# The Lattice Structure of Algebraic Moduls

Thesis by

Gerald Harrison

In Partial Fulfilment of the Requirements

for the Degree of Doctor of Philosophy

California Institute of Technology

Pasadena, California

1943

The writer wishes to express his sincere appreciation for the encouragement and advice of Professor Morgan Ward, under whose direction this dissertation was written.

## Summary of Thesis

The thesis consists of two parts. In Section I the theory of lattices whose elements are nxn matrices with elements in a principal ideal ring is developed. Here the main result is a decomposition theorem stating that such lattices are a direct product of certain well distinguished sublattices whose elements are "primary" elements. The results have an immediate application to the theory of linear form moduls over a principal ideal ring, and in fact the theory was developed with this in mind. Section II gives a rather remarkable property of the above mentioned decomposition theorem when the basis elements of the linear form modul which the matrix represents are algebraic integers, and is therefore a contribution to the multiplicative theory of algebraic moduls.

# Introduction

It was probably Dedekind's study of algebraic moduls in developing the theory of algebraic numbers which led him to introduce and study the abstract algebra called by him a "Dualgruppe", now called a lattice. He showed that the free modular lattice generated by three elements is of order twenty-eight, and exhibited sets of quadratic moduls which actually generate it (Dedekind [2] ). However the modular lattice of submoduls of a linear form modul is not the most general discrete modular lattice; thus, though the free modular lattice on four generators is infinite, the free lattice generated by any finite number of submoduls of a modul of finite order is finite. The question naturally arises as to what lattice identities besides the modular identity are satisfied by the lattice of submoduls of a linear form modul. Though this is as yet an unanswered question, the results of Section I simplifies the problem.

The study of algebraic moduls may be divided into two parts. In the first the theory is simply that of a linear form modul over the ring of rational integers, while in the second the algebraic character of the basis elements plays an essential role and leads to the theory of algebraic numbers and ideals. Section I contains contributions to the former theory, and Section II to the latter. It was found that both theories could

be treated most easily by employing matrices; indeed the first section may be considered a study of the lattice theory of matrices with elements in a principal ideal ring.

The usual $\vee$ and $\wedge$ notation of lattice theory is used (cf. Birkhoff [1]). If $a, b, c, \cdots$ are elements of a lattice, $a$ covers $b$ means (i) $a>b$, (ii) $a\neq b$, and (iii) $a>c>b$ implies $a=c$ or $c=b$. Arrows such as $\rightarrow$ and $\leftrightarrow$ will be used to indicate one way and two way implication, respectively. If $a$ and $b$ are elements of a ring, $a$ divides $b$ will sometimes be written $a|b$, and $a$ and $b$ relatively prime will be indicated by $(a,b)=1$.

## Section I

Let $\mathfrak{M}$ be a closed associative system with elements $A$, $B$, $C$, . . . and a unique right and left unit element $I$. The closure operation is written as a multiplication and the identity of two elements $A$ and $B$ of $\mathfrak{M}$ is indicated by $A \equiv B$. The set consisting of the elements of $\mathfrak{M}$ forms a partially ordered set $\mathfrak{O}$ if the ordering relation $>$ is defined by

$$A > B \longleftarrow B \equiv AC, \qquad A, B, C \in \mathfrak{M}$$

and the associated equivalence relation $=$ by

$$A = B \longleftarrow A > B, B > A, \qquad A, B \in \mathfrak{M}.$$

For $A \equiv AI$ implies $A > A$ for each element $A$ of $\mathfrak{M}$, and the transitivity of the ordering relation may easily be verified to depend on the associativity of the closure operation of $\mathfrak{M}$. Since $A \equiv IA$ it follows $I > A$ for each element $A$ of $\mathfrak{O}$; thus $I$, the unit element of $\mathfrak{M}$, is also the unit element of $\mathfrak{O}$. Of course there is another partially ordered set $\mathfrak{O}^*$ which the elements of $\mathfrak{M}$ form with respect to the ordering relation of right division, i.e.

$$A > B \longleftarrow B \equiv CA.$$

However $\mathfrak{O}$ and $\mathfrak{O}^*$ are abstractly identical and we will confine our attention to $\mathfrak{O}$.

The set of elements of $\mathfrak{M}$ which possess inverses forms a group which will be denoted by $\mathfrak{I}$. $\mathfrak{I}$ is not a null set since

$J$ is its own inverse. It is easily seen that $A=B$ if and only if there is an element $J$ of $\mathcal{J}$ such that $A \equiv BJ$.

An element $P$ of $\mathcal{M}$ will be called a prime if $P \equiv AB$ implies that one and only one of $A$ or $B$ is an element of $\mathcal{J}$. It is a simple matter to show that

$$A \text{ covers } B \longrightarrow B \equiv AP, \ P \text{ a prime.}$$

For $A > B$ implies $B \equiv AP$, and $A \neq B$ implies $P$ is not an element of $\mathcal{J}$. Suppose $P \equiv QR$; then $B \equiv AQR$, and $A > AQ > AQR \equiv B$. Since $A$ covers $B$, either $A = AQ$ or $AQ = AQR$; hence one and only one of $Q$ or $R$ is in $\mathcal{J}$, and $P$ is a prime. However the converse

(1.1) $$B \equiv AP, \ P \text{ a prime} \longrightarrow A \text{ covers } B$$

is not in general true without some additional assumption on $\mathcal{M}$. If $B \equiv AP$, $P$ a prime, it does follow that $A > B$ and $A \neq B$. Suppose $A > C > B$; then $B \equiv CR$, $C \equiv AQ$, and $B \equiv AQR$. Thus

(1.2) $$B \equiv AQR \equiv AP.$$

If $\mathcal{M}$ is a semi-group in which left cancellation is permissible we may conclude $QR \equiv P$, and since $P$ is a prime, one of $Q$ or $R$ is in $\mathcal{J}$, thus proving (1.1). However left cancellation is only a sufficient condition for (1.1) to hold, and we shall see in our study of matrices that (1.1) may be proved by an argument on the "norms" of the elements involved without any appeal to the cancellation law.

If $P$ is a prime and $P = Q$, then $Q$ is a prime, i.e. $P$ a prime implies each element of the set $P\mathcal{J}$ is a prime. Also if $P$ is a prime then each element of the set $\mathcal{J}P$ is a prime, though

$P \neq JP$ in general, for $J$ in $\mathfrak{J}$. Thus there may be associated a class of primes $\mathfrak{J}P$ with each prime $P$ of $\mathfrak{M}$ and each prime of $\mathfrak{M}$ is in one and only one of these classes. Suppose the following condition holds:

$\mathfrak{C}$. If an element $A$ of $\mathfrak{M}$ has one decomposition as the product of primes belonging to a single class $\mathfrak{J}P$, $P$ a prime, then all decompositions of $A$ as a product of primes has as its prime factors only primes of $\mathfrak{J}P$. $A$ will then be called a primary element with respect to $\mathfrak{J}P$.

$\mathfrak{C}$ implies the set of primary elements with respect to a fixed set of primes $\mathfrak{J}P$ is closed under the closure operation of $\mathfrak{M}$, i.e. if $A$ and $B$ are primary elements with respect to $\mathfrak{J}P$, then $AB$ is also a primary element with respect to $\mathfrak{J}P$. Thus if $\mathfrak{P}$ denotes the set of all primary elements with respect to $\mathfrak{J}P$ together with the set $\mathfrak{J}$, then $\mathfrak{P}$ is a closed associative system with the same unique right and left unit $I$ as $\mathfrak{M}$. The elements of $\mathfrak{P}$ also form a partially ordered set with respect to left division, which we denote by $\mathfrak{D}_{\mathfrak{P}}$.

