Part II

Seminar on Siegel's Theorem

The Proof of Siegel's Theorem on Finitely many quasi-integral points on a Curve, defined over a Number Field, of genus ≥ 1.

Michael Fried

Outline of the Proof of Siegels Theorem

Pages 1-13 covered Hilbert Irreducibility Theorem and variants, Weil Decomposition Thm., proof of Siegel's Theorem in genus 1 case, and some applications of the Thue-Siegel-Roth Theorem to genus 0 curves to find out when they might have infinitely many quasi-integral solutions in some number field K.

Contents

Section I - Siegel's Fundamental Inequalities, and modulo Statement A (below), the proof of Siegel's Theorem - $\mathcal{C}/K$ of genus ≥ 1. Then for any $\varphi \in K(\mathcal{C})$ (function field of $\mathcal{C}$), $\nexists$ no infinite quasi-integral set $\mathcal{M}$ of K-rational places of $\mathcal{C}$ with respect to φ.

Section II - Abel's Theorem, Jacobi Inversion

Section III - Theta Functions, Riemann Inversion

Section IV - (assuming Mordell-Weil Finiteness Theorem) Proof of Statement A - $\exists$ a field L, $[L:K] < \infty$ and infinitely many integers n with the property that there is a function field $L(\mathcal{C}_n)$ (called the n-division field of $\mathcal{C}$) where;

① If $\mathcal{C}$ has genus g, $\mathcal{C}^n$ is an unramified cover of $\mathcal{C}$ of degree n^{2g} $\ni$ given any infinite set of L-rat. places of $\mathcal{C}$, $\exists$ an ∞-sequence $\mathcal{M}_n$ of L-rat. places of $\mathcal{C}_n$, each lying over a place of $\mathcal{M}$

② If $K(\mathcal{C}) = K(x,y)$, then $K(\mathcal{C}_n) = K(\Phi_1, \Phi_2)$ where the poles of Φ_1 are not among an apriori finite set of points of $\mathcal{C}_n$, and Φ_1 and Φ_2 are connected by a polynomial equation $F(\Phi_1, \Phi_2) = 0$ with coeffics. in L and of degree at most $hg^3 n^{2g-2}$ in $\forall$ argument. Here $h = [K(\mathcal{C}) : K(x)]$.

Section I -

Prop. 1 - $\mathcal{C}$ defined over no. field K, $\mathcal{M}$ an ∞-set of K-rat. places of $K(\mathcal{C})$. Suppose $x, u \in K(\mathcal{C})$ (of orders h and r on $\mathcal{C}$ - order of $x = [K(\mathcal{C}) : K(x)]$) are totally bounded on $\mathcal{M}$ (i.e. x and u are bounded on $\mathcal{M}$ and the places $\mathcal{M}^{(\sigma)}$, places conjugate to $\mathcal{M}$ by $\sigma : K \to \mathbb{C}$, for all isomorphisms σ). Then, for $\delta > 0$ $\exists$ an infinite subsequence $\mathcal{M}(\delta)$ of $\mathcal{M}$ $\ni$

$$(1) \qquad |N_{K/\mathbb{Q}}(D_x(\mathfrak{p}))|^{\frac{r}{h}-\delta} \ll |N_{K/\mathbb{Q}}(D_u(\mathfrak{p}))|$$

where $D_x(\mathfrak{p}) = \prod_{i=1}^{h} E(q_i, \mathfrak{p})$, $\{q_i\}_1^h$ the poles of x, as in the Decomposition Thm.

Note - This is not just a theorem about distributions.

Def - Let $\mathcal{N}$ = infinite subsequence of $\mathcal{M} \ni \forall \sigma$, $\mathcal{N}^{(\sigma)}$ converges to a place $\bar{\mathfrak{p}}_{(\sigma)}$ of $K^{(\sigma)}(\mathcal{C}^{(\sigma)})$. Do not confuse $(\bar{\mathfrak{p}})^{(\sigma)}$ and $\bar{\mathfrak{p}}_{(\sigma)}$. In addition, assume neither x nor u has poles on $\mathcal{N}$. We will use $\mathcal{N}$ later, and without loss assume that $\mathcal{M} = \mathcal{N}$

Lemma 5 - If $x, v \in K(\mathcal{C})$, $\mathcal{C}$ any curve, then v is integral over $K[x]$ iff poles of v are all among poles of x (actually proved in Lemma 1).

Proof of Prop. 1 -

For $\forall\, n \in \mathbb{Z}^+$, apply R.R. to find $u_n \in K(\mathcal{C})$ $\ni$ $(u_n) = \dfrac{(D_x)^n\, \mathfrak{U}_n}{(D_u)^{t_n}}$ for $t_n = \left[\dfrac{g+r+nh}{r}\right]$. From Lemma 5, u_n is integrally dependent on u, so $|N_{K/\mathbb{Q}}(u_n(\mathfrak{p}))|$ is bounded on $\mathcal{N}$. Thus,

$|N(D_x(\mathfrak{p}))|^n \ll |N(D_u(\mathfrak{p}))|^{t_n}$ if we exclude from $\mathcal{N}$ the zeros of u_n. However, for n large $\frac{n}{t_n} > \frac{r}{h} - \delta$.

Q.E.D.

Prop. 2 - Let $\mathcal{C}$, K, $\mathcal{M}$, $\mathcal{N}$ and x be as in Prop. 1. Let $z \in K(\mathcal{C})$ of order r, be quasi-integral on $\mathcal{M}$.

Then for some $\sigma : K \to \mathbb{C}$, $\bar{\mathfrak{p}}_{(\sigma)}$ is a pole of $z^{(\sigma)}$ (and thus from weak form of Bezout's theorem, $\bar{\mathfrak{p}}_{(\sigma)}$ is algebraic). Let $\bar{\mathfrak{p}}_{(\sigma)}$ be a pole of order j of $z^{(\sigma)}$, L a finite ext. of $K^{(\sigma)}$. If $\varphi \in L(C)$ vanishes at $\bar{\mathfrak{p}}_{(\sigma)}$, then $\exists$ an infinite subsequence $\mathfrak{N}' \in \mathfrak{N} \ni$

$$② \quad |\varphi(\mathfrak{p}^{(\sigma)})| \ll \frac{1}{|N(D_x(\mathfrak{p}))|^{\frac{r}{2hlj}}}, \quad l = [K:\mathbb{Q}].$$

Proof -

Replacing z by $z+a$, we may assume $z^{(\sigma)}(\bar{\mathfrak{p}}_{(\sigma)}) \neq 0$ for all σ. Thus, $\frac{1}{z}$ is totally bounded on $\mathfrak{N}$. Apply Prop. 1 with $u = \frac{1}{z}$. Since z is quasi-integral, $N_u(\mathfrak{p})$ is finitary on $\mathfrak{N}$, and so;

$$|N(\tfrac{1}{z}(\mathfrak{p}))| \ll \left|\frac{1}{N(D_u(\mathfrak{p}))}\right| \ll \frac{1}{|N(D_x(\mathfrak{p}))|^{\frac{r}{h}-\delta}}, \quad \mathfrak{p} \in \mathfrak{N}.$$

Thus, $\exists$ an ∞-subsequence $\mathfrak{N}'$, and a fixed σ $\ni$

$$③ \quad \left|\frac{1}{z^{(\sigma)}(\mathfrak{p}^{(\sigma)})}\right| \ll \frac{1}{|N(D_x(\mathfrak{p}))|^{\frac{r}{lh}-\delta'}} \text{ for } \mathfrak{p} \in \mathfrak{N}'$$

From the total boundedness of x, x cannot be quasi-integral on $\mathfrak{N}$, or else it would take on only finitely many values. Thus, from the Decomposition theorem $N(D_x(\mathfrak{p}))$ is unbounded on $\mathfrak{N}'$, and $\bar{\mathfrak{p}}_{(\sigma)}$ is a pole of $z^{(\sigma)}$. If its order is j, $\varphi \in L(C)$ vanishing at $\bar{\mathfrak{p}}_{(\sigma)}$, then $\varphi^j z^{(\sigma)}$ is bounded on $(\mathfrak{N}')^{(\sigma)}$. Therefore, $|\varphi(\mathfrak{p}^{(\sigma)})| \ll \frac{1}{|N(D_x(\mathfrak{p}))|^{\frac{r}{jhl}-\delta'}}$ for $\mathfrak{p} \in \mathfrak{N}'$. Let $\delta' = \frac{r}{2jhl}$.

