University of
Al-Tahddi

Faculty of
Science

Department of Mathematics

Some Applications of Smith Normal Form

By

Muftah M. A. Elhassi
(032313)

Supervised by

Dr. Shaban A. Traina

Spring 2008

University of
Al-Tahddi

Faculty of
Science

Department of Mathematics

Some Application of Smith Normal Form

A dissertation submitted to the department of mathematics in partial fulfillment of the requirements for the degree of Master of Science in mathematics

By

Muftah M. A. Elhassi

Supervised by

Dr. Shaban A. Traina

2008

التاريخ: ....
الموافق: ....
الرقم الإشاري: ....

Faculty of Science

Department of Mathematics

Title of Thesis

Some Applications of Smith Normal Form

By

Muftah M. A. Elhassi

Approved by:

Dr. Shaban A. Traina ....
(Supervisor)

Dr. Ali A. Daw ....
(External examiner)

Dr. Ameer Abdul M. Jaseem ....
(Internal examiner)

Countersigned by:

Dr. Ahmed Farag Mhgoub

(Dean of faculty of science)

بِسْمِ اللهِ الرَّحْمَنِ الرَّحِيمِ

﴿قَالُوا سُبْحَانَكَ لا عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ﴾

صـــدق الله العظيم

سورة البقرة الآية (32)

Dedication

To my lovely Family…

To my faithful friends…

To all of those have given me a hand

In this thesis

Muftah Elhassi

Acknowledgment

Before every thing, I shall thank "Allah" s.w.t, for supporting, helping and guidance to finish this work.

I would like to express my gratitude and appreciation for those who helped me to make this thesis comes to live!

The guidance, encouragement and inspiration of Dr. Shaban A. Traina, my supervisor, are kindly acknowledged and deeply appreciated special thanks to the department of mathematics.

Last but not least, my family and friends who stand with me during this hard way to obtain this degree, especially my best friend Mr. Eng. Ahmed Alhwity who had a significant contribution.

Thank you,

Introduction

Smith normal form was introduced in 1869 by its founder Mr. Henry John Stephen Smith, born in 2 Nov. 1826 in Dublin, Ireland. Mr. Smith had important contributions in number theory where he worked on elementary divisors. He provided that any integer can be expressed as the sum of k squares for any fixed k. From 1859 to 1865 he prepared a report in five parts on the Theory of Numbers. He analyzed the work of other mathematicians but added much of his own. After that he introduced the smith normal form for matrices. In 1975 he gave examples of discontinuous sets which are similar to the Sierpinsks gasket. His paper was published in the proceeding of the London Mathematical Society for 1875 contains a description of the Cantor set eight years before Cantor [7].

In this thesis we gather all important information and material about smith normal form; as it's known that smith normal form is used in different fields and has a lot of applications (e.g. solving systems of Diophantine equations over the domain of entries, determining the canonical decomposition of finitely generated abelian groups, determining the similarity of two matrices and computing additional normal forms such as Frobenius and Jordan normal form).

Even though, we faced a huge problem in getting information about smith normal form due to the leakage in sources and references, however, we could succeed to find some references and papers which provided our thesis with a number of significant information.

This thesis has been organized into three chapters as follows:

Chapter 1: introduces some definitions and basic theories which are considered as our research bases.

Chapter 2: studies the smith normal form and its properties. It shows that smith normal form is unique.

Chapter 3: has two main parts, first part, demonstrates one of the applications of smith normal form, i.e. "every finitely generated abelian group can be represented by relation matrix".
Second part, list a code of our developed software which can construct the smith normal form using the computer in a smart and fast manner.

Contents

Chapter One

Preliminaries

1.1 Linear Algebra:

Definition 1.1.1 [5]

A vector space V over the field F and $x_1,x_2,\dots,x_n$ any finite element in V, or ($x_1,x_2,\dots,x_n \in V$) the finite sum of the form $c_1x_1+c_2x_2+\dots+c_nx_n = \sum_1^n c_ix_i$ is said to be ***linear Combination*** of the vectors $x_1,x_2,\dots,x_n$, where $c_1,c_2,\dots,c_n \in F$.

Remark:

A linear combination is called ***trivial*** if all its coefficients $c_i=0$ and nontrivial if at least one coefficient is different from zero.

Example 1.1.2:

In F^n, any vector $x=(a_1,a_2,\dots,a_n)$ can be written as a linear combination such that :

$$x = a_1e_1+\dots+a_ne_n. \text{Where } e_1=(1,0,\dots,0),\dots,e_n=(0,\dots,1).$$

Definition 1.1.3 [16]

Let $S=\{x_1,x_2,\dots,x_n\}$ be a set of vectors in a vector space V, the set S ***spans*** V or V is ***spanned*** by S if every vector in V is a linear combination of the vectors in S.

Example 1.1.4:

In example 1.1.2 F^n is spanned by the vectors $e_1,e_2,\dots,e_n$.

Definition1.1.5 [4]

A finite set $\{x_1,x_2,\dots,x_n\}$ of a vector space V over a field F is said to be ***linearly dependent*** if there exist scalars $c_1,c_2,\dots,c_n \in F$, not all are zero , such that $c_1x_1+c_2x_2+\dots+c_nx_n=0$.

Definition1.1.6 [4]

A finite set $\{x_1, x_2, \ldots, x_n\}$ of a vector space V over a field F is said to be ***linearly independent*** if the trivial solution is the only solution of $c_1x_1+c_2\ x_2+\ldots+c_n\ x_n=0$. Where the scalars $c_1, c_2, \ldots, c_n \in F$,

Example 1.1.7:

The vectors $e_1, e_2, \ldots, e_n$ of F^n are linearly independent since $c_1e_1+c_2e_2+\ldots+c_ne_n = (c_1, 0, \ldots, 0)+(0, c_2, \ldots, 0)+\ldots+(0, \ldots, c_n) = (c_1, c_2, \ldots, c_n) = (0, \ldots, 0)$.
Implies that $c_1=c_2=\ldots=c_n=0$

Definition1.1.8 [14]

A set of vectors $S=\{x_1, x_2, \ldots, x_n\}$ in a vector space V is called a ***Basis*** for V if S spans V and S is linear independent.

Example 1.1.9:

In example 1.1.2 the vectors $e_1, e_2, \ldots, e_n$ of F^n is a basis (or is called ***canonical basis or natural basis***) of F^n.

Theorem 1.1.10:

Every nonzero vector space V possesses a basis.

Definition 1.1.11 [5]

The rank of matrix is the maximal number of rows or columns of linearly independent in a given matrix.

1.2 Group Theory

Definition 1.2.1 [9]

A Group is a non empty set G with a binary operation $*$ on G such that: for all $a, b, c \in G$:

i. G is associative, i.e $(a*b)*c = a*(b*c)$.
ii. G has identity element: there is $e \in G$ s.t $a*e=a=e*a$.
iii. G has the inverse element: for all $a \in G$, there is $b \in G$ s.t $a*b=e=b*a$. where b is the inverse element of a.

Example 1.2.2:

The set of integers Z, and the set of rational number Q, also the set of real number R are groups with addition.

Definition 1.2.2:

A group G is called ***abelian (commutative)*** if $a*b=b*a$, for all $a, b \in G$.

Definition 1.2.3 [9]

A group G is said to be *cyclic* if there is a in G such that for all x *in* G we have $x=a^n$ for some n *in* Z, a is called the generator of G denote by $G=\langle a \rangle$.

Example 1.2.4:

The set of integers Z with addition is a cyclic group with generators *1* and *-1*, i.e. $Z=\langle 1 \rangle, \langle -1 \rangle$.

Example 1.2.5:

The set of residue classes modulo 4, $Z_4=\{[0],[1],[2],[3]\}$ with addition is cyclic group with generators [1] and [3] i.e $Z_4=\langle [1] \rangle$, $Z_4=\langle [3] \rangle$.

1.3 Ring Theory

Definition 1.3.1 [9]

A nonempty set R is said to be ***a Ring*** if there are two binary operations addition (+) and multiplication (.) such that:

i) $a+b=b+a$ for all $a, b \in R$.

ii) $(a+b)+c=a+(b+c)$ for all $a, b, c \in R$.

iii) There exists an element 0 such that $a+0=a=0+a$ for every $a \in R$. (0 is additive identity of R).

iv) given $a \in R$, there exists, $b \in R$ such that $a+b=0=b+a$ ($b=-a$, the additive inverse of a).

v) $a.(b.c)=(a.b).c$ for all $a,b,c \in R$.

vi) $a.(b+c)=a.b+a.c$ and $(b+c).a=b.a+c.a$; for all $a,b,c \in R$.

Remarks:

1) A ring R is called ***a ring with unity***, if there is an element $e \in R$ such that $a.e=e.a=a$ for every $a \in R$.

2) A ring R is called ***a commutative ring***, if $a.b=b.a$ for all $a,b \in R$.

Example1.3.2:

The set of integers Z *is* a commutative ring with unity, under (+) and (.).

Definition 1.3.4 [9]

Let R be a ring and S subset of R. S is called ***a subring*** of R if S is a ring with respect to addition and multiplication of R.

Example 1.3.5:

nZ is a subring of Z.

Definition 1.3.6 [8]

A commutative ring R with unity is ***an integral domain** if $a \cdot b = 0$ in R implies* that $a = 0$ or $b = 0$.

Example 1.3.7:

The ring of rational numbers Q is an integral domain.

Definition 1.3.8 [8]

A ring with unity is said to be ***a division ring*** if any nonzero element has a multiplicative inverse.

Example 1.3.9:

The ring of rational numbers Q is a division ring.

Definition 1.3.10 [15]

A ring R is said to be ***a field*** if R is a commutative division ring.

Example 1.3.11:

The ring of rational numbers Q, and the ring of real numbers R are fields.

Definition 1.3.12:

Let R be an integral domain with zero *and* unity e. Let $a, b \in R$ with $a \neq 0$, we say that ***a divides b** (or a* is ***a factor*** of *b)* if $b = ca$ for some $c \in R$, this is denoted by a/b iff $b = ca$ for some $c \in R$.

Definition 1.3.13 [8]

If u in R and $u \neq 0$, then u is called ***a unit*** in R, *if there* is v in R such that $u \, . \, v = e$.