We will now investigate an important instance of the above theory in which

(i) the partially ordered set $\mathfrak{D}$ is a lattice,

(ii) each partially ordered set $\mathfrak{D}_{\mathfrak{P}}$ is a sublattice of $\mathfrak{D}$, and

(iii) the lattice $\mathfrak{D}$ is a direct product of the sublattices $\mathfrak{D}_{\mathfrak{P}}$.

Henceforth $\mathcal{M}$ shall denote the set of all non-singular $n \times n$ matrices with elements in the ring $\mathcal{R}$ of rational integers. The determinant of a matrix $A$ will be called its norm and will be denoted by $n(A)$. Thus a matrix $A$ is non-singular if and only if $n(A) \neq 0$. The associative closure operation is taken as row by column matric multiplication, and the unique right and left unit $I$ is the $n \times n$ matrix with 1's in the principal diagonal positions and 0's elsewhere. Though we are restricting $\mathcal{R}$ to be the ring of rational integers in order to simplify the notation and avoid circumlocutions regarding associates, many of our main results hold when $\mathcal{R}$ is any principal ideal ring.

Matrices which possess inverses, i.e. elements of the group $\mathcal{J}$, will be called unimodular, while the term unit matrix will be reserved for $I$ (cf. MacDuffee [1], p. 30). A matrix is unimodular if and only if its norm is a unit of $\mathcal{R}$ (MacDuffee [1], Theorem 20.1). If $A \equiv B J$, where $J$ is unimodular, we shall call $A$ and $B$ right associates or simply associates. Thus $A = B$ if and only if $A$ and $B$ are associates.

Matrices which are neither unimodular nor prime will be called composite. A composite matrix can be expressed as a product of at most a finite number of primes (MacDuffee [1], Theorem 20.3). It is clear that if the norm of a matrix $A$ is a prime of $\mathcal{R}$, then $A$ is a prime of $\mathcal{M}$. The converse is a corollary of the following theorem.

Theorem 1.1. If the norm of a non-singular matrix $A$ is divisible by a prime $p$ of $\mathcal{R}$, there exists a prime matrix $P$ of $\mathcal{M}$ such that

(i) $n(P) = p$,

(ii) $A \equiv BP$, $B$ an element of $\mathcal{M}$.

Of course $n(A) = n(B)\,p$ .

In the proof of this theorem we shall apply certain well-known results concerning matrices in Hermite's normal form (see MacDuffee [1], Theorem 22.1). Let $A_1$ be an an associate of $A$ which is in Hermite's normal form. Then

$$A \equiv A_1 J$$

where $J$ is unimodular, and $A_1$ is of the form

$$A_1 \equiv \begin{bmatrix} \alpha^{1,1} & \alpha^{1,2} & \cdots & \alpha^{1,n} \\ & \alpha^{2,2} & \cdots & \alpha^{2,n} \\ & & \ddots & \\ & & & \alpha^{n,n} \end{bmatrix}$$

where all elements below the principal diagonal are 0. Now $n(A_1) = \alpha^{1,1}\alpha^{2,2} \cdots \alpha^{n,n}$, and since $p$ divides $n(A_1)$, $p$ a prime, if follows $p$ divides some $\alpha^{i,i}$ ; let $\alpha^{n,n}$ be the $\alpha$ of smallest superscripts which is divisible by $p$. Let

$$B \equiv \begin{bmatrix} \beta^{1,1} & \beta^{1,2} & \cdots & \beta^{1,n} \\ & \beta^{2,2} & \cdots & \beta^{2,n} \\ & & \ddots & \\ & & & \beta^{n,n} \end{bmatrix}, \qquad P_1 \equiv \begin{bmatrix} 1 & & & k_{1,n} \\ & 1 & & k_{2,n} \\ & & \ddots & \vdots \\ & & 1 & k_{n-1,n} \\ & & & p \\ & & & & 1 \\ & & & & & \ddots & 1 \end{bmatrix}$$

where $\rho$ occurs in the $r^{1}$th row and $r^{1}$th column of $P_1$. Then

$$B \times P_1 \equiv \begin{pmatrix} \beta^{1,1} & \beta^{1,2} & \cdots & \beta^{1,r-1} & \beta^{1,1}k_{1,r} + \beta^{1,2}k_{2,r} + \cdots + \beta^{1,r}\rho & \beta^{1,r+1} & \cdots & \beta^{1,n} \\ & \beta^{2,2} & \cdots & \beta^{2,r-1} & \beta^{2,2}k_{2,r} + \cdots + \beta^{2,r}\rho & \beta^{2,r+1} & \cdots & \beta^{2,n} \\ & & \ddots & & & & & \\ & & & & \beta^{r,r}\rho & \beta^{r,r+1} & \cdots & \beta^{r,n} \\ & & & & & \beta^{r+1,r+1} & \cdots & \beta^{r+1,n} \\ & & & & & & \ddots & \\ & & & & & & & \beta^{n,n} \end{pmatrix}$$

Let $\beta^{i,j} = \alpha^{i,j}$, $i \le j \le n$, $i = 1, 2, \cdots, n$, except when $j = r$. Then $A_1 \equiv BP_1$, if integers $k_{1,r}, k_{2,r}, \cdots, k_{r-1,r}$ and $\beta^{1,r}, \beta^{2,r}, \cdots, \beta^{r,r}$ exist such that

$$\beta^{r,r}\rho = \alpha^{r,r},$$

$$\beta^{r-1,r-1}k_{r-1,r} + \beta^{r-1,r}\rho = \alpha^{r-1,r},$$

$$\beta^{r-2,r-2}k_{r-2,r} + \beta^{r-2,r-1}k_{r-1,r} + \beta^{r-2,r}\rho = \alpha^{r-2,r},$$

$$\cdots \quad \cdots \quad \cdots$$

$$\beta^{2,2}k_{2,r} + \cdots \quad + \beta^{2,r}\rho = \alpha^{2,r},$$

$$\beta^{1,1}k_{1,r} + \beta^{1,2}k_{2,r} + \cdots \quad + \beta^{1,r}\rho = \alpha^{1,r}.$$

The first equation is solvable for $\beta^{r,r}$ by hypothesis. Since $(\alpha^{i,i}, \rho) = (\beta^{i,i}, \rho) = 1$, $i < r$, the remaining equations may be solved one after the other, the second for $k_{r-1,r}$ and $\beta^{r-1,r}$, the third for $k_{r-2,r}$ and $\beta^{r-2,r}, \cdots$, and finally the $r^{1}$th for $k_{1,r}$ and $\beta^{1,r}$. Hence

$$A \equiv (BP_1)J \equiv BP.$$

where $P \equiv P_1 J$ and $n(P) = p$, as was to be shown. That $n(A) = n(B)p$ follows from the general theorem that if $A$ and $B$ are any $n \times n$ matrices, then $n(AB) = n(A)n(B)$.

Corollary 1.1. An element $P$ of $\mathfrak{M}$ is a prime of $\mathfrak{M}$ if and only if $n(P)$ is a prime of $\mathfrak{R}$. If $n(P) = p$, we say that $P$ belongs to $p$.

