BULL. AUSTRAL. MATH. SOC. MOS 1065, 1250

VOL. 1 (1969), 345-352.

A note on certain subsets of algebraic integers

T. W. Atterton

This paper is concerned with certain subsets of a finite extension K of the quotient field of an integral domain R. These subsets are contained in the integral closure of R in K and when R is integrally closed they are identical with it, but generally they need not even be rings. Various inclusion relations are studied and examples are given to show that these inclusions may be strict (with one exception which is still undecided).

Introduction

R will denote a fixed integral domain with quotient field k. K is a finite extension of k of degree n. This paper will be concerned with properties of certain subsets R_a (defined below) of K related to integral closure. In addition the set R_M of elements of K whose (monic) minimal polynomial has coefficients in R, the set R_C of elements of K whose characteristic polynomial has coefficients in R and the set R_U of elements of K which possess a representative matrix (with respect to some basis of K over k) all of whose elements lie in R will be considered.

Let $a_1, a_2, \ldots, a_n$ (denoted in short by $\mathbf{a}$) be any basis for K over k. The set

$$R\mathbf{a} = Ra_1 + Ra_2 + \ldots + Ra_n$$

will be called a *basis R-module*. If $b \in K$ let $b \to B = (\beta_{ij})$ denote the

Received 18 June 1969.

regular representation of K into $M_n(k)$, the ring of $n \times n$ matrices with elements in k. ($M_n(R)$ is similarly defined.) That is

$$ba_i = \sum \beta_{ij} a_j , \quad \beta_{ij} \in k \qquad (i = 1,2,\ldots,n) .$$

A subset R_a of K is defined as follows: if $b \in K$ then $b \in R_a$ if and only if $B \in M_n(R)$, i.e. $\beta_{ij} \in R$ for $i,j = 1,2,\ldots,n$: R_a is called the *coefficient domain* of the corresponding basis R-module Ra.

1. Properties of coefficient domains

It is easily verified that R_a is an integral domain containing R (strictly if $n > 1$) and that

P1. $R_a \cap k = R$.

P2. *The quotient field of* R_a *is* K.

P3. $R_a = R_{\lambda a}$, *any* $\lambda \in k_0$ *(the set of non-zero elements of* k*),* *where* λa *denotes the basis* $\lambda a_1, \lambda a_2, \ldots, \lambda a_n$ *of* K *over* k.

P4. *If* b *is any element of* K *then there exists an element* β *(depending on* b*) of* R_0 *(the set of non-zero elements of* R*)* *such that*

$$\beta b \in R_a .$$

P5. *All elements of* R_a *are integral over* R*, i.e. they satisfy* *monic polynomials with coefficients in* R.

Proof. The field polynomial $|xI-B|$ of any element b of R_a (where $b \to B$ with respect to the basis a and I denotes the identity matrix) is monic and has coefficients in R. This polynomial is satisfied by b and hence b is integral over R.

For any element $b \in K$, its (K over k) *trace* will be denoted by $T(b)$ and its (K over k) *norm* by $N(b)$.

The *integral closure* of R in K will be denoted by J, and consists

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

of the set of elements of K integral over R. As usual, by the *integral closure of an integral domain* will be meant the integral closure of that domain in its quotient field. For properties of integral closure the reader is referred to [5], Chapter 5, pages 254-264. The integral closure of R (in k) will be denoted by $\overline{R}$. It follows that $\overline{R} = J \cap k$ and that R is integrally closed if and only if $J \cap k = R$.

THEOREM 1. *If a is any non-zero element of K there exists a basis of K over k such that the representative matrix of a with respect to this basis is*

$$\mathrm{diag}(C,C,\ldots,C)$$

where C is the companion matrix of the minimal polynomial of a.

COROLLARY. *The field polynomial of any element a of K is a power of the minimal polynomial of a.*

Proof. See [4], page 8.

THEOREM 2. *The coefficients of the minimal polynomial of any element of J belong to $J \cap k$.*

Proof. See [5], Theorem 4, page 260.

COROLLARY. *If R is integrally closed the coefficients of the minimal polynomial of any element of J belong to R, i.e. J is equal to the set of elements whose minimal polynomial has coefficients in R.*

By the notation $\bigcup R_{\mathfrak{a}}$ or R_U will be meant the union of all bases $\mathfrak{a}$ of the coefficient domains $R_{\mathfrak{a}}$.

