CHAPTER - III

PART - I

The proof of the main theorem of Siegel for indefinite forms over K.

22. This Chapter is devoted to the study of indefinite forms. The first part of this Chapter deals with the units of indefinite symmetric matrices. Units of indefinite symmetric matrices with elements in K are infinite in number. In order to construct a measure for this group of units the fundamental space $\mathcal{F}$ for the discontinuous group of mappings $\gamma \longrightarrow U'\gamma U$ of a subspace of $\mathcal{R}$ into itself, is constructed. Measure of the unit group is 1/Volume of $\mathcal{F}$.

Definition: Let G be a topological group and let H be a discrete subgroup of G. If M is a subset of G and a e H then the set M a is an image of M. A fundamental set F relative to H is defined by the following properties.

ϕ is the empty set

(1) F G = G (2) $Fa \cap F = \phi$ whenever

(3) F is a Borel set in G. (1) and (2) assure that every point of G is covered by one and only image of F.

Siegel* [9] proved that a fundamental set exists if G satisfies the second axiom of countability.

Definition: An image F a of F is called a neighbour of F if $\bar{F}a \cap \bar{F} \neq 0$ where $\bar{F}$ is the closure of F.

If F has only a finite number of neighbours then H is generated by a finite number of elements.

Definition: Let T be a topological space of points and let $\tau \to f(\tau, \lambda)$ be an open continuous representation of G as a transitive group of homeomorphic mappings of T on itself. The representation $\tau \to f(\tau, a)$, $a \in H$ of H in T is called discontinuous if no sequence $f(\tau, a_n)$ $(n = 1, 2, \ldots)$ converages to a point in T as a_n runo over the distinct elements of H.

As mentioned above the fundamental space F relative to H can be constructed if the points τ wheme the discontinuity property (relative to H) does not hold are omitted from T.

If G is taken as the unimodular group of a given order m over K and H as the group of units U of an integral

* pp 674, 675, 676 for definitions.

symmetric matrix in K the volume of the fundamental space constructed in the space of all symmetric matrices in $K_{1/2}$ of a given order and with a given determinant is the (inverse of the measure of the unit group). This measure is useful in formulating the main theorem of Siegel for indefinite forms.

In the article on reduction theory the conditions were written down for $\gamma \in K_{1/2}$ to be definite. Also the reduced space of definite symmetrice matrices with a given determinant was constructed. For the diagonal elements the conditions were written as $|\gamma[x]| \geq |\delta_k|$ for all integral columns x and the nondiagonal elements were taken with values bounded below. $\mathcal{R}$ serves as the fundamental space for a representation of the space of definite symmetric matrices with a given determinant by means of the transformation $R \to U'RU$ where U is a unit of the symmetric matrix. . In order to prove the discontinuity U can be taken from the unimodular group. This gives also that the unimodular group is finitely generated.

This method does not apply to indefinite symmetric matrices because the units of a certain indefinite symmetric matrix are infinite in number and that spoils the discontinuity, of the mappings $\gamma \to U'\gamma U$. So a fundamental space has to be constructed. It is shown that, in the case of the function fields, such a fundamental space differs from the reduced space of all symmetric matrices with a given determinant by only a countable number of points.

The left hand side of the main theorem of Siegel now admits an interpretation and the arithmetical parts proceeds on the same lines as for the rational number field, done by Siegel [6] .

The formula of Gauss and Eisenstein holds with a restriction on the degrees of the terms of $\mathfrak{t}$. $A_0(\mathfrak{S},\mathfrak{T})$ can be evaluated with an alteration in the method of induction of Chapter II. This method can be used also in Chapter II.

The quantity $\rho(\mathfrak{S})$ which is a constant with respect to $\mathfrak{S}$ can be proved to be constant also for varying $\mathfrak{S}$. This is done at the end of this Chapter.

23. The reduced space $\mathcal{R}$ and the units.

The underlying principle in this passage is not very much different from that in the rational number field. It is yet another instance during the course of our generalizations where we use the compactness of the space $K_{1/2}$ instead of the arcwise connectedness of the space of real numbers.

Let $\mathcal{R}$ be the space of reduced symmetric matrices of a given order r and with a given determinant. $\Gamma(\mathfrak{S})$ is the group of units of the symmetric matrix $\mathfrak{S}$.

N.B. The argument which follows goes through without the restriction on the determinant $|\mathfrak{S}| \cdot \Gamma(\mathfrak{S})$ does not leave the whole space fixed. It is not difficult to note that the only units which leave the whole of $\mathcal{R}$ fixed are the trivial units.

No subgroup of $\Gamma(\gamma)$ can leave the whole space $\mathcal{R}$ fixed because this is again a subgroup of the unimodular group. Let $\mathcal{R}_1$ be the subspace of $\mathcal{R}$ such that no element H_1 of $\mathcal{R}_1$ is fixed by all the elements in $\Gamma(\gamma)$. Let $\Gamma(\gamma, H_1)$ be the subgroup of $\Gamma(\gamma)$ which fixes H_1 . A repeated application of the compactness of the space gives the fundamental space as described below. Let $\mathcal{R}_2$ be the subspace of $\mathcal{R}_1$ such that no element of $\mathcal{R}_1$ is fixed by the whole of $\Gamma(\gamma, H_1)$. Let H_2 be an element of $\mathcal{R}_2$ and so on.

$$\mathcal{R} \supset \mathcal{R}_1 \supset \mathcal{R}_2 \supset \text{---} \supset \mathcal{R}_n \supset \text{---}$$

If this process terminates in a point H then H is not fixed by any $\Gamma(\gamma, H_n)$ and therefore not by $\Gamma(\gamma)$. If it terminates in a subspace ($\mathcal{R}_n$ say) then there exists a $H_n \in \mathcal{R}_n$ for which there is not $\mathcal{R}_{n+1}$. Consider the group $\Gamma(\gamma, H_n)$. Let $\mathcal{R}_{11}$ be the subspace of $\mathcal{R}_1$ consisting of elements not fixed by the whole of $\Gamma(\gamma, H_n)$, $\mathcal{R}_{12}$ the subspace of $\mathcal{R}_2$ with the same property and so on upto $\mathcal{R}_{1n-1}$

$$\mathcal{R} \supset \mathcal{R}_{11} \supset \text{---} \supset \mathcal{R}_{1n-1}$$

Choose $H_{1n-1} \in \mathcal{R}_{1n-1}$ and repeat the process.

$$\mathcal{R} \supset \mathcal{R}_{21} \supset \text{---} \supset \mathcal{R}_{2n-2}$$

where $\mathcal{R}_{21} = \mathcal{R}_{11}$. We have other similar sequences and finally $\mathcal{R} \supset \mathcal{R}_{m1} \supset K$,

because $\mathcal{R}_{12} \supset \mathcal{R}_{22} \supset \mathcal{R}_{32} \supset \text{---}$ and this process must terminate in a point, say K_0 .

Either $\Gamma(\gamma, K_0)$ fixes the whole of $\mathcal{R}$ and the whole space or K_0 is not fixed by any element of $\Gamma(\gamma)$ If k_0 is not fixed by any element of $\Gamma(\gamma)$ the point K is not an isolated point in the metric defined by the valuation in $1/x$ (when K is represented as a point of R^r, r being the order of K_0)

Suppose K_0 is written as $(\overline{A_{ij}})$. The last statement is true because all the points which have the same first terms as K_0 (in the power series expansions in $(\overline{A_{ij}})$) are represented by K_0;* if $\Gamma(\gamma, K_0)$ fixes the whole of $\mathcal{R}$, $K_0 \in \mathcal{R}_{m1}$ for if H_{mn} is the point of $\mathcal{R}_{m1}$ which defines K that is, if K_0 is not fixed by any element of $\Gamma(\gamma, H_{mn})$, $\Gamma(\gamma, K_0) \cap \Gamma(\gamma, H_{mn})$ is empty and H_{mn} is not fixed by any element of $\Gamma(\gamma, K_0)$ and therefore $\Gamma(\gamma, K_0)$ does not fix the whole of $\mathcal{R}$. Therefore H_{mn} as defined above does not exist and $K_0 \in \mathcal{R}_{m1}$

If $K_0 \in \mathcal{R}_{m1}$, $\mathcal{R}_{m1}$ can be taken instead of $\mathcal{R}$ and $\Gamma(\gamma, K_0)$ instead of $\Gamma(\gamma)$ and the above process can be repeated again so that one actually arrives at a K_0 such that $\mathcal{R} \supset \mathcal{R}_{11} \supset K_0$ where K_0 is not fixed by any element of $\Gamma(\gamma)$

Given $\Gamma(\gamma)$ the set of points K_0 not fixed by any element of $\Gamma(\gamma)$ and which belong to $\mathcal{R}$ form a subspace $\mathcal{F}$ .The space $\mathcal{F}$ is the fundamental space for the discontinuous group of mappings $R \to U'RU$ where R belongs to the space covered by the images of $\mathcal{F}$ by means of the elements of $\Gamma(\gamma)$. The space $\mathcal{F}$ is

* This difficulty is overcome by taking the 'p-adic' representation of $\mathcal{R}$ but the reasoning given here is enough to prove that K_0 is not isolated.

compact and has only a finite number of neighbour if $\mathfrak{R}$ is represented the Euclidean space by the p - adic representation. This proves that $\Gamma(\gamma)$ is finitely generated. Also $\mathfrak{F}$ differs from the space of all γ of a given order and with a given determinant only by a countable number of points. So we have proved the

<u>THEOREM A</u>: $\Gamma(\gamma)$ is finitely generated.

