PRIME IDEALS AND INTEGRAL DEPENDENCE

I. S. COHEN AND A. SEIDENBERG

Let $\mathfrak{R}$ and $\mathfrak{S}$ be commutative rings such that $\mathfrak{S}$ contains, and has the same identity element as, $\mathfrak{R}$. If $\mathfrak{p}$ and $\mathfrak{P}$ are prime ideals in $\mathfrak{R}$ and $\mathfrak{S}$ respectively such that $\mathfrak{P} \cap \mathfrak{R} = \mathfrak{p}$ then we shall say that $\mathfrak{P}$ lies over, or contracts to, $\mathfrak{p}$. If over every prime ideal in $\mathfrak{R}$ there lies a prime ideal in $\mathfrak{S}$, we shall say that the "lying-over" theorem holds for the pair of rings $\mathfrak{R}$ and $\mathfrak{S}$.

Suppose now that $\mathfrak{q}$ and $\mathfrak{p}$ are prime ideals in $\mathfrak{R}$ such that $\mathfrak{q} \subset \mathfrak{p}$. If for every prime ideal $\mathfrak{Q}$ in $\mathfrak{S}$ lying over $\mathfrak{q}$ there exists a prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lying over $\mathfrak{p}$ and containing $\mathfrak{Q}$, then the "going-up" theorem will be said to hold for $\mathfrak{R}$ and $\mathfrak{S}$. Similarly, if for every prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lying over $\mathfrak{p}$ there exists a prime ideal $\mathfrak{Q}$ in $\mathfrak{S}$ lying over $\mathfrak{q}$ and contained in $\mathfrak{P}$, then the "going-down" theorem will be said to hold.

Below we are concerned with the case where $\mathfrak{S}$ is integrally dependent on $\mathfrak{R}$. In this case we shall prove the "lying-over" and "going-up" theorems (§1). With certain additional conditions on $\mathfrak{R}$ and $\mathfrak{S}$, also the "going-down" theorem is proved (§2). Counterexamples are given to show that none of these conditions can be omitted (§3).

All of the results of this paper (except Theorem 7) have been proved by Krull[1] when the rings are free from zero-divisors. The present proofs are essentially simpler than Krull's and at the same time do not require that the rings be integral domains.

1. The "lying-over" and "going-up" theorems. Let $\mathfrak{R}$ and $\mathfrak{S}$ be commutative rings with $\mathfrak{R}$ contained in $\mathfrak{S}$ and with a common identity element, and let $\mathfrak{S}$ be integral over $\mathfrak{R}$. We examine first the question of whether the "lying-over" theorem holds for the rings $\mathfrak{R}$ and $\mathfrak{S}$. We remark that if a maximal ideal in $\mathfrak{S}$ necessarily contracts to a maximal ideal in $\mathfrak{R}$, and if $\mathfrak{R}$ has a single maximal ideal $\mathfrak{p}$, then for the prime ideal $\mathfrak{p}$ it is certainly true that there exists a prime ideal in $\mathfrak{S}$ lying over $\mathfrak{p}$; in fact, every maximal ideal of $\mathfrak{S}$ will lie over $\mathfrak{p}$. This remark is the motivation behind the following theorem.

THEOREM 1. *Let $\mathfrak{S}$ be integral over $\mathfrak{R}$, and let the prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lie over the prime ideal $\mathfrak{p}$ in $\mathfrak{R}$, that is, $\mathfrak{P} \cap \mathfrak{R} = \mathfrak{p}$. Then $\mathfrak{p}$ is maximal if and only if $\mathfrak{P}$ is maximal.*

Presented to the Society, September 15, 1945; received by the editors October 31, 1945.

[1] *Zum Dimensionsbegriff der Idealtheorie*, Math. Zeit. vol. 42 (1937) pp. 745–766. Especially relevant are Theorems 1–6 and the considerations on pp. 756–757.

PROOF. Consider the residue-class rings $\mathfrak{S}^* = \mathfrak{S}/\mathfrak{P}$ and $\mathfrak{R}^* = \mathfrak{R}/\mathfrak{p}$. Since $\mathfrak{P} \cap \mathfrak{R} = \mathfrak{p}$ the ring $\mathfrak{S}^*$ may be considered to contain $\mathfrak{R}^*$; $\mathfrak{R}^*$ and $\mathfrak{S}^*$ are integral domains, and $\mathfrak{S}^*$ remains integral over $\mathfrak{R}^*$. Theorem 1 then reduces to the following well known statement:

If $\mathfrak{R}$ and $\mathfrak{S}$ are integral domains and $\mathfrak{S}$ is integral over $\mathfrak{R}$ then $\mathfrak{R}$ is a field if and only if $\mathfrak{S}$ is a field.

