CHAPTER - I

PART - I

6. This chapter is devoted to a discussion of the reduction theory of quadratic forms over the field of rational functions in one variable over a finite field. A short account of the indefinite forms is also given. Results analogous to the known theorems of Siegel [5] are mentioned. These analogues include the improvements, due to Siegel, of the Hasse - Witt theorems the proofs of which are also sketched here in view of their importance in the main theory. We begin with the following.

Definition:

A form $\sum_{i,j=1}^{m} A_{ij} x_i x_j$, $A_{ij} \in K$ is said to represent zero nontrivially if it takes the value zero for a set of values of $(x_1, \ldots, x_m)$ all of which are not zero simultaneously.

We start with the known theorem of Hasse and Witt with a proof due to Hasse modified in a suitable way.

Theorem I : [Hasse - Witt]

a. If $\gamma[x]$ is a quadratic form of nonzero determinant and with coefficients from k, K, it is a zero form if and only it is an f-adic zero form for all prime polynomials f and at $1/x$

b. If $\gamma[x]$ is a quadratic form with nonzero determinant and with coefficients from $k(x)$ then it represents in $k(x)$ an element $f_1 \in k(x)$ if and only if it represents f_1 in K_f for all f and at $1/x$; that is, for values of X_i in K_f and $K_{1/x}$ where the X_i are the variables of the form $\gamma[x]$.

Definition:

A unit of a symmetric matrix γ is an integral matrix with determinant an element in k , satisfying the equation $U'\gamma U = \gamma$

The proof of Hasse-Witt theorem which is given here is only a general exposition of a known result. It is a direct analogue of the proof of Hasse given in the case of the rational number field. The generalization of the Hasse symbol is also used here. This symbol is also used to prove that the units of an indefinite symmetric matrix are infinite in number. Very elementary properties of the symbol are used in the proofs. A proof of this last statement can be found in Eichler [20] Jkm 16·1 p103

Proof of Hasse - Witt theorem:

(1) m = 2

$\gamma[x]$ is of the form $Ax^2 + Bxy + Cy^2$

$A\gamma[x] = (Ax + \frac{By}{2})^2 + (AC - \frac{B^2}{4})y^2$

If $\gamma[x]$ is a zero form in K_f for all f and $K_{1/2}$, then $\frac{B^2}{4} - AC$ is the square of an element from K= $k(x)$

$A\gamma[x]$ is a zero form in $k(x)$ and therefore $\gamma[x]$.

(2) m = 3

There is no loss of generality if $\gamma[x]$ is taken to be of the diagonal and integral form $A_1x_1^2 + A_2x_2^2 + A_3x_3^2$ because a rational transformation gives the first and multiplication by an integer gives the latter. If f be a prime polynomial which divides the determinant of $\gamma[x]$, it can be assumed, without any loss of generality, that f divides one of A_1, A_2, A_3 (say A_3) and that $(A_1, A_2, A_3) = 1$. If $A_1x_1^2 + A_2x_2^2 + A_3x_3^2$ is zero modulo f there exists a polynomial r such that

$$A_1r^2 + A_2 \equiv 0 \pmod{f}$$

the transformation

$$\begin{pmatrix} f & r & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

takes $\gamma[x]$ into a form fG such that the determinant of G is equal to the determinant of $\gamma[x]$ divided by f and G is a zero form in K or K_f if and only if $\gamma[x]$ is. G is equivalent to a diagonal form G' in R_f with the same determinant as G. We can start with G' as the diagonal form and repeat the process on $\gamma[x]$ till we get a form the determinant

of which is a unit. This represents zero nontrivially by a theorem of Chevalley [8] . Therefore $\sigma[x]$ represents zero nontrivially in K. [B.W.Jones. [12]] pp 66 -73

(3) m = 4

If $\sigma[x]$ is of the diagonal form and the determinant of $\sigma[x]$ is a square $\sigma[x]$ can be taken to be of the form $A_1x_1^2 + A_2x_2^2 + A_3x_3^2 + A_4x_4^2$ with any f dividing only two of the coefficients. In case f divides A_1 and A_2 the Hasse symbol,

$$C_f\ \sigma[x] = -A_3'A_4'/f \quad \text{if } A_3 = fA_3',\ A_4 = fA_4'$$

$A_3'x_3^2 - A_4'x_4^2$ can be taken to be of the form fF' where F' is of the form $B_1y_3^2 + 2B_2y_3y_4 + B_3y_4^2$ the determinant of which is $A_3'A_4'$. All these transformation take $\sigma[x]$ into G which has determinant equivalent to the determinant of σ/f^2

