CHAPTER - II

The proof of the main theorem for definite forms :

12. The main theorem of Siegel for definite or indefinite forms consists of two parts one of which is the arithmetical part. The arithmetical part is a generalization of Gauss's theorem on the representation of a positive integer as a sum of three sequares. Eisenstein generalized it to the number of representations of a positive integer t by means of a certain quadratic form $\mathfrak{S}$ when t and $\mathfrak{S}$ are taken from the rational number field and when they are mutually coprime. These formulae were generalized by Siegel for an arbitrary symmetric matrix $\mathfrak{T}$ representable by the symmetric matrix $\mathfrak{S}$. In this Chapter Siegel's results for definite forms are mentioned. The results for the indefinite forms are given in detail in the next Chapter. Here we have a short account of the

Methods of Siegel:

The different steps in the proofs as Siegel gave them are (1°) The convergence of the product $\prod_f \alpha_f \, (\gamma, \mathcal{T})$ taken over all the prime polynomials f such that the product of the sequence at any stage is divisible by almost all polynomials of lower degree.

(2°) The Generalization of the formula of Gauss and Eisenstein and

(3°) The induction part of the proof of the main theorem which is our identity. (1°) is proved on the same lines as Siegel using the Gaussian sums for function fields defined by Carlitz; an account of (2°) shall be given and the different steps in deriving the formula. Hasse - Witt theorems and the theorems on the genera are used in deriving this formula. Particular cases of the formulae, as already mentioned, were derived by Gauss and Eisenstein for the rational number field.

In proving (1°) and (2°) for function fields the discreteness of the valuation is made use of. Especially wherever connectedness or arcwise connectedness is used in Siegel's proofs one has to make use of the discreteness of the valuation to get the results for function fields. This is noticed at a first instance in Lemma 9*. Later on when the analytical part of the proof has to be given again these methods are required. It is desirable, therefore, to summarize here the different steps of the analytical part of the proof as it is understood and interpreted to facilitate this work. Part of it is already found in the introduction.

* this thesis

Chapter II can be taken, as far as these results are concerned, to be a particular case of Chapter III. So we proced to establish the identity and our

13. THEOREM

$$\frac{\bar{A}(\mathfrak{S},\mathfrak{T})}{A_0(\mathfrak{S},\mathfrak{T})} = \rho(\mathfrak{S})\ \epsilon_{mn}\ \prod_f \alpha_f(\mathfrak{S},\mathfrak{T})$$

where the product on the right hand side runs over all the polynomials f such that the product at every state is divisible by almost all polynomials of lower degree.

Lemmas from Siegel which can be directly generalized are Lemmas 1 to 7 Siegel [5] and Lemm 11 page 535 [5]

Given an integral representation of $\mathfrak{T}$ by $\mathfrak{S}$, say $\mathfrak{C}_0$ it is possible to find a general parameter solution. This is given by the following lemma which needs minor modifications from Siegel [5] pp 536

Lemma 1 : If $\mathfrak{C}_0'\mathfrak{S}\mathfrak{C}_0 = \mathfrak{T}$ be a representation in K, K_f or $K_{1/x}$ then any other representation $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ in K, K_f or $K_{1/x}$ for which $(\mathfrak{C}_0'\mathfrak{S}\mathfrak{C} - \mathfrak{T})^{-1}$ exists ~~and it~~ is given, (with the help of an alternating matrix $\mathfrak{A} = \mathfrak{A}^{(m)}$ from K, K_f or $K_{1/x}$ respectively and a matrix $\mathfrak{B} = \mathfrak{B}^{(m,n)}$ from the same field) in the form,

$$\mathfrak{C} = \mathfrak{C}_0 + 2\mathfrak{B}(\mathfrak{A} - \mathfrak{B}'\mathfrak{S}\mathfrak{B})^{-1}\mathfrak{B}'\mathfrak{S}\mathfrak{C}_0 \qquad 1.1$$

Eqn (8) page 536 Siegel [5]

If conversely $\mathfrak{A}$ is an alternating matrix from K, K_f or $K_{1/x}$ and $\mathfrak{B}$ an arbitrary matrix from the same field for which $(\mathfrak{A} - \mathfrak{B}'\mathfrak{S}\mathfrak{B})^{-1}$ exists then $\mathfrak{C}$ is a solution of $\mathfrak{x}'\mathfrak{S}\mathfrak{x} = \mathfrak{T}$

This lemma is used to give the dimension of the manifold defined by the equation $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$. The proof of the lemma is given here in detail. It is the same as that given by Siegel except that we do not have the connectedness here to be made use of; on the other hand it is made clear that all that is needed is only the continuity, in the metric defined by the valuation in $1/x$ of

$$X = X_0 - \frac{B'\mathfrak{S}X_0}{B'\mathfrak{S}B} \cdot B$$

as a function of X_0 where B is a column matrix , X is a row matrix and $\mathfrak{S}$ is a symmetric matrix of order greater than one.

Lemma 2 : Let $\mathfrak{S}$ and $\mathfrak{T}$ both lie on K, K_f or $K_{1/x}$. For $n < m$ the equation $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$ (4) defines an irreducible manifold of dimension mn $-\frac{n(n+1)}{2} = \nu$. For n=m by the adjunction of $(|\mathfrak{T}|/|\mathfrak{S}|)^{1/2}$ to the corresponding field, is obtained, on which there exist exactly two different algebraic manifolds of demension ν on one of which $|\mathfrak{X}| = \rho$ and on the other $|\mathfrak{X}| = -\rho$ if -1 is a quadratic residue modulo p these two manifolds can be identified.

Proof: For m = n = 1 the assertion is trivial. Let m $>$ 1. If the equation $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$ has no solution in K or $K_{1/x}$ we adjoin ρ . Over the extended field we get two algebraic manifolds of dimension ν . Assume n = 1 so that $\mathfrak{X}$ is a row matrix X and if $X = X_0$ is a solution any other solution is given by

$$X = X_0 - \frac{2B'\mathfrak{S}X_0}{B'\mathfrak{S}B} \cdot B$$

where B' is also a row matrix.

If B is replaced by λB by the homogeneity of the equation we have the same relations. That is, instead of all elements in the colomn B, m-1 ratios of the different elements of X fix X uniquely in terms of X_0. If $\mathfrak{X}_0'\gamma\mathfrak{X}_1 \neq \mathfrak{T}$ when the valuation in $1/_2$ is chosen as a metric we have sufficiently many solutions of the equation (4) for a continuous passage from $\mathfrak{X}_0$ to $\mathfrak{X}_1$, to be possible by means of the equation

$$X = X_0 - \frac{B'\gamma X_0}{B'\gamma B} . B$$

If $\mathfrak{X}_0\gamma\mathfrak{X}_1 = \mathfrak{T}$ choose X_2 a row matrix such that $x_1'\gamma x_2 \neq \mathfrak{T}, x_0'\gamma x_2 \neq \mathfrak{T}$ so that we can determine $\mathfrak{X}_2$ and then $\mathfrak{X}_1$ in terms of $\mathfrak{X}_2$. This gives once again a continuous passage from X_0 to X_1 as described above. Assume that $\mathfrak{T}$ has the form $\begin{pmatrix}\mathfrak{T}_1 & 0\\ 0 & t\end{pmatrix}$. If $\mathfrak{X} = (\mathfrak{y}\,x)$ then the