To prove this statement we note that if $\mathfrak{R}$ is a field it follows trivially that $\mathfrak{S}$ is a field. Conversely, let $\mathfrak{S}$ be a field and let $a(\neq 0)$ be an element of $\mathfrak{R}$. We wish to prove $1/a \in \mathfrak{R}$. Since $1/a \in \mathfrak{S}$, it is integral over $\mathfrak{R}$ and hence we have an equation of integral dependence:

$$(1/a)^n + c_1(1/a)^{n-1} + \cdots + c_n = 0, \qquad c_i \in \mathfrak{R}.$$

Multiplying this equation by a^{n-1} we obtain

$$1/a = -(c_1 + c_2 a + \cdots + c_n a^{n-1}) \in \mathfrak{R}.$$

This proves that $\mathfrak{R}$ is a field, and completes the proof of Theorem 1.

THEOREM 2. *Let $\mathfrak{S}$ be integral over $\mathfrak{R}$. Then for every prime ideal $\mathfrak{p}$ in $\mathfrak{R}$ there exists a prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lying over $\mathfrak{p}$.*

PROOF. If $\mathfrak{R}$ contains only one maximal ideal, and this is $\mathfrak{p}$, then certainly the theorem holds for $\mathfrak{p}$; namely, as noted above, any maximal ideal of $\mathfrak{S}$ (such ideals certainly exist[2]) lies over $\mathfrak{p}$. If $\mathfrak{R}$ and $\mathfrak{S}$ are integral domains then the theorem can be reduced to this trivial case by the device of forming quotient rings. In fact, we form the quotient rings $\mathfrak{R}' = \mathfrak{R}_{\mathfrak{p}}$ (=the set of elements in the quotient field of $\mathfrak{R}$ of the form a/b, $a, b \in \mathfrak{R}$, $b \notin \mathfrak{p}$) and $\mathfrak{S}' = \mathfrak{S}_{\mathfrak{p}}$ (=the set of elements in the quotient field of $\mathfrak{S}$ of the form α/b, $\alpha \in \mathfrak{S}$, $b \in \mathfrak{R}$, $b \notin \mathfrak{p}$). The ring $\mathfrak{S}'$ is integral over $\mathfrak{R}'$; moreover $\mathfrak{R}'$ has a single maximal ideal, namely $\mathfrak{p}' = \mathfrak{R}' \cdot \mathfrak{p}$, and $\mathfrak{p}' \cap \mathfrak{R} = \mathfrak{p}$. If $\mathfrak{P}'$ is a maximal ideal of $\mathfrak{S}'$, then by our initial remark, $\mathfrak{P}'$ lies over $\mathfrak{p}'$. We assert that $\mathfrak{P} = \mathfrak{P}' \cap \mathfrak{S}$ lies over $\mathfrak{p}$. In fact, $\mathfrak{P} \cap \mathfrak{R} = \mathfrak{P}' \cap \mathfrak{S} \cap \mathfrak{R} = \mathfrak{P}' \cap \mathfrak{R} = \mathfrak{P}' \cap \mathfrak{R}' \cap \mathfrak{R} = \mathfrak{p}' \cap \mathfrak{R} = \mathfrak{p}$. This completes the proof if $\mathfrak{R}$ and $\mathfrak{S}$ are integral domains.

If $\mathfrak{R}$ and $\mathfrak{S}$ are not integral domains we cannot form the required quotient rings. Nevertheless, the above argument can be adapted to commutative rings in general. Namely, consider the set W of ideals in $\mathfrak{S}$ which contract to ideals contained in $\mathfrak{p}$; W is not empty, since it certainly contains the zero ideal. Let $\mathfrak{P}$ be a maximal element[2] of W. We assert that $\mathfrak{P}$ is prime and lies over $\mathfrak{p}$.

[2] We make use here of the following statement, which is an immediate consequence of Zorn's Lemma: *Let W be a nonvoid set of ideals in some ring; assume that if a subset W' of W has the property that of any two of its ideals one contains the other, then the union of all the ideals of W' is a member of W. Then W has a maximal element.*

For let α and β be elements of $\mathfrak{S}$ not in $\mathfrak{P}$, $\alpha\beta \in \mathfrak{P}$. Then $(\mathfrak{P}, \alpha)$ and $(\mathfrak{P}, \beta)$ contain $\mathfrak{P}$ properly, so that $(\mathfrak{P}, \alpha) \cap \mathfrak{R} \not\subseteq \mathfrak{p}$, $(\mathfrak{P}, \beta) \cap \mathfrak{R} \not\subseteq \mathfrak{p}$. Hence there exist elements a and b in $\mathfrak{R}$ but not in $\mathfrak{p}$ such that $a \equiv \sigma\alpha(\mathfrak{P})$, $b \equiv \tau\beta(\mathfrak{P})$, $\sigma, \tau \in \mathfrak{S}$. Then $ab \equiv \sigma\tau\alpha\beta(\mathfrak{P})$, $ab \in \mathfrak{P} \cap \mathfrak{R} \subseteq \mathfrak{p}$; this is a contradiction, and thus $\mathfrak{P}$ is prime. If $\mathfrak{P} \cap \mathfrak{R} \subset \mathfrak{p}$ properly, let $d \in \mathfrak{p}$, $d \notin \mathfrak{P}$. Then $(\mathfrak{P}, d) \supset \mathfrak{P}$ properly, whence $(\mathfrak{P}, d) \cap \mathfrak{R} \not\subseteq \mathfrak{p}$, so that there exists an element $c \in \mathfrak{R}$, $c \notin \mathfrak{p}$, such that $c \equiv \sigma d(\mathfrak{P})$, $\sigma \in \mathfrak{S}$. Since $\mathfrak{S}$ is integral over $\mathfrak{R}$, σ satisfies an equation

