Downloaded from rsta.royalsocietypublishing.org

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

On Integrally Dependent Integral Domains

P. M. Grundy

Phil. Trans. R. Soc. Lond. A 1947 **240**, 295-326
doi: 10.1098/rsta.1947.0004

Email alerting service

Receive free email alerts when new articles cite this article - sign up in the box at the top right-hand corner of the article or click **here**

To subscribe to *Phil. Trans. R. Soc. Lond. A* go to: **http://rsta.royalsocietypublishing.org/subscriptions**

This journal is © 1947 The Royal Society

Downloaded from rsta.royalsocietypublishing.org

ON INTEGRALLY DEPENDENT INTEGRAL DOMAINS

By P. M. GRUNDY

(*Communicated by W. V. D. Hodge, F.R.S.—Received 25 April 1946*)

CONTENTS

INTRODUCTION

The subject of this paper is the simultaneous ideal theory of a pair of integral domains $\mathfrak{R}$ and $\mathfrak{S} \supseteq \mathfrak{R}$, of which $\mathfrak{R}$ is integrally closed, and $\mathfrak{S}$ integrally dependent on $\mathfrak{R}$. It is assumed that the quotient field L of $\mathfrak{S}$ is a finite separable extension of the quotient field K of $\mathfrak{R}$. The device of quotient rings effects a preliminary simplification in many of the proofs; the quotient rings $\mathfrak{R}_S$ and $\mathfrak{S}_S$, with respect to any existent multiplicatively closed set S of non-zero elements of $\mathfrak{R}$, also satisfy the above basic postulates for $\mathfrak{R}$ and $\mathfrak{S}$. Another method of preliminary simplification, valuable in the discussion of ramification theory, is the adjunction of Kronecker indeterminates. Such indeterminates (algebraically independent over K) are denoted by y or z; in connexion with the regular representation of L, they are regarded as adjoined to K. This method is expedited by the known fact that $\mathfrak{R}[y_1, \ldots, y_m]$ and $\mathfrak{S}[y_1, \ldots, y_m]$ also satisfy the above postulates for $\mathfrak{R}$ and $\mathfrak{S}$. In particular, $\mathfrak{R}[y_1, \ldots, y_m]$ is integrally closed, and the degree of $L(y_1, \ldots, y_m)$ over $K(y_1, \ldots, y_m)$ is equal to the degree of L over K. Integral domains satisfying the conditions imposed on $\mathfrak{R}$ and $\mathfrak{S}$ are of common occurrence in algebraic geometry; the resulting interplay of geometrical and ideal-theoretic ideas makes such cases of outstanding interest.

The main results of this paper are given in Part I. The investigation is modelled on the well-known theory of the 'classical' case when $\mathfrak{R}$ is an integrally closed domain in which the (maximal and) weak minimal conditions for ideals hold. The simpler theory of the discriminant- and different-ideals, complementary modules, and norms, is assembled in §§ 1 to 3. Problems involving the structure of the extended ideal $\mathfrak{p}\mathfrak{S}$ of a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$—ramification theory—are introduced in § 4, where certain fundamental theorems of Krull are stated. The rest of Part I is concerned with ramification theory. The theorems of §§ 6 and 7 are valid for *strongly convergent* prime ideals, a new concept defined in § 5; these theorems are generalizations of those clustering round the classical Different-Theorem. If the maximal condition (Hilbert basis condition) holds in $\mathfrak{R}$, every prime ideal of $\mathfrak{R}$ is strongly convergent. The theorems of § 6 hold, more generally, for *convergent* prime ideals. The class of convergent prime ideals also includes the maximal ideal of any rank 1 valuation

The Royal Society is collaborating with JSTOR to digitize, preserve, and extend access to *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences.* www.jstor.org

Downloaded from rsta.royalsocietypublishing.org

ring. Part II is essentially an appendix; the results given briefly in §§ 8 and 9 are often needed in Part I. The counter-examples in § 10 have some bearing on the theory of convergent prime ideals.

For the purposes of this paper, an integral domain (besides being a commutative ring without null-factors) is required to have unity distinct from zero. The null ideal, but not the unit ideal, is included amongst the prime ideals of an integral domain. The quotient process is used in the following form: if $\mathfrak{m}$ is an $\mathfrak{R}$-submodule of L, and $\mathfrak{n}$ any subset of L, $\mathfrak{m}:\mathfrak{n}$ is the set of all $\alpha \in L$ such that $\alpha\mathfrak{n} \subseteq \mathfrak{m}$. Ideals, unless otherwise specified, are fractional ideals†. 'Integrally closed' is used in the sense adopted by Krull.‡ A monic polynomial in x is one with leading coefficient unity, as in Albert (1937). It should be observed that $\mathfrak{S}_\mathfrak{p}$ denotes the quotient ring of $\mathfrak{S}$ with respect to the system of elements *of* $\mathfrak{R}$ *not in* $\mathfrak{p}$, and that the isolated component of an integral $\mathfrak{S}$-ideal with respect to the same system is denoted similarly. A polynomial over $\mathfrak{R}$ (i.e. with coefficients in $\mathfrak{R}$) is congruent to zero modulo an $\mathfrak{R}$-ideal if all its coefficients belong to that ideal. Any other questions of terminology can be settled by reference to my paper (Grundy 1942).

Conventions. The following notation is used throughout Part I: $\mathfrak{R}$ denotes an integrally closed domain with quotient field K, L a separable extension-field of K of finite degree n, and $\mathfrak{S} \supseteq \mathfrak{R}$ an integral domain integrally dependent on $\mathfrak{R}$, with quotient field L. The letter $\mathfrak{p}$ stands for a prime ideal of $\mathfrak{R}$. All further restrictions are stated in the enunciation of the results concerned. The symbols $\mathfrak{D}, \mathfrak{d}, \mathfrak{e}, \mathfrak{c}(\ )$, and * have a fixed significance defined in § 1. A supplementary list of conventions governing the notation will be found in § 4.

PART I

1. Fundamental constructions

The ideas introduced in this section are closely connected with the regular representation of L. As far as (1.8) the results are standard in the classical theory, and their generalization calls for scarcely any alteration of the proofs.§ Theorems 1 and 2, on the other hand, deal with a problem which is not in doubt in the classical case.

It is familiar that the characteristic coefficients of any element α of $\mathfrak{S}$ are elements of $\mathfrak{R}$. The norm $N(\alpha)$, trace $T(\alpha)$, and discriminant $D(\alpha)$ belong to $\mathfrak{R}$, and the different $d(\alpha)$ to $\mathfrak{S}$. (This notation is similar to that in § 9. We reserve x for the dummy variable appearing in characteristic and minimal polynomials.) Since α is a root of its characteristic polynomial

† An $\mathfrak{R}$-submodule $\mathfrak{a}$ of K is an $\mathfrak{R}$-ideal if $\mathfrak{R}:\mathfrak{a} \neq (0)$, and an integral $\mathfrak{R}$-ideal if $\mathfrak{a} \subseteq \mathfrak{R}$. The class of $\mathfrak{R}$-ideals is closed under the four operations $+$, $.$, $:$ and $\cap$.

‡ The words 'ganz abgeschlossen', where they appear in van der Waerden (1931), must accordingly be translated as 'totally closed'. The distinction between integrally closed and totally closed domains was emphasized by Krull (1932). Every totally closed domain is integrally closed, but the converse is false. An integrally closed domain in which the maximal condition holds is totally closed. Cf. also Lorenzen (1939).

§ See, for example, Fricke (1928); on the conductor, Grell (1927*a*, 1927*b*). A concise account of the classical theory from a modern point of view is given by Krull (1939*b*).

Schmeidler (1928) has generalized parts of the Dedekind-Weber theory of algebraic functions of one variable to functions of $m-1$ variables $y_2, \ldots, y_m$ over a perfect (vollkommen) field P. He does not, however, work directly with $y_2, \ldots, y_m$, but with new variables $x_2, \ldots, x_m$ obtained by a linear transformation with indeterminate coefficients. Under these conditions, his paper includes (1.6), the expression $(d(\alpha))^{-1}\mathfrak{R}[\alpha]$ for the module complementary to $\mathfrak{R}[\alpha]$, and the inequalities $\mathfrak{d}\mathfrak{e} \subseteq \mathfrak{S}$, $\mathfrak{D}\mathfrak{e} \subseteq \mathfrak{S}$.

Downloaded from rsta.royalsocietypublishing.org

$f(x)$, $N(\alpha) \in \alpha\mathfrak{S}$; so α is a unit of $\mathfrak{S}$ if and only if $N(\alpha)$ is a unit of $\mathfrak{R}$. By expressing the fact that the discriminant of the polynomial $(x-\alpha)^{-1}f(x)$ belongs to $\mathfrak{S}$, we obtain the relation $D(\alpha) \in (d(\alpha))^2\,\mathfrak{S}$. Still assuming that $\alpha \in \mathfrak{S}$, it is a well-known consequence of Theorem 17 that

(1.1) $d(\alpha)\,\mathfrak{S} \subseteq \mathfrak{R}[\alpha]$; *a fortiori* $D(\alpha)\,\mathfrak{S} \subseteq \mathfrak{R}[\alpha]$. These relations still hold when $\mathfrak{S}$ is replaced by its integral closure in L.

Let $\omega_1, \ldots, \omega_n$ be a basis for L over K, and $\theta_1, \ldots, \theta_n$ the complementary basis, the elements ω_i being in $\mathfrak{S}$. It follows from (9.2) and (9.1) successively that

$$\theta_i D(\omega_1, \ldots, \omega_n) \in \mathfrak{R}.(\omega_1, \ldots, \omega_n), \tag{1.2}$$

$$D(\omega_1, \ldots, \omega_n)\,\mathfrak{S} \subseteq \mathfrak{R}.(\omega_1, \ldots, \omega_n). \tag{1.3}$$

Again, putting $e_{ij} = T(\omega_i\omega_j)$, $D = |e_{ij}|$, and denoting the elements of the (symmetric) inverse matrix by E_{ij}, then

$$\begin{aligned}\theta_i\theta_j - E_{ij} &= \theta_i\theta_j - E_{ij}\sum_s \omega_s\theta_s \quad \text{from (9.4)}\\ &= \sum_t E_{it}\omega_t \sum_s E_{sj}\omega_s - E_{ij}\sum_{t,s} E_{st}\omega_t\omega_s\\ &= \sum_{t,s}\{E_{it}E_{sj} - E_{ij}E_{st}\}\omega_t\omega_s.\end{aligned}$$

By determinantal theory, $E_{ij}D$ and $\{E_{it}E_{sj} - E_{ij}E_{st}\}D$ belong to $\mathfrak{R}$. Hence

$$\theta_i\theta_j D(\omega_1, \ldots, \omega_n) \in \mathfrak{S} \quad (i,j = 1, \ldots, n). \tag{1.4}$$

Complementary modules. The complementary module $\mathfrak{m}^*$ of an $\mathfrak{R}$-submodule $\mathfrak{m}$ of L is defined to be the set of all $\beta \in L$ such that† $T(\beta\mathfrak{m}) \subseteq \mathfrak{R}$. It is clear that $\mathfrak{m}^{**} \supseteq \mathfrak{m}$, and hence that $\mathfrak{m}^{***} = \mathfrak{m}^*$, because $\mathfrak{m}^* \supseteq (\mathfrak{m}^{**})^* = (\mathfrak{m}^*)^{**} \supseteq \mathfrak{m}^*$. If $\omega_1, \ldots, \omega_n$ and $\theta_1, \ldots, \theta_n$ are complementary bases of L, the modules $\mathfrak{R}.(\omega_1, \ldots, \omega_n)$ and $\mathfrak{R}.(\theta_1, \ldots, \theta_n)$ are mutually complementary. When $\mathfrak{m}$ does not possess a basis of this form, even locally, $\mathfrak{m}^{**}$ may be distinct from $\mathfrak{m}$ (see further (3.6)). Given any $\alpha \in \mathfrak{S}$, primitive for L over K, § 9 shows that the basis complementary to $1, \alpha, \ldots, \alpha^{n-1}$ is $\eta_0/d(\alpha), \ldots, \eta_{n-1}/d(\alpha)$; here the η_{i-1} are defined by the identity $f(x) = (x-\alpha)(\eta_0 + \ldots + \eta_{n-1}x^{n-1})$, where $f(x)$ is the characteristic polynomial of α. It is clear that $\mathfrak{R}.(\eta_0, \ldots, \eta_{n-1}) = \mathfrak{R}.(1, \alpha, \ldots, \alpha^{n-1})$, and follows that the modules

$$\mathfrak{R}[\alpha] \quad \text{and} \quad (d(\alpha))^{-1}\mathfrak{R}[\alpha]$$

are mutually complementary.

Definitions. The *discriminant-ideal* $\mathfrak{D}$ of $\mathfrak{S}$ over $\mathfrak{R}$ is the $\mathfrak{R}$-ideal generated by all discriminants $D(\alpha_1, \ldots, \alpha_n)$ $(\alpha_1, \ldots, \alpha_n \in \mathfrak{S})$. The *different-ideal*‡ $\mathfrak{d}$ of $\mathfrak{S}$ over $\mathfrak{R}$ is the $\mathfrak{S}$-ideal generated by the differents $d(\alpha)$, for all $\alpha \in \mathfrak{S}$. The letter $\mathfrak{e}$ stands for the module *complementary to* $\mathfrak{S}$.

† For any $\mathfrak{R}$-submodule $\mathfrak{M}$ of L, $T(\mathfrak{M})$ denotes the set of all $T(\gamma)$ $(\gamma \in \mathfrak{M})$. Clearly $T(\mathfrak{M})$ is an $\mathfrak{R}$-submodule of K.

‡ Previous work involving the different-ideal seems to have been carried out under strong finiteness-conditions. The different-ideal does, however, appear implicitly in Zariski's work (1939, 1940), where $\mathfrak{R}$ is a polynomial ring; it also occurs in a special case in Schmeidler (1928).

In the classical theory, the different-ideal is defined to be $\mathfrak{S}:\mathfrak{e}$; but the only property of $\mathfrak{S}:\mathfrak{e}$ required for the classical ramification theorem is that, in the cases considered, it coincides with our $\mathfrak{d}$. Further support for our definition is gained from Theorem 13, where the significance of $\mathfrak{d}$ is made plain. The ramification theorem of Grell (1936), on the other hand, seems to favour the classical definition. If it should turn out that both $\mathfrak{d}$ and $\mathfrak{S}:\mathfrak{e}$ have to be retained in the general theory, it may be best to reserve the classical term 'ramification ideal' for the latter. The connexion between $\mathfrak{d}$ and $\mathfrak{e}$ is examined in § 2.

Downloaded from rsta.royalsocietypublishing.org

Evidently $\mathfrak{e}$ contains $\mathfrak{S}$, and admits multiplication by $\mathfrak{S}$, while it follows from Theorem 17 that $d(\alpha)\,\mathfrak{e} \subseteq \mathfrak{R}[\alpha]$, for any $\alpha \in \mathfrak{S}$. Thus $\mathfrak{e}$ is an $\mathfrak{S}$-ideal such that $\mathfrak{e} \supseteq \mathfrak{S}$, $\mathfrak{d}\mathfrak{e} \subseteq \mathfrak{S}$. Another property of $\mathfrak{e}$, expressed by the relation $\mathfrak{D}\mathfrak{e}^2 \subseteq \mathfrak{S}$, follows readily from (1.4). If $\mathfrak{a}$ is any non-null $\mathfrak{S}$-ideal, the condition for $\beta \in \mathfrak{a}^*$ is $T(\beta\mathfrak{a}\mathfrak{S}) \subseteq \mathfrak{R}$, i.e. $\beta\mathfrak{a} \subseteq \mathfrak{e}$; hence

$$\mathfrak{a}^* = \mathfrak{e} : \mathfrak{a}. \tag{1.5}$$

The conductor $\mathfrak{c}(\alpha)$ of an element $\alpha \in \mathfrak{S}$ (with respect to $\mathfrak{S}$) is defined to be the conductor of $\mathfrak{R}[\alpha]$ with respect to $\mathfrak{S}$, viz. $\mathfrak{R}[\alpha] : \mathfrak{S}$. For any $\alpha \in \mathfrak{S}$,

$$\mathfrak{c}(\alpha) = d(\alpha)\,\mathfrak{e}. \tag{1.6}$$

This equation certainly holds when $d(\alpha) = 0$; for then $K(\alpha)$ is a proper subfield of L, so that $\mathfrak{c}(\alpha) = (0)$. When $d(\alpha) \neq 0$, the condition for γ to belong to $(d(\alpha))^{-1}\,\mathfrak{c}(\alpha)$ is, in the notation of Theorem 17, that $T(\gamma\eta_{i-1}\mathfrak{S}) \subseteq \mathfrak{R}$ $(i = 1, \ldots, n)$. Since $\eta_{i-1} \in \mathfrak{S}$, and $\eta_{n-1} = 1$, these inequalities hold if and only if $\gamma \in \mathfrak{e}$.

Quotient rings. In proofs involving the quotient rings $\mathfrak{R}_S$ and $\mathfrak{S}_S = \mathfrak{R}_S.\mathfrak{S}$ (where S is an existent multiplicatively closed set of non-zero elements of $\mathfrak{R}$), it is necessary to know what are the discriminant-ideal, etc., of $\mathfrak{S}_S$ with respect to $\mathfrak{R}_S$. The results are straightforward:

(1.7) The discriminant-ideal of $\mathfrak{S}_S$ over $\mathfrak{R}_S$ is $\mathfrak{D}.\mathfrak{R}_S$, and the different-ideal is $\mathfrak{d}.\mathfrak{S}_S$. If $\mathfrak{S}$ has a finite $\mathfrak{R}$-basis, the complementary ideal of $\mathfrak{S}_S$ over $\mathfrak{R}_S$ is $\mathfrak{e}.\mathfrak{S}_S$.

(1.8) If $\mathfrak{n}$ is any finite $\mathfrak{R}$-submodule of L, and $\mathfrak{n}^*$ is the complementary module, the complementary module of $\mathfrak{n}.\mathfrak{R}_S$ over $\mathfrak{R}_S$ is $\mathfrak{n}^*.\mathfrak{R}_S$.

Proof. The discriminant-ideal of $\mathfrak{S}_S$ over $\mathfrak{R}_S$ obviously contains $\mathfrak{D}\mathfrak{R}_S$. Since the elements of $\mathfrak{S}_S$ are those of the form $u^{-1}\alpha$ $(u \in S, \alpha \in \mathfrak{S})$, the reverse inequality follows from the equation $D(u_1^{-1}\alpha_1, \ldots, u_n^{-1}\alpha_n) = (u_1 \ldots u_n)^{-2} D(\alpha_1, \ldots, \alpha_n)$, wherein $u_1 \ldots u_n$ is a unit of $\mathfrak{R}_S$. A similar argument disposes of the different-ideal. The rest of (1.7) is included in (1.8), which asserts that the relation $\beta \in \mathfrak{n}^*\mathfrak{R}_S$ is necessary and sufficient for $T(\beta\mathfrak{n}\mathfrak{R}_S) \subseteq \mathfrak{R}_S$. The sufficiency follows from the simplest properties of the trace. Conversely, suppose that $T(\beta\mathfrak{n}) \subseteq \mathfrak{R}_S$. Because $\mathfrak{n}$ has a finite $\mathfrak{R}$-basis, there exists $u \in S$ such that $uT(\beta\mathfrak{n}) \subseteq \mathfrak{R}$, whence $u\beta \in \mathfrak{n}^*$.

THEOREM 1. *A necessary and sufficient condition for* $\mathfrak{S}_\mathfrak{p}$ *to possess an* $\mathfrak{R}_\mathfrak{p}$*-basis of* n *terms is that* $\mathfrak{D}\mathfrak{R}_\mathfrak{p}$ *be a principal ideal of* $\mathfrak{R}_\mathfrak{p}$.

The necessity is trivial, from (1.7) and the transformation law for discriminants. When $\mathfrak{D}\mathfrak{R}_\mathfrak{p}$ is a principal ideal of $\mathfrak{R}_\mathfrak{p}$ there exist, by (8.8), elements $\omega_1, \ldots, \omega_n$ of $\mathfrak{S}$ such that

$$\mathfrak{D}\mathfrak{R}_\mathfrak{p} = D(\omega_1, \ldots, \omega_n).\mathfrak{R}_\mathfrak{p}.$$

A device borrowed from the classical theory completes the proof. Any element $\alpha \in \mathfrak{S}_\mathfrak{p}$ is expressible as $\alpha = a_1\omega_1 + \ldots + a_n\omega_n$ with $a_i \in K$; and here, by the transformation law for discriminants,

$$a_i^2 D(\omega_1, \ldots, \omega_n) = D(\omega_1, \ldots, \omega_{i-1}, \alpha, \omega_{i+1}, \ldots, \omega_n) \in \mathfrak{D}\mathfrak{R}_\mathfrak{p}.$$

Thus $a_i^2 \in \mathfrak{R}_\mathfrak{p}$, $a_i \in \mathfrak{R}_\mathfrak{p}$, and consequently $\omega_1, \ldots, \omega_n$ is an $\mathfrak{R}_\mathfrak{p}$-basis for $\mathfrak{S}_\mathfrak{p}$.

COROLLARY (using (8.6) and (8.7)). *Suppose* $\mathfrak{D}$ *has a finite* $\mathfrak{R}$*-basis. Then* $\mathfrak{D}$ *is inversive if and only if, for every* $\mathfrak{p}$, $\mathfrak{S}_\mathfrak{p}$ *has an* n*-term* $\mathfrak{R}_\mathfrak{p}$*-basis.*

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Downloaded from rsta.royalsocietypublishing.org

THEOREM 2. *Let* $\mathfrak{p}$ *be a maximal ideal* (*of* $\mathfrak{R}$).

