

SOME MULTIPLICATIVE PROPERTIES OF COMPLETE IDEALS⁽¹⁾

BY

H. T. MUHLY AND M. SAKUMA⁽²⁾

1. Let L be a noetherian domain that is integrally closed in its quotient field F . To each ideal A of L is assigned an ideal A_a , the integral closure or completion of A , that consists of all elements $x \in L$ for which an equation of the form, $x^n + a_1x^{n-1} + \dots + a_n = 0$, $a_i \in A^i$, holds. If Ω is the set of all valuations v of F such that the associated valuation ring R_v contains L , then A_a coincides with the ideal $A_b = \{x; v(x) \geq v(A), \forall v \in \Omega\}$, [2; 3]. An ideal A is said to be complete if $A = A_a$, and the set of all complete ideals is denoted by $\Gamma(L)$. If A and B belong to $\Gamma(L)$, the product AB may not belong to $\Gamma(L)$, but the completion of the product $(AB)_a$ does. Hence a binary composition " \times " is defined on $\Gamma(L)$ by the condition, $A \times B = (AB)_a$. Under this composition $\Gamma(L)$ is a commutative semigroup with an identity in which the cancellation law holds [2].

In case L is a two dimensional regular local ring, Zariski has shown [4, Appendix 5] that $(\Gamma(L), \times)$ is a Gaussian semigroup, and that the composition \times is ordinary product. In this paper we study the case in which L is a two dimensional normal local domain which is subject to conditions less stringent than regularity. (See §2 below.) It is shown that modulo a simple equivalence relation the semigroup $(\Gamma_0(L), \times)$ is Gaussian, where $\Gamma_0(L)$ is the subset of $\Gamma(L)$ that consists of primary ideals belonging to the maximal ideal of L . However $(\Gamma_0(L), \times)$ is not Gaussian in an absolute sense for in simple examples it is seen that the maximal ideal M of L is an irreducible element of $(\Gamma(L), \times)$ that is not "prime." (Here we are using the semigroup terminology of Jacobson [1, Chapter IV].)

Our methods are direct extensions of those of Zariski. In case L is regular, the form ring associated with L and the sequence of powers of the maximal ideal M is a polynomial ring over a field and Zariski's arguments are based in part on the fact that such a ring is a unique factorization domain. In our case the form ring is an integrally closed noetherian domain, and we obtain results analogous to Zariski's by using the Artin theory of factorization in the sense of "quasi-equality" that is valid in such domains.

2. Let (L, M) be an integrally closed local domain of dimension two and assume that L has an infinite residue field k . Let u_1, u_2, \dots, u_n be a fixed minimal basis

Presented to the Society, November 18, 1961; received by the editors January 2, 1962.

(1) Work on this paper was completed under NSF grant NSF-G17850.

(2) On leave from Tokushima University, Tokushima, Japan.

of the maximal ideal M , and let $R = k[X_1, X_2, \dots, X_n]$ where the X_i are indeterminates. Denote by N the ideal in R generated by forms $\check{f}(X)$ ⁽³⁾ of degree t that are such that $f(u) \in M^{t+1}$. If $\mathfrak{o} = R/N = k[x_1, x_2, \dots, x_n]$, then \mathfrak{o} is the form ring of L and has transcendence degree 2 over k . Since N is homogeneous it defines a variety in the projective space $P_{n-1}(k)$, which is in this case an algebraic curve. Our considerations in this paper will be based largely on the following two assumptions:

- (1) \mathfrak{o} is an integrally closed domain so that the variety V defined by N is irreducible and arithmetically normal;
- (2) the linear system cut out on V by the hyperplanes of its ambient space is nonspecial.

The fact that \mathfrak{o} is a domain implies that the pseudo-valuation v_M defined by the sequence of powers of M can be extended to a valuation of F . We shall follow the terminology of Zariski and speak of the v_M -value of an element or ideal of L as the order of the element or ideal. We denote by Ω_0 that subset of Ω that consists of valuations v distinct from v_M that are such that R_v (the valuation ring of v) dominates L . (That is, $M_v \cap L = M$, where M_v is the maximal ideal of R_v .) Let N^* be the ideal generated by all forms $\check{f}(X)$ of degree t such that $v(f(u)) > tv(M)$ for all $v \in \Omega_0$. It is easy to verify that $N^* = \text{Rad } N$, and since (1) implies that N is prime we have $N^* = N$. Since v_M is a valuation it follows that if u is an element of order one then $M^t : uL = M^{t-1}$ for all $t \geq 1$. Moreover, the ring

$$L_u = L[u_1/u, u_2/u, \dots, u_n/u]$$

is integrally closed in F . In fact, if θ is integral over L_u , then θ satisfies an equation, $\theta^t + a_1\theta^{t-1} + \dots + a_t = 0$, $a_i \in L_u$. If d_i is the degree of a_i as a polynomial in $u_1/u, \dots, u_n/u$ and if e is an integer such that $ei \geq d_i$ for all i , then $u^{ei}a_i \in M^{ei}$ and $u^e\theta \in (M^e)_a$. Since M^e is a valuation ideal it is complete so that it follows that $\theta \in L_u$. It is to be noted that if M_u is a maximal ideal in L_u such that $M_u \cap L = M$, then L_u/M_u is algebraic over k . In fact, the field L_u/M_u is generated over k (as a polynomial ring) by the M_u -residues of the quotients $u_1/u, u_2/u, \dots, u_n/u$. (See [6].)

Our second assumption implies that if $\check{f}(x)$ and $\check{g}(x)$ are homogeneous elements of \mathfrak{o} of degree r and s respectively such that the ideal $\mathfrak{o}\check{f} + \mathfrak{o}\check{g}$ is irrelevant, then the ideal $\mathfrak{o}\check{f} + \mathfrak{o}\check{g}$ contains all homogeneous elements of \mathfrak{o} of degree not less than $r + s$. In fact, if $\phi(A, t)$ denotes the k -dimension of the space of forms of degree t in A , then when (\check{f}, \check{g}) is irrelevant, $\phi((\check{f}, \check{g}), t) = \phi(\mathfrak{o}\check{f}, t) + \phi(\mathfrak{o}\check{g}, t) - \phi(\mathfrak{o}(\check{f}\check{g}), t)$ in view of the fact that \mathfrak{o} is integrally closed. Since all multiples of the system of

(3) If $f(X) \in L[X_1, X_2, \dots, X_n]$ we shall use the notation $\check{f}(X)$ to denote the element of R obtained from f by taking its coefficients modulo M . Similarly, if $\check{f}(X)$ is a given element of R (or if $\check{f}(x)$ is a given element of R/N) then $f(X)$ will denote a representative polynomial for $\check{f}(X)$ or for $\check{f}(x)$ with coefficients in L . This convention will be used throughout the paper without further mention.

hyperplane sections on V are complete and nonspecial, a simple application of the Riemann-Roch theorem yields the desired result.

