# Moduli space of pairings on complex roots of unity

Laurent Poinsot

LIPN - UMR CNRS 7030
Université Paris XIII, Sorbonne Paris Cité - Institut Galilée

Joint-work with Nadia El Mrabet - Université Paris 8

14th International Conference on Arithmetic, Geometry, Cryptography and Coding Theory
Marseille

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Pairings

Let $A, B, C$ be three modules over some commutative ring $R$ with a unit.

A pairing is a non-degenerate bilinear map $f\colon A \times B \to C$.

Non-degeneracy means that $\gamma_f\colon a \in A \mapsto f(a, \textvisiblespace)$ and $\delta_f\colon b \in B \mapsto f(\textvisiblespace, b)$ are both one-to-one.

# Examples

• Let $1 \to A \to G \to B \to 1$ be a short exact sequence of groups, where $A, B$ are Abelian, and $A$ lies in $Z(G)$. The commutator $[\cdot, \cdot]$ of $G$ factors to a bilinear map $[\cdot, \cdot]\colon B \times B \to A$ which is non-degenerate if, and only if, $A = Z(G)$ (R. Baer, 1938).

• Let $\langle \cdot \mid \cdot \rangle\colon A \times \widehat{A} \to \mathbb{R}/\mathbb{Z}$ defined by $\langle a \mid \chi \rangle = \chi(a)$.

• Weil, Tate pairings and their recent generalizations to Abelian varieties.

• Let $R$ be any field, and $X$ be any set. Let us denote by $\mathbb{K}^{(X)}$ the vector space of finitely supported maps (*i.e.*, the vector space with basis $X$). Let $\langle \cdot \mid \cdot \rangle\colon \mathbb{K}^X \times \mathbb{K}^{(X)} \to \mathbb{K}$ be given by $\langle f \mid g \rangle = \sum_{x \in X} f(x)g(x)$ is a pairing.

# Cryptographic applications

- MOV attack to solve discrete logarithm problem by transport from an elliptic curve to a finite field.
- A. Joux's one-round key exchange tri-partite Diffie-Hellman protocol.
- Identity-based cryptography.

# Objective of this talk

• Provide a classification of pairings – under a suitable equivalence relation – from finite Abelian groups to the complex unit circle.

• Show that the set of equivalence classes of pairings is almost a moduli space: it is actually a subset of rational points of some (pro-)affine algebraic variety.

Warning: The classification from this talk is of course different from C.T.C Wall's classification of skew or symmetric non-singular bilinear forms on finite Abelian groups (1964) because the equivalence relations under consideration are not the same. My equivalence relation is of categorical origin since it is the relation of isomorphism in a suitable category.

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Notations

Let $\mathcal{C}$ be a category.

The class of objects of $\mathcal{C}$ is denoted by $\mathcal{Ob}(\mathcal{C})$.

Let $A, B$ be objects of $\mathcal{C}$. The class of arrows from $A$ to $B$ is denoted by $\mathcal{C}(A, B)$. Of course, $f \in \mathcal{C}(A, B)$ is also denoted by $f\colon A \to B$.

# Names of categories

- Let $\mathcal{C}$ be a category.

- $\mathcal{C}_{mono}$ is the subcategory of $\mathcal{C}$ consisting of the objects of $\mathcal{C}$ and with arrows the monomorphisms (left cancellable arrows).

- $\mathcal{C}_{iso}$ is the core of $\mathcal{C}$, *i.e.*, the groupoid with objects those of $\mathcal{C}$, and arrows the isomorphisms in $\mathcal{C}$.

- More generally, if $S$ is a class of arrows containing for each object its identity morphism, and closed under composition, then $\mathcal{C}_S$ is the subcategory of $\mathcal{C}$ defined in the obvious way.

- Usual categories of sets $\mathcal{Set}$, $\mathcal{Ab}$ and $\mathcal{Ab}_{fin}$ of Abelian and finite Abelian groups.

- Let $R$ be a commutative ring with a unit ($R \neq 0$). Let $R$-$\mathcal{Mod}$ be the category of $R$-modules, and let $R$-$\mathcal{Free}_{fin}$ be its full subcategory of free $R$-modules of finite rank.

- Finally, $R$-$\mathcal{CAlg}$ denotes the category of commutative $R$-algebras with a unit.

# Monoidal category

A monoidal category is a category $\mathcal{C}$ with a bifunctor $\otimes\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, an object $I$, and three natural isomorphisms

- $\alpha\colon \textvisiblespace \otimes (\textvisiblespace \otimes \textvisiblespace) \cong (\textvisiblespace \otimes \textvisiblespace) \otimes \textvisiblespace$ (associativity constraint or associator),
- $\lambda\colon I \otimes \textvisiblespace \cong id_{\mathcal{C}}$ (left unit),
- $\rho\colon \textvisiblespace \otimes I \cong id_{\mathcal{C}}$ (right unit).

that satisfy some coherence axioms.