equation $\mathfrak{X}'\gamma\mathfrak{X} = \mathfrak{T}$ can be decomposed into three equations $\mathfrak{y}'\gamma\mathfrak{y} = \mathfrak{T}_1, \mathfrak{y}'\gamma x = 0, x'\gamma x = t$. by induction assumption $\mathfrak{y}'\gamma\mathfrak{y} = \mathfrak{T}_1$ defines an algebraic manifold of $\frac{m(n-1)-n}{2}(n-1)$ dimensions and the general solution can be expressed in the neighbourhood of $\mathfrak{y}_0$ as a rational function of ν_1 parameters. Because $\mathfrak{y}'\gamma\mathfrak{y} = \mathfrak{T}_1$, $\mathfrak{y}$ is of rank n-1. The general solution $\mathfrak{y}'\gamma x = 0$ gives $x = \mathfrak{h}\tau$ where $\mathfrak{h} = \mathfrak{h}$ (m , m-n+1) of rank m - n + 1 and τ is an arbitrary column of m - n + 1 elements. If $\mathfrak{R}$ is such that $(\mathfrak{R}\mathfrak{y}) = \begin{pmatrix}E\\ 0\end{pmatrix}$, $\gamma = \mathfrak{R}'\gamma_1\mathfrak{R}$ then γ_1 can be written as $\begin{pmatrix}\mathfrak{T}_1 & \mathfrak{T}_2\\ \mathfrak{T}_2 & \mathfrak{T}_3\end{pmatrix}$

If $\mathfrak{R}x = y$ then $\mathfrak{y}'\gamma x = (\mathfrak{T}_1\ \mathfrak{T}_2)\,y$ and $\mathfrak{h} = \mathfrak{R}^{-1}(-\mathfrak{T}_1^{-1}\mathfrak{T}_2)$

$\mathfrak{h} = \mathfrak{R}^{-1}\left(-\mathfrak{T}_1^{-1}\mathfrak{T}_2\right)$ is a choice of $\mathfrak{h}$. Then

$$\mathfrak{y}'\gamma x = (\mathfrak{T}_1, \mathfrak{T}_2)\ y$$

$$\mathfrak{R}(\mathfrak{y}\mathfrak{h}) = \begin{pmatrix}E^{(n-1)}, & -\mathfrak{T}_1^{-1}\mathfrak{T}_2\\ 0 & E^{(m-n+1)}\end{pmatrix}$$

where $\mathfrak{y}\mathfrak{z}$ is nonsingular and has an inverse; and because

$$(\mathfrak{y}\mathfrak{z})'\gamma(\mathfrak{y}\mathfrak{z}) = \begin{pmatrix} \mathfrak{T}_1 & 0 \\ 0 & \mathfrak{z}'\gamma\mathfrak{z} \end{pmatrix}$$

the matrix $\mathfrak{z}'\gamma\mathfrak{z} = \mathfrak{T}_4$ is of nonzero determinant.

The equation $T'\mathfrak{T}_4T = t$ goes into the equation $X'\gamma X = t$ by means of $X = \mathfrak{z}T$ ($\mathfrak{z}$ is in K or $K_{1/x}$ as required) then $X'\gamma X = t$ is an irreducible manifold of $\nu_1 + m - n$ dimensions. This finishes the induction. In case m=n by successively reducing the equation in the last stage two irreducible manifolds are obtained corresponding to the sign of f

14. The Calculation of the $\mathfrak{f}$-adic densities.

For the solution of the equation $\mathfrak{x}'\gamma\mathfrak{x} = \mathfrak{T}$ the calculation of the $\mathfrak{f}$-adic densities is carried out next using Gaussian sums for the rational function field introduced by Carlitz* [11].

The $\mathfrak{f}$-adic densities play an important role in the theory as it is already known to the reader.

The number of solutions $\mathfrak{x}$ of $\mathfrak{x}'\gamma\mathfrak{x} \equiv \mathfrak{T} \pmod{\mathfrak{f}}$ is $A_\mathfrak{f}(\gamma,\mathfrak{T})$ and it is denoted by $A_\mathfrak{f}(\gamma,\mathfrak{T},b)$ if $\mathfrak{x}$ has the greatest divisor b. $A_\mathfrak{f}(\gamma,\mathfrak{T},e) = B_\mathfrak{f}(\gamma,\mathfrak{T})$ is the number of primitive representations modulo $\mathfrak{f}$. This number depends precisely on the classes of γ and $\mathfrak{T}$ in $R_\mathfrak{f}$

* The Singular Series of Sums of Squares of Polynomials pp 1105 - 1120. Duke Math. Journal (1947)

<u>Lemma 3</u> : Let f be a prime polynomial which does not divide $|\mathfrak{S}|\,|\mathfrak{T}|$. Then all the representations of $\mathfrak{T}$ by $\mathfrak{S}$ are primitive. If δ and ϵ denote the Legendre symbols $\left((-1)^{m/2}|\mathfrak{S}|/f\right)$ and $\left(\frac{(-1)^{\frac{m-n}{2}}|\mathfrak{S}|\,|\mathfrak{T}|}{f}\right)$ and if degree of $f = r$ then

$$p^{r\frac{n(n+1)}{2}-mn}\;A_f(\mathfrak{S},\mathfrak{T})$$

$$=\left(1-\delta p^{-\frac{rm}{2}}\right)\left\{1+\varepsilon p^{r\frac{n-m}{2}}\right\}$$

times $$\prod_{k=1}^{n/2}\left\{1-p^{r\,\overline{2k-m}}\right\} \quad m\text{ even, } n\text{ even}$$

$$=\left(1-\delta p^{-\frac{rm}{2}}\right)\prod_{k=1}^{\frac{n-1}{2}}\left(1-p^{r\,\overline{2k-m}}\right)$$ ~~$(1-p^{r}$ (modd, neven)~~

meven, nodd

$$=\prod_{k=1}^{n}\left(1-p^{r\,\overline{2k-m-1}}\right) \quad m\text{odd, } n\text{even}$$

$$=\prod_{k=1}^{\frac{n-1}{2}}\left(1-p^{r\,\overline{2k-m-1}}\right) \text{ times } \left(1+\varepsilon p^{r\frac{1-m}{2}}\right)$$

modd, nodd

For calculation of $A_f(\mathfrak{S},\mathfrak{T})$ one can assume that the $\mathfrak{T}$ is a diagonal matrix the diagonal elements of which are $t_1, \text{-- -- -- --}, t_n$. Let $\mathfrak{x}$ represent the first column of $\mathfrak{X}$. That is $\mathfrak{x}'\mathfrak{S}\mathfrak{x} \equiv t$ (mod f). Let A be any other solution which is a solution of this congruence. Because A is primitive A can be completed by a complement to a unimodular matrix

$$(A\;\mathfrak{b}) \equiv \mathfrak{b}_1 \ (\text{mod} f)$$

can be so chosen that

$$(\mathfrak{b}_1'\mathfrak{S}\mathfrak{b}_1) \equiv \begin{pmatrix} t_1 & 0 \\ 0 & \mathfrak{S}_1 \end{pmatrix} \ (\text{modulo } f)$$