Q.E.D.

Theorem 5 - Proof of Siegel's theorem modulo statement A.

Assume with no loss that x is quasi-integral on an infinite set $\mathfrak{M}$ of K-rat. places. We apply prop. 2 in $L(C_n)$. For $\mathfrak{p}_n \in \mathfrak{M}_n$, we can regard x as quasi-integral on $\mathfrak{M}_n$ (part ① of statement A). For simplicity, replace $K^{(\sigma)}$ by K in prop. 2, and let x be the function z of that proposition. Φ, can play the role of x in prop. 2, after we have used part ③ of statement A to presume that Φ_1 is totally bounded on $\mathfrak{M}_n$.

<u>Remainder of translation of Prop. 2</u>

X has order hn^{2g} on C_n

Φ_1 has order less than or equal to $hg^3 n^{2g-2}$

The order of the pole of x at $\mathfrak{p}_n$ (replacement for $\mathfrak{p}_{(\sigma)}$ of <u>Prop. 2</u>) is $\leq h$, since C_n/C is unramified.

For φ, choose $\varphi = \Phi_1 - \Phi_1(\mathfrak{p}_n)$. Since $\mathfrak{p}_n$ is algebraic, so is $\Phi_1(\mathfrak{p}_n)$.

Let $\frac{\rho(\mathfrak{p}_n)}{\eta(\mathfrak{p}_n)}$ be a representation of $\Phi_1(\mathfrak{p}_n)$ where $(\rho, \eta) = 1$, $\rho, \eta \in \mathcal{O}_L$. <u>Prop. 2</u> implies

$$④ \quad \left|\Phi_1(\mathfrak{p}_n) - \frac{\rho}{\eta}\right| < \frac{M}{|N_{K/\mathbb{Q}}(\eta)|^{\frac{hn^{2g}}{(l)(h)(2hg^3n^{2g-2})}}} = \frac{M}{|N(\eta)|^{n^2/2lg^3}}$$

for all $\mathfrak{p}_n \in \mathfrak{M}_n$.

$\dfrac{\prod_\sigma (|\rho^{(\sigma)}| + |\eta^{(\sigma)}|)}{|\prod_\sigma \eta^{(\sigma)}|}$ is bounded because $\left|\frac{\rho^{(\sigma)}}{\eta^{(\sigma)}}\right|$ is bounded for $\forall\, \sigma$, on $\mathfrak{M}_n$.

But, $\frac{\rho}{\eta}$ satisfies an equation $\prod_\sigma (\eta^{(\sigma)} T - \rho^{(\sigma)}) = 0$ whose rat. integer coeffics. are $\leq 2^l \prod_\sigma (|\eta^\sigma| + |\rho^\sigma|)$.

Thus, $H\left(\frac{\rho}{\eta}\right) \leq \left(2^l \prod_\sigma \dfrac{(|\eta^\sigma| + |\rho^\sigma|)}{N\left(\frac{\rho}{\eta}\right)}\right) N\left(\frac{\rho}{\eta}\right) \ll N\left(\frac{\rho}{\eta}\right)$.

Therefore, from ④ we obtain

$$⑤ \quad \left|\Phi_1(\mathfrak{p}_n) - \frac{\rho}{\eta}\right| < \frac{M'}{\left|H\left(\frac{\rho}{\eta}\right)\right|^{un^2}} \quad \text{where } u = \frac{1}{2hlg^3}$$

for infinitely many distinct $\frac{\rho}{\eta} \in L$. For n large, $un^2 > 2$, and thus ⑤ contradicts <u>T.S.R.</u>

Q.E.D.

<u>Note</u> - Our proof needs all of <u>T.S.R.</u> since the degree of $\Phi_1(\mathfrak{p}_n)$ over K (as an algebraic no.) changes with n, <u>Thue's theorem</u> is not enough. Siegel's original proof was therefore much harder, and in fact gave motivation for the <u>Thue-Siegel-Roth Thm.</u>

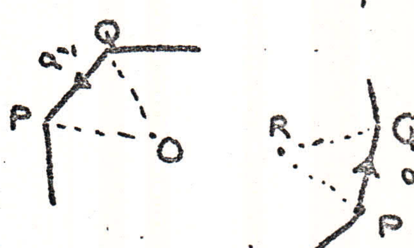
Section II

Expository Comments on Abelian Integrals, Abel's Theorem, Jacobi Inversion Problem

Description of the Normal Form of a Riemann Surface

Our algebraic functions give natural coverings of the R. sphere, so they may be triangulated in a completely combinatorial way. We take a triangulation $\Delta = \bigcup\limits^{n} S_i$ (S_i are triangles) of C, and produce a normal form illustrating the $2g$ - lin. indep. homology cycles in a manner convenient for integrations to be performed later.

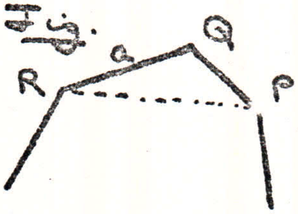
ⓐ Map S_1 onto Δ_1 (barycentrically, where Δ_1 is a Euclidean triangle). Select S_2 adjacent to S_1 and map it Δ_2 adjacent to Δ_1 along the corresponding edge. The coherent orientations of S_1 and S_2 assign an orientation to $|S_1| \cup |S_2|$ and so to the boundary of $\Delta_1 \cup \Delta_2$. Take S_3 having an edge in common with S_1 or S_2 and map it onto Δ_3 adjacent to the corresponding edge of Δ_1 or Δ_2 and make sure this is the only place where it hits Δ_1 or Δ_2. Continue until, when we are done; we obtain a plane polygon Π (which we assume regular) with boundary E having positive orientation. Π has $n+2$ sides, and $n+2$ is even.



a and a^{-1} are to be identified, and we proceed around the edges of Π to give Π the symbol $(a \cdots a^{-1} \cdots)$.

ⓑ If a, a^{-1} appear adjacently we may remove $a a^{-1}$ from the symbol (unless we only have C = sphere). We now form a topologically homeomorphic diagram where all the vertices are P (i.e. the same).

Fig.

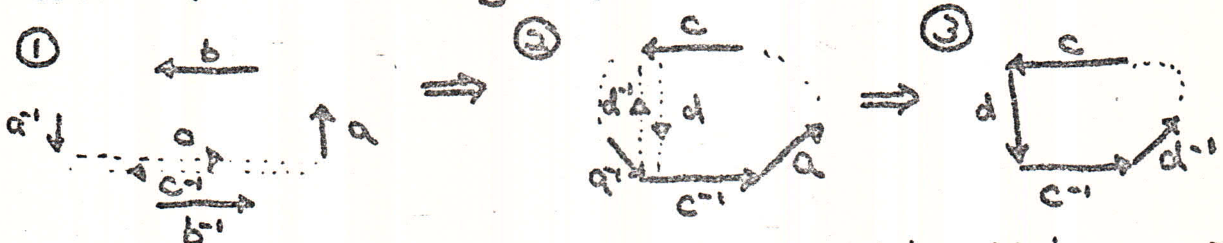


If we cut along $\overline{RP}$, and then join a to a^{-1}, we gain a vertex P, and lose a vertex Q. Continue until all vertices are P.

(c) a pair of edges ~~a~~ a and b are <u>linked</u> if they appear in the symbol in the order $\ldots a \ldots b \ldots a^{-1} \ldots b^{-1}$. If c and c^{-1} are linked with no other letters, then d between c and $c^{-1} \Rightarrow d^{-1}$ is also. This is easily seen to imply that P (the common vertex pt.) does not have a manifold nbd. Thus c and c^{-1} are linked with some other letter.

<u>Prop. 3</u> - Normal form of a compact R.S. is a polygon (topologically homeomorphic to the R.S.) with identifications given by the symbol (1) aa^{-1} (if a sphere), or (2) $a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1}$, and g is a topological invariant.

<u>Proof</u> -
For the 1st part, we move linked pairs next to each other, without destroying any linked pairs which are already adjacent.



Using a suitable triangulation it is easy to see that the $2g$ 1-cycles $a_1, b_1, \ldots, a_g, b_g$ form a homology basis for H_1. Since the R.S. is orientable, $H_2 = \mathbb{Z}$, and so $\chi = \sum_{i=0}^{2} (-1)^i \dim_{\mathbb{Z}} H_i = 2 - 2g =$ <u>Euler Characteristic</u> is a topological invariant. Q.E.D.

