METHODS
OF
ALGEBRAIC GEOMETRY

by

W. V. D. HODGE, Sc.D., F.R.S.

Formerly Lowndean Professor of Astronomy and Geometry, and Fellow of Pembroke College, Cambridge

and

D. PEDOE, Ph.D.

Emeritus Professor of Mathematics University of Minnesota

VOLUME III

BOOK V: BIRATIONAL GEOMETRY

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1954
Reissued in the Cambridge Mathematical Library 1994

ISBN 0 521 46775 6 paperback

Transferred to digital printing 2003

CONTENTS

BOOK V

BIRATIONAL GEOMETRY

CHAPTER XV

IDEAL THEORY OF COMMUTATIVE RINGS

In Volume II we were concerned mainly with the geometry of varieties in projective space, regarded as subvarieties of the space. We had, however, occasion to consider relations between different varieties of the same space, or of different spaces; for this we used the correspondence theory of Chapter XI. In particular, use was made from time to time of birational correspondences between irreducible varieties; if U and V are irreducible varieties in spaces with coordinate systems $(x_0, \ldots, x_n)$ and $(y_0, \ldots, y_m)$ respectively, they are in birational correspondence if there exists a correspondence between them whose equations include equations of the form

$$x_i f_j(y_0, \ldots, y_m) - x_j f_i(y_0, \ldots, y_m) = 0 \quad (i,j = 0, \ldots, n),$$
$$y_i g_j(x_0, \ldots, x_n) - y_j g_i(x_0, \ldots, x_n) = 0 \quad (i,j = 0, \ldots, m),$$

where not all forms $f_i(y)$ vanish on V, and not all forms $g_i(x)$ vanish on U. An important branch of the theory of algebraic varieties deals with the investigation of properties common to birationally equivalent varieties. In this theory we are concerned, not so much with the properties of individual varieties as varieties in projective space, as with properties of sets of algebraic varieties which are birationally equivalent to one another. This branch of the theory of varieties is called *birational geometry*.

The purpose of this volume is to introduce the reader to the algebraic methods which have proved most useful in birational geometry, and to establish certain basic results with which a geometer must be familiar before he embarks on a systematic study of birational geometry. For this purpose, it is necessary to develop more fully certain algebraic concepts introduced in Volume I, and to introduce new ones. In Chapter I the notion of a ring was introduced, and mention has also been made in earlier

chapters of ideals in a ring, but only the most elementary properties of these have been used. It is now necessary to study commutative rings, and ideals in them, more systematically, and the present chapter is devoted to this end.

1. Ideals in a commutative ring. Let $\mathfrak{R}$ be any commutative ring. A non-empty set $\mathfrak{i}$ of elements of $\mathfrak{R}$ is said to form an *ideal* in $\mathfrak{R}$ if it has the two properties: (i) if α and β are any elements belonging to $\mathfrak{i}$, then $\alpha - \beta$ belongs to $\mathfrak{i}$, (ii) if α belongs to $\mathfrak{i}$ and ρ is any element of $\mathfrak{R}$, then $\rho\alpha$ belongs to $\mathfrak{i}$.

The ring $\mathfrak{R}$ contains a zero element; if we take this to be ρ in (ii), then $0.\alpha = 0$ is in $\mathfrak{i}$. Thus every ideal in $\mathfrak{R}$ contains the zero of $\mathfrak{R}$. On the other hand, if a set $\mathfrak{i}$ consists solely of the zero of $\mathfrak{R}$, it satisfies the conditions (i) and (ii); hence it is an ideal. We call this the *zero ideal* of $\mathfrak{R}$. Again, if $\mathfrak{i}$ includes every element of $\mathfrak{R}$, it also satisfies conditions (i) and (ii); hence it forms an ideal, which we call the *unit ideal* of $\mathfrak{R}$. Thus every commutative ring contains at least two ideals, the zero ideal and the unit ideal. These two ideals are sometimes called *improper ideals*, and any ideal distinct from the zero ideal and the unit ideal is called a *proper ideal*.

If $\mathfrak{R}$ has unity e and $\mathfrak{i}$ contains e, $\mathfrak{i}$ contains $\rho e = \rho$, where ρ is any element of $\mathfrak{R}$. Hence $\mathfrak{i}$ is the unit ideal if it contains e.

It is convenient to determine at the outset which commutative rings possess no ideals other than the two improper ideals. We consider two cases.

Case I. Suppose that $\mathfrak{R}$ contains two elements ρ, ω such that $\rho\omega \neq 0$. (This is certainly the case when the ring has unity.) For such an element ω we consider the set $\mathfrak{i}$ of elements $\sigma\omega$, where σ can be any element in $\mathfrak{R}$. It is clear that $\mathfrak{i}$ satisfies the conditions (i) and (ii), and hence it is an ideal, and since $\mathfrak{i}$ contains $\rho\omega \neq 0$ it is not the zero ideal. If $\mathfrak{R}$ has only improper ideals, it follows that $\mathfrak{i} = \mathfrak{R}$, and hence if ν is any element of $\mathfrak{R}$, there exists an element x in $\mathfrak{R}$ such that

$$x\omega = \nu.$$

Let e be a solution of this equation when $\nu = \omega$, and let x be a solution for an arbitrarily chosen element ν of $\mathfrak{R}$. Then

$$e\nu = ex\omega = x(e\omega) = x\omega = \nu.$$

It follows that $\mathfrak{R}$ has unity, namely, e. Now let ν be any non-zero element of $\mathfrak{R}$. The set of elements of the form $\sigma\nu$, where σ is any

element of $\mathfrak{R}$, forms an ideal $\mathfrak{j}$ which contains the element $e\nu = \nu$, and $\mathfrak{j}$ is therefore the unit ideal. Then there exists an element ν' in $\mathfrak{R}$ such that $\nu'\nu = e$. Hence every non-zero element in $\mathfrak{R}$ has an inverse. $\mathfrak{R}$ is therefore a field.

Conversely, suppose that $\mathfrak{R}$ is a field, and let $\mathfrak{i}$ be any ideal in $\mathfrak{R}$ which is not the zero ideal. $\mathfrak{i}$ contains a non-zero element α. Let β be any element of $\mathfrak{R}$. By property (ii), $\mathfrak{i}$ contains $\beta\alpha^{-1}.\alpha = \beta$. Hence $\mathfrak{i}$ contains every element of $\mathfrak{R}$ and is therefore the unit ideal.

Case II. Suppose that $\mathfrak{R}$ is a commutative ring, not consisting solely of the zero element, such that, if α, β are any two elements of $\mathfrak{R}$, $\alpha\beta = 0$, and let ω be any non-zero element of $\mathfrak{R}$. The set of elements $0, \pm\omega, \pm 2\omega, \pm 3\omega, \ldots$ clearly forms an ideal $\mathfrak{i}$ in $\mathfrak{R}$, different from the zero ideal. Hence, if the only ideals in $\mathfrak{R}$ are improper, $\mathfrak{i} = \mathfrak{R}$. The elements $0, \pm\omega, \pm 2\omega, \pm 3\omega, \ldots$ cannot all be distinct, for, if they were, the elements $0, \pm 2\omega, \pm 4\omega, \ldots$ would constitute a proper ideal in $\mathfrak{R}$, and we are assuming that every ideal in $\mathfrak{R}$ is improper. Let m be the smallest positive integer such that $m\omega = 0$. Then $0, \omega, 2\omega, \ldots, (m-1)\omega$ are the elements of $\mathfrak{R}$. If m is composite, say $m = ab$ where $a > 1, b > 1$, the set $0, a\omega, 2a\omega, \ldots, (b-1)a\omega$ would, clearly, constitute a proper ideal in $\mathfrak{R}$, contrary to our hypothesis. Hence m is a prime number p. From this it follows that if Ω is the 2×2 matrix over the ring of integers modulo p,

$$\Omega = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$\mathfrak{R}$ is isomorphic with the ring consisting of $0, \Omega, 2\Omega, \ldots, (p-1)\Omega$, and we can verify at once that if $\mathfrak{R}$ is isomorphic with this ring, the only ideals in it are improper. Hence we have

THEOREM I. *A ring $\mathfrak{R}$ which is a field contains only improper ideals. Conversely, any ring whose only ideals are improper ideals is either a field or is isomorphic with the ring of matrices of the form*

$$\begin{pmatrix} 0 & k \\ 0 & 0 \end{pmatrix}$$

over the ring of integers reduced modulo p, for some prime number p.

