§1. Hermite Normal Form.

Hermite [4] had proved that any matrix $A$ with rational integral entries and having the same rank as its number of columns can be (lower) triangularized on multiplication by a unimodular matrix on the left.

In this Chapter, we prove a corresponding result in the case of arbitrary Dedekind domains (Theorem 3.1.6). The triangular form is not unique, without further restrictions, even in the special case of rational integers $\mathbb{Z}$. For non-singular matrices over $\mathbb{Z}$, we make it unique by insisting that the diagonal entries $t_{jj}$ be positive and the entries in the $j$th column below $t_{jj}$ be restricted to a fixed residue system modulo $t_{jj}$ (Hermite normal form). In the general case under consideration, we prove a similar result (Theorem 3.1.9 and Theorem 3.1.10).

We have stated all the theorems together in §1.1, since they are closely interlinked. These have been proved in §1.2.
In the course of the proofs, we develop a sort of 'Division Algorithm' on matrices (Lemma 3.1.14).

In §2, we show as an application that the problem of finding right divisor classes of matrices can be reduced to that of finding 'generalized triangular divisors' of generalized diagonal matrices. We also show that in case the Dedekind domain \( \mathcal{O} \) has the additional property that the number of elements in \( \mathcal{O}/\alpha \) is finite for every integral ideal \( \alpha \), then the number \( d(A) \) of divisor classes of a given matrix \( A \) is finite. We obtain this number explicitly in case \( A \) is of rank 1. We also give an upper bound on a lower bound on \( d(A) \) in the general case. Finally, we evaluate \( d(A) \) in some special cases.

The results in this chapter are from a paper by the author submitted for publication.

§1.1. Statement Of The Main Results.

Let \( \mathcal{O} \) be a Dedekind domain and let \( k \) be the field of quotients of \( \mathcal{O} \). We recall Definition 2.3.5 and Remark 2.3.7.

(Definition 2.3.5) Two matrices \( A_1 \) and \( A_2 \) in \( k \) with the same
number of columns will be called **left equivalent in** \( \mathcal{S} \) (notation: \( A_1 \sim L A_2 \)) if there exist integral matrices \( U_1 \) and \( U_2 \) satisfying

\[
A_1 = U_2 A_2 ,
\]

and

\[
A_2 = U_1 A_1 .
\]

(Adámek 2.3.7). Two matrices \( A_1 \) and \( A_2 \) in \( k \) with the same number of columns are left equivalent in \( \mathcal{S} \) if and only if there exists a primitive, reduced matrix \( U_2 \), which is \( G \)-reduced on the right, \( G \) being a left unit of \( A_2 \); and satisfies

\[
A_1 = U_2 A_2 .
\]

**NOTATION 3.1.1.** An equivalence class of left equivalent matrices will be called, after Siegel [10], a 'left ray'.

**DEFINITION 3.1.2.** Let \( B \) be a non-zero integral matrix. For integral matrices \( A_1 \) and \( A_2 \), we shall say that \( A_1 \) is congruent to \( A_2 \) modulo \( B \) (notation: \( A_1 \equiv A_2 \pmod{B} \)) if there exists an integral matrix \( X \) such that \( A_1 - A_2 = XB \).

**NOTATION 3.1.3.** An equivalence class determined by the equivalence relation defined in Definition 3.1.2 will be called
a congruence class modulo $B$. (This should perhaps be called a left congruence class modulo $B$, but we do not use right congruences and so we omit the prefix 'left').

**Definition 3.1.4.** Let $T$ be a non-zero integral matrix and let $C$ be any matrix in $k$. By a $C$-reduced congruence class modulo $B$, we shall mean the subclass of congruence class modulo $B$ consisting of matrices which are $C$-reduced on the left.

**Definition 3.1.5.** A matrix $T = (T_{ij})$ where each $T_{ij}$ is a matrix of rank $\leq 1$ and $T_{ij} = 0$ for $j > i$ will be called a generalized (lower) triangular matrix.

We give below four theorems. Theorem 3.1.6 states that there is a generalized triangular matrix in the equivalence class of left equivalent matrices having the same rank as the number of columns. Theorem 3.1.9 says that a 'normal' choice is possible. Theorem 3.1.10 shows the extent to which the normalised choice is unique. Theorem 3.1.11 is another version of the three theorems in a form we use in the applications in §2.

**Theorem 3.1.6.** If $A^{(m|k)}$ is an integral matrix of rank $n$,
then there exists a generalized triangular matrix
\( T(\mathbb{C}, n) = (T_{ij}) \) left equivalent to \( A \) and satisfying

(i) Each \( T_{ij} \) is a 2 x 1 matrix,

(ii) Each \( T_{jj} \) is of rank 1, and

(iii) \( T \) has \( n \) dependent pairs of rows.

**Notation 3.1.7.** Let \( \Phi \) denote a complete set of representatives of left rank-1 matrices. Let \( B \) be a non-zero integral matrix of rank 1 and let \( C \) be any matrix in \( k \). Let \( \Phi(B, C) \) denote a complete set of representatives of \( C \)-reduced congruence classes modulo \( B \).

**Definition 3.1.8.** Let \( T = (T_{ij}) \) be a generalized triangular matrix such that each \( T_{jj} \) is of rank 1. Let \( C_j \) be a left unit of \( T_{jj} \). We say that \( T \) is in the (generalized) Hermite normal form (referred to fixed representative systems \( \Phi \) and \( \Psi \)) if the following conditions are satisfied:

\[
\begin{align*}
(1) & \quad T_{jj} \in \Phi \quad \text{for } 1 \leq j \leq n, \\
(2) & \quad T_{ij} \in \Psi \left( T_{jj}, C_j \right) \quad \text{for each } 1 \leq j < i \leq n.
\end{align*}
\]

**Theorem 3.1.9.** Let the notation be as in Theorem 3.1.6.
For each $j$, $1 \leq j \leq n$, fix a left unit $G_j$ of $T_{jj}$. The matrix $T$ may then be chosen in the Hermite normal form. (hereafter abbreviated H.N.F.).