Example 1.3.14

$\{-1, 1\}$ is the set of all units in Z.

1.4 Ideals and Quotient Ring

Definition 1.4.1 [8]

Let R be a ring and I be a subring of R. I is called:

i) A ***left ideal***, if $r\,a \in I$ for any $r \in R$, and any $a \in I$.

ii) A ***right ideal***, if $a\,r \in I$ for any $r \in R$ and any $a \in I$, and

iii) An ***ideal (two – sided ideal)*** if $r\,a \in I$, $a\,r \in I$ for any $r \in R$ and any $a \in I$.

Example 1.4.2:

1. $5Z$ is an ideal of Z.
2. $\{[0],[2],[4]\}$ is an ideal of Z_6.
3. $\{0\}$, R are (trivial) ideals of a ring R.

Definition 1.4.3 [8]

Let I be an ideal of a ring R. ***The Quotient ring*** **of** R **by** I defined by $R/I = \{r+I : r \in R\}$.

Addition and multiplication can be defined on R / I as follows:

$$(r_1+I) + (r_2+I) = (r_1+r_2) + I,$$

$$(r_1+I) \, . \, (r_2+I) = r_1 r_2 + I.$$

Theorem 1.4.4:

Let I be an ideal of a ring R. Then:

i) R/I is a ring called the quotient ring.

ii) If R is a commutative, then is so R/I.

iii) If R has unity e, then R/I has unity $e+I$.

Lemma 1.4.5 [15]

Let R be a ring with identity e. If I is an ideal of R such that $e \in I$, then $I=R$.

Definition 1.4.6 [5]

An ideal generated by a single element is called a ***principal ideal.***

Definition 1.4.7 [5]

A ring R which all ideals are principal is called ***a principal ideal ring.***

Examples 1.4.8:

The ring of integers is a principal ideal ring.

Definition 1.4.9 [8]

An integral domain D is called ***a principal ideal domain*** denoted by (P.I.D) if every ideal of D is a principal ideal.

Definition 1.4.10 [5]

An Euclidean evaluation ν on an Integral domain D is a function ν : $D-\{0\}\rightarrow\{0,1,2,...\}$ such that:

i) $\nu(a)\leq\nu(ab)$ for any a, $b\in D-\{0\}$.

ii) for any a, $b\in D$ with $b\neq 0$, there are q, $r\in$ D such that $a=bq+r$ where $r=0$ or $\nu(r)\leq\nu(b)$. D with the Euclidean evaluation is called **Euclidean Domain**, denoted by (ED).

Theorem 1.4.11 [5]

Every Euclidean Domain is a principal ideal domain.

Examples 1.4.12:

The set of integers Z is an Euclidean Domain.

Theorem 1.4.13[6]

Let R be a Euclidean Domain. Then every ideal in R is principal.

Definition 1.4.14 [10]

Let R be a commutative ring .Let $a,b\in R$. The element c of R is a **greatest common divisor** of a and b iff c/a, c/b, and if d $\in R$ is any other element of R such that d/a and d/b, then d/c.

Theorem 1.4.15 [10]

Let R be Euclidean Domain and let a and b be nonzero elements of R. Then a and b have at least one greatest common divisor. Moreover if c and d are both greatest common divisors of a and b then $d=cu$ for some unit $u\in R$.

Finally if c is any greatest common divisor of a and b then there are elements $x,y \in R$ so that $c = ax+by$.

Theorem 1.4.16 [10]

Let R be commutative ring and $a_1,a_2,\ldots, a_k \in$ R. The element c of R is a greatest common divisor of $a_1,a_2,\ldots,a_k$ iff c divides all of the elements $a_1,a_2,\ldots,a_k$ and if d is any other element of R that divides all of $a_1,a_2,\ldots,a_k$, then d/c.

Theorem 1.4.17 [10]

Let R be a Euclidean Domain *and* let $a_1,a_2,\ldots a_k$ be nonzero elements of R . Then $a_1,a_2,\ldots,a_k$ have at least one greatest common divisor . Moreover if c and d are both greatest common divisors of $a_1,a_2,\ldots,a_k$,then $d=cu$ for some unit $u \in R$. Finally if c is any greatest common divisor of $a_1,a_2,\ldots,a_k$ then there are elements $x_1,x_2,\ldots,x_k \in R$ so that

$c=a_1x_1+ a_2x_2+\ldots+ a_kx_k$

Moreover the greatest common divisor c is the generator of the ideal $\langle a_1,a_2,\ldots,a_k\rangle$ of R.

Definition 1.4.18 [10]

Let $A \in M_{m\times n}(R)$. Then define $I_k(A)$:= ideal of R generated by $k \times k$ sub-determinants of A , for $1 \le k \le min\{m,n\}$.

Examples 1.4.19:

Let $R = \mathbb{Z}$ be the ring of integers and let $A=\begin{bmatrix} 4 & 6 \\ 8 & 10 \\ 14 & 12 \end{bmatrix}$.

The principle ideal generated by the greatest common divisor of the elements.

The 1×1 sub-determinants of A are just its elements.

Thus $I_1(A)=\langle 4,6,8,10,12,14\rangle=\langle 2\rangle$,

The 2×2 sub-determinants of A are just its elements. Thus

$$I_2(A)=\left\langle \det\begin{bmatrix}4 & 6\\ 8 & 10\end{bmatrix}, \det\begin{bmatrix}4 & 6\\ 14 & 12\end{bmatrix}, \det\begin{bmatrix}8 & 10\\ 14 & 12\end{bmatrix} \right\rangle = \langle -8,-36,-44 \rangle = \langle 4\rangle.$$

Lemma 1.4.20 [10]

Let $A\in M_{m\times n}(R)$ and $P\in M_{m\times n}(R)$. Then the inclusion $I_k(AP)\subseteq I_k(A)$ for all k with $1\leq k\leq min\{m,n\}$.

Theorem 1.4.21 [10]

Let $A\in M_{m\times n}(R)$ and $Q\in M_{m\times n}(R)$, and any $P\in M_{m\times n}(R)$, then $I_k(QAP)\subseteq I_k(A)$ holds for $1\leq k\leq min\{m,n\}$.

If also P and Q are invertible, then $I_k(QAP) = I_k(A)$.

1.5 Ring Homomorphisms

Definition 1.5.1 [9]

Let R and R' be two rings. A mapping Φ from R *to* R' is said to be ***a ring homomorphism*** (or a homomorphism) if for all elements a, b of R we have $\Phi(a+b)=\Phi(a)+\Phi(b)$, and

$\Phi(ab)=\Phi(a)\,\Phi(b)$.

Lemma 1.5.2 [15]

If Φ is a homomorphism of R into R', then

1) $\Phi(0) = 0_{R'}$.
2) $\Phi(-a) = -\Phi(a)$, $a \in R$.

Remark1.5.3:

We define Φ to be an injective (surjective) if Φ is an one to one (onto). A bijective is an injective and surjective.

Definition 1.5.4:

A homomorphism Φ from R to R' is said to be:

1) An ***epimorphism*** if it is surjective.
2) A ***monomorphism*** if it is injective.
3) An ***isomorphism*** if it is bijective.

Definition 1.5.5 [8]

Let Φ be a homomorphism from a ring R to a ring R', then ***the kernel*** of Φ is the set of all elements $r \in R$ such that $\Phi(r) = 0_{R'}$. This set will be denoted by $ker\Phi$. *i.e.* $ker\Phi = \{r \in R : \Phi(r) = 0_{R'}\} = \Phi^{-1}(0_{R'})$.

Example 1.5.6:

If R and R' are two rings, then the mapping $\Phi : R \rightarrow R'$ defined by
$\Phi(r) = 0$ for all $r \in R$
is a homomorphism, and $ker\Phi = R$. It is called ***the zero homomorphism.***

Definition1.5.7 [9]

If R is a ring and I is an ideal of R, then the mapping $\Phi : R \rightarrow R/I$ defined by $\Phi(r) = r+I$ for all $r \in R$, is a homomorphism, and $ker\Phi = I$. It is called ***the natural (or canonical) homomorphism***.

Lemma 1.5.8 [5]

The homomorphism $\Phi : R \rightarrow R'$ is a monomorphism if and only if $ker\Phi = \{0\}$.

Definition 1.5.9 [5]

Let R and R' be two rings. They said to be ***isomorphic*** if there is an isomorphism of one onto the other. It is denoted by $R \cong R'$.

Theorem 1.5.10 (First Homomorphism Theorem)[9]

Let R and R' be two rings, and let Φ be a ***homomorphism*** from R onto R' with $ker\Phi = K$. Then R' *isomorphic* to R/K.

Theorem 1.5.11 (Correspondence Theorem)[9]

Let R and R' be two rings, and let Φ be a homomorphism from R onto R' with $ker\Phi = K$. If J is an ideal of R', *let* $I = \{a \in R : \Phi(a) \in J\}$. Then I is an Ideal of $K \subset I$ and I/K isomorphic to J. This sets up *a 1-1* correspondence between all the ideals of R' and those of R that contain K.

Theorem 1.5.12(Second Homomorphisms Theorem)[9]

Let R be a ring, and let I and J be two ideals of R. Then J is an ideal of $I+J$, $I \cap J$ is an ideal of I, and $(I+J)/J \cong I/I \cap J$.

Theorem 1.5.13 (Third homomorphism Theorem)[9]

Let R and R' be two rings, and let Φ be a homomorphism from R onto R'. If J is an ideal of R' and $I=\{a \in R: \Phi(a) \in J\}$, then $R/I \cong R'/J$. Equivalently, if J is an ideal of R and $J \subset I$ is an ideal of R, then $R/I \cong (R/J)/(I/J)$.

1.6 Module

Definition 1.6.1 [8]

Let R be a ring .*M* ***is a left R-module (left module over R)*** **if**:

i) M is an additive abelian group (w.r.t +), and

ii) There is a map $\Psi : R \times M \to M$ denoted by rm satisfying the conditions

   a) $r(m_1+m_2)=rm_1+rm_2$.

   b) $(r_1+r_2)\, m=r_1m+r_2m$.

   c) $(r_1r_2)\, m=r_1\,(r_2m)$ *for all* $r, r_1, r_2 \in R$ *and* $m, m_1, m_2 \in M$.

   d) $e\, m = m$, *if* R *has unity* e.

