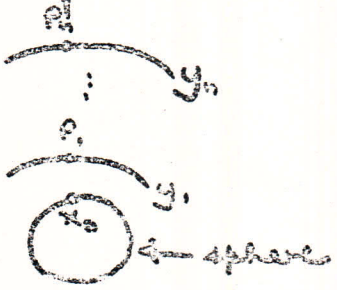
Part I – Lectures on Algebraic Functions

Preliminaries

Assume the curve $\mathcal{C}$ over $K = \mathbb{C}$ is absolutely irreducible, given by $f(x,y) = 0$. The function field $K(x,y)$ = quotient field of $K[X,Y]/(f(X,Y))$ or any isomorphic field, and we denote $K(x,y)$ by $K(\mathcal{C})$, $\mathbb{C}(x,y)$ by $\mathbb{C}(\mathcal{C})$.

$\mathbb{C}(x) \subset \mathbb{C}(x,y)$, and the function x represents the Riemann sphere. The different sheets of the Riemann surface (hereafter abbreviated R.S.) for the curve represent the different roots of $f(x,y) = 0$ in y, for a fixed indeterminate x. Above the place $x = x_0$ on the sphere we have places (i.e. for each root y_0 of $f(x_0,y) = 0$ we obtain a Puiseux expansion:

$$y = y_0 + a_1(x-x_0)^{\frac{1}{k}} + a_2(x-x_0)^{\frac{2}{k}} + \dots).$$



For all but finitely many x_0, there will be n distinct zeros $y_0^1, \dots, y_0^n$; and to each corresponding expansion we get $k = 1$. Thus we parametrize the corresponding places by $(t + x_0,\ y_0^{(i)} + a_1^{(i)}t + a_2^{(i)}t^2 + \dots)$ $i = 1, \dots, n$ (where the values of t give us the values a x and y in a nbh. of this place, and thus we obtain the values of any function in $\mathbb{C}(x,y)$ in this nbh.).

The pts. (x_0, y_0) of the curve for which y_0 is a multiple point fall into two classes:

① Those for which $k > 1$. Over x_0 lie k of the sheets "come together" and the pt. of coming together is represented by the place $(t^k + x_0,\ y_0 + a_1t + a_2t^2 + \dots)$ (i.e. $(x-x_0)^{\frac{1}{k}}$ is a local parameter).

② Those for which $k = 1$ (i.e. at least two distinct places with the same center) represent a singular point of the curve. It is the singular points that make life hard for geometers (as in Bezout's theorem) but in this work they will cause us no difficulty.

Note - there could be 'mixing' of ① and ② at the places above $x = x_0$.

Def - K-rat. point on $\mathcal{C}$ is one whose coords. are in K. Then $\exists$ (with finitely many exceptions) a 1-1 correspondence between K-rational places (coefficients of power-series are in K) and K-rat. pts. on $\mathcal{C}$.

Thm - If $u \in \mathbb{C}(x,y)$, $\sum_{\mathfrak{p}, \text{ places of } \mathcal{C}} v_{\mathfrak{p}}(u) = 0$. Looking at $u - a$ (instead of u) for $a \in \mathbb{C}$ we see that this tells us that each value is assumed (with multiplicity) the same number of times as is assumed at ∞.

Proof -

Assume that the sheets for $y_1, \dots, y_k$ come together over the place $x = 0$, and call this place $\mathfrak{p}$. If $v_{\mathfrak{p}}(u) = v$, then $y_1 = a_0 + a_1 x^{\frac{1}{k}} + \cdots$ and $y_2, \dots, y_k$ are obtained by replacing $x^{\frac{1}{k}}$ by $\zeta_k^j x^{\frac{1}{k}}$, $j = 1, \dots, k-1$, in this expansion (where ζ_k is a primitive k-th root of 1). So, $u(x, y_1) = b_\nu x^{\frac{\nu}{k}} + \cdots$ and $\prod_1^k u(x, y_i) = c_\nu x^{\nu} + \cdots$. Therefore, we may conclude, the sum of the orders of u at places over the places $x = 0$ on the x-sphere is ν; the order of the function (in x) $\prod_1^n u(x, y_i)$ at $x = 0$. But $\prod_1^n u(x, y_i) = g(x)$ is a rational function of x, so $\sum_{\mathfrak{p} \in \mathcal{C}} v_{\mathfrak{p}}(u) = \sum_{\text{p on } x\text{-sphere}} \sum_{\mathfrak{P} | \mathfrak{p}} v_{\mathfrak{P}}(u)$

$= \sum_{\mathfrak{p} \text{ on } x\text{-sphere}} v_{\mathfrak{p}}(g(x)) = 0$ (the last by the fundamental theorem of algebra). Q.E.D.

Differentials

Fact - Every function meromorphic on the R.S. $\mathcal{C}$ is a rational function of x and y.

Proof -

Let z be a complex variable, u a meromorphic function on $\mathcal{C}$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ denote the places above a place on the x-sphere, so

$\sum_{i=1}^n \left(u(\mathfrak{p}_i) \prod_{j \neq i} (z - y(\mathfrak{p}_j)) \right) = h(x, z)$ is a polynomial in z

whose coeffics. are symmetric functions of $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, and so are rational functions of x. Assume $x = a$ is such that $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are distinct places. Let $z = y(\mathfrak{p}_1)$, and $F(z) = \prod_i (z - y(\mathfrak{p}_i))$. Then we obtain

$u(\mathfrak{p}_1) = \dfrac{h(x(\mathfrak{p}_1), y(\mathfrak{p}_1))}{F'(y(\mathfrak{p}_1))}$. Or, $u = \dfrac{h(x,y)}{F'(y)}$ (where we extend the evaluation to places over branch pts. by using the fact that u, $F'(y)$, $h(x,y)$ are all meromorphic). Q.E.D.

Def - A differential is an expression $f(t)\,dt$, where locally $f(t)$ is a meromorphic function of t; and if the coordinate nbds. of t and t^* overlap (i.e. $t^* = t^*(t)$) then, $f^*(t^*)\dfrac{dt^*}{dt} = f^*(t^*(t))\dfrac{d(t^*(t))}{dt} = f(t)$

(i.e. this is what we mean when we say $f^*(t^*)\,dt^* = f(t)\,dt$ in the region where t^* and t represent common places of the R.S.).