The next theorem will be proved.

<u>THEOREM B</u>: $\mathfrak{F}$ differs from the space of all γ of given order and with a given determinant only by a countable number of points.

<u>Proof</u>: Consider the two spaces $\mathfrak{R}$ and $\mathfrak{R}_1$. Let $\gamma_1 \in \mathfrak{R}$ but not to $\mathfrak{R}$. Then $\Gamma(\gamma) \subset \Gamma(\gamma_1)$. Of all these γ_1 with this property there must be one γ_0 with the property that all the $\Gamma(\gamma_1) \subset \Gamma(\gamma_0)$. Consider γ_0 and $\mathfrak{R}$ and proceed as for γ and $\mathfrak{R}$. Let $\mathfrak{R}_{10}$ be the space corresponding to $\mathfrak{R}_1$. Those points which are in $\mathfrak{R}$ but not in $\mathfrak{R}_{10}$ are only finite number corresponding to the trivial units. Before one arrives at K_0 there are only a countable number of such spaces as $\mathfrak{R}_{ij}$. Therefore the difference between $\mathfrak{R}$ and F is a countable. Here we make use of some properties of the unit group mentioned in Paragraphs 10. chapter I.

24. Evaluation $A_0(\gamma, \mathfrak{f})$ is possible with a slight alteration in the method of induction of Chapter II.

In order to explain this point we proceed to evaluate $A_0(\gamma, \mathfrak{f})$ by induction. For binary indefinite forms we use the correspondence between ideal theory and binary quadratic forms. It proceeds exactly in the same way as for definite forms. We shall next do the evaluation for ternary diagonal forms.

Consider $\begin{pmatrix} A_1 & & \\ & A_2 & \\ & & A_3 \end{pmatrix}$ and (B_1)

Here γ is of order three and $\mathfrak{f}$ is of order one. The density $A_0(\gamma, \mathfrak{f})$ is $1/\ell$ times the measure of the group of units in the quadratic algebraic function fields when γ is of order two and $\mathfrak{f}$ is of order one.

$1/\ell$ is the constant in the thesis of Artin for indefinite binary forms.

Now in the equation

$$A_1 x_1^2 + A_2 x_2^2 + A_3 x_3^2 = B_1 y_1^2$$

$A_1 x_1^2 + A_2 x_2^2$ is a binary form of determinant $A_1 A_2$ and if it represents a certain f of degree greater than that of B, $A_3 x_3^2$ represents f in $p^{\frac{\nu - r}{2}}$ ways $|A_3| = p^r$, $|f| = p^\nu$ and $B_1 y_1^2$ represents f in $p^{\frac{\nu - s}{2}}$ ways, $|B_1| = p^s$.

Therefore if C is defined as in Chapter II for $A_1x_1^2+A_2x_2^2$ it is $C\,p^{\frac{\nu-r}{2}} \Big/ p^{\frac{\nu-s}{2}} = C\,p^{\frac{s-r}{2}}$ for $A_1x_1^2+A_2x_2^2+A_3x_3^2$

for ν sufficiently large, that is, of all these representations, for every one of $p^{\frac{\nu-r}{2}}$ on the left only one on the right is relevant. This proves the theorem for m=3, n=1.

Before we consider for more general forms we have (ii) the second part of the induction is that which asserts we can proceed from (m,n) to (m,n+1). Let us start with m,1 as before; we shall prove for m,2

$$A_1x_1^2+A_2x_2^2+A_3x_3^2 = B_1 = f_1 \qquad \text{———} (1)$$
$$A_1y_1^2+A_2y_2^2+A_3y_3^2 = B_2 = f_2 \qquad \text{———} (2)$$

We next make use of the identity

$$\left| \Sigma a_i^2 \, \Sigma b_j^2 \right| = \Big| (\Sigma a_i b_i)^2 + \underset{i\neq j}{(\Sigma a_i b_j)^2}$$
$$-2\,\Sigma a_i a_j b_k b_l \; - 2\,\Sigma a_i a_j \, b_i b_j \Big|$$
$$\leq \max\Big(\big|\sum_{i\neq j}(a_i b_j)^2\big|,\ |a_i a_j b_k b_l| \quad i\neq k, j\neq l \Big)$$

simultaneously

For a_i we give the value $\sqrt{A_i}\,x_i$ and for b_i we give the value $\sqrt{A_i}\;y_i$ because $\Sigma a_i b_i = 0$

$$\Big| \Sigma (a_i b_j)^2 + 2\sum_{i\neq j} a_i a_j \, b_i b_j \Big| = \Big| (\sum_{i\neq j} a_i b_j)^2 \Big|$$

So far we used f_1 and f_2 by specifying their degrees and leading coefficients. So there are at least $\sqrt{|f_1|\,|f_2|}$ possibilities for the $|a_i b_j|$ of which only one is relevant for us depending on which exactly are the f_1 and f_2 we take into consideration. If there are more than $\sqrt{|f_1|\,|f_2|}$ possibilities

that means one of the $\sqrt{A_i}\, x_i$ or $\sqrt{A_j}\, x_j'$ takes a value greater than $\sqrt{|f_1|}$ or $\sqrt{|f_2|}$. This is possible because the forms are indefinite. Even in such a possibility the existence of $A_0(\sigma, \tau)$ is proved for m=2, n=1 and it has been extended for m=2, n $>$ 1. Therefore taking the equations (1) and (2) as the restricting conditions on $\sqrt{A_i}\, x_i$, $\sqrt{A_j}\, x_j'$ this situation can be accounted for.

The rest of the argument to complete the main theorem is exactly as for the definite forms. This procedure is not repeated and ~~exhibiting~~ results in Chapter II are exhibited as a special case at the end of this Chapter.

For the nondiagonal forms we have a different type of argument where we use the reduced matrices which we already have constructed.

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

P is of order r and diagonal. If we cut the r^{th} row and r^{th} column we are omitting $2A_{r,m+1}\, x_{m+1}\, x_r$ from the form. We can have the above matrix with $A_{r,m+1}$ as the maximum of the diagonal elements of P and

$$|A_{m+1}| \leq |A_{r\,m+1}|$$

If we omit x_r, x_{m+1} the form has m-1 elements and along with $A_{r\,m+1} x_{m+1} x_r + A_{m+1} x^2_{m+1}$ it is γ.
If the average is C for m-1, 1 it is

$$C \left\{ |A_r^2| \right\}^{-1} |f|^{\frac{2-1-1}{2}} |f|^2/|f|$$
$$= \alpha_{m1} \|\gamma\|^{-\frac{1}{2}} \|\tau\|^{\frac{m+1-1}{2}}$$

for $m+1, 1$
$\alpha_{m+1,1} = \alpha_{m1}$

25. Measure of the unit group and measure of representation.

In article 23 the existence of the fundamental space was proved and volume of the fundamental space is inverse of the measure of the unit group. The fundamental space F for the discontinuous group of mappings $R \to U'RU$ (where R belongs to the space covered by the images of F by means of the elements of $\Gamma(\gamma)$ differs from the reduced space of symmetric matrices with a given determinant by a countable number of points. The space covered by the images of F by means of the elements of $\Gamma(\gamma)$ is the $\mathfrak{h}$ space. Call the volume of F, *$\{\mu^{-1}(\gamma)\}$
N.B. $1/\mu^{-1}(\gamma) \neq \mu(\gamma)$

Measure of representation: Let γ be the matrix of a nondegenerate rational quadratic form and let t be an element of K represented by γ so that $\gamma[y] = t$

* Notation

for an integral column Y, that is, the elements of Y belong to $k[x]$. Along with $\underline{Y}$, U $\underline{Y}$ is also a solution of the above equation where U is a unit of $\mathfrak{T}$. Because such units are not finite in number and the nature of the 'number' of representations of the above equation even otherwise is not known we define the <u>measure of Representation</u>. This can be generalized later to the number of representations. Let $\mathfrak{M}$ be a symmetric matrix which belongs to $K_{1/x}$ with the same index of inertia as $\mathfrak{T}$. Consider all the solutions

$$Y_0 = Y_0^{(n, n-1)} \quad \text{which belong to} \quad K_{1/x}$$

satisfying $\mathfrak{T}[Y] = \mathfrak{M}$ where $Y = (\underline{Y}\ Y_0)$

$\mathfrak{M}$ has the form $\begin{pmatrix} t & \underline{q}' \\ \underline{q} & R \end{pmatrix}$

Let Ω be the set of all matrices $\mathfrak{U}$ with elements in $K_{1/x}$ such that $\mathfrak{T}[\mathfrak{U}] = \mathfrak{T}$, Ω is a compact topological group. Instead of Ω consider the surface $\Omega(\mathfrak{M})$ Consisting of solutions Y of the matrix equation

$$\mathfrak{T}[\underline{Y}] = \mathfrak{M}$$

Let $\Omega(\underline{Y}, R)$ be the surface determined by Yo.