$$\sigma^n + a_1\sigma^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathfrak{R}.$$

From this follows

$$(\sigma d)^n + da_1(\sigma d)^{n-1} + \cdots + d^n a_n = 0.$$

Since $c \equiv \sigma d(\mathfrak{P})$, we have

$$c^n + da_1c^{n-1} + \cdots + d^n a_n \equiv 0 \ (\mathfrak{P}).$$

Since the left side is in $\mathfrak{R}$, this congruence holds mod $\mathfrak{p}$, and since $d \in \mathfrak{p}$, we have $c^n \in \mathfrak{p}$, $c \in \mathfrak{p}$, a contradiction. This completes the proof.

THEOREM 3. *Let $\mathfrak{S}$ be integral over $\mathfrak{R}$. Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{R}$ containing the ideal $\mathfrak{a}$. If $\mathfrak{A}$ is an ideal in $\mathfrak{S}$ such that $\mathfrak{A} \cap \mathfrak{R} = \mathfrak{a}$ then there exists a prime ideal in $\mathfrak{S}$ containing $\mathfrak{A}$ and lying over $\mathfrak{p}$.*

PROOF. This theorem follows directly from Theorem 2 if we take the residue class rings $\mathfrak{S}/\mathfrak{A}$ and $\mathfrak{R}/\mathfrak{a}$.

Conversely, Theorem 2 follows from Theorem 3 by placing $\mathfrak{A} = (0)$. Theorem 3 can, in fact, be proved directly along the same lines as Theorem 2. Thus the two theorems are equivalent; but in Theorem 2 the content takes the form of the "lying-over" theorem, in Theorem 3 it takes the form of the "going-up" theorem.

Theorem 1 implies that if two distinct prime ideals of $\mathfrak{S}$ lie over the same maximal ideal of $\mathfrak{R}$, then neither of these two prime ideals can contain the other. This side of the theorem can be strengthened through the following.

THEOREM 4. *Let $\mathfrak{S}$ be integral over $\mathfrak{R}$, and let the prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lie over $\mathfrak{p}$ in $\mathfrak{R}$. Then no ideal in $\mathfrak{S}$ properly containing $\mathfrak{P}$ can contract to $\mathfrak{p}$ in $\mathfrak{R}$.*

PROOF. If we take the residue-class rings $\mathfrak{S}/\mathfrak{P}$ and $\mathfrak{R}/\mathfrak{p}$, the theorem reduces to the following:

If the integral domain $\mathfrak{S}$ is integral over the ring $\mathfrak{R}$ then any nonzero ideal of $\mathfrak{S}$ contracts to a nonzero ideal of $\mathfrak{R}$.

Suppose, then, that $\alpha \in \mathfrak{S}$, $\alpha \neq 0$; if

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0, \qquad c_i \in \mathfrak{R},$$

is an equation of integral dependence of least possible degree for α then $c_n \neq 0$. For $c_n = 0$ would yield

$$\alpha^{n-1} + c_1\alpha^{n-2} + \cdots + c_{n-1} = 0,$$

that is, an equation of integral dependence for α of degree less than n. Since $c_n \in (\alpha) \cap \mathfrak{R}$, $(\alpha) \cap \mathfrak{R} \neq (0)$. This completes the proof.

2. **The "going-down" theorem.** Unlike the "going-up" theorem, the "going-down" theorem requires assumptions on the 0-divisors of $\mathfrak{R}$ and $\mathfrak{S}$. Even in the case of integral domains, however, the "going-down" theorem will not hold without further assumption on $\mathfrak{R}$: the assumption made below is that $\mathfrak{R}$ is integrally closed in its quotient field.