Def - Residue of $u \in \mathbb{C}(x,y)$ at $\mathfrak{p}$ is $\operatorname{res}_{\mathfrak{p}} u = \dfrac{1}{2\pi i}\displaystyle\int_{|t|=\epsilon} u\left(\frac{dx}{dt}\right)dt$ where ϵ is taken small enough to exclude any branch pts. except possibly $\mathfrak{p}$ itself. We call $u(dx)$ the differential associated with u. The residue of u is independent of the local parameter t (but does depend on x). This allows us to integrate with respect to x by keeping track of which sheet of the R.S. we are on.

Thm - Sum of Residues of u at all places on C is 0 (just apply Cauchy's theorem which is of course valid on any R.S.).

Thm - Since the ratio of two differentials is a globally defined meromorphic function, the divisors of differentials $u\,dx$, $u \in \mathbb{C}(x,y)$ is a divisor class - the canonical class W.

Def - a differential $u\,dx$ of C with no poles is said to be of the 1st kind.

Riemann-Roch - Let $\bar{K}$ be the alg. closure of K in $\mathbb{C}$, $\mathcal{U}$ an arbitrary divisor of $\mathbb{C}/\bar{K}$. Then $\ell(\mathcal{U}) = d(\mathcal{U}) + 1 - g + \ell(\mathcal{W}/\mathcal{U})$ where g is the topological genus (i.e. the R.S. $\mathbb{C}$ is a sphere with g handles), $\ell(\mathcal{U})$ = dim. over $\bar{K}$ of functions $u \in \bar{K}(\mathbb{C}) \ni (u) \mathcal{U}$ is positive. actually the theorem is easily shown (assuming this version is known) with $\bar{K}$ replaced by K, as long as we properly define $d(\mathcal{U})$ to be - $\deg \mathcal{U} = \sum_{\mathfrak{p} \in \operatorname{supp} \mathcal{U}} n_{\mathfrak{p}} [K(\mathfrak{p}) : K]$ where $\mathcal{U} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$ and $K(\mathfrak{p})$ is the field obtained by adjoining the coeffics. of the parametrization of the place $\mathfrak{p}$ to the field K (actually $K(\mathfrak{p}) = K(x_0, y_0)$ where (x_0, y_0) is the center of $\mathfrak{p}$).

Def - $\mathcal{U}$ is called special if $\ell(\mathcal{W}/\mathcal{U}) \neq 0$, non-special otherwise.

Consequences of R.R. -

Thm - $d((dx)) = 2g-2$ and thus,

$$2g-2 = \sum_{\substack{e_{\mathfrak{p}} = v_{\mathfrak{p}}(x - x(\mathfrak{p})) \\ \text{where } x(\mathfrak{p}) \text{ is finite}}} (e_{\mathfrak{p}} - 1) - \sum_{\substack{s_{\mathfrak{p}} = -v_{\mathfrak{p}}(x) \\ \text{where } x \text{ has a pole at } \mathfrak{p}}} (s_{\mathfrak{p}} + 1)$$

$$= \sum (e_{\mathfrak{p}} - 1) + \sum (s_{\mathfrak{p}} - 1) - 2 \sum s_{\mathfrak{p}} = V - 2n$$ where V is the ramification index of the function x, n is the # of sheets (i.e. # of times infinity is assumed).

Example - If t is the local parameter at $\mathfrak{p}$, $x = x_0 + t^k$ (k = # of sheets coming together at $\mathfrak{p}$); $e_{\mathfrak{p}} - 1 = k-1$; so we get a contribution to V only at places above branch pts. We compute the genus of $\boxed{y^4 = x^4 - 1}$. Look for $x_0 \ni$ the expansion of y in $x - x_0$ is of the form $\sum a_i (x-x_0)^{i/k}$ where $k > 1$.

$y = \sqrt[4]{1 - (x - x_0 + x_0)^4}$ and for finite x_0, we get $k > 1$ iff $x_0 =$ a fourth root of 1. For each such x_0, all 4 sheets come together, and so $\sum_{e_{\mathfrak{p}} = v_{\mathfrak{p}}(x - x(\mathfrak{p}))} (e_{\mathfrak{p}} - 1) = 4(4-1)$. Over $x_0 = \infty$, change x to $\frac{1}{z}$, so $y^4 = \frac{1 - z^4}{z^4}$, and we see that there is no ramification at 0 for this equation. Thus, in the equation $y^4 = x^4 - 1$ there is no ramification at ∞. Thus, $12 - 2(4) = 2g-2$.

the genus of this curve is therefore $g = 3$.

Thm - There are g lin. indep. differentials of 1st kind over $\bar{K}$.

Proof -

$\ell(W) = g$. If we write $W = (dx)$, then the functions $u \ni (u)(dx) = (u\,dx)$ are positive divisors, form a vector space of dim. g. Q.E.D.

Thm - $C/\bar{K}$ has a rational function field iff $g = 0$.

Proof -

If $g = 0$, from R.R. $\exists$ a function having only a single pole of order one at a given place $\mathfrak{p}$. The number of poles of a non-constant function x is $[\bar{K}(C) : \bar{K}(x)]$, so $\bar{K}(C) = \bar{K}(x)$. Conversely, if $\bar{K}(C) = \bar{K}(x)$, x takes on each value once on the R.S., so $V = 0$, and $2g - 2 + 2 = V \Rightarrow g = 0$. Q.E.D.

Thm - Two R.S.'s are conformally equivalent iff their function fields are isomorphic (just use the fact that a function meromorphic on a R.S. is a rat. function of x and y where $\bar{K}(x,y)$ is the function field).

Theorems about Curves over Number Fields

We will prove Siegel's Theorem (first for just genus 1 curves, and the Hilbert Irreducibility Thm. In Siegel's Theorem we will need some form of the following two theorems, which we will not prove.

I. Thue-Siegel-Roth - Let $|\alpha|$ stand for ordinary absolute value of a complex number α. If α is algebraic, and K is a fixed number field, then for any constants $C > 0$, $\chi > 2$, the inequality

$$|\alpha - \eta| < \frac{C}{H^{\chi}(\eta)}$$

has only finitely many solutions $\eta \in K$. Here $H(\eta)$ is the max. of the absolute value of the integer coeffics. of the defining polynomial for η over $\mathbb{Z}$.

II. Mordell-Weil Theorem - For a curve of genus g we say that $\mathfrak{p}_1 \cdots \mathfrak{p}_g$ (a product of g places) is a place set.

