ON THE STRUCTURE AND IDEAL THEORY OF COMPLETE LOCAL RINGS

BY
I. S. COHEN

Introduction. The concept of a local ring was introduced by Krull [7][1], who defined such a ring as a commutative ring $\mathfrak{R}$ in which every ideal has a finite basis and in which the set $\mathfrak{m}$ of all non-units is an ideal, necessarily maximal. He proved that the intersection of all the powers of $\mathfrak{m}$ is the zero ideal. If the powers of $\mathfrak{m}$ are introduced as a system of neighborhoods of zero, then $\mathfrak{R}$ thus becomes a topological ring, in which the usual topological notions —such as that of regular sequence (§2)—may be defined. The local ring $\mathfrak{R}$ is called complete if every regular sequence has a limit. Let $\mathfrak{m}=(u_1, u_2, \cdots, u_n)$ and assume that no element of this basis may be omitted. If the ideals $(u_1, u_2, \cdots, u_i)$, $i=1, 2, \cdots, n$, are all prime, $\mathfrak{R}$ is said to be a regular local ring[2] of dimension n.

It was conjectured by Krull [7, p. 219] that a complete regular local ring $\mathfrak{R}$ of dimension n whose characteristic equals that of its *residue field* $\mathfrak{R}/\mathfrak{m}$ is isomorphic to the ring of formal power series in n variables with coefficients in this field. If on the other hand the characteristics are different, so that the characteristic of $\mathfrak{R}$ is zero and that of $\mathfrak{R}/\mathfrak{m}$ is a prime number p, then $\mathfrak{R}$ cannot have this structure. In this case we note that p must be contained in $\mathfrak{m}$. Krull then conjectured that if $\mathfrak{R}$ is unramified (that is, if p is not contained in $\mathfrak{m}^2$), then $\mathfrak{R}$ is uniquely determined by its residue field and its dimension. He conjectured finally that every complete local ring is a homomorphic image of a complete regular local ring.

These conjectures are proved in §§4–7, in particular, in Theorem 15 and its corollaries. Actually the basic result, to the proof of which is devoted Part II (§§4–6), is the one concerning arbitrary (that is, not necessarily regular) complete local rings. It is proved (Theorems 9 and 12) that every complete local ring $\mathfrak{R}$ is a homomorphic image of a complete regular local ring of a specific type, namely, the ring of all power series in a certain number of variables with coefficients taken from a field or from a valuation ring of a certain simple kind. This follows easily as soon as it is shown that a suitable "coefficient domain" can be imbedded in $\mathfrak{R}$, and the burden of the proof of

Presented to the Society, December 27, 1942; received by the editors July 14, 1945.

[1] Numbers in brackets refer to the Bibliography at the end of the paper.

[2] This is equivalent to Krull's definition of a *p-Reihenring*, as given in §7; the equivalence is proved in Theorem 14 and its corollary. The term "regular local ring" was introduced by Chevalley [1].

the structure theorems therefore lies in demonstrating the possibility of this imbedding (Theorems 9 and 11).

This problem is similar to that of the structure of a field complete with respect to a valuation, a question considered by Hasse and Schmidt [3], Teichmüller [12], and MacLane [9]. In case the residue field $\mathfrak{R}/\mathfrak{m}$ is of characteristic zero, the imbedding is accomplished relatively easily by means of a generalization of Hensel's Lemma on valuation rings. If $\mathfrak{R}/\mathfrak{m}$ and $\mathfrak{R}$ are of characteristic p then the methods of Teichmüller apply with little modification, provided that $\mathfrak{R}/\mathfrak{m}$ is algebraically perfect; but if $\mathfrak{R}/\mathfrak{m}$ is imperfect, there arise essentially new difficulties, for the overcoming of which a generalization of the idea of a local ring is introduced in Part I. Finally, if $\mathfrak{R}$ and $\mathfrak{R}/\mathfrak{m}$ have different characteristics, then the methods of MacLane can be applied, but here, too, the properties of generalized local rings must be used if $\mathfrak{R}/\mathfrak{m}$ is imperfect.

Part III deals with the properties of a regular local ring $\mathfrak{R}$. If $\mathfrak{R}$ is complete its structure is explicitly described in §7 as a power series ring over a field or over a complete discrete valuation ring (Theorem 15) except, possibly, when $\mathfrak{R}$ is of characteristic zero and $p \in \mathfrak{m}^2$ ($\mathfrak{R}$ is *ramified*); in this case a necessary condition and a sufficient condition are given (Theorem 17, corollary) for $\mathfrak{R}$ to be a power series ring. In any case if $\mathfrak{R}$ is ramified, it is a specific kind of extension of a power series ring (Theorem 17). More generally any complete local ring without zero-divisors is a finite module over a power series ring (Theorem 16). In §8 some questions in complete local rings are considered, including factorization and dimension theory. Some results previously known for rings of power series over infinite fields are extended to the case of finite coefficient fields (see footnotes 19 and 25). The well known theorem of Macaulay on unmixed ideals in polynomial rings is proved for arbitrary regular local rings. In §9 a relative ramification degree is defined analogous to that for valuation rings.

Part I deals with preliminary definitions and results needed for the rest of the paper, in particular with generalized local rings.

Several of the original proofs (notably, those of Theorems 5 and 16 and Lemma 15) have been changed following the appearance of Chevalley's paper on local rings [1], from which various suggestions for simplifications have been obtained.

Thanks are due to A. Seidenberg for a critical reading of the manuscript of this paper and for many valuable suggestions.

Part I

1. **Elementary properties.** Definition. A *local ring* is a commutative ring $\mathfrak{R}$ with an identity element in which:

(1) The set $\mathfrak{m}$ of all non-units is an ideal in $\mathfrak{R}$;

(2) Every ideal in $\mathfrak{R}$ has a finite basis.

The above definition was given by Krull [7], who proved the following important property [7, Theorem 2]:

If $\mathfrak{a}$ *is an ideal in* $\mathfrak{R}$, *then*

$$\bigcap_{k=1}^{\infty} (\mathfrak{a}, \mathfrak{m}^k) = \mathfrak{a}. \tag{1}$$

For $\mathfrak{a} = (0)$, we have the special case

$$\bigcap_{k=1}^{\infty} \mathfrak{m}^k = (0). \tag{2}$$

This relation suggests a type of ring more general than the local ring. We introduce it in order to facilitate certain of the proofs in Part II.

Definition. A *generalized local ring* (g.l.r.) is a commutative ring with an identity element in which:

(1) The set $\mathfrak{m}$ of all non-units is an ideal with a finite basis;

(2) $\bigcap_{k=1}^{\infty} \mathfrak{m}^k = (0)$.

This clearly includes the concept of local ring, in view of (2). The ideal $\mathfrak{m}$ is necessarily a maximal ideal and contains every ideal in $\mathfrak{R}$ different from the unit ideal; thus it is the only maximal ideal in $\mathfrak{R}$. We shall denote this unique maximal ideal by $\mathfrak{m}$.

Lemma 1. *If* $\mathfrak{a}$ *is an ideal in the* g.l.r. $\mathfrak{R}$ *such that* $\mathfrak{m} = (\mathfrak{a}, \mathfrak{m}^2)$, *then* $\mathfrak{a} = \mathfrak{m}$.

Proof. In case $\mathfrak{R}$ is a local ring, the lemma follows from (1). In the general case, let $\{u_1, \cdots, u_n\}$ be a basis of $\mathfrak{m}$: $\mathfrak{m} = (u_1, \cdots, u_n)$; such a basis exists by property (1) of the definition of a g.l.r. Since $\mathfrak{m} = (\mathfrak{a}, \mathfrak{m}^2)$,

$$u_i = \sum_{j=1}^{n} c_{ij} u_j + a_i, \qquad i = 1, 2, \cdots, n,$$

where $c_{ij} \in \mathfrak{m}$ and $a_i \in \mathfrak{a}$. This implies

$$\sum_{j=1}^{n} (\delta_{ij} - c_{ij}) u_j = a_i.$$

If d denotes the determinant $|\delta_{ij} - c_{ij}|$, then $du_j \equiv 0(\mathfrak{a})$, $j = 1, 2, \cdots, n$; and since clearly $d \equiv 1(\mathfrak{a})$, it follows that $u_j \equiv 0(\mathfrak{a})$. Thus $\mathfrak{m} \subseteq \mathfrak{a}$, as was to be proved.

If $\{u_1, \cdots, u_n\}$ is a basis for $\mathfrak{m}$, it is said to be a *minimal basis* if no proper subset is a basis.

Since $\mathfrak{m}$ is maximal, the ring $\mathfrak{R}/\mathfrak{m}$ of residue classes is a field, called the *residue field*. We shall always denote it by P. If $c \in \mathfrak{R}$, then the map of c in the natural homomorphism of $\mathfrak{R}$ on P will be called the *residue* of c, and will often be denoted by $\bar{c}$. The ring $\mathfrak{m}/\mathfrak{m}^2$ may clearly be regarded as a P-module—that is, as a vector space over P.

Lemma 2. *If* $\mathfrak{R}$ *is a* g.l.r., *then the elements* $u_1, u_2, \cdots, u_n$ *in* $\mathfrak{m}$ *form a* *minimal basis for* $\mathfrak{m}$ *if and only if they give rise modulo* $\mathfrak{m}^2$ *to elements which form a* P*-basis for* $\mathfrak{m}/\mathfrak{m}^2$. *The number of elements in a minimal basis of* $\mathfrak{m}$ *is equal to the dimension of* $\mathfrak{m}/\mathfrak{m}^2$ *over* P; *any two minimal bases have the same number of elements. If* $\{u_1, u_2, \cdots, u_n\}$ *is a minimal basis for* $\mathfrak{m}$, *and if* $v_i=\sum_{j=1}^n c_{ij}u_j$, $i=1, 2, \cdots, n$, $c_{ij}\in\mathfrak{R}$, *then* $\{v_1, v_2, \cdots, v_n\}$ *is a basis if and only if the determinant* $|c_{ij}|$ *is not in* $\mathfrak{m}$; *it is then necessarily minimal.*

Proof. Let $\{u_1, u_2, \cdots, u_n\}$ be a minimal basis of $\mathfrak{m}$. If the residues mod $\mathfrak{m}^2$ of the u_i do not form a P-basis for $\mathfrak{m}/\mathfrak{m}^2$, then they must be linearly dependent over P. Thus there is a relation $c_1u_1+c_2u_2+\cdots+c_nu_n\equiv 0(\mathfrak{m}^2)$, with $c_i\in\mathfrak{R}$, and at least one c_i—say c_1—not in $\mathfrak{m}$. Then c_1 is a unit, and so $u_1\in(u_2, \cdots, u_n, \mathfrak{m}^2)$; thus $\mathfrak{m}=(u_2, \cdots, u_n, \mathfrak{m}^2)$ and by Lemma 1, $\mathfrak{m}=(u_2, \cdots, u_n)$. However, this contradicts the minimality of $\{u_1, u_2, \cdots, u_n\}$.

Conversely, suppose $u_1, u_2, \cdots, u_n$ are elements of $\mathfrak{m}$ giving rise mod $\mathfrak{m}^2$ to elements of $\mathfrak{m}/\mathfrak{m}^2$ which form a P-basis. Then obviously $\mathfrak{m}=(u_1, u_2, \cdots, u_n, \mathfrak{m}^2)$, and by Lemma 1, $\mathfrak{m}=(u_1, u_2, \cdots, u_n)$. If $\{u_1, u_2, \cdots, u_n\}$ were not a minimal basis, then, say, $u_1\in(u_2, \cdots, u_n)$. But this would imply that the residues mod $\mathfrak{m}^2$ of $u_2, \cdots, u_n$ form a P-basis, which is false.

This proves the first statement; the rest of the lemma now follows easily.

Whenever we write $\mathfrak{m}=(u_1, u_2, \cdots, u_n)$, where $\mathfrak{m}$ is the maximal ideal in a g.l.r. $\mathfrak{R}$, *we shall always mean that these elements form a minimal basis for* $\mathfrak{m}$, unless the contrary is explicitly stated.

Suppose now that $\mathfrak{m}=(u_1, u_2, \cdots, u_n)$, and let $R=\mathrm{P}[x_1, x_2, \cdots, x_n]$ be the polynomial ring over P in n indeterminates. If $c\in\mathfrak{R}$, let $f(u_1, u_2, \cdots, u_n)$ be a form of some degree $k(\geqq 0)$ in $u_1, u_2, \cdots, u_n$ with coefficients in $\mathfrak{R}$ (but not all in $\mathfrak{m}$) such that

$$c\equiv f(u_1, u_2, \cdots, u_n)(\mathfrak{m}^{k+1}).$$

If each coefficient of f is replaced by its residue, and if each u_i is replaced by x_i, then we obtain a form $\bar{f}(x_1, x_2, \cdots, x_n)$ of degree k in R; this is called an *initial form* of the element c.

Since $\bigcap\mathfrak{m}^k=(0)$ we see that if $c\neq 0$ there is a k such that $c\equiv 0(\mathfrak{m}^k)$, $c\not\equiv 0(\mathfrak{m}^{k+1})$. Thus $c=f(u_1, u_2, \cdots, u_n)$, where f is a form of degree k whose coefficients are not all in $\mathfrak{m}$, and c has an initial form of degree k. Hence every element of $\mathfrak{R}$ has at least one initial form, except possibly the element zero; in any case we consider the zero of R to be an initial form of the zero of $\mathfrak{R}$.

If c and d have $\bar{f}$ and $\bar{g}$, respectively, as initial forms, then cd has $\bar{f}\bar{g}$ as initial form; and if $\bar{f}$ and $\bar{g}$ are of the same degree, then $\bar{f}+\bar{g}$ (if it does not vanish) is an initial form of $c+d$.

If $\mathfrak{a}$ is an ideal in $\mathfrak{R}$, then the homogeneous ideal $\mathfrak{a}'$ in R generated by the initial forms of all elements in $\mathfrak{a}$ is called the *form ideal* of $\mathfrak{a}$ [7, p. 208]. Note that if $\bar{f}(x_1, x_2, \cdots, x_n)$ is a *homogeneous* element of $\mathfrak{a}'$, then it is actually the initial form of some element in $\mathfrak{a}$.

If also $\mathfrak{m}=(v_1, v_2, \cdots, v_n)$, then by Lemma 2, $v_i=\sum_{j=1}^{n}c_{ij}u_j$, where $|c_{ij}| \not\equiv 0(\mathfrak{m})$. The effect on the polynomial ring $R=\mathrm{P}[x_1, \cdots, x_n]$ is to subject it to the linear transformation $y_i=\sum_{j=1}^{n}\bar{c}_{ij}x_j$, $|\bar{c}_{ij}|\neq 0$. The initial forms and form ideals are thus essentially independent of the particular minimal basis chosen.

For the remainder of this section $\mathfrak{R}$ is a local ring.

Definition. The ideal $\mathfrak{a}$ in $\mathfrak{R}$ is said to have *dimension* r if there exists at least one chain $\mathfrak{a}\subseteq\mathfrak{p}_r\subset \cdots \subset\mathfrak{p}_1\subset\mathfrak{p}_0=\mathfrak{m}$, where the $\mathfrak{p}_i$ are prime ideals, but no such chain with more than $r+1$ prime ideals $\mathfrak{p}_i$. If $\mathfrak{p}$ is prime, it is said to have *rank*[3] r if there exists at least one chain $\mathfrak{p}\supset\mathfrak{p}_{r-1}\supset \cdots \supset\mathfrak{p}_1\supset\mathfrak{p}_0\supseteq(0)$, where the $\mathfrak{p}_i$ are prime, but no such chain with more than r ideals $\mathfrak{p}_i$. (See [7, p. 209].)

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathfrak{R}$ and $\mathfrak{a}\subseteq\mathfrak{b}$, then the dimension of $\mathfrak{a}$ is at least as great as that of $\mathfrak{b}$. The dimension of $\mathfrak{a}$ is clearly equal to the maximum of the dimensions of its associated prime ideals. We therefore define the *rank* of $\mathfrak{a}$ to be the minimum of the ranks of its associated prime ideals. If $\mathfrak{p}$ is prime, then the sum of its rank and dimension is at most the rank of $\mathfrak{m}$, which equals the dimension of (0). That this latter is really finite is implied by the following fundamental theorem [7, p. 220, Theorem 7*]:

If $\mathfrak{p}$ is a minimal prime ideal of the ideal $\mathfrak{b}=(b_1, b_2, \cdots, b_r)$ having r elements in its basis, then the rank of $\mathfrak{p}$ is at most r.

The rank of $\mathfrak{m}$ is therefore at most n if $\mathfrak{m}=(u_1, u_2, \cdots, u_n)$.

Definition. The *dimension* of $\mathfrak{R}$ is the rank of $\mathfrak{m}$.

We observe finally that if $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals and $\mathfrak{p}$ contains $\mathfrak{p}'$ properly, then the rank of $\mathfrak{p}$ is greater than that of $\mathfrak{p}'$, while the dimension of $\mathfrak{p}$ is less than that of $\mathfrak{p}'$.

2. **Complete local rings.** In any generalized local ring $\mathfrak{R}$, a topology can be introduced by taking the ideals $\mathfrak{m}, \mathfrak{m}^2, \mathfrak{m}^3, \cdots$ to be neighborhoods of zero. This is the *natural topology* of $\mathfrak{R}$. It is immediate that $\mathfrak{R}$ thus becomes a Hausdorff space satisfying the first axiom of countability in which addition and multiplication are continuous; thus $\mathfrak{R}$ is a topological ring. Any primary ideal belonging to $\mathfrak{m}$ is open and closed in this topology.

Definition. The sequence $\{a_n\}$ of elements of $\mathfrak{R}$ is *regular* if, given any $m>0$, $a_h-a_k\in\mathfrak{m}^m$ for h and k sufficiently large.

It is clear that a necessary and sufficient condition that $\{a_n\}$ be regular is that $\lim_{n\to\infty}(a_{n+1}-a_n)=0$.

Definition. The g.l.r. $\mathfrak{R}$ is said to be *complete* if every regular sequence in $\mathfrak{R}$ has a limit in $\mathfrak{R}$.

In a complete local ring a sufficient condition for the convergence of an infinite series $\sum_{n=1}^{\infty}a_n$ is that $\lim a_n=0$.

[3] We use the term "rank" (following Lasker and Macaulay) rather than Krull's "*Dimensionsdefekt.*"

Definition. If $\mathfrak{R}$ is g.l.r., then $\mathfrak{R}^*$ is a *completion* of $\mathfrak{R}$ if:

(1) $\mathfrak{R}^*$ is a topological ring (satisfying the first countability axiom) containing $\mathfrak{R}$ both as a subring and a subspace;

(2) $\mathfrak{R}$ is dense in $\mathfrak{R}^*$;

(3) $\mathfrak{R}^*$ is complete.

Theorem 1. *Every* g.l.r. $\mathfrak{R}$ *has a completion which is unique to within isomorphism over* $\mathfrak{R}$[4].

Proof. If a and b are distinct elements of $\mathfrak{R}$, then there is a positive integer k such that $a-b\equiv 0(\mathfrak{m}^k)$, $a-b\not\equiv 0(\mathfrak{m}^{k+1})$. We then define $\rho(a, b)=2^{-k}$. It is clear that ρ is a metric for $\mathfrak{R}$ and that regularity of a sequence in this metric is equivalent to regularity as defined above. By a well known theorem, $\mathfrak{R}$ can be extended to a space $\mathfrak{R}^*$, complete with respect to a metric ρ which is an extension of the metric of $\mathfrak{R}$, such that $\mathfrak{R}$ is dense in $\mathfrak{R}^*$. If a^*, b^* are elements of $\mathfrak{R}^*$, then there are sequences $\{a_n\}$ and $\{b_n\}$ in $\mathfrak{R}$ such that $a^*=\lim a_n$, $b^*=\lim b_n$. We then define $a^*+b^*=\lim (a_n+b_n)$, $a^*b^*=\lim (a_nb_n)$. It is immediate that this definition of addition and multiplication in $\mathfrak{R}^*$ is independent of the particular sequences $\{a_n\}$ and $\{b_n\}$ chosen, and that $\mathfrak{R}^*$ thus becomes a ring containing $\mathfrak{R}$ as a subring.

It is easily seen that the relations

$$\rho(a - b, a' - b') \leqq \rho(a, a') + \rho(b, b'), \quad \rho(ab, a'b') \leqq \rho(a, a') + \rho(b, b')$$

hold for elements of $\mathfrak{R}$. Hence, by the continuity of the distance function, they hold also in $\mathfrak{R}^*$, and it follows that $\mathfrak{R}^*$ is a topological ring. Since $\rho(a^*, b^*)=\rho(a^*-b^*, 0)$, metric regularity in $\mathfrak{R}^*$ is equivalent to regularity as defined above. Thus $\mathfrak{R}^*$ is a completion of $\mathfrak{R}$.

If $\mathfrak{R}_1^*$ is another completion, let a^* be any element of $\mathfrak{R}^*$. Then $a^*=\lim a_n$, where $a_n\in\mathfrak{R}$. The sequence $\{a_n\}$ is regular and so has a limit a_1^* in the complete ring $\mathfrak{R}_1^*$. The mapping $a^*\rightarrow a_1^*$ is easily seen to be a homeomorphism and an isomorphism of $\mathfrak{R}^*$ on $\mathfrak{R}_1^*$ which leaves invariant every element of $\mathfrak{R}$. Thus $\mathfrak{R}^*$ is essentially unique.

We now show that the completion of a g.l.r. is again a g.l.r. As such it has a natural topology defined by the powers of its maximal ideal. But it has also a topology in consequence of its being a completion, and we prove in the next theorem that these coincide. The proof could be made somewhat shorter by making use of the specific construction for the completion, but it seems better to use merely the defining properties.

Theorem 2. *If* $\mathfrak{R}$ *is a* g.l.r., *then so is its completion* $\mathfrak{R}^*$, *and the topology of* $\mathfrak{R}^*$ *coincides with its natural topology. If* $\mathfrak{m}^*$ *is the maximal ideal of* $\mathfrak{R}^*$, *then there is a* 1-1 *correspondence between the primary ideals* $\mathfrak{q}$ *in* $\mathfrak{R}$ *belonging to*

[4] In the case where $\mathfrak{R}$ is a local ring this theorem has been given by Krull [7, p. 218, Theorem 14] in a less precise form.

$\mathfrak{m}$ *and the primary ideals* $\mathfrak{q}^*$ *in* $\mathfrak{R}^*$ *belonging to* $\mathfrak{m}^*$; *if, namely,* $\mathfrak{q}$ *and* $\mathfrak{q}^*$ *correspond, then* $\mathfrak{q}^*=\mathfrak{R}^*\cdot\mathfrak{q}$, $\mathfrak{q}=\mathfrak{q}^*\cap\mathfrak{R}$. *In particular,*

$$(3)\qquad \mathfrak{m}^{*k}=\mathfrak{R}^*\cdot\mathfrak{m}^k,\qquad \mathfrak{m}^{*k}\cap\mathfrak{R}=\mathfrak{m}^k,\qquad k=1,2,\cdots.$$

The residue fields of $\mathfrak{R}$ *and* $\mathfrak{R}^*$ *are isomorphic. A minimal basis for* $\mathfrak{m}$ *is also one for* $\mathfrak{m}^*$.

Proof. (a) First we show that *if* $\mathfrak{b}$ *is any ideal in* $\mathfrak{R}$ *and* $b^*\in\mathfrak{R}^*\cdot\mathfrak{b}$, then[5] $b^*=\lim_{k\to\infty}b_k$, *where* $b_k\in\mathfrak{b}$. For let $b^*=\sum a_i^*b_i'$, $a_i^*\in\mathfrak{R}^*$, $b_i'\in\mathfrak{b}$; then $a_i^*=\lim_{k\to\infty}a_{ik}$, $a_{ik}\in\mathfrak{R}$. Hence $b^*=\lim_{k\to\infty}\sum_i a_{ik}b_i'$, and we take $b_k=\sum_i a_{ik}b_i'$.

(b) *If* $\mathfrak{b}=\mathfrak{m}^h$, *then also the converse of this statement is true.* For suppose $b^*\in\mathfrak{R}^*$, and $b^*=\lim b_k$, with $b_k\in\mathfrak{m}^h$. We may assume that $b_k-b_{k-1}\in\mathfrak{m}^{h+k-1}$ $(k\geqq 1)$ and $b_0=0$. Hence if $v_1, v_2, \cdots, v_N$ are the power products of $u_1, u_2, \cdots, u_n$ (the basis elements for $\mathfrak{m}$) of degree h, then $b_k-b_{k-1}=\sum_{i=1}^{N}c_{ki}v_i$, where $c_{ki}\in\mathfrak{m}^{k-1}$. The infinite series $\sum_k c_{ki}$ converges in $\mathfrak{R}^*$ since $c_{ki}\to 0$. Thus $b^*=\sum_{k=1}^{\infty}(b_k-b_{k-1})=\sum_{i=1}^{n}v_i\sum_{k=1}^{\infty}c_{ki}\in\mathfrak{R}^*\cdot\mathfrak{m}^h$.

(c) *If* $\mathfrak{q}$ *is a primary ideal belonging to* $\mathfrak{m}$, *then* $\mathfrak{R}^*\cdot\mathfrak{q}\cap\mathfrak{R}=\mathfrak{q}$. For if $b\in\mathfrak{R}^*\cdot\mathfrak{q}\cap\mathfrak{R}$, then by (a), $b=\lim b_k$, $b_k\in\mathfrak{q}$. Since $\mathfrak{q}$ is open in $\mathfrak{R}$, $b-b_k\in\mathfrak{q}$ for large k, hence $b\in q$.

(d) In particular, $\mathfrak{R}^*\cdot\mathfrak{m}^h\cap\mathfrak{R}=\mathfrak{m}^h$. For $h=1$, this implies that $\mathfrak{R}^*\cdot\mathfrak{m}\neq\mathfrak{R}^*$. *We assert that* $\mathfrak{R}^*\cdot\mathfrak{m}$ *contains all the non-units in* $\mathfrak{R}^*$, *hence is the ideal of non-units*. Suppose, namely, that b^* is in $\mathfrak{R}^*$ but not in $\mathfrak{R}^*\cdot\mathfrak{m}$, and let $b^*=\lim b_k$, $b_k\in\mathfrak{R}$. Only a finite number of the b_k can be in $\mathfrak{m}$, for if infinitely many were, then by (b), b^* would be in $\mathfrak{R}^*\cdot\mathfrak{m}$, contrary to the choice of b^*. Since only a finite number of b_k are in $\mathfrak{m}$, we may assume that none are and so each b_k is a unit. Since $b_{k+1}^{-1}-b_k^{-1}=b_{k+1}^{-1}b_k^{-1}(b_k-b_{k+1})$, it follows that $\{b_k^{-1}\}$ is a regular sequence in $\mathfrak{R}$, hence has a limit b_1^* in $\mathfrak{R}^*$. Then $b^*b_1^*=1$ and b^* is a unit; thus every element of $\mathfrak{R}^*$ not in $\mathfrak{R}^*\cdot\mathfrak{m}$ is a unit. Let $\mathfrak{m}^*=\mathfrak{R}^*\cdot\mathfrak{m}$; equations (3) now follow, in view of (c).

(e) *For any* b^* *in* $\mathfrak{R}^*$, *there is an element* b *in* $\mathfrak{R}$ *such that* $b^*\equiv b(\mathfrak{m}^{*h})$. Namely, let $b^*=\lim b_k$, $b_k\in\mathfrak{R}$. Since $\{b_k\}$ is a regular sequence there is an integer i such that $b_k-b_i\in\mathfrak{m}^h$ for $k>i$. Hence $b^*-b_i=\lim_{k\to\infty}(b_k-b_i)\in\mathfrak{R}^*\cdot\mathfrak{m}^h$, by (b)—that is, $b^*-b_i\in\mathfrak{m}^{*h}$.

Together with (3)—which implies that $\mathfrak{R}/\mathfrak{m}^h$ may be considered a subring of $\mathfrak{R}^*/\mathfrak{m}^{*h}$—(e) shows that the two rings coincide. For $h=1$, this means that the residue fields of $\mathfrak{R}^*$ and $\mathfrak{R}$ coincide.

(f) *The ring* $\mathfrak{R}^*$ *is a* g.l.r. For suppose $b^*\in\bigcap\mathfrak{m}^{*h}$. Since $b^*\in\mathfrak{R}^*$, $b^*=\lim b_k$, $b_k\in\mathfrak{R}$; for a fixed h, we have by (a), and since $b^*\in\mathfrak{R}^*\cdot\mathfrak{m}^h$, that $b^*=\lim a_k$, $a_k\in\mathfrak{m}^h$. Thus for large k, $b_k\equiv a_k(\mathfrak{m}^h)$, hence $b_k\equiv 0(\mathfrak{m}^h)$. Since this holds for all h, $\lim b_k=0$—that is, $b^*=0$. Thus $\bigcap\mathfrak{m}^{*h}=(0)$.

Also, $\mathfrak{m}^*$ has a finite basis, for $\mathfrak{m}^*=\mathfrak{R}^*\cdot\mathfrak{m}=\mathfrak{R}^*\cdot(u_1, u_2, \cdots, u_n)$. This

[5] Throughout this proof "lim" means limit with respect to the topology which $\mathfrak{R}^*$ has in virtue of its being a completion.

basis is actually minimal. For suppose $u_1 = b_2^* u_2 + \cdots + b_n^* u_n$, $b_i^* \in \mathfrak{R}^*$. By (e) there is a b_i in $\mathfrak{R}$ such that $b_i^* \equiv b_i(\mathfrak{m}^*)$. Thus $u_1 \equiv \sum_{i=2}^n b_i u_i (\mathfrak{m}^{*2})$, and since $u_1 - \sum_{i=2}^n b_i u_i \in \mathfrak{R}$, (3) implies that $u_1 \in (u_2, \cdots, u_n, \mathfrak{m}^2)$. By Lemma 1, we would have $\mathfrak{m} = (u_2, \cdots, u_n)$, contradicting the minimality of the basis $\{u_1, \cdots, u_n\}$.