If there exists an $\mathfrak{x} = \mathfrak{C}$ with $\mathfrak{x} \equiv A$ (modulo f) then $\mathfrak{C}$ can be completed by a complement $\mathfrak{U}$ to a unimodular matrix $(\mathfrak{C}\,\mathfrak{U}_1) = \mathfrak{U}_2$, $\mathfrak{C}$ itself has the form $\mathfrak{U}_1 \begin{pmatrix} 1 & \mathfrak{B}' \\ 0 & \mathfrak{C} \end{pmatrix}$ with integral $\mathfrak{B}, \mathfrak{C}$. Because $\mathfrak{C}_1'\mathfrak{S}\mathfrak{C}_1$ is congruent to a diagonal matrix formed by $t_2, \;---, t_n,$ To a given A we have an $\mathfrak{U}_1$ and an $\mathfrak{S}_p$ and the solutions now depend on the number of solutions of

$$\mathfrak{x}_1'\mathfrak{S}\mathfrak{x}_1 \equiv \mathfrak{T} \pmod f$$

Therefore $A_f(\mathfrak{S}, \mathfrak{T}) = \sum_A A_f(\mathfrak{S}_0, t_1)$ where A satisfies $A'\mathfrak{S}A \equiv t_1 \pmod f$

If n=1 $A_f(\mathfrak{S}_0, \mathfrak{T}_1) = 1$

When ω is a primitive p^{th} root of unity p^r times the number of solutions of A is the same as

$$\sum_{h, A \bmod f} \omega^{h\,\mathrm{Sgn}\,(A'\mathfrak{S}A - t)} \quad \text{equation 21, Siegel [5] p. 541.}$$

where h and the elements of A run through all the integers modulo f and r is the degree of f . There the analogy of the Gaussian sums in function fields and the properties of the Gaussian sums are used (Carlitz [11])

$$\sum_{(P,f)} \omega^{\mathrm{Sgn}\,P^2} = \bar{G}$$ where P is a

polynomials prime to f . Then

$$\sum_{(P,f)=1} \omega^{h\,\mathrm{Sgn}\,P^2} = \left(\frac{h}{P}\right)\bar{G} \quad \text{eqn 22 , Siegel [5] , p 541}$$

where (h/p)

denotes the Legendre symbol. To calculate the number of A we take γ to be the diagonal matrix with diagonal elements $(\delta_1, - - - - , \delta_n)$ the product of which is $|\gamma|$. By the product formula of Gaussian sums

$$\sum_{A (\mathrm{mod}\, f)} \omega^{\lambda \, Sgn \, A' \gamma A} = \bar{G}^{m} \left(\frac{|\gamma|}{f}\right)\left(\frac{\lambda}{f}\right)^{m}$$

λ runs through all the resides modulo f except 0 .

The evaluation of the Gaussian sums proceeds on the same principle as for the number field. When m is even the sum occuring on the right is - 1 and $(-t_1 / f)$ G when m is is odd. The special case m=1, $|\gamma| = t$ gives

$$G^2 = (-1/f)\, p^{r}$$

and the number of A required $= p^{r(m-1)}\left(1 - \delta p^{-\frac{rm}{2}}\right)$ m even

$$= p^{r(m-1)}\left(1 + \epsilon p^{r\frac{1-m}{2}}\right) m \text{ odd}$$

[Cf , eqns 23, 24, 25, Siegel [5] page 541]

where δ and ϵ are the Legendre symbols

$$\left(\frac{(-1)^{m/2}|\gamma|}{f}\right), \left(\frac{(-1)^{\frac{m-1}{2}}|\gamma| t_1}{f}\right)$$

Let now $n > 1$ and the assertion be true for n-1 instead of n.

$$|\gamma| \, |\mathfrak{N}_1|^2 \equiv t_1 |\gamma| \; (\text{modulo} f)$$

Therefore

$$\left(\frac{|\gamma_1|}{f}\right) = \left(\frac{|\gamma| t_1}{f}\right)$$

Further the number of A from what has been derived above is

$$p^{r(m-1)}\left(1-\delta p^{-\frac{rm}{2}}\right) \quad m\text{ even}$$

$$p^{r(m-1)}\left(1+\varepsilon p^{r\frac{1-m}{2}}\right) \quad m\text{ odd}$$

$$\left\{p^{r\frac{(n-1)n}{2}-(m-1)(n-1)}\right\} A_f(\gamma, 7)$$

equal to

(1) $$p^{r(m-1)}\left(1-\delta p^{-\frac{rm}{2}}\right)\left\{1+\varepsilon p^{r\frac{n-m}{2}}\right\}\prod_{k=1}^{\frac{m-2}{2}}\left\{1-\delta p^{r\overline{2k-m}}\right\}$$

m even, n even

m even, n even

(2) $$p^{r(m-1)}\left(1-\delta p^{-\frac{rm}{2}}\right)\prod_{k=1}^{\frac{n-1}{2}}\left(1-p^{r\overline{2k-m}}\right)$$

m even, n odd

(3) $$p^{r(m-1)}\left(1+\varepsilon p^{r\frac{1-m}{2}}\right)\prod_{k=1}^{\frac{m-1}{2}}\left(1-p^{r\overline{2k-m-1}}\right)$$

m odd, n odd

(4) $$p^{r(m-1)}\prod_{k=1}^{m/2}\left(1-p^{r\overline{2k-m-1}}\right)$$

m odd, n even.

That is

$$\alpha_{\mathfrak{p}}(\mathfrak{S},\mathfrak{T}) = A_{\mathfrak{p}}(\mathfrak{S},\mathfrak{T}) \Big/ |\mathfrak{p}|^{mn - \frac{n(n+1)}{2}}$$

$$= \left(1-\delta p^{-\frac{rm}{2}}\right)\left(1+\varepsilon p^{r\frac{n-m}{2}}\right)$$

$$\text{times} \prod_{k=1}^{n/2-1} \left(1-p^{r\,\overline{2k-m}}\right)$$

m even, n even

$$= \left(1-\delta p^{-\frac{rm}{2}}\right) \prod_{k=1}^{n-1)/2} \left(1-p^{r\,\overline{2k-m}}\right)$$

m even, n odd

$$= \left(1+\varepsilon p^{r\frac{n-m}{2}}\right) \prod_{k=1}^{\frac{n-1}{2}} \left(1-p^{r\,\overline{2k-m-1}}\right)$$

m odd, n odd

$$= \prod_{k=1}^{n/2} \left(1-p^{r\,\overline{2k-m-1}}\right)$$ m odd, n even

To prove the convergence of the product of the $\mathfrak{p}$-adic densities $\alpha_{\mathfrak{p}}(\mathfrak{S},\mathfrak{T})$ it is enough to take all the $\mathfrak{p}$ prime to $|\mathfrak{S}||\mathfrak{T}|$. The explicit evaluation of $\alpha_{\mathfrak{p}}(\mathfrak{S},\mathfrak{T})$ when $\mathfrak{p}$ divides $|\mathfrak{T}||\mathfrak{S}|$ is done for some special cases at the end of the section. This is necessary in the course of the main theorem when the order of $\mathfrak{S}$ is two and that of $\mathfrak{T}$ is one or two especially for the estimation of the constant $f(\mathfrak{S})$

Further, for the different powers $\mathfrak{p}^{a}$ of $\mathfrak{p}$ the nature of $A_{\mathfrak{p}^{a}}(\mathfrak{S},\mathfrak{T})$ is given in the next three lemmas. Proofs are as given in Siegel [5]. pp 542 - 544 .

