# THE ELEMENTARY DIVISOR THEOREM FOR CERTAIN RINGS WITHOUT CHAIN CONDITION 

OLAF HELMER

1. Introduction. The Elementary Divisor Theorem is known to hold in principal ideal rings and in rings with Euclidean algorithm. ${ }^{1}$ It is an open question whether it holds in every Pruifer ring, that is, in every domain of integrity in which every ideal with finite basis is a principal ideal. ${ }^{2}$ (A Prüfer ring can also be characterized as a domain of integrity in which the greatest common factor of any finite number of elements can be represented as a linear combination of these elements.) The Elementary Divisor Theorem will here be proved for what will be called "adequate" rings. They are special Prüfer rings, but not restricted by any equivalent to a chain condition, so that they comprise considerably more than just the principal ideal rings. ${ }^{3}$
2. Definition of adequate rings. Let $R$ be a domain of integrity, $a, b$ in $R$, and $a \neq 0$. By a relatively prime part of $a$ with respect to $b$, written $R P(a, b)$, we shall understand a factor $a_{1}$ of $a$ such that, if $a=a_{1} \cdot a_{2}$,
(i) $\left(a_{1}, b\right)=1$,
(ii) $\left(a_{3}, b\right) \neq 1$ for any non-unit factor $a_{3}$ of $a_{2} .{ }^{4}$
$R P(a, b)$ may or may not exist; if it does, it is, in a sense, a largest factor of $a$ that is relatively prime to $b$.

We now define $R$ to be an adequate ring if
(i) $R$ is a Prüfer ring,
(ii) $R P(a, b)$ exists for all $a, b$ in $R$ with $a \neq 0$.
3. Relationship to Prüfer rings and principal ideal rings. By definition every adequate ring is a Prüfer ring. On the other hand, every

[^0]principal ideal ring is adequate; for in a ring of that kind we have unique prime power decomposition, and hence the existence of $R P(a, b)$ for $a \neq 0$ is obvious. An example of an adequate ring which is not a principal ideal ring is furnished by the set of integral functions with coefficients in a field $F$. That a ring of this type is a Prüfer ring has been proved in a previous paper. ${ }^{5}$ The existence of $R P(a, b)$ is an immediate consequence of the unique factorization theorem for integral functions (Theorem 6 of the same paper). Theorem 8 of that paper, finally, states that the ring is not a principal ideal ring.
4. Six lemmas. Now let $R$ be an adequate ring. Among the properties of such a ring are those stated in the six lemmas below. The first four are well known, and hold in any Prüfer ring; sketches of their proofs have been included, however, for reasons of completeness.

Lemma 1. If $f \mid a b$ and $(f, a)=1$, then $f \mid b$.
Proof. Let $h f+k a=1$; then $f \mid a b k=b(1-h f)=b-b h f$ and hence $f \mid b$.

Lemma 2. An element a has an inverse $a^{*} \bmod b$,

$$
\begin{equation*}
a \cdot a^{*} \equiv 1(\bmod b) \tag{1}
\end{equation*}
$$

if and only if $(a, b)=1$. Moreover, $a^{*}$, if it exists, is uniquely determined $\bmod b$.

Proof. If $a a^{*} \equiv 1(\bmod b)$, then $a a^{*}=1+b k$ and hence $(a, b)=1$. Conversely, if $(a, b)=1$, then $h$ and $k$ exist such that $h a+k b=1$, and hence $a h \equiv 1(\bmod b)$ and $a^{*}=h$. Finally, if $a a^{*} \equiv a a^{* *} \equiv 1(\bmod b)$, then $a^{*} \equiv a^{*}\left(a a^{* *}\right) \equiv\left(a a^{*}\right) a^{* *} \equiv a^{* *}(\bmod b)$.

Lemma 3. The congruences

$$
\begin{equation*}
x \equiv a_{i}\left(\bmod m_{i}\right), \quad i=1,2, \cdots, n \tag{2}
\end{equation*}
$$

have a simultaneous solution $x$, provided any two $m_{i}$ are relatively prime. Moreover, the solution is uniquely determined $\bmod m$, where $m=m_{1} m_{2} \cdots m_{n}$.