Let $P^{(0)}$ be a fixed place set. If $P^{(1)}$ and $P^{(2)}$ are given place sets, then $\exists$ a place set $P^{(3)}$ (whose class is unique) $\ni$ $\left(\frac{P^{(1)}}{P^{(0)}}\right)\left(\frac{P^{(2)}}{P^{(0)}}\right) \sim \left(\frac{P^{(3)}}{P^{(0)}}\right)$. We say that the class of $P^{(3)}$ is the sum of the classes of $P^{(1)}$ and $P^{(2)}$. This is the addition of pts. on an elliptic curve ($g=1$). If $P^{(0)}, P^{(1)}, P^{(2)}$ are k-rational, then so is $P^{(3)}$. The Mordell-Weil theorem says that the group of k-rat. place sets are finitely generated.

Mordell ('On the rational solutions of indeterminate equations of 3rd and 4th degree' - Proc. of Cambridge Phil. Soc. (1922) - pg. 179) showed this for elliptic curves over the rationals.

Weil - 'Sur l'arithmetique sur Courbes Algebrique' acta. math., Vol. 52, pg. 281 - (1928).

Mordell conjectured that the k-rat. pts. on a curve of genus ≥ 2 are finite. While nothing much has been done on this conjecture, Manin and Grauert (independently) have shown that a curve of genus ≥ 2 defined over a function field K, have infinitely many K-rat. pts. iff it has infinitely many pts. over the algebraic closure of the constant field of K (i.e. the curve is defined over the alg. closure of the constant field of K).

Statement of Hilbert Irreducibility -

Let $f(\Sigma_1, \cdots, \Sigma_n, t) \in \Phi[\Sigma_1, \cdots, \Sigma_n, t]$ be irreducible. Then $\exists$ ∞-many integer tuples $(x_1, \cdots, x_n) \ni f(x_1, \cdots, x_n, t)$ remains irreducible. More generally, the same result is true if we replace t be a vector-valued variable, or Φ by any number field.

We show that if $n=1$;

A. There $\exists$ a set of integers I, of asymptotic density one $\ni$ $x_0 \in I \Rightarrow f(x_0, t)$ is irreducible.

B. There $\exists$ an arithmetic progression P of integers $\ni$

$x_0 \in P \Rightarrow f(x_0, t)$ is irreducible. (7)

Proof of A (slight modification of the proof in Lang, 'Diophantine Geometry').

① If $f(x,t)$ is irreducible, we write $f(x,t) = \left[\prod_1^n (t - t_i)\right]^{h(x)}$ where $h(x)$ is a rational function. For $\forall$ partition of the integers $1, 2, \cdots, n$ into two non-empty, disjoint sets A and B, we decompose $f(x,t) = g_A(x,t)\, g_B(x,t)$ where one of the coefficients of g_A (as a polynomial in t) is not a rational function of x. Call one of these coefficients Z_A. If x_0 is an integer for which $f(x_0, t)$ is reducible (assume $h(x_0) \neq 0$), there exists a set $A \ni Z_A(x_0)$ is in Φ. Assume the set of x_0 for which such a set A exists has positive assymptotic density.

⊛ Then $\exists$ at least one $A \ni Z_A(x_0) \in \Phi$ for a set of integers x_0 of positive assymptotic density.

② We retain property ⊛ if we multiply $Z_A(x)$ by an element of $\Phi[x]$, and we do so in order that we may assume $Z_A(x)$ is integral over $\mathbb{Z}[x]$ (i.e. $Z_A(x_0)$ is an integer).

Expand the algebraic function $Z_A(x)$ at infinity to obtain $Z_A(x) = a_n x^{\frac{n}{m}} + a_{n-1} x^{\frac{n-1}{m}} + \cdots$. Since $Z_A(x)$ takes on integer values for infinitely many integers x_0; $a_n, a_{n-1}, \cdots$ are all real.

Look at,

$$F(x) = \begin{vmatrix} 1 & x_i & \cdots & x_i^n & Z_A(x_i) \\ \vdots & & & & \vdots \\ 1 & x_{i+n} & \cdots & x_{i+n}^n & Z_A(x_{i+n}) \\ 1 & x & \cdots & x^n & Z_A(x) \end{vmatrix} \quad \text{where } x_i < x_{i+1} < \cdots < x_{i+n+1}.$$

$F(x_i) = \cdots = F(x_{n+i}) = 0$. Therefore, if we pick C is that $G(x) = F(x) - C(x - x_i)\cdots(x - x_{i+n})$ will vanish at x_{i+n+1}, then $G(x)$ vanishes at $n+2$ pts. Thus, $G^{(n+1)}(x)$ vanishes at at least one value $x_i < \tau < x_{i+n+1}$.

$G^{(n+1)}(x) = F^{(n+1)}(x) - (n+1)!\,C$, so $C = \frac{F^{(n+1)}(T)}{(n+1)!}$

where by direct calculation

$F^{(n+1)}(T) = Z_A^{(n+1)}(T)\,V_n$, where V_n is the Vandermonde determinant. Since $V_n(x_{i+n+1} - x_i)\cdots(x_{i+n+1} - x_{i+n}) = V_{n+1}$ we see that

$$\frac{Z_A^{(n+1)}(T)}{(n+1)!} = \frac{\begin{vmatrix} 1 & x_i & \cdots & x_i^n & Z_A(x_i) \\ \vdots & & & & \vdots \\ 1 & x_{i+n+1} & \cdots & x_{i+n+1}^n & Z_A(x_{i+n+1}) \end{vmatrix}}{V_{n+1}} .$$

Lemma - If I is a set of integers ($I = x_1 < x_2 < x_3 < \ldots$) with positive assymptotic density, then $\exists$ constant $B \ni |x_{i+n+1} - x_i| < B$ for ∞-many i.

Proof -

$\liminf \frac{i}{x_i}$ = assymptotic density of AI. If for any $B > 0$, $|x_{i+n+1} - x_i| > B$ for all but finitely many integers i, then $|x_{(n+1)l}| = \left|\sum_{k=0}^{l}(x_{(n+1)k} - x_{(n+1)(k-1)})\right| > Bl - C$, for some constant C, (dependent on B, but not on l).

$\frac{(n+1)l}{x_{(n+1)l}} < \frac{l(n+1)}{Bl - C}$, so $\liminf \frac{i}{x_i} \le \liminf \frac{l(n+1)}{x_{(n+1)l}} < \frac{l(n+1)}{Bl - C}$,

so $\liminf \frac{i}{x_i} < \frac{n+1}{B}$. But, since B was arbitrary, this contradicts the positive density of I. Q.E.D.