**Theorem 3.1.10.** Let $A(\mathbb{Z},n)$ be an integral matrix of rank $n$. Let $R(\mathbb{Z},n)$ be $S(\mathbb{Z},n)$ be two matrices left equivalent to $A$, and let both $R$ and $S$ be in H.N.F. referred to the same representative systems $\Phi$ and $\Psi$. Then $R = S$.

**Theorem 3.1.11.** If $A(\mathbb{Z},n)$ is an integral matrix of rank $n$ having $n$ dependent pairs of columns, then there is a generalized triangular matrix $T(\mathbb{Z},n) = (T_{ij})$ left equivalent to $A$ and satisfying

1. Each $T_{ij}$ is a $2 \times 2$ matrix,
2. Each $T_{jj}$ is of rank 1,
3. $T$ has $n$ dependent pairs of rows and $n$ dependent pairs of columns.

Further, fixing left units $G_j$ of $T_{jj}$, we may choose $T$ in H.N.F. Finally, with these fixed choices the H.N.F. is unique.
§1.2. The Proofs.

In the proof of Theorem 3.1.6 and later we shall use the following:

Remark 3.1.12. Let $A$ and $B$ be any matrices in $k$. Suppose there exists a left unit $C$ of $B$ satisfying $AC = A$. If $Y$ is a matrix satisfying $BY = C$, then $AB = X$ implies that $XY = A$. If, in particular $X = 0$, then $AB = 0$ implies that $A = 0$.

Proof of Theorem 3.1.6. We note at the outset that the rank of the matrix $A$ is the same as its number of columns.

Let $K$ be any separable extension of $k$ of degree $n = r(i)$. Given the matrix $A$, we use Proposition 2.1.13 to find lattices $K$ and $L$ with generators $\beta_1, \ldots, \beta_m$ and $\alpha_1, \ldots, \alpha_n$ respectively such that $A$ is the corresponding Lattice matrix of $k$ with respect to $L$. Thus,

\[ \beta = A \alpha. \]  

(2)

Since $\alpha_1, \ldots, \alpha_n$ is a base of $K/k$ and $K$ is a lattice on $K$, there exists (see [8], Theorem 81:3) a base $\gamma_1, \ldots, \gamma_n$ of $K/k$ with

$\gamma_j \in k \alpha_1 + \cdots + k \alpha_j$, for $1 \leq j \leq n$;
and there are non-zero ideals \( \mathcal{M}_1, \ldots, \mathcal{M}_n \) in \( k \) such that

\[
\mathcal{N} = \mathcal{M}_1 y_1 + \ldots + \mathcal{M}_n y_n.
\]

It follows, therefore, that we have

\[
\gamma = T^* \alpha
\]

where

\[
T^* = \begin{pmatrix}
t_{11} & 0 & \ldots & 0 \\
t_{21} & t_{22} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
t_{n1} & t_{n2} & \ldots & t_{nn}
\end{pmatrix}
\]

is a lower triangular matrix in \( k \). Since \( \mathcal{O} \) is a Dedekind domain, let \( \mathcal{M}_i = \mathcal{O} a_i + \mathcal{O} b_i \) for \( 1 \leq i \leq n \). Then

\[
\mathcal{N} = \mathcal{O} \zeta_1 + \mathcal{O} \gamma_1 + \ldots + \mathcal{O} \zeta_n + \mathcal{O} \gamma_n,
\]

where \( \zeta_1 = \gamma_1 a_1 \) and \( \gamma_1 = \gamma_1 b_1 \). Thus,
\[ \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = \begin{pmatrix} t_{11} a_1 & 0 & \cdots & 0 \\ t_{12} b_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{1n} a_n & t_{2n} a_n & \cdots & t_{nn} a_n \\ t_{1n} b_n & t_{2n} b_n & \cdots & t_{nn} b_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = T \alpha, \text{ say.} \]

Since \( \xi_1, \xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n \) are two sets of generators of \( M \), there exists a primitive matrix \( U \) such that

\[ \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = U \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = UA \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}; \text{ using (2).} \]

Consequently, \( UA \alpha = T \alpha \). Now, since the matrices \( UA \) and \( T \) are in \( k \), we have

\[ UAW = TW, \]
where

$$W = \begin{pmatrix}
\alpha_1(1) & \cdots & \alpha_1(n) \\
\vdots & \ddots & \vdots \\
\alpha_n(1) & \cdots & \alpha_n(n)
\end{pmatrix}$$

$$\alpha_1 = \alpha_1(1), \ldots, \alpha_1(n)$$ being conjugates of $$\alpha_1$$ over $$k$$.

Notice that $$r(W) = n$$, the extension $$K/k$$ being separable.

Hence the n-rowed identity matrix $$W(n)$$ is a left unit of $$W$$ so that there exists $$X = W^{-1}$$ satisfying $$WX = E(n)$$. Thus $$U \ A = T$$, in view of Remark 3.1.12.

Also, we may assume, as usual, that $$U$$ and $$A$$ have a common unit (Recall 1.9). Thus, $$A$$ is left equivalent to

$$T = (T_{ij})$$ where $$T_{ij}$$ is the $$2 \times 1$$ matrix $$\begin{pmatrix} t_{ij} & a_i \\ t_{ij} & b_i \end{pmatrix}$$ for $$i \geq j$$,

and the null matrix otherwise. Clearly, this $$T$$ is of the desired kind; and hence the theorem is proved.

