Pairings from a tensor product point of view

Nadia El Mrabet, Laurent Poinsot

Pairings from a tensor product point of view

Nadia El Mrabet[1]* and Laurent Poinsot[2]

[1] Université Paris 8, LIASD, France,
elmrabet@ai.univ-paris8.fr,
http://www.ai.univ-paris8.fr/~elmrabet/
[2] Université Paris 13, Sorbonne Paris Cité, LIPN, CNRS (UMR 7030), France,
laurent.poinsot@lipn.univ-paris13.fr,
http://lipn.univ-paris13.fr/~poinsot/

Abstract. Pairings are particular bilinear maps, and as any bilinear maps they factor through the tensor product as group homomorphisms. Besides, nothing seems to prevent us to construct pairings on other abelian groups than elliptic curves or more general abelian varieties. The point of view adopted in this contribution is based on these two observations. Thus we present an elliptic curve free study of pairings which is essentially based on tensor products of abelian groups (or modules). Tensor products of abelian groups are even explicitly computed under finiteness conditions. We reveal that the existence of pairings depends on the non-degeneracy of some universal bilinear map, called the canonical bilinear map. In particular it is shown that the construction of a pairing on $A \times A$ is always possible whatever a finite abelian group A is. We also propose some new constructions of pairings, one of them being based on the notion of group duality which is related to the concept of non-degeneracy.

Keywords: Pairing, tensor product, finite abelian group, module, duality.

Mathematics Subject Classification (2010) 15A69, 11E39

1 Introduction

A bilinear map is a function of two variables that belong to two finite abelian groups, and with values in another abelian group, such that when fixing one of its variable the map thus obtained is a homomorphism of groups. Bilinear maps were originally introduced in cryptography in order to solve the discrete logarithm problem [24]. Due to bilinearity it is possible to transport this problem from a group for which it is assumed to be difficult to another one where the problem becomes easier. Afterwards, bilinear maps were used to define tripartite Diffie-Hellman key exchange protocol [18]. In these two situations, the bilinear maps under consideration are assumed to be non-degenerate, and are called pairings. For such a map $f\colon A \times B \to C$, this means that apart from the identity element of A (respectively, B), there is no members of A (respectively, of B) that annihilate every member of B (respectively, of A). For these kinds of use the groups A, B, C are cyclic groups. Many pairings considered in the literature are naturally associated to some objects arising in algebraic (projective) geometry such as elliptic curves and more generally abelian varieties. For a long time pairings were variants of the Weil [31] and Tate [33] pairings over genus 1 or 2 curves over finite fields. More recently pairings over more general abelian varieties have been proposed [21] and even based on dot-products [26] for homomorphic encryption.

More attention was given to pairings over elliptic curves for at least two reasons. First of all, it seems that the security level of such pairings with respect to the discrete logarithm problem

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

and to pairing inversions is high (see for instance [8]). Secondly, these pairings may be computed rather efficiently (with help of an efficient finite field arithmetic [1, 12] or by optimized versions of Miller's algorithm [14, 34]). Apart from these two important cryptographic issues, pairings are bilinear maps between finite abelian groups, and as any bilinear map, a pairing descends to the tensor product of abelian groups as a usual group homomorphism. It seems rather natural to study pairings through the notion of tensor product, and it is the point of view adopted in this contribution. More precisely, we study, and construct, bilinear maps between finite abelian groups (and more generally between modules over some fixed ring) seen as homomorphisms from a tensor product to an abelian group (or a module). This provides an elliptic curve free presentation of pairings between abstract groups. Not all our results are difficult, some of them are folklore, and lot of them may even be qualified as simple for group-theorists, but we think that one of the main worth of this work is to provide a unified treatment of pairings in an abstract setting. This approach is quite natural since many properties of pairings are independent from algebraic geometry. Because we have chosen to work at the abstract groups level, we do not deal with the cryptographic issues of efficiency and security. We believe that these gaps are balanced by the results stated in this contribution, and our rather general approach to pairings. We also believe that this work may serve as a basis for new constructions of cryptographically relevant pairings on other group structures than elliptic curves (see for instance [21, 26]).

The remainder of this contribution is organized as follows: Section 2 fixes the general notations, provides basic definitions about bilinear maps and pairings, and contains a brief overview on pairing-based cryptography. Section 3 is about the tensor product of groups and modules themselves, of which it provides a number of useful properties. Section 4 is entirely devoted to the tensor product of finite abelian groups: the rules to compute any such tensor product are presented. It also deals with the canonical bilinear map (which is canonically attached to a tensor product) and the fact that non-degeneracy of a bilinear map depends of that of a canonical bilinear map. Section 5 contains several constructions of pairings. Some properties about known pairings are also recovered.

2 An introduction to pairing-based cryptography

2.1 Some notations and definitions

Before introducing the notion of pairings and their use in cryptography, let us begin with some notations, useful hereafter in 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 $x \mapsto f(x,y)$. The identity element of a group G is denoted either by 1_G or by 0_G (or 1 or 0) whether G is given in multiplicative or additive notation. Let G, H, K be three groups (abelian or not). A map $f\colon G \times H \to K$ is said to be *bilinear* if for every $g \in G$, and every $h \in H$, the maps $f(g,\cdot)\colon H \to K$ and $f(\cdot,h)\colon G \to K$ are homomorphisms of groups. The set of all bilinear maps from $G \times H$ to K is then denoted by $\mathcal{Bil}(G \times H, K)$. Actually, this notion may be defined in another setting, that of modules over some commutative ring. In this contribution, R always denotes a commutative ring with a unit 1_R. Given three R-modules, A, B, C, we say that a map $f\colon A \times B \to C$ is *R-bilinear* whenever 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 R-linear. When $R = \mathbb{Z}$, then $\mathbb{Z}$-bilinear maps are exactly bilinear maps between abelian groups. In what follows, the set of all R-bilinear maps from $A \times B$ to C is denoted by $\mathcal{Bil}_R(A \times B, C)$. Moreover, we denote $\mathcal{Bil}_{\mathbb{Z}}(A \times B, C)$ simply by $\mathcal{Bil}(A \times B, C)$ since when A, B, C are abelian

groups both notions of bilinearity coincide. Continuing with notations, if G, H are groups, then $\mathcal{Hom}(G, H)$ is the set of all group homomorphisms from G to H, and if A, B are two R-modules, then $\mathcal{Hom}_R(A, B)$ is the set of all R-linear maps from A to B. Again if A, B are abelian groups, then $\mathcal{Hom}(A, B) = \mathcal{Hom}_{\mathbb{Z}}(A, B)$.

Example 1. Let A be an abelian group. Let $R^\star$ be the group of invertible elements of R. A bilinear map $f\colon A \times A \to R^\star$ is called a *bicharacter* [29]. When furthermore $f(a, b)f(b, a) = 1$ and $f(a, a) = \pm 1$ for every $a, b \in A$, f is said to be a *commutation factor* [32]. Such commutation factors are used to define color Lie superalgebras [3].

One of the main feature of a pairing (the definition of which is recalled hereafter) is the notion of non-degeneracy. Let G, H, K be three groups and A, B, C be three R-modules. Let $f \in \mathcal{Bil}(G \times H, K)$ (respectively, $f \in \mathcal{Bil}_R(A \times B, C)$). The map f is said to be *left non-degenerate* if the map $g \in G \mapsto f(g, \cdot)$ (respectively, $a \in A \mapsto f(a, \cdot)$) is one-to-one. In other terms this means that if for every $h \in H$ (respectively, every $b \in B$), $f(g, h) = 1_K$ (respectively, $f(a, b) = 0_C$), then $g = 1_G$ (respectively, $a = 0_A$). The notions of *right non-degeneracy* are the evident symmetric ones, 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 *degenerate* if it is not non-degenerate. In its original form, a *pairing* is a non-degenerate bilinear map between finite abelian groups. For our purpose the definition of a pairing is somewhat extended to allow pairings between non-abelian groups or R-modules. In brief, a *pairing* is a non-degenerate map $f \in \mathcal{Bil}(G \times H, K)$ (respectively, $f \in \mathcal{Bil}_R(A \times B, C)$) where G, H, K are groups (respectively, A, B, C are R-modules). In particular, there is no size issue in the definition of a pairing although our examples will be given under finiteness assumptions. We also sometimes use the traditional "bracket" notation $\langle \cdot \mid \cdot \rangle$ to denote a pairing.

Example 2. 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 [2], $[\cdot, \cdot]$ descends to the quotient as a bilinear map $[\cdot, \cdot]\colon B \times B \to A$. Moreover it is alternating (*i.e.*, $[x, x] = 1$ for every $x \in B$). Finally, it is non-degenerate if, and only if, $A = Z(G)$, so that we obtain a pairing $[\cdot, \cdot]\colon G/Z(G) \times G/Z(G) \to Z(G)$ (whenever $G/Z(G)$ is abelian).

