ON INTEGRAL BASES

HENRY B. MANN

A commutative ring without zero divisors in which the ideal classes form a group is called a Dedekind ring. In such a ring every irreducible ideal is maximal and therefore a prime ideal and every ideal can be decomposed uniquely into prime ideals.

In all that follows $\mathfrak{F}$ will denote the quotient field of a Dedekind ring $\mathfrak{J}$, $\mathfrak{F}'$ a separable algebraic extension of degree n of $\mathfrak{F}$ and $\mathfrak{J}'$ the ring of all elements of $\mathfrak{F}'$ which satisfy monic equations with coefficients in $\mathfrak{J}$. The elements of $\mathfrak{J}$ and $\mathfrak{J}'$ will be called the integers of $\mathfrak{F}$ and $\mathfrak{F}'$ respectively.

A set of n elements $\omega_1, \cdots, \omega_n$ of $\mathfrak{J}'$ such that every element of $\mathfrak{J}'$ can be written in the form

$$x_1\omega_1 + \cdots + x_n\omega_n, \qquad x_i \in \mathfrak{J} \tag{1}$$

is called an integral basis of $\mathfrak{J}'$ over $\mathfrak{J}$ or of $\mathfrak{F}'$ over $\mathfrak{F}$. When no confusion can arise we shall call it for short an integral basis.

If every ideal in $\mathfrak{J}$ is principal then every ideal of $\mathfrak{J}'$ has an integral basis over $\mathfrak{J}$ [4, vol. 2, p. 81 bottom]. In this paper we are interested in finding necessary and sufficient conditions for a field $\mathfrak{F}'$ to have an integral basis over a field $\mathfrak{F}$. Our goal is to find necessary and sufficient conditions which can be given in terms of the ideal decomposition and of congruence relations in $\mathfrak{F}$. A complete solution of this problem will be given for the case that $\mathfrak{F}'$ is a quadratic extension of $\mathfrak{F}$. From our results it will be seen that the condition that every ideal of $\mathfrak{J}$ is principal is also necessary if every algebraic extension of $\mathfrak{F}$ is to have a relative integral basis over $\mathfrak{F}$.

Let $\mathfrak{a}$ be an ideal of $\mathfrak{J}'$. If there exist integers $\alpha_1, \alpha_2, \cdots, \alpha_n$ in $\mathfrak{a}$ such that every integer in $\mathfrak{a}$ can be written in the form

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n, \qquad x_i \in J \tag{2}$$

then $\alpha_1, \cdots, \alpha_n$ is called a module basis of $\mathfrak{a}$ over $\mathfrak{J}$. The words over $\mathfrak{J}$ will be deleted if no confusion can arise. The question whether $\mathfrak{J}'$ has an integral basis over $\mathfrak{J}$ must be distinguished from the question whether a given ideal $\mathfrak{a}$ in $\mathfrak{J}'$ has a module basis over $\mathfrak{J}$. Indeed if $\mathfrak{J}'$ has an integral basis over $\mathfrak{J}$ and $\mathfrak{A}$ is an ideal of $\mathfrak{J}'$ generated by an ideal $\mathfrak{a}$ in $\mathfrak{J}$ then $\mathfrak{A}$ has a module basis if and only if $\mathfrak{a}^n$ is principal [5, p. 21].

Presented to the Society, August 27, 1957; received by the editors October 7, 1956 and, in revised form, May 10, 1957.

The definition of relative norm, different and discriminant used in this paper is that given in Chapter 12 of [2]. The notation used there will also be used in this paper except that different and discriminant will always be taken in $\mathfrak{F}'$ over $\mathfrak{F}$.