Remark 3.1.13. It is easy to see that the restriction '$$A$$ is integral' is not necessary in the above theorem. (Theorem 3.1.6).
For use in the proof of Theorem 3.1.9, we first prove a lemma which gives a sort of 'Division Algorithm'. We are unable however to obtain counterpart of the remainder being 'smaller' than the dividend. This lemma may be of independent interest.

Lemma 3.1.14. Let \( A = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \) and \( B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \) be integral matrices of rank 1. Let \( C \) and \( D \) be left units of \( A \) and \( B \) respectively. We can find a \( C, D \)-reduced integral matrix \( (2, 2)^{-1} \) of rank 1 satisfying

\[
A = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} + R
\]

where \( R^{(2, 1)} \) is integral and \( C R = R \). Moreover, fixing \( R \) in \( \Psi(2, C) \) (Recall Notation 3.1.7, Page 85) fixes \( Q \).

PROOF. Suppose that

\[
C = \begin{pmatrix} c_1 & c_2 \\ \mu c_1 & \mu c_2 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} d_1 & \lambda d_1 \\ d_2 & \lambda d_2 \end{pmatrix}
\]

Choose an integral \( x \) such that \( \mu x, \lambda x \) and \( \lambda \mu x \) are integral and set
Clearly Q is integral and \( r(Q) = 1 \). Since \( C^2 = C \) (Recall 1.5), we have,

\[
Q = \begin{pmatrix}
x & \lambda x \\
\mu x & \lambda \mu x
\end{pmatrix}.
\]

which gives that \( c_1 + \mu c_2 = 1 \). It follows therefore that \( C Q = Q \). Similarly \( Q D = Q \). Thus \( Q \) is \( C, D \)-reduced and we define \( R = A - Q B \) to get (3).

Now, if \( A = Q_1 B + R_1 \) with \( C, D \)-reduced integral matrix \( Q_1 \) of rank 1, then \( R \equiv R_1 \mod B \). Thus, since \( R \) and \( R_1 \in \mathcal{Y}(B, C) \), we have \( R = R_1 \). Hence \( (Q - Q_1) B = 0 \) and using Remark 3.1.12, we conclude that \( Q - Q_1 = 0 \).

**Proof of Theorem 3.1.9.** We now show how a matrix left equivalent to the matrix \( T \) of Theorem 3.1.6 satisfying the
additional condition (1) of Definition 3.1.8 can be obtained.

We observe first of all that multiplying $T$ on the left by $V = \text{diag } [V_1, \ldots, V_n]$ changes $T_{jj}$ to $V_j T_{jj}$. It is thus possible to choose $T$ in such a way that for every $j$, $T_{jj} \in \Phi$.

We now show how $T_{ij} (1 > j)$ are to be chosen in $\Psi(T_{jj}, C_1)$. This is done by induction; starting from $j = n - 1$ we come down to $j = 1$. If $T_{n, n-1} = 0$, we make no change. Otherwise, $r(T_{n, n-1}) = 1$ and using Lemma 3.1.14, we find a $C_n : C_{n-1}$-reduced integral matrix $Q_{n, n-1}$ of rank 1 and $C_n$-reduced matrix $R_{n, n-1}$ such that

$$T_{n, n-1} = Q_{n, n-1} T_{n, n} + R_{n, n-1}.$$ 

Let $C = \text{diag } [C_1, \ldots, C_n]$. Then, the multiplication of $T$ on the left by the $2n \times 2n$ primitive, right $C$-reduced matrix $W(n, n-1) = W = (W_{rs})$ (say) defined by

$$W_{rs} = \begin{cases} 
C_s & \text{if } r = s \\
- Q_{n, n-1} & \text{if } r = n, s = n - 1 \\
0 & \text{otherwise}
\end{cases}$$
has the effect of changing \( T_{n-1} \) to

\[
T_{n-1} \to T_{n-1} T_{n-1} \n^{-1} \n^{-1}
\]

while the rest of the entries in the \((n-1)\)th column and all the entries in the \(n\)th column of \( T \) remain unchanged. Thus, it is possible to choose \( T \) in such a way that \( T_{n-1} \) is in \( \n (T_{n-1} n^{-1}, n) \).

Let us now assume that for each \( i \) and \( j, j > t \) and \( i > j, T_{ij} \) have already been chosen to lie in \( \n (T_{ij}, n) \).

We show how \( T \) must be altered now to get each \( T_{it} \) satisfying the requirements of the theorem. If \( T_{it} = 0 \), we make no change. Otherwise \( r(T_{it}) = 1 \). We first observe that the multiplication of \( T \) on the left by the primitive, right \( n \)-reduced matrix

\[
W(i, t) = (W_{rs}) \quad \text{(say)}
\]

defined by

\[
W_{rs} = \begin{cases} 
C_s & \text{if } r = s \\
-a_{it} & \text{if } r = i, s = t \\
0 & \text{otherwise}
\end{cases}
\]

changes \( T_{it} \) to \( (T_{it} - a_{it} T_{tt} \), while the entries fixed
earlier (i.e. corresponding to \( j > t \)) remain unaltered. But, by Lemma 3.1.14, we can choose \( \xi_t \) suitably to get a matrix \( T_t \) of the desired kind. The induction is thus complete.

**Proof of Theorem 3.1.10.** Let \( R^{(2n,n)} = (R_{ij}) \) and \( S^{(2n,n)} = (S_{ij}) \) be generalized triangular matrices with \( n \) dependent pairs of rows. Let \( R_{ij} \) and \( S_{ij} \) be \( 2 \times 1 \) matrices and let \( r(R_{jj}) = r(S_{jj}) = 1 \). Further, let \( R \) be left equivalent to \( S \). We first show that for each \( j \), \( R_{jj} \sim_L S_{jj} \).

