J. Math. Cryptol. ? (????), 1 – 20
DOI 10.1515/jmc-????-???

Moduli space of pairings on the complex roots of unity

Laurent Poinsot and Nadia El Mrabet

Communicated by ???

Abstract. Beginning with a general concept of bilinear maps and pairings in any (symmetric) monoidal closed category, we provide a description of the moduli space of pairings, *i.e.*, a complete solution to the classification problem of pairings, up to isomorphism, from finite abelian groups to the group of complex roots of unity (which appears to be exactly the same as the classification of finite abelian groups up to isomorphism). We also provide an algebraic description of the monoid of equivalence classes of pairings as a projective limit of monoids (with a zero). Moreover we prove a geometric property satisfied by this monoid, namely that it embeds as a submonoid of the rational points of an algebraic monoid (on an algebraic closed field).

Keywords. Pairing, bilinear map, finite decomposition monoid, locally finite monoid, monoid scheme.

2010 Mathematics Subject Classification. Primary 11E99, 20M99; Secondary 11E39, 14L15, 20M10.

1 Introduction

The classification of bilinear maps, or more precisely bilinear forms and pairings, has been a long standing problem, investigated by many authors [6, 10, 14, 16, 17]. This problem was solved by C. Riehm [14] for non-degenerate bilinear forms on a finite dimensional vector space, and by C.T.C Wall [16] for non-singular (or perfect) skew-symmetric bilinear maps from a finite abelian group to the group $\mathbb{Q}/\mathbb{Z}$ of roots of unity, and also for symmetric bilinear maps from a finite abelian p-group, p odd, to $\mathbb{Q}/\mathbb{Z}$. In any cases we observe that the domain of the bilinear map is of the form $a \times a$, where a is a (finite-dimensional) vector space or a finite abelian group, and two bilinear maps, say $f\colon a \times a \to c$, and $g\colon b \times b \to c$, are said to be equivalent if there is an isomorphism $\alpha\colon a \to b$ such that $g(\alpha(x), \alpha(y)) = f(x, y)$ for every $x, y \in a$. Here we also deal with the classification problem of non-degenerate bilinear maps, hereafter called pairings, but in a somewhat different

One of the authors, Nadia El Mrabet, was supported by French ANR INS 2012 project SIMPATIC.

setting. Foremost our results are category-theoretic in nature. In fact from our point of view pairings form a full subcategory of the slice category $\otimes/c$ over an object c in a monoidal closed category. Thus bilinearity, at least for the beginning of this paper, referred to some monoidal tensor product $\otimes$, and it is not imposed for a bilinear map $f\colon a\otimes b\to c$ that $a\cong b$. The idea, as always with category theory, is to provide some general results that may be instanced in particular domains of interest, and to provide relations between the categories into consideration. It also brings a new perspective on well-known objects. For instance it is shown here that the category of pairings is itself symmetric monoidal. Moreover the definition of a category comes with the definition of its morphisms. According to our choice, a morphism α between two bilinear maps $f\colon a\otimes b\to c$ and $g\colon d\otimes e\to c$ is a pair of morphisms in the ambient monoidal category (α,β), $\alpha\colon a\to d$, $\beta\colon b\to e$, such that $g\circ(\alpha\otimes\beta)=f$. Here is the main difference with earlier works on the same subject: our equivalence relation (of a category-theoretic nature) is coarser than the one discussed above (it identifies more bilinear maps than the classical equivalence), which explains, at least in part, in why our solution to the classification problem of pairings from finite abelian groups to the roots of unity appears so simple: to each isomorphic class of finite abelian groups corresponds one, and only one, isomorphic class of pairings. Apart from the (rather disappointing) classification of pairings, we also provide two descriptions of the monoid (of equivalence classes) of pairings. An algebraic one as a so-called Rees quotient of the monoid (of equivalence classes) of bilinear maps by its prime ideal of degenerate maps, and also a geometrico-algebraic description as a submonoid of rational points (when we consider an algebraic closed field) of some pro-affine algebraic monoid. The later characterization is based on a fundamental property satisfied by the monoid of pairings, namely local finiteness, meaning that any pairing admits only finitely many decompositions as a sum of (non-trivial) pairings.

The plan of the paper is as follows. First we list our terminology and definitions from category theory in Section 2. In particular we introduce the category of bilinear maps (and that of pairings), and prove some results such as the preservation of non-degeneracy and perfectness by the isomorphism relation of the category of bilinear maps (Lemma 2.6). Then in Section 3, restricting to the categories of modules, abelian groups or commutative monoids, we provide a symmetric monoidal structure $\perp$ on the categories of bilinear maps and of pairings, lifted from the coproduct of the ambient category. This symmetric monoidal tensor factors through the quotient by the isomorphism relation and provides a structure of commutative monoid on equivalent classes of pairings. Theorem 3.4 here is essential since it claims that the "sum", with respect to $\perp$, of two bilinear maps is a pairing if, and only if, the two factors are pairings themselves. This leads, in Section 4, to the idea of decomposing a pairing into "smaller" ones (see for instance Lemma 4.8). In fact two Subsections 4.1 and 4.2 are devoted to general results about some classes of combinatorial monoids, namely finite decomposition monoids and its subclass of locally finite monoids. In particular we prove (Theorem 4.3) that any monoid from the former class gives rise to a monoid scheme (and thus to an algebraic monoid when the base ring is an algebraic closed field). It is also shown that the monoid (of equivalence classes) of pairings is locally finite (and thus it is also a finite decomposition monoid) so that it may be embedded into rational points of a larger algebraic monoid (or more generally, a monoid scheme), and thus may be referred to as the *moduli space of pairings*. Finally in the Sections 5 and 6 we describe the solutions, already discussed above, to the classification problems of pairings on finite abelian groups to roots of unity, and on free modules of finite rank to the base ring.

2 A categorical setting for bilinear maps

2.1 Category-theoretic notions and notations

Even if it is not essential hereafter we assume a universe given (see [12]). Small sets refer to its members while by classes (or large sets) is meant subsets of the universe. Let $\mathcal{C}$ be a category. The class of its objects is denoted by $\mathbf{Ob}(\mathcal{C})$, and if $a, b \in \mathbf{Ob}(\mathcal{C})$, then the class of arrows (also called maps or morphisms or even $\mathcal{C}$-morphisms) from a to b is denoted by $\mathcal{C}(a, b)$ (of course it is also denoted by $f\colon a \to b$). The isomorphism relation in any category is denoted by $\cong$. If S is a class of arrows of $\mathcal{C}$ closed under composition and that contains all the identity maps of $\mathcal{C}$, then $\mathcal{C}_S$ is the obvious subcategory of $\mathcal{C}$ with arrows S. For instance, $\mathcal{C}_{\mathbf{mono}}$ is the subcategory obtained by taking for S the class of all monomorphisms (left cancellable arrows) of $\mathcal{C}$, and $\mathcal{C}_{\mathbf{iso}}$ is the core of $\mathcal{C}$, *i.e.*, the groupoid with objects those of $\mathcal{C}$ and arrows its isomorphisms.

In what follows we consider several categories such as the category $\mathbf{Set}$ of sets, $\mathbf{CMon}$ (respectively, $\mathbf{CMonfin}$) of (respectively, finite) commutative monoids, $\mathbf{Ab}$ (respectively, $\mathbf{Abfin}$) of (respectively, finite) abelian groups. When R is a commutative ring with a unit, then ${}_R\mathbf{Mod}$ is the category of R-modules (in particular, ${}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$), and ${}_R\mathbf{Modfreefin}$ its full subcategory of free R-modules of finite rank (here R is assumed to be non-zero). Finally ${}_R\mathbf{CAlg}$ denotes the category of commutative R-algebras with a unit.

A monoidal category will be identified with its underlying category, and its tensor is denoted by $\otimes$ (except the usual tensor product $\otimes_R$ of R-modules). The commutativity constraint of a symmetric monoidal category is denoted by σ. A *monoidal closed category* is a symmetric monoidal category ([12]) such that for each object b of $\mathcal{C}$, the functor $-\otimes b\colon \mathcal{C} \to \mathcal{C}$ admits a right adjoint $(-)^b\colon \mathcal{C} \to \mathcal{C}$

(which is referred to as the *internal hom functor* or *exponential*), *i.e*, for every objects a, c, there is a bijection $\lambda_{a,b,c} \colon \mathcal{C}(a \otimes b, c) \xrightarrow{\sim} \mathcal{C}(a, c^b)$ natural in a and c (and that can be made in a unique way also natural in b). As examples of such categories: every cartesian closed category ($\mathbf{Set}$, Kelley spaces, the category of all small categories, any topos, ...), the slice categories of any locally cartesian category, $\mathbf{CMon}$ (with internal hom functor the biadditive maps), $\mathbf{Ab}$, ${}_R\mathbf{Mod}$, ${}_R\mathbf{Modfreefin}$, the category of commutative and cocommutative Hopf algebras on a base field (see [9]), the category of Banach space with short maps, with internal hom the bounded linear maps (see [2]) and with the projective tensor product. Of course, because $\mathcal{C}$ is assumed symmetric, for each object b, $b \otimes -$ also admits a right adjoint (see [3], Proposition 6.4 p. 294).