<u>Notation</u> - We denote an arbitrary differential by $d\omega$, and if $\bar{P}(p_1, p_2)$ is a given path between p_1 and p_2 on $\mathcal{C}$, we denote $\omega(p_1, p_2 : \bar{P})$ by $\int_{\bar{P}(p_1,p_2)} d\omega$ (if $\bar{P}(p_1, p_2)$ does not pass through a pole of $d\omega$). If we fix p_1, $\omega(p)$ is a multiple-valued function on the R.S., called an <u>abelian integral</u> (of <u>1st kind</u> if it has no singularities). Let the paths representing the sides of the normal form of $\mathcal{C}$ be designated, $A_1, B_1, \ldots, A_g, B_g$ and $b_k = -\int_{A_k} d\omega$, $a_k = \int_{B_k} d\omega$ (ω an integral of 1st kind)

are called the <u>periodicity moduli of ω</u>.

<u>Prop. 3a</u> - On a simply connected region of the R.S. (in particular the interior of π), an integral of 1st kind is a single-valued function $\omega^*(\wp)$. If $\bar{P}(\wp_0, \wp)$ intersects the canonical cuts A_k, B_k only finitely many times, then $\int_{\bar{P}(\wp_0,\wp)} d\omega = \omega^*(\wp) - \sum_{k=1}^{g} (m_k a_k + n_k b_k)$, $m_k, n_k \in \mathbb{Z}$ (because every curve is homotopic to a cycle).

<u>Prop. 4</u> - If ω is a non-zero integral of 1st kind, having moduli $a_k = \alpha_k + i\alpha_k'$, $b_k = \beta_k + i\beta_k'$, then $\sum_{k=1}^{g} (\alpha_k \beta_k' - \alpha_k' \beta_k) > 0$ and thus;

(a) not all the a_k are zero, (b) not all the b_k are zero

(c) a_k and b_k are not all real, nor all pure imaginary

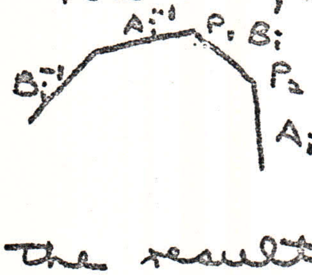
(d) If $\{\omega_i\}_1^g$ are a set of integrals of 1st kind, $-\int_{A_k} d\omega_i = b_{ik}$, $\int_{B_k} d\omega_i = a_{ik}$, then $\{\omega_i\}_1^g$ are linearly dependent iff $|a_{ik}| = 0$ or $|b_{ik}| = 0$.

<u>Prop. 5</u> - Let ω, ω' be two integrals of 1st kind. Then $\sum_1^g (a_i b_i' - b_i a_i') = 0$.

<u>Proof</u> -

Let $d\omega = df$ in the interior of π, and consider $\int_E f\, d\omega' = 0$, by <u>Cauchy's thm</u> since $f\, d\omega'$ has no poles.

However; $-\int_{A_i^{-1}} (f - a_i)\, d\omega' = \int_{A_i} f\, d\omega'$ because



$f(P_1) = f(P_2) + \int_{P_2}^{P_1} d\omega$ (<u>note</u> - P_1 and P_2 should be indentified, but we want to signify having gone around the loop B_i). We obtain the result by adding up all these relations. Q.E.D.

<u>Prop. 4</u> - follows in a similar manner using Green's theorem to compute $\iint_{\text{int.}\,\pi} d\omega\, d\bar{\omega}$ where $d\bar{\omega}$ means (in terms of the local parameter) $\overline{f(t)}\, d\bar{t}$.

<u>Notation</u> - vectors $(s_1, \cdots, s_g) \in \mathbb{C}^g$ will be denoted $\underset{\sim}{s}$, and the corresponding column vectors $\begin{pmatrix} s_1 \\ \vdots \\ s_g \end{pmatrix}$ by $\underset{\sim}{s}^{-}$.

Prop. 6 - Linearly indep. integrals of 1st kind, $\{\omega_i\}_1^g$ $\exists \ni$ the periods matrix is of form;

$$\bar{\Omega} = \begin{pmatrix} 4\pi i & & 0 & a_{11} & \cdots & a_{1g} \\ & 4\pi i & & \vdots & & \vdots \\ 0 & & \ddots\, 4\pi i & a_{g1} & \cdots & a_{gg} \end{pmatrix}$$

These integrals $\{\omega_i\}_1^g$ are unique for fixed cuts A_k, B_k and are called a normal system.

The submatrix $\bar{\Omega}_A = (a_{ij})$ of $\bar{\Omega}$ is symmetric and its real part is negative definite. This all follows from Prop. 4 and Prop. 5.

Prop. 7 - If $\mathfrak{A} = \prod_1^m \mathfrak{p}_\ell$, $\mathfrak{A}' = \prod_1^m \mathfrak{p}_\ell'$, then we define $\int_{\mathfrak{A}}^{\mathfrak{A}'} d\omega_i$ to be $\sum_{\ell=1}^m \int_{\mathfrak{p}_\ell}^{\mathfrak{p}_\ell'} d\omega_i$ for $i = 1, \cdots, g$, and the vectors of integrals $\left(\int_{\mathfrak{A}}^{\mathfrak{A}'} d\omega_1, \cdots, \int_{\mathfrak{A}}^{\mathfrak{A}'} d\omega_g\right) = \int_{\mathfrak{A}}^{\mathfrak{A}'} d\underset{\sim}{\omega}$ is unique mod Ω where Ω is the 2g-dim. $\mathbb{Z}$-module of periods.

Prop. 8 - (we do not prove - Abel's Theorem) - Two disjoint integral divisors $\mathfrak{A}$ and $\mathfrak{A}'$ are lin. equiv. iff $\int_{\mathfrak{A}}^{\mathfrak{A}'} d\underset{\sim}{\omega} \equiv 0 \bmod \Omega$ (where $d\underset{\sim}{\omega}$ will henceforth mean the vector of normalized abelian differentials of 1st kind)

Note - as usual we call integral divisors with g primes in them place sets.

Cor - Unless $\mathfrak{A}$ is special place set, there is no place set $\mathfrak{A}' \ni \int_{\mathfrak{A}^\circ}^{\mathfrak{A}'} d\underset{\sim}{\omega} \equiv \int_{\mathfrak{A}^\circ}^{\mathfrak{A}} d\underset{\sim}{\omega}$, because this $\Rightarrow \mathfrak{A} \sim \mathfrak{A}'$ so that $\dim \mathfrak{A} \geq 2$, and by R.R., $i(\mathfrak{A}) \neq 0$.

Prop. 9 - (addition Theorem) - Let $\mathfrak{A}^\circ$ be a place set, $\mathfrak{B}$ and $\mathfrak{B}^\circ$ arbitrary integral divisors of degree $m \geq 1$. Then $\exists$ a place set $\mathfrak{A}_\circ \ni \int_{\mathfrak{B}^\circ}^{\mathfrak{B}} d\underset{\sim}{\omega} \equiv \int_{\mathfrak{A}_\circ}^{\mathfrak{A}} d\underset{\sim}{\omega}$, and $\mathfrak{A}$ is unique unless it is special. Moreover, the places of $\mathfrak{A}$ depend algebraically on those of $\mathfrak{A}^\circ, \mathfrak{B}, \mathfrak{B}^\circ$ in such a way, that if $\mathfrak{A}^\circ, \mathfrak{B}, \mathfrak{B}^\circ$ are K-rat., then so is $\mathfrak{A}$.

Proof -

This is equiv. to $\int_{\mathfrak{B}^\circ\mathfrak{A}}^{\mathfrak{B}\mathfrak{A}^\circ} d\underset{\sim}{\omega} \equiv 0$, and the solutions of this are the $\mathfrak{A} \ni \mathfrak{B}\mathfrak{A}^\circ \sim \mathfrak{B}^\circ\mathfrak{A}$ by Abel - Neumann Theorem. By R.R. $\mathfrak{A}$ always exists. Q.E.D.