(g) If $\mathfrak{q}$ is a primary ideal of $\mathfrak{m}$, then $\mathfrak{R}^* \cdot \mathfrak{q}$ is a primary ideal of $\mathfrak{m}^*$, and we have seen that $\mathfrak{R}^* \cdot \mathfrak{q} \cap \mathfrak{R} = \mathfrak{q}$. Conversely, if $\mathfrak{q}^*$ is a primary ideal of $\mathfrak{m}^*$, then $\mathfrak{q} = \mathfrak{q}^* \cap \mathfrak{R}$ is a primary ideal of $\mathfrak{m}$. Moreover, $\mathfrak{R}^* \cdot \mathfrak{q} = \mathfrak{q}^*$, for if $b^* \in \mathfrak{q}^*$, then by (e) there is a b in $\mathfrak{R}$ such that $b^* - b \in \mathfrak{R}^* \cdot \mathfrak{m}^h \subseteq \mathfrak{R}^* \cdot \mathfrak{q}$ (for suitable h). Since $b^* - b \in \mathfrak{q}^*$, $b \in \mathfrak{q}^* \cap \mathfrak{R} = \mathfrak{q}$, so that $b^* \in \mathfrak{R}^* \cdot \mathfrak{q}$.

(h) It remains to prove only that the given topology of $\mathfrak{R}^*$ is its natural topology. We note that these topologies coincide on $\mathfrak{R}$, because $\mathfrak{R}$ is a subspace of $\mathfrak{R}^*$ and because of equations (3). It is therefore sufficient to find for every sequence $\{b_k^*\}$ in $\mathfrak{R}^*$ a sequence $\{b_k\}$ in $\mathfrak{R}$ such that $\{b_k^* - b_k\}$ is a null sequence in both topologies.

Let $\{U_k\}$ be a system of neighborhoods of zero in $\mathfrak{R}^*$ (with respect to its given topology). For a fixed k, let $b_k^* = \lim_{h \to \infty} a_h$. Then for large h, $b_k^* - a_h \in U_k$. But from the proof of (e) it is clear that $b_k^* - a_h \in \mathfrak{m}^{*k}$ for large h. Hence if we let $b_k = a_h$ for some fixed large value of h, we have $b_k^* - b_k$ in both U_k and $\mathfrak{m}^{*k}$. Thus $\{b_k\}$ is the desired sequence.

The proof of Theorem 2 is now complete.

Even though our interest lies primarily in local rings, we must consider also generalized local rings since a proof involving local rings may well lead to a ring which is only a generalized local ring. It is therefore of fundamental importance that we can always get back to an actual local ring:

THEOREM 3. *If a generalized local ring is complete, then it is a local ring*[6].

From Theorem 2 we have as an immediate consequence that the completion of a g.l.r. is a local ring.

Proof. Let $\mathfrak{R}$ be a complete g.l.r. It is necessary to prove merely that every ideal $\mathfrak{a}$ in $\mathfrak{R}$ has a finite basis. Let $\mathfrak{m} = \mathfrak{R} \cdot (u_1, u_2, \cdots, u_n)$.

If $\mathfrak{a}'$ is the form ideal of $\mathfrak{a}$, then $\mathfrak{a}' = (\bar{\psi}_1(x), \cdots, \bar{\psi}_s(x))$, where $\bar{\psi}_i(x)$ is a homogeneous polynomial in $R = P[x_1, \cdots, x_n]$, $i = 1, 2, \cdots, s$. Let $\bar{\psi}_i(x)$ be of degree k_i; we assume $\mathfrak{a} \neq \mathfrak{R}$, so that $k_i > 0$. For each i there is an element a_i in $\mathfrak{a}$ having $\bar{\psi}_i(x)$ as an initial form. We shall show that $\mathfrak{a} = (a_1, a_2, \cdots, a_s)$.

Let a be an element of $\mathfrak{a}$ and suppose that $a \in \mathfrak{m}^k$. Then $a = \psi(u)$, a form of degree k. Let $\bar{\psi}(x)$ be the corresponding initial form in R (or zero, in case all the coefficients of $\psi(u)$ are in $\mathfrak{m}$). Since $\bar{\psi}(x) \in \mathfrak{a}'$, we have $\bar{\psi}(x) = \sum \bar{A}_i(x)\bar{\psi}_i(x)$, where $\bar{A}_i(x)$ is a form of degree $k - k_i$ (or $\bar{A}_i(x) = 0$). Let $A_i(u)$ be a form of degree $k - k_i$ in $u_1, \cdots, u_n$ corresponding to $\bar{A}_i(x)$; then $a' = \sum_{i=1}^s A_i(u) a_i$ is an element of $\mathfrak{R}$ having $\sum \bar{A}_i(x)\bar{\psi}_i(x) = \bar{\psi}(x)$ as initial form. Hence $a - a' \in \mathfrak{m}^{k+1}$.

[6] The proof of this theorem is implicitly contained in Krull [7, p. 218].

But $a-a'$ is again a member of $\mathfrak{a}$ and so by repeating the previous argument we have an element $a''=\sum A_i'(u)a_i$, where $A_i'(u)$ is a form of degree $k+1-k_i$, and $a-a'-a''\in\mathfrak{m}^{k+2}$. Continuing in this way, we get s sequences $A_i(u), A_i'(u), \cdots, A_i^{(h)}(u), \cdots (i=1, 2, \cdots, s)$, where $A_i^{(h)}(u)$ is a form of degree $k+h-k_i$, and

$$a \equiv \sum_{h=0}^{r}\sum_{i=1}^{s} A_i^{(h)}(u)a_i(\mathfrak{m}^{k+r+1}), \qquad r = 0, 1, \cdots . \tag{4}$$

For each i, $\sum_{h=0}^{\infty}A_i^{(h)}(u)$ is a convergent series, since $\mathfrak{R}$ is complete, and has a sum c_i in $\mathfrak{R}$. Hence the right side of (4) has the element $\sum_{i=1}^{s}c_ia_i$ as limit (as $r\rightarrow\infty$). On the other hand (4) implies that the limit is a. Thus $a=\sum c_ia_i$, and so $(a_1, \cdots, a_s)=\mathfrak{a}$.

For the remainder of this section $\mathfrak{R}$ is a local ring. In this case, we can add to Theorem 2 the following [7, p. 218]: *If* $\mathfrak{a}$ *is any ideal in* $\mathfrak{R}$, *then*

$$\mathfrak{R}^*\cdot\mathfrak{a}\cap\mathfrak{R} = \mathfrak{a}. \tag{5}$$

For if $c\in\mathfrak{R}^*\cdot\mathfrak{a}$, then $c=\sum c_i^*a_i$, $c_i^*\in\mathfrak{R}^*$, $a_i\in\mathfrak{a}$. For a fixed k, there exists a c_i in $\mathfrak{R}$ such that $c_i^*\equiv c_i(\mathfrak{m}^{*k})$; so $c\equiv\sum c_ia_i(\mathfrak{m}^{*k})$. Thus $c-\sum c_ia_i\in\mathfrak{m}^{*k}\cap\mathfrak{R}=\mathfrak{m}^k$, $c\in(\mathfrak{a}, \mathfrak{m}^k)$. Since this holds for all k, (1) implies that $c\in\mathfrak{a}$.

It may be pointed out that (5) is characteristic for local rings in the sense that if it holds for a g.l.r. $\mathfrak{R}$, then $\mathfrak{R}$ is actually a local ring. Namely, equation (5) and Theorem 3 imply that every increasing sequence of ideals of $\mathfrak{R}$ is finite. It follows that (1) is also characteristic for local rings; (1) is equivalent to the statement that the ideal $\mathfrak{a}$ is a closed set. We do not know whether there exists a g.l.r. which is not a local ring.

If $\mathfrak{a}$ is an ideal $(\neq\mathfrak{R})$ in the local ring $\mathfrak{R}$, then the ring $\mathfrak{R}'=\mathfrak{R}/\mathfrak{a}$ is clearly also a local ring with $\mathfrak{m}'=\mathfrak{m}/\mathfrak{a}$ as maximal ideal. The homomorphism of $\mathfrak{R}$ on $\mathfrak{R}'$ is a continuous open mapping. For continuity, observe that the sets $\mathfrak{m}'^k$ form a set of neighborhoods of zero in $\mathfrak{R}'$ and that the inverse images $(\mathfrak{m}^k, \mathfrak{a})$ are open in $\mathfrak{R}$. That the mapping is open follows from the fact that the sets $\mathfrak{m}^k$, which form a system of neighborhoods of zero in $\mathfrak{R}$, map onto the open sets $\mathfrak{m}'^k$ of $\mathfrak{R}'$.

If $\mathfrak{R}$ is complete, then so is $\mathfrak{R}'$. For if $\{a_k'\}$ is a regular sequence in $\mathfrak{R}'$, then $a_k'-a_{k-1}'\rightarrow 0$. Therefore $a_k'-a_{k-1}'\in\mathfrak{m}'^{h(k)}$, with $h(k)\rightarrow\infty$. Let $b_k(k\geqq 1)$ be an element of $\mathfrak{m}^{h(k)}$ which maps onto $a_k'-a_{k-1}'$, let b_0 map onto a_0'. If $a_k=\sum_{i=0}^{k}b_i$, then a_k maps onto a_k' and $\{a_k\}$ is regular, hence has a limit a in $\mathfrak{R}$. If a maps onto a' in $\mathfrak{R}'$, the continuity of the mapping shows that $a_k'\rightarrow a'$.

If $\mathfrak{R}$ is not complete let $\mathfrak{R}^*$ be its completion. In view of (5), $\mathfrak{R}/\mathfrak{a}$ may be considered a subring of $\mathfrak{R}^*/\mathfrak{R}^*\cdot\mathfrak{a}$. Since $(\mathfrak{a}, \mathfrak{m}^k)=(\mathfrak{R}^*\cdot\mathfrak{a}, \mathfrak{m}^{*k})\cap\mathfrak{R}$, $\mathfrak{R}/\mathfrak{a}$ is actually a subspace of $\mathfrak{R}^*/\mathfrak{R}^*\cdot\mathfrak{a}$. Thus the latter is the completion of the former.

Hensel's Lemma for valuation rings can be generalized without difficulty to local rings:

THEOREM 4. *Let* $\mathfrak{R}$ *be a complete local ring. Let* $f(z)$ *be a polynomial in* $\mathfrak{R}[z]$ *of degree* n, *and let* $g_0(z)$ *and* $h_0(z)$ *be polynomials in* $\mathfrak{R}[z]$ *such that*:

(a) $g_0(z)=az^r+a'z^{r-1}+\cdots$, $a\not\equiv 0(\mathfrak{m})$, $h_0(z)$ *of degree not greater than* $n-r$, $0<r<n$;

(b) $f(z)\equiv g_0(z)h_0(z)(\mathfrak{m})$;

(c) $g_0(z)$ *and* $h_0(z)$ *are relatively prime* mod $\mathfrak{m}$.

Then there exist polynomials $g(z)$ *and* $h(z)$ *in* $\mathfrak{R}[z]$ *of degrees* r *and* $n-r$ *respectively such that*

$$g(z) = az^r+\cdots, \qquad f(z)=g(z)h(z), \qquad g(z)\equiv g_0(z)(\mathfrak{m}), \qquad h(z)\equiv h_0(z)(\mathfrak{m}).$$

Proof. Starting with g_0 and h_0 we construct two sequences $\{g_k(z)\}$ and $\{h_k(z)\}$ of polynomials in $\mathfrak{R}[z]$ such that

$$g_k(z) = az^r+\cdots, \quad \text{degree of } h_k(z)\leqq n-r, \tag{6}$$

$$g_{k+1}(z)\equiv g_k(z)(\mathfrak{m}^{k+1}), \qquad h_{k+1}(z)\equiv h_k(z)(\mathfrak{m}^{k+1}), \tag{7}$$

$$f(z)\equiv g_k(z)h_k(z)(\mathfrak{m}^{k+1}). \tag{8}$$

This is sufficient to prove the theorem, for (6) and (7), together with the completeness of $\mathfrak{R}$, imply that the sequences $\{g_k\}$ and $\{h_k\}$ have limits $g(z)$ and $h(z)$ respectively. Then (8) implies that $f(z)=g(z)h(z)$, and the other statements in the theorem are then obvious.

We proceed by induction, assuming that $g_0, g_1, \cdots, g_k$ and $h_0, h_1, \cdots, h_k$ have been defined so that they satisfy (6), (7), and (8). Clearly, for $k=0$, the given g_0 and h_0 will suffice. Let $\mathfrak{m}^{k+1}=(v_1, v_2, \cdots, v_N)$. We now define

$$g_{k+1}(z) = g_k(z)+\sum_{i=1}^{N} v_ir_i(z), \qquad h_{k+1}(z)=h_k(z)+\sum_{i=1}^{N} v_is_i(z), \tag{9}$$

where the $r_i(z)$ and $s_i(z)$ are as yet unspecified polynomials whose degrees are less than r and not greater than $n-r$ respectively. It is clear that (6) and (7) are thereby satisfied. We now determine r_i and s_i so that also (8) is satisfied for g_{k+1} and h_{k+1}.

From (9),

$$f-g_{k+1}h_{k+1} = f-g_kh_k-\sum_i v_i(s_ig_k+r_ih_k)-\sum_{i,j} v_iv_jr_is_j.$$

On the other hand, by (8),

$$f-g_kh_k=\sum_i v_ip_i(z)$$

where the $p_i(z)$ are polynomials whose degrees may be assumed to be at most n, since the same is true of $f-g_kh_k$. These two relations give

$$f - g_{k+1}h_{k+1} \equiv \sum_i v_i(p_i - s_i g_k - r_i h_k)(\mathfrak{m}^{k+2}).$$

In order to obtain (8) for g_{k+1} and h_{k+1} it is sufficient to show that r_i and s_i can be determined so that $p_i \equiv s_i g_k + r_i h_k(\mathfrak{m})$, or equivalently—since $g_k \equiv g_0(\mathfrak{m})$ and $h_k \equiv h_0(\mathfrak{m})$—so that

$$p_i \equiv s_i g_0 + r_i h_0(\mathfrak{m}).$$

But this is surely possible, since g_0 and h_0 are relatively prime mod $\mathfrak{m}$. Moreover, since the degrees of g_0, h_0, and p_i are r, not greater than $n-r$, and n respectively, we may select r_i of degree less than r, and s_i of degree not greater than $n-r$. This completes the proof.

3. **Subrings and extensions of local rings.** Consider two generalized local rings $\mathfrak{R}$ and $\mathfrak{S}$, with $\mathfrak{R}$ a subring of $\mathfrak{S}$. $\mathfrak{R}$ and $\mathfrak{S}$ necessarily have the same identity element, as follows from the following general remark:

A g.l.r. $\mathfrak{S}$ *has no idempotent elements except* 0 *and* 1. For if $e^2 = e$, $e \neq 0$, $e \neq 1$, then $e(1-e) = 0$ and since $e \neq 0$, $1 - e \neq 0$, each is a zero-divisor and is a nonunit. Hence so is $1 = e + (1-e)$, a contradiction.

We shall always let $\mathfrak{m}$ and $\mathfrak{M}$ denote the maximal ideals of $\mathfrak{R}$ and $\mathfrak{S}$ respectively. The contracted ideal $\mathfrak{M} \cap \mathfrak{R}$ is a prime ideal contained in $\mathfrak{m}$. In order to make a comparative study of the two rings and their residue fields, we shall require that these two ideals be the same. That is, we shall be concerned with the condition

$$\mathfrak{M} \cap \mathfrak{R} = \mathfrak{m}. \tag{10}$$

If this condition is satisfied, then there is a natural isomorphism of the residue field $\mathrm{P} = \mathfrak{R}/\mathfrak{m}$ of $\mathfrak{R}$ onto a subfield of the residue field $\Sigma = \mathfrak{S}/\mathfrak{M}$ of $\mathfrak{S}$. We may therefore consider P to be imbedded in Σ.

Since $\mathfrak{R} \subseteq \mathfrak{S}$, there are two topologies which one may consider in $\mathfrak{R}$. First there is the natural topology of $\mathfrak{R}$, and second there is the topology imposed on it by $\mathfrak{S}$. If these two are equivalent—that is, if $\mathfrak{R}$ is not only a subring but also a subspace of $\mathfrak{S}$—then $\mathfrak{R}$ and $\mathfrak{S}$ are said to be *concordant.* Sets of neighborhoods of zero for the two topologies are the ideals $\{\mathfrak{m}^k\}$ $(k = 1, 2, \cdots)$ and $\{\mathfrak{M}^k \cap \mathfrak{R}\}$ $(k = 1, 2, \cdots)$, respectively. In order that $\mathfrak{R}$ and $\mathfrak{S}$ be concordant it is necessary and sufficient that each ideal of either set contain an ideal of the other set. In particular $\mathfrak{M} \cap \mathfrak{R}$ must contain some power of $\mathfrak{m}$, hence must contain $\mathfrak{m}$ itself. This means that (10) holds. And if (10) holds then $\mathfrak{M}^k \cap \mathfrak{R} \supseteq \mathfrak{m}^k$ for every k.

For the concordance of $\mathfrak{R}$ and $\mathfrak{S}$, we must have also that each $\mathfrak{m}^k$ contains an ideal $\mathfrak{M}^i \cap \mathfrak{R}$. For each i, let $k(i)$ be such that

$$\mathfrak{M}^i \cap \mathfrak{R} \subseteq \mathfrak{m}^{k(i)}, \qquad \mathfrak{M}^i \cap \mathfrak{R} \not\subseteq \mathfrak{m}^{k(i)+1}. \tag{11}$$

Clearly the sequence $\{k(i)\}$ is nondecreasing. The requirement that each $\mathfrak{m}^k$ contain an ideal $\mathfrak{M}^i \cap \mathfrak{R}$ is equivalent to

$$\lim_{i\to\infty} k(i) = \infty. \tag{12}$$

(This condition is certainly satisfied if some $k(i)=\infty$—that is, if for some i, $\mathfrak{M}^i \cap \mathfrak{R} = (0)$.) In general (10) does not imply (12). However there are two cases in which it does, as stated by the next two theorems.

THEOREM 5. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be generalized local rings such that $\mathfrak{R} \subseteq \mathfrak{S}$, $\mathfrak{M} \cap \mathfrak{R} = \mathfrak{m}$. If $\mathfrak{R}$ is complete, then $\mathfrak{R}$ and $\mathfrak{S}$ are concordant*[7].

Proof. We prove that (12) holds. If it does not, then the $k(i)$ must be constant from a certain point on, say $k(i)=k$ for $i \geqq h$. Placing $\mathfrak{a}_i = \mathfrak{M}^i \cap \mathfrak{R}$, we have $\mathfrak{a}_i \subseteq \mathfrak{m}^k$, $\mathfrak{a}_i \not\subseteq \mathfrak{m}^{k+1}$ $(i \geqq h)$.

For each fixed integer j $(\geqq 1)$, consider the decreasing chain

$$(\mathfrak{a}_h, \mathfrak{m}^{k+j}) \supseteq (\mathfrak{a}_{h+1}, \mathfrak{m}^{k+j}) \supseteq (\mathfrak{a}_{h+2}, \mathfrak{m}^{k+j}) \supseteq \cdots .$$

These ideals are all primary and belong to $\mathfrak{m}$ and they all contain $\mathfrak{m}^{k+j}$, which is likewise primary. Since $\mathfrak{m}$ has a finite basis, it follows by a well known theorem[8] that these chains terminate. Hence for each j there is an integer $n(j)$ such that $(\mathfrak{a}_i, \mathfrak{m}^{k+j}) = (\mathfrak{a}_{n(j)}, \mathfrak{m}^{k+j})$ for $i \geqq n(j)$; moreover we may assume that $h \leqq n(1) \leqq n(2) \leqq \cdots, k+j \leqq n(j)$.

We now construct a sequence $\{a_j\}$ in $\mathfrak{R}$ such that for all $j \geqq 1$, $a_j \in a_{n(j)}$ and

$$a_j \equiv a_{j+1}(\mathfrak{m}^{k+j}). \tag{13}$$

Let, namely, a_1 be an element in $\mathfrak{a}_{n(1)}$ not in $\mathfrak{m}^{k+1}$. Assume $a_1, a_2, \cdots, a_j$ to be defined. Then $a_j \in \mathfrak{a}_{n(j)} \subseteq (\mathfrak{a}_{n(j+1)}, \mathfrak{m}^{k+j})$, and the existence of an a_{j+1} in $\mathfrak{a}_{n(j+1)}$ satisfying (13) is then clear. The sequence $\{a_j\}$ is regular by (13), and hence it has a limit a in $\mathfrak{R}$. Again by (13) it follows that

$$a \equiv a_j(\mathfrak{m}^{k+j}), \qquad j \geqq 1.$$

Since $\mathfrak{m} \subseteq \mathfrak{M}$, this congruence means that $a - a_j \in \mathfrak{M}^{k+j}$. But $a_j \in \mathfrak{a}_{n(j)} \subseteq \mathfrak{a}_{k+j} \subseteq \mathfrak{M}^{k+j}$; thus $a \in \mathfrak{M}^{k+j}$ for all j, $a=0$. Applying this congruence for $j=1$, we obtain $a_1 \equiv 0(\mathfrak{m}^{k+1})$ contrary to the selection of a_1. This completes the proof.

THEOREM 6. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be generalized local rings, $\mathfrak{R} \subseteq \mathfrak{S}$, $\mathfrak{M} \cap \mathfrak{R} = \mathfrak{m}$. If $\mathfrak{m}$ is a principal ideal, then $\mathfrak{R}$ and $\mathfrak{S}$ are concordant.*

Proof. We must prove (12), where $k(\imath)$ is defined by (11); let $\mathfrak{m}=(u)$. If (12) does not hold, then as in the previous theorem the $k(i)$ are constant from a certain point, say equal to k. Since $\mathfrak{M}^i \cap \mathfrak{R}$ is in $\mathfrak{m}^k$ but not in $\mathfrak{m}^{k+1}$, there is an element a_i in $\mathfrak{M}^i \cap \mathfrak{R}$ such that $a_i = c_i u^k$, with c_i a unit in $\mathfrak{R}$. Hence

[7] Cf. Chevalley [1, Lemma 7].

[8] For this theorem, as well as the concept of the length of a primary ideal and the properties of composition sequences (to be used later), see Krull [4, p. 31].

$u^k=c_i^{-1}a_i\in\mathfrak{M}^i$, all i, so that $u^k=0$. Thus $\mathfrak{m}^k=(0)=\mathfrak{m}^{k+1}$, contradicting the fact that $\mathfrak{M}^i\cap\mathfrak{R}\not\subseteq\mathfrak{m}^{k+1}$.

It is immediate that if $\mathfrak{S}$ contains and is concordant with $\mathfrak{R}$, then the closure of $\mathfrak{R}$ in $\mathfrak{S}$ is a completion of $\mathfrak{R}$.

We now introduce a new relation between two g.l.r.'s stronger than that of concordance; this relation, together with Lemmas 3 and 4, is fundamental in the proof of the structure theorems of Part II.

Definition. Let $\mathfrak{R}$ and $\mathfrak{S}$ be g.l.r.'s, $\mathfrak{R}\subseteq\mathfrak{S}$. Then $\mathfrak{S}$ is said to be *unramified* with respect to $\mathfrak{R}$ if there exists a minimal basis for $\mathfrak{m}$ which is also a minimal basis for $\mathfrak{M}$, and if for every positive integer k it is true that

$$\mathfrak{M}^k\cap\mathfrak{R}=\mathfrak{m}^k. \tag{14}$$

From the definition it follows that

$$\mathfrak{M}=\mathfrak{S}\cdot\mathfrak{m}.$$

Moreover *any* minimal basis for $\mathfrak{m}$ will be a minimal basis for $\mathfrak{M}$ (by Lemma 2). From (14) we see that if $\mathfrak{S}$ is unramified with respect to (u.w.r.t.) $\mathfrak{R}$, then $\mathfrak{S}$ and $\mathfrak{R}$ are concordant. The relation of being unramified is transitive. That is, if $\mathfrak{R}$, $\mathfrak{S}$, and $\mathfrak{S}'$ are three g.l.r.'s such that $\mathfrak{R}\subseteq\mathfrak{S}\subseteq\mathfrak{S}'$, and if $\mathfrak{S}'$ and $\mathfrak{S}$ are u.w.r.t. $\mathfrak{S}$ and $\mathfrak{R}$ respectively, then $\mathfrak{S}'$ is u.w.r.t. $\mathfrak{R}$. Finally, Theorem 2 shows that the completion of $\mathfrak{R}$ is u.w.r.t. $\mathfrak{R}$.

Lemma 3. *Let $\mathfrak{R}$, $\mathfrak{S}$, and $\mathfrak{R}_\alpha$ (where α runs over some index system) be rings satisfying the conditions*:

(a) *For every α, $\mathfrak{R}\subseteq\mathfrak{R}_\alpha\subseteq\mathfrak{S}$, and $\mathfrak{S}$ is the smallest ring containing all $\mathfrak{R}_\alpha$;*

(b) *$\mathfrak{R}$ is a* g.l.r., *and each $\mathfrak{R}_\alpha$ is a* g.l.r. *which is* u.w.r.t. $\mathfrak{R}$;

(c) *Given any two of the rings $\mathfrak{R}_\alpha$, $\mathfrak{R}_\beta$ there exists a ring $\mathfrak{R}_\gamma$ which is* u.w.r.t. *$\mathfrak{R}_\alpha$ and $\mathfrak{R}_\beta$.*

Then $\mathfrak{S}$ is a g.l.r. *which is* u.w.r.t. *$\mathfrak{R}$ and each $\mathfrak{R}_\alpha$; the residue field of $\mathfrak{S}$ is the join of the residue fields of the $\mathfrak{R}_\alpha$.*

Proof. From conditions (a) and (c) it follows that any finite set of elements of $\mathfrak{S}$ is contained in some $\mathfrak{R}_\alpha$.

Let $\mathfrak{m}=\mathfrak{R}\cdot(u_1,\cdots,u_n)$, so that generally $\mathfrak{m}_\alpha=\mathfrak{R}_\alpha\cdot(u_1,\cdots,u_n)$, where $\mathfrak{m}_\alpha$ is the maximal ideal of $\mathfrak{R}_\alpha$. We assert that the ideal $\mathfrak{M}=\mathfrak{S}\cdot(u_1,\cdots,u_n)$ consists of all non-units of $\mathfrak{S}$. First, $\mathfrak{M}\neq\mathfrak{S}$, for otherwise $1=a_1u_1+\cdots+a_nu_n$, $a_i\in\mathfrak{S}$. If $\mathfrak{R}_\alpha$ contains $a_1,\cdots,a_n$, then $1\in\mathfrak{R}_\alpha\cdot(u_1,\cdots,u_n)=\mathfrak{m}_\alpha$, a contradiction. Second, every non-unit a of $\mathfrak{S}$ is in $\mathfrak{M}$; for if a is in $\mathfrak{R}_\alpha$, then a is a non-unit in $\mathfrak{R}_\alpha$, hence $a\in\mathfrak{m}_\alpha\subseteq\mathfrak{M}$. The notation $\mathfrak{M}=\mathfrak{S}\cdot(u_1,\cdots,u_n)$ must be justified by showing that this basis is minimal. But this is clear, for if, for example, $u_1\in\mathfrak{S}\cdot(u_2,\cdots,u_n)$, then $u_1\in\mathfrak{R}_\alpha\cdot(u_2,\cdots,u_n)$ for some $\mathfrak{R}_\alpha$, and this contradicts (b).

Similarly it can be proved that $\mathfrak{M}^k\cap\mathfrak{R}_\alpha=\mathfrak{m}_\alpha{}^k$. For if $a\in\mathfrak{M}^k\cap\mathfrak{R}_\alpha$, then by (c), $a \in \mathfrak{m}_\beta{}^k$ for some β such that $\mathfrak{R}_\beta$ contains and is u.w.r.t. $\mathfrak{R}_\alpha$. Then $a \in \mathfrak{m}_\beta{}^k \cap \mathfrak{R}_\alpha = \mathfrak{m}_\alpha{}^k$, as was asserted. From this it follows that $\bigcap \mathfrak{M}^k = (0)$. Thus $\mathfrak{S}$ is a g.l.r., and it is clearly u.w.r.t. $\mathfrak{R}$ and each $\mathfrak{R}_\alpha$.

It is this lemma which necessitates the introduction of the g.l.r. For the proof given here does not suffice to show that $\mathfrak{S}$ is an actual local ring, even if each $\mathfrak{R}_\alpha$ is.

LEMMA 4. *Let $\mathfrak{R}$ be a local ring, $\mathfrak{S} = \mathfrak{R}[v]$, where v is a root of the polynomial $f(z) = z^m + a_1 z^{m-1} + \cdots + a_m$ $(a_i \in \mathfrak{R})$, but of no polynomial of lower degree. Let, moreover, $\bar{f}(z) = z^m + \bar{a}_1 z^{m-1} + \cdots + \bar{a}_m$ be irreducible over* P. *Then $\mathfrak{S}$ is a local ring, unramified with respect to $\mathfrak{R}$, with $\mathfrak{S} \cdot \mathfrak{m}$ as maximal ideal, and* $[\Sigma : \mathrm{P}] = m$. *If $\mathfrak{a}$ is an ideal in $\mathfrak{R}$, then $\mathfrak{S} \cdot \mathfrak{a} \cap \mathfrak{R} = \mathfrak{a}$. $\mathfrak{S}$ is complete if and only if $\mathfrak{R}$ is.*

(Note: P and Σ are the residue fields of $\mathfrak{R}$ and $\mathfrak{S}$; $\bar{a}_i$ is the residue of a_i modulo $\mathfrak{m}$.)