Proof. Let $m=m_{i} M_{i}$. Since any two $m_{i}$ are relatively prime it follows that $\left(m_{i}, M_{i}\right)=1$. Hence, by Lemma 2, the $M_{i}$ possess inverses $M_{i}^{*} \bmod m_{i}$. It is seen at once that

$$
\begin{equation*}
x \equiv a_{1} M_{1} M_{1}^{*}+\cdots+a_{n} M_{n} M_{n}^{*}(\bmod m) \tag{3}
\end{equation*}
$$

[^1]is a required solution, and the uniqueness is obvious.
Lemma 4. Let $a_{1}, a_{2}, \cdots, a_{n}$ not be all zero, and
\[

$$
\begin{equation*}
\left(a_{1}, a_{2}, \cdots, a_{n}\right)=d \tag{4}
\end{equation*}
$$

\]

then there exist elements $a_{i j}(i=2, \cdots, n ; j=1, \cdots, n)$ such that

$$
\left|\begin{array}{cccc}
a_{1} & a_{2} & \cdots & a_{n}  \tag{5}\\
a_{21} & a_{22} & \cdots & a_{2 n} \\
\cdot & \cdot & \cdots & \cdot \\
a_{n 1} & a_{n 2} & \cdots & a_{n n}
\end{array}\right|=d
$$

Proof. If all but one $a_{k}$ are zero, then $d=a_{k}$. Choose $a_{2 k}=\cdots=a_{n k}=0$, and the unity matrix for the rest of the $a_{i j}$; the resulting determinant will be $d$ or $-d$, if $-d$, a change of one 1 into -1 will put things right. If, on the other hand, no more than $n-2$ of the $a_{k}$ are zero, we can proceed by induction. For $n=1$ the assertion is trivially correct. For $n>1$ let

$$
\begin{equation*}
d^{\prime}=\left(a_{2}, \cdots, a_{n}\right) ; \tag{6}
\end{equation*}
$$

by induction we can find $a_{i j}(i=2, \cdots, n-1 ; j=2, \cdots, n)$ such that

$$
\left|\begin{array}{ccc}
a_{2} & \cdots & a_{n}  \tag{7}\\
a_{22} & \cdots & a_{2 n} \\
\cdot & \cdots & \cdot \\
a_{n-1,2} & \cdots & a_{n-1, n}
\end{array}\right|=d^{\prime}
$$

Suppose now that

$$
\begin{equation*}
d=\left(a_{1}, d^{\prime}\right)=h \cdot a_{1}+k \cdot d^{\prime} \tag{8}
\end{equation*}
$$

We can then complete our determinant as follows:

$$
\left|\begin{array}{cccc}
a_{1} & a_{2} & \cdots & a_{n}  \tag{9}\\
0 & a_{22} & \cdots & a_{2 n} \\
\cdot & \cdot & \cdots & \cdot \\
0 & a_{n-1,2} & \cdots & a_{n-1, n} \\
(-1)^{n-1} k & (-1)^{n} h a_{2} / d^{\prime} & \cdots & (-1)^{n} h a_{n} / d^{\prime}
\end{array}\right|=h \cdot a_{1}+k \cdot d^{\prime}=d .
$$

Lemma 5. $R P(a, b)$ is uniquely determined except for a unit factor.
Proof. Let

$$
\begin{equation*}
a=a_{1} \cdot a_{2}=a^{\prime} \cdot a^{\prime \prime} \tag{10}
\end{equation*}
$$

where $a_{1}$ and $a^{\prime}$ are both largest factors of $a$ that are relatively prime to $b$. We show first that $\left(a_{2}, a^{\prime}\right)=1$. Suppose that $\left(a_{2}, a^{\prime}\right)=d \neq 1$; then $d \mid a_{2}$, and by definition of $a_{1},(d, b) \neq 1$; but $d \mid a^{\prime}$ implies $(d, b) \mid\left(a^{\prime}, b\right)$, so that $\left(a^{\prime}, b\right) \neq 1$, which is impossible by definition of $a^{\prime}$. Hence $\left(a_{2}, a^{\prime}\right)=1$, and we can now apply Lemma 1: since $a_{2} \mid a^{\prime} a^{\prime \prime}$, it follows that $a_{2} \mid a^{\prime \prime}$. Similarly $a^{\prime \prime} \mid a_{2}$, so that $a_{2}$ and $a^{\prime \prime}$ can only differ by a unit factor.