(1) *If* $\mathfrak{S}_\mathfrak{p}$ *possesses an n-term* $\mathfrak{R}_\mathfrak{p}$*-basis, the algebra* $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ *over the field* $\mathfrak{R}/\mathfrak{p}$ *has rank n.*

(2) *Assume that* $\mathfrak{S}$ *has a finite* $\mathfrak{R}$*-basis. If elements* $\alpha_1, \ldots, \alpha_m$ *of* $\mathfrak{S}$ *form an* $\mathfrak{R}/\mathfrak{p}$*-basis for* $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$, *then* $\alpha_1, \ldots, \alpha_m$ *form an* $\mathfrak{R}_\mathfrak{p}$*-basis for* $\mathfrak{S}_\mathfrak{p}$. *The rank of* $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ *over* $\mathfrak{R}/\mathfrak{p}$ *is therefore at least n.*

(1) When $\mathfrak{S}_\mathfrak{p}$ possesses an n-term $\mathfrak{R}_\mathfrak{p}$-basis, the basis elements $\omega_1, \ldots, \omega_n$ may be taken in $\mathfrak{S}$. Thus every $\beta \in \mathfrak{S}$ satisfies an equation

$$u\beta = b_1\omega_1 + \ldots + b_n\omega_n \quad (b_i \in \mathfrak{R},\ u \in \mathfrak{R},\ u \not\equiv 0\ (\mathfrak{p})).$$

Taking $v \in \mathfrak{R}$ such that $vu \equiv 1 \bmod \mathfrak{p}$, it is seen that

$$\beta \equiv v(b_1\omega_1 + \ldots + b_n\omega_n)\ (\mathfrak{p}\mathfrak{S}),$$

and it follows that $\omega_1, \ldots, \omega_n$ form an $\mathfrak{R}/\mathfrak{p}$-basis for $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$. Now $\mathfrak{p}\mathfrak{S}_\mathfrak{p} = \mathfrak{p}\mathfrak{R}_\mathfrak{p}.(\omega_1, \ldots, \omega_n)$. Coupled with the linear independence of $\omega_1, \ldots, \omega_n$ over K, this shows that the congruence

$$a_1\omega_1 + \ldots + a_n\omega_n \equiv 0\ (\mathfrak{p}\mathfrak{S}) \quad (a_i \in \mathfrak{R})$$

can only hold if the a_i all belong to $\mathfrak{p}\mathfrak{R}_\mathfrak{p} \cap \mathfrak{R} = \mathfrak{p}$.

(2) By hypothesis, $\mathfrak{S}$ has a finite $\mathfrak{R}$-basis, and $\mathfrak{S} = \mathfrak{p}\mathfrak{S} + \mathfrak{R}.(\alpha_1, \ldots, \alpha_m)$. Thus the $\mathfrak{R}$-module $\mathfrak{M} = \mathfrak{S}/\mathfrak{R}.(\alpha_1, \ldots, \alpha_m)$ has a finite $\mathfrak{R}$-basis, and $\mathfrak{M} = \mathfrak{p}\mathfrak{M}$. According to Theorem 6 of Grundy (1942), $\mathfrak{p}$ cannot contain the annihilating ideal of $\mathfrak{M}$; there exists $u \in \mathfrak{R}$ such that

$$u\mathfrak{S} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_m), \quad u \not\equiv 0\ (\mathfrak{p}).$$

Hence $\mathfrak{S}_\mathfrak{p} = \mathfrak{R}_\mathfrak{p}.(\alpha_1, \ldots, \alpha_m)$, and $m \geqslant n$.

COROLLARY.† *Let* $\mathfrak{p}$ *be a maximal ideal. Assuming that* $\mathfrak{S}$ *has a finite* $\mathfrak{R}$*-basis, an element* $\alpha \in \mathfrak{S}$ *is primitive for the algebra* $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ *over* $\mathfrak{R}/\mathfrak{p}$ *if and only if* $\mathfrak{c}(\alpha) \cap \mathfrak{R} \nsubseteq \mathfrak{p}$.

If, in fact, $\mathfrak{S} = \mathfrak{p}\mathfrak{S} + \mathfrak{R}[\alpha]$, the theorem shows that $\mathfrak{S}_\mathfrak{p} = \mathfrak{R}_\mathfrak{p}[\alpha]$. The conductor of $\mathfrak{R}_\mathfrak{p}[\alpha]$ with respect to $\mathfrak{S}_\mathfrak{p}$, which by (1.6) and (1.7) is $d(\alpha).\mathfrak{e}\mathfrak{S}_\mathfrak{p} = d(\alpha)\,\mathfrak{e}\mathfrak{R}_\mathfrak{p} = \mathfrak{c}(\alpha)\,\mathfrak{R}_\mathfrak{p}$, therefore contains unity; so $\mathfrak{c}(\alpha)$ contains an element of $\mathfrak{R}$ not in $\mathfrak{p}$. Conversely, the relation $\mathfrak{c}(\alpha) \cap \mathfrak{R} \nsubseteq \mathfrak{p}$ implies that $1 \in \mathfrak{p} + \mathfrak{c}(\alpha)$, whence $\mathfrak{S} \subseteq \mathfrak{p}\mathfrak{S} + \mathfrak{c}(\alpha)\,\mathfrak{S} \subseteq \mathfrak{p}\mathfrak{S} + \mathfrak{R}[\alpha]$.

Results obtained by Muhly (1943) indicate that the general problem of finding workable conditions sufficient for $\mathfrak{S}$ to have an n-term $\mathfrak{R}$-basis is too difficult to be tackled at present. The corresponding local problem‡—conditions for $\mathfrak{S}_\mathfrak{p}$ to have an n-term $\mathfrak{R}_\mathfrak{p}$-basis—is probably much simpler; but of course Theorems 1 and 2 cannot be regarded as a solution. It would be natural to include the following among the postulates: (i) $\mathfrak{R} = \mathfrak{R}_\mathfrak{p}$ a unique factorization domain, (ii) $\mathfrak{S} = \mathfrak{S}_\mathfrak{p}$ integrally closed. Assuming (i), it would be enough to find conditions sufficient for $\mathfrak{D}$ to be a v-ideal§ of $\mathfrak{R}$. Since Theorem 3 shows that under certain circumstances $\mathfrak{e}$ is a v-ideal of $\mathfrak{S}$, it seems that (3.13) may be relevant; a solution of the problem might well come through some improvement in norm theory.

† When $\mathfrak{R}$ is a polynomial ring, this is Theorem 9 of Zariski (1939).

‡ It is well known that $\mathfrak{S}_\mathfrak{p}$ does not always possess an n-term $\mathfrak{R}_\mathfrak{p}$-basis. An example is obtained by taking $\mathfrak{R} = \mathfrak{k}[y^4, z^4]$ and $\mathfrak{S} = \mathfrak{k}[y^4, y^3z, yz^3, z^4]$, where y and z are indeterminates over a field $\mathfrak{k}$ of characteristic zero. In this case $\mathfrak{D} = y^{12}z^{12}(y^4, z^4)^2$ is not inversive. Another example is given by $\mathfrak{R} = \mathfrak{k}[y^3, y^2z, yz^2, z^3]$ and $\mathfrak{S} = \mathfrak{k}[y^3, y^2z, z^3]$. Here $\mathfrak{S}$ is integrally closed, but $\mathfrak{D} = (y^3, y^2z, yz^2)$ is again not inversive.

§ Cf. footnote †, p. 300.

Downloaded from rsta.royalsocietypublishing.org

2. On the complementary ideal

When $\mathfrak{R}$ is a Z.P.I. ring† and $\mathfrak{S}$ is integrally closed, the ideals $\mathfrak{d}$ and $\mathfrak{e}$ defined in § 1 satisfy the equation $\mathfrak{de} = \mathfrak{S}$, subject to certain safeguards. That is the content of Lemma 1, a classical theorem, although the proof below is not entirely orthodox. It is also known that the method of prime ideal quotient rings‡ enables the bulk of the classical theory to be generalized to the case when $\mathfrak{R}$ is a v-Z.P.I. ring. In that case (with safeguards, etc.) one would expect to find the product $\mathfrak{de}$ 'v-equivalent' to $\mathfrak{S}$, i.e. $\mathfrak{S}:\mathfrak{de} = \mathfrak{S}$. This is true under the conditions of Theorem 3, and follows at once from the latter; but, under such conditions, the theorem shows further that $\mathfrak{e}$ *is a v-ideal.*§

Lemma 1. *Assume that* $\mathfrak{S}$ *is integrally closed,* $\mathfrak{R}$ *a Z.P.I. ring, and that the field* $\mathfrak{S}/\mathfrak{q}$ *is separable over* $\mathfrak{R}/(\mathfrak{q} \cap \mathfrak{R})$, *for every non-null prime ideal* $\mathfrak{q}$ *of* $\mathfrak{S}$. *Then* $\mathfrak{de} = \mathfrak{S}$.

Disregard the trivial case when $\mathfrak{R}$ has a finite number of elements, and so is a field. In view of (1.6) and the remark in § 1 that $\mathfrak{de} \subseteq \mathfrak{S}$, it will be enough to prove the following: Given any non-null prime ideal $\mathfrak{q}$ of $\mathfrak{S}$, there exists an $\alpha \in \mathfrak{S}$ such that $\mathfrak{c}(\alpha) \nsubseteq \mathfrak{q}$.

Let $\mathfrak{q} \cap \mathfrak{R} = \mathfrak{p}, \mathfrak{pS} = \mathfrak{q}^s\mathfrak{h}$, where $s \geqslant 1$, and the integral $\mathfrak{S}$-ideal $\mathfrak{h}$ is not divisible by $\mathfrak{q}$. Because the only $\mathfrak{S}$-ideals between $\mathfrak{S}$ and $\mathfrak{q}^s$ are powers of $\mathfrak{q}$, Theorem 20 supplies an element $\alpha \in \mathfrak{S}$ primitive for $\mathfrak{S}/\mathfrak{q}^s$ over $\mathfrak{R}/\mathfrak{p}$, which may be chosen so that $\alpha \not\equiv 0 \bmod \mathfrak{q}$. Any element congruent to α mod $\mathfrak{q}^s$ shares these properties. It can therefore be arranged that $\alpha \equiv 0 \bmod \mathfrak{h}$, and further that α be a primitive element for L over K. Hence $\mathfrak{S} = \mathfrak{R}[\alpha] + \mathfrak{q}^s$ and $\alpha\mathfrak{q}^s \subseteq \mathfrak{pS}$, so that $\alpha\mathfrak{S} \subseteq \mathfrak{R}[\alpha] + \mathfrak{pS}$. By a trivial induction $\alpha^r\mathfrak{S} \subseteq \mathfrak{R}[\alpha] + \mathfrak{p}^r\mathfrak{S}$ for all $r \geqslant 1$. Taking $\mathfrak{c}(\alpha) \cap \mathfrak{R} = \mathfrak{p}^t\mathfrak{a}$ (where $t \geqslant 0, \mathfrak{a} \subseteq \mathfrak{R}, \mathfrak{a} \nsubseteq \mathfrak{p}$), it follows that

$$\alpha^{t+1}\mathfrak{a} \,.\, \mathfrak{S} \subseteq \mathfrak{R}[\alpha] + \mathfrak{a}\mathfrak{p}^{t+1}\mathfrak{S} \subseteq \mathfrak{R}[\alpha] + \mathfrak{c}(\alpha)\,\mathfrak{S} \subseteq \mathfrak{R}[\alpha].$$

Thus $\alpha^{t+1}\mathfrak{a} \subseteq \mathfrak{c}(\alpha)$, whence $\mathfrak{c}(\alpha) \nsubseteq \mathfrak{q}$.

Theorem 3. *Assume that* $\mathfrak{S}$ *is integrally closed,* $\mathfrak{R}$ *a v-Z.P.I. ring, and that the quotient field of* $\mathfrak{S}/\mathfrak{q}$ *is separable over that of* $\mathfrak{R}/(\mathfrak{q} \cap \mathfrak{R})$, *for every minimal prime ideal* $\mathfrak{q}$ *of* $\mathfrak{S}$. *Then* $\mathfrak{e} = \mathfrak{S}:\mathfrak{d}$.

For any minimal prime ideal $\mathfrak{p}$ of $\mathfrak{R}$, $\mathfrak{R}_\mathfrak{p}$ is a Z.P.I. ring, and the same is therefore true of $\mathfrak{S}_\mathfrak{p}$. (In fact, both are principal ideal rings.) By the theory of quotient rings (Grell (1927*a*); also in § 13 of Grundy (1942)), every non-null prime ideal of $\mathfrak{S}_\mathfrak{p}$ has the form $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$, where $\mathfrak{q}$ is a minimal prime ideal of $\mathfrak{S}$ such that $\mathfrak{q} \cap \mathfrak{R} = \mathfrak{p}$. It is also a standard result, formulated more exactly in (4.4), that the structure of the quotient fields of $\mathfrak{R}/\mathfrak{p}$ and $\mathfrak{S}/\mathfrak{q}$ is the same as that of the fields $\mathfrak{R}_\mathfrak{p}/\mathfrak{p}\mathfrak{R}_\mathfrak{p}$ and $\mathfrak{S}_\mathfrak{p}/\mathfrak{q}\mathfrak{S}_\mathfrak{p}$. Thus $\mathfrak{R}_\mathfrak{p}$ and $\mathfrak{S}_\mathfrak{p}$ satisfy the conditions of Lemma 1.

Since always $\mathfrak{de} \subseteq \mathfrak{S}$, it is only necessary to prove that $\mathfrak{S}:\mathfrak{d} \subseteq \mathfrak{e}$; consider any $\beta \in \mathfrak{S}:\mathfrak{d}$. For every minimal prime ideal $\mathfrak{p}$ of $\mathfrak{R}$, $\beta \,.\, \mathfrak{d}\mathfrak{S}_\mathfrak{p} \subseteq \mathfrak{S}_\mathfrak{p}$. By (1.7) and Lemma 1, β belongs to the

† A Z.P.I. ring is an integrally closed domain in which the (maximal and) weak minimal conditions hold—cf. Krull (1939*b*).

A v-ideal of an integral domain $\mathfrak{o}$ is an $\mathfrak{o}$-ideal $\mathfrak{a}$ such that $\mathfrak{o}:(\mathfrak{o}:\mathfrak{a}) = \mathfrak{a}$. On v-ideals and v-Z.P.I. rings, see Krull (1939*b*, 1935), and chapter xiv of van der Waerden (1931). Any v-Z.P.I. ring is totally closed, and is the intersection of its quotient rings with respect to its minimal prime ideals; and every such quotient ring is a Z.P.I. ring. If $\mathfrak{R}$ is a v-Z.P.I. ring, and $\mathfrak{S}$ integrally closed, then $\mathfrak{S}$ is a v-Z.P.I. ring (Krull 1939*b*, n. 17).

‡ In the original work of Kronecker, König, and others, such results were obtained by the device of 'functionals'. Cf. n. 35 of Krull (1935).

§ On the other hand, $\mathfrak{d}$ is not necessarily a v-ideal. For an example, take $\mathfrak{R} = \mathfrak{k}[y^2, z^2]$ and $\mathfrak{S} = \mathfrak{k}[y, z]$, where y and z are indeterminates over a field $\mathfrak{k}$ of characteristic zero. In this case $\mathfrak{d} = \mathfrak{S}.yz(y, z)$.

Downloaded from rsta.royalsocietypublishing.org

complementary ideal of $\mathfrak{S}_\mathfrak{p}$ over $\mathfrak{R}_\mathfrak{p}$; $T(\beta\mathfrak{S}_\mathfrak{p}) \subseteq \mathfrak{R}_\mathfrak{p}$, and *a fortiori* $T(\beta\mathfrak{S}) \subseteq \mathfrak{R}_\mathfrak{p}$. Since $\mathfrak{R} = \bigcap \mathfrak{R}_\mathfrak{p}$, where $\mathfrak{p}$ runs through all minimal prime ideals of $\mathfrak{R}$, it follows that

$$T(\beta\mathfrak{S}) \subseteq \mathfrak{R}, \quad \beta \in \mathfrak{e}.$$

COROLLARY. *Under the conditions of the theorem,* $\mathfrak{c}(\alpha)$ *is a v-ideal of* $\mathfrak{S}$, *for any* $\alpha \in \mathfrak{S}$.

A special case of Theorem 3, stated in a form equivalent to the Corollary, was proved by Schmeidler (1928). Some remarks on his paper will be found in footnote §, p. 296.

3. NORM THEORY

The norm process adopted in this paper differs from that of Fitting (1937), the most obvious difference being that here the determinants are exclusively of order n. The choice between the various definitions is a question which cannot yet be regarded as settled. The present definition can at least claim serious consideration, on the grounds that it agrees with the 'classical' definition, and that most of the standard theorems of classical norm theory are special cases of the results of this section.† Moreover, these results are closely connected with the problem mentioned at the end of § 1; it is hoped that they will help to suggest a method for its solution.

In order to avoid trivial exceptional cases, attention is restricted to modules of a class H, defined as follows: *The class* H *shall consist of all* $\mathfrak{R}$*-submodules* $\mathfrak{m}$ *of* L *such that both* $\mathfrak{S}:\mathfrak{m} \neq (0)$ *and* $\mathfrak{m}:\mathfrak{S} \neq (0)$. It is clear that every non-null $\mathfrak{S}$-ideal belongs to H, and hence, using (1.3), that necessary and sufficient conditions for $\mathfrak{m}$ to belong to H are: (i) $\mathfrak{m} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_n)$, with some $\alpha_1, \ldots, \alpha_n \in L$, and (ii) $\mathfrak{m}$ contains n linearly independent elements. The product of a finite number of members of H belongs to H; in fact, H is closed under the four operations $+, \cdot, :$, and $\cap$. The module complementary to a member of H also belongs to H. When the maximal condition holds in $\mathfrak{R}$, every member of H has a finite $\mathfrak{R}$-basis.

Clarendon type Greek letters are used to stand for ordered sets of n elements of L; thus $\boldsymbol{\alpha}$ stands for the set $\alpha_1, \ldots, \alpha_n$. If $\boldsymbol{\omega}$ is a K-basis of L, there exist unique elements $a_{ij} \in K$ such that $\alpha_i = \sum_j a_{ij}\omega_j$. The determinant $|a_{ij}|$ is denoted by $N(\boldsymbol{\alpha};\boldsymbol{\omega})$. Several properties of this symbol follow at once from linear algebra and the elements of the theory of the regular representation of L:

(3.1) $N(\xi\boldsymbol{\alpha};\zeta\boldsymbol{\omega}) = N(\xi\zeta^{-1})\, N(\boldsymbol{\alpha};\boldsymbol{\omega})$. If $\mathfrak{R}.(\boldsymbol{\alpha}) \subseteq \mathfrak{R}.(\boldsymbol{\omega})$, then

$$N(\boldsymbol{\alpha};\boldsymbol{\omega}) \in \mathfrak{R} \quad \text{and} \quad {}^*\boldsymbol{\omega}\,.\,N(\boldsymbol{\alpha};\boldsymbol{\omega}) \subseteq \mathfrak{R}.(\boldsymbol{\alpha}).$$

(3.2) For any bases $\boldsymbol{\omega}$ and $\boldsymbol{\theta}$ of L over K,

$$N(\boldsymbol{\alpha};\boldsymbol{\omega})\, N(\boldsymbol{\beta};\boldsymbol{\theta}) = N(\boldsymbol{\alpha};\boldsymbol{\theta})\, N(\boldsymbol{\beta};\boldsymbol{\omega}).$$

† An important exception is the classical theorem expressing $N(\mathfrak{m};\mathfrak{n})$, where $\mathfrak{m} \subseteq \mathfrak{n}$, as the product of the annihilating ideals of the composition factors of $\mathfrak{n}/\mathfrak{m}$. On norm theory in the classical case when $\mathfrak{R}$ is a Z.P.I. ring, see Grell (1927*b*, 1936), and cf. Fitting (1937).

In multiplicative ideal theory, if one is working with a Prüfer ideal-system of $\mathfrak{R}$-ideals obeying the 'semi-group condition' of Lorenzen (1939), another construction is available.—The norm $N(\mathfrak{b})$ of a finite $\mathfrak{S}$-ideal $\mathfrak{b} = \mathfrak{S}.(\beta_1, \ldots, \beta_s)$ may be defined to be the ideal generated by the coefficients of the distinct power-products in $N(\beta_1 y_1 + \ldots + \beta_s y_s)$, where $y_1, \ldots, y_s$ are indeterminates.

Downloaded from rsta.royalsocietypublishing.org

(3.3) If α and α^* are complementary bases, likewise β and β^*, then

$$N(\alpha;\beta) = N(\beta^*;\alpha^*), \quad N(\alpha;\alpha^*) = D(\alpha), \quad \{N(\alpha;\beta^*)\}^2 = D(\alpha)\,D(\beta).$$

Definition. For any modules $\mathfrak{m}, \mathfrak{n}$ of the class H, the *norm of* $\mathfrak{m}$ *with respect to* $\mathfrak{n}$ (over $\mathfrak{R}$), $N(\mathfrak{m};\mathfrak{n})$, is the $\mathfrak{R}$-module generated by the elements $N(\alpha;\beta)$, for all α, β satisfying

$$\mathfrak{m} \supseteq \mathfrak{R}.(\alpha), \quad \mathfrak{n} \subseteq \mathfrak{R}.(\beta).$$

It is an immediate consequence of (3.1) that $N(\mathfrak{m};\mathfrak{n})$ *is a non-null* $\mathfrak{R}$*-ideal.* Further, from (3.1) and (3.2),

(3.4) If $\mathfrak{m} \subseteq \mathfrak{n}$ (both members of H), then $N(\mathfrak{m};\mathfrak{n}) \subseteq \mathfrak{R}$, $\mathfrak{n}N(\mathfrak{m};\mathfrak{n}) \subseteq \mathfrak{m}$.

(3.5)† If $\mathfrak{m}_1, \ldots, \mathfrak{m}_4 \in H$,

$$N(\mathfrak{m}_1;\mathfrak{m}_2)\,N(\mathfrak{m}_3;\mathfrak{m}_4) = N(\mathfrak{m}_1;\mathfrak{m}_4)\,N(\mathfrak{m}_3;\mathfrak{m}_2).$$

A property of complementary modules is relevant at this point:

(3.6) Provided $\mathfrak{m}$ belongs to H, $\mathfrak{m}^{**}$ is the intersection of all modules $\mathfrak{n}$ which contain $\mathfrak{m}$ and possess an n-term $\mathfrak{R}$-basis.