Remarks1.6.2:

(i) A right R-module is defined similarly except the map $M \times R \to M$ and denote by mr $\forall\ r \in R,\ \forall\ m \in M$.

(ii) If R is commutative any left R-module M can be made right R-module by defining $mr = rm$.

(iii) An R-module with unity e is called ***unital module (unitary*** module***)***.

(iv) A module M is called ***Trivial module*** if R is a ring and M is abelian group such that $rm=0$ for all $r \in R$, $\forall\ m \in M$.

Example1.6.3:

(i) A ring R is an R-module.

(ii) Any abelian group is a Z-module.

(iii) Any ideal of a ring R is an R-module.

Definition 1.6.4 [5]

Let M be an R-module. A subset N of M is said to be ***an R-submodule*** of M if:

(i) N is a subgroup of the additive group M.

(ii) $rn \in N$ for all $r \in R$ and $n \in N$.

Example1.6.5:

Let M be an R-module, then M and $\{0\}$ are submodule of M.

Definition1.6.6 [1]

Let R be a ring and M, N be R-modules. A map $\Phi : M \rightarrow N$ is called an ***R-module homomorphism*** if for any $x, y \in M$ and any $r \in R$ we get:

(i) $\Phi(x+y) = \Phi(x) + \Phi(y)$

(ii) $\Phi(rx) = r\Phi(x)$.

Φ is monomorphism if it is *1-1*, Φ is epimorphism if it is onto, Φ *is* isomorphism if it is *1-1* and onto.

Definition1.6.7 [5]

Let M be an R-module and N a submodule of M then $N \leq M$. $M/N = \{x+N : x \in M\}$, the set of all cosets of N in M. M/N is an abelian group w.r.t the addition of cosets $(x+N)+(y+N)=(x+y)N$.

Define ***the Quotient module*** of M *by* N as follows:

$$r(x+N)=rx+N,\ \forall\ r\in R,\ \forall m\in M.$$

Remark:

If M is unitary, then so is M/N.

Definition 1.6.8 [1]

The map $\Phi: M\to M/N$ given by $\Phi(x) = x+N$ for all $x\in M$ is called ***the natural homomorphism.***

it is onto and $ker\Phi=\{x\in M: \Phi(x)=N\}=\{x\in M: x+N=N\}=N.$

Definition 1.6.9 [6]

Let A be a subset of an R-module M. A is said to be ***linearly independent*** set if for any finite number of distinct elements $a_1,a_2,\ldots,a_n$ of A, such that : $r_1a_1+r_2a_2+\ldots+r_na_n= 0$, $r_i\in R$,then $r_i=0$. Otherwise, A is called ***linearly dependent.***

Definition 1.6.10 [6]

Let M be an R-module and let A be a subset of M. we shall say that A ***is a basis*** of M if A generates (or spans) M , i.e A spans M if $M=\langle A \rangle$; and A is linearly independent.

Definition 1.6.11 [15]

Let R be a ring with unity, an R-module F is called ***free R-module (F)*** if F has a basis A. Denoted by $F(A)$.(***F(A)*** is called ***a free module on the set*** *A*).

Example1.6.12:

Let R be a ring with unity e and n a positive integer, the R-module R^n is a free R-module on the subset $\{e_1, e_2, \ldots, e_n\} \subsetneq R^n$, where $e_1=(e,0,\ldots,0),\ldots,e_n=(0,\ldots,e)$. $\{e_1, e_2, \ldots, e_n\}$ is a basis for R^n.

Chapter Two

The Smith Normal Form

2.1 Introduction:

We will describe (the smith normal form) a procedure that is very similar to reduction of a matrix to echelon form. And the result is that every matrix over a principal ideal domain is equivalent to a matrix in smith normal form.

Definition 2.1.1 (The Smith normal form)[3]

Let R be a principal ideal domain and let A be an $m \times n$ matrix with entries in R. If there are nonzero $a_1, \ldots, a_m \in R$ Such that a_i divides a_{i+1} for each $i < m$ then A is in Smith Normal Form, i.e.

$$A = \begin{pmatrix} a_1 & & & \\ & a_m & & \\ & & 0 & \\ & & & 0 \end{pmatrix}$$

We explain the basic idea by numerical example.

Let us start with the following matrix:

$$\begin{pmatrix} 0 & 0 & 22 & 0 \\ -2 & 2 & -6 & -4 \\ 2 & 2 & 6 & 8 \end{pmatrix}$$

We assume a free Z– module with basis x_1, x_2, x_3, x_4 and a sub-module K generated by u_1, u_2, u_3, u_4, where $u_1 = 22x_3$, $u_2 = -2x_1 + 2x_2 - 6x_3 - 4x_4$, $u_3 = 2x_1 + 2x_2 + 6x_3 + 8x_4$.

The first step is to bring the smallest positive integer. To the position 1-1 Thus interchange row 1 and 3 to obtain

$$\begin{pmatrix} 2 & 2 & 6 & 8 \\ -2 & 2 & -6 & -4 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

Since all entries in column 1, and similarly in row 1, are divisible by 2, we can pivot about the 1-1 position; in other words, use the 1-1 entry to produce zeros. Thus add row 1 to row 2 *i.e.* [2 2 6 8] + [-2 2 -6 -4]

To get:

$$\begin{pmatrix} 2 & 2 & 6 & 8 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

Add -1 times column 1 to column 2, then add -3 times column 1 to column 3, and add -4 times column 1 to column 4, The result is

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

Add -1 times column 2 to column 4, and we have

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

We note that 4 does not divide 22 *i.e.* a_i not divide a_{i+1} Therefore the condition of smith normal form not satisfy.

So we have more work to do. Add row 3 to row 2 to get

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 22 & 0 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

we pivot about the 2-2 position, 4 does not divide 22, but if we add -5 times column 2 to column 3, we have

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & 22 & 0 \end{pmatrix}$$

Interchange columns 2 and 3 to get

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 22 & 0 & 0 \end{pmatrix}$$

Add-11times row 2 to row 3 to obtain

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & -44 & 0 \end{pmatrix}$$

Finally, add-2 times column 2 to column 3, and the multiply row (or column) 3 by -1, the result is

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 44 & 0 \end{pmatrix}$$

Which is the smith normal form of the original matrix.

2.2 Equivalence of Matrices with entries in a principal ideal domain (p.i.d):

Two $m \times n$ matrices with entries in a principal ideal domain($p.i.d$) D are said to be equivalent if there exists an invertible matrix P in $M_{m,n}(D)$ and an invertible matrix Q in $M_{m,n}(D)$such that $B=PAQ$. It is clear that this defines an equivalence relation in the set $M_{m,n}(D)$ of $m \times n$ matrices with entries in D.

Theorem 2.2.1 [11]

If $A \in M_{m,n}(D)$, D a principal ideal domain (p.i.d), then A is equivalent to a matrix which has the "diagonal" form diag $\{d_1, d_2, \ldots, d_r, \ldots, 0\}$

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

Where the $d_i \neq 0$ *and* d_i/d_j *if* $i \leq j$.

2.3 The Existence of the Smith normal form [13]

We will to simplify matrices $A \in M_{m \times n}(R)$ as possible by use of elementary row and columns.

Every matrix $A \in M_{m \times n}(R)$ is equivalent to a diagonal matrix. Moreover by requiring that the diagonal elements satisfy some extra conditions on the diagonal elements this diagonal form is unique.

Theorem 2.3.1 (Existence of the Smith normal form)

Let R be an Euclidean domain. Then every $A \in M_{(m \times n)}(R)$ is equivalent to diagonal matrix of the form

$$\begin{pmatrix} f_1 & & & & & \\ & f_2 & & & & \\ & & \ddots & & & \\ & & & f_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

This is an matrix $M_{m \times n}$ and all off diagonal elements are 0, where

$f_1 / f_2 / \ldots / f_{r-1} / f_r$.

Proof:

We use induction on $m + n$. The case is $m+n = 2$ in which case the matrix A is 1×1 and there is nothing to prove. So let $A \in M_{m \times n}(R)$ and assume that the result is true for all matrices in any $M_{m'\times n'}(R)$, where $m'+n'<m+n$, if $A=0$ then A is already in the required form and there is nothing to prove, so assume that $A\neq 0$.

Let $\delta : R \to \{0,1,2,\ldots\}$ be as in the definition of Euclidean domain and let $\mathcal{A}$ be the set of all entries of elements of matrices equivalent to A ,and let $f_1 \in \mathcal{A}$ be a nonzero element of $\mathcal{A}$ that minimizes δ. That is $\delta(f_1) \leq \delta(a)$ for all $0 \neq a \in \mathcal{A}$. (Recall that $\delta(0)$ is undefined, so we leave it out of the competition for minimizer) Let B be a matrix equivalent to A that has f_1 as an element. If f_1 is in the i, j – th place of B , then we can interchange the first and i-th row of B and then the first and j –th column of B and assume that f_1 is in the 1,1 place of B . (Interchanging rows and columns are elementary row and column operations and so the resulting matrix is still equivalent to A) . So B is of the form

$$B=\begin{pmatrix} f_1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

We can use the division algorithm in R to find a quotient and remainder when the elements $b_{21}, b_{31},\ldots, b_{m1}$ of the first column are divided by f_1.