Lemma 6. Let $R P(a, b)=r$, and let $d \mid a$ with $(d, r)=1$; then $R P(d, b)=1$.

Proof. Let $a=r \cdot s$. By assumption and Lemma 1, $d \mid s$. Hence, by definition of $r$ and $s,(\delta, b) \neq 1$ for every non-unit factor $\delta$ of $d$, and consequently $R P(d, b)=1$.
5. A preparatory theorem. The main result of this paper will be a consequence of the following theorem.

Theorem 1. Let

$$
M=\left(\begin{array}{cccc}
a_{11} & a_{12} & \cdots & a_{1 k}  \tag{11}\\
a_{21} & a_{22} & \cdots & a_{2 k} \\
\cdot & \cdot & \cdots & \cdot \\
a_{n 1} & a_{n 2} & \cdots & a_{n k}
\end{array}\right)
$$

be a matrix with coefficients in an adequate ring $R$, let

$$
\begin{equation*}
1<n=\operatorname{rank} M \leqq k \tag{12}
\end{equation*}
$$

and

$$
\begin{equation*}
\left(a_{11}, a_{12}, \cdots, a_{1 k}, a_{21}, \cdots, a_{n k}\right)=d \tag{13}
\end{equation*}
$$

then there exist $t_{1}, t_{2}, \cdots, t_{n-1}$ in $R$ such that

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{k}\right)=d \tag{14}
\end{equation*}
$$

where

$$
\begin{equation*}
A_{i}=a_{1 i} t_{1}+a_{2 i} t_{2}+\cdots+a_{n-1, i} t_{n-1}+a_{n i}, \quad i=1,2, \cdots, k \tag{15}
\end{equation*}
$$

Proof. (a) Suppose the theorem has been proved for $d=1$. Then the general case results as follows. Let

$$
\begin{equation*}
N=(1 / d) \cdot M \tag{16}
\end{equation*}
$$

the coefficients

$$
\begin{equation*}
b_{i j}=a_{i j} / d \tag{17}
\end{equation*}
$$

of the matrix $N$ are then relatively prime, and the theorem is considered proved for this case; there are, therefore, quantities $t_{1}, t_{2}, \cdots, t_{n-1}$ in $R$ such that

$$
\begin{equation*}
\left(B_{1}, B_{2}, \cdots, B_{k}\right)=1, \tag{18}
\end{equation*}
$$

where

$$
\begin{equation*}
B_{i}=b_{1 i} t_{1}+b_{2 i} t_{2}+\cdots+b_{n-1, i} t_{n-1}+b_{n i}=A_{i} / d \tag{19}
\end{equation*}
$$

Hence

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{k}\right)=d \cdot\left(B_{1}, B_{2}, \cdots, B_{k}\right)=d \tag{20}
\end{equation*}
$$

(b) For $d=1$ the proof will be given by induction with respect to $n$. First, let $n=2$. We have to find $t$ so that the

$$
\begin{equation*}
A_{i}=a_{1 i} t+a_{2 i}, \quad i=1,2, \cdots, k, \tag{21}
\end{equation*}
$$

have the greatest common factor 1 . Note that any common factor of $A_{i}$ and $A_{j}$ is also a factor of

$$
D_{i j}=\left|\begin{array}{ll}
a_{1 i} & a_{1 j}  \tag{22}\\
a_{2 i} & a_{2 j}
\end{array}\right|=a_{1 i} A_{j}-a_{1 j} A_{i} .
$$

If, therefore, we set

$$
\begin{equation*}
D=\left(D_{12}, D_{13}, D_{23}, D_{14}, \cdots, D_{k-1, k}\right), \tag{23}
\end{equation*}
$$

then, however $t$ be chosen,

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{k}\right) \mid D \tag{24}
\end{equation*}
$$

On account of (12), not all $D_{i j}$ are zero; hence $D \neq 0$, and we may define:

$$
\left\{\begin{array}{l}
D_{1}=R P\left(D, a_{11}\right),  \tag{25}\\
D_{2}=R P\left(\frac{D}{D_{1}}, a_{12}\right), \\
\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\
D_{k}=R P\left(\frac{D}{D_{1} D_{2} \cdots D_{k-1}}, a_{1 k}\right)
\end{array}\right.
$$

