THEORIE DES NOMBRES
BESANÇON

Années 1979-1980
et 1980-1981

ARITHMETIC OF MATRICES OVER DEDEKIND DOMAINS

Asha NARANG

"ARITHMETIC OF MATRICES OVER DEDEKIND DOMAINS"

(Lecture delivered at a Faculty Seminar in Besançon on 2. 4. 1981).

By Asha NARANG

Elementary number theory is done in the ring $\mathbb{Z}$ of integers. Here one is interested in questions like divisibility which is the same as the solvability of $xa = b$, solvability of diophantine equations including linear equations, system of linear equations i. e. solvability of matrix equation $XA = B$, arithmetical functions, prime factorization and g. c. d. etc ...

These questions have been asked over a Dedekind domain $\mathfrak{o}$ also and can be asked quite meaningfully in the set M of all matrices (with entries) in $\mathfrak{o}$. We have tackled some such problems in M. At times we deal with matrices over k ; k = the field of quotients of $\mathfrak{o}$.

The tools available are :

(1) The theory developed by Siegel (Ann. of Maths, vol. 38, 1937) to deal with matrices (including singular matrices) over the ring of integers of an algebraic number field, which has been extended to the case of Dedekind domains by Bhandari (Ph. D. Thesis, Panjab Univ., Chandigarh, India, 1975). In particular, we use the existence of units, generalized inverses, their properties and notion of discriminant of a matrix. To recall :

Definition : Let A be any matrix in k (notation : $A \in k$). An integral matrix C (i. e. $C \in \mathfrak{o}$) of the same rank as that of A and satisfying $CA = A$ is called a left unit of A.

Such a unit exists. In fact, these are infinitely many unless the rank r(A) of A equals the number of rows of A, in which case the identity matrix is the only left unit of A. Similarly a matrix $D \in \mathfrak{o}$ with $r(D) = r(A)$ and satisfying $AD = A$ is called a right unit of A. Further, if D_1 and D_2

are right units of A, then $D_1 D_2 = D_1$; so that, in particular, units are idempotents.

Definition : Given a matrix A with a left unit C, there exists a matrix X with $r(X) = r(A)$ satisfying $AX = C$. The additional condition $DX = X$ where D is a right unit of A, makes X unique. This unique X, denoted by A^{-1}, is called the generalized C, D-inverse of A.

For a matrix A in k, $\delta(A)$ stands for the ideal generated by r(A)-rowed minors of A. It is called the discriminant of A. If $A \in o$ has discriminant o, we say A is a primitive matrix. If A is non-singular, $\delta(A) = (\det A)$. So, primitive matrix is a generalization of a unimodular matrix.

A matrix A is said to be left C-reduced (or C-reduced on left) if $CA = A$.

(2) The theory of modules over Dedekind domains, especially the theorem of Chevalley and Steinitz, which helps reduce some of the problems to the case of generalized diagonal matrices (i. e. direct sum of matrices of rank 1).

(3) The observation that matrices of rank 1 behave almost like elements of o and especially the observation that $A \in k$, $r(A) = 1$ is integral if and only if $\delta(A) = o$.

Let us first consider the solvability (in o) of

$$XA = B \qquad \text{(I)}$$

Solvability of (I) imposes certain natural conditions on matrices A and B e. g. $BD = B$ for any right unit D of A, which incidentally also implies that $r\left(\begin{pmatrix} A \\ B \end{pmatrix}\right) = r(A)$. We shall assume that these necessary conditions are always there and therefore we shall not mention them everytime. Clearly, the solvability of (I) implies the solvability of

$$XAV = BV \quad \text{for any matrix } V \in o \qquad \text{(II)}$$

On the other hand, solvability of (II) would imply solvability of (I) provided V is a "cancelable" matrix e. g. if V is a unimodular matrix or more generally if V is a left D-reduced matrix. So $XA = B$ is solvable

$\Leftrightarrow XAV = BV$ is solvable for any left D-reduced matrix $V \in o$

$\Leftrightarrow Y\mathcal{U}AV = BV$ is solvable for primitive reduced matrices $\mathcal{U}$ and V.

