Elementary group-theoretic approach to pairings*

Nadia EL Mrabet[1] and Laurent Poinsot[2,3]

1 **SAS-CMP, École des Mines, 13120 Gardanne, France**
`nadia.el-mrabet@emse.fr`

2 **LIPN, CNRS (UMR 7030), University Paris 13, Sorbonne Paris Cité, 93140 Villetaneuse, France**

3 **Secondary adress: CReA, French Air Force Academy, Base aérienne 701, 13361 Salon de Provence, France**
`laurent.poinsot@lipn.univ-paris13.fr`

Abstract

Pairing-based cryptography offers an interesting option for the development of new protocols. In practice the pairings are defined over elliptic curves. This contribution is an analysis of these objects in a more general setting. A pair of finite abelian groups is called "pairing admissible" if there exists a non-degenerate bilinear map, called a "pairing", from the product of these groups to a third one. Using some elementary group-theory, as a main result is proved that two abelian groups are pairing admissible if, and only if, the canonical bilinear map to their tensor product is itself a pairing, if and only if, they share the same exponent. One also observes that being pairing admissible is an equivalence relation among the class of all finite abelian groups, and one proves that the corresponding quotient set admits a structure of a semilattice isomorphic to that of positive integers under divisibility.

Mathematics Subject Classification (2010) 20K01, 15A69, 11E39

1998 ACM Subject Classification G.2 Discrete Mathematics, E.3 Data Encryption

Keywords and phrases Pairing, finite abelian group, tensor product, primary decomposition.

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

A pairing $f\colon A \times B \to C$, where A, B, C, are finite abelian groups, is a non-degenerate bilinear map (see Section 2). In this case one says that A and B are pairing admissible (i.e., there exists a pairing with domain $A \times B$).

Such objects are well-known in cryptography and were used in order to solve the discrete logarithm problem [12]. The pairings were later used as a fundamental ingredient of the tripartite Diffie-Hellman key exchange [7]. Nowadays, pairings are essentially used for identity-based cryptography [4] or to provide short signature schemes [8]. Due to this origin, many known constructions, such as the Weil and Tate pairings, of cryptographic pairings are based on elliptic curves [14]. In [9] is presented a new attack against the discrete logarithm for elliptic curves and revealed a security weakness of pairings over some particular kind of elliptic curves (those with embedding degree a multiple of 6). According to this attack, we are left with an alternative: either increasing the security level for pairings over elliptic curves (increasing the bit size of the groups involved), to the detriment of efficiency, or finding and studying new constructions, outside the realm of elliptic curves. We believe this is the right

[*] One of the authors, Nadia El Mrabet, wishes to acknowledge support from French project ANR INS 2012 SIMPATIC.

time to make a first step in the second direction (see also [10] where a pairing on Theta functions is presented) because new attacks such as the aforementioned are still possible.

Pairings are group-theoretic objects, and as such may be studied using tools from group theory. This is the point of view adopted here. In this work we are interested in the pairing admissibility relation rather than in pairings themselves. The main purpose is thus to provide a complete description of the conditions under which two finite abelian groups may be paired because it is mandatory in order to find new constructions. Such a characterization is provided in terms of the exponent of the groups, and rests on a series of elementary results from group-theory. More precisely it is proved that two finite abelian groups are pairing admissible if, and only if, they share the same exponent. Such a description makes explicit the fact that pairing admissibility is actually an equivalence relation, compatible with the direct sum. As a second main result it is shown that the quotient set under the above relation is isomorphic to the join semilattice of positive integers under divisibility.

In Section 2, one recalls the definition of a pairing. Section 3 is a recollection of well-known results on the structure of finite abelian groups and on the exponent of a finite abelian group and its properties. There is nothing really new in this section, except perhaps Theorem 4, which describes the usual primary decomposition of finite abelian groups as an equivalence of categories. But rather than appealing to some general theories one prefers providing elementary results – which are sufficient to the work presented here – which are put together in this section for the reader's convenience. Section 4 concerns the tensor product of (finite) abelian groups, which is an essential tool to study pairings. Section 5 contains our main results: Theorem 12 describes the primary decomposition of a pairing, Proposition 13 establishes an equivalence between pairing admissibility and non-degeneracy of the canonical bilinear map to the tensor product of two groups, Theorem 16 provides another characterization of pairing admissibility by means of the exponents of the groups under considerations, in Theorem 18 is proved that the set of finite abelian groups up to pairing admissibility forms a semilattice isomorphic to the join semilattice of positive integers under divisibility, and finally a group structure on pairings over cyclic groups is provided in Theorem 19.

2 Pairings

Let us begin with the definition of the central object of this contribution. Let $f\colon X \times Y \to Z$ be any set-theoretic map. For any $x \in X$, we define the map $f(x,\cdot)\colon X \to Z$ by $y \mapsto f(x,y)$, and symmetrically, for any $y \in Y$ is defined $f(\cdot,y)\colon Y \to Z$ by $x \mapsto f(x,y)$.

Let A, B, C be abelian groups. A set-theoretic map $f\colon A \times B \to C$ is said to be *bilinear* (or *bi-additive*) if for every $a \in A$, and every $b \in B$, the maps $f(a,\cdot)\colon B \to C$ and $f(\cdot,b)\colon A \to C$ are homomorphisms of groups. The set of all bilinear maps from $A \times B$ to C is denoted by $\mathcal{B}il(A \times B, C)$.

One of the main feature of a pairing is the notion of non-degeneracy. Let A, B, C be abelian groups. Let $f \in \mathcal{B}il(A \times B, C)$. The map f is said to be *left non-degenerate* if, for each $a \in A$, the map $f(a,\cdot)$ is one-to-one. In other terms this means that if for every $b \in B$, $f(a,b) = 0$, then $a = 0$. The notion of *right non-degeneracy* is the evident symmetric one, while we say that a bilinear map f is *non-degenerate* whenever it is both left and right non-degenerate. The map f is said to be (left, right) *degenerate* if it is not (left, right) non-degenerate.

▶ **Definition 1.** Given finite abelian groups A, B, C, a bilinear map $f\colon A \times B \to C$ is a *pairing* if it is non-degenerate.

One sometimes uses the traditional “bracket” notation $\langle \cdot \mid \cdot \rangle$ to denote a pairing.

▶ **Definition 2.** A pair of finite abelian groups (A, B) is said to be *pairing admissible* if there exists a pairing with domain $A \times B$, or, in other words, if there are a finite abelian group C and a pairing $f \colon A \times B \to C$.

▶ **Example 3.** Let $1 \to A \to G \to B \to 1$ be a short exact sequence of groups, where A, B are abelian groups, and A lies in the center $Z(G)$ of G (*i.e.*, G is a central extension of abelian groups). Let $[g, h] = ghg^{-1}h^{-1}$ be the commutator of $g, h \in G$. According to [3, p. 358], $[\cdot, \cdot]$ factors to the quotient as a bilinear map $[\cdot, \cdot] \colon B \times B \to A$, and it is non-degenerate if, and only if, $A = Z(G)$, so that we obtain a pairing $[\cdot, \cdot] \colon G/Z(G) \times G/Z(G) \to Z(G)$ (if $G/Z(G)$ is abelian).