2.2 Background on pairing-based cryptography

We recall here the basic facts and definitions of pairings over elliptic curves. Let r be a prime integer, A, B, C be three abelian groups of order p. A pairing is a bilinear and non-degenerate map $f\colon A \times B \to C$. We briefly present the most frequent choices for A, B and C in pairing-based cryptography. Let E be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic p. The integer r is chosen to be a prime divisor of $|E(\mathbb{F}_q)|$, co-prime with p. A pairing is usually defined over the points of r-torsion of E: $E[r] = \{\, P \in E(\overline{\mathbb{F}_q})\colon rP = P_\infty \,\}$, where P_∞ is the point at infinity of the elliptic curve. We know that $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ [31, Chap III Cor. 6.4]. The embedding degree k of E relatively to r is the smallest integer such that r divides $(q^k - 1)$. A result of Balasubramanian and Koblitz [4] ensures that, when $k > 1$, all the points of $E[r]$ are rational over the extension $\mathbb{F}_{q^k}$ of degree k, *i.e.*, $E[r] = E(\mathbb{F}_{q^k})$. The group A is then the subgroup generated by a point $P \in E(\mathbb{F}_q)$ of order r. The subgroup B is chosen as another subgroup of order r of $E[r]$, a popular choice is the subgroup generated by a point Q of order r over $E(\mathbb{F}_{q^k})$, such that $\Pi(Q) = qQ$, where Π represents the Frobenius endormorphism over $\mathbb{F}_q$. Finally, the group C is the unique subgroup of order r of

$\mathbb{F}_{q^k}^*$ (it exists and is unique because r divides (q^k-1) and $\mathbb{F}_{q^k}^*$ is a cyclic group). This choice of subgroups may be seen as the restriction to $A \times B$ of the Weil pairing on $E[r] \times E[r]$, or the Tate paring, or one of its variant (reduced Tate, Ate, twisted Ate, optimal pairing or pairing lattices). The Miller algorithm is used to computed all these pairings.

The original objective of pairings in cryptography was to solve the discrete logarithm problem. The pairings shift the discrete logarithm problem from a subgroup over an elliptic curve to a discrete logarithm problem over a finite field. The interest is that the discrete logarithm problem is easier on finite fields compared to elliptic curves [24]. Later, the pairings were used to compose the tripartite Diffie-Hellman key exchange [18]. It was a simplification of the Diffie-Hellman key construction between three entities. Nowadays, pairings are used for several protocols such as identity based cryptography [5] or short signature schemes [19]. The security of pairing-based cryptography lays on the discrete logarithm problem over the three groups A, B and C [8].

3 Tensor product of groups (and modules)

The notions of bilinear maps and tensor product are closely related as it is explained hereafter, and this relation is exploited in section 5 to construct new pairings on finite abelian groups. In brief, every bilinear map factors through a quotient group – the tensor product – as a linear map. The original bilinear map is recovered by composing this linear map with a "universal" bilinear map. Therefore the study of bilinear maps reduces to that of a unique (and universal) bilinear map and of those linear maps which are defined on a particular kind of groups (or R-modules), namely the tensor product. In this section are recalled the constructions of the tensor product of groups and modules together with some of their basic properties. We also explain the reason why it is somewhat useless to define bilinear maps (or pairings) on non-abelian groups. Other properties of bilinear maps in the setting of finite abelian groups are presented in section 4.

3.1 Free (commutative) group and abelianization

The basic notions recalled in this subsection may be found for instance in [7].

Let G be a group. For any elements $g, h \in G$, the *commutator* of g and h is $[g,h] = g^{-1}h^{-1}gh$ (see example 2). The *derived subgroup* $[G,G]$ is generated by all the commutators and it turns to be a normal subgroup of G. It is even the smallest normal subgroup such that the quotient group of G by this subgroup is abelian.Thus the quotient group $G/[G,G]$, denoted by $\mathcal{Ab}(G)$, is an abelian group, called the *abelianization of* G. It satisfies the following property: let A be an abelian group, and $f\colon G \to A$ be a homomorphism of groups, then there is a unique homomorphism of groups $g\colon \mathcal{Ab}(G) \to A$ such that $g \circ \pi = f$, where π denotes the natural epimorphism $G \to \mathcal{Ab}(G)$.

Let X be a set. There exists a way to construct a group $F(X)$, called the *free group over* X, that contains X, and which is the solution[3] of the following "universal problem": for any group G and any set-theoretic map $f\colon X \to G$, there exists a unique homomorphism of groups $g\colon F(X) \to G$ such that $g(x) = f(x)$ for every $x \in X$. The construction is made as follows: for each $x \in X$, we introduce a new symbol, say $\overline{x}$, and we let $\overline{X}$ denote the totality of these symbols. Then, we consider the free monoid $(X \cup \overline{X})^*$ over $X \cup \overline{X}$. It consists of all words (including the empty word ϵ), *i.e.*, finite sequences of elements of $X \cup \overline{X}$. The composition of words is the obvious one (concatenation), and ϵ acts as the identity. Finally, let $\cong$ be the least congruence of $(X \cup \overline{X})^*$

[3] Actually a solution of a universal problem is only unique up to a unique isomorphism in some category, see [23].

containing $\{\,(x\overline{x},\epsilon)\colon x\in X\,\}\cup\{\,(\overline{x}x,\epsilon)\colon x\in X\,\}$ (see [9]). It turns that the quotient monoid $(X\cup\overline{X})^*/\cong$ (also known as the *Grothendieck group completion* of $(X\cup\overline{X})^*$) is actually a group which is precisely the free group $F(X)$.

There also exists a similar construction for abelian groups, and more generally for modules. Recall that R is a commutative ring with a unit 1_R. An element $f\in R^X$ is said to be *finitely supported* whenever the set of all $x\in X$ such that $f(x)\neq 0$ is finite. For instance, for each $x\in X$, the map $\delta_x\in R^X$ that vanishes at all $y\neq x$, and such that $\delta_x(x)=1_R$ is finitely supported. The set of all such functions is denoted by $R^{(X)}$. It is a free R-module with basis X (under identification of δ_x with x for each $x\in X$). In particular, for $R=\mathbb{Z}$, we obtain the *free commutative group* $\mathbb{Z}^{(X)}$ on X. As it is expected, $\mathcal{Ab}(F(X))\cong\mathbb{Z}^{(X)}$ (isomorphic as groups).

3.2 Tensor product: construction and properties

We are now in position to introduce the tensor product of groups and R-modules. Let G,H be two groups (in multiplicative notation), and let N be the normal subgroup of $F(G\times H)$ generated by the elements $(gg',h)(g,h)^{-1}(g',h)^{-1}$ and $(g,hh')(g,h)^{-1}(g,h')^{-1}$ for all $g,g'\in G$, $h,h'\in H$. The quotient group $F(G\times H)/N$ is denoted by $G\otimes H$. We denote by $g\otimes h$ the image of $(g,h)\in G\times H$ in $G\otimes H$ and this clearly defines a bilinear map from $G\times H$ to $G\otimes H$ called the *canonical bilinear map*. The group $G\otimes H$ also satisfies a universal property: for every group K and every bilinear map $f\colon G\times H\to K$, there exists a unique homomorphism of groups $f'\colon G\otimes H\to K$ such that $f'(g\otimes h)=f(g,h)$ for every $g\in G$ and $h\in H$.

