AN ARITHMETIC THEORY OF ADJOINT PLANE CURVES

BY

DANIEL GORENSTEIN

Introduction. In classical algebraic geometry the adjoint curves to an irreducible plane curve are an essential tool in the study of the geometry on the curve. In this paper we shall give an algebro-arithmetic development of the theory of adjoint curves, and shall extend the classical results to irreducible plane curves with arbitrary singularities defined over arbitrary ground fields. Our definition of the adjoint condition at a given singular point of the curve is stated in terms of the conductor between the local ring of the point and its integral closure. The fundamental properties of the adjoint curves are then derived from corresponding properties of the conductor.

The single deepest and most important property of the adjoint curves is that, on a curve of order m, the adjoint curves of order $m-3$ cut out the complete canonical series. This property is equivalent to the fact that the degree of the fixed component of the adjoint series is *twice* the number of conditions which the adjoint curves impose on the curves of sufficiently high order[1]. We shall give two distinct and independent proofs of this proposition.

The first proof is a direct one, based upon a detailed analysis of the singularities of the given curve. This analysis, to which part I is devoted, applies equally well to algebraic number fields, and our treatment will include this case with that of algebraic function fields of one variable.

The second proof is more indirect, depending upon the Riemann-Roch theorem and a generalization of the classical representation theorem of the differentials of the first kind. This proof, which will be given in part II, holds only for plane curves whose function field is separably generated over the ground field.

PART I. LOCAL ANALYSIS OF THE SINGULARITIES

1. Algebraic preliminaries. In this section we shall develop the basic notation and results necessary for the local theory. The notation we establish will be valid simultaneously for algebraic number fields and algebraic function fields of one variable. Let $\mathfrak{o}_0$ be either the ring I of ordinary integers or the

---

[1] For example, an adjoint curve to a curve with ordinary multiple points $P_1, P_2, \cdots, P_s$ of multiplicities $r_1, r_2, \cdots, r_s$ respectively is one which has an (r_i-1)-fold point at each P_i. In this case, the degree of the fixed component is $\sum_{i=1}^{s} r_i(r_i-1)$, while the number of conditions which the adjoint curves impose on the curves of sufficiently high degree is $\sum_{i=1}^{s} r_i(r_i-1)/2$.

ring $k[X]$ of polynomials in an indeterminate X with coefficients in an arbitrary field k. Let $F(Y) \in o_0[Y]$ be irreducible and let y be a root of $F(Y) = 0$. Call $o_0[Y]$, $o_0[y]$ respectively $\mathfrak{O}$ and o. If K denotes the quotient field of o, K is an algebraic number field or an algebraic function field of one variable according as o_0 is I or $k[X]$.

If $\mathfrak{p}$ is a maximal ideal in o, let $o_\mathfrak{p}$ be the ring of quotients of o with respect to $\mathfrak{p}$. If $\mathfrak{p}_0 = \mathfrak{p} \cap o_0$, denote by $o_{\mathfrak{p}_0}$ the quotient ring of o_0 with respect to $\mathfrak{p}_0$. $o_\mathfrak{p}$ and $o_{\mathfrak{p}_0}$ are local rings and, moreover, the completion $o_{\mathfrak{p}_0}^*$ of $o_{\mathfrak{p}_0}$ is a subring and subspace of the completion $o_\mathfrak{p}^*$ of $o_\mathfrak{p}$.

It is well known that there exists at least one and at most a finite number of valuation rings R_i of K, $i = 1, 2, \cdots, r$, which contain $o_\mathfrak{p}$ (compare Chevalley [2, Chapter I, Theorem 1 and Lemma 1](2)). If $\bar{o}_\mathfrak{p}$ denotes the integral closure of $o_\mathfrak{p}$ in K, it follows readily that $\bar{o}_\mathfrak{p} = \bigcap_{i=1}^{r} R_i$. Let $\mathfrak{m}_i$ be the ideal of nonunits in R_i, $i = 1, 2, \cdots, r$, and let $\mathfrak{m}_i' = \mathfrak{m}_i \cap \bar{o}_\mathfrak{p}$. Then $\mathfrak{m}_i' \neq \mathfrak{m}_j'$, $i \neq j$, $\mathfrak{m}_i' \cap o_\mathfrak{p} = \mathfrak{p} o_\mathfrak{p}$ for all $i, j = 1, 2, \cdots, r$, and the $\mathfrak{m}_i'$ are the only ideals in $\bar{o}_\mathfrak{p}$ which contract to $\mathfrak{p} o_\mathfrak{p}$ in $o_\mathfrak{p}$ (Zariski [12, p. 511]). It follows that $\mathfrak{m}_1', \mathfrak{m}_2', \cdots, \mathfrak{m}_r'$ are the only ideals in $\bar{o}_\mathfrak{p}$ which are distinct from the zero or unit ideals, whence $\bar{o}_\mathfrak{p}$ is a semi-local ring in the sense of Chevalley. Since evidently R_i is the ring of quotients of $\bar{o}_\mathfrak{p}$ with respect to $\mathfrak{m}_i'$, $i = 1, 2, \cdots, r$, Proposition 8 of Chevalley [1, p. 700] implies that the completion $\bar{o}_\mathfrak{p}^*$ of the semi-local ring $\bar{o}_\mathfrak{p}$ is isomorphic to the direct sum of the completions R_i^* of R_i:

$$(1) \qquad \bar{o}_\mathfrak{p}^* \cong \sum_{i=1}^{r} R_i^*.$$

On the other hand, let $\mathfrak{P}$ be the maximal ideal in $\mathfrak{O}$ whose residue (mod $F(Y)$) is $\mathfrak{p}$. Then $o_{\mathfrak{p}_0}^*$ can also be regarded as a subring and subspace of the completion $\mathfrak{O}_\mathfrak{P}^*$ of $\mathfrak{O}$ with respect to $\mathfrak{P}$. $\mathfrak{O}_\mathfrak{P}^*$ is a complete regular ring of dimension 2, and as such is a unique factorization domain (Cohen [4, Theorem 18]). The following relation exists between $\mathfrak{O}_\mathfrak{P}^*$ and $o_\mathfrak{p}^*$ (Chevalley [1, Proposition 5, p. 699]):

$$(2) \qquad o_\mathfrak{p}^* \cong \mathfrak{O}_\mathfrak{P}^* / \mathfrak{O}_\mathfrak{P}^* F(Y).$$

Let $F(Y) = \prod_{i=1}^{n} F_i^*$ be a factorization of $F(Y)$ into irreducible elements of $\mathfrak{O}_\mathfrak{P}^*$, in which each factor F_i^* is a nonunit in $\mathfrak{O}_\mathfrak{P}^*$. It is known that the zero ideal in $o_\mathfrak{p}^*$ is the intersection of prime ideals (Zariski [13, p. 356]). This implies, together with (2), that $F_i^* \neq F_j^*$, $i \neq j$. Define $o_j^* = \mathfrak{O}_\mathfrak{P}^* / F_j^*$, $j = 1, 2, \cdots, h$. Then each o_j^* is itself a complete local domain. Moreover, the natural homomorphism of $\mathfrak{O}_\mathfrak{P}^*$ on o_j^* maps $o_0[Y]$ onto a subring of o_j^* which is isomorphic to o. Thus if Σ_j^* denotes the quotient field of o_j^*, we may identify K with a subfield of Σ_j^*, $j = 1, 2, \cdots, h$. It can be further shown, by using

---

(2) Numbers in brackets refer to the bibliography at the end of the paper.

Hensel's lemma (Cohen [4, Theorem 4]), that $\mathfrak{o}_\mathfrak{p}$ is then identified with a subring and subspace of $\mathfrak{o}_j^*$. Since the integral closure $\bar{\mathfrak{o}}_j^*$ of $\mathfrak{o}_j^*$ in Σ_j^* is a complete discrete rank 1 valuation ring, its contraction $\bar{\mathfrak{o}}_j^* \cap K$ is a valuation ring of K containing $\mathfrak{o}_\mathfrak{p}$. It follows readily that each $\bar{\mathfrak{o}}_j^*$ is isomorphic to one of the complete valuation rings R_i^*, and that distinct $\bar{\mathfrak{o}}_j^*$ correspond to distinct R_i^*. We therefore conclude that $h \leq r$.

Conversely, $\mathfrak{o}_{\mathfrak{p}}^*{}_0$ can be identified with a subring and subspace of R_i^*, $i = 1, 2, \cdots, r$. Since $F(Y) = 0$ in $\mathfrak{o}_\mathfrak{p}$, this implies that some $F_j^* = 0$ in R_i^*, whence it can be seen that R_i^* is isomorphic to the corresponding complete valuation ring $\bar{\mathfrak{o}}_j^*$. Thus $r = h$, and for a suitable ordering of the indices $R_i^* = \bar{\mathfrak{o}}_i^*$, $i = 1, 2, \cdots, r$.

Let Σ_0^* be the quotient field of $\mathfrak{o}_{\mathfrak{p}}^*{}_0$. To simplify the exposition, we shall identify K and Σ_0^* with their isomorphic images in Σ_i^*, shall identify $\bar{\mathfrak{o}}_i^*$ with R_i^*, $i = 1, 2, \cdots, r$, and shall identify $\bar{\mathfrak{o}}_\mathfrak{p}^*$ with $\sum_{i=1}^r R_i^*$. With this identification each Σ_i^* is a finite algebraic extension of Σ_0^*. Since F_i^* and F_j^* are relatively prime in $\mathfrak{O}_\mathfrak{P}^*$, $i \neq j$, it can be further shown that $\mathfrak{O}_\mathfrak{P}^*/\mathfrak{O}_\mathfrak{P}^* F(Y) \cong \sum_{i=1}^r \mathfrak{O}_\mathfrak{P}^*/\mathfrak{O}_\mathfrak{P}^* F_i^*$, whence $\mathfrak{o}_\mathfrak{p}^* \cong \sum_{i=1}^r \mathfrak{o}_i^*$ in view of (2). We see then that $\mathfrak{o}_\mathfrak{p}^*$ is identified in a natural way with a subring and subspace of $\bar{\mathfrak{o}}_\mathfrak{p}^*$.

Let v_i, v_i^* be the valuations whose corresponding valuation rings are respectively R_i and R_i^*, $i = 1, 2, \cdots, r$. We shall say that v_i or v_i^* has center $\mathfrak{p}$ in $\mathfrak{o}$.

Every element $z \in \mathfrak{o}_\mathfrak{p}^*$ (or $\bar{\mathfrak{o}}_\mathfrak{p}^*$) has a unique representation of the form $z = \sum_{i=1}^r z_i$, $z_i \in R_i^*$. We define $v_i^*(z) = v_i^*(z_i)$, $i = 1, 2, \cdots, r$. With this convention, we shall call $\mathfrak{q}^* \subset \mathfrak{o}_\mathfrak{p}^*$ (or $\bar{\mathfrak{o}}_\mathfrak{p}^*$) a valuation ideal or simply a v_i^*-ideal if $z \in \mathfrak{o}_\mathfrak{p}^*$ (or $\bar{\mathfrak{o}}_\mathfrak{p}^*$), $v_i^*(z) \geq v_i^*(\mathfrak{q}^*)$, implies $z \in \mathfrak{q}^*$. We also agree to call the intersection of v_i-ideals, $i = 1, 2, \cdots, r$, in $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{p}$, or $\bar{\mathfrak{o}}_\mathfrak{p}$, or the intersection of v_i^*-ideals, $i = 1, 2, \cdots, r$, in $\mathfrak{o}_\mathfrak{p}^*$ or $\bar{\mathfrak{o}}_\mathfrak{p}^*$ a complete $\mathfrak{p}$-ideal in its respective ring. In the one-one correspondence between the primary ideals in $\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}^*$ the complete $\mathfrak{p}$-ideals correspond in a natural way: $\mathfrak{q}$, $\mathfrak{q}^*$ correspond if and only if $v_i^*(\mathfrak{q}^*) = v_i(\mathfrak{q})$, $i = 1, 2, \cdots, r$.

Let $k_0 = \mathfrak{o}_0/\mathfrak{p}_0$; k_0 is either the prime field with $\mathfrak{p}_0$ elements or a finite extension of k. If $k(\mathfrak{p}) = \mathfrak{o}/\mathfrak{p}$, $k(\mathfrak{p})$ is a finite extension of k_0. We define the degree $d_\mathfrak{p}$ of $\mathfrak{p}$ to be, on the one hand, the number of elements in $k(\mathfrak{p})$ or, on the other hand, $[k(\mathfrak{p}):k]$. Furthermore the residue field Δ_i of R_i (or of R_i^*, since their residue fields are isomorphic) is in turn a finite extension of $k(\mathfrak{p})$, $i = 1, 2, \cdots, r$. We define the degree d_i of v_i (or v_i^*) to be the number of elements in Δ_i or $[\Delta_i:k]$, as the case may be.

Let $\mathfrak{q}' \subset \mathfrak{q}$ be zero-dimensional primary ideals in any one of the rings considered above (including $\mathfrak{O}$ and $\mathfrak{O}_\mathfrak{p}^*$). We allow $\mathfrak{q} = (1)$. The additive group of the ring $\mathfrak{q}/\mathfrak{q}'$ can be regarded in a natural way as a finite-dimensional vector space over k_0, and in the algebraic function field case, a fortiori, as a vector space over k. We define then dim $\mathfrak{q}/\mathfrak{q}'$ to be the dimension of this vector space over k. In the alternative case, we define dim $\mathfrak{q}/\mathfrak{q}'$ to be the

total number of elements in $\mathfrak{q}/\mathfrak{q}'$. We also say a given set of elements of $\mathfrak{q}$ are linearly independent modulo $\mathfrak{q}'$ if, on the one hand, their residues are linearly independent over k or, on the other hand, are distinct elements of $\mathfrak{q}/\mathfrak{q}'$.

The notion of the degree $d(\mathfrak{q})$ of a valuation ideal or complete $\mathfrak{p}$-ideal $\mathfrak{q}$ will be of considerable importance in the sequel. We define $d(\mathfrak{q}) = d_i v_i(\mathfrak{q})$ or $d(\mathfrak{q}) = \sum_{i=1}^r d_i v_i(\mathfrak{q})$ according as $\mathfrak{q}$ is a v_i-ideal or complete $\mathfrak{p}$-ideal in $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{p}$, or $\bar{\mathfrak{o}}_\mathfrak{p}$; and define $d(\mathfrak{q}) = d_i v_i^*(\mathfrak{q})$ or $d(\mathfrak{q}) = \sum_{i=1}^r d_i v_i^*(\mathfrak{q})$ according as $\mathfrak{q}$ is a v_i^*-ideal or complete $\mathfrak{p}$-ideal in $\mathfrak{o}_\mathfrak{p}^*$, $\bar{\mathfrak{o}}_\mathfrak{p}^*$, $\mathfrak{o}_i^*$, or R_i^*.