We then have, obviously,

$$
\left(D_{i}, D_{j}\right)=1, \quad i \neq j
$$

because a largest relatively prime factor of a quantity is always prime to the supplementary factor. Consequently, by Lemma 3, there exists a simultaneous solution $t$ of the congruences

$$
\begin{equation*}
t \equiv a_{1 i}^{*} \cdot\left(1-a_{2 i}\right)\left(\bmod D_{i}\right), \quad i=1,2, \cdots, k \tag{27}
\end{equation*}
$$

where $a_{1 i}^{*}$ is an inverse of $a_{1 i} \bmod D_{i}$ :

$$
\begin{equation*}
a_{1 i}^{*} \cdot a_{1 i} \equiv 1\left(\bmod D_{i}\right) \tag{28}
\end{equation*}
$$

(the existence of $a_{1 i}^{*}$ being guaranteed by Lemma 2 , since ( $a_{1 i}, D_{i}$ ) $=1$ by virtue of (25)). With $t$ chosen thus, we shall now show that

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{k}\right)=1 \tag{29}
\end{equation*}
$$

From (21) and (27) we have

$$
\begin{equation*}
A_{i}=a_{1 i} t+a_{2 i} \equiv 1\left(\bmod D_{i}\right) \tag{30}
\end{equation*}
$$

Suppose, now, that the $A_{i}$ have some non-unit factor $c$ in common; then, by (24), it would follow that $c \mid D$. This, together with (30), implies that

$$
\begin{equation*}
\left(c, D_{i}\right)=1 \tag{31}
\end{equation*}
$$

this means that $c$ is a factor of $D$ that is prime to all $D_{i}$, and we can apply Lemma 6, with the result that

$$
\begin{equation*}
R P\left(c, a_{1 i}\right)=1, \quad i=1,2, \cdots, k \tag{32}
\end{equation*}
$$

But then, as $c$ was not supposed to be a unit, none of its non-unit factors is prime to any $a_{1 i}$. In particular,

$$
\left\{\begin{array}{c}
\left(c, a_{11}\right)=c_{1} \neq 1,  \tag{33}\\
\left(c_{1}, a_{12}\right)=c_{2} \neq 1, \\
\cdot \cdot \cdot \cdots \cdot \cdot \\
\left(c_{k-1}, a_{1 k}\right)=c_{k} \neq 1
\end{array}\right.
$$

the $a_{1 i}$ thus have a common non-unit factor $c_{k}$, and, since $c_{k} \mid A_{i}$, it follows that $c_{k}$ is also a factor of $A_{i}-a_{1 i} t=a_{2 i}$. But this is incompatible with the assumption that $d=1$.
(c) Suppose now that the theorem has been proved for values less than $n$; we then have to show that it holds for $n$ provided $d=1$. Let

$$
\begin{equation*}
d_{1}=\left(a_{21}, a_{22}, \cdots, a_{2 k}, a_{31}, \cdots, a_{n k}\right) \tag{34}
\end{equation*}
$$

applying induction, we can find $t_{2}, t_{3}, \cdots, t_{n-1}$ so that

$$
\begin{equation*}
\left(B_{1}, B_{2}, \cdots, B_{k}\right)=d_{1} \tag{35}
\end{equation*}
$$

where

$$
\begin{equation*}
B_{i}=a_{2 i} t_{2}+a_{3 i} t_{3}+\cdots+a_{n-1, i} t_{n-1}+a_{n i}, \quad i=1,2, \cdots, k \tag{36}
\end{equation*}
$$

and it remains to determine $t_{1}$ suitably. We have

$$
\begin{equation*}
A_{i}=a_{1 i} t_{1}+B_{i} \tag{37}
\end{equation*}
$$

with

$$
\begin{align*}
& \left(a_{11}, B_{1}, a_{12}, B_{2}, \cdots, a_{1 k}, B_{k}\right)=\left(a_{11}, a_{12}, \cdots, a_{1 k}, d_{1}\right)  \tag{38}\\
& \quad=\left(a_{11}, a_{12}, \cdots, a_{1 k}, a_{21}, \cdots, a_{n k}\right)=1
\end{align*}
$$

Therefore, using induction with $n=2$, we can find $t_{1}$ such that

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{k}\right)=1 \tag{39}
\end{equation*}
$$

and the proof of Theorem 1 is completed.
6. The case of a square matrix with nonzero determinant. Before taking up the general case of the Elementary Divisor Theorem we shall first treat the case of a nonsingular matrix.