Proof. In view of $\mathfrak{S} = \mathfrak{R}[v]$ and $f(v) = 0$, every element t in $\mathfrak{S}$ is of the form $t = \sum_{i=0}^{m-1} c_i v^i$, $c_i \in \mathfrak{R}$. Since v satisfies no equation of degree less than m, the c_i are uniquely determined. If $\mathfrak{a}$ is an ideal in $\mathfrak{R}$, then clearly t is in $\mathfrak{S} \cdot \mathfrak{a}$ if and only if the c_i are in $\mathfrak{a}$. Hence if $t \in \mathfrak{S} \cdot \mathfrak{a} \cap \mathfrak{R}$, then $t = c_0 \in \mathfrak{a}$, and we have proved that

$$\mathfrak{S} \cdot \mathfrak{a} \cap \mathfrak{R} = \mathfrak{a}. \tag{15}$$

In particular $\mathfrak{S} \cdot \mathfrak{m} \cap \mathfrak{R} = \mathfrak{m}$, and $\mathfrak{S}_0 = \mathfrak{S} / \mathfrak{S} \cdot \mathfrak{m}$ may be considered to contain $\mathrm{P} = \mathfrak{R}/\mathfrak{m}$. Then $\mathfrak{S}_0 = \mathrm{P}[\bar{v}]$, where $\bar{v}$ is the residue of v mod $\mathfrak{S} \cdot \mathfrak{m}$. Since $\bar{f}(\bar{v}) = 0$ and $\bar{f}$ is irreducible, and since P is a field, it follows that $\mathfrak{S}_0$ is a field, so that $\mathfrak{M} = \mathfrak{S} \cdot \mathfrak{m}$ is a maximal ideal. If $\mathfrak{M}'$ is *any* maximal ideal of $\mathfrak{S}$, then $\mathfrak{M}' \cap \mathfrak{R}$ is maximal([9]) in $\mathfrak{R}$, hence $\mathfrak{M}' \cap \mathfrak{R} = \mathfrak{m}$, $\mathfrak{M}' \supseteq \mathfrak{S} \cdot \mathfrak{m} = \mathfrak{M}$, $\mathfrak{M}' = \mathfrak{M}$. Thus $\mathfrak{M}$ is the only maximal ideal of $\mathfrak{S}$. Since $\mathfrak{S}$ is a simple extension of $\mathfrak{R}$, the ideals of $\mathfrak{S}$ have finite bases and $\mathfrak{S}$ is a local ring.

Now $\mathfrak{M}^k = \mathfrak{S} \cdot \mathfrak{m}^k$, and by (15), $\mathfrak{M}^k \cap \mathfrak{R} = \mathfrak{m}^k$. To complete the proof that $\mathfrak{S}$ is u.w.r.t. $\mathfrak{R}$, we must show that if $\mathfrak{m} = \mathfrak{R} \cdot (u_1, \cdots, u_n)$, then $u_1, \cdots, u_n$ form a minimal basis for $\mathfrak{M}$. If not, then, say, $u_1 \in \mathfrak{S} \cdot (u_2, \cdots, u_n) = \mathfrak{S} \cdot (\mathfrak{R} \cdot (u_2, \cdots, u_n))$, and by (15), $u_1 \in \mathfrak{R} \cdot (u_2, \cdots, u_n)$, a contradiction. The relation $[\Sigma : \mathrm{P}] = m$ is clear.

Suppose now that $\mathfrak{R}$ is complete. Let $\{t_h\}$ be a regular sequence in $\mathfrak{S}$, $t_h = \sum_{i=0}^{m-1} c_{hi} v^i$, $c_{hi} \in \mathfrak{R}$. Then for each k, $t_h - t_{h+1} = \sum (c_{hi} - c_{h+1,i}) v^i$ is in $\mathfrak{M}^k = \mathfrak{S} \cdot \mathfrak{m}^k$ for large h; hence $c_{hi} - c_{h+1,i} \in \mathfrak{m}^k$ for large h, and $\{c_{hi}\}$ is a regular sequence for each i. If c_i is its limit, then $\{t_h\}$ clearly has the limit $\sum c_i v^i$. Thus $\mathfrak{S}$ is complete.

If $\mathfrak{S}$ is complete, let $\{c_h\}$ be a regular sequence in $\mathfrak{R}$. Then $\{c_h\}$ is regu-

[9] *If the ring $\mathfrak{S}$ is integrally dependent on the ring $\mathfrak{R}$, and if $\mathfrak{M}$ is a prime ideal in $\mathfrak{S}$ and $\mathfrak{m}$ is its contraction in $\mathfrak{R}$, then $\mathfrak{M}$ is maximal if and only if $\mathfrak{m}$ is.* For the integral domain $\mathfrak{S}/\mathfrak{M}$ is integrally dependent on the integral domain $\mathfrak{R}/\mathfrak{m}$, and it is easy to see that the former is a field if and only if the latter is. Cf. Cohen and Seidenberg [2, Theorem 1].

lar in $\mathfrak{S}$, hence has a limit $\sum_{i=0}^{m-1} a_i v^i$. Thus for each k and large h, $(a_0 - c_h) + \sum_{i=1}^{m-1} a_i v^i \in \mathfrak{M}^k = \mathfrak{S}\cdot\mathfrak{m}^k$, hence $a_0 - c_h \in \mathfrak{m}^k$. So $\lim c_h = a_0 \in \mathfrak{R}$.

THEOREM 7. *Let $\mathfrak{R}$ be a complete local ring and $\mathfrak{S}$ an integral domain containing $\mathfrak{R}$. If $\mathfrak{S}$ is integrally dependent on $\mathfrak{R}$, then the non-units of $\mathfrak{S}$ form an ideal. If $\mathfrak{S}$ is a finite $\mathfrak{R}$-module, then $\mathfrak{S}$ is a complete local ring.*

Proof. Assume $\mathfrak{S}$ is integral over $\mathfrak{R}$. Then $\mathfrak{S}\cdot\mathfrak{m}$ is not the unit ideal [5, p. 749], and therefore neither is its radical. We show that the radical contains all non-units.

Let v be a non-unit in $\mathfrak{S}$. Since v is integral over $\mathfrak{R}$ it satisfies an equation $f(v)=0$, where $f(z)=z^m+a_1z^{m-1}+\cdots+a_m$, $a_i\in\mathfrak{R}$. We assume v satisfies no monic equation of lower degree. Since $a_m = -v(v^{m-1}+\cdots+a_{m-1})$, and v is a non-unit, a_m is also a non-unit in $\mathfrak{R}$, hence $a_m \in \mathfrak{m}$. Now all a_i are in $\mathfrak{m}$. For if not, let a_r be the last one not in $\mathfrak{m}$: $a_r \notin \mathfrak{m}$, $a_i \in \mathfrak{m}$ for $i=r+1, r+2, \cdots, m$, $0<r<m$. Then $f(z) \equiv z^{m-r}(z^r+a_1z^{r-1}+\cdots+a_r)(\mathfrak{m})$, and these factors are relatively prime mod $\mathfrak{m}$ since $a_r \not\equiv 0(\mathfrak{m})$. Hensel's Lemma (Theorem 4) implies that $f(z)$ factors into monic polynomials of degrees r and $m-r$. But this would imply that v satisfies a monic equation of degree less than m. This is false and so each $a_i \in \mathfrak{m}$, $v^m \in \mathfrak{S}\cdot\mathfrak{m}$, v is in the radical of $\mathfrak{S}\cdot\mathfrak{m}$.

If $\mathfrak{S}$ is a finite $\mathfrak{R}$-module, then the ideals of $\mathfrak{S}$ have finite bases, since the same is true of $\mathfrak{R}$. Also $\mathfrak{S}$ is integral over $\mathfrak{R}$, so $\mathfrak{S}$ has an ideal of non-units. The completeness of $\mathfrak{S}$ is shown in the next theorem (first paragraph of the proof).

THEOREM 8. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be local rings with residue fields* P *and* Σ *such that $\mathfrak{R}\subseteq\mathfrak{S}$ and $\mathfrak{R}$ is complete. Then $\mathfrak{S}$ is a finite $\mathfrak{R}$-module if and only if $\mathfrak{S}\cdot\mathfrak{m}$ is a primary ideal belonging to $\mathfrak{M}$ and Σ is a finite algebraic extension of* P. *With these conditions satisfied, $\mathfrak{S}$ is complete and has an $\mathfrak{R}$-basis of $\lambda\mu$ elements, where $\mu = [\Sigma : \mathrm{P}]$ and λ is the length*[8] *of $\mathfrak{S}\cdot\mathfrak{m}$.*

Note. If $\mathfrak{S}\cdot\mathfrak{m}$ is primary for $\mathfrak{M}$, then $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$, so P may be considered a subfield of Σ, and therefore the hypothesis concerning Σ and P has meaning. If, on the other hand, $\mathfrak{S}$ is a finite $\mathfrak{R}$-module, then $\mathfrak{S}$ is integrally dependent on $\mathfrak{R}$. Hence any prime ideal belonging to $\mathfrak{S}\cdot\mathfrak{m}$ is maximal[9] since such an ideal must contract to $\mathfrak{m}$. Thus $\mathfrak{M}$ is the only prime ideal of $\mathfrak{S}\cdot\mathfrak{m}$, which is therefore primary, and so again the statement concerning Σ and P is meaningful.

Proof. If $\mathfrak{S}$ is finite over $\mathfrak{R}$ then clearly Σ is finite over P. Moreover, as observed, $\mathfrak{S}\cdot\mathfrak{m}$ is primary for $\mathfrak{M}$. Hence for some k, $\mathfrak{M}^k\subseteq\mathfrak{S}\cdot\mathfrak{m}$, $\mathfrak{M}^{rk}\subseteq\mathfrak{S}\cdot\mathfrak{m}^r$ for all r. Let $v_1, \cdots, v_m$ form an $\mathfrak{R}$-basis for $\mathfrak{S}$. To prove the completeness of $\mathfrak{S}$, let $\{t_h\}$ be a regular sequence in $\mathfrak{S}$, $t_0=0$. Then for any r, $t_h - t_{h-1} \in \mathfrak{M}^{rk}\subseteq\mathfrak{S}\cdot\mathfrak{m}^r$ for large h. Thus $t_h - t_{h-1} = \sum_{i=1}^m c_{hi}v_i$, where $c_{hi}\in\mathfrak{m}^{n(h)}$, and $n(h)\to\infty$. For each i, $\sum_{h=1}^{\infty} c_{hi}$ converges in $\mathfrak{R}$ (which is complete) to a limit c_i. Then

$$t_j = \sum_{h=1}^{j} (t_h - t_{h-1}) = \sum_{i=1}^{m} v_i \sum_{h=1}^{j} c_{hi}, \qquad \lim_{j\to\infty} t_j = \sum_{i=1}^{m} c_i v_i.$$

(From Theorem 5 it follows that $\mathfrak{S}$ is concordant with $\mathfrak{R}$. However, we have used not this fact, but merely the observation that the identity mapping of $\mathfrak{R}$ in $\mathfrak{S}$ is continuous.)

Now let us assume that $\mathfrak{S}\cdot\mathfrak{m}$ is a primary ideal of length λ belonging to $\mathfrak{M}$. Then, as observed above, $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$ and P may be considered a subfield of Σ. We assume further that $\mu=[\Sigma:\mathrm{P}]$ is finite and prove that $\mathfrak{S}$ has an $\mathfrak{R}$-basis of $\lambda\mu$ elements.

Let $\{\pi_1, \pi_2, \cdots, \pi_\mu\}$ form a field basis for Σ over P, and let p_i be a representative of π_i in $\mathfrak{S}$. Then $p_1, p_2, \cdots, p_\mu$ form an independent $\mathfrak{R}$-basis for $\mathfrak{S}$ mod $\mathfrak{M}$. That is, for every element t in $\mathfrak{S}$, there are elements $a_1, a_2, \cdots, a_\mu$ in $\mathfrak{R}$ such that

$$t \equiv a_1p_1 + a_2p_2 + \cdots + a_\mu p_\mu(\mathfrak{M}), \tag{16}$$

and the a_i are uniquely determined mod $\mathfrak{m}$.

Since $\mathfrak{S}\cdot\mathfrak{m}$ is of length λ, there exists a chain

$$\mathfrak{M} = \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_\lambda = \mathfrak{S}\cdot\mathfrak{m},$$

where each $\mathfrak{q}_j$ is a primary ideal belonging to $\mathfrak{M}$, and there is no ideal between $\mathfrak{q}_{j-1}$ and $\mathfrak{q}_j$. It is well known that

$$\mathfrak{M}\cdot\mathfrak{q}_{j-1} \subseteq \mathfrak{q}_j, \qquad i = 1, 2, \cdots, \lambda,$$

where we define $\mathfrak{q}_0=\mathfrak{S}$. If q_j is in $\mathfrak{q}_{j-1}$ but not in $\mathfrak{q}_j$, then

$$\mathfrak{q}_{j-1} = (q_j, \mathfrak{q}_j), \qquad j = 1, 2, \cdots, \lambda. \tag{17}$$

(We observe for later purposes that we could have selected $p_1=q_1=1$.) We now show that the elements p_iq_j form an $\mathfrak{R}$-basis for $\mathfrak{S}$.

First we show that they form an $\mathfrak{R}$-basis mod $\mathfrak{S}\cdot\mathfrak{m}$. For this purpose it is sufficient to show that the elements $p_1q_j, \cdots, p_\mu q_j$ form an $\mathfrak{R}$-basis for $\mathfrak{q}_{j-1}$ mod $\mathfrak{q}_j$. If, now, $s\in\mathfrak{q}_{j-1}$, then by (17) $s\equiv tq_j(\mathfrak{q}_j)$, $t\in\mathfrak{S}$. By (16), $s\equiv\sum_{i=1}^{\mu}a_ip_iq_j$ $(\mathfrak{M}\cdot\mathfrak{q}_{j-1})\equiv 0(\mathfrak{q}_j)$. Thus for every s in $\mathfrak{S}$ there are elements a_{ij} in $\mathfrak{R}$ such that $s\equiv\sum a_{ij}(p_iq_j)$ $(\mathfrak{S}\cdot\mathfrak{m})$.

There exist, for each s in $\mathfrak{S}$, $\lambda\mu$ sequences $\{a_{ij}^{(0)}, a_{ij}^{(1)}, \cdots, a_{ij}^{(k)}, \cdots\}$ $(a_{ij}^{(k)}\in\mathfrak{R})$ such that for all k, $a_{ij}^{(k)}\equiv a_{ij}^{(k+1)}$ $(\mathfrak{m}^{k+1})$, and

$$s \equiv \sum_{i,j} a_{ij}^{(k)}(p_iq_j)(\mathfrak{S}\cdot\mathfrak{m}^{k+1}). \tag{18}$$

For $k=0$, the $a_{ij}^{(k)}$ have been shown to exist. If $a_{ij}^{(k)}$ has been defined, (18) implies that $s=\sum a_{ij}^{(k)}(p_iq_j)+\sum s_hw_h$, where $s_h\in\mathfrak{S}$, $w_h\in\mathfrak{m}^{k+1}$. But

$$s_h \equiv \sum_{i,j} b_{hij}(p_iq_j)(\mathfrak{S}\cdot\mathfrak{m}), \qquad b_{hij} \in \mathfrak{R},$$

$$s \equiv \sum_{i,j} a_{ij}^{(k)}(p_iq_j) + \sum_{i,j}\left(\sum_h b_{hij}w_h\right)(p_iq_j)(\mathfrak{S}\cdot\mathfrak{m}^{k+2}).$$

Placing $a_{ij}^{(k+1)} = a_{ij}^{(k)} + \sum_h b_{hij}w_h$, we see that the induction is complete. For each i and j, $\{a_{ij}^{(k)}\}$ is a regular sequence, hence has a limit a_{ij} in $\mathfrak{R}$. We conclude from (18) that $s = \sum a_{ij}(p_iq_j)$, and the p_iq_j thus form an $\mathfrak{R}$-basis for $\mathfrak{S}$.

Recalling that we could have selected $p_1 = q_1 = 1$, we obtain the following for the case $\lambda = \mu = 1$.

COROLLARY. *Let $\mathfrak{R}$ be a complete local ring, $\mathfrak{S}$ a local ring containing $\mathfrak{R}$ such that $\mathfrak{S}\cdot\mathfrak{m} = \mathfrak{M}$. If the residue fields of $\mathfrak{R}$ and $\mathfrak{S}$ coincide, then $\mathfrak{S} = \mathfrak{R}$.*

We shall see in Part III that the members p_iq_j of the $\mathfrak{R}$-basis need not be independent over $\mathfrak{R}$ and we shall obtain a sufficient condition (Theorem 23) for independence.

PART II

4. **The structure theorems. Characteristic zero.** A decisive factor in the statement as well as the proof of the structure theorems for local rings is the relative value of the characteristics of the ring and its residue field. The characteristic of the latter is naturally either zero or a prime number p. The characteristic of the local ring $\mathfrak{R}$ itself, however, may well be a positive integer q which is not a prime, since $\mathfrak{R}$ may have zero-divisors. However q must be a power of a prime. For if $q = rs$, $r > 1$, $s > 1$, $(r, s) = 1$, then since $rs = 0$, r and s are zero-divisors and are contained in the maximal ideal $\mathfrak{m}$ of $\mathfrak{R}$. Since there exist integers a and b such that $1 = ar + bs$, we have $1 \in \mathfrak{m}$, which is impossible. Thus $q = p^k$, where p is a prime. In this case the residue field P has characteristic p.

Thus the following are seen to be the only cases possible:

(a) $\mathfrak{R}$ and P are both of characteristic zero.

(b) $\mathfrak{R}$ and P are both of characteristic p.

(c) $\mathfrak{R}$ is of characteristic zero, P of characteristic p.

(d) $\mathfrak{R}$ is of characteristic $p^k (k > 1)$, P of characteristic p.

The first two cases are called the *equal-characteristic* cases; the other two, the *unequal-characteristic* cases. Case (d) can arise only if $\mathfrak{R}$ has zero-divisors.

If $\mathfrak{S}$ is a local ring containing $\mathfrak{R}$, then $\mathfrak{R}$ and $\mathfrak{S}$ have the same characteristic (since they have the same identity). If $\mathfrak{M} \cap \mathfrak{R} = \mathfrak{m}$, then the residue fields also have the same characteristic, and $\mathfrak{R}$ and $\mathfrak{S}$ fall into the same one of the four cases. In particular, $\mathfrak{R}$ and its completion are under the same case.

To see that all four cases are actually possible, we first prove a general result.

LEMMA 5. *Let $\mathfrak{R}$ be a complete[10] local ring with $\mathfrak{m} = \mathfrak{R}\cdot(u_1, u_2, \cdots, u_n)$;*

[10] If $\mathfrak{R}$ is not complete, then $\mathfrak{S}$ will still be a (non-complete) local ring. The proof is similar to that of Theorem 3.

let $\mathfrak{S}=\mathfrak{R}\{x_1, x_2, \cdots, x_m\}$ *be the ring of formal power series in m indeterminates* $x_1, x_2, \cdots, x_m$ *with coefficients in* $\mathfrak{R}$. *Then* $\mathfrak{S}$ *is a complete local ring with maximal ideal* $(u_1, \cdots, u_n, x_1, \cdots, x_m)$, *and residue field isomorphic to that of* $\mathfrak{R}$.

Proof. Let $\mathfrak{M}$ denote this ideal. If $t\in\mathfrak{S}$, then $t=\sum_{k=0}^{\infty}t_k$, where t_k is a form of degree k in $x_1, \cdots, x_m$ with coefficients in $\mathfrak{R}$. It is clear that $t\in\mathfrak{S}\cdot(x_1, \cdots, x_m)$ is equivalent to $t_0=0$ and that $t\in\mathfrak{M}$ is equivalent to $t_0\in\mathfrak{m}$. But this last condition is clearly the condition that t be a non-unit in $\mathfrak{S}$. Thus $\mathfrak{M}$ consists of all non-units of $\mathfrak{S}$. That $\bigcap_{h=1}^{\infty}\mathfrak{M}^h=(0)$ follows from the fact that $\mathfrak{M}^h$ consists of all $t=\sum t_k$ such that for $k=0, 1, \cdots, h-1$ the coefficients of t_k are in $\mathfrak{m}^{h-k}$. Hence $\mathfrak{S}$ is a generalized local ring. Moreover the above basis for $\mathfrak{M}$ is minimal. If, namely, x_1 is superfluous, then $x_1=\sum_{i=1}^{n}p_iu_i+\sum_{j=2}^{m}q_jx_j$, where p_i, $q_j\in\mathfrak{S}$. On expanding the right-hand side into a power series in $x_1, \cdots, x_m$, we see that the second summation yields no term in x_1 alone; and while the first summation may yield such a term, its coefficient must be in $\mathfrak{m}$. Thus the equation is impossible. If, on the other hand, u_1 is superfluous, then $u_1=\sum_{i=2}^{n}p_iu_i+\sum_{j=1}^{m}q_jx_j$, where p_i, $q_j\in\mathfrak{S}$. If p_i' is the constant term of p_i, then $u_1=\sum_{i=2}^{n}p_i'u_i$, and this contradicts the minimality of the basis $(u_1, \cdots, u_n)$ for $\mathfrak{m}$. It is clear that $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$ and that the residue field of $\mathfrak{S}$ coincides with that of $\mathfrak{R}$.

Now $\mathfrak{S}$ is complete (and hence, by Theorem 3, a local ring). For let $\{t^i\}$ $(i=0, 1, \cdots)$ be a regular sequence of elements of $\mathfrak{S}$. We write $t^i=\sum_k t_k{}^i$, where $t_k{}^i$ is a form in $x_1, \cdots, x_m$ of degree k. For any h, we have that $t^i-t^{i+1}\in\mathfrak{M}^h$ for large i. By the remark above, this means that for a fixed k and for any $h>k$, we have $t_k{}^i-t_k{}^{i+1}\equiv 0(\mathfrak{m}^{h-k})$ when i is large (this congruence means that the coefficients of $t_k{}^i-t_k{}^{i+1}$ are in $\mathfrak{m}^{h-k}$). Hence for a fixed k, the coefficients of each monomial in $t_k{}^i$ form a regular sequence, which must then have a limit in $\mathfrak{R}$. Hence there is a form t_k of degree k such that $\lim_{i\to\infty}t_k{}^i=t_k$. Now $\lim_{i\to\infty}t^i=t$, where $t=\sum t_k$. For $t^i-t=\sum(t_k{}^i-t_k)$, and for any h, $t_k{}^i-t_k\equiv 0(\mathfrak{m}^h)$, if $0\leqq k\leqq h-1$ and i is large enough. Hence $t^i-t\in\mathfrak{M}^h$ for i sufficiently large, and the statement is proved.

Any field P may be considered a local ring in which $\mathfrak{m}=(0)$. Consequently the lemma implies that the formal power series ring $\mathrm{P}\{x_1, \cdots, x_n\}$ is a local ring with residue field isomorphic to P. Thus cases (a) and (b) above are possible, and moreover the number of elements in a minimal basis of the ideal of non-units, as well as the residue field, may be prescribed.

For case (c) let $\mathfrak{R}_0$ be the quotient ring[11] of the ring of integers with respect to the ideal (p), where p is a prime number, and let $\mathfrak{R}$ be the completion[12] of $\mathfrak{R}_0$. Then $\mathfrak{R}$ falls under case (c), and so does $\mathfrak{S}=\mathfrak{R}\{x_1, \cdots, x_m\}$, which has $(p, x_1, \cdots, x_m)$ as its maximal ideal. The residue fields of $\mathfrak{R}_0$, $\mathfrak{R}$, and $\mathfrak{S}$ are the prime field of characteristic p, while these local rings are of

[11] For the definition and properties of quotient rings see Krull [4, p. 17].

[12] This is the ring of p-adic integers.

characteristic zero. More generally, in order to obtain an arbitrary residue field of characteristic p, we start with a ring $\mathfrak{R}_0$ which is a discrete unramified valuation ring of characteristic zero with prescribed residue field[13].

Finally, the residue class ring mod $p^k (k > 1)$ of a ring in class (c) gives a ring in class (d).

The structure theorems say in effect that every complete local ring is the homomorphic image of one of the rings which have just been explicitly described. The proofs require a detailed analysis.

Let $\mathfrak{R}$ be any local ring. If F is a field contained in $\mathfrak{R}$, then in the homomorphism of $\mathfrak{R}$ on its residue field P, F will map isomorphically on a subfield Φ of P. Thus $\mathfrak{R}$ and P have the same characteristic. Conversely, if $\mathfrak{R}$ and P have the same characteristic, then $\mathfrak{R}$ contains a field. For let F_0 be the subring of $\mathfrak{R}$ consisting of all integral multiples of the identity. If $\mathfrak{R}$ has characteristic p, then F_0 is already a field. If $\mathfrak{R}$ has characteristic zero, then so has P; F_0 is isomorphic to the ring of integers and each of its elements is a unit. Thus $\mathfrak{R}$ contains the quotient field of F_0.

Definition. If the local ring $\mathfrak{R}$ contains a field F which maps modulo $\mathfrak{m}$ onto the entire residue field P, then F is said to be a *coefficient field* in $\mathfrak{R}$.

If $\mathfrak{R}$ is the ring of power series with coefficients in a field P, then the subfield P of $\mathfrak{R}$ is clearly a coefficient field in the sense just defined. But there may well be other coefficient fields in $\mathfrak{R}$, and there may be fields in $\mathfrak{R}$ which although having a "natural" (in some sense) connection with $\mathfrak{R}$, cannot be extended to a coefficient field. Examples will be given later.

Now let $\mathfrak{R}$ be an arbitrary local ring. Naturally $\mathfrak{R}$ contains a coefficient field only if $\mathfrak{R}$ and P have the same characteristic. The converse is not true: Let P_0 be the rational field, x an indeterminate over P_0, $\mathfrak{R}$ the quotient ring of $\mathrm{P}_0[x]$ with respect to the prime ideal (x^2+1). Then $\mathrm{P}=\mathrm{P}_0(i)$, $i^2=-1$, and $\mathfrak{R}$ surely contains no field isomorphic to P. However, for complete rings, we have:

Theorem 9. *If $\mathfrak{R}$ is a complete local ring which has the same characteristic as its residue field* P, *then $\mathfrak{R}$ contains a coefficient field. If the maximal ideal $\mathfrak{m}$ of $\mathfrak{R}$ has a minimal basis of n elements, then $\mathfrak{R}$ is a homomorphic image of a formal power series ring* $\mathrm{P}\{x_1, \cdots, x_n\}$ *in n indeterminates.*

The second statement of the theorem follows easily from the first. Namely, let F be a coefficient field in $\mathfrak{R}$, and let $\mathfrak{m}=\mathfrak{R}\cdot(u_1, \cdots, u_n)$. If $c\in\mathfrak{R}$, then $c\equiv a(\mathfrak{m})$ for some $a\in F$. We assert that there is a sequence $\{c_k\}$ such that $c\equiv c_k(\mathfrak{m}^{k+1})$, $c_k\in F[u_1, \cdots, u_n]$. Namely take $c_0=a$, and if c_k has been defined, then let $c-c_k=\sum b_iv_i$, where $b_i\in\mathfrak{R}$, v_i is a power product of $u_1, \cdots, u_n$ of degree $k+1$. There exists an a_i in F such that $b_i\equiv a_i(\mathfrak{m})$, $c-c_k\equiv\sum a_iv_i(\mathfrak{m}^{k+2})$; take $c_{k+1}=c_k+\sum a_iv_i$. Thus $c=\lim c_k$, and $\mathfrak{R}$ is the closure of $F[u_1, \cdots, u_n]$. There is a unique homomorphism T of $\mathrm{P}[x_1, \cdots, x_n]$ (where $x_1, \cdots, x_n$

[13] This is discussed in §6.

are indeterminates over P) on $F[u_1, \cdots, u_n]$ such that $x_iT=u_i$ and T, acting on P, is the inverse of the natural mapping of F on P; T is clearly continuous, where the topology of $P[x_1, \cdots, x_n]$ is that imposed by $P\{x_1, \cdots, x_n\}$. Since $\mathfrak{R}$ is complete and is the closure of $F[u_1, \cdots, u_n]$, and since $P\{x_1, \cdots, x_n\}$ is the closure of $P[x_1, \cdots, x_n]$, T can obviously be uniquely extended to a homomorphism of $P\{x_1, \cdots, x_n\}$ on $\mathfrak{R}$.

The proof of the first statement is more difficult. Any coefficient field in $\mathfrak{R}$ must be a maximal subfield of $\mathfrak{R}$—that is, must not be contained in any other subfield of $\mathfrak{R}$. Hence we look for such subfields.

Let F_0 be any field contained in $\mathfrak{R}$. There exists such a field since $\mathfrak{R}$ and P have the same characteristic. If $\{F_\tau\}$ is the set of all subfields of $\mathfrak{R}$ which contain F_0, then by Zorn's Lemma, this set has a maximal element F; F is a maximal subfield of $\mathfrak{R}$ and contains F_0. Let Φ be the subfield of P on which F maps.

Then P *is algebraic over* Φ[14]. Suppose not, and let α be an element of P transcendental over Φ. Let a be an element of $\mathfrak{R}$ such that $\bar{a}=\alpha$. (The bar will be consistently used to denote residues modulo $\mathfrak{m}$.) Then $\mathfrak{m}\cap F[a]=(0)$. For if $\sum c_ia^i\in\mathfrak{m}(c_i\in F)$, then $\sum \bar{c}_i\alpha^i=0$; since $\bar{c}_i\in\Phi$, and α is transcendental over Φ, $\bar{c}_i=0$. Since the mapping of F on Φ is an isomorphism, $c_i=0$, $\sum c_ia^i=0$. Thus every nonzero element of $F[a]$ is a unit in $\mathfrak{R}$, and $\mathfrak{R}$ therefore contains the quotient field $F(a)$. But since $a\notin F$, this contradicts the maximal character of F. Thus the statement is proved.

Every element of P *which is not in* Φ *is inseparable over* Φ. For let α be in P and separable over Φ. Suppose $\phi(\alpha)=0$, where $\phi(z)=z^m+\gamma_1z^{m-1}+\cdots+\gamma_m$ is an irreducible polynomial in $\Phi[z]$. Let $f(z)=z^m+c_1z^{m-1}+\cdots+c_m$, where $c_i\in F$, $\bar{c}_i=\gamma_i$; $f(z)$ is irreducible over F. Now since $\phi(\alpha)=0$, we have $\phi(z)=(z-\alpha)\pi(z)$, where $\pi(z)\in P[z]$, and $z-\alpha$ and $\pi(z)$ are relatively prime since α is separable. Let $p(z)$ be a polynomial in $\mathfrak{R}[z]$ of degree not greater than $m-1$ which maps mod $\mathfrak{m}$ onto $\pi(z)$, and let a in $\mathfrak{R}$ be such that $\bar{a}=\alpha$. Then $f(z)\equiv(z-a)p(z)(\mathfrak{m})$, and $z-a$ and $p(z)$ are relatively prime mod $\mathfrak{m}$. By Hensel's Lemma (Theorem 4), there exist polynomials $z-a_1$ and $p_1(z)$ in $\mathfrak{R}[z]$ such that $f(z)=(z-a_1)p_1(z)$. Since $f(z)$ is irreducible over F and $f(a_1)=0$, $F[a_1]$ is a field containing F. Since F is maximal, $a_1\in F$, f is linear, ϕ is linear, $\alpha\in\Phi$.

