DEFINITIONS OF INTEGRAL ELEMENTS AND QUOTIENT RINGS OVER NON-COMMUTATIVE RINGS WITH IDENTITY

T. W. ATTERTON

(Received 20 October 1969)

Communicated by G. E. Wall

Let B be an associative ring with identity, A a subring of B containing the identity of B. If B is commutative then it is customary to define an element b of B to be integral over A if it satisfies an equation of the form

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \tag{1}$$

for some $a_1, a_2, \cdots, a_n \in A$. This definition does not generalize readily to the case when B is non-commutative. Van der Waerden ([11], p. 75) defines $b \in B$ to be integral over A if all powers of b belong to a finite A-module. This definition is quite satisfactory when A satisfies the ascending chain condition for left ideals, but in the general case this type of integrity is not necessarily transitive, even when B is commutative. Krull [6] calls an element $b \in B$ which satisfies the above condition *almost integral over* A (but he only considers the commutative case). The subset $\bar{A}$ of B consisting of all almost integral elements over A is called the *complete integral closure of* A *in* B. If $\bar{A} = A$, A is said to be completely integrally closed in B. More recently (in [3]), Gilmer and Heinzer (see also Bourbaki, [1]) have discussed these properties in the commutative case and have shown that the complete integral closure of A in B need not be completely integrally closed in B. If B is not commutative, the set $\bar{A}$ of elements of B almost integral over A, may not even form a ring. In [5] p. 122, Jacobson uses a definition equivalent to Van der Waerden's for the non-commutative case but the definition applies only for a very restricted class of rings.

In the present paper a new definition of integrity is proposed which is transitive and is equivalent to the usual definition in the commutative case. It produces an integral closure $\bar{A}$ which is a ring and has the property that $A \subset \bar{A} \subset B$. In section 2 a (presumably) new type of quotient ring is introduced which differs from that used in Jacobson [5], p. 118 or the quotient rings, discussed by Utumi [10] and Lambek [7] p. 94. Our aim is to imitate more closely the theory of commutative rings, using Jacobson's definition of an 'm-system' ([4], p. 195). We define a quotient ring A_s such that $A \subset A_s \subset B$ where S is an m-system of A. This section is devoted almost exclusively however to the case where S is the complement in

A (a ring with identity) of a prime ideal $\mathscr{P}$ of A. For this type of quotient ring a Cohen and Seidenberg 'lying over' theorem is shown to hold (see [2] for the original version or [9], section 10 for a more recent treatment). In the final section some partial results are obtained relating to the question of existence of 'lying over' ideals for the non-commutative case.

1. Integral elements

Let first, B be commutative, A and B have a common identity and suppose that $b \in B$ satisfies an equation of the form (1). Zariski and Samuel ([12], Chapter V) show that this condition is equivalent to the following:

There exists a finitely generated A-module M contained in B with the following two properties:

(1) $$Mb \subset M$$

(2) $$Mx = 0 \text{ for } x \in A[b]$$

(the ring generated by b over A) implies $x = 0$. Condition (2) is obviously satisfied if M is a *unitary* module, i.e. if $1 \in M$. Conversely, if M satisfies the above conditions then there exists a finitely generated unitary A-module N satisfying

(1) $$Nb \subset N$$

and

(2) $$Nx = 0 \text{ for } x \in A[b] \text{ implies } x = 0.$$

Indeed we may take $N = M + A + Ab + \cdots + Ab^{n-1}$. Then condition (2) on N may be omitted as it follows from the fact that N is unitary.

Hence, *b is integral over A if and only if there exists a finitely generated unitary A-module N contained in B such that $Nb \subset N$.* This property will be used as essentially the definition when the restriction that B be commutative is dropped.

Now let A, B be rings (not necessarily commutative) having the same identity and such that $A \subset B$. $\mathscr{C}$ denotes the *centre* of B, i.e. the elements of B commuting with all of B.

If $b \in B$, b is said to be *integral over A* if there exists a finitely generated unitary A-module M, say $Ac_1 + Ac_2 + \cdots Ac_n$, where the generators $c_1, c_2, \cdots, c_n$ all belong to $\mathscr{C}$, such that $Mb \subset M$. Note that M is a two-sided A-module. Further, the apparent asymmetry of this definition is easily removed. Since $Mb \subset M$ there exist n^2 elements $a_{ij} \in A$ such that

$$bc_i = \sum a_{ij} c_j .$$

Since M is unitary, there exist $a_1, \cdots, a_n \in A$ such that $1 = a_1 c_1 + a_2 c_2 + \cdots + a_n c_n$. Then

$$bM = bc_1 A + bc_2 A + \cdots + bc_n A \subset Ac_1 + Ac_2 + \cdots + Ac_n$$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

that is $bM \subset M$. In fact $Mb \subset M$ if and only if $bM \subset M$. The set of elements of B integral over A will be called the *integral closure of A in B* and denoted by $\bar{A}$. A will be called *integrally closed in B* if $A = \bar{A}$.

THEOREM 1. *The integral closure $\bar{A}$ of A in B is a ring containing A.*

PROOF. Let $b, b' \in \bar{A}$ and let $M = Ac_1 + Ac_2 + \cdots + Ac_n$, $M' = Ac_1' + \cdots + Ac_r'$ be finitely generated unitary A-modules such that $c_1, c_2, \cdots, c_n, c_1', \cdots, c_r' \in \mathscr{C}$, $Mb \subset M$ and $M'b' \subset M'$. Then $MM' = M'M$ is a unitary A-module generated by the nr products $c_i c_j' \in \mathscr{C}$ $(i = 1, \cdots, n; j = 1, \cdots, r)$. Also

$$\begin{aligned} MM'(b'b) &= M(M'b')b \\ &\subset MM'b = M'(Mb) \\ &\subset M'M = MM' \end{aligned}$$

and hence $b'b \in \bar{A}$. Further,

$$\begin{aligned} MM'(b+b') &\subset MM'b + MM'b' \\ &= M'(Mb) + M(M'b') \\ &\subset M'M + MM' \\ &= MM' \end{aligned}$$

and therefore $b+b' \in \bar{A}$. This proves that $\bar{A}$ is a ring. If $a \in A$ take $M = A1 = A$. Then $1 \in \mathscr{C}$ and $Aa \subset A$. Hence $a \in \bar{A}$, i.e. $A \subset \bar{A}$.