Theorem 2. Let $R$ be an adequate ring, $M$ a square matrix with coefficients in $R$, and $|M| \neq 0$. Then there exist two matrices $X$ and $Y$ with coefficients in $R$, such that

$$
\begin{equation*}
|X|=|Y|=1 \tag{40}
\end{equation*}
$$

and

$$
X M Y=\left(\begin{array}{cccc}
e_{1} & 0 & \cdots & 0  \tag{41}\\
0 & e_{2} & \cdots & 0 \\
\cdot & \cdots & \cdots & \cdot \\
0 & 0 & \cdots & e_{n}
\end{array}\right)
$$

where the $e_{i}$ are the elementary divisors of $M$.
Proof. For $n=1$ the theorem is trivially true. For $n>1$ assume the theorem proved for all values less than $n$. It is sufficient to consider the case where $e_{1}$ (which is the greatest common factor of the coefficients of $M$ ) equals 1 ; for otherwise we first deal with the matrix $M / e_{1}$, whose elementary divisors are $1, e_{2} / e_{1}, \cdots, e_{n} / e_{1}$; hence if

$$
X \frac{M}{e_{1}} Y=\left(\begin{array}{cccc}
1 & 0 & \cdots & 0  \tag{42}\\
0 & e_{2} / e_{1} & \cdots & 0 \\
\cdot & \cdot & \cdots & \cdot \\
0 & 0 & \cdots & e_{n} / e_{1}
\end{array}\right)
$$

we have at once

$$
X M Y=\left(\begin{array}{cccc}
e_{1} & 0 & \cdots & 0  \tag{43}\\
0 & e_{2} & \cdots & 0 \\
\cdot & \cdots & \cdots & \cdot \\
0 & 0 & \cdots & e_{n}
\end{array}\right)
$$

Let now $e_{1}=1$ and $M=\left(a_{i j}\right)$. Applying Theorem 1 , with $k=n$ and $d=1$, we can find $t_{1}, t_{2}, \cdots, t_{n-1}$ in $R$ such that

$$
\begin{equation*}
\left(A_{1}, A_{2}, \cdots, A_{n}\right)=1 \tag{44}
\end{equation*}
$$

where

$$
\begin{equation*}
A_{i}=a_{1 i} t_{1}+a_{2 i} t_{2}+\cdots+a_{n-1, i} t_{n-1}+a_{n i}, \quad i=1,2, \cdots, n \tag{45}
\end{equation*}
$$

Applying Lemma 4 to these $A_{i}$, a square matrix $A$ with coefficients in $R$ can be found whose first row is $A_{1}, A_{2}, \cdots, A_{n}$ and whose determinant is 1 . If $h_{i}$ is the minor belonging to $A_{i}$, we have

$$
\begin{equation*}
h_{1} A_{1}+h_{2} A_{2}+\cdots+h_{n} A_{n}=1 \tag{46}
\end{equation*}
$$

As $|A|=1$, we can form, in $R$, the inverse matrix

$$
\begin{equation*}
Q=A^{-1} \tag{47}
\end{equation*}
$$

Note that the first column of $Q$ is $h_{1}, h_{2}, \cdots, h_{n}$. If, now, we set

$$
\begin{equation*}
q_{i}=h_{1} a_{i 1}+h_{2} a_{i 2}+\cdots+h_{n} a_{i n}, \quad i=1,2, \cdots, n \tag{48}
\end{equation*}
$$

we can define

$$
\begin{equation*}
P=P_{1} \cdot P_{2} \tag{49}
\end{equation*}
$$

where

$$
P_{1}=\left(\begin{array}{lll}
1 & 0 \cdots & 0  \tag{50}\\
q_{1} & 0 \cdots & -1 \\
. & \cdots & . \\
q_{n-1}-1 \cdots & 0
\end{array}\right), \quad P_{2}=\left(\begin{array}{ccc}
t_{1} \cdots t_{n-1} & 1 \\
0 \cdots 1 & 0 \\
\cdots \cdots & . \\
1 \cdots 0 & 0
\end{array}\right)
$$

