olsun.  $x$  ve  $y$  de sırasıyla  $n \times 1$  ve  $1 \times m$  tipinde bilinmeyen matrisler

olsun. O zaman aşağıdakiler birbirine denktir.

1.  $\left\{ \begin{array}{l} Ax = b \\ x \geq 0 \end{array} \right\}$  sistemi rasyoneller üzerinde bir çözüme sahiptir.
2.  $\left\{ \begin{array}{l} yA \geq 0 \\ yb < 0 \end{array} \right\}$  sistemi rasyoneller üzerinde bir çözüme sahip değildir.

**İspat:**  $1 \implies 2$ : Her  $y \in \mathbb{Q}^n$  için  $yb = yAx$  olur.  $yA \geq 0$  ise  $yb \geq 0$  olur. Bu ise  $\left\{ \begin{array}{l} yA \geq 0 \\ yb < 0 \end{array} \right\}$  sisteminin rasyoneller üzerinde bir çözümünün olmadığı anlamına gelir.

$2 \implies 1$ :  $\left\{ \begin{array}{l} Ax = b \\ x \geq 0 \end{array} \right\}$  sisteminin rasyoneller üzerinde bir çözümü olmasın. O halde ya  $Ax = b$  nin rasyoneller üzerinde bir çözümü yoktur ya da  $Ax = b$  nin her çözümünün en az bir koordinatı negatiftir.

$A$  nın  $i$ -inci kolonunu  $A_i$  ile gösterelim. Her iki durumda da  $\left\{ \begin{array}{l} yA \geq 0 \\ yb < 0 \end{array} \right\}$  sisteminin rasyoneller üzerinde bir çözümünün olduğu gösterilerek çelişki elde edilecektir.

1. Durum: Eğer  $Ax = b$  nin rasyoneller üzerinde bir çözümü yoksa,  $\sum_{i=1}^n x_i A_i = b$  olacak şekilde bir  $(x_1, \dots, x_n) \in \mathbb{Q}^n$  elemanı yoktur. Dolayısıyla  $b$ ,  $\mathbb{Q}^m$  nin  $\{A_1, \dots, A_n\}$  tarafından gerilen  $V$  alt uzayının elemanı olamaz. O halde  $b \notin V$  olduğundan  $yb \neq 0$  olacak şekilde bir  $y \in V^\perp$  seçebiliriz. Şimdi  $yb < 0$  yada  $yb > 0$  olabilir.  $yb < 0$  ise,  $y, \left\{ \begin{array}{l} yA = 0 \\ yb < 0 \end{array} \right\}$  sistemi için bir çözüm olur.  $yb > 0$  ise,  $y$  yerine  $-y$  alarak yine  $\left\{ \begin{array}{l} yA = 0 \\ yb < 0 \end{array} \right\}$  sistemi için bir çözüm bulunmuş olur. Her iki durumda da  $\left\{ \begin{array}{l} yA \geq 0 \\ yb < 0 \end{array} \right\}$  sistemi, rasyoneller üzerinde bir çözüme sahip olur.

2. Durum:  $Ax = b$  nin bir çözüme sahip olduğunu fakat her çözümün en az bir koordinatının negatif olduğunu varsayalım.  $\left\{ \begin{array}{l} yA \geq 0 \\ yb < 0 \end{array} \right\}$  sisteminin bir çözümünün olduğunu göstermek için  $A$  nın kolon sayısı üzerinden tümevarım yapacağız.

$n = 1$  olsun. Bu durumda  $Ax = xA_1 = b$  denkleminin bir koordinatı sıfırdan küçük olacak şekilde en az bir çözümü vardır. Fakat bu durumda yegane koordinat  $x$  olduğundan  $x < 0$  dır.  $y = -b$  olarak

$$yA = -bA_1 = \left(-\frac{1}{x}\right)b^2 \geq 0$$

ve  $yb = -b^2 < 0$  elde ederiz ( $b^2$ ,  $b$  ile  $b$  nin iç çarpımıdır).

$n-1$  için önerme doğru olsun. Eğer  $\sum_{i=1}^n x_i A_i = Ax = b$  denklem sistemi  $x \geq 0$  şeklinde bir çözüme sahip değilse  $\sum_{i=1}^{n-1} x_i A_i = b$  denklem sistemi de bir negatif olmayan çözüme sahip olamaz.  $n-1$  için varsayımımız gereğince her  $1 \leq i \leq n-1$  için  $\begin{cases} yA_i \geq 0 \\ yb < 0 \end{cases}$  olacak şekilde bir  $y \in \mathbb{Q}^m$  vardır. Eğer  $yA_n \geq 0$  ise  $\begin{cases} yA \geq 0 \\ yb < 0 \end{cases}$  olur ki bu bizim aradığımız sonuçtur. Dolayısıyla  $yA_n < 0$  varsayalım. Bu durumda

- 1)  $a_0 = -\frac{yb}{yA_n} < 0$  ve her  $1 \leq i \leq n-1$  için  $a_i = -\frac{yA_i}{yA_n} \geq 0$
- 2)  $\forall 1 \leq i \leq n-1$  için  $A'_i = A_i + a_i A_n$
- 3)  $b' = b + a_0 A_n$

tanımlayalım.

$\sum_{i=1}^{n-1} x'_i A'_i = b'$  denklem sisteminin  $\sum_{i=1}^{n-1} x'_i A_i + \left( \left( \sum_{i=1}^{n-1} a_i x'_i \right) - a_0 \right) A_n = b$  denklem sisteminde denk olduğuna dikkat edelim.  $\sum_{i=1}^{n-1} x'_i A'_i = b'$  denklem sisteminin her  $1 \leq i \leq n-1$  için  $x'_i \geq 0$  olacak şekilde bir çözümü varsa

$$\begin{aligned} b' &= b + a_0 A_n = x'_1 A'_1 + x'_2 A'_2 + \cdots + x'_{n-1} A'_{n-1} \\ &= x'_1 A_1 + x'_2 A_2 + \cdots + x'_{n-1} A_{n-1} + x'_1 a_1 A_n + x'_2 a_2 A_n + \cdots + x'_{n-1} a_{n-1} A_n \end{aligned}$$

dolayısıyla

$$\begin{aligned} b &= x'_1 A_1 + x'_2 A_2 + \cdots + x'_{n-1} A_{n-1} + x'_1 a_1 A_n + x'_2 a_2 A_n + \cdots + x'_{n-1} a_{n-1} A_n - a_0 A_n \\ &= x'_1 A_1 + x'_2 A_2 + \cdots + x'_{n-1} A_{n-1} + \left( -x'_1 \frac{yA_1}{yA_n} - x'_2 \frac{yA_2}{yA_n} - \cdots - x'_{n-1} \frac{yA_{n-1}}{yA_n} + \frac{yb}{yA_n} \right) A_n \\ &= x'_1 A_1 + x'_2 A_2 + \cdots + x'_{n-1} A_{n-1} + \underbrace{\left( -\frac{x'_1 yA_1 + x'_2 yA_2 + \cdots + x'_{n-1} yA_{n-1}}{yA_n} + \frac{yb}{yA_n} \right)}_{\geq 0} A_n \end{aligned}$$

olduğundan  $Ax = b$  nin  $x \geq 0$  formunda bir çözümünün olduğu gösterilmiş olur. O halde her  $1 \leq i \leq n-1$  için  $a_0 < 0$  ve  $a_i \geq 0$  olduğundan  $Ax = b$  nin  $x \geq 0$  formunda bir çözümünün olmadığını kabul edersek  $\sum_{i=1}^{n-1} x'_i A'_i = b'$  sisteminin de her  $1 \leq i \leq n-1$  için  $x'_i \geq 0$  olacak şekilde bir çözümü yoktur. Tümevarım varsayımını bu defa  $\sum_{i=1}^{n-1} x'_i A'_i = b'$  için kullanacak olursak; her  $1 \leq i \leq n-1$  için  $y'A'_i \geq 0$  ve  $y'b' < 0$  olacak şekilde  $y' \in \mathbb{Q}^m$  var olduğu görülür. Şimdi  $\bar{y} = y' - \left( \frac{y'A_n}{yA_n} \right) y$  koyalım.