# Coherence for associativity

## Mac Lane - Stasheff's Pentagon

For all $A, B, C, D \in \mathcal{Ob}(\mathcal{C})$, the following diagram commutes.

$$\begin{tikzcd}
 & A \otimes (B \otimes (C \otimes D)) \arrow[dl, "id_A \otimes \alpha_{B,C,D}"'] \arrow[dr, "\alpha_{A,B,(C \otimes D)}"] & \\
A \otimes ((B \otimes C) \otimes D) \arrow[d, "\alpha_{A,(B \otimes C),D}"'] & & (A \otimes B) \otimes (C \otimes D) \arrow[d, "\alpha_{(A \otimes B),C,D}"] \\
(A \otimes (B \otimes C)) \otimes D \arrow[rr, "\alpha_{A,B,C} \otimes id_D"'] & & ((A \otimes B) \otimes C) \otimes D
\end{tikzcd}$$

# Coherence for units

For all $A, B \in \mathcal{O}b(\mathcal{C})$, the following diagram commutes.

$$\begin{tikzcd}
A \otimes (I \otimes B) \arrow[rr, "\alpha_{A,I,B}"] \arrow[dr, "id_A \otimes \lambda_B"'] & & (A \otimes I) \otimes B \arrow[dl, "\rho_A \otimes id_B"] \\
& A \otimes B &
\end{tikzcd}$$

# Symmetric monoidal category

Let $(\mathcal{C}, \otimes, I, \alpha, \lambda, \rho)$ be a monoidal category. A braiding is a natural isomorphism $\sigma \colon \textvisiblespace \otimes \textvisiblespace \cong (\textvisiblespace \otimes \textvisiblespace) \circ \tau$ where $\tau \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C} \times \mathcal{C}$ is the usual flip $\tau(A, B) = (B, A)$ such that $\sigma_{B,A} \circ \sigma_{A,B} = id_{A \otimes B}$ and $\rho_A = \lambda_A \circ \gamma_{A,I}$ for every objects $A, B$.

A symmetric monoidal category is a monoidal category with a coherent braiding, *i.e.*, for all $A, B, C \in \mathcal{O}b(C)$ the following diagram commutes.

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "id_A \otimes \sigma_{B,C}"'] & (A \otimes B) \otimes C \arrow[r, "\sigma_{(A \otimes B),C}"] & C \otimes (A \otimes B) \arrow[d, "\alpha_{C,A,B}"] \\
A \otimes (C \otimes B) \arrow[r, "\alpha_{A,C,B}"'] & (A \otimes C) \otimes B \arrow[r, "\sigma_{A,C} \otimes id_B"'] & (C \otimes A) \otimes B
\end{tikzcd}$$

# Monoidal closed category

A closed category is a symmetric monoidal category $\mathcal{C}$ in which for each object $B$ the functor $\sqcup \otimes B \colon \mathcal{C} \to \mathcal{C}$ has a specified right adjoint $(\sqcup)^B \colon \mathcal{C} \to \mathcal{C}$ (which is referred to as the internal hom functor or exponential), *i.e.*, for every objects $A, C$, there is a natural isomorphism (in the category of sets)

$$\mathit{Curry}_{A,B,C} \colon \mathcal{C}(A \otimes B, C) \cong \mathcal{C}(A, C^B) \ .$$

Examples: every Cartesian closed category ($\mathcal{S}et$, Kelley spaces, category of all small categories, ...), $\mathcal{A}b$, $\mathcal{A}b_{fin}$, $R$-$\mathcal{M}od$, $R$-$\mathcal{F}ree_{fin}$, commutative Hopf algebras, ...

# Notations concerning coproducts

Let $\mathcal{C}$ be a category with a binary coproduct $\oplus$. In what follows, for every objects $A, B$ of $\mathcal{C}$, $q_A \colon A \to A \oplus B$, $q_B \colon B \to A \oplus B$ denote the natural injections (while they are not required to be injective!).

Let $\alpha \in \mathcal{C}(A, A')$ and $\beta \in \mathcal{C}(B, B')$. Then, $[\alpha, \beta] \in \mathcal{C}(A \oplus B, A' \oplus B')$ denotes the unique arrow $\gamma$ such that $\gamma \circ q_A = q_{A'} \circ \alpha$ and $\gamma \circ q_B = q_{B'} \circ \beta$.

# Slice category

Let $\mathcal{B}, \mathcal{C}$ be 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 $F/C$ over $C$ has

- objects all pairs $(f, A)$ where $A \in \mathcal{O}b(\mathcal{B})$ and $f \in \mathcal{C}(F(A), C)$,

- for each $f \in \mathcal{C}(F(A), C)$ and $g \in \mathcal{C}(F(B), C)$, an arrow $\alpha\colon f \to g$ is a member of $\mathcal{B}(A, B)$ such that the following diagram commutes.

$$\begin{tikzcd}
F(A) \arrow[rr, "F(\alpha)"] \arrow[dr, "f"'] & & F(B) \arrow[dl, "g"] \\
& C &
\end{tikzcd}$$

# Table of contents

1 Introduction

2 Category theoretic definitions and notations

3 Categories of bilinear maps

4 Pairings as a Rees quotient

5 Length of a pairing and local finiteness

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

# The category of bilinear maps

Let us assume that $\mathcal{C}$ is a closed category, and let $\mathcal{D}$ be a full subcategory of $\mathcal{C}$ (it may be $\mathcal{C}$ itself). (These data will be implicitly assumed.)

Let $C$ be a given objects of $\mathcal{C}$. The category of bilinear maps on $C$ is the full subcategory $\mathcal{B}il_{\mathcal{D}}(C)$ of the slice category $\otimes/C$. Objects: $(f,(A,B))$, $A, B$ objects of $\mathcal{D}$ and $f \in \mathcal{C}(A \otimes B, C)$. (It is equivalently defined as the slice category $\otimes \circ (j_{\mathcal{D}} \times j_{\mathcal{D}})$, where $j_{\mathcal{D}} \colon \mathcal{D} \hookrightarrow \mathcal{C}$ is the full inclusion functor.)