Then

$$
\begin{equation*}
\left|P_{1}\right|=\left|P_{2}\right|=(-1)^{n(n-1) / 2} \tag{51}
\end{equation*}
$$

so that

$$
\begin{equation*}
|P|=\left|P_{1}\right| \cdot\left|P_{2}\right|=1 \tag{52}
\end{equation*}
$$

Multiplying out, we obtain

$$
P=\left(\begin{array}{ccccc}
t_{1} & t_{2} & \cdots & t_{n-1} & 1  \tag{53}\\
q_{1} t_{1}-1 & q_{1} t_{2} & \cdots & q_{1} t_{n-1} & q_{1} \\
q_{2} t_{1} & q_{2} t_{2}-1 & \cdots & q_{2} t_{n-1} & q_{2} \\
\cdot & \cdot & \cdots & \cdot & \cdot \\
q_{n-1} t_{1} & q_{n-1} t_{2} & \cdots & q_{n-1} t_{n-1}-1 & q_{n-1}
\end{array}\right) .
$$

Notice that we also have

$$
\begin{equation*}
|Q|=1 \tag{54}
\end{equation*}
$$

We now multiply $M$ from the left by $P$ and from the right by $Q$ :

$$
\begin{align*}
& P M Q=\left(\begin{array}{cccc}
A_{1} & A_{2} & \cdots & A_{n} \\
q_{1} A_{1}-a_{11} & q_{1} A_{2}-a_{12} & \cdots & q_{1} A_{n}-a_{1 n} \\
\cdot & \cdot & \cdots & \cdot \\
q_{n-1} A_{1}-a_{n-1,1} & q_{n-1} A_{2}-a_{n-1,2} & \cdots & q_{n-1} A_{n}-a_{n-1, n}
\end{array}\right)  \tag{55}\\
& \left(\begin{array}{cc}
h_{1} & * \ldots * \\
h_{2} & * \ldots * \\
. & \ldots . . \\
h_{n} & * \ldots *
\end{array}\right)=\left(\begin{array}{ccc}
1 & 0 \cdots \\
0 & * \ldots * \\
\cdot & \ldots . \\
0 & * \ldots *
\end{array}\right)
\end{align*}
$$

where the zeros in the first row of this matrix arise from multiplying the row $A_{1}, A_{2}, \cdots, A_{n}$ by a row of minors of $A$ not belonging to that row, while the zero in the $(i+1)$ st place of the first column results as follows:

$$
\begin{align*}
\left(q_{i} A_{1}-a_{i 1}\right) & h_{1}+\cdots+\left(q_{i} A_{n}-a_{i n}\right) h_{n} \\
& =q_{i}\left(A_{1} h_{1}+\cdots+A_{n} h_{n}\right)-\left(a_{i 1} h_{1}+\cdots+a_{i n} h_{n}\right)  \tag{56}\\
& =q_{i} \cdot 1-q_{i}=0 .
\end{align*}
$$

We can now apply induction to the matrix $M_{1}$ of order $n-1$ that appears in the lower right corner of $P M Q$. Let

$$
X_{1} M_{1} Y_{1}=\left(\begin{array}{llll}
e_{1}^{\prime} & 0 & \cdots & 0  \tag{57}\\
0 & e_{2}^{\prime} & \cdots & 0 \\
\cdot & \cdot & \cdots & \cdot \\
0 & 0 & \cdots & e_{n-1}^{\prime}
\end{array}\right)
$$

where $\left|X_{1}\right|=\left|Y_{1}\right|=1$ and where $e_{1}^{\prime}, e_{2}^{\prime}, \cdots, e_{n-1}^{\prime}$ are the elementary divisors of $M_{1}$. Then, if we set

$$
X=\left(\begin{array}{cc}
1 & 0 \cdots 0  \tag{58}\\
0 & X_{1} \\
. & X_{1} \\
0 &
\end{array}\right) \cdot P, \quad Y=Q \cdot\left(\begin{array}{cc}
1 & 0 \cdots 0 \\
0 & Y_{1} \\
. & \\
0 &
\end{array}\right)
$$

