MULTIPLICATIVE INVARIANTS AND LENGTH FUNCTIONS OVER VALUATION DOMAINS

PAOLO ZANARDO

ABSTRACT. The notion of length function ℓ of Mod R was introduced by Northcott and Reufel in [6]. They described length functions when R is a valuation domain. Vámos [11] investigated additive functions for Noetherian rings. These functions take values that are either nonnegative real numbers or ∞ . We define a multiplicative invariant as a map μ from Fin R, the class of finitely generated R-modules, to a partially ordered multiplicative semigroup Γ , such that $\mu(X) = \mu(Y)\mu(X/Y)$, for $Y \subseteq X$ finitely generated. We investigate the annihilator sets of finitely generated modules over valuation domains. The results we find allow us to show that a certain map μ_T is a multiplicative invariant that enjoys a universal property. Using μ_T we re-obtain a description of length functions over valuation domains, in an alternative way to that in [6].

Introduction. The starting point of the present paper is the notion of length function of Mod R, introduced by Northcott and Reufel, in the 1965 paper [6], as a generalization of the classical Jordan-Hölder length of modules. Namely, if R is any ring, a real-valued map ℓ defined on Mod R is a length function if for any left R-modules $N\subseteq M$, we have $\ell(M)=\ell(N)+\ell(M/N)$, and $\ell(M)=\sup\{\ell(X)\}$, where X ranges over the finitely generated submodules of M. Northcott and Reufel gave some general results and characterized length functions over valuation domains. Shortly after, Vámos in [11] distinguished the two defining properties of a length function, calling a real-valued function ℓ additive if it satisfies the first above property, and upper continuous if it satisfies the second one. In fact, it is easy to show that these properties are independent (see, for instance, our next Remark 3.1). Vámos thoroughly investigated additive functions over Noetherian rings.

²⁰¹⁰ AMS Mathematics subject classification. Primary 13C60, 13A18. Keywords and phrases. Multiplicative invariants, valuation domains, finitely generated modules.

Received by the editors on May 26, 2010.

In 1976 Ribenboim [7] extended the notion of length function to maps λ with values into an ordered abelian group G. Due to the fact that G is not complete, in general, he had to confine λ to a class of finitely presented modules, called *constructible*. The main purpose of Ribenboim's paper was to give correspondences between special length functions λ over a domain R, the valuation overrings of R, and the endomorphisms of the Grothendieck group of constructible R-modules.

The aim of the present paper is two-fold. On the one hand, in the first section we investigate the so-called annihilator sets of finitely generated modules over a valuation domain. The results we find, specifically Theorem 1.2, naturally lead to the notion of multiplicative invariant μ , defined on Fin R, the class of finitely generated R-modules (R a commutative ring), and with values into a partially ordered multiplicative semigroup (Γ, \cdot, \leq) . A multiplicative invariant μ satisfies the following natural properties, for $Y \subseteq X$ finitely generated Rmodules: $\mu(X) = \mu(Y)\mu(X/Y)$; $\mu(Y) \leq \mu(X)$; if Z is a homomorphic image of X, then $\mu(Z) \leq \mu(X)$. In case R is a valuation domain, we prove (Theorems 2.4 and 2.5) that a special map $\mu_{\mathcal{I}}$ is a multiplicative invariant that enjoys a universal property for the class of the so-called valuative invariants (this term is borrowed from [7]). The definition of $\mu_{\mathcal{I}}$ naturally derives from the discussion made in the first section. Namely, if X is a finitely generated R-module, and B_1, \ldots, B_n is any annihilator set of X, we have $\mu_{\mathcal{I}}(X) = B_1 \cdots B_n$. The importance of $\mu_{\mathcal{I}}$ justifies our choice of the multiplicative notation for the semigroup Γ.

The second purpose of our paper is to apply the notion of multiplicative invariant to re-obtain a description of length functions over valuation domains, in a way alternative and more direct than that in [6], and using a different point of view. We briefly summarize it. The infinite length functions ℓ (i.e., whose image is an infinite set) lie in two disjoint classes. Either ℓ is an L-rank, for some prime ideal L of R, or it is valuative (Proposition 4.5). In Proposition 4.2 one finds a characterization of L-ranks, analogous to some results in [6]. In Theorem 4.7 we characterize the valuative length functions using the universal property of $\mu_{\mathcal{I}}$.

It is worth ending this introduction indicating a relevant motivation for the study of length functions, and, more generally, of multiplicative invariants, namely, the developing theory of algebraic entropy. A sketchy definition of the concept of algebraic entropy for endomorphisms of Abelian groups was given in a 1965 paper by Adler et al. [1], dedicated to topological entropy. In 1975 this concept was resumed and developed by Weiss [12], in a paper that related algebraic and topological entropies using Pontryagin duality. In the algebraic context, as well as in other areas of mathematics and physics, entropy is viewed as a measure of the "average disorder" created by a transformation when we repeatedly apply it. Following this philosophy, in [3] Dikranjan et al. thoroughly investigated the algebraic entropy of [1, 12], which turned out to be a very useful tool in the study of endomorphism rings of Abelian p-groups. Thereafter, Salce and Zanardo [10] defined the algebraic entropy for R a commutative ring, and used the rank as an invariant to deal with the case of torsion-free Abelian groups. Many more papers devoted to algebraic entropy in its different aspects have been published, or are going to appear. We quote [2, 5, 9, 13].

In general, to define algebraic entropy, one needs an invariant ℓ of Mod R that measures the "size" of R-modules. As explained in [10], to get a correct definition such ℓ must satisfy a property called "subadditivity," which is weaker than additivity. However, the importance of length functions is crucial. In fact, starting with results in [3, 10], Salce et al. [8] have shown in full generality that, when ℓ is a discrete length function, the related algebraic entropy satisfies the Addition Theorem (see [3, 10] for the statement and a discussion on this fundamental result). In view of the result in [8], in this paper we give some emphasis to the case where ℓ is discrete, i.e., the image of ℓ is a discrete subset of \mathbf{R} .

1. Annihilator sets of finitely generated modules. In the present section, R is a valuation domain, with maximal ideal P and field of quotients Q. By v we denote a fixed valuation on Q such that $R_v = \{x \in Q : v(x) \geq 0\} = R$. In view of the discussion we will make in Section 4, it is worth noting that v is not unique. If v_1 is another valuation of Q such that $R_{v_1} = R$, we can only say that $v(Q^{\times})$ and $v_1(Q^{\times})$ are isomorphic ordered groups (here $Q^{\times} = Q \setminus \{0\}$).

Recall that a valuation v of a field Q has rank one if $v(Q^{\times})$ is an ordered subgroup of \mathbf{R} . In this case, we also say that $R = R_v$ is a rank-one valuation domain. The valuation domain R has rank one if and only if it has Krull dimension one, that is, P is the only nonzero prime ideal of R. A valuation domain of rank one is also called Archimedean.

When I is an ideal of a rank-one valuation domain R, we can define $v(I) = \inf\{v(r) : r \in I\}$, which is either a nonnegative real number, or the symbol ∞ when I = 0. We have v(IJ) = v(I) + v(J) for all ideals I. J.

For a general treatment of valuation domains and their modules we refer to the book by Fuchs and Salce [4].

The aim of this section is to investigate the annihilator sets (defined below) of finitely generated modules over a valuation domain. The results we prove will be applied in our subsequent discussion. For a basic exposition of the theory of finitely generated modules over valuation domains, see [4, Chapter 5.5].

A submodule N of the R-module M is said to be pure if $N \cap rM = rN$ for every $r \in R$ (see [4, Chapter 1]). For M an R-module, we denote by Ann(M) its annihilator. We define gen M to be the minimal cardinality of a generating system of M, when M is finitely generated; otherwise, we set $gen M = \infty$. As usual, by S_n we denote the group of the permutations of the set $\{1, \ldots, n\}$

Let X be a finitely generated R-module over the valuation domain R. Presently, gen $X = \dim_{R/P}(X/PX)$. Say gen X = n, and let $\{x_1, \ldots, x_n\}$ be a generating set for X. Then there exists a reordering $z_i = x_{\tau(i)}$ of the generators x_i (τ a suitable permutation of S_n) such that, setting $Z_0 = 0$ and $Z_i = \langle z_1, \ldots z_i \rangle$, for $1 \leq i \leq n$, the following properties are satisfied

- (a) each Z_i is pure in X;
- (b) for $1 \le i \le n$, Z_i/Z_{i-1} is isomorphic to R/A_i , where

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n$$
.

The above sequence of ideals is determined by X, and is called the annihilator sequence of X. Note that $A_i = \operatorname{Ann}(z_i + Z_{i-1})$.

The above results may be found in [4, Chapter 5.5]. Now we reconsider the arbitrary minimal generating set $\mathcal{G} = \{x_1, \ldots, x_n\}$ of X. For our purposes, we must take care of the order of the x_i . Hence we write $\mathcal{G} = (x_1, \ldots, x_n)$, and we say that \mathcal{G} is an ordered basis of X. For $1 \leq j \leq n$, let $X_0 = 0$, $X_j = \langle x_1, \ldots, x_j \rangle$, and $B_j = \operatorname{Ann}(x_j + X_{j-1})$. Then we say that B_1, \ldots, B_n is the \mathcal{G} -annihilator set of X. We remark that the submodule X_j is not necessarily pure in X.

