Number of submodules of given type

MALLET-BURGUES Louis, SOUANEF Rafik

December 29, 2024

Abstract

We aim to prove proposition 25 that is a formula that enables us to compute the number of submodules of any finite $\mathbb{A}$-module M that are isomorphic to N (also supposed to be a finite $\mathbb{A}$-module), assuming $\mathbb{A}$ is a Dedekind domain that has finite quotients and the invariant factors of M and N are given. We also aim to generalize the convolution product introduced in [Del48] and [MB]. Our work generalizes the formula given in [Del48] to modules with finite cardinality over any Dedekind domain that has finite quotients and gives new proofs for it. We prove it in two different ways : one involves the convolution product we have generalized and one uses elementary methods only. Our approach mostly relies on two induction formulas (see propositions 8 and 10) that enable us to get an explicit formula by iterating it.

1 Introduction

We assume the reader knows the theory of Dedekind rings (see [Lan94], [Coh00]).

In what follows, $\mathbb{A}$ denotes a Dedekind domain that is infinite and such that $\mathbb{A}/I$ is finite for every nonzero ideal I. Note that a finite Dedekind domain is just a finite field and in that case, counting sub-modules (of given type) comes to counting subspaces (of given dimension) of a vector space over a finite field, so we may consider this case of no interest.
Examples : any ring of integers, $\mathbb{Z}$, $\mathbb{Z}_p$, $k[X]$ and $k[[T]]$ with k being a finite field or - more generally - any discrete valuation ring with finite residue field. Furthermore, notice that there are principal ideal domains (that are also Dedekind domains) that do not satisfy this property. Indeed, if $k = \mathbb{C}$, we see that $k[X]$ is a principal ideal domain but the property we require is no longer satisfied. Therefore, we are considering a class of rings that is strictly contained in the class of Dedekind domains.

The problem we try to solve is the following : given two finite $\mathbb{A}$-module M, N (we mean two modules that have finite cardinality), how many submodules of M are isomorphic to N ? Our goal is to solve this problem by giving a formula that depends on the invariant factors of M and N.

First, observe that our hypothesis (on the cardinality of $\mathbb{A}$) and the structure theorem (see [Coh00]) reveals that both M and N are of the form $\mathbb{A}/P_1^{a_1} \times \cdots \times \mathbb{A}/P_r^{a_r}$ for some integers $a_1, ..., a_r \in \mathbb{N}^*$ and some prime ideals $P_1, ..., P_r$.

Also, we need to realize that we can simplify this problem a little. In fact, we can assume that both M and N are P-modules for a given nonzero prime ideal P (that is $P^r.M = 0 = P^r.N$ for some $r \in \mathbb{N}$). Indeed, every finite $\mathbb{A}$-module can be decomposed into a direct sum of P-modules indexed by different prime ideals P (and this decomposition behaves "well" with submodules).

Let $\mathrm{sub}_N(M)$ denote the number of submodules of M that are isomorphic to N and let $\mathrm{NIF}\, M$ denote the number of invariant factors of M. Let $c(P) = |A/P|$. In this case, we get this formula

$$\mathrm{sub}_N(M) = c(P)^{\left(\sum_{k\geq 1}\left(\mathrm{NIF}\, M_{|k} - \mathrm{NIF}\, N_{|k}\right)\mathrm{NIF}\, N_{|k+1}\right)} \prod_{k\geq 1}\left(\prod_{j=\mathrm{NIF}\, N_{|k+1}}^{(\mathrm{NIF}\, N_{|k})-1} \frac{c(P)^{\mathrm{NIF}\, M_{|k}} - c(P)^j}{c(P)^{\mathrm{NIF}\, N_{|k}} - c(P)^j}\right)$$

that we will prove by induction in some sens.

Moreover, we generalize the convolution product introduced in [Del48] and [MB] to the case of $\mathbb{A}$-modules (see section 5) that seems to be linked to counting problems as shown in [Del48] and [MB].

For now, in what follows, P is a nonzero prime ideal of $\mathbb{A}$, M and N are assumed to be P-modules. Also, $c(P)$ denotes the cardinality of $\mathbb{A}/P$ and we let $p \in P \setminus P^2$.

2 Link between Mono and our problem

The starting point of our solution is proposition 2 that will enable us to get an induction formula.

Definition 1. We will denote the set of all injective morphisms $N \to M$ by $\mathrm{Mono}(N, M)$ (that is the set of all monomorphisms $N \to M$). Let $\mathrm{Sub}_N(M)$ denote the set of all submodules of M that are isomorphic to N.

We will use the following rule : $\hom(N, M)$ denotes the cardinality of $\mathrm{Hom}(N, M)$, $\mathrm{mono}(N, M)$ denotes the one of $\mathrm{Mono}(N, M)$ and so on.

The well known definition of subobjects in the theory of category lead us to the following fact.

Proposition 2. Let M, N be finite $\mathbb{A}$-modules. We have the following formula :

$$\mathrm{sub}_N(M) = \frac{\mathrm{mono}(N, M)}{\mathrm{aut}(N)}.$$

Proof. To prove this formula, it's enough to see that there is a correspondence between the submodules of M that are isomorphic to N and the orbits of $\mathrm{Mono}(N, M)$ under the right group action of $\mathrm{Aut}(N)$ (that is $i \cdot g = i \circ g$) (see [MB] for more details).

□

Remark 3. Counting the number of submodules of given type comes to knowing $\mathrm{mono}(N, M)$ for all finite $\mathbb{A}$-modules M, N and that is what we will do next.

Indeed, the previous formula enables us to know $\mathrm{aut}(K)$ as we have $\mathrm{Aut}(K) = \mathrm{Mono}(K, K)$.

3 Induction and explicit formula for mono

Our plan is the following : distinguish two cases to obtain two induction formulas and by iterating it, we will get an explicit formula.

3.1 Case $n_i \geq 2$

We may introduce some definitions and facts in order to prove proposition 8.

Definition 4. Let K be a $\mathbb{A}$-module. Recall the annihilator of K is the ideal $\{x \in \mathbb{A} : \forall k \in K, \quad xk = 0\}$. The annihilator of an element $k \in K$ is defined as the annihilator of the submodules that is generated by k.

Definition 5. Let I be an ideal of $\mathbb{A}$ and let K be a finite P-module. Set $K[I] = \{k \in K : \forall i \in I, i.k = 0\}$ and $I.K = \{i.k : k \in K, i \in I\}$. When I is a prime ideal, we see that $K[I]$ is naturally a vector space over $\mathbb{A}/I$.

Let $(e_1, ..., e_r) \in K^r$ and let $I_i \subset A$ be the annihilator of e_i for all $1 \leq i \leq r$. We say that $(e_1, ..., e_r)$ is a quasi-basis of K if the following map is an isomorphism

$$f : \left| \begin{array}{ccc} \prod_{i=1}^{r} \mathbb{A}/I_i & \longrightarrow & K \\ (x_i) & \longmapsto & \sum x_i e_i \end{array} \right. .$$

Lemma 6. Let $\mathbb{A}$ be a Dedekind domain, let P be a prime ideal and let $p \in P \setminus P^2$. Then, multiplication by p realises isomorphisms $\mathbb{A}/P \xrightarrow{\sim} P/P^2 \xrightarrow{\sim} P^2/P^3 ...$

Proof. Notice we have $J := P + pP^{-1} = A$ where P^{-1} denotes the fractional ideal that is such that $PP^{-1} = A$. Indeed, as we have $P^n \subset J$, we have $J|P$ so that $J = P^j$ for some non negative integer j. By contradiction, suppose $j \neq 0$. Then, we have $pP^{-1} \subset J \subset P$ so that $p \in P^2$ and we have a contradiction (see how p is defined).

Then, there is $b \in P^{-1}$ such that $pb = 1 \mod P$ and multiplication by b is the inverse map of $P^n/P^{n+1} \to P^{n+1}/P^{n+2}$. □

Corollary 7. If A/P is finite, then so are $P/P^2, ...$ and we have $A/P^{r-1} \simeq P.(A/P^r)$ through multiplication by p.

Proof. Indeed, multiplication realises an injective map $A/P^{r-1} \to P.(A/P^r)$ (adapt the proof of previous lemma) and these two modules have same cardinality : $P.(A/P^r) = P/P^r$ has cardinality $|P/P^2| \times |P^2/P^3| \dots$ that is $|A/P|^{r-1}$ and the same can be said for A/P^{r-1}. □

Proposition 8. Suppose $N \simeq \prod_{i=1}^{s} \mathbb{A}/P^{n_i}$, with $n_i \geq 2$ for all i. Then, we have

$$\mathrm{mono}(N, M) = \hom(N[P], M)\, \mathrm{mono}(P.N, P.M).$$

Proof. Here, we prove this proposition using elementary tools.