Let \( R = U \cdot S \) with a primitive matrix \( U \). Since \( S \) has \( n \) dependent pairs of rows, a left unit \( C \) of \( S \) may be chosen in the form \( \text{diag} \left[ C_1, \ldots, C_n \right] \). Taking \( U \cdot C \) instead of \( U \), we may assume that \( U \cdot C = U \). Find \( X \) satisfying \( S \cdot X = C \) (by 1.14). It is easily seen that \( X \) is a generalized triangular matrix and hence so is \( U = R \cdot X \). It follows, therefore, that

\[
\mathcal{O} = \delta(U) = \prod_{j=1}^{n} \delta(U_{jj}) \text{, using 1.19 ;}
\]

and consequently the rank 1 matrices \( U_{jj} \) are primitive. Now, since \( R_{jj} = U_{jj} \cdot S_{jj} \) and \( C_j \) is a common unit between \( U_{jj} \) and \( S_{jj} \), it follows that for each \( j \), \( R_{jj} \sim_L S_{jj} \).

Now let \( R \) and \( S \) be matrices in the H.N.P. with a fixed system \( \Phi \), and left equivalent to \( A \). Since \( R_{jj} \sim_L S_{jj} \),
it follows that $R_{ij} = S_{jj}$.

Thus, all the matrices $R_{ij}$ and $S_{ij}$ for $i \neq j$ may be chosen from a fixed system $\Psi$.

In order to prove the uniqueness, we show that $U = C$.

Since $S_{jj} = R_{jj} = U_{jj} S_{jj}$; $U_{jj}$ is a left unit of $S_{jj}$ and thus $U_{jj} C_j = C_j$ by 1.4. But $U C = U$ implies that $U_{jj} C_j = U_{jj}$. Thus $U_{jj} = C_j$ for each $j$, $1 \leq j \leq n$.

It remains to show, therefore, that for $i > j$, $U_{ij} = 0$.

Suppose $2 \leq t \leq n$. Then, $R = U S$ gives

$$R_t = U_t S_{t-1} t-1 + U tt S_t t-1.$$ 

$$= U_t t-1 S_{t-1} t-1 + S_t t-1;$$ since $U tt = C_t$

i.e. $R_t t-1 \equiv S_t t-1 \pmod{S_{t-1} t-1}$,

and hence $R_t t-1 = S_t t-1$; so that $U_t t-1 S_{t-1} t-1 = 0$.

By Remark 3.1.12, we obtain $U_t t-1 = 0$.

We now proceed by induction. Suppose, we have shown that $U_t t-j = 0$ for $1 \leq j \leq p - 1$. Then $U = U S$ implies that
\[ R_t \ t-p = U_t \ t-p \ S_t \ t-p + U_t \ t \ S_t \ t-p \]

and hence

\[ R_t \ t-p = S_t \ t-p \]

which in turn gives (as before), \( U_t \ t-p = 0 \). Thus \( U = 0 \).

This proves the theorem.

**Proof of Theorem 3.1.11.** Let \( A = A^{(m, \infty, n)}(A_1, \lambda_1, A_1, \ldots, A_n, \lambda_n, A_n) \).

Define \( A^* = (A_1 \ldots A_n) \) so that \( A^* \) is a \( m \times n \) integral matrix of rank \( n \). Thus, by Theorem 3.1.6, there exists a primitive reduced matrix \( U(\mathbb{M}, m) \) such that \( UA^* = T^* = (T_{ij}^*) \) (say) is a generalized triangular matrix having \( n \) dependent pairs of rows. Clearly, then \( UA = T = (T_{ij}) \), where

\[ T_{ij} = (T_{ij}^* \lambda_j T_{ij}^*) \]

is a generalized triangular matrix with \( n \) dependent pairs of rows and \( n \) dependent pairs of columns.

Next, we notice that if \( C_j \) is a left unit of \( T_{ij} \), then \( C_j \) is also a left unit of \( T_{ij}^* \). Therefore, by Theorem 3.1.9, the matrix \( T^* \), and hence the matrix \( T \), may be chosen in H.N.F.

The uniqueness follows as in Theorem 3.1.10.
§2. Applications.

In this section we investigate the problem of right divisors of an integral matrix $A$ of rank $n$.

We fix a right unit $D$ of $A$ and consider only such right divisors of $A$ as are $D$-reduced on the right. Since right divisors of $A$ have necessarily to be of rank $> n$, this condition implies that we are only considering (right) divisors of $A$ which are of rank $n = \text{r}(A)$.

If $G$ is a right divisor of $A$ (i.e. $A = XG$ for an integral matrix $X$), then every matrix in the left ray containing $G$ is also a right divisor of $A$. Such rays will be called divisor classes.

We show that the problem of finding divisor classes of $A$ can be reduced to finding right divisors in Hermite normal form of the generalized Smith normal form of $A$. We use this in the determination of the number of divisor classes.

**Theorem 3.2.1.** Let $A$ be an integral matrix of rank $n$. There is a one-one correspondence between left rays of right divisors of $A$ and $2^n \times 2^n$ right divisors in H.N.F. of $A^\ast$ where $A \sim A^\ast$. 
is in the S.N.F.

PROOF. We first observe that if \( B = U A V \) where \( U \) and \( V \) are primitive reduced matrices, then \( G \) is a right divisor of \( A \) (notation: \( G \mid A \)) if and only if \( G V \mid B \). Moreover, if \( G_1 \) and \( G_2 \) are two right divisors of \( A \), then \( G_1 = G_2 \) if and only if \( G_1 V = G_2 V \). Therefore, there is a one-one correspondence between right divisors of \( A \) and those of \( A^* \). Thus, we just need to show that there is a one-one correspondence between left rays of right divisors of \( A^* \) and \( 2n \times 2n \) right divisors in H.N.F. of \( A^* \).