We define $\alpha_{\mathcal{G}}(X) = B_1 B_2 \cdots B_n$. The ideal $\alpha_{\mathcal{G}}(X)$, a priori, depends upon the choice of the ordered basis. However, the next Theorem 1.2 shows that uniqueness is valid.

We prove a preliminary lemma, useful also in other contexts.

Lemma 1.1. Let R be a valuation domain, $X = \langle x_1, x_2 \rangle$ a two-generated module, where $Rx_1 \cap Rx_2 \neq 0$. Let us consider the ideals $B_1 = \operatorname{Ann}(x_1)$, $B_2 = \operatorname{Ann}(x_2 + Rx_1)$, $C_2 = \operatorname{Ann}(x_2)$, $C_1 = \operatorname{Ann}(x_1 + Rx_2)$. Then there exists a $q \in Q^{\times}$ such that $B_1 = qC_2$ and $B_2 = q^{-1}C_1$.

Proof. By symmetry, we assume that $B_1 = \operatorname{Ann}(x_1) = \operatorname{Ann} X$ and Rx_1 is pure in X, so that $B_2 \supseteq B_1$. Since, by hypothesis, $Rx_1 \cap Rx_2 \neq 0$, we have $B_2 \neq \operatorname{Ann}(x_2) = C_2$. Therefore, we get $B_1 \subseteq C_2 \subset B_2$. Since Rx_1 is pure in X, for every $r \in B_2 \setminus B_1$ we get a relation

$$rx_2 = rq_rx_1, \quad \exists \ q_r \in R.$$

Now we show that $v(q_r) = v(q_s)$, whenever $r, s \in B_2 \setminus C_2$. In fact, assuming without loss of generality that $s \in rR$, we get the relation $s(q_s - q_r)x_1 = 0$. Since $sx_2 = sq_sx_1 \neq 0$, it follows that $v(q_r) = v(q_s)$. Then we may fix $q \in R$ such that $v(q) = v(q_r)$, for all $r \in B_2 \setminus C_2$. We want to show that Ann $(x_2) = C_2 = q^{-1}B_1$. In fact, any $t \in C_2$ is a multiple of some $r \in B_2 \setminus C_2$. Thus we get $0 = tx_2 = tq_rx_1 = tqx_1$, whence $t \in q^{-1}B_1$. It follows that $C_2 \subseteq q^{-1}B_1$. Conversely, if $r \in B_2$ and $r \notin C_2$, then $rq_r \notin B_1$; hence, $r \notin q^{-1}B_1$, and $C_2 \supseteq q^{-1}B_1$ follows.

Now we prove that $C_1 = \operatorname{Ann}(x_1 + Rx_2) = qB_2$. For $r \in B_2$, we get $rqx_1 = rq_r(q/q_r)x_1 \in Rx_2$, since q/q_r is a unit of R, and therefore $qB_2 \subseteq C_1$. Now assume, for contradiction, that $qB_2 \subset C_1$, and choose $t \notin B_2$ such that $tq \in C_1$. Then $tqx_1 = sx_2 \neq 0$, for a suitable $s \in R$ (note that $tq \notin B_1 = qC_2 \subset qB_2$). Then $s \in B_2$, and hence $0 \neq sx_2 = sq_sx_1 = tqx_1$. It follows that $tq - sq_s \in \operatorname{Ann}(x_1) = B_1$. But $v(tq - sq_s) = v(tq)$, being $v(q) = v(q_s)$ and v(t) < v(s), since $t \notin B_2$ and $s \in B_2$. Therefore $tqx_1 = 0$, a contradiction. We conclude that $qB_2 = C_1$, as desired.

We note that the preceding lemma is no longer true if $Rx_1 \cap Rx_2 = 0$, that is, $X = Rx_1 \oplus Rx_2$. To get a counterexample, just choose $B_1 = \operatorname{Ann}(x_1)$ not isomorphic to $C_2 = \operatorname{Ann}(x_2)$.

We introduce a further notation. If $\mathcal{G} = (x_1, \ldots, x_n)$ is an ordered basis of X, for any permutation $\sigma \in S_n$ we set $\mathcal{G}_{\sigma} = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Theorem 1.2. Let R be a valuation domain, X a finitely generated R-module, with ordered basis $\mathcal{G} = (x_1, \ldots, x_n)$. Let B_1, \ldots, B_n be the \mathcal{G} -annihilator set of X. Then $\alpha_{\mathcal{G}}(X) = B_1 B_2 \cdots B_n$ does not depend upon the choice of \mathcal{G} .

Proof. It suffices to show that $\alpha_{\mathcal{G}}(X) = \alpha_{\mathcal{G}_{\sigma}}(X)$ for any permutation $\sigma \in S_n$. In fact, for any ordered basis \mathcal{H} of X, there is a suitable permutation τ such that $\alpha_{\mathcal{H}_{\tau}}(X) = A_1 \cdots A_n$, where $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n$ is the annihilator sequence of X, as explained above. Moreover, since any permutation is a product of transpositions, we readily realize that we may assume σ itself to be a transposition (j, j+1), for some j < n. We make induction on n, the case n=1 being obvious. Actually, the crucial step is to check our assertion for n=2. So let $X=\langle x_1,x_2\rangle$. As in Lemma 1.1, we set $B_1=\operatorname{Ann}(x_1),\ B_2=\operatorname{Ann}(x_2+Rx_1),\ C_2=\operatorname{Ann}(x_2),\ C_1=\operatorname{Ann}(x_1+Rx_2)$. If now $X=Rx_1\oplus Rx_2$, we get $B_1=C_1$ and $B_2=C_2$, and the equality $B_1B_2=C_1C_2$ is trivial. Thus assume that $Rx_1\cap Rx_2\neq 0$. Then Lemma 1.1 shows that $B_1=qC_2$ and $B_2=q^{-1}C_1$, for some $q\in Q^\times$, and therefore $B_1B_2=qC_2q^{-1}C_1=C_1C_2$ yields the required equality.

For $n \geq 3$, we assume by induction that if Z is an R-module with gen $Z \leq n-1$, then, for any ordered basis \mathcal{G}' of Z, $\alpha_{\mathcal{G}'}(Z)$ is independent from \mathcal{G}' . We write $\mathcal{G}^0 = (x_1, \ldots, x_{n-1})$. We pick a transposition σ . If $\sigma(n) = n$, then X_{n-1} is generated by $(x_{\sigma(1)}, \ldots, x_{\sigma(n-1)}) = \mathcal{G}^0_{\sigma}$. By induction, $\alpha_{\mathcal{G}^0}(X_{n-1}) = \alpha_{\mathcal{G}^0}(X_{n-1})$, hence

$$\alpha_{\mathcal{G}}(X) = \alpha_{\mathcal{G}^0}(X_{n-1})B_n = \alpha_{\mathcal{G}^0}(X_{n-1})B_n = \alpha_{\mathcal{G}_{\sigma}}(X).$$

Now we assume that $\sigma(n-1)=n$, $\sigma(n)=n-1$. If $Z=X_{n-2}$, it is readily proved that $\alpha_{\mathcal{G}}(X)=\alpha_{\mathcal{G}_{\sigma}}(X)$ if and only if $\alpha_{\mathcal{G}'}(X/Z)=\alpha_{\mathcal{G}'_{\sigma}}(X/Z)$, where $\mathcal{G}'=(x_{n-1}+Z,x_n+Z)$ is an ordered basis of X/Z and $\mathcal{G}'_{\sigma}=(x_n+Z,x_{n-1}+Z)$. Since X/Z is two-generated, the desired conclusion follows. \square

Example 1.3. As expected, Theorem 1.2 is no longer valid when R is not a valuation domain. For an example, consider the local Noetherian

domain R obtained by the polynomial ring $K[Z_1,Z_2]$ localizing at the maximal ideal $\langle Z_1,Z_2\rangle$ (K a field, the Z_i indeterminates). Consider the finitely generated R-module $X=(Z_1R+Z_2R)/Z_1^2R$, and let $z_i=Z_i+RZ_1^2,\ i=1,2$. Then $X=\langle z_1,z_2\rangle$, and an easy exercise shows that $B_1=\mathrm{Ann}\,(z_1)=Z_1R,\ B_2=\mathrm{Ann}\,(z_2+Rz_1)=Z_1R,\ C_1=\mathrm{Ann}\,(z_2)=Z_1^2R,\ C_2=\mathrm{Ann}\,(z_1+Rz_2)=Z_1R+Z_2R$. Therefore we get $B_1B_2\neq C_1C_2$.

We remark that the preceding theorem will be crucial for the proof of Theorem 2.4, in the next section.

The following easy lemma may be proved by a straightforward induction on k = gen(X/N).

Lemma 1.4. Let R be a valuation domain, X a finitely generated R-module with annihilator sequence $A_1 \subseteq \cdots \subseteq A_n$, N a proper submodule of X. Then the annihilator sequence of X/N has the form $C_1 \subseteq \cdots \subseteq C_k$, where $k = \text{gen}(X/N) \le n$ and $C_i \supseteq A_i$, for $1 \le i \le n$.

We will need the next useful result, that easily follows from the fact that a valuation domain is an "elementary divisor ring" (EDR). For definitions and basic results on EDRs we refer to [4, Chapter 3.6].

Theorem 1.5. Let $Y \subseteq X$ be finitely generated modules over the valuation domain R, with gen X = n, gen Y = k. Then $k \le n$, and there exists an ordered basis $\mathcal{G} = (x_1, x_2, \dots, x_n)$ of X, with \mathcal{G} -annihilator set B_1, \dots, B_n , such that $Y = \langle a_1 x_1, a_2 x_2, \dots, a_k x_k \rangle$, for suitable $a_1, \dots, a_k \in R$, where $a_j \notin B_j$, for $1 \le j \le k$.