If $C_f(\sigma[x]) = -1$, the determinant is not a square because $\sigma[x]$ is a zero form in the field of f -adic numbers and hence $\left(\frac{-A_3'A_4'}{f}\right) = 1$ implies $\left(\frac{A_1A_2}{f}\right) = 1$. Then $A_1x_1^2 + A_2x_2^2$ is taken into f G where the determinant of G is A_1A_2 and $\sigma[x]$ goes into f F' where the determinant of F' is the determinant of $\sigma[x]$ divided by f^2 . Therefore, as in case m=3 the determinant of the form is reduced successively till it is a unit. Then it has a zero for nontrivial values of the variables. If the determinant of $\sigma[x]$ is square free consider $\sigma[x] - x_5^2$ Because it is a zero form in K , $\sigma[x]$ represents N^2 , $N \in R[x]$. $\sigma[x]$ is equivalent to $N^2x^2 + H$. The

Hasse symbol $C_f(H) = 1$ for all f. Then H is a zero form. Therefore $\mathfrak{o}[x]$ is a zero form in K. If $C_f(\mathfrak{o}[x]) = -1$ for some f, H is integrally equivalent to $-N^2y_2^2 + B_1y_1^2 + B_2y_2^2$ and $N^2x^2 + H$ represents zero nontrivially in K. Therefore $\mathfrak{o}[x]$ is a zero form in K. This proves the theorem completely.

7. We shall first prove the theorem, proved by Siegel [10] which is more general than the theorems of Hasse proved above.

Theorem II*: If two quadratic forms with coefficients in K are equivalent in every K_f and $K_{1/x}$ then they are equivalent in K.

The proof is almost the same as in Siegel [10] pp 658

Consider two quadratic forms $F = \sum_{k=1}^{m} A_k x_k^2$, $G = \sum_{k=1}^{n} B_k y_k^2$ with rational coefficients $A_k, B_k \neq 0$ which are equivalent in K_f for all f and in $K_{1/x}$. The product of the determinants, when n=1, is a square in all K_f and $K_{1/x}$ and therefore it is a square in K.

This proves the theorem in the case m=1 because the ratio of the determinants is the square of a trivial unit; this shows that the determinants are elements in K and differ at the most by the square of a trivial unit. Let us assume the theorem for m-1 instead of m. Consider now the quadratic form F. On account of the equivalence of F and G in all K_f and $K_{1/x}$ we see that F-G is a zero form in all these fields, and therefore in K. There exists an integral solution $x = x^{(1)}$, $y = y^{(1)}$ of $F = G$ with $x_1 \neq 0$. Otherwise F and G are zero forms in K

* Lemmas 12, 13, 14 Siegel [10] pp 675 - 678

and we can construct a solution $x^{(2)}$, $y^{(2)}$ of $F \simeq G \pmod{\mathfrak{f}^{\alpha}}$ in K. Hence in any case we can find two matrices $\mathfrak{a}$ and $\mathfrak{b}$ with unit determinant and leading columns $x^{(1)}$ and $y^{(1)}$. F and G are taken by the linear transformation of the matrices $\mathfrak{a}$ and $\mathfrak{b}$ respectively into two quadratic forms F_1 and G_1 of the type $F_2 + A x_1^2$, $G_2 + A y_1^2$. (Witt's theorem) F_2 and G_2 are equivalent in all $K_{\mathfrak{f}}$ and $K_{1/\alpha}$. Therefore F_2 and G_2 are equivalent in K; and therefore F_1 and G_1 are equivalent in K. Therefore F and G are equivalent in K.

Definition:

Let F and G be two quadratic forms with integral coefficients. We say that F represents G rationally without essential denominator if there exists, for every polynomial h, a linear transformation

$$x_k = \sum_{l=1}^{m} h_{kl} y_l \quad \{ h_{kl}, k = 1, 2, \cdots m \}$$

h_{kl} are rational and their denominations are prime to h which takes F into G. If also G represents F rationally without essential denominator F and G are said to be in the same genus.