That is there are $q_2,\ldots,q_m, r_2,\ldots,r_m \in R$ so that $b_{i1} = q_i f_1 + r_i$ where either $r_i = 0$ or $\delta(r_i) < \delta(f_1)$. Then $r_i = b_{i1} - q_i f_1$. Now doing the $m-1$ row operations of taking $-q_i$ times the first row of A and adding to the i-th row we get that B (and thus also A) is equivalent

$$\begin{pmatrix} f_1 & b_{12} & b_{13} & \cdots & b_{1n} \\ b_{21}-q_2f_1 & * & * & \cdots & * \\ b_{31}-q_3f_1 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{m1}-q_mf_1 & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} f_1 & b_{12} & b_{13} & \cdots & b_{1n} \\ r_2 & * & * & \cdots & * \\ r_3 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_m & * & * & \cdots & * \end{pmatrix}$$

Where * is use to represent unspecified elements of R. As this matrix is equivalent to A and by the way that f_1 we must have $r_2 = r_3 = \ldots r_m = 0$ (as otherwise $\delta(r_j) < \delta(f_1)$ and f_1 was chosen so that $\delta(f_1) \le \delta(b)$ for any nonzero element of a matrix equivalent to A). Thus our matrix is of the form

$$\begin{pmatrix} f_1 & b_{12} & b_{13} & \cdots & b_{1n} \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \cdots & * \end{pmatrix}$$

We now clear out the first row in the same manner. There are p_j and s_j so that $b_{1j} = p_jf_1 + s_j$ and either $s_j = 0$ or $\delta(s_i) < \delta(f_1)$. Then by doing the $n-1$ column operations of taking $-p_j$ times the first column and adding to the j-th column we can farther reduce our matrix to

$$\begin{pmatrix} f_1 & a_{12}-p_2f_1 & a_{13}-p_3f_1 & \cdots & a_{1n}-p_nf_1 \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} f_1 & s_2 & s_3 & \cdots & s_n \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \cdots & * \end{pmatrix}$$

Exactly as above this the minimulity of $\delta(f_1)$ over all elements in matrices equivalent to A implies that $s_j = 0$ for $j = 2, \ldots, n$. So we now have that A is equivalent to the matrix

$$C = \begin{pmatrix} f_1 & 0 & 0 & \dots & 0 \\ 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{pmatrix} = \begin{pmatrix} f_1 & 0 & 0 & \cdots & 0 \\ 0 & c_{22} & c_{23} & \cdots & c_{2n} \\ 0 & c_{32} & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & c_{m3} & \cdots & c_{mn} \end{pmatrix}.$$

If either $m = 1$ or $n = 1$ then C is of one of the two forms

$$[f_1, 0, 0, \dots, 0], \text{ or } \begin{pmatrix} f_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and we are done.

So assume that $m, n \geq 2$. We claim that every element in this matrix is divisible by f_1 . To see this consider any element c_{ij} in the i-th row (where $i,j \geq 2$). Then we can the i-th row to the first row to get the matrix:

$$\begin{pmatrix} f_1 & c_{i1} & c_{i2} & \dots & c_{in} \\ 0 & c_{22} & c_{23} & \dots & c_{2n} \\ 0 & c_{32} & c_{33} & \dots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & c_{m2} & \dots & c_{mn} \end{pmatrix}$$

Which is equivalent to A . We use the same manner as above.

There are $t_j, p_j \in R$ for $2 \leq j \leq n$ so that $c_{ij} = t_j f_1 + p_j$ with $p_j = 0$ or $\delta(p_j) < \delta(f_1)$. Then add $-t_j$ times the first column of to the j-th column to get

$$\begin{pmatrix} f_1 & a_{i2} - t_2 f_1 & a_{i3} - t_3 f_1 & \dots & a_{in} - t_n f_1 \\ 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{pmatrix} = \begin{pmatrix} f_1 & p_2 & p_3 & \cdots & p_n \\ 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{pmatrix}$$

As this matrix is equivalent to A again the minimality of $\delta(f_1)$ implies that $\delta(p_j) = 0$ for $j = 2, \ldots, n$. Therefore $c_{ij} = t_j f_1$ which implies that c_{ij} is divisible by f_1.

As each element of C is divisible by f_1 we can write $c_{ij} = f_1 c'_{i\,j}$. Factor the f_1 out of the elements of C implies that we can write C in block form as

$$C = \begin{pmatrix} f_1 & 0 \\ 0 & f_1 C' \end{pmatrix} \quad \text{------} (*)$$

Where C' is $(m-1) \times (n-1)$.

Now at long last we get to use the induction hypothesis.

As $(m-1) + (n-1) < m + n$ the matrix C' is equivalent to a matrix of the form

$$C' \cong \begin{pmatrix} f_2' & & & & & \\ & f_3' & & & & \\ & & \ddots & & & \\ & & & f_r' & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

Where $f'_2, f'_3, \ldots, f'_r$ satisfy $f'_2 \,/\, f'_3 \,/ \ldots /\, f'_r$. (We start at f'_2 rather than f'_1 to make later notation easier.) This means there is a $(m-1) \times (m-1)$ matrix P and an $(n-1) \times (n-1)$ matrices Q so that each of P and Q are products of elementary matrices and so that

$$PC'Q = \begin{pmatrix} f_2' & & & & & \\ & f_3' & & & & \\ & & \ddots & & & \\ & & & f_r' & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

This in turn implies

$$Pf_1C'Q = f_1PC'Q = f_1\begin{pmatrix} f_2' & & & & & \\ & f_3' & & & & \\ & & \ddots & & & \\ & & & f_r' & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

$$= \begin{pmatrix} f_1f_2' & & & & & \\ & f_1f_3' & & & & \\ & & \ddots & & & \\ & & & f_1f_r' & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

The block matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \text{and} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}$$

are of size $m \times m$ and $n \times n$ respectively and are products of elementary matrices. Using our calculation of $Pf_1C'Q$ in equation (*) gives

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} C \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \begin{pmatrix} f_1 & 0 \\ 0 & f_1C' \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}$$

$$= \begin{pmatrix} f_1 & 0 \\ 0 & Pf_1C'Q \end{pmatrix}$$

$$= \begin{pmatrix} f_1 & & & & & \\ & f_1f_2' & & & & \\ & & \ddots & & & \\ & & & f_1f_r' & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

$$= \begin{pmatrix} f_1 & & & & & \\ & f_2 & & & & \\ & & \ddots & & & \\ & & & f_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

Where $f_2 = f_1 f'_2$, $f_3 = f_1 f'_3$,..., $f_r = f_1 f'_r$. As this matrix is equivalent to A to finish the proof it enough to show that $f_1 / f_2 / f_3 / \ldots / f_r$.

As $f_2 = f_1 f'_2$ it is clear that f_1 / f_2 If $2 \le j \le r - 1$ then we have that f'_j / f'_{j+1} so by definition there is a $c_j \in R$ so that $f'_{j+1} = c_j f'_j$.

Multiply by f_1 and use $f_j = f_1 f'_j$ and $f_{j+1} = f_1 f'_{j+1}$ to get $f_{j+1} = f_1 f'_{j+1} = f_1 c_j f'_j = c_j f_j$. This implies that f_j / f_{j+1} and we are done.

2.4 *An application of the Existence of The Smith Normal From*

Invertible matrices are products of elementary matrices.

Theorems 2.3.1 give a very nice characterization of invertible matrices.

Theorem 2.4.1 [10]

Let $A \in M_{n \times n}(R)$ be a square matrix over an Euclidean domain. Then A is invertible if and only if it is a product of elementary matrices.

Proof:

One direction is clear: elementary matrices are invertible, so product of elementary matrices is invertible.

Now assume that A in invertible. Then by theorem *2.3.1* A is equivalent to a diagonal matrix

$$D = \text{diag}\,(f_1, f_2, \ldots, f_r, 0\ldots,0).$$

Hence there are matrices P and Q, each a product of elementary matrices, so that $A = PD\,Q$.

As A, P and Q are invertible their determinants are units (Theorem 1.4.21) and therefore form det (A) = det (P) det (D) det (Q) it follws that det (D) = det (A) det $(P)^{-1}$ det $(Q)^{-1}$ is a unit. But the determinant of a diagonal matrix is the product of its diagonal elements.

Thus in the definition of D if $r < n$ there will be a zero on the diagonal and so det $(D) = 0$, which is not a unit. Thus $r = n$ and so det $(D) = f_1 f_2 \ldots f_n$. But then $f_1(f_2 \ldots f_n$ det $(D)^{-1}) = 1$ so that f_1 is a unit with inverse $f_1^{-1} = (f_2 \ldots f_n$ det $(D)^{-1})$. Likewise each f_k is a unit with inverse f_k^{-1} = det $(D)^{-1} \prod_{j \neq k} f_j$. But then letting E_k be the diagonal matrix

$$E_k = \text{diag}(1, 1, \ldots, f_k, \ldots, 1)$$

We have that E_k is a an elementary matrix and that D factors as

$$D = E_1\, E_2 \ldots E_n.$$

Thus D is a product of elementary matrices. But then $A = PDQ$ is a product of elementary matrices.

2.5 Uniqueness of the Smith normal form [13]

Recall, theorem (1.4.17) , that in a Euclidean domain R that any finite set of elements $\{a_1, a_2, \ldots, a_l\}$ has a greatest common divisor and that greatest common divisor of $\{a_1, a_2, \ldots a_l\}$ is the generator of the ideal $\langle a_1, a_2, \ldots, a_l \rangle$ (which is a principle ideal) . Recall, Definition (1.4.18), for $A \in M_{(m,n)}$ that $I_k(A)$ is the ideal of R generated by all $k \times k$ sub –determinants of A.

is another Smith normal form of A then we have

$$I_k(S') = I_k(A) = I_k(S)$$

and therefore, as greatest common divisors are unique up to multiplication by units, there are units $u_1, u_1, \ldots, u_r$ of R such that

$f'_1 = u_1 f_1, f'_1 f'_2 = u_2 f_1 f_2, f'_1 f'_2 f'_2 = u_2 f_1 f_2 f_3, \ldots, f'_1 f'_2, \ldots, f'_k = u_k f_a f_2, \ldots, f_k.$

This implies $f'_1 = u_1 f_1$ and $f'_j = u_j^{-1}{}_{-1} u_j f_j$ for $2 \le j \le k$.

Which show $f_1, \ldots, f_r$ are unique up to multiplication by units.

Theorem 2.5.2 [12]

If A is a matrix with entries in a principal ideal domain R, then there are invertible matrices P and Q over R such that PAQ is in Smith Normal Form.

Proof:

Let us illustrate the idea by consider the 2×2 matrix, i.e.

Suppose we have $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Let $e = \gcd(a, c)$, and $e = ax + cy$ for some $x, y \in R$, where $a = e\alpha$ and $c = e\beta$ for some $\alpha, \beta \in R$. Then $e = ax + cy = e\alpha x + e\beta y \Rightarrow 1 = \alpha x + \beta y$..