If $B = \bar{A}$, i.e. if every element of B is integral over A then B is said to be *integral over A* or *integrally dependent on A*.

LEMMA. *If $A \subset B$ and B is integral over A then the centre of A is contained in the centre of B.*

PROOF. Let $\mathscr{C}_1$ be the centre of A and $\mathscr{C}$ be the centre of B. Let $d \in \mathscr{C}_1$ and $b \in B$. Since B is integral over A,

$$b = a_1 c_1 + a_2 c_2 + \cdots + a_n c_n$$

where $a_1, a_2, \cdots, a_n \in A$ and $c_1, c_2, \cdots, c_n \in \mathscr{C}$.

Then

$$\begin{aligned} bd &= a_1 c_1 d + a_2 c_2 d + \cdots + a_n c_n d \\ &= da_1 c_1 + da_2 c_2 + \cdots + da_n c_n \\ &= db \end{aligned}$$

Hence $d \in \mathscr{C}$, that is $\mathscr{C}_1 \subset \mathscr{C}$.

THEOREM 2. *If A, B, C are rings having the same identity such that $A \subset B \subset C$, B is integral over A and C is integral over B then C is integral over A.*

PROOF. Let $x \in C$. Suppose $\mathscr{C}'$ is the centre of C and suppose $M =$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

$Bc_1+Bc_2+\cdots+Bc_n$ where $c_1, c_2, \cdots, c_n \in \mathscr{C}'$ is unitary and such that $Mx \subset M$. Then for $i = 1, 2, \cdots, n$

$$xc_i = \sum_{j=1}^{n} b_{ij} c_j \tag{2}$$

and $x = b_1c_1+b_2c_2+\cdots+b_nc_n$ where $b_i \in B$ $(i = 1, 2, \cdots, n)$ and $b_{ij} \in B$ $(i, j = 1, 2, \cdots, n)$. Since B is integral over A there exist finitely generated unitary A-modules M_{ij}, N_k with generators in the centre $\mathscr{C}$ of B such that $M_{ij}b_{ij} \subset M_{ij}$ for each $i, j = 1, \cdots, n$ and $N_kb_k \subset N_k$ for each $k = 1, \cdots, n$.

Let $N = \prod_{i,j,k} M_{ij}N_k$ (i.e. the product of the n^2 A-modules M_{ij} with the n A-modules N_k). Each of these modules commute with one another so the product may be taken in any order. Further N is a finitely generated unitary A-module with generators in $\mathscr{C}$ having the property that for each i, j

$$Nb_{ij} \subset N \text{ and for each } k,\ Nb_k \subset N.$$

Finally, let $L = N+Nc_1+Nc_2+\cdots+Nc_n$. Then L is an A-module of the required type (unitary with generators in $\mathscr{C}'$) such that

$$Lx \subset L, \text{ because}$$
$$Nxc_i \subset Nc_1+\cdots+Nc_n \text{ (from (2))}$$

(and therefore $(Nc_1+Nc_2+\cdots+Nc_n)x \subset L$) and $Nx \subset Nc_1+Nc_2+\cdots+Nc_n$ (from (2)).

COROLLARY. *The integral closure $\bar{A}$ of A in B is integrally closed in B.*

The definition of $b \in B$ being integral over A may be reworded as follows:

P1. *b is integral over A if and only if there exist elements $c_1, c_2, \cdots, c_n \in \mathscr{C}$ and elements $a_{ij}, a_k \in A$ $(i, j, k = 1, 2, \cdots, n)$ such that*

$$bc_i = \sum_{j=1}^{n} a_{ij} c_j \qquad (i = 1, 2, \cdots, n)$$

and

$$1 = \sum_{k=1}^{n} a_k c_k .$$

Some other elementary properties will be listed below.

P2. *If $\mathscr{C} \subset A$ then A is integrally closed in B. If $A \subset \mathscr{C}$ then $\bar{A} \subset \mathscr{C}$.*

PROOF. Let $b \in \bar{A}$ and suppose $bM \subset M$ where $M = Ac_1+Ac_2+\cdots+Ac_n$ and $c_1, c_2, \cdots, c_n \in \mathscr{C}$. Then $bM \subset A$ and hence $b \in A$ since M is unitary. The second statement is proved similarly.

P3. *If b is integral over A and commutes with all of A then b satisfies an equation of the form*

$$b^n+a_1b^{n-1}+\cdots+a_{n-1}b+a_n = 0$$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

where $a_1, a_2, \cdots, a_n \in A$. *Conversely, if* $b \in \mathscr{C}$ *and* b *satisfies an equation of this form then* $b \in \bar{A}$.

PROOF. Let b be as in P1.