Theorem III*:

(Siegel [10] 659) If two quadratic forms with integral coefficients are equivalent in all $\mathfrak{f}$-adic integers and $K_{1/\alpha}$ then they are also semiequivalent.

Siegel [10] Lemmas 15, 16, 17 pp 678 - 680

Lemma

Let γ be the matrix of a quadratic form with coefficients in K, K_f or $K_{1/x}$. If $\mathcal{U}$ denotes any skew symmetric matrix such that the determinant $|\mathcal{U}+\gamma| \neq 0$ then $\mathcal{L} = (\mathcal{U}+\gamma)^{-1}(\mathcal{U}-\gamma)$ is a unit of γ in that field and $|E-\mathcal{L}| \neq 0$. Conversely if $\mathcal{L}$ is a unit such that $|E-\mathcal{L}| \neq 0$ a skew symmetric matrix $\mathcal{U}$ exists such that $\mathcal{L} = (\mathcal{U}+\gamma)^{-1}(\mathcal{U}-\gamma)$

Proof of the theorem:

(Siegel) For any prime polynomial f a matrix $\mathcal{M}_f$ of R_f exists such that $\gamma[\mathcal{M}_f] = 7$. There exists $\mathcal{M}_0 \in K$ such that $\gamma[\mathcal{M}_0] = 7$ by the theorem proved above.

A matrix $\mathcal{M}_f$ exists in R_f such that $\gamma[\mathcal{M}_f] = \gamma_f$ is a diagonal matrix. Then $\mathcal{M}_f^{-1} \in R_f$. Put

$$\mathcal{L}_f = \mathcal{M}_f^{-1}\mathcal{M}_0\mathcal{M}_f^{-1}\mathcal{M}_f$$

and obtain $\mathcal{R}_f$ a diagonal matrix with diagonal elements ± 1 such that $|\mathcal{L}_f - \mathcal{R}_f| \neq 0$. Further $\gamma_f[\mathcal{R}_f] = \gamma$. Put

$$\mathcal{M}_f^* = \mathcal{M}_f\mathcal{R}_f\mathcal{M}_f^{-1}\mathcal{M}_f \in R_f, \quad \gamma[\mathcal{M}_f^*] = 7$$

because

(Siegel [9])

Let h be any polynomial and f a prime factor of h $\mathcal{L}_f = \mathcal{M}_f^*\mathcal{M}_0^{-1}$ is a unit of γ in R_f, $|E-\mathcal{L}_f| \neq 0$ therefore a skew symmetric matrix exists in R_f such that

$$|\mathcal{U}_f+\gamma| \neq 0$$

If β is any arbitrarily large positive integer, a skew symmetric matrix, with integral elements $\mathfrak{U}_f$ exists in R_f such that the congruence $\mathfrak{U} \equiv \mathfrak{U}_f \ (f^\beta)$ is satisfied for all prime polynomials f which are factors of h; all elements of $\mathfrak{A}_f^*$ are f-adic integers. Hence for sufficiently large β the inequality $|\mathfrak{U}+\mathfrak{V}| \neq 0$, and the rational matrix $\mathfrak{A}^* = (\mathfrak{U}+\mathfrak{V})^{-1}(\mathfrak{U}-\mathfrak{V})$ is f-adically integral for all prime factors of h.

This means that the denominators of the elements of $\mathfrak{A}^*$ are prime to h . On the other hand $\mathfrak{V}[\mathfrak{A}^*] = \mathfrak{V}[\mathfrak{A}_0] = \mathfrak{T}$ Hence $\mathfrak{V}$ represents $\mathfrak{T}$ rationally without essential denominator. Similarly $\mathfrak{T}$ represents $\mathfrak{V}$, that is, $\mathfrak{V}$ and $\mathfrak{T}$ are in the same genus (Siegel [10])

If $\mathfrak{V}$ and $\mathfrak{T}$ are in the same genus, they have the same determinant differing at the most by the square of a unit.

Also the equations

(i) $\mathfrak{x}'\mathfrak{V}\mathfrak{x} \equiv \mathfrak{T} \pmod{f}$

(ii) $\mathfrak{x}'\mathfrak{T}\mathfrak{x} \equiv \mathfrak{V} \pmod{f}$

are solvable in R_f for all f prime or not. $|\mathfrak{T}|/|\mathfrak{V}|$ is a unit at all f and at $1/\infty$ and $|\mathfrak{T}||\mathfrak{V}|$, as it is known, is a square in K so that $|\mathfrak{T}||\mathfrak{V}| / |\mathfrak{V}|^2$ is a square and a unit at all f and at $1/\infty$. Therefore it is the square of a unit.

