Chapter 3
Rings defined by matrix canonical forms

3.1 Hermite and elementary divisor rings

In this section we assume that R is always a commutative ring with nontrivial identity. The following few definitions are given in a possibly noncommutative setting.

Definition 3.1. It is said that matrices A and B over a ring R are *equivalent* ($A \sim B$) if there are invertible matrices P and Q over the ring R of appropriate sizes such that $A = PBQ$. We say that a matrix A over a ring R admits a *canonical diagonal reduction* if it is equivalent to a diagonal matrix

$$\begin{pmatrix} \varepsilon_1 & 0 & \dots & 0 & 0 & \dots 0 \\ 0 & \varepsilon_2 & \dots & 0 & 0 & \dots 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\ 0 & 0 & \dots & \varepsilon_r & 0 & \dots 0 \\ 0 & 0 & \dots & 0 & 0 & \dots 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots 0 \end{pmatrix}$$

where $\varepsilon_{i+1}R \subset \varepsilon_i R$ for any $i \in \{1, \dots, r-1\}$. If every matrix over a ring R admits a canonical diagonal reduction then R is said to be an *elementary divisor ring*. If every 1×2 (2×1) matrix over R admits a canonical diagonal reduction then it is said that R is a *right (left) Hermite ring*. It is clear that in the case of commutative rings every right Hermite ring it is a left Hermite and we simply call them as the *Hermite rings*.

Remark 3.1. Let R be an Hermite ring. Then for any elements $a, b \in R$ exists an invertible 2×2 matrix P and there exists an element $d \in R$ such that

$$(a,b)P = (d,0).$$

Suppose that

$$P = \begin{pmatrix} x & u \\ y & v \end{pmatrix} \quad \text{and} \quad P^{-1} = \begin{pmatrix} a_1 & b_1 \\ r & s \end{pmatrix}.$$

Then $ax+by=d$, $a=da_1$, $b=db_1$, $a_1R+b_1R=R$ and $aR+bR=dR$, i.e. R is a Bezout ring.

Theorem 3.1. *(**Henriksen's criterion**) [25] A commutative Bezout ring R is an Hermite ring if and only if for any elements $a,b \in R$ there exist $d,a_1,b_1 \in R$ such that $a=a_1d$, $b=b_1d$, $a_1R+b_1R=R$.*

Proof. Due to the remark preceding this theorem it remains to show that if for any elements $a,b \in R$ there are $a_1,b_1,d \in R$ such that $a_1R+b_1R=R$, $a=a_1d$, $b=b_1d$ then R is an Hermite ring.

Let $a_1s+b_1t=1$ for some elements $s,t \in R$. Then matrix

$$Q = \begin{pmatrix} s & -b_1 \\ t & a_1 \end{pmatrix}$$

is invertible and $(a,b)Q=(d,0)$. □

Theorem 3.2. *A commutative Bezout ring R is an Hermite ring if and only if* $\text{st.r.}(R)=2$.

Proof. Let R be an Hermite ring and let $aR+bR+cR=R$. Let $d \in R$ be such element that $aR+bR=dR$. Then by Theorem 3.1 $a=a_1d$, $b=b_1d$ and $a_1u+b_1v=1$ for some $u,v,a_1,b_1 \in R$. Since $aR+bR+cR=R$ then $dR+cR=R$. Let's prove that

$$(a+vc)R+(b-uc)R=R.$$

Note that

$$(a+cv)u+(b-cu)v=au+bv=d$$

and

$$(a+vc)b_1+(b-uc)(-a_1)=c(a_1u+b_1v)=c$$

i.e. $d,c \in (a+vc)R+(b-uc)R$. Since $dR+cR=R$ we conclude that

$$(a+vc)R+(b-uc)=R$$

that was desired.

It remains to prove that a commutative Bezout ring of stable range 2 is an Hermite ring. Let a,b be arbitrary elements of a ring R. Since R is a Bezout ring

$aR+bR=dR$ for a some $d\in R$. Then there exist elements $u,v,a_1,b_1\in R$ such that $au+bv=d$, $a=a_1d$, $b=b_1d$. Let $c_1=1-a_1u-b_1v$. Then $dc_1=0$ and $a_1R+b_1R+c_1R=R$.