Let $(e_1, ..., e_s)$ be a quasi-basis of N such that e_i has annihilator P^{n_i}. Consider the map

$$\mathrm{res} : \left| \begin{array}{ccc} \mathrm{Mono}(N, M) & \longrightarrow & \mathrm{Mono}(P.N, P.M) \\ f & \longmapsto & f \end{array} \right. .$$

This map is well defined. Moreover, it is surjective and more precisely, every $g \in \mathrm{Mono}(P.N, P.M)$ satisfies $|\mathrm{res}^{-1}(\{g\})| = \hom(N[P], M) = |M[P]|^s$. Indeed, observe that (pe_i) is a quasi-basis of $P.N$ (see corollary 7) and let $f_i \in M$ be such that $g(pe_i) = pf_i$. Now, we see that $f \in \mathrm{Mono}(N, M)$ satisfies $\mathrm{res}(f) = g$ if and only if we have $pf(e_i) = pf_i$ for all i, that is $f(e_i) = f_i + p_i$ where $p_i \in M[P]$ (see $(*)$). To prove this, we may prove that if $f : N \to M$ is the morphism defined by $f(e_i) = f_i + p_i$ for some $p_i \in M[P]$ then f is injective. Observe (again) that we have $\mathrm{res}(f) = g$ and let $x \in N$ be such that $f(x) = 0$. Then, we have $f(px) = 0 = g(px)$ and since g is injective we get $px = 0$ i.e. $x \in N[P] \leq P.N$ (as $n_i \geq 2$). As a consequence, we have $f(x) = 0 = g(x)$ and again, since g is injective, we get $x = 0$. The formula now comes from a well known combinatoric result.

It remains to precise $(*)$, that is to prove that for all $x \in M$, we have $px = 0$ if and only if $\widetilde{p}x = 0$ for all $\widetilde{p} \in P$. Suppose we have $px = 0$. As M is finite, the structure theorem (see [Coh00]) shows that there is an integer $m \in \mathbb{N}^*$ such that $P^m.M$ is trivial. Notice that we have $J := P^m + pP^{-1} = A$, where P^{-1} denotes the fractional ideal that is such that $PP^{-1} = A$. Indeed, as we have $P^m \subset J$, we have $J|P^m$ so that $J = P^j$ for some non negative integer j. By contradiction, suppose $j \neq 0$. Then, we have $pP^{-1} \subset J \subset P$ so that $p \in P^2$ and we have a contradiction (see how p is defined). Then, we can write $\widetilde{p} = pa + p_m$ with $a \in \mathbb{A}$ and $p_m \in P^m$ so that $\widetilde{p}x = apx + p_m x = 0$. □

3.2 Case $n_i = 1$

Proposition 9. Let M, N be two finite P-modules. We have

$$\mathrm{mono}(N \times \mathbb{A}/P, M) = \mathrm{mono}(N, M) \times (|M[P]| - |N[P]|)\,.$$

Proof. There is a one-to-one correspondence between monomorphisms $N \times \mathbb{A}/P \xrightarrow{f} M$ on one hand and monomorphisms $N \xrightarrow{g} M$ plus some element $a \in M[P] \setminus g(N)$ on the other hand.

In addition, we have for all $g \in \mathrm{Mono}(N, M)$:

$$|M[P] \setminus g(N)| = |M[P]| - |g(N) \cap M[P]|$$

and since g is injective, we have :

$$g(N) \cap M[P] = g(N[P]) \simeq N[P].$$

Therefore it turns out that the cardinality of $M[P] \setminus g(N)$ does not depend on g and then one has :

$$\mathrm{mono}(N \times \mathbb{A}/P, M) = \mathrm{mono}(N, M) \times \left(|M[P]| - |N[P]|\right).$$

□

By iterating this last formula, we get the following formula.

Proposition 10. Let M, N be two finite P-modules. Let d denote the greatest integer such that $(\mathbb{A}/P)^d$ is a direct factor of N. Setting $N \simeq (\mathbb{A}/P)^d \times K$, let ℓ denote the number of invariant factors of K. Then, we have

$$\mathrm{mono}(N, M) = \mathrm{mono}(K, M) \times \prod_{j=0}^{d-1} \left(|M[P]| - c(P)^{\ell+j}\right).$$

Proof. We proceed by induction on d. If $d = 0$, then the product that is to the right is empty and then it is 1, in a way that the formula holds.

Assume the formula is true for $d-1$. Then, we have

$$\begin{aligned}\mathrm{mono}(N, M) &= \mathrm{mono}((\mathbb{A}/P)^d \times K, M) \\ &= \mathrm{mono}((\mathbb{A}/P)^{d-1} \times K, M) \times \left(|M[P]| - \left|\left(\mathbb{A}/P\right)^{d-1} \times K\right)[P]\right|\right)\end{aligned}$$

by proposition 9. Since K has no direct factor of the form $\mathbb{A}/P$, we get :

$$\begin{aligned}\mathrm{mono}(N, M) &= \mathrm{mono}((\mathbb{A}/P)^{d-1} \times K, M) \times \left(|M[P]| - c(P)^{d-1}c(P)^{\ell}\right) \\ &= \mathrm{mono}(K, M) \times \prod_{k=0}^{d-2} \left(|M[P]| - c(P)^{\ell+k}\right) \times \left(|M[P]| - c(P)^{\ell+d-1}\right) \\ &= \mathrm{mono}(K, M) \times \prod_{k=0}^{d-1} \left(|M[P]| - c(P)^{\ell+k}\right)\end{aligned}$$

by induction. □

3.3 Induction formula

Definition 11. For any finite P-module K, set $n_p(K) := |K[P]|$.

Mixing the last two subsections, we get the following theorem.

Theorem 12. Let $N \simeq \prod_{i=1}^{s} (\mathbb{A}/P^{n_i})^{E_i}$ and M be two finite P-modules with $n_i, E_i \in \mathbb{N}^*$ and (n_i) strictly decreasing. We have

$$\mathrm{mono}(N,M) = \left(\prod_{j=0}^{n_s-2} \hom(N[P], P^j.M)\right)\left(\prod_{j=1}^{E_s} n_p(P^{n_s-1}.M) - c(P)^{E_s-j+\sum_{k=1}^{s-1} E_k}\right) \times \mathrm{mono}\left(\prod_{i=1}^{s-1} (\mathbb{A}/P^{n_i-(n_s-1)})^{E_i}, P^{n_s-1}.M\right).$$

Proof. We simply iterate the results that we just obtained and observe that we have $(P^j.N)[P] = N[P]$ as long as $j < n_s - 1$ before using the result of the previous section for the case $j = n_s - 1$.

We proceed by induction on n_s. If $n_s = 1$, then the first factor is an empty product and hence is 1. We simply wrote the formula that we already gave in the previous subsection.

Now, assume $n_s > 1$ and the result is true for previous ranks. We recall proposition 8 :

$$\mathrm{mono}(N,M) = \hom(N[P], M)\,\mathrm{mono}(P.N, P.M).$$

Moreover, we have $P.N = \prod_{i=1}^{s} (\mathbb{A}/P^{n_i-1})^{E_i}$. Then, by induction, we have

$$\mathrm{mono}(P.N,P.M) = \left(\prod_{j=0}^{n_s-1-2} \hom((P.N)[P], P^j.(P.M))\right)\left(\prod_{j=1}^{E_s} n_p(P^{n_s-1-1}.(P.M)) - c(P)^{E_s-j+\sum_{k=1}^{s-1} E_k}\right) \times \mathrm{mono}\left(\prod_{i=1}^{s-1} (\mathbb{A}/P^{(n_i-1)-(n_s-1-1)})^{E_i}, P^{n_s-1-1}.(P.M)\right).$$

Substitute $j' = j+1$ in the first product and we get (because $(P.N)[P] = N[P]$ since $n_s \geq 2$) :

$$\mathrm{mono}(P.N,P.M) = \left(\prod_{j=1}^{n_s-2} \hom(N[P], P^j.M)\right)\left(\prod_{j=1}^{E_s} n_p(P^{n_s-1}.M) - c(P)^{E_s-j+\sum_{k=1}^{s-1} E_k}\right) \times \mathrm{mono}\left(\prod_{i=1}^{s-1} (\mathbb{A}/P^{n_i-(n_s-1)})^{E_i}, P^{n_s-1}.M\right).$$

It remains to see that the factor $\hom(N[P], M)$ coming from proposition 8 corresponds to the term of the product when $j = 0$.