THEOREM 1. *Let* $\mathfrak{a}$ *be an ideal of* $\mathfrak{J}'$. *If* $\mathfrak{a}$ *has the module basis* $\alpha_1, \cdots, \alpha_n$ *then*

$$\begin{vmatrix} \alpha_1 & , \cdots , & \alpha_n \\ \alpha_1^{(2)} & , \cdots , & \alpha_n^{(2)} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_1^{(n)} & , \cdots , & \alpha_n^{(n)} \end{vmatrix} = N(\mathfrak{a})\mathfrak{D}^{1/2} \tag{3}$$

where $\mathfrak{D}$ *denotes the discriminant of* $\mathfrak{F}'$ *over* $\mathfrak{F}$ *and Equation* (3) *is to be read as an equation between ideals.*

Theorem 1 is well known in the case that $\mathfrak{F}$ is the field of rational numbers. A proof of Theorem 1 would also result from a suitable modification of Lemmas 1 and 4, §8, Chapter IV of [6]. We shall give here a proof which is entirely self-contained.

To prove Theorem 1 we shall first show: *If* $\alpha_1, \cdots, \alpha_n$ *are any* n *numbers of the ideal* $\mathfrak{a}$ *then*

$$|\alpha_i^{(k)}|^2 = \begin{vmatrix} \alpha_1 & , \cdots , & \alpha_n \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_1^{(n)} & , \cdots , & \alpha_n^{(n)} \end{vmatrix}^2 \equiv 0 \pmod{N^2(\mathfrak{a})\mathfrak{D}}. \tag{4}$$

PROOF. Let $\mathfrak{d}$ be the different of $\mathfrak{F}'$ over $\mathfrak{F}$ then $\mathfrak{D} = N(\mathfrak{d})$. Let α be any number of the ideal $(\mathfrak{a}^2\mathfrak{d})^{-1}$. We have

$$N(\alpha)\,|\alpha_i^{(k)}|\,|\alpha_i^{(k)}|^t = |\alpha^{(k)}\alpha_i^{(k)}|\,|\alpha_i^{(k)}|^t = T(\alpha\alpha_i\alpha_j),$$

where T denotes the trace in $\mathfrak{F}'$ over $\mathfrak{F}$. But $\alpha\alpha_i\alpha_j$ is in the ideal $(\mathfrak{d})^{-1}$ and hence its trace is integral. This proves (4).

Suppose now that $\alpha_1, \cdots, \alpha_n$ is a basis of the ideal $\mathfrak{a}$ and that $|\alpha_i^{(k)}| \equiv 0 \pmod{\mathfrak{p}N^2(\mathfrak{a})\mathfrak{D}}$, where $\mathfrak{p}$ is a prime ideal. Choose $\alpha = \mathfrak{c}(\mathfrak{a}^2\mathfrak{d})^{-1}$ where $(\mathfrak{c}, \mathfrak{p}\mathfrak{a}^2\mathfrak{d}) = 1$. Then $|T(\alpha\alpha_i\alpha_j)| \equiv 0 \pmod{\mathfrak{p}}$ and we can solve in $\mathfrak{J}$ nontrivially the congruences

$$\sum x_j T(\alpha\alpha_i\alpha_j) \equiv 0 \pmod{\mathfrak{p}}.$$

Put

$$\omega = \sum_{j=1}^{n} x_j \alpha_j,$$

then

$$T(\omega\alpha\alpha_i) \equiv 0 \pmod{\mathfrak{p}}$$

and for any choice $y_1, \cdots, y_n$ in $\mathfrak{J}$

$$T\left(\omega\alpha \sum_{i=1}^{n} \alpha_i y_i\right) \equiv 0 \pmod{\mathfrak{p}}.$$

Thus for every $\xi \in \mathfrak{a}$ we have $T(\omega\alpha\xi) \equiv 0 \pmod{\mathfrak{p}}$. Let π be an arbitrary number in the ideal $(\mathfrak{p})^{-1}$. Then $T(\pi\omega\alpha\xi) \equiv 0 \pmod 1$ and hence

$$\pi\omega\alpha \in (\mathfrak{a}\mathfrak{d})^{-1}. \tag{5}$$

The relation (5) implies

$$\omega\mathfrak{c}(\mathfrak{p}\mathfrak{a}^2\mathfrak{d})^{-1} \subset (\mathfrak{a}\mathfrak{d})^{-1}$$