Lemma 1. *The image of $\otimes\colon G\times H\to G\otimes H$ generates $G\otimes H$, the group $G\otimes H$ is abelian, and $\mathcal{Ab}(G)\otimes\mathcal{Ab}(H)\cong G\otimes H$ (in particular, $G\otimes H$ is an abelian group).*

Proof. The set $G\times H$ generates the free group $F(G\times H)$, and the natural map $F(G\times H)\to G\otimes H$ is onto. Then, the group $G\otimes H$ is generated by the image of $G\times H$. Let $f\colon G\times H\to K$ be a bilinear map, where K is another group (say in additive notation even if it is not assumed to be commutative). Let $g,g'\in G$, $h,h'\in H$. We have $f(g,h)+f(g,h')+f(g',h)+f(g',h')=f(g,hh')+f(g',hh')=f(gg',hh')=f(gg',h)+f(gg',h')=f(g,h)+f(g',h)+f(g,h')+f(g',h')$ so that $f(g,h')+f(g',h)=f(g',h)+f(g,h')$. Thus any two elements of the image of f commute, so the image of f generates a commutative subgroup of K. This proves that $G\otimes H$ is abelian. Let $\gamma\colon G\times H\to\mathcal{Ab}(G)\times\mathcal{Ab}(H)$ be the canonical map which is onto. It is clear that if $f\in\mathcal{Bil}(G\times H,K)$, then $f\circ\gamma\in\mathcal{Bil}(\mathcal{Ab}(G)\times\mathcal{Ab}(H),K)$. We thus define a map $\Psi\colon\mathcal{Bil}(G\times H,K)\to\mathcal{Bil}(\mathcal{Ab}(G)\times\mathcal{Ab}(H),K)$ by $\Psi(f)=f\circ\gamma$. It turns that it is one-to-one (since γ is onto). Because the image of $f\in\mathcal{Bil}(G\times H,K)$ generates an abelian subgroup in K, for a fixed $h\in H$ the kernel of the homomorphism $f(\cdot,h)\colon g\in G\to f(g,h)\in K$ contains $[G,G]$ in such a way that $f(g,h)=f(g',h)$ for every $g'g^{-1}\in[G,G]$. The same holds for $f(g,\cdot)\colon h\in H\mapsto f(g,h)\in K$ for all fixed $g\in G$. This implies that $f=f'\circ\gamma$ for some $f'\colon\mathcal{Ab}(G)\times\mathcal{Ab}(H)\to K$. Because γ is onto, it can be checked that f' is bilinear. It follows that Ψ is a bijection, and it is even natural in K (see [23]). The last statement then follows from usual category theoretic arguments. □

It follows from lemma 1 that it is unnecessary to consider tensor product for non-abelian groups. This is the reason why bilinear maps are defined on abelian groups.

More generally, it is also possible to define the tensor product of R-modules. Let A,B be two R-modules (in additive notation), and let C be the submodule of $R^{(A\times B)}$ generated by the elements $(a+a',b)-(a,b)-(a',b)$, $(a,b+b')-(a,b)-(a,b')$, $(\alpha a,b)-\alpha(a,b)$, $(a,\alpha b)-\alpha(a,b)$ for all $a,a'\in A$,

$b, b' \in B$, $\alpha \in R$. Then, the quotient R-module $R^{(A\times B)}/C$ is called the *tensor product* of A and B, and is denoted by $A \otimes_R B$. It is the solution of the following universal problem: let D be a R-module, and let $f \in \mathcal{Bil}_R(A \times B, D)$. Then, there exists a unique R-linear map $g\colon A \otimes_R B \to D$ such that $g(a \otimes b) = f(a, b)$ for all $a \in A$, $b \in B$ (where $\otimes\colon A \times B \to A \otimes_R B$ is the restriction to $A \times B$ of the canonical epimorphism from $R^{(A\times B)}$ to $A \otimes_R B$, and it is actually a R-bilinear map also called the *canonical bilinear map*).

Remark 1. Taking R to be $\mathbb{Z}$, then we recover the tensor product of abelian groups and it follows that $\mathcal{Ab}(G) \otimes_{\mathbb{Z}} \mathcal{Ab}(H) \cong G \otimes H \cong \mathcal{Ab}(G) \otimes \mathcal{Ab}(H)$ for every groups G, H. Moreover the maps $(a, b) \in A \times B \mapsto a \otimes b \in A \otimes B$ and $(a, b) \in A \times B \mapsto a \otimes b \in A \otimes_{\mathbb{Z}} B$ are also (essentially) the same, where A, B are abelian groups.

In what follows, if A, B are two abelian groups, then $A \otimes B$ stands for $A \otimes_{\mathbb{Z}} B$ (according to the above remark there is no confusion).

It is clear by construction that $A \otimes_R B$ is spanned as a R-module by $a \otimes b$ where $(a, b) \in A \times B$. Therefore any element of $A \otimes_R B$ is given as a finite sum $\alpha_1(a_1 \otimes b_1) + \cdots + \alpha_n(a_n \otimes b_n)$, $\alpha_i \in R$, $a_i \in A$, $b_i \in B$, $i = 1, \cdots, n$. Such elements are referred to as *tensors* while generating elements of the form $a \otimes b$ are called *elementary* (or *basic*) *tensors*.

Other properties of the tensor product are recalled below. The first result is given without proof since it is easy. The proofs of the two other may be found for instance in [7].

Lemma 2. *Let A and B be two R-modules with respective spanning sets S and T. Then, $A \otimes_R B$ is generated as a R-module by the basic tensors $s \otimes t$, $s \in S$, $t \in T$.*

Lemma 3. *Let A, B be two R-modules. There is a unique isomorphism of R-modules $\sigma\colon A \otimes_R B \cong B \otimes_R A$ such that $\sigma(a \otimes b) = (b \otimes a)$ for every $a \in A$, $b \in B$.*

Lemma 4. *Let A be a R-module, and $(B_i)_{i\in I}$ be a finite family of R-modules (*i.e.*, I is assumed to be a finite set). Then, there is a unique isomorphism of R-modules $\delta\colon A \otimes_R \bigoplus_{i\in I} B_i \cong \bigoplus_{i\in I}(A \otimes_R B_i)$ such that $\delta(a \otimes (b_i)_{i\in I}) = (a \otimes b_i)_{i\in I}$ for every $a \in A$ and $(b_i)_{i\in I} \in \bigoplus_{i\in I} B_i$.*

Remark 2. It may be shown that $\otimes_R$ is also "associative": $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$ for every R-modules A, B, C (this isomorphism is natural in A, B, C). Together with lemma 3, this shows that the category of R-modules with the tensor product is a symmetric monoidal category (see [23]). Loosely speaking this means that the bracketing of factors in a n-fold tensor product is irrelevant (because any two n-fold tensor products that differ only in the position of brackets are canonically isomorphic). The notion of multilinear maps $f\colon A_1 \times \cdots \times A_n \to B$ (where the A_i's and B are R-modules) (see for instance [6, 10, 13, 16, 30]) is equivalent to that of linear maps $f\colon A_1 \otimes_R \cdots \otimes_R A_n \to B$ (bilinear maps are recovered with $n = 2$). In particular, any such multilinear map is actually induced by a unique bilinear map, for instance $f\colon A_1 \times (A_2 \otimes_R \cdots \otimes_R A_n) \to B$. We take advantage of this remark to indicate that the notion of tensor product was already used in [6] (remark 7.1 and subsection 7.2) but in a somewhat limited way since it was not the purpose of the authors. In this contribution we limit ourselves to bilinear maps.

4 Tensor product of finite abelian groups

In this section we focus on the tensor product of finite abelian groups that is even explicitly computed. Moreover we give some conditions under which a pairing may exist.

4.1 Some computations of tensor products

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. In what follows, (a,b) denotes the greatest common divisor of a and b. The cyclic group of integers modulo a is denoted by $\mathbb{Z}_a$ (and also C_a when considered multiplicatively written).

Lemma 5. *For every positive integers a, b, $\mathbb{Z}_a \otimes \mathbb{Z}_b \cong \mathbb{Z}_{(a,b)}$*

Proof. Since (a,b) divides both a and b, the map $f\colon \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{(a,b)}$ given by $f(x \bmod a, y \bmod b) = (xy) \bmod (a,b)$ 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 $\pi((x \bmod a)\otimes(y \bmod b)) = (xy) \bmod (a,b)$. We observe that $\pi((x \bmod a)\otimes 1) = x \bmod (a,b)$ 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, $a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$ belongs to its kernel, and we obtain a homomorphism of groups $g\colon \mathbb{Z}_{(a,b)} \to \mathbb{Z}_a \otimes \mathbb{Z}_b$ such that $g(x \bmod (a,b)) = x(1\otimes 1) = ((x \bmod a)\otimes 1 = 1\otimes(x \bmod b)$ for all x. We have $\pi(g(x \bmod (a,b))) = \pi((x \bmod a)\otimes 1) = x \bmod (a,b)$ 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 $1 \otimes 1$. □

Remark 3. It follows from lemma 5 that $\mathbb{Z}_a \otimes \mathbb{Z}_b = (0)$ if, and only if, a and b are co-prime.

Lemmas 3, 4 and 5 imply the following result that actually covers all examples of finite abelian groups.

