COLLOQUIUM MATHEMATICUM

VOL. XLVIII 1984 FASC. 2

SUBMODULES OF A TORSION-FREE AND FINITELY GENERATED MODULE OVER A DEDEKIND RING

BY

G. ARCHINARD (GENEVA)

1. Introduction. Let A be a Dedekind ring, K its quotient field, M a torsion-free and finitely generated A-module, and let KM denote the tensor product $K \otimes_A M$, which is a vector space of finite dimension over K.

Definition 1. The *rank* of M is the dimension of KM.

Let m be the rank of M and let $(\alpha_i)_{i=1,\ldots,m}$ be a basis of KM; we consider the sets

$$I_i = \{x \in K \mid \mu + x\alpha_i \in M \text{ for some } \mu \in K\alpha_1 + \ldots + K\alpha_{i-1}\}.$$

Clearly, these sets depend on the order of the basis elements α_i and are non-zero fractional ideals of A (cf. [3]).

Definition 2. The sets I_i $(i = 1, \ldots, m)$ are the *ideals associated with M for the basis* (α_i).

In the same manner we define the ideals J_i $(i = 1, \ldots, m)$ associated with a submodule N of M for the basis (α_i) of M. Each such J_i is an ideal contained in I_i and we have $J_i \neq (0)$ for $i = 1, \ldots, m$ if and only if the ranks of N and M are equal.

In Section 2, we prove a theorem of Artin's and recall some other results obtained by Artin in [1]. Our proof is much more detailed than that given in [1] because we need the details for later applications.

In Sections 3 and 4, we use associated ideals to express the index of a submodule and to give an upper bound on the number of submodules of a given index.

In Section 5, we first establish a connexion between the associated ideals and the discriminant of a module. It seems to us that this result (Lemma 5) and those of Sections 3 and 4 are new. Then, in Theorems 4 and 5 and in Corollaries 3 and 4, for the modules considered in this section we obtain some results which are well known if these modules are rings of algebraic integers. Our proofs use only elementary calculation with ideals in a Dedekind ring, whereas the proofs for rings of algebraic integers are usually obtained by localization arguments.

2. A theorem of Artin's.

THEOREM 1 (cf. [1]). *Let M be a torsion-free and finitely generated module over a Dedekind ring A of rank m and let I_i be the ideals associated with M for a basis (β_i) of KM over K, where K is the quotient field of A. Then there exists a basis (α_i) of KM over K such that $M = I_1\alpha_1 + \ldots + I_m\alpha_m$.*

Proof. By definition, $M \cap K\beta_1 = I_1\beta_1$, and if $m = 1$, this establishes the theorem with $\alpha_1 = \beta_1$.

For the case $m \geqslant 2$, we use induction: we let $\alpha_1 = \beta_1$ and we assume the existence of numbers $\alpha_j \in KM$, $j = 1, \ldots, i-1$ $(2 \leqslant i \leqslant m)$, linearly independent over K and such that conditions

$$M \cap (K\alpha_1 + \ldots + K\alpha_{i-1}) = I_1\alpha_1 + \ldots + I_{i-1}\alpha_{i-1}, \tag{1}$$

$$K\alpha_1 + \ldots + K\alpha_{i-1} = K\beta_1 + \ldots + K\beta_{i-1} \tag{2}$$

are satisfied. Then we construct a number $\alpha_i \in KM$ such that (1) and (2) are satisfied when $i-1$ is replaced by i.

For this purpose we consider $a_1, \ldots, a_r \in I_i$ and $b_1, \ldots, b_r \in I_i^{-1}$ such that $a_1 b_1 + \ldots + a_r b_r = 1$. For every $l = 1, 2, \ldots, r$, there is some $\mu_l \in K\beta_1 + \ldots + K\beta_{i-1}$ such that $\mu_l + a_l\beta_i \in M$. We take

$$\alpha_i = \sum_{l=1}^{r} b_l(\mu_l + a_l\beta_i).$$

First, we prove that $I_i\alpha_i \subset M$. Indeed, for $x \in I_i$ we have $xb_l \in A$ since $b_l \in I_i^{-1}$, and $xb_l(\mu_l + a_l\beta_i) \in M$ since $\mu_l + a_l\beta_i \in M$. This proves the above inclusion.