We now return to the general theory of ideals in a commutative ring $\mathfrak{R}$. We can construct an ideal in $\mathfrak{R}$ as follows. Let $\omega_1, \ldots, \omega_r$ be a finite set of elements in $\mathfrak{R}$, and consider the set $\mathfrak{i}$ of elements in $\mathfrak{R}$ which can be written in the form

$$\alpha_1\omega_1 + \ldots + \alpha_r\omega_r + n_1\omega_1 + \ldots + n_r\omega_r, \qquad (1)$$

where $\alpha_1, \ldots, \alpha_r$ are any elements of $\mathfrak{R}$, and $n_i\omega_i$ stands for the sum of n_i elements each equal to ω_i. If $\mathfrak{R}$ has unity e, we can write the element as

$$(\alpha_1 + n_1 e)\,\omega_1 + \ldots + (\alpha_r + n_r e)\,\omega_r = \alpha_1'\omega_1 + \ldots + \alpha_r'\omega_r,$$

where $\alpha_1', \ldots, \alpha_r'$ are in $\mathfrak{R}$, so that it is unnecessary to include the terms $n_1\omega_1, \ldots, n_r\omega_r$ in (1). It can be verified at once that the set $\mathfrak{i}$ satisfies the conditions (i) and (ii), and hence forms an ideal. The ideal is usually described as the ideal *generated by* $\omega_1, \ldots, \omega_r$, or *having the basis* $\omega_1, \ldots, \omega_r$, and is denoted by $\mathfrak{R}.(\omega_1, \ldots, \omega_r)$. From the definition of the basis, it is clear that the elements of a basis for an ideal $\mathfrak{i}$ belong to $\mathfrak{i}$. It is not, however, clear that every ideal in $\mathfrak{R}$ has a finite basis, that is that, given an ideal $\mathfrak{i}$ in $\mathfrak{R}$, there exists a finite set of elements of $\mathfrak{i}$, say, $\omega_1, \ldots, \omega_r$, such that $\mathfrak{i} = \mathfrak{R}.(\omega_1, \ldots, \omega_r)$. If the ring $\mathfrak{R}$ has the property that every ideal in $\mathfrak{R}$ possesses a finite basis, we say that *the Basis Theorem holds in* $\mathfrak{R}$. Many results can be proved for rings in which the Basis Theorem holds which are not true for more general rings. An example of a ring in which the Basis Theorem holds is provided by the ring of polynomials in r indeterminates over a commutative field [IV, § 2, Th. I]. For certain special rings, such as the ring of natural integers, or the ring of polynomials in one indeterminate over a commutative field, it can be proved that every ideal has a basis consisting of a single element. An ideal in a ring $\mathfrak{R}$ generated by a single element is called a *principal ideal*, and a ring in which every ideal is a principal ideal is called a *principal ideal ring*.

We now introduce certain notational conventions. If α is any element of the ideal $\mathfrak{i}$ we shall write $\alpha \in \mathfrak{i}$, or, more usually,

$$\alpha = 0 \ (\mathfrak{i}),$$

and when $\mathfrak{i} = \mathfrak{R}.(\omega_1, \ldots, \omega_r)$, we shall also write this in the form

$$\alpha = 0 \pmod{\omega_1, \ldots, \omega_r}.$$

If $\mathfrak{j}$ is an ideal every element of which is in $\mathfrak{i}$, we shall write $\mathfrak{j} \subseteq \mathfrak{i}$, or, more usually,

$$\mathfrak{j} = 0 \ (\mathfrak{i}).$$

It is clear that if we have, simultaneously,

$$\mathfrak{j} = 0 \ (\mathfrak{i}) \quad \text{and} \quad \mathfrak{i} = 0 \ (\mathfrak{j}),$$

then $\mathfrak{i} = \mathfrak{j}$.

We now define the elementary operations which can be performed on ideals.

I. Let $\mathfrak{i}, \mathfrak{j}$ be ideals in the commutative ring $\mathfrak{R}$. Consider the set $\mathfrak{k}$ of elements of $\mathfrak{R}$ which can be written in the form $\alpha+\beta$, where

$$\alpha = 0 \ (\mathfrak{i}) \quad \text{and} \quad \beta = 0 \ (\mathfrak{j}).$$

If $\alpha+\beta$ and $\alpha'+\beta'$ are two such elements,

$$(\alpha+\beta)-(\alpha'+\beta') = (\alpha-\alpha')+(\beta-\beta'),$$

where $$\alpha-\alpha' = 0 \ (\mathfrak{i}) \quad \text{and} \quad \beta-\beta' = 0 \ (\mathfrak{j}),$$

and if ρ is any element of $\mathfrak{R}$,

$$\rho(\alpha+\beta) = \rho\alpha+\rho\beta,$$

where $$\rho\alpha = 0 \ (\mathfrak{i}), \quad \rho\beta = 0 \ (\mathfrak{j}).$$

Hence $\mathfrak{k}$ is an ideal, which we denote by $(\mathfrak{i}, \mathfrak{j})$; it is called the *join* of $\mathfrak{i}$ and $\mathfrak{j}$.

The join $(\mathfrak{i}, \mathfrak{j})$ has the following properties, the proofs of which are immediate:

(i) $$\mathfrak{i} \subseteq (\mathfrak{i}, \mathfrak{j}), \quad \mathfrak{j} \subseteq (\mathfrak{i}, \mathfrak{j});$$

(ii) $$(\mathfrak{i}, \mathfrak{j}) = (\mathfrak{j}, \mathfrak{i});$$

(iii) $$(\mathfrak{i}, \mathfrak{i}) = \mathfrak{i};$$

(iv) if $\mathfrak{a} = (\mathfrak{i}, \mathfrak{j}), \quad \mathfrak{b} = (\mathfrak{j}, \mathfrak{k})$, where $\mathfrak{k}$ is any other ideal of $\mathfrak{R}$,

$$(\mathfrak{a}, \mathfrak{k}) = (\mathfrak{i}, \mathfrak{b}),$$

since these consist of the elements of $\mathfrak{R}$ which can be written in the form $\alpha+\beta+\gamma$, where

$$\alpha = 0 \ (\mathfrak{i}), \quad \beta = 0 \ (\mathfrak{j}), \quad \gamma = 0 \ (\mathfrak{k}).$$

Without ambiguity we can write $(\mathfrak{a}, \mathfrak{k}) = (\mathfrak{i}, \mathfrak{b}) = (\mathfrak{i}, \mathfrak{j}, \mathfrak{k})$. By extension, we can define the join of any finite number of ideals.

(v) If $\mathfrak{i}$ and $\mathfrak{j}$ both possess finite bases:

$$\mathfrak{i} = \mathfrak{R}.(\omega_1, \ldots, \omega_r),$$

$$\mathfrak{j} = \mathfrak{R}.(\nu_1, \ldots, \nu_s),$$

then $$(\mathfrak{i}, \mathfrak{j}) = \mathfrak{R}.(\omega_1, \ldots, \omega_r, \nu_1, \ldots, \nu_s).$$

II. If $\mathfrak{i}$, $\mathfrak{j}$ are ideals in $\mathfrak{R}$, the set of elements α of $\mathfrak{R}$ such that

$$\alpha = 0 \ (\mathfrak{i}) \quad \text{and} \quad \alpha = 0 \ (\mathfrak{j})$$

clearly form an ideal. We denote this by $[\mathfrak{i}, \mathfrak{j}]$, and call it the *intersection* of $\mathfrak{i}$ and $\mathfrak{j}$. The following properties of the intersection are immediate:

(i) $$[\mathfrak{i}, \mathfrak{j}] \subseteq \mathfrak{i}, \quad [\mathfrak{i}, \mathfrak{j}] \subseteq \mathfrak{j};$$

(ii) $$[\mathfrak{i}, \mathfrak{j}] = [\mathfrak{j}, \mathfrak{i}];$$

(iii) $$[\mathfrak{i}, \mathfrak{i}] = \mathfrak{i};$$

(iv) $$[\mathfrak{i}, [\mathfrak{j}, \mathfrak{k}]] = [[\mathfrak{i}, \mathfrak{j}], \mathfrak{k}],$$

where $\mathfrak{k}$ is any other ideal in $\mathfrak{R}$. We can, without ambiguity, write $[\mathfrak{i}, [\mathfrak{j}, \mathfrak{k}]] = [\mathfrak{i}, \mathfrak{j}, \mathfrak{k}]$. We can, similarly, define the intersection of any number of ideals in $\mathfrak{R}$.

III. If $\mathfrak{i}$ and $\mathfrak{j}$ are ideals in $\mathfrak{R}$, the set of elements of $\mathfrak{R}$ of the form $\alpha\beta$, where

$$\alpha = 0 \ (\mathfrak{i}) \quad \text{and} \quad \beta = 0 \ (\mathfrak{j}),$$

do not form an ideal in $\mathfrak{R}$. But the elements of $\mathfrak{R}$ which can be written as finite sums $\sum_1^s \alpha_k \beta_k$, where

$$\alpha_k = 0 \ (\mathfrak{i}) \quad \text{and} \quad \beta_k = 0 \ (\mathfrak{j}),$$

for $k = 1, \ldots, s$, do form an ideal, as can be verified at once. We call this the *product* of $\mathfrak{i}$ and $\mathfrak{j}$, and denote it by $\mathfrak{ij}$. It can be verified at once that the multiplication of ideals in a commutative ring is commutative and associative:

$$\mathfrak{ij} = \mathfrak{ji}, \quad \mathfrak{i}(\mathfrak{jk}) = (\mathfrak{ij})\mathfrak{k} = \mathfrak{ijk}.$$

Moreover, we have

$$\mathfrak{ij} = 0 \ (\mathfrak{i}),$$

$$\mathfrak{ij} = 0 \ (\mathfrak{j}),$$

hence

$$\mathfrak{ij} \subseteq [\mathfrak{i}, \mathfrak{j}].$$

If we take $\mathfrak{j} = \mathfrak{i}$, we can define the powers $\mathfrak{i}^2, \mathfrak{i}^3, \ldots, \mathfrak{i}^\rho, \ldots$ of $\mathfrak{i}$ for any integer ρ ($\rho \geqslant 1$). If $\mathfrak{R}$ has unity, and (1) is the unit ideal, any element α of $\mathfrak{i}$ can be written as $e\alpha$, and is therefore in $\mathfrak{i}(1)$. Hence $\mathfrak{i} = 0 \ (\mathfrak{i}(1))$.