The next lemma is folklore. We give a proof for the sake of completeness.

Lemma 1.6. Let R be a valuation domain, $X = \langle x_1, \ldots, x_n \rangle$, $Y = \langle a_1 x_1, \ldots, a_n x_n \rangle$ finitely generated R-modules, where gen X = gen Y = n $(a_i \in R)$. Then $X/Y = \bigoplus_{i=1}^n R(x_i + Y)$, where $R(x_i + Y) \cong R/a_i R$, for $1 \leq i \leq n$.

Proof. Let us verify that $X/Y = \bigoplus_{i=1}^n R(x_i + Y)$. Assume, for contradiction, that there exist elements $r_i \in R \setminus a_i R$, $i \in F \subseteq \{1, \ldots, n\}$, such that

$$\sum_{i \in F} r_i x_i \in Y.$$

Say $a_i = r_i t_i$, where $t_i \in P$ for all $i \in F$. Pick $j \in F$ such that $v(t_j)$ is maximum. Then $t_j r_i \in a_i R$, say $t_j r_i = s_i a_i$, for all $i \in F$, $i \neq j$. Multiplying the above relation by t_j , we get

$$a_j x_j + \sum_{i \in F, i \neq j} s_i a_i x_i \in t_j Y \subseteq PY.$$

It follows that gen $Y \leq n-1$, a contradiction. A similar argument shows that Ann $(x_i + Y) \subseteq a_i R$, for $1 \leq i \leq n$, and the reverse inclusion is trivial.

The final result of this section is also crucial to establish the next Theorem 2.4.

Proposition 1.7. Let $X = \langle x_1, \ldots, x_n \rangle$, $Y = \langle a_1 x_1, \ldots, a_n x_n \rangle$ be finitely generated modules over the valuation domain R, with gen X = gen Y = n ($a_i \in R$). For $1 \le i \le n$, define $X_0 = 0$, $X_i = \langle x_1, \ldots, x_i \rangle$, $Y_0 = 0$, $Y_i = \langle a_1 x_1, \ldots, a_i x_i \rangle$, $A_i = \text{Ann } (x_i + X_{i-1})$ and $B_i = \text{Ann } (a_i x_i + Y_{i-1})$. Then $B_i = a_i^{-1} A_i$, for $1 \le i \le n$.

Proof. Let us fix an index k, with $1 \le k \le n$. If k = 1, we readily get $B_1 = \operatorname{Ann}(a_1x_1) = a_1^{-1}A_1$, since $A_1 = \operatorname{Ann}(x_1)$. So we assume that $k \ge 2$. Pick any $s \in B_k$; then $sa_kx_k \in Y_{k-1} \subseteq X_{k-1}$ yields $sa_k \in A_k$, and hence we conclude that $B_k \subseteq a_k^{-1}A_k$. Conversely, let us verify that any $r \in a_k^{-1}A_k$ lies in B_k . Since $ra_k \in A_k$, we get

$$ra_k x_k = \sum_{i=1}^{k-1} q_i x_i \quad (\exists \ q_i \in R).$$

First suppose that a_i divides q_i , for all $i \leq k-1$; say $a_i s_i = q_i$. Then $ra_k x_k = \sum_{i=1}^{k-1} s_i a_i x_i \in Y_{k-1}$ yields $r \in B_k$. Assume now, for contradiction, that there is a nonempty subset F of $\{1, \ldots, k-1\}$ such

that, for all $i \in F$, $a_i = t_i q_i$, with $t_i \in P$. Choose $j \in F$ such that $v(t_j)$ is maximum. Then, multiplying the preceding relation by t_j , we easily get $a_j x_j \in \langle a_i x_i : 1 \leq i \leq k, i \neq j \rangle$, which implies that gen $Y \leq n-1$, against our hypothesis. The desired conclusion follows. \square

2. Multiplicative invariants. Let R be a commutative ring, (Γ, \cdot, \leq) a partially ordered semigroup, with commutative multiplication, and denote by $\operatorname{Fin} R$ the class of finitely generated R-modules. An invariant of $\operatorname{Fin} R$ is a map $\mu: \operatorname{Fin} R \to \Gamma$ such that $\mu(X) = \mu(Y)$ whenever the R-modules X,Y are isomorphic.

The invariant μ is said to be *multiplicative* if for any short exact sequence of finitely generated R-modules $0 \to Y \to X \to X/Y \to 0$ the following conditions are satisfied:

- (i) $\mu(X) = \mu(Y)\mu(X/Y)$;
- (ii) $\mu(Y) \leq \mu(X)$;
- (iii) if Z is a homomorphic image of X, then $\mu(Z) \leq \mu(X)$.

One might compare the above definition with that of length function of constructible modules, given by Ribenboim in [7, Section 2].

Example 2.1. We give a pair of examples of multiplicative invariants for Fin **Z**, the class of finitely generated Abelian groups. Let \mathbf{N}^{\times} be the multiplicative semigroup of strictly positive integers, and define a map μ_1 as follows: $\mu_1(G) = |G|$, if G is a finite Abelian group, and $\mu_1(G) = \infty$, if G is finitely generated and infinite. Adopting the usual conventions for the symbol ∞ , namely, $n < \infty$, $n \cdot \infty = \infty \cdot \infty = \infty$, for all $n \in \mathbf{N}^{\times}$, $\Gamma_1 = \mathbf{N}^{\times} \cup \{\infty\}$ becomes an ordered semigroup. Then Lagrange theorem shows that $\mu_1 : \operatorname{Fin} \mathbf{Z} \to \Gamma_1$ is a multiplicative invariant.

In the same spirit, consider the multiplicative semigroup $\Gamma_2 = \prod_{i>0} N_i \cup \{\infty\}$, where $N_i = \mathbf{N}^{\times}$ for all i>0, and the multiplication is pointwise. We endow $\Gamma_2 \setminus \{\infty\}$ either with the component-wise partial order, or with the lexicographic (total) order. In both cases, let $\mathcal{P} = \{p_i\}_{i>0}$ be the set of prime numbers and, for $m = \prod_{i>0} p_i^{n_i}$ a positive integer (where almost all the n_i are zero), define $s(m) = (p_i^{n_i})_{i>0} \in \prod_{i>0} N_i$. Then the map $\mu_2 : \operatorname{Fin} \mathbf{Z} \to \Gamma_2$ defined by $\mu_2(G) = s(|G|)$ if G is finite, and $\mu_2(G) = \infty$ otherwise, is a multiplicative invariant.

Proposition 2.2. Let μ be a multiplicative invariant of Fin R, where R is a commutative ring. Let $X = \langle x_1, \ldots, x_n \rangle$ be a finitely generated R-module, and, for $1 \leq i \leq n$, define $X_0 = 0$, $X_i = \langle x_1, \ldots, x_i \rangle$. If $X_i/X_{i-1} \cong R/A_i$ ($1 \leq i \leq n$), then $\mu(X) = \prod_{i=1}^n \mu(R/A_i)$. In particular, μ is determined by the values $\mu(R/I)$, where I is an ideal of R (possibly improper).

Proof. The desired formula follows at once by induction, using property (i). \Box

Let $\mu : \operatorname{Fin} R \to \Gamma$ be a multiplicative invariant, and $\varphi : \Gamma \to \Gamma_1$ an ordered morphism of partially ordered semigroups. Then, clearly, the map $\mu_1 = \varphi \circ \mu : \operatorname{Fin} R \to \Gamma_1$ is also a multiplicative invariant of $\operatorname{Fin} R$.

Lemma 2.3. Let μ be a multiplicative invariant of Fin R, where R is an integral domain. Then $\mu(R/yzR) = \mu(R/yR)\mu(R/zR)$, for all $y, z \in R$.

Proof. The exact sequence

$$0 \longrightarrow R/yR \longrightarrow R/yzR \longrightarrow R/zR \longrightarrow 0$$
 yields $\mu(R/yzR) = \mu(R/yR)\mu(R/zR)$.

In general, the property proved in Lemma 2.3 is valid only for cyclic modules with principal annihilator. We say that the multiplicative invariant μ is *valuative* if the following property holds

(iv)
$$\mu(R/I)\mu(R/J) = \mu(R/IJ)$$
, for all ideals I, J of R .

The reason for the choice of the term valuative, that derives from [7, Section 3], is explained in the forthcoming Remark 4.6. In the final section we will see that the invariants related to the so-called L-ranks do not satisfy (iv).

Now we take R to be a valuation domain, and denote by $\mathcal{I}(R)$ the multiplicative semigroup of the ideals of R (that includes the improper ideal R as the neutral element). We consider the total order on $\mathcal{I}(R)$ defined by I < J if and only if $I \supset J$.

We define a map $\mu_{\mathcal{I}}$: Fin $R \to \mathcal{I}(R)$ as follows:

if X is a finitely generated R-module, $\mu_{\mathcal{I}}(X) = B_1 \cdots B_n$, where B_1, \ldots, B_n is the \mathcal{G} -annihilator set of X, for some ordered basis \mathcal{G} of X

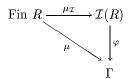
Theorem 2.4. Let R be a valuation domain. Then the map $\mu_{\mathcal{I}}$ is a well-defined multiplicative invariant of Fin R.