Thus either $P=\Phi$ or P is purely inseparable over Φ. *If* P (*hence also* $\mathfrak{R}$) *is of characteristic zero, Theorem* 9 *is therefore proved.* It should be observed that in this case (of characteristic zero) there is considerable latitude in general in the choice of F. In fact, unless P is absolutely algebraic, there are infinitely many possibilities. Namely, let a be an element of F which is transcendental over the prime subfield E of F. Then every nonzero element of $E[a+cu_1]$, $c\in E$, is a unit in $\mathfrak{R}$, so that $\mathfrak{R}$ contains the field $E(a+cu_1)$ and hence also a maximal field F_c containing this one. The infinitely many fields

[14] The completeness of $\mathfrak{R}$ is not used in the proof of this statement.

F_c are all distinct, yet each is a coefficient field in $\mathfrak{R}$. If on the other hand P is absolutely algebraic, then F is uniquely determined in $\mathfrak{R}$.

The failure of this proof for characteristic p is not merely a defect of the method but lies in the nature of things. It will be seen in the next section that a maximal subfield of $\mathfrak{R}$ need not be a coefficient field.

5. **Characteristic p.** In this section $\mathfrak{R}$ is a complete local ring of arbitrary characteristic, while P is assumed to be of characteristic p; thus $p\in\mathfrak{m}$. The multiplicative representatives, defined below, will be used also in the next section.

We make certain conventions as to notation. When used as an exponent the number p^k (k an integer) will be denoted by $p(k)$. We continue to use the bar to denote the residue of an element modulo $\mathfrak{m}$, but occasionally brackets will be used; thus $\bar{a}$ and $[a]$ both denote the residue modulo $\mathfrak{m}$ of an element a in $\mathfrak{R}$.

Lemma 6. *If a, $b\in\mathfrak{R}$, and $a\equiv b(\mathfrak{m}^h)$, $h>0$, then $a^{p(k)}\equiv b^{p(k)}(\mathfrak{m}^{h+k})$, $k=1, 2, \cdots$.*

For $a=b+c$, $c\in\mathfrak{m}^h$, $a^p=b^p+pb^{p-1}c+\cdots+c^p\equiv b^p(\mathfrak{m}^{h+1})$, and the lemma follows by induction [12, p. 144, Lemma 8].

Definition. If $\alpha\in\mathrm{P}$, a *multiplicative representative* of α is an element a in $\mathfrak{R}$ such that $\bar{a}=\alpha$ and a has a p^kth root in $\mathfrak{R}$ for every positive integer k [12, p. 143].

This name is justified in Lemma 8.

Lemma 7. *The element α in P has a multiplicative representative if and only if α is a p^kth power in P for every positive integer k. The multiplicative representative of α is unique. If Φ is a subfield of P which is algebraically perfect, then every element of Φ has a multiplicative representative; if F is a perfect subfield of $\mathfrak{R}$, then every element of F is the multiplicative representative of its residue.*

Proof. Suppose a in $\mathfrak{R}$ is a multiplicative representative of α. Then $a=a_k^{p(k)}$, $a_k\in\mathfrak{R}$, and $\alpha=\bar{a}_k^{p(k)}$ is a p^kth power in P. If also b is a multiplicative representative of α, then $b=b_k^{p(k)}$, $\bar{b}_k^{p(k)}=\alpha=\bar{a}_k^{p(k)}$, $\bar{b}_k=\bar{a}_k$, $b_k\equiv a_k(\mathfrak{m})$, hence by Lemma 6, $b_k^{p(k)}\equiv a_k^{p(k)}(\mathfrak{m}^{k+1})$, $b\equiv a(\mathfrak{m}^{k+1})$, all k, hence $b=a$.

Suppose $\alpha^{p(-k)}$ is in P for every $k>0$; let a_k in $\mathfrak{R}$ be an element having this as residue. Then $\bar{a}_{k+1}=\alpha^{p(-k-1)}$, $[a_{k+1}{}^p]=[a_{k+1}]^p=\alpha^{p(-k)}=\bar{a}_k$, so $a_{k+1}{}^p\equiv a_k(\mathfrak{m})$. Hence for any h ($\geqq 0$) and any $k>h$, $a_{k+1}{}^{p(k+1-h)}\equiv a_k{}^{p(k-h)}(\mathfrak{m}^{k+1-h})$. Hence for fixed h, $\{a_k{}^{p(k-h)}\}$ is regular in the complete local ring $\mathfrak{R}$, hence has a limit b_h in $\mathfrak{R}$. Clearly $b_0=b_h{}^{p(h)}$ for all h, and $\bar{b}_0=\alpha$, so b_0 is the multiplicative representative of α.

The rest of the lemma follows directly from the definition of a perfect field.

Lemma 8. *If α and β in P have the respective multiplicative representatives a*

and b, then $\alpha\beta$ has the multiplicative representative ab. If $\mathfrak{R}$ is of characteristic p, then $\alpha+\beta$ has the multiplicative representative $a+b$.

For by hypothesis, $a=a_k{}^{p(k)}$, $b=b_k{}^{p(k)}$, where $\bar{a}=\alpha$, $\bar{b}=\beta$. Hence $ab=(a_kb_k)^{p(k)}$, and $[ab]=\alpha\beta$. If $\mathfrak{R}$ is of characteristic p, then $a+b=(a_k+b_k)^{p(k)}$, and $[a+b]=\alpha+\beta$.

If $\mathfrak{R}$ and P are both of characteristic p and if P is algebraically perfect, then Theorem 9 *is proved.* For every element of P has a multiplicative representative in $\mathfrak{R}$, and by Lemma 8 the set of all these is a field, which is then necessarily a coefficient field.

This field is the only coefficient field in $\mathfrak{R}$. For if F is any such field, then F is isomorphic to P, hence is perfect. By Lemma 7, every element of F is a multiplicative representative, and so F consists of all these.

We see here precisely the opposite of the situation for characteristic zero: if $\mathfrak{R}$ and P are of characteristic p, and P is perfect, then the "imbedding" of P in $\mathfrak{R}$ is unique. If P is not absolutely algebraic, then we can as above find fields F_c in $\mathfrak{R}$ not contained in F. Thus F_c is not contained in any coefficient field in $\mathfrak{R}$, and this shows why the method for characteristic zero fails in this case.,

The case where P is imperfect will now be considered. Recalling that $p(k)$ denotes p^k, we define: If A is a subset of P, then $A^{p(k)}$ consists of all $\alpha^{p(k)}$, $\alpha\in A$. It is well known that $\mathrm{P}^{p(k)}$ and $\mathrm{P}^{p(-k)}$ are fields isomorphic to P, that the intersection $\mathrm{P}^{p(\infty)}$ of all the fields $\mathrm{P}^{p(k)}$ $(k>0)$ is the largest perfect field contained in P, and that the union $\mathrm{P}^{p(-\infty)}$ of all the fields $\mathrm{P}^{p(-k)}$ $(k>0)$ is the smallest perfect field containing P.

Definition. A *p-basis*[15] of P is a set Γ of elements γ_τ in P such that:

(a) $[P^p(\gamma_1, \cdots, \gamma_r):\mathrm{P}^p]=p^r$ for any r distinct elements of Γ;

(b) $\mathrm{P}=\mathrm{P}^p(\Gamma)$.

If P is perfect, only the void set is a p-basis. But if P is imperfect, then there exist non-void sets satisfying (a); any maximal such set (which must exist, by Zorn's Lemma) satisfies also (b). Thus a p-basis always exists.

Lemma 9. *If Γ is a p-basis for* P, *then $\mathrm{P}=\mathrm{P}^{p(k)}(\Gamma)$ for every $k>0$; $\Gamma^{p(-k)}$ is a p-basis for $\mathrm{P}^{p(-k)}$.*

For $\mathrm{P}=\mathrm{P}^p(\Gamma)$, $\mathrm{P}^p=\mathrm{P}^{p(2)}(\Gamma^p)$, $\mathrm{P}=\mathrm{P}^{p(2)}(\Gamma^p, \Gamma)=\mathrm{P}^{p(2)}(\Gamma)$; now use induction. For the second statement observe that $\alpha\rightarrow\alpha^{p(-k)}$ is an isomorphism of P on $\mathrm{P}^{p(-k)}$.

Lemma 10. *Let $\mathfrak{R}$ be an arbitrary commutative ring with an identity, $\mathfrak{R}'=\mathfrak{R}[\cdots, z_\tau, \cdots]$ a polynomial ring over $\mathfrak{R}$ in a set $\{z_\tau\}$ of independent indeterminates; let $f_\tau(z_\tau)$ be a monic polynomial over $\mathfrak{R}$ in z_τ of degree $k_\tau>0$. If a polynomial $g(\{z_\tau\})$ in $\mathfrak{R}'$ of degree less than k_τ in z_τ is contained in the ideal in $\mathfrak{R}'$ generated by the $f_\tau(z_\tau)$, then $g=0$.*

[15] This definition, as well as Lemma 9, is due to Teichmüller [12, Lemmas 9 and 10].

Proof. Without loss of generality, we may assume that the z_τ are finite in number, $\mathfrak{R}'=\mathfrak{R}[z_1, \cdots, z_n]$, and we proceed by induction, observing that the lemma is trivial if $n=1$. We assume it proved for $n-1$ variables. Suppose, then, that $g\in(f_1, \cdots, f_n)$, $g=\sum_{i=1}^n h_i(z_1, \cdots, z_n)f_i(z_i)$. Since $f_n(z_n)$ is monic of degree k_n, we may assume each h_i to be of degree less than k_n in z_n $(1\leqq i\leqq n-1)$. Since g is of degree less than k_n in z_n, it follows that $h_n(z_1, \cdots, z_n)=0$. Now write $g=\sum g_jx_n{}^j$, $h_i=\sum h_{ij}x_n{}^j$, where g_j, $h_{ij}\in\mathfrak{R}[z_1, \cdots, z_{n-1}]$. Then $\sum_j g_jx_n{}^j=\sum_j x_n{}^j\sum_{i=1}^{n-1}h_{ij}f_i$, $g_j=\sum h_{ij}f_i$. By induction assumption $g_j=0$, hence $g=0$.

As stated at the beginning of this section $\mathfrak{R}$ is assumed complete and of arbitrary characteristic, P is of characteristic p. Moreover we assume that P is imperfect, for otherwise the statements which follow are vacuously true. The symbols P, Σ, $\mathrm{P}^{(1)}$, P_k, $\cdots$ will always denote the residue fields of the respective generalized local rings $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{R}^{(1)}$, $\mathfrak{R}_k$, $\cdots$.

LEMMA 11. *Let $\mathfrak{R}$ be a complete local ring such that* P *is imperfect, and let* $\Gamma=\{\gamma_\tau\}$ *be a p-basis for* P; *let c_τ in $\mathfrak{R}$ be such that $\bar{c}_\tau=\gamma_\tau$. Then $\mathfrak{R}$ can be extended to a complete local ring $\mathfrak{R}_1$, unramified with respect to $\mathfrak{R}$, with residue field* $\mathrm{P}^{p(-1)}$, *and containing a pth root of every c_τ.*

Proof. Let $\mathfrak{R}'=\mathfrak{R}[\{z_\tau\}]$, where the z_τ are independent indeterminates over $\mathfrak{R}$ in 1-1 correspondence with the c_τ. Let $\mathfrak{R}''$ be the residue class ring of $\mathfrak{R}'$ with respect to the ideal generated by all the polynomials $z_\tau{}^p-c_\tau$. Lemma 10 implies that $\mathfrak{R}''$ contains a subring isomorphic to $\mathfrak{R}$ and we identify this subring with $\mathfrak{R}$. If a_τ is the residue class of z_τ, then $\mathfrak{R}''=\mathfrak{R}[\{a_\tau\}]$, $a_\tau{}^p=c_\tau$.

If $\{a_1, \cdots, a_n\}$ is any finite set of the a_τ, then $\mathfrak{R}^{(n)}=\mathfrak{R}[a_1, \cdots, a_n]$ is a local ring u.w.r.t. $\mathfrak{R}$ and with residue field $\mathrm{P}^{(n)}=\mathrm{P}(\gamma_1{}^{p(-1)}, \cdots, \gamma_n{}^{p(-1)})$. This is trivial for $n=0$, and we assume it proved for $n-1$. Then $\mathfrak{R}^{(n)}=\mathfrak{R}^{(n-1)}[a_n]$, and we apply Lemma 4 of Part I. The element a_n is a root of z^p-c_n, but (by Lemma 10) of no equation of lower degree. Moreover $z^p-\bar{c}_n=z^p-\gamma_n$ is irreducible over $\mathrm{P}^{(n-1)}$, for otherwise $\gamma_n{}^{p(-1)}\in\mathrm{P}^{(n-1)}=\mathrm{P}(\gamma_1{}^{p(-1)}, \cdots, \gamma_{n-1}{}^{p(-1)})$, $\gamma_n\in\mathrm{P}(\gamma_1, \cdots, \gamma_{n-1})$, $[\mathrm{P}^p(\gamma_1, \cdots, \gamma_n):\mathrm{P}^p]\leqq p^{n-1}$, contradicting condition (a) in the definition of a p-basis. Lemma 4 now implies that $\mathfrak{R}^{(n)}$ is a local ring u.w.r.t. $\mathfrak{R}^{(n-1)}$, and $\mathrm{P}^{(n)}=\mathrm{P}^{(n-1)}[\bar{a}_n]=\mathrm{P}^{(n-1)}[\gamma_n{}^{p(-1)}]=\mathrm{P}(\gamma_1{}^{p(-1)}, \cdots, \gamma_n{}^{p(-1)})$. Since $\mathfrak{R}^{(n-1)}$ is u.w.r.t. $\mathfrak{R}$, so is $\mathfrak{R}^{(n)}$, by the transitivity of this relation.

Thus every ring $\mathfrak{R}[a_{\tau_1}, \cdots, a_{\tau_n}]$ is a local ring u.w.r.t. $\mathfrak{R}$ and with residue field $\mathrm{P}(\gamma_{\tau_1}{}^{p(-1)}, \cdots, \gamma_{\tau_n}{}^{p(-1)})$; here $\{a_{\tau_1}, \cdots, a_{\tau_n}\}$ is any finite subset of $\{a_\tau\}$. It is also clear that such a ring is u.w.r.t. $\mathfrak{R}[a_{\tau_1}, \cdots, a_{\tau_m}]$ if $m<n$. We now apply Lemma 3 with these rings as the $\mathfrak{R}_\alpha$ and with $\mathfrak{R}''$ as $\mathfrak{S}$. Thus $\mathfrak{R}''$ is a generalized local ring, u.w.r.t. $\mathfrak{R}$ and having residue field $\mathrm{P}''=\mathrm{P}(\Gamma^{p(-1)})=\mathrm{P}^{p(-1)}$. If $\mathfrak{R}_1$ is the completion of $\mathfrak{R}''$, then the lemma is proved, in view of Theorems 2 and 3.

LEMMA 12. *Under the hypothesis of Lemma* 11, *$\mathfrak{R}$ can be extended to a com-*

plete local ring $\mathfrak{S}$, u.w.r.t. $\mathfrak{R}$, *with residue field* $\Sigma=\mathrm{P}^{p(-\infty)}$; *moreover* c_τ *will be the multiplicative representative in* $\mathfrak{S}$ *of* γ_τ.

Proof. The ring $\mathfrak{R}_1$ of Lemma 11 satisfies the same conditions as $\mathfrak{R}$; a p-basis for P_1 is $\Gamma^{p(-1)}=\{\gamma_\tau^{p(-1)}\}$; the element[16] $a_\tau=c_\tau^{p(-1)}$ maps into $\gamma_\tau^{p(-1)}$. The application of Lemma 11 to $\mathfrak{R}_1$ yields a complete local ring $\mathfrak{R}_2$, u.w.r.t. $\mathfrak{R}_1$ (and hence u.w.r.t. $\mathfrak{R}$ also), $\mathrm{P}_2=\mathrm{P}_1^{p(-1)}=\mathrm{P}^{p(-2)}$, and $\mathfrak{R}_2$ contains a pth root[16] $c_\tau^{p(-2)}$ of $c_\tau^{p(-1)}$. Continuing in this way, a sequence $\mathfrak{R}\subset\mathfrak{R}_1\subset\mathfrak{R}_2\subset\cdots\subset\mathfrak{R}_k\subset\cdots$ is obtained in which $\mathfrak{R}_k$ is a complete local ring u.w.r.t. all preceding $\mathfrak{R}_i$ and $\mathfrak{R}$, $\mathrm{P}_k=\mathrm{P}^{p(-k)}$, $\mathfrak{R}_k$ contains $c_\tau^{p(-k)}$, whose residue is $\gamma_\tau^{p(-k)}$. If $\mathfrak{S}_0$ is the union of all the $\mathfrak{R}_k$, then by Lemma 3, $\mathfrak{S}_0$ is a generalized local ring, u.w.r.t. $\mathfrak{R}$. If $\mathfrak{S}$ is the completion of $\mathfrak{S}_0$, then by Theorems 2 and 3, $\mathfrak{S}$ is a local ring which is u.w.r.t. $\mathfrak{R}$. Moreover, the residue field $\Sigma=\Sigma_0=\bigcup_k\mathrm{P}_k=\mathrm{P}^{p(-\infty)}$. Clearly $\mathfrak{S}$ contains $c_\tau^{p(-k)}$ for all k, and so c_τ is the multiplicative representative of γ_τ.

For the applications of Lemma 12 it is necessary to observe that we have actually proved it in the following more precise form:

Let B be a homomorphism of $\mathfrak{R}$ modulo $\mathfrak{m}$ on a field P, and let Σ be the minimal perfect extension of P. Then $\mathfrak{R}$ can be extended to a complete local ring $\mathfrak{S}$, u.w.r.t. $\mathfrak{R}$, and B can be extended to a homomorphism of $\mathfrak{S}$ (modulo $\mathfrak{M}$) on Σ.

We can now complete the proof of Theorem 9; we consider namely, the case where $\mathfrak{R}$ and P are both of characteristic p, and P is imperfect.

Since the complete local ring $\mathfrak{S}$ of Lemma 12 has a perfect residue field Σ, the set S of all multiplicative representatives in $\mathfrak{S}$ of elements of Σ is a coefficient field in $\mathfrak{S}$. Let R be the subfield of S which corresponds to P. *Then Theorem* 9 *is proved if it can be shown that* $R\subseteq\mathfrak{R}$. Hence suppose $a\in R$; then for a fixed k, $\bar{a}\in\mathrm{P}=\mathrm{P}^{p(k)}(\Gamma)$ (Lemma 9), and $\bar{a}^{p(-k)}\in\mathrm{P}(\Gamma^{p(-k)})$. Hence there is an a_k in $\mathfrak{R}[\{c_\tau^{p(-k)}\}]$ such that $\bar{a}_k=\bar{a}^{p(-k)}$. Thus $\bar{a}_k=[a^{p(-k)}]$, $a_k\equiv a^{p(-k)}(\mathfrak{M})$, $a_k^{p(k)}\equiv a(\mathfrak{M}^{p(k)})$. Thus $a=\lim a_k^{p(k)}$; since $a_k^{p(k)}\in\mathfrak{R}^{p(k)}[\{c_\tau\}]\subseteq\mathfrak{R}$, and since $\mathfrak{R}$ is complete, hence closed in $\mathfrak{S}$, it follows that $a\in\mathfrak{R}$, as was to be proved.

The demonstration of Theorem 9 is now complete in all cases. A more complete statement can be made as follows:

THEOREM 10. *Let R be the coefficient field referred to in Theorem* 9. *Then*:

(a) *If* P *is of characteristic zero, R may be chosen as any maximal subfield of* $\mathfrak{R}$; *it is unique if* P *is absolutely algebraic, and may be selected in infinitely many ways otherwise.*

(b) *If* P *is of characteristic p and is perfect, then R is unique and consists of*

[16] Since $\mathfrak{R}$ need not be of characteristic p, pth roots need not be unique and it may seem that the notation $c_\tau^{p(-k)}$ is ambiguous. However the method of construction of $\mathfrak{R}_k$ selects one of the p^kth roots of c_τ so that it is, in fact, a pth root of $c_\tau^{p(-k+1)}$.

the multiplicative representatives of the elements of P; *R contains every perfect subfield of* $\mathfrak{R}$.

(c) *If* P *is of characteristic p and is imperfect, then R may be chosen in infinitely many ways; it must contain every perfect subfield of* $\mathfrak{R}$; *but a maximal subfield of* $\mathfrak{R}$ *need not be a coefficient field even though it contains the largest perfect subfield of* $\mathfrak{R}$.

Proof. Parts (a) and (b) have been proved. We consider the case where P is imperfect. Let R be any coefficient field in $\mathfrak{R}$ and F any perfect subfield of $\mathfrak{R}$. If F maps onto the subfield Φ of P, let F' be the subfield of R corresponding to Φ. By Lemma 7, F and F' consist of the multiplicative representatives of the residues of their elements, and these residues are in both cases the elements of Φ; hence $F=F'\subseteq R$. The maximal perfect subfield of $\mathfrak{R}$ is thus the same as the maximal perfect subfield of R, namely $R^{p(\infty)}$, which is therefore independent of the particular coefficient field chosen.

The particular coefficient field R constructed in the proof of Theorem 9 is such that (by Lemma 12) it must contain every c_τ. But in the choice of c_τ there was considerable arbitrariness since it was required only that $\bar{c}_\tau=\gamma_\tau$ (Lemma 11). Let d_τ be another element of $\mathfrak{R}$ having the residue γ_τ; then there is a coefficient field R' containing d_τ. Naturally $R\neq R'$ since $c_\tau-d_\tau$ is a nonunit. Obviously this method will yield infinitely many distinct coefficient fields.

Let F be the maximal perfect subfield of $\mathfrak{R}$. For a fixed τ, let $d=c_\tau{}^p+u_1$ (u_1 is an element in a minimal basis of $\mathfrak{m}$). Since $\bar{d}=\gamma_\tau{}^p$, which is transcendental over $P^{p(\infty)}$, $F[d]\cap\mathfrak{m}=(0)$, so that $\mathfrak{R}$ contains the quotient field $F(d)$ and hence contains also a maximal field R' containing $F(d)$. We assert that R' is not a coefficient field. For if it were, then, being isomorphic to P, it would contain an element a such that $a^p=d$. So $\bar{a}=\gamma_\tau$, $a\equiv c_\tau(\mathfrak{m})$, $d=a^p\equiv c_\tau{}^p(\mathfrak{m}^p)$, $u_1\in\mathfrak{m}^p$, which is false. The last statement is thereby proved.

This last statement may be illustrated by an example, which shows also that even a "natural" subfield of $\mathfrak{R}$ need not be extendable to a coefficient field. Let Δ be an imperfect field, a an element of Δ having no pth root in Δ. In the polynomial ring $\Delta[z]$ the ideal (z^p-a) is prime; form the quotient ring of $\Delta[z]$ with respect to (z^p-a) and let $\mathfrak{R}$ be the completion of this quotient ring. Then $\mathrm{P}=\Delta(a^{p(-1)})$, and since $a\not\equiv z^p(\mathfrak{m}^p)$, it follows easily, as in the above proof, that a is not contained in a coefficient field in $\mathfrak{R}$. Hence Δ is not contained in any such field, although Δ would seem to have an intrinsic connection with $\mathfrak{R}$.

COROLLARY. *Let* $\mathfrak{R}$ *and* $\mathfrak{S}$ *be two complete local rings such that* $\mathfrak{R}\subseteq\mathfrak{S}$ *and* $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$; *let R and S be respective coefficient fields in* $\mathfrak{R}$ *and* $\mathfrak{S}$. *If* P *is perfect, then R and S may be selected so that $R\subseteq S$. If* P *is imperfect, then R and S cannot always be so selected.*

Proof. Since $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$, we have $\mathrm{P}\subseteq\Sigma$. If P is of characteristic zero, let R

be any coefficient field in $\mathfrak{R}$; then R is contained in some maximal subfield S of $\mathfrak{S}$. If P is of characteristic p and perfect, then so is the (uniquely determined) coefficient field R in $\mathfrak{R}$, and R is contained in any coefficient field in $\mathfrak{S}$, by (b) and (c).

To show the truth of the last statement, consider the example preceding the corollary. Let Δ' be the smallest perfect extension of Δ, and let $a=\alpha^p$, $\alpha\in\Delta'$. Let $\mathfrak{R}_0$ and $\mathfrak{S}_0$ be the quotient rings of $\Delta[z]$ and $\Delta'[z]$ with respect to (z^p-a) and $(z-\alpha)$ respectively. Then $\mathfrak{R}_0\subset\mathfrak{S}_0$ and $\mathfrak{S}_0$ is concordant with $\mathfrak{R}_0$, hence $R\subset S$, where $\mathfrak{R}$ and $\mathfrak{S}$ are the completions. Now Σ is isomorphic to Δ', which is perfect, and hence Δ' is the only coefficient field in $\mathfrak{S}$, by (b). But Δ' can contain no coefficient field R of $\mathfrak{R}$, for if it did, then $a\in R$, which we have seen to be impossible.

6. **The unequal-characteristic case.** Throughout this section $\mathfrak{R}$ will always be a complete local ring whose residue field P has characteristic p. The characteristic of $\mathfrak{R}$ may be either zero or a power of p. If it is p itself then we have Case (b) of §4, and Theorem 11 will imply a proof of Theorem 9 for Case (b). The proof given in the previous section, however, was far simpler than that of Theorem 11. In any case there is little duplication since the lemmas of the previous section are needed in the present one.

The essential feature here will be the imbedding in $\mathfrak{R}$ of a "coefficient ring" by analogy with the imbedding of the residue field in the equal characteristic case. This ring will be obtained from a *complete, discrete, unramified valuation ring of characteristic zero with residue field of characteristic* p. Such rings (referred to hereafter simply as *v-rings*) may be characterized as *complete local rings which are of characteristic zero and have no zero-divisors and in which the maximal ideal is generated by an ordinary prime number* p. For if $\mathfrak{V}$ is a local ring of this description, then every a in $\mathfrak{V}$ is of the form ep^k where e is a unit, $k\geqq 0$. Defining $v(a)=k$ we have a discrete valuation of $\mathfrak{V}$ in which $\mathfrak{V}$ is complete; if v is extended to the quotient field of $\mathfrak{V}$, then $\mathfrak{V}$ is the valuation ring. Since $v(p)=1$ it follows that the residue field is of characteristic p and that $\mathfrak{V}$ is unramified; thus $\mathfrak{V}$ is a v-ring. Conversely, it is obvious that a v-ring is always a local ring of this type.

We shall make use of the following lemma:

LEMMA 13. *If* P *is an arbitrary field of characteristic* p, *then there exists a v-ring* $\mathfrak{V}$ *with a residue field isomorphic to* P.

This fundamental existence theorem is due to Hasse and Schmidt [3, Theorem 20, p. 63]. A particularly simple proof was given by MacLane [9, Theorem 2].

The imbedding theorem can now be proved:

THEOREM 11. *Let* $\mathfrak{R}$ *be a complete local ring with residue field* P *of characteristic* p. *Then* $\mathfrak{R}$ *is concordant with a certain subring which is the homomorphic map of a v-ring and which has* P *as residue field.*

Proof. To begin with, suppose there is given a v-ring $\mathfrak{V}$ and a homomorphism T of $\mathfrak{V}$ on a subring R of $\mathfrak{R}$. Then R is a complete local ring whose maximal ideal is generated by the element p (that is, by the p-fold of the identity of $\mathfrak{R}$). If $\mathfrak{R}$ has characteristic zero, then T is an isomorphism; if it has characteristic p, then R is isomorphic to the residue field of $\mathfrak{V}$; if the characteristic is p^k $(k>1)$, then $(R\cdot p)^k=(0)$, so that the topology of R is discrete—and hence the completeness trivial. In any case the maximal ideal $R\cdot p$ of R is contained in $\mathfrak{m}$ (the maximal ideal of $\mathfrak{R}$), so that

$$\mathfrak{m}\cap R = R\cdot p.$$

It follows from Theorem 6 that $\mathfrak{R}$ is concordant with R. Thus if a subring R of $\mathfrak{R}$ is the map of a v-ring, then it is necessarily concordant with $\mathfrak{R}$. The residue field of R may then be considered a subfield of P, and the theorem states that R can be so selected that this residue field is P itself.

We now proceed to the construction and assume first that P is perfect.

According to Lemma 13, there exists a v-ring $\mathfrak{V}$ with residue field $\cong$P; thus there is a homomorphism A of $\mathfrak{V}$ on P with kernel $\mathfrak{V}\cdot p$. The ring $\mathfrak{V}$ contains the ring $\mathfrak{J}$ of ordinary integers and we can map $\mathfrak{J}$ by a homomorphism T on the ring I generated in $\mathfrak{R}$ by the identity. If B denotes the natural mapping of $\mathfrak{R}$ on P, then both A and TB map $\mathfrak{J}$ on the prime subfield P_0 of P. Since a prime field has no automorphisms, A and TB must be equal on $\mathfrak{J}$. The quotient ring[11] of $\mathfrak{J}$ with respect to the prime ideal $\mathfrak{J}\cdot p$ is a local ring which is concordant with $\mathfrak{V}$ (by Theorem 6) and its closure in $\mathfrak{V}$ is clearly a v-ring $\mathfrak{V}_0$ which is concordant with $\mathfrak{V}$. (In fact $\mathfrak{V}$ is unramified with respect to $\mathfrak{V}_0$.) Similarly the quotient ring of I with respect to $I\cdot p$ is concordant with $\mathfrak{R}$ and so is its closure R_0. Now it is clearly possible to extend T to a mapping of the one quotient ring on the other, and thence by continuity to a mapping of $\mathfrak{V}_0$ on R_0; this last extension is possible because R_0 is complete.