Now, (1) is assumed to be true by hypothesis. We have then

$$M \supset I_1\alpha_1 + \ldots + I_{i-1}\alpha_{i-1}$$

and, by the preceding result,

$$M \supset I_1\alpha_1 + \ldots + I_i\alpha_i.$$

This implies

$$M \cap (K\alpha_1 + \ldots + K\alpha_i) \supset I_1\alpha_1 + \ldots + I_i\alpha_i.$$

To prove the converse inclusion, let us consider

$$v \in M \cap (K\alpha_1 + \ldots + K\alpha_i).$$

We have then $v = \mu + x\alpha_i \in M$, where $\mu \in K\alpha_1 + \ldots + K\alpha_{i-1}$ and $x \in K$. By construction,

$$x\alpha_i = x\sum_{l=1}^{r} b_l\mu_l + x\sum_{l=1}^{r} b_l a_l\beta_i = \mu' + x\beta_i,$$

where $\mu' \in K\beta_1 + \ldots + K\beta_{i-1}$.

Because of condition (2), which is assumed to be true by hypothesis, we have also $\mu \in K\beta_1 + \ldots + K\beta_{i-1}$, and then

$$v = \mu'' + x\beta_i, \quad \text{where } \mu'' = \mu + \mu' \in K\beta_1 + \ldots + K\beta_{i-1}.$$

By the definition of I_i, $x \in I_i$. Then $x\alpha_i \in M$, as we established above. Hence the condition $v = \mu + x\alpha_i \in M$ implies $\mu \in M$ and we have $\mu \in M \cap (K\alpha_1 + \ldots + K\alpha_{i-1})$. From (1) we obtain $\mu \in I_1\alpha_1 + \ldots + I_{i-1}\alpha_{i-1}$ and, finally, we have $v \in I_1\alpha_1 + \ldots + I_i\alpha_i$, which establishes the inclusion

$$M \cap (K\alpha_1 + \ldots + K\alpha_i) \subset I_1\alpha_1 + \ldots + I_i\alpha_i.$$

Thus, condition (1) is satisfied for i.

Obviously, condition (2) is also satisfied for i. By induction, these conditions are satisfied for m and, consequently, the equality $M = I_1\alpha_1 + \ldots + I_m\alpha_m$ holds.

Remark. Artin [1] considers a Dedekind ring A, its quotient field K, a vector space V of finite dimension over K, and establishes the theorem for an A-submodule M of V such that $aM \subset A\omega_1 + \ldots + A\omega_m$ for some $a \in A$ and some basis $(\omega_i)_{i=1,\ldots,m}$ of V. (The existence of some a for which this inclusion is satisfied does not depend on the choice of the basis (ω_i).) Obviously, such a submodule is a torsion-free and finitely generated A-module. Our proof of Theorem 1 is more detailed but essentially the same as that given by Artin and, in fact, Theorem 1 can be used to prove, in turn, that a torsion-free and finitely generated A-module M satisfies the above-described property for the vector space KM. Indeed, M is an A-submodule of KM and from the formula $M = I_1\alpha_1 + \ldots + I_m\alpha_m$, established in Theorem 1, we deduce easily that $aM \subset A\alpha_1 + \ldots + A_m\alpha_m$ for some $a \in A$.

We give now, without proof, some results which Artin established in [1] and which we will use in Section 5. (The proofs are based on elementary properties of the ideals in a Dedekind ring.)

PROPERTY 1. *The basis (α_i) in Theorem 1 can be chosen in such a manner that $m-1$ of the ideals I_i are arbitrarily prescribed.*

PROPERTY 2. *If I_i and I_i' are the ideals associated with M for the respective bases (α_i) and (α_i'), then*

$$\prod_{i=1}^{m} I_i = d \prod_{i=1}^{m} I_i'$$

with some $d \in K$.

That means that the class of the product of the associated ideals is independent of the chosen basis: this is the *Steinitz class* of M.

From these two properties, one deduces easily the following

PROPERTY 3. *A torsion-free and finitely generated module over a Dedekind ring is free if and only if its Steinitz class is the class of principal ideals.*

3. Application of Artin's theorem to the case of a submodule.

COROLLARY 1. *Let M be a torsion-free and finitely generated A-module of rank m, N a submodule of M, and I_i (respectively, J_i) the ideals associated with M (respectively, N) for a basis (β_i) of KM over K. Then the following index formula holds:*

$$(M : N) = \sum_{i=1}^{m} (I_i : J_i).$$

Proof. Theorem 1 furnishes a basis (α_i) of KM over K such that $M = I_1 \alpha_1 + \dots + I_m \alpha_m$ and it is easily seen that the ideals I_i and J_i are associated with M and N for this new basis.