THEOREM 3. *$J = \bigcup R_{\mathfrak{a}}$ if and only if R is integrally closed.*

Proof. Suppose that $J = \bigcup R_{\mathfrak{a}}$. Then by P1, $J \cap k = R$. Hence R is integrally closed. Conversely, suppose R is integrally closed.

Let $c \in J$. By the Corollary to Theorem 2, the minimal polynomial of c has its coefficients in R. Therefore by Theorem 1, there exists a basis $\mathfrak{b}$ such that c is represented by the block diagonal matrix $\mathrm{diag}(C,C,\ldots,C)$ with respect to $\mathfrak{b}$, where C is the companion matrix of the minimal polynomial of c and therefore has all its elements in R. Hence $c \in R_{\mathfrak{b}}$ and so $J \subset \bigcup R_{\mathfrak{a}}$. But $\bigcup R_{\mathfrak{a}} \subset J$ by P5. Hence $J = \bigcup R_{\mathfrak{a}}$.

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

THEOREM 4. *For any basis* $\mathfrak{a}$ *the integral closure of* $R_{\mathfrak{a}}$ *is* J .

Proof. Let $b \in K$ be integral over $R_{\mathfrak{a}}$. But $R_{\mathfrak{a}} \subset J$ so b is integral over J and therefore by the transitivity of integral closure, $b \in J$. Hence the integral closure of $R_{\mathfrak{a}}$ is contained in J . Conversely, any element of J satisfies a monic polynomial with coefficients in $R \subset R_{\mathfrak{a}}$. Hence the integral closure of $R_{\mathfrak{a}}$ is J .

COROLLARY. $R_{\mathfrak{a}}$ *is integrally closed if and only if* $R_{\mathfrak{a}} = J$.

THEOREM 5. *If* R *is integrally closed and* K *is a separable extension of* k *then its integral closure* J *in* K *is contained in a basis* R*-module.*

Proof. See [5], Theorem 7, page 264.

COROLLARY. *If* K *is a separable extension of* k , J *is contained in a basis* $\overline{R}$*-module. In fact, if* $\mathfrak{a}$ *is any basis of* K *over* k *all of whose elements belong to* J , *and* $\mathfrak{b}$ *is the dual of* $\mathfrak{a}$ *then* $J \subset \overline{R}\,\mathfrak{b}$.

Proof. See [5], page 265.

We define $\overline{R}_{\mathfrak{a}}$ to be the set of elements $b \in K$ such that $ba_1, ba_2, \ldots, ba_n \in \overline{R}a = \overline{R}a_1 + \overline{R}a_2 + \ldots + \overline{R}a_n$ i.e. if $b \to B \in M_n(k)$ with respect to $\mathfrak{a}$ then we define b to lie in $R\mathfrak{a}$ if and only if $B \in M_n(R)$. As before, $\overline{R}_{\mathfrak{a}}$ is an integral domain and the following elementary properties hold:

P6. $\overline{R}_{\mathfrak{a}} \supset R_{\mathfrak{a}}$.

P7. $\overline{R}_{\mathfrak{a}} \cap k = \overline{R}$.

P8. $\overline{R}_{\mathfrak{a}} = \overline{R}_{\lambda\mathfrak{a}}$ *for any* $\lambda \in k_0$.

P9. $\overline{R}_{\mathfrak{a}} \subset J$.

P10. $\overline{R}_{\mathfrak{a}} = R_{\mathfrak{a}}$ *if and only if* $\overline{R} = R$, *i.e. if and only if* R *is integrally closed.*

Proof. If $\overline{R} = R$ the result is obvious. Suppose $\overline{R}_{\mathfrak{a}} = R_{\mathfrak{a}}$. Let

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

$\alpha \in \overline{R}$. Then since $\overline{R}_a \supset \overline{R}$ we have $\alpha \in \overline{R}_a$, i.e. $\alpha \in R_a$. Hence by P1, $\alpha \in R$. Thus $\overline{R} = R$.

THEOREM 6. $J = \cup \overline{R}_a$.

Proof. By P9, $J \supset \cup \overline{R}_a$.

Also if $b \in J$, then by Theorems 1 and 2 there exists a basis $\mathfrak{c}$ of K over k such that $b \in \overline{R}_{\mathfrak{c}}$.

Hence $J \subset \cup \overline{R}_a$ and so $J = \cup \overline{R}_a$.