In what follows if $(f,(A,B))$ is such an object, then it is identified with $f$ itself and I use the following notations: $L_f = A$ and $R_f = B$.

Thus an arrow $\alpha$ in $\mathcal{B}il_{\mathcal{D}}(C)$ from $f \in \mathcal{C}(L_f \otimes R_f, C)$ to $g \in \mathcal{C}(L_g \otimes R_g, C)$, $L_f, R_f, L_g, R_g$ objects of $\mathcal{D}$, *i.e.*, $\alpha \in \mathcal{B}il_{\mathcal{D}}(C)(f,g)$, is a pair $(\alpha_l, \alpha_r)$ with $\alpha_l \in \mathcal{D}(L_f, L_g)$, and $\alpha_r \in \mathcal{D}(R_f, R_g)$ such that the following diagram commutes.

$$\begin{tikzcd}
L_f \otimes R_f \arrow[rr, "\alpha_l \otimes \alpha_r"] \arrow[dr, "f"'] & & L_g \otimes R_g \arrow[dl, "g"] \\
& C &
\end{tikzcd}$$

# Currying

Since $\mathcal{C}$ is assumed closed, for each $f \in \mathcal{C}(L_f \otimes R_f, C)$, we may define its adjoint $\gamma_f \in \mathcal{C}(L_f, C^{R_f})$ as $\mathcal{C}urry_{L_f, R_f, C}(f)$.

Because $\mathcal{C}$ is assumed to be symmetric with braiding say $\sigma$, we may define another adjoint $\delta_f \in \mathcal{C}(R_f, C^{L_f})$ as $\mathcal{C}urry_{R_f, L_f, C}(\sigma_{L_f, R_f}(f))$.

# Category of pairings on $C$

A pairing on $C$ is a bilinear map $f \in \mathcal{C}(A \otimes B, C)$ such that both arrows $\gamma_f$ and $\beta_f$ are monomorphisms in $\mathcal{C}$.

This is the translation of non-degeneracy in this setting.

The category of pairings on $C$ is the full subcategory $\mathcal{Pair}_{\mathcal{D}}(\mathcal{C})$ of $\mathcal{Bil}_{\mathcal{D}}(C)$ with objects all the pairings on $C$.

# Perfect pairing

A pairing $f$ on $C$ is said to be perfect whenever $\gamma_f$ and $\delta_f$ are actually isomorphisms in $\mathcal{C}$.

The category of perfect pairings on $C$ is the full subcategory $\mathscr{Perf}_{\mathcal{D}}(\mathcal{C})$ of $\mathscr{Pair}_{\mathcal{D}}(\mathcal{C})$ (and obviously also of $\mathscr{Bil}_{\mathcal{D}}(C)$) with objects all the perfect pairings on $C$.

In brief: $\mathscr{Perf}_{\mathcal{D}}(C) \hookrightarrow \mathscr{Pair}_{\mathcal{D}}(C) \hookrightarrow \mathscr{Bil}_{\mathcal{D}}(C) \hookrightarrow \otimes/C$ (where the arrows denote the full inclusion functors).

# Isomorphisms in these categories

Let $f, g$ be two objects of $\mathcal{Bil}_{\mathcal{D}}(C)$, and let $\alpha = (\alpha_l, \alpha_r)\colon f \to g$ be an arrow.

The arrow $\alpha \in \mathcal{Bil}_{\mathcal{D}}(C)_{iso}(f, g)$ (respectively, $\mathcal{Bil}_{\mathcal{D}}(C)_{mono}(f, g)$) if, and only if, $\alpha_l \in \mathcal{D}_{iso}(L_f, L_g)$ (resp., $\mathcal{D}_{mono}(L_f, L_g)$) and $\alpha_r \in \mathcal{D}_{iso}(R_f, R_g)$ (resp., $\mathcal{D}_{mono}(R_f, R_g)$).

Because $\mathcal{Perf}_{\mathcal{D}}(C)$ and $\mathcal{Pair}_{\mathcal{D}}(C)$ are full subcategories of $\mathcal{Bil}_{\mathcal{D}}(C)$, their isomorphisms are the same as those of $\mathcal{Bil}_{\mathcal{D}}(C)$.

## Remark

Let $f, g \in \mathcal{Ob}(\mathcal{Bil}_{\mathcal{D}}(C))$ such that $f \cong g$ (as bilinear maps). We observe that $f$ is a pairing (respectively, a perfect pairing) if, and only if, $g$ also is.

Similarly, let us assume that $f, g \in \mathcal{Ob}(\mathcal{Pair}_{\mathcal{D}}(C))$. Then, $f$ is a perfect pairing if, and only if, $g$ is so.

Therefore, an equivalence class (under isomorphism) of bilinear maps (respectively, pairings) either contains no pairings (respectively, perfect pairings) or all its members are pairings (respectively, perfect pairings).

# Remarks

Let us denote by $\mathcal{Cat}$ the category of all (large) categories.

We may define a functor $\mathcal{Bil}_{\mathcal{D}}(\textvisiblespace)\colon \mathcal{C} \to \mathcal{Cat}$ as follows.