In what follows we also needs to deal with coproducts so that here are introduced some notations about them. Let $\mathcal{C}$ be a category with binary coproducts. Let a, b be two objects of $\mathcal{C}$, then a coproduct diagram of a and b will be denoted as $a \xrightarrow{q_A} a \oplus b \xleftarrow{q_B} b$, where q_a and q_b are the natural "injections" (while they are not required to be monomorphisms), and if $\alpha \colon a_1 \to a_2$ and $\beta \colon b_1 \to b_2$, the unique arrow f making the following diagram commute

$$\begin{array}{ccccc} a_1 & \xrightarrow{q_{a_1}} & a_1 \oplus b_1 & \xleftarrow{q_{b_1}} & b_1 \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle\beta} \\ a_2 & \xrightarrow{q_{a_2}} & a_2 \oplus b_2 & \xleftarrow{q_{b_2}} & b_2 \end{array} \qquad (2.1)$$

is denoted by $\alpha \oplus \beta$ (of course it depends on the choices of the coproduct diagrams of a_1, b_1, and of a_2, b_2).

Finally slice categories are central in this work and thus deserved a short paragraph on their own. Let $\mathcal{B}$ and $\mathcal{C}$ be two categories, let $F \colon \mathcal{B} \to \mathcal{C}$ be a functor, and let c be a fixed object of $\mathcal{C}$. The *slice category* [12] F/c of F over c has objects all pairs (f, a) where a is an object of $\mathcal{B}$ and $f \in \mathcal{C}(F(a), c)$, and an arrow between two objects (f, a) and (g, b) of F/c is an arrow $\alpha \colon a \to b$ in $\mathcal{B}$ such that the following triangle commutes.

$$\begin{array}{ccc} F(a) & \xrightarrow{F(\alpha)} & F(b) \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & c & \end{array} \qquad (2.2)$$

Composition of arrows is defined in the obvious way. In particular the identity arrow $id_{(f,a)}$ in F/c of an object (f, a) is given by the identity map id_a in $\mathcal{B}$. Of course, a morphism $\alpha\colon (f,a) \to (g,b)$ in F/c is an isomorphism if, and only if, $\alpha\colon a \to b$ is an isomorphism in $\mathcal{B}$.

2.2 Categories of bilinear maps

Let us fix some data for the remainder of this contribution. Let $\mathcal{C}$ be a monoidal closed category, and let $\mathcal{D}$ be any full subcategory of $\mathcal{C}$ (of course it may be $\mathcal{C}$ itself). The full embedding from $\mathcal{D}$ to $\mathcal{C}$ is denoted by j.

Definition 2.1. Given an object c of $\mathcal{C}$, the *category* $\mathbf{Bil}_{\mathcal{D}}(c)$ *of bilinear maps on* c is the slice category $\otimes \circ (j \times j)/c$.

In details an object of $\mathbf{Bil}_{\mathcal{D}}(c)$, called a *bilinear map on* c, is a pair $(f,(a,b))$, where a,b are objects of $\mathcal{D}$, and $f\colon a\otimes b \to c$ is a $\mathcal{C}$-morphism, and a morphism $\alpha\colon (f,(a,b)) \to (g,(d,e))$ is a pair (α,β) of $\mathcal{D}$-morphisms $\alpha\colon a \to d$ and $\beta\colon b \to e$ such that the following triangle commutes.

$$\begin{array}{ccc} a\otimes b & \xrightarrow{\alpha\otimes\beta} & d\otimes e \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & c & \end{array} \tag{2.3}$$

Remark 2.2. Our terminology may cause some trouble with the usual one. For instance, if $(f,(a,b))$ is a bilinear map on c in the category of R-modules, then it is a **linear map** $f\colon a\otimes b \to c$. But since there is a unique **bilinear map** (in the usual sense) $f_0\colon a\times b \to c$ associated to f we are rather on the safe side.

Because $\mathcal{C}$ is assumed closed, for each $f \in \mathcal{C}(a\otimes b, c)$, we may define its *left adjoint* $\gamma_f \in \mathcal{C}(a, c^b)$ as $\lambda_{a,b,c}(f)$. By symmetry we also define a *right adjoint* $\delta_f \in \mathcal{C}(b, c^a)$ by $\lambda_{b,a,c}(f \circ \sigma_{b,a})$. By definitions these are considered as left and right adjoints of the bilinear map $(f,(a,b))$ on c. When $\mathcal{C} = \mathbf{Set}$, then for a bilinear map $(f,(a,b))$, $f\colon a\times b \to c$, and $\gamma_f\colon a \to c^b$ is given by $x \mapsto \gamma_f(x,-)$, while $\delta_f\colon b \to c^a$ is equal to $y \mapsto f(-,y)$. If $\mathcal{C} = {}_R\mathbf{Mod}$, then for a bilinear map $(f,(a,b))$, $f\colon a\otimes_R b \to c$ (so that f may be identified with a usual R-bilinear map $f_0\colon a\times b \to c$), $\gamma_f\colon a \to {}_R\mathbf{Mod}(b,c)$ is given by $x \mapsto f_0(x,-)$, and $\delta_f\colon b \to {}_R\mathbf{Mod}(a,c)$ is defined by $y \mapsto f_0(-,y)$ (where ${}_R\mathbf{Mod}(d,c)$ is seen as a R-module in a canonical way, $d = a,b$). If $\mathcal{C} = \mathbf{CMon}$, then for a bilinear map $(f,(a,b))$, γ_f and δ_f are given as in the R-module case (with R-bilinearity replaced by biadditivity).

Definition 2.3. A *pairing* on c is a bilinear map $(f,(a,b))$ such that both adjoints γ_f and δ_f are monomorphisms. In this situation we also say that $(f,(a,b))$ is a *non-degenerate* bilinear map on c. A *pairing* $(f,(a,b))$ is said to be *perfect* when γ_f and δ_f are also epimorphisms (*i.e.*, right cancelable arrows), so that they are isomorphisms.

Remark 2.4. We observe that when $\mathcal{C} = \mathbf{Ab} = {}_{\mathbb{Z}}\mathbf{Mod}$ (or even $\mathcal{C} = {}_R\mathbf{Mod}$) are recovered the usual notions of non-degeneracy and of perfect pairings (see [15]).

The *category of (perfect) pairings on* c, denoted by $\mathbf{Pair}_{\mathcal{D}}(c)$ (respectively, $\mathbf{Perf}_{\mathcal{D}}(c)$), is defined as the full subcategory of $\mathbf{Bil}_{\mathcal{D}}(c)$ (respectively, $\mathbf{Pair}_{\mathcal{D}}(c)$) with objects all the (perfect) pairings on c. In brief, we have a sequence of full inclusion functors $\mathbf{Perf}_{\mathcal{D}}(c) \hookrightarrow \mathbf{Pair}_{\mathcal{D}}(c) \hookrightarrow \mathbf{Bil}_{\mathcal{D}}(c) \hookrightarrow \otimes \circ (j \times j)/c$.

2.3 Some obvious functorial properties

The definition of $\mathbf{Bil}_{\mathcal{D}}(c)$ is actually functorial in c: let $\mathbf{CAT}$ be the category of all (large) categories. We may define a functor $\mathbf{Bil}_{\mathcal{D}}(-)\colon \mathcal{C} \to \mathbf{CAT}$ as follows. Let c_1, c_2 be two objects of $\mathcal{C}$, and let $\phi \in \mathcal{C}(c_1, c_2)$. Then, $\mathbf{Bil}_{\mathcal{D}}(\phi)$ is the functor from $\mathbf{Bil}_{\mathcal{D}}(c_1)$ to $\mathbf{Bil}_{\mathcal{D}}(c_2)$ which acts as the identity on arrows, and maps a bilinear map $(f,(a,b))$ on c_1 to $(\phi \circ f,(a,b))$ which of course is a bilinear map on c_2. By restriction (and corestriction), we may define two other functors:

(i) $\mathbf{Pair}_{\mathcal{D}}(-)\colon \mathcal{C}_{\mathbf{mono}} \to \mathbf{CAT}_{\mathbf{fullemb}}$ (where $\mathbf{fullemb}$ is the class of all full embeddings, *i.e.*, full functors, injective on arrows). Thus if there are some monomorphisms $c_1 \to c_2$, then $\mathbf{Pair}_{\mathcal{D}}(c_1)$ may be seen as a full subcategory of $\mathbf{Pair}_{\mathcal{D}}(c_2)$. (If $j \in \mathcal{C}_{\mathbf{mono}}(c_1, c_2)$, then $e_j\colon \mathbf{Bil}_{\mathcal{D}}(c_1) \hookrightarrow \mathbf{Bil}_{\mathcal{D}}(c_2)$ is a full embedding defined on objects by $e_j(f,(a,b)) = (j \circ f,(a,b))$ and which is the identity on arrows.)