□

Remark 13. This formula is still true when N is the trivial module if we consider $s = 0$, $E_s = 0 = n_s$ in this case.

3.4 Explicit formula

Theorem 14. Let $N \simeq \prod_{i=1}^{s} (\mathbb{A}/P^{n_i})^{E_i}$ and M be two finite P-modules with $n_i, E_i \in \mathbb{N}^*$ and (n_i) strictly decreasing. Setting $n_{s+1} = 1$, we have :

$$\mathrm{mono}(N,M) = \prod_{i=0}^{s-1} \left(\prod_{\substack{0 \le j \\ j \le n_{s-i} - (n_{s-(i-1)}-1) - 2}} n_p(P^{j+n_{s-(i-1)}-1}.M)^{\sum_{k=1}^{s-i} E_k} \right) \times \left(\prod_{j=1}^{E_{s-i}} n_p(P^{n_{s-i}-1}.M) - c(P)^{E_{s-i}-j+\sum_{k=1}^{s-1-i} E_k} \right)$$

Proof. We proceed by induction on $|N|$ and $|M|$. If N is the trivial module, then we have 1 on both sides and the formula holds.

Now, assume N is as in the statement. We simply make use of theorem 12 and induction hypothesis applied to the last factor to conclude. Indeed, for all $1 \le i \le s-1$, set $c_i = n_i - (n_s - 1)$. By what we just said, we get

$$\begin{aligned}\mathrm{mono}(N,M) = &\left(\prod_{j=0}^{n_s-2} \hom(N[P], P^j.M) \right) \left(\prod_{j=1}^{E_s} n_p(P^{n_s-1}.M) - c(P)^{E_s-j+\sum_{k=1}^{s-1} E_k} \right) \times \\ &\prod_{i=0}^{s-1-1} \left(\prod_{\substack{0 \le j \\ j \le c_{s-1-i} - (c_{s-1-(i-1)}-1) - 2}} n_p(P^{j+c_{s-1-(i-1)}-1}.(P^{n_s-1}.M))^{\sum_{k=1}^{s-1-i} E_k} \right) \times \\ &\left(\prod_{j=1}^{E_{s-1-i}} n_p(P^{c_{s-1-i}-1}.(P^{n_s-1}.M)) - c(P)^{E_{s-1-i}-j+\sum_{k=1}^{s-1-1-i} E_k} \right).\end{aligned}$$

Substitute $i' = i+1$ and we get :

$$\begin{aligned}\mathrm{mono}(N,M) = &\left(\prod_{j=0}^{n_s-2} \hom(N[P], P^j.M) \right) \left(\prod_{j=1}^{E_s} n_p(P^{n_s-1}.M) - c(P)^{E_s-j+\sum_{k=1}^{s-1} E_k} \right) \times \\ &\prod_{i=1}^{s-1} \left(\prod_{\substack{0 \le j \\ j \le c_{s-i} - (c_{s-(i-1)}-1) - 2}} n_p(P^{j+c_{s-(i-1)}-1}(P^{n_s-1}.M))^{\sum_{k=1}^{s-i} E_k} \right) \times \\ &\left(\prod_{j=1}^{E_{s-i}} n_p(P^{c_{s-i}-1}.(P^{n_s-1}.M)) - c(P)^{M_{s-i}-j+\sum_{k=1}^{s-1-i} E_k} \right).\end{aligned}$$

Moreover, we have

$$\begin{aligned}\forall 1 \leq i \leq s-1 \quad & c_{s-i} - (c_{s-(i-1)} - 1) - 2 = n_{s-i} - (n_{s-(i-1)} - 1) - 2 \\ & P^{j+c_{s-(i-1)}-1}.(P^{n_s-1}.M) = P^{j+n_{s-(i-1)}-1}.M \\ & P^{c_{s-i}-1}.(P^{n_s-1}.M) = P^{n_{s-i}-1}M.\end{aligned}$$

Then, we have :

$$\begin{aligned}\mathrm{mono}(N,M) = & \left(\prod_{j=0}^{n_s-2} \hom(N[P], P^j.M)\right)\left(\prod_{j=1}^{E_s} n_p(P^{n_s-1}.M) - c(P)^{E_s - j + \sum_{k=1}^{s-1} E_k}\right) \times \\ & \prod_{i=1}^{s-1}\left(\prod_{\substack{0\leq j \\ j \leq n_{s-i} - (n_{s-(i-1)}-1) - 2}} n_p(P^{j+n_{s-(i-1)}-1}.M)^{\sum_{k=1}^{s-i} E_k}\right) \times \\ & \left(\prod_{j=1}^{E_{s-i}} n_p(P^{n_{s-i}-1}.M) - c(P)^{E_{s-i} - j + \sum_{k=1}^{s-1-i} E_k}\right).\end{aligned}$$

It remains to see that the first two factors constitute the term of index $i = 0$ of the product that follows them. Indeed, we have $\hom(F, P^j.M) = n_p(P^j.M)^{\dim(F)}$ for all finite-dimensional $\mathbb{A}/P$-vector spaces F .□

□

Remark 15. It is easy to compute $n_p(P^k.M)$ if the invariant factors of M are given. Indeed, if $M \simeq \prod_{i=1}^{r} \mathbb{A}/P^{m_i}$ with $m_i \geq 1$ and (m_i) decreasing, then :

$$P^k.M \simeq \prod_{i=1}^{t} \mathbb{A}/P^{m_i - k}$$

with t being the largest integer i such that $m_i > k$. Therefore, we have :

$$n_p(P^k.M) = \left|\prod_{i=1}^{t} \mathbb{A}/P^{m_i-k}[P]\right| = \left|(\mathbb{A}/P)^t\right| = c(P)^t.$$

3.5 Another formulation

In order to give a simpler formula, we may introduce notation first.

Definition 16. Let M be a finite P-module. For all $k \geq 1$, let $v_k(M)$ denote the number of factors $\mathbb{A}/P^k$ in the decomposition of M, in a way that we have

$$M \simeq \prod_{k\geq 1} \left(\mathbb{A}/P^k\right)^{v_k(M)}.$$

Let NIF M denote the number of invariant factors of M, that is

$$\text{NIF } M = \sum_{k\geq 1} v_k(M).$$

Observe that we have $v_k(M \times N) = v_k(M) + v_k(N)$ and $\text{NIF}(M \times N) = \text{NIF } M + \text{NIF } N$.

Also, for all $\ell \geq 1$, let $M_{|\ell}$ be the truncated module :

$$M_{|\ell} = \prod_{k\geq \ell} \left(\mathbb{A}/P^k\right)^{v_k(M)}.$$

Finally, observe that we have $\text{NIF } M_{|\ell} = \sum_{k\geq \ell} v_k(M)$.

Definition 17. Let M be a $\mathbb{A}$-module. We say that M has I-torsion if for all $m \in M, i \in I$, we have $im = 0$. We say that M has no I-torsion if we have

$$\forall x \in M, \quad (\forall i \in I, \quad ix = 0) \implies x = 0.$$

Lemma 18. Let M be a finite P-module and let $j \geq 0$. We have

- $|M[P]| = c(P)^{\text{NIF } M}$
- $v_k(P^j.M) = v_{k+j}(M)$.