Lemma 6. *Let $(a_i)_{i=1}^m$, and $(b_j)_{j=1}^n$ be two families of positive integers. Let $A = \bigoplus_{i=1}^m \mathbb{Z}_{a_i}$, and $B = \bigoplus_{j=1}^n \mathbb{Z}_{b_j}$. Then, $A\otimes B \cong \bigoplus_{\substack{i=1,\cdots,m\\ j=1,\cdots,n}} \mathbb{Z}_{(a_i,b_j)}$ where the isomorphism is given by the unique group homomorphism such that $((x_1 \bmod a_1,\cdots,x_m \bmod a_m)\otimes(y_1 \bmod b_1,\cdots,y_n \bmod b_n)) \mapsto ((x_iy_j) \bmod (a_i,b_j))_{\substack{i=1,\cdots,m\\ j=1,\cdots,n}}$. Moreover, the canonical bilinear map $\otimes$ is then given by $\otimes\colon A\times B \to \bigoplus_{\substack{i=1,\cdots,m\\ j=1,\cdots,n}} \mathbb{Z}_{(a_i,b_j)}$ with $(x_1 \bmod a_1,\cdots,x_m \bmod a_m)\otimes(y_1 \bmod b_1,\cdots,y_n \bmod b_n) = ((x_iy_j) \bmod (a_i,b_j))_{\substack{i=1,\cdots,m\\ j=1,\cdots,n}}$.*

Any finite abelian group A is isomorphic to a direct product $\bigoplus_{p\in P}\left(\bigoplus_{i\in A_p}\mathbb{Z}_{p^i}\right)$ where P is the set of all prime numbers, for each $p \in P$, A_p is a finite subset of $\mathbb{N}_+$ such that all but finitely many A_p's are non-void (hence $\bigoplus_{p\in P}\left(\bigoplus_{i\in A_p}\mathbb{Z}_{p^i}\right)$ is a false infinite sum since $\bigoplus_{i\in\emptyset}\mathbb{Z}_{p^i} \cong (0)$ for every $p \in P$ with $A_p = \emptyset$). This decomposition is unique up to isomorphism, and we refer to it as the *primary decomposition*. All these results make possible to compute $A \otimes B$ for any finite abelian groups A, B using lemma 6, and also to deduce an essential finiteness result for tensor products.

Lemma 7. *The tensor product of two finite groups is finite. Moreover, using the above notations, for every finite abelian groups A, B, the primary decomposition of $A \otimes B$ is given by*

$$A \otimes B \cong \bigoplus_{p\in P}\left(\bigoplus_{i\in A_p}\bigoplus_{j\in B_p}\mathbb{Z}_{p^{\min(i,j)}}\right).$$

Proof. Let A and B be two finite abelian groups. Then each of them admits a decomposition in direct sum of finite cyclic groups, and their tensor product is finite according to lemma 6. Because the tensor product of two groups is isomorphic to the tensor product of their abelianization (lemma 1), the expected conclusion holds (we implicitly used the two easy facts that the abelianization of a finite group is finite, and the isomorphism relation of groups preserves the order). □

Remark 4. The tensor product of two finite groups does not depend on the decomposition of the abelianization of each group into a direct sum of cyclic groups. Indeed, $\otimes$ is a functor (and even a bifunctor), and it is an obvious property of functors to transform isomorphisms into isomorphisms. More precisely, for groups (finite or not) G, G', H, H' such that $G \cong G'$ and $H \cong H'$, then $G \otimes H \cong G' \otimes H'$. The converse assertion is false since for instance $\mathbb{Z}_6 \otimes \mathbb{Z}_4 \cong \mathbb{Z}_2 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$.

4.2 Non-degeneracy of the canonical bilinear map

In this subsection we present a sufficient condition for the canonical bilinear map $\otimes$ to be non-degenerate. We also prove that the canonical bilinear map from $A \times A$ to the tensor square $A \otimes A$ always is non-degenerate for each finite abelian group A, providing an infinite family of pairings.

Lemma 8. *Let a and b be two positive integers. The canonical bilinear map $\otimes\colon (x \bmod a, y \bmod b) \in \mathbb{Z}_a \times \mathbb{Z}_b \to (xy) \bmod (a,b) \in \mathbb{Z}_{(a,b)} \cong \mathbb{Z}_a \otimes \mathbb{Z}_b$ 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 $a = (a,b) = b \neq 1$. Let $x \bmod a \neq 0$ such that for every y, $(xy) \bmod a = 0$, then we obtain a contradiction when $y = 1$. Therefore, $\otimes$ is non-degenerate. Now, let us assume that $(a,b) < a$ for instance. Then, $(a,b) \bmod a \neq 0$, and for all y, $(a,b)y \bmod (a,b) = 0$ so that $\otimes$ is degenerate. □

Let p be a prime number. Let A, B be two finite abelian p-groups (that is, finite abelian groups of order p^n for some n), and C be an abelian group. The theorem of invariant factors imply that $A \cong \bigoplus_{i=1}^{m} \mathbb{Z}_{p^{\alpha_i}}$ with $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_m \geq 1$, and $B \cong \bigoplus_{j=1}^{n} \mathbb{Z}_{p^{\beta_j}}$ with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n \geq 1$. We recall that the *exponent* $\mathit{exp}(G)$ of a finite group G is the least common multiple of the orders of the elements of G. 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, $f((\mathit{exp}(B)1, 0, \cdots, 0), (y_1, \cdots, y_n)) = f((1,0,\cdots,0), \mathit{exp}(B)(y_1, \cdots, y_n)) = f((1,0,\cdots,0),(0,\cdots,0)) = 1$ for every $y_1, \cdots, y_n$. Thus f would be degenerate. Therefore, $\mathit{exp}(A) = \mathit{exp}(B)$. The following lemma is thus proved.

Lemma 9. *Let A, B be two finite abelian p-groups, and C be an abelian group. Let $f\colon A \times B \to C$ be a pairing. Then, $\mathit{exp}(A) = \mathit{exp}(B)$.*

Let $A \cong \bigoplus_{p \in P} A(p)$ and $B \cong \bigoplus_{p \in P} B(p)$ be the primary decomposition of two finite abelian groups A and B. For each prime number p, let $A(p) \cong \bigoplus_{i=1}^{n_A(p)} \mathbb{Z}_{p^{\alpha_i}}$ and $B(p) \cong \bigoplus_{j=1}^{n_B(p)} \mathbb{Z}_{p^{\beta_j}}$ be the invariant factor decomposition of each factor of the primary decomposition. Let p, q be two distinct prime numbers. Then by lemma 6, $A(p) \otimes B(q) \cong \bigoplus_{i=1}^{n_A(p)} \bigoplus_{j=1}^{n_B(p)} \mathbb{Z}_{(p^{\alpha_i}, q^{\beta_j})} \cong (0)$. Thus, again by lemma 6, $A \otimes B \cong \bigoplus_{p \in P} A(p) \otimes B(p)$. Let $f\colon A \times B \to A \otimes B$ be a bilinear map. Then, $f(a,b) = 0$ for every $a \in A(p)$, $b \in B(q)$ with distinct prime numbers p, q. For each prime number p, let $f_p\colon A(p) \times B(p) \to A(p) \otimes B(p)$ be the obvious restriction of f, which also is a bilinear map. Then, $f((a_p)_{p \in P}, (b_p)_{p \in P}) = (f_p(a_p, b_p))_{p \in P}$. In particular $\otimes_p\colon A(p) \times B(p) \to A(p) \otimes B(p)$ is the corresponding canonical bilinear map so that $(a_p)_{p \in P} \otimes (b_p)_{p \in P} = (a_p \otimes_p b_p)_{p \in P}$.

Theorem 1. *Using the above notations, 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 (and in particular, according to lemma 9,* $\mathit{exp}(A(p)) = \mathit{exp}(B(p))$*). More generally,* $f \in \mathcal{Bil}(A \times B, A \otimes B)$ *is a pairing if, and only if,* $f_p \in \mathcal{Bil}(A(p) \times B(p), A(p) \otimes B(p))$ *is a pairing for each prime number* p*.*

Proof. It is obviously sufficient to prove the second assertion. It is clear that non-degeneracy of all f_p implies non-degeneracy of f. Now, let us assume that f is non-degenerate but there is some prime number p_0 and $a \in A(p_0)$, $a \neq 0$ such that $f_p(a, b) = 0$ for every $b \in B(p)$. Then, let us consider $(a_p)_{p\in P} \in A$ such that $a_p = 0$ for every $p \neq p_0$, and $a_{p_0} = a$. Then, for every $(b_p)_{p\in P} \in B$, $f((a_p)_p, (b_p)_p) = 0$ which contradicts non-degeneracy of f. □

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

Lemma 10. *Let* A, B *be two non-trivial* R*-modules. If there are a* R*-module* C *and a pairing* $\langle \cdot \mid \cdot \rangle\colon A \times B \to C$*, then the canonical bilinear map* $\otimes\colon A \times B \to A \otimes_R B$ *is non-degenerate.*

Proof. By contraposition, let us assume that $\otimes\colon A \times B \to A \otimes_R B$ is degenerate, and for instance that it is not left non-degenerate. Then, 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 R-linear map $f\colon A \otimes_R B \to C$ such that $f(a \otimes b) = \langle a \mid b \rangle$. In particular, $\langle a_0 \mid b \rangle = f(a_0 \otimes b) = f(0) = 1_C$ for all $b \in B$. Therefore, $\langle \cdot \mid \cdot \rangle$ is left degenerate. □

We anticipate a result from subsection 5.4 to state a sufficient condition for the existence of a pairing, from the cartesian square to the tensor square of some abelian group, provided by the following result.