For those i for which $|x_{i+n+1} - x_i|$ is bounded (as a function of i), $Z_A^{(n+1)}(T_i)$ is an integer/integer with bounded denominator. But $Z_A^{(n+1)}(T) \to 0$ as $T \to \infty$, so $Z_A^{(n+1)}(x) \equiv 0$, since it must be zero for infinitely many T_i (and $Z_A^{(n+1)}(x)$ is an algebraic function). Thus, $Z_A(x)$ is a polynomial. We easily check by Cramer's rule that its coefficients are in $\mathbb{Q}$.

Q.E.D.

Proof of B - (originally due to Chingel in acta arith - 1965)

Let $f_{A_i}(X,Z)$ be the curve defined by $X, Z_{A_i}(X)$ (as in proof of A), and $F(X,Z) = \prod_i f_{A_i}(X,Z)$. If we show that the hypothesis (i.e. $X_0 \in P \Rightarrow F(X_0,Z)=0$ has an integer solution Z_0) implies that $\exists$ a rational function $Z(X) \ni F(X,Z(X)) \equiv 0$, we have a contradiction to the fact that none of the $Z_{A_i}(X) \in \mathbb{Q}(X)$.

applying the theorem we just proved, $\exists$ an integer $\bar{X} \ni f_{A_i}(\bar{X},Z)$ is irreducible for all i. If $f_{A_i}(\bar{X},Z)$ is linear in Z, then we easily deduce that $f_{A_i}(X,Z) = h(X) - cZ$ (c a constant), and our contradiction follows. If $f_{A_i}(\bar{X},Z)$ is not linear in Z, then since it is irreducible $\exists$ a prime p_{A_i} (very large) $\ni$ $f_{A_i}(\bar{X},Z) \equiv 0 \bmod p_{A_i}$ has no solution in Z. Look at the arithmetic progression $\{\bar{X} + (\prod_i p_{A_i})m\}$ $(m=1,2,\dots)$. If we assume that the arithmetic progression P does not exist, $\exists$ $Z_0 = \bar{X} + (\prod_i p_{A_i})m_0$ (for some m_0) $\Rightarrow$ $F(X_0,Z_0) = 0$ for some integer Z_0. But this means $f_{A_i}(X_0,Z_0) = 0$ for some i, and this contradicts $f_{A_i}(X_0,Z_0) \equiv f_{A_i}(\bar{X},Z_0) \not\equiv 0 \bmod p_{A_i}$. Q.E.D.

Weil's Distribution theory - this will be a very important tool in our investigation of functions $u \in K(C)$. The final theorem that we will obtain in this section has as a particular consequence; if $(u) = (D)^l$ for some divisor D of $C(C)$, then u is "essentially" the l-th power of some function of $K(C)$.

For $\forall$ place $\mathfrak{p}$ of C, we let $K_{\mathfrak{p}}$ be the field obtained by adjoining the coordinates (of the center) of $\mathfrak{p}$ to K.

Def - A distribution d on C, rational relative to K, is a function whose value at each algebraic place $\mathfrak{p}$ is an integral ideal of $K_{\mathfrak{p}}$, and such that d assigns conjugate ideals to conjugate places. Product of distributions is defined pt.-wise; $(dd')(\mathfrak{p}) = d(\mathfrak{p})\,d'(\mathfrak{p})$. Two distributions d and d' are equivalent ($d \sim d'$) if $\exists\ a, a' \in \mathcal{O}_K$ (integers of K) $\ni$ $d(\mathfrak{p}) \mid a'd'(\mathfrak{p})$ and $d'(\mathfrak{p}) \mid a\,d(\mathfrak{p})$ for $\forall$ alg. place $\mathfrak{p}$. If $(d, d') \sim 1$, then d and d' are relatively prime, and if $\exists\ d'' \ni d \sim d'd''$, then d' divides d.

Def - If $h \in K(C)$, $\mathfrak{p}$ neither a zero nor pole of h, the ideal $(h(\mathfrak{p}))$ can be written $\frac{A(\mathfrak{p})}{B(\mathfrak{p})}$ (integral ideals of $K_{\mathfrak{p}}$ with $(A, B) = 1$). At a pole of h put $A = 1, B = 0$ and at a zero put $A = 0, B = 1$. The distribution whose value at $\forall$ algebraic pt. $\mathfrak{p}$ is $B(\mathfrak{p})$, is designated by $[h]$. Also we denote by D_h, the divisor of the poles of h.

Lemma 1 - Let $u, v \in K(C)$, and $D_v \mid D_u$, then $[v] \mid [u]$.

Proof -

Let the equation connecting u and v be $g_0(u)v^r + g_1(u)v^{r-1} + \cdots + g_r(u) = 0$ and divide by u^r. We easily deduce the $\deg g_i \leq i$, if we know that $\frac{v}{u}$ is integral over $K[\frac{1}{u}]$. But $\frac{v}{u}$ has all its poles among poles of $\frac{1}{u}$, so the place extension implies that $\frac{v}{u}$ is integral over $\frac{1}{u}$.

We may write the equation relating u and v in the form $gv^r + up(u,v) + q(v) = 0$ where all coefficients are in $\mathcal{O}_K$, p and q are polynoms. of total degree $r-1$, g is a non-zero constant.

Let $u(\mathfrak{p}) = A/C$, $v(\mathfrak{p}) = B/C$; A, B, C ideals of $K_{\mathfrak{p}}$ with $(A, B, C) = 1$. The ideal $(u(\mathfrak{p})\,p(u(\mathfrak{p}), v(\mathfrak{p}))\,C^r,\ q(v(\mathfrak{p}))C^r) \mid gv^r(\mathfrak{p})C^r \Rightarrow$ $(A, C) \mid gB^r \Rightarrow (A, C) \mid g$. So $[u] = \frac{C}{(A,C)} \sim C$.

since $[v] \mid C$, we obtain $[v] \mid [u]$. Q.E.D.

Lemma 2 - Let u and v have no common poles, then $([u],[v]) = 1$.

Proof -

Let $g_0(u)v^r + \ldots + g_r(u) = 0$ be defining relation between u and v. Divide by highest power of u and let $u \to \infty$. If the highest power of u is not in $g_0(u)$, then there will be $\leq r-1$ finite values of v at places which are poles of u. Thus, one of the poles of u is also a pole of v.

We therefore conclude that the defining equation has the form $gu^s v^r + p(u,v) = 0$ where $\deg p \leq r+s-1$, $\deg_u p \leq s$, $\deg_v p \leq r$, and g (along with all other coeffics.) is in $\mathcal{O}_K$.