3 A glance at the structure of finite abelian groups

This section contains known results about the structure of finite abelian groups and about the exponent of a group – results which are used in an essential way hereafter – put together for the reader’s convenience. We do not claim to any originality here, since the results may be recovered from more general theories, however, at least to our taste, this “pedestrian” approach seems more appropriate for our purposes. Of course one only provides proofs for those results which, to our knowledge, are not stated in the same form in the literature, even if they follow from more sophisticated techniques.

3.1 Primary components

Let us fix some notations used in what follows. Given a category [11] $\mathbf{C}$, and two objects c, d of this category, $\mathbf{C}(c, d)$ denotes the set of all morphisms from c to d. The categories of interest are here $\mathcal{Ab}$, and $\mathcal{Abfin}$, the category of all abelian groups, and of the finite ones respectively (with homomorphism of groups as morphisms).

$\mathbb{Z}_n$ denotes the cyclic group of order n, and 0 stands for the trivial group. Let $\mathbb{P}$ be the set of all prime numbers. For $p \in \mathbb{P}$, a *p-group* is a group all of whose elements have orders a power of p. The full sub-category of $\mathcal{Abfin}$ spanned by the p-groups is denoted by ${}_p\mathcal{Abfin}$.

The order $o(A)$ of a finite abelian p-group is of course a power of p. Given an abelian group A, and $p \in \mathbb{P}$, let $A[p] := \{\, x \in A \colon o(x) = p^n \text{ for some } n \,\}$. It is rather clear that $A[p]$ is a p-group. If A is a finite abelian group, then $A \simeq \bigoplus_{p\in\mathbb{P}} A[p]$ (this is a finite direct sum since for all but finitely many primes p, $A[p] \simeq 0$). This decomposition is referred to as the *primary component decomposition* of A, and the $A[p]$’s are called the *primary components* of A.

It is not difficult to see that if B is a subgroup of A which is a p-group, then B is a subgroup of $A[p]$, and also that $o(A[p])$ is the power of p that occurs in the factorization of $o(A)$. The decomposition into primary component is unique in a “strong sense” (see [15]): If A is a finite abelian group, $A \simeq \bigoplus_{p\in\mathbb{P}} H(p)$, and each $H(p)$ is a p-group, then each $H(p) \simeq A[p]$. It then follows easily that two finite abelian groups are isomorphic, if and only if, they have isomorphic primary components.

3.2 A category-theoretic recasting of the primary component decomposition

The decomposition into primary components is actually the object part of a natural equivalence which we now explain. Let A be any finite abelian group, and let $A \simeq \bigoplus_{p\in\mathbb{P}} A[p]$ be its decomposition into primary components (recall here that there are only finitely many primes p such that $A[p] \not\simeq 0$, hence it is a usual finite direct sum).

With the projection $\pi_p^A \colon A \to A[p]$ and the canonical inclusion $q_p^A \colon A[p] \hookrightarrow A$, $p \in \mathbb{P}$, any member x of A may be written as $x = \sum_{p\in\mathbb{P}} q_p^A(\pi_p^A(x))$ (this is an algebraic sum because, once again, there are only finitely many p with $\pi_p^A(x) \neq 0$).

It is clear that for any prime numbers p, q, and for any finite abelian p-group A and q-group B, $\mathcal{Abfin}(A, B) = 0$ whenever $p \neq q$ (indeed, $o(x) = p^i$, so that $p^i f(x) = f(p^i x) = 0$, but $o(f(x)) = q^j$, thus q^j divides p^i), and for every $f \in \mathcal{Abfin}(A, B)$, $f(A[p]) \subseteq B[p]$ for the same reason (indeed, let us assume to the contrary that for some $x \in A[p]$, $f(x) \notin B[p]$, thus there exists at least a prime $q \neq p$ such that $\pi_q^B(f(x)) \neq 0$, otherwise $f(x)$ would be equal to 0, and, as such, be a member of $B[p]$, it then follows that $\pi_q^B \circ f \circ q_p^A \colon A[p] \to B[q]$ is a non-zero group homomorphism, which provides a contradiction).

It then follows that $\mathcal{Abfin}(A, B) \simeq \bigoplus_{p\in\mathbb{P}} \mathcal{Abfin}(A[p], B[p])$. Moreover for each p, the set $\mathcal{Abfin}(A[p], B[p])$ is a finite abelian group, and because for $n = \max\{\, i \in \mathbb{N} \colon \forall x \in A[p],\ p^i x = 0 \,\}$, $p^n f = 0$, it follows that $o(f)$ is a power of p, therefore $\mathcal{Abfin}(A[p], B[p])$ is itself a finite abelian p-group.

According to the "strong uniqueness" property of the primary decomposition applied to $\mathcal{Abfin}(A, B)$, we see that for each prime p, $\mathcal{Abfin}(A, B)[p] \simeq \mathcal{Abfin}(A[p], B[p])$.

Now let us consider the category $\bigoplus_{p\in\mathbb{P}} {}_p\mathcal{Abfin}$ whose objects are families $(A_p)_{p\in\mathbb{P}}$ where A_p is a finite abelian p-group for each p, and for only finitely many p, $A_p \not\simeq 0$, and whose morphisms $f \colon (A_p)_p \to (B_p)_p$ are just sequences of homomorphisms $(f_p)_{p\in\mathbb{P}}$ with $f_p \in \mathcal{Ab}(A_p, B_p)$, $p \in \mathbb{P}$. The composition being the obvious one. Let $\mathbf{Prim} \colon \mathcal{Abfin} \to \bigoplus_p \mathcal{Abfin}$ be the functor defined by $\mathbf{Prim}(A) = (A[p])_{p\in\mathbb{P}}$, and for each $f \in \mathcal{Ab}(A, B)$, $\mathbf{Prim}(f) = (f_p)_p \colon (A[p])_p \to (B[p])_p$ is given by $f_p = \pi_p^B \circ f \circ q_p^A$. A direct consequence of the primary decomposition theorem is the following.