Then $\sum_{j=1}^{n}(a_{ij}-b\delta_{ij})c_j = 0$ $(i = 1, 2, \cdots, n)$. These n homogeneous equations equations have a non-trivial solution $c_1, c_2, \cdots, c_n$ (since $\Sigma a_k c_k = 1$). Since all quantities in these equations commute, the determinant Δ of the coefficients exists and

$$\Delta c_1 = \Delta c_2 = \cdots = \Delta c_n = 0.$$

Using $\Sigma a_k c_k = 1$ it follows that $\Delta = 0$. This yields, on expansion, the desired equation for b. Conversely, if $b \in \mathscr{C}$ satisfies an equation

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0$$

let $M = A + Ab + \cdots + Ab^{n-1}$. Then M is a finitely generated unitary A-module such that $Mb \subset M$. Hence $b \in \bar{A}$.

The following fact has already been used in the proof of Theorems 1 and 2.

P4. *Given any finite number of elements* $b_1, b_2, \cdots, b_k$ *of* $\bar{A}$ *(with corresponding modules* $M_1, M_2, \cdots, M_k$*) there exists a unitary* A*-module* M *with generators in* $\mathscr{C}$ *such that* $Mb_1 \subset M$, $Mb_2 \subset M, \cdots, Mb_k \subset M$. *Equivalently, using P*1, *the same set of elements* $c_1, c_2, \cdots, c_n$ *of* $\mathscr{C}$ *may be used in the definitions of* $b_1, b_2, \cdots, b_k$ *being integral over* A.

PROOF. Take $M = M_1 M_2 \cdots M_k$.

The question naturally arises, in the previous proposition, as to what happens when one considers more than a finite number of elements of $\bar{A}$. This question is partially answered in the following theorem:

THEOREM 3. *If* $\mathscr{C}$ *is a finitely generated (necessarily unitary)* A*-module then* $\bar{A} \subset \mathscr{C}$.

PROOF. Let $\mathscr{C} = Ac_1 + Ac_2 + \cdots + Ac_n$ where

$$\sum_{j=1}^{n} a_j c_j = 1 \qquad (a_1, a_2, \cdots, a_n \in A). \tag{1}$$

Let $b \in \bar{A}$ and suppose, by P1, that $c_1', c_2', \cdots, c_m' \in \mathscr{C}$ are such that

$$bc_j' = \sum a_{jr}' c_r' \qquad (j = 1, 2, \cdots, m) \tag{2}$$

(where all $a_{jr}' \in A$) and also that

$$b = \sum a_j' c_j' \tag{3}$$

(where $a_1', \cdots, a_m' \in A$). Hence

$$bc_i = \sum a_j' c_i c_j' \qquad (i = 1, \cdots, n). \tag{4}$$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

Also there exists $a_{ijk} \in A$ such that

$$c_i c_j' = \sum a_{ijk} c_k \qquad (i = 1, 2, \cdots, n;\ j = 1, 2, \cdots, m). \tag{5}$$

Finally, from (4) and (5),

$$bc_i = \sum a_j' a_{ijk} c_k \tag{6}$$

Equations (1) and (6) imply $\bar{A} \subset \mathscr{C}$.

COROLLARY. *If B is integral over A and $\mathscr{C}$ is a finitely generated A-module then B is commutative.*

P5. *If $\emptyset(B)$ is a homomorphic image of B then $\emptyset(\bar{A})$ is integral over $\emptyset(A)$ ($\emptyset$ is a ring homomorphism).*

PROOF. Let $b \in \bar{A}$ be as in P1. Then $\emptyset(c_1), \cdots, \emptyset(c_n) \in \emptyset(\mathscr{C})$ (which is also the centre of $\emptyset(B)$) are such that

$$\emptyset(b)\emptyset(c_i) = \sum \emptyset(a_{ij})\emptyset(c_j)$$

and

$$\emptyset(1) = \sum \emptyset(a_k)\emptyset(c_k)$$

Hence from P1, $\emptyset(b)$ is integral over $\emptyset(A)$.

P6. *If B is integral over A and Q is an ideal in B, then*

$$\frac{B}{Q} \text{ is integral over } \frac{A}{Q \cap A}.$$

PROOF. $A/(Q \cap A)$ may be thought of as a subring of B/Q because of the isomorphism $A/(Q \cap A) \cong (A+Q)/Q$. Also $(\mathscr{C}+Q)/Q$ is contained in the centre of B/Q. The result now follows from P1 and P5.

We conclude this section by considering some examples.

EXAMPLE 1. It is trivial to show that the set of integral elements $\bar{A}$ is contained in the set of integral elements according to the Van der Waerden definition. Thus if $b \in \bar{A}$ has corresponding module M then $b, b^2, b^3, \cdots, \in M$, and b is almost integral over A. To distinguish these in the non-commutative case we choose A to be the set Z of rational integers and B to be the ring Q_i of *integral quaternions*, i.e. all elements x of the form $x = \frac{1}{2}(a+bi+cj+dk)$ where $a, b, c, d \in Z$ and are either all even or all odd. Then any such element satisfies a monic quadratic

$$x^2 - ax + \tfrac{1}{4}(a^2+b^2+c^2+d^2) = 0$$

with coefficients in Z. Hence the Van der Waerden (or complete) integral closure of A in B is B. However, since $A = \mathscr{C}$ it follows from P2 that $A = \bar{A}$.

EXAMPLE 2. To obtain a non-commutative example where $\bar{A} \neq A$ or B we

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

take A to be the commutative ring Z of rational integers and B to be $Q[\sqrt{2}] = Q+Q\sqrt{2} = Q+\sqrt{2}Q$ where Q denotes the set of quaternions with integer coefficients, i.e. the set of $x = a+bi+cj+dk$ where $a, b, c, d, \in Z$, and $\sqrt{2}$ is assumed to commute with each element of Q. Here $\mathscr{C} = Z[\sqrt{2}]$ and $\mathscr{C} \supset A$. Hence by P2, $\bar{A} \subset Z[\sqrt{2}]$. Conversely, if $x = a+b\sqrt{2}$ where $a, b \in Z$ then

$$x^2-2ax+(a^2-2b^2) = 0.$$

Since $x \in \mathscr{C}$ it follows from P3 that $x \in \bar{A}$. Hence $\bar{A} = Z[\sqrt{2}]$. In this example both A and $\bar{A}$ are commutative. It is easy to show that, in general, A commutative implies $\bar{A}$ is commutative.

