Revista de la
Unión Matemática Argentina
Volumen 27, 1976 .

ON THE INVARIANT FACTORS

Enzo R. Gentile

Let R be a commutative ring with identity $1 \neq 0$. We say that an R-module M has a *principal representation* if there exists a sequence $A_1,\ldots,A_n$ of ideals of R satisfying:

i) $R \neq A_1 \supset \ldots \supset A_n \neq 0$

ii) $M \simeq R/A_1 \oplus \ldots \oplus R/A_n$

where $\simeq$ denotes R-module isomorphism. Under these conditions we simply say that $(A_1,\ldots,A_n)$ gives 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 ideals $(A_1,\ldots,A_n)$ (See [1], Prop.2, § 4, N° 1).

THEOREM. *Let* $(A_1,\ldots,A_n)$ *and* $(B_1,\ldots,B_m)$ *give principal representations of an* R*-module* M. *Then*

m1) $n = m$

m2) $A_i = B_i$, *for all* $i = 1,\ldots,n$.

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 sequence of ideals $(A_1,\ldots,A_n)$ are then called the *invariant factors* of the module.

The present proof avoids the use of exterior algebras (loc.cit.) and improves our first version as given in [2] using tensor product. In the case of R = **Z**, the ring of rational integers, the proof is even simpler since one can use there cardinality arguments.

NOTATION AND PREREQUISITES.

a) For any pair of R-modules A and B, we denote with Hom(A,B) the R-module of R-morphisms of A into B. We shall use the elementary functorial properties of Hom, such as the fact that it commutes with finite direct sums.

b) Let A and B be ideals of R. With (A:B) we denote the quotient ideal of R of all r satisfying $rB \subset A$. If $x \in R$ we shall write, by abuse of notation, (A:x) to denote the ideal of R of all r satisfying $r.x \in A$. Clearly (A:x) = R if and only if $x \in A$.

Let A be an ideal of R. Considering the natural R-module structure of R/A, x(R/A), for any $x \in R$, is a submodule of R/A.

To start with, we prove two lemmas.

LEMMA 1. *There is a natural isomorphism*

$$R/(A:x) \simeq x(R/A)$$

for any $x \in R$.

Proof. The following diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & R/A \\ {\scriptstyle m_x}\downarrow & & \downarrow{\scriptstyle m'_x} \\ R & \xrightarrow{f} & R/A \end{array}$$

where f is the canonical morphism, m_x is the multiplication by x in R and m'_x is the multiplication by x (as operator) in R/A, is commutative. Therefore

$$x(R/A) = m'_x(f(R)) = f(m_x(R)) \simeq R/(\mathrm{Ker}(f.m_x))$$

and since $\mathrm{Ker}(f.m_x) = (A:x)$ we are done.

LEMMA 2. *Let* A *and* B *be ideals in* R. *Then there is a natural isomorphism*

$$\mathrm{Hom}(R/A, R/B) \simeq (B:A)/B.$$

Proof. Let 1_A and 1_B denote the canonical generators of the cyclic modules R/A and R/B, respectively. The morphisms of R/A into R/B are of the form $1_A \longrightarrow k.1_B$, with $k \in R$. Now, an element $k \in R$ defines actually a morphism of R/A into R/B if and only if: for every $y \in A$, $k.y \in B$. But this is equivalent to saying that $k \in (B:A)$. Moreover $k \in (B:A)$ defines the null morphism if and only if $k \in B$. This shows well the isomorphism above.

PROOF OF THE THEOREM.