we obtain immediately

$$
X M Y=\left(\begin{array}{lllll}
1 & 0 & 0 & \cdots & 0  \tag{59}\\
0 & e_{1}^{\prime} & 0 & \cdots & 0 \\
0 & 0 & e_{2}^{\prime} & \cdots & 0 \\
. & . & \cdot & \cdots & \\
0 & 0 & 0 & \cdots & e_{r-1}^{\prime}
\end{array}\right)
$$

and all that remains to be shown is that

$$
\begin{equation*}
e_{i}=e_{i-1}^{\prime}, \quad i=2,3, \cdots, n \tag{60}
\end{equation*}
$$

Now, clearly, the determinant divisors of $X M Y$ are $1, e_{1}^{\prime}, e_{1}^{\prime} e_{2}^{\prime}, \cdots$, $e_{1}^{\prime} e_{2}^{\prime} \cdots e_{n-1}^{\prime}$; hence its elementary divisors are $1, e_{1}^{\prime}, e_{2}^{\prime}, \cdots, e_{n-1}^{\prime}$, and the rest follows from the fact that "equivalent" matrices (here $M$ and $X M Y$ ) have the same elementary divisors (proof literally as for the ring of rational integers).
7. The general case. We can now prove the general Elementary Divisor Theorem:

Theorem 3. Let $R$ be an adequate ring, and $M$ a matrix of type ( $m, n$ ) with coefficients in $R$. Then there exist two matrices $X$ and $Y$ with coefficients in $R$ and of types $(m, m)$ and ( $n, n$ ) respectively, such that

$$
\begin{equation*}
|X|=|Y|=1 \tag{61}
\end{equation*}
$$

and

$$
X M Y=\left(\begin{array}{llllll}
e_{1} & 0 & & \cdots & & 0  \tag{62}\\
0 & e_{2} & & & & \\
\cdot & & \cdot & & & \\
\cdot & & \cdot & & & \\
& & & e_{r} & & \\
\cdot & & & & 0 & \\
& & & & & \cdot \\
\cdot & & & & & \cdot \\
0 & \cdot & & \cdots & & \cdot \\
0 & & &
\end{array}\right)
$$

where $e_{1}, e_{2}, \cdots, e_{r}$ are the elementary divisors of $M$.

Proof. (a) Let $M=\left(a_{i j}\right)$, of rank $r$. If $r=0$, we can set $X=E_{m}$ and $Y=E_{n}$. Otherwise not all $a_{i j}$ are zero, and we have

$$
\begin{equation*}
\left(a_{11}, a_{12}, \cdots, a_{1 n}, a_{21}, \cdots, a_{m n}\right)=d \neq 0 \tag{63}
\end{equation*}
$$

The case where $m=n=r$ is covered by Theorem 2. If $r<m$ or $r<n$ or both, it will be shown below that $M$ can be transformed unitarily into a matrix of the form

$$
\left(\begin{array}{ll}
N & 0  \tag{64}\\
0 & 0
\end{array}\right)
$$

where $N$ is of type ( $r, r$ ) (and hence $|N| \neq 0$ ). Once this has been done, Theorem 2 can be applied to $N$; and if, say, $X_{1}$ and $Y_{1}$ take $N$ into the desired normal form, then

$$
X=\left(\begin{array}{cc}
X_{1} & 0  \tag{65}\\
0 & E_{m-r}
\end{array}\right), \quad Y=\left(\begin{array}{cc}
X_{2} & 0 \\
0 & E_{n-r}
\end{array}\right)
$$

will do the same for $M$.
(b) Let $r<m$. The $m$ rows of $M$ must then be linearly dependent in $R$ :

$$
\begin{equation*}
j_{1} a_{1 i}+j_{2} a_{2 i}+\cdots+j_{m} a_{m i}=0, \quad i=1,2, \cdots, n, \tag{66}
\end{equation*}
$$

where the $j_{i}$ may be assumed to be relatively prime. By Lemma 4 we can find elements $j_{i k}$ in $R(i=1, \cdots, m-1 ; k=1, \cdots, m)$ such that the matrix

$$
J=\left(\begin{array}{cccc}
j_{11} & j_{12} & \cdots & j_{1 m}  \tag{67}\\
\cdot & \cdot & \cdots & \cdot \\
j_{m-1,1} & \cdot & \cdots & j_{m-1, m} \\
j_{1} & j_{2} & \cdots & j_{m}
\end{array}\right)
$$

has determinant 1 ; and if we multiply $M$ on the left by $J$, we obtain a matrix whose last row consists of zeros.