3. If M_1 is a maximal ideal of the ring $L_1 = L[u_2/u_1, \dots, u_n/u_1]$ such that $M_1 \cap L = M$, and if $c_i (i = 2, 3, \dots, n)$ is the residue of u_i/u_1 modulo M_1 , then c_i is algebraic over k and the point $C = (1, c_2, \dots, c_n)$ belongs to V . Indeed, if $f(X)$ is a form of degree t that belongs to N then $f(u) \in M^{t+1}$. Hence $f(1, u_2/u_1, \dots, u_n/u_1)$ belongs to $ML_1 \subset M_1$, which shows that $\bar{f}(1, c_2, \dots, c_n) = 0$. Moreover, if \mathfrak{p} is the prime ideal in $k[x_2/x_1, \dots, x_n/x_1]$ determined by point C , and if

$$\bar{f}_1(x_2/x_1, \dots, x_n/x_1), \dots, \bar{f}_t(x_2/x_1, \dots, x_n/x_1)$$

is a basis for \mathfrak{p} , a straightforward computation shows that the ideal $ML_1 + L_1 f_1(\dots, u_i/u_1, \dots) + \dots + L_1 f_t(\dots, u_i/u_1, \dots)$ is equal to M_1 . Conversely, if $C = (1, c_2, \dots, c_n)$ is any point of V that is algebraic over k (here we have assumed $c_1 \neq 0$ and normalized) and if $(\bar{h}_1(\dots, x_i/x_1, \dots), \dots, \bar{h}_s(\dots, x_i/x_1, \dots))$ is the non-homogeneous prime ideal determined by C , then $ML_1 + \sum_j L_1 h_j(\dots, u_i/u_1, \dots)$ is a maximal ideal in L_1 that lies over M . In particular, if $v \in \Omega_0$, and if $v(u_1) \leq v(u_i)$, $i = 2, 3, \dots, n$ then L_1 is a subring of the valuation ring R_v and $M_v \cap L_1$ is a maximal ideal M_1 of L_1 such that $M_1 \cap L = M$. In fact, since $u_1 L_1$ is the center of v_M in L_1 it is prime, so that if M_1 is not maximal in L_1 then $M_1 = u_1 L_1$. This shows that R_v contains the quotient ring of L_1 at $u_1 L_1$, and since this latter ring is a maximal subring of F it follows that R_v coincides with it and $v = v_M$. This contradicts the fact that $v \in \Omega_0$. The point C of V that is associated with this ideal M_1 will be called the focus of v on the variety V . Some properties of the foci of valuations are described in the following lemmas. All of the ideas here are adaptations of some of those expounded in [5].

For any element θ of L of order t there is a form $\bar{\theta}_t(X) \in R$ of degree t such that $\theta - \theta_t(u) \in M^{t+1}$, and any two such forms are congruent modulo N . Hence the element $\bar{\theta}_t(x)$ of \mathfrak{v} is uniquely determined by θ . This element is called the leading form of θ .

LEMMA 3.1. *If θ is of order t , $v \in \Omega_0$ is such that $v(u_1) = v(M)$, and $C = (1, c_2, \dots, c_n)$ is the focus of v , then $v(\theta) > v(M^t)$ if and only if $\bar{\theta}(1, c_2, \dots, c_n) = 0$.*

Proof. Clear.

COROLLARY. *If x_i is not contained in the homogeneous prime ideal \mathfrak{p} of \mathfrak{v} corresponding to the focal point C of $v (v \in \Omega_0)$, then $L_i = L[u_1/u_i, \dots, u_n/u_i]$ is a subring of R_v .*

LEMMA 3.2. *The set $S_v = \{\theta; \text{ord } \theta = t, v(\theta) = v(M^t)\}$ is multiplicatively closed or each $v \in \Omega_0$.*

Proof. Since v_M is a valuation, the order of a product is the sum of the orders of the factors, and from this the lemma follows immediately.

LEMMA 3.3. *The set $Z = \{x/y; \text{ord } x \geq \text{ord } y, y \in S_v\}$ is a local ring which dominates L . In fact, if u is an element of order one in L such that $v(u) = v(M)$ then $L_u \subset Z$ and Z is a quotient ring of L_u at a maximal ideal M_u such that $M_u \cap L = M$.*

Proof. If u satisfies the conditions of the lemma then $L_u \subset Z \subset R_v$, where R_v is the valuation ring of v . If M_u is the center of v in L_u , then $M_u \cap L = M$, and M_u is maximal since $v \neq v_M$. Hence we need only observe that the quotient ring of L_u at M_u coincides with Z , and this is straightforward, q.e.d.

The local ring Z is called the first quadratic transform of L in the direction of v . In view of the above lemmas it is clear that if two valuations of Ω_0 have the same focal point C then they determine, the same quadratic transform. Indeed all valuations which dominate Z have the same focal point. For this reason we say that Z is the quadratic transform corresponding to the focal point C , and we denote it by $L'(C)$ or by $L'(p)$, where p is the ideal of C in \mathfrak{o} .