Lemma 4 : Let f^{b} be the highest power of f dividing $|\mathfrak{T}|$ and let $a > 2b$ and $g = f^{a}$.

Then the numbers

$$|f|^{a\left\{\frac{n(n+1)}{2} - mn\right\}} A_{f^a}(\mathfrak{S},\mathfrak{T}) \quad \text{and}$$

$$f^{a\left\{\frac{n(n+1)}{2} - mn\right\}} B_{f^a}(\mathfrak{S},\mathfrak{T}) \quad \text{are}$$

independent of a. Lemma 13 Siegel [5] page 542

Lemma 5 : Let f^{b} be the highest power of the polynomial f occurring in $|\mathfrak{T}|$ and let $a > 2b$. To each integral solution $\mathfrak{C}_1$ of $\mathfrak{C}_1'\mathfrak{S}\mathfrak{C}_1 \equiv \mathfrak{T}$ (mod f^{a}) there exists in R_f a solution of $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ with $\mathfrak{C} \equiv \mathfrak{C}_1$ (mod f^{a-b})

Lemma 14 Siegel [5] p. 544

Lemma 6 : Let q and r be two coprime polynomials and let $\mathfrak{S}, \mathfrak{T}$ be in R_{qr}

$$A_{qr}(\mathfrak{S},\mathfrak{T}) = A_q(\mathfrak{S},\mathfrak{T})\, A_r(\mathfrak{S},\mathfrak{T})$$
$$B_{qr}(\mathfrak{S},\mathfrak{T}) = B_q(\mathfrak{S},\mathfrak{T})\, B_r(\mathfrak{S},\mathfrak{T})$$

If $\mathfrak{C}_1'\mathfrak{S}\mathfrak{C}_1 = \mathfrak{T}_1$ is a representation in R_q and $\mathfrak{C}_2'\mathfrak{S}\mathfrak{C}_2 = \mathfrak{T}_2$ a representation in R_r then there exists in R_{qr} a $\mathfrak{C}$ with $\mathfrak{C} \equiv \mathfrak{C}_1$ (mod q) $\mathfrak{C}_1$ in R_q and $\mathfrak{C} \equiv \mathfrak{C}_2$ (mod r) in R_r and $\mathfrak{C}'\mathfrak{S}\mathfrak{C} = \mathfrak{T}$ in R_{qr} Lemma 15 Siegel [5], 544

This is an immediate consequence of the Chinese Remainder theorem.

Lemma 7 : Let $\mathfrak{B} = \mathfrak{B}^{(n)}$ be in R_q and let the determinant $|\mathfrak{B}|$ be a polynomial dividing q . $\mathfrak{T} = \mathfrak{B}'\mathfrak{T}_1\mathfrak{B}$ with integral $\mathfrak{T}_1$, $|\mathfrak{T}_1|$ and $|\mathfrak{T}|^{3} | q$. Then $A_f(\mathfrak{S},\mathfrak{T},\mathfrak{B})) = |\mathfrak{B}|^{n-m-1} B_f(\mathfrak{S},\mathfrak{T})$

Lemma 17 Siegel [5] p. 546

Units:

The number of integral solutions of the equation $\mathfrak{x}'\gamma_i\mathfrak{x}=\gamma_i$ is denoted by $E(\gamma_i)$. The solutions are called the units of γ when $\gamma_i = \gamma$. The number of $A_f(\gamma)$ such that $\mathfrak{x}'\gamma\mathfrak{x} \equiv \gamma$ (mod f) is denoted by $E_f(\gamma)$ for a polynomial f. If q and r are two coprime polynomials

$$E_{qr}(\gamma) = E_q(\gamma)\, E_r(\gamma)$$

Also $$A_{qr}(\gamma) = A_q(\gamma)\; A_r(\gamma)$$

Lemma 8 : If f^b is the highest power of f dividing $|\gamma|$ and if $a>2b$, $g=f^a$ then the number $\frac{1}{2}|f|^{-\frac{m(m-1)}{2}}E_f(\gamma)$ is independent of a and has in the case $b=0$ the value

$$\prod_{k=1}^{\frac{m-1}{2}}\left(1-p^{-2rk}\right) \text{ or } \left\{1-p^{-\frac{rm}{2}}\;\frac{(-1)^{m/2}|\gamma|}{f}\right\}$$ Lemma 18 Siegel [5] page 547

according as m is odd or even. In Chapter I three lemmas, proved by Siegel, were stated on the genera of quadratic forms. There is one more lemma on the convergence of the product of the f-adic densities when the f run through all the polynomials, so arranged that the product of these polynomials at each stage is divisible by almost all polynomials of lower degree.

Lemma 9 : Let m=2 and $-|\gamma|$ be a square, m=n+2 and $-|\gamma|\,|\mathfrak{T}|$ a square. The product of all the $\alpha_f(\gamma,\mathfrak{T})$ over the sequence of f mentioned as above converges and its value is zero only if one factor is zero.

Proof is the same as given in Siegel [5]. Lemma 19 page 548

The next section is on the arithmetical part of the main theorem of Siegel, Here no new ideas, other than those given by Siegel, are introduced. Subsequently in the analytical part of the proof methods, essentially characteristic of the field of rational functions, are introduced for certain quantitative estimates. A rather brief summary is given of the arithmetical part of the proof.

PART - II

The Arithmetical part of the proof of the main theorem for definite symmetric matrices.

15. The arithmetical part consists of two formulae which are used directly in the analytical part.The second formula which is to be used here will be used in the analytical part in a limiting form. The procedure to the limit is possible only with the help of lemma 17 Siegel [5]. It is a sort of comparison of formulae (1) and (2) given below* with a method of induction true to this theory that gives the final identity which is the main theorem of Siegel. More details of this are given in the analytical part. These can be derived as particular cases of the results in Chapter III.

The first formula has a particular case done by Gauss and Eisenstein and Siegel called it the generalized formula of Gauss and Eisenstein in the small. Here $\mathfrak{S}$ and $\mathfrak{T}$ are of orders m and n.

* page 54 of this thesis

1. Generalized formula of Gauss and Eisentstein $(m > n)$

$$\sum_{\gamma_k v \gamma} \frac{B(\gamma_k, \mathfrak{T})}{E(\gamma_k)} = \sum_{\{\mathfrak{H}\}} F(\mathfrak{H}, \gamma)\, M(\mathfrak{H})$$

$$= \sum_{(\mathfrak{H}_k) v (\mathfrak{H})} \frac{1}{E(\mathfrak{H}_k)} \qquad \text{Eqn 49 Siegel [5] page 557}$$

$\gamma_k v \gamma$ means that γ_k and γ are in the same genus and $\mathfrak{H}_k$ runs through all the distinct genus representants of definite $\mathfrak{H}$ (m-n). $F(\mathfrak{H}, \gamma)$ is the number of reduced $\mathfrak{Q}$ such that

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{Q} \\ \mathfrak{Q}' & |\mathfrak{T}|^{-1}\mathfrak{H} + \mathfrak{Q}'\mathfrak{T}^{-1}\mathfrak{Q} \end{pmatrix} \qquad \text{Siegel [5] pp 559}$$

is in the same genus as γ. $\mathfrak{Q}$ and $\mathfrak{H}$ are to be defined.