▶ **Theorem 4.** *The functor* $\mathbf{Prim}$ *is an equivalence of categories.*

Proof. $\mathbf{Prim}$ is of course a functor. It is full and faithful: let A, B be two finite abelian groups, and let $f_p \colon A[p] \to B[p]$ for every prime p (thus there are only finitely many p such that $f_p \neq 0$). Then, by universality of the biproduct (see [11]), there is a unique homomorphism $f \colon A \to B$ such that for every prime p, $\pi_p^B \circ f \circ q_p^A = f$. $\mathbf{Prim}$ is essentially surjective: let $(A(p))_p$ be an object of $\bigoplus_{p\in\mathbb{P}} {}_p\mathcal{Abfin}$. Thus $A(p) \not\simeq 0$ for only finitely many prime p. Now, $\mathbf{Prim}(\bigoplus_p A(p)) \simeq (A(p))_p$. Thus, $\mathbf{Prim}$ yields an equivalence of category. ◀

3.3 Lattice-theoretic properties of the least common multiple

A good reference for the notion recalled below is [1]. Let $(L, \vee)$ be a join semilattice. Then, for each finite non void subset E of L, $\bigvee E := \sup E$ exists, and may be computed as follows by induction on the cardinality of E. If $|E| = 1$, then $\bigvee E = e$ for the unique member e of E, and if $|E| = n + 1$, $n \geq 1$, $\bigvee E = (\bigvee(E \setminus \{\, e \,\})) \vee e$ (this does not depend on the chosen member e of E). If $E = \bigcup_{i\in I} E_i$, where $I \neq \emptyset$ and finite, and each E_i is a finite non void set of L (so is E), one has

$$\bigvee E = \bigvee\{\, \bigvee E_i \colon i \in I \,\}.$$

This equality is referred to as the *general associativity property* of $\vee$. If, furthermore, L admits a bottom element $\perp$, then $\bigvee \emptyset = \perp$ (and one can extend the above property for the empty family).

One also recalls that the set $\mathbb{N}_+ := \mathbb{N} \setminus \{\, 0 \,\}$ of all positive natural integers becomes a lattice, with bottom element 1, under the divisibility relation in which the least common multiple lcm is the join operation and the greatest common divisor gcd is the meet operation. In particular, the general associativity property holds for lcm (and also for gcd). In what follows if $E = \{ k_i \colon i \in I \}$ is any finite subset of $\mathbb{N}_+$ (I is finite), one denotes $\bigvee E$ by $\mathrm{lcm}(k_i \colon i \in I)$. (One has $\mathrm{lcm}(\emptyset) = 1$.)

3.4 Around the exponent

The *exponent* of a group G is the smallest positive integer n such that $nx = 0$ for all $x \in G$ if such an n exists. It is denoted by $\mathit{exp}(G)$. This quantity is fundamental for subsequent developments.

▶ **Theorem 5.** *[13, Theorem 2.13, p. 29] If A is a finite abelian group, then $\mathit{exp}(A)$ exists and is the least common multiple of the orders of elements of A, and A is cyclic if, and only if, $\mathit{exp}(A) = o(A)$.*

▶ Remark. If A, B are two isomorphic finite abelian groups, then $\mathit{exp}(A) = \mathit{exp}(B)$.

▶ **Lemma 6.** *For every finite abelian group A, $\mathit{exp}(A) = \prod_{p\in\mathbb{P}} \mathit{exp}(A[p])$. In particular, for every finite abelian groups A, B, $\mathit{exp}(A) = \mathit{exp}(B)$ if, and only if, for each prime p, $\mathit{exp}(A[p]) = \mathit{exp}(B[p])$.*

Proof. Let A be a finite abelian p-group. Then, $\mathit{exp}(A)$ is a power of p. Since there are only finitely many primes p such that $A[p] \not\simeq 0$, it follows that $\prod_{p\in\mathbb{P}} \mathit{exp}(A[p])$ is a natural integer. Then of course, $\prod_{p\in\mathbb{P}} \mathit{exp}(A[p])$ is itself the least common multiple of $(\mathit{exp}(A[p]))_{p\in\mathbb{P}}$. But each $\mathit{exp}(A[p])$ is the least common multiple of the orders of elements of $A[p]$, so that $\prod_{p\in\mathbb{P}} \mathit{exp}(A[p])$ becomes the least common multiple of the orders of the elements of A by the general associativity property, and thus it is equal to $\mathit{exp}(A)$. The second assertion is obvious because $\prod_{p\in\mathbb{P}} \mathit{exp}(A[p])$ is the prime factor decomposition of $\mathit{exp}(A)$. ◀

There is another useful decomposition of finite abelian groups.

▶ **Theorem 7.** *[16, p. 336] Let A be a finite abelian group. Then,*

$$A \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_\ell}, \tag{1}$$

where either $A \simeq 0$ in such a way that $\ell = 1$, and $n_1 = 1$, or $A \not\simeq 0$, and $n_1 \neq 1$, and for $i = 1, \cdots, \ell - 1$, $n_i \mid n_{i+1}$. The numbers $\ell, n_1, \cdots, n_\ell$ are uniquely determined by A, and are called the invariant factors *of A, $(\ell, n_1, \cdots, n_\ell)$ is the* invariant factor list *of A, while the decomposition given in equation (1) is referred to as the* invariant factor decomposition *of A. One also observes that $o(A) = \prod_{i=1}^{\ell} n_i$.*

▶ **Corollary 8.** *One has $\mathit{exp}(A \oplus B) = \mathrm{lcm}(\mathit{exp}(A), \mathit{exp}(B))$ for every finite abelian groups A, B. More generally, for every finite family $(A_i)_{i\in I}$ of finite abelian groups, $\mathit{exp}(\bigoplus_{i\in I} A_i) = \mathrm{lcm}(\mathit{exp}(A_i) \colon i \in I)$. In particular, for each finite abelian group A, if $(\ell, n_1, \cdots, n_\ell)$ is its invariant factor list, then $\mathit{exp}(A) = n_\ell$.*

Proof. $\mathit{exp}(A \oplus B) = \mathrm{lcm}(o(a, b) \colon (a, b) \in A \times B) = \mathrm{lcm}(\mathrm{lcm}(o(a), o(b)) \colon a \in A,\ b \in B)$ (according to [2, Theorem 8.1, p. 157]), while $\mathrm{lcm}(\mathit{exp}(A), \mathit{exp}(B)) = \mathrm{lcm}(\mathrm{lcm}(o(a) \colon a \in A), \mathrm{lcm}(o(b) \colon b \in B))$, hence by the general associativity law for the lcm, both are equal. Now, one can proceed by induction for the second assertion. If $I = \emptyset$, then $\bigoplus_{i\in\emptyset} A_i \simeq 0$, and thus $\mathit{exp}(0) = 1$, while $\mathrm{lcm}(\emptyset) = 1$. If $|I| = 1$, say $I = \{ 1 \}$, then $\mathit{exp}(\bigoplus_{i\in} A_i) = \mathit{exp}(A_1)$, while $\mathrm{lcm}(\mathit{exp}(A_i) \colon i \in I) = \mathrm{lcm}(\mathit{exp}(A_1)) = A_1$ (see Subsection 3.3). For each $j \in I$, one has $\bigoplus_{i\in I} A_i \simeq (\bigoplus_{i\in A\setminus\{\,j\,\}} A_i) \oplus A_j$, then the first part of the proof tells us that

$$\begin{aligned} \mathit{exp}(\textstyle\bigoplus_{i\in I} A_i) &= \mathit{exp}((\textstyle\bigoplus_{i\in A\setminus\{\,j\,\}} A_i) \oplus A_j) \\ &= \mathrm{lcm}(\mathit{exp}(\textstyle\bigoplus_{i\in A\setminus\{\,j\,\}} A_i), \mathit{exp}(A_j)). \end{aligned} \tag{2}$$