But

$$\mathfrak{i}(1) = 0 \ (\mathfrak{i}).$$

Therefore

$$\mathfrak{i}(1) = \mathfrak{i}.$$

IV. If $\mathfrak{i}$ and $\mathfrak{j}$ are two ideals of $\mathfrak{R}$, let us consider the elements γ of $\mathfrak{R}$ such that

$$\gamma\alpha = 0 \ (\mathfrak{i}),$$

for every element α of $\mathfrak{j}$. If γ and γ' are two such elements, and ρ is any element of $\mathfrak{R}$, we see that

$$(\gamma-\gamma')\alpha = 0 \ (\mathfrak{i}) \quad \text{and} \quad \rho\gamma\alpha = 0 \ (\mathfrak{i})$$

for every element α of $\mathfrak{j}$. Hence the elements γ with the stated property form an ideal in $\mathfrak{R}$. We call this ideal the *quotient of* $\mathfrak{i}$ *by* $\mathfrak{j}$, and denote it by $\mathfrak{i}:\mathfrak{j}$. We have, at once,

$$\mathfrak{i} = 0 \ (\mathfrak{i}:\mathfrak{j}),$$

and

$$\mathfrak{i}:\mathfrak{i} = \mathfrak{R}.$$

We now prove certain properties of the four operations which we have defined.

THEOREM II. $\qquad \mathfrak{i}(\mathfrak{j},\mathfrak{k}) = (\mathfrak{ij},\mathfrak{ik})$.

Let $\alpha_1, \alpha_2, \ldots$ be elements of $\mathfrak{i}$, $\beta_1, \beta_2, \ldots$ elements of $\mathfrak{j}$, and $\gamma_1, \gamma_2, \ldots$ be elements of $\mathfrak{k}$. Any element of $\mathfrak{i}(\mathfrak{j},\mathfrak{k})$ is of the form

$$\sum_1^s \alpha_a(\beta_a+\gamma_a) = \sum_1^s \alpha_a\beta_a + \sum_1^s \alpha_a\gamma_a \in (\mathfrak{ij},\mathfrak{ik});$$

hence

$$\mathfrak{i}(\mathfrak{j},\mathfrak{k}) \subseteq (\mathfrak{ij},\mathfrak{ik}). \tag{2}$$

Conversely, any element of $(\mathfrak{ij},\mathfrak{ik})$ is of the form

$$\sum_1^s \alpha_a\beta_a + \sum_1^t \alpha_{s+b}\gamma_{s+b} = \sum_1^{s+t} \alpha_a(\beta_a+\gamma_a) \in \mathfrak{i}(\mathfrak{j},\mathfrak{k}),$$

where $\beta_{s+1} = \ldots = \beta_{s+t} = \gamma_1 = \ldots = \gamma_s = 0$. Hence

$$(\mathfrak{ij},\mathfrak{ik}) \subseteq \mathfrak{i}(\mathfrak{j},\mathfrak{k}). \tag{3}$$

The result follows from (2) and (3).

THEOREM III.

$$[\mathfrak{i}_1,\mathfrak{i}_2,\ldots,\mathfrak{i}_r]:\mathfrak{j} = [\mathfrak{i}_1:\mathfrak{j},\mathfrak{i}_2:\mathfrak{j},\ldots,\mathfrak{i}_r:\mathfrak{j}].$$

If $\qquad \gamma\mathfrak{j} = 0 \ ([\mathfrak{i}_1,\mathfrak{i}_2,\ldots,\mathfrak{i}_r])$,

then $\qquad \gamma\mathfrak{j} = 0 \ (\mathfrak{i}_a) \quad (a = 1,\ldots,r)$.

Hence $\qquad \gamma = 0 \ (\mathfrak{i}_a:\mathfrak{j}) \quad (a = 1,\ldots,r)$,

and therefore $\qquad \gamma = 0 \ ([\mathfrak{i}_1:\mathfrak{j},\mathfrak{i}_2:\mathfrak{j},\ldots,\mathfrak{i}_r:\mathfrak{j}])$.

Therefore $$[\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_r] : \mathfrak{j} \subseteq [\mathfrak{i}_1 : \mathfrak{j}, \mathfrak{i}_2 : \mathfrak{j}, \ldots, \mathfrak{i}_r : \mathfrak{j}]. \tag{4}$$

Conversely, if $$\gamma \in [\mathfrak{i}_1 : \mathfrak{j}, \mathfrak{i}_2 : \mathfrak{j}, \ldots, \mathfrak{i}_r : \mathfrak{j}],$$

$$\gamma\mathfrak{j} = 0 \ (\mathfrak{i}_a) \quad (a = 1, \ldots, r),$$

and hence $$\gamma\mathfrak{j} = 0 \ ([\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_r]),$$

that is, $$\gamma \in [\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_r] : \mathfrak{j}.$$

Hence $$[\mathfrak{i}_1 : \mathfrak{j}, \mathfrak{i}_2 : \mathfrak{j}, \ldots, \mathfrak{i}_r : \mathfrak{j}] \subseteq [\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_r] : \mathfrak{j}, \tag{5}$$

and the theorem follows from (4) and (5).

THEOREM IV. $$[\mathfrak{i}, \mathfrak{j}]\,(\mathfrak{i}, \mathfrak{j}) = 0 \ (\mathfrak{ij}).$$

By Theorem II, $$[\mathfrak{i}, \mathfrak{j}]\,(\mathfrak{i}, \mathfrak{j}) = ([\mathfrak{i}, \mathfrak{j}]\,\mathfrak{i}, [\mathfrak{i}, \mathfrak{j}]\,\mathfrak{j}).$$

Since $$[\mathfrak{i}, \mathfrak{j}] = 0 \ (\mathfrak{i}) \quad \text{and} \quad [\mathfrak{i}, \mathfrak{j}] = 0 \ (\mathfrak{j}),$$

$$[\mathfrak{i}, \mathfrak{j}]\,\mathfrak{i} = 0 \ (\mathfrak{ij}), \quad [\mathfrak{i}, \mathfrak{j}]\,\mathfrak{j} = 0 \ (\mathfrak{ij}),$$

and the result follows.

Corollary I. If $(\mathfrak{i}, \mathfrak{j}) = \mathfrak{R}$, *and* $\mathfrak{R}$ *has unity, then* $[\mathfrak{i}, \mathfrak{j}] = \mathfrak{ij}$. For

$$[\mathfrak{i}, \mathfrak{j}]\,(\mathfrak{i}, \mathfrak{j}) = [\mathfrak{i}, \mathfrak{j}]\,\mathfrak{R} = [\mathfrak{i}, \mathfrak{j}].$$

Hence $$[\mathfrak{i}, \mathfrak{j}] \subseteq \mathfrak{ij} \subseteq [\mathfrak{i}, \mathfrak{j}].$$

A *maximal* ideal in $\mathfrak{R}$ is defined as an ideal $\mathfrak{i} \neq \mathfrak{R}$ such that if $\mathfrak{j}$ is any ideal with the properties

$$\mathfrak{i} = 0 \ (\mathfrak{j}), \quad \mathfrak{j} \neq 0 \ (\mathfrak{i}),$$

then $\mathfrak{j} = \mathfrak{R}$. From Theorem IV we deduce

Corollary II. If R has unity and $\mathfrak{i}$ *is a maximal ideal in* $\mathfrak{R}$, *and* $\mathfrak{j} \neq 0$ $(\mathfrak{i})$, *then* $[\mathfrak{i}, \mathfrak{j}] = \mathfrak{ij}$. Since $\mathfrak{j} \neq 0$ $(\mathfrak{i})$, $(\mathfrak{i}, \mathfrak{j})$ contains $\mathfrak{i}$, and at least one element not in $\mathfrak{i}$. Since $\mathfrak{i}$ is maximal, we must have

$$(\mathfrak{i}, \mathfrak{j}) = \mathfrak{R},$$

the unit ideal, and the result follows from Corollary I.