Clearly, if $r<n$, an analogous multiplication of $M$ on the right by a unitary matrix will generate a last column of zeros.

This procedure can be applied repeatedly. If

$$
X_{1} M X_{2}=\left(\begin{array}{cc}
M_{1} & 0  \tag{68}\\
0 & 0
\end{array}\right)
$$

where $M_{1}$ is of type $\left(m_{1}, n_{1}\right)$ with $r<m_{1}$ or $r<n_{1}$, a further row or column of $M_{1}$ (and hence of $M$ ) can be turned into zeros. This process will break off only when the form

$$
\left(\begin{array}{ll}
N & 0  \tag{69}\\
0 & 0
\end{array}\right)
$$

with $N$ of type ( $r, r$ ) has been reached. This, according to (a), completes the proof.

College of the City of New York

## THE GEOMETRY OF VELOCITY SYSTEMS

## EDWARD KASNER AND JOHN DeCICCO

1. Introduction. In connection with the investigation of the differential geometric properties of positional fields of force, Kasner introduced certain important systems of curves which he termed velocity systems. ${ }^{1}$ In this paper, we propose to present some of the old and many new geometric properties of any velocity system.

Since velocity systems serve to characterize the conformal group, many of our results are logically theorems of conformal geometry. This may be contrasted with the study of all the trajectories of positional fields of force, which is essentially differential projective geometry.
2. Velocity systems. We shall find it most convenient for our study to use the minimal coordinates $u=x+i y, v=x-i y, p=d v / d u$, $q=d^{2} v / d u^{2}$, where, of course, $(x, y)$ are the cartesian coordinates of the plane.

In the plane, consider a particle of unit mass moving in any field of force whose components parallel to the $u$-axis and the $v$-axis are $d(u, v)$ and $c(u, v)$. The equations of motion are

$$
\begin{equation*}
\frac{d^{2} u}{d t^{2}}=d(u, v), \quad \frac{d^{2} v}{d t^{2}}=c(u, v), \tag{1}
\end{equation*}
$$

where $t$ is the time. Now if $r$ is the radius of curvature along a trajectory, we have

$$
\begin{equation*}
\omega^{2}=r N \tag{2}
\end{equation*}
$$

[^2]
[^0]:    Received by the editors, May 29, 1942.
    ${ }^{1}$ B. L. van der Waerden, Moderne Algebra, vol. 2, Berlin, 1931, p. 122. For further reference, see the papers by J. H. M. Wedderburn (J. Reine Angew. Math. vol. 167 (1932)), N. Jacobson (Ann. of Math. (2) vol. 38 (1937)), and O. Teichmüller (Preuss. Akad. Wiss. Sitzungsber. 1937).
    ${ }^{2}$ Rings of this kind were considered by H. Prüfer in Untersuchungen über Teilbarkeitseigenschaften in Körpern, J. Reine Angew. Math. vol. 168 (1932).
    ${ }^{3}$ My thanks are due to Professor Reinhold Baer for several helpful suggestions.
    ${ }^{4}$ Notation throughout this paper: " $a, b, \cdots$ )" for "greatest common factor of $a, b, \cdots, "$ " $a \mid b$ " for " $a$ is a factor of $b$," " $a=b$ " for " $a$ equals $b$ except possibly for a unit factor." (This last convention serves the purpose of replacing statements about principal ideals simply by statements about their generating elements.)

[^1]:    ${ }^{5}$ Theorem 9 in Divisibility properties of integral functions, Duke Math. J. vol. 6 (1940) p. 351.

[^2]:    Presented to the Society, February 22, 1941, under the title Conformal geometry of velocity systems; received by the editors June 23, 1942.
    ${ }^{1}$ Kasner, Differential-geometric aspects of dynamics, Amer. Math. Soc. Colloquium Publications vol. 3 (1912); Trans. Amer. Math. Soc. vols. 9-10 (1908-1909).