Def - Let $\mathfrak{A}^0$ be a fixed place set of $\mathcal{C}$. abelian coordinates of a place set $\mathfrak{A}$ are $\underline{s} = \int_{\mathfrak{A}^0}^{\mathfrak{A}} d\underline{w}$. From Prop. 9, if $\mathfrak{A}$ and $\mathfrak{B}$ are place sets, $\exists$ a place set C $\ni \int_{\mathfrak{A}_0}^{\mathfrak{A}} d\underline{w} + \int_{\mathfrak{A}^0}^{\mathfrak{B}} d\underline{w} \equiv \int_{\mathfrak{A}^0}^{C} d\underline{w}$ (from $\int_{\mathfrak{A}^0}^{C} \equiv \int_{(\mathfrak{A}^0)^2}^{\mathfrak{A}\mathfrak{B}}$ has a solution C.). From Abel-Neumann, the class of C is unique. We call C the sum of $\mathfrak{A}$ and $\mathfrak{B}$: $\mathfrak{A} + \mathfrak{B} = C$ iff $\left(\frac{\mathfrak{A}}{\mathfrak{A}^0}\right)\left(\frac{\mathfrak{B}}{\mathfrak{A}^0}\right) \sim \frac{C}{\mathfrak{A}^0}$.

Prop. 10 - (we do not prove - Jacobi Inversion Theorem) The map $\mathfrak{A} \to \int_{\mathfrak{A}^0}^{\mathfrak{A}} d\underline{w}$ induces a homomorphism from $\mathcal{D}_0 \to T_g$ (divisor classes of degree 0 into complex g-space mod periods, where the multiplication on $\mathcal{D}_0$ is the obvious one, the addition on T_g that described above). Jacobi proved this is onto.

Prop. 11 - The set of points on T_g corresponding to non-special divisors is an algebraic set of dim $< g$.

Proof -

We are asking; if $\mathfrak{A} = \prod^{g} \mathfrak{p}_i$, when is it possible that $\dim W\mathfrak{A}^{-1} > 0$. Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_g$ be divisors of lin. indep. differentials of the first kind. Then $\frac{\mathfrak{A}_i}{\mathfrak{A}_1} = (V_i)$ for some function V_i.

Put $V = \sum_1^g c_i V_i$. We note that the divisors $\mathfrak{A}$ which are of form N_V = numerator of divisor of $V = (\mathfrak{A})$(something) (and V has only $\mathfrak{A}_1$ in its denominator) are those for which $V(\mathfrak{p}_k) = 0$, $k = 1, \ldots, g$. Since $V_1, \ldots, V_g$ are lin. indep. functions, the set of $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ which satisfy $\det|V_i(\mathfrak{p}_j)| \neq 0$ are open and dense.

Q.E.D.

For the proofs of Props. 8 and 10 (and anything else that is not clear), see Chap. 10 of Springer's book on Riemann Surfaces. Once you get around the confusion due to fact that he proves the 'strong' Riemann Roch Theorem, the rest of the chapter 10 can be read easily.

Riemann Inversion

Introduction -

By Jacobi Inversion, $\int_{\mathfrak{a}_0}^{\mathfrak{a}} d\underset{\sim}{\omega} = \underset{\sim}{s}$ defines $\mathfrak{a}$ as a function of $\underset{\sim}{s}$. The function $\mathfrak{a}(\underset{\sim}{s}) = \mathfrak{a}(\underset{\sim}{s} + \underset{\sim}{c})$ if $\underset{\sim}{c}^T$ is a column of the periods matrix, and this function is single-valued when $\mathfrak{a}$ is not special. This is touchy to have single-valuedness of a function at a place on T_g depend on the value of the function. The Riemann Inversion Problem is designed to correct this situation.

Let $n(\underset{\sim}{z})$ be a meromorphic function on $\mathbb{C}^g$. The periods of $n(\underset{\sim}{z})$ form a closed sub-group ($\mathbb{Z}$-module)

Def. - If G is the group of periods of $n(\underset{\sim}{z})$, then $n(\underset{\sim}{z})$ said to be degenerate if $d > 0$ where d is the dimension of the maximal $\mathbb{R}$-module contained in G.

Lemma 7 - A meromorphic function $n(\underset{\sim}{z})$ is degenerate iff $\exists$ a non-sing. matrix $M : \underset{\sim}{z} \to \underset{\sim}{w}$ (i.e. $M\underset{\sim}{z}^T = \underset{\sim}{w}^T$) $\ni n(\underset{\sim}{z}) = \zeta(\underset{\sim}{w})$ is independent of one of the variables $w_1, \cdots, w_g$.

Proof -

If $d > 0$, $\exists$ non-zero period $\sigma \in G(n) \ni \lambda\sigma \in G(n)$ for all $\lambda \in \mathbb{R}$. Let M_1 be a non-sing. matrix of which σ is the first column, and put $M = M_1^{-1}$.

Then $M\sigma^T = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$ is a period of $n((M, \underset{\sim}{w}^T)^T)$.

Thus, $\zeta(w_1+\lambda, w_2, \cdots, w_g) \equiv \zeta(w_1, \cdots, w_g)$ for all $\lambda \in \mathbb{R}$, so $\zeta(\underset{\sim}{w})$ does not depend on w_1. Q.E.D.

Lemma 8 - A non-degenerate meromorphic function on $\mathbb{C}^g$ cannot have more than $2g$ indep. periods over $\mathbb{Z}$

Proof -

From Lemma 7, the group $G(n)$ of a non-deg. meromorphic function is discrete. Any $2g+1$ periods $\sigma_1, \cdots, \sigma_{2g+1}$ are lin. dependent over the reals. It is now easy to show that some linear combination over $\mathbb{Z}$ of $\sigma_1, \cdots, \sigma_{2g+1}$ is 'very' close to the origin. This contradicts discreteness. Q.E.D.

Theta Functions

Theorem 6 $\Rightarrow \exists$ no abelian entire functions.
Let $\hat{a}_1, \dots, \hat{a}_g$ be the transposed vectors of the g columns of Ω to the right, forming the matrix

$$\Omega_{\hat{A}} = \begin{pmatrix} \hat{a}_{11} & \cdots & \hat{a}_{1g} \\ \vdots & & \vdots \\ \hat{a}_{g1} & \cdots & \hat{a}_{gg} \end{pmatrix} = (\hat{a}_1^T \cdots \hat{a}_g^T)$$

We will attempt to follow the simplest procedure for obtaining entire functions (those that work will be called theta functions) whose quotients will be abelian functions having for periods the columns of the matrix Ω.

① To ensure that $h(\underline{z}) = \dfrac{\Phi_1(\underline{z})}{\Phi_2(\underline{z})}$ has period πi in each variable separately, we assume $\Phi_i(\underline{z}) = \sum B_{\underline{n}}^{(i)} e^{2\underline{n}\cdot\underline{z}}$.

② We require that there $\exists$ g functions $\varphi_i(\underline{z})$, $i = 1, \dots, g$

$$\ni \ \varphi_j(\underline{z}) = \frac{\Phi_1(\underline{z} + \hat{\underline{a}}_j)}{\Phi_1(\underline{z})} = \frac{\Phi_2(\underline{z} + \hat{\underline{a}}_j)}{\Phi_2(\underline{z})}$$

③ From Thm 6, we know we can't select $\varphi_j(\underline{z})$ to be constant, and since they have period πi in $\forall$ variable separately, the simplest choice that could possibly work is

$\varphi_j(\underline{z}) = C_j e^{2\underline{k}_j \cdot \underline{z}}$ where $\underline{k}_j$ is an integral vector.

④ We work with Φ_1 alone (calling it Φ), in order to see if Φ will be satisfactory for suitable $\underline{k}_j$, $j = 1, \dots, g$.

Note - If K is the matrix with columns $\underline{k}_i^T$, then $\det K = m \neq 0$.

argument -

If $\det K = 0$, then $\exists$ integral vector $\underline{n} \ni K \cdot \underline{n}^T = 0$.

Thus, $\Phi(\underline{z} + \sum_{i=1}^{g} n_i \hat{\underline{a}}_i) = C_1^{n_1} \cdots C_g^{n_g} e^{2(n_1 \underline{k}_1 + \cdots + n_g \underline{k}_g)} \Phi(\underline{z})$

$= C_1^{n_1} \cdots C_g^{n_g} \Phi(\underline{z})$. This contradicts Thm. 6 since the columns of $\Omega_{\hat{A}}$ are lin. indep. over $\mathbb{Z}$.