THEOREM V. $$\mathfrak{i} : (\mathfrak{j}_1, \ldots, \mathfrak{j}_r) = [\mathfrak{i} : \mathfrak{j}_1, \ldots, \mathfrak{i} : \mathfrak{j}_r].$$

If $\gamma \in \mathfrak{i} : (\mathfrak{j}_1, \ldots, \mathfrak{j}_r)$,

$$\gamma\mathfrak{j}_a = 0 \ (\mathfrak{i}) \quad (a = 1, \ldots, r).$$

Hence $$\gamma \in [\mathfrak{i} : \mathfrak{j}_1, \ldots, \mathfrak{i} : \mathfrak{j}_r]. \tag{6}$$

On the other hand, if $\gamma \in [\mathfrak{i} : \mathfrak{j}_1, \ldots, \mathfrak{i} : \mathfrak{j}_r]$,

$$\gamma \mathfrak{j}_a = 0 \ (\mathfrak{i}) \quad (a = 1, \ldots, r),$$

and hence

$$\gamma \in \mathfrak{i} : (\mathfrak{j}_1, \ldots, \mathfrak{j}_r). \tag{7}$$

The result follows from (6) and (7).

We conclude this section with a discussion of some consequences of the assumption that the Basis Theorem holds in $\mathfrak{R}$. We take $\mathfrak{R}$ to be any commutative ring for which the Basis Theorem holds. Suppose that $\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3, \ldots$ is a sequence of ideals in $\mathfrak{R}$ such that

$$\mathfrak{i}_1 = 0 \ (\mathfrak{i}_2), \quad \mathfrak{i}_2 = 0 \ (\mathfrak{i}_3), \ldots, \quad \mathfrak{i}_r = 0 \ (\mathfrak{i}_{r+1}), \ldots.$$

Let us consider the set $\mathfrak{i}$ of elements of $\mathfrak{R}$ which can be written as finite sums $\sum_{j=1}^{k} \alpha_j$, where each α_j belongs to some ideal $\mathfrak{i}_j$ of the sequence. It is clear that $\mathfrak{i}$ satisfies the two properties which define an ideal. Since the Basis Theorem holds in $\mathfrak{R}$, there exists in $\mathfrak{i}$ a finite set of elements $\omega_1, \ldots, \omega_r$ forming a basis for $\mathfrak{i}$. Since ω_a is in $\mathfrak{i}$,

$$\omega_a = \sum_{j=1}^{s_a} \alpha_{aj},$$

where $\alpha_{aj} \in \mathfrak{i}_j$. Let $t = \max [s_1, \ldots, s_r]$. Since

$$\alpha_{aj} = 0 \ [\mathfrak{i}_j], \quad \mathfrak{i}_j = 0 \ (\mathfrak{i}_t),$$

for all relevant values of j, $\alpha_{aj} \in \mathfrak{i}_t$, and hence

$$\omega_a = 0 \ (\mathfrak{i}_t) \quad (a = 1, \ldots, r),$$

and therefore

$$\mathfrak{i} = 0 \ (\mathfrak{i}_t). \tag{8}$$

Let k be any integer greater than t. If $\alpha \in \mathfrak{i}_k$, then $\alpha \in \mathfrak{i}$, from the definition of $\mathfrak{i}$, and hence

$$\mathfrak{i}_k = 0 \ (\mathfrak{i}).$$

Therefore, by (8),

$$\mathfrak{i}_k = 0 \ (\mathfrak{i}_t).$$

But since $k > t$,

$$\mathfrak{i}_t = 0 \ (\mathfrak{i}_k),$$

and therefore

$$\mathfrak{i}_k = \mathfrak{i}_t.$$

Thus for the sequence $\mathfrak{i}_1, \mathfrak{i}_2, \ldots$ there exists a finite integer t such that

$$\mathfrak{i}_t = \mathfrak{i}_{t+1} = \mathfrak{i}_{t+2} = \ldots.$$

Conversely, suppose that the ring $\mathfrak{R}$ has the property that if $\mathfrak{i}_1, \mathfrak{i}_2, \ldots$ is any sequence of ideals in $\mathfrak{R}$ such that

$$\mathfrak{i}_1 = 0 \ (\mathfrak{i}_2), \quad \mathfrak{i}_2 = 0 \ (\mathfrak{i}_3), \ldots,$$

then there necessarily exists a finite integer t such that

$$\mathfrak{i}_t = \mathfrak{i}_{t+1} = \mathfrak{i}_{t+2} = \ldots.$$

We show that this implies that the Basis Theorem holds in $\mathfrak{R}$. Let $\mathfrak{j}$ be any ideal in $\mathfrak{R}$, and let ω_1 be any element of $\mathfrak{j}$. Then, clearly,

$$\mathfrak{i}_1 = \mathfrak{R}.(\omega_1) = 0 \ (\mathfrak{j}).$$

If $\mathfrak{i}_1$ is not equal to $\mathfrak{j}$, $\mathfrak{j}$ contains an element ω_2 not in $\mathfrak{i}_1$, and we have

$$\mathfrak{i}_2 = \mathfrak{R}.(\omega_1, \omega_2) = 0 \ (\mathfrak{j}),$$
$$\mathfrak{i}_1 = 0 \ (\mathfrak{i}_2).$$

If $\mathfrak{i}_2$ is not equal to $\mathfrak{j}$, we select an element ω_3 in $\mathfrak{j}$ but not in $\mathfrak{i}_2$, and proceed as before. We apply the hypothesis on $\mathfrak{R}$ to the sequence $\mathfrak{i}_1, \mathfrak{i}_2, \ldots$. Then there exists an integer t such that

$$\mathfrak{i}_t = \mathfrak{i}_{t+1} = \ldots$$

(unless the sequence ends at $\mathfrak{i}_t$). From the equation $\mathfrak{i}_t = \mathfrak{i}_{t+1}$, it follows that $\omega_{t+1} \in \mathfrak{i}_t$, which conflicts with the method of constructing ω_{t+1}. Hence the sequence ends at $\mathfrak{i}_t$. But the sequence can only end there if $\mathfrak{i}_t = \mathfrak{j}$. It follows that $\mathfrak{j} = \mathfrak{i}_t = \mathfrak{R}.(\omega_1, \ldots, \omega_t)$. Hence $\mathfrak{j}$ has a finite basis.

If $\mathfrak{i}$ and $\mathfrak{j}$ are two ideals of $\mathfrak{R}$ such that

$$\mathfrak{i} = 0 \ (\mathfrak{j}),$$

$\mathfrak{i}$ is said to be a *multiple* of $\mathfrak{j}$, and $\mathfrak{j}$ is said to be a *factor* of $\mathfrak{i}$. If

$$\mathfrak{j} \neq 0 \ (\mathfrak{i}),$$

$\mathfrak{i}$ is a *proper* multiple of $\mathfrak{j}$, and $\mathfrak{j}$ is a *proper* factor of $\mathfrak{i}$. In this terminology the result just proved is equivalent to

THEOREM VI. *A necessary and sufficient condition that the Basis Theorem hold in $\mathfrak{R}$ is that any sequence of ideals in $\mathfrak{R}$ with the property that each ideal of the sequence is a proper multiple of its successor is a finite sequence.*

Sometimes it is convenient to take as the fundamental property of $\mathfrak{R}$ the property that any sequence of ideals such that each is

a proper multiple of its successor is finite. We then say that the 'ascending chain-condition' holds in $\mathfrak{R}$.

Two corollaries of Theorem VI may be noted.

Corollary I. If the Basis Theorem holds in $\mathfrak{R}$, *any non-vacuous set of ideals contains at least one ideal which is not a proper multiple of any ideal of the set.*

The proof is obvious.

Corollary II. (*Principle of Induction for Ideals.*) *If the Basis Theorem holds in* $\mathfrak{R}$, *and* E *is any property which* (i) *holds for the unit ideal*, (ii) *holds for an ideal* $\mathfrak{i}$ *when it holds for all proper factors of* $\mathfrak{i}$, *then* E *holds for all ideals in* $\mathfrak{R}$.

Suppose that the corollary is false, and consider the set S of ideals for which E does not hold. By Corollary I, there exists in the set an ideal $\mathfrak{i}$ which is not a proper multiple of any ideal of the set. $\mathfrak{i}$ is not the unit ideal since, by hypothesis, E holds for the unit ideal. $\mathfrak{i}$ has proper factors (for instance, the unit ideal, which satisfies our definition of a proper factor), and since none of these proper factors can belong to S, $\mathfrak{i}$ being maximal in S, it follows from condition (ii) that E holds for $\mathfrak{i}$. But $\mathfrak{i}$ is in S, and hence E does not hold for it. We thus have a contradiction. It follows that S must be vacuous, and our assumption that the corollary is not true is invalid.

2. Prime ideals and primary ideals. An ideal $\mathfrak{p}$ in the com mutative ring $\mathfrak{R}$ is said to be a *prime ideal* if the equation

$$\alpha\beta = 0 \ (\mathfrak{p})$$

implies either $\alpha = 0 \ (\mathfrak{p})$

or $\beta = 0 \ (\mathfrak{p})$.