By induction, one gets $\mathit{exp}(\bigoplus_{i\in A\setminus\{\,j\,\}} A_i) = \mathrm{lcm}(\mathit{exp}(A_i) \colon i \neq j)$, thus $\mathit{exp}(\bigoplus_{i\in I} A_i)$ is equal to $\mathrm{lcm}(\mathrm{lcm}(\mathit{exp}(A_i) \colon i \neq j), \mathit{exp}(A_j)) = \mathrm{lcm}(\mathit{exp}(A_i) \colon i \in I)$. Concerning the last assertion, one has $A \simeq \bigoplus_{i=1}^{\ell} \mathbb{Z}_{n_i}$, hence $\mathit{exp}(A) = \mathrm{lcm}(\mathit{exp}(\mathbb{Z}_{n_i}) \colon i = 1, \cdots, \ell) = \mathrm{lcm}(n_i \colon i = 1, \cdots, \ell)$ (since the $\mathbb{Z}_{n_i}$'s are cyclic) $= n_\ell$ because $n_i \mid n_{i+1}$ for all $i = 1, \cdots, \ell - 1$. ◀

▶ Remark. **1.** Let **Abfin** be the class of all finite abelian groups, and let $\mathbb{N}_+ = \mathbb{N} \setminus \{\,0\,\}$. Then, the map $\mathit{exp} \colon \mathbf{Abfin} \to \mathbb{N}_+$ is onto[1]. (Note that $\mathit{exp}(0) = 1$.)

2. It might of course happen that $\mathit{exp}(A) = \mathit{exp}(B)$, while $A \not\simeq B$. For instance, one has $\mathit{exp}(\underbrace{\mathbb{Z}_n \oplus \cdots \oplus \mathbb{Z}_n}_{\ell \text{ factors}}) = \mathrm{lcm}(\mathit{exp}(\mathbb{Z}_n) \colon i = 1, \cdots, \ell) = \mathrm{lcm}(n \colon i = 1, \cdots, \ell) = n$ for every $\ell > 0$.

4 Tensor product of finite abelian groups

4.1 Tensor product of abelian groups

The tensor product of abelian groups is a special instance, for $R = \mathbb{Z}$, of the well-known tensor product of R-modules over a commutative ring R with a unit. It "classifies" the bilinear maps in a sense made precise hereafter. Given two abelian groups A and B, their *tensor product* $A \otimes B$ is an abelian group, equipped with a bi-additive map $\phi_{A,B} \colon A \times B \to A \otimes B$, called the *canonical bilinear map*, which is characterized by the following universal property: for each abelian group C, and each bilinear map $f \colon A \times B \to C$, there exists a unique homomorphism of groups $g \colon A \otimes B \to C$ such that $g \circ \phi_{A,B} = f$. This implies that $\mathit{Ab}(A \otimes B, C) \simeq \mathit{Bil}(A \times B, C)$, canonically by $g \mapsto g \circ \phi_{A,B}$.

The existence of $A \otimes B$ has not hitherto been asserted. Let us review one of its classical construction. Let X be any set. A member f of the set of functions $\mathbb{Z}^X$ is said to be *finitely-supported* whenever $\{\,x \in X \colon f(x) \neq 0\,\}$ is a finite set. The set of all such maps is denoted by $\mathbb{Z}^{(X)}$. It admits a natural structure of an abelian group given by point-wise operations, and it is even the free abelian group generated by X.

Given two abelian groups A and B, their tensor product $A \otimes B$ may be realized as the quotient of the free abelian group $\mathbb{Z}^{(A\times B)}$, generated by the set $A \times B$, by the its subgroup generated by $(x, y + y') - (x, y) - (x, y')$, $(x + x', y) - (x, y) - (x', y)$, for all $x, x' \in A$ and $y, y' \in B$. The canonical bilinear map then is the restriction of the canonical epimorphism $\pi \colon \mathbb{Z}^{(A\times B)} \to A \otimes B$ to the set $A \times B$ (more precisely its image into $\mathbb{Z}^{(A\times B)}$). The value $\phi_{A,B}(a, b)$ is often denoted by $a \otimes b$, and $\phi_{A,B}$ itself may be denoted by $\otimes$. The members of $A \otimes B$ are referred to as *tensors*, and a tensor of the form $a \otimes b$ is called an *elementary tensor*. It is clear from its construction that $A \otimes B$ is generated by the elementary tensors (hence a member of $A \otimes B$ may be written as a sum of a finite number of elementary tensors).

▶ Remark. It follows from its construction that $A \otimes 0 \simeq 0 \simeq 0 \otimes A$ for every abelian group A.

[1] Of course, strictly speaking, **Abfin** is not a (small) set. But there are no set-theoretic difficulties to define the map exp as we did. Indeed, one can choose, by the axiom of choice, a representative of each member of the class $\mathbf{Abfin}/\simeq$ of isomorphism classes of finite abelian groups, and it is an easy exercise from elementary set-theory to see that the class of all these representatives really forms a set. According to the second point of Remark 3.4, exp could be equally defined on this set of representatives.

4.2 Category-theoretic properties

From a category-theoretic viewpoint, $\otimes$, loosely speaking, endows the category $\mathcal{Ab}$ with a structure of a symmetric monoidal closed category. These details are rather irrelevant for this contribution, but some of their consequences are important. The reader should refer to [11] for the details. The following consequences will be freely used in what follows:

1. Since $\otimes$ is a bifunctor, it automatically preserves isomorphisms, i.e., if $A \simeq A'$, and $B \simeq B'$, then $A \otimes B \simeq A' \otimes B'$. The converse is false in general. E.g., according to Lemma 9 below, $\mathbb{Z}_6 \otimes \mathbb{Z}_4 \simeq \mathbb{Z}_2 \simeq \mathbb{Z}_2 \otimes \mathbb{Z}_2$.
2. There are canonical (even coherent [11])) isomorphisms: $\alpha\colon (A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$, $\sigma\colon A \otimes B \simeq B \otimes A$, $\lambda\colon \mathbb{Z} \otimes A \simeq A$ and $\rho\colon A \otimes \mathbb{Z} \simeq A$.
3. For every (finite) abelian groups A, B, $\mathcal{Ab}(A, B)$ ($\mathcal{Abfin}(A, B)$) is a (finite) abelian group, and there exists a canonical group isomorphism $\mathcal{Ab}(A \otimes B, C) \simeq \mathcal{Ab}(A, \mathcal{Ab}(B, C))$ (there is also a canonical isomorphism $\mathcal{Abfin}(A \otimes B, C) \simeq \mathcal{Abfin}(A, \mathcal{Abfin}(B, C))$).
4. Since, for every abelian group A, $- \otimes A$ admits a right adjoint, then it is itself a left adjoint, and as such it preserves all colimits that exist in the category of abelian groups. In particular, because it is also additive[2], $(\bigoplus_{i\in I} A_i) \otimes A \simeq \bigoplus_{i\in I}(A_i \otimes A)$, canonically. The canonical isomorphism γ satisfies $\gamma((a_i)_{i\in I} \otimes a) = (a_i \otimes a)_{i\in I}$ for every $(a_i)_i \in \bigoplus_{i\in I} A_i$ and every $a \in A$. Using the symmetry σ (point (2) above), it follows that $A \otimes -$ also is a left adjoint, and thus one also has a canonical isomorphism $\delta\colon A \otimes (\bigoplus_{i\in I} A_i) \to \bigoplus_{i\in I}(A \otimes A_i)$ such that $\delta(a \otimes (a_i)_{i\in I}) = (a \otimes a_i)_{i\in I}$.
5. When A, B are finite abelian groups, then $A \otimes B$ is also finite (see Proposition 11 in what follows). Then, the above isomorphisms γ and δ restricts to the category of finite abelian groups (hence assuming that A and the A_i's are finite, $i \in I$, and the index set I also is finite). Indeed, $- \otimes A$ and $A \otimes -$, for A finite, are also left adjoint (additive) functors from $\mathcal{Abfin}$ to itself, and thus preserve all colimits that exist in $\mathcal{Abfin}$. However, while being close to be a symmetric monoidal closed category, $\mathcal{Abfin}$ is not since the unit $\mathbb{Z}$ of the tensor does not belong to it.