Proof. First, observe that we have :

$$M[P] \simeq \prod_{k\geq 1} \left(\mathbb{A}/P^k\right)^{v_k(M)}[P] \simeq \prod_{k\geq 1} \left(\mathbb{A}/P\right)^{v_k(M)} \simeq \left(\mathbb{A}/P\right)^{\text{NIF } M}$$

so we have $|M[P]| = c(P)^{\text{NIF } M}$. Then, we have (see corollary 7) :

$$P^j.M \simeq \prod_{k\geq 1} P^j.\left(\mathbb{A}/P^k\right)^{v_k(M)} \simeq \prod_{k\geq j+1} \left(\mathbb{A}/P^{k-j}\right)^{v_k(M)} \simeq \prod_{k\geq 1} \left(\mathbb{A}/P^k\right)^{v_{k+j}(M)}$$

which proves the second formula. □

Theorem 19. Let M, N be two finite P-modules. We have the following explicit formula

$$\text{mono}(N, M) = c(P)^{\left(\sum_{k\geq 1} \text{NIF } M_{|k} \text{ NIF } N_{|k+1}\right)} \prod_{k\geq 1} \left(\prod_{j=\text{NIF } N_{|k+1}}^{(\text{NIF } N_{|k})-1} \left(c(P)^{\text{NIF } M_{|k}} - c(P)^j\right) \right).$$

Proof. We successively use the formulas we proved earlier :

$$\begin{aligned}
\operatorname{mono}(N,M) &= \operatorname{mono}\left(\prod_{k\geq 1}\left(\mathbb{A}/P^k\right)^{v_k(N)}, M\right)\\
&= \operatorname{mono}\left(\prod_{k\geq 2}\left(\mathbb{A}/P^k\right)^{v_k(N)}, M\right) \times \prod_{j=0}^{v_1(N)-1}\left(|M[P]| - c(P)^{j+\operatorname{NIF} N_{|2}}\right)\\
&= \operatorname{mono}\left(N_{|2}, M\right) \times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right)\\
&= \operatorname{mono}\left(P.N_{|2}, P.M\right)\hom\left(N_{|2}[P], M\right) \times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right).
\end{aligned}$$

Observe that we have $P.N_{|2} = P.N$ (here $P.N_{|2}$ means $P.(N_{|2})$). Moreover, if E has P-torsion and has cardinality $c(P)^d$, the bahavior of hom regarding cartesian produit gives $\hom(E,M) = \hom(\mathbb{A}/P, M)^d = |M[P]|^d = c(P)^{d\operatorname{NIF} M} = |E|^{\operatorname{NIF} M}$. Then, we obtain this formula :

$$\begin{aligned}
\operatorname{mono}(N,M) &= \operatorname{mono}\left(P.N, P.M\right)\left|N_{|2}[P]\right|^{\operatorname{NIF} M} \times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right)\\
&= \operatorname{mono}\left(P.N, P.M\right)c(P)^{\operatorname{NIF} M \operatorname{NIF} N_{|2}} \times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right).
\end{aligned}$$

Keep in mind this last formula and iterate this process by applying this last formula to $P.N$ and $P.M$ to obtain :

$$\begin{aligned}
\operatorname{mono}(N,M) &= \operatorname{mono}\left(P^2.N, P^2.M\right)c(P)^{\operatorname{NIF}(P.M)\operatorname{NIF}((P.N)_{|2})} \times \prod_{j=\operatorname{NIF}(P.N)_{|2}}^{\operatorname{NIF} P.N-1}\left(c(P)^{\operatorname{NIF} P.M} - c(P)^j\right) \times c(P)^{\operatorname{NIF} M}\\
&\quad\times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right)\\
&= \operatorname{mono}\left(P^2.N, P^2.M\right)c(P)^{\operatorname{NIF} M_{|2}\operatorname{NIF} N_{|3}} \times \prod_{j=\operatorname{NIF} N_{|3}}^{\operatorname{NIF} N_{|2}-1}\left(c(P)^{\operatorname{NIF} M_{|2}} - c(P)^j\right) \times c(P)^{\operatorname{NIF} M \operatorname{NIF} N_{|2}}\\
&\quad\times \prod_{j=\operatorname{NIF} N_{|2}}^{\operatorname{NIF} N-1}\left(c(P)^{\operatorname{NIF} M} - c(P)^j\right)
\end{aligned}$$

(see $\mathrm{NIF}((P.N)_{|2}) = \mathrm{NIF}\, N_{|3}$). Then, we have :

$$\mathrm{mono}(N,M) = \mathrm{mono}(P^2.N, P^2.M) \times c(P)^{\left(\sum_{k=1}^{2} \mathrm{NIF}\, M_{|k}\, \mathrm{NIF}\, N_{|k+1}\right)} \prod_{k=1}^{2} \left(\prod_{j=\mathrm{NIF}\, N_{|k+1}}^{(\mathrm{NIF}\, N_{|k})-1} \left(c(P)^{\mathrm{NIF}\, M_{|k}} - c(P)^j \right) \right).$$

Iterate the formula and after ℓ steps we get :

$$\mathrm{mono}(N,M) = \mathrm{mono}(P^\ell.N, P^\ell.M) \times c(P)^{\left(\sum_{k=1}^{\ell} \mathrm{NIF}\, M_{|k}\, \mathrm{NIF}\, N_{|k+1}\right)} \prod_{k=1}^{\ell} \left(\prod_{j=\mathrm{NIF}\, N_{|k+1}}^{(\mathrm{NIF}\, N_{|k})-1} \left(c(P)^{\mathrm{NIF}\, M_{|k}} - c(P)^j \right) \right).$$

This formula holds for all $\ell \geq 0$ and taking ℓ big enough so that $P^\ell.N$ is the trivial module, we obtain the expected formula. □ □

Remark 20. The exponent $S = \sum_{k\geq 1} \mathrm{NIF}\, M_{|k}\, \mathrm{NIF}\, N_{|k+1}$ that appears in theorem 19 can be written as

$$\begin{array}{rccccccccccc} S = & & v_1w_2 & + & v_1w_3 & + & v_1w_4 & + & v_1w_5 & + & \dots \\ & + & v_2w_2 & + & 2v_2w_3 & + & 2v_2w_4 & + & 2v_2w_5 & + & \dots \\ & + & v_3w_2 & + & 2v_3w_3 & + & 3v_3w_4 & + & 3v_3w_5 & + & \dots \\ & + & v_4w_2 & + & 2v_4w_3 & + & 3v_4w_4 & + & 4v_4w_5 & + & \dots \\ & \vdots & \vdots & & \vdots & & \vdots & & \vdots & & \ddots \end{array}$$

with $v_k = v_k(M)$ and $w_k = v_k(N)$.

3.6 Submodules' type and (total) number of submodules

The formula we obtained with theorem 19 enables us to describe all the possible structures for N to be a submodule of M. More precisely, our aim is to prove propositions 22 and 24 which are results that are probably already well known but here, we give a proof based on our work. These two propositions will be used to give a formula for the number of submodules of any finite P-module, that is the last proposition of this subsection. First, we introduce a lemma.

Lemma 21. Let $(u_n)_{n\geq 1}$ and $(v_n)_{n\geq 1}$ be two sequences of real numbers with finitely many non zero terms. Assume (u_n) is decreasing. The following conditions are equivalent.

- there exists $n \geq 1$ such that $u_n < v_n$.
- there exists $n \geq 1$ such that $v_{n+1} \leq u_n < v_n$.

Proof. The second one obviously implies the first. The other way around, let $n \geq 1$ be maximal for the property $u_n < v_n$. By contradiction, suppose we have $u_n < v_{n+1}$.Then, we have $u_{n+1} \leq u_n < v_{n+1}$ so that $n+1$ satisfies the property $u_{n+1} < v_{n+1}$ which is a contradiction. □

Proposition 22. Let M, N be two finite P-modules. The following conditions are equivalent :

- N is (isomorphic to) a submodule of M
- $\mathrm{mono}(N, M) > 0$
- $\forall k \geq 1,\ \mathrm{NIF}\, N_{|k} \leq \mathrm{NIF}\, M_{|k}$.

Remark 23. Duality for $\mathbb{A}$-modules (that we will define later) gives the same condition to see whether N is a quotient of M.

Proof. The first two conditions are clearly equivalent. Then, by theorem 19, the condition $\mathrm{mono}(B, A) = 0$ means there exists $k \geq 1$ such that

$$\mathrm{NIF}\, N_{|k+1} \leq \mathrm{NIF}\, M_{|k} < \mathrm{NIF}\, N_{|k}.$$

Apply the previous lemma to $(\mathrm{NIF}\, M_{|k})$ and $(\mathrm{NIF}\, N_{|k})$ to see that the third condition is equivalent to the others. □

We can also express this condition in terms of invariant factors.

Proposition 24. Let M and N be two finite P-modules. Let (m_i) (resp.(n_i)) be the decreasing sequence of non negative integers such that $M \simeq \prod_{i=1}^{r} \mathbb{A}/P^{m_i}$ and $N \simeq \prod_{i=1}^{s} \mathbb{A}/P^{n_i}$. The following conditions are equivalent :

- N is (isomorphic to) a submodule of M
- We have $s \leq r$ and for all $1 \leq i \leq s$, we have $n_i \leq m_i$.

Proof. Observe that $\mathrm{NIF}\, M_{|k}$ (resp. $\mathrm{NIF}\, N_{|k}$) counts how many $1 \leq i \leq r$ satisfy $m_i \geq k$ (resp $n_i \leq k$).