$$\begin{aligned}
 \bar{y}A &= y'A - \left( \frac{y'A_n}{yA_n} \right) yA \\
 &= \begin{pmatrix} y'A'_1 & y'A'_2 & \cdots & y'A'_{n-1} & y'A_n \end{pmatrix} \\
 &\quad - \begin{pmatrix} y'a_1A_n + \frac{y'A_n}{yA_n}yA_1 & y'a_2A_n + \frac{y'A_n}{yA_n}yA_2 & \cdots & y'a_{n-1}A_n + \frac{y'A_n}{yA_n}yA_{n-1} & \frac{y'A_n}{yA_n}yA_n \end{pmatrix} \\
 &= \begin{pmatrix} y'A'_1 & y'A'_2 & \cdots & y'A'_{n-1} & y'A_n \end{pmatrix} \\
 &\quad - \begin{pmatrix} y'A_n \left( a_1 + \frac{yA_1}{yA_n} \right) & y'A_n \left( a_2 + \frac{yA_2}{yA_n} \right) & \cdots & y'A_n \left( a_{n-1} + \frac{yA_{n-1}}{yA_n} \right) & y'A_n \end{pmatrix} \\
 &= \begin{pmatrix} y'A'_1 & y'A'_2 & \cdots & y'A'_{n-1} & y'A_n \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & 0 & y'A_n \end{pmatrix} \\
 &= \begin{pmatrix} y'A'_1 & y'A'_2 & \cdots & y'A'_{n-1} & 0 \end{pmatrix} \geq 0 \\
 &\implies \bar{y}A \geq 0 \\
 y'b' < 0 &\implies y'(b + a_0A_n) < 0 \implies y'b + a_0y'A_n < 0 \implies y'b - \left( \frac{y'A_n}{yA_n} \right) yb < 0 \\
 &\implies \bar{y}b < 0
 \end{aligned}$$

Böylece tümevarım ve dolayısıyla ispat tamamlanmış olur. ■

3. bölümde lemma 3.13 un tersini yapmak için Minkowski-Farkas Lemma'ya ihtiyaç duyduğumuzu söylemiştik. Şimdi lemma 3.13 un tersini yapabiliriz.

**Teorem 4.2**  $V, \mathbb{Q}^n$  nin bir alt uzayı olsun.  $V$  nin tek negatif olmayan elemanı 0 ise  $V^\perp$  in bir kuvvetli pozitif elemanı vardır.

**İspat:**  $m_i = (m_{i1}, \dots, m_{in})$  olmak üzere  $B = \{m_1, \dots, m_r\}$ ,  $V$  nin bir bazı olsun.

$$A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{r1} & m_{r2} & \cdots & m_{rn} \\ 1 & 0 & \cdots & 0 \end{pmatrix} \text{ ve } b = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

olsun.  $\left\{ \begin{matrix} yA \geq 0 \\ yb < 0 \end{matrix} \right\}$  sisteminin rasyoneller üzerinde bir çözümünün olmadığını gösterelim.

Eğer  $y = (y_1, \dots, y_{r+1})$  bu sistem için bir çözüm ise  $yb < 0$  olduğundan  $y_{r+1} < 0$  olur.  $yA \geq 0$  olduğundan

$$\left( \sum_{i=1}^r y_i m_{i1} + y_{r+1}, \sum_{i=1}^r y_i m_{i2}, \dots, \sum_{i=1}^r y_i m_{in} \right) \geq 0$$

olur ve buradan

$$\left( \sum_{i=1}^r y_i m_{i1}, \sum_{i=1}^r y_i m_{i2}, \dots, \sum_{i=1}^r y_i m_{in} \right) \geq (-y_{r+1}, 0, \dots, 0)$$

olur. Böylece  $\sum_{i=1}^r y_i m_i$  nin ilk koordinatı sıfırdan büyük, geri kalanların ise sıfıra eşit yada sıfırdan büyük olur.  $V$ ,  $(0, \dots, 0)$  dan başka negatif olmayan eleman içermediğinden dolayı bu bir çelişkidir. Minkowski Farkas Lemma'dan dolayı,  $\left\{ \begin{array}{l} Ax = b \\ x \geq 0 \end{array} \right\}$  sisteminin rasyoneller üzerinde bir çözümü vardır.  $a_1 = (a_{11}, \dots, a_{1n})$  bu sistemin bir çözümü olsun. O zaman  $a_1 \geq 0$  ve matris çarpımından dolayı  $a_1 \in V^\perp$ ,  $a_{11} = 1$  dir.

Benzer şekilde devam ettiğimizde,

$$A = \begin{pmatrix} m_{11} & \cdots & m_{1i} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{ri} & \cdots & m_{rn} \\ 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}$$

matrisi ile  $a_i = (a_{i1}, \dots, a_{in})$  elemanını elde ederiz öyle ki  $a_i \in V^\perp$ ,  $a_{ii} = 1$  ve  $a_i \geq 0$  dır. O halde  $a = \sum_{i=1}^n a_i$ ,  $V^\perp$  de bir kuvvetli pozitif elemandır. ■

$\mathbb{Q}^n$  nin bir  $V$  alt uzayının, (eğer varsa) ilk koordinatı sıfırdan büyük bir negatif olmayan elemanını bulacak bir işlemler zincirini verebilmek için Minkowski-Farkas' lemmanın ispatındaki fikri kullanacağız.

$m_i = (m_{i1}, \dots, m_{in})$  olmak üzere eğer  $B = \{m_1, \dots, m_r\}$ ,  $V$  nin bir bazı ise  $x = (x_1, \dots, x_n)$  nin  $V$  nin elemanı olması için gerek ve yeter koşul  $x = \sum_{i=1}^r y_i m_i$  olacak şekilde  $y = (y_1, \dots, y_r) \in \mathbb{Q}^r$  elemanının var olmasıdır. Matris gösterimini kullanarak bunu

$$A = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix}$$

olmak üzere  $yA = x$  şeklinde ifade edebiliriz.

$A$  nın  $i$ -inci kolonunu  $A_i$  ile gösterelim.  $x_i = yA_i$  olduğundan, eğer  $x$  ilk koordinatı sıfırdan büyük olan bir negatif olmayan eleman ise her  $i$  için

$$yA_i \geq 0$$

$$yA_1 > 0$$

dır. Bu nedenle  $V$  nin ilk koordinatı sıfırdan büyük bir negatif olmayan elemana sahip olması için gerek ve yeter koşul  $yA_1 > 0$  ve her  $i \in \{2, \dots, n\}$  için  $yA_i \geq 0$  olacak şekilde bir  $y \in \mathbb{Q}^r$  olmasıdır. O zaman dikkatimizi  $yA_1 > 0$  ve her  $i \in \{2, \dots, n\}$  için  $yA_i \geq 0$  olacak şekilde bir  $y \in \mathbb{Q}^r$  bulmaya yoğunlaştıralım.