4.3 On the tensor product of finite abelian groups

The objective of this subsection is to compute the tensor product of finite abelian groups. So it seems natural to compute at first the easiest example. The following result is well-known (see for instance [6]), and its proof is given in virtue of completeness.

▶ **Lemma 9.** *For every positive integers a, b, $\mathbb{Z}_a \otimes \mathbb{Z}_b \simeq \mathbb{Z}_{\gcd(a,b)}$, and the canonical bilinear map $\otimes\colon \mathbb{Z}_a \otimes \mathbb{Z}_b \to \mathbb{Z}_{\gcd(a,b)}$ is given by $(x \bmod b) \otimes (y \bmod b) = xy \bmod \gcd(a, b)$.*

Proof. Since $\gcd(a, b)$ divides both a and b, the map $f\colon \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{\gcd(a,b)}$ given by $f(x \bmod a, y \bmod b) = (xy) \bmod \gcd(a, b)$ is well-defined. Moreover it is bilinear so that it gives rise to a group homomorphism $\pi\colon \mathbb{Z}_a \otimes \mathbb{Z}_b \to \mathbb{Z}_{(a,b)}$ such that $\pi((x \bmod a) \otimes (y \bmod b)) = (xy) \bmod \gcd(a, b)$. We observe that $\pi((x \bmod a) \otimes 1) = x \bmod \gcd(a, b)$ for every x, so that π is onto. Let $\mathbb{Z} \to \mathbb{Z}_a \otimes \mathbb{Z}_b$ be given by $x \mapsto x(1 \otimes 1)$. This is clearly a homomorphism of groups, and for $x \in a\mathbb{Z}$, we have $x(1 \otimes 1) = ((x \bmod a) \otimes 1) = 0$. Similarly, when $x \in b\mathbb{Z}$, we have $x(1 \otimes 1) = 1 \otimes (x \bmod b) = 0$. Therefore, $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$ belongs to its kernel, and we obtain a homomorphism of groups $g\colon \mathbb{Z}_{\gcd(a,b)} \to \mathbb{Z}_a \otimes \mathbb{Z}_b$ such that $g(x \bmod \gcd(a, b)) = x(1 \otimes 1) = ((x \bmod a) \otimes 1 = 1 \otimes (x \bmod b)$ for all x. We

[2] Hence tensorizations preserve not only the coproduct – the direct sum – but also the whole biproduct structure, i.e., also the projections.

have $\pi(g(x \bmod \gcd(a,b))) = \pi((x \bmod a) \otimes 1) = x \bmod \gcd(a,b)$ for every x. We have $g(\pi(x(1 \otimes 1))) = xg(1) = x(1 \otimes 1)$. This is sufficient to check that π and g are inverses one from the other because all tensors in $\mathbb{Z}_a \otimes \mathbb{Z}_b$ have the form $x(1 \otimes 1)$ for some $x \in \mathbb{Z}$. Indeed, for an elementary tensor $(x \bmod a) \otimes (y \bmod b) = (xy)(1 \otimes 1)$. So sums of elementary tensors are also multiple of $1 \otimes 1$. The second point is obvious. ◀

▶ Remark. It follows from lemma 9 that $\mathbb{Z}_a \otimes \mathbb{Z}_b \simeq 0$ if, and only if, a and b are co-prime.

Lemma 9 in combination with the properties recalled in Subsection 4.2 imply the following result that actually covers all examples of finite abelian groups, and shows once for all that the tensor product of finite abelian groups is itself finite.

▶ **Lemma 10.** *One has* $A \otimes B \simeq \bigoplus_{\substack{i=1,\cdots,m \\ j=1,\cdots,n}} \mathbb{Z}_{\gcd(a_i,b_j)}$, *with* $A = \bigoplus_{i=1}^{m} \mathbb{Z}_{a_i}$, *and* $B = \bigoplus_{j=1}^{n} \mathbb{Z}_{b_j}$, *where the isomorphism is given by the unique group homomorphism such that*

$$\begin{array}{ll} & ((x_1 \bmod a_1, \cdots, x_m \bmod a_m) \otimes (y_1 \bmod b_1, \cdots, y_n \bmod b_n)) \\ \mapsto & ((x_i y_j) \bmod \gcd(a_i, b_j))_{\substack{i=1,\cdots,m \\ j=1,\cdots,n}}. \end{array} \tag{3}$$

Moreover, the canonical bilinear map $\otimes$ *is then given by*

$$\otimes \colon A \times B \to \bigoplus_{\substack{i=1,\cdots,m \\ j=1,\cdots,n}} \mathbb{Z}_{\gcd(a_i,b_j)} \tag{4}$$

with $(x_1 \bmod a_1, \cdots, x_m \bmod a_m) \otimes (y_1 \bmod b_1, \cdots, y_n \bmod b_n)$
$= ((x_i y_j) \bmod \gcd(a_i, b_j))_{\substack{i=1,\cdots,m \\ j=1,\cdots,n}}$.

Let A be a finite abelian p-group, and B be a finite abelian q-group for prime numbers p, q, both assumed non trivial. Then, $A \otimes B \simeq 0$ whenever $p \neq q$. Indeed the invariant factor decomposition implies that $A \simeq \bigoplus_{i=1}^{m} \mathbb{Z}_{p^{\alpha_i}}$ with $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m \geq 1$, and $B \simeq \bigoplus_{j=1}^{n} \mathbb{Z}_{q^{\beta_j}}$ with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n \geq 1$. Thus, according to Lemma 10 and 9, $A \otimes B \simeq \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathbb{Z}_{p^i} \otimes \mathbb{Z}_{q^j} = 0$ whenever $p \neq q$. If $p = q$, the one has $A \otimes B \simeq \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathbb{Z}_{p^{\min\{\,i,j\,\}}}$. In particular, $A \otimes B$ is also a finite abelian p-group. Of course if A or B is trivial, then $A \otimes B \simeq 0$.