Suppose N is a submodule of M. By the previous proposition, we have $\mathrm{NIF}\, N_{|k} \leq \mathrm{NIF}\, M_{|k}$ for all $k \geq 1$. Take $k = 1$ and we obtain $s \leq r$. Now, by contradiction, suppose there exists $1 \leq j \leq s$ such that $n_j > m_j$. Then, take $k = n_j$ and observe that we have $\mathrm{NIF}\, N_{|k} > \mathrm{NIF}\, M_{|k}$. □

Proposition 25. Let M, N be two finite P-modules. We have the following formula :

$$\mathrm{sub}_N(M) = c(P)^{\left(\sum_{k\geq 1} \left(\mathrm{NIF}\, M_{|k} - \mathrm{NIF}\, N_{|k}\right) \mathrm{NIF}\, N_{|k+1}\right)} \prod_{k\geq 1} \left(\prod_{j=\mathrm{NIF}\, N_{|k+1}}^{(\mathrm{NIF}\, N_{|k})-1} \frac{c(P)^{\mathrm{NIF}\, M_{|k}} - c(P)^j}{c(P)^{\mathrm{NIF}\, N_{|k}} - c(P)^j} \right).$$

Proof. This is given by propositions 2 and 19 as $\mathrm{Aut}(N) = \mathrm{Mono}(N, N)$ since N is finite. □

Remark 26. -As a corollary, we could show that this last quantity is a polynomial function of $c(P)$ if $m_1, ..., m_r, n_1, ...n_s$ are given.

-To obtain the total number of submodules of M, it remains to sum this last quantity as N runs over the possible submodules (up to isomorphism) of M (see propositions 22 and 24).

-This formula is identical to the one Delsarte obtained in [Del48] (see formula (20), consider $\mathbb{A} = \mathbb{Z}$, p prime and $P = \langle p \rangle$).

4 Duality

In this section, we introduce a notion of duality that generalizes Pontryagin's duality to finite $\mathbb{A}$-modules. The reader might see [LP00] to have a quick overview of this duality and find more general proofs in [HR63]. Then, we will use this duality to define a convolution product.

We recall our notation : $\mathbb{A}$ is an infinite Dedekind domain such that for every nonzero ideal I, we have $\mathbb{A}/I$ is finite, P is a nonzero prime ideal and $p \in P \setminus P^2$. We may denote $\overline{x}$ or $\mathrm{cl}_n(x)$ the class of $x \in A$ modulo P^n.

4.1 Generalization

Definition 27. The modules $\mathbb{A}/P^n$ constitute a direct system if we consider the multiplication by p as n runs over $\mathbb{N}^*$:

$$\begin{array}{ccc} \mathbb{A}/P^n & \to & \mathbb{A}/P^{n+1} \\ \overline{x} & \mapsto & \overline{px} \end{array}.$$

Then, we can set $\mathbb{A}_{P^\infty} = \varinjlim \mathbb{A}/P^n$ in the category of $\mathbb{A}$-modules.

Definition 28. Let M be a $\mathbb{A}$-module. We say that M is $\mathbb{A}$-divisible (or divisible) if we have

$$\forall m \in M, \forall a \in \mathbb{A} \setminus \{0\}, \exists\, m' \in M : \quad m = am'.$$

Proposition 29. The module $\mathbb{A}_{P^\infty}$ is divisible.

Proof. Let $X = \mathrm{cl}_n(x) \in \mathbb{A}/P^n \subset \mathbb{A}_{P^\infty}$. Observe that, by construction, X is of the form pY as we identified $\mathrm{cl}_n(x)$ with $p\,\mathrm{cl}_{n+1}(x)$.

Let $a \in \mathbb{A} \setminus \{0\}$. Let r be the greatest integer such that $a \in P^r$ (i.e. the P-adic valuation of (a)). Notice that we have $p^r \in P^r$ and for all $k \in \mathbb{N}$ we have

$$J := P^n + aP^{-r} = A$$

where P^{-r} denotes the fractional ideal that is such that $P^r P^{-r} = A$. Indeed, as we have $P^n \subset J$, we have $J | P^n$ so that $J = P^j$ for some non negative integer j. By contradiction, suppose $j \neq 0$. Then, we have $aP^{-r} \subset J \subset P$ so that $a \in P^{r+1}$ and we have a contradiction (see how r is defined).

Therefore, we can write $ab = p^r \mod P^{n+r}$ for some $b \in \mathbb{A}$ and we have $X = p^r\,\mathrm{cl}_{n+r}(x) = aY$ with $Y = b\,\mathrm{cl}_{n+r}(x)$.

□

This last proposition is what makes everything work well in this duality theory.

Definition 30. Let M be a $\mathbb{A}$-module. Let $\widehat{M}$ denote the dual of M :

$$\widehat{M} = \mathrm{Hom}_{\mathbb{A}-\mathrm{mod}}(M, \mathbb{A}_\infty)$$

where

$$\mathbb{A}_\infty = \bigoplus_{Q \text{ non-zero prime}} \mathbb{A}_{Q^\infty}.$$

Elements of $\widehat{M}$ are called $\mathbb{A}$-characters of M.

Proposition 31. The $\mathbb{A}$-module $\mathbb{A}_\infty$ is divisible.

Proof. This is a direct consequence of $\mathbb{A}_{Q^\infty}$ being divisible. □

Theorem 32. Let M be a finite $\mathbb{A}$-module (i.e. finite as a set). We have $M \simeq \widehat{M}$.

Proof. First, observe that we have $\widehat{M \oplus N} \simeq \widehat{M} \oplus \widehat{N}$. Then, by the structure theorem, it suffices to prove our theorem when $M = \mathbb{A}/P^n$. We have :

$$\widehat{\mathbb{A}/P^n} = \mathrm{Hom}_{\mathbb{A}-\mathrm{mod}}(\mathbb{A}/P^n, \mathbb{A}_\infty) \simeq \mathbb{A}_\infty[P^n] \simeq \bigoplus_{Q \text{ prime}} \mathbb{A}_{Q^\infty}[P^n] = \mathbb{A}_{P^\infty}[P^n]$$

as $\mathbb{A}_{Q^\infty}$ has no P^n-torsion when $Q \neq P$. Indeed, let $X = \mathrm{cl}_m(x) \in \mathbb{A}/Q^m \subset \mathbb{A}_{Q^\infty}$ have P^n-torsion. Observe that we have $J := Q^m + P = \mathbb{A}$ as we have $J|Q^m$, $J|P$ and P, Q are different prime ideals. Let $a \in P, b \in Q^m$ such that $a + b = 1$. Then, we have $X = (a+b)\,\mathrm{cl}_m(x) = a\,\mathrm{cl}_m(x) + b\,\mathrm{cl}_m(x) = 0$.

To conclude, now observe that we have $\mathbb{A}_{P^\infty}[P^n] \simeq \mathbb{A}/P^n$. Indeed, to see that, it suffices to understand that if $\mathrm{cl}_m(x) \in \mathbb{A}_{P^\infty}$ has P^n torsion, then we can suppose $m = n$. Let us separate two cases. If $m < n$, then $\mathrm{cl}_m(x) = \mathrm{cl}_n(p^{n-m}x)$. If $m > n$ then let us prove that there is $y \in \mathbb{A}$ such that $\mathrm{cl}_m(x) = \mathrm{cl}_m(py)$. First, observe we have $x \in P^{m-n}$ has $\mathrm{cl}_m(x)$ has P^n-torsion. Again, since we have $P^m + pP^{-1} = \mathbb{A}$, we can write $x = py \mod P^m$. Hence, we have $\mathrm{cl}_m(x) = \mathrm{cl}_{m-1}(y) \in \mathbb{A}_{P^\infty}$ and by iterating this process, we may end up with $m = n$. □

Theorem 33. Let M be a finite $\mathbb{A}$-module and let N be a submodule of M. We can extend any $\mathbb{A}$-character of N to M, i.e. the induced map :

$$\widehat{N} \longrightarrow \widehat{M}$$

is onto.

Proof. We can copy the proof of this fact for finite abelian groups or we can see that $\mathbb{A}_\infty$ is injective as it is divisible and $\mathbb{A}$ is a Dedekind domain. □

Corollary 34. We have the following canonical isomorphism

$$\alpha : \left| \begin{array}{ccc} M & \longrightarrow & \widehat{\widehat{M}} \\ m & \longmapsto & (\chi \in \widehat{M} \mapsto \chi(m)). \end{array} \right.$$

Proof. The last theorem shows that this map is injective and then with theorem 32 we can conclude. □

4.2 Correspondence between submodules and quotients

We will now use duality to recall a correspondence between submodules and quotients that will enable us to study the convolution product that we will introduce.