It is clear that the unit ideal is always prime, and that the zero ideal is prime if and only if $\mathfrak{R}$ contains no divisors of zero. Again, if $\mathfrak{p}$ is prime, and $\mathfrak{i}$ and $\mathfrak{j}$ are two ideals of $\mathfrak{R}$ such that

$$\mathfrak{ij} = 0 \ (\mathfrak{p}),$$

then either $\mathfrak{i} = 0 \ (\mathfrak{p})$

or $\mathfrak{j} = 0 \ (\mathfrak{p})$.

Indeed, suppose that $\mathfrak{i} \neq 0 \ (\mathfrak{p})$.

Then there exists an element α in $\mathfrak{i}$ which is not in $\mathfrak{p}$. If β is any element of $\mathfrak{j}$, $\alpha\beta \in \mathfrak{ij}$, and hence

$$\alpha\beta = 0 \ (\mathfrak{p}).$$

Since α is not in $\mathfrak{p}$, and $\mathfrak{p}$ is prime, it follows that β is in $\mathfrak{p}$. Hence

$$\mathfrak{j} = 0 \ (\mathfrak{p}).$$

An ideal $\mathfrak{q}$ in $\mathfrak{R}$ is said to be *primary* if the equation

$$\alpha\beta = 0 \ (\mathfrak{q}),$$

together with the inequality

$$\alpha \not\equiv 0 \ (\mathfrak{q}),$$

implies

$$\beta^\rho = 0 \ (\mathfrak{q}),$$

for a suitable integer ρ. A prime ideal is, of course, primary.

If $\mathfrak{R}$ is the principal ideal ring formed by the natural integers, the ideal $\mathfrak{R}.(d)$ is prime if and only if d is a prime number, and is primary if and only if d is a power of a prime number. For our purposes, however, a more suggestive example is provided by the ring $\mathfrak{R} = K[x, y]$ of polynomials in two independent indeterminates over the ground field K. Let $\mathfrak{p} = \mathfrak{R}.(x, y)$. The elements of $\mathfrak{p}$ are just those polynomials whose constant term is zero. If α and β are two polynomials whose product has constant term zero, then either α or β must have constant term zero and hence belongs to $\mathfrak{p}$. Thus $\mathfrak{p}$ is prime. Next, let $\mathfrak{q} = \mathfrak{R}.(x, y^2)$. Any element of $\mathfrak{q}$ is of the form

$$ax + (cx^2 + 2dxy + ey^2) + (lx^3 + 3mx^2y + 3nxy^2 + py^3) + \ldots.$$

Let

$$\alpha = a_1 + (b_1x + c_1y) + \ldots$$

and

$$\beta = a_2 + (b_2x + c_2y) + \ldots.$$

If $\alpha\beta \in \mathfrak{q}$, we must have

$$a_1a_2 = 0, \quad a_1c_2 + a_2c_1 = 0.$$

If α does not belong to $\mathfrak{q}$, a_1 and c_1 cannot both be zero. It follows at once that we must have $a_2 = 0$. But if a_2 is zero,

$$\beta^2 = (b_2^2x^2 + 2b_2c_2xy + c_2^2y^2) + \ldots$$

has the form of an element of $\mathfrak{q}$. Hence $\mathfrak{q}$ is primary. If $c_2 \not\equiv 0$, β does not belong to $\mathfrak{q}$, hence $\mathfrak{q}$ is not a prime ideal.

Now let $\mathfrak{q}$ be any primary ideal in a commutative ring $\mathfrak{R}$, and consider the set of elements $\alpha, \beta, \ldots$ of $\mathfrak{R}$ which have the property that some power of them belongs to $\mathfrak{q}$. If

$$\alpha^\rho = 0 \ (\mathfrak{q}) \quad \text{and} \quad \beta^\sigma = 0 \ (\mathfrak{q}),$$

then $(\alpha-\beta)^{\rho+\sigma-1}$ is equal to a sum of terms each of which is either the product of α^ρ by an element of $\mathfrak{R}$ or the product of β^σ by an element of $\mathfrak{R}$, and is therefore in $\mathfrak{q}$. Hence $(\alpha-\beta)^{\rho+\sigma-1} \in \mathfrak{q}$, and so $\alpha-\beta$ is in the set. Similarly, if ξ is any element of $\mathfrak{R}$,

$$(\xi\alpha)^\rho = \xi^\rho \alpha^\rho = 0 \ (\mathfrak{q}).$$

Hence $\xi\alpha$ is in the set, which is therefore an ideal, which we denote by $\mathfrak{p}$. We now show that $\mathfrak{p}$ is a prime ideal. Suppose that α and β are such that

$$\alpha\beta = 0 \ (\mathfrak{p}), \quad \alpha \not\equiv 0 \ (\mathfrak{p}).$$

Since $\alpha\beta \in \mathfrak{p}$, there exists an integer ρ such that

$$\alpha^\rho \beta^\rho = 0 \ (\mathfrak{q}).$$

Since α is not in $\mathfrak{p}$, α^ρ is not in $\mathfrak{q}$, and, since $\mathfrak{q}$ is primary, there exists an integer τ such that $\beta^{\rho\tau} \in \mathfrak{q}$. Hence β is in $\mathfrak{p}$. This proves that $\mathfrak{p}$ is prime. $\mathfrak{p}$ is called the prime ideal *belonging to* $\mathfrak{q}$, or the *radical* of $\mathfrak{q}$. It is clear that

$$\mathfrak{q} = 0 \ (\mathfrak{p}),$$

and that $\mathfrak{q} = \mathfrak{p}$ if and only if $\mathfrak{q}$ is prime.

From the definition of a primary ideal and its radical, we see that if

$$\alpha\beta = 0 \ (\mathfrak{q}) \quad \text{and} \quad \alpha \not\equiv 0 \ (\mathfrak{q}),$$

then

$$\beta = 0 \ (\mathfrak{p}).$$

Hence $\mathfrak{q}$ and its radical $\mathfrak{p}$ are related by the following properties:

(i) if $\alpha\beta = 0 \ (\mathfrak{q})$ and $\alpha \not\equiv 0 \ (\mathfrak{q})$, then $\beta = 0 \ (\mathfrak{p})$;

(ii) $\mathfrak{q} = 0 \ (\mathfrak{p})$,

(iii) $\beta = 0 \ (\mathfrak{p})$ implies $\beta^\rho = 0 \ (\mathfrak{q})$,

for a suitable integer ρ.

We may note that if $\mathfrak{R}$ has unity and $\mathfrak{q}$ is not the unit ideal, then (i) implies (ii). (If $\mathfrak{q}$ is the unit ideal, (i) does not define $\mathfrak{p}$.) If β is any element of $\mathfrak{q}$, we have

$$1.\beta = 0 \ (\mathfrak{q}),$$

and since $\mathfrak{q}$ is not the unit ideal it does not contain 1. Hence, by (i),

$$\beta = 0 \ (\mathfrak{p}).$$

Therefore

$$\mathfrak{q} = 0 \ (\mathfrak{p}).$$

We now show that if $\mathfrak{q}$ and $\mathfrak{p}$ are two ideals in $\mathfrak{R}$ satisfying the properties (i), (ii), (iii), then $\mathfrak{q}$ is primary, and $\mathfrak{p}$ is its radical. More briefly, we shall say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary*. From (i) and (iii) it follows that $\mathfrak{q}$ is primary. To show that $\mathfrak{p}$ is its radical, let β be any element of $\mathfrak{R}$ such that $\beta^\rho \in \mathfrak{q}$ for some integer ρ. If $\beta \in \mathfrak{q}$, then $\beta \in \mathfrak{p}$, by (ii). If β does not belong to $\mathfrak{q}$, let ρ ($\rho > 1$) be the smallest integer such that $\beta^\rho \in \mathfrak{q}$. Then

$$\beta . \beta^{\rho-1} = 0 \ (\mathfrak{q}),$$

and

$$\beta^{\rho-1} \neq 0 \ (\mathfrak{q}),$$

hence, by (i),

$$\beta = 0 \ (\mathfrak{p}).$$

This, taken with condition (iii), gives

THEOREM I. *A primary ideal* $\mathfrak{q}$ *and its radical* $\mathfrak{p}$ *are characterised by the properties* (i), (ii), (iii).