Theorem 2. *Let* A *be a finite abelian group. Then, the canonical bilinear map* $\otimes\colon A \times A \to A \otimes A$ *is non-degenerate.*

Proof. Since A is a finite abelian group, it admits a decomposition into cyclic groups $A \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}$ for some integers d_i. In subsection 5.4 is proved that there exists at least one pairing $(\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}) \times (\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}) \to C_N$, where C_N denotes the cyclic group of order N, with $N = \prod_{i=1}^{n} d_i$. Therefore according to lemma 10, the canonical bilinear map $\otimes\colon (\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}) \times (\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}) \to (\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}) \otimes (\bigoplus_{i=1}^{n} \mathbb{Z}_{d_i})$ is non-degenerate. Let $\phi\colon A \to \bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}$ be an isomorphism of groups. Let us assume that there exists $a_0 \in A$ such that $a_0 \otimes a = 0$ for every $a \in A$. Then, $\phi(a_0) \otimes \phi(a) = 0$ for every $a \in A$. Since ϕ is onto, this implies that $\phi(a_0) \otimes a' = 0$ for every $a' \in \bigoplus_{i=1}^{n} \mathbb{Z}_{d_i}$. So that $\phi(a_0) = 0$ (by non-degeneracy), and thus $a_0 = 0_A$. □

Remark 5. Theorem 2 provides an infinite family of pairings because in this situation $\otimes$ is itself a pairing. This generalizes some optimized constructions of pairings over elliptic curves on finite fields as defined in [14] such as Weil ([25]), Tate ([33]) and ate ([15]) pairings which may be defined on $\mathbb{Z}_a \times \mathbb{Z}_a$ for some integer a and with values in the group of a-th roots of the unity $\mu_a \cong \mathbb{Z}_a \cong \mathbb{Z}_a \otimes \mathbb{Z}_a$ in a finite field $\mathbb{F}_{p^n}$ (where a divides $p^n - 1$). We observe however that these pairings are usually defined on a bigger cartesian product of groups (see for instance [31] concerning Weil pairing).

Remark 6. We also observe that there are some pairings $f\colon A \times B \to C$ where A, B, C are finite abelian groups such that A and B are non-isomorphic. For instance, let p be a prime number, and $m > 1$ be an integer. Then, 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 Constructions of bilinear maps and pairings

In full generality the canonical bilinear map is not always non-degenerate (even when the tensor product does not collapse to zero, see the discussion after lemma 10). As stated in lemma 10, non-degeneracy of this function is a necessary condition for the existence of pairings. In this section, we present other constructions of bilinear maps and pairings using the fact that the set of all bilinear maps, from some fixed $A \times B$ to C, forms an abelian group (or R-module). Moreover we prove that for a particular choice of A, B and C, $\mathcal{Bil}(A \times B, C)$ is actually a ring, and that the pairings are exactly the group of units of this ring (see theorem 3).

5.1 Abelian group structure of bilinear maps (and pairings)

First of all, we know from the proof of lemma 1 that for every groups G, H, K, $\mathcal{Bil}(G \times H, K) \cong \mathcal{Bil}(\mathcal{Ab}(G) \times \mathcal{Ab}(H), K)$. According to the universal property of tensor product of groups, $\mathcal{Bil}(G \times H, K) \cong \mathcal{Hom}(G \otimes H, K)$. Therefore, for every triple of abelian groups (respectively, R-modules) A, B, C, $\mathcal{Bil}(A \times B, C) \cong \mathcal{Hom}(A \otimes B, C)$ (respectively, $\mathcal{Bil}_R(A \times B, C) \cong \mathcal{Hom}_R(A \otimes_R B, C)$). But the later is itself an abelian group (respectively, a R-module) with point-wise operations, so that $\mathcal{Bil}(A \times B, C)$ (respectively, $\mathcal{Bil}_R(A \times B, C)$) becomes an abelian group (respectively, a R-module). More precisely, let A, B, C be three R-modules, and let us assume that A, B are given in additive notation (recall that $0_A, 0_B$ are the identity elements of A and B) and C is multiplicatively written (recall that 1_C is the identity of C), we have for $f, g \in \mathcal{Bil}_R(A \times B, C)$ and $\alpha \in R$, three new bilinear maps fg, f^{-1}, $f^\alpha \in \mathcal{Bil}_R(A \times B, C)$ defined by $(fg)(a, b) = f(a, b)g(a, b)$, $f^{-1}(a, b) = (f(a, b))^{-1}$ and $f^\alpha(a) = (f(a))^\alpha$ (where the scalar multiplication in C is given by $(\alpha, c) \mapsto c^\alpha$ because C is assumed to be in multiplicative notation) for all $a \in A$, $b \in B$. This also defines a structure of $\mathbb{Z}$-module given by $f^n(a, b) = (f(a, b))^n$ for all $a \in A$, $b \in B$, $n \in \mathbb{Z}$. The following (obvious) construction uses direct product of modules (or abelian groups).

Lemma 11. *Let $(C_i)_{i=1}^n$ be a family of R-modules, and A, B be R-modules. Let $f_i \in \mathcal{Bil}_R(A \times B, C_i)$ for $i = 1, \cdots, n$. Then, the map $(f_1, \cdots, f_n) \colon A \times B \to C_1 \times \cdots \times C_n$ defined by $(f_1, \cdots, f_n)(a, b) = (f_1(a, b), \cdots, f_n(a, b))$ belongs to $\mathcal{Bil}_R(A \times B, C_1 \times \cdots \times C_n)$. Moreover, if at least one of the f_i's is non-degenerate, then $(f_1, \cdots, f_n)$ itself is non-degenerate.*

Let us study the group structure of $\mathcal{Bil}(A \times B, C)$ in an easy case. For every group G, let $\mathcal{End}(G) = \mathcal{Hom}(G, G)$ which is a ring when G is abelian. Let a, b be two positive integers. Then, we have the following sequence of group isomorphisms $\mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{(a,b)}) \cong \mathcal{Hom}(\mathbb{Z}_a \otimes \mathbb{Z}_b, \mathbb{Z}_{(a,b)}) \cong \mathcal{End}(\mathbb{Z}_{(a,b)})$. It easy to check that $\mathcal{End}(\mathbb{Z}_n) \cong \mathbb{Z}_n$ as rings for any n. So that $\mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{(a,b)})$ may also be equipped with a structure of commutative ring with a unit isomorphic to $\mathbb{Z}_{(a,b)}$. Moreover, as a cyclic group of order (a, b), and therefore as a $\mathbb{Z}$-module, $\mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{(a,b)})$ is generated by the canonical bilinear map $\otimes$. Thus $\mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_{(a,b)})$ is the free $\mathbb{Z}_{(a,b)}$-module generated by $\otimes$, or, in other terms, it is isomorphic to the group $\mathbb{Z}_{(a,b)}$, so that for any bilinear map $f \colon \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{(a,b)}$, there exists a unique $k_f \in \mathbb{Z}_{(a,b)}$ such that $f = \otimes^{k_f}$, where we recall that $\otimes^{k_f}(x \bmod a, y \bmod b) = k_f xy \bmod (a, b)$. It follows that if $\otimes$ is non-degenerate, then f is a pairing if, and only if, $(k_f, (a, b)) = 1$. Moreover, if $\otimes$ is degenerate, then there is no pairing defined on $\mathbb{Z}_a \times \mathbb{Z}_b$ by lemma 10. Thus, according to lemma 8, a pairing $f \in \mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$ is exactly a generator of the cyclic group $\mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$ of order a. The following result is proved.

Theorem 3. *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 of the ring $\mathbb{Z}_a$ under multiplication. In particular, there are exactly $\phi(a)$ pairings*

in this situation, and if $f \in \mathcal{Bil}(\mathbb{Z}_a \times \mathbb{Z}_a, \mathbb{Z}_a)$ is a pairing, then any other pairing g has the form f^{k_g}, for a unique $k_g \in \mathbb{Z}_a$ invertible modulo a. Moreover, if p is a prime number, then the group of pairings in $\mathcal{Bil}(\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p^*$.

Remark 7. Let p be a prime number. Let $f \in \mathcal{Bil}(\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p)$ be a pairing. According to theorem 3, any other pairing is given by f^k for $k \in \mathbb{Z}_p^*$ as it was already noticed in [8] (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 write in [34] that "there is essentially only one pairing".