EXAMPLE 3. To obtain a non-trivial example for the case A non-commutative we simply extend the rings in Example 2 to *complete matrix rings*. In the matter of notation, if R is a ring, then R_n denotes the complete matrix ring (and also algebra) consisting of all $n \times n$ matrices with elements in R. We now take $A = Z_n$, $B = Q[\sqrt{2}]_n$ where $Q[\sqrt{2}]$ is as described in Example 2. Then it can be shown that $\mathscr{C}$ consists of the set of *scalar* matrices of $Z[\sqrt{2}]_n$. Let $T \in \bar{A}$ where $C_1, C_2, \cdots, C_n \in \mathscr{C}$ are such that

$$TC_i = \sum A_{ij}C_j \qquad (i = 1, \cdots, n)$$

and $\sum A_iC_i = I$, where all $A_i, A_{ij} \in A = Z_n$ and I is the unit matrix. If for $i = 1, \cdots, n$ we write $C_i = (a_i+b_i\sqrt{2})I$ where $a_i, b_i \in Z$ then the above equations can be written

$$(a_i+b_i\sqrt{2})T = \sum (a_j+b_j\sqrt{2})A_{ij} \qquad (i = 1, \cdots, n)$$
$$\sum (a_i+b_i\sqrt{2})A_i = I.$$

These imply $T \in Z[\sqrt{2}]_n$. Conversely consider the matrix units E_{ij} having 1 in the i, j th place and zeros elsewhere. Then $E_{ij} \in \bar{A}$ (because $E_{ij} \in A$). Finally, by P3 $\mathscr{C} \subset \bar{A}$. The scalar matrices of $Z[\sqrt{2}]_n$ and the E_{ij} together generate all of $Z[\sqrt{2}]_n$. Hence $\bar{A} = Z[\sqrt{2}]_n$.

2. Quotient rings and prime ideals

In this section we will study the concept of a quotient ring defined somewhat differently from Jacobson and Utumi (see [5] p. 118); or [7] p. 94; or (10]), but more directly related to the theory of commutative rings. No apology is made for using the same notation.

First, in the matter of definitions, we use Jacobson's idea of an 'm-system' ([4], p. 195). A subset S of a ring R is called an *m-system* if (i) $0 \notin S$ and (ii) whenever $a, b \in S$ there exists $x \in R$ such that $axb \in S$. The following proposition is easily proved by induction:

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

P7. *If S is an m-system of a ring R and $s_1, s_2, \cdots, s_n \in S$ then there exist $r_1, r_2, \cdots, r_{n-1} \in R$ such that $s_1 r_1 s_2 \cdots r_{n-1} s_n \in S$.*

Next, a *prime ideal* $\mathscr{P}$ in a ring A is defined to be a two-sided ideal with the property that if α, β are ideals of A such that $\alpha\beta \subset \mathscr{P}$ then either $\alpha \subset \mathscr{P}$ or $\beta \subset \mathscr{P}$. A list of properties of prime ideals is given in [8], Chapter 4. Amongst these we select for reference:

P8. *$\mathscr{P}$ is a prime ideal in A if and only if $\mathscr{P}$ is an ideal with the property that $aAb \subset \mathscr{P}$ implies $a \in \mathscr{P}$ or $b \in \mathscr{P}$.*

P9. *$\mathscr{P}$ is a prime ideal in A if and only if the complement $A - \mathscr{P}$ of $\mathscr{P}$ in A is an m-system.*

If S is an m-system of a ring A and $A \subset B$ then the *quotient ring* A_S is defined to be the set of elements $b \in B$ such that there exists an element $s(b) \in S$ such that

$$sAb \subset A \quad \text{and} \quad bAs \subset A.$$

Note that, if A has a 1, this implies $sb \in A$ and $bs \in A$.

P10. *A_S is a ring containing A.*

PROOF. If $b \in A$ choose any $s \in S$. Hence $A_S \supset A$. If $b_1, b_2 \in A_S$ let $s_1, s_2 \in S$ be such that

$$s_1 A b_1 \subset A, \quad b_1 A s_1 \subset A,$$
$$s_2 A b_2 \subset A, \quad b_2 A s_2 \subset A.$$

Since $s_1, s_2 \in S$ it follows that $s_2 a s_1 \in S$ for some $a \in A$ and then

$$(s_2 a s_1) A (b_1 b_2) \subset s_2 a A b_2 \subset s_2 A b_2 \subset A.$$

Also $(b_1 b_2) A (s_2 a s_1) \subset b_1 A a s_1 \subset A$. Hence $b_1 b_2 \in A_S$.

Now consider $b_1 - b_2$.

$$\begin{aligned} s_2 a s_1 A (b_1 - b_2) &\subset s_2 a (s_1 A b_1 + s_1 A b_2) \\ &\subset s_2 a (A + s_1 A b_2) \\ &= s_2 a A + s_2 (a s_1 A) b_2 \\ &\subset A. \end{aligned}$$

Hence $b_1 - b_2 \in A_S$ and so A_S is a ring.

