A NOTE ON THE UNIQUENESS OF THE INVARIANT FACTORS

por ENZO R. GENTILE

Universidad de Buenos Aires

Let R denote a commutative ring with identity. We say that a R-module M has a *principal representation* if there exist ideals

$$\alpha_1, \alpha_2, \ldots, \alpha_n \text{ of } R$$

satisfying

i) $R \neq \alpha_1 \supset \alpha_2 \supset \ldots \supset \alpha_n \neq 0$

ii) $M \cong R/\alpha_1 \, (+) \, R/\alpha_2 \, (+) \ldots (+) \, R/\alpha_n$
where $\cong$ denotes R-module isomorphism.

Under these conditions we say simply that $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a principal representation of M.

In this Note we intend to give an elementary proof of the following known result on the uniqueness of the ideal α_i's. See: *Bourbaki, N.*, Algèbre, Chap. 7, 1964, Prop. 2 § 4, nº 1).

THEOREM: Let $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $(\beta_1, \beta_2, \ldots, \beta_m)$ be principal representations of an R-module M. Then

$m1)$ $m = n$, and

$m2)$ $\alpha_i = \beta_i$ for all i, $i = 1, \ldots, m$.

It is a well known and classical result that if R is a principal ideal domain then there is, for any finitely generated torsion module, a principal representation associated to it. The ideals α_i's are then called the *invariant factors* (or also the torsion factors) of the module.

The present proof avoids the use of exterior algebras (loc. cit.) and only assumes known the following properties of tensor product of modules ($(\times)$ denotes tensor product)

$t1$ $(\times)$ commutes with finite direct sums

$t2$ If α and β are ideals of R, there is a natural isomorphism

$$R/\alpha \, (\times) \, R/\beta \cong R/\,(\alpha + \beta)$$

When R is particularized to Z, the ring of rational integers, this proof turns out to be remarkably easy.

PROOF OF THE THEOREM

Let α be an ideal of R. We define, for $x \in R$

$$(\alpha : x) = \} \, r \, / \, r \in R \text{ and } r . x \in \alpha \, \}$$

Clearly $(\alpha : x)$ is an ideal of R and satisfies

$$(\alpha : x) = R \text{ if and only if } x \in \alpha .$$

Considering the natural R-module structure of R/α we have the easy

LEMMA: There is a natural isomorphism

$$R \, / \, (\alpha : x) \cong x . \, (R \, / \, \alpha)$$

Proof: The following diagram

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & R/\alpha \\ {\scriptstyle p_x}\downarrow & & \downarrow{\scriptstyle p'_x} \\ R & \xrightarrow{\ f\ } & R/\alpha \end{array}$$

where f is the canonical homomorphism
p_x the multiplication by x in R
p'_x the multiplication by x (as operator) in R/α,

is commutative. Therefore

$$x . (R/\alpha) = p'_x \, (f(R)\,) = f(p_x(R)\,) \cong R/\mathrm{Ker}\,(f . p_x)$$

and since

$$\mathrm{Ker}\,(f . p_x) = (\alpha : x)$$

our contention, follows.

We now assume an isomorphism

(1) $$R/\alpha_1 (+) \ldots (+) \, R/\alpha_n \cong R/\beta_1 \, (+) \ldots (+) \, R/\beta_m$$

be given.

Let τ be a maximal proper ideal of R containing α_1. Tensoring both sides of (1) by R/τ and using the fact that $\alpha_i + \tau = \tau$, for all $i = 1, \ldots, n$, gives the isomorphism

(2) $$R/\tau (+) \ldots (+) R/\tau \cong R/(\beta_1 + \tau) (+) \ldots (+) \, R/(\beta_m + \tau)$$

We now observe that (2) is also a R/τ isomorphism and being the

quotient R/τ a field, (2) is an isomorphism of vector spaces over R/τ.
By the invariance of the dimension and the fact that

$$R/(\beta_i + \tau) = R/\tau \text{ or } 0, \text{ for all } i, i = 1, \ldots, m$$

we have the inequality

$$n \leqslant m$$

By the same argument we get

$$m \leqslant n$$

Therefore $n = m$, and this proves the first part of the theorem.
Let now $x \epsilon \alpha_1$. The multiplication by x on both sides of (1) and the Lemma give the isomorphism

$$(3) \qquad R/(\alpha_1 : x)(+) \ldots (+)R/(\alpha_m : x) \cong R/(\beta_1 : x)(+) \ldots (+) R/(\beta_m : x)$$

Notice that (3) gives also isomorphic principal representations and so by the first part of the theorem we must have the same number of terms on both sides. Since $R/(\alpha_1 : x) = 0$, there must be at least an index i, $1 \leqslant i \leqslant m$, for which

$$R/(\beta_i : x) = 0, \text{ that is } x \epsilon \beta_i$$

As $\beta_i \subset \beta_1$, wen can conclude that

$$\alpha_1 \subset \beta_1$$

By the same argument we get

$$\beta_1 \subset \alpha_1$$

Therefore $\alpha_1 = \beta_1$.
Let us assume now the equalities

$$\alpha_i = \beta_i \qquad \text{for } i < k \leqslant m$$

If $x \epsilon \alpha_k$ we have

$$(\alpha_i : x) = (\beta_i : x) = R \quad \text{if} \quad i < k$$
$$\text{and} \qquad (\alpha_k : x) = R.$$

Multiplying on both sides of (1) by x, we are, by the same argument as before, led to

$$(\beta_k : x) = R \qquad \text{,that is } x \epsilon \beta_k$$

It follows that $\alpha_k \subset \beta_k$. In analogous way we get that $\beta_k \subset \alpha_k$.

Therefore $\alpha_k = \beta_k$. By an inductive argument we can conclude that $\alpha_i = \beta_i$ for all i, $i = 1, \ldots, m$. The theorem is now proved.

THE CASE $R = Z$.

Modules are then abelian groups and to say that M has a principal representation means that there exist positive integers $d_1, \ldots, d_m$ satisfying

i) $1 < d_1$ and $d_i \mid d_j$ if $i \leqslant j$

ii) $M \cong Z/(d_1)(+)\ldots(+)Z/(d_m)$

where the bar | refers, as usual, to divisibility, and (d_i) denotes the ideal generated in Z by d_i.

Let $(d_1, \ldots, d_n)$ and $(s_1, \ldots, s_m)$ be sets of positive integers satisfiying condition i). Let us assume an isomorphism

$$(4) \quad Z/(d_1)(+)\ldots(+)Z/(d_n) \cong Z/(s_1)(+)\ldots(+)Z/(s_m)$$

We get, after tensoring both sides of (4) by $Z/(d_1)$:

$$(5) \quad Z/(d_1)(+)\ldots(+)Z/(d_1) \cong Z/((s_1, d_1))(+)\ldots(+)Z/((s_m, d_1))$$

where (s_i, d_1) denotes the g.c.d. of s_i and d_1.

By cardinality arguments applied to (5) we get

$$(6) \qquad d_1^n = (s_1, d_1) \ldots (s_m, d_1)$$

Since $(s_i, d_1) \leqslant d_1$, (6) gives at once

$$n \leqslant m$$

In the same way we get

$$m \leqslant n$$

Therefore $n = m$.

But then (6) implies that $d_1 \leqslant s_1$ and by the same reasons $s_1 \leqslant d_1$. Therefore $d_1 = s_1$. By an inductive argument we prove that $d_i = s_i$ for all i.