Proof. To simplify the notation, we write $\mu_{\mathcal{I}} = \mu$. Proposition 1.2 shows that μ is well-defined, since $\mu(X)$ does not depend on the choice of \mathcal{G} . We note that μ is also valuative, by definition. Let us prove that μ is multiplicative. The main point is to show that property (i) holds, that is, for any $Y \subseteq X$ finitely generated R-modules we have $\mu(X) = \mu(Y)\mu(X/Y)$. Applying Theorem 1.5, we choose an ordered set of generators $\mathcal{G} = (x_1, \ldots, x_n)$ of X, with \mathcal{G} -annihilator set B_1, \ldots, B_n such that $Y = \langle a_1 x_1, \ldots, a_k x_k \rangle$, for suitable $a_1, \ldots, a_k \in R$, with $a_j \notin B_j$ for all $j \leq k$. By induction on gen (X/Y) we may also assume that $a_i \in P$, for all $i \leq k$, so that $\mathcal{G}_0 = (a_1 x_1, \ldots, a_k x_k)$ and $\mathcal{G}_1 = (x_1 + Y, \ldots, x_n + Y)$ are ordered bases of Y and X/Y, respectively. By Proposition 1.7, the \mathcal{G}_0 -annihilator set of Y is $a_1^{-1}B_1, \ldots, a_k^{-1}B_k$. Moreover, using Lemma 1.6, it is easily seen that the \mathcal{G}_1 -annihilator set of X/Y is $a_1 R, \ldots, a_k R, B_{k+1}, \ldots, B_n$. It follows that $\mu(X) = \mu(Y)\mu(X/Y)$.

Now we easily see that (ii) holds, namely, $\mu(Y) = \prod_{i=1}^k a_i^{-1} B_i \le \mu(X) = \prod_{i=1}^n B_i$, since $\prod_{i=1}^k a_i^{-1} B_i \supseteq \prod_{i=1}^n B_i$. Similarly, an application of Lemma 1.4 shows that property (iii) holds. \square

The invariant $\mu_{\mathcal{I}}$ enjoys a universal property for valuative invariants.

Theorem 2.5. Let R be a valuation domain, μ : Fin $R \to \Gamma$ a valuative invariant. Then there exists an ordered morphism $\varphi : \mathcal{I}(R) \to \Gamma$ such that the following diagram commutes



Proof. Using Proposition 2.2, we easily see that it suffices to show that the map $\varphi: I \mapsto \mu(R/I)$ is an ordered morphism from $\mathcal{I}(R)$ to Γ . Since μ is valuative, we get $\varphi(IJ) = \mu(R/IJ) = \mu(R/I)\mu(R/J) = \varphi(I)\varphi(J)$. Moreover, if $I \leq J$, then, by definition, $I \supseteq J$, and so R/I is a quotient of R/J. Then property (iii) implies $\mu(R/I) \leq \mu(R/J)$, hence $\varphi(I) \leq \varphi(J)$.

Remark 2.6. The importance of the invariant $\mu_{\mathcal{I}}$ justifies our choice of the multiplicative notation for the semigroup Γ . As a matter of fact, in the next section we will use the traditional additive notation for the so-called generalized length functions, introduced in [6].

3. Generalities on length functions. For the basic concepts, we will follow the ideas and terminology introduced by Northcott and Reufel [6] and developed by Vámos [11]. Although not strictly necessary at a first stage, we prefer to work in a commutative environment.

Let R be a commutative ring, and denote by $\mathbf{R}_{\geq 0}$ the set of the nonnegative real numbers. An $Archimedean\ function$ of $\mathrm{Mod}\ R$ is a map $\ell:\mathrm{Mod}\ R\to\mathbf{R}_{\geq 0}\cup\{\infty\}$ such that $\ell(M)=\ell(N)$ whenever the R-modules M,N are isomorphic. Note that $(\mathbf{R}_{\geq 0}\cup\{\infty\},+,\leq)$ becomes an ordered additive semigroup, once we assume the usual conventions for the symbol ∞ , namely, for any $r\in\mathbf{R}_{\geq 0},\ r<\infty,\ r+\infty=\infty+\infty=\infty$. This semigroup is also complete, that is, any nonempty subset has sup and inf. However, note that $\mathrm{Im}\ (\ell)=\{\ell(M):M\in\mathrm{Mod}\ R\}$, the image of ℓ , in general neither is a subsemigroup, nor is complete in the partial order induced by $\mathbf{R}_{\geq 0}\cup\{\infty\}$.

The Archimedean function ℓ is said to be additive if for any short exact sequence of R-modules $0 \to N \to M \to M/N \to 0$ we have $\ell(M) = \ell(N) + \ell(M/N)$. An additive function automatically satisfies $\ell(N) \le \ell(M)$ and $\ell(M/N) \le \ell(M)$, for any R-modules $N \subseteq M$.

We note at once that there exist additive functions that are meaningless. Namely, we say that the additive function ℓ is trivial if its set of values is a singleton, which, necessarily, is either $\{0\}$ or $\{\infty\}$. In what follows, any additive function considered will be automatically assumed to be nontrivial. Note that $\ell(0) = 0$ when ℓ is additive and nontrivial.

Of course, every additive function ℓ gives raise to a multiplicative invariant μ , just restricting ℓ to Fin R and defining $\mu(X) = e^{\ell(X)}$ (with the convention $e^{\infty} = \infty$).

The Archimedean function ℓ is said to be *upper continuous* if, for any R-module M, $\ell(M) = \sup\{\ell(X)\}$, where X ranges over the finitely generated submodules of M. Note that the upper continuity of ℓ implies that $\ell(N) \leq \ell(M)$ whenever $N \subseteq M$. Moreover, ℓ is upper continuous if and only if, for any set of R-modules $\{N_{\alpha}\}_{\alpha<\lambda}$, we have $\ell(\sum_{\alpha<\lambda}N_{\alpha})=\sup\{\ell(N_{\alpha}):\alpha<\lambda\}$ (cf. [11, Proposition 8]).

The standard examples of additive invariants are the dimension of vector spaces, when R is a field, the torsion-free rank of R-modules, when R is an integral domain, and, for an arbitrary ring R, the Jordan-Holder length of R-modules. Of course, these three invariants are upper continuous, as well.

Following [6], an additive upper continuous function is called (generalized) length function.

For any assigned length functions ℓ_1 , ℓ_2 of Mod R and nonnegative real numbers α, β , it is clear that $\alpha \ell_1 + \beta \ell_2$ is also a length function. However, this obvious fact will not be relevant for our discussion.

For M an R-module, we denote by \mathcal{F}_M the set of the finitely generated submodules of M.

Remark 3.1. We will mostly deal with generalized length functions, the more interesting and useful case. However, one may easily see that the notions of additive and upper continuous are independent, even for Archimedean functions of the class of Abelian groups or vector spaces. Consider the following examples.

- (a) Let us split the set \mathcal{P} of prime numbers as $\mathcal{P} = H_1 \cup H_2$, where H_1, H_2 are disjoint and nonempty. We define ℓ on the class of Abelian groups as follows: if G is an infinite Abelian group, then $\ell(G) = \infty$; if G_p is a finite p-group, with $p \in H_1$, then $\ell(G_p) = 0$; if G_q is a finite q-group, with $q \in H_2$, then $\ell(G_q) = \log |G_q|$; if G is any finite group, then $\ell(G)$ is the sum of the invariants of its primary components. A direct and easy verification shows that ℓ is an additive function (cf. [3]). However, ℓ is not upper continuous. For instance, if $p \in H_1$ and G is any infinite p-group, then $\ell(G) = \infty$ but $\ell(X) = 0$ for any finite subgroup X of G.
- (b) Let Q be a field. We define an Archimedean function ℓ_1 of Q-vector spaces as follows: $\ell_1(V) = 0$ if $\dim_Q(V) \leq 1$, $\ell_1(W) = \dim_Q(W)$ if $\dim_Q(W) \geq 2$. It is clear that ℓ_1 is upper continuous, but not additive.

We have an immediate additive version of Proposition 2.2.

Proposition 3.2. Let ℓ be an additive function of Mod R, where R is an integral domain. Let $X = \langle x_1, \ldots, x_n \rangle$ be a finitely generated R-module, and, for $1 \leq i \leq n$, define $X_0 = 0$, $X_i = \langle x_1, \ldots, x_i \rangle$. If $X_i/X_{i-1} \cong R/A_i$ $(1 \leq i \leq n)$, then $\ell(X) = \sum_{i=1}^n \ell(R/A_i)$.

From Proposition 3.2 and upper continuity, we at once get the following result.

Proposition 3.3. Let ℓ be a length function of $\operatorname{Mod} R$, where R is an integral domain. Then ℓ is completely determined by the values $\ell(R/I)$, as I ranges over the ideals of R.

The following lemma is related to Proposition 3 and Theorem 1 of [11]. The second somehow technical property will be needed in the final section.

Lemma 3.4. Let ℓ be an upper continuous function of Mod R, where R is a commutative ring.

- (i) ℓ is additive if and only if for any short exact sequence of R-modules $0 \to N \to X \to X/N \to 0$, with X finitely generated, we have $\ell(X) = \ell(N) + \ell(X/N)$.
- (ii) Let the following additional condition be satisfied: for any R-modules $N \subseteq X$ with X finitely generated, $\ell(X/N) = \inf \{\ell(X/Y) : Y \in \mathcal{F}_N\}$. Then ℓ is additive if and only if for any short exact sequence $0 \to Y \to X \to X/Y \to 0$, with X, Y finitely generated, we have $\ell(X) = \ell(Y) + \ell(X/Y)$.