We have $\begin{pmatrix} x & y \\ -\beta & \alpha \end{pmatrix}^{-1} = \begin{pmatrix} \alpha & -y \\ \beta & x \end{pmatrix}$. So the matrix $\begin{pmatrix} x & y \\ -\beta & \alpha \end{pmatrix}$ is invertible.

Moreover, $\begin{pmatrix} x & y \\ -\beta & \alpha \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e & bx + dy \\ -a\beta + c\alpha & -b\beta + d\alpha \end{pmatrix}$.

Then reduces this matrix to the form $\begin{pmatrix} e & u \\ 0 & v \end{pmatrix}$.

A similar argument, applied to the first row instead of the first column, allows us to multiply on the right by an invertible matrix and obtain a matrix to the form $\begin{pmatrix} e_1 & 0 \\ * & * \end{pmatrix}$.

Where $e_1 = \gcd(e,u)$. Continuing this process, alternating between the first row and the first column, will produce a sequence of elements $e, e_1, \ldots$ such that e_1 divides e, e_2 divides e_1, and so on.

In terms of ideals, $(e) \subsetneq (e_1) \subsetneq \ldots$

Because any increasing sequence of principal ideals stabilizers in a principal ideal domain, we get after finitely many steps, with a matrix of the form $\begin{pmatrix} f & 0 \\ g & h \end{pmatrix}$ or $\begin{pmatrix} f & g \\ 0 & h \end{pmatrix}$ in which f divides g.

One more row or column operation will then yield a matrix of the form $\begin{pmatrix} f & 0 \\ 0 & k \end{pmatrix}$.

Thus, by multiplying on the left and right by invertible matrices, we obtain a diagonal matrix.

Once we have reduced to a diagonal matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, to get the Smith Normal Form, let $d = \gcd(a,b)$.

Where $d = ax + by$ for some $x, y \in R$.

Moreover, $a = d\alpha$ and $b = d\beta$ for some $\alpha, \beta \in R$.

By performing the row and column operations, yielding

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ ax & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ ax+by & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ d & b \end{pmatrix}$$

$$\to \begin{pmatrix} 0 & -b\alpha \\ d & b \end{pmatrix} \to \begin{pmatrix} 0 & -b\alpha \\ d & 0 \end{pmatrix} \to \begin{pmatrix} d & 0 \\ 0 & -b\alpha \end{pmatrix}$$

a diagonal matrix in Smith Normal Form since d divides $-b\alpha$.

Chapter Three

Some Applications of the smith normal form

3.1 Generators and Relations:

Let R be a principal ideal domain and let M be a finitely generated R-module. If $\{m_1, \cdots, m_n\}$ is a set of generators of M, then we have a surjective R-module homomorphism $\varphi : R^n \longrightarrow M$ given by sending $(r_1, \cdots, r_n) \xrightarrow{\varphi} \sum_{i=1}^{n} r_i m_i$. The $Ker\varphi = \{(r_1, \cdots, r_n) | \varphi((r_1, \cdots, r_n)) = 0\} = K$. So we have by the first isomorphism theorem, $M \cong R^n / K$.

If $(r_1, \ldots, r_n) \in K$, then $\sum_{i=1}^{n} r_i m_i = 0$.

Thus, an element of K gives rise to a relation among the generators $\{m_1, \cdots, m_n\}$.

Lemma 3.1.1 [12]

The submodule K of R is finitely generated.

Proof:

Suppose that $\{k_1, k_2, \ldots, k_m\} \subseteq R^n$ is a generating set for K.

If $k_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, then the matrix (a_{ij}) over R as the relation matrix for M relative to the generating set $\{m_1, \cdots, m_n\}$ of M and the generating set $\{k_1, \ldots, k_m\}$ of K. This matrix has k_i as its *i-th* row for each i.

(Since this matrix depends not just on the generating sets for M and K but by the order in which we write the elements), we use ordered sets, or lists, to denote generating sets. We will write $[m_1, \ldots, m_n]$ to denote an ordered n-tuple.

Example 3.1.2:

Let $M = Z_4 \oplus Z_{12}$, where M is generated by $m_1 = ([1]_4, 0)$ and $m_2 = (0, [1]_{12})$.

Moreover, $4m_1 = 0$ and $12m_2 = 0$.

Consider the homomorphism $\varphi : Z \oplus Z \longrightarrow M$ sending $(r,s) \mapsto (rm_1, sm_2)$,

then $ker\ (\varphi) = \{(r,s) \in Z \oplus Z : (r + 4Z, s + 12Z) = (0,0)\}$

$= \{(4a, 12b) : a, b \in Z\}$.

Thus, every element $(4a, 12b)$ in the kernel can be written as:

$a\,(4, 0) + b\,(0, 12)$ for some $a, b \in Z$.

Therefore, $[(4,0), (0,12)]$ is an ordered generating set for $ker\ (\varphi)$.

The relation matrix for this generating set is then the diagonal matrix.

$$\begin{pmatrix} 4 & 0 \\ 0 & 12 \end{pmatrix}.$$

Example 3.1.3:

Suppose that M is abelian group have generators $\{m_1, m_2\}$, and suppose the relation submodule K is generated by $[(3,0), (0,6)]$.

Then the relation matrix is the diagonal matrix $\begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}$.

So, the relation submodule K relative to $[m_1, m_2]$ is:

$$K = \{a(3,0) + b(0,6) : a, b \in Z\} = \{(3a, 6b) : a, b \in Z\}$$

Furthermore, K is also the kernel of the map $\sigma : Z^2 \to Z_3 \oplus Z_6$ which is defined by $\sigma(r,s) = (r + 3Z, s + 6Z)$. Therefore, $Z^2 / K \cong Z_3 \oplus Z_6$.

However, $M \cong Z^2 / K$. Therefore, $M \cong Z_3 \oplus Z_6$.

Remark:

Generating sets for a module M and for a relation submodule K are not unique.

Example 3.1.4:

Suppose that M be abelian group with generators $[m_1, m_2]$,

such that $2m_1 + 4m_2 = 0$ and $-2m_1 + 6m_2 = 0$.

Then the relation submodule K contains $k_1 = (2,4)$ and $k_2 = (-2,6)$.

If these generate K, then the relation matrix is $\begin{pmatrix} 2 & 4 \\ -2 & 6 \end{pmatrix}$.

Note that K is also generated by k_1 and k_1+k_2.

These pairs are *(2,4)* and *(0,10)*. Therefore relative to this new generating set of K, the relation matrix is $\begin{pmatrix} 2 & 4 \\ 0 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ -2 & 6 \end{pmatrix}$.

Lemma 3.1.5 [12]

Consider M be a finitely generated R-module, with ordered generating set $[m_1, \ldots, m_n]$. Suppose that the relation submodule K is generated by $[k_1, \ldots, k_p]$. Let A be the $n \times p$ relation matrix relative to these generators.

(i) Let $Q \in M_n(R)$ be an invertible matrix and write $Q^{-1} = (q_{ij})$. If m'_j is defined by $m'_j = \sum_i q_{ij} m_i$ for $1 \le j \le n$, then $[m'_1, \ldots, m'_n]$ is a generating set for M and the rows of AQ generate the corresponding relation submodule. Therefore, AQ is a relation matrix relative to $[m'_1, \ldots, m'_n]$.

(ii) Let P and Q be $P \times P$ and $n \times n$ invertible matrices, respectively. If $B = PAQ$, then B is the relation matrix relative to an appropriate ordered set of generators of M and of the corresponding relation submodule.

Proposition 3.1.7 [12]

Let A is a relation matrix for an R-module M. If there are invertible matrices P and Q for which

$$PAQ = \begin{pmatrix} a_1 & 0 & & \cdots \\ 0 & a_2 & & \cdots \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$$ is a diagonal matrix, then

$M \cong R/(a_1) \oplus \ldots \oplus R/(a_n)$.

3.2 Algorithm for computing the Smith Normal Form [13]

As we mentioned in chapter two, we know the smith normal form of principal ideal domain (P.I.D) inputs. An example of P.I.D is the set of integers. Therefore, we developed to calculate and evaluate the smith normal form for any $n \times m$ matrix A with entries from the ring of integers. We take into account that smith normal form is unique.

Algorithm Idea 3.2.1

The algorithm has two stages:

The first stage is to produce a diagonalization from a given matrix over a principle ideal domain R.

The diagonal matrix has the form

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

The second stage, we compute the invariant factors of the diagonal matrix obtained in the first stage.

The Steps For The Smith Normal Form 3.2.2

The first stage is to produce any diagonalization from the matrix A, the steps are as following:

Step 1. Interchange columns and rows so that a_{11} is the element of smallest absolute value among all nonzero elements in the first row and first column of the matrix .Go to step 2.

Step 2. if a_{11}/a_{1j}, for $j = 2,3,\dots,n$, go to step 3.Otherwise do not divide $a_{11}/a1j$,for some $j = k(say)$. Let $a_1k = qa_{11} + r$ where q, r are integers and $0 \langle r \langle a_{11}$ .Let $A[\ ,k]$ denote the kth column of A.

Replace $A[\ ,k]$ by $A[\ ,k] - qA[\ ,1]$. Go to step 1.

Step 3. If a_{11}/a_{i1} for $i = 2,3,\dots,n$, go to step 4.Othersise do not divides a_{11}/a_{i1}

for some $i=k$ (say). Let $a_{k1}=qa_{11}+r$ where q,r are integers and $0<r<a_{i1}$. Let $A[k,\ ]$ denote the kth row of A. Replace $A[k,\ ]$ by $A[k,\ ]-qA[1,\ ]$ .Go to step 1.

Step 4. a_{i1}/a_{ij} for $j=2,3,...n$ and a_{11}/a_{i1} for $i=2,3,....,n$.
Either assume $a_{1j}=q_j a_{11}$, then replace $A[\ ,j]$ by $A[\ ,j]-q_j A[\ ,1]$for $j=2,3,...,n$. This will ensure that the first row of the matrix has only the first element nonzero. Then since it can be similarly assumed that $a_{i1}=q_i' a_{11}$ for $i=2,3,....,n$, every element $a_{i1}, i=2,3,....,n$,can be set to zero.