Aşağıdakilere dikkat edelim;

1. Eğer problemimiz  $\begin{pmatrix} A_1 & \dots & A_{n-1} \end{pmatrix}$  matrisi için bir çözüme sahip değilse  $A$  için de bir çözüme sahip olamaz,
2. Eğer problemimiz  $\begin{pmatrix} A_1 & \dots & A_{n-1} \end{pmatrix}$  için  $z$  gibi bir çözüme sahip ve  $zA_n \geq 0$  ise  $zA$ ,  $V$  nin ilk koordinatı sıfırdan büyük olan bir negatif olmayan elemanıdır.
3. Bir önceki durumda olduğu gibi eğer  $z$ ,  $\begin{pmatrix} A_1 & \dots & A_{n-1} \end{pmatrix}$  için bir çözüm fakat  $zA_n < 0$  ise Minkowski Farkas' lemmanın ispatındaki gibi  $a_i$  ve  $A'_i$  ( $1 \leq i \leq n-1$ ) tanımlanır. Burada iki alt durumu irdeleyeceğiz (detaylarla ilgilenmeyeceğiz);
  - (a) Eğer  $z'A'_1 > 0$  ve  $\forall i \in \{2, \dots, n-1\}$  için  $z'A'_i \geq 0$  olacak şekilde bir  $z' \in \mathbb{Q}^r$  varsa  $y = z' - ((z'A_n) / (zA_n))z$  tanımlar ve  $yA_1 > 0$ ,  $\forall i \in \{2, \dots, n\}$  için  $yA_i \geq 0$  elde ederiz.
  - (b) Eğer  $z'A'_1 > 0$  ve  $\forall i \in \{2, \dots, n-1\}$  için  $z'A'_i \geq 0$  olacak şekilde bir  $z' \in \mathbb{Q}^r$  yoksa  $yA_1 > 0$  ve  $\forall i \in \{2, \dots, n\}$  için  $yA_i \geq 0$  olacak şekilde bir  $y \in \mathbb{Q}^r$  yoktur.

**Algoritma 4.3 (FP)** Algoritmanın girdisi, satırları  $\mathbb{Q}^n$  nin bir  $V$  altuzayı için bir baz olan  $A$  matrisi, çıktısı ise  $V$  de ilk koordinatı sıfırdan büyük olan bir negatif olmayan elemandır. Eğer böyle bir eleman yoksa algoritma “yanlış” sonucunu üretir. Adımlar;

1. Eğer  $n = 1$  ise  $i = \min \{k \mid a_{k1} \neq 0\}$  olmak üzere  $y = (0, \dots, 0, a_{i1}, 0, \dots, 0)$  alınır ve sonuç olarak  $x = yA = yA_1$  yapılır. Eğer  $A_1$  in bütün bileşenleri sıfır ise problemin çözümü yoktur ve dolayısıyla “yanlış” sonucu üretilir.
2. Eğer  $n > 1$  ise problem  $\begin{pmatrix} A_1 & \dots & A_{n-1} \end{pmatrix}$  için çözülür. Eğer  $\begin{pmatrix} A_1 & \dots & A_{n-1} \end{pmatrix}$  için bir çözüm yoksa  $A$  için de bir çözüm yoktur, aksi halde  $z$ ,  $\mathbb{Q}^r$  nin  $zA_1 > 0$  ve  $\forall i \in \{2, \dots, n-1\}$  için  $zA_i \geq 0$  olacak şekildeki bir elemanı olsun.
  - (a) Eğer  $zA_n \geq 0$  ise  $zA$ ,  $V$  nin ilk koordinatı sıfırdan büyük bir negatif olmayan elemanıdır. O halde çıktı olarak  $zA$  alınır.



- (b) Eğer  $zA_n < 0$  ise  $A'_i = A_i - ((zA_i) / (zA_n))A_n$  alınır ve problem  $\left( \begin{matrix} A'_1 & \dots & A'_{n-1} \end{matrix} \right)$  için çözülür.
- i. Eğer  $\left( \begin{matrix} A'_1 & \dots & A'_{n-1} \end{matrix} \right)$  için bir çözüm yoksa, özgün problemin de çözümü yoktur ve dolayısıyla “yanlış” sonucu üretilir.
- ii. Eğer  $z'$ ,  $\left( \begin{matrix} A'_1 & \dots & A'_{n-1} \end{matrix} \right)$  için bir çözüm ise  $y = z' - ((z'A_n) / (zA_n))z$  tanımlanır ve çıktı olarak  $x = yA$  alınır.  $\diamond$

Bu algoritmayı bir örnekle açıklayalım.

**Örnek 4.4**  $V = \mathbf{L}_{\mathbb{Q}}(\{(1, -1, 1, 1), (0, 1, -1, -1), (-1, 1, 0, -1)\})$  verilsin. O zaman

$$A = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & -1 \end{pmatrix}$$

dir. Biz,  $V$  nin ilk koordinatı sıfırdan büyük olan bir negatif olmayan eleman arıyoruz. Bu ise

$$yA_1 > 0, yA_2 \geq 0, yA_3 \geq 0, yA_4 \geq 0$$

olacak şekilde bir  $y \in \mathbb{Q}^3$  bulmaya denktir. Algoritmayı izlersek, problemi  $\left( \begin{matrix} A_1 & A_2 & A_3 \end{matrix} \right)$ ,  $\left( \begin{matrix} A_1 & A_2 \end{matrix} \right)$  için dolayısıyla ilk önce  $A_1$  için çözmeliyiz. Problemi bu şekilde indirgeyebildiğimize dikkat edelim.  $a_{11} \neq 0$  olduğundan  $z = (1, 0, 0)$  olarak  $zA_1 = 1 > 0$  olduğunu görebiliriz. Fakat  $zA_2 = -1 < 0$  olduğundan  $z$ ,  $\left( \begin{matrix} A_1 & A_2 \end{matrix} \right)$  için bir çözüm olamaz. O zaman

$$A'_1 = A_1 - ((zA_1) / (zA_2))A_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

oluşturulur.  $z' = (0, 1, 0)$ ,  $A'_1$  için bir çözümdür. Buradan

$$y = z' - ((z'A_2) / (zA_2))z = (1, 1, 0)$$

tanımlarız.  $yA_1 = 1 > 0$  ve  $yA_2 = 0 \geq 0$  olduğuna dikkat edelim. Bu elemanın  $\left( \begin{matrix} A_1 & A_2 & A_3 \end{matrix} \right)$  için bir çözüm olup olamayacağını kontrol edelim.  $yA_3 = 0 \geq 0$  olduğundan  $y$ ,  $\left( \begin{matrix} A_1 & A_2 & A_3 \end{matrix} \right)$  için bir çözümdür. Son olarak  $yA_4 = 0 \geq 0$  dır. Böylece  $yA = (1, 0, 0, 0)$ ,  $V$  nin ilk koordinatı sıfırdan büyük bir negatif olmayan elemanıdır.  $\diamond$

Eğer  $V$  nin  $i$ –inci koordinatı sıfırdan büyük olan bir negatif olmayan elemanın olup olmadığıyla ilgileniyorsak, biraz önce tanımladığımız algoritmayı

$$\begin{pmatrix} A_i & A_{i+1} & \dots & A_n & A_1 & \dots & A_{i-1} \end{pmatrix}$$

matrisine uygulamalıyız. Böylece her  $i$  için,  $i$ –inci koordinatı sıfırdan büyük bir negatif olmayan eleman (var olması koşuluyla) bulabiliriz.

Eğer her  $i$  için böyle elemanlar varsa, bunların hepsini toplayarak  $V$  nin bir kuvvetli pozitif elemanını elde etmiş oluruz. Ancak, Algoritma FP nin  $i$ –inci koordinatı sıfırdan büyük bir negatif olmayan eleman bulmakta başarısız olduğu bir  $i$  varsa,  $V$  nin bir kuvvetli pozitif elemanı yoktur. Bu algoritmanın geliştirilebileceğine de dikkat edelim. İşe ilk koordinatı sıfırdan büyük olan bir negatif olmayan eleman aramakla başlarız. Eğer bulduğumuz eleman bir kuvvetli pozitif eleman ise dururuz, değilse bunun koordinatlarında sıfırın ilk bulunduğu yere bakarız ve sonra burası için algoritmayı tekrar ederiz. Bulacağımız yeni elemaya öncekini ekler ve bu işleme devam ederiz. Bir kuvvetli pozitif eleman bulduğumuzda veya Algoritma FP, gereken bir koordinatı sıfırdan büyük olan bir negatif olmayan eleman bulmakta başarısız olduğunda dururuz. Bu nedenle algoritmayı aşağıdaki gibi de tanımlayabilirdik.