Let $C, C'$ be two objects of $\mathcal{C}$ and let $\phi \in \mathcal{C}(C, C')$. Then, $\mathcal{Bil}_{\mathcal{D}}(\phi)\colon \mathcal{Bil}_{\mathcal{D}}(C) \to \mathcal{Bil}_{\mathcal{D}}(C')$ is the functor defined for an object $f \in \mathcal{C}(L_f \otimes R_f, C)$ by $\mathcal{Bil}_{\mathcal{D}}(\phi)(f) = \phi \circ f \in \mathcal{C}(A \otimes B, C')$ and which acts as the identity on arrows.

By restriction, we may define two other functors:

- $\mathcal{Pair}_{\mathcal{D}}(\textvisiblespace)\colon \mathcal{C}_{mono} \to \mathcal{Cat}_{full\,emb}$ (where "*full emb*" stands for "full embedding", *i.e.*, a particular class of functorial monomorphisms: full functors, injective on arrows). So for every monomorphism $\phi \in \mathcal{C}(C, C')$, $\mathcal{Pair}_{\mathcal{D}}(C)$ may be seen as a full subcategory of $\mathcal{Pair}_{\mathcal{D}}(C')$.
- $\mathcal{Perf}_{\mathcal{D}}(\textvisiblespace)\colon \mathcal{C}_{iso} \to \mathcal{Cat}_{iso}$.

By definition of functors, if $C \cong C'$ (isomorphic objects in $\mathcal{C}$), then $\mathcal{Bil}_{\mathcal{D}}(C) \cong \mathcal{Bil}_{\mathcal{D}}(C')$ and $\mathcal{Pair}_{\mathcal{D}}(C) \cong \mathcal{Pair}_{\mathcal{D}}(C')$ (isomorphic categories). The converse may be false ($\mathcal{C} = \mathcal{Ab}$, $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(0) \cong \mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{Z})$).

# Remark

Let us assume that $\mathcal{E} \hookrightarrow \mathcal{D} \hookrightarrow \mathcal{C} = R\text{-}\mathscr{Mod}$ are full embeddings of categories (*i.e.*, $\mathcal{E}$ is a full subcategory of $\mathcal{D}$ which a full subcategory of $\mathcal{C}$).

We have the following commutative diagram of full inclusions for every $C \in \mathcal{O}b(\mathcal{C})$.

$$\begin{tikzcd}
\mathscr{Perf}_{\mathcal{D}}(C) \arrow[r, hook] & \mathscr{Pair}_{\mathcal{D}}(C) \arrow[r, hook] & \mathscr{Bil}_{\mathcal{D}}(C) \\
\mathscr{Perf}_{\mathcal{E}}(C) \arrow[r, hook] \arrow[u, hook] & \mathscr{Pair}_{\mathcal{E}}(C) \arrow[r, hook] \arrow[u, hook] & \mathscr{Bil}_{\mathcal{E}}(C) \arrow[u, hook]
\end{tikzcd}$$

# Adjoints related to perfect pairings for $\mathcal{C} = R\text{-}\mathcal{Mod}$

Let $\mathcal{D}$ be a full subcategory of $R\text{-}\mathcal{Mod}$, let $C$ be a given $R$-module, and let $f \in \mathcal{Ob}(\mathcal{Perf}_{\mathcal{D}}(C))$.

For every $\phi \in R\text{-}\mathcal{Mod}(D_f, D_f)$, there is a unique ${}^{\dagger}\phi \in R\text{-}\mathcal{Mod}(R_f, R_f)$ such that $f \circ (\phi \otimes id_{R_f}) = f \circ (id_{L_f} \otimes {}^{\dagger}\phi)$. (Define ${}^{\dagger}\phi(y) = \delta_f^{-1}(f(\phi(\cdot) \otimes y)) \in R_f$ for each $y \in R_f$.)

For every $\psi \in R\text{-}\mathcal{Mod}(R_f, R_f)$, there is a unique $\psi^{\dagger} \in R\text{-}\mathcal{Mod}(L_f, L_f)$ such that $f \circ (id_{L_f} \otimes \psi) = f \circ (\psi^{\dagger} \otimes id_{R_f})$ (Define $\psi^{\dagger}(x) = \gamma_f^{-1}(f(x \otimes \psi(\cdot)))$.)

Actually, ${}^{\dagger}(\textvisiblespace) \colon R\text{-}\mathcal{Mod}(L_f, L_f) \to R\text{-}\mathcal{Mod}(R_f, R_f)^{op}$ and $(\textvisiblespace)^{\dagger} \colon R\text{-}\mathcal{Mod}(R_f, R_f)^{op} \to R\text{-}\mathcal{Mod}(L_f, L_f)$ are isomorphisms of $R$-algebras, inverse one from the other.

In particular when $\mathcal{D} = R\text{-}\mathcal{Free}_{fin}$, if $f \colon L_f \otimes R_f \to C$ is a perfect pairing, then $L_f \cong R_f$.

# Example

- Let $R = \mathbb{Z}$ so that $\mathcal{C} = \mathcal{Ab}$ and let $\mathcal{D} = \mathcal{Ab}_{fin}$. Let $A$ be a finite Abelian group, and let us consider the natural pairing $\langle \cdot \mid \cdot \rangle_A \colon A \times \widehat{A} \to \mathbb{R}/\mathbb{Q}$ defined by the evaluation $\langle a \mid \chi \rangle_A = \chi(a)$, where $\widehat{A} = \mathcal{Ab}(A, \mathbb{R}/\mathbb{Q})$. Let $\phi \in \mathcal{Ab}_{fin}(A, A)$, then ${}^{\dagger}\phi \in \mathcal{Ab}_{fin}(\widehat{A}, \widehat{A})$ is given by ${}^{\dagger}\phi(\chi) = \chi \circ \phi$.