Any such $\mathfrak{n}$ contains $\mathfrak{m}^{**}$, because $\mathfrak{n}^{**} = \mathfrak{n}$. The fact that $\bigcap \mathfrak{n} \subseteq \mathfrak{m}^{**}$ is seen by remarking that $\mathfrak{m}^*$ (which also belongs to H) is the union of modules of the form $\mathfrak{R}.(\omega)$, with ω linearly independent over K.

(3.7) For any $\mathfrak{m}, \mathfrak{n} \in H$, $N(\mathfrak{m};\mathfrak{n}) = N(\mathfrak{m};\mathfrak{n}^{**})$. If $\mathfrak{m} = \mathfrak{m}^{**}$, $N(\mathfrak{m};\mathfrak{n}) = N(\mathfrak{n}^*;\mathfrak{m}^*)$.

The first assertion follows from (3.6); the second from the first and (3.3).

Local theory. For any prime ideal $\mathfrak{p}$ of $\mathfrak{R}$, let $N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n})$ denote the norm of $\mathfrak{m}\mathfrak{R}_{\mathfrak{p}}$ with respect to $\mathfrak{n}\mathfrak{R}_{\mathfrak{p}}$ (over $\mathfrak{R}_{\mathfrak{p}}$).

THEOREM 4. *If* $\mathfrak{m}, \mathfrak{n} \in H$, *and if* $\mathfrak{n}$ *has a finite* $\mathfrak{R}$*-basis,* $N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n}) = \mathfrak{R}_{\mathfrak{p}}.N(\mathfrak{m};\mathfrak{n})$. *Under the same conditions*

$$N(\mathfrak{m};\mathfrak{n}) = \bigcap N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n}),$$

where $\mathfrak{p}$ *runs through all maximal ideals of* $\mathfrak{R}$.

Proof. It is clear that $N(\mathfrak{m};\mathfrak{n}) \subseteq N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n})$, and in fact that $\mathfrak{R}_{\mathfrak{p}}.N(\mathfrak{m};\mathfrak{n}) \subseteq N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n})$, the latter being an $\mathfrak{R}_{\mathfrak{p}}$-ideal. On the other hand, consider any α, β such that $\mathfrak{m}\mathfrak{R}_{\mathfrak{p}} \supseteq \mathfrak{R}_{\mathfrak{p}}.(\alpha)$, $\mathfrak{n}\mathfrak{R}_{\mathfrak{p}} \subseteq \mathfrak{R}_{\mathfrak{p}}.(\beta)$. There exists $u \in \mathfrak{R}$ such that $\mathfrak{m} \supseteq \mathfrak{R}.(u\alpha)$, $u \not\equiv 0 \bmod \mathfrak{p}$; because $\mathfrak{n}$ has a finite $\mathfrak{R}$-basis, there also exists $v \in \mathfrak{R}$ such that $v\mathfrak{n} \subseteq \mathfrak{R}.(\beta)$, $v \not\equiv 0 \bmod \mathfrak{p}$. From these relations it follows that

$$(uv)^n\,N(\alpha;\beta) = N(u\alpha;v^{-1}\beta) \in N(\mathfrak{m};\mathfrak{n}).$$

This shows that $N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n}) \subseteq \mathfrak{R}_{\mathfrak{p}}.N(\mathfrak{m};\mathfrak{n})$, and completes the proof that

$$N_{\mathfrak{p}}(\mathfrak{m};\mathfrak{n}) = \mathfrak{R}_{\mathfrak{p}}.N(\mathfrak{m};\mathfrak{n}).$$

The intersection formula follows from (8.1).

(3.8) Suppose that $\mathfrak{m}, \mathfrak{n} \in H$, and that $\mathfrak{n}$ has a finite $\mathfrak{R}$-basis. If $N(\mathfrak{m};\mathfrak{n})$ is an inversive $\mathfrak{R}$-ideal, then $\mathfrak{m}\mathfrak{R}_{\mathfrak{p}}$ and $\mathfrak{n}^*\mathfrak{R}_{\mathfrak{p}}$ have $\mathfrak{R}_{\mathfrak{p}}$-bases of n terms, for every prime ideal $\mathfrak{p}$ of $\mathfrak{R}$.

† The special case $N(\mathfrak{m}_1;\mathfrak{m}_2)\,N(\mathfrak{m}_2;\mathfrak{m}_3) = N(\mathfrak{m}_1;\mathfrak{m}_3)\,N(\mathfrak{m}_2;\mathfrak{m}_2)$ is an analogue of the classical formula $N(\mathfrak{a}_1;\mathfrak{a}_2)\,N(\mathfrak{a}_2;\mathfrak{a}_3) = N(\mathfrak{a}_1;\mathfrak{a}_3)$. See also (3.9).

Downloaded from rsta.royalsocietypublishing.org

Proof. Assume for the moment that $\mathfrak{R} = \mathfrak{R}_\mathfrak{p}$. According to (8.6) and (8.8), there exist $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ satisfying the relations $\mathfrak{R}.(\boldsymbol{\alpha}) \subseteq \mathfrak{m}$, $\mathfrak{R}.(\boldsymbol{\beta}) \supseteq \mathfrak{n}$, and such that $N(\boldsymbol{\alpha};\boldsymbol{\beta})$ is a generating element for the principal ideal $N(\mathfrak{m};\mathfrak{n})$. Any γ of $\mathfrak{m}$ is expressible as

$$\gamma = c_1\alpha_1 + \ldots + c_n\alpha_n \ (c_i \in K),$$

where

$$c_1 = N(\gamma, \alpha_2, \ldots, \alpha_n;\boldsymbol{\alpha})$$
$$= N(\gamma, \alpha_2, \ldots, \alpha_n;\boldsymbol{\beta})\, N(\boldsymbol{\beta};\boldsymbol{\alpha}),$$

so that

$$c_1 \in N(\mathfrak{m};\mathfrak{n})\, N(\boldsymbol{\beta};\boldsymbol{\alpha}) = \mathfrak{R}.$$

Similarly $c_2, \ldots, c_n \in \mathfrak{R}$, whence $\mathfrak{m} = \mathfrak{R}.(\boldsymbol{\alpha})$. It follows from this result and (3.7) that

$$N(\mathfrak{n}^*;\mathfrak{m}^*) = N(\mathfrak{m};\mathfrak{n});$$

and thence, by a repetition of the argument, that the basis complementary to $\boldsymbol{\beta}$ is an $\mathfrak{R}$-basis for $\mathfrak{n}^*$. In the general case $(\mathfrak{R} + \mathfrak{R}_\mathfrak{p})$, (3.8) follows from the preceding proof and (1.8) and the equation

$$\mathfrak{R}_\mathfrak{p}.N(\mathfrak{m};\mathfrak{n}) = N_\mathfrak{p}(\mathfrak{m};\mathfrak{n}).$$

(3.9) Let $\mathfrak{m}$ be a finite $\mathfrak{R}$-module of the class H. Then a necessary and sufficient condition for the equation

$$N(\mathfrak{m};\mathfrak{m}) = \mathfrak{R}$$

is that $\mathfrak{m}\mathfrak{R}_\mathfrak{p}$ have an $\mathfrak{R}_\mathfrak{p}$-basis of n terms, for every maximal ideal $\mathfrak{p}$ of $\mathfrak{R}$.

The necessity follows from (3.8), and the sufficiency from Theorem 4.

(3.10) If $\mathfrak{m}, \mathfrak{n} \in H$, if $\mathfrak{n}$ has a finite $\mathfrak{R}$-basis, and if $\mathfrak{g}$ is an inversive $\mathfrak{R}$-ideal,

$$N(\mathfrak{g}\mathfrak{m};\mathfrak{n}) = \mathfrak{g}^n N(\mathfrak{m};\mathfrak{n}).$$

Because $\mathfrak{g}\mathfrak{R}_\mathfrak{p}$ is a principal ideal (by (8.6)), and by Theorem 4,

$$N_\mathfrak{p}(\mathfrak{g}\mathfrak{m};\mathfrak{n}) = \mathfrak{g}^n\mathfrak{R}_\mathfrak{p}.\, N_\mathfrak{p}(\mathfrak{m};\mathfrak{n}) = \mathfrak{R}_\mathfrak{p}.\,\mathfrak{g}^n N(\mathfrak{m};\mathfrak{n}).$$

Hence $N(\mathfrak{g}\mathfrak{m};\mathfrak{n}) = \cap\, \mathfrak{R}_\mathfrak{p}.\,\mathfrak{g}^n N(\mathfrak{m};\mathfrak{n}) = \mathfrak{g}^n N(\mathfrak{m};\mathfrak{n})$.

(3.11) If $\mathfrak{a}, \mathfrak{b}$ are non-null $\mathfrak{S}$-ideals, $\mathfrak{h}$ an inversive $\mathfrak{S}$-ideal, and $\mathfrak{S}$ and $\mathfrak{b}$ have finite $\mathfrak{R}$-bases, then $N(\mathfrak{a};\mathfrak{b}) = N(\mathfrak{a}\mathfrak{h};\mathfrak{b}\mathfrak{h})$. Subject to the same conditions on $\mathfrak{a}, \mathfrak{h}$, and $\mathfrak{S}$,

$$N(\mathfrak{a}\mathfrak{h};\mathfrak{S})\, N(\mathfrak{S};\mathfrak{S}) = N(\mathfrak{a};\mathfrak{S})\, N(\mathfrak{h};\mathfrak{S}).$$

The conditions imply that $\mathfrak{h}$ has a finite $\mathfrak{R}$-basis, by (8.5). The first equation is another deduction from Theorem 4: $N_\mathfrak{p}(\mathfrak{a};\mathfrak{b}) = N_\mathfrak{p}(\mathfrak{a}\mathfrak{h};\mathfrak{b}\mathfrak{h})$, because $\mathfrak{h}\mathfrak{R}_\mathfrak{p}$ is a principal ideal† of $\mathfrak{S}_\mathfrak{p}$. The second equation follows from the first, using (3.5).

Connexion with $\mathfrak{D}$. An inspection of (3.3) shows that in every case

$$N(\mathfrak{S};\mathfrak{e}) \supseteq \mathfrak{D}.$$

If $\mathfrak{S}$ (and therefore $\mathfrak{e}$) has an n-term $\mathfrak{R}$-basis, the sign of equality will hold. This last remark can be extended, in the usual way, by means of Theorem 4; using (1.7), we deduce

(3.12) Suppose that $\mathfrak{S}$ and $\mathfrak{e}$ have finite $\mathfrak{R}$-bases, and that $\mathfrak{S}_\mathfrak{p}$ has an n-term $\mathfrak{R}_\mathfrak{p}$-basis, for every maximal ideal $\mathfrak{p}$ of $\mathfrak{R}$. Then $N(\mathfrak{S};\mathfrak{e}) = \mathfrak{D}$.

† $\mathfrak{h}\mathfrak{R}_\mathfrak{p} = \mathfrak{h}\mathfrak{S}_\mathfrak{p}$ is a principal ideal of $\mathfrak{S}_\mathfrak{p}$ by (8.6)—the maximal ideals of $\mathfrak{S}_\mathfrak{p}$, which are those lying over $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$, are finite in number, as noted in § 4.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES
PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Downloaded from rsta.royalsocietypublishing.org

(3.13) If† $\mathfrak{e}^* = \mathfrak{S}$, $N(\mathfrak{S};\mathfrak{e})$ is integrally dependent on $\mathfrak{D}$.

Proof. Consider any $\mathfrak{a}$ and $\mathfrak{b}^*$ such that $\mathfrak{R}.(\mathfrak{a}) \subseteq \mathfrak{S}$, $\mathfrak{R}.(\mathfrak{b}^*) \supseteq \mathfrak{e}$; denote the basis complementary to $\mathfrak{b}^*$ by $\mathfrak{b}$. As noted in (3.3), $\{N(\mathfrak{a};\mathfrak{b}^*)\}^2 = D(\mathfrak{a})\,D(\mathfrak{b})$. Because $\mathfrak{e}^* = \mathfrak{S}$, $\mathfrak{b}$ is contained in $\mathfrak{S}$. Thus $N(\mathfrak{S};\mathfrak{e})$, being generated by certain elements whose squares belong to $\mathfrak{D}^2$, is integrally dependent on $\mathfrak{D}$.

4. General ramification theory

As a preliminary to the main topics of this and the following sections, the existence and properties of the prime ideals of $\mathfrak{S}$ which lie over a given prime ideal of $\mathfrak{R}$ must first be considered. A prime $\mathfrak{S}$-ideal $\mathfrak{q}$ is said to *lie over* $\mathfrak{p}$ if $\mathfrak{q} \cap \mathfrak{R} = \mathfrak{p}$.

Because $\mathfrak{S}$ is integrally dependent on $\mathfrak{R}$, $\mathfrak{S}/\mathfrak{q}$ is integrally dependent on $(\mathfrak{R}+\mathfrak{q})/\mathfrak{q}$, for any prime ideal $\mathfrak{q}$ of $\mathfrak{S}$. The degree and reduced degree of the quotient field of $\mathfrak{S}/\mathfrak{q}$ (the *residue field* of $\mathfrak{q}$) over that of $(\mathfrak{R}+\mathfrak{q})/\mathfrak{q}$ are called the *degree* and *reduced degree* of $\mathfrak{q}$ over $\mathfrak{R}$. By a well-known identification principle,‡ $(\mathfrak{R}+\mathfrak{q})/\mathfrak{q}$ may be identified with $\mathfrak{R}/\mathfrak{p}$, where $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{R}$. Thus one may speak of the degree, separability, etc., of the residue field of $\mathfrak{q}$ over that of $\mathfrak{p}$. When $\mathfrak{p}$ is maximal, any polynomial over $\mathfrak{R}$ is congruent mod $\mathfrak{p}$ to a product of polynomials irreducible mod $\mathfrak{p}$, and this factorization mod $\mathfrak{p}$ is unique mod $\mathfrak{p}$.

(4.1) Suppose that $\mathfrak{p}$ is maximal, and that $\mathfrak{q}$ is a prime $\mathfrak{S}$-ideal lying over $\mathfrak{p}$. Let θ be any element of $\mathfrak{S}[y_1, \ldots, y_m]$, where $y_1, \ldots, y_m$ are indeterminates. Then there exists a polynomial $g(x; y_1, \ldots, y_m)$ over $\mathfrak{R}$, monic in x, such that

(i) $g(x; y_1, \ldots, y_m)$ is irreducible mod $\mathfrak{p}$;

(ii) $g(\theta; y_1, \ldots, y_m) \equiv 0 \ (\mathfrak{q})$;

(iii) every polynomial $h(x; y_1, \ldots, y_m)$ over $\mathfrak{R}$, such that $h(\theta; y_1, \ldots, y_m) \equiv 0 \ (\mathfrak{q})$, is divisible mod $\mathfrak{p}$ by $g(x; y_1, \ldots, y_m)$.

In fact, let $\bar{\theta}$ be the image of θ in $\mathfrak{L}[y_1, \ldots, y_m]$, where $\mathfrak{L} = \mathfrak{S}/\mathfrak{q}$, $\mathfrak{k} = \mathfrak{R}/\mathfrak{p}$. The minimal polynomial $\bar{g}(x)$ of $\bar{\theta}$ over $\mathfrak{k}(y_1, \ldots, y_m)$ has its coefficients in $\mathfrak{k}[y_1, \ldots, y_m]$, because the latter is integrally closed. Take $g(x; y_1, \ldots, y_m)$ to be a polynomial over $\mathfrak{R}$ monic in x, whose image mod $\mathfrak{p}$ is $\bar{g}(x; y_1, \ldots, y_m) = \bar{g}(x)$. The proof is completed by applications of Gauss's Lemma.

The polynomial $g(x)$ of (4.1), whose non-leading coefficients naturally are only unique mod $\mathfrak{p}$, is known as the *minimal polynomial of* θ mod $\mathfrak{q}$.

(4.2) The prime $\mathfrak{S}$-ideals lying over $\mathfrak{p}$ correspond 1-1 with the prime $\mathfrak{S}_\mathfrak{p}$-ideals lying over $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$, the correspondence being that between contracted and extended ideals.

The assertion follows from the theory of quotient rings (e.g. from Grundy 1942, § 13).

(4.3) Suppose $\mathfrak{q}$ is a prime $\mathfrak{S}$-ideal lying over $\mathfrak{p}$. Then the quotient ring of $\mathfrak{S}_\mathfrak{p}$ with respect to $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ is $\mathfrak{S}_\mathfrak{q}$. In the 1-1 correspondence (of extended and contracted ideals) between all integral $\mathfrak{S}_\mathfrak{p}$-ideals and those integral $\mathfrak{S}$-ideals $\mathfrak{a}$ such that $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}$, (i) $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$-primary ideals of $\mathfrak{S}_\mathfrak{p}$ correspond to $\mathfrak{q}$-primary ideals of $\mathfrak{S}$; (ii) the isolated component of $\mathfrak{p}\mathfrak{S}_\mathfrak{p}$ with respect to $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ corresponds to $(\mathfrak{p}\mathfrak{S})_\mathfrak{q}$.

† I.e. if $\mathfrak{e}:\mathfrak{e} = \mathfrak{S}$. This will certainly be the case if $\mathfrak{S}$ is totally closed. On integral dependence of ideals, and totally closed domains, cf. Lorenzen (1939).

‡ Krull (1935, p. 3). Corresponding elements in the natural isomorphism between $(\mathfrak{R}+\mathfrak{q})/\mathfrak{q}$ and $\mathfrak{R}/(\mathfrak{q} \cap \mathfrak{R})$ are identified.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Downloaded from rsta.royalsocietypublishing.org

For proof, every element of the quotient ring $\mathfrak{H}$ of $\mathfrak{S}_\mathfrak{p}$ with respect to $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ is expressible as $\alpha a^{-1}(\beta b^{-1})^{-1}$, with $\alpha, \beta \in \mathfrak{S}$; $a, b \in \mathfrak{R}$; $a, b \not\equiv 0 \bmod \mathfrak{p}$; $\beta \not\equiv 0 \bmod \mathfrak{q}$. Since $\alpha a^{-1}(\beta b^{-1})^{-1} = \alpha b(a\beta)^{-1}$, it is clear that $\mathfrak{H} \subseteq \mathfrak{S}_\mathfrak{q}$. The reverse inequality, $\mathfrak{H} \supseteq \mathfrak{S}_\mathfrak{q}$, follows from the fact that

$$(\mathfrak{q}\mathfrak{S}_\mathfrak{p}) \cap \mathfrak{S} = \mathfrak{q}.$$

Of the remarks about the 1-1 correspondence, (i) follows from quotient-ring theory (e.g. from Grundy 1942, § 13). Finally, the result just proved for $\mathfrak{H}$ shows that the isolated component of $\mathfrak{p}\mathfrak{S}_\mathfrak{p}$ with respect to $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ is $(\mathfrak{p}\mathfrak{S}_\mathfrak{q}) \cap \mathfrak{S}_\mathfrak{p}$; and to justify (ii) it is only necessary to add that $(\mathfrak{p}\mathfrak{S}_\mathfrak{q}) \cap \mathfrak{S}_\mathfrak{p} \cap \mathfrak{S} = (\mathfrak{p}\mathfrak{S}_\mathfrak{q}) \cap \mathfrak{S} = (\mathfrak{p}\mathfrak{S})_\mathfrak{q}$.

(4.4) Suppose $\mathfrak{q}$ is a prime $\mathfrak{S}$-ideal lying over $\mathfrak{p}$, the residue field of $\mathfrak{p}$ being embedded in that of $\mathfrak{q}$ according to the identification principle. Then another application of the identification principle sends these fields into the residue fields of $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$ and $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ respectively.

Like (4.1)–(4.3), this is a known result often encountered without formal statement or proof. The identification principle requires us to start by identifying $\mathfrak{R}/\mathfrak{p}$ with the subring $(\mathfrak{R}+\mathfrak{q})/\mathfrak{q}$ of $\mathfrak{S}/\mathfrak{q}$. These integral domains may in turn be simultaneously identified† with $R = (\mathfrak{R}+\mathfrak{q}\mathfrak{S}_\mathfrak{p})/\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ and $S = (\mathfrak{S}+\mathfrak{q}\mathfrak{S}_\mathfrak{p})/\mathfrak{q}\mathfrak{S}_\mathfrak{p}$. The residue fields of $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$ and $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ are identified with the quotient fields of $\mathfrak{k} = (\mathfrak{R}_\mathfrak{p}+\mathfrak{q}\mathfrak{S}_\mathfrak{p})/\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ and $\mathfrak{L} = \mathfrak{S}_\mathfrak{p}/\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ respectively. Clearly $R \subseteq \mathfrak{k}$, $S \subseteq \mathfrak{L}$. That $\mathfrak{k}$ is contained in the quotient field of R follows from the definition of $\mathfrak{R}_\mathfrak{p}$, and because any element of $\mathfrak{R}$ not in $\mathfrak{p}$ is not in $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$; similarly $\mathfrak{L}$ is contained in the quotient field of S. (Actually, both $\mathfrak{k}$ and $\mathfrak{L}$ are fields.)

THEOREM 5. *Given any prime ideal* $\mathfrak{p}$ *of* $\mathfrak{R}$, *there exists a prime ideal* $\mathfrak{q}$ *of* $\mathfrak{S}$ *lying over* $\mathfrak{p}$.

This is one of a series of existence-theorems proved by Krull (1937). The theorems in question hold under conditions more general than those postulated throughout Part I of this paper—as a matter of fact, that is true of almost all the results of this section. The proof of Theorem 5 reduces essentially to the remarks that unity cannot be integrally dependent on the prime ideal $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$; so Theorem 14 supplies a prime ideal of $\mathfrak{S}_\mathfrak{p}$ which contains $\mathfrak{p}\mathfrak{S}_\mathfrak{p}$, and consequently lies over $\mathfrak{p}\mathfrak{R}_\mathfrak{p}$. In the paper of Krull (1937), again, (4.5)–(4.7) are deduced rapidly from the form of Theorem 5 proved there—

(4.5) A prime $\mathfrak{S}$-ideal $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ $(= \mathfrak{q} \cap \mathfrak{R})$ is maximal.