THEOREM 5. *Let $\mathfrak{R}$ be an integral domain integrally closed in its quotient field, $\mathfrak{S}$ a ring integral over $\mathfrak{R}$, with none of its zero-divisors in $\mathfrak{R}$. Then the "going-down" theorem holds for $\mathfrak{R}$ and $\mathfrak{S}$; that is, if $\mathfrak{q}$ and $\mathfrak{p}$ are prime ideals in $\mathfrak{R}$ with $\mathfrak{q} \subset \mathfrak{p}$, then for every prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lying over $\mathfrak{p}$ there exists a prime ideal $\mathfrak{Q}$, contained in $\mathfrak{P}$, and lying over $\mathfrak{q}$.*

Before proving this theorem we prove two lemmas.[3]

LEMMA 1. *Let $\mathfrak{S}$ be integral over $\mathfrak{R}$ and let $\mathfrak{q}$ be an ideal in $\mathfrak{R}$. Then the set of elements in $\mathfrak{S}$ satisfying an equation of the form*

$$\alpha^m + c_1\alpha^{m-1} + \cdots + c_m = 0, \qquad c_i \in \mathfrak{q}, \tag{1}$$

is the radical of $\mathfrak{S} \cdot \mathfrak{q}$.

PROOF. If α satisfies the above equation then $\alpha^m \in \mathfrak{S} \cdot \mathfrak{q}$, so that α is in the radical of $\mathfrak{S} \cdot \mathfrak{q}$. Conversely if α is in the radical, then $\alpha^k \in \mathfrak{S} \cdot \mathfrak{q}$ for some k. Thus it is sufficient to prove that every element α in $\mathfrak{S} \cdot \mathfrak{q}$ satisfies an equation of the given form. For elements of the form σq, where $\sigma \in \mathfrak{S}$, $q \in \mathfrak{q}$, this is immediate. For let σ satisfy the equation

$$\sigma^m + d_1\sigma^{m-1} + \cdots + d_m = 0, \qquad d_i \in \mathfrak{R};$$

then

$$(\sigma q)^m + d_1 q(\sigma q)^{m-1} + \cdots + d_m q^m = 0.$$

Since every element of $\mathfrak{S} \cdot \mathfrak{q}$ is the sum of a finite number of terms of the form σq it remains to show that the sum of two elements of $\mathfrak{S}$

[3] These lemmas are somewhat stronger than is actually necessary for the theorem.

satisfying an equation of the form of (1) also satisfies such an equation.

Let then

$$\alpha^m + c_1\alpha^{m-1} + \cdots + c_m = 0, \qquad c_i \in \mathfrak{q},$$
$$\beta^n + d_1\beta^{n-1} + \cdots + d_n = 0, \qquad d_i \in \mathfrak{q}.$$

It follows from these equations that every power α^r, $r \geqq m$, can be written in the form

$$\alpha^r = e_1\alpha^{m-1} + \cdots + e_m, \qquad e_i \in \mathfrak{q},$$

and every power β^s, $s \geqq n$, in the form

$$\beta^s = f_1\beta^{n-1} + \cdots + f_n, \qquad f_i \in \mathfrak{q}.$$

Let the products $\alpha^i\beta^j$, $0 \leqq i \leqq m-1$, $0 \leqq j \leqq n-1$, arranged in some order, be designated by τ_k, $k=1, \cdots, mn$. Then every product $\alpha^r\beta^s$ with $r+s \geqq m+n-1$ can be written as a linear combination of the τ's with coefficients in $\mathfrak{q}$. Hence if $l=m+n-1$ then

$$(\alpha+\beta)^l\tau_i = \sum_j q_{ij}\tau_j, \qquad q_{ij} \in \mathfrak{q}, i = 1, \cdots, mn.$$

From these equations we obtain

$$\tau_i \cdot \det\left((\alpha+\beta)^l\delta_{ij} - q_{ij}\right) = 0, \qquad i = 1, \cdots, mn.$$

Since one of the τ_i is 1, the determinant is zero, and this is an equation for $\alpha+\beta$ of the form of (1).

LEMMA 2. *Let $\mathfrak{R}$ be integrally closed in its total quotient ring*[4] *$\mathfrak{R}$. If $f(x)$ and $g(x)$ are monic polynomials in $\mathfrak{R}[x]$ and $h(x)=f(x)g(x)$ is in $\mathfrak{R}[x]$ then $f(x)$ and $g(x)$ are in $\mathfrak{R}[x]$.*

PROOF. Consider the residue-class ring $\mathfrak{R}[x]/f(x)$. Since $f(x)$ is monic, this ring contains a ring isomorphic to $\mathfrak{R}$ and a root θ of $f(x)$. In this way, it is possible to form an extension ring of $\mathfrak{R}$ in which $f(x)$ and $g(x)$ factor into linear factors, say

$$f(x) = \prod_i (x - \alpha_i), \qquad g(x) = \prod_j (x - \beta_j).$$

Since $h(\alpha_i)=0$ and $h(\beta_j)=0$, the α_i and β_j are integral over $\mathfrak{R}$. Hence also the elementary symmetric functions of the α_i and β_j, which are the coefficients of $f(x)$ and $g(x)$, are integral over $\mathfrak{R}$. Since $\mathfrak{R}$ is integrally closed, these coefficients are in $\mathfrak{R}$.

[4] The total quotient ring of $\mathfrak{R}$ consists of all quotients a/b, where a and b are in $\mathfrak{R}$ and b is not a zero-divisor.