**Algoritma 4.5 (SP)** Algoritmanın girdisi; satırları  $\mathbb{Q}^n$  nin bir  $V$  altuzayı için bir baz olan  $A$  matrisi, çıktısı ise  $V$  nin  $x$  gibi (var olması koşuluyla) bir kuvvetli pozitif elemanıdır. Eğer böyle bir eleman yoksa algoritma “yanlış” sonucunu üretir. Adımlar;

1. Algoritma FP,  $A$  matrisine uygulanır. Algoritma başarısız olursa “yanlış” sonucunu üretir. Aksi halde  $y$ , algoritma FP nin çıktısı ise  $x = yA$  alınır.
2. Eğer  $x$  in bütün koordinatları sıfırdan büyük ise çıktı olarak  $x$  alınır. Aksi halde  $x$  in koordinatları içindeki ilk sıfır bulunur. Bu sıfırın bulunduğu koordinatına  $i$  ise Algoritma FP,  $\begin{pmatrix} A_i & \dots & A_n & A_1 & \dots & A_{i-1} \end{pmatrix}$  matrisine uygulanır. Eğer Algoritma FP hata verirse “yanlış” sonucu üretilir. Eğer Algoritma FP nin çıktısı  $z$  ise  $x$ ,  $x + (zA_1, \dots, zA_n)$  şeklinde yeniden tanımlanır ve bu adım tekrar edilir.  $\diamond$

**Örnek 4.6** Örnek 4.4 de  $(1, 0, 0, 0) \in V$  bulmuştuk. Ancak  $zA_3 = -1 < 0$  olduğundan  $z$ ,

$\begin{pmatrix} A_2 & A_3 \end{pmatrix}$  matrisine indirgenen problemimiz için çözüm olamaz. O zaman

$$A'_2 = A_2 - ((zA_2)/(zA_3))A_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

ve  $z'A'_2 > 0$  olacak şekilde  $z'$  yi hesaplamalıyız.  $z' = (0, 0, 1)$  olarak

$$y = z' - ((z'A_3)/(zA_3))z = (0, 0, 1)$$

elde ederiz.  $yA_2 = 1 \geq 0$  ve  $yA_3 \geq 0$  fakat  $yA_4 = -1 < 0$  olduğundan bir adım daha tekrarladığımızda

$$A'_2 = A_2 - ((zA_2)/(zA_4))A_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$A'_3 = A_3 - ((zA_3)/(zA_4))A_4 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$$

elde ederiz.  $A'_2$  nin tüm bileşenleri sıfır olduğundan, algoritma,  $z'A'_2 > 0$  olacak şekilde bir  $z'$  bulmakta başarısız olur.

Bu yüzden  $V$  de ikinci koordinatı sıfırdan büyük olacak şekilde bir negatif olmayan eleman yoktur. Dolayısıyla  $V$  de kuvvetli pozitif bir eleman yoktur.  $\diamond$

Eğer bu algoritmada, Algoritma FP nin “yanlış” ürettiği yerde durmasaydık, sonuçta bulacağımız eleman,  $V$  nin maksimum sayıda sıfırdan büyük koordinatı olan bir elemanı olacaktı.

**Algoritma 4.7 (MCP)** Algoritmanın girdisi; satırları  $\mathbb{Q}^n$  nin bir  $V$  altuzayı için bir baz olan  $A$  matrisi, çıktısı ise  $V$  nin maksimum sayıda sıfırdan büyük koordinatı olan  $x$  gibi bir negatif olmayan elemanıdır. Adımlar;

1.  $x = 0$  alınır.
2. Tüm  $i$  ler için Algoritma FP,  $\begin{pmatrix} A_i & \dots & A_n & A_1 & \dots & A_{i-1} \end{pmatrix}$  matrisine uygulanır. Eğer Algoritma FP “yanlış” sonucunu üretirse hiçbirşey yapılmaz, eğer çıktı  $z$  ise  $x$ ,  $x + (zA_1, \dots, zA_n)$  şeklinde yeniden tanımlanır ve devam edilir.  $\diamond$

Bu algoritmada ikinci adımın her  $i$  için tekrarlanmak zorunda olmadığına dikkat edelim. Sadece  $x$  in koordinatları içindeki her sıfır için yapılmalıdır.

**Örnek 4.8** Örnek 4.4 'e geri dönelim. Bildiğimiz gibi  $\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \end{pmatrix}$  için  $x = (1, 0, 0, 0)$  elde etmiş ve  $\begin{pmatrix} A_2 & A_3 & A_4 & A_1 \end{pmatrix}$  için Algoritma FP “yanlış” sonucunu üretmişti. Algoritma FP yi  $\begin{pmatrix} A_3 & A_4 & A_1 & A_2 \end{pmatrix}$  ye uygularsak  $y = (1, 0, 1)$  elde ederiz. Dolayısıyla

$$x = (1, 0, 0, 0) + (0, 0, 1, 0) = (1, 0, 1, 0)$$

dir.  $\begin{pmatrix} A_4 & A_1 & A_2 & A_3 \end{pmatrix}$  için Algoritma FP “yanlış” çıktısı verir. Bu yüzden sonuç olarak aradığımız eleman  $x = (1, 0, 1, 0)$  dir.  $\diamond$

## 4.2 Monoidlere Uygulanışları

Burada, bu bölümde verdiğimiz algoritmaları, sadeleşmeli monoidlere uygulayacağız.

### 4.2.1 $\mathbb{N}^n / \sim_M$ Formundaki Bir Monoidin Grup Olup Olmadığının Kontrolü

$M = \mathbf{G}(\{m_1, \dots, m_r\}) \subseteq \mathbb{Z}^n$  verilsin.  $\mathbb{N}^n / \sim_M$  nin grup olup olmadığını bilmek istiyoruz. Önerme 1.26 den bu ancak ve ancak  $M$  nin bir kuvvetli pozitif eleman içermesi durumunda olur.  $\mathbb{Q}^n$  nin  $V = \mathbf{L}_{\mathbb{Q}}(\{m_1, \dots, m_r\})$  alt uzayını tanımlayalım. Dolayısıyla  $V$  nin bir kuvvetli pozitif eleman içermesi için gerek ve yeter koşul  $M$  nin bir kuvvetli pozitif eleman içermesidir. O halde  $V$  nin bir kuvvetli pozitif eleman içerip içermediğini saptamak için Algoritma SP yi kullanabiliriz.

### 4.2.2 $\mathbb{N}^n / \sim_M$ Formundaki Bir Monoidin Afin Olup Olmadığının Saptanması, Eğer Afin İse $S \simeq \mathbb{N}^n / \sim_M$ Olacak Şekilde Bir $k \in \mathbb{N} \setminus \{0\}$ ve $\mathbb{N}^k$ nin Bir Sonlu Doğuraylı $S$ Alt Monoidinin Bulunması

$M = \mathbf{G}(\{m_1, \dots, m_r\}) \subseteq \mathbb{Z}^n$  verilsin.  $\mathbb{N}^n / \sim_M$  nin bir afin yarıgrubu olup olmadığını bilmek istiyoruz. Bu sebeple teorem 3.15 den dolayı bunun sadeleşmeli, burulmasız ve indirgenmiş olup olmadığını saptamak zorundayız.

1. Önerme 1.21 den  $\mathbb{N}^n / \sim_M$  nin sadeleşmeli olduğu aşikardır.

2.  $M \cap \{e_1, \dots, e_n\} = \emptyset$  varsayabiliriz (önerme 3.10 a bakınız).  $M$  nin invaryant faktörlerini ve  $M$  nin denklemlerini hesaplayalım. Eğer  $M$  homojen değilse  $\mathbb{N}^n / \sim_M$  burulmasız değildir ve bu yüzden  $\mathbb{N}^k$  nin bir alt monoidine izomorfik olamaz. Aksi halde

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{r1}x_1 + \dots + a_{rn}x_n &= 0 \end{aligned}$$

$M$  nin denklemleri olsun.