▶ Remark. Let A be a finite abelian p-group, and B be a finite abelian q-group for prime numbers p, q, with $p \neq q$. Then, for any bilinear map $f \colon A \times B \to C$, one also has $f = 0$. Indeed, such a map factors uniquely as an homomorphism $g \colon A \otimes B \to C$, and, according to the above discussion, $A \otimes B = 0$. In brief, in this case $\mathcal{Bil}(A \times B, C) = 0$ for every finite abelian group C.

Now let A, B be two finite abelian groups. Then, the decomposition into primary components leads to $A \otimes B \simeq (\bigoplus_{p \in \mathbb{P}} A[p]) \otimes (\bigoplus_{p \in \mathbb{P}} B[p]) \simeq \bigoplus_p \bigoplus_q A[p] \otimes B[q] \simeq \bigoplus_p A[p] \otimes B[p]$. From the above discussion $A[p] \otimes B[p]$ is a finite abelian p-group so that $A[p] \otimes B[p]$ is (isomorphic to) the p-primary component of $A \otimes B$. The following result is thus proved.

▶ **Proposition 11.** *The tensor product of two finite abelian groups is finite (hence also is the tensor product of a finite number of finite abelian groups by associativity of* $\otimes$ *up to the isomorphism* α*). Moreover, for every finite abelian groups* A, B, *the primary decomposition of* $A \otimes B$ *is given by* $A \otimes B \simeq \bigoplus_{p \in P} A[p] \otimes B[p]$.

5 Group-theoretic properties of pairings

5.1 Primary components of a bilinear map

Let A, B, C be finite abelian groups. Let $f \in \mathfrak{Bil}(A \times B, C)$. Then for every $(p, q) \in \mathbb{P}^2$, $p \neq q$, and every $(a, b) \in A[p] \times B[q]$, $f(a, b) = 0$ (since $A[p] \otimes B[q] = 0$).

Moreover, for each $(a, b) \in A[p] \times B[p]$, $f(a, b) \in C[p]$ (indeed, for each $a \in A[p]$, $f(a, \cdot) \in \mathfrak{Abfin}(B, C)$, so that by Subsection 3.2, $f(a, \cdot) \colon B[q] \to C[q]$ for every prime numbers q, and in particular for $q = p$), i.e., $f(A[p] \times B[p]) \subseteq C[p]$ for each prime p.

Furthermore for each p, the restriction $f_p \colon A[p] \times B[p] \to C[p]$ of f is easily seen to be a bilinear map. Using the notations from Subsection 3.2, one has

$$\begin{aligned} f(a, b) &= f(\textstyle\sum_p q_p^A(\pi_p^A(a)), \sum_q q_q^B(\pi_q^B(b))) \\ &= \textstyle\sum_p f(q_p^A(\pi_p^A(a)), q_p^B(\pi_p^B(b))) \\ &= \textstyle\sum_p q_p^C(f_p(\pi_p^A(a), \pi_p^B(b))), \end{aligned} \tag{5}$$

and thus $\pi_p^C(f(a, b)) = f_p(\pi_p^A(a), \pi_p^B(b))$.

In particular, if one considers for f the canonical bilinear map $\otimes \colon A \times B \to A \otimes B$, and if one denotes by $\otimes_p \colon A[p] \times B[p] \to A[p] \otimes B[p]$ the corresponding canonical bilinear map for each prime p, then it follows that $a \otimes b = \sum_{p \in \mathbb{P}} \pi_p^A(a) \otimes_p \pi_p^B(b)$.

▶ **Theorem 12.** *Let A, B be two finite abelian groups. The canonical bilinear map $\otimes \colon A \times B \to A \otimes B$ is non-degenerate if, and only if, for every prime number p, $\otimes_p$ is non-degenerate. More generally, $f \in \mathfrak{Bil}(A \times B, A \otimes B)$ is a pairing if, and only if, $f_p \in \mathfrak{Bil}(A[p] \times B[p], A[p] \otimes B[p])$ is a pairing for each prime number p.*

Proof. It is obviously sufficient to prove the second assertion. Let us assume that all f_p's are non-degenerate. Let $a \in A$ such that for every $b \in B$, $f(a, b) = 0$. Then due to the decomposition into a direct sum, it follows that one has $f_p(\pi_p^A(a), \pi_p^B(b)) = 0$. By non-degeneracy of f_p (since π_p^B is onto) this implies that $\pi_p^A(a) = 0$ for each p, and thus $a = 0$. Now, let us assume that f is non-degenerate but there are some prime number p_0 and $a_{p_0} \in A[p_0]$, $a \neq 0$, such that $f_{p_0}(a_{p_0}, b) = 0$ for every $b \in B[p_0]$. Then, let us consider $a \in A$ such that $\pi_p^A(a) = 0$ for every $p \neq p_0$, and $\pi_{p_0}^A(a) = a_{p_0}$, i.e., $a = q_p^A(a_{p_0})$. Then, for every $b \in B$, $f(a, b) = \sum_p f(\pi_p^A(a), \pi_p^B(b)) = f_{p_0}(a_{p_0}, b) = 0$ which contradicts non-degeneracy of f. ◀

5.2 A characterization of pairing admissible groups

Next proposition explains in what extent non-degeneracy of the canonical bilinear map is essential for the existence of pairings.

▶ **Proposition 13.** *Let A, B be two finite abelian groups. (A, B) is pairing admissible if, and only if, the canonical pairing $\otimes \colon A \times B \to A \otimes B$ is non-degenerate.*

Proof. The converse assertion is immediate. Let us prove the necessity of the condition. By contraposition, let us assume that $\otimes \colon A \times B \to A \otimes B$ is degenerate, e.g., it is not left non-degenerate. Then, A is necessarily non trivial, and there exists $a_0 \in A$, $a_0 \neq 0_A$, such that for every $b \in B$, $a_0 \otimes b = 0$. Let $\langle \cdot \mid \cdot \rangle \colon A \times B \to C$ be a bilinear map. Then, there exists a unique group homomorphism $f \colon A \otimes B \to C$ such that $f(a \otimes b) = \langle a \mid b \rangle$. In particular, $\langle a_0 \mid b \rangle = f(a_0 \otimes b) = f(0) = 0_C$ for all $b \in B$. Therefore, $\langle \cdot \mid \cdot \rangle$ is left degenerate. ◀

According to Proposition 13 it seems relevant to study the conditions under which the canonical bilinear map is non-degenerate. Let us begin, as always, with the easiest case.

▶ **Lemma 14.** *Let a and b be two positive integers. The canonical bilinear map $\otimes\colon (x \bmod a, y \bmod b) \in \mathbb{Z}_a \times \mathbb{Z}_b \to (xy) \bmod \gcd(a,b) \in \mathbb{Z}_{\gcd(a,b)} \simeq \mathbb{Z}_a \otimes \mathbb{Z}_b$ is non-degenerate if, and only if, $a = b$.*

Proof. If $a = b = 1$, then all groups are trivial, and the result is obvious. Let $a = \gcd(a,b) = b \neq 1$. Let $x \bmod a \neq 0$ such that for every y, $(xy) \bmod a = 0$, then letting $y = 1$ leads to a contradiction. Therefore, $\otimes$ is non-degenerate. Conversely, let us assume e.g. that $\gcd(a,b) < a$. Then, $\gcd(a,b) \bmod a \neq 0$, and for all y, $\gcd(a,b)y \bmod \gcd(a,b) = 0$ so that $\otimes$ is degenerate. ◀

▶ Remark. Lemma 14 just states that a pair of cyclic groups $(\mathbb{Z}_a, \mathbb{Z}_b)$ is pairing admissible if, and only if, $a = b$.