If $\mathfrak{q}' \subset \mathfrak{q}$ are each v_i-ideals, v_i^*-ideals, or complete $\mathfrak{p}$-ideals, it is easily verified that $\dim \mathfrak{q}/\mathfrak{q}' \leq d(\mathfrak{q}') - d(\mathfrak{q})$. Moreover, it is a direct consequence of the independence of places that $\dim \mathfrak{q}/\mathfrak{q}' = d(\mathfrak{q}') - d(\mathfrak{q})$ if $\mathfrak{q}$, $\mathfrak{q}'$ are valuation ideals or complete $\mathfrak{p}$-ideals in any one of the integrally closed rings $\bar{\mathfrak{o}}_\mathfrak{p}$, $\bar{\mathfrak{o}}_\mathfrak{p}^*$, R_i^*, and hence, in particular, that $d(\mathfrak{q}) \leq \dim (1)/\mathfrak{q}$.

For valuation ideals or complete $\mathfrak{p}$-ideals in $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}^*$, or $\mathfrak{o}_i^*$, we shall also introduce the integer $\delta(\mathfrak{q}) = \dim (1)/\mathfrak{q}$. Thus $\delta(\mathfrak{q}) \leq d(\mathfrak{q})$. We shall see in part II that this integer has a special geometric significance. If $\mathfrak{q}' \subset \mathfrak{q}$ is also a v_i-ideal, v_i^*-ideal, or complete $\mathfrak{p}$-ideal in $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}^*$, or $\mathfrak{o}_i^*$, as the case may be, we have $\dim \mathfrak{q}/\mathfrak{q}' = \dim (1)/\mathfrak{q}' - \dim (1)/\mathfrak{q}$, whence

$$(3) \qquad \dim \mathfrak{q}/\mathfrak{q}' = \delta(\mathfrak{q}') - \delta(\mathfrak{q}) \leq d(\mathfrak{q}') - d(\mathfrak{q}).$$

This inequality leads finally to the concept of a *regular ideal*.

DEFINITION. A v_i-ideal, v_i^*-ideal, or complete $\mathfrak{p}$-ideal $\mathfrak{q}$ in $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}^*$, or $\mathfrak{o}_i^*$ is called a regular ideal if, for any v_i-ideal, v_i^*-ideal, or complete $\mathfrak{p}$-ideal $\mathfrak{q}' \subset \mathfrak{q}$, we have

$$(4) \qquad \delta(\mathfrak{q}') - \delta(\mathfrak{q}) = d(\mathfrak{q}') - d(\mathfrak{q}).$$

2. Some properties of the conductor.

THEOREM 1. *If $\mathfrak{C}_i^*$ is the conductor between R_i^* and $\mathfrak{o}_i^*$, $i = 1, 2, \cdots, r$, then $\mathfrak{C}_i^*$ is the largest regular ideal in $\mathfrak{o}_i^*$.*

Proof. To simplify the notation, we drop the subscript i. Let $z_0 \in \mathfrak{C}^*$, $v^*(z_0) = v^*(\mathfrak{C}^*)$. If $z \in R^*$ and $v^*(z) \geq v^*(\mathfrak{C}^*)$, then $v^*(z/z_0) \geq 0$, whence $z/z_0 \in R^*$. Thus $z = z_0(z/z_0) \in \mathfrak{C}^*$, whence $\mathfrak{C}^*$ is in fact a v^*-ideal.

Let $\mathfrak{q}^* \subset \mathfrak{C}^*$ be a v^*-ideal, and let $a = v^*(\mathfrak{q}^*) - v^*(\mathfrak{C}^*)$. If $\mathfrak{S}^*$ is the ideal in R^* of value a, $\dim R^*/\mathfrak{S}^* = da$. If ζ_j, $j = 1, 2, \cdots, da$ form a basis for R^* modulo $\mathfrak{S}^*$, the elements $z_0\zeta_j$ are in $\mathfrak{C}^*$ and are linearly independent modulo $\mathfrak{q}^*$, whence $\delta(\mathfrak{q}^*) - \delta(\mathfrak{C}^*) \geq ad$, while $\delta(\mathfrak{q}^*) - \delta(\mathfrak{C}^*) \leq ad$ by (3). We conclude that $\mathfrak{C}^*$ is a regular ideal in $\mathfrak{o}^*$.

We shall now show that for any regular ideal $\mathfrak{M}^*$ in $\mathfrak{o}^*$, $\mathfrak{M}^* \subset \mathfrak{C}^*$. It will suffice to prove:

$$(5) \qquad z \in R^*, \ v^*(z) \geq v^*(\mathfrak{M}^*) \quad \text{imply} \quad z \in \mathfrak{o}^*.$$

For if $z \in R^*$, $\phi \in \mathfrak{M}^*$, $v^*(z\phi) \geq v^*(\mathfrak{M}^*)$ whence $z\phi \in \mathfrak{o}^*$. Hence $\phi \in \mathfrak{C}^*$, and so $\mathfrak{M}^* \subset \mathfrak{C}^*$.

Let $z \in R^*$, $v^*(z) \geq v^*(\mathfrak{M}^*)$. Denote by $\{\mathfrak{q}_j^*\}$ the sequence of v^*-ideals in $\mathfrak{o}^*$; and let $v^*(z) = b$. We construct a sequence of elements $z_j \in \mathfrak{q}_{b+j}^*$, $j = 0, 1, 2, \cdots$, such that $v^*(z - \sum_{j=0}^{h} z_j) > v^*(\mathfrak{q}_{b+h}^*)$ for every integer h. Suppose z_j, $j = 0, 1, \cdots, h-1$, have been constructed. Since $\mathfrak{q}_{b+h}^* \subset \mathfrak{M}^*$, $\mathfrak{q}_{b+h}^*$ is itself a regular ideal, and so $\delta(\mathfrak{q}_{b+h+1}^*) - \delta(\mathfrak{q}_{b+h}^*) = d$. Let $t \in R^*$ with $v^*(t) = v^*(\mathfrak{q}_{b+h}^*)$. The previous equality implies at once that for any $\alpha \in \Delta$, there exists an element $\eta \in \mathfrak{q}_{b+h}^*$ such that the residue in Δ of η/t is α. It follows from this remark that we can find an element $z_h \in \mathfrak{q}_{b+h}^*$ such that $v^*([z - \sum_{j=0}^{h-1} z_j] - z_h) > v^*(t)$, whence $v^*(z - \sum_{j=0}^{h} z_j) > v^*(\mathfrak{q}_{b+h}^*)$, as asserted.

Since $\bigcap_{j=0}^{\infty} \mathfrak{q}_j^* = (0)$ and since $\mathfrak{o}^*$ is complete, it follows from Chevalley [1, Lemma 7, p. 695] that the series $\sum_{j=0}^{\infty} z_j$ is convergent in $\mathfrak{o}^*$ to an element z^*. Since by construction $v^*(z - z^*) = \infty$, $z - z^* = 0$, and hence $z \in \mathfrak{o}^*$, which proves (5).

On the basis of the preceding analysis, we prove two theorems concerning the conductor $\mathfrak{C}_\mathfrak{p}$ between $\bar{\mathfrak{o}}_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}$. The first theorem gives the complete structure of $\mathfrak{C}_\mathfrak{p}$, while the second gives a valuation-theoretic characterization of $\mathfrak{C}_\mathfrak{p}$.

THEOREM 2. *Let $\mathfrak{C}_\mathfrak{p}^*$ be the conductor between $\bar{\mathfrak{o}}_\mathfrak{p}^*$ and $\mathfrak{o}_\mathfrak{p}^*$, and let ω_i^* be the residue in $\mathfrak{o}_i^*$ of the elements $\prod_{j \neq i} F_j^*$, $i = 1, 2, \cdots, r$. Then*

$$\mathfrak{C}_\mathfrak{p}^* = \sum_{i=1}^{r} \mathfrak{C}_i^* \omega_i^*, \quad \mathfrak{C}_\mathfrak{p} = \mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p}, \quad and \quad \mathfrak{C}_\mathfrak{p}^* = \mathfrak{o}_\mathfrak{p}^* \mathfrak{C}_\mathfrak{p}.$$

THEOREM 3. *$\mathfrak{C}_\mathfrak{p}$ is the largest regular $\mathfrak{p}$-ideal in $\mathfrak{o}_\mathfrak{p}$.*

We prove both theorems simultaneously. Let $\Omega_i^* = \prod_{j \neq 1} F_j^*$, $i = 1, 2, \cdots, r$, and let Ω^* be the ideal $(\Omega_1^*, \Omega_2^*, \cdots, \Omega_r^*)$ in $\mathfrak{O}_\mathfrak{P}^*$. Since $\mathfrak{O}_\mathfrak{P}^* F(Y) = \bigcap_{i=1}^{r} \mathfrak{O}_\mathfrak{P}^* \Omega_i^*$, it is easily verified that $\Omega^* / \mathfrak{O}_\mathfrak{P}^* F(Y) = \sum_{i=1}^{r} \mathfrak{o}_i^* \omega_i^*$. In view of the identification of $\mathfrak{o}_\mathfrak{p}^*$ with a subring of $\bar{\mathfrak{o}}_\mathfrak{p}^*$, it follows that $\sum_{i=1}^{r} \mathfrak{o}_i^* \omega_i^* \subset \mathfrak{o}_\mathfrak{p}^*$ and hence also $\sum_{i=1}^{r} \mathfrak{C}_i^* \omega_i^* \subset \mathfrak{o}_\mathfrak{p}^*$. The first assertion of Theorem 2 thus has a meaning. In addition, it follows that $\overline{\mathfrak{C}}^* = \sum_{i=1}^{r} \mathfrak{C}_i^* \omega_i^*$ is an ideal in $\mathfrak{o}_\mathfrak{p}^*$ and, since $\overline{\mathfrak{C}}^*$ is manifestly the conductor between $\bar{\mathfrak{o}}_\mathfrak{p}^*$ and $\sum_{i=1}^{r} \mathfrak{o}_i^* \omega_i^*$, that $\overline{\mathfrak{C}}^* \subset \mathfrak{C}_\mathfrak{p}^*$. The proof that $\mathfrak{C}_\mathfrak{p}^* \subset \overline{\mathfrak{C}}^*$ depends upon two assertions:

(a) $\overline{\mathfrak{C}}^*$ is a regular ideal.

(b) No ideal containing $\overline{\mathfrak{C}}^*$ properly is a regular ideal.

Let $\mathfrak{q}^* \subset \overline{\mathfrak{C}}^*$ be a complete $\mathfrak{p}$-ideal in $\mathfrak{o}_\mathfrak{p}^*$. Denote by Ω_i^*, $i = 1, 2, \cdots, r$, the v_i^*-ideal in $\mathfrak{o}_i^*$ such that $v_i^*(\Omega_i^* \omega_i^*) = v_i^*(\mathfrak{q}^*)$. If $z \in \mathfrak{q}^*$, write $z = \sum_{i=1}^{r} z_i$, $z_i \in R_i^*$. If $\phi_i = z_i / \omega_i^*$, $i = 1, 2, \cdots, r$, $v_i^*(\phi_i) \geq v_i^*(\Omega_i^*) \geq v_i^*(\mathfrak{C}_i^*)$, whence $\phi_i \in \mathfrak{o}_i^*$, and, in fact, $\phi_i \in \Omega_i^*$. Thus $z = \sum_{i=1}^{r} \phi_i \omega_i^*$, and it follows that $\mathfrak{q}^* = \sum_{i=1}^{r} \Omega_i^* \omega_i^*$. In particular, this implies that $\overline{\mathfrak{C}}^*$ is a complete $\mathfrak{p}$-ideal.

Since, by Theorem 1, each $\mathfrak{C}_i^*$ is regular,

$$\delta(\mathfrak{Q}_i^*) - \delta(\mathfrak{C}_i^*) = d_i[v_i^*(\mathfrak{Q}_i^*) - v_i^*(\mathfrak{C}_i^*)], \qquad i = 1, 2, \cdots, r,$$

whence $\delta(\mathfrak{q}^*) - \delta(\overline{\mathfrak{C}}^*) = \sum_{i=1}^r d_i[v_i^*(\mathfrak{Q}_i^*) - v_i^*(\mathfrak{C}_i^*)] = d(\mathfrak{q}^*) - d(\overline{\mathfrak{C}}^*)$. Thus $\overline{\mathfrak{C}}^*$ is a regular ideal as asserted in (a).

Consider now the complete ideals $\mathfrak{A}_j^*$ in $\mathfrak{o}_\mathfrak{p}^*$ defined by the relations:

$$v_j^*(\mathfrak{A}_j^*) = v_j^*(\overline{\mathfrak{C}}^*) - 1, \quad v_k^*(\mathfrak{A}_j^*) = v_k^*(\overline{\mathfrak{C}}^*), \qquad k \neq j, j = 1, 2, \cdots, r.$$

If $\mathfrak{q}^* \supset \overline{\mathfrak{C}}^*$ properly is a complete $\mathfrak{p}$-ideal in $\mathfrak{o}_\mathfrak{p}^*$, $\mathfrak{q}^* \supset \mathfrak{A}_j^*$ for some j. To prove that $\mathfrak{q}^*$ is not a regular ideal, it is sufficient, in view of (3), to show that

$$(6) \qquad\qquad \delta(\overline{\mathfrak{C}}^*) - \delta(\mathfrak{A}_j^*) < d_j, \qquad\qquad j = 1, 2, \cdots, r.$$

For definiteness, take $j = 1$, and suppose $z \in \mathfrak{A}_1^*$. Write $z = \sum_{i=1}^r z_i$, $z_i \in R_i^*$. By assumption, $v_i^*(z_i) \geq v_i^*(\overline{\mathfrak{C}}^*) = v_i^*(\mathfrak{C}_i^* \omega_i^*)$, for all $i > 1$, whence $z_i \in \mathfrak{C}_i^* \omega_i^*$, $i > 1$. It follows that we can find an element $z' \in \overline{\mathfrak{C}}^*$ such that $z - z' = z_1$. If Z, Z' are representatives of z, z' in $\mathfrak{O}_\mathfrak{P}^*$, this implies that $Z - Z' = \Phi\Omega_1^*$, $\Phi \in \mathfrak{O}_\mathfrak{P}^*$. If ϕ is the residue of Φ in $\mathfrak{o}_\mathfrak{p}^*$, we conclude that $z \equiv \phi\omega_1^* \pmod{\overline{\mathfrak{C}}^*}$. This implies in turn that $\dim \mathfrak{A}_1^*/\overline{\mathfrak{C}}^* \leq \dim \mathfrak{q}_1^*/\mathfrak{C}_1^*$, where $\mathfrak{q}_1^*$ is the v_1^*-ideal in $\mathfrak{o}_1^*$ immediately preceding $\mathfrak{C}_1^*$. By Theorem 1, $\dim \mathfrak{q}_1^*/\mathfrak{C}_1^* = \delta(\mathfrak{C}_1^*) - \delta(\mathfrak{q}_1^*) < d_1$. This proves (6) and hence also (b).