3. Eğer  $\mathbb{N}^n / \sim_M$  indirgenmiş ise  $M$ ,

$$a_1x_1 + \dots + a_nx_n = 0, \text{ her } i \text{ için } a_i > 0$$

formunda bir denkleme sahip olmak zorundadır (önerme 3.9 ve 3.14 dan). Bu ise ancak ve ancak  $\mathbb{Q}^n$  nin

$$V = \mathbf{L}_{\mathbb{Q}}(\{(a_{11}, \dots, a_{1n}), \dots, (a_{r1}, \dots, a_{rn})\})$$

alt uzayının bir kuvvetli pozitif elemana sahip olması durumunda mümkündür.  $V$  ye Algoritma SP yi uygulayalım. Eğer sonuçta “yanlış” üretilirse yarıgrubumuz afin değildir. Aksi halde  $(a_1, \dots, a_n)$ ,  $V$  nin bir kuvvetli pozitif elemanı olsun. Paydaları elimine edebileceğimizden her  $i$  için  $a_i \in \mathbb{N} \setminus \{0\}$  varsayabiliriz. Bu denklemi yeteri kadar büyük pozitif tamsayılarla çarpar ve diğer denklemlere eklersek  $M$  için

$$\begin{aligned} b_{11}x_1 + \dots + b_{1n}x_n &= 0 \\ &\vdots \\ b_{s1}x_1 + \dots + b_{sn}x_n &= 0 \end{aligned}$$

(her  $i, j$  için  $b_{ij} \in \mathbb{N}$ ) şeklinde yeni denklemler elde ederiz. Dolayısıyla  $\mathbb{N}^s$  nin

$$\{(b_{11}, \dots, b_{s1}), \dots, (b_{1n}, \dots, b_{sn})\}$$

tarafından doğurulan alt monoidi  $\mathbb{N}^n / \sim_M$  ye izomorfik olur (teorem 3.15 in ispatında olduğu gibi).

**Örnek 4.9**  $M = \mathbf{G}(\{(1, -1, 1, -1), (3, 2, 0, -2), (2, 3, -1, -1), (1, 4, -2, 0)\})$  verilsin. İnvaryant faktörlerini hesaplırsak  $d_1 = d_2 = 1$  elde ederiz. Böylece,  $M$  nin denklemleri

$$\begin{aligned} 2x_1 + x_3 + 3x_4 &= 0 \\ -4x_1 + x_2 - 5x_4 &= 0 \end{aligned}$$

olur. Birinci denklemi 2 ile çarpıp ikinci denkleme eklersek

$$(x_1, x_2, x_3, x_4) \in M \iff \begin{aligned} 2x_1 + x_3 + 3x_4 &= 0 \\ x_2 + 2x_3 + x_4 &= 0 \end{aligned}$$

buluruz. Bu durumda Algoritma SP yi uygulamaya gerek yoktur. Dolayısıyla  $\mathbb{N}^4 / \sim_M$  monoidi  $\mathbb{N}^2$  nin

$$S = \langle (2, 0), (0, 1), (1, 2), (3, 1) \rangle$$

alt monoidine izomorftir.  $\diamond$

**Örnek 4.10**  $M = \mathbf{G}(\{(2, -1, -1), (1, 1, -3), (1, -2, -1)\})$  grubunu düşünelim.  $M$  nin invaryant faktörleri  $d_1 = d_2 = 1$  ve  $d_3 = 9$  dur. Bu yüzden  $\mathbb{N}^3 / \sim_M$  burulmasız değildir ve buradan  $\mathbb{N}^3 / \sim_M$  bir afin yarıgrubu değildir. Bu durumda  $M$  nin denklemleri

$$x_1 - x_2 + 3x_3 \equiv 0 \pmod{9}$$

dur ve bu yüzden  $\mathbb{N}^3 / \sim_M$  monoidi  $\langle [1]_9, [8]_9, [3]_9 \rangle = \mathbb{Z}_9$  'a izomorftir olur.  $\diamond$

**Örnek 4.11**  $M = \mathbf{G}(\{(2, -3, 1), (-1, 1, -4)\})$  verilsin. İnvaryant faktörleri  $d_1 = d_2 = 1$  ve denklemleri

$$11x_1 + 7x_2 - x_3 = 0$$

bulunur.  $\mathbb{Q}^3$  'ün  $V = \mathbf{L}_{\mathbb{Q}}(\{(11, 7, -1)\})$  alt uzayının kuvvetli pozitif elemanı yoktur. Bunun anlamı ise,  $\mathbb{N}^3 / \sim_M$  indirgenmiş değildir ve bu yüzden  $\mathbb{N}^3 / \sim_M$  bir afin yarıgrubu değildir.  $\mathbb{N}^3 / \sim_M$  nin  $\mathbb{Z}$  nin  $\{11, 7, -1\}$  tarafından doğurulan alt monoidine izomorftir olduğunu dolayısıyla  $\mathbb{N}^3 / \sim_M$  nin  $\mathbb{Z}$  ye izomorftir olduğuna dikkat edelim.  $\diamond$

**4.2.3**  $\mathbb{N}^n / \sim_M = U(\mathbb{N}^n / \sim_M) + C$  ve  $U(\mathbb{N}^n / \sim_M) \cap C = \{0\}$  **Olacak Şekilde  $\mathbb{N}^n / \sim_M$  nin Birimlerinin Kümesi İle Bir  $C$  Alt Monoidinin Hesaplanması**

Eğer  $x, y \in S$  ve  $x + y \in U(S)$  ise

$$z + (x + y) = (z + x) + y = y + (z + x) = 0$$

olacak şekilde bir  $z \in S$  vardır. Bu yüzden  $x$  ve  $y$  nin her ikisi de  $U(S)$  nin elemanıdır. Bu fikir kullanılarak aşağıdaki sonuç kolayca ispatlanabilir.

**Önerme 4.12**  $S$  ,  $U(S) \cap \{s_1, \dots, s_n\} = \{s_1, \dots, s_r\}$  olacak şekilde  $\{s_1, \dots, s_n\}$  tarafından doğurulan bir monoid olsun. O zaman,

1.  $U(S) = \langle s_1, \dots, s_r \rangle$  ,
2.  $\langle s_{r+1}, \dots, s_n \rangle$  monoidi indirgenmiştir ,
3.  $\langle s_1, \dots, s_r \rangle \cap \langle s_{r+1}, \dots, s_n \rangle = \{0\}$  ve  $S = \langle s_1, \dots, s_r \rangle + \langle s_{r+1}, \dots, s_n \rangle$  dir. □

$S$  nin doğuray kümesinin seçimine bağlı olarak  $U(S)$  tek türlü bellidir, fakat  $\langle s_{r+1}, \dots, s_n \rangle$  tek türlü belli değildir. Bu yüzden  $\langle s_{r+1}, \dots, s_n \rangle$  alt monoidine  $U(S)$  nin *komplementi* (tümleyeni) diyeceğiz.

**Önerme 4.13**  $M$  ,  $\mathbb{Z}^n$  nin bir alt grubu olsun. O zaman

$$U(\mathbb{N}^n / \sim_M) \cap \{[e_1], \dots, [e_n]\} = \{[e_{i_1}], \dots, [e_{i_r}]\}$$

olması için gerek ve yeter koşul

1. eğer  $(y_1, \dots, y_n) \in M \cap \mathbb{N}^n$  ise her  $i \notin \{i_1, \dots, i_r\}$  için  $y_i = 0$  ,
2. eğer  $i \in \{i_1, \dots, i_r\}$  ise  $x_i > 0$  aksi halde  $x_i = 0$  olacak şekilde bir  $(x_1, \dots, x_n) \in M$  var olmasıdır.