For the remainder of this section it will be assumed that A has an identity. When $\mathscr{P}$ is a prime ideal of A (and $A \subset B$) the complement $A - \mathscr{P}$ of $\mathscr{P}$ in A is an m-system. Using this m-system, denote by $A_{\mathscr{P}}$ the corresponding quotient ring $(A \subset A_{\mathscr{P}} \subset B)$, i.e. $b \in A_{\mathscr{P}}$ if and only if there exists $s \in A - \mathscr{P}$ such that $sAb \subset A$ and $bAs \subset A$. The respective left, right and two-sided ideals $A_{\mathscr{P}}\mathscr{P}$, $\mathscr{P}A_{\mathscr{P}}$, $A_{\mathscr{P}}\mathscr{P}A_{\mathscr{P}}$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

are of some interest. The last of these contains the first two. That it is a proper ideal follows from the next theorem.

THEOREM 4. $(A_{\mathscr{P}}\mathscr{P}A_{\mathscr{P}}) \cap A = \mathscr{P}$.

PROOF. Let $b \in (A_{\mathscr{P}}\mathscr{P}A_{\mathscr{P}}) \cap A$. Suppose

$$b = b_1 p_1 b_1' + b_2 p_2 b_2' + \cdots + b_n p_n b_n'$$

where $b_i, b_i' \in A_{\mathscr{P}}$, $p_i \in \mathscr{P}$ $(i = 1, 2, \cdots, n)$. Choose, for $i = 1, 2, \cdots, n$ elements $s_i, s_i' \in A - \mathscr{P}$ such that

$$s_i A b_i \subset A, \; b_i A s_i \subset A, \quad s_i' A b_i' \subset A, \quad b_i' A s_i' \subset A \quad (i = 1, 2, \cdots, n),$$

and $a_1, \cdots, a_{n-1}, a_1', \cdots, a_{n-1}' \in A$ such that

$$s = s_1 a_1 s_2 \cdots a_{n-1} s_n \in A - \mathscr{P}$$

and

$$s' = s_1' a_1' s_2' \cdots a_{n-1}' s_n' \in A - \mathscr{P}.$$

Then $sAbAs' \subset \mathscr{P}$ because any term of the form

$$s_1 a_1 s_2 \cdots (s_i \cdots a_{n-1} s_n A b_i) p_i (b_i' A s_1' a_1' \cdots s_i') \cdots s_n'$$

is contained in $\mathscr{P}$. Since A has an identity, $A^2 = A$ and therefore

$$(AsA)(AbA)(As'A) \subset \mathscr{P}.$$

Since $\mathscr{P}$ is prime this implies either s, b or s' belongs to $\mathscr{P}$. Hence $b \in \mathscr{P}$ and the theorem is established.

We now define $\mathscr{P}'$ as the set of elements $b \in A_{\mathscr{P}}$ such that there exist s, $s' \in A - \mathscr{P}$ for which $sAbAs' \subset \mathscr{P}$.

P11. *$\mathscr{P}'$ is an ideal of $A_{\mathscr{P}}$ containing $A_{\mathscr{P}}\mathscr{P}A_{\mathscr{P}}$.*

PROOF. $A_{\mathscr{P}}\mathscr{P}A_{\mathscr{P}} \subset \mathscr{P}'$ from the proof of Theorem 4. To show that $\mathscr{P}'$ is an ideal let $b_1, b_2 \in \mathscr{P}'$ where

$$s_1 A b_1 A s_1' \subset \mathscr{P}, \quad s_2 A b_2 A s_2' \subset \mathscr{P}$$

and

$$s_1, s_1', s_2, s_2' \in A - \mathscr{P}.$$

There exist $a, a' \in A$ such that $s = s_2 a s_1$ and $s' = s_2' a' s_1' \in A - \mathscr{P}$. Then

$$sA(b_1 - b_2)As' \subset s_2 a(s_1 A b_1 A s_2' a' s_1') + (s_2 a s_1 A b_2 A s_2') a' s_1' \subset \mathscr{P}.$$

Hence $b_1 - b_2 \in \mathscr{P}'$.

Let $x \in A_{\mathscr{P}}$. Then there exists $r \in A - \mathscr{P}$ such that $rAx \subset A$ and $xAr \subset A$. Since $r, s_1' \in A - \mathscr{P}$ there exists $a_1 \in A$ such that $t = r a_1 s_1' \in A - \mathscr{P}$. Then for $s_1, t \in A - \mathscr{P}$ we have

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

$$s_1 Ab_1 xAt = s_1 Ab_1(xAr)a_1 s_1' \subset s_1 Ab_1 As_1' \subset \mathscr{P}.$$

Hence $b_1 x \in \mathscr{P}'$. Similarly $xb_1 \in \mathscr{P}'$. Thus $\mathscr{P}'$ is an ideal.

THEOREM 5. *$\mathscr{P}'$ is a proper prime ideal of $A_{\mathscr{P}}$ with the property that $\mathscr{P}' \cap A = \mathscr{P}$.*

PROOF. We first show that $\mathscr{P}' \cap A = \mathscr{P}$. That $\mathscr{P}' \cap A \supset \mathscr{P}$ follows from P11 and Theorem 4. Now let $b \in \mathscr{P}' \cap A$. Then for some $s, s' \in A - \mathscr{P}$ we have $sAbAs' \subset \mathscr{P}$. Hence

$$(AsA)(AbA)(As'A) \subset \mathscr{P}.$$

The fact that $\mathscr{P}$ is prime and $b \in A$ implies that one of s, b or s' belongs to $\mathscr{P}$. Hence $b \in \mathscr{P}$ and $\mathscr{P}' \cap A = \mathscr{P}$.