Now, let $x_i^{(l_i)}$ be a representative system of the classes of I_i modulo J_i, $i = 1, \dots, m$. Then a simple calculation will show that every class of M modulo N has one and only one representative of the form $x_1^{(l_1)} \alpha_1 + \dots + x_m^{(l_m)} \alpha_m$. This establishes the announced formula.

THEOREM 2. *Let M be a torsion-free and finitely generated A-module of rank m, $(\alpha_i)_{i=1,\dots,m}$ a basis of KM, and I_i $(i = 1, \dots, m)$ ideals of A such that $M = I_1 \alpha_1 + \dots + I_m \alpha_m$.*

Then if N is a submodule of M, of rank m, whose associated ideals for (α_i) are J_i, $i = 1, \dots, m$, then there is a basis (β_i) of KM for which $N = J_1 \beta_1 + \dots + J_m \beta_m$ and which is obtained from (α_i) through a matrix $C = (c_{ik})$ $((\beta_i) = C(\alpha_i))$ satisfying the conditions

$$c_{ik} = \begin{cases} 0 & \text{for } i < k, \\ 1 & \text{for } i = k, \end{cases} \qquad c_{ik} \in J_i^{-1} I_k \quad \text{for } i > k. \tag{3}$$

(As mentioned in the Introduction, the obvious conditions $J_i \subset I_i$ $(i = 1, \dots, m)$ are also satisfied.)

Conversely, if J_i are non-zero ideals of A such that $J_i \subset I_i$ $(i = 1, \dots, m)$ and if $(\beta_i) = C(\alpha_i)$ for a matrix C satisfying (3)*, then $J_1 \alpha_1 + \dots + J_m \alpha_m$ is a submodule of M whose associated ideals for (α_i) are J_i.*

Proof. From the proof of Theorem 1 we deduce that $N = J_1 \beta_1 + \dots + J_m \beta_m$ for some $\beta_1 = \alpha_1$ and $\beta_i = \sum_{l=1} b_l \mu_l + \alpha_i$ $(i = 2, \dots, m)$ with $b_l \in J_i^{-1}$ and $\mu_l \in K\alpha_1 + \dots + K\alpha_{i-1}$ such that $\mu_l + a_l \alpha_i \in N$ for some $a_l \in J_i$. We have then

$$\mu_l = x_{l1} \alpha_1 + \dots + x_{l,i-1} \alpha_{i-1} \in M, \quad \text{where } x_{lk} \in I_k.$$

Hence we can write

$$\beta_i = \sum_{k=1}^{m} c_{ik} \alpha_k,$$

where $c_{ik} = \sum_{l=1}^{r} b_l x_{lk} \in J_i^{-1} I_k$ for $i < k$, $c_{ii} = 1$, and $c_{ik} = 0$ for $i > k$. This proves the direct assertion. The converse is immediate.

Remark. The assertion of Theorem 2 is somewhat similar to that of the *invariant factors theorem* ([2], Section 22). However, Theorem 2 gives an expression for the module M which is independent of the choice of the submodule N and, therefore, it can be used for the study of all the submodules of M, while, in the invariant factors theorem, the expression for M depends on the chosen submodule.

4. Submodules with the same associated ideals for a given basis. Let M be of rank m, (α_i) a basis of KM over K, I_i ideals of A such that $M = I_1 \alpha_1 + \dots + I_m \alpha_m$, and J_i ideals such that $J_i \subset I_i$. Let $C = (c_{ij})$ and $C' = (c'_{ij})$ be two matrices satisfying conditions (3) relatively to the ideals I_i and J_i and let $(\beta_i) = C(\alpha_i)$ and $(\beta'_i) = C'(\alpha_i)$.

We first establish some technical results which enable us to give a sufficient condition for the submodules $J_1 \beta_1 + \dots + J_m \beta_m$ and $J_1 \beta'_1 + \dots$ $\dots + J_m \beta'_m$ to be equal.

Then we give an upper bound for the number of submodules of M which have the ideals J_i as associated ideals for (α_i).

Lastly, we assume that the number of ideals with a given finite index in A is finite and, under this obviously necessary condition, we prove that the number of submodules of a given finite index is also finite.