**İspat:**  $\implies$ :  $(a_1, \dots, a_n) \in M \cap \mathbb{N}^n$  alalım. Eğer  $a_i > 0$  ise

$$(a_1, \dots, a_n) - 0 \in M \implies ((a_1, \dots, a_n), 0) \in \sim_M \implies [(a_1, \dots, a_n)] = [0]$$

ve dolayısıyla

$$[e_i] + (a_1 [e_1] + \dots + (a_i - 1) [e_i] + \dots + a_n [e_n]) = [(a_1, \dots, a_n)] = [0]$$

dır. Buradan  $[e_i] \in U(\mathbb{N}^n / \sim_M)$  dır. Bu, birinci koşulun ispatıdır.

$[e_{i_1}], \dots, [e_{i_r}] \in U(\mathbb{N}^n / \sim_M)$  olduğundan  $\sum_{j=1}^r [e_{i_j}] \in U(\mathbb{N}^n / \sim_M)$  dir. Bu yüzden

$$\sum_{j=1}^r [e_{i_j}] + \sum_{i=1}^n a_i [e_i] = [0]$$

olacak şekilde  $\sum_{i=1}^n a_i [e_i] \in \mathbb{N}^n / \sim_M$  vardır.

$$(x_1, \dots, x_n) = (a_1, \dots, a_{i_1} + 1, \dots, a_{i_r} + 1, \dots, a_n)$$

elemanı da ikinci koşulu gerçekler.

$\Leftarrow$ :  $(x_1, \dots, x_n) \in M$ ,  $\forall i \in \{i_1, \dots, i_r\}$  için  $x_i > 0$  ve geri kalan koordinatları sıfır olacak şekilde bir eleman olsun. Daha önce olduğu gibi,

$$\{[e_{i_1}], \dots, [e_{i_r}]\} \subseteq U(\mathbb{N}^n / \sim_M)$$

olur. Eğer  $[e_i]$  bir birim ise  $[e_i] + [(a_1, \dots, a_n)] = [0]$  olacak şekilde bir  $[(a_1, \dots, a_n)] \in \mathbb{N}^n / \sim_M$  vardır. Bu ise

$$(a_1, \dots, a_i + 1, \dots, a_n) \in M \cap \mathbb{N}^n$$

anlamına gelir. Birinci hipotezimizden dolayı  $i \in \{i_1, \dots, i_r\}$  dir.  $\square$

Bu iki sonuç ile  $\mathbb{N}^n / \sim_M$  formundaki bir monoidin birimleri grubunu ve bunun komplementini hesaplayabiliyoruz.  $V$ ,  $\mathbb{Q}^n$  nin  $M$  tarafından gerilen alt uzayını göstermek üzere  $x$ , Algoritma MCP nin  $V$  ye uygulanması sonucu elde edilen eleman olsun.

- Eğer  $x = (0, \dots, 0)$  ise  $U(\mathbb{N}^n / \sim_M) = \{0\}$  ve sonuç olarak  $\mathbb{N}^n / \sim_M$  indirgenmiştir.
- Eğer  $\{i_1, \dots, i_r\} = \{i \mid x_i \neq 0\}$  ise  $U(\mathbb{N}^n / \sim_M) = \langle [e_{i_1}], \dots, [e_{i_r}] \rangle$  ve  $U(\mathbb{N}^n / \sim_M)$  nin komplementi  $\langle \{[e_i] \mid i \notin \{i_1, \dots, i_r\}\} \rangle$  dir.

**Örnek 4.14**  $M = \mathbf{G}(\{(1, 1, 1, -1), (1, 2, 2, -1)\})$  verilsin.  $V$  nin bir bazı

$$\{(1, 1, 1, -1), (1, 2, 2, -1)\}$$

dir. Algoritma MCP nin  $V$  ye uygulanması sonucundaki çıktı  $(0, 1, 1, 0)$  dır. Buradan  $U(\mathbb{N}^4 / \sim_M) = \langle [e_2], [e_3] \rangle$  ve bunun komplementi de  $\langle [e_1], [e_4] \rangle$  dir.  $\diamond$

**Önerme 4.15**  $S$  sonlu doğuraylı bir monoid ve  $C$  de  $U(S)$  nin komplementi olsun.  $\tau$ ,  $U(S) \times C$  üzerinde

$$(x, y) \tau (x', y') \iff x + y = x' + y'$$

şeklinde tanımlanan bir kongruans olsun. O zaman  $S \simeq (U(S) \times C) / \tau$  dir.



**İspat:**

$$\varphi : U(S) \times C \longrightarrow S$$

$$\varphi(x, y) = x + y$$

tanımlanır ve  $\tau = \ker(\varphi)$  alınırsa ispat biter. ■

#### 4.2.4 Rasyonel Katsayılı Bir Homojen Lineer Denklem Sisteminin, Tüm Koordinatları Negatif Olmayan Tamsayı Olacak Şekilde Bir Aşık Olmayan Çözüme Sahip Olup Olmadığının Belirlenmesi

$$a_{11}x_1 + \cdots + a_{1n}x_n = 0$$

$$\vdots$$

$$a_{r1}x_1 + \cdots + a_{rn}x_n = 0$$

rasyonel katsayılı homojen lineer denklem sistemi verilsin.  $(x_1, \dots, x_n) \in \mathbb{N}^n \setminus \{0\}$  şeklinde bir çözüm olup olmadığını bilmek istiyoruz. Bu ise,  $\mathbb{Q}^n$  nin bu denklemler tarafından tanımlanan alt uzayının sıfırdan farklı bir negatif olmayan elemanının olup olmadığını bilmeye eşdeğerdir. Bu yüzden lineer cebir metodlarını kullanarak  $V$  için bir  $B$  bazını bulmalı ve satırları  $B$  nin elemanı olan matrise Algoritma MCP yi uygulamalıyız. Algoritmanın çıktısının paydalarını elimine edince ortaya çıkan eleman aradığımız elemandır.

**Örnek 4.16** Bir negatif olmayan tamsayı çözüme sahip olan

$$x_1 + x_4 = 0$$

$$x_2 - x_3 = 0$$

denklem sistemini göz önüne alalım. Bu denklemler tarafından tanımlanan  $V$  altuzayı

$$V = \mathbf{L}_{\mathbb{Q}}(\{(1, 1, 1, -1), (1, 2, 2, -1)\})$$

dir.  $V$  ye Algoritma MCP uygulanması sonucu elde edilen çıktının  $(0, 1, 1, 0)$  olduğunu biliyoruz ve dolayısıyla bu, verilen denklem sistemi için tüm koordinatları sıfır yada sıfırdan büyük bir aşık olmayan çözümdür. ◇

#### 4.2.5 $\mathbb{N}^n$ nin İki Sonlu Doğuraylı Alt Monoidinin Kesişiminin Aşık Olup Olmadığının Belirlenmesi, Eğer Aşık Değilse Kesişimindeki Bir Elemanın Bulunması

$S_1$  ve  $S_2$ ,  $\mathbb{N}^n$  nin, sırasıyla  $\{a_1, \dots, a_r\}$  ve  $\{b_1, \dots, b_s\}$  tarafından doğurulan iki alt monoidi olsun.  $S_1$  ve  $S_2$  nin aşık olmayan bir ortak elemana sahip olup olmadığını bilmek istiyoruz. Eğer

$$\begin{aligned} a_i &= (a_{i1}, \dots, a_{in}) & 1 \leq i \leq r \\ b_j &= (b_{j1}, \dots, b_{jn}) & 1 \leq j \leq s \end{aligned}$$

ise bu problem

$$\begin{aligned} a_{11}x_1 + \dots + a_{r1}x_r - b_{11}x_{r+1} - \dots - b_{s1}x_{r+s} &= 0 \\ &\vdots \\ a_{1n}x_1 + \dots + a_{rn}x_r - b_{1n}x_{r+1} - \dots - b_{sn}x_{r+s} &= 0 \end{aligned}$$

denklem sisteminin en az iki koordinatı (bunlardan birisi 1 ile  $r$ -inci koordinat arasında, diğeri 1 ile  $s$ -inci koordinat arasında olmak üzere) sıfırdan farklı olan bir negatif olmayan tamsayı çözümünün olup olmadığı problemine dönüşür.