We observe that \( A^* \) is a matrix of rank \( n \), having \( n \) dependent pairs of columns. So, if \( G \) is a (reduced) right divisor of \( A^* \), then \( G \) also has \( n \) dependent pairs of columns. Using Theorem 3.1.11, we find a primitive reduced matrix \( W \) such that \( W G = T(\mathbf{m}; \mathbf{m}) \) is a generalized triangular matrix. Moreover, such a matrix \( T \) is unique under the additional condition (1) of Definition 3.1.8. Clearly \( T \mid A^* \). Thus, \( T \) is a \( 2n \times 2n \) right divisor in H.N.F. of \( A^* \). Finally, the map carrying the left ray containing \( G \) to the matrix \( T \) is one-one. This proves the theorem.
THEOREM 3.2.2. Let $A$ be a primitive matrix and let $B$ be an integral matrix. Let $C = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. There is a one-one correspondence between left rays of right divisors of $C$ and left rays of right divisors of $B$.

PROOF. By Theorem 2.1.9, there exist $A^*$ and $B^*$ such that

$$A \sim A^*, \quad B \sim B^*$$

where

$$A^* = \text{diag} \left[ A_1, \ldots, A_r \right] \text{ (say)},$$

$$B^* = \text{diag} \left[ B_1, \ldots, B_s \right] \text{ (say)},$$

are in the S.N.F. By Remark 2.2.13, $C \sim C^*$ where

$$C^* = \text{diag} \left[ A_1, \ldots, A_r, B_1, \ldots, B_s \right].$$

Moreover, since $A$ is primitive, $C^*$ is in the S.N.F. Thus, in view of the above theorem, it is enough to establish a one-one correspondence between $2(r + s) \times 2(r + s)$ right divisors in H.N.F. of $C^*$ and $2s \times 2s$ right divisors in H.N.F. of $B^*$. 
Let $T = \begin{pmatrix} T_A & 0 \\ \lambda & T_B \end{pmatrix}$ be any $2(r + s) \times 2(r + s)$ right divisor in the H.N.F. of $\mathfrak{C}^*$. Then clearly $T_B$ is in the H.N.F. and $T_B \mid \mathfrak{C}^*$. Also, since $T_A \mid \mathfrak{C}^*$, the matrix $T_A$ is also primitive. Consequently $k = 0$; since $T$ is in the H.N.F.

Therefore, the map

$$I = \begin{pmatrix} T_A & 0 \\ 0 & T_B \end{pmatrix} \rightarrow T_B$$

gives the desired one-one correspondence.

**Definition 3.2.5.** Let $\mathfrak{M}$ be an integral ideal and let $A_1, A_2$ be integral matrices. By $A_1 \equiv A_2 \pmod{\mathfrak{M}}$, we mean that, all the entries of $A_1 - A_2$ are in $\mathfrak{M}$. An equivalence class determined by this relation will be called a congruence class modulo $\mathfrak{M}$.

**Definition 3.2.6.** Let $\mathfrak{M}$ be an integral ideal and let $C$ be any matrix in $k$. By a $C$-reduced congruence class modulo $\mathfrak{M}$, we shall mean the subclass of an equivalence class modulo $\mathfrak{M}$, consisting of matrices $C$-reduced on the left.

We prove:

**Theorem 3.2.5.** Let $\mathfrak{M}(2,2)$ be an integral matrix of rank 1
with a right unit D. If $B^{G,2}$ is an integral matrix of rank 1 satisfying $BD = B$, then $B \equiv 0 \pmod{A}$ if and only if $B \equiv 0 \pmod{\delta(A)}$.

Before proving the theorem, we observe the following:

**Remark 3.2.6.** If A is a matrix of rank 1, then $A \equiv 0 \pmod{\sigma}$ if and only if $\delta(A) \leq \sigma$. In particular, A is primitive if and only if $\delta(A) = \sigma$.

**Proof.** If $B \equiv 0 \pmod{A}$, then $\delta(B) \leq \delta(A)$ which in turn implies, by Remark 3.2.6, that $B \equiv 0 \pmod{\delta(A)}$. On the other hand, if $B \equiv 0 \pmod{\delta(A)}$, then again by Remark 3.2.6, $\delta(B) \leq \delta(A)$. But $AD = A$ and $BD = B$. Thus, if

$$D = \begin{pmatrix} d_1 & \lambda d_1 \\ d_2 & \lambda d_2 \end{pmatrix},$$

then

$$A = \begin{pmatrix} a_1 & \lambda a_1 \\ a_2 & \lambda a_2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_1 & \lambda b_1 \\ b_2 & \lambda b_2 \end{pmatrix}.$$  

It follows, therefore, that the g.c.d. $(b_1, b_2) \leq \text{the g.c.d.}(a_1, a_2)$ so, there exist $x_1, x_2, x_3, x_4$ in $\sigma$ such that

"
\[ b_1 = x^1 a_1 + x^2 a_2 \]

and

\[ b_2 = x^3 a_1 + x^4 a_2 \]

Thus, \( \beta = X \alpha \) where \( X = \begin{pmatrix} x^1 & x^2 \\ x^3 & x^4 \end{pmatrix} \) is integral.

This proves the theorem.

Remark 3.2.7. The above theorem shows that in case \( \alpha \) is a 2 \( \times \) 2 matrix of rank 1 in \( \mathcal{O} \), there is a one-one correspondence between congruence classes modulo \( \alpha \) and congruence classes modulo \( \delta(\alpha) \). In particular, it shows that the number of congruence classes modulo \( \alpha \) is finite if and only if the number of congruence classes modulo \( \delta(\alpha) \) is finite.