Or assume $a_{i1}=q_i a_{11}$, then replace $A[i,\ ]$ by $A[i,\ ]-q_i A[1,\ ]$, for $j=2,....,n$. This will ensure that the first column of the matrix has only the first element nonzero. Then since it can be similarly assumed that $a_{1j}=q_j a_{11}'$, for $j=2,3,....,n$, every element $a_{1j}, j=2,....,n$ can be set to zero.

Step 5. The matrix is now of the form

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & & & \\ & & \ddots & \\ 0 & & \cdots & a_{nn} \end{pmatrix}$$

Step 1 to 4 are now applied to the submatrix

$$\begin{pmatrix} a_{22} & & \cdots & 0 \\ 0 & a_{33} & \cdots & 0 \\ \vdots & & & \\ & & \ddots & \\ 0 & & \cdots & a_{nn} \end{pmatrix}$$

And the process continues until the matrix is completely diagonalized.

The first stage of the algorithm will convert the matrix A into diagonal form,

$$\begin{pmatrix} x_1 & & \cdots & 0 \\ & x_2 & \cdots & 0 \\ \vdots & & \ddots & \\ & \cdots & & x_n \end{pmatrix}$$

The second stage of the process is to compute the invariant factors from this diagonalization.

Step 6 If x_1/x_i, $i = 2,\dots,n$, then check that x_2/x_i, $i = 3,\dots,n$. This process is repeated until value x_j is found such that do not divides x_j/x_i for some $j\langle i \leq n$. Say do not divides x_j/x_k row k of the matrix is added to row j and the algorithm is reentered to create a new x_j of smaller value.

3. 3 The program

Unit 1 listing:

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
  Dialogs, Grids, StdCtrls, Buttons, ComCtrls, XPMan, ExtCtrls, Menus;

type
  TForm1 = class(TForm)
    StringGrid1: TStringGrid;
    StringGrid2: TStringGrid;
    XPManifest1: TXPManifest;
    GroupBox1: TGroupBox;
    BitBtn2: TBitBtn;
    BitBtn1: TBitBtn;
    Edit2: TEdit;
    UpDown2: TUpDown;
    Label2: TLabel;
    UpDown1: TUpDown;
    Edit1: TEdit;
    Label1: TLabel;
    Panel1: TPanel;
    BitBtn4: TBitBtn;
    BitBtn3: TBitBtn;
    WaitLabel: TLabel;
    MainMenu1: TMainMenu;
    operation1: TMenuItem;
    RandomNumbers1: TMenuItem;
    SmithNormalFormis1: TMenuItem;
    ShowDetails1: TMenuItem;
    N1: TMenuItem;
    N2: TMenuItem;
    Close1: TMenuItem;
    About1: TMenuItem;
    AboutProgram1: TMenuItem;
    StepLabel: TLabel;
    procedure Fill_A_Matrix_BtnClick(Sender: TObject);
    procedure FormCreate(Sender: TObject);
    procedure BitBtn4Click(Sender: TObject);
    procedure Edit1Change(Sender: TObject);
    procedure Edit2Change(Sender: TObject);
    procedure BitBtn1Click(Sender: TObject);
    procedure BitBtn2Click(Sender: TObject);
    procedure BitBtn3Click(Sender: TObject);
    procedure StringGrid1KeyPress(Sender: TObject; var Key: Char);
    procedure Close1Click(Sender: TObject);
    procedure SmithNormalFormis1Click(Sender: TObject);
```

continue...

```
  procedure RandomNumbers1Click(Sender: TObject);
  procedure ShowDetails1Click(Sender: TObject);
  procedure AboutProgram1Click(Sender: TObject);
  private
    { Private declarations }
public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

uses Unit2, InfoUnt, Unit3;

{$R *.dfm}
//*******************
Function FillA:Boolean;
Var i,j:Integer;
begin
  try
  Result := True;
  for i:=1 to n do for j:=1 to n do
A[i,j]:=StrToInt(Form1.StringGrid1.Cells[j-1,i-1]);
  except
     Result := False;
     Application.MessageBox('Please... Enter Integere
Values.','Info',MB_OK);
  end;
end;//FillA...
procedure EmptyGrid(G:TStringGrid);
var i,j:Integer;X:Shortint;
begin
    for i:=0 to G.ColCount-1 do
      for j:=0 to G.RowCount-1 do G.Cells[i,j] := '';
end;
//*******************
procedure TForm1.FormCreate(Sender: TObject);
begin
  StringGrid1.Cells[0,0]:='-2';StringGrid1.Cells[0,1]:='-
3';StringGrid1.Cells[0,2]:='-12';

StringGrid1.Cells[1,0]:='3';StringGrid1.Cells[1,1]:='3';StringGrid1
.Cells[1,2]:='12';

StringGrid1.Cells[2,0]:='0';StringGrid1.Cells[2,1]:='0';StringGrid1
.Cells[2,2]:='6';
//  FillA;
end;
```

continue...

```
procedure TForm1.Fill_A_Matrix_BtnClick(Sender: TObject);
Var i,j:Integer;
begin
  for i:=1 to n do for j:=1 to StringGrid2.ColCount do
StringGrid2.Cells[j-1,i-1] := IntToStr(A[i,j]);
end;

procedure TForm1.BitBtn4Click(Sender: TObject);
var Flag,IsSmith:Boolean;i:Integer;
begin
InfoForm.Tag := 0;
Step := 0;
if FillA=False then exit;
Screen.Cursor := crHourGlass;
WaitLabel.Visible := True;Refresh;
try
  InfoForm.RichEdit1.Lines.Clear;
  repeat
    IsSmith := False;
    for i := 1 to n-1 do
    begin
      Flag := False;
      repeat
        LessVal(i);
        Flag := DivOK(i);
        DivData(i);
      until Flag;
    end;//for...
    IsSmith := IsSmithNormal;
  until IsSmith;
  AbsOfMatrix;
  Fill_A_Matrix_BtnClick(Sender);
  WaitLabel.Visible := False;
  Screen.Cursor := crDefault;
  StepLabel.Caption := 'Number of Step :'+IntToStr(Step);
except
  WaitLabel.Visible := False;
  Screen.Cursor := crDefault;
  raise;
end;
end;

procedure TForm1.Edit1Change(Sender: TObject);
begin
  n := UpDown1.Position;
  StringGrid1.RowCount := UpDown1.Position;
  StringGrid2.RowCount := UpDown1.Position;
end;
```

continue...

```
procedure TForm1.Edit2Change(Sender: TObject);
begin
  Z := UpDown2.Position;
  StringGrid1.ColCount := UpDown2.Position;
  StringGrid2.ColCount := UpDown2.Position;

end;

procedure TForm1.BitBtn1Click(Sender: TObject);
var
  Flag,IsSmith:Boolean;i:Integer;
begin
if(UpDown1.Position*UpDown2.Position>225)then
  if Application.MessageBox('.ÓÝæÇ... åÐå ÇáÚãáíÉ ÑÈãÇ ÊÃÎÐ æÞÊ Øæíá
ãä ÇáæÞÊ ¿ì
ÇãÊÇÈÚÉ','ÊäÈíå',MB_YESNO+MB_RIGHT+MB_ICONINFORMATION+MB_DEFBUTTON2
)=mrNo then
      Exit;
InfoForm.Tag := 1;
Step := 0;
if FillA=False then exit;
Screen.Cursor := crHourGlass;
WaitLabel.Visible := True;Refresh;
try
  InfoForm.RichEdit1.Lines.Clear;

  InfoForm.RichEdit1.Lines.Add('Stratr time : '+TimeToStr(Now));
  showMatrix;
  repeat
      IsSmith := False;
      for i := 1 to n-1 do
      begin
          Flag := False;
          repeat
              LessVal(i);
              Flag := DivOK(i);
              DivData(i);
          until Flag;
      end;//for...
      IsSmith := IsSmithNormal;
  until IsSmith;
  AbsOfMatrix;
  InfoForm.RichEdit1.Lines.Add('Smith Normal Form is:');
  showMatrix;
  Fill_A_Matrix_BtnClick(Sender);
  WaitLabel.Visible := False;
  Screen.Cursor := crDefault;
  StepLabel.Caption := 'Number of Step :'+IntToStr(Step);
except
  WaitLabel.Visible := False;
  Screen.Cursor := crDefault;
  raise;
end;
```

continue...

```
InfoForm.RichEdit1.Lines.Add('End time : '+TimeToStr(Now));
InfoForm.ShowModal;
end;

procedure TForm1.BitBtn2Click(Sender: TObject);
begin
  Close;
end;

procedure TForm1.BitBtn3Click(Sender: TObject);
var i,j:Integer;X:Shortint;
begin
    EmptyGrid(StringGrid2);
    X := 33;
    Randomize;
    for i:=0 to StringGrid1.ColCount-1 do
      for j:=0 to StringGrid1.RowCount-1 do StringGrid1.Cells[i,j]
:= IntToStr(Random(X));

end;

procedure TForm1.StringGrid1KeyPress(Sender: TObject; var Key:
Char);
begin
  EmptyGrid(StringGrid2);
end;

procedure TForm1.Close1Click(Sender: TObject);
begin
  BitBtn2Click(Sender);
end;

procedure TForm1.SmithNormalFormis1Click(Sender: TObject);
begin
  BitBtn4Click(Sender)
end;

procedure TForm1.RandomNumbers1Click(Sender: TObject);
begin
  BitBtn3Click(Sender)
end;

procedure TForm1.ShowDetails1Click(Sender: TObject);
begin
  BitBtn1Click(Sender)
end;

procedure TForm1.AboutProgram1Click(Sender: TObject);
begin
  AboutBox.ShowModal;
```

Unit 2 listing:

```
unit Unit2;

interface

Procedure LessVal(P:Integer);
Procedure AToM;
Function DivOK(P:Integer):Boolean;
Procedure DivData(P:Integer);
Function IsSmithNormal:Boolean;
procedure showMatrix;
procedure AbsOfMatrix;

var
  A:array[1..100,1..100] of Integer;
  M:array[1..100,1..100] of Integer;
  n:Integer=3;z:Integer=3;
  Step:Integer=0;

implementation

uses SysUtils, InfoUnt;

Procedure AToM;
Var i,j:Integer;
begin
  for i:=1 to n do for j:=1 to n do M[i,j]:=A[i,j];
end;//AToM...