LEMMA 1. *Let $B = (b_{ik})$, $i, k = 1, \dots, m$, be a matrix with components in K such that $b_{ii} = 1$ and $b_{ik} = 0$ for $i > k$. Let x_i be the coordinates of a vector $x \in K^m$, y_i those of $y = Bx$, and let $I_i \neq (0)$, $i = 1, \dots, m$, be ideals of A. Then the following three properties are equivalent*:

$$x_i \in I_i \text{ for } i = 1, \dots, m \Rightarrow y_i \in I_i \text{ for } i = 1, \dots, m, \tag{4}$$

$$y_i \in I_i \text{ for } i = 1, \dots, m \Rightarrow x_i \in I_i \text{ for } i = 1, \dots, m, \tag{5}$$

$$b_{ik} \in I_i I_k^{-1}, \quad 1 \leqslant i < k < m. \tag{6}$$

Proof. We use the equality $y = Bx$ in the form

$$y_i = x_i + b_{i,i+1} x_{i+1} + \dots + b_{im} x_m, \quad i = 1, \dots, m.$$

To prove (6)$\Rightarrow$(5) we consider $y_i \in I_i$, $i = 1, \dots, m$. Then, of course, $x_m = y_m \in I_m$. As the induction hypothesis we suppose $x_k \in I_k$ for $k = i+1, \dots, m$ $(1 < i \leqslant m)$. Then, from (6) we have $b_{ik} x_k \in I_i$, and hence

$$x_i = y_i - b_{i,i+1} x_{i+1} - \dots - b_{im} x_m \in I_i.$$

Therefore (5) is satisfied.

Using similar arguments, one proves easily also (5)$\Rightarrow$(6) and (4)$\Leftrightarrow$(6).

LEMMA 2. *Let* $C = (c_{ik})$ *and* $C' = (c'_{ik})$ *be* $(m\times m)$*-matrices such that* $c'_{ik} = c_{ik} = 0$ *for* $i<k$ *and* $c'_{ii} = c_{ii} = 1$ *and let* $(d_{ik}) = C'C^{-1}$. *Then* $d_{ik} = 0$ *for* $i<k$, $d_{ik} = 1$ *for* $i=k$, *and*

$$d_{ik} = \sum_{j=k}^{i} (c'_{ij}-c_{ij})A_{jk} \quad \text{for } i>k,$$

where $A_{kk} = 1$ *and, for* $j>k$,

$$(7)\qquad A_{jk} = (-1)^{j-k}\begin{vmatrix} c_{k+1,k} & 1 & 0 & \dots 0 & 0 \\ c_{k+2,k} & c_{k+2,k+1} & 1 & \dots 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ c_{j-2,k} & c_{j-2,k+1} & c_{j-2,k+2} & \dots 1 & 0 \\ c_{j-1,k} & c_{j-1,k+1} & c_{j-1,k+2} & \dots c_{j-1,j-2} & 1 \\ c_{j,k} & c_{j,k+1} & c_{j,k+2} & \dots c_{j,j-2} & c_{j,j-1} \end{vmatrix}.$$

Proof. This is a manner of writing $C'C^{-1}$, when C and C' satisfy the above hypothesis.

LEMMA 3. *Let* I_i *and* J_i *be non-zero ideals of* A *with* $I_i \supset J_i$, $i = 1, \dots, m$, *let* $c_{ik} \in J_i^{-1} I_k$ *for* $i>k$, *and let* $H_j = J_i I_i^{-1}$. *Then*

$$A_{jk} \in J_j^{-1} H_{j-1}^{-1} \dots H_{k+1}^{-1} I_k \quad \text{for } j>k,$$

where A_{jk} *are the numbers defined in Lemma* 2.

Proof. The expansion of the determinant given in formula (7) yields

$$(8)\qquad A_{jk} = -\sum_{l=k}^{j-1} c_{jl} A_{lk} \quad \text{for } j>k.$$

Then we fix k $(1 \leqslant k \leqslant m-1)$ and proceed by induction on j from $k+1$ to m.

For $j = k+1$ we have $A_{k+1,k} = -c_{k+1} \in J_{k+1}^{-1} I_k$.

We now assume $A_{lk} \in J_l^{-1} H_{l-1}^{-1} \dots H_{k+1}^{-1} I_k$ for $l = k+1, \dots, j-1$. Then

$$c_{jl} A_{lk} \in J_j^{-1} H_l^{-1} \dots H_{k+1}^{-1} I_k.$$

From the inclusion $I_i \supset J_i$ we infer that H_i is an integral ideal, and hence

$$c_{jl} A_{lk} \in J_j^{-1} H_{j-1}^{-1} \dots H_{k+1}^{-1} I_k.$$

The proof is completed by using formula (8).