Because any finite abelian group decomposes in a natural way into a finite direct sum of finite abelian p-groups, for varying p, let us study the non-degeneracy conditions of the canonical bilinear map between p-groups.

Let p be a prime number. Let A, B be two finite abelian p-groups, and C be a finite abelian group. According to the invariant factor decomposition, $A \simeq \bigoplus_{i=1}^{m} \mathbb{Z}_{p^{\alpha_i}}$ with $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m \geq 1$, and $B \simeq \bigoplus_{j=1}^{n} \mathbb{Z}_{p^{\beta_j}}$ with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n \geq 1$. Therefore, $\mathit{exp}(A) = p^{\alpha_1}$ and $\mathit{exp}(B) = p^{\beta_1}$.

Let $f\colon A \times B \to C$ be a pairing. Let us assume for instance that $\mathit{exp}(A) > \mathit{exp}(B)$. Then,

$$\begin{array}{rcl} f((\mathit{exp}(B)1, 0, \cdots, 0), (y_1, \cdots, y_n)) & = & f((1, 0, \cdots, 0), \mathit{exp}(B)(y_1, \cdots, y_n)) \\ & = & f((1, 0, \cdots, 0), (0, \cdots, 0)) \\ & = & 1 \end{array} \tag{6}$$

for every $y_1, \cdots, y_n$. Thus f would be degenerate. Therefore, $\mathit{exp}(A) = \mathit{exp}(B)$. Conversely, let us assume that $\mathit{exp}(A) = \mathit{exp}(B)$, so in the above notation $\alpha_1 = \beta_1$. One has

$$A \otimes B \simeq \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathbb{Z}_{p^{\min\{\alpha_i, \beta_j\}}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \bigoplus_{i=2}^{m} \mathbb{Z}_{p^{\alpha_i}} \oplus \bigoplus_{j=2}^{n} \mathbb{Z}_{p^{\beta_j}} \oplus \bigoplus_{i=2}^{m} \bigoplus_{j=2}^{n} \mathbb{Z}_{p^{\min\{\alpha_i n \beta_j\}}},$$

and thus $\mathit{exp}(A \otimes B) = p^{\alpha_1}$. Now, let us assume that the canonical bilinear map $\otimes\colon A \times B \to A \otimes B$ is degenerate. Then, under the previous isomorphism, this means for instance that there exists a non-zero $(a_1 \bmod p^{\alpha_1}, a_2 \bmod p^{\alpha_2}, \cdots, a_m \bmod p^{\alpha_m})$ such that for every $(b_1 \bmod p^{\alpha_1}, b_2 \bmod p^{\beta_2},$
$\cdots, b_n \bmod p^{\beta_n})$, we have

$$\begin{array}{rl} & (a_1 \bmod p^{\alpha_1}, \cdots, a_m \bmod p^{\alpha_m}) \otimes (b_1 \bmod p^{\alpha_1}, \cdots, b_n \bmod p^{\beta_n}) \\ = & (a_1 b_1 \bmod p^{\alpha_1}, \cdots, a_1 b_n \bmod p^{\beta_n}, \cdots, a_m b_1 \bmod p^{\alpha_n}, \cdots, \\ & a_i b_j \bmod p^{\min\{\alpha_i, \beta_j\}}, \cdots, a_m b_n \bmod p^{\min\{\alpha_m, \beta_n\}}) \\ = & 0. \end{array} \tag{7}$$

So if one takes $b_1 = 1$, $b_j = 0$ for each j, it follows that $(a_1, a_2, \cdots, a_m) = (0, 0, \cdots, 0)$ which yields to a contradiction. The following lemma is thus proved (also using Proposition 13).

▶ **Lemma 15.** *Let A, B be two finite abelian p-groups. (A, B) is pairing admissible if, and only if, $\mathit{exp}(A) = \mathit{exp}(B)$. In particular, $\otimes\colon A \times B \to A \otimes B$ is a pairing if, and only if, $\mathit{exp}(A) = \mathit{exp}(B)$.*

One now states the main characterization of pairing admissible pairs.

▶ **Theorem 16.** *For every finite abelian groups A, B, (A, B) is pairing admissible if, and only if, $\mathit{exp}(A) = \mathit{exp}(B)$.*

Proof. According to Theorem 12, (A, B) is pairing admissible if, and only if, for each prime p, $(A[p], B[p])$ is pairing admissible if, and only if, for each prime p, $\mathscr{exp}(A[p]) = \mathscr{exp}(B[p])$ (by Lemma 15) if, and only if, $\mathscr{exp}(A) = \mathscr{exp}(B)$ (by Lemma 6). ◀

▶ **Example 17.** According to Theorem 16 (but it may be checked by hand), for any prime number p and any integer $m > 1$, the canonical bilinear map $\otimes\colon \mathbb{Z}_p^m \times \mathbb{Z}_p \to \mathbb{Z}_p^m$ given by $(x_i \bmod p)_{i=1}^m \otimes (y \bmod p) = (x_i y \bmod p)_{i=1}^m$ is non-degenerate.

5.3 Semilattice of equivalence classes of groups under pairing admissibility

From Theorem 16 it follows that the relation defined by $A \sim B$ if, and only if, (A, B) is pairing admissible, is an equivalence relation among the class **Abfin** of all finite abelian groups.

By Corollary 8, $\mathscr{exp}(A \oplus B) = \mathrm{lcm}(\mathscr{exp}(A), \mathscr{exp}(B))$. Therefore for any $A \sim B$, $C \sim D$, one has $A \oplus C \sim B \oplus D$, and thus there is a well-defined operation, still denoted by $\oplus$, on the equivalence classes of finite abelian groups mod $\sim$ such that $(A \mod \sim) \oplus (B \mod \sim) = (A \oplus B) \mod \sim$. It turns out that $\mathbf{Abfin}/\sim$ is a commutative monoid under $\oplus$ and with $0 \mod \sim$ has identity.

It is even an idempotent monoid (since $\mathscr{exp}(A \oplus A) = \mathscr{exp}(A)$). Hence it is a join-semilattice with a bottom element $0 \mod \sim$ (with partial order relation given by $A \mod \sim \leq B \mod \sim$ if, and only if, $(A \oplus B) \mod \sim = B \mod \sim$). Let $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, and let us define a bijection $C\colon \mathbb{N}_+ \to \mathbf{Abfin}/\sim$ by $C_n = \mathscr{exp}^{-1}(\{n\}) = \{A \in \mathbf{Abfin}\colon \mathscr{exp}(A) = n\}$. It is merely clear that $C_{\mathrm{lcm}(m,n)} = C_m \oplus C_n$. Hence, the following result holds.