Definition 35. Let M be a finite $\mathbb{A}$-module. For all $N \leq M$, let $N^\perp$ denote the submodule of $\widehat{M}$ consisting of all characters that are identically zero over N.

Conversely, for all $K \leq \widehat{M}$, let $K^\top$ be the kernel of K, that is the intersection of the kernel of all characters $\chi \in K$.

Proposition 36. Let M be a finite $\mathbb{A}$-module. Let $N \leq M$ and let $K \leq \widehat{M}$. We have canonical isomorphisms

$$N^\perp \simeq \widehat{M/N} \text{ and } K^\top \simeq \widehat{\widehat{M}/K}.$$

In particular, we have

$$|M| = |N| \left|N^\perp\right| = |K| \left|K^\top\right|.$$

Moreover, the two operations $\perp$ and $\top$ we just introduced are compatible in the following way

$$(N^\perp)^\top = N \text{ and } (K^\top)^\perp = K.$$

These two operations induce bijections between the set of all submodules of M and those of $\widehat{M}$.

Proof. First, we have

$$\widehat{M/N} = \mathrm{Hom}(M/N, \mathbb{A}_\infty) \simeq \{\chi \in \mathrm{Hom}(M, \mathbb{A}_\infty) : N \leq \mathrm{Ker}(\chi)\} = N^\perp.$$

Then, using corollary 34, we get

$$\widehat{\widehat{M}/K} = \mathrm{Hom}(\widehat{M}/K, \mathbb{A}_\infty) \simeq \{\chi \in \widehat{\widehat{M}} : K \leq \mathrm{Ker}(\chi)\} \simeq \{m \in M : \forall \chi \in K, \chi(m) = 0\} = K^\top.$$

The other equalities then result from theorem 32.

Also, notice that we have

$$N \subset (N^\perp)^\top$$

so that these two sets are equal as they have same cardinality. We can do something analogous to prove the last equality mentionned.

□

Proposition 37. Let M be a finite $\mathbb{A}$-module. Let $\mathcal{S}(M)$ denote the set of all submodules of M. There exists a decreasing bijection $\Gamma : \mathcal{S}(M) \to \mathcal{S}(M)$ such that we have

$$\forall N \leq M, \quad \Gamma(N) \simeq M/N \text{ and } \Gamma^{-1}(N) \simeq M/N.$$

Proof. Let $M \xrightarrow{\theta} \widehat{M}$ be an isomorphism (there exists one, see theorem 32). Such an isomorphism induces a bijection Θ between submodules of M and submodules of $\widehat{M}$. Let Γ be the composite function

$$\mathcal{S}(M) \xrightarrow{\Theta} \mathcal{S}(\widehat{M}) \xrightarrow{\bullet^\top} \mathcal{S}(M).$$

As the composite of two bijections - each of these being a decreasing and an increasing function respectively- Γ is a decreasing bijection. It remains to see that we have

$$\Gamma(N) = \Theta(N)^\top \cong \widehat{\widehat{M}/\Theta(N)} \cong \widehat{M}/\Theta(N) = \theta(M)/\theta(N) \cong M/N$$

and

$$\Gamma^{-1}(N) = \Theta^{-1}(N^\perp) \cong N^\perp \cong \widehat{M/N} \cong M/N.$$

□

5 Convolution product and another proof

We will now introduce a convolution product and give another proof for proposition 8 that makes use of this convolution product. Notice this convolution product generalizes Dirichlet convolution (see [MB]).

Let $\mathcal{A}$ be a complete set of representatives of all finite $\mathbb{A}$-modules, that is for every $\mathbb{A}$-module M, there is a unique $N \in \mathcal{A}$ such that $M \simeq N$.

Now, consider the set $\mathcal{MF}$ of all functions $\mathcal{A} \to \mathbb{C}$ and we may call such functions modular functions. Modular functions can also be seen as "functions" from the category of all finite $\mathbb{A}$-modules to $\mathbb{C}$ such that any two isomorphic imputs have the same image. If $f \in \mathcal{MF}$ and M is a finite $\mathbb{A}$-module, we may write $f(M)$, meaning $f(N)$ where $N \in \mathcal{A}$ is such that $N \simeq M$.

We can now definite the convolution product for $\mathcal{MF}$ by

$$\forall f, g \in \mathcal{MF}, \quad \boxed{f * g(M) = \sum_{N \leq M} f(N) g(M/N)}$$

where N runs over the set of <u>all</u> submodules of M (we do <u>not</u> consider submodules up to isomorphism here).

Proposition 38. Let $\delta \in \mathcal{MF}$ be defined by $\delta(0) = 1$ and $\delta(M) = 0$ for all non trivial finite $\mathbb{A}$-module M.

$(\mathcal{MF}, +, *)$ is a commutative $\mathbb{C}$-algebra whose units are the functions $f \in \mathcal{MF}$ such that $f(\{0\}) \neq 0$ and whose neutral element is δ.

Proof. Let $M \in \mathcal{A}$ and let Γ be like in proposition 37. Let $f, g \in \mathcal{MF}$.

The convolution product is commutative :

$$f * g(M) = \sum_{N \leq M} f(N)g(M/N) = \sum_{K \leq M} f(\Gamma^{-1}(K))g(K) = \sum_{K \leq M} f(M/K)g(K) = g * f(M)$$

by sustituting $K = \Gamma(H)$ and using proposition 37.

Also, the convolution product is associative as we have on one hand

$$\begin{aligned} f * (g * h)(M) &= \sum_{N \leq M} f(N)(g * h)(M/N) \\ &= \sum_{N \leq M} \sum_{K \leq M/N} f(N)g(K)h(M/N/K) \\ &= \sum_{N \leq M} \sum_{N \leq L \leq M} f(N)g(L/N)h\left(\frac{M/N}{L/N}\right) \\ &= \sum_{N \leq M} \sum_{N \leq L \leq M} f(N)g(L/N)h(M/L) \end{aligned}$$

and on the other hand

$$\begin{aligned} (f * g) * h(M) &= \sum_{L \leq M} (f * g)(L)h(M/L) \\ &= \sum_{L \leq M} \sum_{N \leq L} f(N)g(L/N)h(M/L). \end{aligned}$$

The neutral element is δ and this is clear.

Then, if $f(0) \neq 0$, we can construst by induction on $|M|$ (as M runs over $\mathcal{A}$) a complex number $g(M)$ (here, g does not denote an arbitrary element of $\mathcal{MF}$ anymore). Indeed, define $g(0) = 1/f(0)$ and

$$g(M) = -\frac{1}{f(1)} \sum_{N < M} g(N)f(M/N)$$

in a way that $g \in \mathcal{MF}$ satisfies $g * f = \delta$ and as the law is commutative, we also have $f * g = \delta$. □

□

Definition 39. A modular function $f \in \mathcal{MF}$ is said to be multiplicative if for all $M, N \in \mathcal{A}$ whose annihilators are coprime, we have $f(M \times N) = f(M)f(N)$ and $f(\{0\}) = 1$. Let $\mathcal{MM}$ denote the set of all multiplicative modular functions.

Lemma 40. Let $M, N \in \mathcal{A}$ have coprime annihilators. All submodules of $M \times N$ constist in products $K \times L$ with $K \leq M, L \leq N$ so that we have a bijection

$$\mathcal{S}(M) \times \mathcal{S}(N) \xrightarrow{\sim} \mathcal{S}(M \times N)$$

where $S(M)$ denotes the set of all submodules of M.

Proof. Let $T \in S(M \times N)$, $K = \pi_M(T), L = \pi_N(T)$ be the projections of K onto M and N respectively. Let I, J denote the annihilator of M and N respectively. As I and J are coprime, we can find $i \in I, j \in J$ such that $i + j = 1$. Let $(k, l) \in K \times L$. There is $(a, b) \in N \times M$ such that $(k, a), (b, l) \in T$ and therefore we have

$$(k, l) = j(k.a) + i(b, l) \in T$$

so that $T = K \times L$. □

Proposition 41. The set $\mathcal{MM}$ is a subgroup of $\mathcal{MF}^\times$.