Böylece,  $S_1 \cap S_2 \neq \{0\}$  olup olmadığını, eğer böyleyse kesişimdeki bir elemanı bulmak için Algoritma MCP yi uygulayabiliriz.

## 5. ALGORİTMALAR VE ARİTMETİK İŞLEMLER İÇİN NESNEL YAPI

Bu bölümde tezde verilen algoritmalar için bilgisayar programı yazmak amacıyla kullanılacak nesneler (object) için bir takım öneriler vereceğiz. Bu tür programlar, çoğu kez *C* veya *Pascal* lisanları kullanılarak yazılır. Burada yapacağımız öneri MS Visual Basic için olacaktır.

Önce aritmetikle işe başlayalım. Bu konuda literatürde pek çok program vardır. Aşağıda tanıtacağımız `clsTamSayi` aritmetik için işlevselliği yüksek bir nesnedir. Bu nesne için kodlar yazılmıştır. Burada kullanılan algoritma yeni olmamakla beraber, programın kendisi, erişilebilir açık kod olması bakımından bir katkı sağlayacaktır.

Bu nesnede büyük tam sayılarla ilgili aritmetik işlemler yapılmaktadır. Bu tezde açıklanan algoritmalarda hesaplar yapılırken ortaya çıkan tam sayılar, bir çok bilgisayarın tam sayıları temsil etmekte kullandığı 16 bit veya 32 bitlik normal sayı sınırını kolaylıkla aşabilmektedir. Bu olgu, gündeme büyük sayılarla aritmetik işlemler yapma gereğini getirmektedir. Büyük sayılarla ilgili pek çok kaynak vardır. Biz Gary Darby tarafından yazılan ve bölme algoritması için Hansen'in (Hansen, 1994) verdiği fikri kullanan `TInteger` bileşenindeki fikirleri kullanacağız. Gary Darby'nin programı Delphi kullanılarak yazılmıştır. Bu fikirleri kullanarak bizim yazdığımız programda pek çok iyileştirme ve farklılık vardır. Belki de en temel farklılık “çıkarma” işleminde olacaktır. Bunu kısaca açıklayalım.

Bilgisayar dünyasında *ikinin tümleyeni* (two's complement) olarak bilinen işlem bir sayının toplamsal tersinin yazılmasında kullanılır. Aslında buna toplamsal ters demek yanlış olur. Durumu daha kolay açıklayabilmek için tam sayıların 8 bit olarak temsil edildiğini varsayalım. Bu bitleri sağdan sola doğru 0,...,7 olarak adlandıralım. 7—inci bit işaret biti olup, 1 ise sayı negatif, 0 ise sayı pozitif veya 0 dır. İkinin tümleyenini alabilmek için bir sayının tüm bitleri teryüz edilir ve elde edilen sayıya 1 eklenir. O halde 00000011 sayısının ikinin tümleyenini bulmak için önce 11111100 ve daha sonra 11111101 elde edilir. Bu iki sayı iki modülüne göre toplanınca

$$\begin{array}{r}
00000011 \\
11111101 \\
+ \text{-----} \\
100000000
\end{array}$$

elde edilir. Fakat bilgisayarımız 8 bitlik olduğundan en başta duran 1 kaybedilecektir. Dolayısıyla sonuç 00000000 olur. O halde 11111101 sayısı 00000011 sayısının tam sayıların temsil edilebildiği ölçüde toplamsal tersidir.

Aslında bu fikir sadece 2 tabanı için geçerli değildir.  $1 < b$  herhangi bir tam sayı ve  $n = (c_k, c_{k-1}, \dots, c_0)_b$  sayısı  $n$  pozitif tam sayısının  $b$  tabanına göre temsili olsun. Her  $0 \leq i \leq k$  için  $0 \leq c_i \leq b-1$  olduğundan  $0 \leq b-1-c_i \leq b-1$  dir.

$$m = 1 + (b-1-c_k, b-1-c_{k-1}, \dots, b-1-c_0)_b$$

sayını düşünelim. Bu durumda

$$\begin{aligned}
n + m &= 1 + \sum_{i=0}^k (c_i + b-1-c_i) b^i \\
&= 1 + \sum_{i=0}^k (b-1) b^i \\
&= \sum_{i=0}^{k+1} b^i - \sum_{i=0}^k b^i \\
&= b^{k+1} \\
&= \left( 1, \underbrace{0, 0, \dots, 0}_{k \text{ tane}} \right)_b
\end{aligned}$$

elde edilir. O halde tam sayıların sadece  $k$  rakam ile ifade edilebildiği bir bilgisayarda  $m$  sayısı  $n$  nin toplamsal tersidir. Bundan faydalanarak

$$x = (x_k, x_{k-1}, \dots, x_0)_b \text{ ve } y = (y_s, y_{s-1}, \dots, y_0)_b$$

iki tam sayı ve  $s \leq k$  olsun.  $x - y$  sayısının  $b$  tabanına göre bir temsili yazacak bir algoritmayı yukarıdaki fıkirden faydalanarak yazalım. Burada aslında çıkarma yapmak

yerine toplama yapmak istiyoruz. Toplama işlemi için alışlagelmiş toplama algoritmasına sadece yukarıdaki fikir eklenecektir. Böylece çıkarma işleminin çok daha kolay programlanabilir olduğu görülecektir.

**Algoritma 5.1**  $x \geq y$  olduğuna göre aşağıdaki algoritma  $x - y$  sayısını hesaplayıp sonucu  $x$  sayısına atayan bir algoritmadır.

```

i = 0
elde = 1
do while i <= k
    if i ≤ s then z = x(i) + b − 1 − y(i) + elde else z = x(i) + b − 1 + elde
    if z >= b then elde = 1 else elde = 0
    x(i) = z mod b
    i = i + 1
loop

```

◇

Program taban olarak  $b = base = 100$  kullanmaktadır. Kullanıcı sayıları 10 tabanına göre girmekte ve bu sayılar program tarafından 100 tabanına çevrilmektedir. Kullanıcı bir çıktı istediğinde, istenen sonuçlar 10 tabanına çevrilerek verilmektedir.

Şimdi sınıfları tanıyalım.

**clsTamSayi sınıfı :** Bu sınıfın 4 tane temel unsuru **Isaret**, **tRakamlar**, **tRakamSay**, **tMax** dır. Isaret public bir özelliktir ve bu sınıf ile temsil edilen sayının işaretini saklamak için kullanılmaktadır. 0 sayısının işareti 1 olarak alınmaktadır. tRakamlar bu sınıfın default özelliğidir ve boyutu önceden verilmeyen bir byte dizisidir. Bu dizi verilen tamsayının 100 tabanına göre temsilini tutmaktadır.  $x_k \neq 0$  olmak üzere verilen sayı  $x = (x_k, x_{k-1}, \dots, x_0)_b$  ise  $tRakamSay = k + 1$  dir. Eğer  $x = 0$  ise  $tRakamSay = 1$  olur. Isaret ise aşıkâr anlamdadır. Yeni bir sınıf elemanı, bir başka deyişle clsTamSayi tipinde bir  $x$  tamsayısı oluşturulunca bu dizi 16 eleman içerecek şekilde boyutlandırılmaktadır. Eğer hesaplar sırasında veya ilk atama aşamasında  $x$  sayısı için 16 dan daha çok eleman gerekiyorsa o zaman tRakamlar dizisi 16 nın bu gerekli sayıyı ilk geçen katı kadar eleman içerecek şekilde boyutlandırılmaktadır. tMax bu dizinin alabileceği bu maksimum eleman sayısını göstermektedir.