(4.6) If $\mathfrak{q}$ lies over $\mathfrak{p}$, $\mathfrak{q}\mathfrak{S}_\mathfrak{p}$ is a minimal prime over-ideal of $\mathfrak{p}\mathfrak{S}_\mathfrak{p}$. As $\mathfrak{q}_\tau$ runs through the distinct prime $\mathfrak{S}$-ideals lying over $\mathfrak{p}$, $\mathfrak{q}_\tau\mathfrak{S}_\mathfrak{p}$ runs through all the distinct maximal ideals of $\mathfrak{S}_\mathfrak{p}$.

(4.7) If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are distinct prime $\mathfrak{S}$-ideals lying over the same prime ideal of $\mathfrak{R}$, $\mathfrak{q}_1 \nsubseteq \mathfrak{q}_2$.

For the discussion of ramification theory proper, some further deductions from Theorem 5 are needed. (4.8) and (4.9) are similar to results already used by Krull (1939*a*). First, combining (8.1), (4.6), and (4.3), it is seen that $\mathfrak{b}\mathfrak{S}_\mathfrak{p} = \bigcap \mathfrak{b}\mathfrak{S}_{\mathfrak{q}_\tau}$ for any $\mathfrak{S}$-ideal $\mathfrak{b}$, whence $\mathfrak{b}_\mathfrak{p} = \bigcap \mathfrak{b}_{\mathfrak{q}_\tau}$ provided $\mathfrak{b} \subseteq \mathfrak{S}$. It follows that

(4.8) As $\mathfrak{q}_\tau$ runs through the distinct prime $\mathfrak{S}$-ideals lying over $\mathfrak{p}$,

$$\mathfrak{S}_\mathfrak{p} = \bigcap \mathfrak{S}_{\mathfrak{q}_\tau} \quad \text{(quotient rings)},$$

$$(\mathfrak{a}\mathfrak{S})_\mathfrak{p} = \bigcap (\mathfrak{a}\mathfrak{S})_{\mathfrak{q}_\tau} \quad \text{(isolated components in } \mathfrak{S}),$$

† The identifications are correct because by the modular axiom

$$(\mathfrak{R}+\mathfrak{q}) \cap \mathfrak{q}\mathfrak{S}_\mathfrak{p} = (\mathfrak{R} \cap \mathfrak{q}\mathfrak{S}_\mathfrak{p}) + \mathfrak{q} = \mathfrak{p} + \mathfrak{q} = \mathfrak{q},$$

and because $\mathfrak{S} \cap \mathfrak{q}\mathfrak{S}_\mathfrak{p} = \mathfrak{q}$.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES
PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Downloaded from rsta.royalsocietypublishing.org

where $\mathfrak{a}$ is any integral ideal of $\mathfrak{R}$. If $\mathfrak{p}$ is a minimal prime over-ideal of $\mathfrak{a}$, the isolated components $(\mathfrak{a}\mathfrak{S})_{\mathfrak{q}_\tau}$ are respectively $\mathfrak{q}_\tau$-primary ((4.7) and Theorem 15).

When $\mathfrak{p}$ is a maximal ideal, and $\mathfrak{a}$ is $\mathfrak{p}$-primary, every element of $\mathfrak{R}$ not in $\mathfrak{p}$ has in $\mathfrak{R}$ an inverse mod $\mathfrak{a}$. It is easy to deduce that $(\mathfrak{a}\mathfrak{S})_{\mathfrak{p}} = \mathfrak{a}\mathfrak{S}$; hence a refinement of (4.8) is obtained:

(4.9) If $\mathfrak{p}$ is maximal, and $\mathfrak{a}$ is $\mathfrak{p}$-primary, then

$$\mathfrak{a}\mathfrak{S} = \bigcap (\mathfrak{a}\mathfrak{S})_{\mathfrak{q}_\tau},$$

with the $\mathfrak{q}_\tau$ as in (4.8). In particular, $\mathfrak{a}$ may be any power of $\mathfrak{p}$, by (8.4).

(4.10) Let $y_1, \ldots, y_m$ be indeterminates. An element A of $\mathfrak{S}[y_1, \ldots, y_m]$ is congruent to zero mod $\bigcap \mathfrak{q}_\tau$ if and only if, in the minimal equation $A^k + a_1 A^{k-1} + \ldots + a_k = 0$ of A over $K(y_1, \ldots, y_m)$, the coefficients a_i are all congruent to zero mod $\mathfrak{p}$.

Proof.† The condition stated is obviously sufficient for A to be congruent to zero mod $\bigcap \mathfrak{q}_\tau$. In the proof of its necessity, let the coefficients of the distinct power-products in A be $\alpha_1, \ldots, \alpha_l$. Let M_1 be the smallest normal extension-field of K containing $\alpha_1, \ldots, \alpha_l$; let M_2 be the smallest field containing M_1 and L, $\mathfrak{T}_1$ the integral closure of $\mathfrak{R}$ in M_1, and $\mathfrak{T}_2$ the integral closure of $\mathfrak{R}$ in M_2. Every prime $\mathfrak{T}_2$-ideal $\mathfrak{r}$ lying over $\mathfrak{p}$ lies over one of the $\mathfrak{q}_\tau$, and consequently contains $\alpha_1, \ldots, \alpha_l$. By Theorem 5, every prime $\mathfrak{T}_1$-ideal $\mathfrak{s}$ lying over $\mathfrak{p}$ is the contracted ideal of such an $\mathfrak{r}$. Hence $\alpha_1, \ldots, \alpha_l \in \bigcap \mathfrak{s}$; and this property is shared by the conjugates of the α_i over K, since the aggregate of all $\mathfrak{s}$ is obviously invariant under the Galois group of M_1 over K. It follows that $a_1, \ldots, a_k$ are congruent to zero mod $\mathfrak{R} \cap (\bigcap \mathfrak{s}) = \mathfrak{p}$.

(4.11) The number of prime ideals of $\mathfrak{S}$ lying over $\mathfrak{p}$ is finite, at most n.

The finiteness could be deduced from the Conjugates Theorem of Krull (1937), but a direct proof of (4.11) is easy. Assume, without loss of generality, that $\mathfrak{p}$ is maximal. If there existed distinct $\mathfrak{q}_0, \ldots, \mathfrak{q}_n$ lying over $\mathfrak{p}$, one could choose $\gamma_i \in \mathfrak{S}$, making $y_0\gamma_0 + \ldots + y_n\gamma_n$ congruent to $y_i \bmod \mathfrak{q}_i$ (y_i indeterminates; $i = 0, \ldots, n$); the characteristic polynomial of $y_0\gamma_0 + \ldots + y_n\gamma_n$ would have the $n+1$ mod $\mathfrak{p}$ factors $x - y_0, \ldots, x - y_n$, which is impossible.

Conventions. For the rest of Part I, the prime ideals of $\mathfrak{S}$ lying over $\mathfrak{p}$ will be denoted by $\mathfrak{q}_1, \ldots, \mathfrak{q}_e$. The degree (finite or ∞) of $\mathfrak{q}_i$ will be denoted by n_i, and its reduced degree by n_i'. The ramification rank ρ_i of $\mathfrak{q}_i$ is defined in § 6.

(4.12) We have $\mu(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_e)^n \subseteq \mathfrak{p}\mathfrak{S}$, where μ is $n!$ times the unity element of $\mathfrak{R}$. If the residue field of $\mathfrak{p}$ has characteristic zero, $\mathfrak{q}_i^n \subseteq (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ ($i = 1, \ldots, e$).

The first assertion is obtained by putting $A = y_1\gamma_1 + \ldots + y_n\gamma_n$ in (4.10), with any

$$\gamma_1, \ldots, \gamma_n \in (\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_e),$$

and considering the coefficient of $y_1 \ldots y_n$. *A fortiori* $\mu(\mathfrak{q}_1 \ldots \mathfrak{q}_e)^n \subseteq \mathfrak{p}\mathfrak{S}$, so by (4.7) the second assertion follows.

THEOREM 6 (general discriminant theorem).‡

(1) $n_1' + \ldots + n_e' \leqslant n$, *with equality if and only if* $\mathfrak{p} \nmid \mathfrak{D}$.

(2) *If* $\mathfrak{p} \nmid \mathfrak{D}$, *then* $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i} = \mathfrak{q}_i$, *and the residue field of* $\mathfrak{q}_i$ *is separable over that of* $\mathfrak{p}$, *for all* $i = 1, \ldots, e$.

† Cf. Krull (1939*a*), part (*c*) of the proof of the general discriminant theorem. We give the proof of (4.10) in a form which clearly holds for any L algebraic over K, not necessarily finite or separable.

‡ This comprehensive statement comprises Theorems 2, 3, and 5 of Krull (1939*a*); but Krull does not assume that L is separable over K.

Downloaded from rsta.royalsocietypublishing.org

The proof of Theorem 6 also discloses that, when $\mathfrak{p} \nmid \mathfrak{D}$, and $\mathfrak{R}/\mathfrak{p}$ has an infinite number of elements, there exists $\alpha \in \mathfrak{S}$ such that $D(\alpha) \not\equiv 0 \bmod \mathfrak{p}$. When $\mathfrak{p} \nmid \mathfrak{D}$, and $\mathfrak{p}$ is maximal, elements $\omega_1, \ldots, \omega_n$ of $\mathfrak{S}$ form an $\mathfrak{R}/\mathfrak{p}$-basis for $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ if and only if $D(\omega_1, \ldots, \omega_n) \not\equiv 0 \bmod \mathfrak{p}$. These corollaries are equally relevant as supplements to Theorems 7 and 10.

It goes without saying that the general discriminant theorem contributes enormously towards the solution of the central problems of ramification theory—viz. *Given* $\mathfrak{p}$, *what can be said about* (*a*) *the isolated primary components* $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ *of* $\mathfrak{p}\mathfrak{S}$, *and* (*b*) *the residue fields of the* $\mathfrak{q}_i$? The theorem provides a sufficient condition for the $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ to be prime ideals, coupled with the separability of the residue fields of the $\mathfrak{q}_i$; but that condition is not universally necessary, as Krull himself has remarked. It will be shown, in Theorem 7, that the condition is necessary as well as sufficient when $\mathfrak{S}$ has a finite $\mathfrak{R}$-basis. A related question, of some importance in geometrical applications, is whether $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1} = \mathfrak{q}_1$, and the residue field of $\mathfrak{q}_1$ is separable, irrespective of the behaviour of $\mathfrak{q}_2, \ldots, \mathfrak{q}_e$. That is a question untouched by the general discriminant theorem; it is solved, under the assumption that $\mathfrak{p}$ is 'strongly convergent', by Theorem 13.

THEOREM 7.† *Suppose that* $\mathfrak{S}$ *has a finite* $\mathfrak{R}$*-basis. Then the following two propositions are equivalent:* (i) $\mathfrak{p} \nmid \mathfrak{D}$*;* (ii) $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i} = \mathfrak{q}_i$, *and the residue field of* $\mathfrak{q}_i$ *is separable over that of* $\mathfrak{p}$, *for all* $i = 1, \ldots, e$.

With Theorem 6 already available, it only remains to show that (ii) implies the inequality $n'_1 + \ldots + n'_e \geqslant n$. The problem is transferred to $\mathfrak{R}_{\mathfrak{p}}$ and $\mathfrak{S}_{\mathfrak{p}}$ by (4.3) and (4.4), so it may be assumed without loss of generality that $\mathfrak{p}$ is a maximal ideal. In that case, when (ii) holds, $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ is a semi-simple separable algebra of rank $n'_1 + \ldots + n'_e$ over $\mathfrak{R}/\mathfrak{p}$. By Theorem 2 (2), the rank of $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ over $\mathfrak{R}/\mathfrak{p}$ is at least n.

5. LEMMAS ON CONVERGENT PRIME IDEALS

It has been mentioned that certain problems in ramification theory are untouched by the theory of the discriminant-ideal, as represented by Theorems 6 and 7. The rest of Part I is devoted to such problems. The results of §§ 6 and 7, applicable to *strongly convergent* prime ideals, are generalizations of the main classical theorems on prime ideal structure associated with the classical different-theorem.‡ The need for such generalizations is placed beyond doubt by the fact that a case of Theorem 13 has already been used in the geometrical papers of Zariski. In § 7 there is also a discriminant theorem, Theorem 10, which to some extent overlaps Theorem 7. If the maximal condition holds in $\mathfrak{R}$, every prime ideal of $\mathfrak{R}$ is strongly

† The statement and proof of Theorem 7 would clearly remain valid if, contrary to one of the conditions laid down in the Introduction, L were inseparable over K.

‡ Cf. Krull (1939*b*), Fricke (1928), Dedekind & Weber (1882). The classical different-theorem is not actually a special case of Theorem 13, but can be deduced from Theorem 8 by a similar method. Theorems for *minimal* prime ideals, deducible from the classical theorems by the method of prime ideal quotient rings (as indicated in n. 35 of Krull (1935)), are likewise included in the results of §§ 6 and 7. The preceding remarks about the classical different-theorem do not apply to the more penetrating ramification theorem of Grell (1936).

The first step towards a generalization of the kind effected here was taken by Zariski, who proved special cases of Theorems 9 and 13 (Theorems 4 and 7 of Zariski (1939); Theorem 11 of Zariski (1940)). As far as I am aware, the only previous theorems of this type other than those mentioned above, apart from the general discriminant theorem, are to be found in the theory of complete (rank 1) evaluated fields.

Downloaded from rsta.royalsocietypublishing.org

convergent (Krull 1928). Thus the results on strongly convergent prime ideals are valid in the integral domains most frequently used in algebraic geometry.

The key to the theorems on prime ideal structure is Theorem 8, proved in § 6 for *convergent* prime ideals. This represents a further gain in generality; the maximal ideal of a rank 1 valuation ring is always convergent, but is strongly convergent only in the simple case when the valuation is discrete.

The present section is entirely occupied by lemmas. Notwithstanding the title, Lemmas 3, 5, and 6 are independent of the notion of convergence.

Definitions. A prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ is *convergent* if

$$\lim_{r\to\infty}(\mathfrak{a}^r)_{\mathfrak{p}} = (0),$$

for every $\mathfrak{R}$-ideal $\mathfrak{a}\subseteq\mathfrak{p}$ with a finite $\mathfrak{R}$-basis; $\mathfrak{p}$ is *strongly convergent* if

$$\lim_{r\to\infty}(\mathfrak{p}^r)_{\mathfrak{p}} = (0).$$

(5.1) $\mathfrak{p}$ is convergent if and only if the maximal ideal $\mathfrak{p}\mathfrak{R}_{\mathfrak{p}}$ of $\mathfrak{R}_{\mathfrak{p}}$ is convergent, and $\mathfrak{p}$ is strongly convergent if and only if $\mathfrak{p}\mathfrak{R}_{\mathfrak{p}}$ is strongly convergent.

That the convergence of $\mathfrak{p}\mathfrak{R}_{\mathfrak{p}}$ is sufficient for the convergence of $\mathfrak{p}$ is made obvious by the relation $(\mathfrak{a}^r)_{\mathfrak{p}} = (\mathfrak{a}^r\mathfrak{R}_{\mathfrak{p}})\cap\mathfrak{R}$. To prove its necessity, note that any $\mathfrak{R}_{\mathfrak{p}}$-finite ideal $\mathfrak{b}\subseteq\mathfrak{p}\mathfrak{R}_{\mathfrak{p}}$ has the form $\mathfrak{b} = \mathfrak{a}\mathfrak{R}_{\mathfrak{p}}$, where $\mathfrak{a}\subseteq\mathfrak{p}$ is an $\mathfrak{R}$-ideal with a finite $\mathfrak{R}$-basis. If

$$u^{-1}a \ (u, a\in\mathfrak{R}; a\neq 0; u\not\equiv 0 \bmod \mathfrak{p})$$

belonged to $\mathfrak{b}^r$ for all r, a would belong to $\mathfrak{b}^r\cap\mathfrak{R} = (\mathfrak{a}^r)_{\mathfrak{p}}$ for all r, contrary to the definition of convergence. The proof of (5.1) for strong convergence is similar.

LEMMA 2. *Let $\alpha, \beta_1, \ldots, \beta_t$ be elements of $\mathfrak{S}$, and $\mathfrak{a}\subseteq\mathfrak{p}$ an $\mathfrak{R}$-ideal with a finite basis. If $\mathfrak{p}$ is convergent, and for each $r\geqslant 1$ there exists $w_r\in\mathfrak{R}$ such that*

$$w_r\not\equiv 0 \ (\mathfrak{p}),$$

$$w_r\alpha\in\mathfrak{a}^r\mathfrak{S} + K.(\beta_1, \ldots, \beta_t),$$

then $\alpha\in K.(\beta_1, \ldots, \beta_t)$, i.e. α is linearly dependent on $\beta_1, \ldots, \beta_t$ over K.

Assume, without loss of generality, that $\beta_1, \ldots, \beta_t$ are linearly independent over K. Supposing the conclusion false, it must be possible to choose elements $\gamma_{t+1}, \ldots, \gamma_{n-1}$ of $\mathfrak{S}$, such that the set $\alpha, \beta_1, \ldots, \beta_t, \gamma_{t+1}, \ldots, \gamma_{n-1}$ is a K-basis for L. Denoting the discriminant of this basis by D, it is seen by (1.3) that $Dw_r\alpha$ belongs to

$$\mathfrak{a}^r.(\alpha, \beta_1, \ldots, \beta_t, \gamma_{t+1}, \ldots, \gamma_{n-1}) + K.(\beta_1, \ldots, \beta_t).$$

Because $\alpha, \beta_1, \ldots, \beta_t, \gamma_{t+1}, \ldots, \gamma_{n-1}$ are linearly independent, it follows that $Dw_r\in\mathfrak{a}^r$. Thus $D\in(\mathfrak{a}^r)_{\mathfrak{p}}$ for all $r\geqslant 1$, contrary to the convergence of $\mathfrak{p}$.

An almost identical argument would establish

LEMMA 2′. *Let $\alpha, \beta_1, \ldots, \beta_t$ be elements of $\mathfrak{S}$. If $\mathfrak{p}$ is strongly convergent, and for each $r\geqslant 1$ there exists $w_r\in\mathfrak{R}$ such that*

$$w_r\not\equiv 0 \ (\mathfrak{p}),$$

$$w_r\alpha\in\mathfrak{p}^r\mathfrak{S} + K.(\beta_1, \ldots, \beta_t),$$

then $\alpha\in K.(\beta_1, \ldots, \beta_t)$.

Downloaded from rsta.royalsocietypublishing.org

LEMMA 3. *Let* $\mathfrak{q}$ *be a prime ideal of* $\mathfrak{S}$, $\mathfrak{b}$ *an integral ideal of* $\mathfrak{S}$, *and* $\Phi(y_1, \ldots, y_m)$, $\Psi(y_1, \ldots, y_m)$ *polynomials over* $\mathfrak{S}$ *in indeterminates* $y_1, \ldots, y_m$. *If*

$$\Phi(y_1, \ldots, y_m)\,\Psi(y_1, \ldots, y_m) \equiv 0 \ (\mathfrak{b}),$$

and

$$\Phi(y_1, \ldots, y_m) \not\equiv 0 \ (\mathfrak{q}),$$

then

$$\Psi(y_1, \ldots, y_m) \equiv 0 \ (\mathfrak{b}_\mathfrak{q}).$$

Proof. Substituting y^{l_i} for y_i $(i = 1, \ldots, m)$, and denoting $\Phi(y^{l_1}, \ldots, y^{l_m})$, $\Psi(y^{l_1}, \ldots, y^{l_m})$ by $\Phi(y)$, $\Psi(y)$, one obtains the congruence $\Phi(y)\,\Psi(y) \equiv 0 \bmod \mathfrak{b}$. When the positive integers $l_1, \ldots, l_m$ are chosen suitably, the distinct coefficients appearing in $\Phi(y)$ and $\Psi(y)$ are precisely those of the original polynomials $\Phi(y_1, \ldots, y_m)$ and $\Psi(y_1, \ldots, y_m)$. Thus the lemma is reduced to the case of one variable: given that

$$(\alpha_0 + \ldots + \alpha_s y^s)\,(\beta_0 + \ldots + \beta_t y^t) \equiv 0 \ (\mathfrak{b})$$

and

$$(\alpha_0 + \ldots + \alpha_s y^s) \not\equiv 0 \ (\mathfrak{q}),$$

where the α_i and β_i belong to $\mathfrak{S}$, it is necessary to show that

$$(\beta_0 + \ldots + \beta_t y^t) \equiv 0 \ (\mathfrak{b}_\mathfrak{q}).$$

By the Dedekind-Mertens Lemma,†

$$(\alpha_0, \ldots, \alpha_s)^{t+1}\,(\beta_0, \ldots, \beta_t) \subseteq (\alpha_0, \ldots, \alpha_s)^t \mathfrak{b};$$

and the result follows, since the $\mathfrak{S}$-ideal $(\alpha_0, \ldots, \alpha_s)$ is not contained in $\mathfrak{q}$.