If $u(\mathfrak{p}) = A_1/B_1$, $v(\mathfrak{p}) = A_2/B_2$ with $(A_1,B_1) = (A_2,B_2) = 1$, then $p(u(\mathfrak{p}), v(\mathfrak{p}))\, B_1^{s-1} B_2^{r-1} \left(\frac{B_1 B_2}{(B_1,B_2)}\right)$ is an integral ideal.

Therefore $(B_1,B_2) \mid g A_1^s A_2^r$, so $(B_1,B_2) \mid g$ except at finitely many places where A_1, A_2, B_1 or B_2 is 0. But B_1 and B_2 do not vanish together, and A_1, A_2 vanish at only finitely many places, so $\exists\, g' \in \mathcal{O}_K \ni (B_1,B_2) \mid g'$ everywhere. Q.E.D.

Lemma 3 - If every common pole of u and v is a pole of w, then $([u],[v]) \mid [w]$.

Proof -

Pick $a \in K \ni w+a$ has no zero at any pole of v. Since $w+a$ and w have the same poles, Lemma 1 $\Rightarrow [w+a] \sim [w]$. Thus $\frac{u}{w+a}$ and v have no common poles, so $\left(\left[\frac{u}{w+a}\right], [v]\right) \sim 1$. Put $u(\mathfrak{p}) = A_1/B_1$, $v(\mathfrak{p}) = A_2/B_2$ and $(w+a)(\mathfrak{p}) = A_3/B_3$. For some fixed $b \in \mathcal{O}_K$ we get

$$\left(\frac{B_1 A_3}{(B_1A_3, A_1B_3)}, B_2\right) \mid b \Rightarrow (B_1,B_2) \mid b(B_1A_3, A_1B_3) \Rightarrow$$

$$(B_1,B_2) \mid b B_3. \qquad \text{Q.E.D.}$$

Note - If w has the common poles of u and v, then $[w] \mid [u]$, $[w] \mid [v]$, so $[w] \mid ([u],[v])$. But, by Lemma 3,

$([u],[v]) \mid [w]$, so $[w] \sim ([u],[v])$. Similarly, if the common poles of w and h are the common poles of u and v, then $([w],[h]) \sim ([u],[v])$.

Def - Let $\mathfrak{p}_0$ be an algebraic place on C/K. Then $d\mathfrak{p}_0 \overset{\text{def}}{=} ([u],[v])$ where u and v are two functions of $K_{\mathfrak{p}_0}(C)$ having $\mathfrak{p}_0$ as their only common (simple) pole. From notes above $d\mathfrak{p}_0$ is well-defined, and $d\mathfrak{p}_0$ exists by R.R. In addition, as a destribution we define $E(\mathfrak{p},\mathfrak{p}_0)$ to be the value of $d\mathfrak{p}_0$ at $\mathfrak{p}$, and we note that $d\mathfrak{p}_0$ associates conjugate functions to $d\mathfrak{p}_0'$ where $\mathfrak{p}_0'$ is a place conjugate to $\mathfrak{p}_0$. For an arbitrary integral divisor $\mathcal{U} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, let $\mathcal{U}(\mathfrak{p}) = \prod_1^r E(\mathfrak{p},\mathfrak{q}_i)$.

Theorem 1 - Weil's Decomposition Theorem - Let C be an alg. curve defined over K. To each function $f \in K(C)$ $\exists$ an expression

$$f(\mathfrak{p}) = \frac{\lambda}{\mu} \frac{E(\mathfrak{p},\mathfrak{p}_1)\cdots E(\mathfrak{p},\mathfrak{p}_n)}{E(\mathfrak{p},\mathfrak{q}_1)\cdots E(\mathfrak{p},\mathfrak{q}_n)} \quad \text{where } \{\mathfrak{p}_i\}_1^n,$$

$\{\mathfrak{q}_i\}_1^n$ are the zeros and poles of f, $\mathfrak{p}$ runs over alg. places, and the functions λ, μ, and the g.c.d. of the numerator and denominator are finitary (i.e. while these are not constant functions of $\mathfrak{p}$, they do divide an integer independent of $\mathfrak{p}$). Since $N_f(\mathfrak{p}) = \prod_1^n E(\mathfrak{p},\mathfrak{p}_i)$, $D_f(\mathfrak{p}) = \prod_1^n E(\mathfrak{p},\mathfrak{q}_i)$ and both N_f, D_f are K-rational divisors, we see that $N_f(\mathfrak{p})$ and $D_f(\mathfrak{p})$ are principal ideals in $K_{\mathfrak{p}}$. In our expression for $f(\mathfrak{p})$, it is understood that $N_f(\mathfrak{p})$ and $D_f(\mathfrak{p})$ are really generators from $\mathcal{O}_{K_{\mathfrak{p}}}$ of these ideals, and $\lambda, \mu \in \mathcal{O}_{K_{\mathfrak{p}}}$ are not known up to units of $K_{\mathfrak{p}}$.

Proof -

We show $[f] \sim \prod_1^n d\mathfrak{q}_i$, (and similarly $\left[\frac{1}{f}\right] \sim \prod_1^n d\mathfrak{p}_i$). From Lemma 2 $\left([f], \left[\frac{1}{f}\right]\right) \sim 1$, so our theorem will follow. Let u_i, v_i be functions of $K_{\mathfrak{q}_i}(C)$ having $\mathfrak{q}_i$ as a simple pole, and $\ni$ the only common pole of u_i and

πv_i are exactly the poles of f, $[f] \sim ([\pi u_i], [\pi v_i])$. From Lemma 3, $df_i = ([u_i], [v_i]) \mid [f]$, and since $(df_i, df_j) \sim 1$ for $f_i \neq f_j$, $\prod_1^n df_i \mid [f]$. But, also $[\pi u_i] \mid \pi[u_i]$, so $[f] \mid \dfrac{\pi[u_i], \pi[v_i])}{(\text{l.c.m. of } \pi[u_i], \pi[v_i])} \sim \pi df_i$.

Q.E.D.

Theorem 2 - Let $\mathcal{C}/K$ be a curve of pos. genus, and let $\mathfrak{M}$ be an infinite set of K rat. places of $\mathcal{C}$, $x \in K(\mathcal{C})$ (non-constant) quasi-integral on $\mathfrak{M}$. Let $f \in K(\mathcal{C})$ with divisor $(f) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^l \left(\dfrac{r_1 \cdots r_s}{q_1 \cdots q_t}\right)$ where the q_i, r_i are poles of x, $l > 0$. Then $\{(f(\mathfrak{p}))^{\frac{1}{l}}\}$ for $\mathfrak{p} \in \mathfrak{M}$ form a quasi-integral set of numbers in some fixed ext. of K.