LEMMA 4. *Let* M *be a torsion-free and finitely generated* A*-module of rank* m, (α_i) *be a basis of* KM *over* K, I_i *be ideals of* A *such that* $J_i \subset I_i$, *and let* $C = (c_{ik})$ *and* $C' = (c'_{ik})$ *be* $(m\times m)$*-matrices satisfying*

$$(3')\qquad c_{ik} = c'_{ik} = 0 \text{ for } i<k, \quad c_{ii} = c'_{ii} = 1, \quad c_{ik}, c'_{ik} \in J_i^{-1} I_k \text{ for } i>k.$$

Moreover, let $(\beta_i) = C(\alpha_i)$ *and* $(\beta'_i) = C'(\alpha_i)$. *Then, if the condition*

$$(9)\qquad c'_{ij} - c_{ij} \in J_i^{-1} H_j H_{j-1} \dots H_2 H_1 \quad \text{for } i>j$$

(where $H_k = J_k I_k^{-1}$) is satisfied, then the submodules

$$N = J_1 \beta_1 + \dots + J_m \beta_m \quad \text{and} \quad N' = J_1 \beta'_1 + \dots + J_m \beta'_m$$

are equal.

Proof. For $X \in KM$ we can write

$$X = x_1 \beta_1 + \dots + x_m \beta_m = x'_1 \beta'_1 + \dots + x'_m \beta'_m,$$

and from $(\beta'_i) = C' C^{-1} (\beta_i)$ we obtain $(x_i) = {}^t(C' C^{-1})(x'_i)$.

Let ${}^t(C' C^{-1}) = (b_{ik})$; by Lemma 2, we have $b_{ik} = 0$ for $i > k$, $b_{ii} = 1$, and

$$b_{ik} = \sum_{j=i}^{k-1} (c'_{kj} - c_{kj}) A_{ji} \quad \text{for } i < k.$$

By Lemma 1, the equivalence $X \in N \Leftrightarrow X \in N'$ is valid if and only if

$$\sum_{j=i}^{k-1} (c'_{kj} - c_{kj}) A_{ji} \in J_i J_k^{-1} \quad \text{for } 1 \leqslant i < k \leqslant m.$$

This condition is satisfied if (9) is verified. Indeed, we have then, according to Lemma 3,

$$(c'_{kj} - c_{kj}) A_{ji} \in J_k^{-1} J_j H_{j-1} \dots H_2 H_1 J_j^{-1} H_{j-1}^{-1} \dots H_{i+1}^{-1} I_i \subset J_k^{-1} J_i.$$

THEOREM 3. *Let M be a torsion-free and finitely generated A-module of rank m and let I_i be the ideals associated with M for a basis (α_i) of KM over K. Then, if J_i are non-zero ideals of A with $J_i \subset I_i$, then the number of submodules of M having J_i as associated ideals for (α_i) is at most*

$$\prod_{j=1}^{m} (A : J_i I_i^{-1})^{(m-j)(m-j+1)/2}.$$

Proof. As a consequence of Theorem 1 we may assume that

$$M = I_1 \alpha_1 + \dots + I_m \alpha_m.$$

Then, by Theorem 2, there is a mapping from the set of matrices (c_{ik}) satisfying (3) onto the set of submodules of M which have J_i as associated ideals for (α_i). From Lemma 4 we know that the matrices (c_{ik}) and (c'_{ik}) furnish the same submodule if c_{ik} and c'_{ik} are connected by condition (9). Then the number of submodules which have J_i as associated ideals for (α_i) is at most equal to the number of classes formed by the matrices whose coefficients are connected by (9). The number of these classes is

$$\prod_{1 \leqslant j < i \leqslant m} (J_i^{-1} I_j : J_i^{-1} J_j H_{j-1} \dots H_1) = \prod_{1 \leqslant j < i \leqslant m} (A : H_j H_{j-1} \dots H_1)$$
$$= \prod_{j=1}^{m-1} (A : H_j \dots H_1)^{m-j} = \prod_{j=1}^{m-1} (A : H_j)^{(m-j)(m-j+1)/2}.$$

Corollary 2. *Let A be a Dedekind ring in which the number of ideals of a given finite index is finite, whatever this finite index may be, and let M be a torsion-free and finitely generated module over A. Then the number of submodules of M having a given finite index is finite.*

Proof. Let m be the rank of M, let $(\alpha_i)_{i=1,\dots,m}$ be a basis of KM over K, and let I_i be the ideals associated with M for (α_i). We consider separately two cases for the proof:

(a) Some submodule of finite index of M, say N, has rank less than m.