We now impose, on the Dedekind domain \( \mathcal{O} \), the so-called finite norm condition namely that for every integral ideal \( \mathfrak{a} \), the number of elements in \( \mathcal{O}/\mathfrak{a} \) is finite. It is well-known that finite norm condition is satisfied if \( \mathcal{O} \) is the ring of integers of an algebraic number field.

Notation 3.2.8. Let \( \alpha \) be an integral matrix and let \( \mathfrak{D} \) be a right unit of \( \alpha \). We shall denote by \( d(\alpha) \), the number of left rays of right divisors of \( \alpha \), with a (fixed) right unit \( \mathfrak{D} \).
**Theorem 3.2.9.** Let $\mathcal{O}$ be a Dedekind domain satisfying the finite norm condition. For every matrix $A$ in $\mathcal{O}$, $\delta(A)$ is finite.

We first prove a lemma, which is a special case of the theorem. The lemma is also used later in the proof of Theorem 3.2.11.

**Lemma 3.2.10.** Let $A$ be a $2 \times 2$ rank 1 matrix in $\mathcal{O}$ and let $D$ be a fixed right unit of $A$. Then the number of $D$-reduced congruence classes modulo $A$ is $\leq N(\delta(A))$, and in particular finite.

**Proof.** Let $B = \begin{pmatrix} b & \lambda b \\ \mu b & \lambda \mu b \end{pmatrix}$ be a rank 1 matrix in $\mathcal{O}$ such that $DB = B$. Then, by Theorem 3.2.5, $B \equiv 0 \pmod{A}$ if and only if $b, \mu b, \lambda b$ and $\lambda \mu b$ belong to $\delta(A)$. Since the number of choices for $b$ incongruent modulo $\delta(A)$ is $N(\delta(A))$, we get the desired result.

**Remark 3.2.11.** All rank 1 matrices of the same discriminant and having the same right unit belong to the same left ray.

(It is similar to Lemma 2.5.2).

**Proof of Theorem 3.2.9.** Let $r(A) = n$. It follows from Theorem 3.2.1 that $d(A)$ equals the number of $2n \times 2n$ right
divisors in \( \text{H.N.F.} \) of the S.N.F. of \( A \).

So, let \( A(2n,2n) = \text{diag} [ \alpha_1, \ldots, \alpha_n ] \) be in the S.N.F.

Let \( A(2n,2n) = (T_{ij}) \) be a right divisor in \( \text{H.N.F.} \) of \( A \) with

(i) \( T_{jj} \in \Phi \) for \( 1 \leq j \leq n \), and

(ii) \( T_{ij} \in \Psi (T_{jj}, C_i) \) for \( 1 \leq i < j \leq n \).

(Recall Notation 2.1.7, Page 25).

Let \( S = U T \) and let \( U = (U_{ij}) \) where \( U_{ij} \) are \( 2 \times 2 \) integral matrices. We assume, without loss of generality, that

\( S = \text{diag} [ C_1, \ldots, C_n ] \) is a right unit of \( U \). It is easily seen that \( U \) is a generalized triangular matrix so that

\begin{align*}
U_{jj} T_{jj} &= 0 \quad \text{for} \quad 1 \leq j \leq n, \\
U_{ij} T_{jj} + \ldots + U_{ij} T_{ij} &= 0 \quad \text{for} \quad 1 \leq j < i \leq n.
\end{align*}

Thus, we have obtained in terms of the \( \text{S.N.F.} \) invariants of \( 1 \) and the \( \text{H.N.F.} \) invariants of \( S \), a set of necessary and sufficient conditions for the divisibility of \( A \) by \( S \). Therefore, \( c(\lambda_j) \subseteq \mathcal{C}(T_{jj}) \) and consequently each \( \mathcal{C}(T_{jj}) \) can only be one of the finitely many integral divisors of \( c(\lambda_j) \). Thus, in view of Remark 3.3.1.1, for each fixed \( j \), there can only be finitely many distinct matrices \( T_{jj} \). But the matrices \( T_{jj} (i > j) \)
are determined in the $c_i$-reduced congruence classes modulo $T_{ij}$. It follows from Lemma 3.2.10, that for each fixed $T_{ij}$ there can only be finitely many different $T_{ij}$. This completes the proof.

\textbf{Theorem 3.2.12.} Let $\mathcal{O}$ be a Dedekind domain satisfying the finite norm condition. Let $A$ be a matrix in $\mathcal{O}$. Then

(i) $d(A) \geq d(\mathcal{N}(A))$,

(ii) $d(A) = d(\mathcal{N}(A))$ in case $r(A) = 1$.

\textbf{Proof.} (i) follows immediately from Theorem 2.5.1, and (ii) is a consequence of (i) and Remark 3.2.11. This concludes the proof.

In case $A$ is a matrix of rank $> 1$, the determination of $d(A)$ is not easy, except in some special cases. We give here an estimate on $d(A)$, which is easy to obtain.

\textbf{Theorem 3.2.13.} Let $\mathcal{O}$ be a Dedekind domain satisfying the finite norm condition. Let $A$ be a matrix in $\mathcal{O}$ of rank $n$. If $\mathcal{N}_1, \ldots, \mathcal{N}_n$ denote the invariants of $A$, then

(i) $\prod_{i=1}^{n} d(\mathcal{N}_i) \leq d(A)$,
(ii) \( d(\mathbf{A}) \leq \prod_{i=1}^{n} \left( d(\mathbf{A}_i) \left( \frac{n}{\pi} \right)^{n-i} \right) \).