PROOF OF THEOREM 5. Let $\mathfrak{L}$ be the total quotient ring of $\mathfrak{S}$; since no element of $\mathfrak{R}$ is a 0-divisor in $\mathfrak{L}$, $\mathfrak{L}$ contains the quotient field $\mathfrak{K}$ of $\mathfrak{R}$.

Let D be the multiplicatively closed system in $\mathfrak{S}$ consisting of elements of the form $d\delta$, where $d\in\mathfrak{R}$, $d\notin\mathfrak{q}$, $\delta\in\mathfrak{S}$, $\delta\notin\mathfrak{P}$. We consider the set W of ideals in $\mathfrak{S}$ which contain $\mathfrak{S}\cdot\mathfrak{q}$ and do not meet D. We first show that W is not empty; specifically it contains $\mathfrak{S}\cdot\mathfrak{q}$. For suppose $d\delta\in\mathfrak{S}\cdot\mathfrak{q}$. By Lemma 1 there exists an equation $h(x)=0$ of integral dependence for $d\delta$ all of whose coefficients except the leading one are in $\mathfrak{q}$. Let $f(x)=0$ be an equation of least degree which is satisfied by $d\delta$ over $\mathfrak{K}$. Since the leading coefficient of $f(x)$ is not a 0-divisor, we may assume that $f(x)$ is monic. Then $h(x)=f(x)g(x)$, where $g(x)\in\mathfrak{K}[x]$. By Lemma 2, the coefficients of $f(x)$ and $g(x)$ are in $\mathfrak{R}$. Since all the coefficients of $h(x)$ except the first are in $\mathfrak{q}$, it follows by the familiar argument of Gauss' lemma that the same is true for $f(x)$ and $g(x)$.

Let $f(x)=x^n+c_1x^{n-1}+\cdots+c_n$. Clearly $x^n+(c_1/d)x^{n-1}+\cdots+(c_n/d^n)=0$ is the monic equation of least degree satisfied by δ over $\mathfrak{K}$. Just as above for $f(x)$, we have $b_i=c_i/d^i\in\mathfrak{R}$. Since $b_id^i=c_i\in\mathfrak{q}$ and $d^i\notin\mathfrak{q}$ we have $b_i\in\mathfrak{q}$. Hence

$$\delta^n = -b_1\delta^{n-1}-\cdots-b_n\in\mathfrak{S}\cdot\mathfrak{q}\subseteq\mathfrak{P},$$

whence $\delta\in\mathfrak{P}$, a contradiction.

Let, now, $\mathfrak{Q}$ be maximal[2] in W. We have $\mathfrak{Q}\cap\mathfrak{R}\supseteq\mathfrak{S}\cdot\mathfrak{q}\cap\mathfrak{R}\supseteq\mathfrak{q}$, but $\mathfrak{Q}\cap\mathfrak{R}$ cannot contain $\mathfrak{q}$ properly since $\mathfrak{Q}$ does not meet D. Also $\mathfrak{Q}\subset\mathfrak{P}$ since $\mathfrak{Q}$ does not meet D. It remains to prove that $\mathfrak{Q}$ is prime. Suppose, then, that $\gamma\delta\in\mathfrak{Q}$ but $\gamma\notin\mathfrak{Q}$ and $\delta\notin\mathfrak{Q}$. Since $(\mathfrak{Q},\gamma)$ and $(\mathfrak{Q},\delta)$ contain $\mathfrak{Q}$ properly, each of them must intersect D, whence also their product intersects D, since D is multiplicatively closed. This is a contradiction since this product is in $\mathfrak{Q}$. This completes the proof.

3. **Counterexamples.** In order better to see to what extent the hypotheses of Theorem 5 can be weakened, we formulate the three hypotheses as follows:

(A) The ring $\mathfrak{R}$ is integrally closed in its total quotient ring.

(B) A non-zero divisor of $\mathfrak{R}$ remains a non-zero divisor in $\mathfrak{S}$.

(C) $\mathfrak{R}$ is an integral domain.

We show by counterexamples that none of these assumptions can be dropped from Theorem 5.

(A) Let $f(x,y)=y^2-x^2-x^3\in K[x,y]$, where K is a groundfield of characteristic 0. Since the curve $f(x,y)=0$ has a singularity at the origin of the xy-plane, the ring $K[\xi,\eta]=K[x,y]/(f(x,y))$ is not integrally closed in its quotient field; in fact, $\tau=\eta/\xi$ satisfies the equa-