Let J_i, $i = 1, \dots, m$, be the ideals associated with N for (α_i). Then $J_i = (0)$ for some i. The formula of Corollary 1 shows that I_i is finite, and hence A is finite because of its integrality, and M is also finite because of its finite generation. Thus M contains only finitely many submodules.

(b) Every submodule of finite index in M has rank m.

Then, as a consequence of the hypothesis on A, there are finitely many sequences of ideals $J_1, J_2, \dots, J_m$ satisfying

$$\prod_{i=1}^{m} (I_i : J_i) = k.$$

This means that the number of sequences of ideals associated with the submodules of a given index k is finite. Furthermore, by the hypothesis on the rank of the submodules, the ideals J_i, $i = 1, \dots, m$, are all non-zero, and the hypotheses of Theorem 3 are satisfied for each of these sequences of ideals. Therefore, there are finitely many submodules corresponding to each of them. This proves the theorem in case (b).

5. Associated ideals and the discriminant. In this section we consider an integral commutative ring M which has, as in the preceding sections, a structure of torsion-free and finitely generated A-module and we suppose, moreover, that the internal and external products are connected by the relation $\mu(a\mu') = a(\mu\mu')$ for all $a \in A$ and $\mu, \mu' \in M$.

Let K be the quotient field of A. Then KM is a K-algebra and to each $x \in KM$ there corresponds an endomorphism m_x of KM, defined by $m_x(\mu) = x\mu$, whose trace will be denoted by $\mathrm{Tr}\,(x)$. It is easily proved, e.g., by means of Theorem 1 that $\mathrm{Tr}\,(x) \in A$ if $x \in M$.

Now, let m be the rank of M and let $(x_i)_{i=1,\dots,m}$ be elements of KM. Then the *discriminant* $D(x_1, \dots, x_m)$ is defined as

$$D(x_1, \dots, x_m) = \det\big(\mathrm{Tr}\,(x_i x_j)\big).$$

For a submodule N of M, the discriminant $D(N)$ is the ideal generated by the discriminants of all the sequences $(x_i)_{i=1,\dots,m}$, where $x_i \in N$.

If $(y_i) = B(x_i)$ for a matrix B whose coefficients lie in K, it is obvious that $D(y_1, \dots, y_m) = (\det B)^2 D(x_1, \dots, x_m)$. This formula proves that the discriminants of the bases of KM over K are either all zero or all non-zero. In the first case $D(M) = (0)$, and in the second case $D(M) \neq (0)$. In particular, $D(M) \neq (0)$ if K is finite or of finite characteristic (cf. [8], Section 2.7).

The following result gives a useful relation between the discriminant of a module and its associated ideals:

LEMMA 5. *Let M be an integral commutative ring satisfying the hypotheses given at the beginning of the section, let $(\alpha_i)_{i=1,\ldots,m}$ be a basis of KM over K, and $I_1, \ldots, I_m$ the ideals associated with M for this basis. Then*

$$D(M) = (I_1 \ldots I_m)^2 D(\alpha_1, \ldots, \alpha_m).$$

Proof. By Theorem 1 we have $M = I_1\beta_1 + \ldots + I_m\beta_m$ for some $\beta_1 = \alpha_1$ and $\beta_i = \alpha_i + v_i$, where $v_i \in K\alpha_1 + \ldots + K\alpha_{i-1}$, $i = 2, \ldots, m$. Then

$$D(\beta_1, \ldots, \beta_m) = D(\alpha_1, \ldots, \alpha_m).$$

Now, consider $x_i \in M$ for $i = 1, \ldots, m$. Then

$$x_i = \sum_{j=1}^{m} a_{ij}\beta_j,$$

where $a_{ij} \in I_j$ for $i, j = 1, \ldots, m$, and hence

$$D(x_1, \ldots, x_m) = \big(\det(a_{ij})\big)^2 D(\beta_1, \ldots, \beta_m).$$

It is easily seen that the ideal generated by all the elements $\det(a_{ij})$, where $a_{ij} \in I_j$, is the ideal $I_1 \ldots I_m$. And, according to the multiplicative theory of ideals in a Dedekind ring, the ideal generated by all the elements $\big(\det(a_{ij})\big)^2$ is $(I_1 \ldots I_m)^2$. This establishes the required formula.