Definition:

A form $\gamma[x]$ in $k(x)$ or $K_{1/x}$ is said to be definite if it does not represent zero nontrivially in $K_{1/x}$. Otherwise it is said to be indefinite.

4. So far we defined definite and indefinite forms. For the actual existence of the definite forms we have, in the four variables, forms of the type,

$$X_1^2 + a X_2^2 + x X_3^2 + a x X_4^2$$

and other similar forms. The definite ternary forms are partial forms of the definite quaternary forms. Consider $A_1X_1^2 + A_2X_2^2 + A_3X_3^2, A_4X_4^2$ If it is a definite ternary form $A_1X_1^2 + A_2X_2^2 + A_3X_3^2 + A_1A_2A_3X_4^2$ is a definite quaternary form. If $\gamma^{(m)}$ and $\gamma^{(n)}$ are the symmetric matrices the number of solutions of the equation $x'\gamma x = \gamma$ is finite if $\gamma[x]$ and $\gamma[y]$ are definite, and infinite otherwise.

For the definite case it is proved in the following fashion.

Let f be a polynomial of degree ν or $f \in K_{1/x}$ of value p^ν with elements of γ and γ in $K_{1/x}$.

$x'\gamma x = f$ that is, $\sum A_{ij} x_i x_j = f$, $A_{ij} \in K_{1/x}$ has a finite number of solutions which are integral.

To prove this fact f is represented as $a_0 + - - - + a_n p^n$ and Aij as the corresponding p-adic number. Consider the equation $\sum A_{ij} x_i x_j = f$ with these values for Aij and f. It has a finite number

of real integral solutions which correspond to the integral solutions of $\sum A_{ij}x_i x_j = f$ that is, if x_i, x_j are taken as polynomials in $k[x]$. Conversely for every integral solution of the equation $x' \delta x = f$ in $k[x]$ there is an integral solution in the corresponding 'p-adic' equation. The argument can be extended for the more general $\mathfrak{f}$.

We next proceed to consider

PART - II

REDUCTION THEORY

8. Given all the matrices, with a given determinant and with elements in $k_{1/2}$, we can introduce a certain equivalence relation between them and divide them into classes. Of all these classes one is chosen in a certain manner depending on the values of the elements of the matrices and it is called reduced. Further if the set of symmetric matrices has its elements in $k[x]$, it can be proved that the reduced class contains only a finite number of these matrices. The proof of this statement is not too simple. Also reduction theory is used to prove that the units of an indefinite symmetric matrix are finitely generated. As to how this is done will be explained in a subsequent article.

We start with the definition of equivalence.

Equivalence:

A quadratic form $T[x] = \sum_{i,j=1}^{m} A_{ij} x_i x_j$ is said to be equivalent to a form $T[y] = \sum_{i,j=1}^{m} B_{ij} y_i y_j$ if the transformation $x_k = \sum_{l=1}^{m} h_{kl} y_l$ transforms $T[x]$ into $T[y]$ and if a similar transformation takes $T[y]$ into $T[x]$ where $A_{ij}, B_{ij} \in K$ and $h_{kl} \in k(x)$. Let Um denote the group of unimodular matrices from $k(x)$ of order m(integral matrices with determinant a unit). Let T be the symmetric matrix of order m with elements in $K_{1/x}$ and $|T| \neq 0$. For $U \in$ Um, $U'TU$ is said to be equivalent to T. It is an equivalence relation.

Equivalent forms take the same values if x_i, y_i take values in $K_{1/x}$. If U is such that $U'TU = T$, U is called a unit. Units form a group.

Half - Reduced Matrices:

As done by Siegel [13] it can be proved that in each class of T there exists a matrix T_1, satisfying $|T_1[w]| \geq |s_k'|$ for every integral column $w = (w_1, \ldots, w_n)$ with $(w_k, \ldots, w_n) = 1$. If s_k' is an element attained by $T_1[w]$ for some w, $s_k' \neq 0$ for any k because T_1 is definite. The matrix T_1 is called half-reduced. Here we make use of the definiteness of T.