⑤ Consider the following change of variables; If $m = \det K$, find a matrix $A \ni K\hat{A} = mA$, and variables $\underline{u} \ni K\underline{z}^T = m\underline{u}^T$. Define $\Theta(\underline{u})$ by $\Phi(\underline{z}) = \Theta(\underline{u})$. We easily verify the following:

(a) $\Theta(\underline{u} + \pi i \underline{e}_j) = \Theta(\underline{u})$ ($\underline{e}_j$ the j-th unit vector)

(b) $\Theta(\underline{u} + \underline{a}_j) = c_j e^{2m u_j}\,\Theta(\underline{u})$, where $\underline{a}_j^T$ is the j-th column of A.

Without loss we assume m positive (by changing the signs of the entries in $\underline{u}$ and A if necessary). Note also that the translation $\underline{u} \to \underline{u} + \tau$ does not effect the periodicity of Θ (the c_j are replaced by $c_j e^{2m\tau_j}$)

(6) Choose $\tau \ni c_j = e^{m a_{jj}}$, $j = 1, \cdots, g$.

We have therefore the properties

(a') $\Theta(\underline{u} + \pi i \underline{e}_j) = \Theta(\underline{u})$

(b') $\Theta(\underline{u} + \underline{a}_j) = e^{(2u_j + a_{jj})m}\,\Theta(\underline{u})$

(c') $\Theta(\underline{u}) = \sum_{-\infty}^{\infty} A_{\underline{n}}\, e^{2\underline{n}\cdot\underline{u}}$

and every such function is called a <u>theta function of order m</u> (with pseudo-periods $\pi i \underline{e}_j$, and $\underline{a}_1, \cdots, \underline{a}_g$ – but we suppress this).

<u>Additional Properties of Theta Functions</u>

<u>Property 1</u> – $a_{j\ell} = a_{\ell j}$ (i.e. Ω_A is symmetric)

<u>argument</u> –

$\Theta((\underline{u} + \underline{a}_j) + \underline{a}_\ell) = e^{m\{2u_\ell + 2u_j + 2a_{j\ell} + a_{\ell\ell} + a_{jj}\}}\,\Theta(\underline{u}) = \Theta(\underline{u} + \underline{a}_\ell + \underline{a}_j$

<u>Property 2</u> – Every theta function of order m is formally a linear combination of the m^g series

(I) $\Theta(\underline{u}) = \sum_{\underline{n}=-\infty}^{\infty} e^{2(\underline{r} + m\underline{n})\cdot\underline{u} + (2\underline{r} + m\underline{n})A\underline{n}^T}$, $0 \le r_j \le m-1$, $j = 1, \cdots, g$

<u>argument</u> –

Let ℓ be an integer. $\Theta(\underline{u} + \ell\underline{a}_j) = \Theta(\underline{u} + (\ell-1)\underline{a}_j + \underline{a}_j)$

$= e^{m(2u_j + (2\ell-1)a_{jj})}\,\Theta(\underline{u} + (\ell-1)\underline{a}_j) = \cdots = e^{m(2\ell u_j + \ell^2 a_{jj})}\,\Theta(\underline{u})$

In an inductive manner we conclude that

$\Theta(\underline{u} + \ell_1\underline{a}_1 + \cdots + \ell_g\underline{a}_g) = \Theta(\underline{u} + \underline{\ell}A) =$

$e^{m\{2\ell_g(u_g + \ell_1 a_{1g} + \cdots + \ell_{g-1}a_{g-1,g}) + \ell_g^2 a_{gg}\}}\cdot\Theta(\underline{u} + \ell_1\underline{a}_1 + \cdots + \ell_{g-1}\underline{a}_{g-1})$

$= \cdots = e^{m(2\underline{\ell}\cdot\underline{u} + \underline{\ell}A\underline{\ell}^T)}\cdot\Theta(\underline{u})$.

We express $\Theta(\underline{u}) = e^{-m(2\underline{\ell}\cdot\underline{u} + \underline{\ell}A\underline{\ell}^T)}\,\Theta(\underline{u} + \underline{\ell}A)$.

More trivially we may also express

$\Theta(\underline{u}) = \sum A_n e^{2\underline{n}\cdot\underline{u}} = \sum A_{\underline{n} - m\underline{\ell}}\, e^{2(\underline{n} - m\underline{\ell})\cdot\underline{u}}$.

If we carefully equate the Fourier series for these two expressions of $\Theta(\underline{u})$, we obtain

$A_{\underline{n}+m\underline{\ell}} = e^{(2\underline{n}+m\underline{\ell})A\underline{\ell}^T} A_{\underline{n}}$. This clearly shows that the coeffics. $A_{\underline{n}}$ depend only on the residue class mod m of the components of $\underline{n}$. Q.E.D.

We are mostly interested in the case where Ω is the periods matrix obtained from normalized abelian integrals of 1st kind, of a curve C. In this case our theta functions will converge, and the ratio of two of them of the same order will represent an abelian function. More generally,

__Theorem 7__ - Let $A = (a_{ij})$ be a $g \times g$ symmetric complex matrix whose real part is negative definite (__Prop. 6__). Then the series (I) converges absolutely and uniformly, thus representing an entire function in $\mathbb{C}^g$.

__Proof__ -

If $\underline{u}$ is restricted to the region $|u_i| \leq M$, $i = 1, \cdots, g$, then

$|e^{2(\underline{r}+m\underline{\ell})\cdot\underline{u} + (2\underline{r}+m\underline{\ell})A\underline{\ell}^T}| \leq e^{2mgM} e^{2m\underline{\ell}\cdot\mathrm{Re}\,\underline{u} + (2\underline{r}+m\underline{\ell})\mathrm{Re}A\underline{\ell}^T}$

$\mathrm{Re}\,A$ is negative definite, so $\exists\, \mu > 0 \ni \underline{x}\,\mathrm{Re}A\,\underline{x}^T \leq -\mu(\underline{x}\cdot\underline{x})$. The rest follows by easy computation. Q.E.D.

__Riemann Inversion Problem__

For our purposes, we may assume $m = 1$, so that up to a constant factor $\boxed{\Theta(\underline{u}) = \sum_{\underline{n}=-\infty}^{\infty} e^{2\underline{n}\cdot\underline{u} + \underline{n}A\underline{n}^T}}$ is the only theta function we deal with.

__Theorem 8__ (__Riemann Inversion__) - Let p_0 be an arbitrary place of C. Then $\exists$ a place set $\mathfrak{A}_0$ with the property; if $\underline{s}$ is $\ni \Theta(\underline{w}(p, p_0) - \underline{s})$ is not identically zero as a function of $p \in C$, then $\exists$ a __unique place set__ $\mathfrak{A} \ni \int_{\mathfrak{A}_0}^{\mathfrak{A}} d\underline{w} = \underline{s}$.

__Notation__ - $\underline{w}(p) = \underline{w}(p, p_0) = (w_1(p, p_0), \cdots, w_g(p, p_0))$ where $\{w_i\}_1^g$ are our canonical ~~...~~ set of abelian integrals of 1st kind (__Prop. 6__). Let $T(p) = \Theta(\underline{w}(p) - \underline{s})$. For some values of $\underline{s}$, $T(p)$ may vanish identically but it cannot do so for all values of $\underset{\sim}{s}$, since $\Theta(\underset{\sim}{u}) \not\equiv 0$. Notice that $T(\mathfrak{p})$ is a many valued function of $\mathfrak{p}$. When $\mathfrak{p}$ traverses one of the loops A_k in the positive sense, $\underset{\sim}{w}(\mathfrak{p})$ increases by $-\pi i\, \underset{\sim}{e}_k$, so $T(\mathfrak{p})$ returns to its original value. But when $\mathfrak{p}$ traverses a loop B_k, $\underset{\sim}{w}(\mathfrak{p})$ increases by $\underset{\sim}{a}_k$, and the new value of $T(\mathfrak{p})$ is the original multiplied by $e^{2(w_k(\mathfrak{p})-s_k)+a_{kk}}$. In any case, we may speak meaningfully of the zeros of $T(\mathfrak{p})$ for fixed $\underset{\sim}{s}$.