The preceding lemma may, in particular, be applied with $\mathfrak{R}$ in place of $\mathfrak{S}$, $\mathfrak{p}$ in place of $\mathfrak{q}$, and an integral $\mathfrak{R}$-ideal $\mathfrak{a}$ in place of $\mathfrak{b}$; so applied, it shows that the isolated component of $\mathfrak{a}.\mathfrak{R}[y_1, \ldots, y_m]$ with respect to the prime ideal $\mathfrak{p}.\mathfrak{R}[y_1, \ldots, y_m]$ is $\mathfrak{a}_\mathfrak{p}.\mathfrak{R}[y_1, \ldots, y_m]$. Moreover, given any finite ideal $\mathfrak{A} \subseteq \mathfrak{p}.\mathfrak{R}[y_1, \ldots, y_m]$ of $\mathfrak{R}[y_1, \ldots, y_m]$, there exists a finite ideal $\mathfrak{a} \subseteq \mathfrak{p}$ of $\mathfrak{R}$, such that $\mathfrak{A} \subseteq \mathfrak{a}.\mathfrak{R}[y_1, \ldots, y_m]$. Hence

(5.2) If $\mathfrak{p}$ is a convergent prime ideal of $\mathfrak{R}$, and $y_1, \ldots, y_m$ are indeterminates, then

$$\mathfrak{p}.\mathfrak{R}[y_1, \ldots, y_m]$$

is a convergent prime ideal of $\mathfrak{R}[y_1, \ldots, y_m]$. If $\mathfrak{p}$ is strongly convergent, then $\mathfrak{p}.\mathfrak{R}[y_1, \ldots, y_m]$ is strongly convergent.

This result explains why the use of indeterminates is effective in §§ 6 and 7. Direct applications of (5.2) will not be made in those sections, although doubtless it would be possible to do so. Instead, the following extension of Lemma 2 will be used:

LEMMA 4. *Let* $y_1, \ldots, y_m$ *be indeterminates* $(m \geqslant 0)$, $A, B_1, \ldots, B_t$ *elements of* $\mathfrak{S}[y_1, \ldots, y_m]$, *and* $\mathfrak{a} \subseteq \mathfrak{p}$ *an* $\mathfrak{R}$*-ideal with a finite basis. If* $\mathfrak{p}$ *is convergent, and for each* $r \geqslant 1$ *there exists* $W_r \in \mathfrak{R}[y_1, \ldots, y_m]$ *such that*

$$W_r \not\equiv 0 \ (\mathfrak{p}),$$

$$W_r A \in (\mathfrak{a}^r \mathfrak{S})_\mathfrak{p}.\mathfrak{S}[y_1, \ldots, y_m] + K(y_1, \ldots, y_m).(B_1, \ldots, B_t),$$

then A *is linearly dependent on* $B_1, \ldots, B_t$ *over the field* $K(y_1, \ldots, y_m)$.

† See § 9 of Prüfer (1932).

Downloaded from rsta.royalsocietypublishing.org

Given any element η_r of $(\mathfrak{a}^r\mathfrak{S})_\mathfrak{p}.\mathfrak{S}[y_1,\ldots,y_m]$, there exists an element $v_r\in\mathfrak{R}$, incongruent to zero mod $\mathfrak{p}$, such that $v_r\eta_r\in\mathfrak{a}^r.\mathfrak{S}[y_1,\ldots,y_m]$. Hence there exists $V_r\in\mathfrak{R}[y_1,\ldots,y_m]$ (namely $V_r=v_rW_r$), such that

$$V_r\not\equiv 0\ (\mathfrak{p}),$$

$$V_rA\in\mathfrak{a}^r.\mathfrak{S}[y_1,\ldots,y_m]+K(y_1,\ldots,y_m).(B_1,\ldots,B_l).$$

The preceding remark reduces Lemma 4 to a case of Lemma 2, with

$$\mathfrak{R}[y_1,\ldots,y_m],\quad \mathfrak{S}[y_1,\ldots,y_m],\quad \mathfrak{p}.\mathfrak{R}[y_1,\ldots,y_m],\quad \text{and}\quad \mathfrak{a}.\mathfrak{R}[y_1,\ldots,y_m]$$

in place of $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{p}$, and $\mathfrak{a}$ respectively. The convergence of $\mathfrak{p}.\mathfrak{R}[y_1,\ldots,y_m]$ is secured by (5.2).

LEMMA 5. *Suppose that $\mathfrak{p}$ is maximal, and that $\mathfrak{S}/\mathfrak{q}_1$ is separable over $\mathfrak{R}/\mathfrak{p}$. Let α be an element of $\mathfrak{S}$, and $g(x)$ its minimal polynomial* mod $\mathfrak{q}_1$. *Then, given any $\gamma\in\mathfrak{q}_1$ and any integer $r\geqslant 1$, there exists $\beta\in\mathfrak{S}$ satisfying the congruences*

$$\beta\equiv\alpha\ (\mathfrak{q}_1),\quad g(\beta)\equiv\gamma\ (\mathfrak{q}_1^r).$$

After noting that the lemma is trivially true when $r=1$, the proof is obtained by induction over $r\geqslant 2$. Assuming the existence of β_{r-1} such that

$$\beta_{r-1}\equiv\alpha\ (\mathfrak{q}_1),\quad g(\beta_{r-1})\equiv\gamma\ (\mathfrak{q}_1^{r-1}),$$

then

$$g(\beta_{r-1}+\zeta)\equiv g(\beta_{r-1})+\zeta g'(\beta_{r-1})\ (\mathfrak{q}_1^r)$$

for any $\zeta\in\mathfrak{q}_1^{r-1}$. It only remains to take $\beta_r=\beta_{r-1}+\zeta_{r-1}$, where ζ_{r-1} is a solution of the congruence

$$\zeta_{r-1}g'(\beta_{r-1})\equiv\gamma-g(\beta_{r-1})\ (\mathfrak{q}_1^r).$$

Such elements $\zeta_{r-1}\in\mathfrak{q}_1^{r-1}$ exist, because $g'(\beta_{r-1})\equiv g'(\alpha)\not\equiv 0$ mod $\mathfrak{q}_1$.

The next lemma is concerned with 'higher congruences'. In the most intelligible case, when $m=0$, it is essentially equivalent to a theorem about polynomials over a field complete with respect to a rank 1 valuation;† in number theory, with appropriate specializations, it appears as the second theorem of Schönemann.‡

LEMMA 6. *Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{R}$, $y_1,\ldots,y_m$ indeterminates, and $f(x),g(x),h(x)$ monic polynomials in x over $\mathfrak{R}[y_1,\ldots,y_m]$, such that*

$$f(x)\equiv g(x)\,h(x)\ (\mathfrak{p}).$$

Suppose further that $g(x)$ and $h(x)$ have no common factor mod $\mathfrak{p}$.

Then for every $r\geqslant 1$ there exist an element w_r of $\mathfrak{R}[y_1,\ldots,y_m]$, and polynomials $g_r(x)$ and $h_r(x)$ over $\mathfrak{R}[y_1,\ldots,y_m]$, both having leading coefficient w_r, with the following properties:

$$w_r\not\equiv 0\ (\mathfrak{p}),$$

$$w_r^2f(x)\equiv g_r(x)\,h_r(x)\ (\mathfrak{a}^r),$$

$$g_r(x)\equiv w_rg(x)\ (\mathfrak{a}),\quad h_r(x)\equiv w_rh(x)\ (\mathfrak{a}),$$

where $\mathfrak{a}\subseteq\mathfrak{p}$ is a finite $\mathfrak{R}$-ideal independent of r. When $m=0$, w_r may be replaced by unity.

† Albert (1937), p. 296.

‡ Fricke (1928), p. 67.

Downloaded from rsta.royalsocietypublishing.org

We use the abbreviation 'deg f' for the x-degree of $f(x)$; similarly with any other polynomial in x over $\mathfrak{R}[y_1, \ldots, y_m]$. Let $\deg f = t$. Gauss's lemma shows at once that the images of $g(x)$ and $h(x)$ mod $\mathfrak{p}$ are mutually prime polynomials in x over $\mathfrak{k}(y_1, \ldots, y_m)$, where $\mathfrak{k}$ is the field $\mathfrak{R}/\mathfrak{p}$. By an elementary theorem applied to polynomials over $\mathfrak{k}(y_1, \ldots, y_m)$, there exist $W \in \mathfrak{R}[y_1, \ldots, y_m]$, and polynomials $U_i(x), V_i(x)$ over $\mathfrak{R}[y_1, \ldots, y_m]$, such that

$$W \not\equiv 0 \ (\mathfrak{p}),$$

$$\left.\begin{aligned} V_i(x)\, g(x) + U_i(x)\, h(x) &\equiv W x^i \ (\mathfrak{p}), \\ \deg U_i < \deg g, \quad \deg V_i &< \deg h \end{aligned}\right\} \quad (i = 0, \ldots, t-1).$$

Since congruences of polynomials mod $\mathfrak{p}$ involve only a finite number of coefficients, there is a finite $\mathfrak{R}$-ideal $\mathfrak{a} \subseteq \mathfrak{p}$, such that $f(x) \equiv g(x)\, h(x) \bmod \mathfrak{a}$, and

$$V_i(x)\, g(x) + U_i(x)\, h(x) \equiv W x^i \ (\mathfrak{a}) \quad (i = 0, \ldots, t-1). \tag{5.3}$$

The lemma is verified when $r = 1$, with $w_1 = 1$, $g_1(x) = g(x)$, and $h_1(x) = h(x)$. Now proceed by induction over $r \geqslant 2$, assuming the existence of w_{r-1}, $g_{r-1}(x)$, and $h_{r-1}(x)$. The difference $w_{r-1}^2 f(x) - g_{r-1}(x)\, h_{r-1}(x)$ has x-degree less than t, and its coefficients are elements of $\mathfrak{a}^{r-1}.\mathfrak{R}[y_1, \ldots, y_m]$. Multiplying (5.3) by these coefficients, and adding, it follows that

$$v_{r-1}(x)\, g(x) + u_{r-1}(x)\, h(x) \equiv W(w_{r-1}^2 f(x) - g_{r-1}(x)\, h_{r-1}(x)) \ (\mathfrak{a}^r),$$

where $u_{r-1}(x)$, $v_{r-1}(x)$ are polynomials in x over $\mathfrak{R}[y_1, \ldots, y_m]$, such that

$$u_{r-1}(x) \equiv 0 \equiv v_{r-1}(x) \ (\mathfrak{a}^{r-1}),$$

$$\deg u_{r-1} < \deg g, \quad \deg v_{r-1} < \deg h.$$

The proof is completed by putting $w_r = W w_{r-1}^2$,

$$g_r(x) = W w_{r-1} g_{r-1}(x) + u_{r-1}(x),$$

and

$$h_r(x) = W w_{r-1} h_{r-1}(x) + v_{r-1}(x).$$

With these substitutions,

$$\begin{aligned} g_r(x)\, h_r(x) - w_r^2 f(x) &= W w_{r-1}^2 \{v_{r-1}(x)\, g(x) + u_{r-1}(x)\, h(x) - W(w_{r-1}^2 f(x) - g_{r-1}(x)\, h_{r-1}(x))\} \\ &\quad + W w_{r-1} u_{r-1}(x) \{h_{r-1}(x) - w_{r-1} h(x)\} \\ &\quad + W w_{r-1} v_{r-1}(x) \{g_{r-1}(x) - w_{r-1} g(x)\} \\ &\quad + u_{r-1}(x)\, v_{r-1}(x) \\ &\equiv u_{r-1}(x)\, v_{r-1}(x) \ (\mathfrak{a}^r) \\ &\equiv 0 \ (\mathfrak{a}^r), \quad \text{since} \quad 2r-2 \geqslant r. \end{aligned}$$

6. Convergent prime ideals

Definition. Supposing that $\mathfrak{p}$ is a convergent maximal ideal (of $\mathfrak{R}$), consider sets of elements $\alpha_1, \ldots, \alpha_\rho \in \mathfrak{S}$, with the following property: There exist a finite $\mathfrak{R}$-ideal $\mathfrak{a} \subseteq \mathfrak{p}$, and a non-zero element $c \in \mathfrak{R}$, such that

$$c\mathfrak{S} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_\rho) + (\mathfrak{a}^r \mathfrak{S})_{\mathfrak{q}_1} \quad \text{for all } r \geqslant 1.$$

The *ramification rank* ρ_1 of $\mathfrak{q}_1$ is the smallest value of ρ for which such a set $\alpha_1, \ldots, \alpha_\rho$ exists. The ramification ranks $\rho_2, \ldots, \rho_e$ of $\mathfrak{q}_2, \ldots, \mathfrak{q}_e$ are defined similarly.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES
PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Downloaded from rsta.royalsocietypublishing.org

Clearly (by (1.3)) the ρ_i exist and are not greater than n. A definition of the ρ_i when $\mathfrak{p}$ is convergent but not necessarily maximal is given later in this section. The definitions are restricted to convergent $\mathfrak{p}$, because it is only when $\mathfrak{p}$ is convergent that we have a proof of their consistency. So far as this paper is concerned, the real significance of the ρ_i is expressed by Theorem 8.

THEOREM 8. *Suppose that $\mathfrak{p}$ is a convergent maximal ideal, and let θ be any element of $\mathfrak{S}[y_1, \ldots, y_m]$, where $y_1, \ldots, y_m$ are indeterminates $(m \geqslant 0)$. Write $f(x)$ for the characteristic polynomial of θ, $g_i(x)$ for its minimal polynomial* mod $\mathfrak{q}_i$, *and let the x-degree of $g_i(x)$ be k_i. Then ρ_i is divisible by k_i, and*

$$f(x) \equiv \prod_1^e (g_i(x))^{\rho_i/k_i} \ (\mathfrak{p}).$$

The well-known case when $\mathfrak{R}$ is a field can be dismissed at the outset; it may therefore be assumed that $\mathfrak{p} \neq (0)$. There exist $\gamma_1, \ldots, \gamma_e \in \mathfrak{S}$, satisfying the congruences

$$\gamma_i \equiv 1 \ (\mathfrak{q}_i), \quad \gamma_i \equiv 0 \ (\mathfrak{q}_j) \quad (1 \leqslant i \neq j \leqslant e)$$

with respect to the pairwise disjoint ideals $\mathfrak{q}_i$. Because $\mathfrak{p} \neq (0)$, $\mathfrak{R}$ (not being a field) has infinitely many elements; consequently it can be arranged further that $\gamma_1, \ldots, \gamma_e$ be primitive elements for L over K. Introduce new indeterminates $z_1, \ldots, z_e$, and proceed to work with the element

$$\chi = \theta + z_1\gamma_1 + \ldots + z_e\gamma_e,$$

which is a primitive element of $L(y_1, \ldots, y_m, z_1, \ldots, z_e)$ over $K(y_1, \ldots, y_m, z_1, \ldots, z_e)$. The minimal polynomial of χ mod $\mathfrak{q}_i$ is $G_i(x) = g_i(x - z_i)$. Thus χ enjoys the further property† that *the $G_i(x)$ are mutually incongruent* mod $\mathfrak{p}$. The characteristic polynomial $F(x)$ of χ has its coefficients in $\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$; when the presence of these other indeterminates in $F(x)$ is important, we write

$$F(x) = F(x; y_1, \ldots, y_m; z_1, \ldots, z_e).$$

After these preliminaries, the proof of Theorem 8 falls into four parts: in (1), it is shown that $F(x)$ is congruent mod $\mathfrak{p}$ to $\prod_1^e (G_i(x))^{l_i}$, where the l_i are strictly positive integers; in (2), it is shown that $l_i k_i \leqslant \rho_i$; in (3), the inequality $\rho_1 + \ldots + \rho_e \leqslant n$ is derived from part (1); and in (4) these results are collected together to complete the proof.

(1) Since $F(\chi) = 0 \equiv 0 \bmod \mathfrak{q}_i$, $F(x)$ is divisible mod $\mathfrak{p}$ by each of the mutually incongruent irreducible mod $\mathfrak{p}$ polynomials $G_i(x)$, and hence also by their product. The mod $\mathfrak{p}$ factorization of $F(x)$ thus has the form

$$F(x) \equiv H(x) \prod_1^e (G_i(x))^{l_i} \ (\mathfrak{p}),$$

where the l_i are strictly positive integers, and $H(x)$ is a monic polynomial in x over

$$\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e],$$

such that

$$H(\chi) \not\equiv 0 \ (\mathfrak{q}_i) \quad (i = 1, \ldots, e).$$

† These two properties of χ are important in the proof. If it were practicable to confine attention to the characteristic polynomial of an element $\alpha \in \mathfrak{S}$, assumed to have the analogous properties, the whole discussion could be simplified considerably; the appeals to Lemmas 3 and 4, and the introduction of the z_i, could be avoided.

Downloaded from rsta.royalsocietypublishing.org

By Lemma 6 there exist for every $r \geqslant 1$ an element W_r of $\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$, and polynomials $H_r(x)$ and $J_r(x)$ over $\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$, both having leading coefficient W_r, with the following properties:

$$W_r \not\equiv 0 \ (\mathfrak{p}),$$

$$W_r^2 F(x) \equiv H_r(x)\, J_r(x) \ (\mathfrak{a}^r),$$

$$H_r(x) \equiv W_r H(x) \ (\mathfrak{a}), \quad J_r(x) \equiv W_r \prod_1^e (G_i(x))^{l_i} \ (\mathfrak{a}),$$

where $\mathfrak{a} \subseteq \mathfrak{p}$ is a finite $\mathfrak{R}$-ideal independent of r. It follows that

$$H_r(\chi)\, J_r(\chi) \equiv 0 \ (\mathfrak{a}^r \mathfrak{S}),$$

$$H_r(\chi) \equiv W_r H(\chi) \not\equiv 0 \ (\mathfrak{q}_i).$$

Hence, from Lemma 3, $\quad J_r(\chi) \equiv 0 \ (\mathfrak{a}^r \mathfrak{S})_{\mathfrak{q}_i} \quad (i = 1, \ldots, e);$

in other words, by (4.8), $\quad J_r(\chi) \equiv 0 \ (\mathfrak{a}^r \mathfrak{S})_{\mathfrak{p}}.$

Using the convergence of $\mathfrak{p}$ for the first time through Lemma 4, and denoting the x-degree of $H(x)$ by μ, it is seen that $\chi^{n-\mu}$ is linearly dependent on $\chi^{n-\mu-1}, \ldots, \chi, 1$ over the field $K(y_1, \ldots, y_m, z_1, \ldots, z_e)$. If μ were positive, this would contradict the primitivety of χ. It is concluded that $\mu = 0$, i.e.

$$F(x) \equiv \prod_1^e (G_i(x))^{l_i} \ (\mathfrak{p}).$$

(2) By Lemma 6 there exist for every $r \geqslant 1$ an element V_r of $\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$, and polynomials $P_r(x)$ and $Q_r(x)$ over $\mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$, both having leading coefficient V_r, with the following properties:

$$V_r \not\equiv 0 \ (\mathfrak{p}),$$

$$V_r^2 F(x) \equiv P_r(x)\, Q_r(x) \ (\mathfrak{b}_1^r),$$

$$P_r(x) \equiv V_r (G_1(x))^{l_1} \ (\mathfrak{b}_1), \quad Q_r(x) \equiv V_r \prod_2^e (G_j(x))^{l_j} \ (\mathfrak{b}_1),$$

where $\mathfrak{b}_1 \subseteq \mathfrak{p}$ is a finite $\mathfrak{R}$-ideal independent of r. It follows that

$$P_r(\chi)\, Q_r(\chi) \equiv 0 \quad (\mathfrak{b}_1^r \mathfrak{S}),$$

$$P_r(\chi) \equiv V_r (G_1(\chi))^{l_1} \not\equiv 0 \ (\mathfrak{q}_j) \quad (j = 2, \ldots, e).$$

Hence, by Lemma 3, $\quad Q_r(\chi) \equiv 0 \ (\mathfrak{b}_1^r \mathfrak{S})_{\mathfrak{q}_j} \quad (j = 2, \ldots, e).$

By definition of ρ_1, there exist elements $\alpha_1, \ldots, \alpha_{\rho_1} \in \mathfrak{S}$, and a non-zero element $c \in \mathfrak{R}$, and a finite $\mathfrak{R}$-ideal $\mathfrak{b}_2 \subseteq \mathfrak{p}$, such that

$$c\mathfrak{S} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_{\rho_1}) + (\mathfrak{b}_2^r \mathfrak{S})_{\mathfrak{q}_1} \quad \text{for all } r \geqslant 1.$$

The usual determinantal method may now be applied: this relation implies the existence of $a_{ijr} \in \mathfrak{R}[y_1, \ldots, y_m, z_1, \ldots, z_e]$, such that

$$c\chi\alpha_i \equiv \sum_{j=1}^{\rho_1} a_{ijr} \alpha_j \ (\mathfrak{b}_2^r \mathfrak{S})_{\mathfrak{q}_1} \quad (i = 1, \ldots, \rho_1;\ r \geqslant 1).$$

Downloaded from rsta.royalsocietypublishing.org

With $R_r(x)$ denoting the determinant $|x\delta_{ij}-a_{ijr}|$, it follows that

$$R_r(c\chi)\,\alpha_i \equiv 0 \ (\mathfrak{b}_2^r\mathfrak{S})_{\mathfrak{q}_1},$$

whence

$$cR_r(c\chi) \equiv 0 \ (\mathfrak{b}_2^r\mathfrak{S})_{\mathfrak{q}_1}.$$

Combined with (4.8), the above results lead to the new congruence

$$cR_r(c\chi)\,Q_r(\chi) \equiv 0 \ (\mathfrak{b}^r\mathfrak{S})_{\mathfrak{p}},$$

where $\mathfrak{b}=\mathfrak{b}_1+\mathfrak{b}_2$. Using Lemma 4, it is seen that $c^{\rho_1+1}\chi^{\rho_1+n-l_1k_1}$ is linearly dependent on $\chi^{\rho_1+n-l_1k_1-1}, \ldots, \chi, 1$ over the field $K(y_1, \ldots, y_m, z_1, \ldots, z_e)$. If l_1k_1 were greater than ρ_1, this would contradict the primitivety of χ. It is concluded that $l_1k_1 \leqslant \rho_1$, and similarly

$$l_ik_i \leqslant \rho_i \quad (i=1, \ldots, e).$$

(3) In part (1) of this proof, θ is an arbitrary element of $\mathfrak{S}[y_1, \ldots, y_m]$. θ may therefore be replaced by zero; and, according to (1), the characteristic polynomial of $z_1\gamma_1+\ldots+z_e\gamma_e$ is congruent mod $\mathfrak{p}$ to $\prod_1^e (x-z_i)^{t_i}$, where $t_1, \ldots, t_e$ are positive integers. Substituting $1, 0, \ldots, 0$ for $z_1, z_2, \ldots, z_e$, one obtains the congruence

$$\Gamma(x) \equiv (x-1)^{t_1}x^{n-t_1} \ (\mathfrak{p})$$

for the characteristic polynomial $\Gamma(x)$ of γ_1. By the simplest case of Lemma 6 there exist, for every $r \geqslant 1$, monic polynomials $\Delta_r(x)$ and $\mathrm{E}_r(x)$ over $\mathfrak{R}$, with the following properties:

$$\Gamma(x) \equiv \Delta_r(x)\,\mathrm{E}_r(x) \ (\mathfrak{g}^r),$$

$$\Delta_r(x) \equiv (x-1)^{t_1} \ (\mathfrak{g}), \quad \mathrm{E}_r(x) \equiv x^{n-t_1} \ (\mathfrak{g}),$$

where $\mathfrak{g} \subseteq \mathfrak{p}$ is a finite $\mathfrak{R}$-ideal independent of r. It follows that

$$\Delta_r(\gamma_1)\,\mathrm{E}_r(\gamma_1) \equiv 0 \ (\mathfrak{g}^r\mathfrak{S}),$$

$$\mathrm{E}_r(\gamma_1) \equiv \gamma_1^{n-t_1} \not\equiv 0 \ (\mathfrak{q}_1),$$

whence

$$\Delta_r(\gamma_1) \equiv 0 \ (\mathfrak{g}^r\mathfrak{S})_{\mathfrak{q}_1}.$$

Thus

$$\mathfrak{R}[\gamma_1] \subseteq \mathfrak{R}.(1, \gamma_1, \ldots, \gamma_1^{t_1-1}) + (\mathfrak{g}^r\mathfrak{S})_{\mathfrak{q}_1}$$

for all $r \geqslant 1$; and this, by definition of ρ_1, implies that $\rho_1 \leqslant t_1$. Similarly $\rho_i \leqslant t_i$ $(i=1, \ldots, e)$, and consequently

$$\rho_1+\ldots+\rho_e \leqslant n.$$

(4) The relations $\Sigma l_ik_i = n$, $l_ik_i \leqslant \rho_i$, and $\Sigma\rho_i \leqslant n$, proved in (1), (2), and (3), could not hold unless $\Sigma\rho_i = n$ and $l_ik_i = \rho_i$ $(i=1, \ldots, e)$. Thus

$$F(x) \equiv \prod_1^e (G_i(x))^{\rho_i/k_i} \ (\mathfrak{p}).$$

Finally, substitute zero for $z_1, \ldots, z_e$: then $F(x) = F(x; y_1, \ldots, y_m; z_1, \ldots, z_e)$ becomes $f(x)$, $G_i(x) = g_i(x-z_i)$ becomes $g_i(x)$, and the preceding congruence reduces to

$$f(x) \equiv \prod_1^e (g_i(x))^{\rho_i/k_i} \ (\mathfrak{p}).$$

Downloaded from rsta.royalsocietypublishing.org

It is now possible to state the

Definition. When $\mathfrak{p}$ is convergent but not necessarily maximal, the *ramification rank* of $\mathfrak{q}_i$ is the ramification rank, as previously defined, of $\mathfrak{q}_i\mathfrak{S}_\mathfrak{p}$.