To show that $\mathscr{P}'$ is prime, let $xA_{\mathscr{P}}y \subset \mathscr{P}'$ where $x, y \in A_{\mathscr{P}}$. Choose t, $t' \in A - \mathscr{P}$ such that

$$tAx \subset A, \quad xAt \subset A, \quad yAt' \subset A, \quad t'Ay \subset A.$$

From $xAy \subset \mathscr{P}'$ it follows that $tAxAyAt' \subset \mathscr{P}'$ and hence that $tAxAyAt' \subset \mathscr{P}$ since the left hand side is contained in A and $\mathscr{P}' \cap A = \mathscr{P}$. From the fact that $\mathscr{P}$ is prime and that

$$(tAx)A(yAt') \subset \mathscr{P}$$

it follows that either $tAx \subset \mathscr{P}$ or $yAt' \subset \mathscr{P}$. (Take any $a \in A$. Either $tax \in \mathscr{P}$ or $tax \notin \mathscr{P}$. If $tax \notin \mathscr{P}$ then $yAt' \subset \mathscr{P}$). If $tAx \subset \mathscr{P}$ then $tAxAt \subset \mathscr{P}$ and hence $x \in \mathscr{P}'$. If $yAt' \subset \mathscr{P}$ then $t'AyAt' \subset \mathscr{P}$ and hence $y \in \mathscr{P}'$. Hence either $x \in \mathscr{P}'$ or $y \in \mathscr{P}'$, i.e. $\mathscr{P}'$ is prime.

COROLLARY. *If $\mathscr{P}$ is a maximal ideal of A then $\mathscr{P}'$ is a maximal ideal of $A_{\mathscr{P}}$.*

PROOF. (Since A has a 1, every maximal ideal of A is prime). If $\mathscr{Q}'$ is an ideal of $A_{\mathscr{P}}$ such that $\mathscr{Q}' \supset \mathscr{P}'$ than $\mathscr{Q}' \cap A \supset \mathscr{P}$. Hence, since $\mathscr{P}$ is maximal, either $\mathscr{Q}' \cap A = A$ (in which case $\mathscr{Q}' = A_{\mathscr{P}}$) or $\mathscr{Q}' \cap A = \mathscr{P}$. Assume that $\mathscr{Q}'$ is a proper ideal strictly containing $\mathscr{P}'$ and let $b \in \mathscr{Q}'$, $b \notin \mathscr{P}'$. Then for all $s, s' \in A - \mathscr{P}$, $sAbAs' \not\subset \mathscr{P}$. Since $b \in A_{\mathscr{P}}$ choose $s = s' \in A - \mathscr{P}$ such that $sAb \subset A$ and $bAs \subset A$. Then there exist $a_i, a_i' \in A$ such that $\sum sa_i ba_i' s \notin \mathscr{P}$ contradicting the fact that

$$\sum sa_i ba_i' s \in \mathscr{Q}' \cap A \ (= \mathscr{P}).$$

3. Lying over theorems

We return to the case of rings A, B with the same identity such that $A \subset B$ and B is integral over A. $\mathscr{P}$ is any ideal of A. Let $b \in B$. Consider, if they exist, any finite set of elements $c_1, c_2, \cdots, c_n \in \mathscr{C}$ having the properties that

(1) $bc_i = \sum a_{ij} c_j (i = 1, \cdots, n)$ where all $a_{ij} \in A$

(2) there exist $a_1, a_2, \cdots, a_n \in A$ such that $a_1 c_1 + a_2 c_2 + \cdots + a_n c_n = 1$.

(3) $\mathscr{P}c_1 + \mathscr{P}c_2 + \cdots + \mathscr{P}c_n = \mathscr{P}$.

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

If $b \in A$ such a set exists since we may take the set consisting of the single element 1.

P12. *If for $b \in B$ a set $c_1, c_2, \cdots, c_n \in \mathscr{C}$ exists having properties* (1), (2), (3) *then any finite set of generators in $\mathscr{C}$ of $M = Ac_1 + Ac_2 + \cdots + Ac_n$ also has these properties.*

PROOF. Suppose $M = Ad_1 + Ad_2 + \cdots + Ad_r$ where $d_1, d_2, \cdots, d_r \in \mathscr{C}$. Let

$$d_i = \sum \alpha_{ij} c_j \qquad (i = 1, \cdots, r)$$

where $\alpha_{ij} \in A$. Then

$$\begin{aligned} bd_i &= \sum \alpha_{ij} b c_j = \sum \alpha_{ij} a_{jk} c_k \\ &= \sum \alpha_{ij} a_{jk} \beta_{ks} d_s \end{aligned}$$

where $c_k = \sum \beta_{ks} d_s$, $\beta_{ks} \in A$. This proves (1).

Property (2) is obvious since $1 \in M$ and therefore $\sum \alpha_i d_i = 1$, $\alpha_i \in A$.

It is clear from the relations $d_i = \sum \alpha_{ij} c_j$ that $\mathscr{P}d_1 + \mathscr{P}d_2 + \cdots + \mathscr{P}d_r \subset \mathscr{P}$ and from $\sum \alpha_i d_i = 1$ that $\mathscr{P}d_1 + \mathscr{P}d_2 + \cdots \mathscr{P}d_r \supset \mathscr{P}$.

Hence $\mathscr{P}d_1 + \mathscr{P}d_2 + \cdots \mathscr{P}d_r = \mathscr{P}$, proving (3).

A set of elements $c_1, c_2, \cdots, c_n \in \mathscr{C}$ satisfying property (2) will be called *unitary*. If $c_1, \cdots, c_n \in \mathscr{C}$ and $c'_1, \cdots c'_m \in \mathscr{C}$ are two unitary sets their *sum* is defined to be the set $c_1, \cdots, c_n, c'_1, \cdots, c'_m$ and their *product* the set of mn products $c_1 c'_1, \cdots, c_i c'_j, \cdots, c_n c'_m$. It is easy to verify that the sum and product are themselves unitary. If M, M' denote the corresponding unitary A-modules defined by

$$M = Ac_1 + \cdots Ac_n, \; M' = Ac'_1 + \cdots + Ac'_m$$

then their sum $M + M'$ is generated by the sum of the generators and their product $MM' = M'M$ is generated by the product of the generators.