(ii) $\mathbf{Perf}_{\mathcal{D}}(-)\colon \mathcal{C}_{\mathbf{iso}} \to \mathbf{CAT}_{\mathbf{iso}}$.

By definition of functors, if $c_1 \cong c_2$ (isomorphic objects in $\mathcal{C}$), then $\mathbf{Bil}_{\mathcal{D}}(c_1) \cong \mathbf{Bil}_{\mathcal{D}}(c_2)$, $\mathbf{Pair}_{\mathcal{D}}(c_1) \cong \mathbf{Pair}_{\mathcal{D}}(c_2)$ and $\mathbf{Perf}_{\mathcal{D}}(c_1) \cong \mathbf{Perf}_{\mathcal{D}}(c_2)$ (isomorphic categories). But the converse may be false (*e.g.* $\mathcal{C} = \mathbf{Ab}$, $\mathbf{Pair}_{\mathbf{Abfin}}(0) \cong \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Z}^{(X)})$, where $\mathbb{Z}^{(X)}$ is the free abelian group on a set X).

Let us assume that $\mathcal{E} \hookrightarrow \mathcal{D} \hookrightarrow \mathcal{C}$ is a sequence of full embeddings of categories. Then for every object c of $\mathcal{C}$ the following diagram of functors commutes (each arrow being a full embedding).

$$\begin{array}{ccccc} \mathbf{Perf}_{\mathcal{D}}(c) & \hookrightarrow & \mathbf{Pair}_{\mathcal{D}}(c) & \hookrightarrow & \mathbf{Bil}_{\mathcal{D}}(c) \\ \uparrow & & \uparrow & & \uparrow \\ \mathbf{Perf}_{\mathcal{E}}(c) & \hookrightarrow & \mathbf{Pair}_{\mathcal{E}}(c) & \hookrightarrow & \mathbf{Bil}_{\mathcal{E}}(c) \end{array} \tag{2.4}$$

2.4 Preservation of non-degeneracy and perfectness by isomorphism

Remark 2.5. A morphism $(\alpha, \beta)\colon (f, (a, b)) \to (g, (d, e))$ in $\mathbf{Bil}_{\mathcal{D}}(c)$ is an isomorphism if, and only if, $(\alpha, \beta)\colon (a, d) \to (b, e)$ is an isomorphism in $\mathcal{D} \times \mathcal{D}$ if, and only if, $\alpha\colon a \to d$ and $\beta\colon b \to e$ are isomorphisms in $\mathcal{D}$. Because $\mathbf{Perf}_{\mathcal{D}}(c)$ and $\mathbf{Pair}_{\mathcal{D}}(c)$ are both full subcategories of $\mathbf{Bil}_{\mathcal{D}}(c)$, their isomorphisms are the same as those of $\mathbf{Bil}_{\mathcal{D}}(c)$.

Lemma 2.6. *Let $(f, (a, b)), (g, (d, e))$ be two bilinear maps on c such that $f \cong g$ (in $\mathbf{Bil}_{\mathcal{D}}(c)$). If f is a (perfect) pairing, then also is g, and of course they are isomorphic as (perfect) pairings. Similarly, if $(f, (a, b)), (g, (d, e))$ are two pairings on c such that $f \cong g$ (in $\mathbf{Pair}_{\mathcal{D}}(c)$), then f is perfect implies that also is g, and of course they are isomorphic as perfect pairings.*

Proof. Since $f \cong g$, according to Remark 2.5, there are two $\mathcal{D}$-isomorphisms $\alpha\colon a \to d$ and $\beta\colon b \to e$ such that $g \circ (\alpha \otimes \beta) = f$. Thus $\gamma_g = \lambda_{d,e,c}(f \circ \alpha^{-1} \otimes \beta^{-1}) = c^{\beta^{-1}} \circ \lambda_{a,b,c}(f) \circ \alpha^{-1}$ (by naturality of λ, and where $c^{(-)}$ is the obvious contravariant functor from $\mathcal{C}$ to itself) which proves that γ_g is a monomorphism (respectively, isomorphism) when γ_f is so. Symmetrically we get $\delta_g = c^{\alpha^{-1}} \circ \delta_f \circ \beta^{-1}$. The rest of the proof is straightforward. □

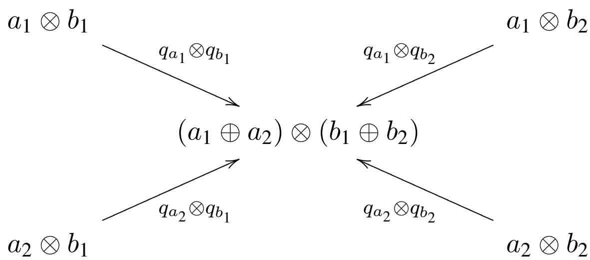
Lemma 2.6 states that the isomorphism relation $\cong$ in $\mathbf{Bil}_{\mathcal{D}}(c)$ (respectively, $\mathbf{Pair}_{\mathcal{D}}(c)$) preserves both non-degeneracy and perfectness (respectively, perfectness). An isomorphism class of bilinear maps (respectively, pairings) either contains no pairings (respectively, perfect pairings) or all its members are pairings (respectively, perfect pairings).

3 A symmetric monoidal structure on $\mathrm{Bil}_{\mathcal{D}}(c)$

From now on, one assumes that $\mathcal{C} = {}_R\mathrm{Mod}$ or $\mathcal{C} = \mathrm{CMon}$, and that the class of objects of $\mathcal{D}$ is closed under coproducts (*i.e.*, if a, b are objects of $\mathcal{D}$, and if d is an object of $\mathcal{C}$ which is a coproduct of a and b, in $\mathcal{C}$, then d belongs to the object class of $\mathcal{D}$).

Remark 3.1. The above assumptions are valid for instance in the following cases (1) $\mathcal{C} = {}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$ and $\mathcal{D} = \mathbf{Abfin}$, (2) $R \neq (0)$, $\mathcal{C} = {}_R\mathbf{Mod}$ and $\mathcal{D} = {}_R\mathbf{Modfreefin}$, and (3) $\mathcal{C} = \mathbf{CMon}$ and $\mathcal{D} = \mathbf{CMonfin}$.

Since $-\otimes b$ and $b \otimes -$ both admit a right adjoint, they preserve colimits, and in particular coproducts $\oplus$. Thus, $(a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \cong (a_1 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_1) \oplus (a_2 \otimes b_2)$ where a_1, a_2, b_1, b_2 are objects of $\mathcal{D}$, and more precisely $(a_1 \oplus a_2) \otimes (b_1 \oplus b_2)$ has the following coproduct presentation



(3.1)

where $q_{a_i} \colon a_i \to a_i \oplus b_j \leftarrow b_j \colon q_{b_j}$ is a coproduct diagram of a_i and b_j. Now, let $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ be two bilinear maps on c. Then, we define $f_1 \perp f_2 \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to c$ as the unique morphism such that $(f_1 \perp f_2) \circ q_{a_1} \otimes q_{b_1} = f_1$, $(f_1 \perp f_2) \circ q_{a_2} \otimes q_{b_2} = f_2$, $(f_1 \perp f_2) \circ q_{a_1} \otimes q_{b_2} = 0_{a_1 \otimes b_2, c}$, $(f_1 \perp f_2) \circ q_{a_2} \otimes q_{b_1} = 0_{a_2 \otimes b_1, c}$ (where $0_{x,y}$ is the unique map $x \to (0) \to y$ for every objects x, y of $\mathcal{C}$). Because $\mathcal{D}$ is assumed to be a full subcategory and its class of objects being closed under $\oplus$, $(f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$ is an object of $\mathbf{Bil}_{\mathcal{D}}(c)$. Practically $(f_1 \perp f_2)((x_1, x_2) \otimes (y_1, y_2)) = f_1(x_1 \otimes y_1) + f_2(x_2 \otimes y_2)$ for every $x_i \in a_i$, $y_i \in b_i$, $i = 1, 2$.