Procedure LessVal(P:Integer);
Var X,i,C,R:Integer;
begin
  C := -1;R := -1;
  X := A[P,P];
  for i:=P+1 to n do
    if(A[P,i]<>0)and(Abs(A[P,i])=Abs(X))then
    begin
       if Abs(A[P,i])> X then
       begin
         C := i;X := A[P,i];
       end;
    end else if(A[P,i]<>0)and(Abs(A[P,i])<Abs(X))then
    begin
         C := i;X := A[P,i];
    end else if X=0 then
    begin
         C := i;X := A[P,i];
    end;
```

continue...

```
  for i:=P+1 to n do
    if(A[i,P]<>0)and(Abs(A[i,P])=Abs(X))then
    begin
       if Abs(A[i,P])> X then
       begin
         C := -1;
         R := i;X := A[i,P];
       end;
    end else if(A[i,P]<>0)and(Abs(A[i,P])<Abs(X))then
    begin
         C := -1;
         R := i;X := A[i,P];
    end else if X=0 then
    begin
         C := -1;
         R := i;X := A[i,P];
    end;
  if(C<>-1)and(X<>0)then
  begin
     AToM;
     for i := 1 to n do
     begin
       A[i,P] := M[i,C];
       A[i,C] := M[i,P];
     end;
     Inc(Step);
     if InfoForm.Tag=1 then
     begin
     InfoForm.RichEdit1.Lines.Add(inttostr(Step)+':Interchange
Column '+inttostr(P)+' And Column '+inttostr(C));
     showMatrix;
     end;
  end else if(R<>-1)and(X<>0)then
  begin
     AToM;
     for i := 1 to n do
     begin
       A[P,i] := M[R,i];
       A[R,i] := M[P,i];
     end;
     Inc(Step);
     if InfoForm.Tag=1 then
     begin
     InfoForm.RichEdit1.Lines.Add(inttostr(Step)+':Interchange Row
'+inttostr(P)+' And Row '+inttostr(R));
     showMatrix;
     end;
  end;
end;//LessVal...
```

continue...

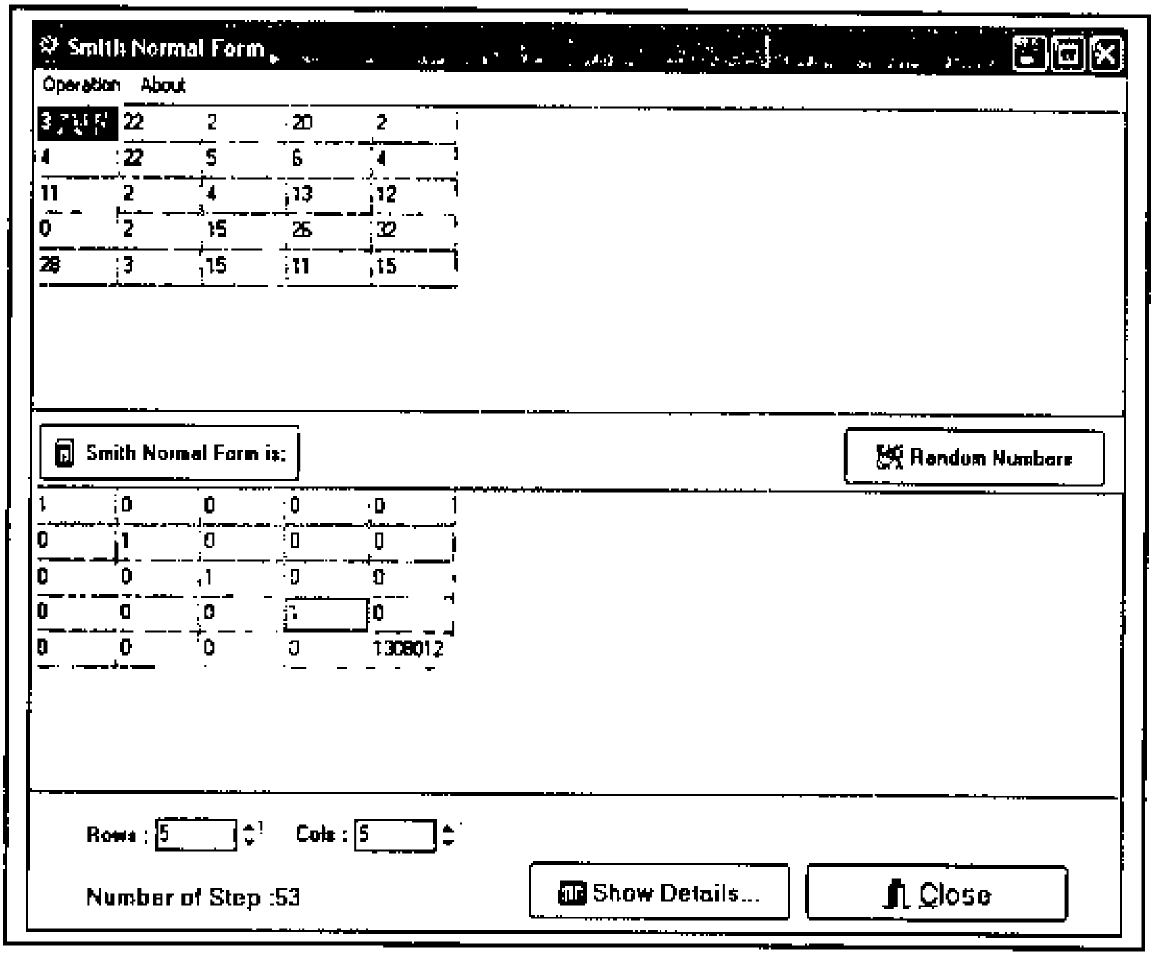
```
Function DivOK(P:Integer):Boolean;
var i:Integer;
begin
   Result := True;
   for i := P+1 to n do
   begin
     Result := ((A[P,i]=0)or( (A[P,i]) Mod A[P,P]=0
))And((A[i,P]=0)or( (A[i,P] Mod A[P,P])=0 ));
     if Result = False then Break;
   end;
end;//DivOK...

Procedure DivData(P:Integer);
var i,j,q:Integer;
begin
   AToM;
   for i:=P+1 to n do
   begin
      if A[P,P]<>0then q := Trunc(A[P,i]/A[P,P])else q := 0;
      for j := 1 to n do
         A[j,i] := -q*A[j,P]+A[j,i];
      if q <> 0 then
      begin
        Inc(Step);
        if InfoForm.Tag=1 then
        begin
        InfoForm.RichEdit1.Lines.Add(inttostr(Step)+':Add
'+inttostr(-q)+' times Column '+inttostr(P)+' to Column
'+inttostr(i));
        showMatrix;
        end;
      end;
   end;//for i...
   for i:=P+1 to n do
   begin
      if A[P,P]<>0then q := Trunc(A[i,P]/A[P,P])else q := 0;
      for j := 1 to n do
         A[i,j] := -q*A[P,j]+A[i,j];
      if q <> 0 then
      begin
        Inc(Step);
        if InfoForm.Tag=1 then
        begin
        InfoForm.RichEdit1.Lines.Add(inttostr(Step)+':Add
'+inttostr(-q)+' times Row '+inttostr(P)+' to Row '+inttostr(i));
        showMatrix;
        end;
      end;
   end;//for i...
end;//DivData...
```

continue

```
Function IsSmithNormal:Boolean;
var i,j:Integer;
begin
  Result :=-True;
  for i:=1 to n-1 do
  begin
    Result := Result And((A[i,i]=0)or((A[i+1,i+1] Mod A[i,i])=0)
);
     if Result=False then
     begin
        for j:=1 to n do A[i,j]:= A[i,j]-A[i+1,j];
        Inc(Step);
        if InfoForm.Tag=1 then
        begin
        InfoForm.RichEdit1.Lines.Add(inttostr(Step)+':Add Row
'+inttostr(i+1)+' to Row '+inttostr(i));
        showMatrix;
        end;
        Break;
     end;
  end;
end;//IsSmithNormal...

procedure showMatrix;
var i,j:Integer;str:String;
begin
  for i := 1 to n do
  begin
    Str := '';
    for j := 1 to z do Str := str+Format('%12d',[A[i,j]]);
    InfoForm.RichEdit1.Lines.Add(str);
  end;
  InfoForm.RichEdit1.Lines.Add('');
end;

procedure AbsOfMatrix;
var i,j:Integer;
begin
  for i := 1 to n do
    for j := 1 to z do A[i,j] := abs(A[i,j]);
end;