**clsTamSayi sınıfının metodları :**

1. Public Property Get Item(ByVal iIndex As Integer) As Byte
2. Public Property Get RakamSay() As Integer
3. Public Sub SetRakamSay(ByVal YeniRakamSay As Integer)
4. Public Sub Trasla() 'bastaki sifirlari sil
5. Public Sub Sifirla()
6. Public Sub PutItem(ByVal iIndex As Integer, ByVal lData As Byte)
7. Public Sub YeniRakamEkle(ByVal lData As Byte)
8. Public Function SayiStr() As String
9. Public Sub MetinSayiAta(s As String)
10. Public Sub SayiAta(i2 As clsTamSayi)
11. Public Sub KucukSayiAta(i2 As Integer)
12. Public Function MutlakKarsilastir(i2 As clsTamSayi) As Integer
13. Public Sub MutlakCikar(i2 As clsTamSayi)
14. Public Sub MutlakTopla(i2 As clsTamSayi)
15. Public Sub Topla(i2 As clsTamSayi)
16. Public Sub Cikar(i2 As clsTamSayi)
17. Public Sub RakamlaCarp(ByVal m As Integer)
18. Public Sub RakamaBol(ByVal m As Integer)
19. Public Function RakamlaBolumdenKalan(ByVal m As Integer) As Integer
20. Public Sub SolaKaydır(miktar As Integer)
21. Public Sub Carp(i2 As clsTamSayi)

22. Public Sub Modulo(i2 As clsTamSayi)
23. Public Function SifiraEsit() As Boolean
24. Public Sub EBOB(ByVal u As clsTamSayi)
25. Public Function trial(r As clsTamSayi, d As clsTamSayi, k As Integer, m As Integer)  
As Integer
26. Public Function smaller(r As clsTamSayi, dq As clsTamSayi, k As Integer, m As Integer) As Boolean
27. Public Sub difference(r As clsTamSayi, dq As clsTamSayi, k As Integer, m As Integer)
28. Public Sub longdivide(y As clsTamSayi, q As clsTamSayi, r As clsTamSayi)
29. Public Sub Bolme(y As clsTamSayi, q As clsTamSayi, r As clsTamSayi)

$\mathbb{Z}^n$  nin alt kümeleri üzerinde yapılacak işlemler için doğurayların satır ve sütun işlemlerine gerek olacaktır. Bunun için aşağıda yazılı sınıfları kullanmak uygun olacaktır. Bu sınıfların metodları ve özelliklerinin ne anlama geldiği çok açıktır.

#### **clsGenarator sınıfının metodları :**

1. Public Property Let Boyut(ByVal vData As Integer)
2. Public Property Get Boyut() As Integer
3. Public Property Get Koordinat(ByVal iIndex As Integer) As clsTamSayi
4. Public Sub SetKoordinat(ByVal iIndex As Integer, ByVal lData As clsTamSayi)

#### **TIslem enum tipi**

```
Public Enum TIslem
    DegisTokus = 0
    EksilleCarp = 1
    LineerEkle = 2
End Enum
```

**clsIslem sınıfının metodları :**

1. Public Property Let Kat(ByVal vData As clsTamSayi)
2. Public Property Get Kat() As clsTamSayi
3. Public Property Let KullanilanIndex(ByVal vData As Integer)
4. Public Property Get KullanilanIndex() As Integer
5. Public Property Let islmDegisenIndex(ByVal vData As Integer)
6. Public Property Get islmDegisenIndex() As Integer
7. Public Property Let Islm(ByVal vData As TIslem)
8. Public Property Get Islm() As TIslem
9. Public Property Get Boyut() As Integer
10. Public Property Get Koordinat(ByVal iIndex As Integer) As clsTamSayi
11. Public Sub SetKoordinat(ByVal iIndex As Integer, ByVal lData As clsTamSayi)

**clsGenaratorSet sınıfının metodları :**

1. Public Property Let Boyut(ByVal vData As Integer)
2. Public Property Get Boyut() As Integer
3. Public Property Get GenMatris(ByVal iIndex As Integer, ByVal jIndex As Integer)  
As clsTamSayi
4. Public Sub SetGenarator(ByVal iIndex As Integer, ByVal lData As clsGenarator)
5. Public Sub YeniGeneratorEkle(ByVal lData As clsGenarator)
6. Public Sub MetinGeneratorEkle(s As String)
7. Public Sub YeniSatirIslemEkle(ByVal lData As clsIslem)
8. Public Sub YeniSutunIslemEkle(ByVal lData As clsIslem)



9. Public Sub SatirIslemUygula(ByVal Islm As TIslem, K As Integer, r As Integer, X As clsTamSayi)
10. Public Sub SutunIslemUygula(ByVal Islm As TIslem, K As Integer, r As Integer, X As clsTamSayi)
11. Public Sub GeneratorleriDosyayaYaz(ByVal Path As String)
12. Public Sub GeneratorleriDosyadanOku(ByVal Path As String)
13. Public Property Get Kat() As clsTamSayi
14. Public Property Let KullanilanIndex(ByVal vData As Integer)
15. Public Property Get KullanilanIndex() As Integer
16. Public Property Let islmDegisenIndex(ByVal vData As Integer)
17. Public Property Get islmDegisenIndex() As Integer
18. Public Property Let Islm(ByVal vData As TIslem)
19. Public Property Get Islm() As TIslem
20. Public Property Get Boyut() As Integer
21. Public Property Get Koordinat(ByVal iIndex As Integer) As clsTamSayi
22. Public Sub SetKoordinat(ByVal iIndex As Integer, ByVal lData As clsTamSayi)

## KAYNAKLAR

- GRILLET, P. A., 1995. Semigroups. An introduction to the structure theory, Dekker, New York.
- HANSEN, P. B., 1994. Multiple-length Division Revisited: a Tour of the Minefield, Software-Practice and Experience, 24(6), 579-601.
- HERZOG, J., 1970. Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math., 3, 175-193.
- HOWIE, J.M., 1995. Fundamentals of Semigroup Theory, Oxford:Clarendon Press.
- KNUTH, D.E., 1997a. The Art of Computer Programming (Vol 1, Fundamental algorithms), 3rd ed., Addison Wesley
- , 1997b. The Art of Computer Programming (Vol 2, Seminumerical algorithms), 3rd ed., Addison Wesley
- REDEI, L., 1965. The theory of finitely generated commutative semigroups, Pergamon.
- ROSALES, J. C., 1995. On finitely generated submonoids of  $N^k$ , Semigroup Forum, 50, 251-262.
- , 1996a. On numerical semigroups, Semigroup Forum, 52, 307-318.
- , 1996b. On symmetric numerical semigroups, J. Algebra, 182, 422-434.
- ROSALES, J. C., GARCIA-SANCHEZ, P. A., 1999. Finitely generated commutative monoids, Nova Science Publ., New York.
- ROSALES, J. C., GARCIA-SANCHEZ, P. A., URBANO-BLANCO, J. M., 1999. On presentations of commutative monoids, Internat. J. Algebra Comput., 5, 539-553.
- ROSALES, J. C., URBANO-BLANCO, J. M., 1996. A deterministic algorithm to decide if a finitely presented abelian monoid is cancellative, Comm. Algebra, 24, 4217-4224.

## ÖZGEÇMİŞ

1981 yılında Adana’da doğdum. İlk, orta ve lise eğitimimi Adana’da tamamladıktan sonra 1998 yılında Ç.Ü. Matematik Bölümünde lisans eğitimime başladım. 2002 yılında mezun olduktan sonra aynı yılın Eylül ayında Ç.Ü. Matematik Bölümünde yüksek lisans eğitimime başladım. Yine aynı yılın Aralık ayında Ç.Ü. Matematik Bölümünde araştırma görevlisi olarak çalışmaya başladım. Halen aynı görevde bulunmaktayım.