The following theorem is obtained by an obvious induction on Theorem 1.1.

Theorem 1.2. Each element of $\mathfrak{M}$ has a decomposition as a product of primes which belong to the prime factors of the norm of the given matrix.

Theorem 1.3. $A$ covers $B$ if and only if

$$B \equiv AP,$$

$P$ a prime. If $n(P) = p$ we say that $A$ covers $B$ with respect to $p$.

The sufficiency has already been demonstrated in the general theory. In proving the necessity assume we have arrived at equation (1.2) in the argument. Then

$$n(A)\,n(Q)\,n(R) = n(A)\,n(P)$$

or

$$n(Q)\,n(R) = n(P)$$

which, with the aid of the corollary above and a property of primes of $\mathfrak{R}$, completes the proof of the theorem.

Corollary 1.3. $A$ covers $B$ if and only if

(i) $A > B$,

(ii) $n(B) = n(A)p$ , $p$ a prime of $\mathfrak{R}$ .

The following two theorems follow directly from Theorems 1.2 and 1.3.

Theorem 1.4. Let $A, B, C$ be non-singular matrices such that

(i) $A > B$, $B \equiv AC$ ,

(ii) $N(C) = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ , where $p_1, p_2, \cdots, p_t$ are primes of $\mathfrak{R}$.

Then every prime chain joining $A$ and $B$ contains $\sum_1^t e_i + 1$ elements (both $A$ and $B$ are included in the chain).

Theorem 1.5. A non-singular matrix has as many distinct decompositions as a product of primes as there are different prime chains joining the matrix to the unit matrix, where two decompositions are distinct if not all corresponding prime matric factors are equal, and two chains are different if they are not identical.

The following theorem holds only when $\mathfrak{R}$ is the ring of rational integers.

Theorem 1.6. There are precisely $p^{n-1}/p-1$ non-associate

prime $n \times n$ matrices belonging to each prime $p$ of $\mathfrak{R}$. The prime matrices are

$$\begin{pmatrix} p & k_{1,2} & \cdots & k_{1,n} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & p & k_{2,3} & \cdots & k_{2,n} \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & p & k_{n-1,n} \\ & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & & p \end{pmatrix}$$

where each $k_{i,j}$, $i<j\leq n$, $(i=1,2,\ldots,n)$ ranges independently through all integer values from $0$ to $p-1$.

The proof is omitted since it is simply a matter of enumerating cases and applying the uniqueness of the canonical associate of a matrix (see MacDuffee [1], Corollary 22.2) If $P$ denotes any one of the prime matrices belonging to $p$ enumerated in the above theorem, then the set $\mathfrak{P}$ of primes referred to in the general theory is the set of primes given in the above theorem together with their associates, i.e. $\mathfrak{P}$ is the set of all primes belonging to $p$. By an argument on the norms of the matrices involved it is clear that condition $\mathfrak{C}$ is fulfilled, and that a primary element of $\mathfrak{M}$ is an element whose norm is a power, say $r \geq 1$, of a prime of $\mathfrak{R}$. $r$ will be called the rank of the primary matrix, and the primary matrix will be said to belong to the prime of $\mathfrak{R}$ of which its norm is a power. Thus a prime is a primary element of rank 1. The rank of a primary matrix will

usually be written as a superscript in parenthesis, e.g. $P^{(r)}$.

Each pair of elements $A$ and $B$ of $\mathcal{O}$ has a greatest common left divisor $A \cup B$ and a least common left multiple $A \cap B$. This was proved by Châtelet [1] when $\mathcal{R}$ is the ring of rational integers. However this can be proved most easily when $\mathcal{R}$ is any ring by appealing to the theory of linear form moduls of order $n$ over a ring $\mathcal{R}$. If $\mathcal{L}$ is such a linear form modul the submoduls of order $n$ of $\mathcal{L}$ form a lattice, in fact a modular lattice, with respect to union and crosscut. If we think of the non-singular $n \times m$ matrices with elements in $\mathcal{R}$ as representatives of the submoduls of $\mathcal{L}$, we can immediately conclude that these matrices form a modular lattice with respect to the ordering relation of left division. (See MacDuffee [1], Theorem 24.1, Corollary 24.1, and Theorem 24.2). Thus associates exist when and only when $\mathcal{R}$ has units, and then they represent the same submodul of $\mathcal{L}$.

Before proceeding with the study of the lattice $\mathcal{O}$ it is interesting to note that when $\mathcal{R}$ is a principal ideal ring the set of $n \times m$ matrices with elements in $\mathcal{R}$ satisfy the following five conditions with respect to matric multiplication:

(i) closure,

(ii) associativity,

(iii) $A = B \rightarrow CA = CB$,

(iv) $C(A \cup B) = CA \cup CB$,

(v) $IA = AI = A$, $I$ the unit matrix.

Thus matric multiplication is a non-commutative ideal multiplication over the lattice of $n \times n$ matrices with elements in $\mathfrak{R}$.

Since $\mathfrak{I}$ is a modular lattice, both Birkhoff covering conditions are satisfied (Birkhoff [1], page 34). This fact is used in proving the next theorem.

Theorem 1.7. If $A$ and $B$ are elements of $\mathfrak{I}$ such that

$A \cup B$ covers $B$ with respect to the prime $p$,

then $A$ covers $A \cap B$ with respect to $p$.

By an inductive argument the proof may be reduced to the case in which $A \cup B$ covers $A$ as well as $B$, so that $A$ and $B$ cover $A \cap B$. Each of these coverings is with respect to primes of $\mathfrak{R}$, so that

$$B \equiv (A \cup B) P, \quad A \equiv (A \cup B) P',$$

$$A \cap B \equiv BQ \quad , \quad A \cap B \equiv AQ' \quad .$$

where $P$, $P'$, $Q$, $Q'$ are primes and we are given $n(P) = p$. Since

$$A \cap B \equiv (A \cup B) PQ \equiv (A \cup B) P'Q'$$

we have

$$n(P)\, n(Q) = n(P')\, n(Q')$$

where each of $n(P)$, $n(Q)$, $n(P')$, and $n(Q')$ is a prime of $\mathfrak{R}$. Hence if $n(Q) = q$ we may conclude that either

$$n(P') = q \text{ and } n(Q') = p,$$

or

$$n(P') = p \text{ and } n(Q') = q.$$

In the former case the theorem is proved. Assume that the latter possibility holds. We will show that it follows that $p = q$, completing the proof. In order to simplify the proof we will appeal to the cancellation law, though this is not necessary. Then

$$PQ \equiv P'Q' \equiv C, \text{ say,}$$

and since $P$ and $P'$ are primes both of which cover $C$, we have

$$C = P \cap P'.$$

Let $P$ and $P'$ be in Hermite's normal form, so that

$$P \equiv \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & p & k_{r,r+1} & \cdots & k_{r,n} \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad P' \equiv \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & p & k'_{s,s+1} & \cdots & k'_{s,n} \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

where all omitted elements are 0's. If $r \neq s$ it is clear that $P$ and $P'$ can not be multiplied on the right by prime matrices in Hermite's normal form to obtain matrices in Hermite's normal form having the same norm unless $p = q$. Assume $r = s$, and let

$$Q \equiv \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & q & l_{r,r+1} & \cdots & l_{r,n} \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad Q' \equiv \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & q & l'_{r,r+1} & \cdots & l'_{r,n} \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

Then

$$PQ \equiv \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & pq & pl_{r,r+1} + k_{r,r+1} & pl_{r,r+2} + k_{r,r+2} & \cdots & pl_{r,n} + k_{r,n} \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

Thus $PQ = P'Q'$ if and only if

$$p l_{r,i} + k_{r,i} \equiv p l'_{r,i} + k'_{r,i} \bmod pq, \qquad i = r+1, r+2, \cdots, n.$$

Hence

$$k_{r,i} \equiv k'_{r,i} \bmod p, \qquad i = r+1, r+2, \cdots, n,$$

and $P = P'$, implying $A = B$, contrary to our hypothesis that $A \cup B$ covers $B$. Hence the theorem.