Let $A \cong \bigoplus_{p\in P} A(p)$ and $B \cong \bigoplus_{p\in P} B(p)$ be two finite abelian groups decomposed following the primary decomposition (each $A(p)$ and $B(p)$ are finite abelian p-groups). For each prime number p, $\mathcal{Bil}(A(p) \times B(p), A(p) \otimes B(p)) \cong \mathcal{End}(A(p) \otimes B(p))$ so that $\mathcal{Bil}(A(p) \times B(p), A(p) \otimes B(p))$ admits a ring structure. From the discussion preceding theorem 1, we know that $\mathcal{Bil}(A \times B, A \otimes B) \cong \bigoplus_{p\in P} \mathcal{Bil}(A(p)\times B(p), A(p)\otimes B(p))$ (group direct sum). Let us assume that for each prime number p, $A(p) = \mathbb{Z}_{p^{n_p}} = B(p)$ (the case $n_p = 0$ is necessarily possible in such a way $A(p) = (0) = B(p)$). Then, according to theorem 3, for each p, the pairings in $\mathcal{Bil}(A(p) \times B(p), A(p) \otimes B(p)) \cong \mathbb{Z}_{p^{n_p}}$ form the group $\mathbb{Z}_{p^{n_p}}^\times$ of invertible elements modulo p^{n_p}, and by theorem 1 the pairings in $\mathcal{Bil}(A\times B, A\otimes B) \cong \bigoplus_{p\in P} \mathbb{Z}_{p^{n_p}}$ is the group direct sum $\bigoplus_{p\in P} \mathbb{Z}_{p^{n_p}}^\times$. Again by theorem 3, if $n_p \in \{ 0, 1 \}$ for every prime number p, then the pairings in $\mathcal{Bil}(A \times B, A \otimes B) \cong \bigoplus_{p\in P} \mathbb{Z}_{p^{n_p}}$ is the group direct sum $\bigoplus_{p\in P_0} \mathbb{Z}_p^*$ (where $P_0 = \{ p \in P \colon n_p = 1 \}$).

5.2 Tensor product of linear maps

One of the main feature of the tensor product that has not been used yet in this contribution is the fact $\otimes_R$ is a bifunctor. In particular, it transforms a pair of linear maps into one linear map as follows. Let A_1, A_2, B_1, B_2 be four R-modules. Let $f \colon A_1 \to A_2$, $g \colon B_1 \to B_2$ be two R-linear maps. Then, the map $f \otimes g \colon A_1 \otimes_R B_1 \to A_2 \otimes_R B_2$ defined by $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$ is a R-module map (be careful that the same symbol $\otimes$ denotes the canonical bilinear map $A_i \times B_i \to A_i \otimes_R B_i$ for $i = 1, 2$). Since $\mathcal{Bil}_R(A_1 \times B_1, A_2 \otimes_R B_2) \cong \mathcal{Hom}_R(A_1 \otimes_R B_1, A_2 \otimes_R B_2)$, it follows that $f \otimes g$ is induced by a (unique) R-bilinear map $h \colon A_1 \times B_1 \to A_2 \otimes_R B_2$ such that $h(a, b) = f(a) \otimes g(b)$ for $a \in A_1$, $b \in B_1$.

Lemma 12. *Let us assume that f is a monomorphism, g is an epimorphism, and that the canonical R-bilinear map $\otimes \colon A_2 \times B_2 \to A_2 \otimes_R B_2$ is non-degenerate, then h is left non-degenerate.*

Proof. Let $a \in A_1$ such that for every $b \in B_1$, $h(a, b) = 0$. Then, $f(a) \otimes g(b) = 0$ for every $b \in B$. Since g is onto, $f(a) \otimes b' = 0$ for all $b' \in B_2$. Since the canonical bilinear map is non-degenerate, $f(a) = 0_{A_2}$, so that $a = 0_{A_1}$ because f is one-to-one. □

5.3 Divide out the kernels

In this subsection is presented a natural way to construct a pairing from a bilinear map by dividing out two kernels.

Let A, B, C be three R-modules (where R is a commutative ring with a unit). The groups A, B are written additively, while C is given in multiplicative notation. Let $f \colon A \times B \to C$ be a R-bilinear map. We define two linear maps $\gamma_f \colon A \to \mathcal{Hom}_R(B, C)$ and $\rho_f \colon B \to \mathcal{Hom}_R(A, C)$ given

respectively by $\gamma_f(a) = f(a,\cdot)$ and $\rho_f(b) = f(\cdot,b)$. Let us define $L_f = \bigcap_{b\in B} \ker f(\cdot,b) = \ker \gamma_f$, $R_f = \bigcap_{a\in A} \ker f(a,\cdot) = \ker \rho_f$ which are respectively a sub-module of A and a sub-module of B (they are sometimes called the *annihilator* of A and B respectively, see [11]). We observe that if $a - a' \in L_f$, then for all $b \in B$, $f(a,b)f(a',b)^{-1} = f(a-a',b) = 1_C$ so that $f(a,b) = f(a',b)$. Therefore, there is a well-defined R-bilinear map $f_1 \colon A/L_f \times B \to C$ such that $f_1(a \bmod L_f, b) = f(a,b)$ for all $a \in A$, $b \in B$. Similarly, we have a well-defined R-linear map $f_2 \colon A \times B/R_f \to C$ such that $f_2(a, b \bmod R_f) = f(a,b)$ for all $a \in A$, $b \in B$. The first map is left non-degenerate while the second is right non-degenerate. We may continue the process in order to get a full non-degeneracy. Let $R_{f_1} = \bigcap_{a \bmod L_f \in A/L_f} \ker f_1(a \bmod L_f, \cdot) = R_f$. Similarly we have $L_{f_2} = L_f$. We obtain two well-defined non-degenerate R-bilinear maps $f_3, f_4 \colon A/L_f \times B/R_f \to C$ such that

$$\begin{aligned} f_3(a \bmod L_f, b \bmod R_f) &= f_1(a \bmod L_f, b) \\ &= f(a,b) \\ &= f_2(a, b \bmod R_f) \\ &= f_4(a \bmod L_f, b \bmod R_f) \end{aligned} \tag{1}$$

for each $a \in A$ and $b \in B$. Thus the two pairings are the same one.

When the bilinear map f into consideration is the canonical bilinear map $\otimes \colon A \times B \to A \otimes_R B$ itself, then we define ${}^\perp B = L_\otimes$, and $A^\perp = R_\otimes$. Moreover, let $\lambda \colon A \to A/{}^\perp B$ and $\delta \colon B \to B/A^\perp$ be the canonical epimorphisms. We have a well-defined non-degenerate pairing $\otimes' \colon A/{}^\perp B \times B/A^\perp \to A \otimes_R B$ such that $\lambda(a) \otimes' \delta(b) = a \otimes b$ for every $a \in A$, $b \in B$. Let us define $\tilde{\otimes} = (\lambda \otimes \delta) \circ \otimes' \in \mathcal{B}il_R(A/{}^\perp B \times B/A^\perp, A/{}^\perp B \otimes_R B/A^\perp)$. It satisfies $(\lambda \otimes \delta)(\lambda(a) \otimes' \delta(b)) = (\lambda \otimes \delta)(a \otimes b) = \lambda(a) \otimes_2 \delta(b)$ for every $a \in A$, $b \in B$, where $\otimes_2 \colon A/{}^\perp B \times B/A^\perp \to A/{}^\perp B \otimes_R B/A^\perp$ is the canonical bilinear map. Actually it is quite clear that $\tilde{\otimes} = \otimes_2$.