- Similarly, let $\mathcal{D} = R\text{-}\mathcal{Free}_{fin}$. We also consider the natural pairing $\langle \cdot \mid \cdot \rangle_n \colon R^n \times (R^n)^* \to R$ given by the evaluation $\langle v \mid \ell \rangle_n = \ell(v)$.

Let $\phi \in R\text{-}\mathcal{Free}_{fin}(R^n, R^n)$, then ${}^{\dagger}\phi \in R\text{-}\mathcal{Free}_{fin}((R^n)^*, (R^n)^*)$ is given by ${}^{\phi}(\ell) = \ell \circ \phi$.

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Rees quotient

Let $S$ be a semigroup, and $I \subseteq S$.

The set $I$ is a (two-sided) ideal of $S$ if

$$SI \subseteq S \supseteq IS \ .$$

An ideal $I$ is said to be prime when $xy \in I$ implies that either $x \in I$ or $y \in I$.

Given an ideal $I$, we may form the Rees quotient $S/I$ of $S$ by $I$: it is the set $(S \setminus I) \sqcup \{ \infty \}$ with the following operation: let $x, y \in S$, then $x \times y = xy$ if $xy \notin I$, $x \times y = \infty$ otherwise, and $z \times \infty = \infty = \infty \times z$ for every $z \in (S \setminus I) \sqcup \{ \infty \}$.

It is equivalently defined as the quotient semigroup $S/\cong_I$ by the congruence $x \cong_I y$ if, and only if, $x, y \in I$ or $x = y$.

# Remark

If $I$ is a prime ideal of $S$, then $S/I$ is zero-divisor free, therefore it is a usual semigroup, say $T$, with a two-sided absorbing element $\infty$ freely adjoined $T^{\infty} = T \sqcup \{ \infty \}$.

# A symmetric monoidal structure on $\mathcal{B}il_{\mathcal{D}}(C)$

From now on, $\mathcal{C} = R\text{-}\mathcal{M}od$, and $\mathcal{D}$ is cocartesian for $\oplus$.

Let $A, B, C, D \in \mathcal{O}b(\mathcal{D})$. Since
$(A \oplus B) \otimes (C \otimes D) \cong (A \otimes C) \oplus (A \otimes D) \oplus (B \otimes C) \oplus (B \otimes D)$,
$(A \oplus B) \otimes (C \otimes D)$ has a coproduct presentation:

$$\begin{tikzcd}
A \otimes C \arrow[dr, "q_A \otimes q_C"] & & A \otimes D \arrow[dl, "q_A \otimes q_D"'] \\
& (A \oplus B) \otimes (C \oplus D) & \\
B \otimes C \arrow[ur, "q_B \otimes q_C"'] & & B \otimes D \arrow[ul, "q_B \otimes q_D"]
\end{tikzcd}$$

# A symmetric monoidal structure on $\mathcal{Bil}_{\mathcal{D}}(C)$

Let $f, g \in \mathcal{Ob}(\mathcal{Bil}_{\mathcal{D}}(C))$.

We define $f \perp g \colon (L_f \oplus L_g) \otimes (R_f \oplus R_g) \to C$ by

$$
\begin{aligned}
(f \perp g) \circ q_{L_f} \otimes q_{R_f} &= f, \\
(f \perp g) \circ q_{L_g} \otimes q_{R_g} &= g, \\
(f \perp g) \circ q_{L_f} \otimes q_{R_g} &= 0_{L_f \otimes R_g, C}, \\
(f \perp g) \circ q_{L_g} \otimes q_{R_f} &= 0_{L_g \otimes R_f, C}
\end{aligned}
$$

where $0_{A,B}$ is the zero arrow from $A$ to $B$.

Because $\mathcal{D}$ is assumed cocartesian for $\oplus$, $f \perp g \in \mathcal{Ob}(\mathcal{Bil}_{\mathcal{D}}(C))$.

# A remark

Let $q_f \in \mathcal{B}il_{\mathcal{D}}(C)(f, f \perp g)$ be defined by $q_f = (q_{L_f}, q_{R_f})$, and similarly, let $q_g \in \mathcal{B}il_{\mathcal{D}}(C)(g, f \perp g)$ be given by $q_g = (q_{L_g}, q_{R_g})$.

It is not true that $(f \perp g, q_f, q_g)$ forms a coproduct for $f, g$.

Nevertheless it satisfies the following universal property: let $h \in \mathcal{B}il_{\mathcal{D}}(C)$, $\alpha \in \mathcal{B}il_{\mathcal{D}}(C)(f, h)$ and $\beta \in \mathcal{B}il_{\mathcal{D}}(C)(g, h)$ such that $h \circ (\alpha_l \otimes \alpha_r) = 0_{L_f \otimes R_f, C}$ and $h \circ (\beta_l \otimes \beta_r) = 0_{L_g \otimes R_g, C}$, then there is a unique arrow $\gamma \in \mathcal{B}il_{\mathcal{D}}(C)$ such that $\gamma \circ q_f = \alpha$ and $\gamma \circ q_g = \beta$, namely $\gamma = ([\alpha_l, \beta_l], [\alpha_r, \beta_r])$.