Proof. First, we have $\mathcal{MM} \subset \mathcal{MF}^\times$ because of proposition 38. Then, if $f, g \in \mathcal{MM}$, we have $f * g \in \mathcal{MM}$. Indeed, we have

$$f * g(0) = f(0)g(0) = 1$$

and if $M, N \in \mathcal{A}$ have coprime annihilators, the previous lemma gives

$$f * g(M \times N) = \sum_{T \leq M \times N} f(T)g((M \times N)/T) = \sum_{K \leq M,\ L \leq N} f(K \times L)g(M/K \times N/L).$$

Now, observe K and L have coprime annihilators, same with M/K and N/L. As $f, g \in \mathcal{MM}$, we have

$$f * g(M \times N) = \sum_{K \leq M,\ L \leq N} f(K)f(L)g(M/K)g(N/L) = (f * g(M))(f * g(N))$$

and that shows $f * g \in \mathcal{MM}$.

Let us now prove that we have $f^{-1} \in \mathcal{MM}$. By induction over the cardinality of M, N, we will show that we have $f^{-1}(M \times N) = f^{-1}(M)f^{-1}(N)$. If M or N is zero then the conclusion is clear. Now, suppose we have M, N non trivial and assume the result is acquired for finite modules with smaller cardinality. Then, we have

$$
\begin{aligned}
0 &= \delta(M \times N) \\
&= \sum_{\substack{K \leq M \\ L \leq N}} f^{-1}(K) f^{-1}(L) f(M/K) f(N/L) \\
&= \sum_{\substack{K < M \\ L < N}} f^{-1}(K) f^{-1}(L) f(M/K) f(N/L) + f^{-1}(M \times N) \\
&\quad + \sum_{K<M} f^{-1}(K) f^{-1}(N) f(M/K) + \sum_{L<N} f^{-1}(L) f^{-1}(M) f(N/L) \\
&= \sum_{K<M} f^{-1}(K) f(M/K) \sum_{L<N} f^{-1}(L) f(N/L) + f^{-1}(M \times N) \\
&\quad - f^{-1}(N) f^{-1}(M) - f^{-1}(M) f^{-1}(N) \\
&= (-1)^2 f^{-1}(M) f^{-1}(N) - 2 f^{-1}(M) f^{-1}(N) + f^{-1}(M \times N)
\end{aligned}
$$

which leads to $f^{-1}(M \times N) = f^{-1}(M) f^{-1}(N)$. □

□

5.1 Möbius function

The goal of this subsection is to define an analogous object to the usual Möbius function and to be able to compute it.

Definition 42. What preceeds shows that the function 1 (outputing 1 for any finite module) is multiplicative and it is a unit whose inverse is also multiplicative. Let μ denote its inverse.

As μ is multiplicative, to describe its behavior, it suffices to know its values at P-modules, P being a prime ideal of $\mathbb{A}$. We will obtain those values after separating two cases : either M has P-torsion (that is M is isomorphic to some $(\mathbb{A}/P)^n$) or it has not.

Proposition 43. For all $n \in \mathbb{N}$, we have :

$$\mu\left((\mathbb{A}/P)^n\right) = (-1)^n c(P)^{\frac{n(n-1)}{2}}.$$

Proof. All submodules of $(\mathbb{A}/P)^n$ are exactly all its vector subspaces (as a $\mathbb{A}/P$-vector space). Any of these submodules is isomorphic to some $(\mathbb{A}/P)^d$ with $0 \leq d \leq n$. The number of submodules that are isomorphic to a $(\mathbb{A}/P)^d$ for a given d is (see proposition 2)

$$\frac{\left|\mathrm{Mono}((\mathbb{A}/P)^d, (\mathbb{A}/P)^n)\right|}{|\mathrm{Aut}(\mathbb{A}/P)^d|} = \frac{(c(P)^n - 1)\dots(c(P)^n - c(P)^{d-1})}{(c(P)^d - 1)\dots(c(P)^d - c(P)^{d-1})}.$$

Now, we have to show that we have, for all n

$$\sum_{d=0}^{n}(-1)^d c(P)^{d(d-1)/2}\frac{(c(P)^n-1)\dots(c(P)^n-c(P)^{d-1})}{(c(P)^d-1)\dots(c(P)^d-c(P)^{d-1})}=\delta((\mathbb{A}/P)^n).$$

We may prove it by induction on n. Assume the result is acquired for all previous cases and let A_n denote the left side of this last equality. Let $D=(c(P)-1)\dots(c(P)^n-1)$.

Then, we have

$$\begin{aligned}
A_n &= \sum_{d=0}^{n}(-1)^d c(P)^0 c(P)^1\dots c(P)^{d-1}\frac{(c(P)^n-1)\dots(c(P)^n-c(P)^{d-1})}{(c(P)^d-1)\dots(c(P)^d-c(P)^{d-1})}\\
&= \sum_{d=0}^{n}(-1)^d\frac{(c(P)^n-1)\dots(c(P)^n-c(P)^{d-1})}{(c(P)^d-1)\dots(c(P)-1)}\\
&= \frac{1}{D}\sum_{d=0}^{n}(-1)^d(c(P)^{d+1}-1)\dots(c(P)^n-1)\times(c(P)^n-1)\dots(c(P)^n-c(P)^{d-1})\\
&= \frac{1}{D}\sum_{d=0}^{n}\prod_{i=0}^{d-1}(c(P)^i-c(P)^n)\prod_{i=d+1}^{n}(c(P)^i-1).
\end{aligned}$$

Now, we may prove by induction on $k\in[\![0,n]\!]$ that we have

$$\sum_{d=0}^{k}\prod_{i=0}^{d-1}(c(P)^i-c(P)^n)\prod_{i=d+1}^{n}(c(P)^i-1)=\prod_{i=1}^{k}(c(P)^i-c(P)^n)\prod_{i=k+1}^{n}(c(P)^i-1).$$

Assume the result is correct for k and let us show it remains correct for $k+1$. We have

$$\begin{aligned}
\sum_{d=0}^{k+1}\prod_{i=0}^{d-1}(c(P)^i-c(P)^n)\prod_{i=d+1}^{n}(c(P)^i-1) &= \prod_{i=1}^{k}(c(P)^i-c(P)^n)\prod_{i=k+1}^{n}(c(P)^i-1)+\prod_{i=0}^{k}(c(P)^i-c(P)^n)\prod_{i=k+2}^{n}(c(\\
&= \prod_{i=1}^{k}(c(P)^i-c(P)^n)\prod_{i=k+2}^{n}(c(P)^i-1)\times\left(c(P)^{k+1}-1+1-c(P)^n\right)\\
&= \prod_{i=1}^{k}(c(P)^i-c(P)^n)\prod_{i=k+2}^{n}(c(P)^i-1)\times\left(c(P)^{k+1}-c(P)^n\right)\\
&= \prod_{i=1}^{k+1}(c(P)^i-c(P)^n)\prod_{i=k+2}^{n}(c(P)^i-1)
\end{aligned}$$

which puts an end to the induction on k. For $k=n$, we get

$$A_n=\frac{1}{D}\prod_{i=1}^{n}(c(P)^i-c(P)^n)=\delta((\mathbb{A}/P)^n).$$

□

Proposition 44. Let M be a finite P-module that has not P-torsion. We have $\mu(M) = 0$.

Proof. Again, we will show that by induction on the cardinality of M. If $M = \mathbb{A}/(P^2)$ (that is the base case), we can follow the same following steps to show the result. Assume the result is acquired for all previous cases. We have

$$\mu(M) = -\sum_{N<M} \mu(N).$$

Hence, we have by induction

$$\mu(G) = -\sum_{N \leq M[P]} \mu(N).$$

As $M[P] < M$ (because M has not P-torsion) and $M[P] \neq 0$, we get

$$\mu(M) = -\mu * 1(M[P]) = -\delta(M[P]) = 0.$$

□

5.2 Another proof

Now, we may recall proposition 8 and prove it using duality. We just need a lemma before.