An obvious induction gives the following result.

Theorem 1.8. If $A$ and $B$ are elements of $\mathfrak{d}$, then

$$n(A)\, n(B) = n(A \cap B)\, n(A \cup B).$$

The norm is thus a multiplicative type of modular functional. If $n(A) = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, the $p_i$ primes, the usual additive modular functional is $\rho(A) = \sum_1^t e_i$, and

$$\rho(A) + \rho(B) = \rho(A \cap B) + \rho(A \cup B).$$

Theorem 1.9. The set of all primary elements of $\mathfrak{d}$ belonging to a fixed prime, say $p$, together with the set $\mathfrak{I}$ of unimodular elements form a dense modular sublattice of $\mathfrak{d}$. This sublattice will be denoted by $\mathfrak{d}_p$.

This follows directly from Theorem 1.8, since $n(A) = p^r$, $n(B) = p^s$ implies $n(A \cap B) = p^u$, $n(A \cup B) = p^v$, where $r+s = u+v$.

We adopt the convention of calling a unimodular element a primary element of rank zero and belonging to each prime of $\mathfrak{R}$. Thus $P^{(\omega)}$ denotes a unimodular matrix.

Theorem 1.10. Let $A$ be an element of $\mathcal{O}$ such that

$$n(A) = p^r k$$

where $p$ is a prime of $\mathcal{R}$ and $(p, k) = 1$. Then there exists a decomposition of the form

$$A \equiv P^{(r)} K$$

where $P^{(r)}$ is a primary element of rank $r$ belonging to $p$, and this decomposition is unique in the sense that if also

$$A \equiv P_1^{(r)} K_1$$

where $P_1^{(r)}$ is a primary element of rank $r$ belonging to $p$, then $P^{(r)} = P_1^{(r)}$. $P^{(r)}$ shall be called the maximal left primary factor of $A$ with respect to $p$.

That there exists a decomposition of the form stated in the theorem is clear from Theorem 1.3. If there are two such decompositions we have $P^{(r)} > A$, $P_1^{(r)} > A$, and hence $P^{(r)} \cap P_1^{(r)} > A$. If $P^{(r)} \neq P_1^{(r)}$, then $P^{(r)} \cap P_1^{(r)}$ is a primary element belonging to $p$ and of rank greater than $r$, a contradiction to $(p^r, k) = 1$. Hence the theorem.

By an induction we have the following theorem.

Theorem 1.11. Corresponding to each order of the distinct prime factors of the norm $n(A)$ of a non-singular matrix $A$ there exists a unique

decomposition of $A$ as the product of primary matrices belonging to the prime factors of $n(A)$.

Theorem 1.12. Let $A$ be an element of $\mathcal{O}$ having the maximal left primary factor $P^{(r)}$ of norm $p^r$, $p$ a prime. Then all primary elements which belong to $p$ and divide $A$ also divide $P^{(r)}$.

For if $P_i^{(s)}$ is a primary element which belongs to $p$ and divides $A$ but does not divide $P^{(r)}$ we have

$$P^{(r)} > P^{(r)} \cap P_i^{(s)} > A$$

where the first containing is proper. This is in contradiction to $P^{(r)}$ being the maximal left primary factor of $A$ with respect to $p$.

A restatement of the above theorem follows.

Corollary 1.12. The maximal left primary factor of an element of $\mathcal{O}$ with respect to a prime $p$ is the meet of the set of all its left primary factors belonging to $p$.

Two elements $A$ and $B$ of $\mathcal{O}$ will be called relatively prime if and only if their join is an element of $\mathcal{J}$, i.e. if and only if $A \cup B = I$. Thus two elements of $\mathcal{O}$ are relatively prime if and only if their only common left factors are unimodular elements.

Theorem 1.13. Two elements $A$ and $B$ of $\mathcal{O}$ are relatively

prime if and only if

$$n(A \cap B) = n(A)\, n(B).$$

This is a consequence of Theorem 1.8 and the discussion above.

Theorem 1.14. If $A$ and $B$ are elements of $\mathfrak{I}$ such that $n(A)$ and $n(B)$ are relatively prime elements of $\mathfrak{R}$, then $A$ and $B$ are relatively prime elements of $\mathfrak{I}$.

For $n(A \cup B)$ is a factor of both $n(A)$ and $n(B)$; hence $n(A \cup B)$ is a unit of $\mathfrak{R}$ and $A \cup B$ is unimodular. The converse of this theorem is not in general true.

Corollary 1.14. Primary elements of $\mathfrak{I}$ belonging to different primes of $\mathfrak{R}$ are relatively prime.

Theorem 1.15. Each element of $\mathfrak{I}$ is equal to the meet of its maximal left primary factors.

Let $n(A) = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $A$ is an element of $\mathfrak{I}$ whose maximal left primary factors are $P_1^{(e_1)}, P_2^{(e_2)}, \ldots, P_t^{(e_t)}$ belonging to the distinct primes $p_1, p_2, \cdots, p_t$, respectively. Since

$$P_i^{(e_i)} > A, \qquad i = 1, 2, \ldots, t,$$

we have

$$P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_t^{(e_t)} > A.$$

By an obvious induction on Corollary 1.14 and Theorem 1.13,

$$n(P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_t^{(e_t)}) = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} = n(A).$$

But if $B$ and $C$ are elements of $\mathfrak{I}$ such that $B > C$ and $n(B) = n(C)$, then $B = C$.

Hence

$$A = P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_t^{(e_t)}.$$

This representation of $A$ is unique since the maximal left primary factors of $A$ are unique.

Now let $p_1, p_2, \cdots, p_i, \cdots$ be some ordering of the primes of $\mathcal{R}$. Applying the convention mentioned just before Theorem 1.10, we may write

$$A = P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_i^{(e_i)} \cap \cdots$$

where $P_i^{(e_i)}$ is the maximal left primary factor of $A$ with respect to the prime $p_i$. We will refer to $P_i^{(e_i)}$ as the component of $A$ with respect to $p_i$; only a finite number of the components of an element of $\mathcal{O}$ are not unimodular. Corresponding components of two elements of $\mathcal{O}$ are components belonging to the same prime of $\mathcal{R}$.

Theorem 1.16. Let $A$ and $B$ be two elements of $\mathcal{O}$. Then $A$ divides $B$ if and only if the components of $A$ divide the corresponding components of $B$.

The sufficiency is obvious. Suppose $A > B$, i.e. $B \equiv AC$, $C$ an element of $\mathcal{O}$, and let $P^{(r)}$ be a component of $A$, $A \equiv P^{(r)}K$, $K$ an element of $\mathcal{O}$. Then $B \equiv P^{(r)}KC$, and $P^{(r)}$ is a left primary factor of $B$. Hence by Theorem 1.12 $P^{(r)}$ divides the corresponding maximal left primary factor of $B$.