Suppose now $z \in \mathfrak{C}_\mathfrak{p}^*$ and $z \notin \overline{\mathfrak{C}}^*$. Then for some i, say $i = 1$, $v_1^*(z) < v_1^*(\overline{\mathfrak{C}}^*)$. Define the complete $\mathfrak{p}$-ideals $\mathfrak{B}_1^*$, $\mathfrak{D}_1^*$ in $\overline{\mathfrak{o}}_\mathfrak{p}^*$, as follows:

$$v_1^*(\mathfrak{B}_1^*) = v_1^*(\overline{\mathfrak{C}}^*) - v_1^*(z) - 1, \quad v_i^*(\mathfrak{B}_1^*) = v_i^*(\overline{\mathfrak{C}}^*), \qquad i > 1;$$

$$v_1^*(\mathfrak{D}_1^*) = v_1^*(\overline{\mathfrak{C}}^*) - v_1^*(z), \quad v_i^*(\mathfrak{D}_1^*) = v_i^*(\overline{\mathfrak{C}}^*), \qquad i > 1.$$

There exist d_1 elements ψ_i, $i = 1, 2, \cdots, d_1$, in $\mathfrak{B}_1^*$ linearly independent modulo $\mathfrak{D}_1^*$. The d_1 elements $z\psi_i$, $i = 1, 2, \cdots, d_1$, are then in $\mathfrak{A}_1^*$ and are linearly independent modulo $\overline{\mathfrak{C}}^*$. Thus $\delta(\overline{\mathfrak{C}}^*) - \delta(\mathfrak{A}_1^*) = d_1$, in contradiction to (6). Therefore $\mathfrak{C}_\mathfrak{p}^* \subset \overline{\mathfrak{C}}^*$, which proves the first assertion of Theorem 2.

It follows from the one-one correspondence between the complete ideals in $\mathfrak{o}_\mathfrak{p}^*$ and $\mathfrak{o}_\mathfrak{p}$ that $\mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p}$ is a regular ideal, while for each $i = 1, 2, \cdots, r$, $\mathfrak{A}_i^* \cap \mathfrak{o}_\mathfrak{p}$ is not a regular ideal, and also that $\mathfrak{C}_\mathfrak{p}^* = \mathfrak{o}_\mathfrak{p}^*(\mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p})$. The argument which proved that $\mathfrak{C}_\mathfrak{p}^* \subset \overline{\mathfrak{C}}^*$ can now be repeated to show that $\mathfrak{C}_\mathfrak{p} \subset \mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p}$.

Conversely, if $z \in \mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p}$, $\eta \in \overline{\mathfrak{o}}_\mathfrak{p}$, $z\eta \in \mathfrak{o}_\mathfrak{p}^* \cap \overline{\mathfrak{o}}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$, whence $\mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p} \subset \mathfrak{C}_\mathfrak{p}$. Hence $\mathfrak{C}_\mathfrak{p}^* \cap \mathfrak{o}_\mathfrak{p} = \mathfrak{C}_\mathfrak{p}$, which completes the proof of Theorem 2.

To complete the proof of Theorem 3, it remains to show that every regular ideal in $\mathfrak{o}_\mathfrak{p}$ is contained in $\mathfrak{C}_\mathfrak{p}$. It will suffice to prove that if $\mathfrak{M}^*$ is a regular ideal in $\mathfrak{o}_\mathfrak{p}^*$, then $\mathfrak{M}^* \subset \mathfrak{C}_\mathfrak{p}^*$. Suppose $z \in \mathfrak{o}_\mathfrak{p}^*$ and $v_i^*(z) \geq v_i^*(\mathfrak{M}^*)$. Define an ordered sequence $\{\mathfrak{q}_m^*\}$ of complete $\mathfrak{p}$-ideals in $\mathfrak{o}_\mathfrak{p}^*$ by the relations: $v_i^*(\mathfrak{q}_m^*) = v_i^*(z) + m$, $i = 1, 2, \cdots, r$. Since $\mathfrak{q}_m^* \subset \mathfrak{M}^*$, $\mathfrak{q}_m^*$ is a regular ideal, $m = 0, 1, 2, \cdots, r$. It follows as in the proof of Theorem 1 that we can construct elements $z_m \in \mathfrak{q}_m^*$, $m = 0, 1, 2, \cdots$, such that, for each integer h, $v_i^*(z - \sum_{m=0}^h z_m) > v_i^*(\mathfrak{q}_{m+h}^*)$, $i = 1, 2, \cdots, r$. Since $\mathfrak{q}_{m+1}^* \subset \mathfrak{q}_m^*$, $\bigcap_{m=0}^\infty \mathfrak{q}_m^* = (0)$, and $\mathfrak{o}_\mathfrak{p}^*$ is complete, it follows again from Lemma 7, Chevalley [1, p. 695],

that the series $\sum_{m=0}^{\infty} z_m$ converges to an element of $\mathfrak{o}_\mathfrak{p}^*$, and hence that $z \in \mathfrak{o}_\mathfrak{p}^*$. We conclude at once that $\mathfrak{M}^* \subset \mathfrak{C}_\mathfrak{p}^*$. Q.E.D.

3. Semi-groups of positive integers. In order to establish a deeper property of the conductor, we must first consider certain arithmetic properties of integers which can be expressed in a specially designated way as a linear combination of n positive integers $b_1, b_2, \cdots, b_n$.

Let $\kappa_i = (b_1, b_2, \cdots, b_i)$, $i = 1, 2, \cdots, n$, and let $s_2, s_3, \cdots, s_n$ be another set of positive integers. We shall be interested in linear combinations of $b_1, b_2, \cdots, b_n$ with non-negative coefficients which for $i = 2, 3, \cdots, n$ are respectively $< s_i(\kappa_{i-1}/\kappa_i)$. An integer which can be written in this fashion will be called a *proper* combination of $b_1, b_2, \cdots, b_n$. We denote by $R_m(b_1, b_2, \cdots, b_n)$ the set of integers which can be expressed in *exactly* m distinct proper combinations of $b_1, b_2, \cdots, b_n$. For any integer c, if $c \in R_m(b_1, b_2, \cdots, b_n)$, we shall write $\chi(c) = m$.

We shall also have to consider linear combinations of $b_1, b_2, \cdots, b_n$ with *positive* coefficients which for $i = 2, 3, \cdots, n$ are respectively $\leq s_i(\kappa_{i-1}/\kappa_i)$. Such a linear combination of $b_1, b_2, \cdots, b_n$ will be called *proper*$^+$, and $R_m^+(b_1, b_2, \cdots, b_n)$ will denote the set of integers expressible in exactly m distinct proper$^+$ combinations of $b_1, b_2, \cdots, b_n$.

Let $d = \prod_{i=2}^n s_i$. We define two integers $\mu_d(b_1, b_2, \cdots, b_n), \nu_d(b_1, b_2, \cdots, b_n)$ which will be important in our considerations: $\mu_d(b_1, b_2, \cdots, b_n) = \sum_{i=2}^n s_i(\kappa_{i-1}/\kappa_i)b_i$, $\nu_d(b_1, b_2, \cdots, b_n) = \mu_d(b_1, b_2, \cdots, b_n) + 1 - \sum_{i=1}^n b_i$.

THEOREM 4. *Assume* $(b_1, \cdots, b_n) = 1$. *Then*
(a) *if* $c \geq \nu_d(b_1, \cdots, b_n)$, $c \in R_d(b_1, \cdots, b_n)$;
(b) $\nu_d(b_1, \cdots, b_n) - 1 \in R_{d-1}(b_1, \cdots, b_n)$;
(c) $\sum_{c=0}^{\nu_d(b_1, \cdots, b_n)-1} \chi(c) = 2^{-1}d \cdot \nu_d(b_1, \cdots, b_n)$.

Proof. We establish a sequence of shorter propositions which together will form the proof of the theorem.

(d) If $c > \mu_d(b_1, b_2, \cdots, b_n)$, then $c \in R_d^+(b_1, \cdots, b_n)$.

If $n = 2$, $(b_1, b_2) = 1$, $s_2 = d$. The relation $c - x_2 b_2 \equiv c - x_2' b_2 \pmod{b_1}$ implies $x_2 \equiv x_2' \pmod{b_1}$. It follows that $c - z_2 b_2 \equiv 0 \pmod{b_1}$ for some integer z_2 such that $1 \leq z_2 \leq b_1$. If $c > \mu_d(b_1, b_2) = db_1 b_2$, it follows that $c - (z_2 + rb_1)b_2$ is a positive multiple of b_1 for $r = 0, 1, 2, \cdots, d - 1$. On the other hand, if $c = y_1 b_1 + y_2 b_2$ is a proper combination of b_1, b_2, $y_2 = z_2 + rb_1$ for some $r = 0, 1, \cdots, d - 1$. Hence $c \in R_d^+(b_1, b_2)$.

We proceed by induction. Since $(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1}) = 1$, we can apply induction to these $n - 1$ integers. Observe also that $s_i(\kappa_{i-1}/\kappa_{n-1})/(\kappa_i/\kappa_{n-1}) = s_i(\kappa_{i-1}/\kappa_i)$, $i = 2, 3, \cdots, n - 1$, so that the upper bounds on the coefficients of $b_2/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1}$ are the same as those of $b_2, \cdots, b_{n-1}$.

Let $d' = \prod_{i=2}^{n-1} s_i$, so that $d = d' s_n$. Since $(\kappa_{n-1}, b_n) = 1$, $c - (z_n + r\kappa_{n-1})b_n \equiv 0 \pmod{\kappa_{n-1}}$ for some z_n such that $1 \leq z_n \leq \kappa_{n-1}$ and for $r = 0, 1, \cdots, s_n - 1$. Let $c_r = (c - (z_n + r\kappa_{n-1})b_n)/\kappa_{n-1}$, $r = 0, 1, \cdots, s_n - 1$. Now, by definition,

$\mu_d(b_1, b_2, \cdots, b_n) = \kappa_{n-1}\mu_{d'}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1}) + s_n\kappa_{n-1}b_n$. It follows from this equality that each $c_r > \mu_{d'}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1})$, since $c > \mu_d(b_1, b_2, \cdots, b_n)$. Hence by induction $c_r \in R_{d'}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1})$, $r = 0, 1, \cdots, s_n - 1$. Thus $c \in R_a(b_1, b_2, \cdots, b_n)$ with $a \geq s_n d' = d$. On the other hand, if $c - y_n b_n \equiv 0 \pmod{\kappa_{n-1}}$ with $0 < y_n \leq s_n\kappa_{n-1}$, $y_n = z_n + r\kappa_{n-1}$ for some $r = 0, 1, \cdots, s_n - 1$. We conclude that $c \in R_d^+(b_1, b_2, \cdots, b_n)$.

(e) If $c \geq \nu_d(b_1, b_2, \cdots, b_n)$, then $c \in R_d(b_1, b_2, \cdots, b_n)$.

In fact, if $c \geq \nu_d(b_1, b_2, \cdots, b_n)$, $c + \sum_{i=1}^n b_i > \mu_d(b_1, b_2, \cdots, b_n)$, whence, by (d), $c + \sum_{i=1}^n b_i \in R_d^+(b_1, b_2, \cdots, b_n)$. Thus $c \in R_d(b_1, b_2, \cdots, b_n)$.

(f) $\mu_d(b_1, b_2, \cdots, b_n) \in R_{d-1}^+(b_1, b_2, \cdots, b_n)$.

For the case $n = 2$, $\mu_d(b_1, b_2) = db_1b_2$. The representations of db_1b_2 are all of the form $db_1b_2 = (db_2 - rb_2)b_1 + (rb_1)b_2$, whence the proper$^+$ representations of db_1b_2 occur for $r = 1, 2, \cdots, d-1$.

We use induction once again. Since $\mu_d(b_1, b_2, \cdots, b_n) \equiv 0 \pmod{\kappa_{n-1}}$ and since $(\kappa_{n-1}, b_n) = 1$, every proper$^+$ representation of $\mu_d(b_1, b_2, \cdots, b_n)$ is of the form $\sum_{i=1}^{n-1} z_i b_i + r\kappa_{n-1}b_n$, $r = 1, 2, \cdots, s_n$. Furthermore $e_r = (\mu_d(b_1, \cdots, b_n) - r\kappa_{n-1}b_n)/\kappa_{n-1} = \mu_{d'}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1}) + (s_n - r)b_n$, $r = 1, 2, \cdots, s_n$. By (d), $e_i = R_{d'}^+(b_1, b_2, \cdots, b_n)$, $i = 1, 2, \cdots, s_n - 1$. By our induction hypothesis $e_{s_n} \in R_{d'-1}^+(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1})$. Consequently $\mu_d(b_1, b_2, \cdots, b_n) \in R_{d-1}^+(b_1, b_2, \cdots, b_n)$.

(g) $\nu_d(b_1, b_2, \cdots, b_n) - 1 \in R_{d-1}(b_1, b_2, \cdots, b_n)$.

This follows at once from (f) and the fact that $\mu_d(b_1, b_2, \cdots, b_n) = \nu_d(b_1, b_2, \cdots, b_n) - 1 + \sum_{i=1}^n b_i$.

(h) For any c, if $c \in R_a(b_1, b_2, \cdots, b_n)$, then $a \leq d$.

The statement: for any m, if $m \in R_a^+(b_1, b_2, \cdots, b_n)$, then $a \leq d$, is proved in the same manner as (d). Applying this remark to $m = c + \sum_{i=1}^n b_i$ will prove (h).

(i) If $c \leq \nu_d(b_1, b_2, \cdots, b_n) - 1$ and $c \in R_a(b_1, b_2, \cdots, b_n)$, then $\nu_d(b_1, b_2, \cdots, b_n) - 1 - c \in R_{d-a}(b_1, b_2, \cdots, b_n)$.

Consider first the case $n = 2$. If $c \in R_a(b_1, b_2)$, we can find an integer z_2, $0 \leq z_2 < b_1$, such that $c = z_1 b_1 + z_2 b_2$. All the representations of c are then of the form $c = (z_1 - rb_2)b_1 + (z_2 + rb_1)b_2$, and the proper representations occur for $r = 0, 1, \cdots, a-1$. Hence $(a-1)b_2 \leq z_1 < ab_2$. Since $\nu_d(b_1, b_2) - 1 = [(d-1)b_2 - 1]b_1 + (b_1 - 1)b_2$, it follows that $\nu_d - 1 - c = y_1 b_1 + y_2 b_2$ with $y_1 = (d-1)b_2 - 1 - z_1$, whence $(d-1-a)b_2 \leq y_1 < (d-a)b_2$, and with $y_2 = b_1 - 1 - z_2$, whence $0 \leq y_2 < b_1 - 1$. We conclude that $(y_1 - rb_2)b_1 + (y_2 + rb_1)b_2$ are proper representations of $\nu_d - 1 - c$ if and only if $r = 0, 1, \cdots, d-a-1$. Hence $\nu_d - 1 - c \in R_{d-a}(b_1, b_2)$.