The second formula is the relation (1) for quantities modulo f. It is [5] p 559, Eqn 51

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

where $(\mathfrak{H})$ runs through all the class representants modulo f $F_f(\mathfrak{H}, \gamma)$ is the number of reduced $\mathfrak{Q}$ for which

$$\begin{pmatrix} \mathfrak{T} & \mathfrak{Q} \\ \mathfrak{Q}' & |\mathfrak{T}|^{-1}\mathfrak{H} + \mathfrak{Q}'\mathfrak{T}^{-1}\mathfrak{Q} \end{pmatrix} = \gamma_0 \qquad \text{Eqn 50, page 559}$$

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 $F_f(\mathfrak{H}, \gamma)$ and $F(\mathfrak{H}, \gamma)$ with one to one correspondence between the class representants $(\mathfrak{H})$ and the genus representants $\{\mathfrak{H}\}$.

Instead of the full proofs of the formula as done by Siegel a brief summary is given referring to the single steps in Siegel's paper [5] , namely equations ; 46,47,48 and 49.

In order to derive the formula (1) initially two other formulae are derived, namely,

$$\frac{B(\mathfrak{S},\mathfrak{T})}{E(\mathfrak{S})} = \sum_{(\mathfrak{H})} \frac{B(\mathfrak{H})}{E(\mathfrak{S})} \quad \text{---}(3)$$

$B(\mathfrak{S},\mathfrak{T})$ is the number of primitive solutions of $\mathfrak{x}'\mathfrak{S}\mathfrak{x} = \mathfrak{T}$ in $K = k[x]$ and $B(\mathfrak{H})$ of the $B(\mathfrak{S},\mathfrak{T})$ primitive representations belong to the same class ($\mathfrak{H}$). $\mathfrak{H}$ is of determinant $|\mathfrak{S}|\,|\mathfrak{T}|^{m-n-1}$. So a first step is to explain the meaning of this last statement. After this is accomplished the next formula is

$$\frac{B(\mathfrak{H})}{E(\mathfrak{S})} = \frac{C(\mathfrak{H},\mathfrak{S})}{E(\mathfrak{H})} \quad \text{---}(4)$$

The definition of $\mathfrak{H}$, $\mathfrak{y}$ and the reduced $\mathfrak{y}$ and $\mathfrak{H}$ give almost the complete statement as well as the proof of the formulae. The proof is really complete only after some of the summations are justified with the help of the Hasse - Witt theorem and Lemmas 20,21 and 24 Siegel [5] . Lemma 24 is needed for the formula in the small. In choosing f to be a multiple of $(|\mathfrak{S}|\,|\mathfrak{T}|^m)^4$ in the latter formula one can see a sufficiently large degree has to be chosen for the polynomials. The composite nature of f needs the lemma repeatedly in the proofs. Siegel [5] pp 558 - 561

PART - III

The analytical part of the proof of the main theorem of Siegel for definite forms

16. The analytical part of the proof of the main theorem of Siegel consists of (1) a complete geometric interpretation of $A_0(\mathfrak{S},\mathfrak{T})$ and (2) the induction part of the proof of the main theorem.

In function fields for this purpose one has to fall back on the thesis of Artin. Artin's results on quadratic function fields can be interpreted as those for binary quadratic forms by making use of the correspondence between ideal theory and quadratic forms. By a method of induction on binary quadratic forms it is evaluated for the more general $\mathfrak{S}$ and $\mathfrak{T}$. The principle is in Siegel but this part differs considerably from Siegel's work on the rational number field.

In the rational number field to calculate $A_0(\mathfrak{S},\mathfrak{T})$ which he calls the density of representation, Siegel represented $\mathfrak{X}$ in the mn dimensional Eulidean space and $\mathfrak{T}$ in the $\frac{n(n+1)}{2}$ dimensional Euclidean space. If $\mathfrak{T}$ is taken as one of a set of points $\mathfrak{B}$, a domain containing $\mathfrak{T}$, $\mathfrak{X}$ traces the domain $\mathfrak{B}'$ and

$$A_0(\mathfrak{S},\mathfrak{T}) = \lim_{D \to \mathfrak{T}} \frac{v(\mathfrak{B}')}{v(\mathfrak{B})}$$

The details can be found in Siegel [5] and [16].

$\rho(\mathfrak{S})$ has been proved equal to one by means of deep analytical methods due to Siegel [5] and it can be proved to be constant even in the case of function fields. This i s found in a later paragraph at the end of Chapter III.

17. $A_0(\mathfrak{S},\mathfrak{T})$ for the various orders of $\mathfrak{S}$ and $\mathfrak{T}$ starting from m = 2, n = 2, in function fields.

As far as the arithmetic is concerned it appears as if this part is different (not radically) from the corresponding analogue in the case of the rational number field. For instance Dirichlet's class number formula was derived as a special case in the rational number field after Siegel gave the complete proof of the identity; whereas in function fields certain quantitative estimates are possible only by applying Dirichlet's formula generalized by Artin. Ultimately, after the complete proof is given the formula can be given a new interpretation in the language of quadratic forms though it is not possible before one completes Siegel's theory for function fields. The original derivation was due to the arithmetic of quadratic extensions of K.

Let D be a square free polynomial, $K(\sqrt{D})$ be the quadratic extension obtained by adjoining $\sqrt{D}$ to K.

The analogue of the class number formula of Dirichlet for function fields reads

$$\lambda = c \prod_{f} \left(1 - \left(\frac{[D]}{f}\right)\frac{1}{|f|}\right)^{-1}$$

where h is the number of ideals of $K(\sqrt{D})$ and f runs through primary [3]* and prime polynomials. $c = 2\sqrt{|D|}/_{p+1}$ in case degree of D is even and $\operatorname{Sgn} D = g$, a primitive element of the nonzero elements of the prime field k .

$c = \sqrt{\frac{|D|}{p}}$ if degree of D is odd.

If α, β is any integral basis of the field $K(\sqrt{D})$ and X, Y are integral elements from any ideal $\{\alpha X + \beta Y\}$ are elements of the ideal and $\{\alpha' X + \beta' Y\}$ are the set of conjugates. The number of inequivalent integral (X, Y) such that $|X^2 - DY^2| = |f|$ is the same as that of the number of inequivalent integral ideals with norm in value equal to that of f at $1/x$. That is, the number of inequivalent integral (X, Y) such that

$$|\alpha X + \beta Y| \; |\alpha' X + \beta' Y| \leq p^{\delta}$$

is the same as the number of integral ideals with norm in the value with respect to $1/x$.