Proof. (i) Let us consider an arbitrary exact sequence of R-modules

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

For any finitely generated submodule X of M we get the exact sequence

$$0 \longrightarrow N \cap X \longrightarrow X \longrightarrow (X+N)/N \longrightarrow 0;$$

hence, by hypothesis, we have $\ell(X) = \ell(N \cap X) + \ell((X+N)/N) \le \ell(N) + \ell(M/N)$. Since $\ell(M) = \sup\{\ell(X) : X \in \mathcal{F}_M\}$, we get the inequality $\ell(M) \le \ell(N) + \ell(M/N)$. To end the proof, we must verify the reverse inequality. Let us take an arbitrary $X \in \mathcal{F}_M$. By hypothesis we have $\ell(M) \ge \ell(X) = \ell(X \cap N) + \ell(X/X \cap N)$; hence, we get

$$\ell(M) \ge \sup \{\ell(X \cap N) + \ell(X/X \cap N) : X \in \mathcal{F}_M\}.$$

Since $N = \sum_{X \in \mathcal{F}_M} X \cap N$ and ℓ is upper continuous, $\ell(N) = \sup\{\ell(X \cap N) : X \in \mathcal{F}_M\}$. Moreover, since for each $Y \in \mathcal{F}_N$ and each $Z \in \mathcal{F}_{M/N}$ there exists an $X \in \mathcal{F}_M$ such that $Z \cong X/X \cap N$ and $Y \subseteq X \cap N$, we get

$$\ell(M) \ge \ell(X) = \ell(X \cap N) + \ell(X/X \cap N) \ge \ell(Y) + \ell(Z);$$

hence, the desired inequality $\ell(M) \ge \ell(N) + \ell(M/N)$ follows.

(ii) By the above proof, it suffices to show that ℓ is additive on the exact sequences

$$0 \longrightarrow N \longrightarrow X \longrightarrow X/N \longrightarrow 0$$

where X is finitely generated. Pick any $Y \in \mathcal{F}_N$. By hypothesis, we have $\ell(Y) + \ell(X/Y) = \ell(X)$; hence, $\ell(N) + \ell(X/Y) \ge \ell(X)$. Thus we get the inequality

$$\ell(X) \le \ell(N) + \inf\{\ell(X/Y) : Y \in \mathcal{F}_N\} = \ell(N) + \ell(X/N).$$

Conversely, from the equality $\ell(X) = \ell(Y) + \ell(X/Y)$ we get $\ell(X/N) + \ell(Y) \leq \ell(X)$, since $\ell(X/N) \leq \ell(X/Y)$ for all $Y \in \mathcal{F}_N$. Taking the sup for $Y \in \mathcal{F}_N$ we get $\ell(X/N) + \ell(N) \leq \ell(X)$. We have thus proved the equality $\ell(X) = \ell(X/N) + \ell(N)$. \square

Example 3.5. It is worth showing that (i) in the preceding lemma is no longer valid if the invariant is not upper continuous. Let $p \neq q$ be prime numbers, V_p (respectively V_q) an infinite direct sum of copies of $\mathbf{Z}/p\mathbf{Z}$ (respectively $\mathbf{Z}/q\mathbf{Z}$). Consider the Archimedean function ℓ of the class of Abelian groups defined as follows: $\ell(X) = 0$ if X is a finitely generated Abelian group, $\ell(V_p \oplus V_q) = 1$, $\ell(G) = \infty$ otherwise. It is clear that ℓ is not additive, but it trivially satisfies additivity on those

short exact sequences whose middle term is finitely generated, since then all terms are finitely generated.

Let us also remark that, even in the case where ℓ is upper continuous, (ii) can fail without the technical hypothesis $\ell(X/N) = \inf \{ \ell(X/Y) :$ $Y \in \mathcal{F}_N$. Let R be a valuation domain whose maximal ideal P is not finitely generated. Define an Archimedean function ℓ on Mod Rin the following way: if X is a finitely generated R/P-module, let $\ell(X) = \dim_{R/P}(X)$; if M is any R-module, then $\ell(M) = \sup\{\ell(X) : \ell(X) = \ell(X) = \ell(X) \}$ $X \in \mathcal{F}_M$, PX = 0. Then ℓ is upper continuous by definition, and the sequence $0 \to P \to R \to R/P \to 0$ shows that ℓ is not additive. As a matter of fact, the referee of the present paper observed that, if R is not almost maximal, then ℓ is not even additive on those short exact sequences with all terms finitely generated. However, under the additional assumption that R is almost maximal, one may show that if $Y \subseteq X$ are finitely generated R-modules, then $\ell(X) = \ell(Y) + \ell(X/Y)$. The proof of this fact is technical and rather long. It uses the linear compactness of the proper quotients of R. We omit this proof, since it is not relevant for the present paper.

Remark 3.6. In Proposition 3 and Theorem 1 of [11] it is shown how to extend, by upper continuity, an additive function of a full subcategory $\mathcal C$ of $\operatorname{Mod} R$ to an additive function of all $\operatorname{Mod} R$. It is worth showing that a similar idea is not applicable to general multiplicative invariants $\mu : \operatorname{Fin} R \to \Gamma$. For this reason we had to define $\mu(X)$ only for finitely generated R-modules X, and, actually, Ribenboim in [7] confined his discussion to constructible R-modules, a subclass of finitely presented modules. To begin with, $\operatorname{Fin} R$ is not a full subcategory of $\operatorname{Mod} R$, since submodules of finitely generated modules need not be finitely generated. Actually, this difficulty is also present for additive functions, but in that case it might be overcome like in the preceding Lemma 3.4. Moreover, the ordered semigroup Γ is not necessarily complete. However, the crucial property, needed by Γ to make the proof of Lemma 3.4 work, is the following

(*) if U_1 , U_2 are subsets of Γ , then $\sup(U_1) \sup(U_2) = \sup(U_1 U_2)$.

It is enjoyed by $(\mathbf{R}_{\geq 0} \cup \{\infty\}, +, \leq)$ but not by any complete semi-group. As a matter of fact, the main ordered semigroup we consider, namely $\mathcal{I}(R)$, is complete: if $A = \{I_{\lambda}\}_{\lambda} \subseteq \mathcal{I}(R)$, then $\sup(A) = \bigcap_{\lambda} I_{\lambda}$

and $\inf(A) = \bigcup_{\lambda} I_{\lambda}$. However, if the valuation domain R contains a prime ideal L which is neither maximal nor zero and satisfies $L \neq L^2$, then $\mathcal{I}(R)$ does not satisfy (*). Let A be the set of ideals that properly contain L. Then $L = \bigcap_{I \in A} I$, and $IJ \supset L$ for all $I, J \in A$. It follows that $\sup(A) = L = \sup(A^2) \neq \sup(A) \sup(A) = L^2$. If we now extend $\mu_{\mathcal{I}}$ to $\operatorname{Mod} R$ by upper continuity, defining, for an R-module M, $\mu_{\mathcal{I}}(M) = \sup\{\mu_{\mathcal{I}}(X) : X \in \mathcal{F}_M\}$, we get an invariant which is not multiplicative. In fact, let $N = \bigoplus_{I \in A} R/I$, and consider the exact sequence

$$0 \longrightarrow N \longrightarrow N \oplus N \longrightarrow N \longrightarrow 0.$$

It is easy to verify that $\mu_{\mathcal{I}}(N) = L = \mu_{\mathcal{I}}(N \oplus N) \neq \mu_{\mathcal{I}}(N) \mu_{\mathcal{I}}(N) = L^2$; hence the extension of $\mu_{\mathcal{I}}$ to Mod R is not multiplicative.

We say that the additive function is singular if $Im(\ell) = \{0, \infty\}$. The additive function ℓ is called infinite (or non-singular) if $0 < \ell(M) < \infty$, for some $M \in Mod R$. Note that the property $\ell(M \oplus N) = \ell(M) + \ell(N)$ implies that the image of an infinite additive function is an infinite set. The additive function ℓ is called discrete if $Im(\ell) \setminus \{\infty\}$ is a discrete subset of $\mathbf{R}_{>0}$.

The following easy lemma was proved in [6]. The natural properties of its statement will be taken for granted, and applied without mentioning the lemma.

Lemma 3.7. Let ℓ be an additive function of Mod R, where R is an integral domain. Then

- (1) if $I \subseteq J$ are ideals of R, then $\ell(R/J) \le \ell(R/I)$;
- (2) for all $y, z \in R$ we have $\ell(R/yzR) = \ell(R/yR) + \ell(R/zR)$. In particular, $\ell(R/y^nR) = n\ell(R/yR)$, for all n > 0.

Now we take R to be a valuation domain, with maximal ideal P and field of quotients Q. By v we denote a fixed valuation on Q such that $R_v = R$.

We recall the following standard property of valuation domains: if L is a prime ideal of R such that $L \neq L^2$, pick any $y \in L \setminus L^2$; then $L = \langle y/a : a \in R \setminus L \rangle$ and $L^{n+1} = yL^n$, for every n > 0.

From now on, we will deal with additive functions which are upper continuous, that is, ℓ will always be a length function in the sense of [6].

Lemma 3.8. Let R be a valuation domain, ℓ a length function of $\operatorname{Mod} R$, and L a prime ideal of R such that $L \neq L^2$. Then

- (1) $\ell(R/L) = \ell(R/yR)$ for all $y \in L \setminus L^2$;
- (2) $\ell(R/L^n) = n \, \ell(R/L)$, for all n > 0.