Proof -

If q is a pole of x, from Theorem 1, the distribution $E(\mathfrak{p}, q)$ is finitary on $\mathfrak{M}$. Thus, on $\mathfrak{M}$:

$f(\mathfrak{p}) = (\text{finitary}) \{E(\mathfrak{p}, \mathfrak{p}_1) \cdots E(\mathfrak{p}, \mathfrak{p}_r)\}^l$ where $\prod_1^r E(\mathfrak{p}, \mathfrak{p}_i)$

$= E_{\mathfrak{p}}$ is an integral ideal of some finite ext. L of K. Choose a representative from $\forall$ class of integral ideals of L, $B_{\mathfrak{p}}$ in the class of $E_{\mathfrak{p}}$. Then $f(\mathfrak{p}) = \{B_{\mathfrak{p}}^l \cdot \_\_\}\left(\dfrac{E_{\mathfrak{p}}}{B_{\mathfrak{p}}}\right)^l$, where the expression in $\{\ \}$ is a principal finitary ideal (because $B_{\mathfrak{p}}$ takes on only finitely many values as a function of $\mathfrak{p}$ - $f(\mathfrak{p})$ and $\dfrac{E_{\mathfrak{p}}}{B_{\mathfrak{p}}}$ are both principal). Thus, $f(\mathfrak{p}) = \epsilon' m' (a')^l$ where ϵ' is a unit, a' is an integer of L, and m' is one of finitely many nos. of L. By Dirichlet unit thm ϵ' can be written $\epsilon_1^{l_1} \cdots \epsilon_r^{l_r} \epsilon^l$ where $\epsilon_1, \cdots, \epsilon_r$ form a base for the units of L, $0 \leq l_i < l$, and ϵ is a unit. Thus, $f(\mathfrak{p}) = m a^l$, $a = \epsilon a'$ and m is only among finitely many nos. of L. Let $L' = L$ with finitely many nos. $m^{\frac{1}{l}}$ adjoined, and we see that $\{f(\mathfrak{p})^{\frac{1}{l}}\} \in L'$ and is quasi-integral on $\mathfrak{M}$.

Q.E.D.

Theorem 3 - C a curve of genus 1 defined over a no. field K. Then $\exists$ no function $u \in K(C)$ quasi-integral on an infinite set $\mathfrak{M}$ of K-rat. places of C. In particular $\exists$ no infinite quasi-integral set of K-rat. pts. on C.

Proof -

① assume u is quasi-integral on $\mathfrak{M}$, $\mathfrak{p}$ a pole of u. By extending K, we assume $\mathfrak{p}$ is K-rat., and by R.R. we obtain an equation $y^2 = c_0(x-c_1)(x-c_2)(x-c_3)$ where c_1, c_2, c_3 are distinct alg. nos., x has a pole of order 2 at $\mathfrak{p}$, y has a pole of order 3 at $\mathfrak{p}$, and neither has any other poles. The divisors $(x-c_i) = \frac{\mathfrak{p}_i^2}{\mathfrak{p}^2}$ for $i = 1,2,3$ may be assumed to consist of K-rat. primes (by extending K again).

② since $E(\mathfrak{p},\mathfrak{q})$ is finitary for $\mathfrak{q} \in \mathfrak{M}$, we apply Thm. 2 to conclude that the values $\sqrt{(x-c_1)(\mathfrak{q})}$, $\sqrt{(x-c_2)(\mathfrak{q})}$, $\sqrt{(x-c_3)(\mathfrak{q})}$ for $\mathfrak{q} \in \mathfrak{M}$, are quasi-integral in some finite ext. L/K. Call these functions $\sqrt{\varphi(\mathfrak{q})}$, $\sqrt{\psi(\mathfrak{q})}$, $\sqrt{\chi(\mathfrak{q})}$ respectively.

③ Consider the function field $L(C)(\sqrt{\varphi}, \sqrt{\psi}, \sqrt{\chi})$ which we call $K^*(C^*)$. Each place of $K(C)$ gives rise to a finite set of places of $K^*(C^*)$ and from these we choose one corresponding to $\forall$ place of $\mathfrak{M}$, thus obtaining an infinite set $\mathfrak{M}^*$ of L-rat. places of $K^*(C^*)$ on which the functions $\rho = \sqrt{\varphi} + \sqrt{\psi}$, $\sigma = \sqrt{\varphi} + \sqrt{\chi}$, $\tau = \sqrt{\psi} - \sqrt{\chi}$ are quasi-integral. It is surprising, but easy to see that the zeros and poles of ρ, σ and τ are all among the poles of x, where x is regarded as a function of $K^*(C^*)$.

Thus, the functions $\frac{\rho}{\tau}$, $\frac{\sigma}{\tau}$ satisfy the hypotheses of Theorem 2 with the integer ℓ arbitrary. We conclude that $\left\{\frac{\rho}{\tau}(\mathfrak{q}^*)\right\}^{\frac{1}{\ell}}$, $\left\{\frac{\sigma}{\tau}(\mathfrak{q}^*)\right\}^{\frac{1}{\ell}}$ are quasi-integral nos. in some fixed field ext. K_ℓ of K, for $\mathfrak{q}^* \in \mathfrak{M}^*$.

note - $\frac{f}{T}$ and $\frac{g}{T}$ are finitary on M^*, but since they are functions, their values on M^* must differ by infinitely many units. Thus, we will be done if we can show that $\frac{f}{T} - \frac{g}{T} = 1 = \xi^l - \eta^l$ $(\xi, \eta \in K_l)$ has only finitely many quasi-integral solutions in K_l. The argument, which we put below, uses the Thue-Siegel-Roth Thm. and has some additional consequences which we will examine in the lecture following.

an application of the Thue-Siegel-Roth

We need - if $f(x,y)$ is a form with coeffics. in K, $a \neq 0$, then $f(x,y) = a$ has only finitely many solutions in $\mathcal{O}_K \times \mathcal{O}_K$ if $f(x,y)$ has at least 3 distinct linear factors.