Lemma 45. Let M, N be two finite $\mathbb{A}$-modules. We have the following formula :

$$\mathrm{mono}(N, M) = \sum_{K \leq N} \mu(K) \hom(N/K, M).$$

Moreover, if N is a P-module, one can just let K runs over the set of all submodules of $N[P]$, that is :

$$\mathrm{mono}(N, M) = \sum_{K \leq N[P]} \mu(K) \hom(N/K, M).$$

Proof. Let us now prove the second formula. First, count morphisms $N \to M$ according to their kernel K :

$$\hom(N, M) = \sum_{K \leq N} \left| \{ f \in \mathrm{Hom}(N, M) \mid \mathrm{Ker}\, f = K \} \right|.$$

By the universal property of the quotient, this quantity is also

$$\hom(N, M) = \sum_{K \leq N} \mathrm{mono}(N/K, M).$$

As this is satisfied by all finite $\mathbb{A}$-modules M, N, we have

$$\hom(\bullet, M) = 1 * \mathrm{mono}(\bullet, M).$$

Hence, we have $\mathrm{mono}(\bullet, M) = \mu * \hom(\bullet, M)$, that is

$$\mathrm{mono}(N, M) = \sum_{K \leq N} \mu(H) \hom(N/K, M).$$

If N is a P-module, the submodules $K \leq N$ such that $\mu(K) \neq 0$ are submodules of $N[P]$ (see proposition 44). □

Remark 46. This together with proposition 2 actually gives the formula (4) from [Del48].

Proposition 47. Suppose $N \simeq \prod_{i=1}^{s} \mathbb{A}/P^{n_i}$, with $n_i \geq 2$ for all i. Then, we have

$$\mathrm{mono}(N, M) = \hom(N[P], M) \, \mathrm{mono}(P.N, P.M).$$

Proof. As we saw with lemma 45, we have

$$\mathrm{mono}(N, M) = \sum_{K \leq N[P]} \mu(K) \hom(N/H, M).$$

Moreover, for all $K \leq N[P]$ we have a restriction morphism

$$\mathrm{res} : \mathrm{Hom}(N/K, M) \to \mathrm{Hom}(P.(N/K), P.M).$$

This morphism is surjective (this can be seen by manipulating a quasi-basis of N/K for instance). Its kernel can naturally be seen as $\mathrm{Hom}((N/K)/P.(N/K), M)$. Then, the isomorphism theorem gives :

$$\hom(N/K, M) = \hom((N/K)/P.(N/K), M) \hom(P.(N/K), P.M).$$

Observe we have $P.(N/K) = (P.N)/K$ and then the isomorphism theorem gives

$$(N/K)/P.(N/K) \simeq N/P.N \simeq N[P]$$

as these last two modules are $\mathbb{A}/P$ vector spaces that have same cardinality.

Mixing this information with the previous formula that deals only with hom, one gets

$$\hom(N/K, M) = \hom(N[P], M) \hom(P.N/K, P.M).$$

Using the formula of lemma 45 that we recalled at the begining of this proof, one finally deduces

$$\mathrm{mono}(N, M) = \hom(N[P], M) \, \mathrm{mono}(P.N, P.M).$$

□

6 Future

We may try to figure out a way to give a "direct" formula to compute the total number of submodules using μ so that we no longer have to sum over all the possible structures.

The algebra of modular functions may be linked to Hall algebras. Indeed, if we keep same notation as the wikipedia page "Hall algebra", it seems that the indicator functions of finite abelian groups play the same role as the u_μ (consider $\mathbb{A} = \mathbb{Z}$).

Also, we hope we could count the number of submodules of given type and cotype (that is the structure of the submodules N and the structure of the quotients M/N is given) by adapting the methods we used in this article. However, we have not found anything interesting yet.

As we have a convolution product, we thought in vain about having an analogous object to Dirichlet series (we only considered the case $\mathbb{A} = \mathbb{Z}$) by considering sums like

$$\sum_{M \in \mathcal{A}} \frac{f(M)}{|M|^s}$$

for some $f \in \mathcal{MM}$ (or $f \in \mathcal{MF}$), $s \in \mathbb{C}$. The minimum to ask is to have the same rule as for usual Dirichlet series regarding the product of such series and we would also need the Dirichlet serie of 1 to converge. The fact that this is not satisfied even when $\mathbb{A} = \mathbb{Z}$ lead us to consider another convolution product by summing over direct factors instead of summing over submodules. It turns out that we get something really similar to the classical Dirichlet convolution (undecomposable modules play the same role as prime numbers) and we have not found anything interesting linked to that.

Another direction could be to define for every $f \in \mathcal{MF}$ and any $\mathbb{A}$-module M with finite quotients

$$L_M(f) = \sum_{N \leq M} \frac{f(M/N)}{|M/N|^s}$$

where N runs over the set of all non trivial submodules of M (and perhaps allow N to be trivial if M is finite) and $s \in \mathbb{C}$, as long as this makes sens. If $f = 1$ and $M = \mathbb{A}$ is a ring of integers of some number field $\mathbb{K}$, then $L_M(f)$ is the Dedekind zeta function of $\mathbb{A}$. The Euler product reveals a link between $L_{\mathcal{O}_\mathbb{K}}(f)$ and all the $L_{\mathcal{O}_\mathbb{L}}(f)$ where $\mathbb{L}$ runs over the set of all the completions of $\mathbb{K}$ and f is completely multiplicative.

Keep considering $M = \mathbb{A}$, and let $f, g \in \mathcal{MF}$ be such that $L_\mathbb{A}(|f| * |g|)$ exists. Therefore, we can apply Fubini's theorem to get

$$\begin{aligned} L_\mathbb{A}(f * g) &= \sum_{I \leq \mathbb{A}} \frac{f * g(\mathbb{A}/I)}{|\mathbb{A}/I|^s} \\ &= \sum_{I \leq \mathbb{A}} \sum_{I \leq J \leq \mathbb{A}} \frac{f(J/I) g(\mathbb{A}/J)}{|J/I|^s \, |\mathbb{A}/J|^s} \\ &= \sum_{J \leq \mathbb{A}} \frac{g(\mathbb{A}/J)}{|\mathbb{A}/J|^s} \underbrace{\sum_{I \leq J} \frac{f(J/I)}{|J/I|^s}}_{= L_J(f)}. \end{aligned}$$

Given J, observe all $I \leq J$ are exactly those of the form JK for $K \leq \mathbb{A}$ and that we have $J/JK \simeq \mathbb{A}/K$ as $\mathbb{A}$-modules since $\mathbb{A}$ is a Dedekind domain. With that said, we see that we have $L_J(f) = L_{\mathbb{A}}(f)$ and $L_{\mathbb{A}}(f * g) = L_{\mathbb{A}}(f)L_{\mathbb{A}}(g)$.

Take $f = 1 = g$ and observe that we have $1 * 1(M)$ is the number of submodules of M for all $M \in \mathcal{A}$ and let us denote $\mathrm{sub}_{\mathrm{tot}}(M)$ this number. Therefore, we have

$$\sum_{I \leq \mathbb{A}} \frac{\mathrm{sub}_{\mathrm{tot}}(\mathbb{A}/I)}{|\mathbb{A}/I|^s} = L_{\mathbb{A}}(1)^2$$

which etablishes a link beetween Dedekind zeta functions and the number of submodules.

The number of submodules of M gets complexe to compute when M is a direct product of many modules and that leads to introduce

$$L_{\mathbb{A}}^{(n)}(f) = \sum_{I_1 \times \cdots \times I_n \leq \mathbb{A}^n} \frac{f(\mathbb{A}/I_1 \times \cdots \times \mathbb{A}/I_n)}{|\mathbb{A}/I_1|^s \cdots |\mathbb{A}/I_n|^s}.$$

Observe that, if f is completely multiplcative, then we have $L_{\mathbb{A}}^{(n)}(f) = L_{\mathbb{A}}(f)^n$.

7 Remerciements

Une discussion avec Nikola TOMIC nous a permis d'avoir l'idée de regarder *P.N* et *P.M* pour trouver une formule de récurrence et on l'en remercie.

On remercie également Nathanaël HASSLER qui a bien voulu relire la version anglaise de ce qui a servi de base à cet article.

References

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Grad. Texts Math.* New York, NY: Springer, 2000.

[Del48] Jean Delsarte. Fonctions de Möbius sur les groupes abeliens finis. *Ann. Math. (2)*, 49:600–609, 1948.

[HR63] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis. Vol. I: Structure of topological groups. Integration theory. Group representations*, volume 115 of *Grundlehren Math. Wiss.* Springer, Cham, 1963.

[Lan94] Serge Lang. *Algebraic number theory.*, volume 110 of *Grad. Texts Math.* New York: Springer-Verlag, 2nd ed. edition, 1994.

[LP00] Ribes Luis and Zalesskii Pavel. *Profinite groups*, volume 40 of *Ergeb. Math. Grenzgeb., 3. Folge*. Berlin: Springer, 2000.

[MB] Louis Mallet-Burgues. Arithmétique des groupes abéliens finis. *arXiv:2305.01987*.