The consistency of the two definitions must be verified. To that end, supposing $\mathfrak{p}$ convergent and maximal, let the ramification ranks of $\mathfrak{q}_i$ and $\mathfrak{q}_i\mathfrak{S}_\mathfrak{p}$ (first definition) be denoted temporarily by ρ_i and ρ_i'. It is clear from the definition and (4.3) that $\rho_i' \leqslant \rho_i$; but $\Sigma\rho_i = n = \Sigma\rho_i'$, by (5.1) and Theorem 8.

COROLLARY 1. *For any convergent* $\mathfrak{p}$, $\rho_1 + \ldots + \rho_e = n$.

COROLLARY 2. *If* $\mathfrak{p}$ *is convergent,* ρ_i *is divisible* (i) *by* n_i, *if the residue field of* $\mathfrak{q}_i$ *is separable over that of* $\mathfrak{p}$; (ii) *by* pn_i', *if the residue field of* $\mathfrak{q}_i$ *is inseparable over that of* $\mathfrak{p}$ *and has characteristic* p.

There is no loss of generality in assuming also that $\mathfrak{p}$ is maximal, by (4.4) and (5.1). Then $\mathfrak{S}/\mathfrak{q}_i$ is known to contain an element of degree n_i or pn_i' over $\mathfrak{R}/\mathfrak{p}$, in the respective cases (i) or (ii).

COROLLARY 3. *With the notation and subject to the conditions of Theorem* 8,

$$(g_i(\theta))^{\rho_i/k_i} \equiv 0 \ (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}.$$

From part (1) of the proof of the theorem, it is seen that $\prod_1^e (G_i(\chi))^{l_i} \equiv 0 \bmod \mathfrak{p}\mathfrak{S}$, and $G_j(\chi) \not\equiv 0 \bmod \mathfrak{q}_1$ $(j = 2, \ldots, e)$. By Lemma 3, $(G_1(\chi))^{l_1} \equiv 0 \bmod (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$; hence, substituting zero for $z_1, \ldots, z_e$, $(g_1(\theta))^{l_1} \equiv 0 \bmod (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$.

The following is a simple deduction from Theorem 8 and Corollary 2:

(6.1) If $\mathfrak{p}$ is convergent and maximal, and $\mathfrak{S}/\mathfrak{q}_1$ separable over $\mathfrak{R}/\mathfrak{p}$, then

$$\mathfrak{d} \subseteq \mathfrak{p}\mathfrak{S} + \mathfrak{q}_1^{(\rho_1/n_1)-1}.$$

A somewhat similar result can be proved without any restriction on $\mathfrak{p}$:

(6.2) $$(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_e)\,\mathfrak{d} \subseteq \mathfrak{p}\mathfrak{S}.$$

Proof. For any $\alpha \in \mathfrak{S}$ and $\beta \in (\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_e)$, in the notation of Theorem 17,

$$\beta d(\alpha) = \sum_1^n \alpha^{i-1} T(\beta\eta_{i-1});$$

and the right-hand side belongs to $\mathfrak{p}\mathfrak{S}$, by (4.10).

THEOREM 9. *If the residue field of* $\mathfrak{p}$ *has characteristic zero, and* $\mathfrak{p}$ *is convergent, then*

$$\mathfrak{q}_i^{\rho_i/n_i} \subseteq (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i} \quad (i = 1, \ldots, e),$$

i.e. the exponent of the primary ideal $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ *is at most* ρ_i/n_i.

As usual, it may be assumed in the proof that $\mathfrak{p}$ is maximal (by (5.1) and (4.3)). It is already known from (4.12) that the exponent of $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ is finite. (Alternatively, under present conditions, the finiteness of the exponent could be deduced from Corollary 3 of Theorem 8 by reasoning similar to that below.) Let $\alpha \in \mathfrak{S}$ be a primitive element for $\mathfrak{S}/\mathfrak{q}_1$ over $\mathfrak{R}/\mathfrak{p}$, and $g(x)$ its minimal polynomial mod $\mathfrak{q}_1$; $g(x)$ is of degree n_1, and $g'(\alpha)$ is not in $\mathfrak{q}_1$. By Lemma 5, α can be chosen so that

$$g(\alpha) \equiv 0 \ (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}.$$

Downloaded from rsta.royalsocietypublishing.org

Let $y_1, \ldots, y_s$ be indeterminates, and $\gamma_1, \ldots, \gamma_s$ any s elements of $\mathfrak{q}_1$, where $s = \rho_1/n_1$. According to Corollary 3 of Theorem 8,

$$\{g(\alpha+y_1\gamma_1+\ldots+y_s\gamma_s)\}^s \equiv 0 \ (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}.$$

By choice of α, this congruence reduces to

$$\{(y_1\gamma_1+\ldots+y_s\gamma_s)\, g'(\alpha)+\ldots\}^s \equiv 0 \ (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1},$$

where the omitted terms are of more than the first degree in $y_1, \ldots, y_s$. Hence it is seen that $\gamma_1 \ldots \gamma_s \in (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$.

7. Strongly convergent prime ideals

The object of this section, and its relation to previous theories, have been fully explained in § 5. In Lemma 7, it is shown that the defining property of the ρ_i can be expressed more simply when $\mathfrak{p}$ is strongly convergent. It may not be amiss to point out that, if *strongly* convergent prime ideals were the only interest, the σ_i of the proof of Lemma 7 could be defined to be the ramification ranks of the $\mathfrak{q}_i$. For strongly convergent $\mathfrak{p}$, the results of § 6, including Corollary 1 of Theorem 8, could then be proved with the σ_i in place of the ρ_i. This remark indicates the lines of an alternative proof of Lemma 7. It is scarcely surprising that Theorem 13 lacks the precision of the classical Different-Theorem. A fuller generalization of the classical theorem would be provided by the contention that $\mathfrak{d} \notin (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$, when the residue field of $\mathfrak{p}$ has characteristic zero; but that contention is falsified by the example of Zariski (1939, p. 272).

(7.1) If $\mathfrak{m}$ is an $\mathfrak{R}$-submodule of $\mathfrak{S}$ such that

$$\mathfrak{S} = \mathfrak{p}\mathfrak{S}+\mathfrak{m},$$

then

$$\mathfrak{S} = \mathfrak{p}^r\mathfrak{S}+\mathfrak{m} \quad \text{for all } r \geqslant 1.$$

The proof by induction is trivial. Hence, from (7.1) and Lemma 2′,

(7.2) *If $\mathfrak{p}$ is a strongly convergent maximal ideal, the algebra $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ has rank at least n over $\mathfrak{R}/\mathfrak{p}$.*

Theorem 10. *Suppose that $\mathfrak{p}$ is strongly convergent. Then the following two propositions are equivalent:* (i) $\mathfrak{p} \nmid \mathfrak{D}$; (ii) $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i} = \mathfrak{q}_i$, *and the residue field of $\mathfrak{q}_i$ is separable over that of $\mathfrak{p}$, for all $i = 1, \ldots, e$.*

Proof. Bearing (5.1) in mind, the proof is the same as that of Theorem 7, except that (7.2) is used instead of Theorem 2 (2).

Lemma 7. *If $\mathfrak{p}$ is a strongly convergent maximal ideal, ρ_1 is the smallest integer ρ with the following property: There exist ρ elements $\alpha_1, \ldots, \alpha_\rho \in \mathfrak{S}$, and a non-zero element $c \in \mathfrak{R}$, such that*

$$c\mathfrak{S} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_\rho)+(\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_1} \quad \textit{for all } r \geqslant 1.$$

Let the smallest integer with the property specified in the enunciation be σ_1, and define $\sigma_2, \ldots, \sigma_e$ similarly. Since Corollary 1 of Theorem 8 asserts that $\rho_1+\ldots+\rho_e = n$, and it is obvious that $\sigma_i \leqslant \rho_i$, the lemma will be established if it is proved that $\sigma_1+\ldots+\sigma_e \geqslant n$.

Let $\beta \in \mathfrak{S}$ be a primitive element for L over K. Take $\alpha_1, \ldots, \alpha_{\sigma_1} \in \mathfrak{S}$, and a non-zero $c_1 \in \mathfrak{R}$, such that

$$c_1\mathfrak{S} \subseteq \mathfrak{R}.(\alpha_1, \ldots, \alpha_{\sigma_1})+(\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_1} \quad \text{for all } r \geqslant 1.$$

Downloaded from rsta.royalsocietypublishing.org

Then there exist $a_{ijr} \in \mathfrak{R}$, such that

$$c_1\beta\alpha_i \equiv \sum_{j=1}^{\sigma_1} a_{ijr}\alpha_j \ (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_1} \quad (i = 1, \ldots, \sigma_1;\ r \geqslant 1).$$

As in part (2) of the proof of Theorem 8, it follows that

$$c_1\Phi_{r1}(c_1\beta) \equiv 0 \ (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_1},$$

where $\Phi_{r1}(x)$ denotes the determinant $|\, x\delta_{ij} - a_{ijr}\,|$. Similarly, there exist monic polynomials $\Phi_{r2}(x), \ldots, \Phi_{re}(x)$ over $\mathfrak{R}$, of degrees $\sigma_2, \ldots, \sigma_e$, and non-zero elements $c_2, \ldots, c_e \in \mathfrak{R}$, such that

$$c_i\Phi_{ri}(c_i\beta) \equiv 0 \ (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_i} \quad (i = 1, \ldots, e;\ r \geqslant 1).$$

By (4.9),
$$\prod_{i=1}^{e} c_i\Phi_{ri}(c_i\beta) \equiv 0 \ (\mathfrak{p}^r\mathfrak{S}).$$

Using the strong convergence of $\mathfrak{p}$ through Lemma 2′, it is deduced that $\Pi c_i^{\sigma_i+1}\beta^{\sigma_i}$ is linearly dependent on $\beta^{\sigma_1+\ldots+\sigma_e-1}, \ldots, \beta, 1$ over K. This would contradict the primitivety of β unless $\sigma_1 + \ldots + \sigma_e \geqslant n$.

The following result analogous to (7.1) forms part of the proof of Theorem 11. (It would also have been possible to use (7.3) in the proof of Lemma 1.)

(7.3) Suppose that $\mathfrak{p}$ is a maximal ideal (of $\mathfrak{R}$), t an integer between 1 and e, and $\mathfrak{m}$ an $\mathfrak{R}$-submodule of $\mathfrak{S}$ such that

$$\mathfrak{S} = \mathfrak{m} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_j}.$$

Then
$$\mathfrak{S} = \mathfrak{m} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_j} \quad \text{for any } r \geqslant 1.$$

It must first be observed that

$$\bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_j} = \mathfrak{p}\mathfrak{S} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_j} \quad \text{for any } r \geqslant 1.$$

In fact, the ideals $(\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_j}$ are respectively $\mathfrak{q}_j$-primary, so the only prime over-ideals of their (direct) meet are $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$; the right-hand side is therefore the meet of its isolated components with respect to $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$, by (8.2). Hence the right-hand side contains the left; but the reverse inequality is obvious. Substituting back, therefore

$$\mathfrak{S} = \mathfrak{p}\mathfrak{S} + \mathfrak{m} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_j}.$$

From this, using (7·1), it follows that

$$\begin{aligned}\mathfrak{S} &= \mathfrak{p}^r\mathfrak{S} + \mathfrak{m} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_j} \\ &= \mathfrak{m} + \bigcap_{1 \leqslant j \leqslant t} (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_i}.\end{aligned}$$

THEOREM 11. *Suppose that $\mathfrak{p}$ is strongly convergent and maximal. Then $\lambda_i n_i \geqslant \rho_i$ $(i = 1, \ldots, e)$, where λ_i denotes the depth of the $\mathfrak{S}$-ideal $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$. If, further, $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ has rank n over $\mathfrak{R}/\mathfrak{p}$, the sign of equality may be inserted.*

In the proof that $\lambda_1 n_1 \geqslant \rho_1$, it is naturally assumed that $\lambda_1 n_1 < \infty$. It is well known that every composition-factor of the $\mathfrak{S}$-module $\mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ is module-isomorphic to $\mathfrak{S}/\mathfrak{q}_1$, and

Downloaded from rsta.royalsocietypublishing.org

thence that the rank of $\mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ qua $\mathfrak{R}/\mathfrak{p}$-module is $n_1\lambda_1$. Accordingly, let elements $\alpha_1, \ldots, \alpha_{n_1\lambda_1}$ of $\mathfrak{S}$ form an $\mathfrak{R}/\mathfrak{p}$-basis for $\mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$:

$$\mathfrak{S} = \mathfrak{R}.(\alpha_1, \ldots, \alpha_{n_1\lambda_1}) + (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}.$$

It follows from (7.3) that $\mathfrak{S} = \mathfrak{R}.(\alpha_1, \ldots, \alpha_{n_1\lambda_1}) + (\mathfrak{p}^r\mathfrak{S})_{\mathfrak{q}_1}$

for all $r \geqslant 1$, whence $\rho_1 \leqslant n_1\lambda_1$ by Lemma 7. When $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ has rank n over $\mathfrak{R}/\mathfrak{p}$, $\Sigma\rho_i = \Sigma n_i\lambda_i$.

THEOREM 12. *Let $\mathfrak{p}$ be a strongly convergent maximal ideal. Suppose that there exists $\alpha \in \mathfrak{S}$ such that $\mathfrak{S} = \mathfrak{p}\mathfrak{S} + \mathfrak{R}[\alpha]$, i.e. that $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ over $\mathfrak{R}/\mathfrak{p}$ possesses a primitive element. Let the characteristic polynomial of α be $f(x)$, and its* mod $\mathfrak{p}$ *factorization*

$$f(x) \equiv g_1^{l_1}(x) \ldots g_t^{l_t}(x) \ (\mathfrak{p}) \quad (l_i > 0),$$

where the $g_i(x)$ are monic polynomials over $\mathfrak{R}$, mutually incongruent and irreducible mod $\mathfrak{p}$.

(1) *$e = t$. With a proper arrangement of the suffixes, $g_i(x)$ is the minimal polynomial of α* mod $\mathfrak{q}_i$; *the degree of $g_i(x)$ is n_i; $\rho_i = l_i n_i$.*

(2) $$\mathfrak{q}_i = \mathfrak{S}.(\mathfrak{p}, g_i(\alpha)), \quad (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i} = \mathfrak{S}.(\mathfrak{p}, g_i^{l_i}(\alpha)).$$

(3) *For given $i = 1, \ldots, t$, the only distinct $\mathfrak{S}$-ideals between $\mathfrak{S}$ and $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ inclusive are $\mathfrak{S}.(\mathfrak{p}, g_i^s(\alpha))$ $(s = 0, 1, \ldots, l_i)$; they form a composition series for $\mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$. The exponent and depth of $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ are both equal to $l_i = \rho_i/n_i$.*

In view of the much simpler nature of the present theorem, the preceding theorems are used sparingly in the proof.

By (7.2), the rank of $\Lambda = \mathfrak{S}/\mathfrak{p}\mathfrak{S}$ over $\mathfrak{R}/\mathfrak{p}$ is exactly n. This algebra is the direct sum $\Lambda = \Lambda_1 \oplus \ldots \oplus \Lambda_e$, where

$$\Lambda_1 = ((\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_2} \cap \ldots \cap (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_e})/(\mathfrak{p}\mathfrak{S}) \cong \mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$$

and cyclically. Let the length of Λ_i, which is the depth of $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$, be λ_i. Let the minimal polynomial (of degree n_i) of α mod $\mathfrak{q}_i$ be $\phi_i(x)$. From well-known representation theory, the characteristic polynomial of α qua element of Λ is $\phi_1^{\lambda_1}(x) \ldots \phi_e^{\lambda_e}(x)$ mod $\mathfrak{p}$. Since α is primitive for Λ, it is seen that the $\phi_i(x)$ are mutually incongruent mod $\mathfrak{p}$, and that

$$f(x) \equiv \phi_1^{\lambda_1}(x) \ldots \phi_e^{\lambda_e}(x) \ (\mathfrak{p}).$$

It follows that $t = e$; with a suitable arrangement of the suffixes, the $\phi_i(x)$ may be identified with the respective $g_i(x)$, and the λ_i equated to the l_i. Because the $\phi_i(x)$ are mutually incongruent mod $\mathfrak{p}$, $\phi_1^{\lambda_1}(\alpha).\Lambda_j = \Lambda_j$ when $j \neq 1$; that is to say, $g_1^{l_1}(\alpha).\Lambda_j = \Lambda_j$ when $j \neq 1$; and of course $g_1^{l_1}(\alpha)$ annihilates Λ_1. Hence

$$g_1^{l_1}(\alpha).\Lambda = \Lambda_2 \oplus \ldots \oplus \Lambda_e,$$

a relation which is equivalent to $\mathfrak{S}.(\mathfrak{p}, g_1^{l_1}(\alpha)) = (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$.

The rest of the theorem, except for the equation $\rho_i = n_i l_i$, is included in (9.5) and Theorem 20. The fact that $\rho_i = n_i l_i$ is an immediate consequence of Theorem 8.

The following result is a partial converse of Theorem 12:

(7.4) If $\mathfrak{p}$ is maximal, and $\mathfrak{R}/\mathfrak{p}$ has characteristic zero, and if the exponent of $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_i}$ is equal to its depth for all $i = 1, \ldots, e$, then $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ has a primitive element over $\mathfrak{R}/\mathfrak{p}$.

Downloaded from rsta.royalsocietypublishing.org

In that case the exponent and depth are finite, by (4.12). The theorems of § 9 are therefore applicable to $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$, which has a primitive element over $\mathfrak{R}/\mathfrak{p}$ by Theorems 20 and 18.

The situation considered in Theorem 12 is somewhat special: there may be no element with the property postulated for α, even when $\mathfrak{S}/\mathfrak{p}\mathfrak{S}$ has rank n over $\mathfrak{R}/\mathfrak{p}$. An example is given on p. 272 of Zariski (1939), where the exponent of $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ is less than ρ_1/n_1. On the other hand, in a case important in the theory of algebraic curves—$\mathfrak{R}$ the ring of polynomials in one variable over a field of characteristic zero, and $\mathfrak{S}$ integrally closed—the conditions of (7.4) are fulfilled for every non-null $\mathfrak{p}$. That is largely why the Different-Theorem of Dedekind & Weber (1882) is easier than the corresponding theorem for algebraic numbers.

(7.5) Suppose that $\mathfrak{p}$ is maximal, and $\mathfrak{S}/\mathfrak{q}_1$ separable over $\mathfrak{R}/\mathfrak{p}$. Then there exists $\alpha \in \mathfrak{S}$ such that

(i) α is primitive for $\mathfrak{S}/\mathfrak{q}_1$ over $\mathfrak{R}/\mathfrak{p}$;

(ii) $g_1(\alpha) \not\equiv 0 \bmod \mathfrak{q}_j$ $(j = 2, \ldots, e)$, where $g_1(x)$ is the minimal polynomial of $\alpha \bmod \mathfrak{q}_1$.