Proof -

With no loss (by transforming $x \to x'$, $y \to y'$ by transforms. of the inhomogeneous unimodular gp.), we may assume $x - \alpha_1 y$, $x - \alpha_2 y$, $x - \alpha_3 y$ are the distinct linear factors. Enlarge K to contain $\alpha_1, \cdots, \alpha_n$. We easily obtain the identity $(\alpha_3 - \alpha_2)\left(\frac{x-\alpha_1 y}{x-\alpha_3 y}\right) - (\alpha_3 - \alpha_1)\left(\frac{x-\alpha_2 y}{x-\alpha_3 y}\right) = \alpha_1 - \alpha_2$. Suppose there are infinitely many solutions (x_0, y_0). Since $f(x,y)$ is a form, there are only finitely many non-associated nos. $\frac{x_0 - \alpha_1 y_0}{x_0 - \alpha_3 y_0}$, $\frac{x_0 - \alpha_2 y_0}{x_0 - \alpha_3 y_0}$ because $(x_0 - \alpha_i y_0) \mid a$ for $i = 1, 2, 3$. Excuse me, I forgot to include the fact that we may suitably modify a, and α_i's so that all of these are algebraic integers.

Thus, for any fixed integer n, $\exists$ ρ_1, ρ_2 $\ni$

$$\frac{x_0 - \alpha_1 y_0}{x_0 - \alpha_3 y_0} = \rho_1 \epsilon_1^n, \quad \frac{x_0 - \alpha_2 y_0}{x_0 - \alpha_3 y_0} = \rho_2 \epsilon_2^n \text{ for } \infty\text{-many}$$

(x_0, y_0) and ϵ_1, ϵ_2 units of K.

We will have a contradiction if we can show that an equation $\boxed{\beta_1 \epsilon_1^n - \beta_2 \epsilon_2^n = \beta_3}$, $\beta_3 \neq 0$ has only finitely many solutions $\epsilon_1, \epsilon_2 \in \mathcal{O}_K$ for some large integer n.

Note - The equation in the box differs from the equation in the last part of the proof of Theorem 3, in that as k changes, the field K_k in which we are obtaining solutions for the latter also changes.

Argument -

Write $\boxed{B_1 X^n - B_2 Y^n = B_3}$ in the form

$\prod_1^n (\lambda_i - \frac{x}{y}) = \frac{c}{y^n}$, and let $h = [K:\mathbb{Q}]$. Then the solutions $\frac{x_0}{y_0}$ have $H(\frac{x_0}{y_0}) \leq (2M)^h$ where $M = \max(|\bar{\lambda}|, |\bar{\mu}|)$

H denotes height, $\bar{|}$ the max. of abs. value of the conjugates. Since the λ_i are distinct, for fixed large n, $\exists$ a constant C_1, and a subsequence $\{\frac{x_0}{y_0}\} \to \alpha_1$ (say), so that $\left|\prod_2^n (\lambda_i - \frac{x_0}{y_0})\right| > C_1$. Assume the λ_i's are in K. Then if necessary we may apply an isomorphism of K to the equation in the box so that we may assume $M = |y_0|$ for some infinite subsequence of $\{\frac{x_0}{y_0}\}$. If it may also be necessary to interchange x and y in the argument.

Thus we obtain;

$|\alpha_1 - \frac{x_0}{y_0}| C_1 < \frac{C}{M^n}$. But, by T-S-R, $|\alpha_1 - \frac{x_0}{y_0}| > \frac{1}{(H(\frac{x_0}{y_0}))^{2+\epsilon}}$ for all but finitely many (x_0, y_0). Therefore,

$\frac{1}{M^{2h+\epsilon'}} < \frac{C_2}{M^n}$ for some constant C_2. If $n > 2h$, this is a contradiction for large M. Q.E.D.

Genus Zero Curves

Lemma 4 - Suppose C is of genus zero, given by the equation $f(x,y) = 0$ having coeffics. in K ($[K:\mathbb{Q}] < \infty$). If $\exists$ a pt. $(\xi, \eta) \in K \times K$ $\ni$ (ξ, η) is not a singular pt. (i.e. y is a single-valued function of x in a nbd. of this pt.) then: $\exists$ a uniformization $x = F(t)$, $y = G(t)$, $t = H(x,y)$ of C with F, G, H rat. functions with coeffics. in K.

Proof -

① $x = F(t)$, $t = H(x,y) \Rightarrow t$ is a single-valued function of x in a nbd. of (ξ,η). assume, without loss, that (ξ,η) is not a branch pt. of the curve, so that y is a power series in x with coeffics. in K (expansion about (ξ,η)), and t is a power series in x with coefficients in L, where $[L:K] < \infty$. since x and t are one-one in a nbd. of (ξ,η), $\left(\frac{dt}{dx}\right)_{(\xi,\eta)} \neq 0$; so $\exists\ a, b \in \bar{\Phi} \ni t' = at + b$ satisfies $\left(\frac{dt'}{dx}\right)_{(\xi,\eta)} = 1$, $t'_{(\xi,\eta)} = 0$. If $t'' = \frac{t'}{1+Ct'}$ where $C = \frac{1}{2}\frac{d^2t'}{dx^2}\Big|_{\xi,\eta}$ we may in addition assume $\frac{d^2t}{dx^2}\Big|_{(\xi,\eta)} = 0$.

② If $\sigma : L/K \to \mathbb{C}$, then $x = F^{(\sigma)}(t^{(\sigma)})$, $y = G^{(\sigma)}(t^{(\sigma)})$ and $t^{(\sigma)} = H^{(\sigma)}(x,y)$ (here x is indeterminate, and $t^{(\sigma)}$ = power series obtained by applying σ to the coefficients of the power series for t in x). Note - $y^{(\sigma)} = y$ since coeffics. of power series for y are in K. since $f^{(\sigma)}(x,y) = f(x,y)$, $t^{(\sigma)}$ gives us a new uniformization of $K(C)$, and therefore $t^{(\sigma)}$ arises from t by a linear transformation. However, since $\frac{dt^{(\sigma)}}{dx}\Big|_{(\xi,\eta)} = 1$, $t^{(\sigma)}\Big|_{(\xi,\eta)} = 0$ and $\frac{d^2t^{(\sigma)}}{dx^2}\Big|_{(\xi,\eta)} = 0$, we see that $t^{(\sigma)} = t$.

Therefore, the equations $x = \frac{1}{n}\sum_{\sigma} F^{(\sigma)}(t)$, $y = \frac{1}{n}\sum_{\sigma} G^{(\sigma)}(t)$, $t = \frac{1}{n}\sum_{\sigma} H^{(\sigma)}(x,y)$ provide a uniformization of C with coeffics. in K. Q.E.D.