THEOREM II. *If* $\mathfrak{q}$ *is* $\mathfrak{p}$-*primary, and* $\mathfrak{i}$ *and* $\mathfrak{j}$ *are ideals of* $\mathfrak{R}$ *such that*

$$\mathfrak{ij} = 0 \ (\mathfrak{q}), \quad \mathfrak{i} \neq 0 \ (\mathfrak{q}),$$

then

$$\mathfrak{j} = 0 \ (\mathfrak{p}).$$

Since $\mathfrak{i}$ is not contained in $\mathfrak{q}$, there is an element α of $\mathfrak{i}$ not contained in $\mathfrak{q}$. If β is any element of $\mathfrak{j}$, $\alpha\beta \in \mathfrak{q}$, and α is not in $\mathfrak{q}$. Hence, by property (i) above, $\beta \in \mathfrak{p}$, that is

$$\mathfrak{j} = 0 \ (\mathfrak{p}).$$

Corollary I. If

$$\mathfrak{ij} = 0 \ (\mathfrak{q}) \quad \textit{and} \quad \mathfrak{j} \neq 0 \ (\mathfrak{p}), \quad \textit{then} \quad \mathfrak{i} = 0 \ (\mathfrak{q}).$$

Corollary II. If

$$\mathfrak{j} \neq 0 \ (\mathfrak{p}), \quad \textit{then} \quad \mathfrak{q} : \mathfrak{j} = \mathfrak{q}.$$

THEOREM III. *If* $\mathfrak{q}$ *and* $\mathfrak{q}'$ *are* $\mathfrak{p}$-*primary, then* $[\mathfrak{q}, \mathfrak{q}']$ *is* $\mathfrak{p}$-*primary.*

(i) If

$$\alpha\beta = 0 \ ([\mathfrak{q}, \mathfrak{q}']) \quad \text{and} \quad \alpha \neq 0 \ ([\mathfrak{q}, \mathfrak{q}']),$$

we have

$$\alpha\beta = 0 \ (\mathfrak{q}) \quad \text{and} \quad \alpha\beta = 0 \ (\mathfrak{q}'),$$

and either

$$\alpha \neq 0 \ (\mathfrak{q}) \quad \text{or} \quad \alpha \neq 0 \ (\mathfrak{q}').$$

Suppose, for instance, that

$$\alpha\beta = 0 \ (\mathfrak{q}) \quad \text{and} \quad \alpha \not\equiv 0 \ (\mathfrak{q}).$$

Then since $\mathfrak{q}$ is $\mathfrak{p}$-primary,

$$\beta = 0 \ (\mathfrak{p}).$$

If $$\alpha \not\equiv 0 \ (\mathfrak{q}'),$$

a similar argument gives $\beta = 0 \ (\mathfrak{p})$.

(ii) $$\mathfrak{q} = 0 \ (\mathfrak{p}) \quad \text{and} \quad \mathfrak{q}' = 0 \ (\mathfrak{p});$$

hence $$[\mathfrak{q}, \mathfrak{q}'] = 0 \ (\mathfrak{p}).$$

(iii) If $\beta \in \mathfrak{p}$, there exist integers ρ, σ such that

$$\beta^\rho = 0 \ (\mathfrak{q}) \quad \text{and} \quad \beta^\sigma = 0 \ (\mathfrak{q}').$$

If $\tau = \max[\rho, \sigma]$, $$\beta^\tau = 0 \ ([\mathfrak{q}, \mathfrak{q}']).$$

It follows from Theorem I that $[\mathfrak{q}, \mathfrak{q}']$ is $\mathfrak{p}$-primary.

THEOREM IV. *If* $\mathfrak{q}$ *is* $\mathfrak{p}$*-primary and* $\mathfrak{q}'$ *is* $\mathfrak{p}'$*-primary, where* $\mathfrak{p} \neq \mathfrak{p}'$, *and if*

$$[\mathfrak{q}, \mathfrak{q}'] \neq \mathfrak{q} \quad \textit{and} \quad [\mathfrak{q}, \mathfrak{q}'] \neq \mathfrak{q}',$$

then $[\mathfrak{q}, \mathfrak{q}']$ *is not primary.*

Since $\mathfrak{p} \neq \mathfrak{p}'$, there exists an element α which is in one of these ideals, but not in the other. Suppose that

$$\alpha = 0 \ (\mathfrak{p}), \quad \alpha \not\equiv 0 \ (\mathfrak{p}').$$

Then no power of α belongs to $\mathfrak{q}'$, while there exists an integer ρ such that

$$\alpha^\rho = 0 \ (\mathfrak{q}).$$

Then $$\alpha^\rho \not\equiv 0 \ ([\mathfrak{q}, \mathfrak{q}']).$$

Since $[\mathfrak{q}, \mathfrak{q}'] \neq \mathfrak{q}'$, there exists an element β which is in $\mathfrak{q}'$ but not in $[\mathfrak{q}, \mathfrak{q}']$, and hence not in $\mathfrak{q}$. Then

$$\alpha^\rho \beta \in \mathfrak{q}\mathfrak{q}' \subseteq [\mathfrak{q}, \mathfrak{q}'],$$

[§ 1, p. 6]. Now $$\beta \not\equiv 0 \ ([\mathfrak{q}, \mathfrak{q}']),$$

and it would follow, if $[\mathfrak{q}, \mathfrak{q}']$ were primary, that some power of α^ρ lay in $[\mathfrak{q}, \mathfrak{q}']$, and hence that some power of α was in $\mathfrak{q}'$. Since α is not in $\mathfrak{p}'$, this contradicts the fact that $\mathfrak{q}'$ is $\mathfrak{p}'$-primary. Hence we conclude that $[\mathfrak{q}, \mathfrak{q}']$ is not primary.

The theorems so far proved in this section do not require the assumption that the Basis Theorem holds in $\mathfrak{R}$. We now go on to prove some results which depend on the assumption that any ideal in $\mathfrak{R}$ has a finite basis. *For the remainder of this section we assume that the Basis Theorem holds in* $\mathfrak{R}$.

Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal in $\mathfrak{R}$, and let $\omega_1, \ldots, \omega_r$ be a basis for $\mathfrak{p}$. Corresponding to ω_i there exists an integer σ_i such that

$$\omega_i^{\sigma_i} = 0 \ (\mathfrak{q}).$$

Let
$$\rho = \sum_{i=1}^{r} (\sigma_i - 1) + 1.$$

Any element of $\mathfrak{p}^\rho$ is of the form

$$\sum_{i=1}^{k} \alpha_i \Omega_i + \sum_{i=1}^{k} n_i \Omega_i,$$

where $\alpha_1, \ldots, \alpha_k$ are in $\mathfrak{R}$, and $n_1, \ldots, n_k$ are integers, and $\Omega_1, \ldots, \Omega_k$ are products of degree ρ in $\omega_1, \ldots, \omega_r$. If, for instance,

$$\Omega_i = \omega_1^{\rho_1} \ldots \omega_r^{\rho_r},$$

then
$$\sum_{i=1}^{r} \rho_i = \rho = \sum_{i=1}^{r} (\sigma_i - 1) + 1,$$

and hence, for some value of j, $\rho_j \geqslant \sigma_j$. Thus $\Omega_i \in \mathfrak{q}$, and hence

$$\mathfrak{p}^\rho = 0 \ (\mathfrak{q}).$$

There may, of course, be an integer σ $(\sigma < \rho)$ such that

$$\mathfrak{p}^\sigma = 0 \ (\mathfrak{q});$$

the smallest integer σ with this property is called the *index* of $\mathfrak{q}$. A primary ideal is prime if and only if its index is 1.

THEOREM V. *Let* $\mathfrak{q}$ *be a primary ideal and* $\mathfrak{p}$ *a prime ideal. If*

$$\mathfrak{q} = 0 \ (\mathfrak{p}), \quad \mathfrak{p}^\sigma = 0 \ (\mathfrak{q}),$$

for some integer σ, *then* $\mathfrak{q}$ *is* $\mathfrak{p}$*-primary.*

Let $\mathfrak{p}'$ be the radical of $\mathfrak{q}$; there exists an integer ρ such that

$$\mathfrak{p}'^\rho = 0 \ (\mathfrak{q}).$$

Hence
$$\mathfrak{p}'^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p},$$

that is,
$$\mathfrak{p}'^\rho = 0 \ (\mathfrak{p}),$$

and, since $\mathfrak{p}$ is prime, we deduce that

$$\mathfrak{p}' = 0 \ (\mathfrak{p}). \tag{1}$$

On the other hand, we have

$$\mathfrak{q} = 0 \ (\mathfrak{p}'),$$

and hence $$\mathfrak{p}^\sigma \subseteq \mathfrak{q} \subseteq \mathfrak{p}'.$$

Therefore, since $\mathfrak{p}'$ is prime,

$$\mathfrak{p} = 0 \ (\mathfrak{p}'). \tag{2}$$

From (1) and (2) we deduce that $\mathfrak{p} = \mathfrak{p}'$.

An ideal $\mathfrak{i}$ in $\mathfrak{R}$ is said to be *reducible* if it can be written in the form

$$\mathfrak{i} = [\mathfrak{j}, \mathfrak{k}],$$

where $\mathfrak{j}$ and $\mathfrak{k}$ are *proper* factors of $\mathfrak{i}$; otherwise it is *irreducible*. A prime ideal (and, in particular, the unit ideal) is irreducible. For if $\mathfrak{i}$ is prime and

$$\mathfrak{i} = [\mathfrak{j}, \mathfrak{k}],$$

we have $$\mathfrak{j}\mathfrak{k} \subseteq [\mathfrak{j}, \mathfrak{k}] = \mathfrak{i},$$

and hence $$\mathfrak{j} = 0 \ (\mathfrak{i}) \quad \text{or} \quad \mathfrak{k} = 0 \ (\mathfrak{i}),$$

and therefore $\mathfrak{j}$ and $\mathfrak{k}$ cannot both be proper factors of $\mathfrak{i}$.