Proof. Let β be an element of $\mathfrak{S}$, primitive for $\mathfrak{S}/\mathfrak{q}_1$ over $\mathfrak{R}/\mathfrak{p}$, and let its minimal polynomial mod $\mathfrak{q}_1$ be $g_1(x)$. It can be arranged that β do not belong to $\mathfrak{q}_1$; for that is inevitable when $n_1 > 1$, and is easily secured when $n_1 = 1$. Taking α to be a solution of the congruences

$$\alpha \equiv \beta \ (\mathfrak{q}_1), \quad \alpha \equiv 0 \ (\mathfrak{q}_j) \quad (j = 2, \ldots, e),$$

then

$$g_1(\alpha) \equiv 0 \ (\mathfrak{q}_1),$$

and

$$g_1(\alpha) \equiv g_1(0) \not\equiv 0 \ (\mathfrak{q}_j).$$

THEOREM 13. *When $\mathfrak{p}$ is strongly convergent, the relation $\mathfrak{d} \notin \mathfrak{q}_1$ holds if and only if both $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1} = \mathfrak{q}_1$, and the residue field of $\mathfrak{q}_1$ is separable over that of $\mathfrak{p}$.*

In the proof it is assumed that $\mathfrak{p}$ is maximal as well as strongly convergent, this restriction being justified by (5.1), (1.7), (4.3), and (4.4). The characteristic polynomial and minimal polynomial mod $\mathfrak{q}_1$ of α are denoted by $f(x)$ and $g_1(x)$ respectively.

The condition $\mathfrak{d} \notin \mathfrak{q}_1$ is necessary. Take α to be such an element as is supplied by (7.5). By Theorems 8 and 11, ($\rho_1 = n_1$ and)

$$f(x) \equiv g_1(x)\, h(x) \ (\mathfrak{p}),$$

where

$$h(\alpha) \not\equiv 0 \ (\mathfrak{q}_1).$$

It follows that

$$d(\alpha) \equiv g_1'(\alpha)\, h(\alpha) \not\equiv 0 \ (\mathfrak{q}_1).$$

The condition $\mathfrak{d} \notin \mathfrak{q}_1$ is sufficient. Take α to be an element of $\mathfrak{S}$ such that $d(\alpha)$ is not in $\mathfrak{q}_1$. Because $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ is $\mathfrak{q}_1$-primary, $d(\alpha)$ has in $\mathfrak{S}$ an inverse mod $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$; hence, using the relation $d(\alpha) \cdot \mathfrak{S} \subseteq \mathfrak{R}[\alpha]$, it follows that

$$\mathfrak{S} = (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1} + \mathfrak{R}[\alpha].$$

A fortiori, α is primitive for $\mathfrak{S}/\mathfrak{q}_1$ over $\mathfrak{R}/\mathfrak{p}$. Now $f(x)$ has a mod $\mathfrak{p}$ factorization

$$f(x) \equiv g_1^s(x)\, h(x) \ (\mathfrak{p}) \quad (s \geqslant 1),$$

where

$$h(\alpha) \not\equiv 0 \ (\mathfrak{q}_1).$$

By choice of α,

$$s g_1^{s-1}(\alpha)\, g_1'(\alpha)\, h(\alpha) \not\equiv 0 \quad (\mathfrak{q}_1).$$

From this it follows, first, that $s = 1$, whence $g_1(\alpha) \equiv 0 \bmod (\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$. Thus the $\mathfrak{R}/\mathfrak{p}$-modules $\mathfrak{S}/\mathfrak{q}_1$ and $\mathfrak{S}/(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1}$ have the same rank, viz. the degree of $g_1(x)$; in other words, $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1} = \mathfrak{q}_1$. (This fact is also a direct consequence of (6.2).) Secondly, it follows that $g_1'(\alpha) \not\equiv 0 \bmod \mathfrak{q}_1$; so $\mathfrak{S}/\mathfrak{q}_1$, being obtained by adjunction of a separable element to $\mathfrak{R}/\mathfrak{p}$, is a separable extension

Downloaded from rsta.royalsocietypublishing.org

of the latter. Moreover, by Theorem 8, the equation $s = 1$ obliges α to satisfy the second condition of (7.5).

COROLLARY 1. *When* $\mathfrak{p}$ *is strongly convergent and maximal, and* $\mathfrak{d} \nsubseteq \mathfrak{q}_1$, *elements* $\alpha \in \mathfrak{S}$ *such that* $d(\alpha)$ *is not in* $\mathfrak{q}_1$ *are characterized by the two conditions of* (7.5).

COROLLARY 2. *Assuming that* $\mathfrak{p}$ *is strongly convergent, and the residue field of* $\mathfrak{q}_1$ *separable over that of* $\mathfrak{p}$, *we have* $(\mathfrak{p}\mathfrak{S})_{\mathfrak{q}_1} = \mathfrak{q}_1$ *if and only if* $\rho_1 = n_1$.

Theorem 13 is subject to two restrictions: the strong convergence of $\mathfrak{p}$, stated explicitly, and the separability of L over K, assumed throughout Part I. It is shown in § 10 that *neither of these restrictions is superfluous*.

PART II

8. GENERAL ADDITIVE IDEAL THEORY

This section contains an outline of some results in the ideal theory of an arbitrary integral domain $\mathfrak{R}$; its scope is limited to supplying the needs of Part I. The restriction to integral domains is convenient, but not always essential. For a systematic account of the theory, reference should be made to Krull (1929), or to the summary in n. 3 of Krull (1935).

The fundamental theorems† are

THEOREM 14. *Let* $\mathfrak{a} \subset \mathfrak{R}$ *be an* $\mathfrak{R}$*-ideal.*

(1) $\mathfrak{a}$ *is contained in at least one maximal ideal, and hence in at least one prime ideal, of* $\mathfrak{R}$.

(2) *Any prime over-ideal of* $\mathfrak{a}$ *contains a minimal prime over-ideal of* $\mathfrak{a}$.

THEOREM 15. *Let* $\mathfrak{p}$ *be a minimal prime over-ideal of an* $\mathfrak{R}$*-ideal* $\mathfrak{a} \subset \mathfrak{R}$. *Then* $\mathfrak{a}_{\mathfrak{p}}$ *is* $\mathfrak{p}$*-primary, and is the smallest* $\mathfrak{p}$*-primary over-ideal of* $\mathfrak{a}$.

These theorems have some interesting consequences.

(8.1) *Suppose* M *is any field containing* $\mathfrak{R}$, *and* $\mathfrak{m}$ *any* $\mathfrak{R}$*-submodule of* M. *Then* $\mathfrak{m} = \bigcap \mathfrak{m}.\mathfrak{R}_{\mathfrak{p}}$, *where* $\mathfrak{p}$ *runs through all maximal ideals of* $\mathfrak{R}$.

Proof. Given any $\beta \in M$, not contained in $\mathfrak{m}$, let $\mathfrak{b}$ be the set of all $b \in \mathfrak{R}$ such that $b\beta \in \mathfrak{m}$. Being an integral $\mathfrak{R}$-ideal distinct from the unit ideal, $\mathfrak{b}$ is contained in at least one maximal ideal $\mathfrak{p}$ of $\mathfrak{R}$. If β belonged to $\mathfrak{m}.\mathfrak{R}_{\mathfrak{p}}$, there would exist $u \in \mathfrak{R}$ satisfying the relations

$$u\beta \in \mathfrak{m}, \quad u \not\equiv 0 \ (\mathfrak{p}),$$

which is impossible.

(8.2) For any $\mathfrak{R}$-ideal $\mathfrak{a} \subset \mathfrak{R}$ we have $\mathfrak{a} = \bigcap \mathfrak{a}_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through all maximal ideals of $\mathfrak{R}$. The formula holds when $\mathfrak{p}$ runs merely through all maximal over-ideals of $\mathfrak{a}$.

This follows from (8.1)—$\mathfrak{a}_{\mathfrak{p}} = \mathfrak{R} \cap \mathfrak{a}\mathfrak{R}_{\mathfrak{p}}$, and $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{R}$ if $\mathfrak{p} \nmid \mathfrak{a}$. Combining (8.2) with Theorem 15 we deduce (8.3), with (8.4) as a corollary:

(8.3) If an $\mathfrak{R}$-ideal $\mathfrak{a} \subset \mathfrak{R}$ has only one (necessarily maximal) prime over-ideal $\mathfrak{p}$, then $\mathfrak{a}$ is $\mathfrak{p}$-primary.

(8.4) If $\mathfrak{p}$ is a maximal ideal of $\mathfrak{R}$, the product of a finite set of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary; and any integral over-ideal (other than $\mathfrak{R}$) of a $\mathfrak{p}$-primary ideal is $\mathfrak{p}$-primary.

Inversive Ideals.‡ An $\mathfrak{R}$-ideal $\mathfrak{a}$ is *inversive* if there exists an $\mathfrak{R}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{R}$. When this equation holds, $\mathfrak{b}$ necessarily coincides with $\mathfrak{R}:\mathfrak{a}$, because

$$\mathfrak{b} \subseteq \mathfrak{R}:\mathfrak{a} = (\mathfrak{R}:\mathfrak{a})\,\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}.$$

Thus $\mathfrak{a}$ is inversive if and only if $(\mathfrak{R}:\mathfrak{a})\,\mathfrak{a} \supseteq \mathfrak{R}$.

† Theorem 14 can be proved in a few lines by means of Zorn's Principle. For Theorems 14 and 15, (8.2) and (8.3), see Krull (1929): Lemma, Theorems 2, 5, 6, and remarks following the latter.

‡ (8.5) is taken from Krull (1930), and (8.6) from Helms (1935).

Downloaded from rsta.royalsocietypublishing.org

(8.5) Any inversive ideal has a finite basis.

The proof is simple. If $\mathfrak{ab} = \mathfrak{R}$, $1 = a_1 b_1 + \ldots + a_s b_s$ $(a_i \in \mathfrak{a},\ b_i \in \mathfrak{b})$; and hence

$$\mathfrak{a} \subseteq \mathfrak{a}.(b_1, \ldots, b_s)\,(a_1, \ldots, a_s) \subseteq \mathfrak{ab}.(a_1, \ldots, a_s) \subseteq (a_1, \ldots, a_s) \subseteq \mathfrak{a}.$$

(8.6) If $\mathfrak{R}$ has only a finite number of maximal ideals, every inversive $\mathfrak{R}$-ideal is a principal ideal.

Suppose that $\mathfrak{ab} = \mathfrak{R}$, and let the distinct maximal ideals of $\mathfrak{R}$ be $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Because $\mathfrak{a}$ is inversive, $\mathfrak{ap}_i \subset \mathfrak{a}$; there exist elements $a_i \in \mathfrak{a}$ such that $a_i \not\equiv 0 \bmod \mathfrak{ap}_i$ $(i = 1, \ldots, t)$. There also exist $c_1, \ldots, c_t \in \mathfrak{R}$, satisfying the congruences $c_i \equiv 1 \bmod \mathfrak{p}_i$, $c_i \equiv 0 \bmod \mathfrak{p}_j$ $(1 \leqslant i \neq j \leqslant t)$, with respect to the pairwise disjoint ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Putting $a = a_1 c_1 + \ldots + a_t c_t$, it is seen that $a \not\equiv 0 \bmod \mathfrak{ap}_i$. Thus $a\mathfrak{b} \not\subseteq \mathfrak{p}_i$ (all i) although $a\mathfrak{b} \subseteq \mathfrak{R}$; $a\mathfrak{b} = \mathfrak{R}$ by Theorem 14; and consequently $\mathfrak{a} = a\mathfrak{R}$.

(8.7) *A non-null $\mathfrak{R}$-ideal $\mathfrak{a}$ is inversive if and only if* (i) $\mathfrak{a}$ *has a finite basis, and* (ii) *for every maximal ideal $\mathfrak{p}$ of $\mathfrak{R}$, $\mathfrak{a}\mathfrak{R}_\mathfrak{p}$ is a principal ideal of $\mathfrak{R}_\mathfrak{p}$.*

The necessity is included in (8.5) and (8.6). Condition (ii) implies that

$$\mathfrak{a}\mathfrak{R}_\mathfrak{p}.(\mathfrak{R}_\mathfrak{p} : \mathfrak{a}\mathfrak{R}_\mathfrak{p}) = \mathfrak{R}_\mathfrak{p}, \quad \text{i.e. } \mathfrak{a}(\mathfrak{R}_\mathfrak{p} : \mathfrak{a}) = \mathfrak{R}_\mathfrak{p},$$

for every maximal ideal $\mathfrak{p}$. According to (i), $\mathfrak{a} = \mathfrak{R}.(a_1, \ldots, a_s)$, say. This implies that the obvious inequality $\mathfrak{R}_\mathfrak{p}.(\mathfrak{R} : \mathfrak{a}) \subseteq (\mathfrak{R}_\mathfrak{p} : \mathfrak{a})$ reduces, in the present case, to equality. (Namely, if $b\mathfrak{a} \subseteq \mathfrak{R}_\mathfrak{p}$, there exist elements u_i of $\mathfrak{R}$ not in $\mathfrak{p}$, such that $u_i b a_i \in \mathfrak{R}$, whence $u_1 \ldots u_s b\mathfrak{a} \subseteq \mathfrak{R}$.) Using these relations, it follows from (8.1) that

$$\mathfrak{a}.(\mathfrak{R} : \mathfrak{a}) = \bigcap \mathfrak{a}(\mathfrak{R} : \mathfrak{a})\,\mathfrak{R}_\mathfrak{p} = \bigcap \mathfrak{a}(\mathfrak{R}_\mathfrak{p} : \mathfrak{a}) = \bigcap \mathfrak{R}_\mathfrak{p} = \mathfrak{R}.$$

The following simple result belonging to the same order of ideas is also used in Part I:

(8.8) Suppose $\mathfrak{R}$ has only one maximal ideal $\mathfrak{P}$. If a subset $\mathfrak{A}$ of the quotient field of $\mathfrak{R}$ generates a principal ideal, $(\mathfrak{A}) = b\mathfrak{R}$, then a generating element for $(\mathfrak{A})$ can be selected from $\mathfrak{A}$.

In fact, $\mathfrak{A} \not\subseteq b\mathfrak{P}$ provided $b \neq 0$; and any element of $b\mathfrak{R}$ not in $b\mathfrak{P}$ is an associate of b.

9. Commutative algebras

Some results in the theory of commutative algebras, which find numerous applications in Part I, are given here. In this section, Λ denotes a commutative algebra over a field $\mathfrak{k}$, of finite rank $m > 0$. It is assumed that Λ has unity, denoted by ϵ, and that $1.\epsilon = \epsilon$, where 1 is the unity element of $\mathfrak{k}$. The zero elements of Λ and $\mathfrak{k}$ are denoted by $\mathbf{0}$ and 0 respectively.

The definition of the regular representation, and definitions of the characteristic polynomial and norm $N(\alpha)$ and trace $T(\alpha)$ of an element $\alpha \in \Lambda$, need not be reproduced here. The discriminant of α is defined to be $D(\alpha) = D(\epsilon, \alpha, \ldots, \alpha^{m-1})$; but it is not hard to prove† that $D(\alpha)$ is equal to the discriminant of the characteristic polynomial of α. It follows from the transformation law for discriminants that the discriminant of m linearly dependent elements of Λ is zero. For m-term bases of Λ over $\mathfrak{k}$, however, there are two possibilities: either every basis has zero discriminant (Λ *has discriminant zero over* $\mathfrak{k}$), or every basis has non-zero

† Cf. Krull (1939*a*), Lemma 4.

Downloaded from rsta.royalsocietypublishing.org

discriminant (Λ *has non-zero discriminant over* $\mathfrak{k}$). These alternatives are elucidated by a theorem of E. Noether:†

Definition. Λ is *semi-simple and separable* if it is the direct sum of separable extension-fields of $\mathfrak{k}$.

THEOREM 16. Λ *has non-zero discriminant over* $\mathfrak{k}$ *if and only if it is semi-simple and separable.*

Complementary Bases. Two bases $\omega_1, \ldots, \omega_m$ and $\theta_1, \ldots, \theta_m$ of Λ over $\mathfrak{k}$ are said to be *complementary* if $T(\omega_i\theta_j) = \delta_{ij}$. These equations are equivalent to $\theta_i = \Sigma\theta_j\, T(\theta_i\omega_j)$; consequently they are equivalent to (9.1), and to (9.2):

(9.1) For any $\beta \in \Lambda$, $\quad \beta = \Sigma\theta_j\, T(\beta\omega_j)$.

(9.2) $$\omega_i = \Sigma\theta_j\, T(\omega_i\omega_j) \quad (i = 1, \ldots, m).$$

These equations, in the form (9.2), imply that $\Sigma T(\omega_i\omega_j)\, T(\theta_j\theta_k) = T(\omega_i\theta_k) = \delta_{ik}$, whence

(9.3) $$D(\omega_1, \ldots, \omega_m)\, .\, D(\theta_1, \ldots, \theta_m) = 1.$$

Thus for the existence of complementary bases it is necessary that Λ have non-zero discriminant over $\mathfrak{k}$. When that condition is fulfilled, the unique basis complementary to $\omega_1, \ldots, \omega_m$ is defined by (9.2). Assuming that these bases are in fact complementary, it is seen from (9.1) that, in the regular representation determined by $\theta_1, \ldots, \theta_m$, the matrix representing β has elements $T(\beta\omega_i\theta_j)$. It follows that $T(\beta(\omega_1\theta_1 + \ldots + \omega_m\theta_m)) = T(\beta)$ for all $\beta \in \Lambda$; and hence, using (9.1) again,

(9.4) $$\omega_1\theta_1 + \ldots + \omega_m\theta_m = \epsilon.$$

Differents. For any $\alpha \in \Lambda$, with characteristic polynomial $f(x)$, the element $\epsilon f'(\alpha)$ is called the *different of* α, denoted by $d(\alpha)$.

The next theorem can easily be proved by the use of conjugates, in the case when Λ is a field; but the theorem belongs more properly to the theory of algebras.

THEOREM 17. *Let* α *be any element of* Λ, *with characteristic polynomial* $f(x)$, *and define elements* $\eta_0, \ldots, \eta_{m-1}$ *of* Λ *by the identity*

$$\epsilon f(x) = (\epsilon x - \alpha)\,(\eta_0 + \eta_1 x + \ldots + \eta_{m-1}x^{m-1}).$$

Then, for any $\beta \in \Lambda$, $\quad \beta d(\alpha) = \epsilon T(\beta\eta_0) + \alpha T(\beta\eta_1) + \ldots + \alpha^{m-1} T(\beta\eta_{m-1})$.

Proof. Let the matrices representing β, α, and η_{i-1} in the regular representation be B, A, and H_{i-1}. Then $(x\mathsf{I} - \mathsf{A})\,\Sigma x^{i-1}\mathsf{H}_{i-1} = f(x)\,\mathsf{I}$, so $\Sigma x^{i-1}\mathsf{H}_{i-1}$ is the adjoint matrix of $(x\mathsf{I} - \mathsf{A})$; $\Sigma\alpha^{i-1}\mathsf{H}_{i-1}$ is the adjoint of $(\alpha\mathsf{I} - \epsilon\mathsf{A})$. Now use the elementary lemma:

If P and Q are m-square matrices with elements in any commutative ring, and Q_a is the adjoint of Q, the coefficient of y in $|\, y\mathsf{P} + \mathsf{Q}\,|$ is trace $(\mathsf{P}\mathsf{Q}_a)$.

Since $|\, y(\beta\mathsf{I} - \epsilon\mathsf{B}) + (\alpha\mathsf{I} - \epsilon\mathsf{A})\,|$ vanishes identically,‡ it follows that the trace of

$$(\beta\mathsf{I} - \epsilon\mathsf{B})\,\Sigma\alpha^{i-1}\mathsf{H}_{i-1}$$

is zero; $$\text{trace}\,(\mathsf{B}\Sigma\alpha^{i-1}\mathsf{H}_{i-1}) = \text{trace}\,(\beta\Sigma\alpha^{i-1}\mathsf{H}_{i-1}).$$

The left-hand side is $\Sigma\alpha^{i-1}T(\beta\eta_{i-1})$, and the right is the coefficient of y in $|\, y\beta\mathsf{I} + \alpha\mathsf{I} - \epsilon\mathsf{A}\,|$, i.e. in $f(y\beta + \alpha)$, which is $\beta f'(\alpha)$.

It follows from the preceding theorem that $N(d(\alpha)) = |\, T(\alpha^{i-1}\eta_{j-1})\,| = (-1)^{\frac{1}{2}m(m-1)}D(\alpha)$. Thus when $D(\alpha) \neq 0$, $d(\alpha)$ is a unit of Λ, and $T(\eta_{i-1}\alpha^{j-1}/d(\alpha)) = \delta_{ij}$; *the basis complementary to* $\epsilon, \alpha, \ldots, \alpha^{m-1}$ *is* $\eta_0/d(\alpha), \ldots, \eta_{m-1}/d(\alpha)$.

† See Krull (1939*a*), Theorem 1.

‡ The element $y\beta + \alpha$ of the extended algebra $\mathfrak{k}(y)\,.\,\Lambda$ is a zero of its own characteristic polynomial.

Downloaded from rsta.royalsocietypublishing.org

Primitive elements. An element $\alpha \in \Lambda$ is said to be *primitive* for Λ over $\mathfrak{k}$ if $\epsilon, \alpha, \ldots, \alpha^{m-1}$ is a $\mathfrak{k}$-basis for Λ, i.e. if $\Lambda = \epsilon\mathfrak{k}[\alpha]$. The non-vanishing of $D(\alpha)$ is a sufficient condition for α to be primitive, but this condition is not necessary, nor need Λ possess any primitive element. It must now be recalled that Λ, being a ring of finite Jordan-Hölder length, is uniquely expressible as the direct sum of monotypic subrings $\Lambda_1, \ldots, \Lambda_e$. Each of the Λ_i is an algebra over $\mathfrak{k}$. It is also convenient to make use of the extended algebra $\Lambda^{(y)} = \mathfrak{k}(y_1, \ldots, y_m) \cdot \Lambda$, where the y_i are indeterminates.