Proof. In case $\ell(R/L) = \infty$ our assertions readily follow from $\ell(R/yR) \ge \ell(R/L)$. Thus we assume that $\ell(R/L) < \infty$. For $y \in L \setminus L^2$, we consider the exact sequence

$$0 \longrightarrow L/yR \longrightarrow R/yR \longrightarrow R/L \longrightarrow 0.$$

Since $\ell(R/yR) = \ell(R/L) + \ell(L/yR)$, it suffices to show that $\ell(L/yR) = 0$. Recall that $L = \langle y/a : a \in R \setminus L \rangle$; hence $L/yR = \bigcup_{a \notin L} (y/a)R/yR$. Now observe that $\ell(R/aR) = 0$ for all $a \in R \setminus L$. In fact, we have $a^nR \supset L$ for all n > 0, since L is a prime ideal, hence $n\ell(R/aR) = \ell(R/a^nR) \le \ell(R/L) < \infty$ for all n. This is possible only if $\ell(R/aR) = 0$. Since $R/aR \cong (y/a)R/yR$, and ℓ is upper continuous, we conclude that $\ell(L/yR) = 0$, as well. Thus, we have proved (1). In order to verify (2), we recall that $L^n = y^{n-1}L$ for all n > 0. Hence we derive the exact sequence

$$0 \longrightarrow L/yL \longrightarrow R/L^n \longrightarrow R/L^{n-1} \longrightarrow 0.$$

By induction, (2) follows if we prove that $\ell(L/yL) = \ell(R/L)$. This last fact is true, since $L/yL = \bigcup_{a \notin L} (y/a)R/yL$, and $(y/a)R/yL \cong R/aL = R/L$ for all $a \in R \setminus L$.

The ideals defined in the next proposition were introduced in [6, Section 3], and point (i) of the result also follows from the discussion there.

Proposition 3.9. Let R be a valuation domain, ℓ a length function of Mod R. Consider the ideals $L_{\ell} = \langle y \in R : \ell(R/yR) > 0 \rangle$, and $L_1 = \langle y \in R : \ell(R/yR) = \infty \rangle$. Then

(i) L_{ℓ} , L_{1} are prime ideals of R, and no prime ideal lies properly between L_{ℓ} and L_{1} . If the ideal I properly contains L_{ℓ} , then $\ell(R/I) = 0$; if I properly contains L_{1} , then $\ell(R/I) < \infty$; if I is properly contained in L_{1} , then $\ell(R/I) = \infty$; if $L_{\ell} \neq L_{1}$, then $\ell(R/L_{1}) = \infty$.

- (ii) If ℓ is discrete and infinite, then $0 < \ell(R/L_{\ell}) < \infty$. Moreover $L_{\ell} = L_{\ell}^2$ if and only if $L_{\ell} = L_1$.
 - (iii) If ℓ is non-discrete, then $L_{\ell} \neq L_1$, $\ell(R/L_{\ell}) = 0$ and $L_{\ell} = L_{\ell}^2$.

Proof. To simplify the notation, we write $L = L_{\ell}$. Note that $1 \notin L$, since $\ell(R/R) = \ell(0) = 0$. Hence both L and $L_1 \subseteq L$ are proper ideals.

- (i) For $a,b \in R \setminus L$ we get $\ell(R/abR) = \ell(R/aR) + \ell(R/bR) = 0$, hence $ab \notin L$. So L is a prime ideal. In a similar way we see that L_1 is prime, as well. If the ideal I contains an element $a \notin L$ (respectively $a \notin L_1$), then $\ell(R/I) \leq \ell(R/aR) = 0$ (respectively $\ell(R/I) \leq \ell(R/aR) < \infty$). If $b \in L_1 \setminus I$, then $\infty = \ell(R/bR) \leq \ell(R/I)$. Finally, assume that there is a prime ideal $J \subset L$, take any $z \in J$, and fix $y \in L \setminus J$. Then $J \subseteq \bigcap_{n>0} y^n R$, whence $\ell(R/zR) \geq \ell(R/J) \geq \ell(R/y^n R) = n \ell(R/yR)$, for all n > 0. Since, by the definition of L, $\ell(R/yR) > 0$, we get $\ell(R/J) = \ell(R/zR) = \infty$, hence $J \subseteq L_1$, since z was arbitrary. In particular, it follows that $\ell(R/L_1) = \infty$ when $L \neq L_1$.
- (ii) Since ℓ is infinite and discrete, we may assume without loss of generality that $\operatorname{Im}(\ell)\subseteq \mathbf{N}$. If $\ell(R/L)\in\{0,\infty\}$, using (i) we easily get $\ell(R/I)\in\{0,\infty\}$, for any ideal I of R. Then Proposition 3.3 shows that $\ell(M)\in\{0,\infty\}$ for any R-module M, impossible. Assume now that $L=L^2$, and pick any $y\in L$. For every n>0 we can write $y=z_1\cdots z_n$, with $z_i\in L$. Then we get $\ell(R/yR)=\sum_{i=1}^n\ell(R/z_iR)\geq n$; hence, $\ell(R/yR)=\infty$, since n>0 was arbitrary. It follows that $L=L_1$. Conversely, if $L\neq L^2$, then Lemma 3.8 shows that $\ell(R/yR)=\ell(R/L)<\infty$ for any $\ell(R/L)<\infty$ for any $\ell(R/L)<\infty$ for any $\ell(R/L)<\infty$
- (iii) Assume, for a contradiction, that $L \neq L^2$. Hence, by Lemma 3.8, $\ell(R/L) = \ell(R/yR) > 0$, for all $y \in L \setminus L^2$. Take any ideal I of R. If $I \supset L$, then $\ell(R/I) = 0$, by (i). If $I \subseteq \bigcap_{n>0} L^n$, then Lemma 3.8 shows that $\ell(R/I) \geq n\ell(R/L)$, for all n > 0, whence $\ell(R/I) = \infty$. So assume that $L^k \supseteq I \supset L^{k+1}$. Then there exist $z_1, \ldots, z_k \in L \setminus L^2$ such that $z_1 \cdots z_k \in I$. Since by Lemma 3.8 we have $\ell(R/z_iR) = \ell(R/L)$ for $1 \leq i \leq k$, we get $k\ell(R/L) = \ell(R/L^k) \leq \ell(R/I) \leq \ell(R/z_1 \cdots z_k R) = \sum_{i=1}^k \ell(R/z_i R) = k\ell(R/L)$. We conclude that $\ell(R/I)$ is either ∞ or an integral multiple of $\ell(R/L)$, for any ideal I of R. Then from Proposition 3.3 we derive that ℓ is discrete, against our present assumption.

Now we exclude that $L=L_1$. Otherwise, for any ideal $I\neq L$, we either get $\ell(R/I)=0$, when $I\supset L$, or $\ell(R/I)=\infty$, when $I\subset L_1=L$.

Again we would conclude that $\ell(R/I)$ is either ∞ or an integral multiple of $\ell(R/L)$, impossible.

Finally, let us define $\delta = \inf \{ \ell(R/yR) : y \in L \}$. Take any $y \in L \setminus L_1$ and n > 0. Then, since $L = L^n$, we get $y = y_1 \cdots y_n$, for suitable $y_i \in L$. It follows that $\ell(R/yR) = \sum_{i=1}^n \ell(R/y_iR) \ge n\delta$. This is possible only if $\delta = 0$, since both y and n were arbitrary. Then $\ell(R/L) \le \ell(R/yR)$ for every $y \in L$, yields $\ell(R/L) \le \delta = 0$. As a by-product, we have also seen that there exists a sequence $\{y_n\}_{n>0}$ of elements of L such that $\ell(R/y_nR) = \alpha_n > 0$, and the real numbers α_n converge to zero. \square

It is worth noting that the set $\{y \in R : \ell(R/yR) > 0\}$ is nonempty, and so this set actually coincides with L_{ℓ} . In fact, assume for contradiction that $\ell(R/yR) = 0$ for every $y \in R$. Then $\ell(R/I) = 0$ for any ideal I of R; hence, Proposition 3.3 yields $\ell(M) = 0$ for any R-module M, so ℓ is trivial, against our standing assumption. On the other hand, it is possible that $\{y \in R : \ell(R/yR) = \infty\} = \emptyset$. In fact, this happens exactly when $\ell = \text{rank}$. In that case we have $L_1 = \langle \emptyset \rangle = 0$.

We will say that L_{ℓ} is the associated prime ideal of ℓ .

4. Description of length functions. In this final section we reobtain a description of length functions over valuation domains. Our main Theorem 4.7, based on the multiplicative invariant $\mu_{\mathcal{I}}$, uses a completely different method from that in [6] and provides some new information. Other results, like the next Proposition 4.2, could be obtained by the discussion in [6]. We also give a proof of these results, for the sake of completeness, and to make our paper self-contained.

As a first step, we examine the singular length functions. This is not a trivial case, as one might guess. Clearly, under the present circumstances, from $\text{Im}(\ell) = \{0, \infty\}$ we get $L_{\ell} = L_1$. The following result characterizes the singular length functions over valuation domains. We omit the proof, that can be obtained adapting that of the next Proposition 4.2.

Theorem 4.1. Let R be a valuation domain, ℓ a singular length function of $\operatorname{Mod} R$, M an R-module. Then

(a) when $\ell(R/L_{\ell}) = 0$, $\ell(M) = 0$ if and only if M is an R/L_{ℓ} -module;

(b) when $\ell(R/L_{\ell}) = \infty$, $\ell(M) = 0$ if and only if M is a torsion R/L_{ℓ} -module.