We thus have a v-ring $\mathfrak{V}_0$ in $\mathfrak{V}$ and a mapping T of $\mathfrak{V}_0$ on a subring R_0 of $\mathfrak{R}$; the mappings A and TB coincide on $\mathfrak{V}_0$ and map it onto the prime subfield P_0 of P.

Let $\mathrm{H}=\{\eta_\tau\}$ be a transcendence basis for P over P_0—that is, a set of elements of P which are algebraically independent over P_0 and such that P is algebraic over $\mathrm{P}_0(\mathrm{H})$. Since P is perfect it contains all roots $\eta_\tau{}^{p(-k)}$ and hence also the subfield $\mathrm{P}_1=\mathrm{P}_0(\mathrm{H}^{p(-\infty)})$ generated by these roots. The subfield P_1 is perfect and so P is separable over P_1.

It follows from Lemma 7 that since P is perfect each η_τ has a multiplicative representative v_τ in $\mathfrak{V}$ and a multiplicative representative y_τ in $\mathfrak{R}$. Moreover each $\eta_\tau{}^{p(-k)}$ has a multiplicative representative v in $\mathfrak{V}$, and by Lemma 8, $v^{p(k)}=v_\tau$, so that we may denote the multiplicative representative of $\eta_\tau{}^{p(-k)}$ in $\mathfrak{V}$ by $v_\tau{}^{p(-k)}$. Similarly the representative of $\eta_\tau{}^{p(-k)}$ in $\mathfrak{R}$ is denoted by $y_\tau{}^{p(-k)}$. Let $Y=\{y_\tau\}$, $V=\{v_\tau\}$.

Now the elements v_τ are algebraically independent over $\mathfrak{V}_0$. For if $f(V)=0$, where f is a polynomial with coefficients in $\mathfrak{B}_0$, then we may assume (since $\mathfrak{B}$ has no zero-divisors) that at least one coefficient is not divisible by p, hence is a unit. Mapping this relation by A into P, we would get an algebraic relation among the η_τ over P_0. Thus the v_τ are independent. Hence the mapping T can be extended to a homomorphism of $\mathfrak{B}_0[V]$ on $R_0[Y]$ such that $v_\tau T=y_\tau$. We assert that

$$(19) \qquad \mathfrak{m} \cap R_0[Y] = R_0[Y]\cdot p, \qquad \mathfrak{B}\cdot p \cap \mathfrak{B}_0[V] = \mathfrak{B}_0[V]\cdot p.$$

For if $g(Y)\in\mathfrak{m}$, where g is a polynomial with coefficients in R_0, then all coefficients must be divisible by p; namely, if they are not then mapping by B into P gives an algebraic relation among the η_τ. Similarly for the other relation.

In the same way we proceed with the elements of $\mathrm{H}^{p(-1)}=\{\eta_\tau{}^{p(-1)}\}$. They also form a transcendence basis for P over P_0. Hence as above we may extend T to a mapping of $\mathfrak{B}_0[V^{p(-1)}]$ on $R_0[Y^{p(-1)}]$ such that $v_\tau{}^{p(-1)}T=y_\tau{}^{p(-1)}$. It is clear that these two extensions of T agree on $\mathfrak{B}_0[V]$. Continuing in this way we extend T to a mapping of $\mathfrak{B}'$ on R', where $\mathfrak{B}'$ is the union of the rings $\mathfrak{B}_0[V^{p(-k)}]$ for all k, and similarly for R'. From (19) and analogous relations for $R_0[Y^{p(-k)}]$ and $\mathfrak{B}_0[V^{p(-k)}]$, we conclude that

$$\mathfrak{m} \cap R' = R'\cdot p, \qquad \mathfrak{B}\cdot p \cap \mathfrak{B}' = \mathfrak{B}'\cdot p,$$

so that $\mathfrak{R}$ and $\mathfrak{B}$ contain the quotient rings R'' and $\mathfrak{B}''$ of R' and $\mathfrak{B}'$ with respect to $R'\cdot p$ and $\mathfrak{B}'\cdot p$ respectively. In the mapping T of $\mathfrak{B}'$ on R' the ideals $\mathfrak{B}'\cdot p$ and $R'\cdot p$ correspond, and therefore T can be extended to a mapping of $\mathfrak{B}''$ on R''. Now $\mathfrak{B}''$ and R'' are local rings concordant with $\mathfrak{B}$ and $\mathfrak{R}$ respectively. If $\mathfrak{B}_1$ and R_1 denote their closures in $\mathfrak{B}$ and $\mathfrak{R}$, then $\mathfrak{B}_1$ is a v-ring, R_1 is complete, and so, finally, T can be extended by continuity to a mapping of $\mathfrak{B}_1$ on R_1.

At this point we have: $\mathfrak{B}_1$ is a v-ring in $\mathfrak{B}$, and T is a homomorphism of $\mathfrak{B}_1$ into $\mathfrak{R}$; the mappings A and TB of $\mathfrak{B}_1$ on P_1 coincide. (This last statement follows from the method of construction of T.)

Consider now the set E of all pairs $(\mathfrak{B}_\sigma, T_\sigma)$, where $\mathfrak{B}_\sigma$ is a v-ring such that $\mathfrak{B}_1\subseteq\mathfrak{B}_\sigma\subseteq\mathfrak{B}$, and T_σ is a homomorphism of $\mathfrak{B}_\sigma$ into $\mathfrak{R}$ such that $T_\sigma=T$ on $\mathfrak{B}_1$ and $A=T_\sigma B$ on $\mathfrak{B}_\sigma$. Let $(\mathfrak{B}_\sigma, T_\sigma)\prec(\mathfrak{B}_\rho, T_\rho)$ be defined to mean that $\mathfrak{B}_\sigma\subseteq\mathfrak{B}_\rho$, and that T_ρ is an extension of T_σ; thus E is a partially ordered set. We wish to apply Zorn's Lemma to this set and must verify that every simply ordered subset E' of E has an upper bound in E. Consider all those $\mathfrak{B}_\rho$ such that $(\mathfrak{B}_\rho, T_\rho)\in E'$. (Note that if also $(\mathfrak{B}_\sigma, T_\sigma)\in E'$, and $\mathfrak{B}_\rho=\mathfrak{B}_\sigma$, then $T_\rho=T_\sigma$, since E' is simply ordered.) Then $\{\mathfrak{B}_\rho\}$ is a set which is simply ordered by inclusion, and each $\mathfrak{B}_\rho$ is certainly unramified with respect to each $\mathfrak{B}_\sigma$ in this set which precedes it; we may assume that $(\mathfrak{B}_1, T)\in E'$. By Lemma 3 (§3), it follows that the union $\mathfrak{B}^*$ of all these $\mathfrak{B}_\rho$ is a generalized local ring (it is, in fact, a local ring, but not complete in general) with maximal ideal

$\mathfrak{B}^*\cdot p$. Evidently $\mathfrak{B}$ is unramified with respect to $\mathfrak{B}^*$, and therefore the closure $\mathfrak{B}_\tau$ of $\mathfrak{B}^*$ in $\mathfrak{B}$ is the completion of $\mathfrak{B}^*$; hence $\mathfrak{B}_\tau$ is a v-ring. If $\mathfrak{B}_\rho \subset \mathfrak{B}_\sigma$, then T_σ is an extension of T_ρ, so that there is a mapping T^* of $\mathfrak{B}^*$ into $\mathfrak{R}$ such that T^* is an extension of each T_ρ, and $A = T^*B$ on $\mathfrak{B}^*$. Finally T^* can be extended to a mapping T_τ of $\mathfrak{B}_\tau$ by continuity, since $\mathfrak{R}$ is complete, and $A = T_\tau B$ on $\mathfrak{B}_\tau$. Thus $(\mathfrak{B}_\tau, T_\tau)$ is an upper bound of E' in E.

Zorn's Lemma implies the existence of a maximal pair $(\mathfrak{B}_\omega, T_\omega)$ in E. *We assert that* $\mathfrak{B}_\omega = \mathfrak{B}$. For suppose that $\mathfrak{B}_\omega \subset \mathfrak{B}$ properly. It follows from the corollary to Theorem 8 that $\mathrm{P}_\omega \subset \mathrm{P}$ properly, where $\mathrm{P}_\omega = \mathfrak{B}_\omega A$. Since $\mathfrak{B}_1 \subseteq \mathfrak{B}_\omega$, $\mathrm{P}_1 \subseteq \mathrm{P}_\omega$ and P is separably algebraic over P_ω.

Let α be in P but not in P_ω, let $\phi(z)$ be the irreducible monic polynomial over P_ω of which α is a root. Let $f(z)$ be a monic polynomial over $\mathfrak{B}_\omega$ of the same degree as $\phi(z)$, and whose coefficients map into those of $\phi(z)$. Let $g(z)$ be the polynomial over $\mathfrak{R}$ which corresponds to $f(z)$ under T_ω; then $g(z)$ maps under B onto $\phi(z)$, since $A = T_\omega B$. By Hensel's Lemma (Theorem 4) there is an element a in $\mathfrak{B}$ such that $f(a) = 0$ and an element c in $\mathfrak{R}$ such that $g(c) = 0$, and $aA = cB = \alpha$. (The details are as in the proof of Theorem 9.) Then T_ω can be extended to a mapping T_ω' of $\mathfrak{B}_\omega' = \mathfrak{B}_\omega[a]$ into $\mathfrak{R}$ such that $aT_\omega' = c$. By Lemma 4, $\mathfrak{B}_\omega'$ is again a v-ring, and clearly $A = T_\omega' B$. Hence $(\mathfrak{B}_\omega', T_\omega')$ is in the set E and properly follows $(\mathfrak{B}_\omega, T_\omega)$. Since this pair was maximal, there is a contradiction, and $\mathfrak{B}_\omega = \mathfrak{B}$.

Thus $\mathfrak{B}$ is mapped homomorphically in $\mathfrak{R}$, and the proof is complete for the case that P is perfect.

It will be observed that the proof we have given yields also the following, at least for perfect residue fields:

COROLLARY 1. *Let* $\mathfrak{R}$ *be a complete local ring,* B *the natural mapping of* $\mathfrak{R}$ *on its residue field* P, *assumed to be of characteristic* p. *Let* $\mathfrak{B}$ *be a v-ring and* A *a homomorphism of* $\mathfrak{B}$ *on* P *with kernel* $\mathfrak{B}\cdot p$. *Then there is a homomorphism* T *of* $\mathfrak{B}$ *in* $\mathfrak{R}$ *such that* $A = TB$.

We now turn to the case where P *is not perfect.* We wish to include a proof of the corollary as well. Hence let $\mathfrak{B}$ be any v-ring satisfying the hypothesis of the corollary. That at least one such ring exists is implied by Lemma 13. If the required mapping can be found then also the theorem will be proved.

Let $\Gamma = \{\gamma_\tau\}$ be a p-basis of P; let c_τ in $\mathfrak{R}$ and w_τ in $\mathfrak{B}$ be such that $c_\tau B = w_\tau A = \gamma_\tau$. By Lemma 12, $\mathfrak{R}$ is contained in a complete local ring $\mathfrak{S}$ with residue field Σ equal to the smallest perfect field containing P, and c_τ is the multiplicative representative in $\mathfrak{S}$ of γ_τ. Moreover B is extended to a mapping of $\mathfrak{S}$ on Σ. Similarly, $\mathfrak{B}$ can be extended to a complete local ring $\mathfrak{W}$ u.w.r.t. $\mathfrak{B}$, and A can be extended to a mapping of $\mathfrak{W}$ on Σ with kernel $\mathfrak{W}\cdot p$; w_τ will be the multiplicative representative of γ_τ in $\mathfrak{W}$. It is immediate that $\mathfrak{W}$ is a v-ring.

Since the residue field Σ is perfect, it follows from the corollary that there is a homomorphism T of $\mathfrak{W}$ into $\mathfrak{S}$ such that $A = TB$ on $\mathfrak{W}$. Necessarily

$w_\tau T = c_\tau$ since w_τ and c_τ are both multiplicative representatives of γ_τ. Namely, $w_\tau A = \gamma_\tau$, hence $(w_\tau T)B = \gamma_\tau$, and $w_\tau T = (w_\tau^{p(-k)}T)^{p(k)}$ is a p^kth power in $\mathfrak{S}$; thus the multiplicative representative of γ_τ in $\mathfrak{S}$ is $w_\tau T$. Hence this must equal c_τ.

If it can now be proved that T maps the subring $\mathfrak{B}$ into $\mathfrak{R}$, then the proof is complete. So let v be an arbitrary element of $\mathfrak{B}$; we shall show that vT is in $\mathfrak{R}$. Since $\mathfrak{R}$ is complete, hence closed in $\mathfrak{S}$, it is sufficient to find a sequence of elements a_k in $\mathfrak{R}$ such that $vT \equiv a_k(\mathfrak{M}^k)$ $(k=1, 2, \cdots)$, where $\mathfrak{M}$ is the maximal ideal of $\mathfrak{S}$.

Since $v \in \mathfrak{B}$, we have $vA \in \mathrm{P}$, $vTB \in \mathrm{P}$; since $\mathfrak{R}B = \mathrm{P}$, there is an a_1 in $\mathfrak{R}$ such that $a_1 \equiv vT(\mathfrak{M})$. We now proceed by induction to define a_{k+1}. Since $vA \in \mathrm{P} = \mathrm{P}^{p(k)}(\Gamma)$ (Lemma 9), $vA = \phi(\Gamma)$, where ϕ is a polynomial with coefficients $\beta^{p(k)}$, $\beta \in \mathrm{P}$. Replacing each β by an element b in $\mathfrak{B}$ such that $bA = \beta$, we get $v \equiv f(W)(\mathfrak{B} \cdot p)$, where f is a polynomial with coefficients $b^{p(k)}$, $b \in \mathfrak{B}$, and $W = \{w_\tau\}$. Thus

$$v = f(W) + up, \qquad u \in \mathfrak{B}.$$

For each b there is a b_1 in $\mathfrak{R}$ such that $bT \equiv b_1(\mathfrak{M})$ hence $(bT)^{p(k)} \equiv b_1{}^{p(k)}(\mathfrak{M}^{k+1})$. Replacing each coefficient $b^{p(k)}$ of f by $b_1{}^{p(k)}$, we get a polynomial g over $\mathfrak{R}$ such that

$$f(W)T \equiv g(C)(\mathfrak{M}^{k+1}),$$

where $C = \{c_\tau\}$. By induction assumption there is a u_k in $\mathfrak{R}$ such that

$$uT \equiv u_k(\mathfrak{M}^k).$$

Combining the last three congruences we obtain

$$vT \equiv g(C) + u_k p(\mathfrak{M}^{k+1}).$$

We may take the right-hand side to be a_{k+1}, since it is in $\mathfrak{R}$, and thus the induction is complete.

Theorem 11 and Corollary 1 are now completely proved.

Corollary 2. *Given two v-rings $\mathfrak{B}$ and $\mathfrak{W}$ with an isomorphism between their residue fields, there is an isomorphism of $\mathfrak{B}$ with $\mathfrak{W}$ which preserves the mapping of the residue fields.*

This follows from Corollary 1 together with the corollary to Theorem 8. Corollary 2 is one of the fundamental uniqueness theorems of Hasse and Schmidt [3, Theorem 19, p. 63] for valuation rings. The simplest proof of this result is due to MacLane [9, Theorem 8, Corollary 1], and our proof of Theorem 11 is essentially a generalization of this proof of MacLane's. If one is dealing only with v-rings, then the use of g.l.r.'s can be avoided because of the evident fact that a g.l.r. whose maximal ideal is principal is a local ring.

Corollary 3. *A complete local ring whose maximal ideal is generated by the* *prime number p is a homomorphic map of a v-ring with the same residue field.*

THEOREM 12. *Let $\mathfrak{R}$ be a complete local ring with residue field* P *of characteristic p. If the maximal ideal $\mathfrak{m}$ of $\mathfrak{R}$ has a minimal basis of n elements then $\mathfrak{R}$ is a homomorphic image of a formal power series ring $\mathfrak{S}$ in n indeterminates over a v-ring whose residue field is* P. *If $p\not\equiv 0(\mathfrak{m}^2)$, then $\mathfrak{S}$ may be taken as a ring in only $n-1$ indeterminates.*

Proof. There exists, by Theorem 11, a v-ring $\mathfrak{V}$ with residue field P, and a homomorphism T of $\mathfrak{V}$ on a subring R of $\mathfrak{R}$.

Let $\mathfrak{m}=\mathfrak{R}\cdot(u_1, \cdots, u_n)$. Since R contains at least one representative of every residue class in P, it can be proved exactly as in Theorem 9 that $\mathfrak{R}$ is the closure of $R[u_1, \cdots, u_n]$. Now T can be extended to a homomorphism of $\mathfrak{V}[x_1, \cdots, x_n]$ (where $x_1, \cdots, x_n$ are indeterminates) on $R[u_1, \cdots, u_n]$, and thence by continuity to a mapping of $\mathfrak{V}\{x_1, \cdots, x_n\}$ on $\mathfrak{R}$.

If $p\not\equiv 0(\mathfrak{m}^2)$, then p may be taken as an element in a minimal basis, say $u_n=p$. Then $R[u_1, \cdots, u_n]=R[u_1, \cdots, u_{n-1}]$, $\mathfrak{V}[x_1, \cdots, x_{n-1}]$ can be mapped on this ring, and the mapping extended to $\mathfrak{V}\{x_1, \cdots, x_{n-1}\}$.

THEOREM 13. *Let R be the subring referred to in Theorem* 11. *Then R is uniquely determined if* P *is perfect or if $\mathfrak{m}=\mathfrak{R}\cdot p$. Otherwise, infinitely many choices are available for R. If $\mathfrak{S}$ is a complete local ring containing $\mathfrak{R}$ and concordant with it, then any corresponding subring S of $\mathfrak{S}$ contains R, provided* P *is perfect.*

Proof. R is a complete local ring with maximal ideal $R\cdot p$ and residue field P. If P is perfect, then the multiplicative representatives of elements of P lie in R. It is then easy to see that R consists precisely of the sums of all "power series" $\sum_{k=0}^{\infty}a_kp^k$, where a_k is a multiplicative representative. Since R is thereby characterized within $\mathfrak{R}$ in an invariant way, it is uniquely determined. If $\mathfrak{S}$ contains and is concordant with $\mathfrak{R}$, then $\Sigma\supseteq$P, and if S is a subring of $\mathfrak{S}$ which is the map of a v-ring, then S is complete and has Σ as residue field. Hence S contains multiplicative representatives for elements of P, so S contains all quantities $\sum a_kp^k$—that is, $S\supseteq R$.

If P is not perfect, we proceed as in Theorem 10. By the construction in Theorem 11, the subring R contains each c_τ. But c_τ was any representative of γ_τ in $\mathfrak{R}$. Now if d is a non-unit of $\mathfrak{R}$ which is not in $\mathfrak{R}\cdot p$, then we may replace c_τ by $c_\tau+bd$ ($b\in\mathfrak{R}$), and there is a ring R containing $c_\tau+bd$. But R cannot contain also $c_\tau+b'd$ if $b\not\equiv b'(\mathfrak{m})$, for if it did, then $(b-b')d\in R\cdot p\subseteq\mathfrak{R}\cdot p$, $d\in\mathfrak{R}\cdot p$, a contradiction. Since infinitely many incongruent values of b are available, the statement is proved.

If $\mathfrak{m}=\mathfrak{R}\cdot p$, then, of course, R must equal $\mathfrak{R}$ and hence is unique.

DEFINITION. If the local ring $\mathfrak{R}$ contains a ring R which is either a v-ring or a field and which maps modulo $\mathfrak{m}$ on the entire residue field of $\mathfrak{R}$, then R is said to be a *coefficient ring* in $\mathfrak{R}$.

A coefficient field (as defined in §4) is a coefficient ring, and a coefficient ring which happens to be a field is a coefficient field. We have thus proved that every complete local ring not of characteristic p^k $(k>1)$ contains a coefficient ring. Moreover the ring of all formal power series over a v-ring (or a field) has this v-ring (or field) as a coefficient ring.

Part III

7. **Regular local rings.** As usual, let $\mathfrak{R}$ denote a local ring, $\mathfrak{m}$ its maximal ideal, $\{u_1, u_2, \cdots, u_n\}$ a minimal basis for $\mathfrak{m}$.

Definition. The local ring $\mathfrak{R}$ is said to be *regular*(2) if for every positive integer k and for every form ϕ (in n variables) of degree k whose coefficients are in $\mathfrak{R}$ but not all in $\mathfrak{m}$, it is true that

$$\phi(u_1, \cdots, u_n) \not\equiv 0(\mathfrak{m}^{k+1}).$$

In order that $\mathfrak{R}$ be a regular local ring it is clearly sufficient that

$$\phi(u_1, \cdots, u_n) \neq 0$$

for any form ϕ of the above description.

The following statements are easily proved: In view of Lemma 2 the criterion for a local ring $\mathfrak{R}$ to be regular does not depend on the particular minimal basis. If the condition of the definition is satisfied for an arbitrary basis of $\mathfrak{m}$, then this basis is necessarily minimal and the local ring is regular. If, in the regular local ring $\mathfrak{R}$, a is exactly divisible by $\mathfrak{m}^h$—that is, if $a\equiv 0(\mathfrak{m}^h)$, $a\not\equiv 0(\mathfrak{m}^{h+1})$—and if b is exactly divisible by $\mathfrak{m}^k$, then ab is exactly divisible by $\mathfrak{m}^{h+k}$. Hence a regular local ring has no zero-divisors. The completion of a regular local ring is also regular (following from equation (3) of Theorem 2).

In the proof of the next theorem we make use of the remarks at the end of §1. First, however, we need a lemma, which is of some interest in itself.

Lemma 14. *Let $\mathfrak{R}$ be a commutative ring with identity element, $\mathfrak{R}'=\mathfrak{R}[z]$, where z is an indeterminate. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathfrak{R}$, then*

$$\mathfrak{R}'\cdot(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{R}'\cdot\mathfrak{a}\cap\mathfrak{R}'\cdot\mathfrak{b}, \qquad \mathfrak{R}'\cdot\mathfrak{a}\cap\mathfrak{R} = \mathfrak{a}.$$

If $\mathfrak{q}$ is primary with associated prime $\mathfrak{p}$, then $\mathfrak{R}'\cdot\mathfrak{q}$ is primary with $\mathfrak{R}'\cdot\mathfrak{p}$ as its prime. If $f(z)$ is a zero-divisor in $\mathfrak{R}'$ then there exists an element $c\neq 0$ in $\mathfrak{R}$ such that $cf(z)=0$(17).

Proof. Since the elements of $\mathfrak{R}'\cdot\mathfrak{a}$ are those and only those of the form $\sum a_k z^k$, $a_k\in\mathfrak{a}$, the first statement is trivial.

Clearly $\mathfrak{R}'\cdot\mathfrak{q}\subseteq\mathfrak{R}'\cdot\mathfrak{p}$ and a power of every element of $\mathfrak{R}'\cdot\mathfrak{p}$ is in $\mathfrak{R}'\cdot\mathfrak{q}$. It remains to show that $f(z)g(z)\in\mathfrak{R}'\cdot\mathfrak{q}$, $f(z)\notin\mathfrak{R}'\cdot\mathfrak{p}$ implies $g(z)\in\mathfrak{R}'\cdot\mathfrak{q}$. Let $f(z)=\sum a_i z^i$, $g(z)=\sum b_j z^j$ $(a_i, b_j\in\mathfrak{R})$, and suppose that $a_0, a_1, \cdots, a_{m-1}\in\mathfrak{p}$,

[17] A direct proof of this last statement was given by McCoy [10, Theorem 2].

$a_m \notin \mathfrak{p}$. If $\mathfrak{a} = \mathfrak{R} \cdot (a_0, a_1, \cdots, a_{m-1})$ then $\mathfrak{a}^k \subseteq \mathfrak{q}$ for some k; placing $\mathfrak{q}_i = \mathfrak{q} : \mathfrak{a}^{k-i}$ $(i=0, 1, \cdots, k)$, we have $\mathfrak{a}\mathfrak{q}_i \subseteq \mathfrak{q}_{i+1}$, $\mathfrak{q}_0 = \mathfrak{R}$, $\mathfrak{q}_k = \mathfrak{q}$. Proceeding by induction we assume $g \in \mathfrak{R}' \cdot \mathfrak{q}_i$ and prove $g \in \mathfrak{R}' \cdot \mathfrak{q}_{i+1}$. If it is not, let b_n be the first b_j not in $\mathfrak{q}_{i+1}$. For the coefficient of z^{m+n} in fg we have

$$\cdots + a_{m-1}b_{n+1} + a_m b_n + a_{m+1}b_{n-1} + \cdots \in \mathfrak{q}_{i+1}.$$

All terms following $a_m b_n$ are in $\mathfrak{q}_{i+1}$; so are those preceding it since $g \in \mathfrak{R}' \cdot \mathfrak{q}_i$ implies $b_j \in \mathfrak{q}_i$, and $\mathfrak{a}\mathfrak{q}_i \in \mathfrak{q}_{i+1}$. Thus $a_m b_n \in \mathfrak{q}_{i+1}$, which is impossible since $a_m \notin \mathfrak{p}$, $b_n \notin \mathfrak{q}_{i+1}$.

For the last statement we may assume that the basis theorem holds in $\mathfrak{R}$. For if it does not, suppose $fg = 0$, $g \in \mathfrak{R}'$, $g \neq 0$. If $\mathfrak{R}_1$ is the smallest subring of $\mathfrak{R}$ containing the identity and the coefficients of f and g, then f is a zero-divisor in $\mathfrak{R}_1[z]$. Since the basis theorem holds in $\mathfrak{R}_1$, our assumption is justified.

Let $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ be an irredundant primary decomposition of (0) in $\mathfrak{R}$, and let $\mathfrak{p}_i$ be the associated prime ideal of $\mathfrak{q}_i$. The first part of the lemma implies that $(0) = \mathfrak{R}' \cdot \mathfrak{q}_1 \cap \cdots \cap \mathfrak{R}' \cdot \mathfrak{q}_s$ is an irredundant primary decomposition of (0) in $\mathfrak{R}'$, and so $\mathfrak{R}' \cdot \mathfrak{p}_1, \cdots, \mathfrak{R}' \cdot \mathfrak{p}_s$ are the prime ideals of (0). Now if f is a zero-divisor, then $(0) : (f) \neq (0)$, so that f is in some $\mathfrak{R}' \cdot \mathfrak{p}_i$. Thus the coefficients of f are in $\mathfrak{p}_i$ and are annihilated by a single element c.

THEOREM 14. *A necessary and sufficient condition that the local ring $\mathfrak{R}$ be regular is that its dimension be equal to the number of elements in a minimal basis of its maximal ideal. In any case the dimension can be at most this number.*

Proof. Let $\mathfrak{m} = (u_1, \cdots, u_n)$ and assume this basis is minimal. By the theorem of Krull quoted in §1 the dimension of $\mathfrak{R}$ is at most n.

Assume first that $\mathfrak{R}$ is regular; then we prove that the ideals (0) and $(u_1, u_2, \cdots, u_i)$, $i = 1, \cdots, n$, give a chain of $n+1$ prime ideals, so that the dimension of $\mathfrak{R}$ is at least n. Observing that this is trivial for $n=1$ we proceed by induction. Let $\mathfrak{R}' = \mathfrak{R}/(u_1)$; if $\mathfrak{m}'$ is the maximal ideal of the local ring $\mathfrak{R}'$, then $\mathfrak{m}' = \mathfrak{R}' \cdot (u_2', \cdots, u_n')$ and this basis is minimal (dashes indicate residue classes mod (u_1)). Now $\mathfrak{R}'$ is regular, for suppose that ϕ' is a form of degree k in $n-1$ letters with coefficients in $\mathfrak{R}'$ but not all in $\mathfrak{m}'$, and that $\phi'(u_2', \cdots, u_n') = 0$. If ϕ is the form of degree k obtained by replacing each coefficient of ϕ' by one of its representatives in $\mathfrak{R}$, then $\phi(u_2, \cdots, u_n) = au_1$, $a \in \mathfrak{R}$. If $a \in \mathfrak{m}^{k-1}$, $a = \psi(u_1, \cdots, u_n)$, where ψ is a form of degree $k-1$, then $\phi(u_2, \cdots, u_n) - u_1\psi(u_1, \cdots, u_n) = 0$. But this is impossible since $\mathfrak{R}$ is regular and not all the coefficients of $\phi - u_1\psi$ (as a form of degree k) are in $\mathfrak{m}$. Hence if a is exactly divisible by $\mathfrak{m}^h$, then $h < k-1$; writing $a = \psi(u_1, \cdots, u_n)$, where ψ is of degree h, we have $u_1\psi(u_1, \cdots, u_n) \in \mathfrak{m}^{h+2}$. Since $\mathfrak{R}$ is regular the coefficients of ψ must be in $\mathfrak{m}$, implying $a \in \mathfrak{m}^{h+1}$. This contradiction shows that $\mathfrak{R}'$ is regular, so that (0) and $(u_2', \cdots, u_i')$, $i = 2, \cdots, n$, give a chain of n prime ideals by the induction hypothesis. Hence $(u_1, u_2, \cdots, u_i)$, $i = 1, 2, \cdots, n$, are prime.

Assume now that $\mathfrak{R}$ is of dimension n. Suppose ψ is a form of degree k over $\mathfrak{R}$ such that $\psi(u_1, \cdots, u_n)=0$. If a is the coefficient of $u_1{}^k$, then

$$au_1{}^k \in (u_2, \cdots, u_n).$$

If $a \notin \mathfrak{m}$, then $u_1{}^k \in (u_2, \cdots, u_n)$. Then if $\mathfrak{p}$ is any minimal prime ideal of $(u_2, \cdots, u_n)$, then $u_1 \in \mathfrak{p}$, $\mathfrak{p}=\mathfrak{m}$. But by Krull's theorem the rank of $\mathfrak{p}$ is at most $n-1$, whereas $\mathfrak{m}$ has been assumed of rank n. Hence $a \in \mathfrak{m}$. We now show that every coefficient of ψ is in $\mathfrak{m}$.