▶ **Theorem 18.** *The map $C\colon \mathbb{N}_+ \to \mathbf{Ab}/\sim$ is an isomorphism of semilattices (with bottom element) from the join semilattice of positive integers under divisibility and $\mathbf{Abfin}/\sim$.*

5.4 Abelian group structure of bilinear maps (and pairings) on cyclic groups

First of all, according to the universal property of the tensor product of groups, $\mathscr{Bil}(A \times B, C) \simeq \mathscr{Abfin}(A \otimes B, C)$ (set-theoretic bijection), for all finite abelian groups A, B, C. But the latter is itself a finite abelian group with point-wise operations, so that the above bijection may be lifted to as an isomorphism of groups by transporting the group structure of $\mathscr{Abfin}(A \otimes B, C)$ on $\mathscr{Bil}(A \times B, C)$ along the bijection. We have for $f, g \in \mathscr{Bil}(A \times B, C)$, two new bilinear maps $f + g, -f \in \mathscr{Bil}(A \times B, C)$ defined by $(f + g)(a, b) = f(a, b) + g(a, b)$, $(-f)(a, b) = -(f(a, b))$ for all $a \in A$, $b \in B$. This of course also defines a structure of $\mathbb{Z}$-module given by $(nf)(a, b) = n(f(a, b))$ for all $a \in A$, $b \in B$, $n \in \mathbb{Z}$.

For every finite abelian group A, let $\mathscr{End}(A) := \mathscr{Abfin}(A, A)$, which is a finite ring. Then, $\mathscr{Bil}(A \times B, A \otimes B) \simeq \mathscr{End}(A \otimes B)$, so that $\mathscr{Bil}(A \times B, A \otimes B)$ also acquires a ring structure. For $f \in \mathscr{Bil}(A \times B, A \otimes B)$, let us denote by $\tilde{f}$ the unique endomorphism of $A \otimes B$ such that $\tilde{f} \circ \phi_{A,B} = f$, where $\phi_{A,B}\colon A \times B \to A \otimes B$ is the canonical bilinear map. For $f, g \in \mathscr{Bil}(A \times B, A \otimes B)$, the ring multiplication $g \cdot f$ thus given by $\tilde{g} \circ \tilde{f} \circ \phi_{A,B} = \tilde{g} \circ f$, and the identity is $\phi_{A,B}$.

Now, let us assume that $A \simeq \mathbb{Z}_a$ and $B \simeq \mathbb{Z}_b$. Then, as rings, $\mathscr{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{\gcd(a,b)}) \simeq \mathscr{End}(\mathbb{Z}_{(a,b)}) \simeq \mathbb{Z}_{(a,b)}$ (the last ring isomorphism is given by $\phi \mapsto \phi(1)$). As a cyclic group of order $\gcd(a, b)$, $\mathscr{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{\gcd(a,b)})$ is generated by $\phi_{A,B}$. Whence for any bilinear map $f\colon \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{\gcd(a,b)}$, there is a unique $n_f \in \mathbb{Z}_{(a,b)}$ such that $f = n_f \phi_{A,B}$. If one assumes that $\phi_{A,B}$ is non-degenerate, i.e., $a = b$ (according to Lemma 14), then it follows easily that f

is non-degenerate if, and only if, $\gcd(n_f, a) = 1$. Therefore, pairings from $\mathbb{Z}_a \times \mathbb{Z}_a$ to $\mathbb{Z}_a$ are in one-one correspondence with the generators of the group $\mathcal{B}il(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$, i.e., they form the group $\mathcal{B}il(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)^\times \simeq \mathbb{Z}_a^\times$ of invertible elements of the ring $\mathcal{B}il(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$.The following result is proved.

▶ **Theorem 19.** *The set of pairings from $\mathbb{Z}_a \times \mathbb{Z}_a$ to $\mathbb{Z}_a$ forms a group isomorphic to the group of invertible elements $\mathbb{Z}_a^\times$ of the ring $\mathbb{Z}_a$. In particular, there are exactly $\phi(a)$ pairings, and if $f \in \mathcal{B}il(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$ is a pairing, then any other pairing g has the form $k_g f$, for a unique $k_g \in \mathbb{Z}_a^\times$. Moreover, if p is a prime number, then the group of pairings in $\mathcal{B}il(\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p^*$.*

▶ Remark. Let p be a prime number. Let $f \in \mathcal{B}il(\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p)$ be a pairing. According to theorem 19, any other pairing is given by kf for $k \in \mathbb{Z}_p^*$ as it was already noticed in [5] (but we observe that the underlying group structure on pairings was not explicitly mentioned). In this situation, the integer k was called the *logarithm* of the pairing *to the base f*. This also explains why F. Vercauteren writes in [17] that “there is essentially only one pairing”.

References

1 Davey, B.A., Priestley, H.A.: Introduction to lattices and order (2nd edition), Cambridge University Press, 2002.

2 Gallian, J.A.: Contemporary abstract algebra (7th edition), Brooks/Cole Cengage Learning, 2010.

3 Baer, R.: Groups with Abelian central quotient group. Transactions of the American Mathematical Society 44(3): 357–386, 1938.

4 Boneh, D. and Franklin, M. K.: Identity-based encryption from the Weil pairing. SIAM Journal of Computing 32(3): 586–617, 2003.

5 Boxall, J., and Enge, A.: Some security aspects of pairing-based cryptography. Technical report of the ANR Project PACE, 2009.

6 Conrad, K.: Tensor products I. Notes of course, available on-line.

7 Joux, A.: A One Round Protocol for Tripartite Diffie-Hellman, ANTS, LNCS 1838: 385–394, 2000.

8 Joye, M., and Neven, G.: Identity-based cryptography. Volume 2 of Cryptology and Information Security Series, IOS Press, 2009.

9 Kim, T. and Barbulescu, R.: Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case, Cryptology ePrint Archive, Report 2015/1027.

10 Lubicz, D., and Robert, D.: Efficient pairing computations with theta functions. In: ANTS-IX. Proceedings of the 9th International Symposium in Algorithmic Number Theory, Nancy, France, July 19-23. Lecture Notes in Computer Science 6197: 251–269, 2010

11 Mac Lane, S.: Categories for the working mathematician. Volume 5 of Graduate Texts in Mathematics, Springer (1971).

12 Menezes, A., Okamoto, T., and Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory 39 (5): 1639–1646, 1993.

13 Roman, S.: Fundamentals of group theory: an advanced approach, Birkhäuser, 2011.

14 Silverman, J.H.: The arithmetic of elliptic curves. Volume 106 of Graduate Texts in Mathematics, Springer (1986).

15 Scott, W.R.: Group theory. Courier Dover Publications, 1964.

16 Vinberg, E.B.: A course in algebra, vol. 56 in Graduate studies in mathematics, American Mathematical Society, 2003.

17 Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theorey 56(1): 455–461, 2010.