PROOF. Let \( \mathbf{A} \sim \mathbf{A}^* \), where \( \mathbf{A}^* = \text{diag} [\mathbf{A}_1, \ldots, \mathbf{A}_n] \) (say) is in the S.N.F. ; so that \( \delta(\mathbf{A}_i) = \mathbf{A}_i \) for \( 1 \leq i \leq n \). For any right divisor \( G_1 \) of \( \mathbf{A}_1 \), \( G_2 \) of \( \mathbf{A}_2 \) and so on, the matrix \( G = \text{diag} [G_1, \ldots, G_n] \) is a right divisor of \( \mathbf{A}^* \). Thus,

\[
\sum_{i=1}^{n} d(\mathbf{A}_i) \geq \prod_{i=1}^{n} d(\mathbf{A}_i).
\]

But, by Theorem 3.2.12, each \( d(\mathbf{A}_i) = d(\mathbf{A}_i) \); and hence (i) is proved.

Let \( T(\mathbf{2}n, \mathbf{2}n) = (T_{ij}) \) be a matrix in H.N.F. and let \( T \mid \mathbf{A}^* \). Then each \( T_{jj} \mid \mathbf{A}_j \) and, by Theorem 3.2.12, there can only be \( d(\mathbf{A}_j) \) different \( T_{jj} \). Further by Lemma 3.2.10, for a fixed \( j \), each \( T_{ij} (i > j) \) has at most \( M(\mathbf{A}_j) \) choices. This proves (ii).

H.M.E. 3.2.14. In view of Remark 2.1.18, (i) (Page 22), we conclude, from (ii) of the above theorem, that

\[
d(i) \leq \left( M(\mathbf{A}_n) \right)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} d(\mathbf{A}_i).
\]
In case \( \lambda_1 = \ldots = \lambda_{n-1} = \sigma \), the above theorem implies that

\[ d(A) = d(\delta(A)) . \]

(This result can be easily obtained directly also, see Theorem 3.2.12).

Let \( \mathcal{O} \) be a Dedekind domain satisfying the finite norm condition. Before evaluating \( d(A) \) for some special matrices of rank > 1, we prove a general result which we use in Example 3.2.18 and Example 3.2.19.

**Theorem 3.2.15.** Let \( A^{(2,2)} \) and \( B^{(2,2)} \) be rank 1 matrices in \( \mathcal{O} \) with \( \delta(A) = a \) and \( \delta(B) = b \). Let \( C, \ C^* \) be left units and let \( D, \ D^* \) be right units of \( A \) and \( B \) respectively. Let \( X \) be an integral matrix which is \( D, \ D^* \) - reduced. Then

\[ A X + Y B = C \quad (1) \]

has an integral solution \( Y \) if and only if \( X \equiv 0 \pmod{\gamma^{-1} \delta(B)} \) where \( \gamma \) is the g.c.d. of \( \delta(A) \) and \( \delta(B) \).

**Proof.** Observe that (1) has an integral solution \( Y \)

\[ \iff Y = - A X B^{-1} \text{ is integral.} \]
\[ \delta(B) \mid \delta(A) \delta(X) \quad \text{by Corollary 2.2.7} \]

\[ \delta(B) \mid \delta(A) \delta(X) \quad \text{using } H \]

\[ \delta^{-1} \delta(B) \mid \delta^{-1} \delta(A) \delta(X) \]

\[ \delta^{-1} \delta(B) \mid \delta(X) \quad \text{since } \delta^{-1} \delta(B) \text{ is prime to } \delta^{-1} \delta(A). \]

\[ X \equiv 0 \pmod{\delta^{-1} \delta(B)}. \]

Hence the theorem is proved.

**Corollary 3.2.16.** Under the notation of Theorem 3.2.15, the number of integral and reduced \( X \) incongruent modulo \( B \) for which (1) has an integral solution is \( M(\delta) \).

**Remark 3.2.17.** The problem of finding integral solution of

\[ A X + B Y = 0 \quad (2) \]

is the same as the problem of finding integral solution of (1); and the number of integral solutions of (1) is equal to the number of integral solutions of (2). For, once the reduction conditions are satisfied, all the arguments are dependent only on the discriminants involved.

**Example 3.2.18.** Let \( A \) be a rank 2 matrix in \( \mathcal{S} \). If \( A \sim A^* \)
where \( A^* = \text{diag} [ A_1, A_2 ] \) is in the S.M.F. with \( \delta(A_1) = \delta(B) \).
Thus, since $T$ is in $H.E.F.$ we have to find, for each fixed pair $T_1, T_2$ satisfying (3), the number of reduced and integral $X$ incongruent modulo $T_1$ which satisfy (4). By Corollary 3.2.16, this number is equal to $N(y)$ where $y$ is the g.c.d. of $\delta(U_2)$ and $\delta(T_1)$. It follows from (3) that $\delta(T_1) = y_t$ and $\delta(U_1) = y^{a_1-t_1}$ where $0 \leq t_1 \leq a_1$; and consequently

$$y = \begin{cases} y^{t_1} & \text{if } t_1 < a_2 - t_2 \\ y^{a_2-t_2} & \text{if } t_1 \geq a_2 - t_2 \end{cases}.$$ 

Thus

$$d(A) = d(A^*) = \sum_{t_1 < a_2 - t_2} (N(y))^{t_1} + \sum_{t_1 \geq a_2 - t_2} (N(y))^{a_2-t_2}.$$ 

\textbf{Example 3.2.13.} Let $A$ be a matrix in $\mathcal{O}$ of rank 3. If $A \sim A^*$ where $A^* = \text{diag} \begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix}$ is in the S.K.F. and $\delta(A_i)$ is a prime ideal $y$ for each $1 \leq i \leq 3$; then

$$d(A) = \sum_{e \leq \delta(A)} e (N(y))^e + 2 N(y) + 4.$$
For, let \( T = \begin{pmatrix} T_1 & 0 & 0 \\ T_2 & T_3 & 0 \\ T_4 & T_5 & T_6 \end{pmatrix} \) be a right divisor in 