An immediate corollary is the following decomposition theorem.

Theorem 1.17. Let

$$A = P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_i^{(e_i)} \cap \cdots,$$

$$B = Q_1^{(f_1)} \cap Q_2^{(f_2)} \cap \cdots \cap Q_i^{(f_i)} \cap \cdots,$$

be decompositions of the elements $A$ and $B$ of $\mathcal{D}$ as the meets of their maximal left primary factors where $P_i^{(e_i)}$ and $Q_i^{(f_i)}$, $i = 1, 2, \cdots$, are corresponding components. Then

$$A \cup B = (P_1^{(e_1)} \cup Q_1^{(f_1)}) \cap (P_2^{(e_2)} \cup Q_2^{(f_2)}) \cap \cdots \cap (P_i^{(e_i)} \cup Q_i^{(f_i)}) \cap \cdots,$$

$$A \cap B = (P_1^{(e_1)} \cap Q_1^{(f_1)}) \cap (P_2^{(e_2)} \cap Q_2^{(f_2)}) \cap \cdots \cap (P_i^{(e_i)} \cap Q_i^{(f_i)}) \cap \cdots.$$

Thus the modular lattice $\mathcal{D}$ is the direct product of the (infinite) set of all $\mathcal{D}_{P_i}$ lattices.

In the case $n=1$ we have the well-known theorem that the lattice of elements of $\mathcal{R}$ with respect to g.c.d. and l.c.m. is the direct product of chains whose elements are powers of primes of $\mathcal{R}$. It is only in this case, i.e. $n=1$, that the primary elements of $\mathcal{D}$ are powers of primes of $\mathcal{D}$ only; if $n>1$ the primary elements of $\mathcal{D}$ are not necessarily powers of primes of $\mathcal{D}$, though powers of primes of $\mathcal{D}$ are primaries. Also it is only in the case $n=1$ in which $\mathcal{M}$ is commutative.

We will sometimes refer to the $\mathcal{D}_{P_i}$ lattices as $p_n$-latices, the $n$ indicating the matrices of $\mathcal{D}$ are $n \times n$. The $p_n$-lattices are thus the fundamental lattice-theoretic structural units of the modular lattice of non-singular $n \times n$ matrices. The "top" of the

Hasse diagram of the $3_2$-lattice is shown in Figure 1, as well as the $2_2$-lattice which is seen to be a sublattice of the $3_2$-lattice. In general the $\rho_n$ - lattice is a sublattice of the $q_m$-lattice if $n \leq m$ and $\rho \leq q$. It is conjectured that the lattice shown in Figure 2 is the lattice of largest order which can be generated by three elements $a, b, c$ of a $\rho_n$-lattice for $n = 2$, and possibly larger values of $n$. If $a', b', c'$ are generating elements of a similar lattice, we may form the direct product of the two lattices. It may easily be verified that the elements

$$A = (a, b') \, , \; B = (b, c') \, , \; C = (c, a')$$

generate the free modular lattice of order twenty-eight (there are, of course other triples of elements of the direct product which generate the free modular lattice). The free modular lattice generated by three elements is thus a subdirect product of the direct product of the lattice of Figure 2 with itself. Figure 3 shows some of the elements at the top of the Hasse diagram of the $2_3$-lattice; each element of the $2_3$-lattice is the unit element of such a lattice. It is seen to be a projective geometry, and in fact each element of a $\rho_n$-lattice, $n > 1$, is a unit element of a projective geometry of rank $n+1$.

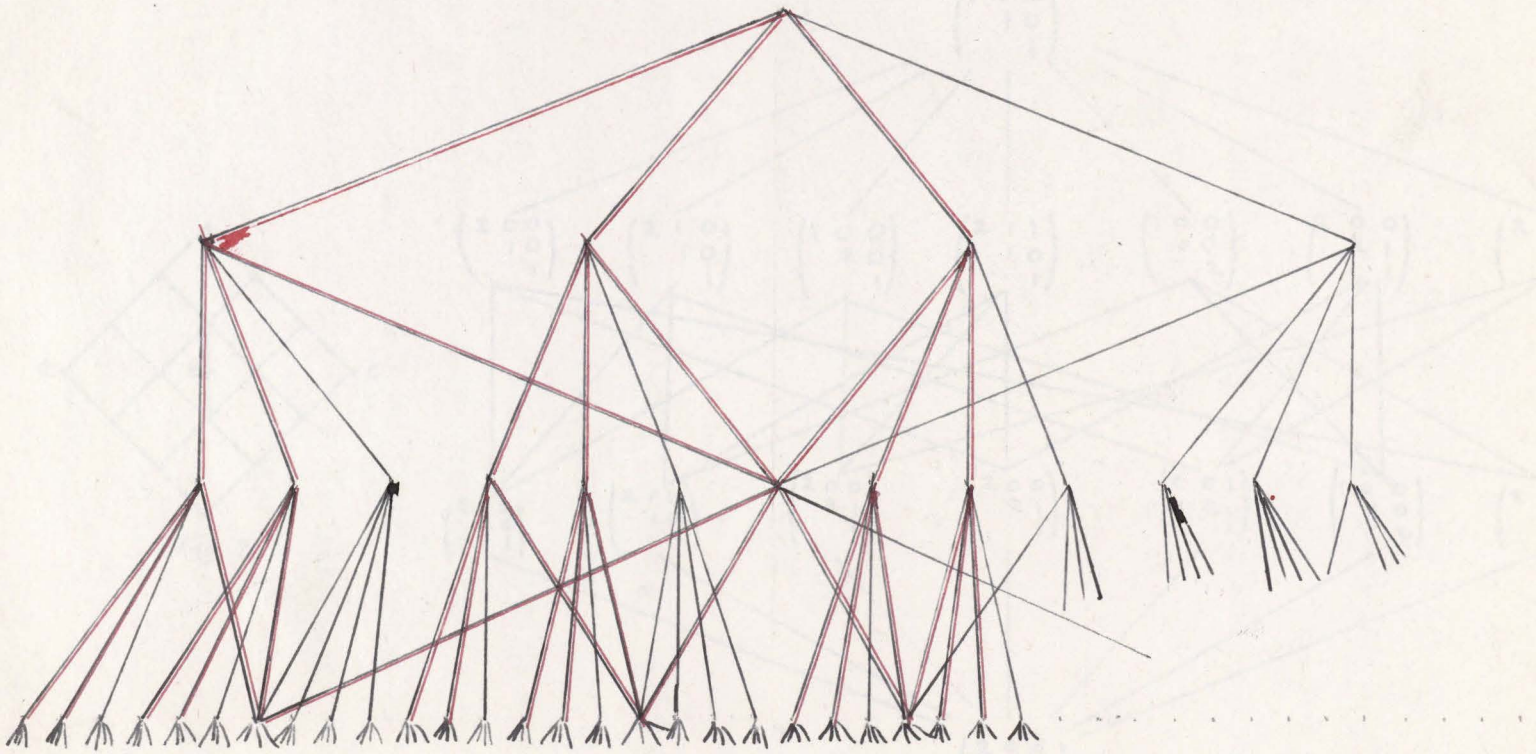

Fig. 1.