Remark 3.2. The operation $\perp$ on bilinear maps is sometimes called *orthogonal sum*, see for instance [6]. But it is not a coproduct. Indeed, let $q_i = (q_{a_i}, q_{b_i})$, $i = 1, 2$. Then q_i is a morphism (in $\mathbf{Bil}_{\mathcal{D}}(c)$) from $(f_i, (a_i, b_i))$ to $(f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$ but $(f_1, (a_1, b_1)) \overset{q_1}{\to} (f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2)) \overset{q_2}{\leftarrow} (f_2, (a_2, b_2))$ fails to form a coproduct diagram for $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ (essentially because the values of the map $f_1 \perp f_2$ on $a_1 \otimes b_2$ and $a_2 \otimes b_1$, which are null, are not determined by those on $a_1 \otimes a_2$ and $b_1 \otimes b_2$).

If $(f_i, (a_i, b_i)), (g_i, (d_i, e_i))$, $i = 1, 2$, are objects of $\mathbf{Bil}_{\mathcal{D}}(c)$, and if (α_i, β_i) is a morphism (in $\mathbf{Bil}_{\mathcal{D}}(c)$) from $(f_i, (a_i, b_i))$ to $(g_i, (d_i, e_i))$, $i = 1, 2$, then the pair of $\mathcal{D}$-morphisms $(\alpha_1 \oplus \alpha_2, \beta_1 \oplus \beta_2)$ is a morphism from $(f_1 \perp g_1, (a_1 \oplus d_1, b_1 \oplus e_1))$

to $(f_2 \perp g_2, (a_2 \oplus d_2, b_2 \oplus e_2))$ or in other terms the following diagram commutes.

$$\begin{array}{ccc} (a_1 \oplus a_2) \otimes_R (b_1 \oplus b_2) & \xrightarrow{(\alpha_1 \oplus \alpha_2) \otimes (\beta_1 \oplus \beta_2)} & (d_1 \oplus d_2) \otimes_R (e_1 \oplus e_2) \\ & {\scriptstyle f_1 \perp f_2} \searrow \quad \swarrow {\scriptstyle g_1 \perp g_2} & \\ & c & \end{array} \tag{3.2}$$

Indeed,

$$\begin{aligned} (g_1 \perp g_2) \circ (\alpha_1 \oplus \alpha_2) \otimes (\beta_1 \oplus \beta_2) \circ q_{a_1} \otimes q_{b_1} &= (g_1 \perp g_2) \circ q_{d_1} \otimes q_{e_1} \circ \alpha_1 \otimes \beta_1 \\ &= g_1 \circ \alpha_1 \\ &= f_1 \\ &= (f_1 \perp f_2) \circ q_{a_1} \otimes q_{b_1} \ , \end{aligned} \tag{3.3}$$

and also,

$$\begin{aligned} (g_1 \perp g_2) \circ (\alpha_1 \oplus \alpha_2) \otimes (\beta_1 \oplus \beta_2) \circ q_{a_1} \otimes q_{b_2} &= (g_1 \perp g_2) \circ q_{d_1} \otimes q_{e_2} \circ \alpha_1 \otimes \beta_2 \\ &= 0_{d_1 \otimes e_2, c} \circ \alpha_1 \otimes \beta_2 \\ &= 0_{a_1 \otimes b_2, c} \\ &= (f_1 \perp f_2) \circ q_{a_1} \otimes q_{b_2} \ , \end{aligned} \tag{3.4}$$

and similarly for the other factors $a_2 \otimes b_2$ and $a_2 \otimes a_1$ of the coproduct $(a_1 \oplus a_2) \otimes (b_1 \oplus b_2)$. So by the universal property of the coproduct, Diagram (3.2) indeed commutes. Let us assume that a choice of coproduct diagrams is made for each pair of object in $\mathcal{C}$ in such a way that $\oplus$ is turned into a bifunctor. Then, $\perp$ also becomes a bifunctor. Moreover it endows $\mathbf{Bil}_{\mathcal{D}}(c)$ with a structure of symmetric monoidal category, where the unit is $0_{(0)\otimes(0),c}$ (which is vacuously a perfect pairing) and for $(f_i, (a_i, b_i)) \in \mathbf{Bil}_{\mathcal{D}}(c)$, $i = 1, 2, 3$, the commutativity constraint is given by

$$\sigma_{(f_1,(a_1,a_2)),(f_2,(a_2,b_2))} = (\sigma_{a_1,a_2}, \sigma_{b_1,b_2}) \colon (f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2)) \to (f_2 \perp f_1, (a_2 \oplus a_1, b_2 \oplus b_1)) \ , \tag{3.5}$$

the associativity constraint is given by

$$\begin{aligned} &\alpha_{(f_1,(a_1,b_1)),(f_2,(a_2,b_2)),(f_3,(a_3,b_3))} = (\alpha_{a_1,a_2,a_3}, \alpha_{b_1,b_2,b_3}) \colon \\ &(f_1 \perp (f_2 \perp f_3), (a_1 \oplus (a_2 \oplus a_3), b_1 \oplus (b_2 \oplus b_3)) \to ((f_1 \perp f_2) \perp f_3, ((a_1 \oplus a_2) \oplus a_3, (b_1 \oplus b_2) \oplus b_3)) \ , \end{aligned} \tag{3.6}$$

the left unit constraint is

$$\lambda_{(f_1,(a_1,b_1))} = (\lambda_{a_1}, \lambda_{b_1}) \colon (0_{(0)\otimes(0),c} \perp f_1, ((0) \oplus a_1, (0) \oplus b_1)) \to (f_1, (a_1, b_1)) \tag{3.7}$$

and the right unit constraint is

$$\rho_{(f_1,(a_1,b_1))} = (\rho_{a_1}, \rho_{a_2})\colon (f_1 \bot 0_{(0)\otimes(0),c}, (a_1 \oplus (0), b_1 \oplus (0))) \to (f_1, (a_1, b_1)) \ , \quad (3.8)$$

where $\sigma_{a,b}$, $\alpha_{a,b,c}$, λ_a and ρ_a are the corresponding constraints of the cocartesian structure $\oplus$ of $\mathcal{C}$. (Coherence for $\bot$ with these constraints is lifted from that of $\oplus$, and the details of the verification are left to the reader.)

Theorem 3.3. *For each object c of $\mathcal{C}$, the category $\mathbf{Bil}_{\mathcal{D}}(c)$ is symmetric monoidal, with monoidal tensor $\bot$.*

The bifunctor $\bot$ also satisfies a crucial property with respect to non-degeneracy and perfectness.

Theorem 3.4. *Let $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ be two objects of $\mathbf{Bil}_{\mathcal{D}}(c)$. The bilinear map $(f_1 \bot f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$ is a pairing (respectively, perfect pairing) if, and only if, $(f_i, (a_i, b_i))$ is a pairing (respectively, perfect pairing), $i = 1, 2$.*