LEMMA 3.4. *Under assumption (1) of §2, the local ring $L'(C)$ is a two-dimensional regular local ring.*

Proof. We use the same notation as above. Since V is normal, C is a simple point of V . If p is the ideal of C in $k[x_2/x_1, \dots, x_n/x_1]$, then there is an element $h(x_2/x_1, \dots, x_n/x_1) \in p, h \notin p^2$. We assert that the two elements u_1 and

$$h(u_2/u_1, \dots, u_n/u_1)$$

together form a basis for the maximal ideal M' in $L'(C)$. In fact, let $f(u_2/u_1, \dots, u_n/u_1)$ be an element of M' . Then $\bar{f}(x_2/x_1, \dots, x_n/x_1)$ is an element of the field of functions Σ on V which vanishes at C and is therefore a local multiple of the uniformizing parameter at C . We therefore have,

$$\bar{f}(x_2/x_1, \dots, x_n/x_1) = h(x_2/x_1, \dots, x_n/x_1) \frac{\bar{\phi}(x_1, \dots, x_n)}{\bar{\psi}(x_1, \dots, x_n)},$$

where $\bar{\phi}$ and $\bar{\psi}$ are forms of the same degree ρ in \mathfrak{o} and $\bar{\psi}$ does not vanish at C . Let $s = \text{deg } \bar{f}, t = \text{deg } h, \bar{g}(x_1, \dots, x_n) = x_1^s \bar{f}(x_2/x_1, \dots, x_n/x_1),$ and $\bar{g}_0(x_1, \dots, x_n) = x_1^t h(x_2/x_1, \dots, x_n/x_1)$. The form

$$x_1^t \bar{\psi}(x_1, \dots, x_n) \bar{g}(x_1, \dots, x_n) - x_1^s \bar{g}_0(x_1, \dots, x_n) \bar{\phi}(x_1, \dots, x_n)$$

vanishes, so that $u_1^t \psi(u_1, \dots, u_n) g(u_1, \dots, u_n) - u_1^s g_0(u_1, \dots, u_n) \phi(u_1, \dots, u_n) = F(u_1, \dots, u_n)$, where F is a form of degree $t + s + \rho + 1$ with coefficients in L . We thus have

$$\frac{\psi(u)}{u_1^\rho} \cdot \frac{g(u)}{u_1^s} = \frac{g_0(u_1, \dots, u_n)}{u_1^t} \cdot \frac{\phi(u)}{u_1^\rho} + \frac{F(u_1, \dots, u_n)u_1}{u_1^{\rho+s+t+1}}$$

Each of the elements $\psi(u)/u_1^p$, $\phi(u)/u_1^p$ and $F(u)/u_1^{p+s+t+1}$ is an element of $L'(C)$ and since $\bar{\psi}$ does not vanish at C , $\psi(u)/u_1^p$ is a unit in $L'(C)$. It thus follows that u_1 and $h(u_2/u_1, \dots, u_n/u_1)$ generate M' . Since u_1L' is a prime ideal, and since $\bar{g}_0(x_1, \dots, x_n)$ is not zero, $g_0(u_1, \dots, u_n)$ is of order t and hence $v_M(h(u_2/u_1, \dots, u_n/u_1)) = 0$. Thus $h(u_2/u_1, \dots, u_n/u_1)$ does not belong to u_1L' so that $\dim L' \geq 2$. Since M' has a basis of two elements, our lemma follows, q.e.d.

4. Let A be an ideal of L , assume that A is of order r and that $\theta^{(1)}, \theta^{(2)}, \dots, \theta^{(s)}$ is a base of A . For at least one i the order of $\theta^{(i)}$ is r and $\text{ord } \theta^{(j)} \geq r$ for all j . Let $\bar{\theta}_r^{(j)}(x)$ be zero if $\text{ord } \theta^{(j)} > r$ and let $\bar{\theta}_r^{(j)}(x)$ be the leading form of $\theta^{(j)}$ if $\text{ord } \theta^{(j)} = r$. These elements generate a homogeneous ideal $\mathfrak{c}(A)$ in \mathfrak{o} which will be called the characteristic ideal of A . It is clear that if $\theta \in A$ then either $\text{ord } \theta > r$ and $\bar{\theta}_r(x)$ is zero by definition or else $\text{ord } \theta = r$ and $\bar{\theta}_r(x)$ is a linear combination of $\bar{\theta}_r^{(1)}(x), \bar{\theta}_r^{(2)}(x), \dots, \bar{\theta}_r^{(s)}(x)$ with coefficients in k . Since $\mathfrak{c}(A)$ is homogeneous, it is quasi-equal (in symbols: \approx) to a power product of homogeneous prime ideals of \mathfrak{o} or else $\mathfrak{c}(A)$ is irrelevant. If $\mathfrak{c}(A) \approx \mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_g^{\alpha_g}$, the prime ideals \mathfrak{p}_i are called the directional ideals of A , and the points C_i of V defined by the ideals \mathfrak{p}_i will be called the directional foci of A .

LEMMA 4.1. *Let A be an M -primary ideal of order r in L and let $v \in \Omega_0$. If \mathfrak{p} is the prime ideal in \mathfrak{o} that corresponds to the focal point C of v , and if $v(A) > v(M^r)$, then $\mathfrak{p} \supset \mathfrak{c}(A)$ so that $\mathfrak{c}(A)$ is not irrelevant and \mathfrak{p} is a directional ideal of A .*

Proof. This follows from Lemma 3.1.

COROLLARY. *If A is a complete ideal of L such that $\mathfrak{c}(A)$ is irrelevant then $A = M^r$, where r is the order of A .*

Proof. Since A and M^r are complete, and $A \subseteq M^r$, the stipulation that $A \neq M^r$ implies that there is a valuation v such that $v(A) > v(M^r)$. Since it can be assumed that $v \in \Omega_0$, the assertion follows, q.e.d.

LEMMA 4.2. *If A and B are ideals of L then $\mathfrak{c}(AB) = \mathfrak{c}(A) \cdot \mathfrak{c}(B)$.*

Proof. Clear.

If A is an ideal of order r and $L'(C)$ is the quadratic transform of L corresponding to focal point C , then $M^rL'(C) = u_1^rL'(C)$, and $u_1^rL'(C) \cap L = M^r$, so that $AL'(C) = u_1^rA'$, where A' is an ideal of $L'(C)$. This ideal A' will be called the local quadratic transform of A under the extension $L \rightarrow L'(C)$.