Since R is a ring of stable range 2 then there exist elements $x,y\in R$ such that

$$(a_1+xc_1)R+(b_1+yc_1)R=R.$$

Hence $(a_1+xc_1)k+(b_1+yc_1)t=1$ for certain $k,t\in R$. It is clear that the matrix

$$P=\begin{pmatrix} a_1+xc_1 & b_1+yc_1 \\ -t & k \end{pmatrix}$$

is invertible and $(a,b)P^{-1}=(d,0)$, i.e. R is Hermite ring. Theorem is proved. □

Theorem 3.3. *[39] Let R be a commutative ring. If all 1×2, 2×1 and 2×2 matrices over R admit a canonical diagonal reduction then R is an elementary divisor ring.*

Proof. Let A be an $m\times n$ matrix. Assume that $m\geq n$. By induction we can suppose that we know a canonical diagonal reduction to be possible for all matrices of size $k\times l$, where $\min\{k\times l\}\leq m$. Due to the assumption in the statement of theorem we can suppose that $m\geq 3$. Write A_1 for the first row of A and A_2 for the remained $m-1$ rows. We can find invertible matrices P_1,Q_1 such that

$$B=P_1A_2Q_1=\operatorname{diag}(x,\ldots).$$

Then also

$$C=\begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix}\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}Q_1=\begin{pmatrix} A_1Q_1 \\ B \end{pmatrix}.$$

Now write D for the first two rows of C and E for the remainder.

Applying the induction again we diagonalize matrix D:

$$F=P_2DQ_2=\operatorname{diag}(y,\ldots).$$

Then

$$H=\begin{pmatrix} P_2 & 0 \\ 0 & I_{m-2} \end{pmatrix}\begin{pmatrix} D \\ E \end{pmatrix}Q_2=\begin{pmatrix} F \\ G \end{pmatrix}.$$

Since y is a divisor of all elements of F then it is also a divisor of all elements of D as follows form

$$D=P_2^{-1}FQ_2^{-1}.$$

In particular, y is a divisor of x. The latter is one of the elements of D. The elements of G are linear combinations of those of E_1, and hence they are divisible by x and so by y. Thus y is a divisor of every element of H. We may now use elementary transformation to sweep out the first column of H and we obtain

$$\begin{pmatrix} y & 0 \\ 0 & K \end{pmatrix},$$

where y is still a divisor of every element of K. Applying induction to K we complete the reduction. Theorem is proved. □

As a consequence we have the following result.

Theorem 3.4. *Let R be a commutative Hermite ring. Then the following statement are equivalent:*

1. R is an elementary divisor ring;

2. Every matrix

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix},$$

where $aR + bR + cR = R$, admits a canonical diagonal reduction.

Proof. By Theorem 3.3 it is enough to prove that any 2×2 matrix admits a canonical diagonal reduction, assuming that (2) holds.

Let A be an 2×2 matrix over R. Since R is an Hermite ring then there exists an invertible matrix Q over R such that

$$AQ = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}.$$

Let $aR + bR + cR = dR$. Since R is an Hermite ring we have $a = da_1$, $b = db_1$, $c = dc_1$, where $a_1R + b_1R + c_1R = R$ for some elements $a_1, b_1, c_1 \in R$. Then

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix}.$$

Since

$$\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}$$

is a matrix that commutes with any 2×2 matrix over R the matrix

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

admits a canonical diagonal reduction if and only if the matrix

$$\begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix}$$

admits a canonical diagonal reduction, as was desired. □

The following theorem can be viewed as a criterion for the commutative Bezout rings in terms of matrix diagonalization.

Theorem 3.5. *[43] Any diagonal matrix over a commutative ring R admits a canonical diagonal reduction if and only if R is a Bezout ring.*

Proof. If for any elements $a, b \in R$ the matrix

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

admits a canonical diagonal reduction

$$P \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} Q = \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix},$$

where P, Q are invertible 2×2 matrices of order 2 and d divides e, then

$$aR + bR = dR + eR = dR,$$

so that R is a Bezout ring.

To establish the converse let R be a Bezout ring and we use the induction on m show to that any diagonal m by n matrix A admits the canonical diagonal reduction. The case $m = 1$ is straightforward. If $m > 1$ we can write

$$A = \begin{pmatrix} a & 0 \\ 0 & A_1 \end{pmatrix},$$

where A_1 is an $m-1$ by $n-1$ diagonal matrix. By the induction hypothesis A_1 admits a canonical diagonal reduction

$$P_1 A Q_1 = \begin{pmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

where P_1, Q_1 are invertible matrices.