$Z(S)$, the zeta function of $K(\sqrt{D})$

$$= \frac{1}{1-p^{-(s+1)}} \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}}$$

$$= \sum_{\mu=0}^{\infty} \frac{p^\mu}{p^{\mu s}} \sum_{\nu=0}^{\infty} \frac{\sigma_\nu}{p^{\nu s}}$$

$$= 1 + \frac{p\sigma_0 + \sigma_1}{p^s} + \frac{p^2\sigma_0 + p\sigma_1 + \sigma_2}{p^{2s}} + ---$$

$$+ \frac{p^{n-2}\sigma_0 + -- + \sigma_{n-2}}{p^{(n-2)s}} + ---$$

$$+ \sum_{\nu=n-1}^{\infty} \frac{p^\nu \sigma_0 + -- + p^{\nu - \overline{n-1}}\sigma_{n-1}}{p^{\nu s}}$$

{* [3] p.54}

with $|N\mathfrak{a}| = p^{\nu}$,

$$Z(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^{s}} = \sum_{\nu=0}^{\infty} \frac{H(p^{\nu})}{p^{\nu s}}$$

Therefore, for $\nu \geqslant n-1$ (using the reciprocity law)

$$\sigma_{\nu} = 0, \quad \nu \geqslant n$$

$$H(p^{\nu}) = p^{\nu}\sigma_0 + p^{\nu-1}\sigma_1 + \text{---} + p^{\nu-n+1}\sigma_{n-1}$$

$$= p^{\nu} \sum_{\mu=0}^{n-1} \frac{\sigma_{\mu}}{p^{\mu}} = h_1 / c\, p^{\nu}$$

h_1 i~~s~~ obtained by taking the residue of the zeta function at s=1 in two ways [3] . Because there are polynomials of degree ν, $1/k$ times ω (where $\omega = p^2 - 1$ or $p - 1$ according as $D = g$ or not) is the value corresponding to $A_0(\gamma, \eta)$. It is the average $\Sigma A(\gamma_i, \eta)/h$ in a neighbourhood of in the valuation with respect to $1/x$. These are also neighbourhoods in the valuation with respect to $1/x$. It is to be noticed that as the valuation with respect to x tends to zero, valuation with respect to $1/x$ tends to ∞ and these still ~~skat~~ satisfy the axioms for neighbourhoods. Also the integers are taken now in the sense of Artin [3] . Define $P(\gamma, \eta) = \Sigma A(\gamma_i, \eta)/h$ and take all the elements (when n = 1) such that $p^{-M} \leq |\eta' - \eta| \leq p^{-N}$ for N and M sufficiently large

$\Sigma P(\gamma, \eta)$ / number of η'

as N $\longrightarrow \infty$ is the value of $A_0(\delta, \mathfrak{z})$. When n > 1 the inequalities are taken for each of the elements of $\mathfrak{z}$ with the corresponding elements of $\mathfrak{z}'$. With the above fact that the neighbourhoods are taken when the distance matric taken with the respect to $^1|_x$ tends to ∞ the above difinition of $A_0(\delta, \mathfrak{z})$ is justified for function fields. That is we have actually taken the 'number'of real representations in the neighbourhood of $\mathfrak{z}$.

After this last most assential digression one can go back to the calculations. Consider the principal binary quadratic forms and take the representations, of polynomials of degree less than that of degree of D = $|\delta|$ by such binary forms; then the above average is calculated in the following fashion. Let f be the polynomial of degree ν less than that of degree of D . Keep in view the equation

$$Z(s) = 1 + \frac{p\sigma_0 + \sigma_1}{p^s} + \frac{p^2\sigma_0 + p\sigma_1 + \sigma_2}{p^{2s}} + ---$$

$$+ \sum_{\nu=n-1}^{\infty} \frac{p^{\nu}\sigma_0 + p^{\nu-1}\sigma_1 + --- + p^{\nu-\overline{n-1}}\sigma_{n-1}}{p^{\nu s}}$$

Consider the polynomials g such that $p^{-M} \leq |g - f| \leq p^{-N}$ for N and M sufficiently large. If one takes the average over such polynomials of $P(\delta, \mathfrak{z})$ and takes the limit as N $\longrightarrow \infty$ the limit is $^1|_{R\omega}$.

For example if f is of degree twothe average is

$$\frac{p^{2}\sigma_0 + p\sigma_1 + \sigma_2 + \text{---} + \lambda/k\,(p^N + \text{---} + p^M)}{p^2 + p^N + \text{---} + p^M}$$

times ω

and the limit of the above avarage is $\lambda 1/k\,\omega$ and for each genus it is $1/k\,\omega$. Here one should make a note of the fact that one considers the average over the polynomials of the same leading (highest degree) coefficient and degree. It is due to this reason that the limit is taken as the neighbourhood shrinks to the point represented by f. This can be given an algebraic interpretation. For if such a polynomial f is taken as

$$a_0 + a_1 z + \text{---} + a_n z^n + \text{---} + a_N z^N + \text{---} + a_M z^M$$

and f is represented for sufficiently large N and M by $X^2 - DY^2$ one gets a set of equations which are relations between the elements of k. For arbitrary D it is not true that these are independent relations; for degree of D can ~~xx~~ be taken sufficiently large and there cannot be more than a certain number of independent relations between the finite number p of elements of k, such a number being bounded. Therefore, whatever be a_0, —— —— $a_{\lambda-\beta}$ the probability is that as N and M tend to infinity one has the same limit for given m and n. Therefore $1/k$ is the $A_0(\gamma,\mathcal{F})$ for a certain f represented by γ and $1/k$ is independent of f. So $1/k$ is the $A_0(\gamma,\mathcal{F})$ for all γ of order two and $\mathcal{F}$ of order one where γ and $\mathcal{F}$ are integral.

So far the calculations have been done only for principal forms. For any arbitrary form $Ax^2 + Bxy + Cy^2$, if f is representable by $Ax^2 + Bxy + Cy^2$, Af is representable by X^2-Dy^2 and if Af is representable by X^2-Dy^2 f is representable by $Ax^2+Bxy+Cy^2$ rationally. Because we consider all the representations (x,y) in $K_{1/z}$ in order to calculate $A_0(\mathfrak{S},\mathfrak{T})$ it is enough to consider the representations of Af by X^2-Dy^2 rationally (Chapter I, paragraph 4).

18. For more general n, $\mathfrak{T}$ is represented as a point in the $\frac{n(n+1)}{2}$ dimensional space over the completion of K at $1/z$ Consider the equation $\mathfrak{x}'\mathfrak{S}\mathfrak{x} = \mathfrak{T}$. For points in the neighbourhood, of $\mathfrak{T}$, denoted by $\mathfrak{B}$, $\mathfrak{x}$ is one of a set of points $\mathfrak{B}'$. Instead of taking all the points in the neighbourhood of $\mathfrak{T}$ one takes $\mathfrak{T}$ with elements which are polynomials g satisfying the condition

$$p^{-M} \leq |g_{ij}-f_{ij}| \leq p^{-N}$$

It is assumed that the $A_0(\mathfrak{S},\mathfrak{T})$ which has been defined above is calculated upto m,1 and it is evaluated for m+1,1. Suppose C is the value upto m and 1. That is if a quadratic form is considered to represent the polynomial f the average is C. Consider a form of the type,

$$A_1x_1^2 + --- + A_mX_m^2 + A_{m+1}X_{m+1}^2$$

There is no loss of generality in assuming the forms to be diagonal. This fact will be explained soon. Consider a polynomial of degree ν. The average $A_0(\mathfrak{S}^{(m+1)}, \mathfrak{T}^{(1)})$ in this case is $Cp^{\frac{\nu-r}{2}}$ because the number of values of Xm+1 is $p^{\frac{\nu-r}{2}}$ once we fix the leading coefficients. If $\nu-r$ is odd it is estimated for a polynomial of degree $\delta+\nu$ sufficiently large such that

$\frac{\delta+\nu-r}{2}$ is integral

C for $m+1, 1$ is

$$\frac{Cp^{\frac{\delta-1}{2}}\, p^{\frac{\delta+\nu-r}{2}}}{p^{\delta-1}} = Cp^{\frac{\nu-r+1}{2}}$$

if ν is even, δ is odd.