Let $\Omega(\underline{Y})$ be the group of those matrices $\mathfrak{M}$ in Ω with $\mathfrak{M}\,\underline{Y}) = \underline{Y}$

Then $\Omega(\underline{Y})$ is a compact topological group. If $\underline{Y}$ is a solution of the equation $\mathfrak{T}[\underline{Y}] = \mathfrak{M}$; V $\underline{Y}$ is also a solution for $V \in \Omega(\underline{Y})$. The mapping Yo $\longrightarrow$ V Yo gives a representation of $\Omega(\underline{Y})$ in $\Omega(q, R)$

As before we have a reduced space for this representation.

The subgroup $\Gamma(\underline{Y})$ of units $\mathfrak{U}$ of $\mathfrak{S}$ with $\mathfrak{U}\underline{Y} = \underline{Y}$ is a discrete subgroup of $\Omega(\underline{Y})$ and the representation Yo $\longrightarrow$ V Yo with $V \in \Gamma(\underline{Y})$ is discontinuous in $\Omega(q,R)$ Let $\bar{F}(\underline{Y})$ be a fundamental space in $\Omega(q,R)$ for the discrete subgroup $\Gamma(\underline{Y})$.

The construction of the fundamental space is carried out as before and $\mu(\underline{Y},\mathfrak{S})$ is the measure of representation.

This procedure can be carried out with a matrix instead of the column $\underline{Y}$ such that $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ with the usual definition for $\mathfrak{T}$ and $\mathfrak{T}$. $\mu(\mathfrak{C},\mathfrak{S})$ is the measure of representation [Siegel, 6].

Take a neighbourhood of $\mathfrak{T}$ and the set of solutions $\mathfrak{X}$ such that $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}_0$ in the neighbourhood of $\mathfrak{T}$ (as in Chapter II).

$\sum_{\mathfrak{T}} \mu(\mathfrak{C},\mathfrak{S})$, (for the different integral $\mathfrak{T}$) by the number of integral $\mathfrak{T}$, in the limit when the neighbourhood shrinks to $\mathfrak{T}$ is denoted by $\bar{\rho}(\mathfrak{C},\mathfrak{S})$

Let $\mathfrak{C}$ run through a full system of integral solutions of $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ such that no two of them arise from one another by left sided multiplication with a unit.

Define

$$\alpha(\gamma,\tau) = \sum_{\Gamma} \bar{\rho}(\Gamma,\gamma) \,, \quad \bar{\rho}(\gamma) = \bar{\rho}(\Gamma,\gamma)$$

Finally ~~xx~~ let

$$\alpha(\gamma_1,\tau) + \cdots + \alpha(\gamma_h,\tau) = \bar{\mu}(\gamma,\tau)$$

$$\frac{\bar{\mu}(\gamma,\tau)}{\bar{\mu}(\gamma)} = \epsilon_{mn} \lim_{|f|\to\infty} \frac{A_f(\gamma,\tau)}{|f|^{mn-\frac{n(n+1)}{2}}}$$

$$\bar{\mu}(\gamma) = \bar{\rho}(\gamma_1) + \cdots + \bar{\rho}(\gamma_h)$$

Eqn 64, page 253 Siegel [6]

with the usual restriction on f is the main theorem of Siegel when γ and τ are indefinite.

It may be worthwhile to include more details about reduction theory and the different reduced spaces. But as such these are not required here.

After the above preparation the proof of the main theorem is carried out in two stages, one to include the arithmetical part and the other the analytical part. The arithmetical part consists of the two formulae generalized from the works of Gauss and Eisenstein. The formula in the small is the same as in Chapter II. The formula in the large is given in the next article.

PART - II

The arithmetical part of the proof for the indefinite forms.

26. Formula of Gauss and Eisenstein in the large:

So far we have not used the result in Chapter II. Hereafter we can look back at Part II, Chapter II for a comparison.

In order to state the formula of Gauss and Eisenstein in the large for indefinite forms one needs two lemmas given below Some of the methods in Chapter II are recalled so that a comparison would help to understand the procedure, not that a comparison is absolutely essential. The next paragraph starts with some ideas from Siegel [6] generalized to function fields. This automatically leads to a comparison with Part II, Chapter II and the formula of Gauss and Eisenstein in the large. The procedure in Chapter II is completely recalled and in part III the analytical part of the proof is written just as in Chapter II.

27. Some ideas from Siegel [6] .

The construction of the reduced $\mathfrak{h}$ and $\mathfrak{y}$ was carried out for definite forms on page 55 following Siegel [5] . The construction of $\mathfrak{h}$ and $\mathfrak{y}$ for indefinite forms is an important step in the formula of Gauss and Eisenstein in the large.

Let $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ be a particular primitive representation in $k[x]$. If $\mathfrak{W}_0$ is a complement of

$$\mathfrak{C},\ (\mathfrak{C}\ \mathfrak{M}_0) = \mathfrak{M}_0$$

$$\mathfrak{q}_0 = \mathfrak{C}'\mathfrak{S}\mathfrak{M}_0 \qquad \mathfrak{Y}_0 = \begin{pmatrix} \mathfrak{T} & \mathfrak{q}_0 \\ \mathfrak{N} & \mathfrak{G} \end{pmatrix}$$

$$|\mathfrak{T}|^{-1}\mathfrak{z}_0 = \mathfrak{M}_0'\mathfrak{S}\mathfrak{M}_0 - \mathfrak{q}_0'\mathfrak{T}^{-1}\mathfrak{q}_0 \qquad \text{——— (1)}$$

$$|\mathfrak{z}_0| = |\mathfrak{S}|\,|\mathfrak{T}|^{m-n-1} \quad \text{and}$$

$$\mathfrak{M}_0'\mathfrak{S}\mathfrak{M}_0 = \mathfrak{Y}_0'\begin{pmatrix} \mathfrak{T}^{-1} & \mathfrak{N}' \\ \mathfrak{N} & |\mathfrak{T}|^{-1}\mathfrak{z}_0 \end{pmatrix}\mathfrak{Y}_0$$

$$= \begin{pmatrix} \mathfrak{T} & \mathfrak{q}_0 \\ \mathfrak{q}_0' & |\mathfrak{T}|^{-1}\mathfrak{z}_0 + \mathfrak{q}_0'\mathfrak{T}^{-1}\mathfrak{q}_0 \end{pmatrix}$$

For any general complement

$$\mathfrak{M} = \mathfrak{C}\mathfrak{F} + \mathfrak{M}_0\mathfrak{W}$$

with integral $\mathfrak{F}$ and unimodular $\mathfrak{W}$ the following equations are true

$$\mathfrak{M} = \mathfrak{M}_0\begin{pmatrix} \mathfrak{G} & \mathfrak{F} \\ \mathfrak{N} & \mathfrak{W} \end{pmatrix} \qquad \mathfrak{y}_0 = \mathfrak{T}\mathfrak{F} + \mathfrak{q}_0\mathfrak{W}$$

$$\mathfrak{z} = \mathfrak{W}'\mathfrak{z}_0\mathfrak{W}$$

Given $\mathfrak{C}$ and $\mathfrak{M}_0$, $\mathfrak{z}_0$ is fixed uniquely and $\mathfrak{z}$ is in the same class as $\mathfrak{z}_0$. That is, the class of $\mathfrak{z}$ is uniquely fixed and $\mathfrak{W}$ is determined in E ($\mathfrak{z}$) ways if $\mathfrak{z}$ is definite. If $\mathfrak{z}$ is indefinite the E ($\mathfrak{z}$) has to be replaced by the measure of the unit group of $\mathfrak{z}$. Also for the number of primitive representations $\mathfrak{C}$ the notion of the measure of representation has to be used. This was introduced in paragraph 23, At this stage the method in Siegel [6] can be compared with that in [5] to establish the formula of Gauss and Eisenstein in the large. Let $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ be a representation of $\mathfrak{T}$ by $\mathfrak{S}$. To a representation $\mathfrak{C}'\mathfrak{S}\mathfrak{C}=\mathfrak{T}$, $\mathfrak{C}$ of $\mathfrak{T}$ by $\mathfrak{S}$ let U be a unit of $\mathfrak{S}$ such that $\mathfrak{U}\mathfrak{C}=\mathfrak{C}$. Let $\mathfrak{X}_0^{(m,m-n)}$ be a matrix in $K_{1/x}$ such that $(\mathfrak{C}\,\mathfrak{X}_0)$ has a determinant different from zero. Then put

$$(\mathfrak{C}\mathfrak{X}_0)'\mathfrak{S}(\mathfrak{C}\mathfrak{X}_0) = \begin{pmatrix} \mathfrak{T} & \mathfrak{y}_0 \\ \mathfrak{y}_0' & \mathfrak{R}_0 \end{pmatrix} \qquad \text{—(3)}$$

so that $\mathfrak{C}'\mathfrak{S}\mathfrak{X}_0 = \mathfrak{y}_0$, $\mathfrak{X}_0'\mathfrak{S}\mathfrak{X}_0 = \mathfrak{R}_0$