It is easy to show, by means of the Principle of Induction for ideals [§ 1, Th. VI, Cor. II], that any ideal $\mathfrak{i}$ is the intersection of a finite number of irreducible ideals. If $\mathfrak{i}$ is irreducible, there is nothing to prove. Suppose that $\mathfrak{i}$ is reducible:

$$\mathfrak{i} = [\mathfrak{j}, \mathfrak{k}],$$

where $\mathfrak{j}$ and $\mathfrak{k}$ are proper factors of $\mathfrak{i}$. If

$$\mathfrak{j} = [\mathfrak{j}_1, \mathfrak{j}_2, \ldots, \mathfrak{j}_r],$$

where $\mathfrak{j}_1, \ldots, \mathfrak{j}_r$ are irreducible ideals, and if

$$\mathfrak{k} = [\mathfrak{k}_1, \mathfrak{k}_2, \ldots, \mathfrak{k}_s],$$

where $\mathfrak{k}_1, \ldots, \mathfrak{k}_s$ are irreducible ideals, then

$$\mathfrak{i} = [\mathfrak{j}_1, \ldots, \mathfrak{j}_r, \mathfrak{k}_1, \ldots, \mathfrak{k}_s]$$

is the intersection of a finite number of irreducible ideals. The property of being the intersection of a finite number of irreducible ideals is true for the unit ideal, and also for any ideal when it is

true for its proper factors. Hence it is true for all ideals in $\mathfrak{R}$. Thus we have

THEOREM VI. *Every ideal in a ring for which the Basis Theorem holds is the intersection of a finite number of irreducible ideals.*

THEOREM VII. *Every irreducible ideal is primary.*

Suppose that the ideal $\mathfrak{i}$ is not primary. We can then find two elements α and β in $\mathfrak{R}$ such that

$$\alpha\beta = 0 \ (\mathfrak{i}), \quad \alpha \neq 0 \ (\mathfrak{i}), \quad \beta^\rho \neq 0 \ (\mathfrak{i}),$$

for every positive integer ρ. The elements of $\mathfrak{R}$ of the form $\xi\beta^a$, where ξ is any element of $\mathfrak{R}$ and a is a fixed integer, clearly form an ideal, which we denote by $\mathfrak{j}_a$; if R has unity, $\mathfrak{j}_a = \mathfrak{R}.(\beta^a)$, but in general if $\mathfrak{R}$ has not unity $\mathfrak{j}_a$ is a proper multiple of $\mathfrak{R}.(\beta^a)$. We see immediately that

$$\mathfrak{i}:\mathfrak{j}_1 \subseteq \mathfrak{i}:\mathfrak{j}_2 \subseteq \mathfrak{i}:\mathfrak{j}_3 \subseteq \ldots.$$

By § 1, Th. VI, there exists an integer r such that

$$\mathfrak{i}:\mathfrak{j}_r = \mathfrak{i}:\mathfrak{j}_{r+1} = \ldots.$$

Let $\mathfrak{k} = \mathfrak{R}.(\alpha)$. The ideal $(\mathfrak{i}, \mathfrak{k})$ is a proper factor of $\mathfrak{i}$, since it contains $\mathfrak{i}$ and also α, which is not in $\mathfrak{i}$. Similarly, the ideal $(\mathfrak{i}, \mathfrak{j}_{r+1})$ is a proper factor of $\mathfrak{i}$, since it contains $\mathfrak{i}$ and $\beta^{r+2} = \beta.\beta^{r+1}$, which is not in $\mathfrak{i}$. The theorem will be proved if we can show that

$$\mathfrak{i} = [(\mathfrak{i}, \mathfrak{k}), (\mathfrak{i}, \mathfrak{j}_{r+1})].$$

Clearly, we have $\mathfrak{i} \subseteq [(\mathfrak{i}, \mathfrak{k}), (\mathfrak{i}, \mathfrak{j}_{r+1})]$. To prove that $[(\mathfrak{i}, \mathfrak{k}), (\mathfrak{i}, \mathfrak{j}_{r+1})] \subseteq \mathfrak{i}$, we consider any element η common to $(\mathfrak{i}, \mathfrak{k})$ and $(\mathfrak{i}, \mathfrak{j}_{r+1})$, and show that it lies in $\mathfrak{i}$. Since $\eta \in (\mathfrak{i}, \mathfrak{k})$,

$$\eta = \gamma + \rho\alpha + n\alpha,$$

where $\gamma \in \mathfrak{i}$, $\rho \in \mathfrak{R}$, and n is an integer. Since $\eta \in (\mathfrak{i}, \mathfrak{j}_{r+1})$,

$$\eta = \delta + \sigma\beta^{r+1},$$

where $\delta \in \mathfrak{i}$ and $\sigma \in \mathfrak{R}$. We therefore have

$$\beta\delta + \sigma\beta^{r+2} = \beta\eta = \beta\gamma + \rho\alpha\beta + n\alpha\beta = 0 \ (\mathfrak{i}),$$

since γ and $\alpha\beta$ belong to $\mathfrak{i}$. Since δ is also in $\mathfrak{i}$, we have

$$\sigma\beta^{r+2} = 0 \ (\mathfrak{i}),$$

and hence $\sigma \in \mathfrak{i} : \mathfrak{j}_{r+2}$. But $\mathfrak{i} : \mathfrak{j}_{r+2} = \mathfrak{i} : \mathfrak{j}_r$. Hence σ belongs to $\mathfrak{i} : \mathfrak{j}_r$. But $\sigma\beta^{r+1} = \sigma(\beta . \beta^r)$, and hence $\sigma\beta^{r+1}$ is contained in $\mathfrak{i}$. It follows that η is in $\mathfrak{i}$. Theorem VII is therefore proved.

Theorems VI and VII, taken together, tell us that every ideal $\mathfrak{i}$ in $\mathfrak{R}$ can be expressed as the intersection of a finite number of primary ideals. Let

$$\mathfrak{i} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r],$$

where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. If $\mathfrak{p}_i = \mathfrak{p}_j$, it follows from Theorem III that $\mathfrak{q}_{ij} = [\mathfrak{q}_i, \mathfrak{q}_j]$ is also $\mathfrak{p}_i$-primary, and in the above expression for $\mathfrak{i}$ as an intersection of primary ideals we can omit $\mathfrak{q}_i$ and $\mathfrak{q}_j$, and put $\mathfrak{q}_{ij}$ in their place. Proceeding in this way, we can combine all the primary ideals $\mathfrak{q}_i$ which have the same radical into a single primary ideal, and so obtain a representation of $\mathfrak{i}$,

$$\mathfrak{i} = [\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s],$$

as the intersection of primary ideals, where $\mathfrak{Q}_i$ is $\mathfrak{P}_i$-primary, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ are all different. $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ are called *primary components* of $\mathfrak{i}$.

Suppose that $\mathfrak{Q}_i$ is such that

$$\mathfrak{Q}_i \supseteq \mathfrak{J}_i = [\mathfrak{Q}_1, \ldots, \mathfrak{Q}_{i-1}, \mathfrak{Q}_{i+1}, \ldots, \mathfrak{Q}_s].$$

Then $\mathfrak{Q}_i$ is said to be an *irrelevant* primary component of $\mathfrak{i}$. In this case

$$\mathfrak{i} = [\mathfrak{Q}_i, \mathfrak{J}_i] = \mathfrak{J}_i,$$

and we can omit the component $\mathfrak{Q}_i$ in the representation of $\mathfrak{i}$. Proceeding, we eventually obtain a representation, say

$$\mathfrak{i} = [\mathfrak{Q}_1, \ldots, \mathfrak{Q}_k],$$

of $\mathfrak{i}$ as the intersection of primary ideals, the radicals of which are all different, and none of which is irrelevant. If we combine two of the components in this representation into one, we get a component which is not primary [Th. IV], and if we omit one of the components we clearly alter the intersection. For this reason the representations $[\mathfrak{Q}_1, \ldots, \mathfrak{Q}_k]$ of $\mathfrak{i}$ is said to be *uncontractible*. For practical purposes it is the uncontractible representations of the ideal, rather than its representations as the intersection of irreducible ideals, which are important.

Examples can be given to show that an ideal $\mathfrak{i}$ may have two distinct uncontractible representations. But there are certain uniqueness theorems which are important, and these we now prove.

THEOREM VIII. *Let* $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ *and* $[\mathfrak{q}'_1, \ldots, \mathfrak{q}'_l]$ *be two uncontractible representations of an ideal* $\mathfrak{i}$ *of* $\mathfrak{R}$, *where* $\mathfrak{q}_j$ *is* $\mathfrak{p}_j$*-primary and* $\mathfrak{q}'_j$ *is* $\mathfrak{p}'_j$*-primary. Then* $k = l$, *and, if the components* $\mathfrak{q}'_j$ *are suitably arranged,* $\mathfrak{p}'_j = \mathfrak{p}_j$ $(j = 1, \ldots, k)$.