and since $(\mathfrak{c}, \mathfrak{a}\mathfrak{p}) = 1$ we find

$$\omega = \sum_{j=1}^{n} x_j \alpha_j \equiv 0 (\mathfrak{a}\mathfrak{p})$$

where not all the x_j are divisible by $\mathfrak{p}$. Let π be in $\mathfrak{F}$ and have ideal denominator $\mathfrak{p}$ then

$$\beta = \sum_{j=1}^{n} x_j \pi\, \alpha_j = \sum_{j=1}^{n} z_j \alpha_j \in \mathfrak{a},\ z_j \in \mathfrak{F},$$

while not all the z_j are integers. But this contradicts the hypothesis that $\alpha_1, \cdots, \alpha_n$ is a module basis of $\mathfrak{a}$. This proves Theorem 1.

COROLLARY. *If $\mathfrak{a}$ is any ideal of $\mathfrak{F}'$ and $\alpha_1, \cdots, \alpha_n$ are n numbers of $\mathfrak{a}$ such that $\left|\alpha_i^{(k)}\right| = N(\mathfrak{a})\mathfrak{D}^{1/2}$ then $\alpha_1, \cdots, \alpha_n$ are a module basis of $\mathfrak{a}$.*

PROOF. Let $\alpha \in \mathfrak{a}$. Since $\left|\alpha_i^{(k)}\right| \neq 0$ we have $\alpha = \sum_{j=1}^{n} x_j\alpha_j$, $x_j \in \mathfrak{F}$. Computing x_j we get

$$x_j = \begin{vmatrix} \alpha_1 & , \cdots, & \alpha_{j-1}, & \alpha & , \cdots, & \alpha_n \\ \cdot & & & & & \\ \cdot & & & & & \\ \cdot & & & & & \\ \alpha_1^{(n)} & , \cdots, & \alpha_{j-1}^{(n)}, & \alpha^{(n)} & , \cdots, & \alpha_n^{(n)} \end{vmatrix} (N(\mathfrak{a})\mathfrak{D}^{1/2})^{-1}.$$

From (4) we see that x_j is integral and therefore $\alpha_1, \cdots, \alpha_n$ a module basis of $\mathfrak{a}$.

We shall now consider quadratic extensions.

THEOREM 2. *Let $\mathfrak{F}$ have characteristic different from 2 and let $\mathfrak{F}'$ be a quadratic extension of $\mathfrak{F}$. The field $\mathfrak{F}'$ has an integral basis over $\mathfrak{F}$ if and only if $\mathfrak{F}'=\mathfrak{F}(D^{1/2})$ where (D) is the discriminant of $\mathfrak{F}'$ over $\mathfrak{F}$.*

PROOF. Let $F'=F(a^{1/2})$. Suppose that $x_1+x_2a^{1/2}$, $y_1+y_2a^{1/2}$, is an integral basis, then by Theorem 1

$$\left(\begin{vmatrix} x_1+x_2a^{1/2}, & y_1+y_2a^{1/2} \\ x_1-x_2a^{1/2}, & y_1-y_2a^{1/2} \end{vmatrix}\right) = (D^{1/2}),$$

where (D) is the discriminant of $\mathfrak{F}'$ over $\mathfrak{F}$. This gives

$$D^{1/2} = 2a^{1/2}(y_1x_2 - x_1y_2), \qquad y_i, x_i \in \mathfrak{F}. \tag{6}$$

Hence $\mathfrak{F}'=\mathfrak{F}(D^{1/2})$.