Lemma 13. *The canonical bilinear map $\otimes_2 \colon A/{}^\perp B \times B/A^\perp \to A/{}^\perp B \otimes_R B/A^\perp$ is non-degenerate.*

Proof. The bilinear map $\otimes' \colon A/{}^\perp B \times B/A^\perp \to A \otimes_R B$ is non-degenerate. Then according to lemma 10, the canonical bilinear map $\otimes_2 \colon : A/{}^\perp B \times B/A^\perp \to A/{}^\perp B \otimes_R B/A^\perp$ is itself non-degenerate. □

5.4 Finite abelian group duality and characters

Let A, B, C be three R-modules. One of the main property of a given pairing $\langle \cdot \mid \cdot \rangle \colon A \times B \to C$ is the non-degeneracy. It exactly states that A embeds into $\mathcal{H}om_R(B,C)$ as a sub-module by $\langle a \mid \cdot \rangle \colon B \to C$ for each $a \in A$, and that B embeds into $\mathcal{H}om_R(A,C)$ also as a sub-module by $\langle \cdot \mid b \rangle \colon A \to C$ for each $b \in B$. Using this idea we may construct a pairing. Let A, C be two R-modules, and let B be a sub-module of $\mathcal{H}om_R(A,C)$. Let $\langle \cdot \mid \cdot \rangle \colon A \times B \to C$ be defined by $\langle a \mid b \rangle = b(a)$ for every $a \in A$, $b \in B$. By its very definition, this is a R-bilinear map which clearly is right non-degenerate. We observe that the elements of A may be seen as linear maps on B as follows: let $a \in A$, and define $\widehat{a} \colon B \to C$ by $\widehat{a}(b) = b(a)$. The facts that $\widehat{a} \in \mathcal{H}om_R(B,C)$ and $\widehat{(\cdot)} \colon a \in A \to \widehat{a} \in \mathcal{H}om_R(B,C)$ is a homomorphism of groups are easily checked. We say that A *seperates the points of* B (following a usual terminology from functional analysis) if $b(a) = 0_C$ for every $b \in B$ implies that $a = 0_A$. Equivalently, this means that the map $\widehat{a} = \langle a \mid \cdot \rangle$ is one-to-one for every non-zero a, so that A embeds into $\mathcal{H}om_R(B,C)$ as a sub-module. In this case, and only in this case, $\langle \cdot \mid \cdot \rangle$ as defined above is a pairing. We now propose two actual examples of such a construction.

Dot-product construction: Let $\mathbb{K}$ be any field. Let V be a d-dimensional vector space over $\mathbb{K}$. Its *(algebraic) dual* V^* is the vector space $\mathcal{Hom}_{\mathbb{K}}(V,\mathbb{K})$ of all linear forms. We observe that V separates the points of V^* since if $v \in V$ is non-zero, then it belongs to some basis of V over $\mathbb{K}$ so that we may choose a linear map $\ell\colon V \to \mathbb{K}$ such that $\ell(v) \neq 0$ and ℓ takes any value for the other elements of the basis. Therefore the $\mathbb{K}$-bilinear form $\langle \cdot \mid \cdot \rangle\colon V \times V^* \to \mathbb{K}$ given by $\langle v \mid \ell \rangle = \ell(v)$ is a pairing. Moreover, if $(e_i)_{i=1}^d$ is a basis of V over the base field, then for each $j = 1, \cdots, d$, we may define a linear form $e^j \in V^*$ by the relations $e^j(e_i) = 1$ if $j = i$, and 0 otherwise. It turns that $(e^i)_{i=1}^d$ is a basis of V^* over $\mathbb{K}$ called the *dual basis* of $(e_i)_{i=1}^d$, and that $V \cong V^*$ (as vector spaces). Under the isomorphism $e^i \mapsto e_i$, the pairing becomes $\langle v \mid w \rangle = \sum_{i=1}^d v_i w_i$, where $v_i = e^i(v)$, $w_i = e^i(w)$ for each $i = 1, \cdots, d$, and we recover the usual dot-product of $\mathbb{K}^d$.

Remark 8. The above construction works in particular when $\mathbb{K}$ is the finite field $\mathbb{F}_{p^n}$ with p^n elements of characteristic p. In this case, any finite-dimensional vector space is actually finite, and we obtain a pairing between finite spaces (and therefore finite abelian groups). When $n = 1$, we recover the construction of "dual pairing vector space" from [26, 27].

Generalized duality of finite abelian groups: Let C_N be a cyclic group of order N, with generator γ. Let A be any finite abelian group. A homomorphism of group $\chi\colon A \to C_N$ is called a *character*. Since for every $a \in A$, $a^{|A|} = 1_A$, it follows that $\chi(a)^{|A|} = 1$. Let d be a divisor of N, and let $\chi \in \mathcal{Hom}(\mathbb{Z}_d, C_N)$. Since for every x, $\chi(x \bmod d)^d = 1$, it follows that $\mathsf{im}(\chi)$ is a subgroup of the unique cyclic subgroup C_d of C_N of order d. Therefore, $\chi(x \bmod d) = \gamma^{\frac{N}{d}j}$ for some $j = 0, \cdots, d-1$ that depends on both χ and x. In particular, we have $\chi(1) = \gamma^{\frac{N}{d}i}$ for some i, and then, $\chi(x \bmod d) = \chi(x1) = \chi(1)^x = \gamma^{\frac{N}{d}ix \bmod d}$. This means that all characters of $\mathbb{Z}_d$ have the form $\chi_i\colon \mathbb{Z}_d \to C_N$ with $\chi_i(x \bmod d) = \gamma^{\frac{N}{d}ix}$ for $i = 1, \cdots, d$. It is not difficult to check that $\Psi\colon \mathbb{Z}_d \to \mathcal{Hom}(\mathbb{Z}_d, C_N)$ given by $\Psi(i) = \chi_i$ is a group isomorphism. (Such a generalized approach for group characters has been used in [28] for other purposes.)

Lemma 14. *Let d_1, d_2 be two divisors of N. Then, $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ and $\mathcal{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}, C_N)$ are isomorphic.*

Proof. The proof is easy since it suffices to observe that $\mathcal{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}, C_N)$ and $\mathcal{Hom}(\mathbb{Z}_{d_1}, C_N) \times \mathcal{Hom}(\mathbb{Z}_{d_2}, C_N)$ are isomorphic since we already know that $\mathcal{Hom}(\mathbb{Z}_{d_i}, C_N)$ is isomorphic to $\mathbb{Z}_{d_i}$ for $i = 1, 2$. Let $q_i\colon \mathbb{Z}_{d_i} \to \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ be the canonical injection for $i = 1, 2$. Let us define the homomorphism of groups $\Phi\colon \mathcal{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}, C_N) \to \mathcal{Hom}(\mathbb{Z}_{d_1}, C_N) \times \mathcal{Hom}(\mathbb{Z}_{d_2}, C_N)$ by $\Phi(\chi) = (\chi \circ i_1, \chi \circ i_2)$ which is obviously one-to-one. For $\chi^{(i)} \in \mathcal{Hom}(\mathbb{Z}_{d_i}, C_N)$, $i = 1, 2$, the map $\chi\colon (x_1, x_2) \mapsto \chi^{(1)}(x_1)\chi^{(2)}(x_2)$ belongs to $\mathcal{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}, C_N)$, and $\Phi(\chi) = (\chi^{(1)}, \chi^{(2)})$. □

From lemma 14 (and its proof), it is easy to see that $\mathcal{Hom}(\bigoplus_{i=1}^m \mathbb{Z}_{d_i}^{m_i}, C_N) \cong \bigoplus_{i=1}^m \mathcal{Hom}(\mathbb{Z}_{d_i}, C_N)^{m_i} \cong \bigoplus_{i=1}^m \mathbb{Z}_{d_i}^{m_i}$ for every divisor d_i of N and every integer m_i, $i = 1, \cdots, m$. For each $i = 1, \cdots, m$, and $x = (x_1, \cdots, x_{m_i}), y = (y_1, \cdots, y_{m_i}) \in \mathbb{Z}_{d_i}^{m_i}$, we define a *dot-product*

$$x \cdot y = \sum_{j=1}^{m_i} (x_j y_j) \bmod d_j \ .$$

Therefore, an isomorphism from $\bigoplus_{i=1}^m \mathbb{Z}_{d_i}^{m_i}$ to $\mathcal{Hom}(\bigoplus_{i=1}^m \mathbb{Z}_{d_i}^{m_i}, C_N)$ may be given by $\Psi(a^{(1)}, \cdots, a^{(m)}) = \chi_{a^{(1)}, \cdots, a^{(m)}}$ for each $a^{(i)} \in \mathbb{Z}_{d_i}^{m_i}$, $i = 1, \cdots, m$, where

$$\chi_{a^{(1)}, \cdots, a^{(m)}}(x^{(1)}, \cdots, x^{(m)}) = \prod_{i=1}^m \gamma^{\frac{N}{d_i} a^{(i)} \cdot x^{(i)}}$$

for every $(x^{(1)},\cdots,x^{(m)}) \in \bigoplus_{i=1}^{m} \mathbb{Z}_{d_i}^{m_i}$ (so that $x^{(i)} \in \mathbb{Z}_{d_i}^{m_i}$ for each $i = 1,\cdots,m$). Consequently, one obtains a bilinear map $\langle \cdot \mid \cdot \rangle \colon \bigoplus_{i=1}^{m} \mathbb{Z}_{d_i}^{m_i} \times \bigoplus_{i=1}^{m} \mathbb{Z}_{d_i}^{m_i} \to C_N$ such that

$$\langle (x^{(1)},\cdots,x^{(m)}) \mid (y^{(1)},\cdots,y^{(m)}) \rangle = \prod_{i=1}^{m} \gamma^{\frac{N}{d_i} x^{(i)} \cdot y^{(i)}}$$

(where $x^{(i)}, y^{(i)} \in \mathbb{Z}_{d_i}^{m_i}$, $i = 1,\cdots,m$) which is right non-degenerate by construction. But this bilinear map is clearly symmetric, therefore it is actually non-degenerate and it defines a pairing.