# Symmetric monoidal structure at the level of arrows

Let $f, f', g, g' \in \mathcal{Bil}_{\mathcal{D}}(C)$, and $\alpha \in \mathcal{Bil}_{\mathcal{D}}(C)(f, f')$, $\beta \in \mathcal{Bil}_{\mathcal{D}}(C)(g, g')$, then $\alpha \perp \beta \in \mathcal{Bil}_{\mathcal{D}}(C)(f \perp g, f' \perp g')$ is defined by

$$\alpha \perp \beta = (\alpha_l \oplus \beta_l, \alpha_r \oplus \beta_r) \ .$$

The unit of $\perp$ is $\mathit{0}_{0 \otimes 0, C}$ and the coherent braiding is given by $\sigma_{f,g} = (\sigma_{L_f, L_g}, \sigma_{R_f, R_g}) \colon f \perp g \to g \perp f$ where $\sigma_{A,B} \colon A \oplus B \cong B \oplus A$ is the natural twist of $\mathcal{C}$.

# An essential property of $\perp$

### Theorem

Let $f, g \in \mathcal{Bil}_{\mathcal{D}}(C)$.

The bilinear map $f \perp g$ is a pairing (respectively, a perfect pairing) if, and only if, $f$ and $g$ are pairings (respectively, perfect pairings) themselves.

As a corollary, the set of equivalent classes of pairings $\underline{\mathcal{Pair}}_{\mathcal{D}}(C)$ is a sub-monoid of the (commutative) monoid $\underline{\mathcal{Bil}}_{\mathcal{D}}(C)$ (under $\perp$) of equivalent classes of bilinear maps, and the set of equivalent classes of perfect pairings $\underline{\mathcal{Perf}}_{\mathcal{D}}(C)$ is a sub-monoid of $\underline{\mathcal{Pair}}_{\mathcal{D}}(C)$.

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Locally finite monoids

Let $S$ be a semigroup, and $x \in S$. A decomposition of $x$ of length $n$ is a $n$-tuple $(x_1, \cdots, x_n) \in S^n$ such that $x = x_1 \cdots x_n$. A decomposition of $x$ is then a decomposition of $x$ of length $n$ for some $n$. A semigroup is said to be locally finite if all its members admit only finitely many decompositions.

If $M$ is a monoid (with identity 1), and $x \in M$, then a decomposition $(x_1, \cdots, x_n)$ of $x$ is said to be non-trivial if no $x_i$'s are equal to 1. A monoid is said to be locally finite if all its members admit only finitely many non-trivial decompositions.

Let $S$ be any semigroup (or monoid), and $x \in S$. We denote by $D_n(x)$ the set of all (non trivial) decompositions of $x$ of length $n$.

## Remark

No elements of a locally finite monoid, except the identity, are invertible. In particular, no group (except the trivial one) may be a locally finite monoid.

# Length

Any locally finite semigroup (respectively, monoid) $S$ may be equipped with a length function defined as follows: for $x \in S$,

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

In particular for a locally finite monoid $M$, $\ell(x) = 0$ if, and only if, $x = 1$.

A member $x$ of $M$ is said to be indecomposable if $\ell(x) = 1$. It is clear that such indecomposable elements generate the monoid $M$.

# Finite decomposition monoids

A monoid $M$ is said to be a finite decomposition monoid if for every $x \in M$,

$$\{ (y, z) \in M^2 \colon x = yz \}$$

is finite. Clearly, any finite monoid is a finite decomposition monoid. So is any locally finite monoid. A non trivial finite group is a finite decomposition but not locally finite monoid.

Let $R$ be a commutative ring with a unit, and let $A$ be a commutative $R$-algebra with a unit. Let $M$ be a finite decomposition monoid. Then, $A^M$ admits a structure of $R$-algebra with a unit given by $(fg)(x) = \sum_{yz=x} f(y)g(z)$ (convolution product). This algebra is denoted by $A[[M]]$ and called the large algebra of $M$ (for instance, $\mathbb{C}[[\mathbb{N}^*]]$ is the algebra of Dirichlet's series).

## Remark: Möbius inversion

If $M$ is a locally finite monoid, then the zêta function $\zeta_A \in A^M$, given by $\zeta_A(x) = 1$ for every $x \in M$, is invertible. ($\zeta_{\mathbb{C}}$ is the usual Riemann zêta function when $M = \mathbb{N}^*$.)

# Finite decomposition and algebraic monoids

Let $M$ be a finite decomposition monoid. Let $R[x_a \colon a \in M]$ be the polynomial algebra in the indeterminate $x_a$, for each $a \in M$ (*i.e.*, the $R$-algebra of the free commutative monoid generated by the set $M$). Then, the functor $(\textvisiblespace)^M \colon R\text{-}\mathcal{CAlg} \to \mathcal{Set}$ (defined at the object level by $A \mapsto A^M$) is a representable functor with representing object $R[x_a \colon a \in M]$ (coordinate ring) since $R\text{-}\mathcal{CAlg}(R[x_a \colon a \in M], A) \cong A^M$.

Moreover, the underlying multiplicative monoid structure of $A[[M]]$ is natural in the algebra $A$ of coefficients. The multiplication $m \colon (\textvisiblespace)[[M]] \times (\textvisiblespace)[[M]] \to (\textvisiblespace)[[M]]$ and the unit $e \colon * \to (\textvisiblespace)[[M]]$ are natural transformations between representable functors. According to Yoneda's lemma they give rise to a structure of bialgebra on $R[x_a \colon a \in M]$, so that $(\textvisiblespace)[[M]]$ becomes a (pro-affine) algebraic monoid.