C at $\delta+\nu$ for m + 1, 1 is $C\, p^{\delta/2}\, p^{\frac{\delta+\nu-r-1}{2}}$

The average in the limit is therefore $Cp^{\frac{\nu-r}{2}}$ because over a large number 'N' of polynomials the arithmetic mean $\frac{C_1 + \,--\, + C_N}{N}$ is equal to the geometric mean $\sqrt[N]{C_1 -- C_N}$, C_i being the averages the ratio between any two elements of the set being bounded . In analogy with number fields take

$$C = \alpha_{m1} \| \gamma^{(m)} \|^{-n/2} \| \mathfrak{z} \|^{\frac{m-n-1}{2}} \text{ for } m,1$$

$$C \text{ for } m+1,1 = \alpha_{m1} \| \gamma^{(m)} \|^{-n/2} \| \mathfrak{z}^{(1)} \|^{\frac{m-n-1}{2}} \text{ times } p^{\frac{\nu-r}{2}}$$

$$= \alpha_{m1} \| \gamma^{(m+1)} \|^{-n/2} \| \mathfrak{z}^{(1)} \|^{\frac{m+1-n-1}{2}}$$

and $\alpha_{m+1,1} = \alpha_{m,1}$. The result is true for m=2,n=1 as derived from Artin's formulae in the previous paragraph.

$\Lambda_0(\gamma, \mathfrak{z})$ for given γ and arbitrary order of $\mathfrak{z}$ is as follows

19. $A_0(\gamma, 7)$ for given γ and arbitrary order of 7 .

As a first step the value of C is assumed for m,1 and it is evaluated for m,2. Consider the equations,

$$A_1 x_1^2 + \text{———} + A_m x_m^2 = f_1 \qquad ----(1)$$

$$A_1 y_1^2 + \text{————} + A_m y_m^2 = f_2 \qquad ---(2)$$

$$\Sigma A_i x_i y_i = 0$$

If the average for (1) is C_1 and that for (2) is C_2 with the conditions (3) out of the $\sqrt{|f_1||f_2|}$ possible values of $\Sigma A_i x_i y_i$ only one is relevant. If $\sqrt{|f_1||f_2|}$ is not an integer it is to be noticed that as before in the limit

$$A_0(\gamma, 7) = \frac{C_1 p^{\delta_1} C_2 p^{\delta_2}}{\sqrt{|f_1||f_2|}\, p^{\delta}} \qquad \delta = \delta_1 + \delta_2$$

or

$$\frac{C_1 p^{\delta_1+1} C_2 p^{\delta_2-1}}{\sqrt{|f_1||f_2|}\, p^{\delta}}$$

or

$$\frac{C_1 p^{\delta_1-1} C_2 p^{\delta_2+1}}{\sqrt{|f_1||f_2|}\, p^{\delta}}$$

depending on the nature of and the degrees δ_1, δ_2 of f_1, f_2 . This is easily calculated to be

$$\alpha_{m1}\alpha_{m1} \|\gamma\|^{-n/2} \|7\|^{\frac{m-n-1}{2}} \qquad n = 2$$

That is $\alpha_{m2} = \alpha_{m1}\alpha_{m1}$

These evaluations would be clearer when one notices in Chapter III, a more general method is given suitable for definite and indefinite forms.

20. The induction part of the proof of the theorem for function fields.

Assume the theorem true for all values of m - n upto a certain μ (here it is 2) it is proved true for m 7 n , $m - n = \mu > 2$

$$\bar{A}(\gamma, \gamma) = \frac{\Sigma A(\gamma_i, \gamma) / E(\gamma_i)}{\Sigma\ 1/E(\gamma_i)} = 1/M(\gamma)$$

$$M(\gamma) = \Sigma\ 1/E(\gamma_i)$$

with the notation for $\mathfrak{z}$ as in Part II, $|\gamma| = |7|\,\mathfrak{z}$ if m and n are replaced by $m-n < \mu$

$$\bar{A}(\gamma, \gamma) = 1/M(|7|\mathfrak{z})$$

$$A_0(\gamma, \gamma) = \alpha_{m-n}\,(|7|\mathfrak{z})^{-\frac{m-n+1}{2}}$$

$$= \alpha_{m-n}\left(|\gamma||7|^{m-n-1}\right)^{-\frac{m-n+1}{2}}$$

Because the theorem is true for $m-n < \mu$

* For the definite case μ can take only the value 2 but the same method of proof with suitable modifications in true even for the indefinite forms. ~~Any way~~ The procedure is not repeated in Chapter III separately. ~~So~~ μ can be taken to be 2 here.

(A) $$\frac{1}{M(|\mathfrak{T}|\,\mathfrak{g})} = \epsilon_{m-n}\,\alpha_{m-n}\left\{|\gamma|\,|\mathfrak{T}|^{m-n-1}\right\}^{-\frac{m-n+1}{2}}$$

$$\text{times}\quad \lim_{|f|\to\infty}\frac{E_f(|\mathfrak{T}|\,\mathfrak{g})}{2^{\omega(f)}\,|f|^{(m-n)(m-n+1)/2}}$$

where f is a polynomial such that $|f|\to\infty$ in such a way that all polynomials of values less than f divide f

Also $M(|\mathfrak{T}|\mathfrak{g}) = M(\mathfrak{g})$

The value of M ($\mathfrak{g}$) given by (A) is substituted in the formulae of Gauss and Eisenstein in the large, that is in

(B) $$\sum_{k=1}^{h}\frac{B(\gamma_k,\mathfrak{T})}{E(\gamma_k)} = \sum_{(\mathfrak{g})} F(\mathfrak{g},\gamma)\,M(\mathfrak{g})$$

and one makes use of the formula in the small to get

$$\sum_{k=1}^{h}\frac{B(\gamma_k,\mathfrak{T})}{E(\gamma_k)} = \|\gamma\|^{\frac{m-n-1}{2}}\,\|\mathfrak{T}\|^{\frac{m-n-1}{2}}\ \text{times}$$
$$\lim_{|f|\to\infty} 2^{\omega(f)}\,|f|^{\frac{(m-n)(m-n+1)}{2}}\,\frac{B_f(\gamma,\mathfrak{T})}{E_f(\gamma)}$$