Proof. Let us denote by g_i the canonical R-bilinear maps, in case $\mathcal{C} = {}_R\mathbf{Mod}$, or biadditive maps, in case $\mathcal{C} = \mathbf{CMon}$, associated to f_i, $i = 1, 2$, and by h that associated to $f_1 \bot f_2$. Let us assume that $f_1 \bot f_2$ is a pairing. Let $x_1 \in a_1$ such that for every $y_1 \in b_1$, $g_1(x_1, y_1) = 0$. Then, for every (y_1, y_2), $h((x_1, 0), (y_1, y_2)) = g_1(x_1, y_1) = 0$ in such a way that $x_1 = 0$ by non-degeneracy of $f_1 \bot f_2$. This easily implies that f_1, and thus also f_2 by a symmetric argument, is non-degenerate. Furthermore to prove that $f_1 \bot f_2$ is a perfect pairing implies that both f_1 and f_2 is a perfect pairing, we assume that for instance f_1 is a pairing but not perfect. So there exists $\phi_1 \in \mathcal{C}(b_1, c)$ that does not belong to the image of γ_{f_1}. Now let $\phi \in \mathcal{C}(b_1 \oplus b_2, c)$ such that $\phi \circ q_{b_1} = \phi_1$ and $\phi \circ q_{b_2} = 0$. Then, ϕ does not belong to the image of $\gamma_{f_1 \bot f_2}$ for if $h((x_1, x_2), (y_1, y_2)) = \phi(y_1, y_2) = \phi_1(y_1)$ and thus $g_1(x_1, y_1) = h((x_1, x_2), (y_1, 0)) = \phi_1(y_1)$ which contradicts the fact that f_1 is not perfect. Let us assume that both f_1 and f_2 are non-degenerate. Let $(x_1, x_2) \in a_1 \oplus a_2$ such that for every $(y_1, y_2) \in b_1 \oplus b_2$, $0 = h((x_1, x_2), (y_1, y_2)) = g_1(x_1, y_1) + g_2(x_2, y_2)$. In particular for every $y_1 \in b_1$, $0 = h((x_1, x_2), (y_1, 0)) = f_1(x_1, y_1)$. Thus $x_1 = 0$. A similar argument shows that x_2 also equals 0. By symmetry this implies that $f_1 \bot f_2$ is non-degenerate. Moreover let us assume that f_1 and f_2 are perfect pairings. Let $\phi \in \mathcal{C}(b_1 \oplus b_2, c) \cong \mathcal{C}(b_1, c) \times \mathcal{C}(b_2, c)$, and let $\phi_i \in \mathcal{C}(b_i, c)$, $i = 1, 2$, be the components of ϕ under the previous natural bijection. Because f_i is a perfect pairing for each $i = 1, 2$, there are unique $x_1 \in a_1$ and $x_2 \in a_2$ such that $g_i(x_i, -) = \phi_i$, $i = 1, 2$. Since $h((x_1, x_2), -) \circ q_{b_i} = g_i(x_i, -) = \phi_i$, $i = 1, 2$, it follows that $h((x_1, x_2), -) = \phi$, and (the same holds for the right adjoint) $f_1 \bot f_2$ is a perfect pairing □

4 Moduli space of pairings

4.1 Rees quotient

Lemma 2.6 shows that $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ is divided into two non-overlapping parts, that of isomorphic classes (in $\mathbf{Bil}_{\mathcal{D}}(c)$ and also in $\mathbf{Pair}_{\mathcal{D}}(c)$) of pairings $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ and that of degenerate bilinear maps $\underline{\mathbf{Degen}}_{\mathcal{D}}(c)$. Thus $\underline{\mathbf{Bil}}_{\mathcal{D}}(c) = \underline{\mathbf{Pair}}_{\mathcal{D}}(c) + \underline{\mathbf{Degen}}_{\mathcal{D}}(c)$ (+ being the set-theoretic disjoint sum). The class $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ may be itself divided into two non-overlapping parts, that of isomorphic classes (in any of $\mathbf{Bil}_{\mathcal{D}}(c)$ or $\mathbf{Pair}_{\mathcal{D}}(c)$ or also $\mathbf{Perf}_{\mathcal{D}}(c)$) of perfect pairings $\underline{\mathbf{Perf}}_{\mathcal{D}}(c)$ and that of non-perfect pairings or "imperfect pairings" $\underline{\mathbf{Imp}}_{\mathcal{D}}(c)$. Thus $\underline{\mathbf{Pair}}_{\mathcal{D}}(c) = \underline{\mathbf{Perf}}_{\mathcal{D}}(c) + \underline{\mathbf{Imp}}_{\mathcal{D}}(c)$. The class $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ of equivalent classes of bilinear maps under the relation of isomorphism in $\mathbf{Bil}_{\mathcal{D}}(c)$ forms a (possibly large) commutative monoid under the operation $\perp$. Theorem 3.4 reads as inclusions of submonoids $\underline{\mathbf{Perf}}_{\mathcal{D}}(c) \subseteq \underline{\mathbf{Pair}}_{\mathcal{D}}(c) \subseteq \underline{\mathbf{Bil}}_{\mathcal{D}}(c)$.

Definition 4.1. The monoid $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ of pairings is referred to as the *moduli space of pairings* (on c).

Let us briefly recall some notions about monoids. A *monoid with a zero* is a monoid M with a distinguished two-sided absorbing element (unique if it exists). A homomorphism between two monoids with a zero is a usual homomorphism of monoids preserving the zeroes. In this way we obtain a (non-full) subcategory of that of monoids. Let M be a monoid. A *congruence* say $\equiv$ of M is an equivalence relation on M such that whenever $x \equiv y$, then for every $a, b \in M$, $axb \equiv ayb$. Of course the quotient $M/\equiv$ of a monoid by such a congruence admits a natural structure of monoid referred to as a *quotient monoid*, and the canonical epimorphism is also a homomorphism of monoids. Let $I \subseteq M$. The set I is said to be a *two-sided ideal* of M if $MI \subseteq I \supseteq IM$. Any two-sided ideal I determines a congruence $\equiv_I$ by stating that $x \equiv_I y$ if, and only if, either $x = y$ or $xy \in I$. The quotient monoid $M/\equiv_I$, called the *Rees quotient* of M by I, and denoted by M/I (see [5]), is isomorphic to the set $(M \setminus I) + \{\infty\}$ equips with the following monoid operation: let $x, y \in M \setminus I$, then $x \cdot y = xy$ whenever $xy \notin I$, and $x \cdot y = \infty$ otherwise, moreover $\infty \cdot x = \infty = x \cdot \infty$ for every $x \in (M \setminus I) + \{\infty\}$, in particular M/I is a monoid with a zero. Of course if $I = \emptyset$, then M/I is isomorphic to the monoid $M^{\infty} = M + \{\infty\}$, *i.e.*, M with a two-sided absorbing element ∞ freely adjoint (the left adjoint to the forgetful functor from monoids with zero to usual monoids). A two-sided ideal I is said to be a *prime ideal* when $I \neq M$ and $xy \in I$ implies that either $x \in I$ or $y \in I$. In this case it is easily checked that $M \setminus I$ is a submonoid of M, and thus $M/I \cong (M \setminus I)^{\infty}$.

It is clear from Theorem 3.4 that $\underline{\mathbf{Degen}}_{\mathcal{D}}(c)$ (respectively, $\underline{\mathbf{Imp}}_{\mathcal{D}}(c)$) is a prime ideal of $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ (respectively, $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$). Thus, $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)/\underline{\mathbf{Degen}}_{\mathcal{D}}(c) \cong \underline{\mathbf{Pair}}_{\mathcal{D}}(c)^{\infty}$, and $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)/\underline{\mathbf{Imp}}_{\mathcal{D}}(c) \cong \underline{\mathbf{Perf}}_{\mathcal{D}}(c)^{\infty}$ (as monoids with zero).

4.2 Finite decomposition and locally finite monoids

Let M be a monoid (with identity element 1). It is said to be a *finite decomposition* monoid (also called *property (D)* in [4], chapter 3) if for every $x \in M$, there are only finitely many $y, z \in M$ such that $x = yz$ (in other terms the multiplication of M has finite fibers). Clearly any finite monoid and any finite group is a finite decomposition monoid. Let R be a commutative ring with a unit, and let A be a commutative R-algebra with a unit. Let us assume that M is a finite decomposition monoid. Then, A^M admits a structure of R-algebra with a unit, called the *large algebra of* M [4] and denoted by $A[[M]]$, with multiplication given by $(fg)(x) = \sum_{yz=x} f(y)g(z)$, called *convolution product*, for $f, g \in A^M$ and $x \in M$.

Example 4.2. The large algebra $\mathbb{C}[[\mathbb{N}^*]]$ is the algebra of Dirichlet's series.

Let X be any set. We may define an obvious presheaf $(-)^X : {}_R\mathbf{CAlg} \to \mathbf{Set}$ which when applied on a commutative algebra A gives A^X, and for any algebra map $\phi\colon A \to B$ associates a set-theoretic map $\phi^X\colon A^X \to B^X$ such that $\phi^X(f)\colon x \in X \mapsto \phi(f(x)) \in B$, for each $f \in A^X$. This is a representable functor with representing object (coordinate ring) the polynomial algebra $R[z_x\colon x \in X]$ in the indeterminates z_x, $x \in X$ (because ${}_R\mathbf{CAlg}(R[z_x\colon x \in X], A) \cong A^X$). Thus $(-)^X$ is an affine scheme (see [7]).

Theorem 4.3. *If M is a finite decomposition monoid, then the affine scheme $(-)^M$ is a monoid scheme.*

Proof. For every commutative algebra A, A^M is more than just a set, it is an algebra $A[[M]]$, and in particular a monoid under convolution product. It is clear that the monoid multiplication $*\colon A[[M]] \times A[[M]] \to A[[M]]$ and the unit $e\colon R \to A[[M]]$ are natural in the algebra A, thus $(-)^M$ is a monoid scheme. □

The monoid scheme from Theorem 4.3 is denoted by $(-)[[M]]$.