This would be of any use if we can find primitive reduced matrices $\mathcal{U}$, V such that $\mathcal{U}AV$ is "simple". In this direction, we have proved :

The equivalence class $\mathcal{U}AV$, $\mathcal{U}$ and V primitive reduced, contains a matrix

$$A^* = \operatorname{diag}[A_1, \ldots, A_n] = \begin{pmatrix} A_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & A_2 & 0 & \cdot & \cdot & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & A_n \end{pmatrix}$$

where A_i are 2×2 rank 1 matrices and $\delta(A_i) \mid \delta(A_{i+1})$ for each i. Moreover $a_i = \delta(A_i)$ are uniquely determined and are nothing but $\delta_i(A)\left(\delta_{i-1}(A)\right)^{-1}$; where by $\delta_i(A)$ we mean the ideal generated by i-rowed minors of A.

This is similar to the classical result of Smith over $\mathbb{Z}$, namely Smith normal form of a matrix. We shall say therefore that A^* is in the generalized Smith normal form (S.N.F.) and write $A \sim A^*$; and that $a_i = \delta(A_i)$ are S.N.F. invariants of A.

Using this we proved :

If $r\left(\binom{A}{B}\right) = r(A)$ then $XA=B$ has an integral solution

$\Leftrightarrow \quad \delta\left(\binom{A}{B}\right) = \delta(A)$

$\Leftrightarrow \quad \binom{A}{B} \sim_L A$, meaning thereby that $\exists$ a primitive reduced matrix W such that $WA = \binom{A}{B}$.

$\Leftrightarrow \quad \binom{A}{B} \sim A$

The non-trivial part is to show that if $\delta\left(\binom{A}{B}\right) = \delta(A)$, then $XA = B$ has an integral solution. We first prove it in case $A = \operatorname{diag}[A_1, \ldots, A_n]$, and $B = \left(b_1\ b_2 \ldots b_{2n}\right)$. The solvability of (I) amounts to solving, for odd i , $\left(x_i\ x_{i+1}\right)A_i = \left(b_i\ b_{i+1}\right)$. We show that under the hypothesis, $\delta(A_i) \mid \delta\left(\left(b_i\ b_{i+1}\right)\right)$ so that $\left(x_i\ x_{i+1}\right)$ is a 1×2 matrix whose discriminant is an integral ideal and hence is an integral matrix.

As it may not always be easy to apply these conditions, we give in terms of S.N.F. invariants of A, a sufficient condition for the solvability of (I), namely : If the last S.N.F. invariant a_n of A divides the first S.N.F. invariant b_1 of B i.e. if $a_n \mid b_1$. Clearly $a_i \mid b_i \quad \forall\, i$ is a necessary condition for solvability of (I).

So it is of interest to determine S.N.F. invariants of matrices. We have shown that

(i) S.N.F. invariants of A^{-1} are just $a_n^{-1}, \ldots, a_1^{-1}$ where $a_1, \ldots, a_n$ are S.N.F. invariants of A.

(ii) If $\left(\delta(A), \delta(B)\right) = 0$, A and B have a common unit then S.N.F. invariants of AB are just $a_1 b_1, \ldots, a_n b_n$ where $a_1, \ldots, a_n$ are S.N.F. invariants of A and $b_1, \ldots, b_n$ are S.N.F. invariants of B. This is a generalization of a result of Newmann. In the absence of the condition $\left(\delta(A), \delta(B)\right) = 0$, the result is false e.g. take $A = \begin{pmatrix} 1 & 1 \\ 0 & \alpha \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ -1 & \alpha \end{pmatrix}$.

(iii) We generalize another result of Newmann and determine S.N.F. invariants of $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, under the condition $\left(\delta(A), \delta(B)\right) = 0$, in terms of those of A and B.