Let $u_i=\sum_{j=1}^n c_{ij}v_j$, where $c_{ij}\in\mathfrak{R}$, $|c_{ij}| \notin \mathfrak{m}$; then $\mathfrak{m}=(v_1, \cdots, v_n)$ (Lemma 2). Substituting in $\psi(u)=0$, we obtain

$$\psi(u_1, \cdots, u_n) = \phi(v_1, \cdots, v_n) = 0.$$

Here ϕ is a form of degree k in which the coefficient of $v_1{}^k$ is $\psi(c_{11}, \cdots, c_{n1})$. By what has just been proved, this coefficient is in $\mathfrak{m}$. Hence if $\bar{\psi}$ is the form obtained by reducing the coefficients of ψ mod $\mathfrak{m}$, then $\bar{\psi}(\bar{c}_{11}, \cdots, \bar{c}_{n1})=0$. This is true for all constants $\bar{c}_{11}, \cdots, \bar{c}_{n1}$ in P, for if at least one $\bar{c}_{i1}\neq 0$, we can find a matrix (c_{ij}) such that $|c_{ij}| \notin \mathfrak{m}$. If, now, the residue field P has infinitely many elements, then every coefficient of $\bar{\psi}$ is zero, hence every coefficient of ψ is in $\mathfrak{m}$, as was to be proved. The proof is thus complete if P is infinite.

If P is finite, let $\mathfrak{R}'=\mathfrak{R}[z]$ where z is an indeterminate. By Lemma 14 every zero-divisor in $\mathfrak{R}'$ has coefficients which are all zero-divisors and hence is in $\mathfrak{R}'\cdot\mathfrak{m}$. Thus we may form the quotient ring $\mathfrak{R}''$ of $\mathfrak{R}'$ with respect to $\mathfrak{R}'\cdot\mathfrak{m}$ (which is prime by Lemma 14). The ring $\mathfrak{R}''$ will be a local ring with maximal ideal $\mathfrak{R}''\cdot\mathfrak{m}=\mathfrak{R}''\cdot(u_1, \cdots, u_n)$, and so the dimension of $\mathfrak{R}''$ is at most n. Since $\mathfrak{R}$ is of dimension n, there exists a chain of prime ideals

$$\mathfrak{m} \supset \mathfrak{p}_{n-1} \supset \mathfrak{p}_{n-2} \supset \cdots \supset \mathfrak{p}_0.$$

By Lemma 14 and the known properties of quotient rings(11) the chain

$$\mathfrak{R}''\cdot\mathfrak{m} \supset \mathfrak{R}''\cdot\mathfrak{p}_{n-1} \supset \mathfrak{R}''\cdot\mathfrak{p}_{n-2} \supset \cdots \supset \mathfrak{R}''\cdot\mathfrak{p}_0$$

consists of distinct prime ideals, and $\mathfrak{R}''$ is thus exactly of dimension n; moreover the above basis of $\mathfrak{R}''\cdot\mathfrak{m}$ is minimal. But the residue field of $\mathfrak{R}''$ is infinite (for it is a simple transcendental extension of P) and hence $\mathfrak{R}''$ is regular. Since $\mathfrak{R}''\cdot\mathfrak{m}$ and $\mathfrak{m}$ have the same minimal basis, and since $\mathfrak{R}''\cdot\mathfrak{m}\cap\mathfrak{R}=\mathfrak{m}$, it follows that also $\mathfrak{R}$ is regular.

COROLLARY. *If $\mathfrak{R}$ is a regular local ring and $\mathfrak{m}=(u_1, \cdots, u_n)$ then for $i=1, 2, \cdots, n$ the ideal $(u_1, \cdots, u_i)$ is prime of rank i and dimension $n-i$, and $\mathfrak{R}/(u_1, \cdots, u_i)$ is a regular local ring.*

Proof. From the induction at the beginning of the proof of the theorem it follows that $\mathfrak{R}/(u_1, \cdots, u_i)$ is a regular local ring of dimension $n-i$; hence $(u_1, \cdots, u_i)$ is prime of dimension $n-i$. The rank of this ideal is at least i, and it cannot be more since the dimension of $\mathfrak{R}$ is n.

We have here tacitly made use of the following remarks:

If $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in the local ring* $\mathfrak{R}$, $\mathfrak{a}\subseteq\mathfrak{b}$, *then the dimension of* $\mathfrak{b}$ *in* $\mathfrak{R}$ *is equal to the dimension of* $\mathfrak{b}/\mathfrak{a}$ *in* $\mathfrak{R}/\mathfrak{a}$. *In particular, the dimension of* $\mathfrak{a}$ *is equal to the dimension of the ring* $\mathfrak{R}/\mathfrak{a}$.

This follows immediately from the 1-1 correspondence between the prime ideals $\mathfrak{p}$ in $\mathfrak{R}$ containing $\mathfrak{b}$ and the prime ideals $\mathfrak{p}/\mathfrak{a}$ in $\mathfrak{R}/\mathfrak{a}$ containing $\mathfrak{b}/\mathfrak{a}$. These remarks will often be used in what follows.

Since a regular local ring $\mathfrak{R}$ has no zero-divisors, it must be of characteristic zero or p. If it is of characteristic zero and its residue field P is of characteristic p, then $p\equiv 0(\mathfrak{m})$. If $p\not\equiv 0(\mathfrak{m}^2)$, then $\mathfrak{R}$ is said to be *unramified.* It will be convenient to call $\mathfrak{R}$ unramified also in the case where $\mathfrak{R}$ and P have the same characteristic. If $\mathfrak{R}$ is unramified then so is its completion; this follows from equation (3). Recalling the definition of "v-ring" given in the previous section, we see that a v-ring is simply an *unramified complete regular local ring of dimension one whose characteristic is different from that of its residue field.*

THEOREM 15. *Let* $\mathfrak{R}$ *be a complete regular local ring of dimension* n, P *its residue field. If* $\mathfrak{R}$ *and* P *have the same characteristic, then* $\mathfrak{R}$ *is isomorphic to a formal power series ring over* P *in* n *variables. If* $\mathfrak{R}$ *and* P *have different characteristics and* $\mathfrak{R}$ *is unramified, then it is isomorphic to a formal power series ring in* $n-1$ *variables over a* v*-ring of residue field* P[18]. *Conversely, such power series rings are unramified complete regular local rings of dimension* n *and of residue field* P.

Proof. We first consider the converse. If $\mathfrak{V}$ is a v-ring, then by Lemma 5 (§4) the power series ring $\mathfrak{S}=\mathfrak{V}\{x_1, \cdots, x_{n-1}\}$ is a complete local ring with maximal ideal $\mathfrak{M}=(x_1, \cdots, x_{n-1}, p)$ and residue field equal to that of $\mathfrak{V}$, and the indicated basis of $\mathfrak{M}$ is minimal. It is clear that the ideals $(x_1, x_2, \cdots, x_i)$, $i=1, 2, \cdots, n-1$, are prime and so together with (0) and $\mathfrak{M}$ we have a chain of $n+1$ prime ideals. Theorem 14 implies that $\mathfrak{S}$ is regular and of dimension n. If the coefficient domain is a field then the proof is similar.

For the first part of the theorem observe that the maximal ideal $\mathfrak{m}$ of $\mathfrak{R}$ has a basis of n elements: $\mathfrak{m}=(u_1, \cdots, u_n)$. By Theorems 9 and 12, $\mathfrak{R}$ is a homomorphic map of one of the indicated power series rings $\mathfrak{S}$. Since $\mathfrak{R}$ has no zero-divisors the kernel of this homomorphism is a prime ideal $\mathfrak{p}$ in $\mathfrak{S}$, and the dimension of $\mathfrak{p}$ must equal that of $\mathfrak{R}$, hence $\mathfrak{p}$ has dimension n. But it has just been shown that $\mathfrak{S}$ has dimension n. Thus $\mathfrak{p}=(0)$ and the mapping is an isomorphism.

The fact that the mapping is isomorphic can also be concluded directly from the fact that $\mathfrak{R}$ is regular.

[18] An example at the end of this section shows that no power series representation is in general possible in the ramified case.

DEFINITION. A *p-adic* ring is an unramified complete regular local ring.

COROLLARY 1. *Two p-adic rings having the same characteristic, dimension, and residue field are isomorphic.*

This follows from the theorem and from Corollary 2 of Theorem 11 (§6).

COROLLARY 2. *Every complete local ring is the homomorphic map of a p-adic ring.*

This follows from Theorems 9 and 12 and the present theorem.

COROLLARY 3. *A ramified complete regular local ring $\mathfrak{R}$ of dimension n is a homomorphic image of an $(n+1)$-dimensional p-adic ring $\mathfrak{S}$ modulo the prime principal ideal generated by an element of a minimal basis of the maximal ideal of $\mathfrak{S}$.*

Proof. By Theorem 14 the maximal ideal $\mathfrak{m}$ of $\mathfrak{R}$ has a basis of n elements; hence, by Theorems 12 and 15, $\mathfrak{R}$ is a homomorphic map of a p-adic ring $\mathfrak{S}$ of dimension $n+1$. The kernel $\mathfrak{p}$ of this mapping is a prime ideal of dimension n, hence must be a minimal prime ideal of $\mathfrak{S}$. If $\mathfrak{M}$ is the maximal ideal of $\mathfrak{S}$, then $\mathfrak{M}=(u_1, \cdots, u_{n+1})$. The maps of these mod $\mathfrak{p}$ form a basis for $\mathfrak{m}$, hence one of them—say the map of u_{n+1}—is in the ideal generated by the rest. So there exist elements $a_1, \cdots, a_n$ in $\mathfrak{S}$ such that $u_{n+1}-a_1u_1- \cdots -a_nu_n \in \mathfrak{p}$. This element may replace u_{n+1} in the basis for $\mathfrak{M}$ hence by the corollary to Theorem 14 it generates a prime ideal; since this ideal is contained in $\mathfrak{p}$, which is minimal, the required conclusion follows.

LEMMA 15. *Let $\mathfrak{R}$ be a local ring of dimension r (>0), $\mathfrak{a}$ an ideal in $\mathfrak{R}$ of rank not less than s, $0 \leqq s \leqq r$. Then there exists a minimal basis $\{u_1, \cdots, u_n\}$ for $\mathfrak{m}$ such that $(\mathfrak{a}, u_{s+1}, \cdots, u_r)$ is a primary ideal belonging to $\mathfrak{m}$. Moreover, if $s>0$, this basis may be taken to include any prescribed element in $\mathfrak{a}$ which is not in $\mathfrak{m}^2$.*

Proof. We recall that the rank of an ideal is the minimum of the ranks of its associated prime ideals.

For each i $(i=s, s+1, \cdots, r)$ we show the existence of a minimal basis $\{x_1, \cdots, x_n\}$ of $\mathfrak{m}$ such that $(\mathfrak{a}, x_{s+1}, \cdots, x_i)$ is of rank not less than i and x_1 is the prescribed element (if any) of $\mathfrak{a}$. For $i=r$ this gives the desired conclusion. We proceed by induction, assuming the existence for some i, $i<r$ (and observing that it is trivial for $i=s$).

If $(\mathfrak{a}, x_{s+1}, \cdots, x_i)$ has rank greater than i, then so does $(\mathfrak{a}, x_{s+1}, \cdots, x_{i+1})$, and the induction argument is complete. Otherwise, let $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ be those prime ideals of $(\mathfrak{a}, x_{s+1}, \cdots, x_i)$ which are of rank i. No one of them can contain another, and since each is distinct from $\mathfrak{m}$ (for $i<r$) none of them can contain all the x_j. Thus for some m, $x_m \notin \mathfrak{p}_1$; renumber the $\mathfrak{p}_j$ so that $x_m \notin \mathfrak{p}_1, \cdots, \mathfrak{p}_k$, $x_m \in \mathfrak{p}_{k+1}, \cdots, \mathfrak{p}_h$ $(1 \leqq k \leqq h)$. For each $j=k+1, \cdots, h$ let $m(j)$ be such that $x_{m(j)} \notin \mathfrak{p}_j$ and let c_j be in $\bigcap_{t \neq j}\mathfrak{p}_t$ but not in $\mathfrak{p}_j$; then

$x_m' = x_m + \sum_{j=k+1}^{h} c_j x_{m(j)}$ is in none of $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$. Since $m(j) \neq m$ we still have a basis for $\mathfrak{m}$ if x_m is replaced by x_m', and since $m \neq s+1, \cdots, i$, the elements $x_{s+1}, \cdots, x_i$ are still present in the new basis. Since x_m' is in no $\mathfrak{p}_j$, $(\mathfrak{a}, x_{s+1}, \cdots, x_i, x_m')$ has rank not less than $i+1$. If $x_1 \in \mathfrak{a}$, then $m \neq 1$, and so x_1 is still present in the new basis. This completes the induction, if we imagine the x's renumbered so that x_m' and x_{i+1} are interchanged. This causes no difficulty, except that the preferred role of x_1 is disturbed if $i+1=1$; however, this can happen only if $s=0$, in which case x_1 plays no exceptional part.

THEOREM 16. *Let $\mathfrak{R}$ be a complete local ring; in the unequal-characteristic case let it be assumed that $\mathfrak{R} \cdot p$ is of rank one. Then $\mathfrak{R}$ is a finite module over a subring $\mathfrak{R}_0$ which is a p-adic ring having the same characteristic, dimension, and residue field as $\mathfrak{R}$*([19]).

(*Note*: The assumption on $\mathfrak{R}p$ is satisfied if p is not a zero-divisor.)

Proof. The hypothesis excludes the case of characteristic p^k $(k>1)$, for in that case $\mathfrak{R} \cdot p$ would be in every prime ideal of (0), hence would be of rank zero. Hence $\mathfrak{R}$ contains a coefficient ring R (for definition, see end of Part II).

If $\mathfrak{R}$ is of dimension r, let $x_1, \cdots, x_r$ be elements such that $(x_1, \cdots, x_r)$ is a primary ideal belonging to $\mathfrak{m}$. The existence follows from Lemma 15, with $\mathfrak{a}=(0)$, $s=0$. In the unequal-characteristic case we require in addition that $x_1=p$; the existence follows from Lemma 15 with $\mathfrak{a}=\mathfrak{R} \cdot p$, $s=1$. (If $r=0$, then $\mathfrak{m}$ is nilpotent, and we have the equal-characteristic case; the ring R is a field and we take $\mathfrak{R}_0=R$.) Then $\mathfrak{R}_0=R\{x_1, \cdots, x_r\}$ is the required ring, by the lemma which follows.

LEMMA 16. *Let $\mathfrak{R}$ be a complete local ring, R a coefficient ring in $\mathfrak{R}$, $x_1, \cdots, x_m$ any elements of the maximal ideal $\mathfrak{m}$ such that (in the unequal-characteristic case) $x_1=p$. Then $\mathfrak{R}_0=R\{x_1, \cdots, x_m\}$ is a complete local ring concordant with $\mathfrak{R}$ and having the same residue field, and its maximal ideal is $\mathfrak{R}_0 \cdot (x_1, \cdots, x_m)$. If $\mathfrak{R} \cdot (x_1, \cdots, x_m)$ is a primary ideal belonging to $\mathfrak{m}$, then $\mathfrak{R}$ is a finite $\mathfrak{R}_0$-module. If, in addition, the dimension of $\mathfrak{R}$ is m, then $\mathfrak{R}_0$ is p-adic and of dimension m.*

[19] This may be regarded as an analogue of E. Noether's well known "normalization theorem," which states that if $\mathfrak{p}$ is a prime ideal in a ring $\mathfrak{R}$ of polynomials (over a field), then $\mathfrak{R}/\mathfrak{p}$ contains a polynomial ring on which it is integrally dependent. That a corresponding statement holds also when $\mathfrak{R}$ is a power series ring is implied by the present theorem, in view of Theorem 15. In the case where the coefficient field is infinite, the normalization theorem for power series rings is not a new result (see Rückert [11, p. 266], Krull [5, Theorems 10, 12]). The indicated theorems of Krull are not special cases of Theorem 16 since he considers power series rings in infinitely many variables, but these two theorems can be deduced from ours and therefore hold also for finite coefficient fields. Thus Theorem 15 in Krull [5] can be stated without exceptions. In this connection, see Theorem 19 of the present paper. The quoted theorems of Krull require the normalization theorem for finite coefficient fields in the polynomial case also; a proof in this case can be found in Zariski [14, p. 506].

Proof. $\mathfrak{R}_0$ consists of all "power series" $c=\sum_{k=0}^{\infty}\phi_k(x_1, \cdots, x_m)$ where ϕ_k is a form over R of degree k in m variables. These series certainly converge in $\mathfrak{R}$, since $\mathfrak{R}$ is complete, and they form a ring. If $\phi_0=0$, then c is clearly in the ideal $\mathfrak{m}_0=\mathfrak{R}_0\cdot(x_1, \cdots, x_m)$. Hence if $c\notin\mathfrak{m}_0$, then $\phi_0\neq 0$ and, in fact, ϕ_0 is a unit in R, so that—by the usual argument—c is a unit in $\mathfrak{R}_0$. Thus $\mathfrak{m}_0$ is the ideal of non-units in $\mathfrak{R}_0$, $\mathfrak{m}_0=\mathfrak{m}\cap\mathfrak{R}_0$, hence $\bigcap_{k=1}^{\infty}\mathfrak{m}_0{}^k=(0)$. Thus $\mathfrak{R}_0$ is a generalized local ring and its residue field coincides with that of $\mathfrak{R}$. The indicated basis of $\mathfrak{m}_0$ need not be minimal. Now $\mathfrak{R}_0$ is complete; this follows easily from the remark that if $c\in\mathfrak{m}_0{}^k$, then $c\equiv\phi(x_1, \cdots, x_m)(\mathfrak{m}_0{}^{k+1})$, where ϕ is a form over R of degree k. Hence $\mathfrak{R}_0$ is a local ring (Theorem 3) and is concordant with $\mathfrak{R}$ (Theorem 5).

If $\mathfrak{R}\cdot(x_1, \cdots, x_m)=\mathfrak{R}\cdot\mathfrak{m}_0$ is primary and belongs to $\mathfrak{m}$, then $\mathfrak{R}$ is a finite $\mathfrak{R}_0$-module by Theorem 8. If $\mathfrak{R}$ has dimension m, then it contains a chain of $m+1$ prime ideals; the contractions of these to $\mathfrak{R}_0$ are distinct[20] and hence $\mathfrak{R}_0$ is of dimension at least m. By Theorem 14, $\mathfrak{R}_0$ is regular and of dimension m. Finally, $\mathfrak{R}_0$ is unramified, for (in the unequal-characteristic case) p occurs in a minimal basis of $\mathfrak{m}_0$.

LEMMA 17. *Let $\mathfrak{R}$ and $\mathfrak{R}_0$ be complete local rings, $\mathfrak{R}_0\subseteq\mathfrak{R}$, and let $\mathfrak{R}$ contain an element x such that $\mathfrak{m}=(x, \mathfrak{R}\cdot\mathfrak{m}_0)$ and for some integer $k\geqq 1$,*

$$x^k\in\mathfrak{R}\cdot\mathfrak{m}_0, \qquad x^{k-1}\notin\mathfrak{R}\cdot\mathfrak{m}_0.$$

If the two rings have the same residue field, then $\mathfrak{R}=\mathfrak{R}_0[x]$, and x satisfies over $\mathfrak{R}_0$ a monic equation of degree k all of whose coefficients (except the first) are in $\mathfrak{m}_0$.

Proof. It is clear that $\mathfrak{R}\cdot\mathfrak{m}_0$ is primary for $\mathfrak{m}$ and of exponent k. Let

$$\mathfrak{q}_j = (x^j, \mathfrak{R}\cdot\mathfrak{m}_0), \qquad j = 0, 1, \cdots, k.$$

Then these ideals are primary and

$$\mathfrak{m} = \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_k = \mathfrak{R}\cdot\mathfrak{m}_0,$$
$$\mathfrak{m}\mathfrak{q}_{j-1} \subseteq \mathfrak{q}_j, \qquad \mathfrak{q}_{j-1} = (x^{j-1}, \mathfrak{q}_j), \qquad j = 1, \cdots, k.$$

All these statements are obvious except that $\mathfrak{q}_{j-1}\neq\mathfrak{q}_j$. But if equality holds, then $x^{j-1}\equiv ax^j(\mathfrak{R}\cdot\mathfrak{m}_0)(a\in\mathfrak{R})$, $x^{j-1}(1-ax)\in\mathfrak{R}\cdot\mathfrak{m}_0$. Since $1-ax$ is a unit, $x^{j-1}\in\mathfrak{R}\cdot\mathfrak{m}_0$, which is impossible since $j-1<k$. These relations show that we have a composition sequence[8] for $\mathfrak{R}\cdot\mathfrak{m}_0$. It follows from the proof of Theorem 8 that the elements $1, x, \cdots, x^{k-1}$ form an $\mathfrak{R}_0$-basis for $\mathfrak{R}$. Then $\mathfrak{R}=\mathfrak{R}_0[x]$, and

$$x^k = a_1x^{k-1} + \cdots + a_k, \qquad a_i \in \mathfrak{R}_0.$$

If not every a_i is in $\mathfrak{m}_0$, then suppose $a_h\notin\mathfrak{m}_0$, $a_i\in\mathfrak{m}_0$ for $i=h+1, \cdots, k$ $(1\leqq h\leqq k)$. Then

[20] Cohen and Seidenberg [2, Theorem 4]. For rings without zero-divisors the statement would follow from Krull [5, Theorem 2].

$$x^{k-h}(x^h - a_1x^{h-1} - \cdots - a_h) \in \mathfrak{R}\cdot\mathfrak{m}_0.$$

Now the right factor is not in $\mathfrak{m}$, hence is a unit, so $x^{k-h}\in\mathfrak{R}\cdot\mathfrak{m}_0$. Since this is impossible, each $a_i\in\mathfrak{m}_0$.

Definition. An *Eisenstein polynomial* over a local ring $\mathfrak{R}_0$ is a polynomial $z^k+a_1z^{k-1}+\cdots+a_k$, where $a_i\in\mathfrak{m}_0$, $i=1,\cdots,k$, $a_k\notin\mathfrak{m}_0^2$. If $\mathfrak{R}=\mathfrak{R}_0[x]$, and x is a root of an Eisenstein polynomial over $\mathfrak{R}_0$, then $\mathfrak{R}$ is said to be an *Eisenstein extension* of $\mathfrak{R}_0$.

A proof similar to that of the Eisenstein irreducibility criterion shows that such a polynomial is irreducible over $\mathfrak{R}_0$.

Theorem 17. *Any complete regular local ring $\mathfrak{R}$ is an Eisenstein extension of a p-adic ring $\mathfrak{R}_0$. An Eisenstein extension of any complete regular local ring is a complete regular local ring of the same characteristic, dimension, and residue field.*

Proof. For the proof of the first statement, we naturally assume the unequal-characteristic case. From Lemma 15, with $\mathfrak{a}=\mathfrak{R}\cdot p$, $s=1$, we obtain a minimal basis $\{u_1, u_2, \cdots, u_r\}$ for $\mathfrak{m}$ such that $\mathfrak{R}\cdot(p, u_2, \cdots, u_r)$ is primary for $\mathfrak{m}$; here r is the dimension of $\mathfrak{R}$. Let R be a coefficient ring in $\mathfrak{R}$. By Lemma 16, $\mathfrak{R}_0=R\{p, u_2, \cdots, u_r\}$ is a p-adic ring having the same residue field as $\mathfrak{R}$. Moreover, $\mathfrak{m}_0=\mathfrak{R}_0\cdot(p, u_2, \cdots, u_r)$, so that $\mathfrak{R}\cdot\mathfrak{m}_0$ is primary for $\mathfrak{m}$ and $\mathfrak{m}=(u_1, \mathfrak{R}\cdot\mathfrak{m}_0)$. If the exponent of $\mathfrak{R}\cdot\mathfrak{m}_0$ is k, then

$$u_1^k \in \mathfrak{R}\cdot\mathfrak{m}_0, \qquad u_1^{k-1}\notin\mathfrak{R}\cdot\mathfrak{m}_0; \tag{20}$$

Lemma 17 implies that $\mathfrak{R}=\mathfrak{R}_0[u_1]$ and that u_1 satisfies an equation

$$u_1^k + a_1u_1^{k-1} + \cdots + a_k = 0, \qquad a_i\in\mathfrak{m}_0. \tag{21}$$

If $a_k\in\mathfrak{m}_0^2$, then by (21)—and since $a_i\in\mathfrak{m}_0$—$u_1^k\in\mathfrak{m}\cdot\mathfrak{m}_0$. Thus $u_1^k \equiv bp(u_2, \cdots, u_r)$, with $b\in\mathfrak{m}$, so that $b\equiv cu_1(u_2, \cdots, u_r)$, $c\in\mathfrak{R}$. Hence $u_1(u_1^{k-1}-cp)\equiv 0(u_2, \cdots, u_r)$. Since $\mathfrak{R}\cdot(u_2, \cdots, u_r)$ is a prime ideal not containing u_1 (Theorem 14, corollary), $u_1^{k-1}\in\mathfrak{R}\cdot(p, u_2, \cdots, u_r)=\mathfrak{R}\cdot\mathfrak{m}_0$, contradicting (20). Thus the proof is complete.

Suppose now that $\mathfrak{R}_0$ is any complete regular local ring of dimension r and $\mathfrak{R}=\mathfrak{R}_0[x]$, where x satisfies the equation

$$x^k + a_1x^{k-1} + \cdots + a_k = 0, \qquad a_1, \cdots, a_k\in\mathfrak{m}_0, \qquad a_k\notin\mathfrak{m}_0^2. \tag{22}$$

As remarked above this equation is irreducible over $\mathfrak{R}_0$, hence also over its quotient field, since $\mathfrak{R}_0$ is integrally closed[21]. Hence $\mathfrak{R}$ is an integral domain and by Theorem 7[22] is a complete local ring. If $\mathfrak{m}$ is its maximal ideal, then $\mathfrak{m}\cap\mathfrak{R}_0=\mathfrak{m}_0$, and by (22), $x^k\in\mathfrak{R}\cdot\mathfrak{m}_0\subseteq\mathfrak{m}$, $x\in\mathfrak{m}$. Let $\{u_1, \cdots, u_r\}$ be a

[21] Krull [7, Theorem 6] has proved that a regular local ring is integrally closed.

[22] It is not actually necessary to use Theorem 7 at this point. Namely, it can be proved that an Eisenstein extension of any local ring is a local ring.

minimal basis of $\mathfrak{m}_0$, with $u_1=a_k$. If $c=\sum_{i=0}^{k-1}c_ix^i(c_i\in\mathfrak{R}_0)$ is in $\mathfrak{m}$, then $c_0\in\mathfrak{m}_0\subseteq\mathfrak{R}\cdot(x,u_2,\cdots,u_r)$, since by (22), $u_1\in\mathfrak{R}\cdot x$. Thus $\mathfrak{m}=\mathfrak{R}\cdot(x,u_2,\cdots,u_r)$. Since $\mathfrak{R}$ is integral over $\mathfrak{R}_0$, it has[23] dimension r, and by Theorem 14, $\mathfrak{R}$ is regular. For c above we have $c\equiv c_0(\mathfrak{m})$, hence the residue fields coincide.

COROLLARY. *Let $\mathfrak{R}$ be a complete regular local ring of characteristic zero with residue field of characteristic p. A necessary condition that $\mathfrak{R}$ be a ring of power series over a complete discrete valuation ring is that $p=e\pi^k$, where e is a unit in $\mathfrak{R}$, π an element of $\mathfrak{m}$ not in $\mathfrak{m}^2$, and k a positive integer. If $k\not\equiv 0(p)$, then this condition is also sufficient.*

Proof. If $\mathfrak{R}$ is a power series ring over the complete discrete valuation ring $\mathfrak{B}$, then by Lemma 5 the prime element π of $\mathfrak{B}$ is in a minimal basis of $\mathfrak{m}$, hence is not in $\mathfrak{m}^2$. Moreover p is a non-unit in $\mathfrak{B}$, hence $p=e\pi^k$, e a unit in $\mathfrak{B}$.

Conversely, assume the hypothesis $p=e\pi^k$ satisfied, with k not divisible by p. Let R be a coefficient ring in $\mathfrak{R}$. Then there is an element d in R such that $e\equiv d(\mathfrak{m})$, $d^{-1}e\equiv 1(\mathfrak{m})$. The residue of $d^{-1}e$ in P is unity, and the polynomial z^k-1 over P has $z=1$ as a simple root since $k\not\equiv 0(p)$. Since $\mathfrak{R}$ is a complete local ring, Hensel's Lemma (Theorem 4) gives the existence in $\mathfrak{R}$ of a kth root c of $d^{-1}e$: $d^{-1}e=c^k$. If $\pi_1=c\pi$, then $\pi_1{}^k=d^{-1}p$ and π_1 is thus the root of an Eisenstein polynomial over R, and $\mathfrak{B}=R[\pi_1]$ is by the theorem a complete regular local ring of dimension one—that is, a complete discrete valuation ring. Since $\pi_1\notin\mathfrak{m}^2$ it may be taken into a minimal basis of $\mathfrak{m}$. From this fact it can be concluded as in the proof of Theorem 12 that $\mathfrak{R}$ is a ring of power series over $\mathfrak{B}$ in $n-1$ variables, where n is the dimension of $\mathfrak{R}$.

For dimension one, Theorem 17 implies that a complete discrete valuation ring is an Eisenstein extension of a v-ring[24], a result due to Hasse and Schmidt [3, Theorem 18, p. 62]. The present theorem gives a certain insight into the structure of ramified complete regular local rings. For such rings we cannot necessarily obtain a power series representation as in Theorem 15, even if ramified valuation rings are admitted as domains of coefficients; this can be easily deduced from the corollary.

To obtain an actual example, we let $\mathfrak{J}$ denote the ring of p-adic integers. Let $\mathfrak{R}_0=\mathfrak{J}\{x\}$ be the ring of power series over $\mathfrak{J}$ in an indeterminate x, so that $\mathfrak{R}_0$ is a p-adic ring of dimension 2 (Theorem 15), with $\mathfrak{m}_0=(p,\ x)$. We adjoin to $\mathfrak{R}_0$ an element y, defined by the Eisenstein equation $y^2=p+x^2$. Then $\mathfrak{R}=\mathfrak{R}_0[y]$ is an Eisenstein extension of $\mathfrak{R}_0$, hence is a complete regular local ring of dimension 2, with $\mathfrak{m}=(x,\ y)$. Since $p=y^2-x^2\in\mathfrak{m}^2$, $\mathfrak{R}$ is surely rami-

[23] If $\mathfrak{R}$ is integrally dependent on $\mathfrak{R}_0$, then any prime ideal in $\mathfrak{R}$ has the same dimension as its contraction in $\mathfrak{R}_0$; if $\mathfrak{R}_0$ is integrally closed, then also the ranks are equal [5, Theorems 7 and 8].