Remark 4.4. Actually it may be proved that $(-)[[M]]$ is a ring scheme (see [11]), but its additive structure is inessential in the present work.

Remark 4.5. Theorem 4.3 also immediately implies that the representing object $R[z_x\colon x \in M]$ of the monoid scheme $(-)[[M]]$ admits a structure of a commutative (cocommutative if, and only if, M is commutative) bialgebra over R (by the Yoneda's lemma).

As a consequence of Theorem 4.3: the monoid M is a subset of a geometrico-algebraic object, namely it embeds as a submonoid of R-points $R[[M]]$ of the monoid scheme.

Remark 4.6. In particular when R is an algebraic closed field, then $(-)[[M]]$ is a usual pro-affine algebraic monoid (affine, in case M is finite), and M is a submonoid of the R-rational points of $(-)[[M]]$.

Let $x \in M$, and let $n \in \mathbb{N}$. A *decomposition* of x of *length* n is a n-tuple $(x_1, \cdots, x_n) \in M^n$ such that $x = x_1 \cdots x_n$, and no $x_i = 1$; the set formed by their totality is denoted by $D_n(x)$. A *decomposition* of x is a member of $D_n(x)$ for some integer n. A monoid M is said to be *locally finite* (see [8]) when $x \in M$ admits only finitely many decompositions. It is easy to see that in a locally finite monoid apart from the unit 1 there are no invertible elements. Thus no group (except the trivial one) may be a locally finite monoid. Of course, a locally finite monoid is a finite decomposition monoid, but the converse is false (consider any finite non-trivial group).

Remark 4.7. Let M be a locally finite monoid, and let R be a commutative ring with a unit. For every commutative R-algebra A with a unit, let $\mathfrak{M}_A$ be the augmentation ideal of $A[[M]]$, *i.e.*, the set of all functions $f \in A^M$ vanishing at the identity of M. Let $1 + \mathfrak{M}_A$ be the set of functions with values 1 at the identity of M. Then, it is quite easy to see that $1 + \mathfrak{M}_{(-)}$ (defined in an obvious way) is a group scheme (for convolution product). In particular if R is an algebraic closed field, then $1 + \mathfrak{M}_{(-)}$ is a pro-affine algebraic group. For instance the *zêta function* $\zeta_A \in A^M$, given by $\zeta_A(x) = 1$ for every $x \in M$, is invertible, its inverse being the so-called *Möbius function*, since $\zeta_A \in 1 + \mathfrak{M}_A$ (see [13]), and $\zeta_{\mathbb{C}}$ is the usual Riemann zêta function when $M = \mathbb{N}^*$.

In any locally finite monoid M may be defined the *length function*

$$\ell(x) = \max\{\, n \in \mathbb{N}\colon D_n(x) \neq \emptyset \,\} ,$$

$x \in M$. In particular, $\ell(x) = 0$ if, and only if, $x = 1$. Any element of length 1 is said to be *indecomposable*. It is clear that such indecomposable elements generate the monoid, and any generating set of M contains the indecomposable elements.

For every $x, y \in M$, $\ell(xy) \geq \ell(x) + \ell(y)$. For each integer n, let us define a two-sided ideal $I_n = \{ x \in M : \ell(x) \geq n \}$ of M, and let M_n be the Rees quotient M/I_n of M by I_n. (In particular, $I_0 = M$, and $M_0 = \{ \infty \}$ is the trivial monoid.) For each $i \geq j$, let $\pi_{i,j} : M_i \to M_j$ be a monoid (with zero) homomorphism defined by $\pi_{i,j}(\infty) = \infty$, and for each $x \in M_i \setminus \{ \infty \}$, $\pi_{i,j}(x) = \infty$ if $\ell(x) \geq j$, and $\pi_{i,j}(x) = x$ if $\ell(x) < j$. It is clear that for every $i \geq j \geq k$, $\pi_{i,k} = \pi_{j,k} \circ \pi_{i,j}$ in such a way that we get a projective system of monoids with zero. The following result is easily obtained.

Lemma 4.8. *We have* $\varprojlim_n M_n \cong M^\infty$ *(as monoids with zero).*

4.3 Local finiteness of pairings

Back to the monoid of bilinear maps, let us assume that either[1] (1) $\mathcal{C} = {}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$ and $\mathcal{D} = \mathbf{Abfin}$, or (2) $R \neq (0)$, $\mathcal{C} = {}_R\mathbf{Mod}$ and $\mathcal{D} = {}_R\mathbf{Modfreefin}$, or (3) $\mathcal{C} = \mathbf{CMon}$, and $\mathcal{D} = \mathbf{CMonfin}$. In case (1) (respectively, (3)), let $s(a) = |a| \in \mathbb{N}^*$ be the order of the finite abelian group a (respectively, cardinal number of the finite commutative monoid a), and in case (2), let $s(a) = \mathbf{rank}_R(a) \in \mathbb{N}$ be the rank of the free R-module of finite rank a (well-defined since R is a non-zero commutative ring with a unit). It is clear that for every $(f, (a, b)) \cong (g, (d, e))$ (in $\mathbf{Bil}_{\mathcal{D}}(c)$), $s(a) = s(d)$ and $s(b) = s(e)$. Moreover for each objects a, b of $\mathcal{D}$, $s(a \oplus b) = s(a)s(b)$, and $s(0) = 1$ in case (1) or (3), and $s(a \oplus b) = s(a) + s(b)$, and $s(0) = 0$ in case (2). Let us denote by $[f, (a, b)]$ the equivalence class of a bilinear map on c. Thus the following lemma follows easily.

Lemma 4.9. *The mapping* $\tilde{s}([f, (a, b)]) = (s(a), s(b))$ *is a well-defined homomorphism of monoids from* $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ *(respectively,* $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ *and respectively,* $\underline{\mathbf{Perf}}_{\mathcal{D}}(c)$*) to* $\mathbb{N}^* \times \mathbb{N}^*$ *in case (1) or (3), and to* $\mathbb{N} \times \mathbb{N}$ *in case (2), where both* $\mathbb{N}^* \times \mathbb{N}^*$ *and* $\mathbb{N} \times \mathbb{N}$ *are given the usual structure of product of monoids.*

As an immediate consequence we obtain the following.

Corollary 4.10. *In any cases (1) or (2) or (3),* $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$*,* $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ *and* $\underline{\mathbf{Perf}}_{\mathcal{D}}(c)$ *are locally finite monoids.*

In cases (1) or (2) or (3), according to Corollary 4.10 and to results from Subsection 4.2, the moduli space of pairings $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ is really a geometrico-algebraic object as a submonoid of the monoid $S[[\underline{\mathbf{Pair}}_{\mathcal{D}}(c)]]$ of S-points (for the convolution product) of the monoid scheme $(-)[[\underline{\mathbf{Pair}}_{\mathcal{D}}(c)]]$, for any commutative ring

[1] In the two first cases, it is easy to see that we can choose a small set of representatives of each class in $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ and thus it is a small monoid.

S with a unit. In particular, if S is an algebraic closed field $\mathbb{K}$, then the moduli space of pairings $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ is a submonoid of $\mathbb{K}$-rational points of the (pro-)affine algebraic monoid $(-)[[\underline{\mathbf{Pair}}_{\mathcal{D}}(c)]]$.

It also follows from Corollary 4.10 and by Lemma 4.8 that in any cases (1) or (2) or (3), $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)/\underline{\mathbf{Degen}}_{\mathcal{D}}(c) \cong \underline{\mathbf{Pair}}_{\mathcal{D}}(c)^{\infty} \cong \varprojlim_n \underline{\mathbf{Pair}}_{\mathcal{D}}(c)/I_n$, and also $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)/\underline{\mathbf{Imp}}_{\mathcal{D}}(c) \cong \underline{\mathbf{Perf}}_{\mathcal{D}}(c)^{\infty} \cong \varprojlim_n \underline{\mathbf{Perf}}_{\mathcal{D}}/I_n$ (as monoids with zero), where I_n is defined as in Subsection 4.2 (as an ideal of $\underline{\mathbf{Bil}}_{\mathcal{D}}(c)$ and of $\underline{\mathbf{Pair}}_{\mathcal{D}}(c)$ respectively).

5 Classification of pairings on $\mathbb{R}/\mathbb{Z}$

Unless stated the contrary, we assume that $\mathcal{C} = \mathbf{Ab}$, $c = \mathbb{R}/\mathbb{Z}$, and $\mathcal{D} = \mathbf{Abfin}$. Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{R}/\mathbb{Z})$ its *dual group*. It is well-known that $a \cong \widehat{a}$ (as finite abelian groups) but the isomorphism is not natural (it depends on a decomposition of a into a product of cyclic sugroups). Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$. By definition, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$ since γ_f and δ_f are abelian group monomorphisms. This implies that $a \cong b$, and that actually γ_f and δ_f are isomorphisms. Thus, $(f, (a, b))$ is a perfect pairing, and the following lemma is proved.