Then it shall be shown that

$$(\mathfrak{C}\mathfrak{X})'\mathfrak{S}(\mathfrak{C}\mathfrak{X}) = \begin{pmatrix} \mathfrak{T} & \mathfrak{y} \\ \mathfrak{y}' & \mathfrak{R} \end{pmatrix}$$

possesses a solution $\mathfrak{X}$ in $K_{1/x}$ if $\mathfrak{y}$ and $\mathfrak{R}=\mathfrak{R}'$ lie sufficiently near to $\mathfrak{y}_0$ and $\mathfrak{R}_0$. Here lemma 1, Chapter II is applied.

In order to solve the equations $\mathfrak{C}'\mathfrak{S}\mathfrak{X}=\mathfrak{y}$, $\mathfrak{X}'\mathfrak{S}\mathfrak{X}=\mathfrak{R}$ put $\mathfrak{X} = \mathfrak{C}\mathfrak{F} + \mathfrak{X}_0\mathfrak{W}$ with unknown $\mathfrak{F}^{(n,m-n)}$ and $\mathfrak{W}^{(m-n)}$. With the abbreviations

$$\mathfrak{R}_0 - \mathfrak{y}_0'\mathfrak{T}^{-1}\mathfrak{y}_0 = \mathfrak{h}_0 \text{ and}$$

$$\mathfrak{R} - \mathfrak{y}'\mathfrak{T}^{-1}\mathfrak{y} = \mathfrak{h}$$

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{y}_0 \\ \mathfrak{y}_0' & \mathfrak{R}_0 \end{pmatrix} = \begin{pmatrix} \mathfrak{T} & \mathfrak{N} \\ \mathfrak{y}_0' & \mathfrak{E} \end{pmatrix}\begin{pmatrix} \mathfrak{T}^{-1} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{h}_0 \end{pmatrix}\begin{pmatrix} \mathfrak{T} & \mathfrak{y}_0 \\ \mathfrak{N} & \mathfrak{E} \end{pmatrix}$$

then $|\mathfrak{h}_0| \neq 0$ and we have further the equations $\mathfrak{T}\mathfrak{F} + \mathfrak{g}_0\mathfrak{W} = \mathfrak{g}$ and $\mathfrak{W}'\mathfrak{h}_0\mathfrak{W} = \mathfrak{h}$. Here $\mathfrak{h}$ must be sufficiently near to $\mathfrak{h}_0$. In the $\frac{(m-n)(m-n+1)}{2}$ dimensional space of pairs $\mathfrak{g}, \mathfrak{R}$ the set of points, for which (3) is soluble, is chosen. By means of (3) the space is mapped to B' (the m(m-n) dimensional) of the $\mathfrak{X}$ space. Any two points $\mathfrak{X}_1, \mathfrak{X}_2$ of the $\mathfrak{X}$ space are called associated if for a certain unit U of the equation $\mathfrak{X}_2 = U\mathfrak{X}_1$ is true. If B is the reduced space of $\mathfrak{X}$ in B' for this equivalence relations volume of B exists and is different from zero. Also for a certain neighbourhood B of $\mathfrak{g}, \mathfrak{R}$ $\frac{\text{volume of B'}}{\text{volume of B}}$ in the limit when B tends to $\mathfrak{g}, \mathfrak{R}$ is the same as $\rho(\mathfrak{C}, \mathfrak{S})$ if $\mathfrak{C}$ is a primitive representation and ($\mathfrak{C}\ \mathfrak{X}_0$) is unimodular. The construction of the measure $\rho(\mathfrak{C}, \mathfrak{S})$ its existence and the inter-relation with the reduced $\mathfrak{h}$ and $\mathfrak{g}$ are given by lemmas 11 and 12, Siegel [6] . These reduced $\mathfrak{h}$ and $\mathfrak{g}$ are defined just as for definite forms. Refer back to the equations (1) and (2). $\mathfrak{h}$ is called reduced once its class ($\mathfrak{h}$) is fixed. Of the possibilities for $\mathfrak{W}$ (which can be measured by $\mu^{-1}(\mathfrak{h})$) one is chosen and to fix $\mathfrak{F}$ in $\mathfrak{G} = \mathfrak{C}\mathfrak{F} + \mathfrak{G}_0\mathfrak{W}$ with primitive $\mathfrak{C}$. Therefore it is enough to consider the case when $\mathfrak{C}$ is primitive. Let $\mathfrak{Y}_0$ be a complement of $\mathfrak{C}$. Then we have the following

28. <u>Lemmas from Siegel [6]</u> :

Lemma 1: Let $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ be a primitive representation and $\mathfrak{Y}_0$ be a complement of $\mathfrak{C}$, that is $(\mathfrak{C}\,\mathfrak{Y}_0)$ is unimodular

Put $\mathfrak{C}'\mathfrak{S}\mathfrak{Y}_0 = \mathfrak{g}_0$, $\mathfrak{Y}_0'\mathfrak{S}\mathfrak{Y}_0 - \mathfrak{g}_0'\mathfrak{T}^{-1}\mathfrak{g}_0 = \mathfrak{h}_0$

If U is a unit of $\mathfrak{S}$ such that $U\mathfrak{L} = \mathfrak{L}$, the equation,

$$U_1^{-1} U U_1 = \begin{pmatrix} \mathfrak{E} & \mathfrak{F}_0 \\ \mathfrak{N} & \mathfrak{W}_0 \end{pmatrix} \qquad (4) \qquad \{49, \text{Siegel } [6]\}$$

defines a unit $\mathfrak{W}_0$ of $\mathfrak{H}_0$ for which

$$\mathfrak{F}_0 = \mathfrak{T}^{-1}\mathfrak{Q}_0 (\mathfrak{E} - \mathfrak{W}_0) \qquad ([50, [6]) \qquad (5)$$

is integral. If conversely $\mathfrak{W}_0$ is such a unit of $\mathfrak{H}_0$ that the matrix $\mathfrak{F}$ defined by (5) is integral, (4) gives a unit U of $\mathfrak{S}$ such that $U\mathfrak{L} = \mathfrak{L}$.

<u>Proof</u>: If $U\mathfrak{L} = \mathfrak{L}$ then $U_1^{-1} U U_1$ is of the form (4) with integral $\mathfrak{F}_0, \mathfrak{W}_0$

Put
$$\mathfrak{T}\mathfrak{F}_0 + \mathfrak{Q}_0 \mathfrak{W}_0 = \mathfrak{Q}$$
$$\mathfrak{W}_0' \mathfrak{H}_0 \mathfrak{W}_0 = \mathfrak{H}$$

Then
$$\begin{pmatrix} \mathfrak{T} & \mathfrak{Q}_0 \\ \mathfrak{N} & \mathfrak{E} \end{pmatrix} \begin{pmatrix} \mathfrak{E} & \mathfrak{F}_0 \\ \mathfrak{N} & \mathfrak{W}_0 \end{pmatrix} = \begin{pmatrix} \mathfrak{E} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{W}_0 \end{pmatrix} \begin{pmatrix} \mathfrak{T} & \mathfrak{Q} \\ \mathfrak{N} & \mathfrak{E} \end{pmatrix} \quad \text{—(7)}$$

Because $U_1^{-1} U U_1$ is a unit of $U_1' \mathfrak{S} U_1$

and
$$U_1' \mathfrak{S} U_1 = \begin{pmatrix} \mathfrak{T} & \mathfrak{Q}_0 \\ \mathfrak{N} & \mathfrak{E} \end{pmatrix} \begin{pmatrix} \mathfrak{T}^{-1} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{H}_0 \end{pmatrix} \begin{pmatrix} \mathfrak{T} & \mathfrak{Q}_0 \\ \mathfrak{N} & \mathfrak{E} \end{pmatrix} \qquad (8)$$

$$= \begin{pmatrix} \mathfrak{T} & \mathfrak{Q}_0 \\ \mathfrak{Q}_0' & \mathfrak{H} + \mathfrak{Q}_0' \mathfrak{T}^{-1} \mathfrak{Q}_0 \end{pmatrix}$$

(4) and (8) give

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{q}_0 \\ \mathfrak{q}_0' & \mathfrak{h}+\mathfrak{q}_0'\mathfrak{T}^{-1}\mathfrak{q}_0 \end{pmatrix} = \begin{pmatrix} \mathfrak{T} & \mathfrak{q} \\ \mathfrak{q}' & \mathfrak{h}+\mathfrak{q}'\mathfrak{T}^{-1}\mathfrak{q} \end{pmatrix}$$

so that $\mathfrak{q}=\mathfrak{q}_0$, $\mathfrak{h}=\mathfrak{h}_0$ and $\mathfrak{W}$ is a unit of $\mathfrak{h}_0$ satisfying (5).