At various times we will be computing the vectors $\underset{\sim}{s}(\mathfrak{A})$ with respect to different base place sets. For instance in Theorem 8, $\underset{\sim}{s}(\mathfrak{A}) = \underset{\sim}{s}_{\mathfrak{A}_0}(\mathfrak{A}) = \int_{\mathfrak{A}_0}^{\mathfrak{A}} d\underset{\sim}{w}$ = abelian coordinate vector of $\mathfrak{A}$ (with respect to $\mathfrak{A}_0$). We will suppress the parenthetical comment when it is clear from the argument which base place set we refer to. Otherwise we will use the cumbersome, but necessary, subscript notation.

Lemma 9 . $T(\mathfrak{p})$ has exactly g zeros.

Proof -

\# of zeros of $T(\mathfrak{p}) = N = \frac{1}{2\pi i}\int_E d(\log T(\mathfrak{p}))$.

$\int_{B_k} d(\log T(\mathfrak{p})) = -\int_{B_k^{-1}} d(\log T(\mathfrak{p}))$, and

$-\int_{A_k^{-1}} d(\log T(\mathfrak{p})) = \int_{A_k} d(\log T(\mathfrak{p})) + d(2w_k(\mathfrak{p}) - 2s_k + a_{kk})$.

Therefore, $N = \frac{1}{2\pi i}\sum_1^g\left(-\int_{A_k} 2\,d w_k(\mathfrak{p})\right) = g$. Q.E.D.

Proof of Theorem 8 -

Let $\mathfrak{A}$ be the divisor of zeros of $\Theta(\underset{\sim}{w}(\mathfrak{p}) - \underset{\sim}{s})$. By the *residue theorem* $\frac{1}{2\pi i}\int_E \underset{\sim}{w}(\mathfrak{p})\, d(\log T(\mathfrak{p})) = \sum_1^g \underset{\sim}{w}(\mathfrak{p}_i)$ $\left(= \int_{\mathfrak{p}^0}^{\mathfrak{A}} d\underset{\sim}{w}\right.$, where $\left.\mathfrak{A} = \prod_1^g \mathfrak{p}_i\right)$. This is really a set of g equations. By integration by parts

$$\frac{1}{2\pi i}\int_E \underset{\sim}{w}\, d\log T = -\frac{1}{2\pi i}\int_E \log T\, d\underset{\sim}{w} = \frac{1}{2\pi i}\sum_1^g\left\{-\int_{A_k}(2w_k + a_{kk})\,d\underset{\sim}{w} + 2s_k\cdot \pi i\, \underset{\sim}{e}_k\right\}$$

(as in *Lemma 9*).

Thus, $\frac{1}{2\pi i}\int_E \underset{\sim}{w}\, d(\log T) = \underset{\sim}{\lambda} + \underset{\sim}{s}$ where

$\underset{\sim}{\lambda} = -\frac{1}{2\pi i}\sum_{k=1}^g \int_{A_k}(2w_k + a_{kk})\,d\underset{\sim}{w}$ is independent of $\underset{\sim}{s}$.

From *Jacobi Inversion*, $\exists\ \mathfrak{A}_0 = \mathfrak{p}_1^0 \cdots \mathfrak{p}_g^0 \ni$ $\underset{\sim}{s} \equiv \int_{\mathfrak{p}_0^g}^{\mathfrak{A}_0} d\underset{\sim}{\omega}$. Combining these results, we see that the place set $\mathfrak{A}$ of the conclusion of *Theorem 8* exists, and is the divisor of zeros of $\Theta(\underset{\sim}{\omega}(\mathfrak{p}) - \underset{\sim}{s})$. For uniqueness, assume $\int_{\mathfrak{A}_0}^{\mathfrak{A}} d\underset{\sim}{\omega} \equiv \int_{\mathfrak{A}_0}^{\mathfrak{A}'} d\underset{\sim}{\omega} \equiv \underset{\sim}{s}$. Then $\Theta(\underset{\sim}{\omega}(\mathfrak{p}) - \int_{\mathfrak{A}_0}^{\mathfrak{A}} d\underset{\sim}{\omega})$ vanishes for all places of $\mathfrak{A}$ and $\mathfrak{A}'$, because this differs from $\Theta(\underset{\sim}{\omega}(\mathfrak{p}) - \int_{\mathfrak{A}_0}^{\mathfrak{A}'} d\underset{\sim}{\omega})$ only be the non-zero factors that occur when the argument is changed by a period. This contradicts *lemma 9* unless $\mathfrak{A} = \mathfrak{A}'$. Q.E.D.

We will start section III with an abstract description of the n-division function field of *Statement A* and then we will one by one ascertain the properties stipulated in *Statement A*. *Theorem 8* will be used later also, to show that the abstractly defined branches of C_n lying over a given branch of C, are well-defined. *Theorem 9* (below) will then imply that there are exactly n^{2g} branches of C_n above each branch of C.

Theorem 9 - Let $\underset{\sim}{b}$ be an arbitrary vector, and $\mathfrak{A}'$ an arbitrary place set of C. Then;

ⓐ For $\mathfrak{p}$ a place of C, $\exists\ n^{2g}$ vectors $\underset{\sim}{\sigma}$, distinct mod Ω $\ni$ $\underset{\sim}{s}_{\mathfrak{A}'}(\mathfrak{p}^g) = \int_{\mathfrak{A}'}^{\mathfrak{p}^g} d\underset{\sim}{\omega} \equiv n\underset{\sim}{\sigma} + \underset{\sim}{b}$ mod Ω.

ⓑ If n is sufficiently large, and we exclude finitely many places $\mathfrak{p}$ of C from consideration, for each $\underset{\sim}{\sigma}$ of part ⓐ $\exists$ a *unique place set* $Q \ni \underset{\sim}{\sigma} \equiv \underset{\sim}{s}_{\mathfrak{A}'}(Q)$.

Proof -

ⓐ The solutions are $\underset{\sim}{\sigma} \equiv \frac{1}{n}(\underset{\sim}{s} - \underset{\sim}{b}) + \frac{1}{n}\sum_{\ell=1}^{g}(g_\ell \pi i \underset{\sim}{e}_\ell + h_\ell \underset{\sim}{a}_\ell)$
$0 \le g_\ell < n$, $0 \le h_\ell < n$, and $g_\ell, h_\ell \in \mathbb{Z}$.

ⓑ Let $\underset{\sim}{\sigma}(\mathfrak{p})$ be one of these solutions, and suppose that the inversion problem is not uniquely solvable. From *Theorem 8*, $\Theta(q, \mathfrak{p}) = \Theta(\underset{\sim}{\omega}(q) - \underset{\sim}{\sigma}(\mathfrak{p}))$ vanishes identically as a function of q. Suppose also that this is true for infinitely many $\mathfrak{p}$, ~~and~~ Then these places have a limit point on C, and the entire function $\Theta(q, \mathfrak{p}) \equiv 0$ (in both variables q and $\mathfrak{p}$).

When p traverses a closed path on C, $\underset{\sim}{S}(p)$ changes by the n-th part of some period. We have kept n fixed so far, but if the identical vanishing of $\Theta(\underset{\sim}{q}, p)$ were to occur for arbitrarily large n, then $\Theta(\underset{\sim}{w}(\underset{\sim}{q}) - \underset{\sim}{S}(p) + \frac{\text{periods}}{n}) \equiv 0$. This implies that $\Theta(\underset{\sim}{u})$ vanishes on a dense subset, and this is impossible.
Q.E.D.

Section IV - Proof of Statement A

Let $\mathfrak{A}'$ be a fixed K-rat. place set. We will use $\mathfrak{A}'$ as our base place set for computation of the abelian coordinates of place sets, for most of this section. Let n_0 be an integer satisfying ① $(n_0, g) =$ ② $n_0 > 1$ is sufficiently large so that the conclusion of Theorem 9 holds. Let the field L be chosen $\ni$ the Mordell-Weil Weak finiteness theorem holds with respect to n_0 and L (i.e. $\mathcal{D}_0 / \mathcal{D}_0^{n_0}$ is finite, wher $\mathcal{D}_0$ is the multiplicative group of L-rat. divisor classes of degree 0). For instance we could pick L so that the n_0 division place sets are all L-rat and also so that L contains the n_0-th roots of 1.

Note - The n_0 division place sets of $K(C)$ are the place sets $Q \ni \underset{\sim}{S}_{\mathfrak{A}'}(Q) = \frac{\text{some period}}{n_0}$.