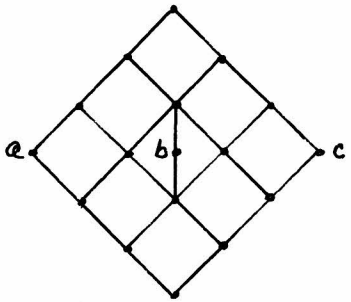


Fig. 2

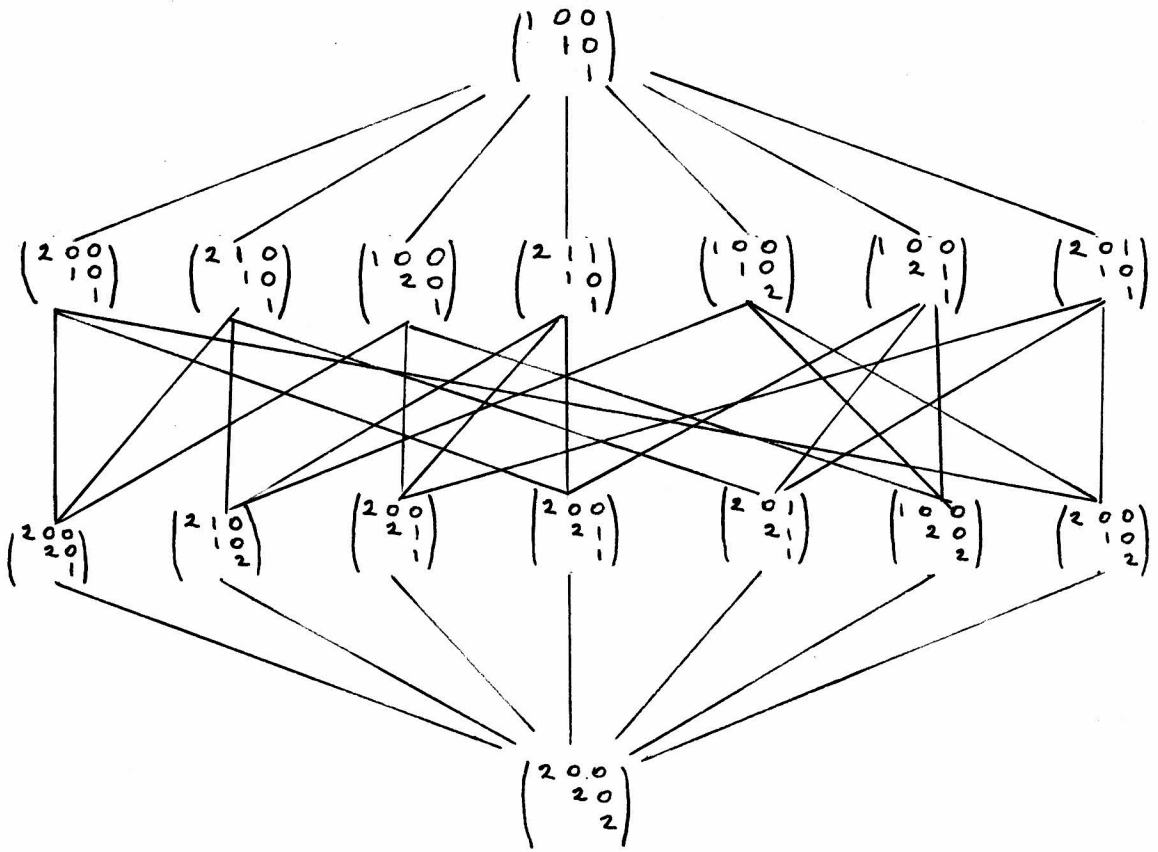

Fig. 3

## Section II

Let $\mathfrak{L}$ be a linear form modul of order $n$ over the ring $\mathfrak{R}$ of rational integers with basis elements $u_1, u_2, \cdots, u_n$. Each submodul of $\mathfrak{L}$ has basis elements of the form $\alpha_j^1 u_1 + \alpha_j^2 u_2 + \cdots + \alpha_j^n u_n$, where the $\alpha_j^i$ are elements of $\mathfrak{R}$. If $\mathfrak{L}_1$ is a submodul of $\mathfrak{L}$ having $m$ such basis elements we may write

$$\mathfrak{L}_1 = (\alpha_1^1 u_1 + \alpha_1^2 u_2 + \cdots + \alpha_1^n u_n, \cdots, \alpha_m^1 u_1 + \alpha_m^2 u_2 + \cdots + \alpha_m^n u_n)$$

or

$$\mathfrak{L}_1 = (u_1\ u_2\ \cdots\ u_n) \times \begin{pmatrix} \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_m^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_m^2 \\ \vdots & & & \\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_m^n \end{pmatrix}$$

Thus the matrix $(\alpha_j^i)$ represents the submodul $\mathfrak{L}_1$ of $\mathfrak{L}$. Every submodul of $\mathfrak{L}$ has a basis of $n$ elements, and hence has a representation as an $n \times n$ matrix. However since we will be dealing with submoduls of $\mathfrak{L}$ before the number of basis elements have been reduced to $n$, it is well to know that the norm of an matrix, and hence of the modul it represents, is the g.c.d. of the set of all $n \times n$ determinants whose columns are chosen from those of the given $n \times m$ matrix (Dedekind [1]). Since each submodul of $\mathfrak{L}$ may be represented by an $n$-rowed matrix, and conversely each $n$-rowed matrix with elements in $\mathfrak{R}$ represents a submodul of $\mathfrak{L}$, we shall speak of $n$-rowed matrices rather than submoduls of $\mathfrak{L}$. Thus two $n$-rowed matrices are equal if and only if they represent the same modul. We are interested in the case in which the basis

elements of $\mathfrak{L}$ are $1, \omega, \ldots, \omega^{n-1}$, where $\omega$ is the root of an $n^{\text{th}}$ degree polynomial with coefficients in $\mathfrak{R}$ and leading coefficient unity, i.e. $\omega$ is an algebraic integer. Each pair of submoduls of $\mathfrak{L}$ may then be multiplied algebraicly, their algebraic product being the submodul of $\mathfrak{L}$ whose basis elements are obtained by multiplying each pair of basis elements of the two moduls. This algebraic multiplication is described in terms of $n$-rowed matrices in the following definition.

Definition 2.1. Let $A$ and $B$ be $n$-rowed matrices with $r$ and $s$ columns, respectively, and let $\mathbf{a} = (1, a_{n-1}, \ldots, a_1, a_0)$ be a $1 \times (n+1)$ matrix with elements in $\mathfrak{R}$, the first element being unity. ($\mathbf{a}$ is called an integral polynomial of degree $n$.) Then the algebraic product of $A$ and $B$ with respect to the integral polynomial $\mathbf{a}$, which we denote by $AB$, is an $n \times rs$ matrix whose columns are obtained by multiplying each column of $A$ with each column of $B$ in the following manner. Let $\alpha_i^1, \alpha_i^2, \ldots, \alpha_i^n$ be the elements in the $i^{\text{th}}$ column of $A$, and $\beta_j^1, \beta_j^2, \ldots, \beta_j^n$ the elements in the $j^{\text{th}}$ column of $B$.