If conversely $\mathfrak{W}_0$ is a unit of $\mathfrak{h}_0$ for which the matrix $\mathfrak{F}_0$ determined by (5) is integral then (7) holds with $\mathfrak{q}=\mathfrak{q}_0$ and (8) gives that $\begin{pmatrix} \mathfrak{E} & \mathfrak{F} \\ \mathfrak{N} & \mathfrak{W}_0 \end{pmatrix}$ is a unit of $U_1'\mathfrak{S}U_1$. The U defines, by 4, a unit of $\mathfrak{S}$ such that $U\mathfrak{C}=\mathfrak{C}$

Lemma 2 : Let not m-n=2 and $|\mathfrak{S}||\mathfrak{T}|$ not a square of an element from the field of power series, happen simultaneously.

Lemma 12 Siegel [6]

If B has, in the space of $\mathfrak{q}$, $\mathfrak{R}$ a content, then the equation

$$(\mathfrak{C}\mathfrak{x})'\mathfrak{S}(\mathfrak{C}\mathfrak{x}) = \begin{pmatrix} \mathfrak{T} & \mathfrak{q} \\ \mathfrak{q}' & \mathfrak{R} \end{pmatrix}$$

determines a $\mathfrak{x}$ space B , which is reduced with respect to the units U of $\mathfrak{S}$ such that $U\mathfrak{C}=\mathfrak{C}$ has a finite content.

Proof: There exists a primitive matrix $\mathfrak{L}^{(m,n)}$ and an integral matrix $\mathfrak{B}^{(n)}$ so that $\mathfrak{L} = \mathfrak{L}_1 \mathfrak{B}$. By the substitution $\mathfrak{T} = \mathfrak{B}'\mathfrak{T}_1\mathfrak{B}$, $\mathfrak{Q} = \mathfrak{B}'\mathfrak{Q}_1$, the equation

$$(\mathfrak{L}\mathfrak{x})'\mathfrak{S}(\mathfrak{L}\mathfrak{x}) = \begin{pmatrix} \mathfrak{T}_1 & \mathfrak{Q}_1 \\ \mathfrak{Q}_1' & \overline{\mathfrak{R}} \end{pmatrix}$$

$$\mathfrak{H}_2 = \mathfrak{T}_0 + \mathfrak{H}_0 \mathfrak{W}_1 \ , \quad \mathfrak{W}_2 = \mathfrak{W}_0 \mathfrak{W}_1$$

Then $\mathfrak{W}_0$ is a unit of $\mathfrak{Z}_0$ and

$$\mathfrak{H}_0 = \mathfrak{T}^{-1}\mathfrak{Q}_0(\mathfrak{E} - \mathfrak{W}_0) = \mathfrak{T}^{-1}\mathfrak{Q}_0(\mathfrak{E} - \mathfrak{W}_0)$$

the $\mathfrak{W}$ form, if $\mathfrak{H}_0$ is integral, a subgroup of finite index with respect to the full unit group of $\mathfrak{Z}_0$.

$|\mathfrak{S}| = |\mathfrak{Z}_0|\,|\mathfrak{T}|$ m-n=2 and $-|\mathfrak{Z}_0|$ being equal to a square do not happen simultaneously. If $\mathfrak{Z}$ runs through such a space that it can be represented as a square in $K_{1/2}$ the same holds for $\mathfrak{W}$; the $\mathfrak{Q}, \mathfrak{R}$ and the $\mathfrak{Q}, \mathfrak{Z}$ also the pairs $\mathfrak{H}, \mathfrak{W}$ and $\mathfrak{Q}, \mathfrak{W}$ have the same property.

Here $|\mathfrak{S}|\,|\mathfrak{T}|$ cannot be extended as a power series in the sense of Puiseux.

(Chevalley: algebraic functions of one variable)

By the substitution

$$(\mathfrak{E}\,\mathfrak{Y}) = \mathfrak{U}\begin{pmatrix}\mathfrak{E} & \mathfrak{F} \\ \mathfrak{N} & \mathfrak{W}\end{pmatrix}$$

That is $\mathfrak{Y} = \mathfrak{E}\mathfrak{F} + \mathfrak{Y}_0\mathfrak{W}$ and the $\mathfrak{Y}$ space is mapped to the $\mathfrak{T}, \mathfrak{W}$ space and because of (8) and (9) by means of the substitutions

$$\mathfrak{T}\mathfrak{F} + \mathfrak{Y}_0\mathfrak{W} = \mathfrak{Y}, \quad \mathfrak{W}'\mathfrak{H}_0\mathfrak{W} = \mathfrak{H}$$
$$\mathfrak{H} + \mathfrak{Y}'\mathfrak{T}^{-1}\mathfrak{Y} = \mathfrak{R}$$

goes over into the $\mathfrak{Y}, \mathfrak{R}$ space. If $\mathfrak{Y}_1, \mathfrak{Y}_2$ are two associated points of the $\mathfrak{Y}$ space $\mathfrak{Y}_2 = \mathfrak{U}\mathfrak{Y}_1$ where $\mathfrak{U}\mathfrak{E} = \mathfrak{E}$, $\mathfrak{U}'\mathfrak{S}\mathfrak{U} = \mathfrak{S}$ and for the values $\mathfrak{F}_i, \mathfrak{W}_i$ and corresponding to $\mathfrak{Y}_1$ and $\mathfrak{Y}_2$

$$\mathfrak{U}\mathfrak{U}_1\begin{pmatrix}\mathfrak{E} & \mathfrak{F}_1 \\ \mathfrak{N} & \mathfrak{W}_1\end{pmatrix} = \mathfrak{U}_1\begin{pmatrix}\mathfrak{E} & \mathfrak{F}_2 \\ \mathfrak{N} & \mathfrak{W}_2\end{pmatrix}$$

from (4) $\mathfrak{F}$ is determined uniquely so that $\mathfrak{Y} = \mathfrak{T}\mathfrak{F} + \mathfrak{Y}_0\mathfrak{W}$ is a given representant of its left residue class modulo $\mathfrak{T}$. Here $\mathfrak{Y}$ is reduced. If $\mathfrak{H}$ and $\mathfrak{Y}$ are both reduced $\mathfrak{R}$ is also called reduced. To call $\mathfrak{H}$ actually reduced for indefinite forms it must be chosen from a certain reduced space. These spaces are dealt with in paragraph 25, of this chapter. The quantities B ($\mathfrak{S}, \mathfrak{T}$) and $E(\mathfrak{H})$ were already generalized to $\mu_B(\mathfrak{S},\mathfrak{T})$ and $\mu^{-1}(\mathfrak{H})$. The quantities B ($\mathfrak{H}$) and C ($\mathfrak{H}, \mathfrak{S}$) have their corrèsponding generalizations $\mu_B(\mathfrak{H})$ and $\mu_C(\mathfrak{H},\mathfrak{S})$. The next paragraph gives the generalizations of the lemma 11 and 12, Siegel [6] .

Hereafter it is assumed that it does not happen at the same time that m-n=2 and $|\mathfrak{S}|\,|\mathfrak{T}|$ is not a square of an element from the field of power series.