P13. *If $b \in B$ is such that there exist two sets of elements $c_1, c_2, \cdots, c_n \in \mathscr{C}$ and $c'_1, c'_2, \cdots, c'_m \in \mathscr{C}$ having properties* (1), (2) *and* (3) *then the sum and product of these elements also have properties* (1), (2) and (3).

PROOF. To say that $c'_1, c'_2, \cdots, c'_m \in \mathscr{C}$ have properties (1), (2), (3) means that

(1) $bc'_i = \sum a'_{ij} c'_j$ $(i = 1, \cdots, m)$ where all $a'_{ij} \in A$

(2) there exist $a'_1, a'_2, \cdots, a'_n \in A$ such that $a'_1 + c'_1 + \cdots + a'_n c'_n = 1$.

(3) $\mathscr{P}c'_1 + \mathscr{P}c'_2 + \cdots + \mathscr{P}c'_n = \mathscr{P}$.

These properties obviously hold for the sum. For the product we observe that

(1) $bc_i c'_k = \sum a_{ij} c_j c'_k$ $(i = 1, \cdots, n;\ k = 1, \cdots, m)$

(2) $\sum a_i a'_j c_i c'_j = 1$, obtained from multiplying together the relations $\sum a_i c_i = 1$ and $\sum a'_j c'_j = 1$.

(3) $\mathscr{P}c_1 c'_1 + \cdots + \mathscr{P}c_i c'_j + \cdots + \mathscr{P}c_n c'_m \subset \mathscr{P}c_1 + \cdots + \mathscr{P}c_i + \cdots + \mathscr{P}c_n = \mathscr{P}$

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

and on the other hand,

$$\mathscr{P}c_1 c_1' + \cdots + \mathscr{P}c_i c_j' + \cdots + \mathscr{P}c_n c_m' \supset \mathscr{P}$$

because if $p \in \mathscr{P}$ then $p = \sum pa_i a_j' c_i c_j'$. This proves P13.

THEOREM 6. *The set of elements $b \in B$ for which there exists $c_1, c_2, \cdots, c_n \in \mathscr{C}$ having properties* (1), (2) *and* (3) *forms a subring $A_{(\mathscr{P})}$ of B containing A.*

PROOF. It is clear that $A \subset A_{(\mathscr{P})}$. Let b, $b' \in A_{(\mathscr{P})}$. Then there exist $c_1, c_2, \cdots, c_n \in \mathscr{C}$ such that

(1) $$bc_i = \sum a_{ij} c_j,\ a_{ij} \in A \qquad (i = 1, \cdots, n)$$

(2) $$\sum a_i c_i = 1,\ a_i \in A \qquad (i = 1, \cdots, n)$$

(3) $$\mathscr{P}c_1 + \mathscr{P}c_2 + \cdots \mathscr{P}c_n = \mathscr{P}$$

and $c_1', c_2', \cdots, c_m' \in \mathscr{C}$ such that

(1)′ $$b'c_i' = \sum a_{ij}' c_j',\ a_{ij}' \in A \qquad (i = 1, \cdots, n)$$

(2)′ $$\sum a_i' c_i' = 1,\ a_i' \in A \qquad (i = 1, \cdots, n)$$

(3)′ $$\mathscr{P}c_1' + \mathscr{P}c_2' + \cdots + \mathscr{P}c_n' = \mathscr{P}.$$

Then for $b - b'$ and bb' use the product of $c_1, \cdots, c_n$ and $c_1', \cdots, c_m'$. Hence $b - b'$, $bb' \in A_{(\mathscr{P})}$, so $A_{(\mathscr{P})}$ is a ring.

Note that, if B is integral over A, then for any element $b \in B$ there exist $c_1, c_2, \cdots, c_n \in \mathscr{C}$ having properties (1) and (2) and, in place of (3), the weaker condition

$$\mathscr{P}c_1 + \mathscr{P}c_2 + \cdots + \mathscr{P}c_n \supset \mathscr{P}.$$

Also if M denotes the unitary A-module $Ac_1 + Ac_2 + \cdots + Ac_n$ then (3) may be written $M\mathscr{P} = \mathscr{P}M = \mathscr{P}$. Zorn's Lemma can be used to show (in the case where (3) is not necessarily satisfied) that for a given ideal $\mathscr{P}$ of A, there exists a unitary A-module M (not necessarily finitely generated) such that $M\mathscr{P} = \mathscr{P}M = \mathscr{P}$.

P14. *If B is integral over A and if, for a given ideal $\mathscr{P}$ of A, $A_{(\mathscr{P})} = B$ then there exists an ideal P of B lying over $\mathscr{P}$. i.e. $P \cap A = \mathscr{P}$.*

PROOF. Consider the set $\mathscr{S}$ of ideals Q of B such that $Q \cap A \subset \mathscr{P}$. Then $\mathscr{S} \neq \emptyset$ since $0 \in \mathscr{S}$. Clearly any totally ordered subset of $\mathscr{S}$ (partially ordered by inclusion) has an upper bound in $\mathscr{S}$. Hence by Zorn's Lemma, $\mathscr{S}$ has a maximal element P. It will be shown that $P \cap A = \mathscr{P}$.