2. Some examples and counter examples

The following subsets of J have already been defined

(i) R_M

(ii) $R_U = \cup R_a$

(iii) R_C .

We will be concerned also with R_G , being the ring generated by R_U . The following inclusion relations hold between these sets:

THEOREM 7. $R_M \subset R_U \subset R_C \subset J$.

Proof. $R_M \subset R_U$ by Theorem 1.

$R_U \subset R_C$ because the characteristic polynomial is obtained from any representative matrix.

$R_C \subset J$ by definition of J .

It will be shown by a later example that the second and third inclusions are, in general, strict. I have no counterexample to show that the first inclusion is not necessarily strict. Further the following examples will show that R_M , R_U , R_C may or may not be rings, and that the ring R_G may or may not be equal to J . In all the following examples R is taken as a non-integrally closed domain, for if R were integrally closed we would have $R_M = R_U = R_C = J$ by the Corollary to Theorem 2.

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

Square brackets denote polynomial extensions and round brackets denote the ratios of polynomials.

EXAMPLE 1. Take $R = Z[\sqrt{5}]$ where Z denotes the rational integers. Then its quotient field is $k = Q(\sqrt{5})$ where Q is the field of rational numbers. The integral closure $\overline{R}$ of R is $Z\left[\frac{1+\sqrt{5}}{2}\right]$. (See [2], Theorem 238, page 207.) Take $K = k(i) = Q(\sqrt{5},i) = Q(\sqrt{5}+i)$. Here $n = [K:k] = 2$. It is not difficult to show that K is a splitting field for the polynomial $x^4 - 8x^2 + 36$ and hence is a normal extension of Q. Further, J is equal to the set of elements of K satisfying monic *quartic* equations with rational integral coefficients.

Now let $b = \alpha + i\beta$, where $\alpha,\beta \in Q(\sqrt{5})$, be any element of K. Then $T(b) = 2\alpha$, $N(b) = \alpha^2 + \beta^2$, and hence $b \in J$ if and only if its trace and norm belong to $Z\left[\frac{1+\sqrt{5}}{2}\right]$. It can be shown that this is equivalent to $\alpha,\beta \in Z\left[\frac{1+\sqrt{5}}{2}\right]$. The proof is straightforward but long and arithmetical and will be omitted. Hence we have the following characterization of J:

THEOREM 8. *The integral closure J of $Z[\sqrt{5}]$ in $K = Q(\sqrt{5},i)$ is equal to the set of elements of the form $\alpha + i\beta$ where $\alpha,\beta \in Z\left[\frac{1+\sqrt{5}}{2}\right]$.*

Let $b = \alpha + i\beta \in R_a$ where $\alpha,\beta \in Q(\sqrt{5})$. Then if with respect to a, $b \to B = (\beta_{ij})$, all β_{ij} belong to $Z[\sqrt{5}]$. Hence $T(b)$, $N(b) \in R = Z[\sqrt{5}]$ and the minimum and field equations of b have coefficients in R. Conversely, suppose b is an element of K whose field equation has coefficients in $Z[\sqrt{5}]$, i.e. the trace and norm of b lie in $Z[\sqrt{5}]$. If $b = \alpha + i\beta \in Z[\sqrt{5}]$ then $\beta = 0$, $T(b) = 2\alpha$, $N(b) = \alpha^2$ and $b = \alpha \to \mathrm{diag}(\alpha,\alpha)$ with respect to any basis of K over k. If $\beta \neq 0$, $b \to \begin{pmatrix} 0 & 1 \\ -(\alpha^2+\beta^2) & 2\alpha \end{pmatrix}$ with respect to the basis $\{1,b\}$. Hence we have

THEOREM 9. *When $R = Z[\sqrt{5}]$ and $K = Q(\sqrt{5}+i)$, $\cup R_a$ consists of*

(i) the set of elements of K whose field equation has coefficients in $Z[\sqrt{5}]$,

(ii) the set of elements $\alpha + i\beta$ $(\alpha,\beta \in Q(\sqrt{5}))$ such that $2\alpha \in Z[\sqrt{5}]$ and $\alpha^2 + \beta^2 \in Z[\sqrt{5}]$.

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

Using Theorem 8 and Theorem 9 *(ii)* it can now be shown (proof omitted) that

THEOREM 10. *In the case where* $R = Z[\sqrt{5}]$ *and* $K = Q(\sqrt{5}+i)$, $\cup R_a$ *is a ring properly contained in* J .