We have one more lemma from Siegel (Lemma 13, [6])

*Lemma 3 : Let $v(B)$ be the content of the space B in the space and $v(\bar{B})$ the content of the space of $\mathfrak{X}$ which satisfy,

$$(\mathfrak{L}\,\mathfrak{X})'\,\mathfrak{S}\,(\mathfrak{L}\,\mathfrak{X}) = \begin{pmatrix} \mathfrak{T} & \mathfrak{Y} \\ \mathfrak{Y}' & \mathfrak{R} \end{pmatrix}$$

Let B shrink to the pair $\mathfrak{Y}, \mathfrak{R}$. Then

$$\lim_{B \to \mathfrak{Y},\mathfrak{R}} \frac{v(\bar{B})}{v(B)} = \mu(\mathfrak{L},\mathfrak{S}) \text{ times } C_{\mathfrak{S},\mathfrak{T}}$$

Lemma 13 , Siegel [6]

where $C_{\mathfrak{S},\mathfrak{T}}$ depends only on $|\mathfrak{S}|\,|\mathfrak{T}|$ and where $\mu(\mathfrak{L},\mathfrak{S})$ depends only on $\mathfrak{S}$ and $\mathfrak{L}$

Proof: Put

$$(\mathfrak{L}\,\mathfrak{X}_1)'\,\mathfrak{S}\,(\mathfrak{L}\,\mathfrak{X}_1) = \begin{pmatrix} \mathfrak{T} & \mathfrak{Y}_1 \\ \mathfrak{Y}_1' & \mathfrak{R}_1 \end{pmatrix}$$

$$(\mathfrak{L}\,\mathfrak{X}) = (\mathfrak{L}\,\mathfrak{X}_1)\begin{pmatrix} \mathfrak{E} & \mathfrak{H} \\ \mathfrak{N} & \mathfrak{W} \end{pmatrix}$$

* This lemma and lemmas 16 and 19, Siegel [5] are applied in the last paragraph of Chapter III and therefore discussed in detail over there.

B_1 is the space corresponding to $\mathfrak{M}_1, \overline{\mathfrak{R}_1}$

From the method of proof and the construction of the reduced spaces inparagraphs 24,25 and 26 it is clear that the orders of $\mathfrak{M}, \mathfrak{R}, \mathfrak{M}_1, \mathfrak{R}_1, \mathfrak{L}$ and the determinant of γ are the only factors to be taken into consideration here.

$$\lim_{B \to \mathfrak{M}, \mathfrak{R}} \frac{v(\overline{B})}{v(B)} = \mu(\mathfrak{L}, \gamma) \text{ times } C_{\gamma, \eta}$$

where $C_{\gamma,\eta}$ depends only the determinants of γ, η and also on the order of $\mathfrak{L}$, $v(\overline{B}) / v(B)$ tends to a finite limit because it exists for the binary forms from the thesis of Artin and it can be extended by induction exactly as we extended the definition of $A_0(\gamma, \eta)$ in paragraph 26.

We can next have the proof of the formula of Gauss and Eisenstein in the large for indefinite forms.

29. <u>Formula of Gauss and Eisenstein in the large:</u>

The formula in the large reads

$$\sum_{\gamma_k \vee \gamma} \frac{\mu_B(\gamma_k, \eta)}{1/\mu^{-1}(\gamma_k)} = \frac{2}{(\mathfrak{z})} \mu_f(\mathfrak{z}, \gamma) \, \mu_H(\mathfrak{z}) \quad (11)$$

$$\mu_H(\mathfrak{z}) = \sum_{\mathfrak{z}_k \vee \mathfrak{z}} 1 / \frac{1}{\mu^{-1}(\mathfrak{z}_k)} = \sum_{\mathfrak{z}_k \vee \mathfrak{z}} \mu^{-1}(\mathfrak{z}_k)$$

$|\mathfrak{z}|$ is given –

$\gamma_k \vee \gamma$ means that γ_k ~~and~~ and γ are in the same genus and $\{\mathfrak{z}\}$ runs through all the distinct genus representants of definite $\mathfrak{z}$ (m-n). $\mu_f(\mathfrak{z},\gamma)$ is the measure of the reduced $\mathfrak{y}$ such that

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{y} \\ \mathfrak{y}' & |\mathfrak{T}|^{-1}\mathfrak{z} + \mathfrak{y}'\mathfrak{T}^{-1}\mathfrak{y} \end{pmatrix}$$

is in the same genus as γ. $\mathfrak{y}$ and $\mathfrak{z}$ are defined.

The second formula is the relation (11) for quantities modulo f. It is

$$\frac{B_f(\gamma,\mathfrak{T})}{E_f(\gamma)} = |\mathfrak{T}|^{\frac{(m-n)(m-n-1)}{2}} \sum_{(\mathfrak{z})} \frac{F_f(\mathfrak{z},\gamma)}{E_f(\mathfrak{z})} \qquad (12)$$

where ($\mathfrak{z}$) runs through all the class representants modulo f. $F(\mathfrak{z},\gamma)$ is the measure of the reduced $\mathfrak{y}$ for which

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{y} \\ \mathfrak{y}' & |\mathfrak{T}|^{-1}\mathfrak{z} + \mathfrak{y}'\mathfrak{T}^{-1}\mathfrak{y} \end{pmatrix} = \gamma_0$$

is equivalent to γ modulo $f/|\mathfrak{T}|$. f is assumed to be a multiple of $(|\gamma|\,|\mathfrak{T}|^m)^4$ in order to identify $F_f(\mathfrak{z},\gamma)$ and $F(\mathfrak{z},\gamma)$. $F_f(\mathfrak{z},\gamma)$ has the same measure $\mu_F(\mathfrak{z},\gamma)$ because one can have a correspondence between the class representants ($\mathfrak{z}$) and the genus representants $\{\mathfrak{z}\}$.

The reduced $\mathfrak{z}$ and $\mathfrak{y}$ have already been defined in paragraphs 29-32.

For the proof we refere back to page 55,57, ~~Chapter II~~ Siegel [5].

Just as in Siegel [6] in order to derive the formula (11) initially two other formulae are derifed, namely

$$\frac{\mu_B(\mathfrak{S},\mathfrak{T})}{\sqrt{\mu^{-1}(\mathfrak{S})}} = \sum_{\mathfrak{z}} \frac{\mu_B(\mathfrak{z})}{\sqrt{\mu^{-1}(\mathfrak{z})}} \qquad \text{—— (13)}$$

$\mu_B(\mathfrak{S},\mathfrak{T})$ is the measure of the primitive solutions $\mathfrak{C}$ nonassociated with respect to the units of $\mathfrak{S}$ in $k[x]$ and $\mu_B(\mathfrak{z})$ those which belong to the same class ($\mathfrak{z}$). $\mathfrak{z}$ is of determinant $|\mathfrak{S}|\,|\mathfrak{T}|^{m-n-1}$. The above statement is explained just as in Siegel [6]. After this is accomplished the next formula is

$$\frac{\mu_B(\mathfrak{z})}{\sqrt{\mu^{-1}(\mathfrak{S})}} = \frac{\mu_C(\mathfrak{z},\mathfrak{S})}{\sqrt{\mu^{-1}(\mathfrak{z})}} \qquad \text{—— (14)}$$

The definition of $\mathfrak{z}, \mathfrak{y}$ and the reduced $\mathfrak{z}$ and $\mathfrak{y}$ give almost the complete statement as well as the proof of the formulae. The proof is really complete only after the summations are justified only with the help of Hasse-Witt theorem. Rest of the argument is as in Siegel [6].

30. An alternative method to the above proof is to derive the formula (12) just as (11) with a restriction on the degrees of the element in $\mathfrak{t}$, $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{z}$ and $\mathfrak{h}$ and then proceed to the limit. The procedure to the limit is justified once again only if we make use of the lemmas in paragraph 27 and the notions in 24-27 . So the proof practically comes to the same. The fact is that this latter procedure is not possible in the rational number field. It is not a very advantageous method either. Still it is interesting to notice this method.

31. The method of induction for the proof of the main theorem is just as in Siegel [5] pp 557-63. The proof is just as for definite forms on pp 65-67 with no restriction on μ. Proof for the definite forms can be derived as a particular case. The results from Artin's thesis are exhibited as special cases of the more general results. This is already done for the definite forms.

For example it is not difficult to see from the definitions that $\frac{\bar{\mu}(\mathfrak{T},\mathfrak{f})}{\bar{\mu}(\mathfrak{T})}$ generalizes $\frac{\bar{A}(\mathfrak{T},\mathfrak{f})}{A_0(\mathfrak{T},\mathfrak{f})}$ from Chapter II.