Lemma 5.1. $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z}) = \mathbf{Perf}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$.

Remark 5.2. Let a, b be two finite abelian groups, and let n be a positive integer. Let $(f, (a, b))$ be a pairing on $\mathbb{Z}/n\mathbb{Z}$. Then, it may be identified with a pairing on $\mathbb{R}/\mathbb{Z}$ (since we know from Subsection 2.3 that $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Z}/n\mathbb{Z})$ is a full subcategory of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$), and thus $a \cong b$, and f is a perfect pairing. Moreover, because the torsion in finite abelian groups, $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z}) \cong \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$ (as categories), and since $\mathbb{C}^* \cong \mathbb{R}/\mathbb{Z}$, $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{C}^*) \cong \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$.

Remark 5.3. Lemma 5.1 is false in general if c is not equal to $\mathbb{R}/\mathbb{Z}$. Indeed, let p be any prime number, and let $n \geq 1$ be an integer. Then the bilinear map $f\colon (\mathbb{Z}/p\mathbb{Z})^n \times \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^n$ given by $f((x_i \pmod p)_{i=1}^n, y \pmod p) = (x_i y \pmod p)_{i=1}^n$ is an imperfect pairing for each $n > 1$. Even if $a \cong b$, Lemma 5.1 is false in general: let $m \geq 1$ and $n > 1$ be two integers, then the bilinear map $g\colon (\mathbb{Z}/n\mathbb{Z})^m \times (\mathbb{Z}/n\mathbb{Z})^m \to (\mathbb{Z}/n\mathbb{Z})^{m^2}$ defined by $g((x_i)_{i=1}^m \pmod n), (y_i)_{i=1}^m \pmod n)) = (x_i y_j \pmod n))_{i,j=1}^m$ is an imperfect pairing for all $m > 1$ (it is not perfect because $\mathbf{Abfin}((\mathbb{Z}/n\mathbb{Z})^m, (\mathbb{Z}/n\mathbb{Z})^{m^2}) \cong (\mathbb{Z}/n\mathbb{Z})^{m^3}$).

Definition 5.4. Let a be a finite abelian group. The *natural pairing* on a is $(\mathbf{nat}_a, (a, \hat{a}))$ where $\mathbf{nat}_a\colon a \otimes \hat{a} \to \mathbb{R}/\mathbb{Z}$ is defined by $\mathbf{nat}_a(x \otimes \chi) = \chi(x)$, $x \in a$, $\chi \in \hat{a}$. (The fact that $(\mathbf{nat}_a, (a, \hat{a}))$ is a pairing essentially follows from Pontryagin duality for finite abelian groups.)

Remark 5.5. For any finite abelian groups a, b, $a \cong b$ (as groups) if, and only if, $(\mathbf{nat}_a, (a, \hat{a})) \cong (\mathbf{nat}_b, (b, \hat{b}))$. It is of course a sufficient condition. It is also necessary: let $\alpha\colon a \to b$ be an isomorphism, and let us define $\beta\colon \hat{a} \to \hat{b}$ by $\beta(\chi) = \chi \circ \alpha^{-1}$. Of course, β is an isomorphism too. Then, $\mathbf{nat}_b(\alpha(x) \otimes \beta(\chi)) = \beta(\chi)(\alpha(x)) = \chi(x) = \mathbf{nat}_a(x \otimes \chi)$, $x \in a$, $\chi \in \hat{a}$.

Theorem 5.6. *Let $(f, (a, b))$ be a pairing on $\mathbb{R}/\mathbb{Z}$. Then,*

$$(f, (a, b)) \cong (\mathbf{nat}_a, (a, \hat{a}))\ .$$

Proof. Since $a \cong b$, let us choose an isomorphism $\alpha\colon b \to a$. Let us define a bilinear map $g_0\colon a \times a \to \mathbb{R}/\mathbb{Z}$ by $g_0(x, y) = f_0(x, \alpha^{-1}(y))$, $x, y \in a$, where $f_0\colon a \times b \to \mathbb{R}/\mathbb{Z}$ is the bilinear map associated to f. It is clear that $(g, (a, a)) \cong (f, (a, b))$ (as bilinear maps) where $g\colon a \otimes a \to \mathbb{R}/\mathbb{Z}$ is the unique group morphism such that $g(x \otimes y) = g_0(x, y)$. By Lemma 2.6, $(g, (a, a))$ and $(f, (a, b))$ are isomorphic as perfect pairings. Thus, $\delta_g\colon a \to \hat{a}$ is an isomorphism, and for $h = g \circ (id_a \otimes \delta_g^{-1})$ we have $(h, (a, \hat{a})) \cong (g, (a, a))$. Moreover, $h(x \otimes \chi) = g(x \otimes \delta_g^{-1}(\chi)) = \delta_g(\delta_g^{-1}(\chi))(x) = \chi(x) = \mathbf{nat}_a(x \otimes \chi)$ for all $x \in a$, $\chi \in \hat{a}$. □

As an immediate consequence of Theorem 5.6, equivalence classes of pairings on $\mathbb{R}/\mathbb{Z}$ and equivalence classes of finite abelian groups are in one-one correspondence since, according to Remark 5.5, for any finite abelian groups a, d, $a \cong d$ (as groups) if, and only if, $(\mathbf{nat}_a, (a, \hat{a})) \cong (\mathbf{nat}_d, (d, \hat{d}))$, and for any pairings $(f, (a, b))$ and $(g, (d, e))$, $(f, (a, b)) \cong (\mathbf{nat}_a, (a, \hat{a})) \cong (\mathbf{nat}_d, (d, \hat{d})) \cong (g, (d, e))$ if, and only if, $a \cong d$.

Because for any finite abelian groups a, b, $\mathbf{Ab}(a \oplus b, \mathbb{R}/\mathbb{Z}) \cong \mathbf{Ab}(a, \mathbb{R}/\mathbb{Z}) \oplus \mathbf{Ab}(b, \mathbb{R}/\mathbb{Z})$ (as finite abelian groups), $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$. Therefore, $(\mathbf{nat}_{a \oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a})) \perp (\mathbf{nat}_b, (b, \hat{b}))$. This implies that any indecomposable pairing is isomorphic to some $(\mathbf{nat}_{\mathbb{Z}/p^i\mathbb{Z}}, (\mathbb{Z}/p^i\mathbb{Z}, \widehat{\mathbb{Z}/p^i\mathbb{Z}}))$, p prime, and $i > 0$ an integer, and for distinct (p, i)'s, they are pairwise non-isomorphic. According to the structure theorem for finite abelian groups, we conclude as follows.

Theorem 5.7. *The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z}) (= \underline{\mathbf{Perf}}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z}))$ is isomorphic to the commutative monoid $\bigoplus_{p \in \mathbb{P}} M_p$, where $\mathbb{P}$ is the set of all prime numbers, and M_p is the free commutative monoid generated by the symbols (p, i), $i \in \mathbb{N}^*$.*

According to Theorem 5.7, $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$ is the commutative monoid freely generated by the isomorphic classes $[(\mathbf{nat}_{\mathbb{Z}/p^i\mathbb{Z}}, (\mathbb{Z}/p^i\mathbb{Z}, \widehat{\mathbb{Z}/p^i\mathbb{Z}}))]$, p prime, and $i > 0$, of indecomposable pairings.

Let p be a prime number, and let $\mathbb{Z}(p^\infty)$ be the Prüfer p-group (see [1]), *i.e.*, the direct limit of $0 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \cdots$ Certainly, $\mathbb{Z}(p^\infty)$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$. Let ${}_p\mathbf{Abfin}$ be the category of finite abelian p-groups. Thus, $\mathbf{Pair}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty)) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Z}(p^\infty)) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ (full embeddings of categories). Therefore, any object $(f, (a, b))$ of $\mathbf{Pair}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty))$ is a perfect pairing, and $a \cong b$. It is easily seen that $\underline{\mathbf{Pair}}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty))$ is the free commutative monoid generated by the symbols (p, i), $i \in \mathbb{N}^*$. Thus the following result is proved.

Corollary 5.8. *The moduli space of pairings* $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{R}/\mathbb{Z})$ *is isomorphic to the commutative monoid* $\bigoplus_{p\in\mathbb{P}} \underline{\mathbf{Pair}}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty))$.