\( LR_p(A) \) and let \( C = \text{diag} \{ C_1, C_2, C_3 \} \) be a left 

unit of \( T \). Then there exists a right \( C \)-reduced matrix 

\[
U = \begin{pmatrix} U_1 & 0 & 0 \\ Y_1 & U_2 & 0 \\ Y_2 & Y_3 & U_3 \end{pmatrix}
\]

such that 

\[
\begin{pmatrix} A_1 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & A_3 \end{pmatrix} = \begin{pmatrix} U_1 & 0 & 0 \\ Y_1 & U_2 & 0 \\ Y_2 & Y_3 & U_3 \end{pmatrix} \begin{pmatrix} T_1 & 0 & 0 \\ T_2 & T_3 & 0 \\ T_4 & T_5 & T_6 \end{pmatrix}.
\]

It follows therefore, 

\( U_1 T_1 = \) for \( 1 \leq i \leq 3 \), \( (5) \)

\( U_2 Y_1 + Y_1 T_1 = 0 \), \( (6) \)

\( U_2 Y_2 + Y_2 X_1 + Y_2 T_1 = 0 \), \( (7) \)

\( U_3 Y_3 + Y_3 T_2 = 0 \). \( (8) \)
It follows from (5) that for $1 \leq i \leq 3$,

$$\begin{cases} 
\delta(T_i) = y & \text{and } \delta(U_i) = \sigma \\
\sigma(T_i) = \sigma & \text{and } \delta(T_i) = y
\end{cases} \quad (\ast)$$

Using this we show that, for each fixed triple $\mathbf{\tau} = (\tau_1, \tau_2, \tau_3)$, the equations (6), (7) and (8) are reduced to three independent equations involving $X_1, X_2, X_3$.

Let $P(\mathbf{\tau})(X_i)$ be the number of $X_i$ satisfying the equation in which it occurs and let $P(\mathbf{\tau}) = P(\mathbf{\tau})(X_1) P(\mathbf{\tau})(X_2) P(\mathbf{\tau})(X_3)$. Then

$$\delta(\mathbf{\tau}) = \sum_{\mathbf{\tau}} P(\mathbf{\tau}) .$$

**Case (1).** $\delta(T_1) = y$, $\delta(T_2) = y$.

Then from (9), $\delta(U_2) = \sigma$ and from (6) we have $X_1 = 0$ so that (7) reduces to

$$U_2 X_2 + Y_2 T_1 = 0 .$$

Therefore, by Corollary 3.2.15,

$$P(\mathbf{\tau})(X_2) = \begin{cases} 
x(\gamma) & \text{if } \delta(U_3) = \gamma \\
1 & \text{if } \delta(U_3) = \sigma \end{cases} .$$
Also from (3),

\[ \Pr(\mathcal{X}_3) = \begin{cases} N(\gamma) & \text{if } \delta(U_3) = \gamma \\ 1 & \text{if } \delta(U_3) = \sigma \end{cases} \]

Thus,

\[ \Pr(\mathcal{T}) = \begin{cases} (N(\gamma))^2 & \text{if } \delta(U_3) = \gamma \\ 1 & \text{if } \delta(U_3) = \sigma \end{cases} \]

Case (ii). \( \delta(T_1) = \gamma \), \( \delta(T_2) = \sigma \).

Then \( x_3 = 0 \), because \( T \) is in R.M.F.; so that (3) gives \( y_3 = 0 \). Therefore (3) reduces to

\[ U_3 x_3 + Y_2 T_1 = 0 \]

and

\[ \Pr(\mathcal{X}_2) = \begin{cases} N(\gamma) & \text{if } \delta(U_2) = \gamma \\ 1 & \text{if } \delta(U_2) = \sigma \end{cases} \]

Since \( \delta(T_2) = \sigma \) implies \( \delta(U_2) = \gamma \) (see (C)) and \( \delta(T_1) = \gamma \), we have from (3) \( \Pr(\mathcal{X}_1) = N(\gamma) \). Thus,
\[ P(\tau) = \begin{cases} (M(y))^2 & \text{if } \sigma(U_3) = y \\ M(y) & \text{if } \sigma(U_3) = \sigma \end{cases} \]

**Case (iii).** \( \sigma(T_1) = \sigma \).

Since \( T \) is in \( H.M.F. \), \( \sigma(T_1) = \sigma \) implies that \( X_1 = \sigma = X_2 \).

Therefore, \( T = \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix} \) and \( T \mid A^* \) if and only if

\[
\begin{pmatrix} T_2 & C \\ X_3 & T_3 \end{pmatrix} \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_3 \end{pmatrix}
\]

But \( d \left( \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_3 \end{pmatrix} \right) = (\nu(y) + 3 \) by Example 3.2.13, with

\[ a_1 = 1 = a_2 \] . Hence

\[
d(\lambda) = d(\lambda^*) = (\nu(y)^2 + 1 + (\nu(y)^2 + \nu(y) + 1)^3 + 3 = (\nu(y)^2 + \nu(y) + 1) + 3 \] .
Example 3.2.20. Let \( A \) be a primitive matrix in \( \sigma \) and let \( B \) be an integral matrix of rank \( n \geq 1 \). If \( C \) denotes the matrix \[
\begin{pmatrix}
A & 0 \\
0 & B
\end{pmatrix}
\]
then, by Theorem 3.2.2, \( d(C) = d(B) \).

In particular, if \( r(1) = 1 \), then,

\[
d(C) = d(1) = d(c(2)) ; \text{ by Theorem 3.2.12.}
\]