Moreover one can see from the definition that in general $\lim_{B \to \mathcal{Y},\mathcal{R}} \frac{v(\bar{B})}{v(B)}$ is part of the contribution to $A_0(\mathfrak{T},\mathfrak{f})$ modulo the units of $\mathfrak{T}$ depending on the nature of $\mathfrak{L}$. In the binary case when $\mathfrak{L}$ is a column matrix, say, $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ and $\mathfrak{f}^{(1)} = t$ and $\mathcal{Y},\mathcal{R}$ are also matrices of order one; also $\bar{\mu}(\mathfrak{T})$ exists from the thesis of Artin because of the correspondence between the inequivalent integral representations of $\mathfrak{X}'\mathfrak{T}\mathfrak{X} = \mathfrak{f}$ and the inequivalent integral ideals with a given norm in $K(\sqrt{D})$, where $|\mathfrak{T}| = D$. And $\bar{\mu}(\mathfrak{T}) = \sum_{\mathfrak{L}} \bar{\rho}(\mathfrak{T},\mathfrak{L})$ is nothing else but $A_0(\mathfrak{T},\mathfrak{f})$ divided by the measure of the unit group of $K(\sqrt{D})$ which is finite. Also $\bar{\mu}(\mathfrak{T}) = \sum_{\mathfrak{L}} \bar{\rho}(\mathfrak{T},\mathfrak{L})$, the number of such $\mathfrak{L}$ is finite because of the above correspondence of ideals and representations. It can be proved that $\bar{\rho}(\mathfrak{L},\mathfrak{T})$ is finite because $\bar{\rho}(\mathfrak{L},\mathfrak{T}) \neq 0$ $\bar{\rho}(\mathfrak{L},\mathfrak{T}) \leq \bar{\mu}(\mathfrak{T}) < \infty$; $\bar{\rho}(\mathfrak{L},\mathfrak{T})$ can be proved to be finite even directly. For forms of order greater than two this can be extended by induction and

$$\lim_{B \to \mathcal{Y},\mathcal{R}} \frac{v(\bar{B})}{v(B)} = \bar{\mu}(\mathfrak{L},\mathfrak{T}) \quad \text{times } C_{\mathfrak{T},\mathfrak{f}}$$

as in lemma 3 can be proved as in Siegel [6] using the usual 'p-adic' representation and the considerations already mentioned under lemmas 12, 13 Siegel [6]

The proofs of formulae (12),(13) and (14) are just as in Siegel [5] pp and after the proparation so far the formulae for the definite case on pages 67-71 can be easily exhibited as particular cases of these formulae

<u>Lemmas 16 Siegel [5]</u> Let f be a polynomial prime to $|\mathfrak{T}|$ and f^{ℓ} the highest power of f in $|\mathfrak{T}| = f^{\ell}|\mathfrak{T}_1|$
If we put $\left(\frac{(-1)^{m/2}|\mathfrak{S}|}{f}\right) = \varepsilon$ or $\left(\frac{(-1)^{\frac{m-1}{2}}|\mathfrak{S}||\mathfrak{T}_1|}{f}\right)$

according as m is even or odd and analogously $\tau = |f|^{\frac{1-m}{2}}$

or $\tau = f^{2-m}$, $q = f^{a}$ and $a > \ell$ the formula

$$q^{1-m} A_q(\mathfrak{S}, \mathfrak{T}) = \left(1 - \varepsilon\, |f|^{-\frac{m}{2}}\right)\left(1 + \varepsilon|\tau| + \varepsilon^2|\tau|^2 + \cdots + \varepsilon^{\ell}|\tau|^{\ell}\right)$$

m even

$$= \left(1 - |f|^{1-m}\right)\left(1 + |\tau| + \cdots + |\tau|^{\frac{\ell-1}{2}}\right)$$

m even, ℓ odd

$$= \left(1 - |f|^{1-m}\right)\left(1 + |\tau| + |\tau|^2 + \cdots + |\tau|^{\frac{\ell}{2}-1} + \frac{|\tau|^{\frac{\ell}{2}}}{1 - \varepsilon|f|^{\frac{1-m}{2}}}\right)$$

modd, leven

32. A final reference to the thesis of Artin (for the time being)

One can look back now at the work done in pages 65-67 A special reference to indefinite binary forms proceeds in the same way once we notice $A_0(\gamma, \mathcal{F})$ exists for m=2, n=1.

h When $\sqrt{D}$ is real, is the same as $\sqrt{|D|}/(p-1)R$ where $|\varepsilon_0| = p^R$ and ε_0 is the fundamental unit which generate the units of γ. log $|\varepsilon_0|$ is the volume of the fundamental space.

We can have the identity for the binary forms as before

Case 1: Number of genera is 2^{s}, $h = \dfrac{\sqrt{|D|}}{(p-1)R}$

$$\frac{1/\mu^{-1}(\gamma)}{h} = A_0(\gamma, \mathcal{F})\, \rho(\gamma)\, \varepsilon_{22}\, |D|\, 2^{s} \prod_{f} \left(1 - \left[\frac{D}{f}\right]\frac{1}{|f|}\right)$$

$$= \alpha_{22}\, |\gamma|^{-3/2} \rho(\gamma)\, \epsilon_{21}\, |D|\, 2^{s} \prod_{f} \left(1 - \left[\frac{D}{f}\right]\frac{1}{|f|}\right)$$

$$R \Big/ \frac{1}{R} \left(1 - \left[\frac{D}{f}\right]\frac{1}{|f|}\right)^{-1} = \frac{(p-1)^2 R^2}{R^2}\, \epsilon_{21}\, |D|^{-\frac{1}{2}} \prod_{f} \left(1 - \left[\frac{D}{f}\right]\frac{1}{|f|}\right) \text{ times } \rho(\gamma)$$

$$\rho(\gamma) = \frac{R^3}{(p-1)^3 R^3} = \frac{1}{(p-1)^3} \qquad \epsilon_{21} = 1.$$

Case 2: Number of genera is 2^{s-1}

$$\rho(\gamma) = \frac{1}{2}\, \frac{R^3}{(p-1)^3 R^3} = \frac{1}{2(p-1)^3}$$

This proves that $\rho(\gamma)$ is constant and it is independent of R. In general $\rho(\gamma)$ can be proved to be bounded with $(p-1)^3/\sqrt{p}^3$ for an upper bound.

More is possible

33. Theorem: $\rho(\gamma)$ is a constant even with respect to γ

__Proof:__ The proof is the same as in Siegel [5] 563-567 and Siegel [6] 255-256 after representing all the matrices concerned in the Euclidean space by means of the 'p-adic' representation. The details are as follows.

Let Q be a polynomial divisible by $|\tau|^3 |\gamma|$

Then

$$\prod_{f|Q} \alpha_f(\gamma, \tau) = \frac{A_\theta(\gamma, \tau)}{|\theta|^{mn - \frac{n(n+1)}{2}}} \neq 0$$

as in equation (74) Siegel [6] p 255. If $f(\tau)$ is an integrable function of the matrix variable τ in the 'τ' space, it is true when γ, τ are in Γ that

$$\frac{A_\theta(\gamma, \tau)}{|\theta|^{mn - \frac{n(n+1)}{2}}} \bar{\mu}(\gamma) \int_D f(\tau)\, d\tau$$

$$= \lim_{t \to \infty} \left(\frac{|\theta|_p}{t}\right)^{\frac{n(n+1)}{2}} \sum_{\substack{\tau_1 \equiv \tau \pmod{\theta} \\ t^{-1}\tau_1 \text{ in } D}} \bar{\mu}(\gamma, \tau_1)\, f(t^{-1}\tau_1)$$

Now in/Slf $\gamma, \mathcal{T}$ are in $k(x)$ they can be taken over to Γ by means of the 'p-adic' representation, $\mathcal{D}$ is the closure of the '$\mathcal{T}$' space when $\mathcal{T}$ is represented in the Euclidean space, t is an integer which satisfies the property $t^{-1}\mathcal{T}$ in $\mathcal{D}$ when the 'p-adic' representation of $\mathcal{T}$ is taken and $|Q|_p$ is the integral value of the polynomial Q by means of the 'p-adic' representation. The p-adic representation is not necessary to write the integrals but their value remains, unaltered with the 'p-adic' representation.