Remark 5.9. Our classification is much simpler than Wall's [16] for essentially the reason that we deal with a (category-theoretic) isomorphism relation within which too many objects are identified. Actually it is even strictly coarser than the usual equivalence relation of bilinear maps. First we observe that for any abelian group without 2-torsion c, no two non-trivial (*i.e.*, $\neq 0$) bilinear maps $f, g\colon a \times a \to c$, f symmetric and g skew-symmetric, may be equivalent in the ordinary sense (for if there is an isomorphism $\alpha\colon a \to a$ such that $f(x, y) = g(\alpha(x), \alpha(y))$, then $g(\alpha(y), \alpha(x)) = f(y, x) = f(x, y) = g(\alpha(x), \alpha(y)) = -g(\alpha(y), \alpha(x))$). Moreover, let $m > 2$ be an odd integer, and let us consider two pairings f, g from $(\mathbb{Z}/m\mathbb{Z})^2 \times (\mathbb{Z}/m\mathbb{Z})^2$ to $\mathbb{Z}/m\mathbb{Z}$ defined respectively by $f((x_1, x_2), (x_3, x_4)) = x_1x_4 + x_2x_3$, and $g((x_1, x_2), (x_3, x_4)) = x_1x_4 - x_2x_3$. We observe that f is symmetric while g is skew-symmetric. Thus these two bilinear maps are non classically equivalent but they are isomorphic in $\mathbf{Bil}_{\mathbf{Abfin}}(\mathbb{Z}/m\mathbb{Z})$ (take $\alpha = id$, and $\beta(x, y) = (-x, y)$ so that $f((x_1, x_2), (x_3, x_4)) = g(\alpha(x_1, x_2), \beta(x_3, x_4))$).

6 Classification of pairings on R

We assume that R is a non-zero commutative ring with a unit, $\mathcal{C} = {}_R\mathbf{Mod}$, $c = R$, and $\mathcal{D} = {}_R\mathbf{Modfreefin}$. Let a be a free R-module of finite rank, and let us denote by $a^\star = {}_R\mathbf{Mod}(a, R)$ its *dual module*.

Remark 6.1. The classification of pairings, up to isomorphism, defined on free modules of finite ranks and with values on the base ring R is more simple than that reported in Section 5. The results and proofs are similar to that from Section 5, and thus they are stated here without proof. The content of this section parallels that from Section 5.

It is clear that $a \cong a^\star$ (as modules) but the isomorphism is not natural (it depends on a free basis of a). Let $(f,(a,b))$ be an object of $\mathbf{Pair}_{{}_R\mathbf{Modfreefin}}(R)$. By definition, $a \hookrightarrow b^\star \cong b \hookrightarrow a^\star \cong a$ since γ_f and δ_f are module monomorphisms. This implies that $a \cong b$, and that actually γ_f and δ_f are isomorphisms. Thus, $(f,(a,b))$ is a perfect pairing, and the following lemma is proved.

Lemma 6.2. $\mathbf{Pair}_{{}_R\mathbf{Modfreefin}}(R) = \mathbf{Perf}_{{}_R\mathbf{Modfreefin}}(R)$.

Definition 6.3. Let a be a free R-module of finite rank. The *natural pairing* on a is $(\mathbf{nat}_a,(a,a^\star))$ where $\mathbf{nat}_a\colon a \otimes_R a^\star \to R$ is defined by $\mathbf{nat}_a(x \otimes \ell) = \ell(x)$, $x \in a$, $\ell \in a^\star$. (The fact that $(\mathbf{nat}_a,(a,a^\star))$ is a pairing essentially follows from the existence of a finite basis for a so that $a \cong a^{\star\star}$.)

Remark 6.4. For any free modules a, b of finite rank, $a \cong b$ (as modules) if, and only if, $(\mathbf{nat}_a,(a,a^\star)) \cong (\mathbf{nat}_b,(b,b^\star))$.

Theorem 6.5. *Let $(f,(a,b))$ be a pairing on R. Then,*

$$(f,(a,b)) \cong (\mathbf{nat}_a,(a,a^\star)) \;.$$

As an immediate consequence of Theorem 6.5, equivalence classes of pairings on R and equivalence classes of free R-modules of finite rank are in one-one correspondence since, according to Remark 6.4, for any free R-modules of finite rank a, d, $a \cong d$ (as modules) if, and only if, $(\mathbf{nat}_a,(a,a^\star)) \cong (\mathbf{nat}_d,(d,d^\star))$, and for any pairings $(f,(a,b))$ and $(g,(d,e))$, $(f,(a,b)) \cong (\mathbf{nat}_a,(a,a^\star)) \cong (\mathbf{nat}_d,(d,d^\star)) \cong (g,(d,e))$ if, and only if, $a \cong d$.

Because for any R-modules a, b, ${}_R\mathbf{Mod}(a \oplus b, R) \cong {}_R\mathbf{Mod}(a,R) \oplus {}_R\mathbf{Mod}(b,R)$ (as modules), $(a \oplus b)^\star \cong a^\star \oplus b^\star$. Therefore, we clearly have $(\mathbf{nat}_{a\oplus b},(a \oplus b,(a \oplus b)^\star)) \cong (\mathbf{nat}_a,(a,a^\star)) \perp (\mathbf{nat}_b,(b,b^\star))$. This implies that there is a unique indecomposable pairing, namely $(\mathbf{nat}_R,(R,R^\star))$. We conclude as follows.

Theorem 6.6. *The moduli space of pairings $\underline{\mathbf{Pair}}_{{}_R\mathbf{Modfreefin}}(R)$ (which is equal to $\underline{\mathbf{Perf}}_{{}_R\mathbf{Modfreefin}}(R)$) is isomorphic to $\mathbb{N}$.*

Bibliography

[1] D.L. Armacost, W. L. Armacost, *On p-thetic groups*, Pacific Journal of Mathematics **41**(2) (1972), 295–301.

[2] F. Borceux, “Handbook of categorical algebra 1, basis category theory,” volume 50 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1994.

[3] F. Borceux, “Handbook of categorical algebra 2, categories and structures,” volume 51 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1994.

[4] N. Bourbaki, “Elements of Mathematics, Algebra 1, chapters 1–3,” Springer, 1998.

[5] A.H. Clifford and G.B. Preston, “The Algebraic Theory of Semigroups, Volume I,” volume 7 of Mathematical Surveys and Monographs, American Mathematical Society, 1961.

[6] F. Deloup, *Monoïde des enlacements et facteurs orthogonaux*, Algebraic and Geometric Topology **5** (2005), 419–442.

[7] M. Demazure and P. Gabriel, “Introduction to algebraic geometry and algebraic groups,” volume 39 of North-Holland Mathematical Studies, North-Holland Publishing Company, 1980.

[8] S. Eilenberg, “Automata, languages, and machines, volume A,” volume 59 of Pure and Applied Mathematics, Academic Press, 1974.

[9] T.F. Fox, *The tensor product of Hopf algebras*, Rendiconti dell’Instituto di Matematica dell’Università di Trieste **24** (1992), 65–71.

[10] P. Gabriel, *Appendix: Degenerate bilinear forms*, Journal of Algebra **31** (1974), 67–72.

[11] M.J. Greenberg, *Algebraic rings*, Transactions of the American Mathematical Society **111**(3) (1964), 472–481.

[12] S. Mac Lane, “Categories for the working mathematician,” volume 5 of Graduate Texts in Mathematics, Springer-Verlag, 1971.

[13] L. Poinsot, G.H.E. Duchamp and C. Tollu, *Möbius inversion formula for monoids with zero*, Semigroup Forum **81** (2010), 446–460.

[14] C. Riehm, *The equivalence of bilinear forms*, Journal of Algebra **31** (1974), 45–66.

[15] J.H. Silverman, “The arithmetic of elliptic curves,” (2nd edition) volume 106 of Graduate Texts in Mathematics, Springer-Verlag, 2009.

[16] C.T.C Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1964), 281–298.

[17] J. Williamson, *On the algebraic problem concerning the normal forms of a linear dynamical system*, American Journal of Mathematics **58** (1936), 141–163.

Received **???**.

Author information

Laurent Poinsot, University Paris 13, Sorbonne Paris Cité, LIPN, CNRS (UMR 7030), 99 av. J.-B. Clément, 93430 Villetaneuse, France.
E-mail: laurent.poinsot@lipn.univ-paris13.fr

Nadia El Mrabet, University Paris 8, 2 rue de la Liberté, 93526 Saint-Denis, France.
E-mail: elmrabet@ai.univ-paris8.fr