tion $\tau^2-1-\xi=0$, and hence is integral over $K[\xi, \eta]$. But $\eta/\xi \notin K[\xi, \eta]$, since $\eta/\xi \in K[\xi, \eta]$ leads to $y \in (x, y^2-x^2-x^3)=(x, y^2)$, which is impossible. Consider now the cylinder erected on the curve $f(x, y)=0$, and let $\mathfrak{R}=K[\xi, \eta, \zeta]=K[x, y, z]/(f(x, y))$ be its ring of nonhomogeneous coordinates. On this cylinder consider an irreducible curve which passes through the point (0, 0, 1) and which lies on only one branch of the cylinder in the neighborhood of this point, say the curve whose prime ideal is $\mathfrak{q}=(\zeta\xi+\eta, \zeta^2-1-\xi)$. Let now $\mathfrak{S}=K[\xi, \tau, \zeta]$, where $\tau=\eta/\xi$. The surface $t^2-1-x=0$, whose general point is (ξ, τ, ζ), is a Cremona transform of the original cylinder; this transformation has the effect of separating the two branches of the cylinder. In this separation, the point (0, 0, 1) is split into two points, (0, −1, 1) and (0, 1, 1); that is, the prime ideals in $\mathfrak{S}$ lying over the prime ideal $\mathfrak{p}=(\xi, \eta, \zeta-1)$ are the prime ideals $\mathfrak{P}_1=(\xi, \tau+1, \zeta-1)$ and $\mathfrak{P}_2=(\xi, \tau-1, \zeta-1)$. Now the curve given by $\mathfrak{q}$ transforms into a curve passing through the point $\mathfrak{P}_1$ (0, −1, 1) but not through the point $\mathfrak{P}_2$ (0, 1, 1). In terms of ideals, one has the prime ideals $\mathfrak{q}$, $\mathfrak{p}$ in $\mathfrak{R}$, with $\mathfrak{q} \subset \mathfrak{p}$, and the prime ideal $\mathfrak{P}_2$ in $\mathfrak{S}$ which lies over $\mathfrak{p}$. But no prime ideal $\mathfrak{Q}$ in $\mathfrak{S}$ lying over $\mathfrak{q}$ could be contained in $\mathfrak{P}_2$. For suppose $\mathfrak{Q} \subset \mathfrak{P}_2$ and $\mathfrak{Q} \cap \mathfrak{R}=\mathfrak{q}$. We have $\zeta\xi+\eta=(\zeta+\tau)\xi \in \mathfrak{Q}$. Now $\zeta+\tau \in \mathfrak{Q}$, together with $\zeta-1 \in \mathfrak{P}_2$ and $\tau-1 \in \mathfrak{P}_2$, would imply $1 \in \mathfrak{P}_2$, which is impossible; $\xi \in \mathfrak{Q}$ would imply $\eta \in \mathfrak{Q}$ and $\zeta^2-1 \in \mathfrak{Q}$, hence $\zeta-1 \in \mathfrak{Q}$, whence $\mathfrak{Q} \cap \mathfrak{R}$ would contain $\mathfrak{p}$. Thus $\zeta+\tau \notin \mathfrak{Q}$ and $\xi \notin \mathfrak{Q}$. This is a contradiction, and completes the proof that the "going-down" theorem fails for $\mathfrak{R}$ and $\mathfrak{S}$. Geometrically, then, the reason for the failure lies in the fact that a non-integrally closed ring $\mathfrak{R}$ allows a variety on which two branches meet and on which consequently there may be subvarieties which lie locally on only one branch.[5]

(B) Let $\mathfrak{R}$ be the ring of integers and let $\mathfrak{S}=\mathfrak{R}[x]/(x^2-x, 2x)$, where x is an indeterminate. Since no integer is in $(x^2-x, 2x)$, $\mathfrak{S}$ may be considered to contain $\mathfrak{R}$, and if α is the residue of x, then $\mathfrak{S}=\mathfrak{R}[\alpha]$, $\alpha^2-\alpha=0$, $2\alpha=0$. If $\mathfrak{q}=(0)$, $\mathfrak{p}=(2)$, $\mathfrak{P}=(2, \alpha-1)$, then $\mathfrak{P}$ is maximal and lies over $\mathfrak{p}$. There is no $\mathfrak{Q}$ such that $\mathfrak{Q} \cap \mathfrak{R}=\mathfrak{q}$, $\mathfrak{Q} \subset \mathfrak{P}$. For if there were, we would have $2\alpha=0 \in \mathfrak{Q}$, but $2 \notin \mathfrak{Q}$, hence $\alpha \in \mathfrak{Q} \subset \mathfrak{P}$; this is impossible since $\alpha-1 \in \mathfrak{P}$.