Consider any integrable function $F(x'\gamma x)$, γ fixed, of the continuous real matrix variable x, where $\underset{m=\mu>n}{x'\gamma x = \mathcal{T}}$

Take $\mathcal{D}$ the closure of the $\mathcal{T}$ space by means of the 'p-adic' representation and the corresponding 'γ' space $\mathcal{D}'$

$$\int_{\mathcal{D}'} F(x'\gamma x)\,dx = \int_{\mathcal{D}} F(\mathcal{T})\ A_0(\gamma,\mathcal{T})\,d\mathcal{T}$$

$$\text{Put } F(\mathcal{T}) = \frac{1}{A_0(\gamma,\mathcal{T})}$$

$$\int_{\mathcal{D}} \frac{dx}{A_0(\gamma, x'\gamma x)} = \int_{\mathcal{D}} d\mathcal{T} = v(\mathcal{D})$$

which gives

$$\int_{\mathcal{D}'} \frac{dx}{A_0(\gamma, x'\gamma x)} = \lim_{g\to\infty} \sum_{C/g \text{ in } \mathcal{D}'} \frac{g^{-mn}}{A_0\left(\gamma, \frac{C}{g}'\gamma\frac{C}{g}\right)} \tag{16}$$

Therefore

$$\sum_{\Sigma/g \text{ in } \mathcal{D}'} \frac{g^{-mn}}{A_0\left(\gamma, \frac{\Sigma'}{g}\gamma\frac{\Sigma}{g}\right)} = \sum_{T/g^2 \text{ in } \mathcal{D}} \frac{g^{-mn} A(\gamma, T)}{A_0\left(\gamma, T/g^2\right)} \qquad (17)$$

taken with the proper meaning for Σ, γ, T and g. When the values $A(\gamma, T)$, $A_0(\gamma, T)$ are taken γ and T are in $k(x)$

$A_0(\gamma, T) = \alpha_{mn} \|\gamma\|^{-n/2} \|T\|^{\frac{m-n-1}{2}}$ as a function of γ and T

$|T/g^2| = |T|\, g^{-2n}$ as a function of T

We see that $A_0(\gamma, T/g^2) = g^{-n(m-n+1)} A_0(\gamma, T)$

Thus

$$\sum_{\Sigma/g \text{ in } \mathcal{D}'} \frac{g^{-mn}}{A_0\left(\gamma, \frac{\Sigma'}{g}\gamma\frac{\Sigma}{g}\right)} = \sum_{T \text{ in } \mathcal{D}_g} g^{-n(n+1)} \frac{A(\gamma, T)}{A_0(\gamma, T)} \qquad (18)$$

Where $\mathcal{D}_g$ denotes the region obtained from $\mathcal{D}$ by the transformation $T^* = g^2 T$ with Jacobian $J\left(T^*/T\right) = g^{n(n+1)}$
It is here the 'p-adic' representation is useful. On multiplying and dividing this ~~expansion~~ expression by $\int_{\mathcal{D}} dT$ we see that

$$\sum \zeta/g \text{ in } D' \frac{g^{-mn}}{A_0(\gamma, \frac{\zeta'}{g}\gamma\frac{\zeta}{g})} = \sum_{\tau \text{ in } D_g} \frac{\frac{A(\gamma,\tau)}{A_0(\gamma,\tau)} \times \int_D d\tau}{\int_{D_g} d\tau} \quad (19)$$

These equations 16,17,18,19 give

$$\operatorname*{Lim}_{g\to\infty} \sum_{\tau \text{ in } D_g} \frac{A(\gamma_k,\tau)}{E(\gamma_k) A_0(\gamma,\tau)} \Big/ v(D_g) = \frac{1}{E(\gamma_k)}$$

because

$$\lim_{g\to\infty} \sum_{\tau \text{ in } D_g} \frac{A(\gamma,\tau)}{A_0(\gamma,\tau)} \Big/ \int_{D_g} d\tau = 1$$

Summing over the genus representants of γ and dividing by $M(\gamma)$

$$\lim_{g\to\infty} \sum_{\tau \text{ in } D_g} \frac{\overline{A}(\gamma,\tau)}{A_0(\gamma,\tau)} \Big/ v(D_g) = 1$$

Put

$$\lim_{q\to\infty} \frac{A_q(\gamma,\tau)}{q^{mn - \frac{n(n+1)}{2}}} = d(\gamma,\tau)$$

In order to prove $f(\gamma)$ is a constant it is enough to prove that

$$\epsilon_{mn} \lim_{g\to\infty} \sum_{\tau \text{ in } D_g} d(\gamma,\tau) \Big/ v(D_g) \text{ is a constant} \quad (20)$$

It is already evaluated for binary forms - definite and indefinite. In the equation 16 the summation is extended over all the lattice points $\mathfrak{L}$ of the $\mathfrak{X}$ space such that $g^{-1}\mathfrak{L}$ lies in $\mathfrak{D}$. Instead only such lattice points $\mathfrak{L}$ are considered which satisfy

$$\mathfrak{L} \equiv \mathfrak{L}_0 \pmod{Q}$$

for a given $\mathfrak{L}_0$ and Q is a polynomial divisible by $|\mathfrak{T}|^3|\gamma|$

$$\sum_{\substack{\mathfrak{L} \equiv \mathfrak{L}_0 \pmod{Q} \\ \mathfrak{L}/g \text{ in } \mathfrak{D}'}} \frac{1}{A_0\left(\gamma, \frac{\mathfrak{L}'}{g}\gamma\frac{\mathfrak{L}}{g}\right)} : v(\mathfrak{D}_g) \longrightarrow \frac{1}{|Q|_p^{mn}}$$

as $g \to \infty$

As on page 225 Siegel [16]

$$\sum_{\substack{\mathfrak{T} \equiv \mathfrak{T}_0 (Q) \\ \mathfrak{T} \text{ in } \mathfrak{D}_g}} \frac{A(\gamma,\mathfrak{T})}{A_0(\gamma,\mathfrak{T})} : v(\mathfrak{D}_g) \longrightarrow \frac{A_Q(\gamma,\mathfrak{T}_0)}{|Q|_p^{mn}}$$

Similarly one can bring the equation (15) to this form.

In order to prove that $\rho(\gamma)$ is a constant it is prove

$$\lim_{g\to\infty} \sum_{\substack{\mathfrak{T} \equiv \mathfrak{T}_0 (Q) \\ \mathfrak{T} \text{ in } \mathfrak{D}_g}} \frac{d(\gamma,\mathfrak{T})}{v(\mathfrak{D}_g)} \Big/ \frac{A_Q(\gamma,\mathfrak{T}_0)}{|Q|_p^{mn}}$$

tends to a constant

Put $\mathcal{T} = t$ and when the corresponding 'p-adic' value is takmn t is said to be in $\mathfrak{D}_g$ or $\mathfrak{D}$

$$\lim_{T \to \infty} \sum_{\substack{|t|_p = 1 \\ t \text{ in } \mathfrak{D}_g,\ t \equiv t_0(Q)}}^{|t|_p = T} d(\gamma, t) = \frac{A_Q(\gamma, t_0)}{|\theta|_p^{mn}} \text{ times a constant}$$

where the constant depends on the nature of γ.

If t_0 is a polynomial representable by γ t_0 in $\mathfrak{D}_g$ is representable by γ in $\mathfrak{D}_g$ and a polynomial divisible by $|\gamma|\, t_0^3$

$$\prod_{(f)} \alpha_f(\gamma, t) = \prod_{f|Q} \alpha_f(\gamma, t) \times \prod_{(f,Q)=1} \alpha_f(\gamma, \mathcal{T})$$

$$\alpha_f(\gamma, t) = \alpha_f(\gamma, t_0), \quad t \equiv t_0(Q)$$

if f divides Q page 227 Siegel [16]

and

$$\prod_f \alpha_f(\gamma, t) = \frac{A_Q(\gamma, t_0)}{|Q|^{m-1}} \times \beta(\gamma, t) \qquad |\theta| \neq |\theta|_p$$

$$\beta(\gamma, t) = \prod_{(f,\theta)=1} \alpha_f(\gamma, t)$$

In order to prove that $f(\gamma)$ is a constant, it is enough to prove

$$\frac{|Q|_p^m}{|Q|^{m-1}\, T} \sum_{\substack{|t|_p = 1 \\ |t|_p \text{ in } \mathfrak{D}_g \\ t \equiv t_0(Q)}}^{T} \beta(\gamma, t) \to \text{a constant as } T \to \infty$$

'p-adic' representation does not affect the problem.

Now we take $\mathfrak{m} = 2k$ and we apply the method on page 228 [16] Siegel [16]. Here we make use of lemma 16, to write

$$\gamma(\sigma, t) = \sum_{d/t} \left(\frac{s}{d}\right) d^{1-k} \qquad d = |\sigma|$$

$$(d, Q) = 1$$

$$\sigma,\ d, t, \theta \in k[x] \quad B = \prod_{(f, \theta) = 1} \left(1 - \left(\frac{s}{f}\right) |f|^{-k}\right)$$

In order to {estimate $\rho(\sigma)$} prove that $\rho(\sigma)$ is equal to one it is enough to prove that

$$\frac{|\theta|_p}{T} B \sum_{|t|_p = 1}^{T} \gamma(\sigma, |t|_p) \quad \text{tends to a constant}$$

σ is 'p-adic' representation

$$|t| \equiv |t_0| \left(|\theta|_p\right)$$

Actually the limit is one

The rest of the argument is one page 230 Siegel [16] and pp 255-256 Siegel [16].

The case k = 1 is already known; when m is odd it is as in page 235 Siegel [16]. For odd orders of σ it can be similarly derived and proved equal to have one simple value as in Siegel [16] page 236.

In the binary case and in the ternary case ϵ_{mn} can be so adjusted that $\rho(\sigma)$ is always equal to one. This would have a siginificance even otherwise.

The details are a direct consequence of the principles in the equation Siegel [6] and the nature of B and γ..