Suppose, on the contrary, that there exists $x \in \mathscr{P}$, $x \notin P$. Then $P + BxB$ is an ideal strictly containing P and therefore $(P + BxB) \cap A \not\subset \mathscr{P}$. Hence there exists $s \in A - \mathscr{P}$ such that $s \in P + BxB$ and therefore there exist also elements b_1, $b_2 \in B$ such that $s - b_1 x b_2 \in P$. Since $b_1, b_2 \in B$, which is integral over A, there exist elements $c_1, c_2, \cdots, c_n \in \mathscr{C}$ such that:

https://doi.org/10.1017/S1446788700009174 Published online by Cambridge University Press

$$b_1 c_i = \sum a_{ij} c_j \qquad (i = 1, \cdots, n),$$
$$b_2 c_i = \sum a'_{ij} c_j \qquad (i = 1, \cdots, n),$$
$$\sum a_i c_i = 1 \text{ where } a_i, a_{ij}, a'_{ij} \in A \qquad (i, j = 1, \cdots, n),$$

$\mathscr{P}c_1 + \mathscr{P}c_2 + \cdots + \mathscr{P}c_n = \mathscr{P}$ (using P13 and the fact that $A_{(\mathscr{P})} = B$). Hence

$$b_1 x b_2 c_i = \sum a_{ij} x b_2 c_j = \sum a_{ij} x a'_{jk} c_k$$

and therefore $b_1 x b_2 = \sum a_{ij} x a'_{jk} a_i c_k$, that is,

$$b_1 x b_2 \in \mathscr{P}c_1 + \mathscr{P}c_2 + \cdots + \mathscr{P}c_n = \mathscr{P}.$$

Hence $s - b_1 x b_2 \in P \cap A \subset \mathscr{P}$. However $s - b_1 x b_2 \in \mathscr{P}$, $b_1 x b_2 \in \mathscr{P}$ imply $s \in \mathscr{P}$, a contradiction.

THEOREM 7. *If B is integral over A and if $\mathscr{P}$ is a maximal ideal of A such that $A_{(\mathscr{P})} = B$ then there exists a maximal ideal P of B such that $P \cap A = \mathscr{P}$.*

PROOF. Define P' to be the set of $b \in B$ for which there exists $s, s' \in A - \mathscr{P}$ making $sAbAs' \subset \mathscr{P}$. Then

(i) $P' \cap A = \mathscr{P}$, because if $b \in \mathscr{P}$ choose $s = s' = 1$. If $b \in P \cap A$ then $sAbAs' \subset \mathscr{P}$ and $s, s' \in A - \mathscr{P}$ imply $b \in \mathscr{P}$ (= prime ideal of A).

(ii) P' is an ideal of B : P' is clearly closed under subtraction. Let $b \in P'$, $x \in B$ where $s, s' \in A - \mathscr{P}$ are such that $sAbAs' \subset \mathscr{P}$ and $c_1, c_2, \cdots, c_n \in \mathscr{C}$ are such that

$$xc_i = \sum a_{ij} c_j, (a_{ij} \in A) \qquad (i = 1, \cdots, n),$$
$$\sum a_i c_i = 1 (a_1, a_2, \cdots, a_n \in A),$$
$$\mathscr{P}c_1 + \mathscr{P}c_2 + \cdots + \mathscr{P}c_n = \mathscr{P}.$$

Then $bxc_i = \sum ba_{ij} c_j$ and hence

$$bx \in bAc_1 + bAc_2 + \cdots bAc_n.$$

Therefore

$$\begin{aligned} sAbxAs' &\subset sAbAs'c_1 + \cdots + sAbAs'c_n \\ &\subset \mathscr{P}c_1 + \cdots + \mathscr{P}c_n \\ &= \mathscr{P}. \end{aligned}$$

Hence $bx \in P'$. Similarly $xb \in P'$ and so P' is an ideal of B.

(iii) P' is contained in a maximal ideal P of B. Hence $P \cap A \supset \mathscr{P}$. Since $\mathscr{P}$ is maximal it follows that $P \cap A = \mathscr{P}$. This concludes the proof of the theorem.

The question remains open as to whether, in the case B integral over A, for a given prime ideal $\mathscr{P}$ of A there exists a prime ideal P of B such that $P \cap A = \mathscr{P}$. This is true when B is commutative (see [2]) or in any of the examples of Section 1. Nevertheless this result is unlikely but a counterexample is still lacking.

References

[1] N. Bourbaki, *Eléments de Mathématique, Algèbre Commutative*, XXX (Hermann, Paris, 1964).
[2] I. S. Cohen and A. Seidenberg, 'Prime ideals and integral dependence', *Bull. Amer. Math. Soc.* 52 (1946), 252–261.
[3] R. W. Gilmer and W. J. Heinzer, 'On the complete integral closure of an integral domain', *J. Australian Math. Soc.* 6 (1966), 351–361.
[4] N. Jacobson, *Structure of Rings* (Colloquium Publications, number 37, Amer. Math. Soc., 1956).
[5] N. Jacobson, *Theory of Rings* (Math. Surveys, number 2, Amer. Math. Soc., New York, 1943).
[6] W. Krull, 'Beiträge zur Arithmetik kommutativer Integritätsbereiche II', *Math. Z.* 41 (1936), 665–679.
[7] J. Lambek, *Lectures on Rings and Modules* (Blaisdell, Mass. 1966).
[8] N. H. McCoy, *The Theory of Rings* (Macmillan, New York, 1964).
[9] M. Nagata, *Local Rings* (Interscience, New York, 1962).
[10] Y. Utumi, 'On Quotient Rings', *Osaka Math. J.* 8 (1956), 1–18.
[11] B. L. van der Waerden, *Modern Algebra*, II (Frederick Ungar, New York, 1950).
[12] O. Zariski and P. Samuel, *Commutative Algebra*, I (Van Nostrand, Princeton, 1962).

Department of Pure Mathematics
University of New South Wales