(C) Let $\mathfrak{A}=(x^2, xy, xz, yz-y, z^2-z)$ be an ideal in the polynomial ring $K[x, y, z]$. Since $\mathfrak{A} \cap K=(0)$, the ring $\mathfrak{S}=K[x, y, z]/\mathfrak{A}$ contains a field isomorphic to K, which we identify with K, and if ξ, η, ζ are the maps of x, y, z in $\mathfrak{S}$ then $\mathfrak{S}=K[\xi, \eta, \zeta]$. Let $\mathfrak{R}=K[\xi, \eta]$; $\mathfrak{R}$ is not an integral domain and $\mathfrak{S}$ is integral over $\mathfrak{R}$. In $\mathfrak{S}$ we have the

[5] This remark was made to us orally by Professor Zariski. The geometrical reasoning permits us to construct a counterexample simpler than Krull's.

decomposition $\mathfrak{S}\cdot(0)=\mathfrak{P}'\cap\mathfrak{Q}$ where $\mathfrak{Q}$ is the prime ideal $(\xi, \zeta-1)$, and $\mathfrak{P}'$ is the primary ideal (η, ζ), of length 2, belonging to the prime ideal $\mathfrak{P}=(\xi,\eta,\zeta)$. In $\mathfrak{R}$ we have the decomposition $\mathfrak{R}\cdot(0)=\mathfrak{p}'\cap\mathfrak{q}$, where $\mathfrak{q}=\mathfrak{Q}\cap\mathfrak{R}=(\xi)$, and $\mathfrak{p}'=\mathfrak{P}'\cap\mathfrak{R}=(\eta)$ is a primary ideal, of length 2, belonging to $\mathfrak{p}=\mathfrak{P}\cap\mathfrak{R}=(\xi, \eta)$. Since any prime ideal in $\mathfrak{S}$ contains $\mathfrak{S}\cdot(0)$, it must contain one of the prime ideals $\mathfrak{P}$, $\mathfrak{Q}$; hence $\mathfrak{P}$ can contain no prime ideal properly. Since, however, $\mathfrak{P}\cap\mathfrak{R}=\mathfrak{p}\supset\mathfrak{q}$ properly, the "going-down" theorem fails.

We now show that hypotheses (A) and (B) are satisfied. An element of $\mathfrak{S}$ is a 0-divisor if and only if it is contained in at least one of the ideals $\mathfrak{P}$, $\mathfrak{Q}$. If this 0-divisor is in $\mathfrak{R}$, then it is in at least one of the ideals $\mathfrak{p}$, $\mathfrak{q}$; but then it is a 0-divisor *of* $\mathfrak{R}$. Thus (B) holds.

It remains to prove that $\mathfrak{R}$ is integrally closed in its total quotient ring. Since $\xi^2=\xi\eta=0$, every element of $\mathfrak{R}$ can be written in the form $a+b\xi+c(\eta)\eta$, where $a, b\in K$, $c(\eta)\in K[\eta]$; moreover, a is unique. The element $a+b\xi+c(\eta)\eta$ is a 0-divisor if and only if $a=0$, since then and only then would it be in one of the ideals $\mathfrak{p}$, $\mathfrak{q}$. Thus the total quotient ring of $\mathfrak{R}$ consists of the quotients whose denominators are of the form $a+b\xi+c(\eta)\eta$, $a\neq 0$. If we multiply numerator and denominator by $a-b\xi$, we may suppose without loss of generality that $b=0$. Suppose now that $\alpha=[d(\eta)+e\xi]/f(\eta)$, where $e\in K$, $d(y)$, $f(y)\in K[y]$, $f(0)=a\neq 0$, is integral over $\mathfrak{R}$. Since $e\xi/f(\eta)=e\xi/a\in\mathfrak{R}$, we have that $\alpha-e\xi/a=d(\eta)/f(\eta)$ is integral over $\mathfrak{R}=K[\xi, \eta]$, hence also over $K[\eta]$ since $\xi^2=0$. Now $K[\eta]$ is a simple transcendental extension of K, hence is integrally closed. Hence $d(\eta)/f(\eta)\in K[\eta]$ and $\alpha\in\mathfrak{R}$. This completes the proof.

The geometry behind the above counterexample is as follows. The ideal $\mathfrak{S}\cdot(0)$ corresponds to the reducible variety (in the xyz-space) consisting of the line $x=z-1=0$ and the point $x=y=z=0$; the ideal $\mathfrak{R}\cdot(0)$ corresponds to the line $x=0$ in the xy-plane. Over the point (0, 0) lie the points (0, 0, 0) and (0, 0, 1). Since the point (0, 0, 0) is isolated for the variety corresponding to $\mathfrak{S}\cdot(0)$, but the point (0, 0) is not isolated for the variety corresponding to $\mathfrak{R}\cdot(0)$, it is clear that the "going-down" theorem must fail for $\mathfrak{R}$ and $\mathfrak{S}$. Now any polynomial $f(\xi, \eta)$ for which $f(0, 0)=0$ is a 0-divisor in $\mathfrak{S}$, since the cylinder $f(x, y)=0$ contains part of the variety of $\mathfrak{S}\cdot(0)$. If $f(\xi, \eta)$ is to be a 0-divisor also in $\mathfrak{R}$, then the projection of the variety of $\mathfrak{S}\cdot(0)$ must not be, from an algebro-geometric point of view, simply the line $x=0$, but should also have an imbedded point at (0, 0); that is, $\mathfrak{R}\cdot(0)$ should have the prime ideal corresponding to (0, 0) as an imbedded component. This is accomplished above by making the isolated component of $\mathfrak{S}\cdot(0)$ corresponding to (0, 0, 0) a proper primary ideal.