We proceed by induction. Assume $c \in R_a(b_1, b_2, \cdots, b_n)$. If $c - z_n b_n \equiv 0 \pmod{\kappa_{n-1}}$ with $0 \leq z_n < \kappa_{n-1}$, let, as above, $c_r = (c - (z_n + r\kappa_{n-1})b_n)/\kappa_{n-1}$, $r = 0, 1, \cdots, s_n - 1$. It is clear that distinct representations of c_r as a proper combination of $b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1}$ will yield distinct representations of c as a proper combination of $b_1, b_2, \cdots, b_n$, and will, in fact, give all possible

proper representations of c. If then $c_r \in R_{a(r)}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1})$, it follows that $a = \sum_{r=0}^{s_n-1} a(r)$.

By induction, $\nu_{d'} - 1 - c_r \in R_{d'-a(r)}(b_1/\kappa_{n-1}, \cdots, b_{n-1}/\kappa_{n-1})$, $r = 0, 1, \cdots$, $s_n - 1$. We have $\nu_d - 1 = \kappa_{n-1}(\nu_{d'} - 1) + (s_n\kappa_{n-1} - 1)b_n$. Therefore, if $\nu_{d'} - 1 - c_r = \sum_{i=1}^{n-1} z_i(b_i/\kappa_{n-1})$, then $\nu_d - 1 - c = \sum_{i=1}^{n-1} z_i b_i + (s_n\kappa_{n-1} - 1 - (z_n + r\kappa_{n-1}))b_n$. This shows that every proper representation of $\nu_{d'} - 1 - c_r$ gives rise to a representation of c as a proper combination of $b_1, b_2, \cdots, b_n$, and hence there are at least $\sum_{r=0}^{s_n-1} (d' - a(r)) = d - a$ proper representations of $\nu_d - 1 - c$.

On the other hand, if $\nu_d - 1 - c = \sum_{i=1}^{n} y_i b_i$, then $y_n = s_n\kappa_{n-1} - 1 - (z_n + r\kappa_{n-1})$ for some $r = 0, 1, \cdots, s_n - 1$, and so $\nu_{d'} - 1 - c_r = \sum_{i=1}^{n-1} y_i(b_i/\kappa_{n-1})$. Thus every representation of $\nu_d - 1 - c$ arises from one of $\nu_{d'} - 1 - c_r$ for some integer $r = 0, 1, \cdots, s_n - 1$. Hence $\nu_d - 1 - c \in R_{d-a}(b_1, b_2, \cdots, b_n)$.

(j). Proof of (c).

It follows from (i) that for every integer $c < \nu_d$, $\chi(c) + \chi(\nu_d - 1 - c) = d$. We consider the pairs of integers: $c, \nu_d - 1 - c$. If ν_d is an even integer, we have exactly $2^{-1}\nu_d$ distinct pairs, and hence $\sum_{c=0}^{\nu_d-1} \chi(c) = d(2^{-1}\nu_d)$. If ν_d is odd, there are $2^{-1}(\nu_d - 1)$ distinct pairs in addition to the single integer $2^{-1}(\nu_d - 1)$ which is paired with itself. Since (i) implies that $2^{-1}(\nu_d - 1) \in R_{d/2}(b_1, b_2, \cdots, b_n)$, we conclude that $\sum_{c=0}^{\nu_d-1} \chi(c) = d(2^{-1}(\nu_d - 1)) + 2^{-1}d = 2^{-1}d\nu_d$. This completes the proof of the theorem.

We conclude with two arithmetic results which we shall need in the next section.

LEMMA 1. *Assume* $b_i > s_{i-1}b_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i = 3, 4, \cdots, n$. *Then there exist non-negative integers* γ_{ij}, $j = 1, 2, \cdots, n-1$; $i = j+1, \cdots, n$, *such that*

(a) $(\kappa_{i-1}/\kappa_i)b_i = \sum_{j=1}^{i-1} \gamma_{ij}b_j$, $i = 2, 3, \cdots, n$;

(b) $0 \leq \gamma_{ij} - \sum_{m=j+1}^{i-1} \gamma_{mj}(s_m - 1) < (\kappa_{j-1}/\kappa_j)$, $j = 2, \cdots, n-1$; $i = j+1$, $\cdots, n$;

(c) $0 \leq \gamma_{i1} - \sum_{m=2}^{i-1} \gamma_{m1}(s_m - 1)$, $i = 2, 3, \cdots, n$.

Proof. We first prove the assertion:

(d) Let c be an arbitrary integer divisible by κ_n and let $a_2, a_3, \cdots, a_n$ be given integers. Then we can write $c = \sum_{i=1}^{n} z_i b_i$ with $a_i \leq z_i < a_i + (\kappa_{i-1}/\kappa_i)$, $i = 2, 3, \cdots, n$.

Since $(\kappa_{n-1}/\kappa_n, b_n/\kappa_n) = 1$, $(c/\kappa_n) - z_n(b_n/\kappa_n) \equiv 0 \pmod{\kappa_{n-1}/\kappa_n}$ for some z_n such that $a_n \leq z_n < a_n + (\kappa_{n-1}/\kappa_n)$. Hence $c - z_n b_n \equiv 0 \pmod{\kappa_{n-1}}$, and (d) follows by induction.

As for the lemma itself, if $n = 2$ we have $(b_1/\kappa_2)b_2 = (b_2/\kappa_2)b_1$. Thus $\gamma_{21} = (b_2/\kappa_2)$. We proceed by induction. Applied to the integers $b_1, b_2, \cdots, b_{n-1}$, we may assume the existence of integers γ_{ij}, $j = 1, 2, \cdots, n-2$; $i = j+1, \cdots, n-1$ which satisfy (a), (b), and (c).

Let $a_j = \sum_{m=j+1}^{n-1} \gamma_{mj}(s_m - 1)$, $j = 1, 2, \cdots, n-2$, and let $a_{n-1} = 0$. Since $(\kappa_{n-1}/\kappa_n)b_n$ is divisible by κ_{n-1}, we can apply (d) to it and to the integers $a_2, a_3, \cdots, a_{n-1}$, as just defined. We conclude that there exist integers

γ_{n1}, γ_{n2}, $\cdots$, γ_{nn-1} such that $(\kappa_{n-1}/\kappa_n)b_n = \sum_{j=1}^{n-1} \gamma_{nj}b_j$ and $0 \leq \gamma_{nj} - a_j < (\kappa_{j-1}/\kappa_j)$, $j = 2, 3, \cdots, n-1$. Hence the integers γ_{nj}, $j = 1, 2, \cdots, n-1$, satisfy (a) and (b). The proof will be completed by showing that γ_{n1} satisfies (c)—that is, $\gamma_{n1} \geq a_1$.

$$\gamma_{n1}b_1 = (\kappa_{n-1}/\kappa_n)b_n - \sum_{j=2}^{n-1} \gamma_{nj}b_j \geq (\kappa_{n-1}/\kappa_n)b_n - \sum_{j=2}^{n-1} (a_j + (\kappa_{j-1}/\kappa_j) - 1)b_j,$$

whence it will suffice to prove that $(\kappa_{n-1}/\kappa_n)b_n - \sum_{j=2}^{n-1} (a_j + (\kappa_{j-1}/\kappa_j) - 1)b_j \geq a_1 b_1$. Using the definition of the integers a_j and condition (a), this last inequality can be rewritten, as follows:

(e) $b_n - \sum_{i=2}^{n-1} (s_i(\kappa_{i-1}/\kappa_i) - 1)b_i \geq 0$.

Since by hypothesis $b_i > s_{i-1}b_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i = 3, \cdots, n$, it follows that

$$b_n > s_{n-1}b_{n-1}(\kappa_{n-2}/\kappa_{n-1}) = [s_{n-1}(\kappa_{n-2}/\kappa_{n-1}) - 1]b_{n-1} + b_{n-1},$$

and (e) follows by induction. Q.E.D.

Let $R(b_1, \cdots, b_n)$ denote the set of integers which may be written as a linear combination of $b_1, \cdots, b_n$ with *arbitrary* non-negative integers.

LEMMA 2. *Assume* $b_i > s_{i-1}b_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i = 3, \cdots, n$. *Then*

(a) *If* $c \in R(b_1, b_2, \cdots, b_n)$, *then* $c \in R_a(b_1, b_2, \cdots, b_n)$ *with* $a \geq 1$.

(b) *If* $c > (b_n/\kappa_n)(\kappa_{n-1}/\kappa_n)$, $\kappa_n c \in R(b_1, \cdots, b_n)$.

(c) *Define* $t_i = t_{i-1}s_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i = 3, \cdots, n$, *with* t_2 *an arbitrary positive integer. Then* $(\kappa_{n-1}/\kappa_n)t_n \geq t_2 + \sum_{i=2}^{n-1}(s_i(\kappa_{i-1}/\kappa_i) - 1)t_i$.

Proof. If $c \in R(b_1, \cdots, b_n)$, $c = \sum_{i=1}^n y_ib_i$, $y_i \geq 0$. Write $y_n = r_n(\kappa_{n-1}/\kappa_n) + z_n$, $0 \leq z_n < (\kappa_{n-1}/\kappa_n)$, $r_n \geq 0$. Since $(\kappa_{n-1}/\kappa_n)b_n = \sum_{j=1}^{n-1} \gamma_{nj}b_j$ and $\gamma_{nj} \geq 0$, $j = 1, 2, \cdots, n$, it follows that $c = \sum_{i=1}^{n-1} y_i' b_i + z_n b_n$ with $y_i' \geq 0$, $i = 1, 2, \cdots, n-1$. Thus by induction we conclude that that $c = \sum_{i=1}^n z_i b_i$, $z_i \geq 0$, $i = 1, 2, \cdots, n$, and $z_i < (\kappa_{i-1}/\kappa_i)$, $i = 2, \cdots, n$. Thus c may be written as a proper combination of $b_1, b_2, \cdots, b_n$ in at least one way, and hence $c \in R_a(b_1, b_2, \cdots, b_n)$ with $a \geq 1$.

Take $n = 2$, and suppose $c > (b_2/\kappa_2)(b_1/\kappa_2)$. As in Theorem 4, (d), $c = y_1(b_1/\kappa_2) + y_2(b_2/\kappa_2)$, $y_i \geq 0$, $i = 1, 2$; whence $\kappa_2 c \in R(b_1, b_2)$. We use induction. If $c > (b_n/\kappa_n)(\kappa_{n-1}/\kappa_n)$, there exists an integer z_n with $0 \leq z_n < (\kappa_{n-1}/\kappa_n)$ such that $c - z_n(b_n/\kappa_n) \equiv 0 \pmod{(\kappa_{n-1}/\kappa_n)}$. Denote the integer $(\kappa_n c - z_n b_n)/\kappa_{n-1}$ by c'. Since $c > (b_n/\kappa_n)(\kappa_{n-1}/\kappa_n)$ and $z_n \leq (\kappa_{n-1}/\kappa_n) - 1$, it follows that $c' > [(b_n\kappa_{n-1}/\kappa_n) - ((\kappa_{n-1}/\kappa_n) - 1)b_n]/\kappa_{n-1} = (b_n/\kappa_n)$. $b_n > s_{n-1}b_{n-1}(\kappa_{n-2}/\kappa_{n-1})$ by hypothesis, and $s_{n-1} \geq 1$, so that $c' > (b_{n-1}/\kappa_{n-1})(\kappa_{n-2}/\kappa_{n-1})$. By induction, $\kappa_{n-1}c' \in R(b_1, \cdots, b_{n-1})$. Since $\kappa_{n-1}c' = \kappa_n c - z_n b_n$, (b) is proved.

(c) is established in the same way as part (e) of Lemma 1.

4. A generalization of a theorem of Seidenberg. Seidenberg [7] has given a detailed analysis of the valuation ideals in a polynomial ring in two independent variables over an algebraically closed ground field. As a special

case of his theory one can obtain the corresponding analysis for the valuation ideals in a nonhomogeneous coordinate ring of a plane algebraic curve (over an algebraically closed ground field). The main tool in his work is the construction, for a given valuation, of a special set of polynomials intrinsically associated with the valuation (Theorem 6).

We shall generalize this construction for valuations of an algebraic function field of one variable over an arbitrary ground field and for discrete valuations of an algebraic number field.

Denote by π_1 the irreducible monic polynomial in X with coefficients in k or the rational prime integer which generates the prime ideal $\mathfrak{p}_0$ in $\mathfrak{o}_0$. Let π_1, π_2 be a basis for the prime ideal $\mathfrak{p}$ in $\mathfrak{o}$. If we assume that π_2 is a monic polynomial in y whose coefficients are, in the one case, in $k[X]$ of degree less than $\deg_X \pi_1$ or, in the other case, non-negative integers less than π_1, then π_2 is uniquely determined. Clearly every element of $\mathfrak{o}$ is congruent modulo $\mathfrak{p}$ to a polynomial in y of degree less than $\deg_y \pi_2$. Let η_i, $i=1, 2, \cdots, d_\mathfrak{p}$, be elements of $\mathfrak{o}$ which form a basis for $\mathfrak{o}$ modulo $\mathfrak{p}$ and such that $\deg_y \eta_i < \deg_y \pi_2$.

THEOREM 5. *Let v be a valuation of K with center $\mathfrak{p}$ in $\mathfrak{o}$. It is possible to construct a set of elements $\pi_3, \pi_4, \cdots, \pi_n$ in $\mathfrak{o}$ which together with π_1, π_2 satisfy all the following conditions:*

(a) *π_i may be written as a monic polynomial in y with coefficients in $\mathfrak{o}_0$, $i=3, \cdots, n$. If $\deg_y \pi_i = t_i$, $i=2, \cdots, n$, and if $v(\pi_i) = b_i$, $i=1, 2, \cdots, n$, while $\kappa_i = (b_1, \cdots, b_i)$, there exist positive integers $s_2, s_3, \cdots, s_n$ such that*

(b) *$t_2 = s_1$ and $t_i = t_{i-1} s_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i=3, \cdots, n$;*

(c) *$b_i > s_{i-1} b_{i-1}(\kappa_{i-2}/\kappa_{i-1})$, $i=3, \cdots, n$;*

(d) *If $d =$ the degree of v, then $d = d_\mathfrak{p} \prod_{i=2}^{n} s_i$; moreover,*

(e) *$(b_1, b_2, \cdots, b_n) = 1$;*

(f) *If $\phi \in \mathfrak{o}$, $v(\phi) \in R(b_1, b_2, \cdots, b_n)$;*

(g) *If $\{\mathfrak{q}_j\}$ denotes the sequence of v-ideals in $\mathfrak{o}$, then the monomials $\eta_h \prod_{i=1}^{n} \pi_i^{a_i}$ with $h=1, 2, \cdots, d_\mathfrak{p}$ and $a_i < s_i(\kappa_{i-1}/\kappa_i)$, $i=2, 3, \cdots, n$, of value $v(\mathfrak{q}_j)$ form an independent basis for $\mathfrak{q}_j$ modulo $\mathfrak{q}_{j+1}$.*

Proof. For brevity, we call a monomial $\eta_h \prod_{i=1}^{r} \pi_i^{a_i}$ with $a_i < s_i(\kappa_{i-1}/\kappa_i)$, $i=2, 3, \cdots, r$, a *canonical product* of $\pi_1, \cdots, \pi_r$. If $\phi \in \mathfrak{o}$ can be expressed as a linear combination (with coefficients in k or in I, as the case may be) of canonical products $\pi_1, \cdots, \pi_r$, we shall write $\phi \in R(\pi_1, \cdots, \pi_r)$.