Next we discuss the solvability of matrix equation

$$AX + YB = T \qquad \text{(III)}$$

under natural reduction conditions. If $\left(\delta(A), \delta(B)\right) = 0$, then (III) has an integral solution. Consequently, in case $\left(\delta(A), \delta(B)\right) = 0$, $\begin{pmatrix} A & T \\ 0 & B \end{pmatrix} \sim \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ and S.N.F. invariants of $\begin{pmatrix} A & T \\ 0 & B \end{pmatrix}$ are S.N.F. invariants of $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.

Another question is the solvability of bilinear equation

$$XAY = b \qquad \text{(IV)}$$

This problem over $\mathbb{Z}$ was studied by Frobenius. In case of Dedekind domains, we prove (a necessary and sufficient condition) :

If $r(A) \geq 2$, then (IV) has an integral solution $\Leftrightarrow \delta_1(A) \mid 0b$.

In case $r(A) = 1$, the result is false e.g. let $A = \begin{pmatrix} 3 & 2+\sqrt{-5} \\ 2-\sqrt{-5} & 3 \end{pmatrix} \in \mathbb{Z}[\sqrt{-5}]$ and $b = 1$.

Next we take up another problem. If $XA = B$ has an integral solution, then we shall say that A is a right divisor of B (notation : $A \mid B$). Notice that for any right unit D of B, $AD = A$. We fix up a right unit D of B and consider only such divisors as are right D-reduced. Obviously the number of such A is infinite, because if $A \mid B$ then for every primitive reduced matrix V, the matrix $VA \mid B$. So we identify A with the left equivalent class containing A and ask if we can count the number of left inequivalent right divisors i.e. divisor classes of B. Again this number is infinite unless the residue class ring o/a is finite for all ideals $a \neq 0$. We impose this condition on o and count the number of divisor classes of B. Since divisors of equivalent matrices are in one-one correspondence, we count the number of divisor classes of S.N.F. of B. To count this :

(i) We find, in left equivalence class of A, a matrix T in the generalized Hermite normal form (H.N.F.). In case of rank 2, a matrix in (generalized) H.N.F. looks like $T = \begin{pmatrix} T_1 & 0 \\ T_2 & T_3 \end{pmatrix}$ where T_i are 2×1 matrices and T_3 belongs to a fixed system of "remainders" modulo T_1.

(ii) Count the number of right divisors in H.N.F. of S.N.F. of B.

This number turns out to be finite. We denote it by $d(B)$ and call it "divisor function". In case $r(B) = 1$, $d(B) = d(\delta(B))$. In case $r(B) = 2$, $d(B)$ has recently been evaluated. In case $r(B) \geq 3$, the problem of explict evaluation of $d(B)$ is still unsolved, even for the special case $o = \mathbb{Z}$.

As an application of S.N.F. of a matrix, we have shown the following : If $\delta(A) = p_1 \ldots p_s$ is the prime ideal decomposition of $\delta(A)$, then there exist matrices $p_1, \ldots, p_s$ with $\delta(p_i) = p_i$ such that $A = p_1 \ldots p_s$. Moreover, p_i and p_{i+1} have a common unit. Once it is proved for $s = 2$, it follows for any s. In view of S.N.F. of A, it is enough to prove it in case $r(A) = 1$. To tackle the problem there, the crucial result is :

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a rank 1 primitive matrix and let a be any integral ideal. Then there exists a 2×2 rank 1 matrix $M_a = \begin{pmatrix} g_1 a & g_2 b \\ g_1 c & g_2 d \end{pmatrix}$ with

$\delta(M_a) = a$. If, in addition, M is an idempotent, then $MM_a = M_a$.

Another application of these results is made by Sunder Lal and V. C. Nanda in their joint paper "On coprime symmetric matrix pairs over Algebraic number fields" to appear in Abh. Math. Sem. Univ. Hamburg Band 51, U. Chirstian had considered ϕ function for matrices over $\mathbb{Z}$, ($\phi(c)$ = the number of coprime symmetric residue classes mod c). They extended the definition of ϕ to matrices over the ring of integers of an algebraic number field and have given a recurrence formula for the evaluation of ϕ and shown the multiplicativity of ϕ.

ASHA NARANG
Mathematics Department
Panjab University
CHANDIGARH - 160014
INDIA