LEMMA 4.3. *Let A be a complete M -primary ideal in L of order r , and let \mathfrak{p}^σ be the highest power of \mathfrak{p} , the ideal of C , that occurs in the quasi-factorization of $\mathfrak{c}(A)$ into a product of prime ideals. Then: (a) The order r' of the transform A' of A is not greater than σ , but is positive if σ is positive. In particular, $A' = L'(C)$ if and only if $\mathfrak{c}(A) \not\subseteq \mathfrak{p}$. (b) If $A' \neq L'(C)$ then A' is primary for M' .*

Proof. Use the same notations as in §3. There must exist an element θ in A such that $\bar{\theta}_r(x) \in \mathfrak{p}^\sigma$, $\bar{\theta}_r(x) \notin \mathfrak{p}^{\sigma+1}$. Hence as in the proof of Lemma 3.4, $\bar{\theta}_r(x)/x_1^r = h(x_2/x_1, \dots, x_n/x_1)^\sigma F(x)/G(x)$, where $F(x)$ and $G(x)$ are forms of like degree ρ , neither F nor G is divisible by \mathfrak{p} , and $h(x_2/x_1, \dots, x_n/x_1)$ is a uniformizing parameter at \mathfrak{p} . It follows that

$$(4.1) \quad u_1^{t\sigma} \theta_r(u_1, \dots, u_n) G(u_1, \dots, u_n) - u_1^r g_0(u_1, \dots, u_n)^\sigma F(u_1, \dots, u_n) = H(u_1, \dots, u_n),$$

where H is a form of degree $t\sigma + r + \rho + 1$ with coefficients in L , and since an equation like 4.1 with $\theta_r(u_1, \dots, u_n)$ replaced by θ and $H(u_1, \dots, u_n)$ replaced by a similar form H_1 is also valid, we have

$$\frac{\theta}{u_1^r} = h(u_2/u_1, \dots, u_n/u_1)^\sigma \cdot \frac{F(u)}{G(u)} + u_1 \frac{H_1(u)}{G(u)u_1^{t\sigma+r+1}}.$$

The element θ/u_1^r belongs to A' , and since $F(u)/G(u)$ is a unit in $L'(C)$, θ/u_1^r does not belong to $M'^{\sigma+1}$. Hence we have $r' \leq \sigma$. Similarly, if $\sigma > 0$ then each element of A' is in M' so that $r' > 0$. Since high powers of $\bar{g}_0(u_1, \dots, u_n)$ and u_1 belong to A it follows that high powers of $g_0/u_1^t = h(u_2/u_1, \dots, u_n/u_1)$ and u_1 belong to A' . Hence A' is primary for M' if $A' \neq L'(C)$, q.e.d.

If $\mathfrak{c}(A) \approx \mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_g^{\alpha_g}$ is a quasi-factorization of the homogeneous ideal $\mathfrak{c}(A)$, then $\mathfrak{c}(A) = \mathfrak{p}_1^{(\alpha_1)} \cap \dots \cap \mathfrak{p}_g^{(\alpha_g)} \cap \mathfrak{a}$ is a primary decomposition of $\mathfrak{c}(A)$. Here $\mathfrak{p}^{(e)}$ stands for the symbolic e th power of \mathfrak{p} , and \mathfrak{a} is an irrelevant ideal. Let $\gamma(A) = \mathfrak{p}_1^{(\alpha_1)} \cap \dots \cap \mathfrak{p}_g^{(\alpha_g)}$, so that $\mathfrak{c}(A) \subseteq \gamma(A)$ and $\gamma(A) = (\mathfrak{c}(A))_v = (\mathfrak{c}(A)^{-1})^{-1}$. A set of forms $\bar{\phi}_1, \bar{\phi}_2, \dots, \bar{\phi}_h$ of degree $s (\leq r)$ in \mathfrak{o} is called a quasi-basis for $\mathfrak{c}(A)$ in case $\mathfrak{c}(A) \subseteq \sum \mathfrak{o} \bar{\phi}_i \subseteq \gamma(A)$.

LEMMA 4.4. (a) For any ideal A of L , $\mathfrak{c}(A_a) \subseteq (\mathfrak{c}(A))_a$ and $\gamma(A_a) = \gamma(A)$. (b) If $A = M^t B$ where t is an integer ≥ 0 , then $\mathfrak{c}(A) \subseteq \mathfrak{c}(B)$ and $\gamma(A) = \gamma(B)$.

Proof. We note first that A and A_a have the same order r . If θ is an element of A_a with a nonzero leading form $\bar{\theta}_r(x)$, then an equation expressing the integral dependence of θ upon A becomes an equation that exhibits the integral dependence of $\bar{\theta}_r(x)$ upon $\mathfrak{c}(A)$ if each coefficient is replaced by its leading form. Hence $\mathfrak{c}(A_a) \subseteq (\mathfrak{c}(A))_a$. Now $(\mathfrak{c}(A))_v \subseteq (\mathfrak{c}(A_a))_v \subseteq ((\mathfrak{c}(A))_a)_v = (\mathfrak{c}(A))_v$, in view of the fact that for any \mathfrak{v} -ideal \mathfrak{a} , $\mathfrak{a}_{av} = \mathfrak{a}_v$. Hence $\gamma(A_a) = \gamma(A)$. Since $\mathfrak{c}(M^t B) = \mathfrak{c}(M^t) \cdot \mathfrak{c}(B)$ and since $\mathfrak{c}(M^t)$ is irrelevant it follows that $\gamma(A) = \gamma(B)$, and the inclusion $\mathfrak{c}(A) \subseteq \mathfrak{c}(B)$ is clear, q.e.d.

PROPOSITION 4.5. If A is a complete M -primary ideal of L and if $\mathfrak{c}(A)$ has a quasi-basis of forms of degree $s < r (= \text{ord } A)$, then there is a complete M -primary ideal B such that $A = M^{r-s} B$. If $\mathfrak{c}(A)$ has no quasi-basis of forms of degree less than r , then A does not admit M as a factor.