It will be convenient to add the statement:

(h) if $\deg_y \phi < t_i$ for some i, then $\phi \in R(\pi_1, \cdots, \pi_{i-1})$ and $v(\phi) \in R(b_1, \cdots, b_{i-1})$.

If $\deg_y \phi < t_2$, it is clear that $\phi = \sum_{i=1}^{m} c_i \eta_{h(i)} \pi_1^{a_i}$, $a_i \geq 0$, and $c_i \in k$ or $c_i \in I$, $i=1, 2, \cdots, m$, whence (h) holds in this case. Assume that $\pi_3, \cdots, \pi_r$ have been constructed satisfying (a), (b), (c), and (h). Then $b_1, \cdots, b_r$ satisfy the hypothesis of Lemmas 1 and 2. Let $\sigma_i = \prod_{j=1}^{i-1} \pi_j^{(\gamma_{ij})}$, $i=2, 3, \cdots, r$, where the γ_{ij} are the integers whose existence is asserted in Lemma 1. Also let

$\psi_i = (\pi_i^{(\kappa_{i-1}/\kappa_i)}/\sigma_i)$, $i = 2, 3, \cdots, r$. By the definition of γ_{ij}, $v(\sigma_i) = (\kappa_{i-1}/\kappa_i)b_i$ and $v(\psi_i) = 0$, $i = 2, 3, \cdots, r$.

As part of our induction hypothesis, we shall assume: if $\alpha_2 = \bar{y}$ and $\alpha_{i+1} = \bar{\psi}_i$, $i = 2, 3, \cdots, r$ ($^-$ denotes the residue, modulo the ideal of nonunits, of an element of the valuation ring of v), then

(i) $s_i = [k_0(\alpha_2, \cdots, \alpha_{i+1}) : k_0(\alpha_2, \cdots, \alpha_i)]$, $i = 2, 3, \cdots, r-1$.

We define s_r by (i) and proceed to construct an element π_{r+1} in $\mathfrak{o}$ satisfying (a), (b), (c) and (h). There exists a unique polynomial $g_r(\alpha_2, \cdots, \alpha_r, Z)$ with coefficients in k_0, monic in Z of degree s_r, whose degree in $\alpha_i < s_{i-1}$, $i = 2, 3, \cdots, r$, and which is zero for $Z = \alpha_{r+1}$. Let $g_r'(y, \psi_2, \cdots, \psi_{r-1}, Z)$ be a monic polynomial obtained from g_r by replacing α_2 by y, α_{i+1} by ψ_i, $i = 2, \cdots, r-1$, and each coefficient by a representative in $\mathfrak{o}_0$.

It follows directly from part (b) of Lemma 1 that $\prod_{i=1}^{r-1} \sigma_i^{s_i-1}$ divides σ_r in $\mathfrak{o}$; and hence by the construction of g_r' and the definition of ψ_i, $\sigma_r^{s_r} \cdot g_r'(y, \psi_2, \cdots, \psi_r) \in \mathfrak{o}$.

We define π_{r+1} to be $\sigma_r^{s_r} \cdot g_r'(y, \psi_2, \cdots, \psi_r)$. By construction

$$v(g_r'(y, \psi_2, \cdots, \psi_r)) > 0,$$

whence $v(\pi_{r+1}) > v(\sigma_r^{s_r}) = s_r(\kappa_{r-1}/\kappa_r)b_r$. Hence (c) holds for π_{r+1}.

The proof of (a) and (b) depends upon the following assertion:

(j) $\deg_y \sigma_i < \deg_y \pi_i^{(\kappa_{i-1}/\kappa_i)} = (\kappa_{i-1}/\kappa_i)t_i$, $i = 2, 3, \cdots, r$. For $i = 2$, σ_2 is a power of π_1 whence $\deg_y \sigma_2 = 0$. Assume (j) for $\sigma_2, \cdots, \sigma_{r-1}$. By definition, $\deg_y \sigma_i = \sum_{j=2}^{i-1} \gamma_{ij} t_j$, $i = 3, \cdots, r$. Combining these relations with the inequalities $\gamma_{rj} \leq (\kappa_{j-1}/\kappa_j) - 1 + \sum_{e=j+1}^{r-1} \gamma_{ej}(s_e - 1)$, $j = 2, 3, \cdots, r-1$, a direct computation yields $\deg_y \sigma_r < \sum_{i=2}^{r-1} [(s_i - 1)\deg_y \sigma_i + (\kappa_{i-1}/\kappa_i) - 1)t_i]$. Applying (j) for $i < r$, we obtain $\deg_y \sigma_r < \sum_{i=2}^{r-1} (s_i(\kappa_{i-1}/\kappa_i) - 1)t_i < (\kappa_{r-1}/\kappa_r)t_r$ by Lemma 2.

The conclusion to be drawn from (j) is the following: the term of highest degree in y in π_{r+1} is either *less than or equal* to the degree in y of $\theta_1 = y^{s_1-1}\sigma_r^{s_r}\prod_{i=2}^r \psi_i^{s_i-1}$, or is *equal* to the degree in y of $\theta_2 = \pi_r^{s_r(\kappa_{r-1}/\kappa_r)}$, since $\deg_y \theta_1 = \deg_y \sigma_r - \sum_{i=2}^{r-1} [(s_i - 1) \deg_y \sigma_i] + s_1 - 1 + \sum_{i=2}^{r-1} (s_i - 1)(\kappa_{i-1}/\kappa_i)t_i$. It follows from Lemma 1 that

$$\deg_y \sigma_r - \sum_{i=2}^{r-1} (s_i - 1) \deg_y \sigma_i \leq \sum_{i=2}^{r-1} ((\kappa_{i-1}/\kappa_i) - 1)t_i$$

whence $\deg_y \theta_1 \leq s_1 - 1 + \sum_{i=2}^{r-1} (s_i(\kappa_{i-1}/\kappa_i) - 1)t_i$. Since $s_1 = t_2$ and $s_r \geq 1$, it follows from Lemma 2 that $\deg_y \theta_1 < s_r(\kappa_{r-1}/\kappa_r)t_r = \deg_y \theta_2$.

Thus π_{r+1} is indeed monic in y of degree $t_{r+1} = s_r(\kappa_{r-1}/\kappa_r)t_r$.

Suppose $\phi \in \mathfrak{o}$ and $\deg_y \phi < t_{r+1}$. Since π_r is monic in y we may write $\phi = \phi_0 + \phi_1 \pi_r \cdots \phi_e \pi_r^e$, $e < s_r(\kappa_{r-1}/\kappa_r)$, and $\deg_y \phi_i < t_r$ (by (b)). Hence by induction $\phi_i \in R(\pi_1, \cdots, \pi_{r-1})$ and $\phi \in R(\pi_1, \cdots, \pi_r)$. The proof that $v(\phi) \in R(b_1, \cdots, b_r)$ depends upon a portion of (g), namely:

(k) The canonical products of $\pi_1, \cdots, \pi_r$ of value $v(\mathfrak{q}_j)$ are linearly independent modulo $\mathfrak{q}_{j+1}$.

For we already know that ϕ is a linear combination of canonical products of $\pi_1, \cdots, \pi_r$, and (k) shows that $v(\phi)$ is equal to the minimum value of the canonical products which occur in the expression for ϕ. Hence $v(\phi) \in R(b_1, \cdots, b_r)$.

To prove (k), proceed inductively, observing that (k) certainly holds for the canonical products of π_1 (if any) of value $v(\mathfrak{q}_j)$. Assume (k) for canonical products of $\pi_1, \cdots, \pi_{r-1}$, and let $\zeta = \sum_{i=1}^{m} c_i \zeta_i$ be a linear combination of canonical products ζ_i of $\pi_1, \cdots, \pi_r$ in which $v(\mathfrak{q}_j) = v(\zeta_i)$, $i = 1, 2, \cdots, m$. We must prove that $\zeta \notin \mathfrak{q}_{j+1}$.

We first prove:

(1) A power product $\chi = \prod_{i=1}^{r} \pi_i^{a_i}$ with $a_i > 0$, $= 0$, or < 0, and with $v(\chi) = 0$ may be expressed in the form $\prod_{i=2}^{r} \psi_i^{m_i}$, $m_i > 0$, $= 0$, or < 0. In fact, $\sum_{i=1}^{r} a_i b_i = 0$, whence $a_r = m_r(\kappa_{r-1}/\kappa_r)$ for some integer $m_r > 0$, $= 0$, or < 0. Thus $\chi = \psi_r^{m_r} \sigma_r^{m_r} \prod_{i=1}^{r-1} \pi_i^{a_i}$. Since $\sigma_r^{m_r} \prod_{i=1}^{r-1} \pi_i^{a_i}$ is a power product of $\pi_1, \cdots, \pi_{r-1}$ and since $v(\psi_r) = 0$, (1) follows readily by induction. An immediate corollary of (1) is that $\overline{(\zeta_i/\zeta_k)} \in k_0(\alpha_2, \cdots, \alpha_{r+1})$ for all $i, k = 1, 2, \cdots, m$.

If $e_i = \exp \pi_r$ in ζ_i, we may assume that $\max (e_1, \cdots, e_m) > 0$ and, for definiteness, that $e_1 = \min (e_1, \cdots, e_m)$. It follows at once from the preceding remark that $\overline{(\zeta/\zeta_1)}$ is a polynomial $P(\alpha_{r+1})$ in α_{r+1} with coefficients in $k_0(\alpha_2, \cdots, \alpha_r)$. Since $e_i < s_r(\kappa_{r-1}/\kappa_r)$ for each i, $\deg_Z P(Z) < s_r$. But if $\zeta \in \mathfrak{q}_{j+1}$, $v(\zeta) > v(\zeta_1)$ whence $\overline{(\zeta/\zeta_1)} = 0 = P(\alpha_{r+1})$, in contradiction to the fact that α_{r+1} satisfies no polynomial of degree $< s_r$ with coefficients in $k_0(\alpha_2, \cdots, \alpha_r)$.

We have thus succeeded in constructing an element π_{r+1} which satisfies (a), (b), (c), and (h). The remainder of the proof consists in showing that after a finite number of such constructions (d), (e), (f), (g) can also be made to hold.

It may happen first of all, at some step in this process that $\pi_{r+m+1} = 0$. In this case, we assert $\pi_1, \cdots, \pi_{r+m}$ satisfy all the conditions of the theorem. Indeed every $\phi \in \mathfrak{o}$ can then be expressed as a polynomial in y with coefficients in $\mathfrak{o}_0$ of degree $< t_{r+m+1}$[3]. By (h), $v(\phi) \in R(b_1, \cdots, b_{r+m})$ and $\phi \in R(\pi_1, \cdots, \pi_{r+m})$ which proves (f), and, in view of (k), also proves (g). Moreover, if $\phi \in K$, $v(\phi) = \sum_{i=1}^{n} a_i b_i$, $a_i > 0$, $= 0$, or < 0, and since K contains an element of value 1, it follows that $(b_1, b_2, \cdots, b_{r+m}) = 1$. Finally (e) implies that $k_0(\alpha_2, \cdots, \alpha_{r+m+1})$ is the entire residue field of v, whence $d = d_\mathfrak{p} \prod_{i=2}^{r+m} s_i$, proving (d).

Suppose now that $\kappa_r = 1$. If $\phi \in \mathfrak{o}$, and $v(\phi) > s_r(\kappa_{r-1}/\kappa_r)b_r$, it follows from Lemma 2 that $v(\phi) \in R(b_1, \cdots, b_r)$. On the other hand, if $\phi \in \mathfrak{o}$, and $v(\phi) \leqq s_r(\kappa_{r-1}/\kappa_r)b_r$, $\phi = \phi_1 + \phi_2\pi_{r+1}$, $\phi_i \in \mathfrak{o}$, $i = 1, 2$, and $\deg_y \phi_1 < t_{r+1}$. Since $v(\pi_{r+1}) > s_r\kappa_{r-1}b_r$, $v(\phi) = v(\phi_1) \in R(b_1, \cdots, b_r)$ by (h). Therefore (e) implies (f).

---

[3] t_{r+m+1} denotes the formal degree of π_{r+m+1} as a polynomial in y.

To prove (e) suppose $\kappa_r > 1$. Then there exists $\phi \in \mathfrak{o}$ such that $v(\phi) \notin R(b_1, \cdots, b_r)$. Suppose π_{r+i}, $i = 1, 2, \cdots, e$, have been constructed and that $b_{r+i} = v(\pi_{r+i}) \in R(b_1, \cdots, b_r)$, $i = 1, 2, \cdots, e$. Assume $b_{r+i} > v(\phi)$ for some i. As above, $\phi = \phi_1 + \phi_2 \pi_{r+i}$, $\deg_y \phi_1 < t_{r+i}$. Hence $v(\phi) = v(\phi_1) \in R(b_1, \cdots, b_{r+i-1}) = R(b_1, \cdots, b_r)$, contrary to the choice of ϕ. Thus if $b_{r+i} \in R(b_1, \cdots, b_r)$, $b_{r+i} < v(\phi)$. Since $b_{r+i+1} > b_{r+i}$, there exists an integer m such that $b_{r+m} = v(\pi_{r+m}) \notin R(b_1, \cdots, b_r)$. We shall show that $\kappa_{r+m} < \kappa_r$. Since certainly $b_{r+m} > b_r(\kappa_{r-1}/\kappa_r)$, $(b_{r+m}/\kappa_{r+m}) > (b_r/\kappa_r)(\kappa_{r-1}/\kappa_{r+m})$. If $\kappa_{r+m} = \kappa_r$, we conclude immediately from Lemma 2 that $b_{r+m} \in R(b_1, \cdots, b_r)$, a contradiction; whence $\kappa_{r+m} < \kappa_r$. Consequently a finite number of constructions of elements π_i, $i = 1, 2, \cdots, n$, will be sufficient to insure that $(b_1, b_2, \cdots, b_n) = 1$.

Assume that the residue field of v contains an element α' not in $k_0(\alpha_2, \cdots, \alpha_{r+1})$. If ϕ_1/ϕ_2 is a representative of α' in K, $\phi_i \in \mathfrak{o}$, $i = 1, 2$, let $b' = v(\phi_1) = v(\phi_2)$. Construct π_{r+i}, $i = 1, 2, \cdots, m+1$, so that $b' < b_{r+m+1}$. As above, write $\phi_i = \phi_i' + \phi_i'' \pi_{r+m+1}$, $\deg_y \phi_i' < t_{r+m+1}$, $i = 1, 2$. Then $b' = v(\phi_i')$, $i = 1, 2$, and by (1) the residue of ϕ_1'/ϕ_2' is in $k_0(\alpha_2, \cdots, \alpha_{r+m+1})$. But clearly this residue is α', whence $\alpha' \in k_0(\alpha_2, \cdots, \alpha_{r+m+1})$. We conclude from the definition of s_i and the preceding results that we can construct elements $\pi_1, \pi_2, \cdots, \pi_n$ in $\mathfrak{o}$ which satisfy (a)–(f).