By a characteristic property of an uncontractible representation, $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are all distinct, and $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_l$ are all distinct. Amongst these $k+l$ prime ideals we can find at least one which is not a proper multiple of any other, and without loss of generality we may assume that $\mathfrak{p}_1$ has this property; $\mathfrak{p}_1$ is not equal to any $\mathfrak{p}_j$ $(j > 1)$, and is at most equal to one $\mathfrak{p}'_j$.

Suppose that $\mathfrak{p}_1$ is not equal to any $\mathfrak{p}'_j$. For any given value of j $(j > 1)$ there exists an element α which is in $\mathfrak{p}_1$ but not in $\mathfrak{p}_j$, since

$$\mathfrak{p}_1 \neq 0 \ (\mathfrak{p}_j).$$

Let ρ be an integer such that $\alpha^\rho \in \mathfrak{q}_1$. If α is not in $\mathfrak{p}_j$, α^ρ is not in $\mathfrak{p}_j$, and hence

$$\mathfrak{q}_1 \neq 0 \ (\mathfrak{p}_j).$$

This holds for $j = 2, \ldots, k$. Again, since

$$\mathfrak{p}_1 \neq 0 \ (\mathfrak{p}'_j),$$

a similar argument shows that

$$\mathfrak{q}_1 \neq 0 \ (\mathfrak{p}'_j),$$

for $j = 1, \ldots, l$. Now [§ 1, Th. III]

$$[\mathfrak{q}_1 : \mathfrak{q}_1, \mathfrak{q}_2 : \mathfrak{q}_1, \ldots, \mathfrak{q}_k : \mathfrak{q}_1] = \mathfrak{i} : \mathfrak{q}_1 = [\mathfrak{q}'_1 : \mathfrak{q}_1, \mathfrak{q}'_2 : \mathfrak{q}_1, \ldots, \mathfrak{q}'_l : \mathfrak{q}_1].$$

Clearly

$$\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{R},$$

and from Theorem II, Corollary II,

$$\mathfrak{q}_j : \mathfrak{q}_1 = \mathfrak{q}_j \quad (j > 1),$$

and

$$\mathfrak{q}'_j : \mathfrak{q}_1 = \mathfrak{q}'_j \quad (j \geqslant 1).$$

Hence

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_k] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_l] = \mathfrak{i},$$

contradicting the assumption that $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ is an uncontractible representation of $\mathfrak{i}$. It follows that $\mathfrak{p}_1$ must be equal to one $\mathfrak{p}'_j$, and by arranging the components $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_l$ suitably we may suppose that $\mathfrak{p}_1 = \mathfrak{p}'_1$.

By Theorem III, $\mathfrak{k} = [\mathfrak{q}_1, \mathfrak{q}'_1]$ is $\mathfrak{p}_1$-primary. Just as above, we can prove that

$$\mathfrak{q}_j : \mathfrak{k} = \mathfrak{q}_j \quad \text{and} \quad \mathfrak{q}'_j : \mathfrak{k} = \mathfrak{q}'_j,$$

provided that $j > 1$ in both cases; and since $\mathfrak{k} \subseteq \mathfrak{q}_1$, $\mathfrak{k} \subseteq \mathfrak{q}_1'$,

$$\mathfrak{q}_1 : \mathfrak{k} = \mathfrak{R} = \mathfrak{q}_1' : \mathfrak{k}.$$

Hence, from the equation

$$[\mathfrak{q}_1, \ldots, \mathfrak{q}_k] : \mathfrak{k} = [\mathfrak{q}_1', \ldots, \mathfrak{q}_l'] : \mathfrak{k},$$

we obtain the equation

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_k] = [\mathfrak{q}_2', \ldots, \mathfrak{q}_l'].$$

We show that $[\mathfrak{q}_2, \ldots, \mathfrak{q}_k]$ is an uncontractible representation of this ideal. Indeed, if

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots, \mathfrak{q}_k] = 0 \ (\mathfrak{q}_i),$$

then

$$[\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots, \mathfrak{q}_k] = 0 \ (\mathfrak{q}_i),$$

contradicting the hypothesis that $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ is an uncontractible representation of $\mathfrak{i}$.

Theorem VIII now follows by a simple argument, using induction on the minimum number of components required to represent an ideal $\mathfrak{i}$ as an uncontractible intersection of primaries. Let k be this number. If $k = 1$, $\mathfrak{i}$ is primary, and $\mathfrak{q}_1 = \mathfrak{i}$. If $[\mathfrak{q}_1', \ldots, \mathfrak{q}_l']$ is another uncontractible representation of $\mathfrak{i}$, the proof given above shows that

$$[\mathfrak{q}_2', \ldots, \mathfrak{q}_l'] = \mathfrak{R},$$

and hence that

$$\mathfrak{q}_i' = \mathfrak{R} \quad (i = 2, \ldots, l).$$

Hence $[\mathfrak{q}_1', \ldots, \mathfrak{q}_l']$ is only uncontractible if $l = 1$, and then $\mathfrak{q}_1' = \mathfrak{q}_1$ and therefore $\mathfrak{p}_1' = \mathfrak{p}_1$. If we now assume the truth of the theorem for ideals which can be represented as an uncontractible intersection of $k-1$ primaries, and consider an ideal $\mathfrak{i}$ which requires k components:

$$\mathfrak{i} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_k] = [\mathfrak{q}_1', \ldots, \mathfrak{q}_l'],$$

the reasoning above shows that:

(i) for a suitable arrangement of the components,

$$\mathfrak{p}_1 = \mathfrak{p}_1';$$

(ii)
$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_k] = [\mathfrak{q}_2', \ldots, \mathfrak{q}_l'];$$

and the hypothesis of induction tells us that $k-1 = l-1$, that is, $k = l$, and the components can be arranged so that

$$\mathfrak{p}_i = \mathfrak{p}_i' \quad (i = 2, \ldots, k).$$

The proof is complete.

To prove our second uniqueness theorem we must first define the isolated and embedded components of an ideal $\mathfrak{i}$. Let $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ be an uncontractible representation of $\mathfrak{i}$, and let $\mathfrak{p}_j$ be the prime ideal belonging to $\mathfrak{q}_j$. By Theorem VIII, $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are prime ideals associated with $\mathfrak{i}$ in a unique way, independent of the uncontractible representation chosen. If $\mathfrak{p}_j$ is not a proper factor of any other prime ideal $\mathfrak{p}_i$ of the set, $\mathfrak{q}_j$ is called an *isolated component* of $\mathfrak{i}$, and if $\mathfrak{p}_j$ is a proper factor of some $\mathfrak{p}_i$, $\mathfrak{q}_j$ is said to be *embedded*. While the embedded components of $\mathfrak{i}$ need not be uniquely determined we can prove

THEOREM IX. *The isolated components of an ideal* $\mathfrak{i}$ *are uniquely determined.*

Let $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ and $[\mathfrak{q}'_1, \ldots, \mathfrak{q}'_k]$ be two uncontractible representations of $\mathfrak{i}$, and suppose that the components are arranged so that $\mathfrak{q}_j$ and $\mathfrak{q}'_j$ are both $\mathfrak{p}_j$-primary. Let $\mathfrak{q}_1$ be an isolated component of $\mathfrak{i}$. Then $\mathfrak{p}_1$ is not a proper factor of any $\mathfrak{p}_j$ $(j > 1)$. Hence $\mathfrak{q}'_1$ is also an isolated component. For convenience, we write

$$\mathfrak{j} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_k], \quad \mathfrak{j}' = [\mathfrak{q}'_2, \ldots, \mathfrak{q}'_k],$$

so that

$$[\mathfrak{q}_1, \mathfrak{j}] = \mathfrak{i} = [\mathfrak{q}'_1, \mathfrak{j}'].$$

Let $\mathfrak{q}_j$ be of index ρ_j. Then

$$\mathfrak{p}_2^{\rho_2} \ldots \mathfrak{p}_k^{\rho_k} = 0 \ (\mathfrak{j}).$$

If $\mathfrak{j} \subseteq \mathfrak{p}_1$, we have

$$\mathfrak{p}_2^{\rho_2} \ldots \mathfrak{p}_k^{\rho_k} = 0 \ (\mathfrak{p}_1),$$

and hence

$$\mathfrak{p}_i = 0 \ (\mathfrak{p}_1)$$

for some value of i greater than 1, contrary to the hypothesis that $\mathfrak{q}_1$ is isolated. Hence

$$\mathfrak{j} \neq 0 \ (\mathfrak{p}_1).$$

Therefore [Th. II, Cor. II],

$$\mathfrak{q}_1 = [\mathfrak{q}_1, \mathfrak{j}] : \mathfrak{j} = \mathfrak{i} : \mathfrak{j} = [\mathfrak{q}'_1, \mathfrak{j}'] : \mathfrak{j},$$

and hence

$$\mathfrak{q}_1 = 0 \ (\mathfrak{q}'_1).$$

Similarly, we show that

$$\mathfrak{j}' \neq 0 \ (\mathfrak{p}_1),$$

and deduce that

$$\mathfrak{q}'_1 = 0 \ (\mathfrak{q}_1).$$

Hence $\mathfrak{q}_1 = \mathfrak{q}'_1$, and the theorem follows.