Proof. We fix a form $\bar{a}(x)$ of degree s in $\gamma(A)$ and write $\mathfrak{o} \bar{a}(x) \approx \mathfrak{c}(A) \cdot \mathfrak{a}$. Fix an element α of order r in A such that the leading form $\bar{\alpha}_r(x)$ is such that $\mathfrak{o} \bar{\alpha}_r(x)$

$\approx c(A) \cdot \mathfrak{b}$, where $c(A) + \mathfrak{b}$ and $\mathfrak{a} + \mathfrak{b}$ are both irrelevant. Select a form $\bar{b}(x)$ of degree, say t , from the ideal \mathfrak{b} such that $\mathfrak{o}\bar{a} + \mathfrak{o}\bar{b}$ is irrelevant. The product $\bar{a}(x)\bar{b}(x)$ must then admit $\bar{\alpha}_r(x)$ as a factor; say $\bar{a}(x)\bar{b}(x) = \bar{\alpha}_r(x)\bar{c}(x)$, where $\bar{c}(x)$ is a form of degree $\rho = s + t - r$. We then have $c(u)\alpha \in M^\rho A$, and the leading form of $c(u)\alpha$ is $\bar{a}(x)\bar{b}(x)$. We define two sequences of polynomials $\{\bar{P}_i(x)\}$ and $\{\bar{Q}_i(x)\}$ inductively, in such a way that the conditions

$$\begin{aligned}
 (*) \quad & P_i(u) \equiv a(u) \pmod{M^{s+1}}, \quad Q_i(u) \equiv b(u) \pmod{M^{t+1}}, \\
 & c(u)\alpha - P_i(u)Q_i(u) \in M^{s+t+i+1}
 \end{aligned}$$

hold for all values of i . To do this we take $P_0(u) = a(u)$, $Q_0(u) = b(u)$. If we assume that \bar{P}_i and \bar{Q}_i have been defined for a given i , we can express the leading form of $c(u)\alpha - P_i(u)Q_i(u)$ as a linear combination $\bar{A}_{t+i+1}(x)\bar{a}(x) + \bar{B}_{s+i+1}(x)\bar{b}(x)$. This follows from the fact that $\mathfrak{o}\bar{a} + \mathfrak{o}\bar{b}$ is irrelevant in view of the assumption in §2. If $P_{i+1}(u) = P_i(u) + B_{s+i+1}(u)$ and $Q_{i+1}(u) = Q_i(u) + A_{t+i+1}(u)$, it is easily seen that P_{i+1} and Q_{i+1} satisfy (*) with i replaced by $i + 1$.

Since $c(u)\alpha \in M^\rho A$ it follows (since A is M -primary) that if i is sufficiently large $P_i(u)Q_i(u) \in M^\rho A$. Let B be the complete M -primary ideal $A : M^{r-s}$. We assert that if i is large then $P_i(u) \in B$. To see this let $v \in \Omega_0$, and assume first that $v(Q_i(u)) = v(M^t)$. Then since $v(P_i) + v(Q_i) \geq v(M^\rho) + v(A)$, we have $v(P_i) + v(M^{r-s}) \geq v(A)$. If on the other hand $v(Q_i) > v(M^t)$, then by Lemma 3.1 $\bar{b}(x)$ must belong to the ideal \mathfrak{p} of the focal point C of v . If this is so, then $\bar{a}(x) \notin \mathfrak{p}$ so that $\mathfrak{p} \not\subset c(A)$. Hence in this case $v(A) = v(M^r)$, and $v(P_i) \geq v(M^s)$, so that again $v(P_i) + v(M^{r-s}) \geq v(A)$. Since A is complete and v is an arbitrary element of Ω_0 , $P_i(u)M^{r-s} \subseteq A$, so that $P_i \in B$. Thus if $\bar{\phi}_1(x), \dots, \bar{\phi}_h(x)$ is a quasi-basis of $c(A)$ consisting of forms of degree s , then there exist elements $\beta_1, \beta_2, \dots, \beta_h$ in B such that $\bar{\beta}_i(x) = \bar{\phi}_i(x)$, $i = 1, 2, \dots, h$.

Let θ be an element of A , and assume first that $\text{ord } \theta = r$. Then $\bar{\theta}_r(x) \in c(A)$ so that $\bar{\theta}_r(x) = \sum G_i(x)\bar{\phi}_i(x)$, where $G_i(x)$ is a form of degree $r - s$. Let $\theta^* = \theta - G_2(u)\beta_2 - \dots - G_h(u)\beta_h$. It is clear that $\theta^* \in A$ and $\bar{\theta}_r^*(x) = G_1(x)\bar{\phi}_1(x)$. Select a form $\bar{G}(x)$ of degree $r - s$ such that $\bar{G} - G_1$ and $\bar{\phi}_1$ together generate an irrelevant ideal in \mathfrak{o} . Let $\theta_1 = \theta^* - G(u)\beta_1$. Then $\theta_1 \in A$ and

$$\bar{\theta}_1(x) = (G_1(x) - \bar{G}(x))\bar{\phi}_1(x).$$

By the same argument as used above we can construct sequences of polynomials $\{p_i(u)\}$ and $\{q_i(u)\}$ such that

$$\begin{aligned}
 (**) \quad & p_i(u) \equiv \phi_1(u) \pmod{M^{s+1}}, \quad q_i(u) \equiv G_1(u) - G(u) \pmod{M^{r-s+1}} \\
 & \theta_1 - p_i(u)q_i(u) \in M^{r+i+1}.
 \end{aligned}$$

If i is large we have $M^{r+i+1} \subseteq BM^{r-s}$ so that $\theta_1 - p_i q_i \in M^{r-s}B$. By an argument similar to the one above we find $p_i(u) \in B$ and therefore $\theta_1 \in M^{r-s}B$. This shows

that $\theta \in M^{r-s}B$ also. If $\text{ord } \theta > r$, fix $\theta_0 \in A$ so that $\text{ord } \theta_0 = r$. Then both θ_0 and $\theta + \theta_0$ belong to $M^{r-s}B$ so that $\theta \in M^{r-s}B$, and $A = M^{r-s}B$.

If A admits M as a factor, say $A = MC$, then the order of C is $r - 1$ and a basis for $\mathfrak{c}(C)$ consisting of forms of degree $r - 1$ would be a quasi-basis for $\mathfrak{c}(A)$. This proves the last assertion, q.e.d.