To complete the proof we need only verify that the canonical products of $\pi_1, \pi_2, \cdots, \pi_n$ of value $v(\mathfrak{q}_j)$ span $\mathfrak{q}_j$ modulo $\mathfrak{q}_{j+1}$. This will establish (g) since the independence of these canonical products has already been proved. If $v(\mathfrak{q}_j) \leq s_n \kappa_{n-1} b_n$ and if $\phi \in \mathfrak{q}_j$, write $\phi = \phi_1 + \phi_2 \pi_n$, with $\deg_y \phi_1 < t_n$. Then $\phi \equiv \phi_1 \pmod{\mathfrak{q}_{j+1}}$ and, by (h), $\phi_1 \in R(\pi_1, \pi_2, \cdots, \pi_{n-1})$.

Suppose that $v(\mathfrak{q}_j) > s_n \kappa_{n-1} b_n$. Using equation (e) of Lemma 1, we have

$$s_n \kappa_{n-1} b_n > \left[\sum_{i=2}^{n} (s_i \kappa_{i-1}/\kappa_i - 1) b_i \right] - (b_1 - 1) = \nu_{d'}(b_1, b_2, \cdots, b_n),$$

where $d' = \prod_{i=2}^{n} s_i$. It follows then from Theorem 4 that $v(\mathfrak{q}_j) \in R_{d'}(b_1, b_2, \cdots, b_n)$. Let $v(\mathfrak{q}_j) = \sum_{i=1}^{n} a_{im} b_i$, $m = 1, 2, \cdots, d'$, be the distinct representations of $v(\mathfrak{q}_j)$ as a proper combination of $b_1, b_2, \cdots, b_n$. Then the d monomials $\eta_h \prod_{i=1}^{n} \pi_i^{(a_{im})}$, $h = 1, 2, \cdots, d_p$; $m = 1, 2, \cdots, d'$, are distinct canonical products of value $v(\mathfrak{q}_j)$, which are linearly independent modulo $\mathfrak{q}_{j+1}$ by (k). We conclude that $\dim \mathfrak{q}_j/\mathfrak{q}_{j+1} = d$ and that these d canonical products span $\mathfrak{q}_j$ modulo $\mathfrak{q}_{j+1}$. Q.E.D.

5. The main theorem.

THEOREM 6. $d(\mathfrak{C}_\mathfrak{p}) = 2\delta(\mathfrak{C}_\mathfrak{p})$, *or equivalently* $\dim \bar{\mathfrak{o}}_\mathfrak{p}/\mathfrak{C}_\mathfrak{p} = 2 \dim \mathfrak{o}_\mathfrak{p}/\mathfrak{C}_\mathfrak{p}$.

Proof. Because of the one-one correspondence between complete $\mathfrak{p}$-ideals in $\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}^*$, we need only prove $d(\mathfrak{C}_\mathfrak{p}^*) = 2\delta(\mathfrak{C}_\mathfrak{p}^*)$. Since $d(\mathfrak{C}_\mathfrak{p}^*) = \sum_{i=1}^{r} d_i v_i^*(\mathfrak{C}_\mathfrak{p}^*)$, and since $\mathfrak{C}_\mathfrak{p}^* = \sum_{i=1}^{r} \mathfrak{C}_i^* \omega_i^*$, this is equivalent to the assertion

$$(7) \qquad \delta(\mathfrak{C}_\mathfrak{p}{}^*) = \frac{1}{2} \sum_{i=1}^{r} d_i v_i{}^*(\mathfrak{C}_i{}^* \omega_i{}^*),$$

which we proceed to verify.

Let $\mathfrak{o}^* = \sum_{i=1}^{r} \mathfrak{o}_i{}^* \omega_i{}^*$. Then clearly

$$(8) \qquad \delta(\mathfrak{C}_\mathfrak{p}{}^*) = \dim \mathfrak{o}_\mathfrak{p}{}^* / \mathfrak{o}^* + \sum_{i=1}^{r} \delta(\mathfrak{C}_i{}^*).$$

(7) follows at once from (8) and from the following two statements:

$$(9) \qquad \dim \mathfrak{o}_\mathfrak{p}{}^* / \mathfrak{o}^* = \frac{1}{2} \sum_{i=1}^{r} d_i v_i{}^*(\omega_i{}^*),$$

$$(10) \qquad \delta(\mathfrak{C}_i{}^*) = \frac{1}{2} d_i v_i{}^*(\mathfrak{C}_i{}^*), \qquad i = 1, 2, \cdots, r.$$

For each j, $2 \le j \le r$, define $\Omega_{ij}^* = \prod_{m=1, m \ne i}^{j} F_m{}^*$, $i = 1, 2, \cdots, j$, and let ω_{ij}^* be the residue of Ω_{ij}^* in $\mathfrak{o}_i{}^*$. Also denote by $\mathfrak{Q}_j{}^*$ the ideal $(\Omega_{1j}^*, \Omega_{2j}^*, \cdots, \Omega_{jj}^*)$ in $\mathfrak{O}_\mathfrak{P}{}^*$. We shall prove

$$(9') \qquad \dim \mathfrak{O}_\mathfrak{P}^* / \mathfrak{Q}_j{}^* = \frac{1}{2} \sum_{i=1}^{i} d_i v_i{}^*(\omega_{ij}^*).$$

Since $\mathfrak{Q}_r{}^* = \mathfrak{o}^*$, $(9')$ implies (9).

We shall prove $(9')$ by induction on r. Let $f_i{}^*$ be the residue of $F_i{}^*$ in $\mathfrak{o}_i{}^*$, $i = 1, 2, \cdots, r$. If $r = 2$, $\mathfrak{Q}_2{}^* = (F_1{}^*, F_2{}^*)$, $\omega_{12}^* = f_2{}^*$, and $\omega_{22}^* = f_1{}^*$, and $(9')$ is a direct result of the following lemma:

LEMMA 3. $\dim \mathfrak{O}_\mathfrak{P}^* / (F_1{}^*, F_2{}^*) = d_1 v_1{}^*(f_2{}^*) = d_2 v_2{}^*(f_1{}^*).$

Proof. It suffices to prove the first equality. Since $F_2{}^*$ is a nonunit in $\mathfrak{O}_\mathfrak{P}^*$, $f_2{}^*$ is a nonunit in $\mathfrak{o}_1{}^*$. Hence $\mathfrak{o}_1{}^*$ contains the ring T^*, which is defined, according as K is an algebraic number field or an algebraic function field, as the completion of $I[f_2{}^*]$ or of $k[f_2{}^*]$ with respect to the principal ideal $(f_2{}^*)$. $\mathfrak{o}_1{}^*$ is, in fact, a finite T^*-module (Chevalley [1, Proposition 5, p. 699]): $\mathfrak{o}_1{}^* = \sum_{i=1}^{s} T^* u_i$, $u_i \in \mathfrak{o}_1{}^*$, $i = 1, 2, \cdots, s$. If L^* denotes the quotient field of T^*, it follows that $[\Sigma_1{}^* : L^*] = s$. On the other hand, $[\Sigma_1{}^* : L^*] = d_1 v_1{}^*(f_2{}^*)$ (Chevalley [2, Theorem 5, p. 61]), whence $s = d_1 v_1{}^*(f_2{}^*)$. Since clearly $\dim \mathfrak{O}_\mathfrak{P}^* / (F_1{}^*, F_2{}^*) = \dim \mathfrak{o}_1{}^* / \mathfrak{o}_1{}^* f_2{}^*$, we have only to verify that $\dim \mathfrak{o}_1{}^* / \mathfrak{o}_1{}^* f_2{}^* = s$.

If $z \in \mathfrak{o}_1{}^*$, $z = \sum_{i=1}^{s} t_i{}^* u_i$, $t_i{}^* \in T^*$. There exist constants c_i in k (or I) such that $t_i{}^* - c_i \in T^* f_2{}^*$, $i = 1, 2, \cdots, s$. It follows at once that $z - \sum_{i=1}^{s} c_i u_i \in \mathfrak{o}_1{}^* f_2{}^*$, and hence that $u_1, u_2, \cdots, u_s$ span $\mathfrak{o}_1{}^*$ modulo $\mathfrak{o}_1{}^* f_2{}^*$. On the other hand, if $\sum_{i=1}^{s} c_i u_i = z f_2{}^*$ with $c_i \in k$ (or I) and $z \in \mathfrak{o}_1{}^*$, we may write $z = \sum_{i=1}^{s} t_i{}^* u_i$, $t_i{}^* \in T^*$, whence $\sum_{i=1}^{s} [c_i - f_2{}^* t_i{}^*] u_i = 0$. Since the u_i are linearly independent modulo T^*, we conclude that $c_i = 0$, $i = 1, 2, \cdots, s$, and so the

u_i are linearly independent modulo $\mathfrak{o}_1{}^*f_2{}^*$. This completes the proof of the lemma.

Now assume (9′) for $j<r$. To prove the assertion for $j=r$, write $\dim \mathfrak{O}_\mathfrak{P}^*/\mathfrak{O}_r{}^* = \dim \mathfrak{O}_\mathfrak{P}^*/\mathfrak{O}_{r-1}^* + \dim \mathfrak{O}_{r-1}^*/\mathfrak{O}_r{}^*$, apply the induction hypothesis for $j=r-1$, and use the equality

$$(11) \qquad \dim (\mathfrak{O}_{r-1}^*/\mathfrak{O}_r{}^*) = \sum_{i=1}^{r-1} d_r v_r{}^*(f_i{}^*),$$

to be verified in the next paragraph. A direct computation will yield (9′) at once.

Define the ideals $\mathfrak{S}_h{}^*$ in $\mathfrak{O}_\mathfrak{P}^*$, $h=0, 1, \cdots, r-1$, as follows: $\mathfrak{S}_0{}^* = \sum_{e=1}^{r-1} (\Omega_{er-1}^*)$; $\mathfrak{S}_h{}^* = \sum_{e=1}^{h} \Omega_{er-1}^*(F_e{}^*, F_r{}^*) + \sum_{e=h+1}^{r-1} (\Omega_{er-1}^*)$, $h=1, 2, \cdots$, $r-1$. Clearly $\mathfrak{S}_0{}^* = \mathfrak{O}_{r-1}^*$, $\mathfrak{S}_{r-1}^* = \mathfrak{O}_r{}^*$. Since $\mathfrak{S}_{h-1}^* \supset \mathfrak{S}_h{}^*$, we prove (11) by showing that $\dim (\mathfrak{S}_h{}^*/\mathfrak{S}_{h-1}^*) = d_r v_r{}^*(f_h{}^*)$, $h=1, 2, \cdots, r-1$. In fact, if $A_i{}^*$, $i=1, 2, \cdots, d_r v_r{}^*(f_h{}^*)$, form a basis for $\mathfrak{O}_\mathfrak{P}^*$ modulo $(F_h{}^*, F_r{}^*)$, it follows from the definition of $\mathfrak{S}_h{}^*$ that the elements $A_i{}^*\Omega_{hr-1}^*$ span $\mathfrak{S}_{h-1}^*$ modulo $\mathfrak{S}_h{}^*$. Moreover, if $A^*\in\mathfrak{O}_\mathfrak{P}^*$ and $A^*\Omega_{hr-1}^*\in\mathfrak{S}_h{}^*$, it follows easily that $A^*\Omega_{hr-1}^* \equiv B^*\Omega_{hr-1}^*F_r{}^* \pmod{F_h{}^*}$, $B^*\in\mathfrak{O}_\mathfrak{P}^*$. Since Ω_{hr-1}^* and $F_h{}^*$ are relatively prime, we have $A^*\in(F_h{}^*, F_r{}^*)$, which implies that the elements $A_i{}^*\Omega_{hr-1}^*$ are linearly independent modulo $\mathfrak{S}_h{}^*$. Hence $\dim (\mathfrak{S}_{h-1}^*/\mathfrak{S}_h{}^*) = d_r v_r{}^*(f_h{}^*)$, as asserted.

To prove (10), let $\mathfrak{B}_i$ be the valuation ideal in $\mathfrak{o}$ defined by $v_i(\mathfrak{B}_i) = v_i{}^*(\mathfrak{C}_i{}^*)$. In view of the natural correspondence of the $v_i{}^*$-ideals in $\mathfrak{o}_i{}^*$ with v_i-ideals in $\mathfrak{o}$, we have only to prove $\delta(\mathfrak{B}_i) = 2^{-1}d_i v_i(\mathfrak{B}_i)$, $i=1, 2, \cdots, r$.

Theorem 1 implies that $\mathfrak{B}_i$ is the largest regular v_i-ideal in $\mathfrak{o}$. For definiteness, take $i=1$, and let $\{\mathfrak{q}_i\}$ be the sequence of v_1-ideals in $\mathfrak{o}$. Let $\pi_1, \cdots, \pi_n$ be the set of elements, constructed in Theorem 5 for v_1, and let $d'=\prod_{i=2}^{n} s_i$. Let $\mathfrak{q}_h$ be the v_1-ideal in the sequence of value $v_{d'}(b_1, \cdots, b_n)$. Theorem 4 (a) implies that, for all $j\geq h$, and for all $m\geq 0$, $v_1(\mathfrak{q}_{j+m})\in R_{d'}(b_1, \cdots, b_n)$, and hence that there exist $d_1=d_\mathfrak{p}d'$ distinct canonical products of $\pi_1, \cdots, \pi_n$ of value $v_1(\mathfrak{q}_{j+m})$. Since these canonical products are linearly independent modulo $\mathfrak{q}_{j+m+1}$, we conclude that $\mathfrak{q}_j$ is a regular v_1-ideal for all $j\geq h$.

On the other hand, $v_{d'}(b_1, \cdots, b_n)-1\in R_{d'-1}(b_1, \cdots, b_n)$, by Theorem 4 (b), whence there exist only $d_\mathfrak{p}(d'-1)<d_1$ canonical products of $\pi_1, \cdots, \pi_n$ of value $v_1(\mathfrak{q}_{h-1})$ which are linearly independent modulo $\mathfrak{q}_h$. It follows that neither is $\mathfrak{q}_{h-1}$ nor any $\mathfrak{q}_j\supset\mathfrak{q}_{h-1}$ a regular v_1-ideal. We conclude that $\mathfrak{q}_h=\mathfrak{B}_1$, and consequently $v_1(\mathfrak{B}_1)=v_{d'}(b_1, \cdots, b_n)$.