As a first application of this formula, we obtain

THEOREM 4 (Artin's criterion [1]). *Let M be an integral commutative ring, with a structure of torsion-free and finitely generated A-module, such that $\mu(a\mu') = a(\mu\mu')$ for all $a \in A$ and $\mu, \mu' \in M$ and such that $D(M)$ is not zero. Let $(\alpha_i)_{i=1,\ldots,m}$ be some basis of KM over K. Then M is free over A if and only if the ideal*

$$\left(\frac{D(M)}{D(\alpha_1, \ldots, \alpha_m)}\right)^{1/2}$$

is principal.

Proof. Let I_i $(i = 1, \ldots, m)$ be the ideals associated with M for (α_i). Then

$$I_1 I_2 \ldots I_m = \left(\frac{D(M)}{D(\alpha_1, \ldots, \alpha_m)}\right)^{1/2}$$

by Lemma 5. Property 3 completes the proof.

Remark. In [1], Artin gives a proof of this criterion for the ideals of the ring of integers of an algebraic field extension and uses localization arguments. Here we use only elementary arguments from the theory of ideals in a Dedekind ring.

THEOREM 5. *Let M be a ring satisfying the hypotheses of Theorem 4 and let N be a submodule of M of the same rank. Then*

$$(M:N) = \left(A:\left(\frac{D(N)}{D(M)}\right)^{1/2}\right).$$

Proof. Let $(\alpha_i)_{i=1,\dots,m}$ be a basis of KM over K and let I_i and J_i be the ideals associated with M and N for this basis.

Applying Lemma 5 to M and N, we obtain

$$D(N) = \left(\frac{J_1 \dots J_m}{I_1 \dots I_m}\right)^2 D(M). \tag{10}$$

On the other hand, we have

$$\left(A:\frac{J_1 \dots J_m}{I_1 \dots I_m}\right) = \prod_{i=1}^{m}\left(A:\frac{J_i}{I_i}\right) = \prod_{i=1}^{m}(I_i:J_i).$$

Then the formula of Corollary 1 completes the proof.

Remark. Formula (10) can be viewed as a generalization of the familiar formula $\Delta_{L/K}(I) = (N_{L/K}(I))^2 \Delta_{L/K}$ valid for a fractional ideal I in a finite extension L of an algebraic field K (see [4]; [5], Chapter III, Section 3: [6]; and [7], Proposition 2.6 and historic notes).

COROLLARY 3. *Let M be a ring satisfying the hypotheses of Theorem 4 and let $(\alpha_i)_{i=1,\dots,m}$ be a basis of KM over K with $\alpha_i \in M$ and such that $(D(\alpha_1, \dots, \alpha_m)) = D(M)$. Then M is free over A with basis (α_i).*

Proof. Let us consider the submodule $N = A\alpha_1 + \dots + A\alpha_m$ of M. From Lemma 5 we deduce that $D(N) = (D(\alpha_1, \dots, \alpha_m))$, and hence $D(N) = D(M)$. The formula of Theorem 5 is reduced to $(M:N) = 1$, and then $M = N$. This proves the assertion.

COROLLARY 4. *Let the Dedekind ring A have no ideal of infinite index and only finitely many ideals of a given finite index, whatever this index may be, and let M be a ring satisfying the hypothesis of Theorem 4. Then the number of submodules of M which have a given non-zero discriminant is finite, whichever this discriminant may be.*

Proof. Submodules having the discriminant $D \neq (0)$ are of the same rank as M and Theorem 5 can be applied. They all have the same finite index $\left(A:(D/D(M))^{1/2}\right)$ in M and are, by Corollary 2, finite in number.

6. An example. Let A be the ring of integers of an absolute quadratic extension K and ω an algebraic integer of degree 3 over K. We consider

$M = A+A\omega+A\omega^2$. Then $KM = K(\omega)$, $M \supset A$, and M is an integral ring which is also a torsion-free and finitely generated A-module of rank 3.

Our purpose here is to describe all subrings of M which contain A and are of index $|\Delta|$, where Δ is the discriminant of K.