On the other hand let $\mathfrak{F}'=\mathfrak{F}(D^{1/2})$. We then have $T(\alpha/D^{1/2})=x_\alpha$, where x_α is an integer in $\mathfrak{F}$. Let the x_α have g.c.d. $\mathfrak{a}$ and let a have ideal denominator $\mathfrak{a}$. Then $T(\alpha a/D^{1/2})\equiv 0 \pmod 1$ for all α and therefore $\mathfrak{d}\equiv 0 \pmod{\mathfrak{a}\mathfrak{d}}$, $\mathfrak{a}=(1)$. Thus we have for any $\alpha\in\mathfrak{F}'$, $T(\alpha/D^{1/2})=\alpha/D^{1/2}-\alpha^{(2)}/D^{1/2}=x_\alpha$, where the set of all x_α generates the unit ideal. Thus there exist numbers $\alpha_1, \cdots, \alpha_m$ in $\mathfrak{F}'$ and $x_1, \cdots, x_m$ in $\mathfrak{F}$ such that

$$x_1(\alpha_1 - \alpha_1^{(2)}) + \cdots + x_m(\alpha_m - \alpha_m^{(2)}) = D^{1/2}.$$

Considering this equation mod 2 we see that

$$D^{1/2} \equiv b \pmod 2, \qquad b \in \mathfrak{J}, \tag{7}$$

Hence $(b+D^{1/2})/2$ is an integer and

$$\begin{vmatrix} 1, & \dfrac{b-D^{1/2}}{2} \\ 1, & \dfrac{b+D^{1/2}}{2} \end{vmatrix} = D^{1/2}.$$

By the Corollary to Theorem 1 this shows that 1, $(b+D^{1/2})/2$ is a basis of $\mathfrak{F}'$ over $\mathfrak{F}$.

THEOREM 3. *Let $\mathfrak{F}'=\mathfrak{F}(a^{1/2})$. Let $(a)=\mathfrak{a}^2\mathfrak{c}$ and $\mathfrak{D}=\mathfrak{d}_1^2\mathfrak{c}'$ where $\mathfrak{c}$ and $\mathfrak{c}'$ are square free. The extension $\mathfrak{F}'$ has an integral basis over $\mathfrak{F}$ if and only if $\mathfrak{c}=\mathfrak{c}'$, $\mathfrak{a}\sim\mathfrak{d}_1$ ($\sim$ indicates equivalence).*

PROOF. If our condition is fulfilled then clearly $\mathfrak{D}=(D)$ where $D\in F$ and $F'=F(a^{1/2})=F(D^{1/2})$ hence F' has an integral basis by

Theorem 2. On the other hand if $F' = F(D^{1/2})$ then

$$a^{1/2} = x + yD^{1/2}, \qquad y \neq 0. \tag{8}$$

Squaring (8) it follows that $x = 0$, hence

$$\mathfrak{a}^2\mathfrak{c} = y^2\mathfrak{b}_1^2\mathfrak{c}'.$$

The square free parts on both sides must coincide and hence $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{a} \sim \mathfrak{b}_1$.

It is possible to compute the discriminant of $\mathfrak{F}(a^{1/2})$ from the ideal decomposition of $\mathfrak{a}$ and from congruence relations satisfied by a modulo the powers of the prime factors of 2 in $\mathfrak{F}$. Thus the criterion of Theorem 3 requires only the knowledge of the ideal decompositions and of congruence relations in $\mathfrak{F}$.

We now use ideal classes defined by a module $\mathfrak{m}$. The ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent (mod $\mathfrak{m}$) if $\mathfrak{a} = x\mathfrak{b}$ with $X \equiv 1 \pmod{\mathfrak{m}}$. This refinement of the concept of equivalence was introduced by Takagi [3]. The ideals which are relatively prime to $\mathfrak{m}$ are divided into equivalence classes and these ideal classes mod $\mathfrak{m}$ form a group.

THEOREM 4. *If $\mathfrak{F}$ has characteristic different from two and if $\mathfrak{F}$ contains an ideal which is not principal then there exists a quadratic extension of $\mathfrak{F}$ which has no integral basis over $\mathfrak{F}$.*

Theorem 4 follows from the following lemma.