Note that if $dR = aR + c_1R$ then there are $u, v, a_1, c \in R$ such that

$$d = ua + vc_1, \quad a = a_1 d, \quad c_1 = cd.$$

Then using the elementary rows and columns transformations we obtain the equivalences

$$\begin{pmatrix} a & 0 \\ 0 & c_1 \end{pmatrix} \sim \begin{pmatrix} a & ua + vc_1 \\ 0 & c_1 \end{pmatrix} \sim \begin{pmatrix} d & a \\ c_1 & 0 \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & a_1 c_1 \end{pmatrix}.$$

Hence

$$A \sim \begin{pmatrix} d & 0 & 0 & \dots & 0 \\ 0 & a_1 c_1 & 0 & \dots & 0 \\ 0 & 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Since d divides c_1, d must divide all the diagonal entries. Applying the induction we obtain a desired property. Theorem is proved. □

Theorem 3.6. *(**Kaplansky criterion**) [39, 25] A commutative Hermite ring is an elementary divisor ring if and only if $aR + bR + cR = R$ and there exist elements p, q such that $paR + (pb + qc)R = R$.*

Proof. Let

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

and suppose PAQ effects the canonical diagonal reduction of A. Since $aR + bR + cR = R$ it is clear that PAQ has a unit u in its upper left corner. Suppose the first row of P consists of p, q and the first column of Q consists of x, y. Then

$$pax + pby + qcy = u$$

whence

$$paR + (pb + qc)R = R.$$

To prove the sufficiency we assume that R is an Hermite ring. Given any nonzero 2 by 2 matrix, we may thus arrange to get a zero say in the lower left corner. We thus obtain the matrix A of the form obtain

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

Since R is a Bezout ring there are $x, y, z, a_1, b_1, c_1 \in R$ such that

$$aR + bR + cR = dR,$$

$$d = xa + yb + zx,$$

$$a = a_1 d, \;\; b = b_1 d, \;\; c = c_1 d.$$

We have excluded the case $d = 0$ and thus we can suppose that

$$xa_1 + yb_1 + zc_1$$

is a unit. Let

$$paR + (pb + qc)R = R,$$

observe that necessary $pR + qR = R$, complete the row p, q to a invertible matrix, and use it to left-multiply A. The results is a matrix with pa, $pb + qc$ for its first row. Right multiplication by a suitable invertible matrix converts this to $1, 0$. We sweep out the element in the lower left corner and thus complete the reduction. Theorem is proved. □

Kaplansky [39] proved that for an adequate ring being an Hermite ring is equivalent to an elementary divisor ring condition.

By Theorems 4.4 and 3.2 we have the following result.

Theorem 3.7. *A commutative adequate Bezout ring is an Hermite ring.*

By Theorems 3.5 and 3.7 we obtain:

Theorem 3.8. *A commutative adequate ring is an elementary divisor ring if and only if it is a Bezout ring.*

3.2 Bezout rings and Shores test

3.3 Stable range and matrix diagonalization

3.4 Pullbacks and D+M-construction

Pullbacks plays an important role in the commutative ring theory as a great source of examples and counter examples.

In this section using the pullback construction we will build new examples of commutative Bezout domains.

Let A, B, C be some commutative rings and $\alpha : A \to C$, $\beta : B \to C$ are ring homomorphism.

Definition 3.2. A commutative ring R together with ring homomorphisms $f : R \to A$ and $g : R \to B$ is called a *pullback* of the pair of homomorphisms $\alpha : R \to C$ and $\beta : B \to C$ if the diagram

$$\begin{array}{ccc} R & \xrightarrow{g} & B \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \beta} \\ A & \xrightarrow{\alpha} & C \end{array}$$

commutes and for any commutative ring R' with ring homomorphism $g' : R' \to B$, $f' : R' \to A$ such that $\alpha f' = \beta g'$ there is a ring homomorphism $h : R' \to R$ such that $gh = g'$ and $fh = f'$.

Definition 3.3. Houston and Taylor [35] have introduced a *pullback of type* $\square$ in a following way. Let I be a nonzero ideal of the commutative domain T and $\phi : T \to T/I = E$ be the natural surjection and D be a commutative domain inside E. Then the commutative domain $R = \phi^{-1}(D)$ arises as a pullback of the following diagram

$$\begin{array}{ccc} R = \phi^{-1}(D) & \longrightarrow & D \\ \downarrow & & \downarrow \\ T & \longrightarrow & T/I = E \end{array}$$

It is worth to note that $R \subseteq T$ and $D \subseteq E$.