9. Reduced Matrices in $K_{1/x}$.

From Siegel's work it is known that the matrix $\mathfrak{f}$ is equivalent to a matrix $\mathfrak{f}_1$, such that $|s_1'| \leq \cdots \leq |s_n'|$ where $s_1', \cdots, s_n'$ are diagonal elements of $\mathfrak{f}_1$. This is required again at the end of the section in order to give a description of the reduced space of symmetric matrices of a given order.

We shall find a matrix $\mathfrak{f}_0 = (A_{ij})$ equivalent to $\mathfrak{f}_1$ and satisfying the following properties:

(1) $\mathfrak{f}_0$ is half-reduced

(2) $|A_{11}| \leq |\sqrt[n]{D}|$

(3) $|A_{11}| \geq |A_{1j}| \quad j > 1$

(4) If $\mathfrak{f}_0^{n-1}[x]$ is the form corresponding to $\mathfrak{f}_0^{(n-1)}$ with first row and column of $\mathfrak{f}_0$ deleted then $\mathfrak{f}_0^{n-1}[x]$ has the same properties.

Construction of $\mathfrak{f}_0$:

(1) is fatisfied following Siegel [13] (2), (3) and (4) will be proved by induction. The construction for binary forms has been done by Artin [3]*. Actually (4) is a consequence of (1),(2) and (3); but here it is proved first.

Let $s_{11}' = A_{11}$, $|A_{11}|$ is the minimum that $\mathfrak{f}$ or $\mathfrak{f}_0$ can take with respect to the valuation in $1/x$ for integral values c_i of the variables x_i, $i = 1, 2, \cdots, n$

* p182

Form a unimodular matrix with $c_1, \ldots, c_k$ as elements of the first column. This takes $\gamma[x]$ into a form with leading coefficient A_{11}. Further the transformation,

$$x_1 = y_1 + c_{12} y_2 + \cdots + c_{1k} y_k$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x_k = c_{k2} y_2 + \cdots + c_{kk} y_k$$

takes the latter into a form

$$G = \sum_{i,j=1}^{m} A'_{ij} x_i x_j \,, \quad A_{11} = A_{11}$$

contains $y_2, \ldots, y_k$ whose values in terms of $x_1, \ldots, x_k$ depend only on c_{ij}, for $i, j > 1$. Hence G is independent of $c_{12}, \ldots, c_{1k}$. These latter can be determined without altering G_1. The terms containing y_1 are

$$A_{11} y_1^2 + 2 \left(A_{11} c_{12} + \sum_{j=1}^{m} A_{ij} c_{j2}\right) y_1 y_2 + \cdots + 2 \left(A_{11} c_{1k} + \sum A_{ij} c_{jk}\right) y_1 y_k$$

The c_{1i} can be determined so that $|A'_{11}| \geq |A'_{ij}|$, $j > 1$ condition (2) is true for m=1 and the case m=2 has been done by Artin [3]. Assume (2) for n=m-1. If B is the leading coefficient of G_1

$$|B| = |A_{11} A'_{22} - A'^{2}_{12}| \leq \sqrt[m-1]{D_1} \; *$$

where D_1, is the determinant of G ; determinant of $A_{11} G = A_{11}^{m} D$ Determinant of G is also $A_{11} D_1$. Therefore $A_{11}^{m} D = A_{11}^{2} D_1$

Call G_1 and $\gamma_1[x]$, G and $\gamma[x]$

From *

$$|A_{11}^2| \leq |B| \leq |A_{11}^{n+2} D|^{1/m-1} \text{ or}$$

$$|A_{11}| \leq |D|^{1/m}$$

$$|A_{11}| \leq |\sqrt[m]{D}|$$

When we take the valuation of the m^{th} root of D it is the valuation which extends $K_{1/\lambda}$ to $K(\sqrt[m]{D})$

(3) is also an essential property for definite forms if the u values are taken with respect to λ .

Conclusion:

γ is the matrix corresponding to G which we now call $\gamma_0[X]$ and satisfies all the requirements.

γ_0 is called a reduced matrix in the class of γ . If now the $A_{ij}'s$ are assumed to be in $k[\lambda]$ the number of matrices that satisfy the above conditions and which have a given determinant is finite. This proves that the class number of definite symmetric matrices is finite when they have a given determinant. We shall next prove the same for indefinite symmetric matrices.