Define $\rho(\gamma)$ by

$$1/M(\gamma) = \rho(\gamma)\,\epsilon_m\alpha_m\,\|\gamma\|^{-\frac{m+1}{2}}\lim_{|f|\to\infty}\frac{E_f(\gamma)}{2^{\omega(f)}\,|f|^{\frac{m(m+1)}{2}}}$$

$$\epsilon_{mm} = \epsilon_{mn}\,\epsilon_{m-n}\quad,\ m>2,\ \epsilon_{11}=1$$

$$\epsilon_{22} = \epsilon_{21}$$

multiply both sides of B by $1/M(\gamma)$

$$\sum_{k=1}^{h} \frac{B(\gamma_k, \mathfrak{T})}{E(\gamma_k)} \Bigg/ \sum_{k=1}^{h} \frac{1}{E(\gamma_k)}$$

$$= \frac{\epsilon_m \alpha_m}{\epsilon_{m-n} \alpha_{m-n} \alpha_{mn}} \|\gamma\|^{-n/2} \|\mathfrak{T}\|^{\frac{m-n-1}{2}} \rho(\gamma) \text{ times } \lim_{|f| \to \infty} \frac{B_f(\gamma, \mathfrak{T})}{|f|^{mn - n\frac{(n+1)}{2}}}$$

One can substitute $A(\gamma, \mathfrak{T})$ and $A_f(\gamma, \mathfrak{T})$ for $B(\gamma, \mathfrak{T})$ and $B_f(\gamma, \mathfrak{T})$ because they vary proportionately and the equation takes the form

$$\frac{\bar{A}(\gamma, \mathfrak{T})}{A_0(\gamma, \mathfrak{T})} = \epsilon_{mn} \lim_{|f| \to \infty} \frac{\chi_{mn} A_f(\gamma, \mathfrak{T})}{|f|^{mn - n\frac{(n+1)}{2}}}$$

$$\text{times } \rho(\gamma)$$

The nature of $\rho(\gamma)$ is considered at the end of Chapter III.

21. The details of the induction part of the proof of the main theorem in function fields with special reference to binary forms:

It has been remarked already that in the last paragraph the discussions were restricted tod diagonal forms. The reason why it is enough to consider the diagonal form is max ($|A_{ij}|$) occurs in the diagonal of $\gamma(m+1)$ when an equivalent reduced form is taken and Am+1 can be taken to be that element. On the right side of the equation $\mathfrak{X}'\gamma\mathfrak{X} = \mathfrak{T}$ once the diagonal elements are taken into account the choice of the nondigaonal elements is restricted. By the choice of the equivalent reduced $\mathfrak{T}$ we are taking the maximum number of possibilities of the $\mathfrak{X}$ and of the choices of $\mathfrak{X}$ which give the required diagonal elements only some are relevant for the nondiagonal elements. In fact, of all the possible choices only one is relevant in the nondiagonal places.

ForrM = n = 1 the equation considered is $\gamma x^2 = \gamma$, $x = \pm 1$ are the two solutions . $\bar{A}(\gamma,\gamma) = 2$, $A_0(\gamma,\gamma)$ is defined equal to $2/\|\gamma\|$. For sufficiently large values of f', $\gamma x^2 \equiv \gamma \pmod{f'}$ gives $x^2 \equiv 1 \ (\mathrm{mod}\ f'/\|\gamma\|)$ which has $2^{\omega(f')}$ solutions. $\omega(f')$ is the number of prime divisors of f' and

$$2 \Big/ \frac{2}{\|\gamma\|} = \epsilon_{11} \cdot \lim 2^{-\omega(f')} 2^{\omega(f')} \|\gamma\|$$

$$= \epsilon_{11} \|\gamma\|$$

Rest of the induction is just the same as in Siegel [5] ; special reference is made to binary forms here.

In order to calculate α_{21} the identity of Siegel is compared with the class number formula of Artin. It reads

$$h = R \prod_{f} \left(1 - \left[\frac{D}{f}\right] \frac{1}{|f|} \right)^{-1}$$

$R = \sqrt{\frac{|D|}{P}}$ if degree of D is odd and it is equal to $2\sqrt{|D|} / p+1$ in case degree of D is even. If, in the formula

$$\frac{\sum A(\gamma_i, \mathfrak{T}) / E(\gamma_i)}{\sum 1/E(\gamma_i)} \Big/ A_0(\gamma, \mathfrak{T}) = \rho(\gamma)\, \epsilon_{mn} \prod_{f} \alpha_f(\gamma, \mathfrak{T})$$

γ and $\mathfrak{T}$ are symmetric binary matrices with the same determinant

$$1 \Big/ \sum 1/E(\gamma_i) = \alpha_{22} |\gamma|^{-1} |\gamma|^{-\frac{1}{2}} \epsilon_{22} \prod_{f} \alpha_f(\gamma, \gamma)$$

that is,

$$\frac{E(\gamma_i)}{h} = 1/_R\, \omega\, \rho(\gamma)\, \epsilon_{22} \prod_{f} \alpha_f(\gamma, \gamma)$$

with a simple calculation of the $\alpha_f(\gamma,\gamma)$ for f dividing $|\gamma|=D, \|\gamma\|=|D|$ and for f not dividing $|\gamma|=D$ separately. The number of genera of γ where $|\gamma|=D$ is 2^{s} or 2^{s-1} according as D is divisible by a prime polynomial of odd degree or not.

Case 1. Number of genera is 2^{s}, $R=\sqrt{\frac{|D|}{p}}$

Then
$$\frac{E(\gamma_i)}{h} = A_0(\gamma,\gamma)\ \rho(\gamma)\ \epsilon_{22}\ |D|\ 2^{s}\ \prod_f\left(1-\left[\frac{D}{f}\right]\frac{1}{|f|}\right)$$
$$\omega/h = \alpha_{22}|\gamma|^{-3/2}\ \rho(\gamma)\ \epsilon_{21}\ |D|\ 2^{s}\ \prod_f\left(1-\left[\frac{D}{f}\right]\frac{1}{|f|}\right)$$

$$\text{i.e}\ \frac{p-1}{1/R\ \prod\left(1-\left[\frac{D}{f}\right]\frac{1}{|f|}\right)^{-1}} = \frac{p\,|D|^{-\frac{1}{2}}}{(p-1)^2}\ \rho(\gamma)\ \prod_f\left(1-\left[\frac{D}{f}\right]\frac{1}{|f|}\right)$$
$$(p-1) = \frac{p^{3/2}\rho(\gamma)}{(p-1)^2}$$
$$\rho(\gamma) = \frac{(p-1)^3}{\sqrt{p}^{\,3}}$$

h is the number of classes in a genera; so for $2^{s}h$ Artin's class number formula is used.

Case 2 : Number of genera is 2^{s}, $R=\frac{2}{p+1}\sqrt{|D|}$

$$\frac{(p+1)}{2\cdot 2/p+1} = \left(\frac{p+1}{2}\right)^2 \qquad \rho(\gamma) = \frac{\left(\frac{p+1}{2}\right)^2}{\left(\frac{p+1}{2}\right)^2} = 1$$

<u>Case 3</u>: Number of genera is 2^{s-1} . The values are half of the values given above. The rest of the induction has been explained already.

f can assume the two values as before

$$f(\tau) = \frac{1}{2} \text{ or } \frac{(p-1)^3}{\sqrt{p^3}}$$

The work done so far can be looked upon as a special case of the next Chapter when all the 'measures' there are replaced by the trival measure. Also from the methods of proof one can see that the results remain unaltered if the variable x is replaced by $x+a$ or $\frac{1}{x+a}$ for $k(x) = k(\frac{1}{x}) = k(x+a) = k(\frac{1}{x+a})$