4. **Some additional remarks.** We saw above that if $\mathfrak{S}$ is integral over $\mathfrak{R}$ then the "lying-over" theorem holds for $\mathfrak{R}$ and $\mathfrak{S}$. An obvious necessary condition for the "lying-over" theorem to hold for a pair of rings $\mathfrak{R}$, $\mathfrak{S}$ is that $\mathfrak{S}\cdot\mathfrak{p}\cap\mathfrak{R}=\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ in $\mathfrak{R}$. This is known to be also a sufficient condition in the case that $\mathfrak{R}$ and $\mathfrak{S}$ are integral domains. We now show this to be true in general.

THEOREM 6. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be two rings, with $\mathfrak{R}\subset\mathfrak{S}$, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{R}$. A necessary and sufficient condition that there exist a prime ideal $\mathfrak{P}$ in $\mathfrak{S}$ lying over $\mathfrak{p}$ is that $\mathfrak{S}\cdot\mathfrak{p}\cap\mathfrak{R}=\mathfrak{p}$.*

PROOF. Suppose $\mathfrak{S}\cdot\mathfrak{p}\cap\mathfrak{R}=\mathfrak{p}$. Let $\mathfrak{P}$ be a maximal element[2] in the set of ideals in $\mathfrak{S}$ which contract to $\mathfrak{p}$. That $\mathfrak{P}$ is prime follows just as in Theorem 2.

THEOREM 7. *Let the ring $\mathfrak{R}$ be contained in the field $\mathfrak{K}$, and let $\theta\in\mathfrak{K}$, $\theta\neq 0$. If $\mathfrak{p}$ is a prime ideal in $\mathfrak{R}$ then in either $\mathfrak{R}[\theta]$ or $\mathfrak{R}[\theta^{-1}]$ there lies a prime ideal over $\mathfrak{p}$.*[6]

PROOF. Suppose that no prime ideal in $\mathfrak{R}[\theta]$ lies over $\mathfrak{p}$. Then $\mathfrak{p}\cdot\mathfrak{R}[\theta]\cap\mathfrak{R}\supset\mathfrak{p}$ properly. Hence there exists an element $b\in\mathfrak{R}$, $b\notin\mathfrak{p}$ such that $b=p_0+p_1\theta+\cdots+p_m\theta^m$, $p_i\in\mathfrak{p}$. But then θ^{-1} satisfies an equation with leading coefficient not in $\mathfrak{p}$. Hence $\mathfrak{R}'[\theta^{-1}]$ is integral over $\mathfrak{R}'$, where $\mathfrak{R}'$ is the quotient ring of $\mathfrak{R}$ with respect to $\mathfrak{p}$, and there exists a prime ideal $\mathfrak{P}'$ in $\mathfrak{R}'[\theta^{-1}]$ which lies over the prime ideal $\mathfrak{R}'\cdot\mathfrak{p}$. Then $\mathfrak{P}=\mathfrak{P}'\cap\mathfrak{R}[\theta^{-1}]$ lies over $\mathfrak{p}$.

The following theorem is the basis on which Krull proves the "going-down" theorem in the case of integral domains. We give a somewhat more direct proof.

THEOREM 8. *Let $\mathfrak{R}$ be integrally closed in its quotient field $\mathfrak{K}$, and let $\mathfrak{S}$ be the integral closure of $\mathfrak{R}$ in a finite normal extension $\mathfrak{L}$ of $\mathfrak{K}$. Then any two prime ideals in $\mathfrak{S}$ which lie over the same ideal in $\mathfrak{R}$ are conjugate.*

PROOF. It is clear that $\mathfrak{S}$ is invariant under every automorphism of $\mathfrak{L}/\mathfrak{K}$; two ideals of $\mathfrak{S}$ are said to be conjugate if one is carried into the other by such an automorphism. Let $\mathfrak{P}_1$ be a prime ideal in $\mathfrak{S}$ and let $\mathfrak{P}_1,\cdots,\mathfrak{P}_m$ be a complete set of distinct conjugates of $\mathfrak{P}_1$. We show that if $\mathfrak{P}$ is a prime ideal in $\mathfrak{S}$ such that $\mathfrak{P}\cap\mathfrak{R}=\mathfrak{P}_1\cap\mathfrak{R}$, then $\mathfrak{P}$ is one of the ideals $\mathfrak{P}_1,\cdots,\mathfrak{P}_m$. For suppose $\mathfrak{P}\neq\mathfrak{P}_i$, $i=1,\cdots,m$. Then by Theorem 4, $\mathfrak{P}\not\subset\mathfrak{P}_i$, $i=1,\cdots,m$. Hence there exists an element $\alpha\in\mathfrak{P}$, $\alpha\notin\mathfrak{P}_i$, $i=1,\cdots,m$. But then none of the

[6] This theorem was given by Professor Chevalley in a Princeton lecture.