Let $\gamma = \gamma^{(m)}$ represent the zero matrix of order nontrivially and let r be maximal. Then there is a unimodular matrix U such that

$$U'\gamma U = \begin{pmatrix} 0 & 0 & P \\ 0 & F & Q \\ P' & Q' & G \end{pmatrix}$$

It is explained as follows. Because γ represents the zero matrix of order r, there exists a column $(h_{11}, \cdots, h_{m1})$ $(h_{11}, \cdots, h_{m1})$ which is primitive and is a nontrivial zero of the quadratic form corresponding to γ. We have an integral m by r matrix with the maximum number of columns with the properties (1) the greatest common diviser of the r-rowed minors is a unit and (2) it takes γ into a zero matrix '0' of order r. Call this matrix H. H can be completed to a unimodular matrix by H_0.

$$(H\ H_0) = U$$

$$U'\gamma U = \begin{pmatrix} 0^r & P_1 \\ P_1' & F_1 \end{pmatrix}$$

P_1 is an r by m- r matrix. Because $|\gamma| \neq 0$ the r rows of P_1 are linearly independent, $m - r \geq r$. By the elementary divisor theorem we can find unimodular matrices U_1 and U_2 such that $U_1\ P\ U_2$ is a (P diagonal) matrix (0, P) such that

$$\begin{pmatrix} U_1' & 0 \\ 0 & U_2' \end{pmatrix}\begin{pmatrix} 0 & P_1 \\ P_1' & F_1 \end{pmatrix}\begin{pmatrix} U_1' & 0 \\ 0 & U_2 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & P \\ 0 & U_2' F_1 U_2 & \\ P & & \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & P \\ 0 & F & Q \\ P' & Q' & G \end{pmatrix}$$

$$= \gamma_2$$

$|F|(P)^2 \neq 0$

$\mathcal{F}$ does not represent zero nontrivially for if it does by a further reduction of this type it can be shown that $\mathcal{T}$ represents a zero matrix of order greater than r nontrivially which is a contradiction to the maximality of r .

The matrix

$$\begin{pmatrix} E & 0 & 0 \\ 0 & V & 0 \\ 0 & 0 & E \end{pmatrix}$$

transforms $\mathcal{T}_2$ with a suitable choice of U into one among a finite set depending only on $|\mathcal{T}|$ because $\mathcal{M}$ P can be chosen as those among a finite set depending on $|\mathcal{T}|$

Let $A = A^{(m-2r)}$, $B = B^{(r)}$ with elements in $k(x)$

Put

$$U_3 = \begin{pmatrix} E & A & B \\ 0 & E & 0 \\ 0 & 0 & E \end{pmatrix}$$

$$U_3' \mathcal{T}_2 U_3 = \begin{pmatrix} 0 & 0 & P \\ 0 & F & A'P + Q \\ P' & PA + Q' & G + B'P + PB \end{pmatrix}$$

Because this is just an addition of multiples of rows of (0 0 P) to (0, F, Q) and (P, Q, G) and because we are in $k[x]$ elements of A and B can be chosen so that the elements of γ_2 are less in value than those of the diagonal elements of P and therefore determinant of γ .

Because there exist only a finite number of elements witha given value there exist only a finite number of such matriees with A and B as required. Therefore the class number of matrices, definite or indefinite, with a given determinant is finite.

10. <u>The Reduced Definite Symmetric Matrices</u>.

In the construction of the half-reduced matrices on page 31 we managed to choose $A_{11}, \text{---}, A_{nn}$ the diagonal elements such that $|A_{11}| \leq \text{---} \leq |A_{nn}|$

The condition (3) of the reduced matrices is obtained by choosing C_{1i} so that $|A'_{11}| \geq |A'_{ij}|$, $j > 1$ on page 31 . Also the choice of C_{1i} is possible in such a way that $|A'_{12}|$ is the smallest value with respect to $1/x$ After the required C_{1i} are chosen, that is C_{12} ---------, C_{22} --------- C_{j2} --------- C_{m2}--------- We can choose C_{13}, C_{23} -------- C_{j3} --------- C_{m3} - so that $|A'_{13}|$ is smallest with respect to $1/x$. The process can be repeated by deleting the first row and column of $\gamma_0 = (A_{ij})$; also the cardinality of the set of matrices with elements in $K_{1/x}$ and each of a given value, is that of the continuum. Of these matrices, those that are equivalent to each other are at most countable because the unimodular matrices (in $k[x]$) are countable. So if we