COROLLARY 1. *If B is a complete M -primary ideal then M^tB is complete when t is sufficiently large.*

Proof. Let $A = (M^tB)_a$. Then $\gamma(A) = \gamma(M^tB) = \gamma(B)$, and if t is large, $\mathfrak{c}(A) \subseteq \mathfrak{c}(B) \subseteq \gamma(A)$. In fact, $\mathfrak{c}(B) = \gamma(B) \cap \mathfrak{i} = \gamma(M^tB) \cap \mathfrak{i} = \gamma(A) \cap \mathfrak{i}$, where \mathfrak{i} is an irrelevant ideal. Now if t is large $\mathfrak{c}(M^t) \subseteq \mathfrak{i}$, and since $\mathfrak{c}(A) \subseteq \mathfrak{c}(M^t)$ it follows that $\mathfrak{c}(A) \subseteq \mathfrak{c}(B)$ as asserted. Thus A is of degree $t + r$ and $\mathfrak{c}(A)$ has a quasi-basis consisting of forms of degree r , where r is $\text{ord } B$. Hence $A = M^{(t+r)-r}B_1$, where B_1 is a complete ideal. Since $v(B) = v(B_1)$ for all $v \in \Omega$, it follows that $B = B_1$, q.e.d.

COROLLARY 2. *A sufficient condition that M^tB be complete for all values of t is that $\mathfrak{c}(B) = \gamma(B)$.*

Proof. Under the present hypothesis the irrelevant ideal \mathfrak{i} above will not occur, so that in the proof of Corollary 1 no restriction need be placed on t , q.e.d.

5. If u is an element of order one and A is an ideal of order r in L , then the extended ideal AL_u is of the form u^rA' where A' is an ideal of L_u that is not contained in uL_u . The ideal A' is called the transform of A and will be denoted by $T_u(A)$.

LEMMA 5.1. *If A is a complete M -primary ideal in L then $T_u(A)$ is a complete ideal of L_u .*

Proof. Let θ be an element of L_u that depends integrally on A' , $\theta^t + a_1\theta^{t-1} + \dots + a_t = 0$, with $a_i \in A'^i$. If we multiply by u^{rt} we find $(u^r\theta)^t + u^r a_1(u^r\theta)^{t-1} + \dots + u^{rt} a_t = 0$, so that the coefficients $u^{ri} a_i$ are elements of $(AL_u)^i$. Hence there is an integer s such that $u^{ri} a_i = \sum (w_{ij}/u^s) \alpha_{ij}$, with $w_{ij} \in L$, $\text{ord } w_{ij} \geq s$, and $\alpha_{ij} \in A^i$. Thus if $u^{ri} a_i = w_i/u^s$, then $w_i \in M^s A^i$. It is clear, that we can take s arbitrarily large here. Now we have $(u^{r+s}\theta)^t + w_1(u^{r+s}\theta)^{t-1} + \dots + u^{st-s} w_s = 0$, and $u^{si-s} w_i \in (M^s A)^i$. If s is large enough to ensure that $M^s A$ is complete we have $u^{r+s}\theta \in M^s A$, and hence $\theta \in A'$, q.e.d.

LEMMA 5.2. *If A and B are complete M -primary ideals of L then $T_u(A \times B) = T_u(A) \times T_u(B)$.*

Proof. Assume that A and B are of orders r and s respectively and that $A' = T_u(A)$, $B' = T_u(B)$. Since $A \times B = (AB)_a$ it follows that the order of $A \times B$ is $r + s$, so that if $T_u(A \times B)$ is the complete ideal C' we have $(A \times B)L_u = u^{r+s}C'$. On the other hand, $(AB)L_u = u^{r+s}A'B'$, and clearly $A'B' \subseteq C'$. If v is any valua-

tion such that $R_v \supset L_u$ then $v(AB) = v(A \times B)$ so that also $v(A'B') = v(C')$. It follows that C' is the completion of $A'B'$, q.e.d.

If A is M -primary then $M^t \subset A$ for some integer t . It follows that $u^{t-r} \in T_u(A)$ so that $u \in \text{Rad } T_u(A)$. On the other hand $T_u(A) \not\subset uL_u$ so that $\text{Rad } T_u(A) \not\subset uL_u$. Since uL_u is prime it follows that if $T_u(A)$ is not the unit ideal then $\text{Rad } T_u(A)$ is an intersection of maximal prime ideals M_1, M_2, \dots, M_s of L_u each of which lies over M . A valuation v_i such that $R_{v_i} \supset L_u$ and $M_{v_i} \cap L_u = M_i$ must belong to the set Ω_0 , and $v_i(T_u(A)) > 0$ so that $v_i(A) > v_i(M')$. By Lemma 4.1 the focus of v_i defines a prime ideal \mathfrak{p}_i of \mathfrak{o} such that $\mathfrak{p}_i \supset \gamma(A)$. The quotient ring of L_u at M_i is the ring $L'(\mathfrak{p}_i)$ introduced in §3, and it is clear that $T_u(A)L'(\mathfrak{p}_i)$ is precisely the local quadratic transform of A described at the beginning of §4. On the other hand, if \mathfrak{p} is any prime ideal of $\gamma(A)$ and if the leading form $\bar{u}(x)$ of u does not belong to \mathfrak{p} , then $L_u \subset L'(\mathfrak{p})$ and the center of $L'(\mathfrak{p})$ in L_u is a maximal ideal M_u of L_u that contains $\text{Rad } T_u(A)$ in view of Lemma 4.3. These remarks can be summarized as follows.

PROPOSITION 5.3. *If the leading form $\bar{u}(x)$ does not belong to any prime ideal of $\gamma(A)$ then there is a 1 : 1 correspondence between the prime ideals of $\gamma(A)$ and the maximal ideals of L_u that divide $\text{Rad } T_u(A)$. Moreover, $T_u(A)$ is an intersection of zero-dimensional primary complete ideals of L_u .*

PROPOSITION 5.4. *Under the same hypothesis as Proposition 5.3, $u^r T_u(A) \cap L = A$.*

Proof. Let $B = u^r T_u(A) \cap L$, so that $BL_u = u^r T_u(A)$ and thus $BL_u = AL_u$, and $A \subseteq B$. If $v \in \Omega$, then either $v(A) = v(M') \leq v(B)$, or $v(A) > v(M')$. In the latter case the focus of v is at a prime ideal of $\gamma(A)$ and $v \in \Omega_0$. Hence $L_u \subseteq R_v$ so that in this case also $v(B) = v(A)$, and since A is complete $B \subseteq A$, q.e.d.