THEOREM 18. *Suppose that each of the monotypic components $\Lambda_1, \ldots, \Lambda_e$ of Λ possesses a primitive element.*

(1) *If $\omega_1, \ldots, \omega_m$ is a basis of Λ, the element $y_1\omega_1 + \ldots + y_m\omega_m$ is primitive for $\Lambda^{(y)}$.*

(2) *If $\mathfrak{k}$ has infinitely many elements, Λ itself possesses a primitive element.*

The proof is given in a condensed form, since Lemma 1 of Krull (1939*a*) is a special case of the theorem. The (monic) minimal polynomial $\Phi(x)$ of $y_1\omega_1 + \ldots + y_m\omega_m$ is a polynomial in the y, say $\Phi(x; y_1, \ldots, y_m)$. Take non-nilpotent primitive elements $\alpha_1, \ldots, \alpha_e$ for $\Lambda_1, \ldots, \Lambda_e$. The (primary) minimal polynomials of $y_1\alpha_1, \ldots, y_e\alpha_e$ are mutually prime, so the minimal polynomial of $y_1\alpha_1 + \ldots + y_e\alpha_e$ is their product, of degree m. Now

$$\Phi(y_1\alpha_1 + \ldots + y_e\alpha_e; z_1, \ldots, z_m) = \mathbf{0},$$

where the z are linear forms in the y over $\mathfrak{k}$, defined by the equation

$$z_1\omega_1 + \ldots + z_m\omega_m = y_1\alpha_1 + \ldots + y_e\alpha_e.$$

Hence the degree of $\Phi(x)$ is at least m.

In part (2) of the theorem, $c_1\alpha_1 + \ldots + c_e\alpha_e$ is a primitive element of Λ, for non-special $c_1, \ldots, c_e \in \mathfrak{k}$.

The preceding theorem directs attention to the question whether the monotypic components Λ_i of Λ possess primitive elements. This question is discussed below, after a preliminary investigation in Theorem 19. *For the rest of this section we assume that Λ is monotypic, with maximal ideal $\mathfrak{q}$ of exponent ν.*

THEOREM 19. *The following five propositions are equivalent:*

(i) *the only ideals of Λ are $\Lambda, \mathfrak{q}, \mathfrak{q}^2, \ldots, \mathfrak{q}^\nu = (\mathbf{0})$;*

(ii) *there is no ideal of Λ strictly between $\mathfrak{q}$ and $\mathfrak{q}^2$;*

(iii) *the $\mathfrak{k}$-modules $\mathfrak{q}^{t-1}/\mathfrak{q}^t$ $(t = 1, \ldots, \nu)$ all have the same rank;*

(iv) *the $\mathfrak{k}$-module $\mathfrak{q}/\mathfrak{q}^2$ has rank not greater than that of $\Lambda/\mathfrak{q}$;*

(v) *$\mathfrak{q}$ is a principal ideal of Λ.*

Proof. If $\mathfrak{g}$ and $\mathfrak{h} \supset \mathfrak{g}$ are Λ-ideals such that the Λ-module $\mathfrak{h}/\mathfrak{g}$ is simple, and η is an element of $\mathfrak{h}$ not in $\mathfrak{g}$, then $\mathfrak{h} = \eta\Lambda + \mathfrak{g}$. The annihilating ideal of $\mathfrak{h}/\mathfrak{g}$ is $\mathfrak{q}$ (Grundy (1942), (11.4)); multiplication by η maps $\Lambda/\mathfrak{q}$ on $\mathfrak{h}/\mathfrak{g}$; and this is a $\mathfrak{k}$-isomorphism, indeed a Λ-isomorphism. Hence (iii) is true when (i) is true, and (iv) is false when (ii) is false. When (ii) is true, there exists $\gamma \in \mathfrak{q}$ such that $\mathfrak{q} = \gamma\Lambda + \mathfrak{q}^2$; for any $t \geqslant 1$, $\mathfrak{q}^t = (\gamma\Lambda + \mathfrak{q}^2)^t \subseteq \gamma\Lambda + \mathfrak{q}^{t+1}$; and consequently $\mathfrak{q} = \gamma\Lambda + \mathfrak{q}^\nu = \gamma\Lambda$. When $\mathfrak{q} = \gamma\Lambda$, any Λ-ideal $\mathfrak{g} \subset \Lambda$ has a basis consisting of multiples of γ—$\mathfrak{g} = \gamma\mathfrak{g}'$, where $\mathfrak{g}'$ is a Λ-ideal. Thus (v) implies (i). The theorem is established by the implications

$$\text{(i)} \rightarrow \text{(iii)},\ \text{(iv)} \rightarrow \text{(ii)},\ \text{(ii)} \rightarrow \text{(v)},\ \text{(v)} \rightarrow \text{(i)},\ \text{and}\ \text{(iii)} \rightarrow \text{(iv)},$$

of which the last is obvious and the rest have been proved.

Downloaded from rsta.royalsocietypublishing.org

(9.5) If $\Lambda = \epsilon\mathfrak{k}[\alpha] + \mathfrak{q}^2$, α is a primitive element for Λ (and conversely). In that case, $\mathfrak{q} = \epsilon g(\alpha).\Lambda$, where $g(x)$ is the minimal polynomial of $\alpha \bmod \mathfrak{q}$ over $\mathfrak{k}$.

It is clear that $\epsilon\mathfrak{k}[\alpha] \cap \mathfrak{q} = \epsilon\mathfrak{k}[\alpha].\gamma$, where $\gamma = \epsilon g(\alpha)$. By the modular axiom, the hypothesis implies that $\mathfrak{q} = \mathfrak{q} \cap \Lambda = \epsilon\mathfrak{k}[\alpha].\gamma + \mathfrak{q}^2$. Hence $\mathfrak{q}^t \subseteq \epsilon\mathfrak{k}[\alpha].\gamma + \mathfrak{q}^{t+1}$ for all $t \geqslant 1$. By trivial inductions, it is seen that $\Lambda = \epsilon\mathfrak{k}[\alpha] + \mathfrak{q}^t$ and $\mathfrak{q} = \epsilon\mathfrak{k}[\alpha].\gamma + \mathfrak{q}^t$; but $\mathfrak{q}^\nu = (\mathbf{0})$.

THEOREM 20. *If Λ has a primitive element, the propositions of Theorem* 19 *are true. If they are true, and $\Lambda/\mathfrak{q}$ is separable over $\mathfrak{k}$, then Λ possesses a primitive element.*†

The first part of the theorem is included in (9.5). Under the conditions of the second part, Λ certainly contains an element α which is primitive mod $\mathfrak{q}$, i.e. such that $\Lambda = \epsilon\mathfrak{k}[\alpha] + \mathfrak{q}$. No more need be said about the case $\nu = 1$. When $\nu > 1$, it can be arranged further that $\epsilon g(\alpha) \not\equiv \mathbf{0} \bmod \mathfrak{q}^2$, where $g(x)$ is the minimal polynomial of $\alpha \bmod \mathfrak{q}$ over $\mathfrak{k}$. Indeed, if this condition is not already satisfied by α it is satisfied by $\alpha + \zeta$, where ζ is an element of $\mathfrak{q}$ not in $\mathfrak{q}^2$; for then $\epsilon g(\alpha+\zeta) \equiv \epsilon g(\alpha) + \zeta g'(\alpha) \equiv \zeta g'(\alpha) \not\equiv \mathbf{0} \bmod \mathfrak{q}^2$. With such an α, if s denotes the degree of $g(x)$, the elements $\epsilon g(\alpha), \alpha g(\alpha), \ldots, \alpha^{s-1} g(\alpha)$ are linearly independent mod $\mathfrak{q}^2$. As (iv) of Theorem 19 is postulated, it follows that $\mathfrak{q} = \epsilon\mathfrak{k}[\alpha].\epsilon g(\alpha) + \mathfrak{q}^2$; hence

$$\Lambda = \epsilon\mathfrak{k}[\alpha] + \mathfrak{q}^2,$$

and α is primitive by (9.5).

COROLLARY. *Suppose that an element $\alpha \in \Lambda$ is primitive* mod $\mathfrak{q}$, *and let $g(x)$ be its minimal polynomial* mod $\mathfrak{q}$. *When the propositions of Theorem* 19 *are true, and $\nu > 1$, α is primitive for Λ if and only if $\epsilon g(\alpha) \not\equiv \mathbf{0} \bmod \mathfrak{q}^2$.*

10. COUNTER-EXAMPLES

F. K. Schmidt‡ has shown how to construct a pair of valuation rings $\mathfrak{F}$ and $\mathfrak{G} \supset \mathfrak{F}$, which satisfy the conditions imposed on $\mathfrak{R}$ and $\mathfrak{S}$ in Part I, except that the quotient field G of $\mathfrak{G}$ is inseparable over the quotient field F of $\mathfrak{F}$. From the relevant properties of $\mathfrak{F}$ and $\mathfrak{G}$, described below, it will be seen that the separability of L over K is not superfluous for Theorems 10 and 13. Another counter-example, derived from that of Schmidt, is given in the second half of this section. In this second example, $\mathfrak{R}$ and $\mathfrak{S} \supset \mathfrak{R}$ are valuation rings satisfying the conditions imposed on $\mathfrak{R}$ and $\mathfrak{S}$ in Part I; but $\mathfrak{R}$ and $\mathfrak{S}$ are of rank 2, so that the maximal ideal of $\mathfrak{R}$ is not convergent. Hence it will be seen that the strong convergence of $\mathfrak{p}$ is not entirely superfluous for Theorems 10 and 13.

Let Γ be any field of prime characteristic p, and

$$G = \Gamma(\bar{u}, \bar{y}_1, \bar{z}_1, \bar{z}_2, \ldots), \quad F = \Gamma(\bar{u}, \bar{y}_1^p, \bar{z}_1, \bar{z}_2, \ldots),$$

where $\bar{u}, \bar{y}_1$, and the $\bar{z}_i$ $(i \geqslant 1)$ are algebraically independent over Γ. It is clear that $G = F(\bar{y}_1)$ is inseparable of degree p over F; the pth power of any element of G belongs to F. Further, put

$$H = \Gamma(\bar{y}_1, \bar{y}_2, \ldots),$$

† Cf. p. 274 of Pickert (1938). I am indebted to Mr P. Hall for drawing my attention to that paper.

‡ Schmidt (1936), particularly p. 449, with the constants a_i replaced by zero. (In this case there is no need to postulate that Γ has infinitely many elements.) The fact that the degree of $\mathfrak{Q}$ over $\mathfrak{F}$ is 1 was pointed out in footnote 44*h* of Krull (1939*b*).

See Krull (1932) for the relevant general valuation theory. On the valuation theory of algebraic extension-fields, cf. Krull (1935), nn. 48, 40; Ostrowski (1934), n. 30 (finiteness of the 'Verzweigungsindex'). Reference may also be made to Theorems 7 and 8 of Krull (1936).

Downloaded from rsta.royalsocietypublishing.org

where $\bar{y}_2, \bar{y}_3, \ldots$ are defined by the equations

$$\bar{u}\bar{y}_{i+1} = \bar{y}_i + \bar{z}_i \quad (i \geqslant 1).$$

Evidently $\bar{u}$ is transcendental over H, and $G = H(\bar{u})$. The ring $\mathfrak{G}$ is now defined to be that valuation ring of G over H in which $\bar{u}$ has positive value. $\mathfrak{G}$ is a rank 1 discrete valuation ring; consequently the same is true of $\mathfrak{F} = F \cap \mathfrak{G}$. The maximal ideals of $\mathfrak{G}$ and $\mathfrak{F}$ are respectively $\mathfrak{Q} = \bar{u}\mathfrak{G}$ and $\mathfrak{P} = \bar{u}\mathfrak{F}$, so $\mathfrak{Q} = \mathfrak{P}\mathfrak{G}$. Because the pth power of every element of $\mathfrak{G}$ belongs to $\mathfrak{F}$, $\mathfrak{G}$ is integrally dependent on $\mathfrak{F}$ (and hence $\mathfrak{G}$ is the only valuation ring of G lying over $\mathfrak{F}$).

The degree of $\mathfrak{Q}$ over $\mathfrak{F}$ is 1; that is to say, every element of $\mathfrak{G}$ is congruent mod $\mathfrak{Q}$ to an element of $\mathfrak{F}$. In fact, any element of $\mathfrak{G}$ is obviously congruent mod $\mathfrak{Q}$ to an element of H; and hence the assertion follows without difficulty from the relations

$$\bar{z}_i \in \mathfrak{F}, \quad \bar{y}_i \equiv -\bar{z}_i \ (\mathfrak{Q}) \quad (i \geqslant 1).$$

Moreover, $\mathfrak{G}$ does not possess a finite $\mathfrak{F}$-basis. Namely, the contrary would imply the existence of a non-zero element c of $\mathfrak{F}$ such that

$$c\mathfrak{G} \subseteq \mathfrak{F}.(1, \bar{y}_1, \ldots, \bar{y}_1^{p-1});$$

but that is impossible, since $\bar{y}_{r+1}$ belongs to $\mathfrak{G}$, and

$$\bar{y}_{r+1} = \bar{u}^{-r}(\bar{z}_1 + \bar{u}\bar{z}_2 + \ldots + \bar{u}^{r-1}\bar{z}_r) + \bar{u}^{-r}\bar{y}_1 \quad (r \geqslant 0).$$

Second Example. Let Δ be the field of rational numbers, and let

$$L = \Delta(u, y_1, z_1, z_2, \ldots), \quad K = \Delta(u, y_1^p, z_1, z_2, \ldots),$$

where u, y_1, and the z_i $(i \geqslant 1)$ are algebraically independent over Δ, and p is a prime number. Clearly L is separable of degree p over K. Let $\mathfrak{B}$ be that rank 1 discrete valuation ring of L which consists of all elements expressible as

$$\frac{\phi(u, y_1, z_1, z_2, \ldots)}{\psi(u, y_1, z_1, z_2, \ldots)},$$

where ϕ, ψ are polynomials with integer coefficients, and $\psi \not\equiv 0 \bmod p$. In the homomorphism from $\mathfrak{B}$ to its residue field G, the ring of integers is mapped on the field Γ of integers reduced mod p. The images $\bar{u}, \bar{y}_1, \bar{z}_1, \bar{z}_2, \ldots$ of $u, y_1, z_1, z_2, \ldots$ in G are algebraically independent over Γ, and $G = \Gamma(\bar{u}, \bar{y}_1, \bar{z}_1, \bar{z}_2, \ldots)$. If $\mathfrak{A}$ denotes the (rank 1 discrete) contracted valuation ring $\mathfrak{B} \cap K$, the residue field F of $\mathfrak{A}$ is the subfield $\Gamma(\bar{u}, \bar{y}_1^p, \bar{z}_1, \bar{z}_2, \ldots)$ of G. *Thus F and G may be identified with the F and G of Schmidt's example.*

It is next proved that $\mathfrak{B}$ is the only valuation ring of L lying over $\mathfrak{A}$. For this, it is enough to prove that if $\mathfrak{B}'$ is any such valuation ring of L (i.e. such that $\mathfrak{B}' \cap K = \mathfrak{A}$), then $\mathfrak{B}' \supseteq \mathfrak{B}$. Now y_1 belongs to $\mathfrak{B}'$ because y_1^p belongs to $\mathfrak{A}$, while $u, z_1, z_2, \ldots$ belong to $\mathfrak{A}$ itself. Taking ϕ and ψ as in the definition of $\mathfrak{B}$, it is seen that $\phi(u, y_1, z_1, z_2, \ldots)$ and $\psi(u, y_1, z_1, z_2, \ldots)$ belong to $\mathfrak{B}'$. Hence it remains to prove that $\psi(u, y_1, z_1, z_2, \ldots)$ is a unit of $\mathfrak{B}'$. That follows from the congruence

$$(\psi(u, y_1, z_1, z_2, \ldots))^p \equiv \psi(u^p, y_1^p, z_1^p, z_2^p, \ldots) \bmod p;$$

for the right-hand side is a unit of $\mathfrak{B}'$ (indeed, of $\mathfrak{A}$); and p is a non-unit of $\mathfrak{B}'$, being a non-unit of $\mathfrak{A}$.

Let $\mathfrak{F}, \mathfrak{G}$ be the valuation rings of F, G, with maximal ideals $\mathfrak{P}, \mathfrak{Q}$ respectively, considered in Schmidt's example. $\mathfrak{S}$ is defined to be the set of elements of $\mathfrak{B}$ whose images in G belong

Downloaded from rsta.royalsocietypublishing.org

to $\mathfrak{G}$—$\mathfrak{S}$ is a discrete valuation ring of rank 2. The contracted valuation ring $\mathfrak{R} = \mathfrak{S} \cap K$ is also discrete, of rank 2; in fact, $\mathfrak{R}$ is the set of elements of $\mathfrak{A}$ whose images in F belong to $\mathfrak{F}$.

Any valuation ring $\mathfrak{S}'$ of L lying over $\mathfrak{R}$ has rank 2, and is therefore contained in a rank 1 valuation ring $\mathfrak{B}'$ of L; the image of $\mathfrak{S}'$ in the residue field of $\mathfrak{B}'$ is a valuation ring $\mathfrak{G}'$, and $\mathfrak{S}'$ consists of all elements of $\mathfrak{B}'$ whose images in the residue field belong to $\mathfrak{G}'$. The valuation ring $\mathfrak{B}' \cap K$ can be none other than $\mathfrak{A}$. By the preceding remarks, $\mathfrak{B}' = \mathfrak{B}$. It follows that $\mathfrak{G}'$ is a valuation ring of G lying over $\mathfrak{F}$, whence $\mathfrak{G}' = \mathfrak{G}$. Thus $\mathfrak{S}' = \mathfrak{S}$; $\mathfrak{S}$ is the only valuation ring of L lying over $\mathfrak{R}$; and consequently $\mathfrak{S}$ is integrally dependent on $\mathfrak{R}$.

The image in G of the maximal ideal $\mathfrak{q}$ of $\mathfrak{S}$ is the maximal ideal $\mathfrak{Q}$ of $\mathfrak{G}$. Since $\mathfrak{Q} = \bar{u}\mathfrak{G}$, it follows that $\mathfrak{q} = u\mathfrak{S}$; similarly, the maximal ideal of $\mathfrak{R}$ is $\mathfrak{p} = u\mathfrak{R}$. Hence $\mathfrak{q} = \mathfrak{p}\mathfrak{S}$.

The image in G of a mod $\mathfrak{q}$ remainder-class in $\mathfrak{S}$ is a mod $\mathfrak{Q}$ remainder-class in $\mathfrak{G}$. Since the latter remainder-class is known to contain an element of $\mathfrak{F}$, the former must contain an element of $\mathfrak{R}$. This shows that the degree of $\mathfrak{q}$ over $\mathfrak{R}$ is 1.

Next, note that $\mathfrak{S}$ does not possess a finite $\mathfrak{R}$-basis; for it is clear that the existence of such a basis would imply the existence of a finite $\mathfrak{F}$-basis for $\mathfrak{G}$.

In conclusion, it is easy to deduce that

$$D(\alpha_1, \ldots, \alpha_p) \equiv 0 \ (\mathfrak{p}), \quad d(\alpha_1) \equiv 0 \ (\mathfrak{q}),$$

for any $\alpha_1, \ldots, \alpha_p \in \mathfrak{S}$. In fact, the contrary hypotheses would imply that $\mathfrak{S}$ had a finite $\mathfrak{R}$-basis,

$$\mathfrak{S} = \mathfrak{R}.(\alpha_1, \ldots, \alpha_p) \quad \text{or} \quad \mathfrak{S} = \mathfrak{R}[\alpha_1]$$

respectively.

References

Albert, A. A. 1937 *Modern Higher Algebra.* Chicago.
Dedekind, R. & Weber, H. 1882 *J. reine angew. Math.* **92**, 181.
Fitting, H. 1937 *J. reine angew. Math.* **178**, 107.
Fricke, R. 1928 *Lehrbuch der Algebra*, **3**. Braunschweig.
Grell, H. 1927*a* *Math. Ann.* **97**, 490.
Grell, H. 1927*b* *Math. Ann.* **97**, 524.
Grell, H. 1936 *Math. Z.* **40**, 629.
Grundy, P. M. 1942 *Proc. Camb. Phil. Soc.* **38**, 241.
Helms, A. 1935 *Math. Ann.* **111**, 438.
Krull, W. 1928 *S.B. Heidelberg. Akad. Wiss.*, Math.-naturw. Klasse, 7. Abhandlung.
Krull, W. 1929 *Math. Ann.* **101**, 729.
Krull, W. 1930 *Math. Z.* **31**, 558.
Krull, W. 1932 *J. reine angew. Math.* **167**, 160.
Krull, W. 1935 Idealtheorie. *Ergebn. Math.* 4, Heft 3.
Krull, W. 1936 *Math. Z.* **41**, 545.
Krull, W. 1937 *Math. Z.* **42**, 745.
Krull, W. 1939*a* *Math. Z.* **45**, 1.
Krull, W. 1939*b* Allgemeine Modul-, Ring- und Idealtheorie. *Enzykl. math. Wiss.* (2nd ed.), **I1**, 11.
Lorenzen, P. 1939 *Math. Z.* **45**, 533.
Muhly, H. T. 1943 *Trans. Amer. Math. Soc.* **54**, 340.
Ostrowski, A. 1934 *Math. Z.* **39**, 269.
Pickert, G. 1938 *Math. Ann.* **116**, 217.
Prüfer, H. 1932 *J. reine angew. Math.* **168**, 1.
Schmeidler, W. 1928 *Math. Z.* **28**, 116.
Schmidt, F. K. 1936 *Math. Z.* **41**, 443.
van der Waerden, B. L. 1931 *Moderne Algebra*, **2** (2nd ed. 1940). Berlin.
Zariski, O. 1939 *Amer. J. Math.* **61**, 249.
Zariski, O. 1940 *Amer. J. Math.* **62**, 187.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES
PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES