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

Séminaire Protection de l'information
Vendredi 29 novembre 2013

Table of contents

1 Introduction

2 Category of pairings

3 A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$

4 Moduli space of pairings

5 Geometric interpretation of the moduli space of pairings

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

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

$$\gamma_f\colon a \in A \mapsto f(a, \cdot)$$

and

$$\delta_f\colon b \in B \mapsto f(\cdot, b)$$

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 $\mathbb{K}$ 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). The map $\langle \cdot \mid \cdot \rangle \colon \mathbb{K}^X \times \mathbb{K}^{(X)} \to \mathbb{K}$ given by $\langle f \mid g \rangle = \sum_{x \in X} f(x)g(x)$ is a pairing.

Cryptographic applications

- MOV attack to solve the 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 categorical setting to study pairings in a unified way in several categories (e.g., abelian groups, modules or commutative monoids).

• Provide a classification of pairings – under a suitable equivalence relation – from finite abelian groups to the complex unit circle (this classification is rather disappointing).

• 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 a categorical nature, since it is the relation of isomorphism in a suitable category, and it is strictly coarser than C.T.C Wall's relation (more pairings are identified).

Table of contents

1. Introduction
2. Category of pairings
3. A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$
4. Moduli space of pairings
5. Geometric interpretation of the moduli space of pairings
6. Classification of pairings on $\mathbb{Q}/\mathbb{Z}$

Table of contents

1. Introduction
2. Category of pairings
3. A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$
4. Moduli space of pairings
5. Geometric interpretation of the moduli space of pairings
6. Classification of pairings on $\mathbb{Q}/\mathbb{Z}$

Bilinear maps

Let c be an abelian group (e.g., $c = \mathbb{Q}/\mathbb{Z}$).

• A bilinear map on c is a pair $(f, (a, b))$ where a, b are both finite abelian groups and f is a group homomorphism $f \colon a \otimes b \to c$ ($\otimes$ being the usual tensor product of abelian groups that classifies bi-additive maps).

Bilinear maps

Let c be an abelian group (e.g., $c = \mathbb{Q}/\mathbb{Z}$).

• A bilinear map on c is a pair $(f, (a, b))$ where a, b are both finite abelian groups and f is a group homomorphism $f\colon a \otimes b \to c$ ($\otimes$ being the usual tensor product of abelian groups that classifies bi-additive maps).

• A pair (α, β) of group homomorphisms between finite abelian groups, $\alpha\colon a \to d$, $\beta\colon b \to e$, is said to be an arrow or a morphism $(\alpha, \beta)\colon (f, (a, b)) \to (g, (d, e))$ if the following triangle commutes

$$\begin{array}{ccc} a \otimes b & \xrightarrow{\alpha\otimes\beta} & d \otimes e \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & c & \end{array} \tag{1}$$

Bilinear maps

Let c be an abelian group (e.g., $c = \mathbb{Q}/\mathbb{Z}$).

• A bilinear map on c is a pair $(f, (a, b))$ where a, b are both finite abelian groups and f is a group homomorphism $f : a \otimes b \to c$ ($\otimes$ being the usual tensor product of abelian groups that classifies bi-additive maps).

• A pair (α, β) of group homomorphisms between finite abelian groups, $\alpha : a \to d$, $\beta : b \to e$, is said to be an arrow or a morphism $(\alpha, \beta) : (f, (a, b)) \to (g, (d, e))$ if the following triangle commutes

$$\begin{array}{ccc} a \otimes b & \xrightarrow{\alpha \otimes \beta} & d \otimes e \\ & {\scriptstyle f} \searrow \quad \swarrow {\scriptstyle g} & \\ & c & \end{array} \tag{1}$$

In other terms, $g_0(\alpha(x), \beta(y)) = f_0(x, y)$ for every $x \in a$, $y \in b$ (where $f_0 : a \times b \to c$ and $g_0 : d \times e \to c$ are the bi-additive maps associated to f and g respectively).

Bilinear maps (cont'd)

• Bilinear maps on c with these morphisms form a category denoted by $\mathbf{Bil}_{\mathbf{Abfin}}(c)$, the composition of morphisms being defined component-wise $(\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) = (\alpha_1 \circ \alpha_2, \beta_1 \circ \beta_2)$, and the identity morphism $id_{(f,(a,b))}$ on $(f, (a, b))$ being just (id_a, id_b).

Bilinear maps (cont'd)

• Bilinear maps on c with these morphisms form a category denoted by $\mathbf{Bil}_{\mathbf{Abfin}}(c)$, the composition of morphisms being defined component-wise $(\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) = (\alpha_1 \circ \alpha_2, \beta_1 \circ \beta_2)$, and the identity morphism $id_{(f,(a,b))}$ on $(f,(a,b))$ being just (id_a, id_b).

• An isomorphism (α, β) from $(f,(a,b))$ to $(g,(d,e))$ is just an arrow $(\alpha, \beta)\colon (f,(a,b)) \to (g,(c,d))$ such that $\alpha\colon a \to d$ and $\beta\colon b \to e$ are both group isomorphisms

Bilinear maps (cont'd)

• Bilinear maps on c with these morphisms form a category denoted by $\mathbf{Bil_{Abfin}}(c)$, the composition of morphisms being defined component-wise $(\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) = (\alpha_1 \circ \alpha_2, \beta_1 \circ \beta_2)$, and the identity morphism $id_{(f,(a,b))}$ on $(f,(a,b))$ being just (id_a, id_b).

• An isomorphism (α, β) from $(f,(a,b))$ to $(g,(d,e))$ is just an arrow $(\alpha, \beta)\colon (f,(a,b)) \to (g,(c,d))$ such that $\alpha\colon a \to d$ and $\beta\colon b \to e$ are both group isomorphisms (thus $(f,(a,b)) \cong (g,(d,e))$ implies $a \cong d$ and $b \cong e$ as finite abelian groups).

(Perfect) Pairings

- A (perfect) pairing (on c) is a bilinear map $(f, (a, b))$ on c such that γ_f and δ_f are both monomorphisms (respectively, isomorphisms) (recall from the introduction that $\gamma_f(x) = f_0(x, \cdot)$ and $\delta_f(y) = f_0(\cdot, y)$).

Remark

In category-theoretical terms, a *monomorphism* f is a left-cancellable morphism. For the categories of sets, abelian groups, commutative monoids, modules over some commutative unital ring, and many other categories but not all, monomorphisms coincide with one-to-one maps.

(Perfect) Pairings

• A (perfect) pairing (on c) is a bilinear map $(f, (a, b))$ on c such that γ_f and δ_f are both monomorphisms (respectively, isomorphisms) (recall from the introduction that $\gamma_f(x) = f_0(x, \cdot)$ and $\delta_f(y) = f_0(\cdot, y)$).

Remark

In category-theoretical terms, a *monomorphism* f is a left-cancellable morphism. For the categories of sets, abelian groups, commutative monoids, modules over some commutative unital ring, and many other categories but not all, monomorphisms coincide with one-to-one maps.

• Let us denote by $\mathbf{Pair}_{\mathbf{Abfin}}(c)$ (resp. $\mathbf{Perf}_{\mathbf{Abfin}}(c)$) the full sub-category of $\mathbf{Bil}_{\mathbf{Abfin}}(c)$ with objects the (perfect) pairings on c.

(Perfect) Pairings

• A (perfect) pairing (on c) is a bilinear map $(f,(a,b))$ on c such that γ_f and δ_f are both monomorphisms (respectively, isomorphisms) (recall from the introduction that $\gamma_f(x) = f_0(x,\cdot)$ and $\delta_f(y) = f_0(\cdot,y)$).

Remark

In category-theoretical terms, a *monomorphism* f is a left-cancellable morphism. For the categories of sets, abelian groups, commutative monoids, modules over some commutative unital ring, and many other categories but not all, monomorphisms coincide with one-to-one maps.

• Let us denote by $\mathbf{Pair}_{\mathbf{Abfin}}(c)$ (resp. $\mathbf{Perf}_{\mathbf{Abfin}}(c)$) the full sub-category of $\mathbf{Bil}_{\mathbf{Abfin}}(c)$ with objects the (perfect) pairings on c.

• $\mathbf{Perf}_{\mathbf{Abfin}}(c)$ is of course a full sub-category of $\mathbf{Pair}_{\mathbf{Abfin}}(c)$.

Some easy functorial properties

• Functorially, if $c_1 \hookrightarrow c_2$, then $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (full embedding of categories).

Some easy functorial properties

• Functorially, if $c_1 \hookrightarrow c_2$, then $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (full embedding of categories).

• Functorially, if $c_1 \cong c_2$, then $\mathbf{Perf}_{\mathbf{Abfin}}(c_1) \cong \mathbf{Perf}_{\mathbf{Abfin}}(c_2)$ (isomorphic categories).

Some easy functorial properties

• Functorially, if $c_1 \hookrightarrow c_2$, then $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (full embedding of categories).

• Functorially, if $c_1 \cong c_2$, then $\mathbf{Perf}_{\mathbf{Abfin}}(c_1) \cong \mathbf{Perf}_{\mathbf{Abfin}}(c_2)$ (isomorphic categories).

• Of course, if $c_1 \cong c_2$, then also $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \cong \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (isomorphic categories), but the converse is false.

Some easy functorial properties

• Functorially, if $c_1 \hookrightarrow c_2$, then $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (full embedding of categories).

• Functorially, if $c_1 \cong c_2$, then $\mathbf{Perf}_{\mathbf{Abfin}}(c_1) \cong \mathbf{Perf}_{\mathbf{Abfin}}(c_2)$ (isomorphic categories).

• Of course, if $c_1 \cong c_2$, then also $\mathbf{Pair}_{\mathbf{Abfin}}(c_1) \cong \mathbf{Pair}_{\mathbf{Abfin}}(c_2)$ (isomorphic categories), but the converse is false. For instance, $\mathbf{Pair}_{\mathbf{Abfin}}(0) \cong \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Z})$.

Isomorphisms preserve non-degeneracy

• An isomorphism class of bilinear maps on c either contains no pairings or all its members are pairings (in other terms, a bilinear map is isomorphic to a pairing if, and only if, it is itself a pairing).

Isomorphisms preserve non-degeneracy

• An isomorphism class of bilinear maps on c either contains no pairings or all its members are pairings (in other terms, a bilinear map is isomorphic to a pairing if, and only if, it is itself a pairing).

• The same holds replacing bilinear maps by pairings, and pairings by perfect pairings in the above sentence.

Isomorphisms preserve non-degeneracy

• An isomorphism class of bilinear maps on c either contains no pairings or all its members are pairings (in other terms, a bilinear map is isomorphic to a pairing if, and only if, it is itself a pairing).

• The same holds replacing bilinear maps by pairings, and pairings by perfect pairings in the above sentence.

• It follows that

$$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c) = \underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \cup \underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$$

of course with

$$\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \cap \underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) = \emptyset$$

Isomorphisms preserve non-degeneracy

• An isomorphism class of bilinear maps on c either contains no pairings or all its members are pairings (in other terms, a bilinear map is isomorphic to a pairing if, and only if, it is itself a pairing).

• The same holds replacing bilinear maps by pairings, and pairings by perfect pairings in the above sentence.

• It follows that

$$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c) = \underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \cup \underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$$

of course with

$$\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \cap \underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) = \emptyset$$

and

$$\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) = \underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c) \cup \underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c)$$

with

$$\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c) \cap \underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c) = \emptyset$$

Remark

Everything remains valid if one replaces

- the category of abelian groups by any *closed symmetric monoidal category* **C** (i.e., with a tensor bifunctor, an internal hom functor, and some properties...),

- the category of finite abelian groups by any full sub-category **D** of **C**.

Remark

Everything remains valid if one replaces

- the category of abelian groups by any *closed symmetric monoidal category* **C** (i.e., with a tensor bifunctor, an internal hom functor, and some properties...),

- the category of finite abelian groups by any full sub-category **D** of **C**.

For instance, **C** may be

- the category of sets ($\otimes = \times$) with **D** the category of finite sets,

- the category of commutative monoids ($\otimes = \otimes_{\mathbb{N}}$ similar to $\otimes_{\mathbb{Z}}$), with **D** that of finite commutative monoids,

- the category $_R\mathbf{Mod}$ of modules on a commutative ring R ($\neq 0$) with a unity ($\otimes = \otimes_R$), and $\mathbf{D} = {}_R\mathbf{Modfreefin}$, the category of free R-modules of finite rank.

Table of contents

1. Introduction
2. Category of pairings
3. A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$
4. Moduli space of pairings
5. Geometric interpretation of the moduli space of pairings
6. Classification of pairings on $\mathbb{Q}/\mathbb{Z}$

Direct sum of abelian groups

Let a, b be two abelian groups, and let $a \oplus b$ denote their direct sum with canonical injections $q_a \colon a \hookrightarrow a \oplus b, x \mapsto (x, 0)$ and $q_b \colon b \hookrightarrow a \oplus b, y \mapsto (0, y)$.

Direct sum of abelian groups

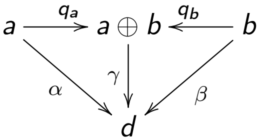
Let a, b be two abelian groups, and let $a \oplus b$ denote their direct sum with canonical injections $q_a \colon a \hookrightarrow a \oplus b, x \mapsto (x, 0)$ and $q_b \colon b \hookrightarrow a \oplus b, y \mapsto (0, y)$.

Categorically, the direct sum $\oplus$ is characterized by a universal property:

Direct sum of abelian groups

Let a, b be two abelian groups, and let $a \oplus b$ denote their direct sum with canonical injections $q_a\colon a \hookrightarrow a \oplus b, x \mapsto (x, 0)$ and $q_b\colon b \hookrightarrow a \oplus b, y \mapsto (0, y)$.

Categorically, the direct sum $\oplus$ is characterized by a universal property: for every abelian group d, and every group homomorphisms $\alpha\colon a \to d$ and $\beta\colon b \to d$, there is a unique group homomorphism $\gamma\colon a \oplus b \to d$ that makes commute the following diagram.



(2)

Direct sum of abelian groups

Let a, b be two abelian groups, and let $a \oplus b$ denote their direct sum with canonical injections $q_a\colon a \hookrightarrow a \oplus b, x \mapsto (x, 0)$ and $q_b\colon b \hookrightarrow a \oplus b, y \mapsto (0, y)$.

Categorically, the direct sum $\oplus$ is characterized by a universal property: for every abelian group d, and every group homomorphisms $\alpha\colon a \to d$ and $\beta\colon b \to d$, there is a unique group homomorphism $\gamma\colon a \oplus b \to d$ that makes commute the following diagram.

$$\begin{array}{ccccc} a & \xrightarrow{q_a} & a \oplus b & \xleftarrow{q_b} & b \\ & \searrow^{\alpha} & \downarrow{\scriptstyle\gamma} & \swarrow_{\beta} & \\ & & d & & \end{array} \tag{2}$$

In concrete terms, $\gamma(x, y) = \alpha(x) + \beta(y)$.

$\otimes$ distributes over $\oplus$

It is a well-known fact that for every abelian groups a_1, a_2, b_1, b_2,

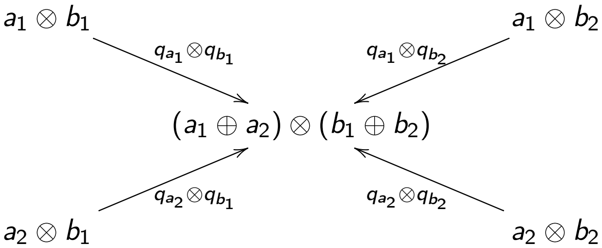
$$(a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \cong (a_1 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_1) \oplus (a_2 \otimes b_2).$$

$\otimes$ distributes over $\oplus$

It is a well-known fact that for every abelian groups a_1, a_2, b_1, b_2,

$$(a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \cong (a_1 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_1) \oplus (a_2 \otimes b_2).$$

More precisely, $(a_1 \oplus a_2) \otimes (b_1 \oplus b_2)$ admits a direct sum presentation as



(This comes from the fact that for every abelian group a, both functors $a \otimes -$ and $- \otimes a$ admit a right adjoint, and this is true in any symmetric monoidal closed category with binary coproducts.)

A tensor bifunctor $\perp$

It is thus possible to define for every abelian group d, and any group homomorphisms $\alpha_1 \colon a_1 \otimes b_1 \to d$, $\beta_1 \colon a_1 \otimes b_2 \to d$, $\alpha_2 \colon a_2 \otimes b_1 \to d$, and $\beta_2 \colon a_2 \otimes b_2 \to d$, a unique group homomorphism $\gamma \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to d$ (using the universal property of the direct sum).

A tensor bifunctor $\perp$

It is thus possible to define for every abelian group d, and any group homomorphisms $\alpha_1 \colon a_1 \otimes b_1 \to d$, $\beta_1 \colon a_1 \otimes b_2 \to d$, $\alpha_2 \colon a_2 \otimes b_1 \to d$, and $\beta_2 \colon a_2 \otimes b_2 \to d$, a unique group homomorphism $\gamma \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to d$ (using the universal property of the direct sum). In more concrete terms,
$\gamma((x_1, x_2) \otimes (y_1, y_2)) = \alpha_1(x_1 \otimes y_1) + \alpha_2(x_2 \otimes y_1) + \beta_1(x_1 \otimes y_2) + \beta_2(x_2 \otimes y_2)$.

A tensor bifunctor $\perp$

It is thus possible to define for every abelian group d, and any group homomorphisms $\alpha_1 \colon a_1 \otimes b_1 \to d$, $\beta_1 \colon a_1 \otimes b_2 \to d$, $\alpha_2 \colon a_2 \otimes b_1 \to d$, and $\beta_2 \colon a_2 \otimes b_2 \to d$, a unique group homomorphism $\gamma \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to d$ (using the universal property of the direct sum). In more concrete terms,
$\gamma((x_1, x_2) \otimes (y_1, y_2)) = \alpha_1(x_1 \otimes y_1) + \alpha_2(x_2 \otimes y_1) + \beta_1(x_1 \otimes y_2) + \beta_2(x_2 \otimes y_2)$.

This makes feasible to define the following (functorial) operation on the bilinear maps $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ on c

A tensor bifunctor $\perp$

It is thus possible to define for every abelian group d, and any group homomorphisms $\alpha_1 \colon a_1 \otimes b_1 \to d$, $\beta_1 \colon a_1 \otimes b_2 \to d$, $\alpha_2 \colon a_2 \otimes b_1 \to d$, and $\beta_2 \colon a_2 \otimes b_2 \to d$, a unique group homomorphism $\gamma \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to d$ (using the universal property of the direct sum). In more concrete terms,
$\gamma((x_1, x_2) \otimes (y_1, y_2)) = \alpha_1(x_1 \otimes y_1) + \alpha_2(x_2 \otimes y_1) + \beta_1(x_1 \otimes y_2) + \beta_2(x_2 \otimes y_2)$.

This makes feasible to define the following (functorial) operation on the bilinear maps $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ on c by
$(f_1, (a_1, b_1)) \perp (f_2, (a_2, b_2)) = (f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$, where
$f_1 \perp f_2 \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to c$ is defined as γ above using
- $\alpha_1 = f_1 \colon a_1 \otimes b_1 \to c$,
- $\alpha_2 = 0 \colon a_2 \otimes b_1 \to c$,
- $\beta_1 = 0 \colon a_1 \otimes b_2 \to c$,
- $\beta_2 = f_2 \colon a_2 \otimes b_2 \to c$.

A tensor bifunctor $\perp$

It is thus possible to define for every abelian group d, and any group homomorphisms $\alpha_1 \colon a_1 \otimes b_1 \to d$, $\beta_1 \colon a_1 \otimes b_2 \to d$, $\alpha_2 \colon a_2 \otimes b_1 \to d$, and $\beta_2 \colon a_2 \otimes b_2 \to d$, a unique group homomorphism $\gamma \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to d$ (using the universal property of the direct sum). In more concrete terms,
$\gamma((x_1, x_2) \otimes (y_1, y_2)) = \alpha_1(x_1 \otimes y_1) + \alpha_2(x_2 \otimes y_1) + \beta_1(x_1 \otimes y_2) + \beta_2(x_2 \otimes y_2)$.

This makes feasible to define the following (functorial) operation on the bilinear maps $(f_1, (a_1, b_1))$ and $(f_2, (a_2, b_2))$ on c by
$(f_1, (a_1, b_1)) \perp (f_2, (a_2, b_2)) = (f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$, where
$f_1 \perp f_2 \colon (a_1 \oplus a_2) \otimes (b_1 \oplus b_2) \to c$ is defined as γ above using
- $\alpha_1 = f_1 \colon a_1 \otimes b_1 \to c$,
- $\alpha_2 = 0 \colon a_2 \otimes b_1 \to c$,
- $\beta_1 = 0 \colon a_1 \otimes b_2 \to c$,
- $\beta_2 = f_2 \colon a_2 \otimes b_2 \to c$.

In concrete terms, $(f_1 \perp f_2)((x_1, x_2) \otimes (y_1, y_2)) = f_1(x_1 \otimes y_1) + f_2(x_2 \otimes y_2)$
(informally speaking, one imposes to a_2, b_1, and also to a_1, b_2, to be "orthogonal" one to the other with respect to $f_1 \perp f_2$).

$\perp$ and non-degeneracy

Proposition

Let $(f_1, (a_1, b_2))$ and $(f_2, (a_2, b_2))$ be two bilinear maps on c.

$\perp$ and non-degeneracy

Proposition

Let $(f_1, (a_1, b_2))$ and $(f_2, (a_2, b_2))$ be two bilinear maps on c.

The bilinear map $(f_1 \perp f_2, (a_1 \oplus a_2, b_1 \oplus b_2))$ is a pairing (respectively, a perfect pairing) if, and only if, $(f_i, (a_i, b_i))$, $i = 1, 2$, are both pairings (respectively, perfect pairings).

Table of contents

1. Introduction
2. Category of pairings
3. A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$
4. Moduli space of pairings
5. Geometric interpretation of the moduli space of pairings
6. Classification of pairings on $\mathbb{Q}/\mathbb{Z}$

Commutative monoid of isomorphic classes of bilinear maps

Of course, being functorial $\perp$ factors through the set of isomorphism classes of bilinear maps, more precisely it gives rise to a structure of monoid on $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$.

Commutative monoid of isomorphic classes of bilinear maps

Of course, being functorial $\perp$ factors through the set of isomorphism classes of bilinear maps, more precisely it gives rise to a structure of monoid on $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$. The unit of this monoid being the isomorphism class of the zero bilinear map $0 \otimes 0 \to c$.

Commutative monoid of isomorphic classes of bilinear maps

Of course, being functorial $\perp$ factors through the set of isomorphism classes of bilinear maps, more precisely it gives rise to a structure of monoid on $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$. The unit of this monoid being the isomorphism class of the zero bilinear map $0 \otimes 0 \to c$.

From the previous proposition, we see that

Commutative monoid of isomorphic classes of bilinear maps

Of course, being functorial $\perp$ factors through the set of isomorphism classes of bilinear maps, more precisely it gives rise to a structure of monoid on $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$. The unit of this monoid being the isomorphism class of the zero bilinear map $0 \otimes 0 \to c$.

From the previous proposition, we see that

$\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c) \subseteq \underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \subseteq \underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$ are inclusions of sub-monoids.

Commutative monoid of isomorphic classes of bilinear maps

Of course, being functorial $\perp$ factors through the set of isomorphism classes of bilinear maps, more precisely it gives rise to a structure of monoid on $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$. The unit of this monoid being the isomorphism class of the zero bilinear map $0 \otimes 0 \to c$.

From the previous proposition, we see that

$\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c) \subseteq \underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c) \subseteq \underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$ are inclusions of sub-monoids.

Definition

We refer to the monoid $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$ to as the moduli space of pairings on c.

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e).

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$).

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$.

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$. An ideal I is a prime ideal if $I \neq M$ and $x \star y \in I$ implies that either $x \in I$ or $y \in I$.

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$. An ideal I is a prime ideal if $I \neq M$ and $x \star y \in I$ implies that either $x \in I$ or $y \in I$.

• Any ideal I of a monoid M gives rise to a monoid with a zero M/I, called the Rees quotient monoid of M by I,

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$. An ideal I is a prime ideal if $I \neq M$ and $x \star y \in I$ implies that either $x \in I$ or $y \in I$.

• Any ideal I of a monoid M gives rise to a monoid with a zero M/I, called the Rees quotient monoid of M by I, and defined by $M/I = (M \setminus I) \sqcup \{ 0 \}$,

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$. An ideal I is a prime ideal if $I \neq M$ and $x \star y \in I$ implies that either $x \in I$ or $y \in I$.

• Any ideal I of a monoid M gives rise to a monoid with a zero M/I, called the Rees quotient monoid of M by I, and defined by $M/I = (M \setminus I) \sqcup \{ 0 \}$, and for every $x, y \in M \setminus I$, $x \cdot y = x \star y$ whenever $x \star y \notin I$, and 0 otherwise (and of course $x \cdot 0 = 0 = 0 \cdot x$, $x \in M/I$).

Some notions about monoids

Let $(M, \star, e)$ be a monoid (i.e., m is an associative binary operation on M with a two-sided unit e). An homomorphism of monoids is a unit-preserving map that "commutes" with the binary operations.

• A monoid with a zero is a monoid together with a distinguished two-sided absorbing element (i.e., $x \star 0 = 0 = 0 \star x$). An homomorphism of monoids with zero is a zero-preserving homomorphism of monoids.

• A subset $I \subseteq M$ of a monoid M is said to be an ideal if $IM \subseteq I \supseteq MI$. An ideal I is a prime ideal if $I \neq M$ and $x \star y \in I$ implies that either $x \in I$ or $y \in I$.

• Any ideal I of a monoid M gives rise to a monoid with a zero M/I, called the Rees quotient monoid of M by I, and defined by $M/I = (M \setminus I) \sqcup \{ 0 \}$, and for every $x, y \in M \setminus I$, $x \cdot y = x \star y$ whenever $x \star y \notin I$, and 0 otherwise (and of course $x \cdot 0 = 0 = 0 \cdot x$, $x \in M/I$). In case I is a prime ideal, then $M \setminus I$ is already a submonoid of M, and M/I is just the monoid $(M \setminus I)^0$, i.e., $M \setminus I$ with a zero 0 freely added.

Back to the monoid of bilinear maps

The previous proposition about preservation of non-degeneracy by $\perp$ also implies that

$\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$,

Back to the monoid of bilinear maps

The previous proposition about preservation of non-degeneracy by $\perp$ also implies that

$\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$,

and

$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c))^{\infty}$.

Back to the monoid of bilinear maps

The previous proposition about preservation of non-degeneracy by $\perp$ also implies that

$\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$,

and

$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c))^{\infty}$.

Also $\underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$

Back to the monoid of bilinear maps

The previous proposition about preservation of non-degeneracy by $\perp$ also implies that

$\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$,

and

$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c))^{\infty}$.

Also $\underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$

and

$\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c))^{\infty}$.

Back to the monoid of bilinear maps

The previous proposition about preservation of non-degeneracy by $\perp$ also implies that

$\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$,

and

$\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Degen}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c))^{\infty}$.

Also $\underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c)$ is a prime ideal of $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$

and

$\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)/\underline{\mathbf{Imp}}_{\mathbf{Abfin}}(c) \cong (\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c))^{\infty}$.

Remark

Everything remains valid if we replace abelian groups for instance by R-modules or by commutative monoids, and **Abfin** by any full sub-category of these.

Table of contents

1 Introduction

2 Category of pairings

3 A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$

4 Moduli space of pairings

5 Geometric interpretation of the moduli space of pairings

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

Bialgebras

Let R be a commutative ring with a unity.

Bialgebras

Let R be a commutative ring with a unity.

An R-algebra A is said to be a coassociative and counital R-bialgebra if it is equipped with two algebra maps $\Delta \colon A \to A \otimes_R A$, and $\epsilon \colon A \to R$, respectively called coproduct and counit which are coassociative and counital.

Bialgebras

Let R be a commutative ring with a unity.

An R-algebra A is said to be a coassociative and counital R-bialgebra if it is equipped with two algebra maps $\Delta\colon A \to A \otimes_R A$, and $\epsilon\colon A \to R$, respectively called coproduct and counit which are coassociative and counital.

This means that the two following diagrams commute.

$$
\begin{array}{ccc}
A & \xrightarrow{\Delta} & A \otimes_R A \\
{\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle id_A \otimes \Delta} \\
A \otimes_R A & \xrightarrow[\Delta \otimes id_A]{} & A \otimes_R A \otimes_R A
\end{array}
\qquad
\begin{array}{ccccc}
R \otimes_R A & \xleftarrow{\epsilon \otimes id_A} & A \otimes_R A & \xrightarrow{id_A \otimes \epsilon} & A \otimes_R R \\
 & {\scriptstyle \cong}\nwarrow & \uparrow{\scriptstyle \Delta} & \nearrow{\scriptstyle \cong} & \\
 & & A & &
\end{array}
\tag{3}
$$

About representable functors

Let **C** be any category, and c be an object of **C**.

About representable functors

Let $\mathbf{C}$ be any category, and c be an object of $\mathbf{C}$. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category $\mathbf{C}$ to the category of sets,

About representable functors

Let $\mathbf{C}$ be any category, and c be an object of $\mathbf{C}$. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category $\mathbf{C}$ to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$,

About representable functors

Let $\mathbf{C}$ be any category, and c be an object of $\mathbf{C}$. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category $\mathbf{C}$ to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$, and that sends any morphism $f \colon d \to d'$ to the map $h^c(f) \colon \mathbf{C}(c, d) \to \mathbf{C}(c, d')$ defined by $g \mapsto f \circ g$.

About representable functors

Let **C** be any category, and c be an object of **C**. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category **C** to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$, and that sends any morphism $f\colon d \to d'$ to the map $h^c(f)\colon \mathbf{C}(c, d) \to \mathbf{C}(c, d')$ defined by $g \mapsto f \circ g$.

• A functor F from **C** to the category of sets is said to be a representable functor if it is isomorphic (in the functor category) to a functor of the form h^c for some object c.

About representable functors

Let $\mathbf{C}$ be any category, and c be an object of $\mathbf{C}$. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category $\mathbf{C}$ to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$, and that sends any morphism $f\colon d \to d'$ to the map $h^c(f)\colon \mathbf{C}(c, d) \to \mathbf{C}(c, d')$ defined by $g \mapsto f \circ g$.

• A functor F from $\mathbf{C}$ to the category of sets is said to be a representable functor if it is isomorphic (in the functor category) to a functor of the form h^c for some object c. This object c is then shown to be unique up to isomorphism, and is called the representing object of F.

About representable functors

Let $\mathbf{C}$ be any category, and c be an object of $\mathbf{C}$. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category $\mathbf{C}$ to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$, and that sends any morphism $f\colon d \to d'$ to the map $h^c(f)\colon \mathbf{C}(c, d) \to \mathbf{C}(c, d')$ defined by $g \mapsto f \circ g$.

• A functor F from $\mathbf{C}$ to the category of sets is said to be a representable functor if it is isomorphic (in the functor category) to a functor of the form h^c for some object c. This object c is then shown to be unique up to isomorphism, and is called the representing object of F.

• A consequence of the Yoneda lemma is that the category of representable functors of $\mathbf{C}$ is equivalent to the opposite category $\mathbf{C}^{\mathbf{op}}$ of $\mathbf{C}$ (any representable functor corresponding to its representing object).

About representable functors

Let **C** be any category, and c be an object of **C**. We define the covariant hom-functor $h^c = \mathbf{C}(c, -)$ from the category **C** to the category of sets, that maps an object d to the set of morphisms $h^c(d) = \mathbf{C}(c, d)$, and that sends any morphism $f \colon d \to d'$ to the map $h^c(f) \colon \mathbf{C}(c, d) \to \mathbf{C}(c, d')$ defined by $g \mapsto f \circ g$.

• A functor F from **C** to the category of sets is said to be a representable functor if it is isomorphic (in the functor category) to a functor of the form h^c for some object c. This object c is then shown to be unique up to isomorphism, and is called the representing object of F.

• A consequence of the Yoneda lemma is that the category of representable functors of **C** is equivalent to the opposite category $\mathbf{C}^{\mathbf{op}}$ of **C** (any representable functor corresponding to its representing object). Recall that $\mathbf{C}^{\mathbf{op}}$ has the same objects and morphisms as **C** but the composition therein is the opposite of that of **C**.

Affine schemes in brief

Let R be any commutative ring with a unity.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R).

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.
When R is an algebraically closed field, and the representing objects are restricted to finitely-generated R-algebras, then representable functors are often called affine algebraic varieties, and if we drop the finiteness assumption, then we obtain pro-affine algebraic varieties.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.
When R is an algebraically closed field, and the representing objects are restricted to finitely-generated R-algebras, then representable functors are often called affine algebraic varieties, and if we drop the finiteness assumption, then we obtain pro-affine algebraic varieties.

• For instance let I be any set, and let us consider the polynomial algebra $R[X_i \colon i \in I]$ in the indeterminates X_i.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.
When R is an algebraically closed field, and the representing objects are restricted to finitely-generated R-algebras, then representable functors are often called affine algebraic varieties, and if we drop the finiteness assumption, then we obtain pro-affine algebraic varieties.

• For instance let I be any set, and let us consider the polynomial algebra $R[X_i : i \in I]$ in the indeterminates X_i. Then, the algebra $R[X_i : i \in I]$ is the representing object of the affine scheme $A \mapsto \mathbf{CAlg}_R(R[X_i : i \in I], A) \cong A^I$ (thus, when I is finite this gives an affine space).

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.
When R is an algebraically closed field, and the representing objects are restricted to finitely-generated R-algebras, then representable functors are often called affine algebraic varieties, and if we drop the finiteness assumption, then we obtain pro-affine algebraic varieties.

• For instance let I be any set, and let us consider the polynomial algebra $R[X_i \colon i \in I]$ in the indeterminates X_i. Then, the algebra $R[X_i \colon i \in I]$ is the representing object of the affine scheme $A \mapsto \mathbf{CAlg}_R(R[X_i \colon i \in I], A) \cong A^I$ (thus, when I is finite this gives an affine space).

• Let R be any algebraically closed field. Let F be an affine scheme with representing object the algebra $\mathcal{O}(F)$.

Affine schemes in brief

Let R be any commutative ring with a unity. Let $\mathbf{CAlg}_R$ be the category of commutative R-algebras with a unity.

• The category of representable functors of $\mathbf{CAlg}_R$ is called the category of affine schemes (on R). It is thus equivalent to $\mathbf{CAlg}_R^{\mathbf{op}}$.
When R is an algebraically closed field, and the representing objects are restricted to finitely-generated R-algebras, then representable functors are often called affine algebraic varieties, and if we drop the finiteness assumption, then we obtain pro-affine algebraic varieties.

• For instance let I be any set, and let us consider the polynomial algebra $R[X_i \colon i \in I]$ in the indeterminates X_i. Then, the algebra $R[X_i \colon i \in I]$ is the representing object of the affine scheme $A \mapsto \mathbf{CAlg}_R(R[X_i \colon i \in I], A) \cong A^I$ (thus, when I is finite this gives an affine space).

• Let R be any algebraically closed field. Let F be an affine scheme with representing object the algebra $\mathcal{O}(F)$. The R-rational points of F are given by $F(R) \cong \mathbf{CAlg}_R(\mathcal{O}(F), R)$.

Monoid schemes

• A monoid scheme M is an affine scheme such that for every algebra A, the set $M(A)$ is a usual monoid, and this naturally in A.

Monoid schemes

• A monoid scheme M is an affine scheme such that for every algebra A, the set $M(A)$ is a usual monoid, and this naturally in A.

• By Yoneda's lemma, this is equivalent to the fact that the representing algebra $\mathcal{O}(M)$ of M is actually a (commutative, unital) coassociative and counital R-bialgebra.

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid.

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid. It is said to be a finite decomposition monoid if its multiplication $\star$ has finite fibers, i.e., for every $x \in M$, there is only finitely many $y, z \in M$ such that $x = y \star z$.

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid. It is said to be a finite decomposition monoid if its multiplication $\star$ has finite fibers, i.e., for every $x \in M$, there is only finitely many $y, z \in M$ such that $x = y \star z$.

If M is a finite decomposition monoid, and A is a commutative R-algebra with a unit, then A^M is provided with a structure of a R-algebra (and even of A-algebra),

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid. It is said to be a finite decomposition monoid if its multiplication $\star$ has finite fibers, i.e., for every $x \in M$, there is only finitely many $y, z \in M$ such that $x = y \star z$.

If M is a finite decomposition monoid, and A is a commutative R-algebra with a unit, then A^M is provided with a structure of a R-algebra (and even of A-algebra), which is commutative if, and only if, M is,

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid. It is said to be a finite decomposition monoid if its multiplication $\star$ has finite fibers, i.e., for every $x \in M$, there is only finitely many $y, z \in M$ such that $x = y \star z$.

If M is a finite decomposition monoid, and A is a commutative R-algebra with a unit, then A^M is provided with a structure of a R-algebra (and even of A-algebra), which is commutative if, and only if, M is, and with multiplication given by

$$(fg)(x) = \sum_{yz=x} f(y)g(z)$$

for $f, g \in A^M$, $x \in M$.

Finite decomposition monoids

Let $(M, \star, e)$ be a monoid. It is said to be a finite decomposition monoid if its multiplication $\star$ has finite fibers, i.e., for every $x \in M$, there is only finitely many $y, z \in M$ such that $x = y \star z$.

If M is a finite decomposition monoid, and A is a commutative R-algebra with a unit, then A^M is provided with a structure of a R-algebra (and even of A-algebra), which is commutative if, and only if, M is, and with multiplication given by

$$(fg)(x) = \sum_{yz=x} f(y)g(z)$$

for $f, g \in A^M$, $x \in M$. This algebra is denoted by $A[[M]]$ and is called the large algebra of M.

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x\colon x \in M]$;

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x \colon x \in M]$;
- $R[X_x \colon x \in M]$ is a coassociative and counital bialgebra, so that $(-)[[M]]$ is a monoid scheme;

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x\colon x \in M]$;
- $R[X_x\colon x \in M]$ is a coassociative and counital bialgebra, so that $(-)[[M]]$ is a monoid scheme;
- M embeds as a sub-monoid into the underlying multiplicative monoid of $R[[M]]$.

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x\colon x \in M]$;
- $R[X_x\colon x \in M]$ is a coassociative and counital bialgebra, so that $(-)[[M]]$ is a monoid scheme;
- M embeds as a sub-monoid into the underlying multiplicative monoid of $R[[M]]$.

Proof: The map $X_x \to \Delta(X_x) = \sum_{yz=x} X_y \otimes X_z$ extends uniquely to an algebra map from $R[X_x\colon x \in M] \to R[X_x\colon x \in M] \otimes_R R[X_x\colon x\colon x \in M]$,

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x\colon x \in M]$;
- $R[X_x\colon x \in M]$ is a coassociative and counital bialgebra, so that $(-)[[M]]$ is a monoid scheme;
- M embeds as a sub-monoid into the underlying multiplicative monoid of $R[[M]]$.

Proof: The map $X_x \to \Delta(X_x) = \sum_{yz=x} X_y \otimes X_z$ extends uniquely to an algebra map from $R[X_x\colon x \in M] \to R[X_x\colon x \in M] \otimes_R R[X_x\colon x\colon x \in M]$, and turns to be a coassociative coproduct.

Finite decomposition monoids (cont'd)

Theorem

For every finite decomposition monoid M,

- $(-)[[M]]\colon A \mapsto A[[M]]$ defines a functor from $\mathbf{CAlg}_R$ to the category of sets;
- It is representable with representing algebra $R[X_x\colon x \in M]$;
- $R[X_x\colon x \in M]$ is a coassociative and counital bialgebra, so that $(-)[[M]]$ is a monoid scheme;
- M embeds as a sub-monoid into the underlying multiplicative monoid of $R[[M]]$.

Proof: The map $X_x \to \Delta(X_x) = \sum_{yz=x} X_y \otimes X_z$ extends uniquely to an algebra map from $R[X_x\colon x \in M] \to R[X_x\colon x \in M] \otimes_R R[X_x\colon x\colon x \in M]$, and turns to be a coassociative coproduct. The map $X_x \mapsto \epsilon(X_x) = 1$ provides the counit. □

What about the moduli space of pairings ?

Let us denote by $|a|$ the order of a finite abelian group a.

What about the moduli space of pairings ?

Let us denote by $|a|$ the order of a finite abelian group a.

The isomorphism relation of bilinear maps $(f,(a,b)) \cong (g,(d,e))$ on c implies that $a \cong d$ and $b \cong e$ (isomorphic groups), and thus $|a| = |d|$ and $|b| = |e|$.

What about the moduli space of pairings ?

Let us denote by $|a|$ the order of a finite abelian group a.

The isomorphism relation of bilinear maps $(f,(a,b)) \cong (g,(d,e))$ on c implies that $a \cong d$ and $b \cong e$ (isomorphic groups), and thus $|a| = |d|$ and $|b| = |e|$.

Since $|a \oplus b| = |a||b|$ and $|0| = 1$, we obtain a well-defined homomorphism of monoids $s\colon \underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c) \to \mathbb{N}^* \times \mathbb{N}^*$ given by $s([f,(a,b)]) = (|a|,|b|)$, where $[f,(a,b)]$ is the isomorphism class of $(f,(a,b))$.

What about the moduli space of pairings ?

Let us denote by $|a|$ the order of a finite abelian group a.

The isomorphism relation of bilinear maps $(f,(a,b)) \cong (g,(d,e))$ on c implies that $a \cong d$ and $b \cong e$ (isomorphic groups), and thus $|a| = |d|$ and $|b| = |e|$.

Since $|a \oplus b| = |a||b|$ and $|0| = 1$, we obtain a well-defined homomorphism of monoids $s\colon \underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c) \to \mathbb{N}^* \times \mathbb{N}^*$ given by $s([f,(a,b)]) = (|a|,|b|)$, where $[f,(a,b)]$ is the isomorphism class of $(f,(a,b))$.

It follows that $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$ is a finite decomposition monoid, and thus also are $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$ and $\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c)$.

What about the moduli space of pairings ?

Let us denote by $|a|$ the order of a finite abelian group a.

The isomorphism relation of bilinear maps $(f,(a,b)) \cong (g,(d,e))$ on c implies that $a \cong d$ and $b \cong e$ (isomorphic groups), and thus $|a| = |d|$ and $|b| = |e|$.

Since $|a \oplus b| = |a||b|$ and $|0| = 1$, we obtain a well-defined homomorphism of monoids $s\colon \underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c) \to \mathbb{N}^* \times \mathbb{N}^*$ given by $s([f,(a,b)]) = (|a|,|b|)$, where $[f,(a,b)]$ is the isomorphism class of $(f,(a,b))$.

It follows that $\underline{\mathbf{Bil}}_{\mathbf{Abfin}}(c)$ is a finite decomposition monoid, and thus also are $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(c)$ and $\underline{\mathbf{Perf}}_{\mathbf{Abfin}}(c)$.

According to the previous theorem, if R is an algebraically closed field, then the moduli space of pairings is a sub-monoid of the R-rational points of an affine monoid scheme.

Table of contents

1. Introduction
2. Category of pairings
3. A symmetric monoidal structure on $\mathbf{Bil}_{\mathbf{Abfin}}(c)$
4. Moduli space of pairings
5. Geometric interpretation of the moduli space of pairings
6. Classification of pairings on $\mathbb{Q}/\mathbb{Z}$

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b}$

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b$

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a}$

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$,

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$, so that $a \cong b$, and $(f, (a, b))$ is a perfect pairing.

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$, so that $a \cong b$, and $(f, (a, b))$ is a perfect pairing. We thus obtain

Lemma

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

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$, so that $a \cong b$, and $(f, (a, b))$ is a perfect pairing. We thus obtain

Lemma

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

Remark

This equality may be false when $c \neq \mathbb{Q}/\mathbb{Z}$ (or more precisely when $c \not\subseteq \mathbb{Q}/\mathbb{Z}$).

Now, let us assume that $c = \mathbb{Q}/\mathbb{Z}$.

Let a be a finite abelian group, and let us denote by $\hat{a} = \mathbf{Ab}(a, \mathbb{Q}/\mathbb{Z})$ its dual (or character) group.

It is well-known that $a \cong \hat{a}$.

Let $(f, (a, b))$ be an object of $\mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$. Then, $a \hookrightarrow \hat{b} \cong b \hookrightarrow \hat{a} \cong a$, so that $a \cong b$, and $(f, (a, b))$ is a perfect pairing. We thus obtain

Lemma

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

Remark

This equality may be false when $c \neq \mathbb{Q}/\mathbb{Z}$ (or more precisely when $c \not\subseteq \mathbb{Q}/\mathbb{Z}$). For instance, le p be a prime number, and $m > 1$, then $f\colon (\mathbb{Z}/p\mathbb{Z})^m \times \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^m$ given by $f((x_i \bmod p)_{i=1}^m, y \bmod p) = (x_i y \bmod p)_{i=1}^m$ is an imperfect pairing.

The duality pairing

Let a be a finite abelian group.

The duality pairing

Let a be a finite abelian group. The duality pairing on a is $(\mathbf{nat}_a, (a, \hat{a}))$ given by $\mathbf{nat}_a(x \otimes \chi) = \chi(x)$ for $x \in a$, $\chi \in \hat{a}$.

The duality pairing

Let a be a finite abelian group. The duality pairing on a is $(\mathbf{nat}_a, (a, \hat{a}))$ given by $\mathbf{nat}_a(x \otimes \chi) = \chi(x)$ for $x \in a$, $\chi \in \hat{a}$.

Theorem

Let $(f, (a, b))$ be a pairing on $\mathbb{Q}/\mathbb{Z}$. Then,

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

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g\colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g\colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Let us define a third perfect pairing $h = g \circ (id_a \otimes \delta_g^{-1})$, isomorphic to g (and of course to f).

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha \colon b \to a$.

Let us define a bi-additive map $g_0 \colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g \colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g \colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Let us define a third perfect pairing $h = g \circ (id_a \otimes \delta_g^{-1})$, isomorphic to g (and of course to f).

We have for every $x \in a$, and $\chi \in \hat{a}$,
$h(x \otimes \chi) = g(x \otimes \delta_g^{-1}(\chi))$

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x,y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g\colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Let us define a third perfect pairing $h = g \circ (id_a \otimes \delta_g^{-1})$, isomorphic to g (and of course to f).

We have for every $x \in a$, and $\chi \in \hat{a}$,
$h(x \otimes \chi) = g(x \otimes \delta_g^{-1}(\chi)) = \delta_g(\delta_g^{-1}(\chi))(x)$

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x,y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g\colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Let us define a third perfect pairing $h = g \circ (id_a \otimes \delta_g^{-1})$, isomorphic to g (and of course to f).

We have for every $x \in a$, and $\chi \in \hat{a}$,
$h(x \otimes \chi) = g(x \otimes \delta_g^{-1}(\chi)) = \delta_g(\delta_g^{-1}(\chi))(x) = \chi(x)$

Proof

Since $a \cong b$, we may choose an isomorphism $\alpha\colon b \to a$.

Let us define a bi-additive map $g_0\colon a \times a \to \mathbb{Q}/\mathbb{Z}$ by $g_0(x, y) = f(x \otimes \alpha^{-1}(y))$, $x, y \in a$, and let us denote by $g\colon a \otimes a \to \mathbb{Q}/\mathbb{Z}$ the corresponding group homomorphism.

Both bilinear maps f and g are isomorphic, and thus g also is a perfect pairing.

In particular, $\delta_g\colon a \to \hat{a}$, $x \mapsto g_0(\cdot, x)$, is an isomorphism from a to $\hat{a}$.

Let us define a third perfect pairing $h = g \circ (id_a \otimes \delta_g^{-1})$, isomorphic to g (and of course to f).

We have for every $x \in a$, and $\chi \in \hat{a}$,
$h(x \otimes \chi) = g(x \otimes \delta_g^{-1}(\chi)) = \delta_g(\delta_g^{-1}(\chi))(x) = \chi(x) = \mathbf{nat}_a(x \otimes \chi)$. □

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$,

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that
$(\mathbf{nat}_{a \oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a})) \perp (\mathbf{nat}_b, (b, \hat{b}))$.

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that
$(\mathbf{nat}_{a \oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a})) \perp (\mathbf{nat}_b, (b, \hat{b}))$.

Corollary

The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ is the free commutative monoid generated by all the (p, i)'s, where p is a prime number, and $i \in \mathbb{N}^*$.

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that
$(\mathbf{nat}_{a\oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a}))\perp(\mathbf{nat}_b, (b, \hat{b}))$.

Corollary

The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ is the free commutative monoid generated by all the (p, i)'s, where p is a prime number, and $i \in \mathbb{N}^*$.

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

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that
$(\mathbf{nat}_{a\oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a}))\perp(\mathbf{nat}_b, (b, \hat{b}))$.

Corollary

The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ is the free commutative monoid generated by all the (p, i)'s, where p is a prime number, and $i \in \mathbb{N}^*$.

Let p be a prime number, and let $\mathbb{Z}(p^\infty)$ be the Prüfer p-group, i.e., the direct limit $0 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \cdots$ Let ${}_p\mathbf{Abfin}$ be the category of finite abelian p-groups.

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that $(\mathbf{nat}_{a\oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a})) \perp (\mathbf{nat}_b, (b, \hat{b}))$.

Corollary

The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ is the free commutative monoid generated by all the (p, i)'s, where p is a prime number, and $i \in \mathbb{N}^*$.

Let p be a prime number, and let $\mathbb{Z}(p^\infty)$ be the Prüfer p-group, i.e., the direct limit $0 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \cdots$ Let ${}_p\mathbf{Abfin}$ be the category of finite abelian p-groups. Then, $\mathbf{Pair}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty)) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ (full embedding of categories).

Consequences

We have $\widehat{(a \oplus b)} \cong \hat{a} \oplus \hat{b}$, so it follows that $(\mathbf{nat}_{a\oplus b}, (a \oplus b, \widehat{(a \oplus b)})) \cong (\mathbf{nat}_a, (a, \hat{a}))\perp(\mathbf{nat}_b, (b, \hat{b}))$.

Corollary

The moduli space of pairings $\underline{\mathbf{Pair}}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ is the free commutative monoid generated by all the (p, i)'s, where p is a prime number, and $i \in \mathbb{N}^*$.

Let p be a prime number, and let $\mathbb{Z}(p^\infty)$ be the Prüfer p-group, i.e., the direct limit $0 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \cdots$ Let ${}_p\mathbf{Abfin}$ be the category of finite abelian p-groups. Then, $\mathbf{Pair}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty)) \hookrightarrow \mathbf{Pair}_{\mathbf{Abfin}}(\mathbb{Q}/\mathbb{Z})$ (full embedding of categories).

Corollary

The monoid $\underline{\mathbf{Pair}}_{{}_p\mathbf{Abfin}}(\mathbb{Z}(p^\infty))$ is free (as a commutative monoid) with basis $\mathbb{N}^*$.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a,

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x)$

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y)$

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y))$

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y)) = -g(\alpha(y),\alpha(x))$.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y)) = -g(\alpha(y),\alpha(x))$.

Let $p > 2$ be a prime number, and let $f_+, f_-\colon (\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$ given by $f_\star((x_1,x_2),(x_3,x_4)) = x_1x_4 \star x_2x_3$, $\star \in \{\pm\}$.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y)) = -g(\alpha(y),\alpha(x))$.

Let $p > 2$ be a prime number, and let $f_+, f_-\colon (\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$ given by $f_\star((x_1,x_2),(x_3,x_4)) = x_1x_4 \star x_2x_3$, $\star \in \{\pm\}$. We observe that f_+ is symmetric, while f_- is skew-symmetric.

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x,y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y)) = -g(\alpha(y),\alpha(x))$.

Let $p > 2$ be a prime number, and let $f_+, f_-\colon (\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$ given by $f_\star((x_1,x_2),(x_3,x_4)) = x_1x_4 \star x_2x_3$, $\star \in \{\pm\}$. We observe that f_+ is symmetric, while f_- is skew-symmetric. Thus they cannot be equivalent mod $\equiv$,

Why is the classification so simple ?

This is because the isomorphism relation identifies too many objects, and much more than C.T.C Wall's equivalence relation.

Recall that C.T.C Wall considers pairings on $\mathbb{Q}/\mathbb{Z}$ and his equivalence relation to classify them is the following $(f,(a,a)) \equiv (g,(b,b))$ if, and only if, there is an isomorphism $\alpha\colon a \to b$ such that $f(x,y) = g(\alpha(x),\alpha(y))$, $x, y \in a$.

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 modulo $\equiv$. Indeed, if $f(x,y) = g(\alpha(x),\alpha(y))$ for an automorphism α of a, then
$g(\alpha(y),\alpha(x)) = f(y,x) = f(x,y) = g(\alpha(x),\alpha(y)) = -g(\alpha(y),\alpha(x))$.

Let $p > 2$ be a prime number, and let $f_+, f_-\colon (\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$ given by $f_\star((x_1,x_2),(x_3,x_4)) = x_1x_4 \star x_2x_3$, $\star \in \{\pm\}$. We observe that f_+ is symmetric, while f_- is skew-symmetric. Thus they cannot be equivalent mod $\equiv$, while they are isomorphic (take $\alpha = id$, and $\beta(x,y) = (-x,y)$ so that $f_+((x_1,x_2),(x_3,x_4)) = f_-(\alpha(x_1,x_2),\beta(x_3,x_4)))$.

To conclude

When $c = \mathbb{Q}/\mathbb{Z}$, the classification of pairings is achieved (there is a one-one correspondence between isomorphic classes of finite abelian groups and isomorphic classes of pairings).

To conclude

When $c = \mathbb{Q}/\mathbb{Z}$, the classification of pairings is achieved (there is a one-one correspondence between isomorphic classes of finite abelian groups and isomorphic classes of pairings).

To obtain more isomorphic classes we must

To conclude

When $c = \mathbb{Q}/\mathbb{Z}$, the classification of pairings is achieved (there is a one-one correspondence between isomorphic classes of finite abelian groups and isomorphic classes of pairings).

To obtain more isomorphic classes we must

- either consider other choices for c, for instance a finite non-cyclic abelian group (in the case c is finite, it may be proved that $f : a \otimes b \to c$ is a pairing, then a and b share the same exponent).

To conclude

When $c = \mathbb{Q}/\mathbb{Z}$, the classification of pairings is achieved (there is a one-one correspondence between isomorphic classes of finite abelian groups and isomorphic classes of pairings).

To obtain more isomorphic classes we must

- either consider other choices for c, for instance a finite non-cyclic abelian group (in the case c is finite, it may be proved that $f: a \otimes b \to c$ is a pairing, then a and b share the same exponent).

- or consider the category of finite commutative monoids in which we should have a richer structure for the moduli space of pairings since there is no dualizable object such as $\mathbb{Q}/\mathbb{Z}$.