Form the formal polynomials

$$\alpha = \alpha_i^1 x^{n-1} + \alpha_i^{n-1} x^{n-2} + \cdots + \alpha_i^2 x + \alpha_i^1 ,$$

$$\beta = \beta_j^n x^{n-1} + \beta_j^{n-1} x^{n-2} + \cdots + \beta_j^2 x + \beta_j^1 ,$$

$$a = x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0 ,$$

where $x$ is an indeterminant over $\mathfrak{R}$. The polynomials $\alpha$ and $\beta$ may be formally multiplied and reduced modulo $a$, i.e.

$$\alpha\beta \equiv \gamma_\kappa^n x^{n-1} + \gamma_\kappa^{n-1} x^{n-2} + \cdots + \gamma_\kappa^2 x + \gamma_\kappa^1 \pmod{a}$$

Then $\gamma_\kappa^1, \gamma_\kappa^2, \ldots, \gamma_\kappa^n$ are the elements of the column of $AB$ which is the product of the $i$'th column of $A$ and the $j$'th column of $B$.

The algebraic product of two $n$-rowed matrices $A$ and $B$ will not be confused with row-by-column matric multiplication discussed in Section I, which, in this section, will be indicated by $A \times B$. To illustrate algebraic multiplication of matrices let $A$ and $B$ be quadratic moduls

$$A = (2, 1+\omega) \quad , \quad B = (3, 2+2\omega)$$

(in Dedekind's notation) where $\omega$ is a root of

$$a = \omega^2 + \omega + 1 .$$

Then

$$AB = (6, 4+4\omega, 3+3\omega, 2+4\omega+2\omega^2).$$

$$AB = (6, 4+4\omega, 3+3\omega, 2\omega).$$

This may be reduced to canonical form to obtain

$$AB = (2, 1+\omega).$$

In matric notation

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 2 \\ 0 & 2 \end{pmatrix},$$

$$a = (1, 1, 1).$$

In multiplying the columns of $A$ and $B$ only the product of the second column of $A$ with the second column of $B$ need be reduced modulo $a$.

Thus

$$\alpha = x+1,$$
$$\beta = 2x+2,$$
$$a = x^2+x+1,$$

$$\alpha\beta = 2x^2+4x+2 \equiv 2x \pmod{x^3+x+1}.$$

Hence

$$AB = \begin{pmatrix} 6 & 4 & 3 & 0 \\ 0 & 4 & 3 & 2 \end{pmatrix},$$

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

We record the following well-known properties of algebraic multiplication all of which go back to Dedekind. $A$, $B$, $C$ are any $n$-rowed matrices.

(i) (Closure) $AB$ is an $n$-rowed matrix.

(ii) (Associativity) $(AB)C = A(BC)$.

(iii) (Commutativity) $AB = BA$.

(iv) $A = B \rightarrow AC = BC$.

(v) $A(B \cup C) = AB \cup AC$.

(iv) and (v) may be used to deduce $A > B \rightarrow AC > BC$. An $n$-rowed matrix $A$ will be called a ring if $A > A^2$. An $n$-rowed matrix $A$ will be called an ideal if

(vi) $IA = A$, where $I$ is the unit $n$-rowed matrix.

The realtion between multiplicative and lattice-theoretic properties of ideals is strong due mainly to (vi). A study of the abstract properties of an arbitrary lattice over which a multiplication satisfying (i) throught (vi) may be defined has been initiated by Ward and furthered by Ward and Dilworth [1]. If $A$ is an ideal, then $A > AB$, and this property may be used to introduce a residuation in the lattice of ideals. However if $A$ and $B$ are $n$-rowed matrices, not ideals, it is not in general true that $A > AB$. In fact any one of the following possibilities may occur: $A > AB$, or $A = AB$, or $AB > A$, or $A$ may not be related to $AB$ through containing. It is not difficult to find algebraic moduls which satisfy $A = A^s$, $s \geq 1$, while $A \neq A^n$ if

$1<r<3$; in fact this property of forming a cyclic group of finite order under algebraic multiplication probably holds for all $n$-rowed matrices satisfying $IA=I$, i.e. $n$-rowed matrices which "generate" the unit matrix. $IA$ is always an ideal, where $A$ is any $n$-rowed matrix. For $I(IA) = I^2A = IA$. We say that $IA$ is the ideal that $A$ generates. $A$ is an ideal if and only if it generates itself. In this connection the following interesting but as yet unanswered question may be raised. Suppose $A$ is an ideal such that $A=BC$ where $B$ and $C$ are non-unit ideals, and suppose that $A_1$ is an $n$-rowed matrix which generates $A$, i.e. $IA_1 = A$. Then do there exist $n$-rowed matrices $B_1$ and $C_1$ such that $A_1=B_1C_1$, where $B_1$ generates $B$ and $C_1$ generates $C$?

A few of the peculiarities of the multiplicative properties of general $n$-rowed matrices are given above to emphasize the weakness of the relationship between their multiplicative and lattice theoretic properties. It is therefore all the more surprising that there is a certain regularity in this respect based upon the decomposition Theorem 1.17. We will need the following lemmas

Lemma 2.1. Let $A$ be an $n$-rowed matrix such that all the elements of a column of $A$ have a factor, say $k$, in common, and let $A_1$ be the $n$-rowed matrix which $A$ becomes on deleting the factor . Then

$$n(A) \mid k\,n(A_1).$$

where the multiplication (e.g. $\epsilon^{1,1}a_1$) is the usual scalar multiplication of matrices by elements of $R$, and the addition is term for term addition of matrices. Then

$$AB = (a_1b_1, a_1b_2, \cdots, a_1b_n, a_2b_1, \cdots, a_2b_n, \cdots, a_nb_1, a_nb_2, \cdots, a_nb_n),$$

$$CD = (c_1d_1, c_1d_2, \cdots, c_1d_n, c_2d_1, \cdots, c_2d_n, \cdots, c_nd_1, c_nd_2, \cdots, c_nd_n),$$

where the multiplications $a_ib_j$ and $c_kd_l$ are the polynomial multiplications described in Df. 2.1 reduced modulo some fixed integral polynomial. The remainder of the proof consists in repeated application of Lemma 2.1. Thus, since

$$c_1d_1 = \epsilon^{1,1}\varphi^{1,1}a_1b_1$$

we have

$$n(CD) \mid \epsilon^{1,1}\varphi^{1,1}\, n(a_1b_1, c_1d_2, \cdots, c_1d_n, c_2d_1, \cdots, c_nd_n).$$

But

$$c_1d_2 = \epsilon^{1,1}\varphi^{1,2}a_1b_1 + \epsilon^{1,1}\varphi^{2,2}a_1b_2.$$

Hence, subtracting $\epsilon^{1,1}\varphi^{1,2}$ times the first column from the second column, and then applying Lemma 2.1,

$$n(CD) \mid (\epsilon^{1,1})^2\varphi^{1,1}\varphi^{2,2}\, n(a_1b_1, a_1b_2, c_1d_3, \cdots, c_1d_n, c_2d_1, \cdots, c_nd_n).$$

But

$$c_1d_3 = \epsilon^{1,1}\varphi^{1,3}a_1b_1 + \epsilon^{1,1}\varphi^{2,3}a_1b_2 + \epsilon^{1,1}\varphi^{3,3}a_1b_3.$$

Hence if we subtract the linear combination $\epsilon^{1,1}\varphi^{1,3}a_1b_1 + \epsilon^{1,1}\varphi^{2,3}a_1b_2$ of the first two columns from the third column, and then apply Lemma 2.1, we obtain

$$n(CD) \mid (\epsilon^{1,1})^3\varphi^{1,1}\varphi^{2,2}\varphi^{3,3}\, n(a_1b_1, a_1b_2, a_1b_3, c_1d_4, \cdots, c_1d_n, c_2d_1, \cdots, c_nd_n).$$

The procedure should now be clear. For example after the first $n$ columns have been thus treated we find

$$n(CD) \mid (\epsilon^{1,1})^n \varphi^{1,1}\varphi^{2,2}\cdots\varphi^{n,n}\, n(a_1b_1, a_1b_2, \ldots, a_1b_n, c_2d_1, \ldots, c_2d_n, \ldots, c_nd_n).$$

Continuing in this fashion we finally obtain

$$n(CD) \mid (\epsilon^{1,1})^n(\epsilon^{2,2})^n\cdots(\epsilon^{n,n})^n(\varphi^{1,1}\varphi^{2,2}\cdots\varphi^{n,n})^n\, n(AB),$$

as was to be shown.