Since $\delta(\mathfrak{B}_1) = \sum_{j=0}^{h-1} \dim (\mathfrak{q}_j/\mathfrak{q}_{j+1})$, where $\mathfrak{q}_0=\mathfrak{o}$, and since $\dim (\mathfrak{q}_j/\mathfrak{q}_{j+1}) = d_\mathfrak{p}\chi(v_1(\mathfrak{q}_j))$, it follows that $\delta(\mathfrak{B}_1) = d_\mathfrak{p}\chi\sum_{j=0}^{h-1}(v_1(\mathfrak{q}_j))$. Furthermore by Theorem 4 (c) we have $\sum_{j=0}^{h-1}\chi(v_1(\mathfrak{q}_j)) = 2^{-1}d'v_{d'}(b_1, \cdots, b_n)$, whence $\delta(\mathfrak{B}_1) = 2^{-1}d_1 v_1(\mathfrak{B}_1)$.

COROLLARY. *If $\bar{\mathfrak{o}}$ is the integral closure of $\mathfrak{o}$ in K, and $\mathfrak{C}$ is the conductor between $\bar{\mathfrak{o}}$ and $\mathfrak{o}$, then $\dim (\bar{\mathfrak{o}}/\mathfrak{C}) = 2 \dim (\mathfrak{o}/\mathfrak{C})$.*

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{o}$. Clearly $\mathfrak{o}_\mathfrak{p}\mathfrak{C}\subset\mathfrak{C}_\mathfrak{p}$. Since $\bar{\mathfrak{o}}_\mathfrak{p}$ is a finite $\mathfrak{o}_\mathfrak{p}$-module (compare Chevalley [2, Theorem 3, chap. 4] or Zariski [12, p. 507]), we have $\bar{\mathfrak{o}}_\mathfrak{p}=\sum_{i=1}^m \mathfrak{o}_\mathfrak{p}\beta_i$, $\beta_i\in K$, $i=1, 2, \cdots, m$. If $z\in\mathfrak{C}_\mathfrak{p}$, then $z\beta_i\in\mathfrak{o}_\mathfrak{p}$, for all $i=1, 2, \cdots, m$. Write $z\beta_i=(\eta_i/\eta_0)$, $\eta_i\in K$, $i=0, 1, \cdots, m$, and $\eta_0\notin\mathfrak{p}$. Then $(\eta_0 z)\beta_i=\eta_i\in\mathfrak{o}$ for each i, whence $\eta_0 z\in\mathfrak{C}$. Hence $z\in\mathfrak{o}_\mathfrak{p}\mathfrak{C}$, and it follows that $\mathfrak{o}_\mathfrak{p}\mathfrak{C}=\mathfrak{C}_\mathfrak{p}$.

Let $\mathfrak{C}=\bigcap_{i=1}^s\mathfrak{q}_i$ be a representation of $\mathfrak{C}$ as the intersection of primary ideals, and let $\mathfrak{p}_i$ be the associated prime ideal of $\mathfrak{q}_i$. The preceding equality implies that $\mathfrak{q}_i=\mathfrak{C}_{\mathfrak{p}_i}\cap\mathfrak{o}$, $i=1, 2, \cdots, s$, and, since $\mathfrak{C}_{\mathfrak{p}_i}$ is a complete $\mathfrak{p}_i$-ideal in $\mathfrak{o}_{\mathfrak{p}_i}$, that each $\mathfrak{q}_i$ is a complete $\mathfrak{p}_i$-ideal in $\mathfrak{o}$. Hence $\mathfrak{C}$ is a complete ideal in $\mathfrak{o}$, and $d(\mathfrak{C})=\dim(\bar{\mathfrak{o}}/\mathfrak{C})=\sum_{i=1}^s d(\mathfrak{C}_{\mathfrak{p}_i})$. Moreover, it is readily verified that $\delta(\mathfrak{C})=\dim(\mathfrak{o}/\mathfrak{C})=\sum_{i=1}^s\delta(\mathfrak{C}_{\mathfrak{p}_i})$. The corollary now follows at once from the theorem.

PART II. THE GEOMETRY IN THE LARGE

6. Geometric preliminaries. Throughout part II, we consider a fixed irreducible plane curve $\Gamma: F(X_0, X_1, X_2)=0$ of degree m, defined over an arbitrary ground field k, with function field K. We denote by (x_0, x_1, x_2) the set of homogeneous coordinates of Γ. For our purposes, it will be convenient to define *a point* of Γ to be a complete set of conjugate points in the ordinary sense. It will also help to make a few minor changes in the notation of part I. If P is a point of Γ, we denote by $\mathfrak{o}_P$ (rather than $\mathfrak{o}_\mathfrak{p}$) the local ring of P on Γ. If v_i, $i=1, 2, \cdots, r$, are the valuations of K whose valuation rings contain $\mathfrak{o}_P$, we say that each v_i has center P on Γ, and call the intersection of v_i-ideals, $i=1, 2, \cdots, r$, in $\mathfrak{o}_P$ a complete P-ideal. Because of the identification of conjugate points, every valuation of K has a uniquely determined center on Γ.

By definition, a prime divisor of K is a complete set of conjugate places of K. To each prime divisor $\boldsymbol{p}$ is associated a unique valuation $v_\boldsymbol{p}$ of K, and conversely. By the center of $\boldsymbol{p}$ on Γ is meant the center of the corresponding valuation $v_\boldsymbol{p}$, and by the degree $d(\boldsymbol{p})$ of $\boldsymbol{p}$ is meant $d(v_\boldsymbol{p})$. A divisor of K is any formal power product $\boldsymbol{B}=\boldsymbol{p}_1^{\mu_1}\boldsymbol{p}_2^{\mu_2}\cdots\boldsymbol{p}_s^{\mu_s}$ of prime divisors $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_s$ with arbitrary integral exponents $\mu_1, \cdots, \mu_s$. Its degree $d(\boldsymbol{B})$ is defined to be $d(\boldsymbol{B})=\sum_{i=1}^s \kappa_i d(\boldsymbol{p}_i)$.

Let $\Gamma': G(X_0, X_1, X_2)=0$ be a curve not containing Γ as a component, and let $\boldsymbol{p}$ be a prime divisor of K. If P is the center of $\boldsymbol{p}$ on Γ, $X_\lambda\neq 0$ at P for some $\lambda=0, 1$, or 2. We define the intersection of Γ and Γ' at $\boldsymbol{p}$ to be the divisor $\boldsymbol{p}^\mu$ where $\mu=v_\boldsymbol{p}(G((x_0/x_\lambda), (x_1/x_\lambda), (x_2/x_\lambda)))$, and define the intersection multiplicity $i(\boldsymbol{p};\Gamma, \Gamma')$ of Γ and Γ' at $\boldsymbol{p}$ to be $d(\boldsymbol{p}^\mu)$. If $\boldsymbol{p}_1=\boldsymbol{p}, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_r$ are all the prime divisors of center P on Γ, we define the intersection multiplicity $i(P;\Gamma, \Gamma')$ to be $\sum_{j=1}^r i(\boldsymbol{p}_j; \Gamma, \Gamma')$. Thus the complete intersection of Γ and Γ' is a divisor (Γ, Γ') whose degree $i(\Gamma, \Gamma')=\sum_{P\in\Gamma} i(P;\Gamma, \Gamma')$. Bézout's theorem asserts that if Γ' is of degree n, $i(\Gamma, \Gamma')=m\cdot n$.

It will be convenient to denote by $g(n)$ the linear series cut out on Γ by

the system of all curves of order n, and by $g(\boldsymbol{B}; n)$ the system of all curves of order n whose complete intersection with Γ contains the integral divisor $\boldsymbol{B}$ as a fixed component. The quantity dim $g(n) -$ dim $g(\boldsymbol{B}; n)$ is a constant for all n sufficiently large. We define $\delta(\boldsymbol{B}) =$ dim $g(n) -$ dim $g(\boldsymbol{B}; n)$ for large n. $\delta(\boldsymbol{B})$ designates the number of conditions which the divisor $\boldsymbol{B}$ imposes on the curves of sufficiently high degree.

Let $\boldsymbol{B}_i$, $i = 1, 2, \cdots, h$, be integral divisors, and assume that each prime factor of $\boldsymbol{B}_i$ has its center at a given point P_i of Γ, $P_i \neq P_j$, $i \neq j$. Then the theorem on the independence of conditions asserts that, if $\boldsymbol{B} = \prod_{i=1}^{h} \boldsymbol{B}_i$, then

$$(12) \qquad\qquad \delta(\boldsymbol{B}) = \sum_{i=1}^{h} \delta(\boldsymbol{B}_i).$$

Let P be a point of Γ and let $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_r$ be the prime divisors of K of center P, with $v_1, \cdots, v_r$ the corresponding valuations. There is a natural one-one correspondence between the integral divisors of the form $\boldsymbol{A} = \boldsymbol{p}_1^{\mu_1} \cdots \cdots \boldsymbol{p}_r^{\mu_r}$ and complete P-ideals $\mathfrak{q}$ in $\mathfrak{o}_P$: $\boldsymbol{A} \leftrightarrow \mathfrak{q}$ if and only if $\mu_i = v_i(\mathfrak{q})$, $i = 1, 2, \cdots, r$. For corresponding pairs $\boldsymbol{A}$, $\mathfrak{q}$, the

$$(13) \qquad\qquad \text{basic equalities } \delta(\boldsymbol{A}) = \delta(\mathfrak{q}), \quad d(\boldsymbol{A}) = d(\mathfrak{q})$$

are easily verified.

7. **Adjoint curves.** Let P be a point of Γ. The conductor $\mathfrak{C}_P$ between $\mathfrak{o}_P$ and $\bar{\mathfrak{o}}_P$ is, by Theorem 3, a complete P-ideal. The divisor corresponding to $\mathfrak{C}_P$ is designated by $\boldsymbol{C}_P$ and is called the adjoint divisor at P.

If P is a simple point of Γ, $\boldsymbol{C}_P$ is the unit divisor. Since Γ has only a finite number of singular points, the divisor $\boldsymbol{C} = \prod_{P \in \Gamma} \boldsymbol{C}_P$ is well-defined and is called the adjoint divisor of Γ.

DEFINITION. An adjoint curve to Γ is any curve which cuts out on Γ a multiple of the adjoint divisor $\boldsymbol{C}$.

LEMMA 4. *If $\boldsymbol{A}$ is any integral divisor, we have $\delta(\boldsymbol{A}\boldsymbol{C}) = \delta(\boldsymbol{C}) + d(\boldsymbol{A})$.*

Proof. Let $\boldsymbol{A}\boldsymbol{C} = \prod_{i=1}^{t} \boldsymbol{A}_{P_i} \boldsymbol{C}_{P_i}$ where $\boldsymbol{A}_{P_i}$, $\boldsymbol{C}_{P_i}$ are the factors of $\boldsymbol{A}$ and $\boldsymbol{C}$ respectively which contain those prime divisors of center P_i on Γ. Let $\mathfrak{q}_i$ be the complete P_i-ideal in $\mathfrak{o}_{P_i}$ which corresponds to $\boldsymbol{A}_{P_i}\boldsymbol{C}_{P_i}$, $i = 1, 2, \cdots, t$. It follows at once from equations (12) and (13) that $\delta(\boldsymbol{C}) = \sum_{i=1}^{t} \delta(\boldsymbol{C}_{P_i})$ $= \sum_{i=1}^{t} \delta(\mathfrak{C}_{P_i})$, and $\delta(\boldsymbol{A}\boldsymbol{C}) = \sum_{i=1}^{t} \delta(\boldsymbol{A}_{P_i}\boldsymbol{C}_{P_i}) = \sum_{i=1}^{t} \delta(\mathfrak{q}_i)$, whence $\delta(\boldsymbol{A}\boldsymbol{C})$ $= \delta(\boldsymbol{C}) + \sum_{i=1}^{t} [\delta(\mathfrak{q}_i) - \delta(\mathfrak{C}_{P_i})]$. Since each $\mathfrak{C}_{P_i}$ is a regular ideal[4],

---

[4] In the case in which k is infinite a simple proof of the regularity of $\mathfrak{C}_P$, for any point P of Γ, can be given. For then there exists an element $z \in \mathfrak{C}_P$ such that $v_j(z) = v_j(\mathfrak{C}_P)$, $j = 1, 2, \cdots, r$, where $v_1, v_2, \cdots, v_r$ are valuations of K of center P on Γ. Let $\mathfrak{q} \subset \mathfrak{C}_P$ be a complete P-ideal. Define the ideal $\mathfrak{q}'$ in $\bar{\mathfrak{o}}_P$ by the relations: $v_j(\mathfrak{q}') = v_j(\mathfrak{q}) - v_j(\mathfrak{C}_P)$, $j = 1, 2, \cdots, r$. Then dim $\bar{\mathfrak{o}}_P/\mathfrak{q}'$ $= d(\mathfrak{q}) - d(\mathfrak{C}_P)$. If ω_i, $i = 1, 2, \cdots, d(\mathfrak{q}) - d(\mathfrak{C}_P)$, form an independent basis for $\bar{\mathfrak{o}}_P$ mod $\mathfrak{q}'$, the elements $z\omega_i$ form an independent basis for $\mathfrak{C}_P$ mod $\mathfrak{q}$. Thus dim $\mathfrak{C}_P/\mathfrak{q} = d(\mathfrak{q}) - d(\mathfrak{C}_P)$ and so $\mathfrak{C}_P$ is a regular ideal.

$$\delta(\mathfrak{q}_i) - \delta(\mathfrak{C}_{P_i}) = d(\mathfrak{q}_i) - d(\mathfrak{C}_{P_i}) = d(A_{P_i}).$$

Hence $\delta(AC) = \delta(C) + d(A)$, as asserted.

THEOREM 7 (THE NOETHER FUNDAMENTALSATZ). *Let* $\Gamma' : G(X) = 0$ *be a curve not containing* Γ *as a component, and let* $A = (\Gamma, \Gamma')$. *Then if* $\Gamma'' : H(X) = 0$ *cuts out a multiple of* AC *on* Γ, *there exist forms* $A(X)$, $B(X)$ *with coefficients in* k *such that* $H(X) = A(X)F(X) + B(X)G(X)$.

Proof[5]. We treat first the case in which the degree n of Γ'' is sufficiently high so that $\delta(AC) = \dim g(n) - \dim (AC; n)$, and also that $n \geqq m + e$, where e is the degree of Γ'. In this case,

$$\dim g(AC; n) = (n+1)(n+2)/2 - (n-m+1)(n-m+2)/2 - \delta(AC).$$

Since $\delta(AC) = \delta(C) + d(A)$ by Lemma 4 and since $d(A) = m \cdot e$, it follows that

(14) $\dim g(AC; n) = nm - em - (1/2)m(m-3)/2 - \delta(C)$.

On the other hand, let g' denote the linear series cut out on Γ by the system of all curves of the form $A(X)F(X) + B(X)G(X) = 0$ of degree n for which $B(X) = 0$ is an adjoint curve. Clearly $g' \subset g(AC; n)$, and $\dim g' \geqq \dim g(C; n-m) = nm - em(m^2 - 3m)/2 - \delta(C)$. It follows from (14) that $g' = g(AC; n)$.