Let us be given an isomorphism

$$(1) \qquad R/A_1 \oplus \ldots \oplus R/A_n \simeq R/B_1 \oplus \ldots \oplus R/B_m$$

Let T be a maximal proper ideal of R containing A_1. By taking $\mathrm{Hom}(\ ,R/T)$ on both sides of (1), by using Lemma 2 and the fact that $(T:A_i) = R$ for all i, $i = 1,\ldots,n$, we get an isomorphism

$$(2) \qquad R/T \oplus \ldots \oplus R/T \simeq (T:B_1)/T \oplus \ldots \oplus (T:B_m)/T$$

We observe that (2) is an isomorphism of R/T - modules. Since the quotient R/T is a field, (2) is an isomorphism of R/T - vector spaces. Furthermore we have that

$$T \subset (T:B_i) \implies (T:B_i) = T \text{ or } R \text{, hence } (T:B_i)/T = R/T \text{ or } 0$$

for all i , $i = 1,\ldots,m$.

By the remark above and the invariance of the dimension for vector spaces, applied to (2) we conclude that $n \leqslant m$.

The same argument shows that $m \leqslant n$. Therefore $n = m$ and this proves the first part of the Theorem.

Let us see the second part. First of all observe that $A_m = B_m$ for both sides of (1) are annihilated by A_m and B_m.

Assume that for some index j is $A_j \neq B_j$, $1 \leqslant j < m$. Without loss of generality we can suppose that j is minimal with that property. Then there exists (say) $x \in A_j$ and $x \notin B_j$. Consequently,

$$\begin{aligned} &(A_i:x) = R \quad \text{for all } i \text{ , } i \leqslant j \text{ ,} \\ &i < j \implies A_i = B_i \implies (B_i:x) = R \text{ , and} \\ &(B_s:x) \neq R \quad \text{for all } j \leqslant s \leqslant m \text{ .} \end{aligned}$$

The restriction of the isomorphism (1) to the multiples of x and Lemma 1, give an isomorphism

$$(3) \qquad R/(A_{j+1}:x) \oplus \ldots \oplus R/(A_m:x) \simeq R/(B_j:x) \oplus \ldots \oplus R/(B_m:x)$$

Next, observe that (3) gives isomorphic principal representations. By the first part of the theorem both must have the same number of terms.

But this is clearly not so. We get a contradiction, therefore $A_i = B_i$ for all i, $i = 1,\ldots,m$. This completes the proof of the Theorem.

CASE $R = Z$ THE RING OF RATIONAL INTEGERS. The proof can be simplified by using cardinality arguments. We illustrate it by proving part m1) of the Theorem.

Let us denote, for any positive integer d, with Z_d the group of integers module d. Let $d_1,\ldots,d_n$; $s_1,\ldots,s_m$ be integers satisfying

$$\begin{aligned} &1 < d_i,\ i \leqslant j \implies d_i \mid d_j \text{ , } 1 \leqslant i,j \leqslant n \\ &1 < s_j,\ i \leqslant j \implies s_i \mid s_j \text{ , } 1 \leqslant i,j \leqslant m \end{aligned}$$

(where $\mid$ denotes divisibility in Z). Moreover assume an isomorphism

$$(4) \qquad Z_{d_1} \oplus \ldots \oplus Z_{d_n} \simeq Z_{s_1} \oplus \ldots \oplus Z_{s_m}$$

We get, by taking $\mathrm{Hom}(\ ,Z_{d_1})$ on both sides of (4), an isomorphism

$$(5) \qquad Z_{d_1} \oplus \ldots \oplus Z_{d_1} \simeq Z_{(s_1,d_1)} \oplus \ldots \oplus Z_{(s_m,d_1)}$$

where $(\ ,\ )$ denotes greatest common divisor.

By cardinality we must have

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

But since $(s_1,d_1) \leqslant d_1$, (6) implies $n \leqslant m$. In the same way we prove that $m \leqslant n$. Therefore $n = m$.

REFERENCES

[1] N.BOURBAKI, *Algèbre*, Chap. 7 (1964).

[2] E.R.GENTILE, *A Note on the Uniqueness of the Invariant Factors*. Revista de la Unión Matemática Argentina, Vol 23, pag. 31-34 (1966).

Universidad de Buenos Aires
Argentina

Recibido en agosto de 1975.