6. We now consider the case in which a zero-dimensional complete ideal A' of L_u is given and we look for ideals A in L such that $T_u(A) = A'$.

PROPOSITION 6.1. *If A' is a zero-dimensional ideal of L_u such that $u \in \text{Rad } A'$, then there exist integers f such that $u^f A'$ is the extension of an ideal of L . If e is the least such integer, let $A_i = u^{e+i} A' \cap L$. Then A_i is an M -primary ideal of order $e + i$, and $A_i L_u = u^{e+i} A'$ so that for all i , $T_u(A_i) = A'$. Moreover, if A' is complete so is A_i .*

Proof. Each element of A' is a polynomial in the ratios u_i/u with coefficients in L . If f is an integer that is not less than the maximum of the degrees of the elements of a basis of A' , then f will satisfy the requirements of the first assertion of the proposition. Since $u \in \text{Rad } A'$ there is an integer t such that $u^t \in A'$, and then $u^{t+e+i} L_u \cap L \subseteq u^{e+i} A' \cap L = A_i$. Thus $M^{t+e+i} \subseteq A_i$ so that A_i is M -primary. Since $A_i \subseteq u^{e+i} L_u \cap L$ we have $A_i \subseteq M^{e+i}$. Since $u^{e+i} A'$ is an extended ideal it is the extension of its contraction with L , so that $u^{e+i} A' = A_i L_u$. Thus $A_i \not\subseteq M^{e+i+1}$

since $A' \not\subseteq uL_u$. Hence the order of A_i is $e + i$ and $T_u(A_i) = A'$. If A' is complete so also are $u^{e+i}A'$ and A_i , q.e.d.

LEMMA 6.2. *If A_0, A_1, \dots is the sequence of ideals introduced above, then for all non-negative integers i and j we have $M^j A_i \subseteq A_{i+j}$, $M^j A_i \subseteq M^{j-1} A_{i+1}$. Moreover, there is an integer i_0 such that $\gamma(A_{i+1}) = \gamma(A_i)$ if $i \geq i_0$.*

Proof. Since $(M^j A_i)L_u = u^{e+i+j}A'$, it follows that $M^j A_i \subseteq A_{i+j}$, and by induction on j , $M^j A_i \subseteq M^{j-1} A_{i+1}$. Now $c(A_{i+1}) \supseteq c(M A_i) = c(M) \cdot c(A_i)$, and since $c(M)$ is irrelevant it follows that $\gamma(A_{i+1}) \supseteq \gamma(A_i)$. The existence of i_0 follows since \mathfrak{o} is noetherian, q.e.d.

LEMMA 6.3. *If $\gamma(A_i) = \mathfrak{p}_1^{(e_1)} \cap \dots \cap \mathfrak{p}_g^{(e_g)}$ when $i \geq i_0$, then $\bar{u} \notin \mathfrak{p}_i$, where $\bar{u}(x)$ is the leading form of u .*

Proof. Since u is of order one, $\bar{u}(x)$ is a linear form in x_1, x_2, \dots, x_n . Since k is infinite there is a second linear form $\bar{w}(x)$ such that the ideal $\mathfrak{o}\bar{u} + \mathfrak{o}\bar{w}$ is irrelevant. Let $\text{Rad } A' = M_1 \cap M_2 \cap \dots \cap M_s$, where M_i is a maximal ideal of L_u such that $M_i \cap L = M$. Since L_u/M_i is algebraic over k there is a polynomial $\bar{g}_i(X)$ in $k[X]$ such that $g_i(w/u) \in M_i$. Hence there is a polynomial $g(X)$ in $L[X]$ with leading coefficient a unit in L such that $g(w/u) \in A'$. If $t = \text{deg } g(X)$ let ρ be an integer such that $\rho t \geq e + i_0$, say $\rho t = e + f$, $f \geq i_0$. Then $u^{\rho t} g^\rho(w/u) \in u^{e+f} A' \cap L = A_f$. Since $u^{\rho t} g^\rho(w/u)$ is a form $\phi(w, u)$ of degree ρt in A_f , it follows that the corresponding form $\bar{\phi}(\bar{w}, \bar{u})$ is an element of $c(A_f)$ and hence of $\gamma(A_f)$. Thus we have $\bar{\phi}(\bar{w}, \bar{u}) \in \mathfrak{p}_i$, $i = 1, 2, \dots, g$, and the coefficient of \bar{w}^ρ is not zero. Hence $\bar{u} \in \mathfrak{p}_i$ implies $\bar{w} \in \mathfrak{p}_i$ and this is not possible since \mathfrak{p}_i is a relevant prime ideal, q.e.d.

LEMMA 6.4. *If $i \geq i_0$, then $(M^j A_i)_a = A_{i+j}$.*

Proof. If $v \in \Omega$ and $v(M^j A_i) > v(M^{e+i+j})$ then $v \in \Omega_0$ and the focal point of v is at one of the ideals \mathfrak{p}_i in view of Lemma 4.1. It follows that $R_v \supseteq L_u$. The same remarks hold if $v(A_{i+j}) > v(M^{e+i+j})$. For such valuations v we have $v(M^j A_i) = v(L_u M^j A_i) = v(L_u A_{i+j}) = v(A_{i+j})$, and for all other $v \in \Omega$, $v(M^j A_i) = v(M^{e+i+j}) = v(A_{i+j})$, so that the lemma follows from the fact that A_{i+j} is complete, q.e.d.

Two complete M -primary ideals of L will be said to be M -equivalent (in symbols $A \sim B$) in case non-negative integers i and j exist such that $(M^i A)_a = (M^j B)_a$. (In view of the cancellation law of Krull [2], one of i and j can be assumed to be zero.) The relation thus defined is obviously an equivalence relation, and we denote the class of ideal A by A^* . In view of Lemma 6.4 we have $A_i^* = A_{i+1}^*$ for all $i \geq i_0$, so that with the zero-dimensional complete ideal A' of L_u we can associate the class A_i^* ($i \geq i_0$). The class will be called the inverse transform of A' and denoted by $S_u(A')$. Since it is clear from the definition of T_u that if $A \sim B$ then $T_u(A) = T_u(B)$, we can regard T_u as a function T_u^* defined on the set of classes A^* . Moreover, if $A \sim B$, then $\gamma(A) = \gamma(B)$ so that we can regard the ideal $\gamma(A)$ as a character of the class A^* , and denote it by $\gamma(A^*)$.