The infinite set of integers n for which $\exists$ an n-div. function field having the propertie of statement A will be the positive integer powe of n_0. For simplicity assume n is always such an integer, but we really use this only in Claim III (bel

Description of the n-Division Function Field

Let $\underset{\sim}{b}$ be a vector, which we will choose explicitly in a little while. Then from Theorem for $\forall$ place p of $K(C)$ $\exists$ exactly n^{2g} classes of place sets $\bar{Q}_1, \cdots, \bar{Q}_{n^{2g}}$ (where $^{-}$ indicates that Q_1 may not be the only place set in $\bar{Q}_1$)

such that

(*) $\underset{\sim}{S}_{\mathfrak{A}'}(\mathfrak{p}^g) \equiv n\,\underset{\sim}{S}_{\mathfrak{A}'}(Q_i) + \underset{\sim}{b} \mod \Omega$, $i = 1, \cdots, n^{2g}$.

If $\phi \in L(C)$, we consider the field F_ϕ of rational symmetric functions (with coeffics. in L) in the variables $\phi(q_1), \cdots, \phi(q_g)$ where $Q = q_1 \cdots q_g$ runs over the place sets that result from (*) for all $\mathfrak{p}$, places of $L(C)$. The field obtained by compositing all the fields F_ϕ, $\phi \in L(C)$ will be our <u>n-division function field</u> $L(C_n)$. $L(C_n)$ is obviously a field, but we claim in addition;

<u>Claim I</u> - $L(C_n)$ contains $L(C)$.

<u>Claim II</u> - The places of $L(C_n)$ lying over a place $\mathfrak{p}$ of $L(C)$ are in one-one correspondence with the <u>classes of place sets</u> $\bar{Q}_1, \cdots, \bar{Q}_{n^{2g}}$ given by condition (*).

<u>Claim III</u> - If $\mathfrak{M}$ is an infinite set of L-rat. places of $L(C)$, then $\underset{\sim}{b}$ can be chosen so that $\exists$ an infinite sequence $\mathfrak{M}_n$ of L-rat. places of $L(C_n)$, where $\forall$ place of $\mathfrak{M}_n$ lies over a place of $\mathfrak{M}$.

<u>Note</u> - <u>Part (1) of statement A</u> (pg. 14) is a little misleading for it seems to say we can uniformly construct our n-division function field without knowing what set $\mathfrak{M}$ might be. However, the proof of Siegel's theorem is of such a nature that we are able to assume $\mathfrak{M}$ is given a priori to the construction of our n-div. function field. Thus, <u>Claim III</u> suffices for the proof we give. anyway, our n-div. funct. field is seen to depend both on $\mathfrak{A}'$ (our base place set) and $\mathfrak{M}$.

In a little while we will write down <u>Claim IV</u> (Part (2) of statement A), and we will prove in order <u>Claim III</u>, then <u>Claim IV</u>. We leave to the <u>appendix</u> the proofs of <u>Claim's I and II</u>, noting that while these are part of the <u>very</u> classical literature, and possibly quite believable, they are nevertheless fairly by quoting fairly hard theorems). So assuming Claims I and II.

Proof of Claim III -

From M.W.W.F.T., for every L-rat. place $\mathfrak{p}$ of $\mathcal{C}$, $\exists$ an L-rat. place set $Q \ni \frac{\mathfrak{p}^g}{\mathfrak{A}'} \sim \left(\frac{Q_1}{\mathfrak{A}'}\right)^{n_0}\left(\frac{B_1}{\mathfrak{A}'}\right)$ where B_1 is L-rat. and as $\mathfrak{p}$ runs over all places of $\mathcal{C}$, $\frac{B_1}{\mathfrak{A}'}$ takes on only finitely many values in $\mathfrak{O}_L^\circ$. For $\forall$ such Q, $\exists$ L-rat. place set $Q_2 \ni \frac{Q_1}{\mathfrak{A}'} \sim \left(\frac{Q_2}{\mathfrak{A}'}\right)^{n_0}\left(\frac{B_2}{\mathfrak{A}'}\right)$, and $\frac{B_2}{\mathfrak{A}'}$ runs over the finite set above.

Continuing, for $n = n_0^r$, and every L-rat. place set $\mathfrak{p}$ of $\mathcal{C}$, $\exists$ an L-rat. place set $Q \ni \frac{\mathfrak{p}^g}{\mathfrak{A}'} \sim \left(\frac{Q}{\mathfrak{A}'}\right)^n\left(\frac{B}{\mathfrak{A}'}\right)$ where $\frac{B}{\mathfrak{A}'}$ as a function of $\mathfrak{p}$ takes on only finitely many values in $\mathfrak{O}_L^\circ$. ~~For ∀ such Q, ∃~~ Thus, as $\mathfrak{p}$ ranges over $\mathfrak{M}$, $\exists$ a fixed B', and an infinite subsequence $\mathfrak{M}' \subset \mathfrak{M} \ni \frac{\mathfrak{p}^g}{\mathfrak{A}'} \sim \left(\frac{Q(\mathfrak{p})}{\mathfrak{A}'}\right)^n\left(\frac{B'}{\mathfrak{A}'}\right)$ for all $\mathfrak{p} \in \mathfrak{M}'$.

Thus, interpreted in abelian coordinate vector language, $\underset{\sim}{S}_{\mathfrak{A}'}(\mathfrak{p}^g) \equiv n\,\underset{\sim}{S}_{\mathfrak{A}'}(Q(\mathfrak{p})) + \underset{\sim}{S}_{\mathfrak{A}'}(B')$. This is the condition (*) of the description of the n-div. function field, so we are done if we put $k = \underset{\sim}{S}_{\mathfrak{A}'}(B')$.

Q.E.D.

We will prove the following theorem in the appendix (where it will be used to prove Claims I, II). You will readily see that Theorem 10 gives us a (useful) description of the n-div. F.F. elements in terms of the Theta Functions. Notice also its resemblance to the Weil Decomposition Theorem.

Theorem 10 - Let $\phi \in L(\mathcal{C})$ with zeros $\{r_i\}_1^m$ and poles $\{t_i\}_1^m$. Then $\exists\ c \in \mathbb{C}$ and paths connecting $\mathfrak{p}_0$ (a fixed place) to $\{r_i\}$ and $\{t_i\} \ni$ for all place set $P = \prod_1^g \mathfrak{p}_i$,

$$\prod_1^g \phi(\mathfrak{p}_i) = c\ \frac{\prod_{j=1}^m \Theta\left(\underset{\sim}{S}_{\mathfrak{A}'}(P) - \int_{\mathfrak{p}_0}^{r_j} d\underset{\sim}{\omega}\right)}{\prod \Theta\left(\underset{\sim}{S}_{\mathfrak{A}'}(P) - \int_{\mathfrak{p}_0}^{t_j} d\underset{\sim}{\omega}\right)}.$$

<u>Claim IV</u> - For suitable constants $T_1, T_2, a, b, c, d \in L$, the functions $\bar{\Phi}_k(\mathfrak{p}_n) = \prod_{i=1}^{g}\left(T_k + \frac{a}{bx(q_i)+cy(q_i)+d}\right)$

$= T_k^g + S_1(\mathfrak{p}_n)T_k^{g-1} + \cdots + S_g(\mathfrak{p}_n)$, $k = 1, 2$, generate $L(\mathcal{C}_n)$. Here $\mathfrak{p}_n$ is generically used for the place sitting over $\mathfrak{p}$, a place of $\mathcal{C}$, given by the place set $Q = \prod_{1}^{g} q_i$.

<u>Claim IV(a)</u> - $\bar{\Phi}_1$ and $\bar{\Phi}_2$ are connected by a polynomial equation $F(\bar{\Phi}_1, \bar{\Phi}_2) = 0$ with coeffics. in L, and of degree at most $hg^3 n^{2g-2}$ in each argument.

<u>Proof of Claim IV</u> -

There is a standard argument for showing that two functions ϕ and ψ of a function field generate the function field. You show that for some $\alpha \in \mathbb{C}$, ϕ assumes the value α (always with multiplicity one) at the places $q_1, \cdots, q_r$ and that the complex nos. $\psi(q_i)$, $i = 1, \cdots, r$ are all distinct. This is a nice exercise.