Definition 3.4. Boynton [4] has introduced the pullback in another way. Let $R \subseteq T$ be any commutative ring extension and I is the nonzero *conductor ideal* of T into R, i.e. suppose that R and T have a common nonzero ideal, and we call the largest nonzero common ideal I as a conductor of T in R. Taking $D = R/I$ and $E = T/I$ we obtain the natural surjection $\eta_1 : T \to E$, $\eta_2 : R \to D$ and the inclusions $i_1 : D \to E$, $i_2 : R \to T$. These maps yield a commutative diagram that is called a *conductor square* $\square$ which defines R as a pullback on η_1 and i_2:

$$\begin{array}{ccc} R & \xrightarrow{i_2} & T \\ {\scriptstyle \eta_1}\downarrow & & \downarrow{\scriptstyle \eta_2} \\ D & \xrightarrow{i_1} & E \end{array}$$

Remark 3.2. Every conductor square $\square$ is a pullback of type $\square$. If in the conductor square $\square$ there is an inclusion of domains $R \subseteq T$ then T is always an over ring of R.

Example 3.1. Let $T = \mathbb{Q}[x]$. Taking $I = x\mathbb{Q}[x]$ we obtain $T/I \cong \mathbb{Q}$. Furthermore, $\mathbb{Z} \cong \{a+I | a \in \mathbb{Z}\} = D \subset T/I$. As the homomorphism

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}[x]/x\mathbb{Q}[x] \cong \mathbb{Q}$$

is a surjection we can consider a domain R as a pullback of type $\square$:

$$R = \phi^{-1}(D) = \phi^{-1}\{a+I | a \in \mathbb{Z}\} = \{h(0) \in \mathbb{Q}[x] : h(x) \in \mathbb{Z}\}.$$

This implies that $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x] = T$. Hence we obtain the following commutative diagram

$$\begin{array}{ccc} R = \phi^{-1}(D) & \longrightarrow & D \\ \downarrow & & \downarrow \\ T & \longrightarrow & T/I = E \end{array}$$

As $\mathbb{Z}$ and $\mathbb{Q}[x]$ are Bezout domains and I is a maximal ideal of T, so $R = \mathbb{Z} + x\mathbb{Q}[x]$ is also a Bezout domain [35].

Denote by $U(D)$ the group of units of a domain D. Given a pullback of type $\square$ the ring homomorphism $\phi : T \to E$ restricts to a group homomorphism

$$g : U(T) \to U(E).$$

As $U(D)$ is a subgroup of $U(E)$ we have a canonical homomorphism

$$\beta : U(E) \to U(E)/U(D).$$

Taking a composition $h = \beta g$ we obtain a homomorphism

$$\phi : U(T) \to U(E)/U(D).$$

Corollary 3.1. *Consider a pullback of type $\square$ in which I is a maximal ideal of T. Then R is a Bezout domain if and only if E is the quotient field of D, D and T are Bezout domains and the natural map*

$$U(T) \to U(E)/U(D)$$

is onto.

Definition 3.5. Let D be a commutative domain which quotient field K and $E \subseteq D$ a subset of D. Denote by

$$\mathrm{End}(E,D) = \{f(x) \in K[x] \mid f(x) \in D \text{ for every } x \in E\}$$

the ring of D-valued polynomials on K with respect to the subset E. If a two-generated ideal I of a ring R has the property that the first of its generators can be chosen randomly from the set of nonzero elements of I then I is called *strongly two-generated ideal*.

A ring in which each two-generated ideal is strongly two-generated is said to be the ring with the *strongly two-generated property*.

Theorem 3.9. *Let R be a commutative domain and $E = \{e_1, \ldots, e_k\}$ a finite nonempty subset of D. Then* $\mathrm{End}(E,D)$ *has the strongly two-generated property if and only if D is a Bezout domain.*

Theorem 3.10. *Suppose that D is a commutative domain and*

$$E = \{e_1, \ldots, e_k\}$$

is nonempty finite subset. Suppose also that D is a Bezout domain that is not a field. Then $\mathrm{End}(E,D)$ *is a Bezout domain if and only if $|E| = 1$.*

Example 3.2. Let $T = \mathbb{Q}[x]$ and $C = \mathbb{Q}[x](x^2+1)$. Consider a quotient-ring

$$B = T/C \cong \mathbb{Q}[i]$$

and $A = \mathbb{Z}[i]$. It is well-known that the ring $\mathbb{Z}[i]$ of the Gaussian integer is a PID and hence it is a Bezout domain.

By Theorem 3.10 the ring

$$R = \{g \in \mathbb{Q}[x] \mid g(i) \in \mathbb{Z}[i]\}$$

is a Bezout domain.

It is known that

$$\mathrm{End}(E,D) = \{f(x) \in K[x] \mid f(e) \in D \text{ for all } e \in E\}$$

is not atomic [57]. Then

$$R = \{g \in \mathbb{Q}[x] \mid g(i) \in \mathbb{Z}[i]\}$$

is a Bezout domain that is not a PID as every PID is atomic.