Finally, the monoid $M$ is a sub-monoid of the $R$-rational points $R[[M]]$ of the pro-affine monoid scheme $(\textvisiblespace)[[M]]$. The constant functor $R\text{-}\mathcal{CAlg} \to \mathcal{Set}$ with value $M$ is a sub-functor of $(\textvisiblespace)[[M]]$, and as such corresponds to a cosieve $I_M$ under the representing object $R[x_a \colon a \in M]$, namely $I_M = \{\, \widehat{a}_A \colon a \in A,\ A \in R\text{-}\mathcal{CAlg} \,\}$ (where $\widehat{a}_A \in R\text{-}\mathcal{CAlg}(R[x_a \colon a \in M], A)$ defined by $\widehat{a}_A(x_b) = 0$ for all $b \neq a$, and $\widehat{a}_A(x_a) = 1_A$).

# Remark: Zêta function

Let $M$ be a locally finite monoid. For every algebra $A$, let $\mathfrak{M}_A$ be the augmentation ideal of $A[[M]]$, *i.e.*, the set all functions $f$ in $A^M$ vanishing at the identity of $M$.

Then, $1 + \mathfrak{M}_{(\_)}$ is a pro-affine algebraic group scheme (this is the reason why in this case the zêta function $\zeta_A$ is invertible).

# Back to pairings

From now, one we assume that $\mathcal{D} = R\text{-}\mathcal{Free}_{\mathit{fin}}$ or $\mathcal{D} = \mathcal{Ab}_{\mathit{fin}}$ if $R = \mathbb{Z}$.

We denote by $[f]$ the class of equivalence under isomorphism of a bilinear map $f \in \mathcal{Bil}_{\mathcal{D}}(C)$.

• Let $\mathcal{C} = \mathcal{Ab}$, and $\mathcal{D} = \mathcal{Ab}_{\mathit{fin}}$. Then, there exists a homomorphism of monoids $c\colon \underline{\mathcal{Bil}}_{\mathcal{Ab}_{\mathit{fin}}}(C) \to \mathbb{N}^* \times \mathbb{N}^*$ given by $c([f]) = (|L_f|, |R_f|)$ (well-defined on equivalence classes).

• Let $\mathcal{C} = R\text{-}\mathcal{Mod}$, and $\mathcal{D} = R\text{-}\mathcal{Free}_{\mathit{fin}}$. Then, there exists a homomorphism of monoids $d\colon \underline{\mathcal{Bil}}_{R\text{-}\mathcal{Free}_{\mathit{fin}}}(C) \to \mathbb{N} \times \mathbb{N}$ given by $d([f]) = (\mathit{rank}(L_f), \mathit{rank}(R_f))$ (well-defined on equivalence classes).

# Back to pairings

From the existence of the morphisms $c$ and $d$, it may be deduced that $\underline{\mathcal{Bil}}_{\mathcal{D}}(C)$, $\underline{\mathcal{Pair}}_{\mathcal{D}}(C)$ and $\underline{\mathcal{Perf}}_{\mathcal{D}}(C)$ are all locally finite monoids.

So they are sub-monoids of rational points of some (pro-affine) algebraic variety.

# Table of contents

1. Introduction
2. Category theoretic definitions and notations
3. Categories of bilinear maps
4. Pairings as a Rees quotient
5. Length of a pairing and local finiteness
6. Classification of pairings on $\mathbb{R}/\mathbb{Z}$

# Pairings are perfect

From now on, $\mathcal{C} = \mathbb{Z}\text{-}\mathcal{Mod} = \mathcal{Ab}$, $\mathcal{D} = \mathcal{Ab}_{fin}$ and $C = \mathbb{R}/\mathbb{Z}$.

Let $A$ be any finite Abelian group, and let us denote by $\widehat{A} = \mathcal{Ab}(A, \mathbb{R}/\mathbb{Z})$ the group of characters (or dual) of $A$. It is well-known that $A \cong \widehat{A}$ (non natural isomorphism).

Let $f \in \mathcal{Ob}(\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z}))$. Then, $L_f \hookrightarrow \widehat{R}_f \cong R_f \hookrightarrow \widehat{L}_f \cong L_f$, so that $L_f \cong R_f$, and $\gamma_f, \delta_f$ are isomorphisms. Thus, $f$ is a perfect pairing, *i.e.*, $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z}) = \mathcal{Perf}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z})$.

# Natural pairing

Let $A$ be a finite Abelian group. The natural pairing is defined by $\langle \cdot \mid \cdot \rangle_A \colon A \times \widehat{A} \to \mathbb{R}/\mathbb{Z}$ by

$$\langle a \mid \chi \rangle_A = \chi(a) \ .$$

## Theorem

Let $f \in \mathcal{O}b(\mathcal{P}air_{\mathcal{A}b_{fin}}(\mathbb{R}/\mathbb{Z}))$, then $f \cong \langle \cdot \mid \cdot \rangle_{L_f}$.

Sketch of the proof: Let $\alpha \colon R_f \cong L_f$, and define $g \colon L_f \times L_f \to \mathbb{R}/\mathbb{Z}$ by $g(a, b) = f(a, \alpha^{-1}(b))$ so that $g \cong f$. Since $\delta_g \colon L_f \to \widehat{L_f}$ is an isomorphism, $h = g \circ (id_{L_f} \otimes \delta_g^{-1}) \cong g$. Moreover, $h(a, \chi) = g(a, \delta_g^{-1}(\chi)) = \delta_g(\delta_g^{-1}(\chi))(a) = \chi(a) = \langle a \mid \chi \rangle_{L_f}$. □

# Equivalence classes of pairings

As a corollary, equivalence classes of pairings and isomorphic classes of finite Abelian groups are in one-one correspondence.