end.
```

3.4 Screenshots:

Calculating smith normal form window:



Show details button:

Smith Normal Form

Stratr time : 10:17:45.132 PM

3	22	2	20	2
4	22	5	6	4
11	2	4	13	12
0	2	15	26	32
28	3	15	11	15

1:Interchange Column 1 And Column 3

2	22	3	20	2
5	22	4	6	4
4	2	11	13	12
15	2	0	26	32
15	3	28	11	15

2:Add -11 times Column 1 to Column 2

2	0	3	20	2
5	-33	4	6	4
4	-42	11	13	12
15	-163	0	26	32
15	-162	28	11	15

3:Add -1 times Column 1 to Column 3

2	0	1	20	2
5	-33	-1	6	4
4	-42	7	13	12
15	-163	-15	26	32
15	-162	13	11	15

4:Add -10 times Column 1 to Column 4

2	0	1	0	2
5	-33	-1	-44	4
4	-42	7	-27	12
15	-163	-15	-124	32
15	-162	13	-139	15

5:Add -1 times Column 1 to Column 5

2	0	1	0	0
5	-33	-1	-44	-1
4	-42	7	-27	8
15	-163	-15	-124	17
15	-162	13	-139	0

Smith Normal Form

6:Add -2 times Row 1 to Row 2

2	0	1	0	0
1	-33	-3	-44	-1
4	-42	7	-27	8
15	-163	-15	-124	17
15	-162	13	-139	0

7:Add -2 times Row 1 to Row 3

2	0	1	0	0
1	-33	-3	-44	-1
0	-42	5	-27	8
15	-163	-15	-124	17
15	-162	13	-139	0

8:Add -7 times Row 1 to Row 4

2	0	1	0	0
1	-33	-3	-44	-1
0	-42	5	-27	8
1	-163	-22	-124	17
15	-162	13	-139	0

9:Add -7 times Row 1 to Row 5

2	0	1	0	0
1	-33	-3	-44	-1
0	-42	5	-27	8
1	-163	-22	-124	17
1	-162	6	-139	0

10:Interchange Column 1 And Column 3

1	0	2	0	0
-3	-33	1	-44	-1
5	-42	0	-27	8
-22	-163	1	-124	17
6	-162	1	-139	0

11:Add -2 times Column 1 to Column 3

1	0	0	0	0
-3	-33	7	-44	-1
5	-42	-10	-27	8
-22	-163	45	-124	17
6	-162	-11	-139	0

Smith Normal Form

12:Add 3 times Row 1 to Row 2

1	0	0	0	0
0	-33	7	-44	-1
5	-42	-10	-27	8
-22	-163	45	-124	17
6	-162	-11	-139	0

13:Add -5 times Row 1 to Row 3

1	0	0	0	0
0	-33	7	-44	-1
0	-42	-10	-27	8
-22	-163	45	-124	17
6	-162	-11	-139	0

14:Add 22 times Row 1 to Row 4

1	0	0	0	0
0	-33	7	-44	-1
0	-42	-10	-27	8
0	-163	45	-124	17
6	-162	-11	-139	0

15:Add -6 times Row 1 to Row 5

1	0	0	0	0
0	-33	7	-44	-1
0	-42	-10	-27	8
0	-163	45	-124	17
0	-162	-11	-139	0

16:Interchange Column 2 And Column 5

1	0	0	0	0
0	-1	7	-44	-33
0	8	-10	-27	-42
0	17	45	-124	-163
0	0	-11	-139	-162

17:Add 7 times Column 2 to Column 3

1	0	0	0	0
0	-1	0	-44	-33
0	8	46	-27	-42
0	17	164	-124	-163
0	0	-11	-139	-162

Smith Normal Form

18:Add -44 times Column 2 to Column 4

1	0	0	0	0
0	-1	0	0	-33
0	8	46	-379	-42
0	17	164	-872	-163
0	0	-11	-139	-162

19:Add -33 times Column 2 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	8	46	-379	-306
0	17	164	-872	-724
0	0	-11	-139	-162

20:Add 8 times Row 2 to Row 3

1	0	0	0	0
0	-1	0	0	0
0	0	46	-379	-306
0	17	164	-872	-724
0	0	-11	-139	-162

21:Add 17 times Row 2 to Row 4

1	0	0	0	0
0	-1	0	0	0
0	0	46	-379	-306
0	0	164	-872	-724
0	0	-11	-139	-162

22:Interchange Row 3 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-11	-139	-162
0	0	164	-872	-724
0	0	46	-379	-306

23:Add -12 times Column 3 to Column 4

1	0	0	0	0
0	-1	0	0	0
0	0	-11	-7	-162
0	0	164	-2840	-724
0	0	46	-931	-306

Smith Normal Form

24:Add -14 times Column 3 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-11	-7	-8
0	0	164	-2840	-3020
0	0	46	-931	-950

25:Add 14 times Row 3 to Row 4

1	0	0	0	0
0	-1	0	0	0
0	0	-11	-7	-8
0	0	10	-2938	-3132
0	0	46	-931	-950

26:Add 4 times Row 3 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-11	-7	-8
0	0	10	-2938	-3132
0	0	2	-959	-982

27:Interchange Row 3 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	2	-959	-982
0	0	10	-2938	-3132
0	0	-11	-7	-8

28:Add 479 times Column 3 to Column 4

1	0	0	0	0
0	-1	0	0	0
0	0	2	-1	-982
0	0	10	1852	-3132
0	0	-11	-5276	-8

29:Add 491 times Column 3 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	2	-1	0
0	0	10	1852	1778
0	0	-11	-5276	-5409

Smith Normal Form

30:Add -5 times Row 3 to Row 4

1	0	0	0	0
0	-1	0	0	0
0	0	2	-1	0
0	0	0	1857	1778
0	0	-11	-5276	-5409

31:Add 5 times Row 3 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	2	-1	0
0	0	0	1857	1778
0	0	-1	-5281	-5409

32:Interchange Row 3 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	-5281	-5409
0	0	0	1857	1778
0	0	2	-1	0

33:Add -5281 times Column 3 to Column 4

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	-5409
0	0	0	1857	1778
0	0	2	-10563	0

34:Add -5409 times Column 3 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	1857	1778
0	0	2	-10563	-10818

35:Add 2 times Row 3 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	1857	1778
0	0	0	-10563	-10818

Smith Normal Form

36:Interchange Column 4 And Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	1778	1857
0	0	0	-10818	-10563

37:Add -1 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	1778	79
0	0	0	-10818	255

38:Add 6 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	1778	79
0	0	0	-150	729

39:Interchange Column 4 And Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	79	1778
0	0	0	729	-150

40:Add -22 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	79	40
0	0	0	729	-16188

41:Add -9 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	79	40
0	0	0	18	-16548

Smith Normal Form

42:Interchange Row 4 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	18	-16548
0	0	0	79	40

43:Add 919 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	18	-6
0	0	0	79	72641

44:Add -4 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	18	-6
0	0	0	7	72665

45:Interchange Column 4 And Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-6	18
0	0	0	72665	7

46:Add 3 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-6	0
0	0	0	72665	218002

47:Add 12110 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-6	0
0	0	0	5	218002

Smith Normal Form

48:Interchange Row 4 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	5	218002
0	0	0	-6	0

49:Add -43600 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	5	2
0	0	0	-6	261600

50:Add 1 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	5	2
0	0	0	-1	261602

51:Interchange Row 4 And Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-1	261602
0	0	0	5	2

52:Add 261602 times Column 4 to Column 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-1	0
0	0	0	5	1308012

53:Add 5 times Row 4 to Row 5

1	0	0	0	0
0	-1	0	0	0
0	0	-1	0	0
0	0	0	-1	0
0	0	0	0	1308012

Smith Normal Form is:

1	0	0	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	1308012

End time : 10:17:45.589 PM

Close

ملخص البحث

قمنا في هذا البحث بتجميع المعلومات الأساسية الهامة عن شكل سميث الإعتيادي , لما له من أهمية في بعض التطبيقات .

فعلي الرغم من عدم توفر الكتب و المراجع المختصة بهذا الموضوع , فقد بذ لنا قصار جهدنا في البحث و التنقيب من خلال القليل المتوفر من بعض أجزاء الكتب و الأوراق البحثية للحصول علي المعلومات الأساسية والهامة عن شكل سميث الإعتيادي ودراسة أحد تطبيقاته .

ولتوضيح فكرة هذا البحث بإيجاز قمنا بتجزئته إلي ثلاثة أبواب:

الباب الأول : وفيه تناولنا بعض التعاريف والنظريات الأساسية التي إعتمدنا عليها في موضوعنا الأساسي وهو شكل سميث الإعتيادي , مع التوضيح بأمثله كلما أمكن .

الباب الثاني: وخصص للتعريف بشكل سميث الإعتيادي وأهم نظرياته كإثبات وجوده و وحدانيته .

الباب الثالث : وفيه عرضنا أحد تطبيقات شكل سميث الإعتيادي وهو تمثيل كل زمرة تبديلية محدودة ومولدة بواسطة علاقة مصفوفات.

وكذلك قمنا بكتابة برنامج يحسب شكل سميث الإعتيادي بصورة سريعة ومختصرة.

References

[1] Adamson, Iain, Elementary Rings and Modules, 1972 by page bros.

[2] Adamson, Iain, Rings, Modules and Algebras, 1971 by page bros.

[3] Ash, Robert, Abstract algebra, 2000 by Robert B. Ash.

[4] Berberian, Sterling, Linear algebra, 1992 by Interprint Ltd.

[5] Burton, David, Abstract and linear algebra, 1972 by Addison-Wesley.

[6] Cohn, P.M., F.R.S, Algebra volume 1, 2nd Edition, 1982 by John Wiley & Sons Ltd.

[7] O'Connor, J J and Robertson, E F, www-groups.dcs.st-and.ac.uk/~history/Printonly/Smith.html.

[8] Dummit, David, and Foote, Richard, Abstract algebra, 1999 by Prentice-Hall, Inc.

[9] Herstein, I.N., Abstract algebra, 3rd Edition, 1996 by Prentice – Hall, Inc.

[10] Howard, Ralph, Rings, Determinants and The Smith Normal Form, and canonical forms for similarity of matrices, (2002).

[11] Jacobson, Nathan, Basic algebra I, 2nd Edition, 1985 by W. H. Freeman and Company.

[12] Morandi, Patrick, The Smith Normal Form of a matrix, (2005).

[13] Rayward-Smith, V. J., On Computing the Smith Normal Form of an integer Matrix, Vol.5, No.4, Page 451-456 (1979).

[14] Samelson, Hans, An introduction to linear algebra, 1974 by John Wiley & Sons, Inc.

[15] Sims, Charles, Abstract algebra, 1984 by John Wiley & Sons, Inc.

[16] Strang, Gilbert, Linear algebra and it's applications, 2nd Edition, 1980 by Academic Press, Inc.

كلية العلوم

قسم الرياضيات

عنوان البحث

بعض تطبيقات شكل سميث الاعتيادي

مقدمة من الطالب

مفتاح منصور الحاسي

** لجنة المناقشة :

1 – د. شعبان علي طرينه ....
(مشرفاً)

2 – د. أمير عبد المجيد جاسم ....
(ممتحناً داخلياً)

3 – د. علي أحمد ضو ....
(ممتحناً خارجياً)

يعتمد

د. احمد فرج المحجوب

أمين اللجنة الشعبية لكلية العلوم

جامعــة التحــدى

كلية العــلوم

بعض تطبيقات شكل سميث الإعتيادى

هذه الرسالة مقدمة لقسم الرياضيات كمتطلب جزئي للحصول على
درجة الماجستير فى علوم الرياضيات

مقدمه من الطالب :مفتاح منصور أحمد الحاسى

الرقم الدراسي : (032313)

إشراف الدكتور : شعبان على طرينه

العام الجامعى 2007 – 2008