If $f(x,y) \in \mathcal{O}_K[x,y]$, we may write our uniformization in the form :

$x = \frac{\phi(u,v)}{\chi(u,v)}$, $y = \frac{\psi(u,v)}{\chi(u,v)}$, $\frac{u}{v} = \frac{H_1(x,y)}{H_2(x,y)}$ where $\phi, \psi, \chi \in \mathcal{O}_K[u,v]$ are forms of the same degree ; $H_1, H_2 \in \mathcal{O}_K[x,y]$. Divide ϕ, ψ, χ by suitable powers of v to obtain 3

some $P_1, Q_1, R_1 \in \mathcal{O}_K[u,v]$

① $P_1\phi + Q_1\psi + R_1\chi = a_1 v^r$, $a_1 \in \mathcal{O}_K$.

similarly, for some polynoms. $P_2, Q_2, R_2 \in \mathcal{O}_K[u,v]$

② $P_2\phi + Q_2\psi + R_3\chi = a_2 u^r$ (where we define P, Q, R's properly so that the exponents of u and v are the same).

Let $A_1, \cdots, A_s$ be ideals representing the distinct classes of the ideal class group G. If we put $L = K(g_1^{\frac{1}{s}}, \cdots, g_s^{\frac{1}{s}})$ where $A_i^s = (g_i)$ (from Fermat's Theorem, an element of a gp. to the exponent of the order of the gp. is the identity), then from the fact that fract. ideals of L form a free abelian gp., we see that every fract. ideal of K is principal in L. If $\bar{x}, \bar{y} \in K$, then $\bar{u}, \bar{v}$ may be chosen in $\mathcal{O}_K$. The ideal $(\bar{u}, \bar{v})$ becomes (δ) in L for some $\delta \in L$.

Suppose $\exists$ c independent of $\bar{x}$ and $\bar{y}$ $\ni$ $c\bar{x}, c\bar{y} \in \mathcal{O}_K$. By our uniformization above, $\chi\left(\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right) \mid c\phi\left(\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right)$, $\chi\left(\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right) \mid c\psi\left(\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right)$ ($\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}$ are both integers in L). From equations ① and ② and $\left[\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right] = 1$, we conclude that ③ $\boxed{\chi\left(\frac{\bar{u}}{\delta}, \frac{\bar{v}}{\delta}\right) = \gamma}$ where $\gamma \in \mathcal{O}_L$ divides $c a_1, a_2$.

<u>Theorem 4</u> - Let C be a curve of genus 0 with irred. equat. $f(x,y) = 0$ having coeffics. in an alg. no. field K. Then $\exists$ an alg. no. field $L \ni f(x,y) = 0$ has an infinite L-<u>quasi-integral</u> set of solutions $(\bar{x}, \bar{y})$ $\Leftrightarrow$ $f = 0$ has a rational parametrization $x = P(t)$, $y = Q(t) \in K(t, \frac{1}{t})$.

<u>Proof</u> -

① If $\chi(u,v)$ has 3 or more distinct linear factors, then our application of T-S-R on pg. (15b) shows there can be only finitely many $(\bar{u}, \bar{v})$ in $\mathcal{O}_K \times \mathcal{O}_K$.

② If χ has at most two distinct linear factors, then x or y become infinite for at most two values of $t = \frac{u}{v}$. Send these by lin. fract. trans. to 0 and ∞, so x and y have the desired form. Let L be any finite ext. of K which contains the coefficients of $P(t), Q(t)$ and also infinitely many units. As t ranges over the units of L, we obtain an infinite L-quasi-int. set of solutions

Heuristic Outline of the Proof of Siegel's Theorem

If $X \in K(C)$ is a function which is quasi-integral on an infinite set of K-rat. places M, then Siegel's fundamental inequalities tell us that we may assume that M has a limit pt. $\mathfrak{P}$ on the R.S. for $C \ni X(\mathfrak{P}) = \infty$. Thus, $\mathfrak{P}$ is an algebraic place. If $\Phi \in K(C)$, $\Phi(\mathfrak{P}) \neq \infty$, then the numbers $\Phi(\mathfrak{p}) \in K$ for $\mathfrak{p} \in M$ approach the algebraic no. $\Phi(\mathfrak{P})$. This is a natural set up for the T-S-R theorem, for if we knew that the nos. $\Phi(\mathfrak{p})$ approached $\Phi(\mathfrak{P})$ 'too quickly' we would then contradict the fact that $\Phi(\mathfrak{P})$ is algebraic. The heart of the proof amounts to showing that there exists a function field containing $K(C)$, and a function Φ in this new function field $\ni$ the places of M lift to K-rat. places of this new function field' (using Nadell-Weil thm) and such that in this new setting we do get the desired contradiction.

Lang in his book Diophantine Geometry manages to dispense with much of the finagling with different functions and eliminates the use of theta functions in his computations altogether. This has a certain advantage because their use in the Siegel theorem is very special, and it was Siegel's deep investigations of quadratic forms that made him such an expert on the properties of theta functions.

Instead, Lang normalizes his curves, assumes they are projective and defines height on the places of the curve directly by embedding them in projective space (our curve is already in projective space, but may be singular). After proving a very deep theorem to the effect that our height functions for different embeddings in projective space are much the

some,* Lang reformulates the T-S-R theorem in terms of the hts. of K-rat. places approaching the ht. of an alg. place on the curve. He then forms the n-division function field by pulling back from the curve a translation of the isogony, multiplication by n, on the Jacobian variety ~~variety~~. The translation being selected in particular so that an infinite subsequence of M pulls back to 'K-rat places' on the n-division curve (' ' just to annoy anybody whose forgotten we may have to take a finite extension of L). From the previously mentioned property of ht. Lang deduces immediately that the height of a pt. on the n-div. curve (embedded in the Jacobian) after multiplication by n is bounded by the n^2 power of the height before multiplication by n. For large n this immediately gives Lang a contradiction to his ~~geometric~~ formulation of the Thue-Siegel-Roth Thm. Lang uses this same property of ht. to prove the infinite descent for Mordell-Weil theorem, and the finiteness of Pic_{V}, and in addition as he does not, as Siegel had to, worry about the degree of the covering of the n-div. function field over C. However, Lemma 2, Lemma 3 of pg. 67 of D.G. while short, require some tools that are both hard and not ~~well~~-known (and to my knowledge not easily accessible). A rather deep ampleness criteria from Weil's Foundations, and some knowledge of the Picard varieties 'functorial properties' being among these tools.

* Quasi-equivalent to Lang.