Conversely, let L be a prime ideal of the valuation domain R.

- (1) If $L \neq L^2$, the map ℓ on $\operatorname{Mod} R$ defined by $\ell(M) = 0$ if M is a torsion R/L-module, and $\ell(M) = \infty$ otherwise, is the unique singular length function such that $L = L_{\ell}$;
- (2) if $L = L^2$, there exist exactly two singular length functions ℓ_1 and ℓ_2 of Mod R with associated prime ideal L, respectively defined by: $\ell_1(M) = 0$ if M is an R/L-module, and $\ell_1(M) = \infty$ otherwise; $\ell_2(M) = 0$ if M is a torsion R/L-module, and $\ell_2(M) = \infty$ otherwise.

Now we examine the infinite length functions of $\operatorname{Mod} R$, and show that they lie in two disjoint classes. The first one is characterized by the following proposition, which is an alternative version of [6, Theorem 6].

Proposition 4.2. Let R be a valuation domain.

- (1) Let ℓ be an infinite length function of $\operatorname{Mod} R$ such that $L_{\ell} = L_1 = \langle y \in R : \ell(R/yR) = \infty \rangle$. For every R-module M we have $\ell(M) = \ell(R/L_{\ell})\operatorname{rank}_{R/L_{\ell}}(M)$, when M is an R/L_{ℓ} -module, and $\ell(M) = \infty$, otherwise. Moreover, necessarily, $0 < \ell(R/L_{\ell}) < \infty$ and $L_{\ell} = L_{\ell}^2$.
- (2) Conversely, let L be an assigned prime ideal of R such that $L=L^2$. For any real number $\alpha>0$, the Archimedean function of $\operatorname{Mod} R$ defined by $\ell(M)=\alpha \operatorname{rank}_{R/L}(M)$, when M is an R/L-module, and $\ell(M)=\infty$, otherwise, is a length function.
- Proof. (1) To simplify the notation, we write $L=L_\ell$. It suffices to prove our statement for every finitely generated R-module X. So, let $A_1\subseteq\cdots\subseteq A_n$ be the annihilator sequence of X. First assume that X is not an R/L-module. Then $\operatorname{Ann}(X)=A_1\subset L$, and therefore, choosing $z\in L\setminus A_1$, we get $\ell(X)\geq \ell(R/A_1)\geq \ell(R/zR)=\infty$. Assume now that X is an R/L-module, or, equivalently, that $A_1\supseteq L$. If $A_i\supset L$ for $1\leq i\leq m$, then X is a torsion R/L-module, and $\ell(X)=\sum_{i=1}^n\ell(R/A_i)=0=\ell(R/L_\ell)$ rank $_{R/L}(X)$. Otherwise, assume that $L=A_1=\cdots=A_k\subset A_{k+1}\subseteq\cdots\subseteq A_n$. Then $X=U\oplus Y$, where U is the direct sum of k copies of R/L, and Y is a torsion R/L-module. It easily follows that $\ell(X)=k\,\ell(R/L)=\ell(R/L)$ rank $_{R/L}(X)$. As a by-

product, we have also shown that ℓ is discrete. Then $0 < \ell(R/L_{\ell}) < \infty$ and $L_{\ell} = L_{\ell}^2$ follow from Proposition 3.9.

(2) It suffices to show that $\ell(X) = \ell(N) + \ell(X/N)$, for any modules $N \subseteq X$, with X finitely generated. If X is an R/L-module, then both N and X/N are R/L-modules, and the desired equality follows, since $\operatorname{rank}_{R/L}$ is a length function of $\operatorname{Mod}(R/L)$. If X is not an R/L-module, then, by definition, $\ell(X) = \infty$. Recall that $\operatorname{Ann}(X) \subset L$. If now $\operatorname{Ann}(N) \subset L$, then $\ell(N) = \infty$ and the desired equality reduces to $\infty = \infty$. Then assume that $\operatorname{Ann}(N) \supseteq L$, and pick any $x \in X$ such that $\operatorname{Ann}(x) \subset L$. Since $L = L^2$, we may take $r_1, r_2 \in L$ such that $r_1 r_2 \notin \operatorname{Ann}(x)$. Then $r_1 r_2 x \neq 0$ implies that $r_2 x \notin N$, since $r_1 N = 0$. It follows that $r_2 \notin \operatorname{Ann}(x+N)$, hence $\operatorname{Ann}(x+N) \subset L$. We conclude that X/N is not an R/L-module, hence from $\ell(X/N) = \infty$ we get the desired equality. \square

The length functions as in Proposition 4.2 are called *L*-rank functions. By the definition, they are all discrete. Note that no *L*-rank function ℓ can be valuative. Indeed, from $0 < \ell(R/L) < \infty$ we get $\ell(R/L^2) = \ell(R/L) \neq \ell(R/L) + \ell(R/L)$.

Proposition 4.3. Let R be a valuation domain, ℓ an infinite length function of Mod R, such that $L_{\ell} \neq L_1$. Then $\ell(R/I) = \inf{\{\ell(R/yR) : y \in I\}}$ for every ideal I of R. In particular, ℓ is completely determined by the values $\ell(R/rR)$, $r \in R$.

Proof. We write $L = L_{\ell}$. Note that ℓ is not an L-rank, since $L \neq L_1$. Let I be any ideal of R. If $I \supset L$, then $\ell(R/I) = 0 = \ell(R/rR)$, for all $r \in I \setminus L$, and if $I \subseteq L_1$, then $\ell(R/I) = \infty = \ell(R/rR)$, for all $r \in I$. These facts follow from Proposition 3.9. Thus we may assume that $L \supseteq I \supset L_1$. We have to distinguish two cases, according to whether ℓ is discrete or not. Assume that ℓ is discrete. Since $\ell \neq L_1$, we get $\ell \neq L_2$, by Proposition 3.9 (ii). So, if $\ell \neq L_2$ if for some $\ell \neq L_1$ for some $\ell \neq L_2$ is discrete. Since $\ell \neq L_1$, for all $\ell \neq L_2$ is discrete.

Let us now assume that ℓ is non-discrete. We start observing that the set $D = \{\ell(R/yR) < \infty : y \in R\}$ is dense in $\mathbf{R}_{\geq 0}$. This fact follows easily, recalling that, by the proof of Proposition 3.9 (iii), there

exists a sequence $\{y_n\}_{n\geq 0}\subset L$ such that the values $\ell(R/y_nR)$ converge to zero. Then consider a non-principal ideal I, with $L\supseteq I\supset L_1$. By the density of D there exists a sequence $\{r_n\}_{n>0}\subseteq R$ such that $\ell(R/I)<\ell(R/r_nR)$, for all n, and $\ell(R/I)=\inf\{\ell(R/r_nR):n>0\}$. Since $\ell(R/I)<\ell(R/yR)$ implies $y\in I$, we get the desired equality $\ell(R/I)=\inf\{\ell(R/yR):y\in I\}$.

Remark 4.4. It is worth remarking that the values $\ell(R/rR)$ do not determine ℓ , when the length function ℓ is an L-rank, with $L \neq 0$. Indeed, under these circumstances we get $\ell(R/rR) \in \{0, \infty\}$ for every $r \in R$, hence ℓ is not determined by these values.

Theorem 4.5. Let ℓ be a length function of $\operatorname{Mod} R$, where R is a valuation domain. Then either ℓ is an L-rank function, for some prime ideal L of R, or it is valuative.

Proof. Let us assume that ℓ is not an L-rank. Hence $L_{\ell} \neq L_1$, and we are in a position to apply Proposition 4.3. Take any two ideals I, J of R. We have

$$\ell(R/I) + \ell(R/J) = \sup\{\ell(R/yR) : y \in I\} + \sup\{\ell(R/zR) : z \in J\}$$

= \sup\{\ell(R/yzR) : y \in I, z \in J\} = \ell(R/IJ).

We have thus seen that ℓ is valuative.

Remark 4.6. Ribenboim in [7] calls a length function valuative if $\ell(R/\sum_{i=1}^n a_i R) = \min\{\ell(R/a_i R) : 1 \leq i \leq n\}$, for every finitely generated ideal $\sum_{i=1}^n a_i R$ of R. Such a condition is trivially verified when R is a valuation domain, whence the name. From the proof of Theorem 4.5 and Proposition 4.3 we easily derive that $\ell(R/I) = \inf\{\ell(R/yR) : y \in I\}$ for any ideal I if and only if $\ell(R/IJ) = \ell(R/I) + \ell(R/J)$, for all ideals I, J. For this reason we have called valuative the multiplicative invariants that satisfy condition (iv) of the second section.

For the purposes of our final result, we make some remarks on the valuations associated to a fixed valuation domain R of rank one. If v_1, v_2 are two valuations of rank one of the field Q that determine the

same valuation domain $R = R_{v_1} = R_{v_2}$, then $v_1(Q^{\times})$ and $v_2(Q^{\times})$ are isomorphic ordered subgroups of **R**. Then $v_1(Q^{\times}) = \alpha v_2(Q^{\times})$ for a suitable real number $\alpha > 0$, and, as a consequence, $v_1 = \alpha v_2$. These facts are well known and easy to verify.