If the degree n of Γ'' is arbitrary, let $P_1, \cdots, P_s$ be the points of intersection of Γ and Γ'. There exists an irreducible curve $\phi(X) = 0$ which does not pass through any P_i, $i = 1, 2, \cdots, s$. By the first part of the theorem, we have, for σ sufficiently large,

(15) $\phi(X)^\sigma H(X) = A(X)F(X) + B(X)G(X)$,

for suitable forms $A(X)$, $B(X)$. Let $X = (X_1/X_0)$, $Y = (X_2/X_0)$, and let ξ_1, ξ_2 be the residues of X, Y respectively modulo $\phi(1, X, Y)$. Let $(G(1, \xi_1, \xi_2)) = \bigcap_{j=1}^h \mathfrak{q}_j$ be the decomposition of this ideal into primary components in the ring $k[\xi_1, \xi_2]$. Since $A(1, \xi_1, \xi_2)F(1, \xi_1, \xi_2) = -B(1, \xi_1, \xi_2)G(1, \xi_1, \xi_2)$, $A(1, \xi_1, \xi_2)F(1, \xi_1, \xi_2) \in \mathfrak{q}_j$ for all $j = 1, 2, \cdots, h$. If, for some j, $F(1, \xi_1, \xi_2) \in \text{rad } \mathfrak{q}_j$, it would imply that the three curves Γ, Γ', and $\phi(X) = 0$ have a point in common, contrary to the construction of $\phi(X)$. Hence $A(1, \xi_1, \xi_2) \in \bigcap_{j=1}^h \mathfrak{q}_j = (G(1, \xi_1, \xi_2))$. It follows easily that $A(X) = A_0(X)G(X) + A_1(X)\phi(X)$, $B(X) = -A_0(X_0)G(X) + B_1(X)\phi(X)$ for suitable forms $A_0(X)$, $A_1(X)$, and $B_1(X)$.

Substituting these relations in (15), we conclude that $\phi(X)^{\sigma-1}H(X) = A_1(X)F(X) + B_1(X)G(X)$. By σ repetitions of this argument, we complete the proof of the theorem.

The completeness of the adjoint series is an immediate corollary of the

---

[5] Compare the proof in Severi [9].

Noether Fundamentalsatz, as is well known([6]).

THEOREM 8. *The adjoint curves of any order cut out complete linear series on* Γ.

8. **Adjoint curves of order** $m-3$ **and the canonical series**([7]). Our present object is to derive the following basic properties of the adjoint curves:

THEOREM 9. *The adjoint curves of order* $m-3$ *cut out on* Γ *outside of the fixed component* **C** *the complete canonical series.*

THEOREM 10. $d(C) = 2\delta(C)$.

As a direct corollary of these two results, we shall also obtain:

THEOREM 11. *If the genus*([8]) *of* Γ *is denoted by g, then*

$$g = (m-1)(m-2)/2 - \delta(C).$$

We shall give two independent proofs of Theorems 9 and 10. In fact, we shall prove first that these two theorems are equivalent to each other. We shall then show that Theorem 10 is a direct consequence of Theorem 6, the main theorem of part I. Finally we shall give a proof of Theorem 9, in the case in which the function field K of Γ is separably generated over k, based upon a representation theorem for the differentials of the first kind of K.

Assume first that $d(C) = 2\delta(C)$. Take n so large that dim $g(n) -$ dim $g(C; n)$ $= \delta(C)$ and that $g(C; n)$ is a nonspecial series([9]). Then, as in (14), dim $g(C; n)$ $= mn - (m^2 - 3m)/2 - \delta(C)$. On the other hand, since $g(C; n)$ is a complete series of degree $mn - d(C)$, it follows by the Riemann-Roch theorem (Chevalley [2, Theorem 7, p. 33]) that dim $g(C; n) = mn - d(C) - g + 1$, whence

(16) $(m-1)(m-2)/2 + \delta(C) - d(C) = g.$

Since $d(C) = 2\delta(C)$, we conclude that

([6]) B. L. van der Waerden [10, p. 216].

([7]) For the definitions of the various concepts concerning algebraic curves which we shall need in this section, we refer the reader to Chapters I and II of Chevalley [2]. We point out, however, that there exists a direct connection between the notion of a *divisor class* of K as defined by Chevalley on p. 19 and the concept of a *complete linear series* on Γ: namely, the integral divisors in a divisor class of K form a complete linear series, which can be cut out on Γ by a linear system of plane curves. In particular, the integral divisors in the canonical divisor class (Chevalley p. 32) form the *canonical series*. Furthermore the degree and dimension of a divisor class is equal respectively to the degree and dimension of the corresponding complete linear series. Hence the canonical series is of dimension g and of degree $2g - 2$, where g is the genus of K (Chevalley, chapter II, Theorems 4 and 6).

([8]) By the genus of Γ we mean the genus of the function field K of Γ.

([9]) A linear series is called *special* if it is a subseries of the canonical series; otherwise it is called *nonspecial*. A series of degree greater than $2g - 2$ is necessarily nonspecial (Chevalley [2, p. 32, corollary]).

(17) $$m(m - 3) - d(C) = 2g - 2,$$

and

(18) $$(m - 1)(m - 2)/2 - \delta(C) = g$$

(which establishes Theorem 11).

(17) implies that deg $g(C; m-3) = 2g-2$, while (18) implies that dim $g(C; m-3) \geqq g$. Since $g(C; m-3)$ is complete, it follows at once from the Riemann-Roch theorem that $g(C; m-3)$ is a special series. In fact, dim $g(C; m-3) - \deg g(C; m-3) + g - 1 \geqq g - (2g-2) + g - 1 = 1$, whence $g(C; m-3)$ is a subseries of the canonical series. Since its degree, $2g-2$, is equal to the degree of the canonical series, it follows that $g(C; m-3)$ is itself the complete canonical series.

Conversely, if we assume Theorem 9, then

$$\deg g(C; m-3) = m(m-3) - d(C) = 2g - 2.$$

Combining this equality with equation (16) gives at once $d(C) = 2\delta(C)$.

To prove Theorem 10, let $P_1, P_2, \cdots, P_s$ be the singular points of Γ. Since $d(\mathbb{C}_{P_i}) = 2\delta(\mathbb{C}_{P_i})$, $i = 1, 2, \cdots, s$, by Theorem 6, we have $d(C_{P_i}) = 2\delta(C_{P_i})$, $i = 1, 2, \cdots, s$, in view of (13). Since $C = \prod_{i=1}^{s} C_{P_i}$, it follows immediately that $d(C) = 2\delta(C)$.

Finally let (X, Y) be a set of nonhomogeneous plane coordinates. For simplicity, denote by $F(X, Y) = 0$ the nonhomogeneous equation of Γ, of degree m, and let (x, y) be corresponding nonhomogeneous coordinates of the general point of Γ. Assume that the function field $K = k(x, y)$ of Γ is separably generated over k. Then either x or y is a separating variable. We assume, for definiteness, that x is a separating variable, and that y is an integral element over $k(x)$[10].

If $\Gamma' : \phi(X_0, X_1, X_2) = 0$ is an adjoint curve to Γ, we shall write $\phi(X, Y) = 0$ for the nonhomogeneous equation of Γ', and shall say that $\phi(X, Y) = 0$ is an adjoint curve of order n if deg $\phi(X, Y) \leqq n$.

Since the differentials of K[11] form one complete divisor class—the canonical class—Theorem 9 is a direct corollary of the following representation theorem.

THEOREM 12. *A differential $\bar{\omega}$ of K is of the first kind if and only if it can be written in the form $(\phi(x, y)/F'_y(x, y))dx$, where $\Gamma' : \phi(X, Y) = 0$ is an adjoint curve of order $m-3$. If $\bar{\omega}$ is of the first kind, the divisor of $\bar{\omega} = (\Gamma, \Gamma')/C$.*

---

[10] If k is infinite, this is no restriction; for then $ax + by = y_1$ will be integral over $k(x)$ for suitable $a, b \in k$, and the curve Γ_1 whose general point is x, y_1 will be projectively equivalent to Γ.

[11] For the definitions of a differential of K, the order of a differential, the divisor of a differential, a differential of the first kind, etc., see Chevalley [2, chapter II, §§5 and 6]. Since x is a separating variable for K, every differential of K is of the form $A dx$, $A \in K$ (Chevalley chapter VI, Theorem 4).

Proof. If $\tilde{\omega}$ is any differential of K, we can write $\tilde{\omega} = (\phi(x, y)/F'_y (x, y))dx$, where $\phi(x, y) \in K$. Let $\mathfrak{o} = k[x, y]$, and let $\mathfrak{C}$ be the conductor between $\bar{\mathfrak{o}}$ and $\mathfrak{o}$. The following results are well known:

$\mathfrak{o}F'_y (x, y) = \mathfrak{C}\mathfrak{D}$ where $\mathfrak{D}$ is the different of K with respect to $k(x)$ (Hecke[6, p. 145]).

$v_p(\mathfrak{D}) = v_p(dx)$ for any prime divisor p of K whose center on Γ is at finite distance in the (X, Y)-plane (Chevalley [2, Theorem 7, p. 110]).

Together these results imply that $v_p(\tilde{\omega}) \geqq 0$ if and only if $v_p(\phi(x, y)) \geqq v_p(\mathfrak{C})$. Thus $\tilde{\omega}$ is of the first kind at finite distance if and only if $v_p(\phi(x, y)) \geqq v_p(\mathfrak{C})$ for all prime divisors of center at finite distance on Γ. Since $\mathfrak{C}$ is a complete ideal, this last condition is equivalent to the assertion $\phi(x, y) \in \mathfrak{C}$, which in turn is equivalent to the statements: $\phi(x, y)$ is a polynomial in x, y and $\phi(x, y) \in \mathfrak{C}_P$ for every point P of Γ at finite distance (compare proof of corollary to Theorem 6).

Consider now the nonhomogeneous plane coordinates: $X' = X_0/X_1$, $Y' = X_2/X_1$; and $\overline{X} = X_0/X_2$, $\overline{Y} = X_1/X_2$. Every point P of Γ at infinity in the (X, Y)-plane (at least one such point exists) is at finite distance in either the (X', Y')- or $(\overline{X}, \overline{Y})$-plane.

If x', y' are nonhomogeneous (X', Y')-coordinates of Γ, then $x' = 1/x$, $y' = y/x$. Write $F(X, Y) = F'(X', Y')/X'^m$ and $\phi(X, Y) = \phi'(X, Y')/X'^h$, where h is the degree of $\phi(X, Y)$. We have $F'_y (x, y) = F'_{y'}(x', y')/x'^{m-1}$ and also, since x is a separating variable, $dx = -(1/x'^2)dx'$. It follows that $\tilde{\omega} = -(\phi'(x', y')x'^{m-3-h}/F'_{y'}(x', y'))dx'$.

In the second case, write $F(X, Y) = \overline{F}(\overline{X}, \overline{Y})/\overline{Y}^m$, $\phi(X, Y) = \bar{\phi}(\overline{X}, \overline{Y})/\overline{Y}^h$, and let $\bar{x}, \bar{y}$ be nonhomogeneous $(\overline{X}, \overline{Y})$-coordinates of Γ. Then $\bar{x} = x/y$, $\bar{y} = 1/y$. If y is also a separating variable, then $dx/F'_y (x, y) = -dy/F'_x (x, y)$, and it follows that $\tilde{\omega} = -(\bar{\phi}(x, y)\bar{y}^{m-3-h}/\overline{F}'_{\bar{y}}(\bar{x}, \bar{y}))d\bar{x}$. If, however, y is not a separating variable, we find directly that $F'_y (x, y) = \overline{F}'_{\bar{y}}(\bar{x}, \bar{y})/\bar{y}^{m-2}$. Let D_x be the unique derivation of K for which $D_x(x) = 1$. We have then by Chevalley [2, Chap. 6, Theorem 9] $d\bar{x} = D_x(\bar{x})dx = (1/y - (x/y^2)D_x(y))dx = (1/y)dx$ since $D_x(y) = 0$. We conclude in this case that $\tilde{\omega} = (\bar{\phi}(\bar{x}, \bar{y})\bar{y}^{m-3-h}/\overline{F}'_{\bar{y}}(\bar{x}, \bar{y}))d\bar{x}$.

For $\tilde{\omega}$ to be of the first kind at *every* point of Γ, it follows from the first part of the proof that we must have (in addition to the conditions already obtained) that $\phi'(x', y')x'^{m-3-h}$ and $\bar{\phi}(\bar{x}, \bar{y})\bar{y}^{m-3-h}$ are polynomials in x', y' and $\bar{x}, \bar{y}$ respectively, which belong to $\mathfrak{C}_P$ for every point P of Γ at finite distance in the (X', Y')- or $(\overline{X}, \overline{Y})$-plane, as the case may be; and conversely. Since $\phi'(x', y')$ and $\bar{\phi}(\bar{x}, \bar{y})$ are not divisible by x' or $\bar{y}$ respectively, these conditions imply that $h \leqq m - 3$.

There exists then a form $\Phi(X_0, X_1, X_2)$ of degree $m - 3$ such that $\Phi(1, x, y) = \phi(x, y)$, $\Phi(x', 1, y') = \phi'(x', y')x'^{m-3-h}$, and $\Phi(x, y, 1) = \bar{\phi}(\bar{x}, \bar{y})\bar{y}^{m-3-h}$. It follows that $\tilde{\omega}$ is of the first kind if and only if $\Phi(X_0, X_1, X_2) = 0$ is an adjoint curve to Γ of order $m - 3$.

The final assertion of the theorem follows directly from the proof.

BIBLIOGRAPHY

1. C. Chevalley, *On the theory of local rings*, Ann. of Math. vol. 44 (1943) pp. 690–708.

2. ———, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, no. 6, New York, American Mathematical Society, 1951.

3. W. L. Chow, *Die geometrische Theorie der algebraischen Funktionen für beliebige vollkommene Körper*, Math. Ann. (1937) pp. 656–682.

4. I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. vol. 59 (1946) pp. 54–106.

5. Enriques-Chisini, *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche*, vol. 2, Bologna, 1915.

6. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, Akademische Verlagsgesellschaft, 1923.

7. A. Seidenberg, *Valuation ideals in polynomials rings*, Trans. Amer. Math. Soc. vol. 57 (1945) pp. 387–425.

8. F. Severi, *Trattato di geometria algebrica*, vol. 1, part I, Bologna, 1926.

9. ———, *Vorlesungen über algebraischen Geometrie*, Leipzig, 1921.

10. B. L. van der Waerden, *Einführung in die algebraische Geometrie*, Die Grundlehren der Mathematischen Wissenschaften, Berlin, 1939.

11. O. Zariski, *Polynomial ideals defined by infinitely near base points*, Amer. J. Math. vol. 60 (1938).

12. ———, *Foundations of a general theory of birational correspondences*, Trans. Amer. Math. Soc. vol. 53 (1943) pp. 490–542.

13. ———, *Analytical irreducibility of normal varieties*, Ann. of Math. vol. 49 (1948) pp. 352–361.

CLARK UNIVERSITY,
    WORCESTER, MASS.