Theorem 2.1. The algebraic product of two primary matrices belonging to the same prime $p$ is also a primary matrix belonging to $p$.

Let $P_1^{(n)}$, $P_2^{(s)}$ be primary matrices belonging to the prime $p$, and assume they are in canonical form, i.e.

$$P_1^{(n)} \equiv \begin{pmatrix} p^{r_1} & \alpha^{1,2} & \cdots & \alpha^{1,n} \\ & p^{r_2} & \cdots & \alpha^{2,n} \\ & & \ddots & \\ & & & p^{r_n} \end{pmatrix}, \quad P_2^{(s)} \equiv \begin{pmatrix} p^{s_1} & \beta^{1,2} & \cdots & \beta^{1,n} \\ & p^{s_2} & \cdots & \beta^{2,n} \\ & & \ddots & \\ & & & p^{s_n} \end{pmatrix},$$

where some $r_i$ and $s_j$ may be zero, but $\sum_1^n r_i = r$, $\sum_1^n s_j = s$. Now in the algebraic product the following $n$ columns occur

$$\begin{matrix} p^{r_1+s_1} & p^{r_1}\beta^{1,2} & p^{r_1}\beta^{1,3} & \cdots & p^{r_1}\beta^{1,n} \\ & p^{r_1+s_2} & p^{r_1}\beta^{2,3} & \cdots & p^{r_1}\beta^{2,n} \\ & & p^{r_1+s_3} & \cdots & p^{r_1}\beta^{3,n} \\ & & & \ddots & \\ & & & & p^{r_1+s_n} \end{matrix}$$

where no reduction modulo the fixed polynomial is necessary. But the determinant having these $n$ columns is a power of $p$, i.e. $p^{r+s}$, and $n(P_1^{(n)}P_2^{(s)})$ divides this determinant. Hence

$n(P_i^{(r)}P_i^{(s)})$ is a power of $P$, ergo the theorem.

The following theorem states a remarkable multiplicative property of the decomposition of Theorem 1.15 in addition to the laftice-theoretic result of Theorem 1.17.

Theorem 2.2. Let $A$ and $B$ be non-singular $n$-rowed matrices having the decompositions

$$A = P_1^{(e_1)} \cap P_2^{(e_2)} \cap \cdots \cap P_t^{(e_t)} \cap \cdots ,$$

$$B = Q_1^{(f_1)} \cap Q_2^{(f_2)} \cap \cdots \cap Q_t^{(f_t)} \cap \cdots ,$$

described in Theorem 1.15. Then

$$AB = P_1^{(e_1)}Q_1^{(f_1)} \cap P_2^{(e_2)}Q_2^{(f_2)} \cap \cdots \cap P_t^{(e_t)}Q_t^{(f_t)} \cap \cdots ,$$

i.e. the components of the algebraic product of $A$ and $B$ are the algebraic products of corresponding components of $A$ and $B$.

Since

$$P_i^{(e_i)} > A ,$$

$$Q_i^{(f_i)} > B ,$$

it follows

$$P_i^{(e_i)}Q_i^{(f_i)} > AB .$$

Thus $P_i^{(e_i)}Q_i^{(f_i)}$ which is a primary matrix belonging to the prime by Theorem 2.1 is a left factor of $AB$. To prove that $P_i^{(e_i)}Q_i^{(f_i)}$ is the maximal left primary factor of $AB$ with respect to $P_i$ we need only show that $n(AB)$ is not divisible by a larger power of $P_i$ than $n(P_i^{(e_i)}Q_i^{(f_i)})$. Let $A_1 = A$, $B_1 = B$, where

$A_1$ and $B_1$ are canonical matrices. Then

$$A_1 = P_i^{(e_i)} C ,$$

$$B_1 = Q_i^{(f_i)} D ,$$

where $n(P_i^{(e_i)}) = p_i^{e_i}$ , $n(Q_i^{(f_i)}) = p_i^{f_i}$ , and further $(p_i, n(C)) = (p_i, n(D)) = 1$. Therefore by Lemma 2.2

$$n(AB) \mid [n(C)\, n(D)]^n \, n(P_i^{(e_i)} Q_i^{(f_i)}) ,$$

where $p_i$ is not a factor of $[n(C)\, n(D)]^n$ . Hence if $p_i^k \mid n(AB)$ then $p_i^k \mid n(P_i^{(e_i)} Q_i^{(f_i)})$ , and the theorem follows.

An immediate corollary of Theorem 2.2 is the following theorem.

Theorem 2.3. A matrix is a ring or ideal if and only if each of its components is a ring or ideal, respectively.

Theorem 2.2. and the above theorem indicate that in making a further study of the multiplicative properties of algebraic moduls, rings, and ideals it is sufficient to confine attention to the $p_n$-lattices. Thus the $p_n$-lattices are the fundamental units of structure of algebraic moduls for multiplicative as well as lattice-theoretic purposes.

A curious corollary of Theorem 2.2 is the following.

Theorem 2.4. If two relatively prime matrices $A$ and $B$ are such that $(\, n(A) \, , \, n(B) \,) = 1$ , then $AB$ is an ideal.

For, since $(\, n(A) \, , \, n(B) \,) = 1$, at least one component of

each pair of corresponding components of $A$ and $B$ is unimodular. Hence each component of the product $AB$ is an ideal, and hence $AB$ is also. Notice that $A$ and $B$ are in <u>any</u> $n$'th degree algebraic number ring. Thus, for example, the product of primary matrices belonging to distinct primes is an ideal, always.

References

G.Birkhoff

1. Lattice Theory, 1940.

A. Châtelet

1. Groupes abeliens finis Paris, 1924.

R. Dedekind

1. Gesammelte mathematische Werke, Dritter Band, Über die Theorie der ganzer algebraischen Zahlen.
2. Gesammelte mathematische Werke, Zweiter Band, Über die von drei Moduln erzeugte Dualgruppe.

C. C. MacDuffee

1. The Theory of Matrices (Ergebnisse der Mathematik und ihrer Grenzgebiete), Springer, 1933.

B. L. Van der Waerden

1. Moderne Algebra, Zweiter Teil, (Zweite Auflage), Chapter XV. Also Chapter XIV on Ganze algebraische Grössen.

M. Ward and R. P.Dilworth

1. Risiduated Lattices, Trans. Amer. Math. Soc. vol. 45 (1939) pp. 335-354.