Let L be a prime ideal of R which is not a union of a strictly ascending chain of prime ideals. Then L properly contains a largest prime ideal J (say), namely the union of the primes strictly contained in L. We say that J is the *immediate successor* of L. Under these circumstances, we denote by $v_{L/J}$ a fixed valuation of the rank one valuation domain R_L/J ; recall that the value group of $v_{L/J}$ is an ordered subgroup of the real numbers. For I an ideal of R, we define

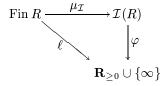
$$v_{L/J}(I) = \inf \{ v_{L/J}(x+J) : x \in I \}.$$

In particular, $v_{L/J}(I) = 0$ if $I \supset L$, and $v_{L/J}(I) = \infty$ if $I \subseteq J$. For any ideal I of R, it is straightforward to check that $v_{L/J}(I)$ coincides with $v_{L/J}(IR_L + J)/J$, and $v_{L/J}(I) = \inf\{v_{L/J}(rR) : r \in I\}$.

In Proposition 3.9 we have seen that for any length function ℓ either $L_{\ell} = L_1$, or L_1 is the immediate successor of L_{ℓ} . Moreover, Proposition 4.2 and Theorem 4.5 show that $L_{\ell} \neq L_1$, whenever ℓ is valuative.

Theorem 4.7. Let R be a valuation domain.

(1) If ℓ is a valuative length function of $\operatorname{Mod} R$, then there exists a real number $\alpha > 0$ such that the map $\varphi : \mathcal{I}(R) \to \mathbf{R}_{\geq 0} \cup \{\infty\}$, $\varphi : I \mapsto \alpha \, v_{L_{\ell}/L_1}(I)$, is a morphism of ordered semigroups that makes the following diagram commute



(2) Conversely, let L be a prime ideal having an immediate successor J, $\alpha > 0$ a real number, $v_{L/J}$ a fixed valuation of the rank one valuation domain R_L/J . Then the map ℓ : Fin $R \to \mathbf{R}_{\geq 0} \cup \{\infty\}$, defined by $\ell(X) = \alpha v_{L/J}(\mu_{\mathcal{I}}(X)), X \in \text{Fin } R$, extends to a unique valuative

length function of $\operatorname{Mod} R$ such that $L_{\ell} = L$ and $L_1 = J$. Moreover ℓ is discrete if and only if $L \neq L^2$.

Proof. (1) Since ℓ is valuative, the map $\varphi : \mathcal{I}(R) \to \mathbf{R}_{\geq 0} \cup \{\infty\}$ defined by $\varphi : I \mapsto \ell(R/I)$ is a morphism of ordered semigroups, and, obviously $\ell = \varphi \circ \mu_{\mathcal{I}}$.

Consider the valuation domain $R^* = R_{L_{\ell}}/L_1$. In a way similar to [6, Theorem 3], we define a map w on R^* in the following way:

$$w(t) = \ell(R/yR), \text{ for } t = y/a + L_1 \in R^* \quad (y \in R, a \in R \setminus L).$$

Using Proposition 3.9 and Lemma 2.3, it is straightforward to verify that w is well-defined and, since $w(t_1t_2) = w(t_1) + w(t_2)$ for any $t_1, t_2 \in R^*$, can be extended to a rank-one valuation (still called w) of the field of quotients Q^* of R^* . Since R^* is a rank-one valuation domain and $R_w = R_{v_{L_\ell/L_1}} = R^*$, we know that $w = \alpha v_{L_\ell/L_1}$, for a suitable real number $\alpha > 0$. Now Proposition 4.3 shows that $\ell(R/I) = \inf \{\ell(R/yR) : y \in I\} = \inf \{\alpha v_{L_\ell/L_1}(y + L_1) : y \in I\} = \alpha v_{L_\ell/L_1}(I)$. It follows that $\varphi = \alpha v_{L_\ell/L_1}$, as required.

(2) To simplify the notation, along the present argument we write $v^* = v_{L/J}$. Since $v^*(IJ) = v^*(I) + v^*(J)$, $\alpha v^* : \mathcal{I}(R) \to \mathbf{R}_{>0} \cup \{\infty\}$ is a morphism of totally ordered semigroups. Hence from Theorem 2.4 we readily get $\ell(X) = \ell(Y) + \ell(X/Y)$, for any finitely generated Rmodules $Y \subseteq X$. We extend ℓ , by upper continuity, to a unique Archimedean function of $\operatorname{Mod} R$. We must prove that this extension, still denoted by ℓ , is a valuative length function. Note that, clearly, $L = \{y \in R : \ell(R/yR) > 0\} \text{ and } J = \{y \in R : \ell(R/yR) = \infty\}.$ It suffices to verify that we are in a position to apply Lemma 3.4 (ii). Take R-modules $N \subseteq X$, with X finitely generated. Say gen (X) = n, gen $(X/N) = k \le n$. We assume that k < n, the case k = n being treatable with a similar, but simpler argument. We choose an ordered basis $\mathcal{G} = (x_1, \dots, x_n)$ of X, with \mathcal{G} -annihilator set B_1, \dots, B_n , in such a way that $X/N = \langle x_1 + N, \dots, x_k + N \rangle$, and, for $1 \leq j \leq k$, $U_j =$ $\langle x_1 + N, \dots, x_j + N \rangle$ is pure in X/N. Let $A_j = \operatorname{Ann}(x_j + N + U_{j-1})$ $(1 \le j \le k, \ U_0 = 0)$. Note that $x_m + N \in U_k = X/N$, for $k < m \le n$, that is, $x_m - \sum_{i=1}^k b_{im} x_i \in N$, for suitable $b_{im} \in R$. By the definition we get $\ell(X/N) = \alpha \sum_{j=1}^k v^*(A_j)$. Now, for $1 \leq j \leq k$, we pick any $r_j \in A_j$. Since U_{j-1} is pure in U_j , we get

$$r_j x_j - r_j \sum_{i=1}^{j-1} a_{ij} x_i \in N,$$

for suitable $a_{ij} \in R$. For $1 \leq j \leq k$, let $z_j = x_j - \sum_{i=1}^{j-1} a_{ij} x_i$, and, for $k+1 \leq m \leq n$, let $z_m = x_m - \sum_{i=1}^k b_{im} x_i \in N$, as above. Then, clearly, $X = \langle z_1, \ldots, z_n \rangle$ and $Y = \langle r_1 z_1, \ldots, r_k z_k, z_{k+1}, \ldots, z_n \rangle \in \mathcal{F}_N$. Now, using Lemma 1.6, it is readily seen that $\ell(X/Y) = \alpha \sum_{j=1}^k v^*(r_j R)$. Recall that $v^*(A) = \inf\{v^*(rR) : r \in A\}$, for any ideal A of R. Since the $r_j \in A_j$ were arbitrary, we conclude that $\ell(X/N) = \inf\{\ell(X/Y) : Y \in \mathcal{F}_N\}$, hence ℓ satisfies the hypothesis of Lemma 3.4 (ii).

Finally, from Proposition 3.9 (ii) and (iii) we readily derive that ℓ is discrete if and only if $L \neq L^2$.

Acknowledgments. The author is grateful to Luigi Salce for useful discussions and suggestions. I am indebted to the referee for suggesting consideration of the case of R almost maximal in Example 3.5.

REFERENCES

- 1. R.L. Adler, A.G. Konheim and M.H. McAndrew, *Topological entropy*, Trans. Amer. Math. Soc. 114 (1965), 309–319.
- 2. M. Akhavin, F. Ayatollah Zadeh Shirazi, D. Dikranjan, A. Giordano Bruno and A. Hosseini, *Algebraic entropy of shift endomorphisms on Abelian groups*, Quaest. Math. **32** (2009), 529–550.
- 3. D. Dikranjan, B. Goldsmith, L. Salce and P. Zanardo, Algebraic entropy for Abelian groups, Trans. Amer. Math. Soc. 361 (2009), 3401–3434.
- 4. L. Fuchs and L. Salce, Modules over Non-Noetherian domains, AMS Math. Surv. Mono. 84 (2001), American Mathematical Society.
- 5. A. Giordano Bruno, Algebraic entropy of generalized shifts on direct products, Comm. Algebra, to appear.
- 6. D.G. Northcott and M. Reufel, A generalization of the concept of length, Quart. J. Math Oxford 16 (1965), 297–321.
- 7. P. Ribenboim, Valuations and length of constructible modules, J. reine Angew. Math. 283/284 (1976), 186-201.
- $\bf 8.~L.~Salce,~P.~V$ ámos and S. Virili, Length functions, multiplicities and algebraic entropy, preprint.
- **9.** L. Salce and P. Zanardo, Commutativity modulo small endomorphisms and endomorphisms of zero algebraic entropy, in Models, modules and Abelian groups, de Gruyter, Boston, MA, 2008.

- ${\bf 10.}$ L. Salce and P. Zanardo, A general notion of algebraic entropy and the rankentropy, Forum Math. ${\bf 21}$ (2009), 579–599.
- $\bf 11.$ P. Vámos, Additive functions and duality over Noetherian rings, Quart. J. Math, Oxford $\bf 19$ (1968), 43–55.
- 12. M.D. Weiss, Algebraic and other entropies of group endomorphisms, Math. Systems Theory 8 (1974/75), 243–248.
- $\bf 13.$ P. Zanardo, Algebraic entropy of endomorphisms over local one-dimensional domains, J. Algebra Appl. 8 (2009), 759–777.

Dipartimento di Matematica Pura e Applicata, Via Trieste 63, 35121 Padova, Italy

Email address: pzanardo@math.unipd.it