choose one matrix to represent a certain equivalent class, the set, of inequivalent matrices the elements of which have a given value, has the cardinality of the continuum. Choose the inequivalent classes to be represented each by a reduced matrix constructed as above; the set, so constructed, given the order of the symmetric matrix and for different values of the elements from $K_{1/\alpha}$ for different values of the determinant, is called $\mathcal{R}$. $\mathcal{R}$ is also used to denote the subspace of $K_{1/\alpha}^{\frac{m(m+1)}{2}}$ when the matrices in $\mathcal{R}$ are represented as poinsts of the space $K_{1/\alpha}^{\frac{m(m+1)}{2}}$ is compact because $K_{1/\alpha}$ is itself compact.

The space $\mathcal{R}$ <u>for the reduced indefinite symmetric matrices</u> arises out of matrices of the type

$$\begin{pmatrix} 0 & 0 & P \\ 0 & F & Q \\ P' & Q' & G \end{pmatrix}$$

where F is a definite symmetric matrix of order $m-2r$ and r is the order of the maximal '0' matrix which γ represents,

$$|F|\,|P|^2 = |\gamma|$$

Given γ, $\|F\| \leq \|\gamma\|$. Also the elements of F can be chosen to have the 'smallest' possible values in the sense described for definite symmetric matrices. Now the elements of P namely $p_1, - - - - , p_r$ all diagonal, can be chosen to have the smallest possible values. That is p_1 is chosen first as the smallest possible. This is possible because of the restrictions on the determinant of γ and the nature of F once γ is given. After choosing p_1, p_2 can be chosen as the smallest possible and so on, These are effected by means of elementary transformations. Now Q and G can be chosen in the same fashion to have elements of

given values less than the values of $p_1, - \cdots , p_r$. The space $\mathfrak{R}$ can be constructed in the same way as for definite symmetric matrices given the order of the elements in $\mathfrak{R}$. The space $\mathfrak{R}$ in $K_{1/2}^{\frac{m(m+1)}{2}}$ likewise constructed is compact.

This space plays in important role in the proof of the statement that the units of an indefinite symmetric matrix are finitely generated.

11. Finally we prove the following statement concerning the units of indefinite forms.

The units of indefinite forms are infinite in number. This has been proved by Artin for binary forms. Consider a ternary form, in $K_{1/2}$ which is indefinite Call it $A_1X_1^2 + A_2X_2^2 + A_3X_3^2$. If $-A_iA_j$ is a square for i,j =1,2,3 every binary partial form of the above ternary form is indefinite and the units are infinite in number. This is true even if $-A_iA_j$ is a non-square for $i,j = 1,2,3$ For consider

$$A_1^2X_1^2 + A_2A_1X_2^2 + A_1A_3X_3^2 = F$$

and the binary form

$$A_2A_1X_2^2 + A_3A_1X_3^2 = G$$

$$C_{1/2}(F) = C_{1/2}(G)$$

which shows there must be a binary partial form which is indefinite and the units are infinite in number. This can be extended by induction to all indefinite forms not necessarily diagonal. A proof of this statement is found in Eichler [20] Thm 16.1 p103.

N.B.Throught we exclude forms of the type X_1X_2

2. Given the value of the determinant, in the set of symmetric matrices in $\mathcal{R}$, with this value for the determinant there are at least two equivalent classes; because the value of the determinant remain s unaltered if it is multiplied by a symmetric matrix, the determinant of which is a unit, a nonsquare. The resulting matrix belongs to a different equivalent class. This fact is used in the construction of the fundamental space for the discontinuous group of mappings $R \to U'RU$ where U is the unit of a symmetric matrix γ, $R \in \mathcal{R}$ and the mapping is into a subspace of the space of symmetric matrices with a given determinant equal to that of γ in value with respect to $1/2$. This is done elaborately in Chapter III.

N.B. : 'p-adic' is not the usual p-adic representation.

The induction part of the proof as in paragraphs 32) Chap III goes through for function fields with a suitable interpretations of the differentials and the valumes. But more is possible by the algebraic methods.

Results in Part I of Chapter III use reduction theory and these are more important than all the previous results for the rest of the developments in Chapter -III.