Hence, in this example,

$$R_M = R_U = R_C \subsetneq J .$$

EXAMPLE 2. Take $R = Z[\sqrt{5}]$, $k = Q(\sqrt{5})$, $K = k(\omega)$ where ω is a primitive cube root of unity. It can be shown again that K is a normal extension of Q and that the integral closure J of $R = Z[\sqrt{5}]$ in $K = Q(\sqrt{5}+\omega)$ consists of the set of elements of K satisfying monic quartic equations with coefficients in Z . The K over k field polynomial of $a = \alpha + \omega\beta$ $(\alpha,\beta \in k)$ is $x^2 - (2\alpha-\beta)x + (\alpha^2+\beta^2-\alpha\beta)$ so that $T(a) = 2\alpha-\beta$, $N(a) = \alpha^2+\beta^2-\alpha\beta$. It now follows that if $\alpha,\beta \in Q(\sqrt{5})$ then $\alpha + \omega\beta \in J$ if and only if $2\alpha-\beta \in Z\left[\frac{1+\sqrt{5}}{2}\right]$ and $\alpha^2+\beta^2-\alpha\beta \in Z\left[\frac{1+\sqrt{5}}{2}\right]$. From this result a straightforward arithmetical proof can be given of:

THEOREM 11. *The integral closure* J *of* $Z[\sqrt{5}]$ *in* $K = Q(\sqrt{5},\omega)$ *consists of the set of elements of the form* $\alpha + \omega\beta$ *where* $\alpha,\beta \in Z\left[\frac{1+\sqrt{5}}{2}\right]$.

We also observe, in $K = k(\omega) = Q(\sqrt{5},\omega)$, $\cup R_a$ is the set of elements of K whose characteristic equation has coefficients in $Z[\sqrt{5}]$. Further the ring generated by $\cup R_a$ is equal to J :

$$a = \frac{1+\sqrt{5}}{2} + \omega\sqrt{5} \in \cup R_a$$

and

$$b = -\omega\sqrt{5} \in \cup R_a .$$

Hence $a + b \in R_G$, i.e. $\frac{1+\sqrt{5}}{2} \in R_G$.

Hence $Z\left[\frac{1+\sqrt{5}}{2}\right] \subset R_G$ and so by Theorem 11, $J \subset R_G$, i.e. $J = R_G$.
We have therefore shown that, in this example,

$$R_M = R_U = R_C \subsetneq J$$

https://doi.org/10.1017/S0004972700042234 Published online by Cambridge University Press

but

$$R_G = J \ .$$

EXAMPLE 3. Let $R = Z[\sqrt{2},\sqrt{5}]$. Then R is not integrally closed in its quotient field $k = Q(\sqrt{2},\sqrt{5}) = Q\left(\frac{1+\sqrt{5}}{\sqrt{2}}\right)$ since

$$\left(\frac{\sqrt{5}+1}{\sqrt{2}}\right)^2 = 3 + \sqrt{5} \ ,$$

and

$$\frac{\sqrt{5}+1}{\sqrt{2}} \notin Z[\sqrt{2},\sqrt{5}] \ .$$

If K is any extension of $k = Q(\sqrt{2},\sqrt{5})$ of even degree then $R_U \subsetneqq R_C$ because $\frac{1+\sqrt{5}}{\sqrt{2}} \notin R_U$ but the characteristic polynomial of $\frac{1+\sqrt{5}}{\sqrt{2}}$ is a power of $\left(x - \frac{1+\sqrt{5}}{\sqrt{2}}\right)^2$ i.e. of $x^2 - \sqrt{2}(1+\sqrt{5})x + (3+\sqrt{5})$.

References

[1] Z.I. Borevitch and I.R. Shafarevitch, *Number theory* (Academic Press, New York, 1966).

[2] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers* (Clarendon Press, Oxford, 1962).

[3] William Judson LeVeque, *Topics in number theory*, Vol. 2 (Addison-Wesley, Reading, Massachusetts, 1956).

[4] Hermann Weyl, *Algebraic theory of numbers* (Princeton University Press, Princeton, New Jersey, 1959).

[5] Oscar Zariski and Pierre Samuel, *Commutative algebra*, Vol. 1 (Van Nostrand, Princeton, New Jersey, 1965).

University of New South Wales,
Kensington, NSW.