Example 3. Let $A = \bigoplus_{i=1}^{m} \mathbb{Z}_{d_i}^{m_i}$ for some integer m.

1. Let γ be a primitive element of the finite field $\mathbb{F}_{p^k}$ (see [20]). Let us assume that d_i is a divisor of $p^k - 1$ for all $i = 1,\cdots,m$. Then, we obtain a pairing from $A \times A$ to $\mathbb{F}_{p^k}^*$ given by $\langle (x^{(1)},\cdots,x^{(m)}) \mid (y^{(1)},\cdots,y^{(m)}) \rangle = \gamma^{\sum_{i=1}^{m} \frac{p^k-1}{d_i} (x^{(i)} \cdot y^{(i)})}$.
2. Let $\gamma = e^{\frac{2i\pi}{N}}$ be a primitive N-th square root of unity in the complex field. Let d_i be a divisor of N for each $i = 1,\cdots,m$. Then, we obtain a pairing from $A \times A$ to $\mathbb{C}^*$ given by $\langle (x^{(1)},\cdots,x^{(m)}) \mid (y^{(1)},\cdots,y^{(m)}) \rangle = e^{\sum_{i=1}^{m} \frac{2i\pi}{d_i} (x^{(i)} \cdot y^{(i)})}$.

Remark 9. The above construction still works when we consider usual group characters (see [22]) as it is shown in the second point of example 3. Let A be an abelian group. In the classical setting a *character* is a homomorphism of groups from A to the multiplicative group $\mathbb{C}^*$. Torsion in A implies that the image of a character belongs to the group of complex $\mathit{exp}(A)$-th roots of unity $C_{\mathit{exp}(A)}$. It is clear that for every decomposition of A into a sum of cyclic groups $\bigoplus_{i=1}^{m} \mathbb{Z}_{d_i}^{m_i}$, d_i divides $\mathit{exp}(A)$ (since A contains an element of order d_i for each i). The above machinery works. Moreover it may be recovered as follows in an abstract setting: let us denote by $\widehat{A} = \mathcal{H}om(A, C_{\mathit{exp}(A)})$ the group of characters, called *dual group of* A. It is well-known that the double dual $\widehat{\widehat{A}}$ is naturally isomorphic to A. The natural bilinear map $\langle \cdot \mid \cdot \rangle \colon A \times \widehat{A} \to C_{\mathit{exp}(A)}$ is given by $\langle a \mid \chi \rangle = \chi(a)$. It is clearly right non-degenerate. Left non-degeneracy follows from $A \cong \widehat{\widehat{A}}$. Indeed, the isomorphism into consideration is given by $\widehat{a}(\chi) = \chi(a)$ for every $a \in A$, $\chi \in \widehat{A}$. Therefore, $\widehat{a}(\chi) = \chi(a) = 1$ for every $\chi \in \widehat{A}$ implies that $\widehat{a} \equiv 1$ which is equivalent to $a = 0_A$. According to lemma 10, this means that for every finite abelian group A, the canonical bilinear map $\otimes \colon A \times A \to A \otimes A$ is non-degenerate.

References

1. Bajard, J.C., Imbert, L., Negre, C., and Plantard, T.: Efficient multiplication in $GF(p^k)$ for elliptic curve cryptography. In: ARITH 16, 16th IEEE Symposium on Computer Arithmetic: 181-187, 2003
2. Baer, R.: Groups with Abelian central quotient group. Transactions of the American Mathematical Society 44(3): 357–386, 1938.
3. Bahturin, Yu., Mikhalev, A.V., Petrogradsky, V.M., and Zaicev, M.V.: Infinite dimensional Lie superalgebras. Volume 7 of De Gruyter Expositions in Mathematics, 1992
4. Blake, I.F., Seroussi, G., and Smart, N.P.: Advances in elliptic curve cryptography. London Mathematical Society, Lecture Note Series, Cambridge University Press 2005.
5. Boneh, D. and Franklin, M. K.: Identity-based encryption from the Weil pairing. SIAM Journal of Computing 32(3): 586–617, 2003

6. Boneh, D., and Silverberg, A.: Applications of multilinear forms to cryptography. Contemporary Mathematics 324: 71–90, 2003
7. Bourbaki, N.: Elements of mathematics - Algebra, chapters 1 to 3. Springer (1998)
8. Boxall, J., and Enge, A.: Some security aspects of pairing-based cryptography. Technical report of the ANR Project PACE, 2009
9. Clifford, A.H., and Preston, G.B.: The algebraic theory of semigroups - volume 2. Volume 7 of Mathematical Surveys and Monographs, American Mathematical Society (1967)
10. Coron, J.-S., Lepoint, T., and Tibouchi, M.: Practical multilinear maps over integer. Cryptology ePrint Archive, Report 2013/183, 21 pages, 2013
11. Eilenberg S., and Mac Lane, S.: Group extensions and homology. Annals of Mathematics 43(4): 757–831, 1942
12. El Mrabet, N., Guilevic, A., and Ionica, S.: Efficient multiplication in finite field extensions of degree 5. In: Proceeding of AFRICACRYPT'11. Lecture Notes in Computer Science 6737: 188–205, 2011
13. Garg, S., Gentry, C., and Halevi, S.: Candidates multilinear maps from ideal lattices. Cryptology ePrint Archive, Report 2012/610, 54 pages, 2012
14. Heß, F.: Pairing lattices. In: Proceedings of Pairing '08, Steven D. Galbraith, Kenneth G. Paterson (Eds.). Lecture Notes in Computer Science 5209: 18–38, 2008
15. Heß, F., Smart, N., and Vercauteren, F.: The Eta-pairing revisited. IEEE Transactions on Information Theory 53 (10): 4595–4602, 2006
16. Huang, M.-D., and Raskind, W.: A multilinear generalization of the Tate pairing. In: McGuire, G., et al. (eds.) Finite Fields. Theory and Applications. Proceedings of the 9th International Conference on Finite Fields and Applications, Dublin, Ireland, July 13-17, American Mathematical Society (AMS), Providence (2009); Contemporary Mathematics 518, 255-263, 2010
17. Hungerford, T.W.: Algebra. Volume 73 in the series Graduate Texts in Mathematics, Springer, 1974
18. Joux, A.: A One Round Protocol for Tripartite Diffie-Hellman, ANTS, LNCS 1838: 385–394, 2000.
19. Joye, M., and Neven, G.: Identity-based cryptography. Volume 2 of Cryptology and Information Security Series, IOS Press, 2009
20. Lidl, R., and Niederreiter, H.: Finite fields (2nd ed.). Cambridge University Press, 1997
21. 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
22. Luong, B.: Fourier analysis on finite abelian groups. Applied and Numerical Harmonic Analysis, Birkhäuser (2009)
23. Mac Lane, S.: Categories for the working mathematician. Volume 5 of Graduate Texts in Mathematics, Springer (1971)
24. 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
25. Miller, V.S.: The Weil pairing, and its efficient calculation. Journal of Cryptology 17 (4): 235–261, 2004
26. Okamoto, T., and Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Proceedings of Pairing '08, Steven D. Galbraith, Kenneth G. Paterson (Eds.). Lecture Notes in Computer Science 5209: 57–74, 2008
27. Okamoto, T., and Takashima, K.: Hierarchical predicate encryption for inner-products. In: Proceedings of Asiacrypt 2009, M. Matsui (Ed.). Lecture Notes in Computer Science 5912: 214–231, 2009
28. Poinsot, L.: Harmonic analysis and a bentness-like notion in certain finite Abelian groups over some finite fields. Preprint arXiv:1304.1731, 20 pages, 2013
29. Ree, R.: Generalized Lie elements. Canadian Journal of Mathematics 12: 493–502, 1960
30. Rothblum, R.: On the circular security of bit-encryption. In: Proceedings of 10th Theory of Cryptography Conference, TCC 2013, Amith Sahai (Ed.). Lecture Notes in Computer Science 7785: 579–598, 2013
31. Silverman, J.H.: The arithmetic of elliptic curves. Volume 106 of Graduate Texts in Mathematics, Springer (1986)
32. Scheunert, M.: Generalized Lie algebras. Journal of Mathematical Physics 20(4): 712-720, 1979
33. Rück, H.-G., and Frey, G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation 62 (206): 865–874, 1994
34. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theorey 56(1): 455–461, 2010