[24] From Theorem 13 it follows that if the valuation ring is ramified, then this v-ring is uniquely determined if and only if the residue field is perfect. In footnote 18 (p. 12) of [3] there is an oversight, in that the v-ring is stated to be unique only if the residue field is absolutely algebraic.

fied. We now show that $\mathfrak{R}$ cannot be a power series ring over a valuation ring —or over any ring, for that matter.

Suppose namely, that $\mathfrak{R}$ is a ring of power series over some ring $\mathfrak{B}$. It is then readily verified that $\mathfrak{B}$ must be a complete local ring. By Lemma 5 its maximal ideal must be principal (so that $\mathfrak{B}$ is a complete discrete valuation ring), and $\mathfrak{R}$ must be a ring of power series in a single variable. By the corollary, p is of the form $e\pi^2$, e a unit. This is impossible if $p\neq 2$. For then $\mathfrak{m}=(y-x,\ y+x)$ so that $(y-x)$ and $(y+x)$ are distinct prime ideals. Since $e\pi^2=(y-x)(y+x)$, π is in each of these prime ideals, hence in their product, and this is impossible.

If $p=2$, we proceed as follows. Since $\mathfrak{B}$ is complete it contains the 2-adic ring $\mathfrak{J}$, and by Lemma 17 we have that $\mathfrak{B}=\mathfrak{J}[\pi]$ and that π satisfies

$$\pi^2 + a\pi + b = 0, \qquad a,\ b \in \mathfrak{J}.$$

On the other hand, $\pi=c+dy\ (c,\ d\in\mathfrak{R}_0)$ and $d\neq 0$; for if $\pi\in\mathfrak{R}_0$, then $\mathfrak{B}\subset\mathfrak{R}_0$, and this is clearly impossible. Since $\pi\notin\mathfrak{R}_0$ the above is the only monic quadratic equation for π over $\mathfrak{R}_0$, hence $2c=-a$, $c^2-d^2y^2=b$. Since $a,\ b\in\mathfrak{J}$, we have $c\in\mathfrak{J}$, $d^2y^2=d^2(2+x^2)\in\mathfrak{J}$. If $d^2=\sum_{i=0}^{\infty}d_ix^i$, $d_i\in\mathfrak{J}$, then the coefficient of x^{n+2} in $d^2(2+x^2)$ is $2d_{n+2}+d_n$. Hence $d_n=-2d_{n+2}=(-2)^kd_{n+2k}$ $(k=1,\ 2,\ \cdots)$, so $d_n=0$. This implies $d=0$, and we have arrived at a contradiction.

Thus also in the case $p=2$, $\mathfrak{R}$ cannot be represented as a power series ring. But it should be observed that in this case the contradiction was not, as in the case $p\neq 2$, due to the assumption of the equation $p=e\pi^2$, but rather it was due directly to the assumption of the representability of $\mathfrak{R}$ as a power series ring. In fact, $p=2$ *is* of this form, since $2=(1+x^2-xy)(x+y)^2$. *Thus the condition* $k\not\equiv 0(p)$ *in the corollary cannot be omitted.*

8. **Ideal theory in regular local rings.** Some of the results of this section are known for rings of power series over a field (Theorems 18 and 19) or even over a v-ring (Theorem 18), at least when the residue field is infinite. Our proofs will be general.

THEOREM 18. *In an unramified complete regular local ring $\mathfrak{R}$ every element is expressible uniquely (up to units) as a product of irreducible elements*[25]. *Every minimal prime ideal of $\mathfrak{R}$ is principal and has dimension one less than that of $\mathfrak{R}$.*

[25] For a ring of power series over an infinite field the unique factorization theorem is classical. For a power series ring over a complete discrete valuation ring with infinite residue field the theorem was proved by Krull [6, Theorem 4], the case of a finite residue field being left open [6, pp. 770, 778]. Theorem 18 establishes factorization for power series over an arbitrary field or v-ring, but not over a ramified valuation ring. However, our proof readily applies also to this case if R is taken to mean the given valuation ring and if p is taken to be the generator of its maximal ideal. All the factorization theorems in Krull [6] can then be stated without the assumption of infinite residue fields.

Proof. By an irreducible element is meant a non-unit ($\neq 0$) which admits no factorization into non-units. Every non-unit is clearly the product of irreducible elements in at least one way. To show uniqueness it must be proved that every irreducible element generates a prime ideal. If $\mathfrak{R}$ is of dimension one this is trivially true. Hence we proceed by induction, assuming it true for rings of dimension $n-1$, where n is the dimension of $\mathfrak{R}$.

Let, then, f be an irreducible element; we show that (f) is a prime ideal. By Krull's Theorem (see §1) the ideal (f) is of rank one, and therefore by Lemma 15 there exists a minimal basis $\{u_1, \cdots, u_n\}$ for $\mathfrak{m}$ such that $(f, u_2, \cdots, u_n)$ is a primary ideal belonging to $\mathfrak{m}$. In the unequal-characteristic case we may assume $u_2=p$. For (p) is prime, since p is an element of some minimal basis of $\mathfrak{m}$ (Theorem 14, corollary). So if p is in any minimal prime ideal of (f), then this prime ideal equals (p), hence $f\in(p)$, hence $(f)=(p)$, since f is irreducible. Thus it would be proved that (f) is prime. Hence it may be assumed that p is in no minimal prime ideal of (f), so that (f, p) is of rank two. Lemma 15, with $\mathfrak{a}=(f, p)$, $s=2$, implies the existence of a minimal basis $\{u_1, \cdots, u_n\}$ for $\mathfrak{m}$ such that $(f, p, u_3, \cdots, u_n)$ is primary for $\mathfrak{m}$ and $u_2=p$.

Let R be a coefficient ring in $\mathfrak{R}$. By Lemma 16, $\mathfrak{R}_0=R\{u_2, \cdots, u_n\}$ is a complete local ring concordant with $\mathfrak{R}$ and having $\mathfrak{m}_0=\mathfrak{R}_0\cdot(u_2, \cdots, u_n)$ as maximal ideal. This basis is minimal. It is clear that $\mathfrak{R}_0$ is isomorphic to a power series ring over a field (or a v-ring) in $n-1$ (or $n-2$) variables and that every element e of $\mathfrak{R}$ is of the form $\sum_{i=0}^{\infty}e_iu_1{}^i$, where e_i is in $\mathfrak{R}_0$ and is uniquely determined. Hence $\mathfrak{R}_0$ is a p-adic ring of dimension $n-1$ and u_1 is transcendental over $\mathfrak{R}_0$. Since by the induction hypothesis unique factorization holds in $\mathfrak{R}_0$ it must hold also in the polynomial ring $\mathfrak{R}_1=\mathfrak{R}_0[u_1]$.

Let $\mathfrak{R}'=\mathfrak{R}/\mathfrak{R}\cdot f$, $\mathfrak{m}'=\mathfrak{m}/\mathfrak{R}\cdot f$, and for $g\in\mathfrak{R}$ let g' denote its residue class modulo $\mathfrak{R}\cdot f$. Then $\mathfrak{R}'$ is a complete local ring with $\mathfrak{m}'=\mathfrak{R}'\cdot(u_1', \cdots, u_n')$ as maximal ideal; this basis need not be minimal. In the homomorphism of $\mathfrak{R}$ on $\mathfrak{R}'$, $\mathfrak{R}_0$ maps on a complete local ring $\mathfrak{R}_0'$ with maximal ideal $\mathfrak{m}_0'=\mathfrak{R}_0'\cdot(u_2', \cdots, u_n')$; this basis will turn out to be minimal. Now $\mathfrak{R}'\cdot\mathfrak{m}_0'$ is primary for $\mathfrak{m}'$ since $\mathfrak{R}\cdot(f, u_2, \cdots, u_n)$ is primary for $\mathfrak{m}$, and $\mathfrak{m}'=(u_1', \mathfrak{R}'\cdot\mathfrak{m}_0')$. Hence if $\mathfrak{R}'\cdot\mathfrak{m}_0'$ is of exponent k, then by Lemma 17, $\mathfrak{R}'=\mathfrak{R}_0'[u_1']$, and u_1' satisfies an equation

$$u_1'^k + a_1'u_1'^{k-1} + \cdots + a_k' = 0, \qquad a_i' \in \mathfrak{m}_0'.$$

If a_i is an element of $\mathfrak{m}_0$ which maps on a_i', then on placing

$$g = u_1^k + a_1u_1^{k-1} + \cdots + a_k,$$

we have that $g\in\mathfrak{R}\cdot f$, $g=hf$ where $h\in\mathfrak{R}$. Now h is a unit, for if not, then

$$h \equiv cu_1(\mathfrak{R}\cdot(u_2, \cdots, u_n)), \qquad c \in \mathfrak{R},$$

$$g \equiv cu_1f(\mathfrak{R}\cdot(u_2, \cdots, u_n)),$$
$$u_1^k \equiv cu_1f(\mathfrak{R}\cdot(u_2, \cdots, u_n)).$$

Since $u_1 \notin \mathfrak{R}\cdot(u_2, \cdots, u_n)$, which is prime, $u_1^{k-1} \in \mathfrak{R}\cdot(f, u_2, \cdots, u_n)$, so $u_1'^{k-1} \in \mathfrak{R}'\cdot(u_2', \cdots, u_n')$, contradicting the fact that this ideal is of exponent k. Thus h is a unit and hence g is an associate[26] of f and therefore is an irreducible element of $\mathfrak{R}$. But it is irreducible also in $\mathfrak{R}_1$, for since all the coefficients (except the first) of g are in $\mathfrak{m}_0$, the same would clearly be true for any factors of g in $\mathfrak{R}_1$. Thus these factors would be non-units in $\mathfrak{R}$, and we would have a contradiction to the fact that g is irreducible in $\mathfrak{R}$. Hence g is irreducible in $\mathfrak{R}_1$ and since unique factorization holds here, $\mathfrak{R}_1\cdot g$ is a prime ideal.

The mapping of $\mathfrak{R}$ on $\mathfrak{R}'$ induces a homomorphism of $\mathfrak{R}_1 = \mathfrak{R}_0[u_1]$ on $\mathfrak{R}_0'[u_1'] = \mathfrak{R}'$. The kernel of this homomorphism is clearly $\mathfrak{R}\cdot g \cap \mathfrak{R}_1$, since $\mathfrak{R}\cdot f = \mathfrak{R}\cdot g$. Now if $d \in \mathfrak{R}\cdot g \cap \mathfrak{R}_1$, then $d = eg$, where $e \in \mathfrak{R}$. Write $e = \sum_{i=0}^{\infty} e_i u_1^i$ $(e_i \in \mathfrak{R}_0)$, and expand eg in powers of u_1. If d is of degree r in u_1, then on comparing the coefficients of u_1^{i+k}, we have

$$e_i + a_1e_{i+1} + \cdots + a_ke_{i+k} = 0$$

provided $i+k>r$. Assuming that for some m it has been proved that $e_i \in \mathfrak{m}_0^m$ for $i>r-k$, this relation gives us $e_i \in \mathfrak{m}_0^{m+1}$ since all $a_j \in \mathfrak{m}_0$. Hence $e_i = 0$ for $i>r-k$, and $e \in \mathfrak{R}_1$. Thus $\mathfrak{R}\cdot g \cap \mathfrak{R}_1 = \mathfrak{R}_1\cdot g$ and the kernel in question is a prime ideal. This means that the ring $\mathfrak{R}'$ has no zero-divisors and hence the ideal $\mathfrak{R}\cdot f$ is prime.

The mapping of $\mathfrak{R}_0$ on $\mathfrak{R}_0'$ is an isomorphism since it is now clear that $\mathfrak{R}\cdot g \cap \mathfrak{R}_0 = (0)$. Thus $\mathfrak{R}_0'$ is of dimension $n-1$, and the same is therefore[23] true of $\mathfrak{R}'$; hence, finally, $\mathfrak{R}\cdot f$ has dimension $n-1$. The rest of the theorem is now obvious.

A consequence of this theorem is[21] that a p-adic ring is integrally closed.

THEOREM 19. *Let $\mathfrak{R}$ be a complete local ring without zero-divisors, and let $\mathfrak{p}$ and $\mathfrak{p}'$ be two prime ideals in $\mathfrak{R}$ such that $\mathfrak{p} \subset \mathfrak{p}'$. Then there exists at least one maximal chain of prime ideals between $\mathfrak{p}$ and $\mathfrak{p}'$, and any two such chains have the same length. If there is no prime ideal between $\mathfrak{p}$ and $\mathfrak{p}'$ then the ranks and dimensions of these ideals differ by unity. The sum of the rank and dimension of any prime ideal in $\mathfrak{R}$ equals the dimension of $\mathfrak{R}$.*

Proof. Let $\mathfrak{p}$ be of dimension s and rank t. We prove the existence of a prime ideal $\mathfrak{p}''$ of dimension $s-1$ such that $\mathfrak{p} \subset \mathfrak{p}'' \subseteq \mathfrak{p}'$.

Consider first the case $\mathfrak{p} = (0)$, so that $s = r$, where r is the dimension of $\mathfrak{R}$. The ring $\mathfrak{R}$ is by Theorem 16 integrally dependent on a p-adic ring $\mathfrak{R}_0$ of dimension r. Since $\mathfrak{p}' \neq (0)$ and $\mathfrak{R}$ has no zero-divisors, $\mathfrak{p}' \cap \mathfrak{R}_0 \neq (0)$ and hence con-

[26] That the element f has an associate of the form of g is, in effect, the Weierstrass preparation theorem.

tains an irreducible element f of $\mathfrak{R}_0$. By the previous theorem, $\mathfrak{R}_0 \cdot f$ is a prime ideal of dimension $r-1$; since $\mathfrak{R}_0 \cdot f \subseteq \mathfrak{p}' \cap \mathfrak{R}_0$ there exists (see Krull [5, Theorem 6]) a prime ideal $\mathfrak{p}''$ in $\mathfrak{R}$ such that $\mathfrak{p}'' \subseteq \mathfrak{p}'$, $\mathfrak{p}'' \cap \mathfrak{R}_0 = \mathfrak{R}_0 \cdot f$. This last relation shows[23] that $\mathfrak{p}''$ has dimension $r-1$, as was to be proved. In the general case, where $\mathfrak{p}$ is of dimension $s<r$, we observe that $\mathfrak{R}/\mathfrak{p}$ is a complete local ring of dimension s and hence $\mathfrak{p}'/\mathfrak{p}$ contains an $(s-1)$-dimensional prime ideal, whose inverse image in $\mathfrak{R}$ is then the required $\mathfrak{p}''$.

If $\mathfrak{p}'' \neq \mathfrak{p}'$, then we insert another prime ideal between them of dimension $s-2$. Continuing this process we eventually reach $\mathfrak{p}'$, and since the dimensions of successive prime ideals in this chain differ by unity, no further prime ideal can be inserted—that is, the chain is maximal. From the preceding construction it follows that if no prime ideal lies between $\mathfrak{p}$ and $\mathfrak{p}'$ then their dimensions differ by unity, and from this in turn it follows that all maximal chains between two fixed prime ideals are of the same length.

To prove that $s+t=r$, observe that there is a prime ideal chain

$$(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{t-1} \subset \mathfrak{p} \subset \mathfrak{p}'_{s-1} \subset \cdots \subset \mathfrak{p}'_1 \subset \mathfrak{p}'_0 = \mathfrak{m}.$$

This is a maximal chain between (0) and $\mathfrak{m}$ containing $s+t+1$ ideals. Since (0) is of dimension r there exists a maximal chain between these two containing $r+1$ ideals. Hence $r+1=s+t+1$. This completes the proof.

The first statement in this theorem is true even if $\mathfrak{R}$ has zero-divisors, whereas the other two statements remain true if it is assumed that the minimal prime ideals of (0) are all of the same dimension.

COROLLARY. *Let $\mathfrak{R}$ be a complete local ring without zero-divisors and $\mathfrak{a}$ an ideal of rank s. If $b_1, \cdots, b_t$ are any non-units of $\mathfrak{R}$, then the rank of $(\mathfrak{a}, b_1, \cdots, b_t)$ is at most $s+t$.*

Proof. It is clearly sufficient to consider the case $t=1$; write $b=b_1$. If $\mathfrak{p}$ is a prime ideal of $\mathfrak{a}$ of rank s, then $(\mathfrak{p}, b)$ is of rank at most $s+1$; for in $\mathfrak{R}/\mathfrak{p}$ $(\mathfrak{p}, b)/\mathfrak{p}$ is of rank at most one (by Krull's theorem, §1), hence $(\mathfrak{p}, b)$ is of rank at most $s+1$ by the present theorem. Since $(\mathfrak{p}, b) \supseteq (\mathfrak{a}, b)$, the latter also is of rank at most $s+1$.

THEOREM 20. *The quotient ring of a p-adic ring with respect to a prime ideal of rank r is an unramified regular local ring*[27] *of dimension r.*

Proof. Let $\mathfrak{R}$ be the p-adic ring, $\mathfrak{p}$ the prime ideal, $\mathfrak{S}$ the quotient ring, $\mathfrak{P} = \mathfrak{S} \cdot \mathfrak{p}$. The ring $\mathfrak{S}$ is clearly a local ring with maximal ideal $\mathfrak{P}$. This ideal has rank equal to that of $\mathfrak{p}$, so that $\mathfrak{S}$ is of dimension r. To show that it is regular we show that $\mathfrak{P}$ has a basis of r elements.

[27] If we adopt for analytic varieties a definition similar to that of Zariski [13, p. 199] for algebraic varieties, then this theorem as applied to power series rings over a field has the following geometric interpretation: An irreducible analytic variety is a simple subvariety of the containing space.

Assume first that either we have the equal-characteristic case or that in the contrary case, $p \notin \mathfrak{p}$. Let $\mathfrak{R}$ be of dimension n; we may suppose $0<r<n$, since the cases $r=0$ or n are trivial. Applying Lemma 15 to $\mathfrak{a}=\mathfrak{p}$ we obtain a minimal basis $\{u_1, \cdots, u_n\}$ for $\mathfrak{m}$ such that $(\mathfrak{p}, u_{r+1}, \cdots, u_n)$ is a primary ideal belonging to $\mathfrak{m}$. In the unequal-characteristic case we may suppose in addition that $u_{r+1}=p$. For since we have assumed that $p \notin \mathfrak{p}$, the ideal $(\mathfrak{p}, p)$ is of rank not less than $r+1$; we apply Lemma 15, with $\mathfrak{a}=(\mathfrak{p}, p)$, obtaining $\mathfrak{m}=(u_1, \cdots, u_n)$, $(\mathfrak{p}, p, u_{r+2}, \cdots, u_n)$ is primary for $\mathfrak{m}$, p occurs among the u_i. Now p cannot be one of $u_{r+2}, \cdots, u_n$, for if it were, then by the corollary to the previous theorem $(\mathfrak{p}, u_{r+2}, \cdots, u_n)$ would have rank at most $n-1$, whereas its rank is actually n since it is primary for $\mathfrak{m}$. This contradiction shows that p is one of $u_1, \cdots, u_{r+1}$, and we suppose $p=u_{r+1}$.

Let R be a coefficient ring in $\mathfrak{R}$. Then $\mathfrak{R}_0=R\{u_{r+1}, \cdots, u_n\}$ is a p-adic ring of dimension $n-r$ and maximal ideal $\mathfrak{m}_0=\mathfrak{R}_0\cdot(u_{r+1}, \cdots, u_n)$, and $u_1, \cdots, u_r$ are algebraically independent over $\mathfrak{R}_0$ (cf. proof of Theorem 18). Let $\mathfrak{S}_1$ be the polynomial ring $\mathfrak{K}_0[u_1, \cdots, u_r]$, where $\mathfrak{K}_0$ is the quotient field of $\mathfrak{R}_0$.

Let $\mathfrak{R}'=\mathfrak{R}/\mathfrak{p}$, $\mathfrak{m}'=\mathfrak{m}/\mathfrak{p}$, and let $\mathfrak{R}_0'$ and $\mathfrak{m}_0'$ be the respective maps of $\mathfrak{R}_0$ and $\mathfrak{m}_0$ in the homomorphism of $\mathfrak{R}$ on $\mathfrak{R}'$. As in the proof of Theorem 18 we obtain that $\mathfrak{R}'\cdot\mathfrak{m}_0'$ is primary for $\mathfrak{m}'$ and hence $\mathfrak{R}'$ is integrally dependent on $\mathfrak{R}_0'$. Now we assert that

$$\mathfrak{R}' = \mathfrak{R}_0'[u_1', \cdots, u_r'], \tag{23}$$

where primes indicate residue classes modulo $\mathfrak{p}$. This can be seen by repeated application of Lemma 17. Namely, let $\mathfrak{R}_j=R\{u_{r-j+1}, \cdots, u_n\}$ $(j=0, 1, \cdots, r)$, so that $\mathfrak{R}_j$ is a complete local ring and $\mathfrak{R}_r=\mathfrak{R}$. Then $\mathfrak{R}_j$ maps onto a subring $\mathfrak{R}_j'$ of $\mathfrak{R}'$ which is a complete local ring with maximal ideal $\mathfrak{m}_j'=(u_{r-j+1}', \cdots, u_n')$. Now $\mathfrak{R}_j'$ is integrally dependent on $\mathfrak{R}_{j-1}'$ and hence $\mathfrak{R}_j'\cdot\mathfrak{m}_{j-1}'$ is primary for $\mathfrak{m}_j'$; moreover, $\mathfrak{m}_j'=(u_{r-j+1}', \mathfrak{R}_j'\cdot\mathfrak{m}_{j-1}')$. Hence by Lemma 17, $\mathfrak{R}_j'=\mathfrak{R}_{j-1}'[u_{r-j+1}']$. This holds for $j=1, \cdots, r$, and so (23) follows. In the mapping of $\mathfrak{R}$ on $\mathfrak{R}'$, $\mathfrak{R}_0[u_1, \cdots, u_r]$ maps on $\mathfrak{R}'$, in view of (23). Hence every element of $\mathfrak{R}$ is congruent modulo $\mathfrak{p}$ to an element of $\mathfrak{R}_0[u_1, \cdots, u_r]$.

Since u_i' is integral over $\mathfrak{R}_0'$, it follows from Theorem 7 that for $i=1, \cdots, r$, $\mathfrak{R}_0'[u_i']$ is a complete local ring, and it is clear that its maximal ideal is generated by $u_i', u_{r+1}', \cdots, u_n'$. Lemma 17 implies that u_i' satisfies over $\mathfrak{R}_0'$ a monic equation with coefficients (other than the first) in $\mathfrak{m}_0'$. Hence $\mathfrak{p}$ contains a polynomial f_i in $\mathfrak{R}_0[u_i]$, where

$$f_i = u_i^{h(i)} + a_{i1}u_i^{h(i)-1} + \cdots + a_{ih(i)}, \qquad a_{ij} \in \mathfrak{m}_0, \ i = 1, \cdots, r.$$

If $\mathfrak{a}=\mathfrak{R}\cdot(f_1, \cdots, f_r)$, then $(\mathfrak{a}, u_{r+1}, \cdots, u_n)$ contains $u_i^{h(i)}$, $i=1, \cdots, r$, hence is a primary ideal belonging to $\mathfrak{m}$. The reasoning of the previous paragraph for the ideal $\mathfrak{p}$ can now be repeated for $\mathfrak{a}$, and we obtain: Every element of $\mathfrak{R}$ is congruent modulo $\mathfrak{a}$ to an element of $\mathfrak{R}_0[u_1, \cdots, u_r]$.

Since $\mathfrak{R}'$ is integrally dependent on $\mathfrak{R}_0'$ and the former has dimension $n-r$ (by Theorem 19), so does[23] the latter. In the mapping of $\mathfrak{R}$ on $\mathfrak{R}'$, $\mathfrak{R}_0$ goes into $\mathfrak{R}_0'$, and since $\mathfrak{R}_0$ also has dimension $n-r$ the mapping of $\mathfrak{R}_0$ on $\mathfrak{R}_0'$ must be an isomorphism. Thus $\mathfrak{p} \cap \mathfrak{R}_0 = (0)$, hence $\mathfrak{K}_0 \subset \mathfrak{S}$, $\mathfrak{S}_1 \subset \mathfrak{S}$; let $\mathfrak{p}_1 = \mathfrak{P} \cap \mathfrak{S}_1$. Since $\mathfrak{a} \subseteq \mathfrak{p}$, the preceding paragraph shows that every element of $\mathfrak{p}$ is congruent modulo $\mathfrak{a}$ to an element of $\mathfrak{p} \cap \mathfrak{R}_0[u_1, \cdots, u_r]$. This latter element is in $\mathfrak{p}_1$. Hence every element of $\mathfrak{P}$ is congruent modulo $\mathfrak{S} \cdot \mathfrak{a}$ to an element of $\mathfrak{S} \cdot \mathfrak{p}_1$. But since each generator f_i of $\mathfrak{a}$ is in $\mathfrak{p}_1$, $\mathfrak{S} \cdot \mathfrak{a} \subseteq \mathfrak{S} \cdot \mathfrak{p}_1$, hence $\mathfrak{P} = \mathfrak{S} \cdot \mathfrak{p}_1$. It is thus sufficient to show that $\mathfrak{p}_1$ has a basis of r elements. As an ideal in the polynomial ring $\mathfrak{K}_0[u_1, \cdots, u_r]$, $\mathfrak{p}_1$ is of dimension zero over $\mathfrak{K}_0$, since it contains the polynomials f_i. The proof is then complete, since it is known[28] that a zero-dimensional prime ideal in a ring of polynomials in r variables has a basis of r elements.

Thus $\mathfrak{S}$ is regular and since it contains the field $\mathfrak{K}_0$, it is certainly unramified.

Now suppose that—in the unequal-characteristic case—$p \in \mathfrak{p}$. Since $\mathfrak{R}$ is unramified $\mathfrak{R} \cdot p$ is prime, and since $\mathfrak{R} \cdot p \subseteq \mathfrak{p}$, $\mathfrak{S} \cdot p$ is a prime ideal in $\mathfrak{S}$. If T is the homomorphism of $\mathfrak{S}$ on $\mathfrak{S}/\mathfrak{S} \cdot p$, then T maps $\mathfrak{R}$ on a subring $\mathfrak{R}T$ of $\mathfrak{S}T$. The kernel of the homomorphism of $\mathfrak{R}$ is $\mathfrak{R} \cdot p$, and since p can be taken as an element of a minimal basis of $\mathfrak{m}$, it follows that $\mathfrak{R}T$ is a regular local ring by Theorem 14, corollary; moreover it is clearly complete and of characteristic p. Now $\mathfrak{S}T$ is a local ring with maximal ideal $\mathfrak{P}T$; in fact $\mathfrak{S}T$ is the quotient ring of $\mathfrak{R}T$ with respect to $\mathfrak{p}T$, and this ideal is of rank $r-1$ by the previous theorem. Hence by the case already considered $\mathfrak{S}T$ is a regular local ring of dimension $r-1$, so that $\mathfrak{P}T$ has a basis of $r-1$ elements. Since $\mathfrak{P}T = \mathfrak{P}/\mathfrak{S} \cdot p$, $\mathfrak{P}$ has a basis of r elements, one of which is p. Hence $\mathfrak{S}$ is regular and unramified.

We are now in a position to extend to arbitrary regular local rings a well known theorem of Macaulay [8, p. 49] on ideals in a polynomial ring.

Definition. An ideal $\mathfrak{a}$ in a regular local ring $\mathfrak{R}$ is *unmixed* if all of its associated prime ideals are of the same rank.

Since $\mathfrak{R}$ is regular, this is equivalent to requiring that all the prime ideals of $\mathfrak{a}$ have the same dimension. For Krull [7, Theorem 11] has proved that in a regular local ring, the sum of the rank and dimension of any ideal is equal to the dimension of the ring. We shall use this fact only for *complete* regular local rings, in which case the statement is part of Theorem 19.

Theorem 21. *Let $\mathfrak{R}$ be a regular local ring and $\mathfrak{a} = (a_1, \cdots, a_r)$ an ideal in $\mathfrak{R}$ having a basis of r elements. If $\mathfrak{a}$ is of rank r, then $\mathfrak{a}$ is unmixed.*

Proof. By the theorem of Krull quoted in §1, every minimal prime ideal

[28] Zariski [14, p. 541, Lemma 9].

of $\mathfrak{a}$ has rank at most r. Since by the hypothesis none can have rank less than r, all the minimal prime ideals of $\mathfrak{a}$ have rank r. The prime ideals of $\mathfrak{a}$ which are of rank greater than r are those and only those which are not minimal; we show that they do not exist.

Let $\mathfrak{R}$ be of dimension n. We consider first the case where $\mathfrak{R}$ is unramified. We then proceed by induction on r. For $r=1$ the theorem follows from the well known fact [4, p. 106] that in an integrally closed ring([21]) all the prime ideals of a principal ideal are minimal prime ideals in the ring, hence are of rank one. Assume then that the theorem is proved for $r-1$ basis elements.

It is sufficient to prove the theorem for r basis elements for the case where $\mathfrak{R}$ is complete. For if this case is proved, let $\mathfrak{R}^*$ be the completion of $\mathfrak{R}$. Then $\mathfrak{R}^*$ is regular and unramified; moreover it is of dimension n, in view of Theorem 14 and of the fact (Theorem 2) that a minimal basis for $\mathfrak{m}$ is also one for $\mathfrak{m}^*$. Now $\mathfrak{R}^*\cdot\mathfrak{a}=\mathfrak{R}^*\cdot(a_1, \cdots, a_r)$ is of rank r at most, by Krull's theorem; actually its rank is exactly r. For by Lemma 15 there exist elements $u_{r+1}, \cdots, u_n$ such that $(\mathfrak{a}, u_{r+1}, \cdots, u_n)$ is primary for $\mathfrak{m}$. By Theorem 2, $(\mathfrak{R}^*\cdot\mathfrak{a}, u_{r+1}, \cdots, u_n)$ is primary for $\mathfrak{m}^*$, hence is of rank n, and by the corollary to Theorem 19 the rank of $\mathfrak{R}^*\cdot\mathfrak{a}$ must be at least r.