LEMMA. *If $\mathfrak{F}$ contains an ideal which is not principal then there exists a number α such that $(\alpha, 2) = 1$, $\alpha \equiv \beta^2 \pmod 4$, $\beta \in \mathfrak{F}$, $\alpha = \mathfrak{b}^2\mathfrak{c}$, where $\mathfrak{c}$ is square free and $\mathfrak{b}$ not principal.*

PROOF. Let $\mathfrak{a}'$ be an ideal which is not principal. We can choose $\mathfrak{a}$ so that $\mathfrak{a} \sim \mathfrak{a}'$, $(\mathfrak{a}, 2) = 1$. Let $\mathfrak{p}$ be a prime factor of $\mathfrak{a}$ which is not principal and choose $\mathfrak{a}_1$, $\mathfrak{a}_2$ in the inverse class mod 4 of $\mathfrak{p}$ and so that $(\mathfrak{a}, \mathfrak{a}_1) = (\mathfrak{a}, \mathfrak{a}_2) = (\mathfrak{a}_1, \mathfrak{a}_2) = 1$. Let $\mathfrak{a}_1 = \mathfrak{b}_1^2\mathfrak{c}_1$, $\mathfrak{a}_2 = \mathfrak{b}_2^2\mathfrak{c}_2$. If $\mathfrak{b}_1$ or $\mathfrak{b}_2$ are not principal then $\mathfrak{p}\mathfrak{a}_1$ or $\mathfrak{p}\mathfrak{a}_2$ are principal and fulfill the conditions of our lemma and if $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are both principal then $\mathfrak{p}^2\mathfrak{c}_1\mathfrak{c}_2$ does.

Theorem 4 now follows easily because if $(\alpha) = \mathfrak{a}^2\mathfrak{c}$ where $\mathfrak{a}$ is not principal $(\alpha, 2) = 1$ and $\alpha \equiv \beta^2 \pmod 4$, then the discriminant of $\mathfrak{F}(\alpha^{1/2})$ is $\mathfrak{c}$ [1, §39] and by Theorem 3 the field $\mathfrak{F}(\alpha^{1/2})$ has no integral basis.

COROLLARY. *Every algebraic extension of $\mathfrak{F}$ has an integral basis if and only if every ideal of $\mathfrak{F}$ is principal.*

The sufficiency of the condition is well known. The necessity follows from Theorem 4.

THEOREM 5. *Let $\mathfrak{F}$ be of characteristic 2, $\mathfrak{F}'$ a quadratic extension of $\mathfrak{F}$. The field $\mathfrak{F}'$ has an integral basis over $\mathfrak{F}$ if and only if $\mathfrak{d}$ is a principal ideal of the groundfield.*

Let $a_1\alpha+b_1$, $a_2\alpha+b_2$ be an integral basis. By Theorem 1 we have

$$\left(\begin{vmatrix} a_1\alpha + b_1, & a_2\alpha + b_2 \\ a_1\alpha^{(2)} + b_1, & a_2\alpha^{(2)} + b_2 \end{vmatrix}\right) = (\alpha + \alpha^{(2)})(b_1a_2 + a_1b_2) = \mathfrak{d}$$

and this proves the necessity of the condition. On the other hand let $\mathfrak{d}=(d)$ where $d\in\mathfrak{J}$. By the definition of d if α is any integer in $\mathfrak{F}'$ then $T(d^{-1}\alpha)=x_\alpha$ where the x_α have g.c.d. (1). Hence there is an integer α such that $\alpha+\alpha^{(2)}=d$ and it follows from the corollary to Theorem 1 that 1, α is a basis for the integers.

REFERENCES

1. E. Hecke, *Vorlesungen ueber die Theorie der algebraischen Zahlen*, New York, Chelsea Publishing Co., 1948.

2. H. B. Mann, *Introduction to algebraic number theory*, Columbus, Ohio State University Press, 1955.

3. T. Takagi, *Ueber eine Theorie des relativ Abelschen Zahlkoerpers*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I vol. 41, Art. 9.

4. B. L. van der Waerden, *Moderne algebra*, Berlin, Springer-Verlag, 1950.

5. C. Chevalley, *L'arithmetic dans les algèbres de matrices*, Actualités Scientifiques et Industrielles, no. 323, Paris, 1936.

6. ———, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, no. 6, 1951.

OHIO STATE UNIVERSITY