Fix T_1, $a_0 = a$, $b_0 = b$, $c_0 = c$, $d_0 = d$, so that $a_0 b_0 c_0 d_0 \neq 0$. Let α be a value assumed (always with multiplicity one) by $\bar{\Phi}_1$, at the places $\mathfrak{p}_n^1, \cdots, \mathfrak{p}_n^\lambda$. It is reasonably obvious (but somewhat tedious to write out), that we may perturb a_0, b_0, c_0, d_0 slightly to a, b, c, d (thus slightly shifting the places $\mathfrak{p}_n^1, \cdots, \mathfrak{p}_n^\lambda$ for which $\bar{\Phi}_1(\mathfrak{p}_n^i) = \alpha$) so that the quantities (as a set of <u>ordered</u> values) $\langle S_1(\mathfrak{p}_n^i), \cdots, S_g(\mathfrak{p}_n^i)\rangle$ are distinct for $i = 1, \cdots, \lambda$. Then T_2 can be chosen so that $\bar{\Phi}_2$ assumes distinct values at $\mathfrak{p}_n^1, \cdots, \mathfrak{p}_n^\lambda$.

Q.E.D.

<u>Proof of Claim IV(a)</u> -

From the form of $\bar{\Phi}_1, \bar{\Phi}_2$, and the fact that there $\exists$ an infinite sequence M_n of L-rat. place sets $\mathfrak{p}_n$, $\bar{\Phi}_1$ and $\bar{\Phi}_2$ assume a lot of values in L. If $F_1(\bar{\Phi}_1, \bar{\Phi}_2) = 0$ is any polynomial relation, then evaluating $\bar{\Phi}_1$ and $\bar{\Phi}_2$ at L-rat. places $\mathfrak{p}_n$, we get a bunch of linear equats. in the coeffics. of F_1, which may be solved to show that the coeffics. of F_1 may be taken in L.

If we show that $\Phi = \Phi_k$ takes on zero $\leq hg^3 n^{2g-2}$ times, then $[K(C_n) : L(\Phi_k)] \leq hg^3 n^{2g-2}$. The number of times zero is assumed on C by $(N_{L(C_n)/L(C)} \Phi)(p) = \prod_{p_n | p} \Phi(p_n) =$ # of times zero is assumed by Φ on C_n.

Note - $L(C_n)/L(C)$ is galois (in fact, abelian).

$$\Phi(p_n) = \prod_1^g \phi(q_i) \text{ where } \phi(q) = t + \frac{a}{bx(q) + cy(q) + d}.$$

ϕ, as a function on C takes on zero at most n times, since $\phi(q) = 0 \Rightarrow x(q) = -(cy(q)+d) - a/t/b$ which can happen for at most n places q of C.

Let ϕ have zeros $\{v_i\}_1^h$, poles $\{t_i\}_1^h$ and apply Theorem 10 to obtain

$$\Phi(p_n) = c \prod_{j=1}^h \frac{\Theta(\underset{\sim}{s}_{v'}(Q) - \int_{p_0}^{v_j} d\underset{\sim}{\omega})}{\Theta(\underset{\sim}{s}_{v'}(Q) - \int_{p_0}^{t_j} d\underset{\sim}{\omega})}$$

We are nearly done, but the final computation is some work, so we break it down into steps.

Step 1 - notation -

$\underset{\sim}{s}_{v'}(p^g) = g\,\underset{\sim}{\omega}(p) + \underset{\sim}{c}$ where $\underset{\sim}{\omega}(p) = \int_{p_0}^{p} d\underset{\sim}{\omega}$, $\underset{\sim}{c} = \int_{v'}^{p_0^g} d\underset{\sim}{\omega}$.

The places p_n above p correspond to place sets Q having abelian coordinates $\underset{\sim}{s}_{v'}(Q) \equiv \frac{g}{n}\underset{\sim}{\omega}(p) + \frac{1}{n}(\underset{\sim}{c} - \underset{\sim}{b})$ $+ \frac{1}{n}(\text{period})$

Let $\int_{p_0}^{v_j} d\underset{\sim}{\omega} = \underset{\sim}{V}_j$, $j = 1, \cdots, h$, and put $\frac{1}{n}(\underset{\sim}{c} - \underset{\sim}{b}) - \underset{\sim}{V}_j = \underset{\sim}{k}_j$.

Thus, the number of zeros of $N_{L(C_n)/L(C)}\Phi$ on C is the number of zeros of

$$\boxed{\Psi(p) = \prod_{j=1}^{h} \prod_{q_\ell, q_\ell' = 0}^{n-1} \Theta\left(\frac{g}{n}\underset{\sim}{\omega}(p) + \underset{\sim}{k}_j + \frac{1}{n}\sum_{\ell=1}^{g}(q_\ell' \pi i \underset{\sim}{e}_\ell + q_\ell \underset{\sim}{a}_\ell)\right)}$$

Since $\Psi(p)$ is entire, we compute $N = \frac{1}{2\pi i}\int_E d(\log \Psi(p))$.

Since $\underset{\sim}{\omega}(p)$ changes by $\pi i \underset{\sim}{e}_k$ along B_k, $\log \Psi(p)$ is the same after passing around the loop B_k. Thus, the contribution to this integral by integrating around B_k is 0.

<u>Step 2</u> - <u>Contribution from the loop A_k</u> -

$\Phi(p)$ is a product of h functions of the form

$$\prod_{\text{periods}} \Theta\left(\tfrac{g}{n}\underset{\sim}{\omega}(p) + \underset{\sim}{k}_\ell + \left(\tfrac{\text{period}}{n}\right)\right) = \Psi_\ell(p).$$

$N = h$ times # of zeros of $\psi_j(p)$. Note that $(g,n)=1 \Longrightarrow$

$$\psi_\ell(p) = \prod_{\text{periods}} \Theta\left(\tfrac{g}{n}\underset{\sim}{\omega}(p) + \underset{\sim}{v}_j + \tfrac{g}{n}(\text{period})\right).$$

We can further break up $\psi_j(p)$ into a product of functions (<u>n^{2g-1} of them</u>), each of the form

$$\boxed{\prod_{g_j=0}^{n-1} \Theta\left(\tfrac{g}{n}\underset{\sim}{\omega}(p) + \underset{\sim}{v}_j + \tfrac{g}{n}g_j \underset{\sim}{a}_j\right) = \chi_j(p)}$$

<u>note</u> - Don't get confused by the subscript on $\chi_j(p)$. This factorization was done <u>just</u> for integration around A_j.

In order to be done, we need only compute $\frac{1}{2\pi i}\int_{A_j} d(\log \chi_j(p)) + \frac{1}{2\pi i}\int_{A_j^{-1}} d(\log \chi_j(p))$, and then multiply by $h\, n^{2g-1} g$.

<u>Step 3 - Final computation</u> -

$$\left(\int_{A_j} + \int_{A_j^{-1}}\right) d(\log \chi_j(p)) = \frac{1}{2\pi i}\int_{A_k} d\left(\log \prod_{g_j=0}^{n-1} \frac{\Theta\left(\frac{g}{n}(\underset{\sim}{\omega} + \underset{\sim}{a}_j) + \underset{\sim}{v}_j + \frac{g}{n} g_j \underset{\sim}{a}_j\right)}{\Theta\left(\frac{g}{n}(\underset{\sim}{\omega}) + \underset{\sim}{v}_j + \frac{g}{n} g_j \underset{\sim}{a}_j\right)}\right)$$

$$= \frac{1}{2\pi i}\int_{A_j} d\left(\log\left(\frac{\Theta\left(\frac{g}{n}\underset{\sim}{\omega} + \underset{\sim}{v}_j + g\underset{\sim}{a}_j\right)}{\Theta\left(\frac{g}{n}\underset{\sim}{\omega} + \underset{\sim}{v}_j\right)}\right)\right) = \frac{1}{2\pi i}\int_{A_j} d\left(\frac{2g^2}{n}\omega_j + 2g v_{jj} + g a_{jj}\right)$$

$$= \frac{g^2}{n},$$

where we have used the fact that $\Theta\left(\frac{g}{n}\underset{\sim}{\omega} + \underset{\sim}{v}_j + g\underset{\sim}{a}_j\right) = e^{2g\left(\frac{g}{n}\omega_j + v_{jj}\right) + g a_{jj}}\, \Theta\left(\frac{g}{n}\underset{\sim}{\omega} + \underset{\sim}{v}_j\right)$.

<u>Q.E.D.</u>

<u>End of Whole Theorem</u>