Since we are assuming the theorem (for r basis elements) for complete rings, $\mathfrak{R}^*\cdot\mathfrak{a}$ is unmixed; that is,

$$\mathfrak{R}^*\cdot\mathfrak{a} = \mathfrak{q}_1^* \cap \cdots \cap \mathfrak{q}_h^*;$$

where $\mathfrak{q}_i^*$ is a primary ideal in $\mathfrak{R}^*$ of rank r. If $\mathfrak{q}_i=\mathfrak{q}_i^*\cap\mathfrak{R}$, then

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$$

since $\mathfrak{R}^*\cdot\mathfrak{a}\cap\mathfrak{R}=\mathfrak{a}$. As for $\mathfrak{a}$ above it follows that the rank of $\mathfrak{R}^*\cdot\mathfrak{q}_i$ is at least as great as that of $\mathfrak{q}_i$. Thus

$$r = \text{rank } \mathfrak{a} \leqq \text{rank } \mathfrak{q}_i \leqq \text{rank } \mathfrak{R}^*\cdot\mathfrak{q}_i \leqq \text{rank } \mathfrak{q}_i^* = r;$$

so the rank of $\mathfrak{q}_i$ is r, and $\mathfrak{a}$ is unmixed.

Thus we may assume $\mathfrak{R}$ is complete. If $\mathfrak{a}$ is mixed, then suppose that $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$ of rank $s>r$. Let $\mathfrak{R}'$ be the quotient ring of $\mathfrak{R}$ with respect to $\mathfrak{p}$; then by the previous theorem $\mathfrak{R}'$ is an unramified regular local ring of dimension s. If $\mathfrak{a}'=\mathfrak{R}'\cdot\mathfrak{a}$ and $\mathfrak{p}'=\mathfrak{R}'\cdot\mathfrak{p}$, then $\mathfrak{a}'=\mathfrak{R}'\cdot(a_1, \cdots, a_r)$ is of rank r and $\mathfrak{p}'$ (which is of rank s) is a prime ideal of $\mathfrak{a}'$. This must be proved impossible. Writing $\mathfrak{R}$, $\mathfrak{a}$, and $\mathfrak{m}$ for $\mathfrak{R}'$, $\mathfrak{a}'$, and $\mathfrak{p}'$, we thus have the following: *In the s-dimensional ring* $\mathfrak{R}$, *the ideal* $\mathfrak{a}=\mathfrak{R}\cdot(a_1, \cdots, a_r)$ *is of rank r, where* $r<s$; *to prove that the maximal ideal* $\mathfrak{m}$ *of* $\mathfrak{R}$ *does not belong to* $\mathfrak{a}$. By reasoning similar to the above it is sufficient to prove this statement for the case where $\mathfrak{R}$ is complete. To prove this it is sufficient to show that $\mathfrak{a}:\mathfrak{m}=\mathfrak{a}$.

If $\mathfrak{b}=(a_1, \cdots, a_{r-1})$, then $\mathfrak{b}$ is of rank at most $r-1$; if its rank were less, then by Theorem 19, corollary, $(\mathfrak{b}, a_r)=\mathfrak{a}$ would have rank less than r, contradicting the hypothesis. Thus $\mathfrak{b}$ is of rank $r-1$ and is therefore unmixed by the induction assumption. We assert that there exists a minimal basis $\{u_1, \cdots, u_s\}$ for $\mathfrak{m}$ such that u_1 is in no prime ideal of $\mathfrak{a}$ of rank r and in no prime ideal of $\mathfrak{b}$ of rank $r-1$ (hence, since $\mathfrak{b}$ is unmixed, in no prime ideal of $\mathfrak{b}$). Namely, take this set of prime ideals and after deleting all those which are contained in any other, denote those that remain by $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ (cf. proof of Lemma 15). Since $r<s$, no $\mathfrak{p}_i$ can be $\mathfrak{m}$. If $\{u_1, \cdots, u_s\}$ is an arbitrary minimal basis of $\mathfrak{m}$, then there is a u_i—say u_1—which is not in $\mathfrak{p}_1$. Renumber the $\mathfrak{p}_i$ so that $u_1 \notin \mathfrak{p}_1, \cdots, \mathfrak{p}_k$, $u_1 \in \mathfrak{p}_{k+1}, \cdots, \mathfrak{p}_h$ $(1 \leqq k \leqq h)$. For each $j=k+1, \cdots, h$, let $m(j)$ be such that $u_{m(j)} \notin \mathfrak{p}_j$ and let c_j be in $\bigcap_{t \neq j} \mathfrak{p}_t$ but not in $\mathfrak{p}_j$. Place $u_1' = u_1 + \sum_{j=k+1}^{h} c_j u_{m(j)}$; then $\{u_1', u_2, \cdots, u_s\}$ is the required basis. Moreover, if $\mathfrak{R}$ presents the equal-characteristic case, so does $\mathfrak{R}/(u_1')$, which is therefore unramified.

But if $\mathfrak{R}$ presents the unequal-characteristic case, we proceed as follows: if p is in no $\mathfrak{p}_i$, we may assume $u_1 = p$, so that $\mathfrak{R}/(u_1)$ is of characteristic p and hence unramified. If p is in some $\mathfrak{p}_i$—say in $\mathfrak{p}_1$—we may assume $u_s = p$ and proceed as above. Then $\mathfrak{R}/(u_1')$ is unramified unless $p \in (u_1', \mathfrak{m}^2)$. Since $u_1' \equiv u_1(\mathfrak{m}^2)$, this would imply $u_s \in (u_1, \mathfrak{m}^2)$, contradicting Lemma 2. Writing u_1 for u_1' we have, finally, a minimal basis as stated above such that $\mathfrak{R}/(u_1)$ is unramified.

The ideal $(\mathfrak{b}, u_1)$ has rank r, hence dimension $n-r$; hence in the $(n-1)$-dimensional p-adic ring $\mathfrak{R}/(u_1)$ the ideal $(\mathfrak{b}, u_1)/(u_1)$ has dimension $n-r$ and rank $r-1$. Since it has a basis of $r-1$ elements it is unmixed by the induction hypothesis; thus also $(\mathfrak{b}, u_1)$ is unmixed. No prime ideal $\mathfrak{p}$ of $(\mathfrak{b}, u_1)$ can contain a_r, for if it did, then $\mathfrak{a} = (\mathfrak{b}, a_r) \subseteq \mathfrak{p}$, hence $\mathfrak{p}$ contains a minimal prime ideal $\mathfrak{p}'$ of $\mathfrak{a}$. Since both $\mathfrak{p}$ and $\mathfrak{p}'$ are of rank r, they are equal, and thus u_1 is in a prime ideal of $\mathfrak{a}$ of rank r, contrary to selection.

Suppose, now, that $c \in \mathfrak{a} : \mathfrak{m}$; we shall show that $c \in \mathfrak{a}$. Since $cu_1 \in \mathfrak{a} = (\mathfrak{b}, a_r)$, there is a d in $\mathfrak{R}$ such that $cu_1 \equiv da_r(\mathfrak{b})$. Hence $da_r \in (\mathfrak{b}, u_1)$, and since a_r is in no prime ideal of $(\mathfrak{b}, u_1)$, $d \in (\mathfrak{b}, u_1)$. Combining with the above, $cu_1 \in (\mathfrak{b}, u_1 a_r)$. Hence for some e in $\mathfrak{R}$,

$$cu_1 \equiv eu_1 a_r(\mathfrak{b}), \qquad u_1(c - ea_r) \equiv 0(\mathfrak{b}).$$

Since u_1 is in no prime ideal of $\mathfrak{b}$, $c - ea_r \in \mathfrak{b}$, $c \in \mathfrak{a}$, as was to be proved.

Now consider the case where $\mathfrak{R}$ is ramified. As before we may assume that $\mathfrak{R}$ is complete. By Corollary 3 to Theorem 15, $\mathfrak{R}$ is the homomorphic image of a p-adic ring $\mathfrak{S}$ in which the kernel is a prime principal ideal $\mathfrak{S} \cdot F$. If $A_1, \cdots, A_r$ are elements of $\mathfrak{S}$ which map into $a_1, \cdots, a_r$ respectively, then $(F, A_1, \cdots, A_r)$ is the complete inverse image in $\mathfrak{S}$ of $\mathfrak{a}$ and moreover has rank $r+1$ (Theorem 19). Since the theorem is proved for the unramified ring $\mathfrak{S}$, $(F, A_1, \cdots, A_r)$ is unmixed and hence also $\mathfrak{a}$ is unmixed. The proof is now complete in all cases.

9. **Applications. The ramification order.** We now return to the question

stated at the end of Part I. For this purpose we need a preliminary result, which is of some interest in itself.

THEOREM 22. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be two regular local rings with maximal ideals* $\mathfrak{m}$ *and* $\mathfrak{M}$ *respectively and assume that* $\mathfrak{S}$ *is integrally dependent on* $\mathfrak{R}$; *let* $\mathfrak{m}=\mathfrak{R}\cdot(u_1, \cdots, u_n)$, *where the indicated basis is minimal. If* ψ *is a form in* n *variables with coefficients in* $\mathfrak{S}$ *such that*

$$\psi(u_1, \cdots, u_n) = 0, \tag{24}$$

then all the coefficients of ψ *are in* $\mathfrak{S}\cdot\mathfrak{m}$.

Proof. Since $\mathfrak{S}$ is integral over $\mathfrak{R}$, it has the same dimension([23]) as $\mathfrak{R}$, namely n; moreover, $\mathfrak{S}\cdot\mathfrak{m}$ is a primary ideal belonging to $\mathfrak{M}$.

We begin the proof by showing that the coefficient c of u_1^k (where k is the degree of ψ) is in $\mathfrak{S}\cdot\mathfrak{m}$. From (24) it follows that

$$cu_1^k \in \mathfrak{S}\cdot(u_2, \cdots, u_n). \tag{25}$$

The ideal $\mathfrak{S}\cdot(u_2, \cdots, u_n)$ has rank $n-1$ for if $\mathfrak{P}$ is one of its prime ideals then $\mathfrak{P}\cap\mathfrak{R}\supseteq\mathfrak{R}\cdot(u_2, \cdots, u_n)$, so that the rank of $\mathfrak{P}\cap\mathfrak{R}$ is at least $n-1$, and so the same([23]) is true of $\mathfrak{P}$. Thus the rank of $\mathfrak{S}\cdot(u_2, \cdots, u_n)$ is at least $n-1$; it is at most $n-1$, by Krull's theorem (§1). By Theorem 21, $\mathfrak{S}\cdot(u_2, \cdots, u_n)$ is unmixed and of rank $n-1$. Hence every associated prime ideal $\mathfrak{P}$ has rank $n-1$, hence so does $\mathfrak{P}\cap\mathfrak{R}$, hence $\mathfrak{P}\cap\mathfrak{R}=\mathfrak{R}\cdot(u_2, \cdots, u_n)$. Thus u_1 is in no prime ideal of $\mathfrak{S}\cdot(u_2, \cdots, u_n)$, and so (25) implies that $c\in\mathfrak{S}\cdot\mathfrak{m}$, as was to be proved.

The proof is concluded as in Theorem 14. Let $u_i=\sum_{j=1}^{n} c_{ij}v_j$, where $c_{ij}\in\mathfrak{R}$, $|c_{ij}|\notin\mathfrak{m}$; then $\mathfrak{m}=\mathfrak{R}\cdot(v_1, \cdots, v_n)$, and substituting in (24), we obtain

$$\psi(u_1, \cdots, u_n) = \phi(v_1, \cdots, v_n) = 0.$$

Here ϕ is a form of degree k in which the coefficient of v_1^k is $\psi(c_{11}, \cdots, c_{n1})$ By what has just been proved

$$\psi(c_{11}, \cdots, c_{n1}) \equiv 0(\mathfrak{S}\cdot\mathfrak{m}).$$

Since $\mathfrak{S}\cdot\mathfrak{m}\cap\mathfrak{R}=\mathfrak{m}$, the ring $\mathfrak{S}/\mathfrak{S}\cdot\mathfrak{m}$ may be considered to contain the residue field $\mathrm{P}=\mathfrak{R}/\mathfrak{m}$. Denoting by $\bar{\psi}$ the form obtained from ψ by replacing each coefficient by its residue class modulo $\mathfrak{S}\cdot\mathfrak{m}$, and denoting by $\bar{c}_{ij}$ the residue class of c_{ij}, we obtain $\bar{\psi}(\bar{c}_{11}, \cdots, \bar{c}_{n1})=0$. The coefficients of $\bar{\psi}$ are in $\mathfrak{S}/\mathfrak{S}\cdot\mathfrak{m}$ and this relation holds for every choice of the elements $\bar{c}_{11}, \cdots, \bar{c}_{n1}$ in the subring P. If, now, P has infinitely many elements, then all the coefficients of $\bar{\psi}$ are zero([29]), hence all the coefficients of ψ are in $\mathfrak{S}\cdot\mathfrak{m}$, and the theorem is proved if P is infinite.

[29] *If T is a ring containing an infinite field* P *whose identity is also the identity in T, then any polynomial $f(z_1, \cdots, z_n)$ over T which vanishes for all values of the z_i in* P *is the zero polynomial.* The proof is the same as the usual one for the case where T is a field, if one takes into account the fact that a nonzero element in P cannot be a zero-divisor in T.

To complete the proof for the case when $\mathfrak{R}$ has a finite residue field, adjoin an indeterminate z to $\mathfrak{S}$, and form the rings $\mathfrak{S}'=\mathfrak{S}[z]$ and $\mathfrak{R}'=\mathfrak{R}[z]$. Let $\mathfrak{S}''$ and $\mathfrak{R}''$ be the quotient rings of $\mathfrak{S}'$ and $\mathfrak{R}'$ with respect to $\mathfrak{S}'\cdot\mathfrak{M}$ and $\mathfrak{R}'\cdot\mathfrak{m}$ respectively. As in the proof of Theorem 14 it follows that $\mathfrak{S}''$ and $\mathfrak{R}''$ are regular local rings of dimension n with respective maximal ideals $\mathfrak{S}''\cdot\mathfrak{M}$ and $\mathfrak{R}''\cdot\mathfrak{m}$. Since $\mathfrak{S}\cdot\mathfrak{m}$ is primary for $\mathfrak{M}$ it follows from Lemma 14 that $\mathfrak{S}'\cdot(\mathfrak{S}\cdot\mathfrak{m})$—that is, $\mathfrak{S}'\cdot\mathfrak{m}$—is primary for $\mathfrak{S}'\cdot\mathfrak{M}$, and $\mathfrak{S}'\cdot\mathfrak{m}\cap\mathfrak{S}=\mathfrak{S}\cdot\mathfrak{m}$. From the properties of quotient rings it follows that $\mathfrak{S}''\cdot(\mathfrak{S}'\cdot\mathfrak{m})$—that is, $\mathfrak{S}''\cdot\mathfrak{m}$—is primary for $\mathfrak{S}''\cdot(\mathfrak{S}'\cdot\mathfrak{M})=\mathfrak{S}''\cdot\mathfrak{M}$, and $\mathfrak{S}''\cdot\mathfrak{m}\cap\mathfrak{S}'=\mathfrak{S}'\cdot\mathfrak{m}$. Hence, finally,

$$\mathfrak{S}''\cdot\mathfrak{m}\cap\mathfrak{S}=\mathfrak{S}\cdot\mathfrak{m}.$$

Assuming for the moment that $\mathfrak{S}''$ is integrally dependent on $\mathfrak{R}''$, we conclude that the present theorem is true for these rings since the residue field of $\mathfrak{R}''$ is infinite. If, then, (24) holds for a form ψ whose coefficients are in $\mathfrak{S}$, then since $\mathfrak{R}''\cdot\mathfrak{m}=\mathfrak{R}''\cdot(u_1,\cdots,u_n)$, these coefficients must be in $\mathfrak{S}''\cdot(\mathfrak{R}''\cdot\mathfrak{m})$—that is, in $\mathfrak{S}''\cdot\mathfrak{m}$. In view of the relation above, the coefficients must be in $\mathfrak{S}\cdot\mathfrak{m}$, as was to be proved.

It remains to show that $\mathfrak{S}''$ is integral over $\mathfrak{R}''$. Suppose $f(z)/g(z)\in\mathfrak{S}''$, where f, $g\in\mathfrak{S}'$, $g\notin\mathfrak{S}'\cdot\mathfrak{M}$. If there is a polynomial $h(z)$ in $\mathfrak{S}'$ such that hg is in $\mathfrak{R}'$ but not in $\mathfrak{R}'\cdot\mathfrak{m}$, then $f/g=hf/hg$ is integral over $\mathfrak{R}''$ since $\mathfrak{S}'$ is integrally dependent on $\mathfrak{R}'$.

Such a polynomial h must exist unless

$$\mathfrak{S}'\cdot g\cap\mathfrak{R}'\subseteq\mathfrak{R}'\cdot\mathfrak{m}.$$

If this holds then there is a prime ideal $\mathfrak{P}'$ in $\mathfrak{S}'$ such that[30]

$$\mathfrak{S}'\cdot g\subseteq\mathfrak{P}',\qquad \mathfrak{P}'\cap\mathfrak{R}'=\mathfrak{R}'\cdot\mathfrak{m}.$$

Thus $\mathfrak{P}'\supseteq\mathfrak{S}'\cdot(\mathfrak{R}'\cdot\mathfrak{m})=\mathfrak{S}'\cdot\mathfrak{m}$, hence $\mathfrak{P}'$ contains the corresponding prime ideal $\mathfrak{S}'\cdot\mathfrak{M}$. But since clearly also $\mathfrak{S}'\cdot\mathfrak{M}$ contracts to $\mathfrak{R}'\cdot\mathfrak{m}$, we have[20] $\mathfrak{P}'=\mathfrak{S}'\cdot\mathfrak{M}$. Hence $g\in\mathfrak{S}'\cdot\mathfrak{M}$, which is false. The theorem is thus completely proved.

Definition. Let $\mathfrak{R}$ and $\mathfrak{S}$ be regular local rings of the same dimension, $\mathfrak{R}\subseteq\mathfrak{S}$. If $\mathfrak{S}\cdot\mathfrak{m}$ is a primary ideal belonging to $\mathfrak{M}$, then the length of $\mathfrak{S}\cdot\mathfrak{m}$ is called the *ramification degree* of $\mathfrak{S}$ with respect to $\mathfrak{R}$.

We observe that if $\mathfrak{R}$ and $\mathfrak{S}$ are regular local rings and if $\mathfrak{S}$ is unramified with respect to $\mathfrak{R}$ according to the definition of §3, then the ramification degree is unity. For since $\mathfrak{m}$ and $\mathfrak{M}$ have a minimal basis in common it follows from Theorem 14 that $\mathfrak{R}$ and $\mathfrak{S}$ are of the same dimension; since $\mathfrak{S}\cdot\mathfrak{m}=\mathfrak{M}$, the length of $\mathfrak{S}\cdot\mathfrak{m}$ is unity. Conversely, if the ramification degree is unity, let $\mathfrak{m}=\mathfrak{R}\cdot(u_1,\cdots,u_n)$ and let this basis be minimal. Since

[30] Cohen and Seidenberg [2, Theorem 3].

$\mathfrak{M}=\mathfrak{S}\cdot\mathfrak{m}=\mathfrak{S}\cdot(u_1, \cdots, u_n)$, this basis for $\mathfrak{M}$ must also be minimal since $\mathfrak{S}$ has dimension n. To prove equation (14), it is enough to show that if an element c of $\mathfrak{R}$ is in $\mathfrak{m}^k$ but not in $\mathfrak{m}^{k+1}$, then it is not in $\mathfrak{M}^{k+1}$. We are given $c=\phi(u_1, \cdots, u_n)$, where ϕ is a form of degree k in n variables with coefficients in $\mathfrak{R}$. If $c\in\mathfrak{M}^{k+1}$ then since $\mathfrak{S}$ is regular the coefficients of ϕ are in $\mathfrak{M}$, hence in $\mathfrak{m}$. But this implies $c\in\mathfrak{m}^{k+1}$, which is a contradiction.

Theorem 23. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be complete regular local rings with quotient fields $\mathfrak{K}$ and $\mathfrak{L}$ and residue fields* P *and* Σ, *respectively; assume also that $\mathfrak{R}\subseteq\mathfrak{S}$, so that $\mathfrak{K}\subseteq\mathfrak{L}$. If $\mathfrak{S}\cdot\mathfrak{m}$ is a primary ideal belonging to $\mathfrak{M}$ and if Σ is a finite algebraic extension of* P, *then $\mathfrak{S}$ is a finite $\mathfrak{R}$-module and*

$$[\mathfrak{L}:\mathfrak{K}] = \lambda[\Sigma:\mathrm{P}], \tag{26}$$

where λ is the ramification degree of $\mathfrak{S}$ with respect to $\mathfrak{R}$.

This relation is a generalization to regular local rings of arbitrary dimension of a theorem well known for dimension one—that is, for discrete valuation rings.

Proof. We make use throughout of the proof and notations of Theorem 8. Since $\mathfrak{S}\cdot\mathfrak{m}$ is assumed primary for $\mathfrak{M}$, we have that $\mathfrak{M}\cap\mathfrak{R}=\mathfrak{m}$, so that P may be considered a subfield of Σ; thus the condition on the residue fields has a meaning. By the quoted theorem $\mathfrak{S}$ is a finite $\mathfrak{R}$-module and hence these two rings have the same dimension; it is thus permissible to speak of the ramification degree. An $\mathfrak{R}$-basis for $\mathfrak{S}$ is formed by the elements p_iq_j $(i=1, \cdots, \mu; j=1, \cdots, \lambda)$, where $\mu=[\Sigma:\mathrm{P}]$. Since $\mathfrak{S}$ is integrally closed in $\mathfrak{L}$, every element of $\mathfrak{L}$ is the quotient of an element of $\mathfrak{S}$ by an element of $\mathfrak{R}$, hence every element of $\mathfrak{L}$ is a linear combination of the p_iq_j with coefficients in $\mathfrak{K}$. Thus $[\mathfrak{L}:\mathfrak{K}]\leqq\lambda\mu$. To prove equality we show that these elements are linearly independent.

Suppose, therefore, that there is a relation

$$\sum_{i=1}^{\mu}\sum_{j=1}^{\lambda} c_{ij}(p_iq_j) = 0, \qquad c_{ij}\in\mathfrak{K}. \tag{27}$$

We may assume $c_{ij}\in\mathfrak{R}$. If not all c_{ij} are zero, then there is an integer k such that all c_{ij} are in $\mathfrak{m}^k$ but not all in $\mathfrak{m}^{k+1}$. Let $\mathfrak{m}=\mathfrak{R}\cdot(u_1, \cdots, u_n)$, and let $v_1, \cdots, v_N$ be the distinct power products of the u_i of degree k. Then $c_{ij}=\sum_{h=1}^{N}c_{ijh}v_h$, $c_{ijh}\in\mathfrak{R}$. Substituting in (27), we obtain

$$\sum_{h=1}^{N} v_h \sum_{i,j} c_{ijh}(p_iq_j) = 0.$$

By the previous theorem we may conclude that

$$\sum_{i,j} c_{ijh}(p_iq_j) \equiv 0(\mathfrak{S}\cdot\mathfrak{m}), \qquad h = 1, \cdots, N.$$

Considering this relation for a fixed h we show by induction on j that all the c_{ijh} are in $\mathfrak{m}$. Assuming this proved for $j=1, \cdots, \nu-1$ $(1 \leqq \nu \leqq \lambda)$, we have

$$\sum_{j=\nu}^{\lambda} q_j\left(\sum_{i=1}^{\mu} c_{ijh}p_i\right) \equiv 0(\mathfrak{S}\cdot\mathfrak{m}).$$

Since $q_{\nu+1}, \cdots, q_\lambda$ are in $\mathfrak{q}_\nu$, this congruence implies that $q_\nu(\sum_i c_{i\nu h}p_i) \in \mathfrak{q}_\nu$, and since $q_\nu \notin \mathfrak{q}_\nu$, we have

$$\sum_{i=1}^{\mu} c_{i\nu h}p_i \equiv 0(\mathfrak{M}).$$

Since $p_1, \cdots, p_\mu$ are linearly independent modulo $\mathfrak{M}$, $c_{1\nu h}, \cdots, c_{\mu\nu h}$ must be in $\mathfrak{m}$. Thus the induction is carried another step. We thus obtain that all $c_{ijh} \in \mathfrak{m}$. Since this implies that all $c_{ij} \in \mathfrak{m}^{k+1}$, we have a contradiction. Thus equation (27) is possible only if all $c_{ij}=0$, and the theorem is proved.

It has incidentally been shown that $\mathfrak{S}$ has an independent $\mathfrak{R}$-basis consisting of exactly $\lambda\mu$ elements, and hence that it can have no $\mathfrak{R}$-basis with less than this number of elements. An example will now be given to show that the elements p_iq_j of the given basis need not be independent—and hence that (26) need not hold—if $\mathfrak{S}$ is not regular.

Let P be an arbitrary field and let $P\{x_1, x_2, x_3, x_4\}$ be the ring of formal power series in four variables. In this ring, let

$$\mathfrak{p} = (x_3^3 - x_2^2x_4,\ x_4^3 - x_1^2x_3,\ x_3x_4 - x_1x_2,\ x_2x_4^2 - x_1x_3^2),$$

and let $\mathfrak{S}$ be the correspondng residue class ring. This ideal is prime; for the corresponding ideal in the polynomial ring $K[x_1, x_2, x_3, x_4]$ is easily seen to be prime (see Macaulay [8, p. 47]), and since its basis consists of homogeneous polynomials, its extension to the power series ring must be prime. Thus $\mathfrak{S}$ is an integral domain and is a complete local ring with maximal ideal $\mathfrak{M}=(u_1, u_2, u_3, u_4)$, where u_i is the residue class of x_i. The ring $\mathfrak{R}=P\{u_1, u_2\}$ is (by Lemma 16) a complete local ring with maximal ideal $\mathfrak{m}=\mathfrak{R}\cdot(u_1, u_2)$. The ideal $\mathfrak{S}\cdot\mathfrak{m}$ is primary with $\mathfrak{M}$ as its prime ideal for it contains u_3^3 and u_4^3. Moreover, a composition series for $\mathfrak{S}\cdot\mathfrak{m}$ is given by

$$\mathfrak{M} = (\mathfrak{S}\cdot\mathfrak{m}, u_3, u_4) \supset (\mathfrak{S}\cdot\mathfrak{m}, u_3^2, u_4) \supset (\mathfrak{S}\cdot\mathfrak{m}, u_3^3, u_4) \supset (\mathfrak{S}\cdot\mathfrak{m}, u_3^3, u_3u_4, u_4^2)$$
$$\supset (\mathfrak{S}\cdot\mathfrak{m}, u_3^3, u_3u_4, u_4^3) = \mathfrak{S}\cdot\mathfrak{m}.$$

From the proof of Theorem 8 it follows that $\mathfrak{S}$ is a finite $\mathfrak{R}$-module having as basis the elements $1, u_3, u_3^2, u_4, u_4^2$, so that $\mathfrak{S}=\mathfrak{R}[u_3, u_4]$. The ring $\mathfrak{S}$ has the same residue field and dimension as $\mathfrak{R}$, and $\mathfrak{R}$ has dimension two for it is clearly the isomorphic image of $P\{x_1, x_2\}$. Thus $\mathfrak{R}$ is regular.

Now if $\mathfrak{K}$ and $\mathfrak{L}$ are the quotient fields of $\mathfrak{R}$ and $\mathfrak{S}$ respectively, then $\mathfrak{L}=\mathfrak{K}(u_3, u_4)=\mathfrak{K}(u_3)$, for $u_4=u_1u_2/u_3$. Since $u_3^4=u_3u_2^2u_4=u_1u_2^3$, $[\mathfrak{L}:\mathfrak{K}]=4$. On the other hand the above composition series for $\mathfrak{S}\cdot\mathfrak{m}$ shows that its length is 5, and thus (26) is not satisfied.

The reason for the failure of the proof of Theorem 23 in this case goes back ultimately (cf. proof of Theorem 22) to the fact that $\mathfrak{S}\cdot u_2$ is mixed. The illustration of this mixed character is, in fact, the purpose of the introduction of the ideal $\mathfrak{p}$ (in the polynomial case) by Macaulay.

Bibliography

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

2. I. S. Cohen and A. Seidenberg, *Prime ideals and integral dependence*, to appear in Bull. Amer. Math. Soc.

3. H. Hasse and F. K. Schmidt, *Die Struktur diskret bewerteter Körper*, J. Reine Angew. Math. vol. 170 (1934) pp. 4–63.

4. W. Krull, *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, IV 3, Berlin, 1935.

5. ———, *Zum Dimensionsbegriff der Idealtheorie* (*Beiträge zur Arithmetik kommutativer Integritätsbereiche*, III), Math. Zeit. vol. 42 (1937) pp. 745–766.

6. ——— *Potenzreihenringe* (*Beiträge zur Arithmetik kommutativer Integritätsbereiche*, V), Math. Zeit. vol. 43 (1938) pp. 768–782.

7. ———, *Dimensionstheorie in Stellenringen*, J. Reine Angew. Math. vol. 179 (1938) pp. 204–226.

8. F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge Tracts in Mathematics and Mathematical Physics, vol. 19, Cambridge, 1916.

9. S. MacLane, *Subfields and automorphism groups of p-adic fields*, Ann. of Math. vol. 40 (1939) pp. 423–442.

10. N. H. McCoy, *Remarks on divisors of zero*, Amer. Math. Monthly vol. 49 (1942) pp. 286–295.

11. W. Rückert, *Zum Eliminationsproblem der Potenzreihenideale*, Math. Ann. vol. 107 (1933) pp. 259–281.

12. O. Teichmüller, *Diskret bewertete perfekte Körper mit unvollkommenen Restklassenkörper*, J. Reine Angew. Math. vol. 176 (1937) pp. 141–152.

13. O. Zariski, *Algebraic varieties over ground fields of characteristic zero*, Amer. J. Math. vol. 62 (1940) pp. 187–221.

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

Harvard University,
Cambridge, Mass.