Since $\mathcal{Ab}(A \oplus B, \mathbb{R}/\mathbb{Z}) \cong \mathcal{Ab}(A, \mathbb{R}/\mathbb{Z}) \times \mathcal{Ab}(B, \mathbb{R}/\mathbb{Z})$, it follows that $\widehat{A \oplus B} \cong \widehat{A} \oplus \widehat{B}$ (isomorphic as groups).

Moreover,

$$\langle \cdot \mid \cdot \rangle_{A \oplus B} \cong \langle \cdot \mid \cdot \rangle_A \perp \langle \cdot \mid \cdot \rangle_B \ .$$

In conclusion, $\underline{\mathcal{Pair}}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z}) = \underline{\mathcal{Perf}}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z}) \cong \bigoplus_{p \in \mathbb{P}} M_p$, where $\mathbb{P}$ is the set of all prime numbers, and $M_p$ is the free commutative monoid generated by prime powers $p^i$'s, $i \in \mathbb{N}^*$. In particular, $\underline{\mathcal{Pair}}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z})$ is a free commutative monoid.

## Remark

The case $\mathcal{C} = R\text{-}\mathcal{Mod}$, $\mathcal{D} = R\text{-}\mathcal{Free}_{fin}$ and $C = R$ may be treated similarly, and it is found that $\underline{\mathcal{Pair}}_{R\text{-}\mathcal{Free}_{fin}}(R) = \underline{\mathcal{Perf}}_{R\text{-}\mathcal{Free}_{fin}}(R) \cong \mathbb{N}$.

# Remark

Let $f\colon A \times B \to \mathbb{Z}_n$ be a pairing. Then, it may be seen as a $\mathbb{R}/\mathbb{Z}$-valued pairing (since $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{Z}_n)$ is a full subcategory of $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z})$) and as such it is a perfect pairing (thus $A \cong B$) and $f$ is isomorphic to $\langle \cdot \mid \cdot \rangle_A$.

## Remark

- Let $f\colon \mathbb{Z}_n^m \otimes \mathbb{Z}_n \to \mathbb{Z}_n^m$ be given by
$f((x_i \bmod n)_{i=1}^m, y) = (x_i y \bmod n)_{i=1}^n$. It is a pairing (obviously non perfect whenever $m > 1$).

- Since $\mathbb{C}^* \cong \mathbb{R}/\mathbb{Z}$ are isomorphic groups, $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{C}^*) \cong \mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z})$.
Moreover, $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{Q}/\mathbb{Z}) \cong \mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Z})$ because of the torsion in finite Abelian groups.

# Remark

Let $p$ be a prime number, and let $\mathbb{Z}(p^\infty)$ be the Prüfer $p$-group, *i.e.*, the direct limit of $0 \hookrightarrow \mathbb{Z}_p \hookrightarrow \mathbb{Z}_{p^2} \hookrightarrow \cdots$ (certainly, $\mathbb{Z}(p^\infty)$ is a sub-group of $\mathbb{Q}/\mathbb{Z}$).

Let $p\text{-}\mathcal{Ab}_{\mathit{fin}}$ be the full subcategory of $\mathcal{Ab}_{\mathit{fin}}$ of all finite Abelian $p$-groups. The category $\mathcal{Pair}_{p\text{-}\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Z}(p^\infty))$ is a full subcategory of $\mathcal{Pair}_{\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Q}/\mathbb{Z})$, therefore each $f \in \mathcal{Ob}(\mathcal{Pair}_{p\text{-}\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Z}(p^\infty))$ may be seen as a perfect pairing (so that $L_f \cong R_f$) with values in $\mathbb{Q}/\mathbb{Z}$, and as so it is isomorphic to $\langle \cdot \mid \cdot \rangle_{L_f}$.

It becomes easy to see that $\underline{\mathcal{Pair}}_{p\text{-}\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Z}(p^\infty))$ is the free commutative monoid $M_p$ generated prime powers $p^i$, $i \geq 1$ in such a way that

$$\underline{\mathcal{Pair}}_{\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Q}/\mathbb{Z}) \cong \bigoplus_{p \in \mathbb{P}} \underline{\mathcal{Pair}}_{p\text{-}\mathcal{Ab}_{\mathit{fin}}}(\mathbb{Z}(p^\infty))$$

# The zêta function of $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Q})$

According to Pierre Cartier and Dominique Foata, for any algebra $A$, the inverse $\mu_A$ of the zêta function $\zeta_A$ of the free monoid $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Q})$ is given by

$$\mu_A([\langle\cdot \mid \cdot\rangle_{\mathbb{Z}_{p^i}}]) = -1_A$$

for all prime numbers $p$ and integers $i > 0$,

$$\mu_A(0) = 1_A \ ,$$

and for all $[f] \in \mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Q})$ with $\ell([f]) \geq 2$,

$$\mu_A([f]) = 0 \ .$$

(Because $\mathcal{Pair}_{\mathcal{Ab}_{fin}}(\mathbb{R}/\mathbb{Q})$ is a free commutative monoid, its length $\ell$ corresponds to the number of generators in a term.)