These subrings are obviously submodules of M of rank 3 and for such a subring, say N, by Theorem 2 we have

$$N = A+J_2(c_{21}+\omega)+J_3(c_{31}+c_{32}\omega+\omega^2),$$

where A, J_2, and J_3 are the ideals associated with N for $(1, \omega, \omega^2)$ and where $c_{ij} \in J_i^{-1}$ for $i = 2, 3$ and $j < i$.

According to Lemma 4, we can consider $c_{21} = c_{31} = 0$, and then we have

$$N = A+J_2\omega+J_3(d\omega+\omega^2), \qquad \text{where } d \in J_3^{-1}.$$

Lemma 4 also proves that we do not change this module if we replace d by some $d' \in J_3^{-1}$ such that $d'-d \in J_3^{-1}J_2$. Conversely, it can easily be proved that if two such modules are equal, then $d'-d \in J_3^{-1}J_2$.

Corollary 1 shows that $|\Delta| = N(J_2J_3)$, where $N(J_i)$ is the absolute norm of J_i.

Moreover, let x, $x' \in J_2$. Then $x\omega$, $x'\omega \in N$, and because N is a ring, we have $xx'\omega'\omega \in N$, whence $xx' \in J_3$. This means that J_3 is a factor of J_2^2.

From these properties we deduce the following result:

Let N be a subring of $M = A+A\omega+A\omega^2$, which contains A and is of index $|\Delta|$. Then:

(a) *if Δ is odd, then N is one of the following submodules*:

$$A+A\sqrt{\Delta}\,\omega+A(d\omega+\omega^2), \qquad \text{where } d = 0, 1, \ldots, |\Delta|-1;$$

(b) *if $\Delta = 4m$ with m odd, then N is one of the following submodules*:

$$A+A\sqrt{\Delta}\,\omega+A(d\omega+\omega^2),$$

where $d = 0, \ldots, m-1, \sqrt{m}, 1+\sqrt{m}, \ldots, m-1+\sqrt{m}$, or

$$A+\mathscr{P}\sqrt{m}\,\omega+\mathscr{P}(d\omega+\omega^2),$$

where $d = 0, 1, \ldots, m-1$ and where $\mathscr{P}$ is the ideal of A such that $\mathscr{P}^2 = (2)$;

(c) *if $\Delta = 4m$ with $m = 2q$ (q odd), then N is one of the submodules given in* (b) *or one of the following*:

$$A+A\sqrt{2m}\,\omega+2A(d\omega+\omega^2), \qquad \text{where } d = 0, 1, \ldots, q-1.$$

It can happen that some of those enumerated submodules are not subrings.

We prove assertion (c). First observe that $|\Delta| = N(\delta)$, where $\delta = 2(\sqrt{m}) = \mathscr{P}^2\sqrt{m} = \mathscr{P}^3\mathscr{Q}$, $\mathscr{P}$ being the ideal of A such that $\mathscr{P}^2 = (2)$ and $\mathscr{Q}$

being prime to $\mathscr{P}$ and such that $\mathscr{Q}^2 = (q)$. Then the condition $N(J_1 J_2) = |\Delta|$ implies that $J_2 J_3 = \delta$ and $J_3 | J_2^2$ implies that J_3 is one of the following ideals: A, $\mathscr{P}$ or $\mathscr{P}^2$. Finally, d is obtained by taking representatives of the classes of J_3^{-1} modulo $J_3^{-1} J_2$.

In cases (a) and (b), J_3 and d are obtained in the same way.

REFERENCES

[1] E. Artin, *Question de base minimale dans la théorie des nombres algébriques*, Colloque international du C.N.R.S., Paris 1950.

[2] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, New York 1962.

[3] L. Fuchs, *A theorem on the relative norm of an ideal*, Commentarii Mathematici Helvetici 21 (1948), p. 29-43.

[4] — *Some theorems on algebraic rings*, Acta Mathematica 81 (1949), p. 285-289.

[5] S. Lang, *Algebraic number theory*, Reading 1970.

[6] H. B. Mann, *On integral bases*, Proceedings of the American Mathematical Society 9 (1958), p. 167-172.

[7] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.

[8] P. Samuel, *Algebraic theory of numbers*, London 1972.

DÉPARTEMENT D'ÉCONOMÉTRIE
UNIVERSITÉ DE GENÈVE

Reçu par la Rédaction le 23. 1. 1980;
en version modifiée le 1. 12. 1980