PROPOSITION 6.5. *If A' is a zero-dimensional complete ideal of L_u such that $u \in \text{Rad } A'$, then $T_u^* S_u(A') = A'$. If A^* is a class of M -primary complete ideals such that $\gamma(A^*) : \circ \bar{u} = \gamma(A^*)$, then $S_u T_u^*(A^*) = A^*$.*

Proof. The first point is clear. To prove the second point let $A \in A^*$ and let $T_u(A) = A'$. If A is of order r , then by Proposition 5.4 we find $u^r A' \cap L = A$. Since $\gamma(A) : \circ \bar{u} = \gamma(A)$, the argument of Lemma 6.4 will show that for $i \geq 0$, $u^{r+i} A' \cap L = (M^i A)_a$, so that A belongs to the class $S_u(A')$, q.e.d.

7. If $A \sim B$ and $C \sim D$ then $A \times C \sim B \times D$, so that if Γ^* is the set of equivalence classes of M -primary ideals then a binary composition is defined on Γ^* by the rule $A^* \circ B^* = (A \times B)^*$. Under this composition Γ^* is a commutative semigroup with identity in which the cancellation law holds. In view of Lemma 5.2, we have $T_u^*(A^* \circ B^*) = T_u^*(A^*) \times T_u^*(B^*)$. It should be noted at this point that since the quotient ring of L_u at any maximal ideal M_u that lies over M is a two-dimensional regular local ring, Zariski's results [4] apply, and hence $T_u^*(A^*) \times T_u^*(B^*) = T_u^*(A^*) T_u^*(B^*)$.

PROPOSITION 7.1. *If A' and B' are complete zero-dimensional ideals of L_u such that $u \in \text{Rad } A'$ and $u \in \text{Rad } B'$, then $S_u(A'B') = S_u(A') \circ S_u(B')$.*

Proof. We fix ideals A and B in L such that $S_u(A') = A^*$ and $S_u(B') = B^*$. Then $S_u(A') \circ S_u(B') = (A \times B)^*$. Since $\gamma(A \times B) \approx \gamma(A) \cdot \gamma(B)$, and since $\bar{u}(x)$ does not belong to any prime ideal of $\gamma(A)$ or of $\gamma(B)$, it follows that $\bar{u}(x)$ does not belong to any prime ideal of $\gamma(A \times B)$. Hence by Proposition 6.5, $S_u T_u^*((A \times B)^*) = (A \times B)^*$, and since $T_u^*((A \times B)^*) = A'B'$, our result is established, q.e.d.

PROPOSITION 7.2. *If A is a complete M -primary ideal of L such that A^* is an irreducible element of the semigroup (Γ^*, \circ) and if u is an element of degree one such that $\gamma(A^*) : \circ \bar{u} = \gamma(A^*)$, then $T_u^*(A^*)$ is an irreducible element of the semigroup of complete L_u -ideals.*

Proof. Let $T_u^*(A^*) = A'$, and assume that A' is reducible, say $A' = B'C'$. Since $u \in \text{Rad } A'$, it follows that $u \in \text{Rad } B'$ and $u \in \text{Rad } C'$, and B' and C' are zero-dimensional complete ideals. By Proposition 7.1 we have $S_u(B'C') = S_u(B') \circ S_u(C')$, so that $A^* = S_u(B') \circ S_u(C')$. Since A^* is irreducible either $S_u(B')$ or $S_u(C')$ is a unit, so that there is an ideal D in L such that say $D^* \circ S_u(C') = M^*$. Hence if E is an ideal of the class $S_u(C')$, there exist integers i and j such that $(M^i D E)_a = M^j$. It follows that both $c(D)$ and $c(E)$ are irrelevant ideals so that D and E are powers of M . In particular, $C' = T_u(E) = L_u$, and this is a contradiction, q.e.d.

PROPOSITION 7.3. *If A^* is an irreducible element of (Γ^*, \circ) it is also a prime element.*

Proof. Assume that $E^* \circ F^* = A^* \circ B^*$ and pick u so that $\bar{u}(x)$ is not in any prime of $\gamma(E^*)$, $\gamma(F^*)$, $\gamma(A^*)$, $\gamma(B^*)$. If E' , F' , A' , B' are the T_u^* -transforms of E^* , F^* , A^* , and B^* then $E'F' = A'B'$. Each of these ideals is zero-dimensional and A' is irreducible by Proposition 7.2. Hence A' must be primary for some maximal ideal M' , and since the quotient ring of L_u at M' is a regular two-dimensional local ring we can apply the results of [4] to conclude that A' is a prime element of the multiplicative semigroup of complete L_u -ideals. Hence either $E' = A'C'$ or $F' = A'D'$. If say the former is true, then $E^* = A^* \circ S_u(C')$, q.e.d.

In view of the fact that (Γ^*, \circ) obviously satisfies the divisor chain condition, this proves that (Γ^*, \circ) is gaussian. In closing we note that if k is a field, $z^2 = x^2 + y^2$, and (L, M) is the quotient ring of $k[x, y, z]$ at the origin, then $(x, y - z, M^2) \times (x, y + z, M^2) = M \times (x, M^2)$, while M is not a factor of either of the first two ideals. Thus even in this simple case, the irreducible ideal M is not a *prime* element of the semigroup (Γ, \times) .

BIBLIOGRAPHY

1. N. Jacobson, *Lectures in abstract algebra*, Vol. I, Van Nostrand, New York, 1951.
2. W. Krull, *Beitrage zur Arithmetik kommutativer Integritatsbereiche*, I. Math. Z. **41** (1936), 545-577.
3. M. Sakuma, *On prime operations in the theory of ideals*, J. Sci. Hiroshima Univ. Ser. A **20** (1957), 101-106.
4. O. Zariski and P. Samuel, *Commutative algebra*, Vol. II, Van Nostrand, Princeton, N. J., 1961.
5. O. Zariski, *Reduction of the singularities of an algebraic surface*, Ann. of Math. (2) **40** (1939), 639-689.
6. ———, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), 362-368.

UNIVERSITY OF IOWA,
IOWA CITY, IOWA